ยุทธศาสตร์การป้องกันไซเบอร์กระทรวงกลาโหม

โดย

พลตรี สุทธิศักดิ์ สลักคำ

รองเจ้ากรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม

สำนักงานปลัดกระทรวงกลาโหม

นักศึกษาวิทยาลัยป้องกันราชอาณาจักร

หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ ๕๗

ประจำปีการศึกษา พุทธศักราช ๒๕๕๗ -๒๕๕๘

บทคัดย่อ

เรื่อง ยุทธศาสตร์การป้องกันไซเบอร์กระทรวงกลาโหม

ลักษณะวิชา ยุทธศาสตร์, การทหาร

ผู้วิจัย พลตรี สุทธิศักดิ์ สลักคำ **หลักสูตร** วปอ. **รุ่นที่** ๕๗

การวิจัยครั้งนี้ มีวัตถุประสงค์ในการศึกษาภัยคุกคามไซเบอร์ ที่มีผลกระทบต่อความมั่นคงของชาติ โดยศึกษาการรับมือของต่างประเทศและประเทศไทย นำมาวิเคราะห์สังเคราะห์และกำหนดเป็นยุทธศาสตร์การป้องกันไซเบอร์กระทรวงกลาโหม ขอบเขตของการวิจัย เป็นการศึกษาจากข้อมูลข่าวสารที่เปิดเผยทางอินเทอร์เน็ต หรือเอกสารที่เผยแพร่สู่สาธารณะ มุ่งเน้นศึกษาหน่วยงานภาครัฐที่เกี่ยวข้องกับไซเบอร์ เป็นการวิจัยเชิงคุณภาพ ผลการศึกษาพบว่าภัยคุกคามไซเบอร์มีวิธีการที่หลากหลายทำให้เกิดความเสียหายต่อบุคคล องค์กร สังคม เศรษฐกิจ และกระทบต่อความมั่นคงของชาติในที่สุด ประเทศต่าง ๆ ที่ใช้เทคโนโลยีสารสนเทศเป็นเครื่องมือหลักในการขับเคลื่อนเศรษฐกิจ และความมั่นคงต่างก็ได้รับผลกระทบอย่างมากในทุก ๆ ด้าน ซึ่งประเทศเหล่านี้ได้ดำเนินการรับมือกับภัยคุกคามไซเบอร์อย่างจริงจัง มีการกำหนดนโยบายและยุทธศาสตร์ชัดเจน มีการจัดตั้งหน่วยงานรับผิดชอบหลักในการดำเนินการด้านไซเบอร์ที่เข้มแข็งชัดเจน ในประเทศไทยพึ่งมีการจัดตั้งคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติขึ้น สำหรับกระทรวงกลาโหม แต่ละหน่วยขึ้นตรงกระทรวงกลาโหมและเหล่าทัพมีการจัดตั้งหน่วยงานรับผิดชอบด้านไซเบอร์เพื่อปกป้องเครือข่ายของตนเอง ปัจจุบันกระทรวงกลาโหมยังขาดนโยบายและยุทธศาสตร์และหน่วยงานรับผิดชอบที่ชัดเจน การดำเนินการด้านไซเบอร์ยังไม่มีเอกภาพ ขาดแคลนเทคโนโลยีและผู้เชี่ยวชาญ ผลการวิจัยครั้งนี้สามารถกำหนดยุทธศาสตร์การป้องกันไซเบอร์กระทรวงกลาโหมได้ ๔ ยุทธศาสตร์ คือ การเสริมสร้างศักยภาพด้านไซเบอร์ของกระทรวงกลาโหม การป้องกันไซเบอร์ การป้องกันไซเบอร์เชิงรุก และการผนึกกำลังด้านไซเบอร์ โดยมีข้อเสนอแนะที่สำคัญคือ ควรจัดให้มีศูนย์บัญชาการไซเบอร์กระทรวงกลาโหม เพื่อเป็นหน่วยรับผิดชอบหลักในระดับนโยบายและยุทธศาสตร์ และจัดให้มีศูนย์ปฏิบัติการไซเบอร์ของกองบัญชาการกองทัพไทยและเหล่าทัพรับผิดชอบการปฏิบัติการไซเบอร์ และกระทรวงกลาโหมควรกำหนดนโยบายและยุทธศาสตร์ที่ชัดเจนให้สอดคล้องกับนโยบายไซเบอร์ในระดับชาติ เพื่อเกื้อกูลต่อการดำเนินงานด้านไซเบอร์ของประเทศไทย ให้มีความมั่นคงปลอดภัย เพื่อนำประเทศไทยไปสู่ความมั่นคง มั่งคั่ง ยั่งยืน

คำนำ

ประเทศไทยมุ่งมั่นที่จะก้าวเข้าสู่ยุคเศรษฐกิจและสังคมดิจิทัลอย่างสมบูรณ์ เพื่อทำให้ประเทศไทยมีความมั่นคง มั่งคั่ง ยั่งยืน ด้วยเหตุนี้ ไซเบอร์จึงเป็นเครื่องมือหลักอันสำคัญที่จำเป็นในการขับเคลื่อนเศรษฐกิจและสังคมดิจิทัล โดยไซเบอร์จะต้องมีความปลอดภัยพร้อมใช้งาน เชื่อถือได้ และมีการรักษาความลับที่ดี จึงจะทำให้เศรษฐกิจและสังคมดิจิทัลเจริญรุ่งเรือง ประสบความสำเร็จได้อย่างรวดเร็ว และได้รับการยอมรับจากนานาประเทศ ด้วยความจำเป็นที่ต้องใช้ไซเบอร์เป็นเครื่องมือหลักในการทำให้เกิดประโยชน์ แต่ขณะเดียวกันก็มีภัยคุกคามไซเบอร์เกิดขึ้นตามมาด้วยอย่างหลีกเลี่ยงไม่ได้ ซึ่งจะส่งผลกระทบต่อเศรษฐกิจและสังคมดิจิทัลอย่างแน่นอนหากไม่สามารถรักษาความมั่นคงปลอดภัยไซเบอร์ไว้ให้ได้ ผลกระทบอาจจะทำให้เศรษฐกิจและสังคมดิจิทัลถูกรบกวนขัดขวาง หรือถูกทำลายถึงขั้นหยุดชะงักได้ สำหรับกระทรวงกลาโหมกำลังก้าวเข้าสู่ยุคการปฏิบัติการที่มีเครือข่ายเป็นศูนย์กลาง ซึ่งจำเป็นต้องพึ่งพาไซเบอร์เป็นเครื่องมือหลักเครื่องมือหนึ่งเช่นเดียวกัน ย่อมไม่สามารถหลีกเลี่ยงภัยคุกคามไซเบอร์ ที่มีความซับซ้อนและพัฒนาไปอย่างรวดเร็วไม่หยุดยั้งได้ ประเทศไทยโดยเฉพาะกระทรวงกลาโหมจะต้องพิจารณาว่าไซเบอร์เป็นพื้นที่ปฏิบัติการ (Domain) หนึ่งเช่นเดียวกับ ทางบก ทางทะเล ทางอากาศ และทางอวกาศ จำเป็นต้องมีการเตรียมการป้องกันไว้ล่วงหน้าเป็นอย่างดี เนื่องจากบุคลากรด้านไซเบอร์ที่มีความรู้ความเชี่ยวชาญนั้นจัดหาได้ยาก ต้องใช้เวลาในการพัฒนาและฝึกฝนอย่างต่อเนื่อง จึงจะสามารถปฏิบัติการไซเบอร์ต่าง ๆ ได้ ด้วยการที่ไซเบอร์ถือว่าเป็นพื้นที่ปฏิบัติการหนึ่ง จึงสามารถมีการปฏิบัติการเช่นเดียวกับพื้นที่ปฏิบัติการอื่น ๆ ดังนั้น การวิจัยครั้งนี้จึงมุ่งไปสู่การจัดทำยุทธศาสตร์การป้องกันไซเบอร์กระทรวงกลาโหม ในลักษณะยุทธศาสตร์การป้องกันประเทศกระทรวงกลาโหม เพื่อเป็นการเตรียมกำลัง เตรียมการใช้กำลังเมื่อจำเป็น และเป็นการป้องกันประเทศให้ปลอดภัยรอดพ้นจากภัยคุกคามไซเบอร์ที่จะมีต่อประเทศไทยในที่สุด

พลตรี

(สุทธิศักดิ์ สลักคำ)

นักศึกษาวิทยาลัยป้องกันราชอาณาจักร

หลักสูตร วปอ. รุ่นที่ ๕๗

ผู้วิจัย

สารบัญ

	หน้า
บทคัดย่อ	**ก**
คำนำ	**ข**
กิตติกรรมประกาศ	**ค**
สารบัญ	**ง**
สารบัญตาราง	**จ**
สารบัญแผนภาพ	**ฉ**
คำอธิบายคำย่อ	**ช**
บทที่ ๑ บทนำ	
ความเป็นมาและความสำคัญของปัญหา	๑
วัตถุประสงค์ของการวิจัย	๓
ขอบเขตของการวิจัย	๓
วิธีดำเนินการวิจัย	๓
ประโยชน์ที่ได้รับจากการวิจัย	๔
คำจำกัดความ	๔
บทที่ ๒ ทบทวนสาระสำคัญของนโยบายความมั่นคงปลอดภัยแห่งชาติ และนโยบายที่เกี่ยวข้อง	๕
ผลประโยชน์แห่งชาติ	๕
(ร่าง)นโยบายความมั่นคงแห่งชาติ พ.ศ.๒๕๕๘ – ๒๕๖๒	๖
คำแถลงนโยบายคณะรัฐมนตรีต่อสภานิติบัญญัติแห่งชาติ	๑๐
กรอบนโยบายความมั่นคงปลอดภัยไซเบอร์แห่งชาติ	๑๑
กฎหมายที่เกี่ยวข้องกับไซเบอร์	๑๒
อำนาจหน้าที่ของกระทรวงกลาโหม	๑๓
ยุทธศาสตร์การป้องกันประเทศกระทรวงกลาโหม พ.ศ.๒๕๕๕	๑๔
สรุป	๑๔

สารบัญ (ต่อ)

	หน้า
บทที่ ๓ ศึกษาการรับมือภัยคุกคามจากไซเบอร์	**๑๕**
ศึกษาภัยคุกคามไซเบอร์ทั่วโลกและการรับมือ	๑๕
ศึกษาหน่วยงานด้านไซเบอร์ของต่างประเทศ	๒๔
ศึกษาหน่วยงานด้านไซเบอร์ในประเทศไทย	๓๒
หน่วยงานด้านไซเบอร์ในกระทรวงกลาโหมและหน่วยงานที่เกี่ยวข้อง	๓๒
สรุป	๓๓
บทที่ ๔ วิเคราะห์เพื่อกำหนดยุทธศาสตร์การป้องกันไซเบอร์กระทรวงกลาโหม	**๓๖**
การป้องกันไซเบอร์ของต่างประเทศ	๓๖
วิเคราะห์ประเด็นสำคัญจากการป้องกันไซเบอร์ของต่างประเทศ	๔๙
วิเคราะห์ลักษณะภัยคุกคามจากสงครามไซเบอร์ของต่างประเทศ	๕๐
วิเคราะห์ภัยคุกคามไซเบอร์ที่มีผลกระทบต่อความมั่นคงของชาติ	๕๑
วิเคราะห์การป้องกันไซเบอร์ของประเทศไทย	๕๒
วิเคราะห์ปัญหาการป้องกันไซเบอร์ของกระทรวงกลาโหม	๕๓
แนวทางการจัดทำยุทธศาสตร์การป้องกันไซเบอร์กระทรวงกลาโหม	๕๓
การกำหนดวัตถุประสงค์และยุทธศาสตร์การป้องกันไซเบอร์กระทรวงกลาโหม	๕๖
การกำหนดยุทธศาสตร์การป้องกันไซเบอร์กระทรวงกลาโหม	๕๖
ยุทธศาสตร์การป้องกันไซเบอร์กระทรวงกลาโหม	๕๘
แนวความคิดทางยุทธศาสตร์การป้องกันไซเบอร์กระทรวงกลาโหม	๕๘
สรุป	๖๒
บทที่ ๕ สรุปและข้อเสนอแนะ	**๖๔**
สรุปสถานการณ์และความพร้อมของกระทรวงกลาโหมด้านไซเบอร์	๖๔
ข้อเสนอแนะ	๖๕
บรรณานุกรม	
ภาคผนวก	
ประวัติย่อผู้วิจัย	

สารบัญตาราง

หน้า

ตารางที่

๔ - ๑ ประเด็นสำคัญการป้องกันไซเบอร์ของต่างประเทศ ๕๐

สารบัญแผนภาพ

หน้า

แผนภาพที่

๓ – ๑ Israel Defense Forces ๒๔

๓ – ๒ Emblem of the Shabak ๒๔

๓ – ๓ Iranian Cyber Army ๒๕

๓ – ๔ Ashiyane ๒๕

๓ – ๕ Iranian Cyber Police ๒๕

๔ – ๑ องค์ประกอบสามด้านในการจัดทำยุทธศาสตร์ ๕๔

๔ – ๒ กรอบแนวคิดการบริหารจัดการศักยภาพ
ด้านไซเบอร์ของกองทัพสหรัฐอเมริกา ๕๔

๔ – ๓ ปัจจัยอื่น ๆ ในการพิจารณากำหนดยุทธศาสตร์ไซเบอร์กระทรวงกลาโหม ๕๖

๕ – ๑ ร่างศูนย์บัญชาการไซเบอร์กระทรวงกลาโหม ๖๙

บทที่ ๑
บทนำ

ความเป็นมาและความสำคัญของปัญหา

แนวนโยบายด้านความมั่นคงของรัฐที่เกี่ยวข้องกับทางทหารตามรัฐธรรมนูญ พ.ศ.๒๕๕๐ กำหนดไว้ใน มาตรา ๗๗ ว่า “รัฐต้องพิทักษ์รักษาไว้ซึ่งสถาบันพระมหากษัตริย์ เอกราช อธิปไตย และบูรณภาพแห่งเขตอำนาจรัฐ และต้องจัดให้มีกำลังทหาร อาวุธยุทโธปกรณ์ และเทคโนโลยีที่ทันสมัย ที่จำเป็น และเพียงพอ เพื่อพิทักษ์รักษาเอกราช อธิปไตย ความมั่นคงของรัฐ สถาบันพระมหากษัตริย์ ผลประโยชน์แห่งชาติ และการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข และเพื่อการพัฒนาประเทศ” การมีเอกราช อธิปไตย บูรณภาพแห่งเขตอำนาจรัฐ การดำรงอยู่อย่างมั่นคงของชาติ และความอยู่ดีมีสุข ปลอดภัย มีศักดิ์ศรี มีอิสระเสรีในการดำเนินชีวิตของประชาชน ถือเป็นความปรารถนาสูงสุดและเป็นสิ่งบ่งชี้ความมั่นคงของชาติ แต่หากพิจารณาถึงปัจจัยหลักที่ประกอบกันและส่งผลต่อความมั่นคงของชาตินั้น เป็นที่ยอมรับในสากลว่า พลังอำนาจแห่งชาติ คือปัจจัยหลักนั้น เป็นสิ่งบ่งชี้ถึงความมั่นคง เข้มแข็ง การพัฒนา และความสงบเรียบร้อยในชาติ โดยแต่ละองค์ประกอบของพลังอำนาจแห่งชาตินั้นล้วนมีความเกี่ยวเนื่องและมีผลกระทบซึ่งกันและกัน ถ้าพิจารณาในภาพรวม พลังอำนาจแห่งชาติโดยทั่วไปอาจประกอบด้วย Diplomatic, Informational, Military และ Economic หรือบางประเทศอาจพิจารณาเพิ่มเติมแตกต่างกันบ้างในรายละเอียด เช่น Political, Military, Economic, Social, Infrastructure และ Information Systems เป็นต้น ประเทศไทยมีหลักการพิจารณาองค์ประกอบของพลังอำนาจแห่งชาติคล้ายคลึงกัน แต่ไม่ว่าจะพิจารณาในลักษณะใด องค์ประกอบที่ได้รับการพิจารณาเป็นปัจจัยหลักที่เหมือนกันคือ สารสนเทศ (Information) ซึ่งหากพิจารณาแก่นสาระสำคัญอย่างสอดคล้องกับสภาพการณ์ของภัยคุกคามต่อความมั่นคงของชาติในปัจจุบันและแนวโน้มในอนาคตแล้วนั้น สามารถพูดได้ว่าสารสนเทศคือไซเบอร์นั่นเอง เนื่องจากปัจจุบันการใช้สารสนเทศมีการเชื่อมต่อออนไลน์โยงใยกันอย่างกว้างขวาง มีการใช้ประโยชน์ตั้งแต่การใช้ในชีวิตประจำวัน การใช้ในการทำงาน การใช้ควบคุมอุปกรณ์ การใช้ควบคุมโรงงาน การใช้ควบคุมโครงสร้างพื้นฐาน ซึ่งเป็นปัจจัยสำคัญของเศรษฐกิจ ไปจนถึงการใช้ในระบบควบคุมบังคับบัญชาของกองทัพ (C^4I) ต่างก็พึ่งพาและใช้สารสนเทศที่มีการเชื่อมต่อออนไลน์แทบทั้งสิ้น การเชื่อมต่อสารสนเทศออนไลน์โยงใยกันอย่างกว้างขวางนี่เอง คือคุณสมบัติของไซเบอร์ จึงมีความจำเป็นอยู่เองที่ระบบเหล่านี้จะต้องได้รับการปกป้องให้พ้นจากภัยคุกคามต่าง ๆ

ทางการทหาร กองทัพที่ทันสมัยในปัจจุบัน ถือว่าไซเบอร์เป็นโดเมนหรือพื้นที่ปฏิบัติการหนึ่ง เช่นเดียวกับพื้นที่ปฏิบัติการ ทางพื้นดิน ทางทะเล ทางอากาศ และทางอวกาศ ที่มีการปฏิบัติการต่าง ๆ ในไซเบอร์ตั้งแต่ยามปกติจนถึงภาวะวิกฤติและภาวะสงคราม

ศักยภาพด้านไซเบอร์ได้กลายเป็นเครื่องมือสำคัญอันดับต้นๆ ที่มีการนำมาใช้ในสถานการณ์ที่มีผลกระทบต่อความมั่นคงของชาติในทุกภูมิภาคทั่วโลก เป็นเครื่องมือที่คู่กรณีพิพาทใช้ในการโจมตีฝ่ายตรงข้าม โดยเฉพาะอย่างยิ่งกับคู่กรณีที่มีศักยภาพทางทหารสูงกว่า นอกจากการนำมาใช้ในทางทหารแล้ว ไซเบอร์ยังเป็นองค์ประกอบที่สำคัญของโครงสร้างพื้นฐานของระบบสาธารณูปโภคพื้นฐานที่ให้บริการประชาชน ให้สามารถดำรงชีวิตประจำวันได้โดยปกติสุข เช่น ไฟฟ้า ประปา ขนส่ง สื่อสาร ธนาคาร รวมถึงส่งผลกระทบโดยตรงต่อเศรษฐกิจ เช่น กระบวนการผลิต ตลาดหลักทรัพย์ ธุรกิจอีคอมเมิร์ซ เป็นต้น ในปัจจุบันประเทศไทยได้ตระหนักถึงภัยคุกคามจากไซเบอร์ที่มีผลกระทบต่อความมั่นคงของชาติ ดังจะเห็นได้จากการกำหนดไว้ในนโยบายความมั่นคงแห่งชาติ ๒๕๕๕ – ๒๕๕๙ ในประเด็นนโยบายที่ ๑ เสริมสร้างเสถียรภาพและภูมิคุ้มกันความมั่นคงและการจัดการภัยคุกคาม และประเด็นนโยบายที่ ๒ เสริมสร้างและพัฒนาศักยภาพการป้องกันประเทศ อีกทั้งมีการดำเนินการที่สำคัญด้านนโยบายความมั่นคงปลอดภัยไซเบอร์ระดับชาติ ได้แก่ การจัดตั้งคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ซึ่งมีนายกรัฐมนตรีเป็นประธาน มีผู้แทนจากหน่วยงานด้านเศรษฐกิจและคุณภาพชีวิต หน่วยงานด้านป้องกันและปราบปรามการกระทำผิด และหน่วยงานความมั่นคงและกระทรวงกลาโหม ได้แก่ รัฐมนตรีว่าการกระทรวงกลาโหม และปลัดกระทรวงกลาโหมร่วมเป็นกรรมการ คณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้ประชุมเมื่อวันที่ ๑๑ มิถุนายน ๒๕๕๖ ณ ตึกไทยคู่ฟ้า ทำเนียบรัฐบาล และมีมติเห็นชอบกรอบนโยบายความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อเป็นแนวทางการดำเนินการด้านไซเบอร์ของประเทศ แต่ด้วยขอบเขตและวัตถุประสงค์ของกรอบนโยบายดังกล่าว ที่มุ่งให้หน่วยงานมีการดำเนินการและการพัฒนาด้านไซเบอร์อย่างเป็นระบบและเป็นแนวทางเดียวกัน จึงมิได้กำหนดกรอบแนวทางการผสานศักยภาพด้านไซเบอร์ระดับชาติสำหรับภารกิจการรักษาความมั่นคงของชาติ โดยเฉพาะในภาวะวิกฤติ ภัยพิบัติจากไซเบอร์ และสงคราม ไซเบอร์ ดังนั้น ยุทธศาสตร์การป้องกันไซเบอร์กระทรวงกลาโหมจึงมีความสำคัญยิ่งเพื่อเป็นแนวทางการผสานศักยภาพด้านไซเบอร์ของส่วนราชการในกระทรวงกลาโหมประสานเข้ากับส่วนราชการด้านความมั่นคงและหน่วยงานที่เกี่ยวข้องอื่น ๆ ให้มีความเข้มแข็ง มีประสิทธิภาพ เพียงพอ และเกื้อกูลซึ่งกันและกันอย่างเหมาะสม สามารถใช้เป็นกรอบเพื่อแปลงไปสู่การกำหนดภารกิจการป้องกันไซเบอร์ของกระทรวงกลาโหมและหน่วยงานที่เกี่ยวข้อง ให้สามารถรับมือกับภัยคุกคามไซเบอร์ ที่นับวันยิ่งทวีความรุนแรง ซับซ้อน ส่งผลกระทบอย่างรวดเร็วเป็นวงกว้างต่อการดำรงชีวิตโดยปกติสุขของประชาชน และส่งผลกระทบต่อความมั่นคงของชาติในที่สุด จึงเป็นความสำคัญที่จะต้องศึกษาถึงภัยคุกคามจากไซเบอร์ที่มีต่อประเทศไทย และหน่วยงานที่เกี่ยวข้อง โดยเฉพาะกระทรวงกลาโหมในฐานะหน่วยงานด้านความมั่นคงจะต้องมียุทธศาสตร์เพื่อใช้ในการป้องกันไซเบอร์ของประเทศให้สามารถใช้งานได้อย่างมีประสิทธิภาพ รวมถึงพร้อมรับมือกับภาวะวิกฤติและภัยพิบัติจากไซเบอร์ที่อาจจะเกิดขึ้น

วัตถุประสงค์ของการวิจัย

๑. เพื่อศึกษาภัยคุกคามจากไซเบอร์ที่มีผลกระทบต่อความมั่นคงของชาติ ในส่วนที่เกี่ยวข้องกับกระทรวงกลาโหมในฐานะของหน่วยงานด้านความมั่นคง เช่น อาชญากรรมทางไซเบอร์ สงคราม ไซเบอร์ การโจมตี การจารกรรม การก่อวินาศกรรม การก่อการร้ายทางไซเบอร์ และการปฏิบัติการข่าวสาร (Information Operations - IO) ในไซเบอร์ที่กระทบต่อความมั่นคงของชาติ เป็นต้น

๒. เพื่อศึกษาการป้องกันไซเบอร์ การรับมือและการเตรียมการรับมือกับภัยคุกคามจากไซเบอร์ของประเทศต่าง ๆ ที่มีศักยภาพ โดยเฉพาะประเทศที่เคยได้รับผลกระทบจากภัยคุกคามไซเบอร์ รวมถึง การป้องกันไซเบอร์ การรับมือ และการเตรียมการรับมือของประเทศไทย

๓. เสนอแนะยุทธศาสตร์การป้องกันไซเบอร์กระทรวงกลาโหม เพื่อใช้เป็นกรอบการดำเนินการและเสริมสร้างศักยภาพด้านการป้องกันไซเบอร์ของกระทรวงกลาโหม ในการรับมือภัยคุกคามจากไซเบอร์

ขอบเขตของการวิจัย

๑. การวิจัยจำกัดขอบเขตเฉพาะ ข้อมูลข่าวสารที่เปิดเผยทางอินเทอร์เน็ต หรือเอกสารที่เผยแพร่โดยทั่วไปของต่างประเทศและประเทศไทย และหลีกเลี่ยงการกล่าวถึง ข้อมูลที่จะเป็นการล่วงละเมิดความลับของทางราชการ

๒. มุ่งเน้นศึกษาส่วนราชการในกระทรวงกลาโหม หน่วยงานภาครัฐ ที่เกี่ยวข้องกับไซเบอร์และมีผลกระทบต่อความมั่นคงของชาติ หากเกิดภาวะวิกฤติ สงครามไซเบอร์ และภัยพิบัติจากไซเบอร์

วิธีดำเนินการวิจัย

การวิจัยนี้เป็นการวิจัยเชิงคุณภาพ โดยศึกษาและวิเคราะห์จากข้อมูลข่าวสารที่เปิดเผยทางอินเทอร์เน็ตหรือเอกสารที่เผยแพร่โดยทั่วไป นโยบายระดับชาติของไทยและต่างประเทศ ในด้านการรับมือกับภัยคุกคามจากไซเบอร์ รวมทั้งพิจารณาจากภารกิจหรือพันธกิจ จุดศูนย์ดุลและจุดล่อแหลม ความเสี่ยง และศักยภาพด้านไซเบอร์ของหน่วยงานที่เกี่ยวข้องกับความมั่นคงของชาติ เพื่อวิเคราะห์และกำหนดยุทธศาสตร์การป้องกันไซเบอร์กระทรวงกลาโหม

ประโยชน์ที่ได้รับจากการวิจัย

๑. ได้รับทราบถึงภัยคุกคามจากไซเบอร์ที่มีผลกระทบต่อความมั่นคงของชาติ และผลเสียหายที่จะเกิดขึ้น เพื่อให้รู้เขา

๒. ได้รับทราบแนวทางการรับมือกับภัยคุกคามจากไซเบอร์ของประเทศต่าง ๆ และของประเทศไทย โดยเฉพาะในกระทรวงกลาโหมในปัจจุบัน เพื่อให้รู้มิตร และ รู้เรา

๓. ได้ข้อเสนอแนะยุทธศาสตร์การป้องกันไซเบอร์กระทรวงกลาโหม ที่จะผสานและเสริมสร้างศักยภาพด้านไซเบอร์ของกระทรวงกลาโหม และหน่วยงานที่เกี่ยวข้อง เพื่อทำให้เกิดความมั่นคงของชาติด้านไซเบอร์

คำจำกัดความ

ไซเบอร์ หมายถึง กิจกรรมการเชื่อมโยงเครือข่ายดิจิทัล ทุกรูปแบบ ซึ่งรวมถึง เนื้อหา และ การทำงานทุกอย่างที่เกิดขึ้นผ่านเครือข่ายดิจิทัล

ดิจิทัล หมายถึง วิธีแทนความหมายของข้อมูลหรือชิ้นงานต่างๆในรูปแบบของตัวเลข เป็นเลขฐานสอง คือ เลข 0 กับ 1 ที่ไม่ต่อเนื่องกัน ซึ่งต่างจากแอนะล็อกที่ใช้ค่าต่อเนื่อง

เครือข่าย หมายถึง กลุ่มของคอมพิวเตอร์และอุปกรณ์ต่างๆ ที่ถูกนำมาเชื่อมต่อกันเพื่อให้ผู้ใช้ในเครือข่ายสามารถติดต่อสื่อสาร แลกเปลี่ยนข้อมูล และใช้อุปกรณ์ต่างๆ ในเครือข่ายร่วมกันได้

บทที่ ๒

ทบทวนสาระสำคัญของนโยบายความมั่นคงปลอดภัยแห่งชาติ และนโยบายที่เกี่ยวข้องกับไซเบอร์

ประเทศไทยได้มีการกำหนดผลประโยชน์แห่งชาติไว้ในนโยบายความมั่นคงแห่งชาติ ซึ่งกระทรวงกลาโหมได้ยึดถือเป็นกรอบในการดำเนินการให้บรรลุซึ่งผลประโยชน์แห่งชาติ โดยปฏิบัติตามอำนาจหน้าที่ที่ได้มีการกำหนดไว้ในกฎหมายที่เกี่ยวข้อง งานด้านหนึ่งที่กระทรวงกลาโหมต้องดำเนินการคืองานด้านไซเบอร์ ที่จะต้องดำเนินการให้สอดคล้องกับนโยบายความมั่นคงแห่งชาติ นโยบายการเตรียมความพร้อมแห่งชาติ นโยบายของรัฐบาลที่เกี่ยวข้อง ซึ่งได้สรุปรวบรวมไว้ดังต่อไปนี้

ผลประโยชน์แห่งชาติ

(ร่าง)นโยบายความมั่นคงแห่งชาติ พ.ศ.๒๕๕๘ – ๒๕๖๒ ได้กำหนดผลประโยชน์แห่งชาติดังนี้

๑. การมีเอกราช อธิปไตย และบูรณภาพแห่งเขตอำนาจรัฐ

๒. การดำรงอยู่อย่างมั่นคง ยั่งยืน ของสถาบันหลักของชาติ

๓. การดำรงอยู่อย่างมั่นคงของชาติและประชาชนจาก การคุกคามทุกรูปแบบ

๔. การอยู่ร่วมกันอย่างสันติสุข มีความเป็นปึกแผ่นมั่นคงทางสังคม ท่ามกลางความแตกต่างหลากหลาย

๕. ความเจริญเติบโตมั่นคงทางเศรษฐกิจของชาติ ความเป็นธรรม และความอยู่ดีมีสุขของประชาชน การมีเกียรติและศักดิ์ศรีของความเป็นมนุษย์

๖. ความยั่งยืนของฐานทรัพยากรธรรมชาติ สิ่งแวดล้อม ความมั่นคงทางพลังงาน อาหารและน้ำ

๗. ความสามารถในการรักษาผลประโยชน์ของชาติ ภายใต้การเปลี่ยนแปลงของสภาวะแวดล้อมระหว่างประเทศ

๘. การอยู่ร่วมกันอย่างสันติ ประสานสอดคล้องกับด้านความมั่นคงในประชาคมอาเซียนและประชาคมโลกอย่างมีเกียรติและศักดิ์ศรี

(ร่าง)นโยบายความมั่นคงแห่งชาติ พ.ศ.๒๕๕๘ – ๒๕๖๒

เป็นนโยบายระดับชาติที่กำหนดกรอบทิศทางหลักในการดำเนินการด้านความมั่นคง เพื่อให้ภาครัฐและภาคส่วนต่างๆ ในสังคม นำไปเป็นกรอบแนวทางดำเนินการในขอบเขตและภารกิจที่เกี่ยวข้อง เพื่อให้สามารถสนองผลประโยชน์แห่งชาติและการรักษาความมั่นคงของประเทศได้อย่างประสานสอดคล้องและเป็นเอกภาพ

วิสัยทัศน์

"ชาติมีเสถียรภาพและเป็นปึกแผ่น ประชาชนมีความมั่นคงในชีวิต ประเทศมีการพัฒนาอย่างต่อเนื่อง ปลอดภัยจากภัยคุกคามข้ามพรมแดน พร้อมเผชิญวิกฤติการณ์ มีบทบาทเชิงรุกในประชาคมอาเซียนและดำเนินความสัมพันธ์กับนานาประเทศอย่างมีดุลยภาพ"

นโยบายฉบับนี้ได้จัดลำดับความสำคัญเพื่อการขับเคลื่อนนโยบายอย่างมีทิศทางที่ชัดเจน โดยกำหนดนโยบายเป็น ๒ ส่วน คือ

ส่วนที่ ๑ นโยบายเสริมสร้างความมั่นคงที่เป็นแก่นหลักของชาติ

นโยบายที่ ๑ เสริมสร้างความมั่นคงของสถาบันหลักของชาติ และการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข

๑. เสริมสร้างความรู้ ความเข้าใจที่ถูกต้องเกี่ยวกับสถาบันชาติ ศาสนา พระมหากษัตริย์

๒. พัฒนาประสิทธิภาพ และความเข้มแข็งของกลไก ที่เกี่ยวข้องกับการป้องกันและป้องปราม การล่วงละเมิดสถาบัน

๓. เผยแพร่และน้อมนำแนวพระราชดำริไปปฏิบัติอย่างเป็นรูปธรรม

๔. เสริมสร้างความเข้มแข็งของการปกครองในระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข

นโยบายที่ ๒ สร้างความเป็นธรรม ความปรองดอง และความสมานฉันท์ในชาติ

๑. ปฏิรูปกลไกการบริหารประเทศทุกระดับ

๒. สร้างความเชื่อมั่นต่อกลไกและกระบวนการยุติธรรม

๓. แก้ไขปัญหาความไม่เป็นธรรมในการถือครองที่ดิน

๔. ส่งเสริมให้ประชาชนเกิดความรู้สึกเป็นส่วนหนึ่งของชาติ อยู่ร่วมกันอย่างสันติสุข มีความรักความภาคภูมิใจในความเป็นชาติไทยและเป็นสังคมพหุวัฒนธรรมที่เข้มแข็ง

๕. สนับสนุนและส่งเสริมการมีส่วนร่วมทางสังคม เศรษฐกิจ และการเมืองของทุกภาคส่วน

นโยบายที่ ๓ ป้องกันและแก้ไขการก่อความไม่สงบในจังหวัดชายแดนภาคใต้

๑. เสริมสร้างสภาวะแวดล้อมที่สันติสุข

๒. ฟื้นฟูความเชื่อมั่นและลดความหวาดระแวงระหว่างประชาชนกับรัฐ

๓. เสริมสร้างสันติสุขและการพัฒนาอย่างยั่งยืนโดยใช้กระบวนการมีส่วนร่วมของทุกภาคส่วนเป็นพลังในการเข้าถึงประชาชน

๔. ส่งเสริมความต่อเนื่องของกระบวนการพูดคุยเพื่อสันติสุข

๕. สร้างความเข้าใจต่อสถานการณ์ความเป็นจริงที่เกิดขึ้น ต่อสังคมทั้งภายในประเทศและภายนอกประเทศ

๖. จัดให้มีกลไกและโครงสร้างการบริหารจัดการของภาครัฐที่มีเอกภาพ

ส่วนที่ ๒ นโยบายความมั่นคงแห่งชาติทั่วไป

นโยบายที่ ๔ จัดระบบการบริหารจัดการชายแดนเพื่อป้องกันและแก้ไขปัญหาข้ามพรมแดน

๑. เสริมสร้างความเป็นหุ้นส่วนทางยุทธศาสตร์ด้านความมั่นคง

๒. ปรับปรุงกลไก และพัฒนาศักยภาพการตรวจคนเข้าเมือง

๓. ส่งเสริมการใช้มิติทางสังคมและวัฒนธรรม ในการเสริมสร้างความสัมพันธ์อันดีทุกระดับกับประเทศเพื่อนบ้าน

๔. จัดระเบียบการพัฒนาพื้นที่ชายแดนให้มีศักยภาพทางด้านเศรษฐกิจ และการเป็นประตูเชื่อมโยงการค้า ที่มีความสมดุลทั้งในมิติเศรษฐกิจและสังคมกับมิติความมั่นคง

นโยบายที่ ๕ สร้างเสริมศักยภาพการป้องกันและแก้ไขปัญหาภัยคุกคามข้ามชาติ

๑. พัฒนาระบบ กลไก และมาตรการที่เข้มแข็ง ในการป้องกันและแก้ไขปัญหาการก่อการร้าย และอาชญากรรมข้ามชาติ

๒. ดำเนินการป้องกันและแก้ไขปัญหาการก่อการร้ายทุกรูปแบบ

๓. เสริมสร้างและพัฒนาความร่วมมือระหว่างประเทศทุกระดับ

๔. เสริมสร้างจิตสำนึกความตระหนักของภาคเอกชน ภาคประชาชนและภาคประชาสังคม

นโยบายที่ ๖ ปกป้อง รักษาผลประโยชน์แห่งชาติทางทะเล

๑. พัฒนาศักยภาพความมั่นคงแห่งชาติทางทะเล

๒. คุ้มครองการใช้ประโยชน์จากทะเล

๓. สร้างความสงบเรียบร้อยและส่งเสริมการใช้ประโยชน์จากทะเล

๔. สร้างความสมดุลและยั่งยืนของทรัพยากรและสิ่งแวดล้อมทางทะเล

๕. พัฒนาทรัพยากรมนุษย์ องค์ความรู้ และความตระหนักรู้ความสำคัญของทะเล

๖. พัฒนาการบริหารจัดการผลประโยชน์ของชาติทางทะเลขององค์กรของรัฐ

นโยบายที่ ๗ จัดระบบ ป้องกัน และแก้ไขปัญหาผู้หลบหนีเข้าเมือง

๑. กำหนดนโยบายต่อผู้หลบหนีเข้าเมือง

๒. แก้ไขปัญหาผู้หลบหนีเข้าเมืองที่ตกค้างและยังไม่สามารถส่งกลับประเทศต้นทาง

๓. จัดระเบียบการจ้างแรงงานต่างด้าวหลบหนีเข้าเมืองโดยคำนึงถึงการรักษาผลประโยชน์ทางด้านเศรษฐกิจที่สอดคล้องกับการรักษาความมั่นคงของชาติ

๔. ปรับปรุงกลไกและพัฒนาศักยภาพการบริหารจัดการเพื่อจัดระเบียบการเข้าเมือง

๕. พัฒนาระบบฐานข้อมูลคนเข้าเมืองและผู้หลบหนีเข้าเมืองให้มีความทันสมัย เป็นปัจจุบัน สามารถเชื่อมโยงระหว่างหน่วยงานที่เกี่ยวข้องอย่างมีประสิทธิภาพ

นโยบายที่ ๘ เสริมสร้างความเข้มแข็งและภูมิคุ้มกันความมั่นคงภายใน

๑. ปกป้องความมั่นคงของชาติจากภัยยาเสพติด

๓. เสริมสร้างความมั่นคงของชาติจากภัยการทุจริตคอร์รัปชั่น

๔. ผนึกกำลังทุกภาคส่วนให้พร้อมเผชิญปัญหาและภัยคุกคามความมั่นคง

นโยบายที่ ๙ เสริมสร้างความมั่นคงทางเทคโนโลยีสารสนเทศและไซเบอร์

๑. ปกป้อง ป้องกัน ภัยคุกคามด้านไซเบอร์ สงครามไซเบอร์ และเสริมสร้างความปลอดภัยระบบเทคโนโลยีสารสนเทศ

๒. พัฒนาการบังคับใช้กฎหมาย โดยการพัฒนาระเบียบและกฎหมายเพื่อความมั่นคงปลอดภัยไซเบอร์ และการพัฒนาเทคโนโลยีสำหรับงานสืบสวนและป้องกันอาชญากรรมไซเบอร์

๓. พัฒนาศักยภาพทางด้านเทคโนโลยีสารสนเทศและไซเบอร์

นโยบายที่ ๑๐ รักษาความมั่นคงของฐานทรัพยากรธรรมชาติ และสิ่งแวดล้อม

๑. พัฒนาระบบการใช้ทรัพยากรธรรมชาติอย่างสมดุลและยั่งยืน ระหว่างการอนุรักษ์และการพัฒนา

๒. เสริมสร้างกระบวนการมีส่วนร่วมของภาคประชาชน และท้องถิ่นในการบริหารจัดการ การตรวจสอบ และการเฝ้าระวังการแสวงประโยชน์จากทรัพยากรธรรมชาติโดยมิชอบ

๓. เสริมสร้างประสิทธิภาพการจัดการสิ่งแวดล้อม

๔. ส่งเสริมการรวมตัวในระดับภูมิภาคอาเซียน เพื่อเป็นภาคีด้านการรักษาทรัพยากรธรรมชาติ และสิ่งแวดล้อม

นโยบายที่ ๑๑ เสริมสร้างความมั่นคงทางพลังงานและอาหาร

๑. เพิ่มศักยภาพการบริหารจัดการพลังงานทั้งระบบ

๒. พัฒนาองค์ความรู้และแสวงหาแหล่งพลังงานทางเลือกที่เป็นมิตรต่อสิ่งแวดล้อม

๓. สร้างความตระหนักให้ทุกภาคส่วนสนับสนุนอย่างจริงจังในการดำเนินการตามกรอบยุทธศาสตร์การจัดการด้านอาหารของประเทศไทย

๔. ฟื้นฟูภาคเกษตรกรรมอันเป็นรากฐานความมั่นคงทางอาหารของไทย

นโยบายที่ ๑๒ พัฒนาระบบการเตรียมพร้อมแห่งชาติเพื่อเสริมสร้างความมั่นคงของชาติ

๑. พัฒนาระบบการเตรียมพร้อมแห่งชาติ ให้ประสานสอดคล้องระหว่างแผนระดับชาติ ระดับจังหวัด ระดับท้องถิ่น และระดับชุมชน

๒. จัดให้มีระบบสั่งการที่มีเอกภาพ

๓. ส่งเสริมและสนับสนุนการมีส่วนร่วมของทุกภาคส่วน

๔. พัฒนาและสนับสนุนการมีระบบฐานข้อมูลเฝ้าระวังและเตรียมพร้อม ด้านภัยพิบัติที่ทันสมัย

นโยบายที่ ๑๓ เสริมสร้างและพัฒนาศักยภาพการป้องกันประเทศ

๑. เสริมสร้างและพัฒนากองทัพให้มีโครงสร้างกำลังกองทัพ และยุทโธปกรณ์ที่เหมาะสม ทันสมัย

๒. เสริมสร้างและพัฒนาศักยภาพของชาติด้วยการผนึกกำลังจากทุกภาคส่วนในการป้องกันประเทศ และให้มีส่วนร่วมในการสนับสนุนการดำเนินงานของกองทัพตั้งแต่ในภาวะปกติ

๓. เสริมสร้างความสัมพันธ์อันดี และความร่วมมือในทุกระดับกับกองทัพประเทศเพื่อนบ้าน กลุ่มอาเซียน และมิตรประเทศ บนพื้นฐานการรักษาผลประโยชน์ร่วมกัน

๔. พัฒนาและนำศักยภาพของกองทัพในยามปกติเข้ามาสนับสนุนภารกิจนอกเหนือจากสงคราม

นโยบายที่ ๑๔ พัฒนาระบบงานข่าวกรองให้มีประสิทธิภาพ

๑. ดำเนินงานข่าวกรองที่มีคุณภาพและแจ้งเตือนภัยล่วงหน้าอย่างมีประสิทธิภาพ

๒. เสริมสร้างความร่วมมืออย่างเป็นเอกภาพในประชาคมข่าวกรอง และหน่วยงานภาครัฐ รวมทั้งหน่วยงานข่าวกรองต่างประเทศ และมีเครือข่ายด้านข้อมูลข่าวสารกับภาคเอกชนและประชาชน

๓. เสริมสร้างและพัฒนาขีดความสามารถของระบบงานข่าวกรองอย่างต่อเนื่อง โดยพัฒนาบุคลากรและเพิ่มศักยภาพของเทคโนโลยี ระบบฐานข้อมูลและองค์กรด้านการข่าว

นโยบายที่ ๑๕ เสริมสร้างดุลยภาพในการดำเนินความสัมพันธ์ระหว่างประเทศ

๑. เสริมสร้างความไว้เนื้อเชื่อใจและป้องกันความขัดแย้งกับประเทศเพื่อนบ้าน

๒. ส่งเสริมบรรยากาศที่นาไปสู่การสำรวจและจัดทำหลักเขตแดนและเส้นเขตแดนทางทะเลกับประเทศเพื่อนบ้านให้บรรลุผล

๓. ส่งเสริมการแลกเปลี่ยนเรียนรู้ทางวัฒนธรรมและความเป็นจริงทางประวัติศาสตร์ของภูมิภาค โดยเน้นที่ความเชื่อมโยงใกล้ชิดกันในมิติทางวัฒนธรรม และการอยู่ร่วมกันมาอย่างยาวนาน

๔. ส่งเสริมให้อาเซียนมีเอกภาพในการดำเนินความสัมพันธ์กับมหาอำนาจ และเป็นเครื่องมือสร้างดุลยภาพทางความสัมพันธ์ระหว่างไทยกับมหาอำนาจ

๕. สนับสนุนให้ประเทศสมาชิกอาเซียนร่วมมือกันอย่างเป็นรูปธรรมในการป้องกันและแก้ไขปัญหาภัยคุกคามรูปแบบใหม่

๖. ดำเนินการอย่างสมดุลในการปรับตัวให้สอดคล้องกับการที่อาเซียนเป็นองค์กรที่ปฏิบัติตามกฎหมายและกฎระเบียบอย่างเคร่งครัดมากขึ้น

๗. เสริมสร้างความพร้อมของประเทศในการจัดตั้งประชาคมการเมืองและความมั่นคงอาเซียน

๘. รักษาดุลยภาพในการดำเนินความสัมพันธ์กับนานาประเทศ โดยมีจุดยืนและท่าทีที่เหมาะสม

๙. เสริมสร้างปัจจัยที่เกื้อหนุนและสร้างสภาวะแวดล้อมที่ลดความหวาดระแวงควบคู่ไปกับการเสริมสร้างความไว้เนื้อเชื่อใจ

คำแถลงนโยบายคณะรัฐมนตรีต่อสภานิติบัญญัติแห่งชาติ

รัฐบาลได้กำหนดนโยบายจำแนกเป็น ๑๑ ด้าน ซึ่งได้นำยุทธศาสตร์การพัฒนาประเทศว่าด้วยการเข้าใจ เข้าถึง และพัฒนาตามแนวพระราชดำริของพระบาทสมเด็จพระเจ้าอยู่หัว เป็นหลักสำคัญ ใช้ปรัชญาของเศรษฐกิจพอเพียงซึ่งทรงเน้นความพอดีพอสมพอควรแก่ฐานะ ความมีเหตุมีผล และการมีภูมิคุ้มกันมาเป็นแนวคิด ใช้แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติฉบับที่ ๑๑ รวมทั้งแนวทางของคณะรักษาความสงบแห่งชาติ และความต้องการของประชาชน เป็นกรอบแนวคิดของนโยบาย โดยมีหัวข้อดังนี้

๑. การปกป้องและเชิดชูสถาบันพระมหากษัตริย์

๒. การรักษาความมั่นคงของรัฐและการต่างประเทศ

๓. การลดความเหลื่อมล้ำของสังคม และการสร้างโอกาสการเข้าถึงบริการของรัฐ

๔. การศึกษาและเรียนรู้ การทะนุบำรุงศาสนา ศิลปะและวัฒนธรรม

๕. การยกระดับคุณภาพบริการด้านสาธารณสุข และสุขภาพของประชาชน

๖. การเพิ่มศักยภาพทางเศรษฐกิจของประเทศ

๗. การส่งเสริมบทบาทและการใช้โอกาสในประชาคมอาเซียน

๘. การพัฒนาและส่งเสริมการใช้ประโยชน์จากวิทยาศาสตร์ เทคโนโลยี การวิจัยและพัฒนาและนวัตกรรม

๙. การรักษาความมั่นคงของฐานทรัพยากร และการสร้างสมดุลระหว่างการอนุรักษ์กับการใช้ประโยชน์อย่างยั่งยืน

๑๐. การส่งเสริมการบริหารราชการแผ่นดินที่มีธรรมาภิบาลและการป้องกันปราบปรามการทุจริตและประพฤติมิชอบในภาครัฐ

๑๑. การปรับปรุงกฎหมายและกระบวนการยุติธรรม

กรอบนโยบายความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

คำสั่งสำนักนายกรัฐมนตรีที่ ๗๖/๒๕๕๕ ลง ๑๙ มี.ค. ๕๕ เรื่อง แต่งตั้งคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Committee) เพื่อเป็นการปกป้อง ป้องกัน หรือรับมือกับสถานการณ์ด้านภัยคุกคาม หรือความเสี่ยงบนไซเบอร์ ที่ส่งผลกระทบต่อการให้บริการหรือการประยุกต์ใช้ข้อมูลคอมพิวเตอร์ เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต วิทยุกระจายเสียง วิทยุโทรทัศน์ และโครงข่ายโทรคมนาคม อันกระทบต่อความมั่นคงของชาติในมิติต่างๆได้อย่างเหมาะสม และมีความเป็นเอกภาพ อาศัยอำนาจตามความในมาตรา ๑๑ (๖) แห่งพระราชบัญญัติระเบียบราชการแผ่นดิน พ.ศ. ๒๕๓๔ ทั้งนี้ คณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ได้มีมติเห็นชอบกรอบนโยบายการรักษาความปลอดภัยไซเบอร์แห่งชาติ ดังนี้

วิสัยทัศน์ "ประเทศไทยมีความมั่นคงปลอดภัยด้านไซเบอร์เป็นที่เชื่อถือและยอมรับในระดับสากล"

๑. เป้าหมายหลัก

๑.๑ การบูรณาการการจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศสังคมมีวัฒนธรรมการตระหนักถึงความเสี่ยง (Risk-aware culture) จากการใช้งานบนโลกไซเบอร์และประชาชนมีความรู้และทักษะในการใช้ประโยชน์จากโลกไซเบอร์ได้อย่างมั่นคงปลอดภัย

๑.๒ มีการกำกับดูแลการใช้งานบนโลกไซเบอร์ให้มีความมั่นคงปลอดภัย โดยคำนึงถึงสิทธิเสรีภาพของประชาชน

๑.๓ มีขีดความสามารถในการตอบสนองภัยคุกคามทางไซเบอร์ในทุกรูปแบบได้อย่างมีประสิทธิภาพ (คน กระบวนการ เครื่องมือ) เพื่อรักษาเสถียรภาพทางเศรษฐกิจ ความมั่นคงแห่งชาติ และคุณภาพชีวิตของประชาชน

๑.๔ มีการคุ้มครองข้อมูลส่วนบุคคล (Privacy) และข้อมูลแสดงตัวตน (Identity) และมีการรักษาความมั่นคงปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ในทุกภาคส่วน

๑.๕ มีความร่วมมือทั้งระหว่างองค์กรภายในประเทศ และองค์กรระหว่างประเทศเพื่อเสริมศักยภาพการรักษาความมั่นคงปลอดภัยไซเบอร์

๒. ยุทธศาสตร์หลัก ๓ ประการ

๒.๑ การบูรณาการการจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศ

๒.๒ การสร้างศักยภาพในการตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคง

ปลอดภัย ไซเบอร์

๒.๓ การปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ

๓. ยุทธศาสตร์รอง ๕ ประการ

๓.๑ การประสานความร่วมมือระหว่างภาครัฐและเอกชนเพื่อความปลอดภัยไซเบอร์

๓.๒ การสร้างความตระหนักและรอบรู้ด้านความมั่นคงปลอดภัยไซเบอร์

๓.๓ การพัฒนาระเบียบและกฎหมายเพื่อความมั่นคงปลอดภัยไซเบอร์

๓.๔ การวิจัยและพัฒนาเพื่อความมั่นคงปลอดภัยไซเบอร์

๓.๕ การประสานความร่วมมือระหว่างประเทศ

กฎหมายที่เกี่ยวข้องกับไซเบอร์

กำหนดขึ้นเนื่องจากการทำธุรกรรมของทั้งภาครัฐและภาคเอกชน ที่พึ่งพาเทคโนโลยีสารสนเทศและการสื่อสารเพิ่มขึ้นอย่างมาก จึงควรให้มีการบริหารจัดการ และการรักษาความมั่นคงปลอดภัย โดยกำหนดเป็นกฎหมายหลายฉบับดังนี้

๑ พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๒ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๔๔ แก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๕๑

๒.๑ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวทางการจัดทำแนวนโยบาย (Certificate Policy) และแนวปฏิบัติ (Certification Practice Statement) ของผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority) พ.ศ. ๒๕๕๒

๒.๒ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง หลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓

๒.๓ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง การรับรองสิ่งพิมพ์ พ.ศ. ๒๕๕๕

๒.๔ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง หน่วยงานรับรองสิ่งพิมพ์ พ.ศ. ๒๕๕๕

๓ พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรม ทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

๓.๑ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

๓.๒ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๒) พ.ศ. ๒๕๕๖

๓.๓ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

๓.๔ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ (แก้คำผิด)

๔ พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓

๔.๑ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง ประเภทธุรกรรมทางอิเล็กทรอนิกส์ และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ ตามวิธีแบบปลอดภัย พ.ศ. ๒๕๕๕

๔.๒ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

อำนาจหน้าที่ของกระทรวงกลาโหม

การกำหนดอำนาจหน้าที่ของกระทรวงกลาโหมได้ปรากฏในกฎหมาย ๒ ฉบับ ฉบับแรก คือ พระราชบัญญัติปรับปรุงกระทรวง ทบวง กรม พ.ศ.๒๕๔๕ โดยในมาตรา ๘ กำหนดให้กระทรวงกลาโหม มีอำนาจหน้าที่เกี่ยวกับการป้องกันและรักษาความมั่นคงของราชอาณาจักรจากภัยคุกคามทั้งภายนอกและภายในประเทศ การรักษาผลประโยชน์แห่งชาติ สนับสนุนการพัฒนาประเทศ และราชการอื่น ตามที่มีกฎหมายกำหนดให้เป็นอำนาจหน้าที่ของกระทรวงกลาโหมหรือส่วนราชการที่สังกัดกระทรวงกลาโหม

ฉบับที่สอง คือ พระราชบัญญัติจัดระเบียบราชการกระทรวงกลาโหม พ.ศ.๒๕๕๑ ซึ่งกำหนดอำนาจหน้าที่ของกระทรวงกลาโหม ดังนี้

๑. พิทักษ์รักษาเอกราชและความมั่นคงแห่งราชอาณาจักรจากภัยคุกคาม ทั้งภายนอกและภายในราชอาณาจักร ปราบปรามการกบฏและการจลาจล โดยจัดให้มีและใช้กำลังทหารตามที่รัฐธรรมนูญแห่งราชอาณาจักรไทยหรือตามที่มีกฎหมายกำหนด

๒. พิทักษ์รักษา ปกป้องสถาบันพระมหากษัตริย์ ตลอดจนสนับสนุนภารกิจของสถาบันพระมหากษัตริย์

๓. ปกป้องพิทักษ์รักษาผลประโยชน์แห่งชาติและการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ ทรงเป็นประมุข พัฒนาประเทศเพื่อความมั่นคงตลอดจนสนับสนุนภารกิจอื่นของรัฐ ในการพัฒนาประเทศ การป้องกันและแก้ไขปัญหาจากภัยพิบัติ และการช่วยเหลือประชาชน

๔. ศึกษา วิจัย พัฒนา และดำเนินการด้านอุตสาหกรรมป้องกันประเทศและพลังงานทหาร ด้านวิทยาศาสตร์และเทคโนโลยีป้องกันประเทศ และด้านกิจการอวกาศ เทคโนโลยีสารสนเทศและการสื่อสาร ทั้งนี้เพื่อสนับสนุนภารกิจของกระทรวงกลาโหมและความมั่นคงของประเทศ

ยุทธศาสตร์การป้องกันประเทศกระทรวงกลาโหม พ.ศ.๒๕๕๕

กระทรวงกลาโหมได้จัดทำเอกสารยุทธศาสตร์การป้องกันประเทศ กระทรวงกลาโหม ขึ้นเมื่อปี พ.ศ. ๒๕๔๖ และได้มีการทบทวนมาแล้ว ๓ ครั้ง ในปี พ.ศ.๒๕๕๑, ๒๕๕๓ และ ๒๕๕๕ เนื่องมาจากการเปลี่ยนแปลงของสภาวะแวดล้อมด้านความมั่นคงของไทย ที่มีการเปลี่ยนแปลงไปอย่างรวดเร็ว ทั้งภายในและภายนอกประเทศ โดยในการทบทวนครั้งล่าสุดเมื่อปี พ.ศ. ๒๕๕๕ เนื่องมาจากการให้ความสำคัญต่อการเผชิญกับภัยคุกคามต่อความมั่นคงแห่งชาติ ทั้งภัยคุกคามแบบดั้งเดิมซึ่งเป็นภัยคุกคามทางทหารโดยตรง และภัยคุกคามรูปแบบใหม่ นอกจากนั้นยังให้ความสำคัญต่อความท้าทายด้านความมั่นคงที่เกิดขึ้น ได้แก่ การสนับสนุนการรวมตัวเป็นประชาคมอาเซียน เป็นต้น

วัตถุประสงค์ในการป้องกันประเทศ ได้กำหนดไว้เป็น ๒ ส่วน ได้แก่ วัตถุประสงค์เฉพาะในการปฏิบัติการทางทหาร และวัตถุประสงค์เฉพาะในการสนับสนุนความมั่นคงของรัฐ ในส่วนของแนวคิดทางยุทธศาสตร์ ยังคงไว้ ๓ ประการเช่นเดิม กล่าวคือ การสร้างความร่วมมือด้านความมั่นคง ผนึกกำลังป้องกันประเทศ และการป้องกันเชิงรุก มีสาระสำคัญที่เกี่ยวข้อง ได้แก่

๑. มาตรการและขีดความสามารถที่ต้องการตามแนวคิดการผนึกกำลังป้องกันประเทศ ซึ่งมีสาระสำคัญคือ การร่วมมือกันระหว่างหน่วยงานที่เกี่ยวข้องเพื่อการรวมกำลังป้องกันประเทศ

๒. มาตรการและขีดความสามารถที่ต้องการตามแนวคิดการสร้างความร่วมมือด้านความมั่นคง ซึ่งมีสาระสำคัญคือ การแสวงความร่วมมือด้านความมั่นคงกับชาติพันธมิตร และมหาอำนาจ

๓. มาตรการและขีดความสามารถที่ต้องการตามแนวความคิดการป้องกันเชิงรุก ซึ่งมีสาระสำคัญคือการป้องกันระบบควบคุมบังคับบัญชา ฯ และสามารถปฏิบัติต่อฝ่ายตรงข้าม

สรุป

กระทรวงกลาโหมได้จัดทำยุทธศาสตร์การป้องกันประเทศเพื่อใช้เป็นกรอบในการดำเนินการของกระทรวงกลาโหม และปรับปรุงให้ทันสมัยอยู่เสมอ ซึ่งปัจจุบันและอนาคตภัยคุกคามไซเบอร์จะเป็นภัยคุกคามรูปแบบใหม่ ที่สำคัญและมีผลกระทบต่อความมั่นคงของชาติอย่างมากที่ประเทศไทยยังไม่เคยได้มีการจัดทำนโยบาย ยุทธศาสตร์ แผนแม่บท และแผนปฏิบัติการต่าง ๆ ไว้รองรับมาก่อน จากการศึกษาเอกสารที่เกี่ยวข้องดังที่ได้กล่าวมาแล้วนั้น จึงเป็นแนวทางที่ต้องนำไปใช้เป็นกรอบในการกำหนดยุทธศาสตร์การป้องกันไซเบอร์ของกระทรวงกลาโหมต่อไป

บทที่ ๓

ศึกษาการรับมือภัยคุกคามจากไซเบอร์

ศึกษาภัยคุกคามไซเบอร์ทั่วโลกและการรับมือ

ประชาชน หน่วยงานภาครัฐและเอกชน มีความเกี่ยวพันธ์กับระบบสารสนเทศและระบบอินเทอร์เน็ตอยู่ตลอดเวลาไม่ว่าจะเป็น การใช้โทรศัพท์มือถือ การค้นหาข้อมูลในระบบอินเทอร์เน็ตจากเว็บไซต์ต่าง ๆ การใช้อิเล็กทรอนิกส์เมล์ในการติดต่อสื่อสารกัน โดยเฉพาะความนิยมในการใช้อินเทอร์เน็ต ที่เพิ่มขึ้นทั่วโลก ทำให้อาชญากรรมคอมพิวเตอร์ที่มีการใช้งานอินเทอร์เน็ตเป็นสื่อกลางในการติดต่อมีสถิติเพิ่มขึ้น โดยเหล่าอาชญากรคอมพิวเตอร์อาศัยช่องทางการโจมตีเหยื่อหรือเป้าหมาย ผ่านทางระบบเครือข่ายอินเทอร์เน็ตที่เป็นเครือข่ายสาธารณะ ผลจากการโจมตีดังกล่าวทำให้หลายองค์กรตลอดจนบุคคลทั่วไป เกิดความเสียหายทางด้านเศรษฐกิจและสังคม ทำให้องค์กรเสียชื่อเสียง เสียความน่าเชื่อถือ กลายเป็นปัญหาระดับชาติ และระดับโลกที่ทุกคนต้องทำความเข้าใจและแก้ปัญหาร่วมกัน ภัยอินเทอร์เน็ตได้มีการเปลี่ยนแปลงปรับรูปแบบวิธีการโดยการใช้เทคนิคที่แตกต่างกันออกไปในการโจมตีเป้าหมาย ซึ่งเป้าหมายหลักของเหล่าแฮกเกอร์กลับไม่ใช่ระบบคอมพิวเตอร์ที่ใช้อยู่ แต่เป็นตัวบุคคล ในการโจมตีด้วยวิธีการที่ เรียกว่า "Social Engineering" หรือการใช้หลักจิตวิทยาในการหลอกล่อเหยื่อให้หลงเชื่อในข้อความหลอกลวงผ่านทางเว็บไซต์หรือ อิเล็กทรอนิกส์เมล์ ดังนั้น การสร้างความตระหนักรู้แก่ผู้ใช้งานคอมพิวเตอร์ทั่วไปสำหรับประชาชนและหน่วยงาน นั้นถือเป็นเรื่องสำคัญอย่างยิ่ง ในการเพิ่มภูมิคุ้มกันให้กับผู้ใช้คอมพิวเตอร์ที่อาจจะยังไม่ทราบถึง วิธีการโจมตีในรูปแบบใหม่ๆ ดังกล่าว เมื่อผู้ใช้คอมพิวเตอร์เกิดความเข้าใจและมีความตระหนักถึงภัยอินเทอร์เน็ตมากขึ้นก็จะช่วยลดผลกระทบจากปัญหาที่เกิดขึ้นได้ในทางปฏิบัติในที่สุด

๑. ภัยคุกคามจากไซเบอร์ในปัจจุบันสามารถสรุปได้ดังต่อไปนี้

๑.๑ ภัยจากการถูกขโมยข้อมูลระบุตัวตน ชื่อผู้ใช้และรหัสผ่าน (Username/ Password and Identity Theft) แฮกเกอร์จะเจาะข้อมูลของเหยื่อ ขโมยชื่อผู้ใช้และรหัสผ่านของเหยื่อ เพื่อแอบโอนเงินจากบัญชีของเหยื่อ หรือ แอบนำบัตรเครดิตของเหยื่อไปใช้โดยที่เหยื่อไม่รู้ตัว ซึ่งกว่าเหยื่อจะทราบว่าโดนขโมยบัตรเครดิต หรือ ถูกโอนเงิน ในบัญชีไปโดยไม่รู้ตัว ก็พบว่าเงินหมดบัญชีไปแล้ว การขโมยเงินจากบัตรเครดิตหรือบัตรเอทีเอ็มมีคดีเกิดขึ้นมากมายในประเทศไทย ในช่วงสองสามปีทีผ่านมา และ มีแนวโน้มที่จะเพิ่มขึ้นในอนาคต เป้าหมายของเหล่าผู้ไม่หวังดีก็คือ ระบบอินเทอร์เน็ตแบงค์กิ้งหรือระบบการให้บริการธนาคารผ่านทางอินเทอร์เน็ต ซึ่งในปัจจุบันทางธนาคารแห่งประเทศไทยได้ออกกฎระเบียบให้ธนาคาร พาณิชย์ทุกธนาคาร ต้องมีกระบวนการในการตรวจสอบความปลอดภัยของระบบออนไลน์ของ ตนเองด้วยการทดสอบเจาะระบบของตนที่เรียกว่า "Penetration

Testing" ก่อนการให้บริการกับประชาชน เป็นการบริหารความเสี่ยง (Risk Management) ที่ถูกต้อง ตามหลักวิชาการ ในปัจจุบันหลายธนาคารในประเทศไทยตกเป็นเป้าหมายของแฮกเกอร์ในการเจาะข้อมูลของลูกค้าธนาคาร ซึ่งแฮกเกอร์มีเทคนิคใหม่ๆ มากมายในการเจาะระบบ ทางธนาคารจึงมีความจำเป็นอย่างยิ่งที่ต้องทดสอบและตรวจสอบระบบด้วยการทำประเมินช่องโหว่และจุดอ่อน (Vulnerability Assessment) และ ทดสอบการเจาะระบบ (Penetration Testing) ก่อนการให้บริการ อีกธุรกิจหนึ่งที่ตกเป็นเป้าหมายของแฮกเกอร์ก็คือ เกมส์ออนไลน์ ซึ่งแฮกเกอร์จะพยายามเจาะข้อมูลของผู้เล่นเกมส์ แล้วเข้าไปในเกมส์เพื่อขโมยทรัพย์สินภายในเกมส์แล้วนำมาขายทอดตลาดในโลกจริง ทำให้ผู้เล่นเกมส์เกิดความเสียหาย เช่น การเสียทรัพย์ เสียทั้งเงินและเวลาในการสะสมทรัพย์สินในเกมส์เหล่านั้น จะมีผลกระทบกับเด็กวัยรุ่นที่ยังไม่สามารถหา เงินได้เอง ต้องเดือดร้อนถึงผู้ปกครองอย่างหลีกเลี่ยงไม่ได้ จะเห็นได้ว่าการโจมตีในโลกออนไลน์หรือในระบบเกมส์บนอินเทอร์เน็ตที่เราเรียกว่า "โลกเสมือน (Virtual World)" ได้มีผลกระทบกับ "โลกแห่งความเป็นจริง (Real World)" ทั้งทางตรงและทางอ้อม ดังนั้นจึงควรเรียนรู้ถึงวิธีการโจมตีในรูปแบบต่างๆ ของแฮกเกอร์ เพื่อที่จะได้สามารถป้องกันตนเอง และบริษัท หรือองค์กรให้ปลอดภัยจากภัยคุกคามจากไซเบอร์ รูปแบบต่าง ๆ ของแฮกเกอร์มีดังต่อไปนี้

๑.๑.๑ Phishing Attack วิธีการโจมตีแบบ "Phishing" กำลังเป็นที่นิยมของแฮกเกอร์ในช่วงหลายปีที่ผ่านมา โดยจะเน้นการโจมตีไปที่กลุ่มผู้ใช้บริการออนไลน์และผู้ใช้บริการ eCommerce เช่น eBay, Amazon หรือ PayPal เป็นต้น และ แฮกเกอร์ยังนิยมโจมตีกลุ่มผู้ใช้บริการอินเทอร์เน็ตแบงค์กิ้งอีกด้วย วิธีการของเหล่ามิจฉาชีพก็คือ การส่งอิเล็กทรอนิกส์เมล์หลอกมายังผู้ใช้บริการออนไลน์ต่างๆ เช่น ผู้ใช้บริการอินเทอร์เน็ตแบงค์กิ้งว่าอิเล็กทรอนิกส์เมล์นั้นถูกส่งมาจาก ธนาคารที่ผู้ใช้บริการติดต่อใช้บริการอยู่ โดยมีการปลอมแปลงชื่อผู้ส่งและที่อยู่ของผู้ส่งว่ามาจากธนาคารดังกล่าว และมีเนื้อความในอิเล็กทรอนิกส์เมล์หลอกให้เหยื่อหลงเข้าไป "Log-on" หรือ "Sign-on" เข้าไปในหน้าเว็บหลอกที่มี URL ปรากฏอยู่ในรูปของ Link ที่อยู่ในเนื้อความของอิเล็กทรอนิกส์เมล์ ซึ่ง Link ดังกล่าวก็จะเชื่อมไปยังเว็บไซต์หลอกที่แฮกเกอร์ได้ทำไว้เพื่อดักชื่อผู้ใช้และรหัสผ่านของเหยื่อ เมื่อเหยื่อหลงเข้าไป "Log-on" ก็เท่ากับว่าไปบอกชื่อผู้ใช้และรหัสผ่านซึ่งเป็นความลับ ให้กับแฮกเกอร์โดยรู้เท่าไม่ถึงการณ์ สำหรับทางแก้ไขที่ได้ประสิทธิภาพก็คือการนำระบบ "ระบบการพิสูจน์ตัวที่ใช้อย่างน้อย 2 องค์ประกอบ (Two-Factor Authentication)" โดยการใช้อุปกรณ์ Token หรือ Smart Card ร่วมกับรหัสผ่าน หรือ ใช้ระบบรหัสผ่านแบบ "One Time Password" (OTP) ซึ่งจะมีความปลอดภัยมากกว่าระบบที่ใช้เพียงแค่ "ชื่อผู้ใช้" และ "รหัสผ่าน" แบบเดิมๆ ที่ไม่สามารถป้องกันวิธีการโจมตีแบบ "Phishing" ได้

๑.๑.๒ Pharming Attack เป็นการโจมตีที่ไม่ต้องใช้วิธีการส่งอิเล็กทรอนิกส์เมล์มาหลอกเหยื่อแบบ Phishing แต่จะใช้วิธีการโจมตีที่ระบบแปลงชื่อของเว็บไซต์เป็นหมายเลขที่อยู่เครื่องคอมพิวเตอร์ (DNS - Domain Name System) หรือ โจมตีที่ข้อมูลของเครื่องลูกข่าย โดยการ "โอนย้าย (Re-Direct)" ชื่อของเว็บไซต์ให้ชี้ไปยัง "หมายเลขที่อยู่เครื่องคอมพิวเตอร์ (IP Address - Internet Protocol

address) ลวง" ที่ไม่ตรงกับ "IP Address จริง" ของเว็บไซต์นั้นๆ ซึ่งเหยื่อจะแยกความแตกต่างแทบไม่ออกเลยระหว่างเว็บไซต์จริงกับเว็บไซต์ ปลอมที่ทางแฮกเกอร์ได้เตรียมไว้ เพราะ ชื่อที่แสดงถึงที่อยู่ของข้อมูลในอินเทอร์เน็ต (URL - Uniform Resource Locator) ของเว็บไซต์ไม่มีการเปลี่ยนแปลง ดังนั้นหนทางป้องกัน Pharming Attack คือการป้องกันระบบ DNS ให้ปลอดภัยจากการโจมตี กล่าวคือ การใช้ระบบ Two Factor Authentication ดังที่กล่าวมาแล้วในตอนต้น

๑.๑.๓ Vishing หรือ Voice SPAM Attack เป็นการโจมตีโดยการใช้ระบบโทรศัพท์เข้ามาเกี่ยวข้อง เราคงเคยได้ยินเรื่อง "แก็งค์โทรตุ๋น ไม่โชว์เบอร์" พฤติกรรมของแก็งค์นี้มีการใช้ระบบ "Automated Calling" หรือระบบ "Voice Over IP" มาใช้ในการโทรหลอกเหยื่อให้หลงคิดว่าเป็นโทรอัตโนมัติจากธนาคารสถาบันการเงิน หรือบริษัทบัตรเครดิต เพื่อทำการหลอกเหยื่อให้หลงเชื่อ จากนั้นก็จะหลอกถามข้อมูลส่วนตัว หรือข้อมูลทางด้านการเงินของเหยื่อ เพื่อนำไปใช้ในการทำบัตรเครดิตปลอม หรือนำไปใช้ในทางมิชอบทางอื่น ทำให้เหยื่อเกิดความเสียหายได้โดยกว่าจะรู้ตัวก็พบว่าเงินได้ออกจากบัญชีไปแล้ว หรือ มีการแอบใช้บัตรเครดิตของเราโดยที่เราไม่ได้เป็นคนใช้จ่าย จึงต้องระมัดระวังไม่หลงเชื่อโดยง่าย

๑.๑.๔ Spyware / Keylogger Attack โปรแกรมดักข้อมูลจากคีย์บอร์ด หรือ Keylogger เป็นโปรแกรมประเภท "Spyware" โดยมีจุดประสงค์ในการดักข้อมูลโดยที่เหยื่อไม่รู้ตัว เกิดจากการที่เหยื่อมักจะเปิดเครื่องทิ้งไว้โดยไม่ได้ Lock หน้าจอคอมพิวเตอร์ เป็นเหตุให้ผู้ไม่หวังดีสามารถทำการติดตั้งโปรแกรม Spyware หรือ Keylogger ผ่านทางการใช้ Thumb Drive หรือ USB Drive ที่ทุกคนใช้กันโดยทั่วไป หลังจากนั้นไม่ว่าเหยื่อจะพิมพ์อะไรก็จะถูกดักข้อมูลบนคีย์บอร์ดและข้อมูล หน้าจอส่งไปยังอีเมล์ของแฮกเกอร์เป็นระยะๆ ทำให้ข้อมูลส่วนตัวของเหยื่อหลุดเข้าไปอยู่ในมือคนร้ายอย่างง่ายดาย ดังนั้น เราควรล็อกหน้าจอคอมพิวเตอร์ทุกครั้งเวลาที่เราไม่ได้อยู่หน้าเครื่องและ การใช้โปรแกรมประเภท Anti-Malware ด้วย

๑.๑.๕ Remote Access Trojan (RAT) Attack เป็นการโจมตีระยะไกลโดยใช้โปรแกรมประเภทม้าโทรจันส่งผ่านมาทางอีเมล์ โดยหลอกว่าเป็นโปรแกรมประยุกต์ทั่วไป เช่น โปรแกรมเกมส์ หรือ โปรแกรมที่ใช้ในการฆ่าไวรัส เป็นต้น เมื่อเหยื่อหลงเข้าใจผิดแล้วสั่ง "Run" โปรแกรมดังกล่าว เหยื่อก็จะถูกควบคุมคอมพิวเตอร์ของตนจากระยะไกล (Remote Access) โดยไม่รู้ตัว ทำให้แฮกเกอร์สามารถเข้ามาล้วงความลับของเหยื่อได้อย่างง่ายดาย การป้องกันที่ได้ผลที่สุดก็คือ การฝึกอบรม "Security Awareness Training" ให้กับผู้ใช้คอมพิวเตอร์ให้รู้เท่าทันวิธีการโจมตีดังกล่าวและมีวินัยในการ เปิดใช้งานโปรแกรมเฉพาะโปรแกรมประยุกต์ที่ใช้ในการทำงานเท่านั้น โดยไม่เข้าไปเปิด หรือ "Run" โปรแกรมที่ไม่ปลอดภัยจะได้ไม่ต้องตกเป็นเหยื่อดังที่กล่าวมาแล้ว

๑.๑.๖ HOAX/SCAM หรือจดหมายหลอกลวง HOAX หรือ SCAM ถือเป็นการ "SPAM" อย่างหนึ่งผ่านทางอีเมล์ มีวัตถุประสงค์ในการส่งอีเมล์หลอกให้เหยื่อเข้าใจผิดว่าได้รับรางวัลหรือ ได้รับเงินผ่านทางอินเทอร์เน็ต ซึ่งเหยื่อจะเกิดความโลภที่จะได้รับเงินก้อนโต จากนั้นมิจฉาชีพก็จะหลอกให้เหยื่อโอน

เงินค่าธรรมเนียม (เงินก้อนเล็ก) เพื่อให้ได้รางวัล (เงินก้อนโต) ดังกล่าว ดังนั้น อีเมล์ประเภทนี้จึงควรลบทิ้งทันทีไม่ต้องไปสนใจ

๑.๑.๗ Theft of Notebook/PC or Mobile Device เป็นการขโมยแบบดั้งเดิมทางกายภาพโดยไม่ต้องใช้เทคนิคทางคอมพิวเตอร์เลย กล่าวคือ การขโมย PC,Notebook,PDA หรือโทรศัพท์มือถือ จากนั้นก็นำไปถอดเอาฮาร์ดดิสก์หรือ SIM Card ออกจากเครื่องเพื่อนำไป "Copy" ข้อมูลของเหยื่อเพื่อวัตถุประสงค์บางอย่าง หรือนำอุปกรณ์คอมพิวเตอร์ของเราไปจำหน่ายต่อในตลาดมือสอง ทำให้เราต้องเสียทั้งข้อมูลในเครื่องและตัวเครื่อง วิธีการป้องกันก็คือ อย่าวางอุปกรณ์พกพา หรือ อุปกรณ์คอมพิวเตอร์ไว้ในที่ที่ไม่ปลอดภัยและควร Backup ข้อมูลไว้เป็นระยะๆ หรือ ควรมีการเข้ารหัสข้อมูล (Data Encryption) เพื่อที่จะป้องกันข้อมูลถึงแม้จะถูกขโมยฮาร์ดแวร์ไป แฮกเกอร์ก็ไม่สามารถเข้าถึงข้อมูลที่เราเข้ารหัสไว้ได้ ทำให้เรายังคงรักษาความลับของข้อมูลไว้ได้จากภัยทั้งเจ็ด เราพบว่าสาเหตุหลักของการถูกโจมตีดังกล่าวก็คือ การที่ผู้ใช้คอมพิวเตอร์ขาดความรู้ความเข้าใจเรื่องเทคนิคการโจมตีของ แฮกเกอร์ ทำให้ขาดความระมัดระวังในการใช้งานอินเทอร์เน็ตโดยรู้เท่าไม่ถึงการณ์ ซึ่งวิธีการแก้ไขที่ได้ผลมากที่สุดก็คือ การให้ความรู้ใหม่ๆ กับผู้ใช้คอมพิวเตอร์ด้วยการจัดทำโปรแกรม "Information Security Awareness Training" ขึ้นในองค์กร เพื่อให้เกิดความตระหนักและรู้เท่าทันถึงภัยดังกล่าว รวมถึงการใช้กระบวนการ และเทคโนโลยีที่ทันสมัยมาแก้ปัญหาในระยะยาว เช่น เทคโนโลยี Two Factor Authentication หรือการเข้ารหัสข้อมูล (Data Encryption) เป็นต้น

๑.๒ ภัยจากการโจมตี Web Server และ Web Application

ปัจจุบันในทางเทคนิค “อุปกรณ์ป้องกันการบุกรุก (Firewall)” ไม่สามารถป้องกันการโจมตีต่อเครื่องคอมพิวเตอร์ผู้ให้บริการเว็บไซต์ (Web Server) และ เครื่องคอมพิวเตอร์ผู้ให้บริการโปรแกรมประยุกต์บนเว็บไซต์ (Web Application) ได้ทั้งหมด เพราะ Firewall จำเป็นต้องเปิดช่องให้ผู้คนสามารถเข้ามาเยี่ยมชมเว็บไซต์ ได้นั่นเอง โดยที่การโจมตีของแฮกเกอร์ นั้นเกิดจากช่องโหว่ที่เป็นวิกฤติความปลอดภัยของเว็บไซต์ 10 ประเภท พบว่า การโจมตีแบบ "การส่งโปรแกรมคอมพิวเตอร์เล็ก ๆ ไปฝังในหน้าเว็บไซต์ที่มีช่องโหว่เพื่อดักขโมยข้อมูลชื่อผู้ใช้และรหัสผ่าน (Cross-Site Scripting)" และ "การเจาะระบบโดยใช้ข้อบกพร่องของระบบฐานข้อมูล (Injection Flaw)" มีสถิติสูงที่สุด ปัญหาส่วนใหญ่เกิดจาก การเขียนโปรแกรม Web application ที่ไม่ปลอดภัยจากความรู้เท่าไม่ถึงการณ์ของโปรแกรมเมอร์ที่นิยมใช้ภาษา ASP,JSP หรือ PHP ซึ่งเปิดช่องโหว่ทางด้าน "Application Security" ให้แก่แฮกเกอร์ที่มีความเชี่ยวชาญในการพัฒนาโปรแกรมด้วยเช่นกัน ดังนั้น ปัญหาที่เกิดจากการเขียนโปรแกรมไม่ปลอดภัยเพียงพอนั้น จะแก้โดยการใช้ Firewall แบบธรรมดาไม่ได้ จำเป็นต้องใช้ "อุปกรณ์ป้องกันการเจาะ Web Application (WAF – Web Application Firewall)" และให้ความรู้แก่โปรแกรมเมอร์เกี่ยวกับการเขียนโปรแกรมที่ปลอดภัย เพื่อป้องกันการโจมตีดังกล่าว

๑.๓ ภัยข้ามระบบปฏิบัติการ (Cross-platform/Multi-platform Attack)

การโจมตีระบบคอมพิวเตอร์ของไวรัสหรือมัลแวร์ ส่วนใหญ่นั้นเกิดขึ้นบนระบบปฏิบัติการ Microsoft Windows แต่ในปัจจุบันผู้ใช้คอมพิวเตอร์มีความนิยมใช้ระบบปฏิบัติการอื่นๆ เช่น OS X ของ Mac และ iPhone รวมถึง Android เป็นต้น

การโจมตีแบบ Cross-platform นั้นจะเป็นการโจมตีผ่านทาง Web Browser เป็นส่วนใหญ่ เพราะทุกระบบปฏิบัติการล้วนใช้ Web Browser เหมือน ๆ กัน เช่น Firefox หรือ Safari เป็นต้น โปรแกรมไม่ประสงค์ดีส่วนใหญ่เขียนด้วยภาษา Java หรือ JavaScript ที่สามารถทำงานบน Web Browser ดังกล่าวได้เป็นอย่างดีแฮกเกอร์ในปัจจุบันพยายามที่จะมุ่งเป้าหมายมาโจมตีอุปกรณ์พกพาและ โทรศัพท์เคลื่อนที่มากขึ้น ดังนั้น เราจึงควรระมัดระวังเวลาใช้อุปกรณ์ดังกล่าวในการเข้าเว็บไซต์ หรือ ดาวน์โหลดโปรแกรมต่างๆ เข้ามาทำงานบนอุปกรณ์พกพา เพราะถ้าไม่ระมัดระวังอาจทำให้เครื่องมีปัญหาในการทำงานจากการรบกวนของโปรแกรมไวรัสหรือมัลแวร์ได้ การติดตั้ง โปรแกรมที่ใช้ซ่อมแซมจุดบกพร่องของโปรแกรมคอมพิวเตอร์ (Patch) และโปรแกรมป้องกันมัลแวร์ ก็สามารถช่วยป้องกันความเสี่ยงที่จะเกิดขึ้นได้

๑.๔ ภัยจากการถูกขโมยข้อมูลหรือข้อมูลความลับรั่วไหลออกจากองค์กร (Data Loss/Leakage and Theft)

ปัญหาด้าน "ความปลอดภัยที่แฟ้มข้อมูล (Data Security)" นั้นกำลังกลายเป็นปัญหาใหญ่ในปัจจุบัน เนื่องจากข้อมูลขององค์กรส่วนใหญ่แล้วจะถูกแปลงให้จัดเก็บในรูปแบบของ ไฟล์ที่อยู่ในรูปแบบ “ดิจิตอลฟอร์แมต” เก็บไว้ในฮาร์ดดิสก์ หรือที่เก็บข้อมูลประเภทต่างๆ ไม่ว่าจะเป็น CD,DVD หรือ เก็บไว้ใน ที่เก็บขนาดใหญ่ เช่น ระบบ NAS หรือ SAN ก็สามารถถูกผู้ไม่หวังดีแอบทำสำเนา (Copy) ข้อมูลออกไปได้โดยง่าย จากการนิยมใช้ Thumb Drive หรือ USB Drive ตลอดจน iPhone/iPod หรืออุปกรณ์ MP3 ต่างๆ ในองค์กร ที่มีความจุข้อมูลค่อนข้างสูง ดังนั้น การป้องกันข้อมูลรั่วไหลจึงทำได้ค่อนข้างยากในทางเทคนิค จำเป็นต้องใช้เทคโนโลยีขั้นสูง เช่น เทคโนโลยี การจัดการสิทธิการเข้าถึงข้อมูล (DRM - Digital Right Management) และเทคโนโลยี ป้องการข้อมูลสูญหาย (DLP - Data Loss Prevention) ในการบริหารจัดการไฟล์ข้อมูลต่างๆ ให้เข้าถึงเฉพาะผู้ใช้ที่ถูกกำหนดสิทธิไว้แล้วเท่านั้น ผู้ใช้ที่ไม่มีสิทธิ์ไม่สามารถเข้าถึง (Access) หรือทำสำเนา (Copy) ไฟล์ดังกล่าวได้จากสถิติพบว่า การขโมยข้อมูลโดย คนในองค์กร (Insider Threat) นั้นมีเปอร์เซ็นต์สูงกว่าการขโมยโดยคนนอก และส่วนใหญ่เกิดจากพนักงานที่ไม่ซื่อสัตย์ หรือมีทัศนคติไม่ดีกับบริษัท (Disgruntled Employee) การเข้ารหัสข้อมูล (Data Encryption) ก็เป็นอีกวิธีหนึ่งในการป้องกันข้อมูลรั่วไหลได้ แต่ในขณะเดียวกันกลับกลายเป็นเทคนิคของแฮกเกอร์ในการแอบซ่อนข้อมูลไม่ให้ เราสามารถทราบได้ว่าแฮกเกอร์กำลังแอบส่งข้อมูลกันอยู่ในกลุ่มของแฮกเกอร์ ด้วยกันเอง ซึ่งมักนิยมใช้เทคโนโลยีที่เรียกว่า "การซ่อนไฟล์ข้อมูลในรูปภาพ (Steganography)" ยกตัวอย่าง การเข้ารหัสข้อมูลของกลุ่มผู้ก่อการร้ายในการถล่มตึก World Trade ที่มหานครนิวยอร์ค (911) เมื่อหลายปีก่อน เป็นต้น

๑.๕ ภัยจากมัลแวร์ (Malware) สแปม (SPAM) , ไวรัส (VIRUS) และ สปายแวร์ (SPYWARE)

โปรแกรมมุ่งร้ายหรือโปรแกรมประสงค์ร้าย ที่เราเรียกกันว่ามัลแวร์ (Malware) นั้น มีรูปแบบของการทำงานที่แตกต่างกันในรายละเอียด จึงทำให้บางครั้งเราเรียกมัลแวร์ในชื่ออื่นๆ เช่น ไวรัส สปายแวร์ หรือแอดแวร์ เป็นต้น

ความสัมพันธ์ของโปรแกรมมุ่งร้ายนั้นมีความเกี่ยวโยงกับ Spam Mail ที่เราได้รับกันเป็นประจำทุกวัน กล่าวคือ Spam Mail เป็นยานพาหนะหรือตัวนำมาซึ่งมัลแวร์ในรูปแบบต่างๆ ดังนั้น ภัยจาก Spam Mail จึงไม่ใช่แค่ความรำคาญ หากแต่ยังนำมาซึ่งโปรแกรมมุ่งร้ายที่อาจแนบมากับไฟล์แนบ (Attached File) หรือ อยู่ในรูปแบบของ ลิงค์ดาวน์โหลด ที่หลอกให้ผู้รับอีเมล์ แล้วเข้าไปดาวน์โหลดโปรแกรมมุ่งร้ายจากอีเมล์ดังกล่าว

ตัวอย่าง โปรแกรมไวรัสหรือเวอร์มที่มีผลกระทบรุนแรงที่ผ่านมา ได้แก่ โปรแกรม "Storm Worm" หรือ "Nuwar@MM Worm" ซึ่งมาในรูปแบบของจดหมายลูกโซ่ที่กล่าวถึงผู้เสียชีวิตชาวยุโรปจากพายุ โดยอาศัยชื่อพายุดึงความสนใจ คนอ่านเมล์พบว่าคนยุโรปตกเป็นเหยื่อสูงสุด ขณะนี้ชาวอเมริกันและเอเชียกลับพบน้อยกว่า เนื่องจากถือเป็นเหตุไกลตัว ถ้าเปลี่ยนชื่ออีเมล์เป็น 'สึนามิ" อาจมีคนเอเชียติดไวรัสมากกว่านี้ก็เป็นได้โปรแกรมไวรัสลักษณะ Storm Worm" นั้น ไม่ใช่ไวรัสคอมพิวเตอร์ธรรมดาๆ แต่เป็นไวรัสที่ทำการยึดเครื่องของเราให้กลายเป็น "BOT (โปรแกรมอัตโนมัติสำหรับทำหน้าที่อย่างใดอย่างหนึ่งบนอินเทอร์เน็ต ซึ่งบอตย่อมาจากคำว่าโรบอต แปลว่า หุ่นยนต์)" ในเครือข่าย "บอตเน็ต (BOTNET)" ของแฮกเกอร์อีกด้วย ทำให้แฮกเกอร์สามารถเข้ามาควบคุมเครื่องคอมพิวเตอร์ของเราได้จากระยะไกล ซึ่งช่วงที่ระบาดพบว่าเครื่องคอมพิวเตอร์ทั่วโลกกว่า 50 ล้านเครื่องที่ถูกโจมตี นับว่าเป็นการโจมตีครั้งใหญ่อีกครั้งหนึ่งของแฮกเกอร์ที่สามารถนำการโจมตี หลายๆ แบบมารวมกันทั้ง BOTNET และ Malware รวมถึง SPAM Mail ด้วยดังนั้น เราจึงควรหมั่นศึกษาข้อมูลข่าวสารใหม่ๆ เกี่ยวกับการแพร่กระจายของไวรัส เพื่อจะได้รู้เท่าทันวิธีการหลอกลวงแบบใหม่ๆ ของกลุ่มผู้ไม่หวังดี จะได้สามารถป้องกันระบบคอมพิวเตอร์ได้อย่างทันท่วงที โดยเฉพาะเวลาที่ยังไม่มีโปรแกรม ANTI-Malware ที่สามารถกำจัดไวรัสดังกล่าวได้ เรียกว่า "Zero-Day Attack"

๑.๖ ภัยจากการใช้โปรแกรมประเภท การรับส่งข้อมูลกันโดยตรง P2P – (Peer-to-Peer) และ ระบบส่งข้อความทันที (IM - Instant Messaging)

จากความนิยมในการใช้โปรแกรมดาวน์โหลด ภาพยนตร์และเพลงต่างๆ ในรูปแบบของไฟล์ ทำให้โปรแกรมประเภท P2P มีสถิติการใช้ ปริมาณการรับส่งข้อมูล (Bandwidth) ของเครือข่ายอินเทอร์เน็ตที่สูงมาก ผู้ใช้อินเทอร์เน็ตตามบ้านล้วนนิยมใช้โปรแกรม P2P เช่น Bittorrent , eMule , Limewire , eDonkey หรือ Kazaa กันอย่างแพร่หลาย ปัญหาก็คือ โปรแกรม P2P เหล่านี้นอกจากจะใช้ Bandwidth ขององค์กรในการดาวน์โหลดไฟล์ต่างๆ แล้ว โปรแกรม P2P ยัง "แบ่งปัน (Share)" ไฟล์ต่างๆ ที่อยู่ในฮาร์ดดิสก์ของ

เราอีกด้วย หลายคนรู้เท่าไม่ถึงการณ์ทำให้ข้อมูลส่วนตัวในฮาร์ดดิสก์ถูกนำไปแชร์ให้คนหลายร้อยล้านคนทั่วโลกที่ใช้โปรแกรม P2P สามารถเข้ามาดาวน์โหลดไฟล์ได้ นอกจากนี้ โปรแกรมมัลแวร์ยังถูกปล่อยอยู่ตามเครือข่าย P2P โดยจะตั้งชื่อโปแกรมให้มีความน่าสนใจ เพื่อหลอกล่อให้ผู้อ่านโปรแกรม P2P ดาวน์โหลดไปใช้งาน โดยที่ผู้ใช้ไม่ทราบว่าโปรแกรมเหล่านั้น ถูกเขียนขึ้นมาเพื่อวัตถุประสงค์ในการลักลอบดักข้อมูล (Keylogger) หรือทำให้กลายเป็นบอตของเครือข่ายบอตเน็ต ซึ่งทำให้แฮกเกอร์สามารถเข้ามาควบคุมเครื่องคอมพิวเตอร์ได้จากระยะไกลโดย ไม่รู้ตัว ดังนั้น การใช้งานโปรแกรมประเภท P2P จำเป็นต้องมีการควบคุมไม่ให้ผู้ใช้ในองค์กรสามารถใช้งานได้ตามใจชอบ เพราะอาจส่งผลกระทบกับเครือข่ายขององค์กรจากการถูกโจมตีโดยไวรัสและ แฮกเกอร์ในที่สุด องค์กรควรออกประกาศนโยบายด้านความปลอดภัยสารสนเทศและให้ผู้ใช้งาน คอมพิวเตอร์ในองค์กรลงนามในเอกสารหนังสือยินยอมการใช้งานระบบสารสนเทศของ องค์กรอย่างปลอดภัยหรือที่รู้จักกันทั่วไปว่า เอกสาร นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ (AUP - Acceptable use Policy) และจัดให้มีโปรแกรมฝึกอบรมให้ผู้ใช้คอมพิวเตอร์ตระหนักถึงภัยคุกคามทางอินเทอร์เน็ตที่มากับโปแกรมประเภท P2P ดังกล่าวโปรแกรมประเภท Instant Messaging หรือ IM เช่น AIM , YIM และโปแกรมยอดฮิต MSN ก็จัดอยู่ในประเภทเดียวกันกับโปรแกรม P2P ซึ่งผู้ใช้งานโปรแกรม IM ก็มีโอกาสจะติดไวรัสที่ถูกส่งมาจากคู่สนทนาที่กำลัง "Chat" กันอยู่ เนื่องจากคู่สนทนาของเราติดไวรัสก่อน จึงทำให้เครื่องของคู่สนทนาทำการส่งไวรัสออกไปยังทุกคนที่กำลัง "Online" อยู่ในระบบ Instant Messaging ด้วยวิธีการนี้ ทำให้ไวรัสหรือวอร์มสามารถแพร่กระจายได้ด้วยความรวดเร็วเป็นทวีคูณจนสร้าง ความเสียหายให้กับเครือข่ายขององค์กรได้ในที่สุด ดังนั้น องค์กรจึงจำเป็นต้องควบคุมการใช้งานโปรแกรมประเภท IM โดยเฉพาะควบคุมการ Upload/Download ไฟล์ผ่านทางโปรแกรมดังกล่าว ก็จะช่วยแก้ปัญหาความปลอดภัยได้ในระดับหนึ่ง

๑.๗ ภัยจากแฮกเกอร์มืออาชีพข้ามชาติ (Professional International Blackhat Attack)

ในปัจจุบันการโจมตีของแฮกเกอร์นั้นมักจะมีจุดมุ่งหมายชัดเจน เพื่อโจมตีบุคคลหรือองค์กรที่แฮกเกอร์ได้ทำการบ้านและวางแผนล่วงหน้ามาเป็นอย่างดี เรียกได้ว่าแฮกเกอร์ได้ทำการสืบข้อมูลของเหยื่อก่อนที่จะลงมือโจมตีเหยื่อ ซึ่งส่วนใหญ่แฮกเกอร์หวังผลทางด้านการเงิน ดังนั้นบุคคลระดับมหาเศรษฐีของโลกหลายคนล้วนเคยตกเป็นเหยื่อของแฮกเกอร์มา แล้วทั้งนั้น นอกจากวัตถุประสงค์ทางด้านการเงินแล้ว แฮกเกอร์ในบางประเทศก็มีวัตถุประสงค์ทางด้านการเมือง กล่าวคือ โจมตีเป้าหมายประเทศคู่แข่งโดยการเข้ามาล้วงความลับ หรือ "Spy" เพื่อหวังผลทางการเมืองระหว่างประเทศ ซึ่งเคยมีกรณีโจมตีรัฐบาลของประเทศสหรัฐ ประเทศอังกฤษ และประเทศเยอรมัน จากแฮกเกอร์ในประเทศแถบเอเชียมาแล้ว แฮกเกอร์ที่น่ากลัวและมีศักยภาพในการโจมตีสูงได้แก่ แฮกเกอร์จากประเทศจีนและรัสเซีย ดังนั้น ภัยจากแฮกเกอร์นั้นยังเป็นภัย "Classic" ที่เรายังมองข้ามไม่ได้ ยิ่งเป็นเรื่องของมั่นคงของชาติยิ่งต้องเพิ่มระดับของความปลอดภัยให้กับ ระบบมากขึ้นเท่านั้น

๑.๘ ภัยไร้สายจากการใช้งานอุปกรณ์ Mobile และ Wireless (Mobile/ Wireless Attack)

การโจมตีผ่านทางระบบไร้สายกำลังเป็นที่นิยมมากขึ้นในหมู่แฮกเกอร์ เนื่องจากเป็นการยากที่จะแกะรอยแฮกเกอร์และง่ายที่จะเข้าระบบ Wireless LAN ที่ไม่มีความปลอดภัยเพียงพอ ในปัจจุบันหลายองค์กรในกรุงเทพมหานครมีการเปิดใช้ Wireless LAN กันอย่างไม่ปลอดภัย รวมถึงผู้ใช้ ADSL ตามบ้านก็เช่นกัน เป็นเหตุให้แฮกเกอร์สามารถใช้สิ่งที่เรียกว่า " War Driving" และ "War Chalking" ในการเข้าโจมตีเครือข่าย Wireless LAN ผ่านทาง Access Point ที่ไม่ได้เข้ารหัส หรือมีการเข้ารหัสที่อ่อนแอเกินไป เช่น เข้ารหัสด้วย WEP Algorithm ดังนั้น การใช้งาน Wireless LAN จำเป็นต้องมีการเข้ารหัสที่ปลอดภัย ในปัจจุบันนิยมใช้ WPA version 2 Algorithm และควรมีการทำ Authentication เพื่อตรวจสอบชื่อผู้ใช้และรหัสผ่านก่อนการใช้งานทุกครั้ง นอกจากจะทำให้ปลอดภัยขึ้นแล้ว ยังเป็นการปฏิบัติตามประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารตาม พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 อีกด้วย อุปกรณ์ประเภทพกพา (Handheld) เช่น อุปกรณ์ PDA , Smart Phone หรือ Mobile Phone เองก็มีโอกาสถูกโจมตีแบบไร้สายเช่นกัน โดยส่วนใหญ่จะเป็นการโจมตีผ่านทาง WiFi หรือ Bluetooth ทำให้เจ้าของเครื่องถูกแอบขโมยโทรศัพท์ฟรีโดยเจ้าของเครื่องต้องเป็นคนจ่าย ค่าโทรศัพท์เอง หรือ ถูกแอบดึงข้อมูล address book หรือ SMS/MMS ออกจากเครื่องโดยที่เจ้าของไม่รู้ตัวเลย นอกจากนี้อาจทำให้เครื่องแฮงค์โดยไม่ทราบสาเหตุ หรือ โทรเข้า / ออกไม่ได้ เป็นต้น

๑.๙ ภัยจากการโจมตีด้วยเทคนิค DoS (Denial of Services) หรือ DDoS (Distributed Denial of Services) Attack

วัตถุประสงค์หลักของแฮกเกอร์หรือผู้ไม่หวังดีส่วนใหญ่จะทำการการขโมยข้อมูล การละเมิดความลับ (ความลับ - Confidentiality) หรือแอบแก้ไขข้อมูล (ความเชื่อถือได้ - Integrity) หรือทำให้ระบบของเป้าหมายไม่สามารถทำงานได้ตามปกติ (ความพร้อมใช้งาน - Availability) และการโจมตีโดยวิธีการที่เรียกว่า DoS หรือ DDoS Attack ซึ่งโดยปกติแล้วเว็บไซต์ประเภทออนไลน์เซอร์วิสหรืออีคอมเมิรส์ จะตกเป็นเป้าหมายของการโจมตีในลักษณะนี้ ทำให้เว็บไซต์ดังกล่าวไม่สามารถให้บริการได้ ส่งผลให้ลูกค้าเกิดความไม่พอใจ หรือ ทำให้ธุรกิจขาดรายได้ที่ควรจะได้ตามปกติปัจจุบันการแก้ปัญหาDoS หรือ DDoS Attack นิยมแก้ปัญหาโดยการใช้อุปกรณ์ ป้องกันการบุกรุก (IPS - Intrusion Prevention System) บางรุ่นที่มีความสามารถในการป้องกัน DoS หรือ DDoS Attack ได้เป็นอย่างดีการโจมตีในลักษณะนี้เป็นที่นิยมของผู้ก่อการร้ายไฮเทค(Cyber Terrorism) เรียกได้ว่าเป็นการก่อวินาศกรรมในโลกไซเบอร์ แต่มีผลกระทบในโลกของความเป็นจริงยกตัวอย่าง เช่น แฮกเกอร์บุกเข้าโจมตีระบบ SCADA ของการไฟฟ้าหรือการประปา เพื่อให้ไฟฟ้าดับหรือน้ำไม่ไหล หรือโจมตีเขื่อน เพื่อสั่งปล่อยน้ำออกจากเขื่อนโดยไม่ได้รับอนุญาต เป็นต้น

ในประเทศออสเตรเลีย เคยมีผู้ไม่หวังดีเข้าเจาะระบบ SCADA โดยผ่านทางอุปกรณ์ไร้สาย (Wireless LAN) เพื่อเข้ามาสั่งให้ระบบปล่อยน้ำเสียลงในแม่น้ำทำให้สัตว์น้ำต้องเสียชีวิต เป็นจำนวนมาก เป็นต้น

สรุปได้ว่าการโจมตีแบบนี้ส่วนใหญ่มักเกิดที่ ISP หรือ ผู้ให้บริการอินเทอร์เน็ต หรือไม่ก็เกิดขึ้นกับเว็บไซต์ยอดนิยมต่างๆ เช่น เว็บข่าว, เว็บกีฬา ,เว็บบันเทิงที่คนนิยมเข้าไปชมกันบ่อยๆ ดังนั้นเว็บไซต์เหล่านี้ควรมีการป้องกันที่เป็นระบบและควรทำการทดสอบการเจาะระบบ เพื่อเป็นการตรวจสอบว่าระบบมีความปลอดภัย และเพื่อเป็นการพิสูจน์ความแข็งแรงของระบบขององค์กรว่าจะสามารถทนทานต่อการโจมตีแบบ DoS หรือ DDoS Attack ได้

๑.๑๐ ภัยที่เกิดขึ้นจากตัวของเราเอง(Negligence Information Security)

จุดอ่อนที่อ่อนที่สุดในระบบ ก็คือ ตัวของเราเอง หรือ "P" = "People" ใน PPT (People Process and Technology) ซึ่งแนวความคิดในการโจมตีระบบส่วนใหญ่ปัจจุบันเน้นการใช้เทคนิค "Social Engineering" เพื่อหลอกเหยื่อให้หลงเข้าใจผิดในเรื่องที่แฮกเกอร์ปลอมแปลงแต่งขึ้นตาม วัตถุประสงค์ที่จะให้เหยื่อทำตามในสิ่งที่แฮกเกอร์ได้กำหนดไว้ล่วงหน้า เช่น ให้เหยื่อเปิดไฟล์มัลแวร์ที่เป็นโปรแกรมม้าโทรจัน เป็นต้น

จาก : หนังสือ eLeader Thailand ประจำเดือน เดือนกุมภาพันธ์ 2551

๑.๑๑ APT - Advanced Persistent Threat

ซึ่งจัดเป็นภัยคุกคามขั้นสูง ที่ระบุเป้าหมายการโจมตีที่ชัดเจน มีจุดประสงค์เพื่อขโมยข้อมูลสำคัญของเป้าหมายหรือสร้างความเสียหายให้มากที่สุด โดยมีความพยายามที่จะได้มาหรือแก้ไขเปลี่ยนแปลงข้อมูลด้วยวิธีที่ยากต่อการค้นพบ ยากที่จะกำจัดออกไป และยากที่จะสืบสาวว่าใครเป็นผู้กระทำ ส่วนประกอบสำคัญที่สุดของ APT คือความสามารถของผู้โจมตีที่จะปรับเปลี่ยนยุทธวิธีได้ตลอดเวลา ทำให้วิธีการป้องกันเดิมๆ ไม่สามารถรับมือกับการโจมตีแบบล่าสุดได้ เช่น โปรแกรมป้องกันไวรัสมักปล่อยให้ไวรัสที่เปลี่ยนแปลงตัวเองอัตโนมัติผ่านไปได้ ขณะที่ Firewall ไม่สามารถดักจับการโจมตีที่มากับการจราจรของข้อมูลสูงๆ ได้อย่างมีประสิทธิภาพ หรือกระบวนการปรับปรุงข้อมูลอัตโนมัติก็อาจจะปรับปรุงระบบปฏิบัติการไม่ทันผู้โจมตีเหล่านี้ที่ฉวยโอกาสค้นหาช่องโหว่ของแพตช์แล้วโจมตีผ่านช่องโหว่นั้นAPT มีองค์ประกอบ 3 อย่าง ดังนี้

Advanced - ผู้ที่โจมตี จะเป็นผู้ที่มีความสามารถและมีทรัพยากรที่พร้อมสำหรับการโจมตี วิธีการโจมตีจะใช้เครื่องมือและเทคนิคหลายอย่างไว้ด้วยกัน ซึ่งเป็นไปได้ตั้งแต่การใช้ความรู้ทางคอมพิวเตอร์ขั้นสูงเพื่อเจาะระบบ โดยเฉพาะในเรื่องการหลบเลี่ยงการตรวจจับ ไปจนถึงการใช้เทคนิคพื้นฐาน Social Engineering ซึ่งเป็นการโจมตีโดยอาศัยหลักจิตวิทยาเพื่อหลอกลวงคนให้เปิดเผยข้อมูลสำคัญ ส่วนใหญ่แล้วจะดำเนินงานกันเป็นกลุ่มมากกว่าทำคนเดียว และอาจจะเป็นไปได้ว่ามีแหล่งสนับสนุนเงินลงทุนในการปฏิบัติการนี้อยู่เบื้องหลัง เช่นการสนับสนุนโดยรัฐบาลที่เป็นปรปักษ์

Persistent – ลักษณะการโจมตีจะเป็นแบบค่อยเป็นค่อยไป เนื่องจากผู้โจมตีต้องแฝงตัวเข้าไปอยู่ในระบบโดยไม่ให้เป้าหมายรู้ตัว ซึ่งอาจต้องใช้เวลาแค่วันเดียว เป็นสัปดาห์ เป็นเดือนหรือนานจนเป็นปีก็ได้ จุดประสงค์เพื่อรอเวลาที่จะสร้างความเสียหาย หรือรวบรวมข้อมูลสำคัญที่ต้องการให้ได้มากที่สุดเท่าที่จะทำได้

timeThreat – คือภัยคุกคามที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสารซึ่งจะทำงานได้ด้วยตัวเองโดยรอเวลาหรือคำสั่งจากผู้ควบคุม อาทิเช่น ไวรัส บอทเน็ต ซอมบี้ หรือเวิร์ม เป็นต้น

๒. ตัวอย่างการถูกโจมตี

เหตุการณ์นี้เกิดขึ้นกับบริษัทโซนี่ซึ่งเป็นบริษัทอิเล็กทรอนิกส์ชั้นนำในด้านเครื่องใช้ไฟฟ้าและอิเล็กทรอนิกส์ และเป็นผู้ผลิตเครื่องเล่นเกมส์ชื่อดัง Playstation ได้ถูกโจมตีอย่างต่อเนื่องทำให้เกิดการรั่วไหลของข้อมูลสำคัญ ทำให้โซนี่ต้องหยุดการให้บริการเพลย์สเตชั่นเป็นเวลานาน นำมาซึ่งความเสียหายทางการเงินเป็นจำนวนมหาศาล playstation-retro-logo-sticker-700x700 อีกตัวอย่างเป็นการโจมตีที่เกิดขึ้นกับเครือข่ายของบริษัท ล็อกฮีด มาร์ติน (Lockheed Martin) ซึ่งเป็นบริษัทที่ผลิตเทคโนโลยีทางการทหารที่ใหญ่ที่สุดในโลก ถูกโจมตีเพื่อจารกรรมข้อมูลการออกแบบเครื่องบินรบและเทคโนโลยีอาวุธที่สำคัญโดยการโจมตีที่เกิดขึ้นกับโซนี่เกิดจากการบุกรุกเครื่องแม่ข่ายเว็บ (web server) ที่ไม่ได้แก้ไขช่องโหว่ของโซนี่เอง แต่การโจมตีที่เกิดกับ ล็อกฮีด มาร์ติน เป็นผลพวงมาจากการโจมตีที่เกิดขึ้นกับบริษัท RSA บริษัททางด้านความปลอดภัยเครือข่ายชื่อดัง โดยเริ่มแรกพนักงานของ RSA ได้รับอีเมลแนบไฟล์สเปรดชีทที่โจมตีช่องโหว่ Adobe Flash Player และติดตั้งประตูหลัง (backdoor) และส่วนประกอบอื่น ๆ ของมัลแวร์ จากนั้นมัลแวร์ดังกล่าวจึงถูกใช้เพื่อเข้าถึงระบบของ RSA และขโมยข้อมูลทางเทคนิคของ SecurID ซึ่งเป็นการยืนยันตัวตนสองปัจจัย (two-factor authentication) RSA ยืนยันว่าข้อมูลดังกล่าวถูกใช้เพื่อโจมตีล็อกฮีด มาร์ติน

ศึกษาหน่วยงานด้านไซเบอร์ของต่างประเทศ

๑ หน่วยงานไซเบอร์ของต่างประเทศ

๑.๑ **อิสราเอล** มีความสามารถในเชิงรุก แต่ระเบียบและกลยุทธ์ไม่เป็นที่เปิดเผยมากนัก มีองค์กรรับผิดชอบดังนี้

๑.๑.๑ หน่วย 8200 (Unit 8200) ของกองกำลังป้องกันอิสราเอล (Israel Defense Forces) ประกอบด้วยนายทหารและทหารที่เกณฑ์มา เน้นสงครามไซเบอร์อยู่สามส่วน คือ รวบรวมข่าวสาร ป้องกัน และโจมตี

แผนภาพที่ ๓ – ๑ Israel Defense Forces

๑.๑.๒ Shin Bet รับผิดชอบป้องกันระบบของรัฐบาล โครงสร้างพื้นฐานของชาติ และข้อมูลทางการเงิน

แผนภาพที่ ๓ – ๒ Emblem of the Shabak

๑.๑.๓ หน่วยงาน C^4I (ตั้งปลายทศวรรษ 1990) รับผิดชอบด้านการสื่อสารและการจัดองค์กรทางการป้องกันทางไซเบอร์

๑.๑.๔ หน่วย Matzov หรือ ศูนย์เข้ารหัสและความปลอดภัยสารสนเทศ ทำหน้าที่หาข่าวและเทคโนโลยีของฝ่ายตรงข้ามโดยเน้นเทคโนโลยีการเจาะระบบ นอกจากนั้นยังรับผิดชอบผลิตโปรแกรมเข้ารหัสให้กับโครงข่ายของกองกำลังป้องกันอิสราเอล, Shin Bet และ Mossad มีทีมทดสอบไฟล์วอลและการเข้ารหัส

๑.๑.๕ National Cybernetic Taskforce (ก่อตั้ง 18 พ.ค.54) เพื่อต่อต้างการเจาะระบบเข้าเครือข่ายสำคัญ และป้องกันอุตสาหกรรมภาคเอกชนจากการโดยดักขโมยข้อมูล เน้นเชิงรับ ให้การสนับสนุนการวิจัยและการสอนในมหาวิทยาลัยทางด้านความปลอดภัยไซเบอร์

๑.๒ อิหร่าน ทำงานโดยการประสานงานกันภายในกองทัพ

๑.๒.๑ หน่วยสงครามไซเบอร์ของ Islamic Revolutionary Guard ผู้ปฏิบัติงาน ๒,๔๐๐ คน งบประมาณ ๗๖ ล้านดอลล่าร์ (ใหญ่เป็นลำดับที่ ๒ ของโลก ข้อมูลปี ๒๐๑๐) มีการจ้างกลุ่มแฮกเกอร์จากภาคประชาชน คือ กลุ่ม Iranian Cyber Army (ซึ่งมีความสัมพันธ์กับกลุ่มแฮกเกอร์ Ashiyane)

แผนภาพที่ ๓ – ๓ Iranian Cyber Army

แผนภาพที่ ๓ – ๔ Ashiyane

๑.๒.๒ หน่วยงานตำรวจไซเบอร์ของอิหร่าน (ปี ๒๐๑๑) เพื่อตรวจกิจกรรมในเว็บเครือข่ายสังคม

แผนภาพที่ ๓ – ๕ Iranian Cyber Police

๑.๒.๓ Cyber Command (ประกาศแผนจัดตั้ง มิ.ย.๕๔) สำหรับกองทัพ เพื่อป้องกันการโจมตีทางไซเบอร์และรวมศูนย์การปฏิบัติการ

๑.๓ อเมริกา

๑.๓.๑ หน่วยงาน Homeland Security เน้นป้องกันภายในประเทศจากการโจมตีไซเบอร์ มีหน่วยงานย่อย คือ National Cyber Security Division ทำงานประสานกับภาคเอกชนและประสานงานกับต่างประเทศ ป้องกันโครงสร้างพื้นฐานของประเทศ และภายใน National Cyber Security Division มี National Cyber Response Coordination Group ซึ่งประกอบด้วยหน่วยงานรัฐ ๑๓ หน่วย คอยรับมือเหตุการณ์โจมตีทางไซเบอร์ระดับชาติ

๑.๓.๒ หน่วยงาน FBI

๑.๓.๓ กระทรวงกลาโหม

๑.๓.๔ หน่วยงาน US Cyber Command ซึ่งทำงานภายใต้ US Strategic Command รับผิดชอบภัยคุกคามที่เกิดกับโครงสร้างพื้นฐานทางไซเบอร์ของกองทัพ ประกอบด้วย Army Forces Cyber Command, the Twenty-fourth Air Force, Fleet Cyber Command และ Marine Forces Cyber Command นอกจากนี้ยังทำงานประสานกับ กระทรวงกลาโหมและ Homeland Security ภายใต้บันทึกข้อตกลงทางความปลอดภัยไซเบอร์เมื่อเดือนตุลาคม ๒๐๑๐

นอกจากนี้ นโยบายทบทวนไซเบอร์สเปซปี ๒๐๑๑ วางบทบาทให้กับหน่วยงานรัฐในการปกป้องโครงสร้างพื้นฐานไซเบอร์ โดยเพิ่มเจ้าหน้าที่ด้านความปลอดภัยไซเบอร์และเพิ่มความตระหนักต่อภัยคุกคามปัจจุบันต่อหน่วยงานรัฐ เนื้อหาหลายส่วนมีในกลยุทธความปลอดภัยแห่งชาติเมื่อปี ๒๐๑๐ เดือนพฤษภาคม ๒๐๑๑ กลยุทธไซเบอร์สเปซระหว่างชาติมีระบุว่า สหรัฐจะใช้ทุกวิถีทางที่จำเป็นในการปกป้องตนเองและมิตรประเทศจากภัยคุกคาม ก่อนจะใช้กำลังทหาร

๑.๔ เยอรมัน

๑.๔.๑ เยอรมันออกหลักนิยมใหม่เกี่ยวกับความปลอดภัยไซเบอร์ และกำลังก่อตั้งองค์กรใหม่ ๒ องค์กร เพื่อต่อสู้กับภัยคุกคามไซเบอร์ รัฐบาลเยอรมันวางแผนจะตั้งศูนย์ป้องกันภัยไซเบอร์แห่งชาติ (National Cyber defense Center) ในปี ๒๐๑๑ ภายใต้กระทรวงมหาดไทย (Ministry of the Interior) ศูนย์แห่งใหม่จะผสมผสานทรัพยากรจากหน่วยงานรัฐบาลหลายหน่วยงาน รวมถึงตำรวจจากรัฐบาลกลาง หน่วยข่าวกรองฝ่ายข่าวต่างประเทศ และมีตัวแทนจากภาคอุตสาหกรรมด้วย กลยุทธในปี ๒๐๑๑ เน้นไปที่ปกป้องโครงสร้างพื้นฐานทางสารสนเทศที่สำคัญ เสริมสร้างความปลอดภัยและความมั่นคงให้ระบบเทคโนโลยีสารสนเทศ ก่อตั้งศูนย์รับมือไซเบอร์แห่งชาติ (National Cyber Response Center) และสภาความปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Council) ปรับปรุงการบังคับใช้กฎหมาย สนับสนุนความร่วมมือกับนานาชาติ ทำให้เทคโนโลยีสารสนเทศเป็นที่เชื่อถือและไว้วางใจได้ และทำการฝึกอบรมผู้ทำงานไซเบอร์

๑.๔.๒ ศูนย์ป้องกันภัยไซเบอร์แห่งชาติ เป็นหน่วยงานหลักในการปกป้องความปลอดภัยไซเบอร์ของเยอรมัน มีหน้าที่รายงานสำนักงานความปลอดภัยสารสนเทศแห่งชาติ (Federal Office for Information Security) แต่ไม่มีศักยภาพในการจู่โจม หน่วยงานใหม่นี้เริ่มจากคณะทำงาน ๖ ท่านจากหน่วยงานความปลอดภัยของเยอรมัน BSI ๒ ท่านจากสำนักงานปกป้องรัฐธรรมนูญของเยอรมัน (German Office for the Protection of the Constitution) ซึ่งเป็นหน่วยข่าวกรองภายใน และ ๒ ท่านจากสำนักงานปกป้องพลเรือนและช่วยบรรเทาหายนภัยแห่งชาติ (the Federal Office of Civil Protection and Disaster Assistance หรือ BBK) ในอนาคต สำนักงานตำรวจแห่งชาติ, สำนักงานสืบสวนอาชญากรรมแห่งชาติ, Bundesnachrichtendienst, Bundeswehr, และสำนักงานสืบสวนอาชญากรรมทางศุลกากร จะส่งผู้เชี่ยวชาญเข้าร่วมทำงานด้วย สภาความปลอดภัยไซเบอร์แห่งชาติ รับผิดชอบประสานงานด้านเทคนิคการป้องกันและนโยบายไซเบอร์ ตัวแทนอาวุโสจากกองทัพก็จะเข้าร่วมด้วย

๑.๔.๓ หน่วยงานทางทหารของเยอรมันและหน่วยข่าวกรองมีหน่วยไซเบอร์ภายในด้วย หน่วยงานความปลอดภัยของเยอรมัน BSI กำลังลงทุนวิจัยและพัฒนาศักยภาพทางไซเบอร์ กระทรวงปฏิบัติการเครือข่ายคอมพิวเตอร์และสารสนเทศ ร่วมกับหน่วยหาข้อมูลทางกลยุทธเบื้องต้นที่เป็นหน่วยใน Bundeswehr โดยมีนายพลกองทัพอากาศเป็นผู้นำ พร้อมบุคลากรกองทัพอีก ๗๖ ท่าน จากแผนกวิทยาการคอมพิวเตอร์ใน Bundeswehr จะพัฒนาศักยภาพทั้งทางเชิงรุกและเชิงรับ

๑.๕ อังกฤษ

๑.๕.๑ กลยุทธความปลอดภัยไซเบอร์ของอังกฤษ เผยแพร่เมื่อ เดือนมิถุนายน ๒๐๐๙ ประกอบด้วยแนวทาง ๓ ประการ คือ ลดความเสี่ยง ฉกฉวยโอกาส และพัฒนาการตอบสนองต่อเหตุการณ์ไซเบอร์ ประการแรก คือลดความเสี่ยงโดยลดช่องโหว่และลดผลกระทบจากเหตุการณ์ไซเบอร์ ประการต่อมา

คือฉกฉวยโอกาส ทางอังกฤษจะรวบรวมข่าวกรอง สนับสนุนนโยบายของรัฐบาล และดำเนินการกับฝ่ายตรงข้าม ประการสุดท้าย พัฒนาการตอบสนองต่อเหตุการณ์ไซเบอร์โดยการเพิ่มความรู้และความตระหนัก พัฒนาหลักนิยมและนโยบาย พัฒนาธรรมาภิบาลและโครงสร้างการตัดสินใจ ขยายศักยภาพทางเทคนิคและบุคลากร ในปี ๒๐๑๐ กลยุทธความปลอดภัยไซเบอร์แห่งชาติเน้นที่ "การถูกโจมตีเครือข่ายไซเบอร์ของอังกฤษจากประเทศฝ่ายตรงข้าม และอาชญากรรมไซเบอร์ขนาดใหญ่" ให้เป็นสิ่งจำเป็นสูงสุดในการรักษาความปลอดภัยไซเบอร์ อังกฤษกำหนดงบประมาณ ๖๕๐ ล้านปอนด์สำหรับแผนสี่ปี (๒๐๐๙ - ๒๐๑๓) ตามเอกสารทบทวนกลยุทธด้านการป้องกันและความปลอดภัยปี ๒๐๑๐

๑.๕.๒ ศูนย์ปฏิบัติการความปลอดภัยไซเบอร์ รับผิดชอบพัฒนาศักยภาพทั้งทางด้านการโจมตีและการป้องกัน งานหลักคือคอยเฝ้าระวังการพัฒนาและสภาพการใช้งานระบบเทคโนโลยีสารสนเทศของรัฐบาล วิเคราะห์แนวโน้มและปรับปรุงการรับมือเหตุการณ์ไซเบอร์ ศูนย์ปฏิบัติการความปลอดภัยไซเบอร์กำหนดปฏิบัติการต้นปี ๒๐๑๑ โดยมีผู้ทำงานเริ่มต้น ๑๙ ท่าน ศูนย์ปฏิบัติการความปลอดภัยไซเบอร์ไม่ได้รับงบประมาณช่วงปี ๒๐๐๙ - ๒๐๑๐ ดังนั้น ศูนย์บัญชาการสื่อสารของรัฐบาล คณะรัฐมนตรี หน่วยงานรักษาความปลอดภัยและบังคับใช้กฎหมายได้ร่วมกันออกค่าใช้จ่ายเบื้องต้นให้

๑.๕.๓ สำนักงานความปลอดภัยไซเบอร์และสร้างความมั่นใจระบบสารสนเทศ (The Office of Cyber Security and Information Assurance) ประสานงานกับสำนักงานคณะรัฐมนตรีเรื่องนโยบายและกลยุทธของรัฐบาล โดยเน้นไปที่สนับสนุนด้านการศึกษา และการสร้างความตระหนักด้านไซเบอร์และส่งเสริมความร่วมมือกับนานาชาติ ผู้อำนวยการสำนักงานความปลอดภัยไซเบอร์และสร้างความมั่นใจระบบสารสนเทศรายงานตรงไปยังคณะที่ปรึกษาความมั่นคงแห่งชาติ (National Security Advise) ค่าใช้จ่ายในการดำเนินงานสำนักงานความปลอดภัยไซเบอร์และสร้างความมั่นใจระบบสารสนเทศประจำปีงบประมาณ ๒๐๐๙ - ๒๐๑๐ อยู่ที่ ๑๓๐,๐๐๐ ปอนด์ อังกฤษวางแผนลงทุน ๑.๐๖ พันล้านเหรียญสหรัฐระยะเวลา ๔ ปี ในความพยายามด้านความปลอดภัยไซเบอร์

๑.๖ **สวีเดน**

สวีเดนประกาศนโยบายและจัดตั้งสถาบันเพื่อรับมือภัยคุกคามไซเบอร์ หน่วยงานพันธกิจประชาชน (Civil Contingencies Agency หรือ MSB) จะก่อตั้งศูนย์ประสานงานปฏิบัติการไซเบอร์แห่งชาติขึ้น ศูนย์ฯ นี้เน้นที่งานป้องกันและประสานงานการรับมือเหตุการณ์ไซเบอร์ และทางศูนย์ฯ นี้จะทำงานร่วมกับกองทัพสวีเดนอย่างใกล้ชิด เพื่อวิเคราะห์ระบบในอนาคตที่จะปกป้องสารสนเทศอันเป็นความลับของชาติ ในปี ๒๐๑๑ สวีเดนประกาศแผนรับมือเหตุการณ์ทางเทคโนโลยีสารสนเทศแห่งชาติที่เป็นเหตุการณ์รุนแรง (National Response Plan for Serious IT Incidents) เน้นไปที่แนวทางร่วมมือกับภาคอุตสาหกรรมและหน่วยงานอื่นเพื่อลดผลร้ายจากภัยคุกคามไซเบอร์

๒ ภูมิภาคเอเชีย

๒.๑ จีน

๒.๑.๑ คณะกรรมาธิการทหารกลางของจีนกำหนดให้ Informationalization เป็นปัจจัยสำคัญในการขยายขีดความสามารถในการต่อสู้ของกองทัพ และกองทัพปลดปล่อยประชาชนใช้ Informationalization โดยเน้นเป็นทิศทางและกลยุทธของกองทัพ หลักนิยมทางทหารของจีนกำหนดให้ทุ่มเทความพยายามให้กับการผสมผสานความสามารถการรบในทางไซเบอร์และอิเล็กทรอนิกส์หากมีการกระทบกระทั่งหรือมีความขัดแย้งเกิดขึ้น

๒.๑.๒ กองทัพอากาศของกองทัพปลดปล่อยประชาชนรับผิดชอบด้านปฏิบัติการข่าวสารและต่อต้านมาตรการข่าวสาร แต่ผู้สังเกตการณ์ภายนอกเชื่อว่า กรมที่ 4 ซึ่งรับผิดชอบต่อต้านมาตรการทางอิเล็กทรอนิกส์ร่วมกับสถาบันวิจัย นอกจากทำการพัฒนาเทคโนโลยีสงครามสารสนเทศแล้ว ยังทำหน้าที่รับผิดชอบเพิ่มศักยภาพทางไซเบอร์ของกองทัพอีกด้วย กรมที่ 3 รับผิดชอบงานข่าวกรองจากการดักสัญญาณ ทำหน้าที่รวบรวม วิเคราะห์ และเจาะสารสนเทศอิเล็กทรอนิกส์ ทั้งกรมที่ 4 และ 3 ทำงานวิจัยขั้นสูงด้านความปลอดภัยสารสนเทศ นอกจากนี้ กองทัพปลดปล่อยประชาชนยังทำงานร่วมกับมหาวิทยาลัยและเอกชนอย่างใกล้ชิด โดยกองทัพบางหน่วยตั้งอยู่ในองค์กรการค้าและมหาวิทยาลัย

๒.๒ อินเดีย

ช่วงปลายทศวรรษ 1990 กองทัพอินเดียได้เพิ่มการสงครามอิเล็กทรอนิกส์และปฏิบัติการข่าวสารเข้าไปในหลักนิยม เพื่อทำให้กองทัพทันสมัยในสี่ด้านด้วยกัน คือ เทคโนโลยีสารสนเทศ สงครามอิเล็กทรอนิกส์ การปกป้องโครงสร้างพื้นฐาน และกองทัพที่คล่องตัว ในเดือนธันวาคม 2009 เจ้าหน้าที่ระดับสูงในกองทัพอินเดีย ได้เน้นความจำเป็นที่อินเดียต้องพัฒนาศักยภาพในการต่อสู้ภัยคุกคาม โดยเฉพาะภัยคุกคามไซเบอร์

อินเดียมีหน่วยงานในกลาโหมหลายหน่วยที่รับผิดชอบด้านความปลอดภัยไซเบอร์ หน่วย Defence Information Warfare Agency ทำหน้าที่ประสานงานเพื่อตอบสนองการสงครามสารสนเทศ หน่วย Defence Intelligence Agency และ National Technical Intelligence Communication Center ร่วมกันตั้งชุด Cybersquad เพื่อค้นหาช่องโหว่ในระบบของรัฐบาล หน่วย Defense Research and Development Organization รับผิดชอบทดสอบระบบสงครามอิเล็กทรอนิกส์

ปี 2005 กองทัพอินเดียได้จัดให้มีงานความปลอดภัยไซเบอร์ในระดับแผนกและจัดให้มีการตรวจสอบด้านความปลอดภัย ในเดือน เมษายน 2010 ได้จัดให้มีห้องทดลองความปลอดภัยไซเบอร์ในวิทยาลัยวิศวกรรมสื่อสารของกองทัพ

ส่วนวิจัยและวิเคราะห์ในสำนักนายกรัฐมนตรีเป็นส่วนหลักในการข่าวกรองทางอิเล็กทรอนิกส์ ซึ่งมีศูนย์สื่อสารข่าวกรองเทคนิคแห่งชาติ ให้ข่าวกรองทางเทคนิคและทางอิเล็กทรอนิกส์แก่หน่วยงานต่างๆ และดักรับการสื่อสารของฝ่ายตรงข้าม

ไม่นานมานี้ บอร์ดที่ปรึกษาความปลอดภัยแห่งชาติได้แนะนำให้จัดตั้งศูนย์บัญชาการความปลอดภัยไซเบอร์กลางตามแบบอย่างศูนย์บัญชาการไซเบอร์ของอเมริกา

ปัจจุบันนี้ องค์การวิจัยเทคนิคแห่งชาติ ร่วมกันหน่วยงานข่าวกรองกลาโหมได้พัฒนาศักยภาพในการจู่โจมไซเบอร์

นอกจากนี้อินเดียยังทำบันทึกความเข้าใจที่ไม่ผูกมัดกับอเมริกาในความร่วมมือทางเทคนิคและการปฏิบัติการเพื่อขัดขวางภัยคุกคามไซเบอร์

๒.๓ สิงคโปร์

นโยบายไซเบอร์สิงคโปร์เน้นความปลอดภัยเทคโนโลยีสารสนเทศและอุตสาหกรรมการสื่อสาร Singapore Infocomm Technology Security Authority คอยดูแลปฏิบัติการความปลอดภัยทางเทคโนโลยีสารสนเทศและปกป้องสิงคโปร์จากภัยคุกคามระดับชาติ หน่วยงานนี้ทำงานภายใต้กรมความปลอดภัยภายใน (Internal Security Department) กระทรวงกิจการภายใน (Ministry of Home Affairs) หน่วยงานนี้ได้จัดทำรายชื่อมืออาชีพทางสารสนเทศให้ช่วยป้องกันทางไซเบอร์

คณะกรรมการความมั่นคงปลอดภัยของชาติ Infocomm ได้จัดทำนโยบายไซเบอร์และกลยุทธความปลอดภัย คณะกรรมการอยู่ภายใต้โครงข่ายของ Singapore Infocomm Development Authority มีการออกแผนแม่บทความปลอดภัย Infocomm ในปี 2005 เพื่อให้เกิดความมั่นใจความปลอดภัยทางไซเบอร์ โดยแผนแม่บทนี้นำโดย Infocomm Development Agency เพื่อให้เกิดความปลอดภัยต่อประชากร ภาคเอกชน และภาครัฐ โดยสร้างความตระหนักต่อความเสี่ยงทางไซเบอร์ พัฒนามาตรการความปลอดภัยที่เหมาะสม พัฒนาศักยภาพของชาติและขยายขอบเขตในการวิจัยและพัฒนาเทคโนโลยีด้านความปลอดภัย และพัฒนาให้โครงสร้างพื้นฐานที่สำคัญสามารถใช้งานได้ตลอดเวลาเมื่อมีเหตุฉุกเฉิน นำมาซึ่งการจัดตั้ง ศูนย์เฝ้าระวังภัยคุกคามไซเบอร์แห่งชาติ

๒.๔ มาเลเซีย

กระทรวงกลาโหมของมาเลเซียดำเนินนโยบายความปลอดภัยเทคโนโลยีสารสนเทศเพื่อป้องกันรัฐบาลและธุรกิจจากการโจมตีไซเบอร์ ภารกิจส่วนหนึ่ง คือ สร้างความมั่นใจต่อความปลอดภัยในระบบเครือข่ายและป้องกันเหตุการณ์ไซเบอร์ไม่ให้มีผลระทบต่อเศรษฐกิจอย่างร้ายแรง นายกรัฐมนตรีของมาเลเซียเริ่มโครงการความปลอดภัยไซเบอร์ (Cyber Security Malaysia) ในการประชุมสภาเทคโนโลยีสารสนเทศแห่งชาติในปี ๒๐๐๗ โครงการนี้เป็นส่วนหนึ่งของกระทรวงวิทยาศาสตร์ เทคโนโลยีและนวัตกรรม โดยทางโครงการได้ดำเนินงานศูนย์ช่วยเหลือผู้ใช้งานอินเตอร์เน็ต ศูนย์อบรมสำหรับผู้ประกอบอาชีพด้านนี้ และแจ้งข่าวภัยคุกคามไซเบอร์ต่อสาธารณะอย่างสม่ำเสมอ ทางหน่วยงานได้เข้าไปเกี่ยวข้องกับการบังคับใช้กฎหมายเพื่อต่อสู้กับอาชญากรรมไซเบอร์ หลังจากการโจมตีไซเบอร์ต่อเนื่องหลายครั้งต่อเว็บไซต์ของรัฐบาลเมื่อมิถุนายน ๒๐๑๑ ทางรัฐบาลมาเลเซียได้ประกาศว่าจะเริ่มนำกฎหมายใหม่ๆ ที่เกี่ยวกับความปลอดภัยไซเบอร์มาใช้ รวมถึงวิธีการเข้ารหัสข้อมูลที่ดีกว่าเดิม ดังนี้

Communications & Multimedia Act 1998
Malaysian Communications & Multimedia Commission Act 1998
Digital Signature Act 1997
Computer Crimes Act 1997
Telemedicine Act 1997
Optical Discs Act 2000
Copyright Act 1987
Trade Marks Act 1976
Patents Act 1983
Industrial Designs Act 1996
Layout Designs of Integrated Circuits Act 2000
Geographical Indications Act 2000
Trade Description Act 1972
Intellectual Property Corporation of Malaysia Act 2002
E-Commerce Act

การโจมตีมาเลเซีย เมื่อ มิถุนายน ๒๐๑๑ เป็นการโจมตีจากกลุ่ม Anonymous ในปฏิบัติการ Operation Malaysia เพื่อประท้วงรัฐบาลมาเลเซียที่ใช้กฎหมายปิดกั้นสื่อภาพยนตร์และโทรทัศน์

อย่างเข้มงวด รวมถึงปิดกั้นเว็บไซต์ Pirate Bay และ WikiLeaks เว็บที่ถูกโจมตีมีจำนวน ๙๑ แห่ง ในจำนวนนี้ ๕๑ แห่ง เกี่ยวข้องกับรัฐบาล ลักษณะการโจมตีเพื่อให้เว็บใช้งานไม่ได้

๒.๕ พม่า

กรมคอมพิวเตอร์บริการกลาโหม (Defense Services Computer Directorate) ซึ่งก่อตั้งช่วงทศวรรษ ๑๙๙๐ เพื่อให้กองทัพทันสมัย ได้ปรับภารกิจให้ครอบคลุมการสงครามที่มีศูนย์กลางบนเครือข่าย เพิ่มศักยภาพทางไซเบอร์ และการสงครามอิเล็กทรอนิกส์ กลยุทธของกองทัพพม่าขยายครอบคลุมการสงครามไซเบอร์ ในฐานะที่เป็นส่วนหนึ่งของสงครามประชาชนภายใต้สภาวะการณ์ทันสมัย คาดการณ์ว่าสภาสันติภาพและการพัฒนาแห่งรัฐ (State Peace and Development Council) ซึ่งควบคุมกองทัพอยู่ได้รับเทคโนโลยีการสงครามไซเบอร์จากประเทศในเอเชีย

๒.๖ เวียดนาม

กรมขนส่งและเทคโนโลยีทั่วไป สังกัดกระทรวงความปลอดภัยสาธารณะของเวียดนาม, ทีมตอบสนองเหตุฉุกเฉินด้านคอมพิวเตอร์ของเวียดนาม, และกลุ่มข้อมูลระหว่างชาติ ดำเนินการต่อเนื่องเพื่อร่างแผนความปลอดภัยสารสนเทศล่วงหน้าเพื่อใช้ตลอดทศวรรษถัดไป เวียดนามมีแผนลงทุน ๔๒ ล้านเหรียญสหรัฐ เพื่อปกป้องข้อมูลสำคัญที่อ่อนไหว และจัดตั้งศูนย์เทคโนโลยีแห่งชาติหนึ่งแห่ง และหน่วยงานความปลอดภัยสารสนเทศหนึ่งแห่ง

ศึกษาหน่วยงานด้านไซเบอร์ในประเทศไทย

หน่วยงานด้านไซเบอร์ระดับชาติ ซึ่งมีความเกี่ยวข้องกับการปฏิบัติด้านไซเบอร์ของกระทรวงกลาโหม ประกอบด้วยหน่วยด้านนโยบาย/ยุทธศาสตร์ และหน่วยด้านปฏิบัติ ดังนี้

๑. สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ มีทำหน้าที่โดยสรุป คือ ทำหน้าที่เป็นเลขานุการสำหรับงานด้านไซเบอร์ระดับชาติ นอกจากนี้ยังมีหน้าที่เกี่ยวข้องสำคัญในการดำเนินการให้ธุรกรรมอิเล็กทรอนิกส์ของประเทศไทยมีความมั่นคงปลอดภัย ซึ่งเป็นส่วนประกอบหนึ่งที่สำคัญของการพัฒนาเศรษฐกิจของชาติ

๒. ศูนย์ประสานการรักษาความระบบปลอดภัยคอมพิวเตอร์ประเทศไทย (ThaiCERT) สังกัดสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ซึ่งจัดตั้งตั้งแต่ปี พ.ศ.๒๕๔๓ ทำหน้าที่ตอบสนอง รับมือและจัดการกับเหตุการณ์ความมั่นคงปลอดภัยคอมพิวเตอร์ (Incident Response) ให้คำแนะนำ เกี่ยวกับภัยคุกคามทาง และให้การสนับสนุนที่จำเป็น รวมทั้งติดตามและเผยแพร่ข่าวสารและเหตุการณ์ทางด้านความมั่นคงปลอดภัยทางด้านคอมพิวเตอร์ต่อสาธารณชน ตลอดจนทำการศึกษาและพัฒนา

เครื่องมือและแนวทางต่างๆ ในการปฏิบัติเพื่อเพิ่มความมั่นคงปลอดภัยในการใช้คอมพิวเตอร์และเครือข่ายอินเทอร์เน็ต รวมทั้งประสานงานระหว่างหน่วยงานต่างประเทศที่เป็นสมาชิกขององค์กรระดับภูมิภาคและระดับสากลด้านความมั่นคงปลอดภัยคอมพิวเตอร์ และกับหน่วยงานในประเทศ ทั้งภาครัฐ เอกชน มหาวิทยาลัย ผู้ให้บริการอินเทอร์เน็ต หรือผู้เกี่ยวข้อง ในการตอบสนองและจัดการกับเหตุการณ์ความมั่นคงปลอดภัยที่ได้รับแจ้ง ปัจจุบันเป็นหน่วยงานสังกัด สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

หน่วยงานด้านไซเบอร์ในกระทรวงกลาโหมและหน่วยงานที่เกี่ยวข้อง

หน่วยงานด้านไซเบอร์ของกระทรวงกลาโหม ประกอบด้วยหน่วยรับผิดชอบด้านนโยบาย/ยุทธศาสตร์ กับหน่วยรับผิดชอบด้านปฏิบัติ ซึ่งองค์ประกอบของหน่วยงานรวมถึงคณะกรรมการที่มีหน้าที่รับผิดชอบเกี่ยวข้องกับงานด้านไซเบอร์ของกระทรวงกลาโหม ต้องพิจารณาดำเนินการเปลี่ยนแปลงให้สอดคล้องและรองรับกับทิศทางการรักษาความมั่นคงปลอดภัยไซเบอร์ระดับชาติต่อไป ซึ่งเมื่อดำเนินการแล้วเสร็จจะสามารถสนับสนุนการพัฒนา การใช้ และการบริการจัดการศักยภาพด้านไซเบอร์ของกระทรวงกลาโหม ให้เป็นไปอย่างมีประสิทธิภาพยิ่งขึ้น หากพิจารณาถึงหน่วยงานที่มีอยู่ทั้งของกระทรวงกลาโหมและหน่วยงานที่เกี่ยวข้องในปัจจุบัน มีรายละเอียดดังนี้

๑. หน่วยงานด้านไซเบอร์ที่รับผิดชอบด้านนโยบาย/ยุทธศาสตร์ของกระทรวงกลาโหม ได้แก่ ศูนย์รักษาความปลอดภัยคอมพิวเตอร์ กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม มีหน้าที่โดยสรุป คือ ประสานงานในด้านนโยบาย/ยุทธศาสตร์ไซเบอร์ทั้งที่ได้รับมอบหมายจากระดับชาติ และที่อยู่ในขอบเขตความรับผิดชอบของกระทรวงกลาโหม แปลงนโยบาย/ยุทธศาสตร์เพื่อนำไปสู่การกำหนดแนวทางปฏิบัติ ซึ่งการปฏิบัติงานที่สำคัญได้แก่ การดำเนินการจัดทำยุทธศาสตร์การป้องกันไซเบอร์กระทรวงกลาโหมการดำเนินการเพื่อการพิจารณาแต่งตั้งคณะกรรมการการป้องกันไซเบอร์กระทรวงกลาโหมเพื่อทำหน้าที่พิจารณา กลั่นกรอง ตัดสินใจ กำหนดแนวทางด้านนโยบาย/ยุทธศาสตร์ไซเบอร์ของกระทรวงกลาโหม เป็นต้น

ศูนย์รักษาความปลอดภัยคอมพิวเตอร์ มีความสัมพันธ์และการประสานงานกับหน่วยไซเบอร์ของกองบัญชาการกองทัพไทย และเหล่าทัพ ในด้านนโยบายและยุทธศาสตร์ การสนับสนุนและการดำเนินการในภาพรวมของทั้งกระทรวงกลาโหม นอกจากนี้ยังมีความสัมพันธ์กับหน่วยไซเบอร์ภายนอกกระทรวงกลาโหมเพื่อเตรียมความพร้อมและการประสานงานการปฏิบัติด้านไซเบอร์ร่วมกับหน่วยรับผิดชอบอื่น ๆ ภายนอกกระทรวงกลาโหม เช่น กระทรวงเทคโนโลยีสารสนเทศ ศูนย์ประสานการรักษาความปลอดภัยระบบคอมพิวเตอร์ประเทศไทย รวมทั้งหน่วยรับผิดชอบโครงสร้างพื้นฐานสำคัญของรัฐ และความร่วมมือด้านไซเบอร์กับมิตรประเทศ เป็นต้น

ศูนย์รักษาความปลอดภัยคอมพิวเตอร์ ยังมีหน้าที่ในฐานะหน่วยปฏิบัติในขอบเขตความรับผิดชอบต่อหน่วยงานในสังกัดสำนักงานปลัดกระทรวงกลาโหม รวมทั้งมีหน้าที่รับผิดชอบในฐานะเป็นองค์ประกอบหนึ่งของศูนย์ประสานการรักษาความปลอดภัยระบบคอมพิวเตอร์กระทรวงกลาโหม (MODCERT) ซึ่งอยู่ระหว่างการจัดตั้งเพื่อรองรับแนวทางการบริหารจัดการด้านไซเบอร์ระดับชาติ

๒. หน่วยงานด้านไซเบอร์ที่รับผิดชอบด้านปฏิบัติของกระทรวงกลาโหม ประกอบด้วย

๒.๑ กองรักษาความปลอดภัยสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร มีความรับผิดชอบหลักในด้านการบริการและการรักษาความปลอดภัยระบบสารสนเทศของกองบัญชาการกองทัพไทย และมีหน้าที่รับผิดชอบในฐานะเป็นองค์ประกอบหนึ่งของศูนย์ประสานการรักษาความปลอดภัยระบบคอมพิวเตอร์กระทรวงกลาโหม (MODCERT)

๒.๒ กองปฏิบัติการสงครามเครือข่าย สำนักปฏิบัติการ กรมยุทธการทหาร มีความรับผิดชอบหลักในการจัดการและบูรณาการการปฏิบัติการไซเบอร์ในระดับกองทัพไทย เช่น จัดทำยุทธศาสตร์การปฏิบัติการไซเบอร์ของกองทัพไทย เป็นต้น และมีหน้าที่รับผิดชอบในฐานะเป็นองค์ประกอบหนึ่งของศูนย์ประสานการรักษาความปลอดภัยระบบคอมพิวเตอร์กระทรวงกลาโหม (MODCERT)

๒.๓ ศูนย์ไซเบอร์กองทัพบก (เป็นหน่วยงานที่แปรสภาพจากศูนย์เทคโนโลยีทางทหาร) มีความรับผิดชอบหลักในการปฏิบัติการไซเบอร์ของกองทัพบก เพื่อสนับสนุนการปฏิบัติภารกิจในความรับผิดชอบ และมีหน้าที่รับผิดชอบในฐานะเป็นองค์ประกอบหนึ่งของศูนย์ประสานการรักษาความปลอดภัยระบบคอมพิวเตอร์กระทรวงกลาโหม (MODCERT)

๒.๔ กองสงครามไซเบอร์ กองสงครามไซเบอร์ สำนักปฏิบัติการ กรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ มีความรับผิดชอบหลักในการปฏิบัติการไซเบอร์ของกองทัพเรือ เพื่อสนับสนุนการปฏิบัติภารกิจในความรับผิดชอบ และมีหน้าที่รับผิดชอบในฐานะเป็นองค์ประกอบหนึ่งของศูนย์ประสานการรักษาความปลอดภัยระบบคอมพิวเตอร์กระทรวงกลาโหม (MODCERT)

๒.๕ กองสงครามไซเบอร์ สำนักระบบบัญชาการและควบคุม กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ มีความรับผิดชอบหลักในการปฏิบัติการไซเบอร์ของกองทัพอากาศ เพื่อสนับสนุนการปฏิบัติภารกิจในความรับผิดชอบ และมีหน้าที่รับผิดชอบในฐานะเป็นองค์ประกอบหนึ่งของศูนย์ประสานการรักษาความปลอดภัยระบบคอมพิวเตอร์กระทรวงกลาโหม (MODCERT)

๓. สมาคมความมั่นคงปลอดภัยระบบสารสนเทศ (Thailand Information Security Association; TISA) เป็นสมาคมไม่แสวงหากำไรของกลุ่มนักวิชาชีพด้านความมั่นคงปลอดภัยสารสนเทศในประเทศไทย

๔. ประชาคมความมั่นคงปลอดภัยไซเบอร์ (Thailand Cybersecurity Community) ไม่ใช่หน่วยงานแต่เป็นการรวมตัวของหน่วยงานเป็นประชาคมที่มีวัตถุประสงค์และกิจกรรมสร้างเครือข่ายความร่วมมือการรักษาความ มั่นคงปลอดภัยไซเบอร์ของประเทศไทย โดยมีกระทรวงกลาโหมโดยศูนย์รักษาความปลอดภัยคอมพิวเตอร์ กรมเทคโนโลยีสารสนเทศ เป็นเจ้าภาพ สมาชิกจากทุกภาคส่วน เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยเกิดความเข้มแข็ง สามารถรับมือกับภัยคุกความทั้งในปัจจุบันและอนาคต ทำหน้าที่ส่งเสริมเผยแพร่ และแลกเปลี่ยนความรู้ เทคโนโลยี แนวทางปฏิบัติของการรักษาความมั่นคงปลอดภัย ไซเบอร์ รวบรวมเหตุภัยคุกคาม ผลกระทบ และแนวทางแก้ไข เพื่อแบ่งปันแจ้งเตือนให้สมาชิกเตรียมการป้องกันและหาหนทางแก้ไข ระดมสมอง ทรัพยากร และกำลังคนเข้าช่วยเหลือ แก้ปัญหาต่าง ๆ ของสมาชิก รวมทั้งการพัฒนาบุคลากร และการแลกเปลี่ยนบุคลากร และสร้างกระแส ความรู้ ความเข้าใจ ที่ถูกต้องในสังคม

สรุป

ภัยคุกคามไซเบอร์ทำให้เกิดความเสียหายต่อบุคคล ต่อองค์กร ต่อสังคม ต่อเศรษฐกิจ และทำให้เกิดความเสียหายต่อความมั่นคงของประเทศในที่สุด รูปแบบการโจมตีมีหลากหลาย และมีการพัฒนาวิธีการใหม่ ๆ อยู่ตลอดเวลา ซึ่งบางครั้งอาจจะใช้วิธีการเดิม ๆ แต่ใช้ความพยายามอย่างต่อเนื่อง หรืออาจจะทำงานเป็นทีมที่มีการสนับสนุนจากรัฐจนพบช่องโหว่หรือจุดอ่อนจนสามารถโจมตีได้สำเร็จ ดังนั้นการป้องกันต้องมีการดำเนินการอย่างต่อเนื่องเช่นเดียวกัน ในหลาย ๆ ประเทศรวมถึงประเทศไทยได้ตระหนักถึงอันตรายจากภัยคุกคามไซเบอร์ ได้เริ่มดำเนินการกับไซเบอร์อย่างจริงจัง มีการจัดตั้งหน่วยงาน มีการสร้างความตระหนัก และประสานความร่วมมือระหว่างประเทศมากขึ้น แต่ภัยคุกคามไซเบอร์ยังไม่หมดไป ดังนั้นจึงจำเป็นต้องดำรงความต่อเนื่องในการดำเนินการป้องกันไซเบอร์ของประเทศและกระทรวงกลาโหมต่อไป

บทที่ ๔

วิเคราะห์เพื่อกำหนดยุทธศาสตร์การป้องกันไซเบอร์ กระทรวงกลาโหม

การป้องกันไซเบอร์ของต่างประเทศ

๑ เอกสาร The DoD CYBER STRATEGY, 17 April 2015

๑.๑ ภัยคุกคามหลักทางไซเบอร์

ในปี ค.ศ.๒๐๑๕ ผู้อำนวยการสำนักข่าวกรองแห่งชาติของสหรัฐฯ ได้กล่าวถึงภัยคุกคามทางไซเบอร์ไว้ว่าเป็นภัยคุกคามทางยุทธศาสตร์อันดับหนึ่งต่อสหรัฐฯ เป็นครั้งแรกที่ถูกจัดวางไว้เหนือหัวข้อการก่อการร้าย นับตั้งแต่เหตุการณ์การโจมตีวันที่ ๑๑ กันยายน ค.ศ.๒๐๐๑ ฝ่ายตรงข้ามได้ปฏิบัติการทางไซเบอร์ที่ชั่วร้ายต่อผลประโยชน์ของสหรัฐฯ ที่กระจายอยู่ทั่วโลก และในลักษณะที่ต้องการทดสอบขีดจำกัดว่าสหรัฐฯ และชุมชนนานาชาติจะทนรับได้เพียงใด แฮกเกอร์อาจเจาะเข้าเครือข่ายและระบบต่าง ๆ ของสหรัฐฯ โดยมีเหตุผลที่หลากหลาย เช่น ขโมยสำเนาทรัพย์สินทางปัญญา ก่อกวนการดำเนินงานขององค์กรโดยมีวัตถุประสงค์ทางการเมืองหรือทางอุดมคติ หรือโจมตีเพื่อก่อกวนและทำลายเพื่อบรรลุวัตถุประสงค์ต่าง ๆ ทางทหารฝ่ายตรงข้ามที่มีศักยภาพได้ลงทุนลงแรงทางไซเบอร์อย่างมีนัยสำคัญเป็นขีดความสามารถที่ปฏิบัติได้จริง แต่สามารถปฏิเสธความรับผิดได้อย่างมีเหตุผลรองรับ โดยพุ่งเป้าไปยังผลประโยชน์ของสหรัฐฯ ทั้งรัสเซียและจีน ต่างก็ได้พยายามพัฒนาขีดความสามารถและยุทธศาสตร์ทางไซเบอร์ขั้นสูง แฮกเกอร์ชาวรัสเซียที่มีฝีมือทางไซเบอร์ซ่อนตัวได้เก่ง และทราบวัตถุประสงค์ของแฮกเกอร์รัสเซียได้ยาก แฮกเกอร์จีนขโมยคัดลอกทรัพย์สินทางปัญญา (Intellectual Property) จากธุรกิจทั่วโลก เพื่อประโยชน์ต่อบริษัทต่าง ๆ ของจีน และเพื่อตัดตอนไม่ให้สหรัฐฯ เข้ามาแข่งขันได้ ส่วนแฮกเกอร์อิหร่านและเกาหลีเหนือมีขีดความสามารถทางไซเบอร์ที่ด้อยกว่า แต่แฮกเกอร์กลุ่มนี้ได้แสดงความมุ่งร้ายต่อสหรัฐฯ และผลประโยชน์ของสหรัฐฯ ออกมาอย่างโจ่งแจ้งในโลกไซเบอร์ นอกเหนือจากภัยคุกคาม ที่ได้รับการสนับสนุนจากรัฐต่างชาติแล้ว แฮกเกอร์ที่ไม่ได้รับการสนับสนุนจากรัฐต่างชาติ เช่น กลุ่มรัฐอิสลามอิรักและเลแวนต์ (The Islamic State in Iraq and the Levant; ISIL) ใช้โลกไซเบอร์เพื่อหานักสู้เข้ากลุ่ม และเผยแพร่แนวความคิดชวนเชื่อ และประกาศความมุ่งมั่นที่จะให้ได้มาซึ่งขีดความสามารถทางไซเบอร์ด้านการก่อกวนและทำลายล้าง แฮกเกอร์อาชญากรเหล่านี้ได้กระทำการอันเป็นภัยคุกคามที่ต้องให้ความสนใจโดยเฉพาะอย่างยิ่ง ต่อสถาบันการเงินต่าง ๆ และกลุ่มทางอุดมคติมักใช้เหล่าแฮกเกอร์เพื่อ

ขยายผลทางการเมืองของกลุ่มตน ภัยคุกคามทั้งที่ได้รับการสนับสนุนจากรัฐต่างชาติหรือไม่ได้รับการสนับสนุน มักจะผสานตัวอยู่ด้วยกัน กลุ่มที่รักชาติมักจะโจมตีทางไซเบอร์แทนรัฐของตน และกลุ่มแฮกเกอร์ที่ไม่ได้รับการสนับสนุนจากรัฐ ก็อาจปกปิดการกระทำให้กับแฮกเกอร์ที่ได้รับการสนับสนุนจากรัฐ พฤติกรรมเหล่านี้ทำให้เกิดโอกาสที่จะคาดการณ์ได้อย่างยากลำบากยิ่งขึ้น หรือทำให้คาดการณ์ผิดได้

๑.๒ การแพร่หลายของมัลแวร์

รหัสชั่วร้ายที่แพร่หลายไปทั่วโลก หรือที่เรียกซอฟต์แวร์ประสงค์ร้ายเหล่านี้ว่ามัลแวร์ ได้เพิ่มความเสี่ยงต่อเครือข่ายและข้อมูลต่าง ๆ ของสหรัฐฯ การกระทำการขัดขวางหรือทำลายระบบทางทหารหรือระบบควบคุมทางอุตสาหกรรมนั้นต้องการความเชี่ยวชาญ แต่ฝ่ายตรงข้ามที่มีศักยภาพไม่จำเป็นต้องมีเงินเป็นพันล้านดอลลาร์เพื่อพัฒนาขีดความสามารถในการโจมตี เพราะกลุ่มรัฐชาติหรือกลุ่มใด ๆ ก็ตาม หรือแม้กระทั่งแฮกเกอร์เดี่ยว ๆ สามารถหาซื้อมัลแวร์ทำลายล้างระบบหรือขีดความสามารถอื่น ๆ ได้จากตลาดมืด และแฮกเกอร์ที่ได้รับการสนับสนุนจากรัฐต่างชาติหรือไม่ได้รับการสนับสนุน ต่างก็จ่ายเงินจ้างผู้เชี่ยวชาญให้ค้นหาจุดอ่อนและพัฒนาวิธีเจาะระบบต่าง ๆ ได้ การปฏิบัติในลักษณะนี้ได้สร้างตลาดที่อันตรายและควบคุมไม่ได้ เพื่อรับใช้แฮกเกอร์หลากหลายคน ภายใต้ระบบที่ดำเนินไปในระดับนานาชาติ แต่บ่อยครั้งที่มีวัตถุประสงค์เพื่อการแข่งขัน เนื่องจากขีดความสามารถทางไซเบอร์ที่พร้อมใช้งานมีมากขึ้น กระทรวงกลาโหมประเมินว่าแฮกเกอร์ ทั้งที่ได้รับการสนับสนุนจากรัฐต่างชาติหรือไม่ได้รับการสนับสนุน จะยังดำรงการค้นหาและมุ่งมั่นพัฒนาขีดความสามารถทางไซเบอร์ เพื่อใช้ต่อต้านผลประโยชน์ของสหรัฐฯ ต่อไป

๑.๓ ความเสี่ยงต่อเครือข่ายและโครงสร้างพื้นฐานของกลาโหม

เครือข่ายและระบบต่าง ๆ ที่กระทรวงกลาโหมเป็นเจ้าของนั้นมีจุดอ่อนต่อการบุกรุกและโจมตี นอกเหนือจากเครือข่ายของกระทรวงกลาโหมเองแล้ว การโจมตีทางไซเบอร์อาจเกิดกับโครงสร้างพื้นฐานสำคัญของชาติและทรัพยากรหลักซึ่งกระทรวงกลาโหมต้องพึ่งพาเพื่อปฏิบัติการซึ่งจะส่งผลต่อความสามารถของกองทัพที่จะปฏิบัติการอย่างต่อเนื่อง จะเป็นผลดีหากกระทรวงกลาโหมได้รับทราบว่าทรัพย์สินที่สำคัญของตนมีจุดอ่อนใดบ้าง ผ่านทางโครงการประกันภารกิจ (Mission Assurance Program) สำหรับทรัพย์สินหลักจำนวนมาก กระทรวงกลาโหมได้ทำกำหนดว่า โครงสร้างพื้นฐานของเครือข่ายทางกายภาพของรัฐที่โครงสร้างพื้นฐานหลักของกลาโหมพึ่งพาอยู่มีอะไรบ้าง แต่ก็ยังมีภารกิจอีกมากที่จะต้องกระทำเพื่อให้โครงสร้างพื้นฐานทางไซเบอร์ของกลาโหมมีความมั่นคงปลอดภัยนอกจากการโจมตีเพื่อทำลายและก่อกวนแล้ว แฮกเกอร์ยังขโมยสำเนาสารสนเทศเพื่อการปฏิบัติการ และทรัพย์สินทางปัญญา จากรัฐบาลสหรัฐฯ และกลุ่มการค้าต่าง ๆ ที่จะส่งผลต่อกระทรวงกลาโหม เป้าหมายของการขโมยยังรวมถึงผู้พัฒนาอาวุธ รวมไปถึงบริษัทการค้าที่สนับสนุนการขนส่งให้กับกองบัญชาการขนส่งของสหรัฐฯ (U.S. Transportation Command;

USTRANSCOM) สุดท้ายนี้ กระทรวงกลาโหมเผชิญกับความเสี่ยงด้านความไม่แน่นอนของความต่อเนื่องในการสนับสนุนงบประมาณจากรัฐบาลสหรัฐฯ ถึงแม้กระทรวงกลาโหมได้จัดลำดับความสำคัญของการเฉลี่ยจัดสรรทรัพยากรภายในงบประมาณที่ได้รับเพื่อพัฒนาขีดความสามารถทางไซเบอร์ ความไม่แน่นอนของงบประมาณในแต่ละปี ทำให้กระทรวงกลาโหมต้องวางแผนในการสร้างขีดความสามารถทางไซเบอร์ภายใต้งบประมาณกลาโหมโดยรวมที่ลดลงเรื่อย ๆ กระทรวงกลาโหมต้องคงไว้ซึ่งการให้ความสำคัญในการลงทุนลงแรงทางไซเบอร์ไว้ก่อน และพัฒนาขีดความสามารถที่จำเป็นเพื่อปกป้องผลประโยชน์ของสหรัฐฯ ทั้งภายในประเทศสหรัฐฯ เองและในต่างประเทศ

๑.๔ การป้องกันไม่ให้เกิดสภาพแวดล้อมที่มีความเสี่ยงในอนาคต

เมื่อต้องเผชิญกับภัยคุกคามที่ยกระดับขึ้น กระทรวงกลาโหมต้องสนับสนุนให้พัฒนาและสร้างยุทธศาสตร์การป้องปรามทางไซเบอร์ที่ครอบคลุม เพื่อยังยั้งแฮกเกอร์ตัวสำคัญ ทั้งที่ได้รับการสนับสนุนจากรัฐต่างชาติหรือไม่ได้รับการสนับสนุน เพื่อไม่ให้โจมตีทางไซเบอร์ต่อผลประโยชน์ของสหรัฐฯ เนื่องจากแฮกเกอร์ในโลกไซเบอร์ ทั้งที่ได้รับการสนับสนุนจากรัฐต่างชาติหรือไม่ได้รับการสนับสนุน นั้นหลากหลายและมีจำนวนมาก และเครื่องมือทางไซเบอร์ที่ใช้ทำลายล้างนั้น สามารถสรรหาได้ ดังนั้น ยุทธศาสตร์ในการยับยั้งที่มีประสิทธิผล ต้องการชุดนโยบายและต้องมีขีดความสามารถที่จะส่งผลต่อพฤติกรรมของแฮกเกอร์ที่ได้รับการสนับสนุนจากรัฐต่างชาติหรือไม่ได้รับการสนับสนุน

ในขณะที่กระทรวงกลาโหมสร้างกองกำลังภารกิจไซเบอร์และขีดความสามารถโดยรวม กระทรวงกลาโหมคาดการณ์ว่า การยับยั้งการโจมตีทางไซเบอร์ต่อผลประโยชน์ของสหรัฐฯ จะสำเร็จได้ ไม่ใช่แค่เชื่อมโยงนโยบายทางไซเบอร์ต่าง ๆ เข้าไว้ด้วยกันเท่านั้น แต่สหรัฐฯ ต้องปฏิบัติสิ่งต่าง ๆ ให้ครบถ้วน รวมทั้ง นโยบาย ประกาศ การตรวจจับการโจมตีอย่างเป็นรูปธรรมและขีดความสามารถ ในการเตือนภัย แนวทางการทำงานเมื่ออยู่ในสถานะป้องกันตัว กระบวนการตอบสนองต่อเหตุการณ์อย่างมีประสิทธิผล และความอ่อนตัวโดยรวมของเครือข่ายและระบบต่าง ๆ ของสหรัฐฯ ดังนั้น การหยุดยั้งกลุ่มแฮกเกอร์ในโลกไซเบอร์ ต้องได้รับความใส่ใจจากกระทรวงและหน่วยงานต่าง ๆ ของสหรัฐฯ ในส่วนของกระทรวงกลาโหมนั้น มีบทบาทจำเพาะจำนวนหนึ่งที่ต้องกระทำส่วนหนึ่งในการยังยั้งการโจมตีทางไซเบอร์นั้น ต้องทำให้ฝ่ายตรงข้ามรับรู้ หรือจูงใจให้เชื่อว่า หากฝ่ายตรงข้ามโจมตีสหรัฐฯ แล้ว จะต้องจ่ายค่าตอบแทนเป็นความทุกข์ยากที่มีราคามากจนไม่สามารถรับได้ และจะต้องลดโอกาสที่ฝ่ายตรงข้ามจะโจมตีสำเร็จ สหรัฐฯ ต้องประกาศหรือแสดงขีดความสามารถในการตอบโต้ที่มีประสิทธิผล เพื่อยับยั้งไม่ให้ฝ่ายตรงข้ามเริ่มการโจมตี พัฒนาขีดความสามารถในการป้องกันที่มีประสิทธิผล เพื่อป้องกันไม่ให้การโจมตีประสบผล และต้องเสริมความอ่อนตัวโดยรวมให้กับระบบต่าง ๆ ของสหรัฐฯ เพื่อให้ทนต่อการโจมตีในกรณีที่การโจมตีทะลวงผ่านแนวป้องกันของสหรัฐฯ เข้ามาได้ นอกจากนั้นสหรัฐฯ ต้องการการข่าวกรองที่เข้มแข็งมากขึ้น ความสามารถในการทำ

นิติวิทยาศาสตร์ทางดิจิตอลหรือการแกะรอย และขีดความสามารถในการตรวจจับและแจ้งเตือนภัยเหล่านี้ เพื่อลดจำนวนการโจมตีที่ไม่ทราบที่มาจากในโลกไซเบอร์ และเพิ่มความเชื่อมั่นว่าการโจมตีมาจากแหล่งใด

การตอบโต้: สหรัฐฯ ต้องสร้างความกระจ่างว่า จะมีการตอบโต้ต่อการโจมตีทางไซเบอร์ต่อผลประโยชน์ของสหรัฐฯ ผ่านขีดความสามารถของกลาโหม สหรัฐฯ ได้แสดงออกถึงนโยบายการประกาศนี้ไว้ในเอกสาร 2011 United States International Strategy for Cyberspace ในเอกสาร Department of Defense Cyberspace Policy Report to Congress of 2011 และผ่านการกล่าวในที่สาธารณะโดยประธานาธิบดีสหรัฐฯ และรัฐมนตรีกลาโหม สหรัฐฯ จะยังคงตอบโต้การโจมตีทางไซเบอร์ต่อผลประโยชน์ของสหรัฐฯ โดยด้านเวลา ลักษณะ และสถานที่สหรัฐฯ เป็นผู้เลือก และใช้อุปกรณ์ต่าง ๆ อย่างเหมาะสมตามอำนาจของสหรัฐฯ และสอดคล้องกับกฎหมายที่ประยุกต์ใช้ได้

การป้องกัน: ในขณะที่กระทรวงกลาโหมมีความก้าวหน้าในการสร้างกองกำลังภารกิจไซเบอร์ กระทรวงกลาโหมต้องเพิ่มขีดความสามารถในการป้องกัน เพื่อปกป้องเครือข่ายของกลาโหมเอง และปกป้องชาติจากการโจมตีทางไซเบอร์ที่สลับซับซ้อน และต้องทำงานกับกระทรวงและหน่วยงานอื่น ๆ กับแนวร่วมและพันธมิตรนานาชาติ และกับภาคเอกชนเพื่อเสริมการป้องกันผ่านความมั่นคงปลอดภัยทางไซเบอร์ที่ได้รับการปรับปรุง

ความอ่อนตัว: เนื่องจากขีดความสามารถของกระทรวงกลาโหมไม่สามารถประกันว่าจะป้องกันการโจมตีทางไซเบอร์ได้สำเร็จทุกกรณี กระทรวงกลาโหมต้องลงทุนลงแรงไปกับระบบต่าง ๆ ที่มีความอ่อนตัวและระบบสำรองพร้อมใช้ เพื่อให้คงความสามารถในการปฏิบัติการเมื่อต้องเผชิญกับการโจมตีทางไซเบอร์ในลักษณะที่ก่อกวนหรือทำลายระบบเครือข่ายของกลาโหม อย่างไรก็ตาม กระทรวงกลาโหมไม่สามารถดูแลด้านความอ่อนตัวในองค์กรนอกอำนาจความรับผิดชอบของกระทรวงกลาโหมได้ เพื่อให้ความอ่อนตัวประสบผลสำเร็จในฐานะปัจจัยในการยับยั้งอย่างมีประสิทธิผล หน่วยงานของรัฐหน่วยอื่น ๆ ต้องทำงานกับเหล่าเจ้าของและผู้ปฏิบัติงานโครงสร้างพื้นฐานที่สำคัญ และกับภาคเอกชนอย่างกว้างขวางขึ้น เพื่อพัฒนาระบบต่าง ๆ ที่มีความอ่อนตัวและระบบสำรองพร้อมใช้ ที่สามารถทนต่อการโจมตีอย่างมีศักยภาพได้ มาตรการความอ่อนตัวที่มีประสิทธิผล สามารถจูงใจฝ่ายตรงข้ามที่มีศักยภาพในการโจมตี ว่า ความคิดจะเริ่มโจมตีทางไซเบอร์ต่อเครือข่ายและระบบต่าง ๆ ของสหรัฐฯ จะไม่ทราบแหล่งที่มาของการโจมตีทางไซเบอร์ ซึ่งเป็นพื้นฐานของยุทธศาสตร์การยับยั้งทางไซเบอร์ที่มีประสิทธิผล เพราะการไม่รู้ตัวผู้โจมตีทำให้เกิดกิจกรรมการโจมตีทางไซเบอร์ที่ชั่วร้าย โดยกลุ่มที่ได้รับการสนับสนุนจากรัฐต่างชาติหรือไม่ได้รับการสนับสนุน ในเรื่องของการข่าวกรอง การรับรู้แหล่งที่มา และการแจ้งเตือน ทางกระทรวงกลาโหมและชุมชนข่าวกรองได้ลงทุนลงแรงไปอย่างสำคัญไปกับขีดความสามารถในการรวบรวมแหล่งที่มาทั้งหมด

ในการวิเคราะห์ และในการเผยแพร่ ทั้งหมดนี้เพื่อให้ทราบชัดถึงกิจกรรมในโลกไซเบอร์ของแฮกเกอร์ทั้งที่ได้รับการสนับสนุนจากรัฐต่างชาติหรือไม่ได้รับการสนับสนุน ขีดความสามารถของการข่าวกรองและการรับรู้แหล่งที่มาของการโจมตีทางไซเบอร์ ช่วยเปิดโปงตัวตนทางไซเบอร์ของแฮกเกอร์ บ่งบอกจุดเริ่มต้นของการโจมตี และช่วยพิจารณากลยุทธ์ เทคนิค และกระบวนการต่าง ๆ การรับรู้แหล่งที่มาของการโจมตีทางไซเบอร์ทำให้กระทรวงกลาโหมหรือหน่วยงานอื่น ๆ สามารถดำเนินการตอบโต้และป้องกันต่อการโจมตีทางไซเบอร์ที่เข้ามาได้การรับรู้แหล่งที่มาของการโจมตีทางไซเบอร์ ว่ามาจากภาครัฐหรือเอกชน มีบทบาทสำคัญในการยับยั้งไม่ให้แฮกเกอร์โจมตีแต่แรก กระทรวงกลาโหมจะยังคงร่วมมืออย่างใกล้ชิดกับภาคเอกชนและหน่วยงาน อื่น ๆ ของรัฐบาลสหรัฐฯ เพื่อเสริมการรับรู้แหล่งที่มาของการโจมตีทางไซเบอร์ งานนี้มีความสำคัญ โดยเฉพาะอย่างยิ่งเพื่อยับยั้ง กลุ่มเคลื่อนไหวทางการเมืองหรือกลุ่มอุดมการณ์ต่าง ๆ องค์กรอาชญากรรมต่าง ๆ และแฮกเกอร์อื่น ๆ ซึ่งได้รับขีดความสามารถทางไซเบอร์เพิ่มมากขึ้นตามกาลเวลาสุดท้าย ขีดความสามารถต่าง ๆ ทางไซเบอร์ของสหรัฐฯ จะแสดงให้แฮกเกอร์ ทั้งที่ได้รับการสนับสนุนจากรัฐต่างชาติหรือไม่ได้รับการสนับสนุน ได้เห็นว่า ไม่ว่าการโจมตีทางไซเบอร์ต่อผลประโยชน์ของสหรัฐฯ จะทำให้กองทัพสหรัฐฯ ได้รับอนุญาตให้ตอบโต้อย่างเต็มที่หรือไม่ก็ตาม แต่หากได้แสดงให้เห็นว่าการโจมตีนั้น ๆ เป็นภัยคุกคามต่อความมั่นคงปลอดภัยแห่งชาติสหรัฐฯ แล้ว ก็อาจได้รับอนุญาตให้มีการตอบโต้ในลักษณะที่ไม่ใช่ทางทหารในบางลักษณะ เพื่อตอบโต้ต่อการโจมตีและการบุกรุกในบางลักษณะ สหรัฐฯ อาจปฏิบัติการทางการทูต บังคับใช้กฎหมาย หรืออาจพิจารณากำหนดมาตรการลงโทษทางเศรษฐกิจ

ยกตัวอย่าง สหรัฐฯ ใช้ข้อมูลที่ยืนยันได้และทราบแหล่งที่มาเพื่อผูกมัดจีนเข้ากับความเสี่ยงเรื่องลอบเข้าถึงข้อมูลทางเศรษฐกิจของสหรัฐฯ การรับรู้แหล่งที่มาของข้อมูลนี้ทำให้สหรัฐฯ แสดงความห่วงใยเกี่ยวกับผลกระทบของการขโมยสำเนาทรัพย์สินทางปัญญาอันเกี่ยวข้องกับจีนต่อความสามารถในการแข่งขันทางเศรษฐกิจของสหรัฐฯ และความเสี่ยงที่มีศักยภาพส่งผลต่อความมีเสถียรภาพทางยุทธศาสตร์โดยกิจกรรมที่เกี่ยวข้องกับจีน เนื่องจากสิ่งเหล่านี้ฝ่าฝืนกฎหมายและเพื่อยับยั้งจีนจากการลอบเข้าถึงข้อมูลไซเบอร์ในอนาคต กระทรวงยุติธรรมสหรัฐฯ ได้ตั้งข้อกล่าวหาสมาชิกกองทัพปลดปล่อยประชาชนจีนจำนวน ๕ คน ว่าขโมยสำเนาทรัพย์สินทางปัญญาของสหรัฐฯ ไปเพื่อประโยชน์โดยตรงต่อบริษัทหลายแห่งของจีน กระทรวงกลาโหมจะสนับสนุนกระทรวงยุติธรรมและหน่วยงานอื่น ๆ ในการสำรวจเครื่องมือและขีดความสามารถใหม่ ๆ เพื่อช่วยยับยั้งกิจกรรมในโลกไซเบอร์ในลักษณะนั้น

๑.๕ เป้าหมายทางยุทธศาสตร์

เพื่อลดความเสี่ยงและปกป้องผลประโยชน์ของสหรัฐฯ ในสภาพแวดล้อมที่ต้องคำนึงถึงความมั่นคงปลอดภัยทั้งในปัจจุบันและในอนาคต กระทรวงกลาโหมได้วางเป้าหมายทาง

ยุทธศาสตร์จำนวน ๕ ประการ รวมถึงวัตถุประสงค์จำเพาะ เพื่อใช้ในการปฏิบัติและภารกิจต่าง ๆ ให้บรรลุเป้าหมายดังกล่าว

๑.๕.๑ สร้างและคงความพร้อมด้านกองกำลังและขีดความสามารถในการปฏิบัติการทางไซเบอร์เพื่อการปฏิบัติการอย่างมีประสิทธิผลในโลกไซเบอร์ กระทรวงกลาโหมมุ่งหวังให้กองกำลังและบุคลากรได้รับการฝึกฝนให้มีมาตรฐานสูงที่สุด เตรียมพร้อมและพรั่งพร้อมไปด้วยความสามารถทางเทคนิคอย่างดีที่สุดเมื่อเทียบกับชาติอื่น ๆ ในปี ค.ศ.๒๐๑๓ กระทรวงกลาโหมได้ริเริ่มลงทุนลงแรงอย่างมากไปกับบุคลากรและเทคโนโลยีทางไซเบอร์ โดยเริ่มกับกองกำลังภารกิจ ไซเบอร์ (Cyber Mission Force; CMF) ปัจจุบันกระทรวงกลาโหมต้องคงไว้ซึ่งการลงทุนลงแรงอย่างดี โดยฝึกฝนคนสร้างองค์กรและระบบควบคุมสั่งการที่มีประสิทธิผล และพัฒนาขีดความสามารถตามที่กระทรวงกลาโหมต้องการเพื่อปฏิบัติการในโลกไซเบอร์ โดยพัฒนาอย่างเต็มที่ ยุทธศาสตร์นี้ ได้กำหนดวัตถุประสงค์จำเพาะเพื่อให้บรรลุ ในการจัดวางกำลังคน ฝึกฝน และติดอาวุธให้กับกองกำลังและบุคลากรจากปัจจุบันไปจนถึงอีกห้าปีข้างหน้า และต่อไปอีก

๑.๕.๒ ปกป้องเครือข่ายสารสนเทศกลาโหม ประกันความปลอดภัยของข้อมูลกลาโหมและลดความเสี่ยงภารกิจกลาโหม ในขณะที่กระทรวงกลาโหมไม่สามารถปกป้องเครือข่ายและระบบต่าง ๆ ทุกแห่ง จากการบุกรุกทุก ๆ ชนิดได้ อันเนื่องมาจาก พื้นที่ที่จะถูกโจมตีทางเครือข่ายทั้งหมดของกระทรวงกลาโหมนั้นใหญ่เกินกว่าจะป้องกันภัยคุกคามได้ทั้งหมด และกว้างเกินกว่าจะอุดช่องว่างจุดอ่อนได้หมด ดังนั้น กระทรวงกลาโหมต้องกระทำตามขั้นตอน โดยบ่งชี้ทรัพยากรที่ต้องการปกป้องและจุดอ่อนต่าง ๆ จัดลำดับความสำคัญ และปกป้องเครือข่ายและข้อมูลที่มีความสำคัญที่สุดก่อน เพื่อให้สามารถปฏิบัติภารกิจได้อย่างมีประสิทธิผล กระทรวงกลาโหมต้องวางแผนและฝึกฝน เพื่อให้สามารถปฏิบัติงานได้ในสภาพแวดล้อมทางไซเบอร์ที่ประสิทธิภาพลดลงหรือถูกก่อกวน ซึ่งเกิดขึ้นได้หากกระทรวงกลาโหมถูกโจมตีเครือข่ายและข้อมูลสำเร็จ หรือเกิดในกรณีที่โครงสร้างพื้นฐานที่สำคัญซึ่งกระทรวงกลาโหมต้องพึ่งพิง ซึ่งก็มีแผนดำเนินการและแผนปฏิบัติการต่อเนื่อง แต่ก็ถูกรบกวนจนใช้การไม่ได้ สุดท้ายกระทรวงกลาโหมต้องยกระดับเทคโนโลยีและนวัตกรรมให้ล้ำหน้าภัยคุกคาม โดยขยายขีดความสามารถด้านการป้องกันภัยทางไซเบอร์ รวมถึงการสร้างและใช้งานสถาปัตยกรรมทางเครือข่ายที่ป้องกันตัวเองได้ดีขึ้น ในสภาพแวดล้อมที่ใช้งานสารสนเทศร่วมกัน (Joint Information Environment; JIE) นอกเครือข่ายของกระทรวงกลาโหม กระทรวงกลาโหมต้องทำงานกับภาคเอกชนเพื่อช่วยปกป้องข้อมูลการค้าที่เกี่ยวข้องกับอุตสาหกรรมทางทหาร และเตรียมตัวช่วยหน่วยงานอื่น ๆ เสริมความปลอดภัยระบบเครือข่ายและข้อมูลของสหรัฐฯ ต่อต้านการโจมตีทางไซเบอร์และการลอบเข้าจารกรรมข้อมูลทางไซเบอร์

๑.๕.๓ เตรียมพร้อมปกป้องมาตุภูมิสหรัฐฯ และผลประโยชน์สำคัญของสหรัฐฯ ไม่ให้ชะงักหรือเสียหายจากการโจมตีทางไซเบอร์ที่จะก่อให้เกิดผลเสียหายอย่างสำคัญ กระทรวงกลาโหมต้องทำงานกับพันธมิตรระหว่างหน่วยงาน ภาคเอกชน และต่างชาติที่ถือเป็นแนวร่วมและพันธมิตร เพื่อหยุดยั้ง หรือถ้าจำเป็นก็ต้องเอาชนะ การโจมตีทางไซเบอร์ที่จะทำให้เกิดผลเสียหายอย่างสำคัญ ต่อมาตุภูมิและผลประโยชน์ของสหรัฐฯ กระทรวงกลาโหมต้องพัฒนาการข่าวกรอง การแจ้งเตือน และขีดความสามารถทางการปฏิบัติการของตน ให้สามารถลดผลกระทบจากการโจมตีทางไซเบอร์ที่ซับซ้อนชั่วร้าย ก่อนที่การโจมตีนั้น ๆ จะส่งผลกระทบต่อผลประโยชน์ของสหรัฐฯ จะต้องคงเส้นคงวาต่อการบังคับใช้กฎหมายและนโยบาย กระทรวงกลาโหมต้องมีการข่าวกรองที่ละเอียด เป็นขั้นตอน คาดการณ์ได้ และปฏิบัติได้ โดยใช้การข่าวกรองกับเครือข่ายและระบบต่าง ๆ ในระดับโลก เพื่อทราบขีดความสามารถของฝ่ายตรงข้าม และรู้ถึงตัวแทนจำหน่ายและตลาดมัลแวร์ เพื่อปกป้องชาติ กระทรวงกลาโหมต้องสร้างความร่วมมือกับหน่วยงานอื่น ๆ ของรัฐ เพื่อเตรียมปฏิบัติการทางไซเบอร์ร่วมกัน เพื่อที่จะหยุดยั้ง หรือถ้าจำเป็นก็ต้องเอาชนะความก้าวร้าวในโลก ไซเบอร์ กระทรวงกลาโหมเน้นไปที่การสร้างขีดความสามารถ กระบวนการ และแผนที่จำเป็นเพื่อให้ภารกิจนี้ประสบผลสำเร็จ

๑.๕.๔ สร้างและคงไว้ซึ่งทางเลือกหรือแผนทางไซเบอร์ซึ่งปฏิบัติได้จริง เพื่อใช้ทางเลือกดังกล่าวควบคุมไม่ให้ความขัดแย้งยกระดับขึ้น และเพื่อจัดแต่งสภาพแวดล้อมแห่งความขัดแย้งในทุกขั้นตอน ระหว่างช่วงเวลาแห่งความตึงเครียดที่เพิ่มสูงขึ้น หรือความเป็นปรปักษ์อย่างเฉียบพลัน กระทรวงกลาโหมจะต้องเตรียมทางเลือกจำนวนหนึ่งให้กับประธานาธิบดี เพื่อใช้จัดการกับการยกระดับความขัดแย้ง ถ้าได้รับคำสั่ง กระทรวงกลาโหมจะต้องสามารถใช้การปฏิบัติการทาง ไซเบอร์เพื่อขัดขวางเครือข่ายการสั่งการและควบคุมของฝ่ายตรงข้าม รวมถึงหยุดการทำงานของโครงสร้างพื้นฐานที่สำคัญที่เกี่ยวกับทางทหาร และขีดความสามารถทางด้านอาวุธด้วย ในฐานะเป็นส่วนหนึ่ง ของชุดเครื่องมือที่มีให้สหรัฐฯ ใช้งาน กระทรวงกลาโหมต้องพัฒนา ทางเลือกทางด้าน ไซเบอร์ที่ใช้งานได้จริง และรวมทางเลือกทางไซเบอร์เหล่านี้เข้ากับแผนการต่าง ๆ ของกระทรวงกลาโหม กระทรวงกลาโหมจะพัฒนาขีดความสามารถทางไซเบอร์เพื่อให้สำเร็จวัตถุประสงค์ทางด้านความมั่นคงปลอดภัยหลัก ๆ ด้วยความแม่นยำ เพื่อลดการสูญเสียชีวิตและความเสียหายต่อทรัพย์สิน เพื่อให้มั่นใจว่าความพยายามทั้งหมดเป็นหนึ่งเดียวกัน กระทรวงกลาโหมจะทำใช้หน่วยบัญชาการต่อสู้ (Combatant Commands) เพื่อวางแผนและประสานการปฏิบัติการทางไซเบอร์ให้สอดคล้องกัน เป็นการปฏิบัติการเคลื่อนไหวทั่วทุกพื้นที่การรบทางทหาร

๑.๕.๕ สร้างและคงไว้ซึ่งพันธมิตรและหุ้นส่วนระหว่างชาติที่เข้มแข็ง เพื่อยับยั้งภัยคุกคามร่วม และเพิ่มความมั่นคงปลอดภัยและเสถียรภาพระหว่างชาติ ภารกิจทางไซเบอร์ของกระทรวงกลาโหมทั้งสามประการต้องการความร่วมมืออย่างใกล้ชิดกับแนวร่วมและพันธมิตรต่างชาติทั้งหลาย ในความผูกพันทางไซเบอร์กับนานาชาติ กระทรวงกลาโหมมุ่งสร้างความสามารถทางด้านความมั่นคงปลอดภัยทางไซเบอร์และการป้องกันภัยทางไซเบอร์ให้กับชาติพันธมิตร และสร้างสัมพันธภาพในการปฏิบัติการให้มีความลึกซึ้งเมื่อกาลและสภาพมีความเหมาะสม

ทรัพยากรทางไซเบอร์เป็นที่ต้องการอย่างสูง แต่เมื่อเทียบกันแล้วเป็นสิ่งที่ขาดแคลน กระทรวงกลาโหมต้องตัดสินใจอย่างยากลำบาก และมุ่งเริ่มต้นสร้างความสามารถกับชาติพันธมิตรในพื้นที่ผลประโยชน์ที่สำคัญของสหรัฐฯ กำลังตกอยู่ในความเสี่ยง จากบัดนี้ไปอีกห้าปีข้างหน้า นอกจากความพยายามสร้างความสามารถทางไซเบอร์ให้กับชาติพันธมิตรตามที่ต่าง ๆ ซึ่งกำลังดำเนินอยู่ในปัจจุบันแล้ว กระทรวงกลาโหมจะมุ่งเน้นสานความสัมพันธ์กับนานาชาติในบริเวณต่าง ๆ ดังนี้ ตะวันออกกลาง เอเชียแปซิฟิก และชาติพันธมิตรหลักของนาโต ตลอดยุทธศาสตร์นี้กระทรวงกลาโหมจะประเมินสภาพแวดล้อมระหว่างชาติอย่างต่อเนื่อง และพัฒนาความเป็นพันธมิตรใหม่ ๆ ขึ้น เพื่อตอบสนองต่อความท้าทายและโอกาสใหม่ ๆ ที่เกิดขึ้น

๒ เอกสาร Australian Government Defence White Paper 2013

๒.๑ ร่วมมือกับสหรัฐ อังกฤษ เพื่อขยายขีดความสามารถในการรับมือ และลงทุนในเทคโนโลยี เพิ่มพูนขีดความสามารถในการวิเคราะห์สถานการณ์เพื่อการตอบสนองที่ทันท่วงที และอยู่ล้ำหน้าภัยคุกคาม

๒.๒ ตั้งศูนย์รักษาความปลอดภัยไซเบอร์ เพื่อยกระดับขีดความสามารถในการปกป้องระบบเครือข่ายจากการโจมตีทางไซเบอร์ โดยควบคุมและใช้ประโยชน์จากขีดความสามารถของผู้เชี่ยวชาญในประเทศ ผสานเข้ากับขีดความสามารถที่มีอยู่เดิมของหน่วยงานด้านความมั่นคง เช่น กรมสื่อสารของทหาร (ซึ่งจะยกระดับเป็นกรมสื่อสารแห่งชาติ) หน่วยข่าวกรองทหาร หน่วยการภาพและภูมิสารสนเทศ (ซึ่งจะเปลี่ยนชื่อเป็นหน่วยข่าวกรองการภาพ (GeoInt) แห่งชาติ) ตำรวจแห่งชาติ โดยให้กลาโหมเป็นผู้ปฏิบัติงานหลักในศูนย์นี้ มีบอร์ดบริหารและมีเลขาธิการ Attorney-General Department เป็นผู้บังคับบัญชา (** Attorney-General Department รับผิดชอบงานสามด้าน คือ บริการงานกฎหมายแก่ประชาชน, งานด้านยุติธรรมที่เกี่ยวกับความมั่นคงของชาติและอาชญากรรม, งานประสานงานด้านนโยบายและยุทธศาสตร์)

๒.๓ สิ่งนี้จะทำหน้าที่ให้หน่วยเกี่ยวข้องเกิดความเข้าใจในภัยคุกคามไซเบอร์ มีการตอบสนอบต่อภัยได้อย่างสะดวกรวดเร็วและมีประสิทธิภาพ เป็นศูนย์รวมของความร่วมมือกับพันธมิตรทุกภาคส่วน

๒.๔ กลาโหมยังคงเดินหน้าผสานเรื่องไซเบอร์เข้าในแผนปฏิบัติงานประจำ กระบวนการควบคุมบังคับบัญชา เพื่อให้ระบบสารสนเทศและการสื่อสาร ให้เป็นไปอย่างทั่วถึงในกระทรวงกลาโหม

๓ เอกสาร Defense of Japan 2013

๓.๑ ขยายขีดความสามารถด้านไซเบอร์ของกระทรวงกลาโหมและกองกำลังป้องกันตนเอง

๓.๒ ขยายขีดความสามารถด้านไซเบอร์ให้ครอบคลุมทั่วประเทศโดยเฉพาะภาคเอกชน

๓.๓ ริเริ่มความร่วมมือกับกลุ่มที่มีศักยภาพด้านไซเบอร์ในประเทศ รวมไปถึงชาติพันธมิตร

๓.๔ ส่งเสริมการวิจัยและพัฒนา มีสถาบันวิจัยและพัฒนาทำหน้าที่พัฒนาองค์ประกอบสำหรับการฝึกทางไซเบอร์

๓.๕ จัดลำดับความเร่งด่วนของการพัฒนาขีดความสามารถ มีการร่วมลงทุนกับภาคส่วนต่างๆ ในประเทศเพื่อพัฒนาขีดความสามารถให้ก้าวล้ำในด้านการปกป้องระบบเครือข่าย การปฏิบัติการไซเบอร์ และการกลับคืนสภาพปกติได้อย่างรวดเร็วเมื่อถูกโจมตี

๓.๖ ปรับปรุงขีดความสามารถในการตอบสนองการโจมตี เริ่มตั้งแต่ระดับนโยบายของรัฐบาล ที่ให้มีการเสริมสร้างระบบป้องกันการโจมตี เสริมสร้างความร่วมมือกันภายในประเทศในทุกภาคส่วน ได้แก่ ตำรวจ มหาดไทย ICT พาณิชย์ โดยมีกระทรวงกลาโหม เป็นผู้ประสานงานหลัก มีการจัดตั้งหน่วยเคลื่อนที่เร็วเข้าช่วยแก้ปัญหาการโจมตีไซเบอร์ที่เกิดขึ้น ณ องค์กรต่างๆ มีการฝึกอบรมแลกเปลี่ยนความรู้ข่าวสารการโจมตี

๓.๗ แนวทางการรับมือการโจมตีทางไซเบอร์

๓.๗.๑ ยกระดับความปลอดภัยระบบสารสนเทศและระบบสื่อสาร (ใช้ไฟร์วอลและซอฟต์แวร์ตรวจจับไวรัส)

๓.๗.๒ ปรับปรุงระบบป้องกันไซเบอร์ (ปรับปรุงระบบตรวจสอบเครือข่ายและอุปกรณ์วิเคราะห์ทางไซเบอร์)

๓.๗.๓ พัฒนากฎระเบียบ (ออกคำสั่ง กระทรวงกลาโหมเกี่ยวกับ IA และเพิ่มความแข็งแกร่งให้กับระบบ)

๓.๗.๔ พัฒนาทรัพยากรมนุษย์ (ส่งคนไปเรียนกับ Carnegie Mellon และโรงเรียนชั้นนำในสหรัฐ โรงเรียนเหล่า)

๓.๗.๕ ขยายการแชร์ข้อมูลข่าวสารระหว่างกัน (ระหว่างกระทรวงและหน่วยงานของรัฐกับสหรัฐ)

๓.๗.๖ วิจัยด้านเทคโนโลยีขั้นสูง (วิจัยด้านเทคโนโลยีและองค์ประกอบแวดล้อมการฝึกไซเบอร์)

๓.๘ ขีดความสามารถการป้องกันการโจมตีไซเบอร์ เมื่อ ก.ย.๒๐๑๒ ได้ผลิตเอกสารชื่อ Towards Stable and Effective Use of Cyberspace by MOD and SDF เพื่อเป็นแนวทางในการจัดทำระบบป้องกันที่มีลักษณะ “ผสมผสานและคงทน” ซึ่งปัจจุบันได้มีการดำเนินตามสิ่งที่ริเริ่มจากโครงการนั้นแล้วหลักการพื้นฐาน เพื่อให้ภารกิจของกระทรวงกลาโหมและกองกำลังป้องกันตนเอง บรรลุวัตถุประสงค์ จึงมีความจำเป็นที่ต้องแสวงโอกาสจากการใช้งาน cyberspace ควบคู่ไปกับการจำกัดทุกๆ ความเสี่ยงที่อาจเป็นปัญหา เช่น ปกป้องรักษาระบบสิ่งสาธารณูปโภคพื้นฐาน พัฒนาขีดความสามารถการปฏิบัติการในไซเบอร์ ซึ่งถือว่าเป็นมิติของการรบใหม่เช่นเดียวกับ บก ทะเล อากาศ และอวกาศ เพื่อให้บรรลุวัตถุประสงค์เหล่านั้น จึงจะต้องดำเนินการตามแนวนโยบาย ดังนี้

๓.๘.๑ ขยายขีดความสามารถและระบบของกระทรวงกลาโหมและกองกำลังป้องกันตนเอง

๓.๘.๒ ความร่วมมือกันจากทุกภาคส่วนทั่วทั้งประเทศ โดยเฉพาะภาคเอกชน

๓.๘.๓ ความร่วมมือกับต่างประเทศ โดยเฉพาะชาติพันธมิตร

๓.๙ กระทรวงกลาโหม และกองกำลังป้องกันตนเอง ได้ริเริ่ม

๓.๙.๑ จัดตั้ง “กลุ่มป้องกันไซเบอร์” เพื่อเป็นเครื่องมือของกระทรวง กลาโหมและกองกำลังป้องกันตนเอง ในการปรับปรุงระบบสำหรับการปฏิบัติงาน เช่น ขยายขีดความสามารถการเฝ้าตรวจระบบเครือข่าย การวิจัยด้านเทคโนโลยีการฝึกทางไซเบอร์ การผลิตบุคลากรที่มีขีดความสามารถสูงด้านไซเบอร์ โดยจัดให้มีหลักสูตรด้านรักษาความปลอดภัยระบบเครือข่ายตั้งแต่ระดับโรงเรียนนายร้อย สถาบันศึกษาภายในประเทศ และส่งไปศึกษายังต่างประเทศ

๓.๙.๒. รวมเรื่องการป้องกันการโจมตีจากไซเบอร์เข้าไปในทุกฟังก์ชันงานของการป้องกันระบบสารสนเทศ ปกป้องระบบโครงสร้างพื้นฐานด้านสารสนเทศของทหารและระบบควบคุมบังคับบัญชา

๓.๙.๓. ใช้ประโยชน์จากการดำเนินการในระดับรัฐบาลที่รับผิดชอบการป้องกันการโจมตีและเป็นแหล่งรวมของผู้เชี่ยวชาญและทักษะที่จำเป็นทั่วทั้งประเทศ

๓.๙.๔. กำหนดประกาศใช้กฎระเบียบและกระบวนการตอบสนองต่อการโจมตีทางไซเบอร์

๓.๙.๕. ดำเนินโครงการวิจัยเทคโนโลยีขั้นสูงด้านไซเบอร์

๓.๑๐ ความร่วมมือระหว่างกระทรวงกลาโหมและกองกำลังป้องกันตนเองกับหน่วยงานอื่นๆ มีความร่วมมือกับหน่วยงานภาครัฐ ได้แก่ National Information Security Center (NISC) ซึ่งเป็นหน่วยงานที่เกิดจากความร่วมมือกับสหรัฐ ซึ่งได้มีข้อตกลงร่วมกันในการร่วมมือด้านการป้องกันไซเบอร์ ตัวอย่างเช่น การฝึกการตอบสนองเมื่อมีเหตุการณ์โจมตีทางไซเบอร์ เป็นต้น นโยบายที่เกี่ยวข้องกับไซเบอร์ มีคณะกรรมการนโยบายไซเบอร์ ซึ่งมี รองรัฐมนตรีว่าการกระทรวงกลาโหมเป็นประธาน ทำหน้าที่ด้านนโยบาย ได้แก่ การร่วมมือกับต่างประเทศและองค์กรที่เกี่ยวข้อง การจัดโปรแกรมการฝึกบุคลากรด้านไซเบอร์ การผสานความร่วมมือไปยังภาคอุตสาหกรรมป้องกันประเทศ และดูแลไปถึงความเสี่ยงที่อาจเกิดขึ้นกับระบบ Supply Chain

๔. เอกสาร Chinese Military Modernization and Force Development A Western Perspective

๔.๑ จีนมีหลักนิยม Integrated Network Electronic Warfare เป็นเอกสารที่รวมเรื่อง Cyber warfare และ EW ในพื้นที่การรบ ซึ่งเป็นการใช้ขีดความสามารถทั้งสองเรื่องในการลดขีดความสามารถของระบบ C4ISR ของฝ่ายตรงข้าม ด้วยการปฏิบัติการสงครามเครือข่ายและเครื่องมือทางสงครามอิเล็กทรอนิกส์

๔.๒ จีนมีหลักการ เรื่อง information confrontation ซึ่งได้มีการผนวกรวมขีดความสามารถการทำสงครามข้อมูลข่าวสาร ทั้งที่เป็นอิเล็กทรอนิกส์และไม่เป็นอิเล็กทรอนิกส์ ให้รวมอยู่ในศูนย์บัญชาการเดียวกัน โดยทำงานทั้งยามสงบและยามสงคราม เพื่อให้ได้มาซึ่งความเหนือกว่าทางข้อมูลข่าวสาร

๔.๓ หน่วยงาน ๓ ประเภท ได้แก่ Informatisation, Strategic Planning and Training ได้รับการปรับปรุงให้รองรับการพัฒนาและใช้ขีดความสามารถด้านไซเบอร์ ซึ่งหน่วยงานที่รับผิดชอบได้แก่ กรมที่ ๓ Signals Intelligence มีหน้าที่ปกป้องระบบเครือข่ายและรวบรวมข้อมูลข่าวสาร มีเจ้าหน้าที่ประกอบด้วยทหารและพลเรือน และอีกหน่วยคือ กรมที่ ๔ Electronic Countermeasures มีหน้าที่ โจมตีระบบเครือข่ายและปฏิบัติการสงครามอิเล็กทรอนิกส์ ซึ่งทั้งสองกรมนี้เป็นหน่วยขึ้นตรงต่อ General Staff Department

๔.๔ จีนใช้ความสามารถ computer network exploitation (CNE) ในการรวมรวมข้อมูลข่าวสารในเรื่อง การเมือง เศรษฐกิจ อุตสาหกรรมป้องกันประเทศ ของประเทศเป้าหมาย รวมทั้งมุมมองที่ประเทศนั้นๆ มีต่อจีน จีนรวบรวมข้อมูลไปทำเป็นเป้าหมายการโจมตี เช่น ระบบรักษาความปลอดภัยเครือข่าย ระบบการขนส่ง ระบบอื่นๆ ที่สนับสนุนการรบ

๔.๕ จีนใช้ขีดความสามารถการทำสงครามไซเบอร์ใน ๓ ลักษณะ ได้แก่ รวมรวมข้อมูลข่าวสารและใช้ในการโจมตีระบบเครือข่าย จำกัดหรือชะลอการตอบโต้ของฝ่ายตรงข้ามด้วยการโจมตีระบบเครือข่ายด้านการขนส่ง สื่อสาร การค้า และใช้เสริมขีดความสามารถการโจมตีทางกายภาพ

๔.๖ หลักนิยม ๒ เรื่อง ที่เป็นพื้นฐานการทำสงครามไซเบอร์ ได้แก่ Science of Strategy, and Science of Campaigns ได้ให้ความสำคัญแก่การทำสงครามข้อมูลข่าวสารว่าทำให้ได้มาซึ่งความเหนือกว่าทางข้อมูลข่าวสาร และการทำสงครามเครือข่าย มีเป้าหมายกระทำต่อระบบ C2 (command and control system) และระบบคมนาคมขนส่ง โดยให้ทำตั้งแต่ในระยะแรกเริ่มของความขัดแย้ง โดยเฉพาะในเอกสาร Science of Strategy ได้ระบุว่าระบบควบคุมบังคับบัญชาเป็นหัวใจของการรวมรวบข้อมูลข่าวสาร และการควบคุมการยุทธ ดังนั้นจึงต้องจัดการที่ระบบนี้ก่อน

๔.๗ ในขณะเดียวกัน จีนยังเสริมสร้างความสัมพันธ์ด้านการทูต การแสดงบทบาทในเวทีระดับนานาประเทศ ที่มีการถกแถลงในเรื่องไซเบอร์ เช่น ความร่วมมือระหว่างจีนกับรัสเซียในการกำหนดกฎบัตรด้านความปลอดภัยข้อมูลข่าวสาร ซึ่งเป็นระบุให้รัฐมีอำนาจในการควบคุมข้อมูลข่าวสาร ทั้งการไหลของข้อมูลข่าวสารและเนื้อหาได้

๕. เอกสาร Republic of Korea 2010 Defense White Paper

๕.๑ การเพิ่มขีดความสามารถการตอบโต้ภัยคุกคามไซเบอร์ พัฒนาขีดความสามารถของระบบรักษาความปลอดภัยข้อมูล และเทคโนโลยีรักษาความปลอดภัยไซเบอร์ เพื่อให้การปฏิบัติการทางทหารสามารถดำเนินไปได้โดยเรียบร้อยจากภัยคุกคามไซเบอร์ทั้งยามสงบและยามสงคราม เมื่อปี 2009 รัฐบาลได้ประกาศให้ดำเนินการจัดทำระบบรักษาความปลอดภัยข้อมูลข่าวสารและการเตรียมการรับมือภัยคุกคามไซเบอร์อย่างเป็นระบบ มีการตั้ง CERT เพื่อดูแลระบบข้อมูลข่าวสารด้านความมั่นคงตลอด ๒๔ ชั่วโมง และการทบทวนภารกิจของหน่วยงานภาครัฐใหม่เพื่อให้รองรับการรักษาความปลอดภัยข้อมูลข่าวสาร มีการจัดตั้งหน่วยงาน Cyber Warfare Response Center และ Cyber Command มีการใช้ระบบป้องกันไวรัสคอมพิวเตอร์ การป้องกันระบบเมล์ ได้มีการแยกระบบเครือข่ายสำหรับการรบออกจากระบบเครือข่ายที่ใช้งานปกติและใช้การเข้ารหัส มีการกำหนดสิทธิการเข้าถึงข้อมูลเพื่อให้ระบบการแบ่งปันข้อมูลข่าวสาร

๕.๒ มีความปลอดภัยและใช้งานได้โดยเรียกว่า Classified Data Management System และยังมีการจัดการเพื่อป้องกันการรั่วไหลของข้อมูลส่วนบุคคล

๕.๓ มีความร่วมมือที่แน่นแฟ้นเพื่อตอบโต้ต่อภัยคุกคามไซเบอร์ มีความร่วมมือระดับนานาชาติ และการแลกเปลี่ยนข้อมูลภัยคุกคาม เป็นสิ่งสำคัญสำหรับการรับมือ เกาหลีใต้และสหรัฐฯ ได้มีความร่วมมือกันโดยในปี 2009 ทั้งสองประเทศได้ทำ MOU ด้าน Information Assurance and Cooperation on Computer Network Defense และ ROK ได้ส่งทีมเข้าร่วม

ICDW นอกจากนี้ ในปี 2010 ได้มีการจัดประชุม ROK-US Information Assurance Working Group Meeting เพื่อมีการทำข้อตกลงในกิจกรรมความร่วมมือระหว่างกัน ROK ยังได้มีกิจกรรมส่งเสริมความร่วมมือระดับรัฐบาลชาติพันธมิตรในการแบ่งปันข้อมูลข่าวสารที่เป็นประโยชน์ในการตอบโต้ภัยคุกคาม โดยการรับเป็นเจ้าภาพการสัมมนาด้าน Defense Information Assurance ทุกปี

๖. เอกสาร Norwegian Defence 2013 FACTS and FIGURES

กองกำลังป้องกันไซเบอร์ได้สถาปนาขึ้นเมื่อ ก.ย.2012 มีบทบาทหน้าที่สำคัญในการปกป้องขีดความสามารถการติดต่อสื่อสารและข้อมูลข่าวสารของกองทัพ หน้าที่หลักคือปกป้องระบบเครือข่าย หน่วยงานที่อยู่ภายใต้การควบคุม ได้แก่ ศูนย์ความเป็นเลิศด้านควบคุมบังคับบัญชาและข้อมูลข่าวสาร ห้องทดลองการรบ และหน่วยดำเนินงานด้านสนับสนุน

๗. เอกสาร French White Paper Defense and National Security 2013

๗.๑ ฝรั่งเศสเห็นความสำคัญของการมีความพร้อมรับมือภัยคุกคามไซเบอร์ตั้งแต่ปี 2008 โดยอย่างน้อยต้องดำเนินการให้เทียบเท่ากับอังกฤษและเยอรมัน

๗.๒ เห็นความสำคัญของการต้องมีการสนับสนุนด้วยวิทยาศาสตร์ขั้นสูง และผู้เชี่ยวชาญทางเทคโนโลยี

๗.๓ มีการลงทุนงบประมาณจำนวนมากในการออกแบบและพัฒนาระบบรักษาความปลอดภัยขั้นสูง มีการเฝ้าระวังและตรวจสอบอย่างถี่ถ้วนในระบบเครือข่ายการสื่อสาร

๗.๔ มีการเสริมความปลอดภัยให้กับระบบข้อมูลข่าวสารที่สำคัญ มีนโยบายรักษาความปลอดภัย มีการบริการจัดการอุปกรณ์สื่อสารตั้งแต่การจัดหา เพื่อให้เกิดความปลอดภัย มีการกระจายนโยบายจากส่วนกลางให้ฝ่ายปกครองท้องถิ่นได้จัดทำระเบียบ ข้อกำหนดการใช้งานไซเบอร์สเปซ รัฐบาลกลางกำหนดให้ผู้ผลิตว่า/บริษัทคู่สัญญา ว่าจะต้องดำเนินการให้อุปกรณ์ที่จัดหานั้นเป็นไปตามระดับการรักษาความปลอดภัย

๗.๕ รัฐบาลกำหนดมาตรฐานความปลอดภัยว่าต้องปฏิบัติตามเพื่อให้ภาครัฐมีความปลอดภัย ทั้งปรับปรุงกฎระเบียบกระบวนการที่เกี่ยวข้อง

๗.๖ รัฐบาลตรวจผู้ประกอบการที่เกี่ยวข้องว่าได้ทำตามมาตรฐานที่กำหนดและดำเนินการตรวจสอบด้วยโดยเฉพาะระบบที่มีความอ่อนไหว ทั้งภาครัฐและเอกชน โดยต้องส่งแผนการดำเนินการยามมีเหตุวิกฤตและเมื่อนั้นหน่วยงานภาครัฐสามารถเข้าควบคุมการดำเนินการได้ทันที

๗.๗ นโยบายการตอบสนองต่อการโจมตีทางไซเบอร์แห่งชาติ มีที่มาจากสถานการณ์ภัยคุกคามไซเบอร์ของโลกใน ๒ ลักษณะ ได้แก่

๗.๗.๑ ติดตั้งระบบรักษาความปลอดภัยข้อมูลข่าวสารของรัฐ ให้มีความมั่นคงแข็งแรง ทนทาน หน่วยด้านโครงสร้างพื้นฐานแห่งรัฐและอุตสาหกรรมที่สำคัญได้รับการปกป้อง ซึ่ง

ทั้งหมดอยู่ในการดูแลของสำนักนายกรัฐมนตรี และได้รับการสนับสนุนโดยใกล้ชิดจากหน่วยงานภาครัฐต่างๆ เพื่อตรวจจับและประเมินภัยคุกคามไซเบอร์ที่มีต่อประเทศให้ได้โดยเร็วที่สุด

๗.๗.๒ ในยามที่ผลประโยชน์แห่งรัฐถูกบุกรุก นโยบายแห่งชาติกำหนดให้ใช้ขีดความสามารถเชิงริเริ่มด้าน IT ซึ่งเกี่ยวข้องกับขีดความสามารถด้านการข่าว ทำให้ภัยคุกคามนั้นมีความกระจ่างชัดโดยให้ทราบถึงที่มาของการโจมตี ทำให้ได้รับข้อมูลที่จำเป็นต่อดำเนินการป้องกัน การใช้ความสามารถเชิงริเริ่มด้าน IT นั้นกระทำโดยสอดคล้องกับระดับของภัยคุกคามหรือความรุนแรงของการโจมตี

๗.๘ ความปลอดภัยประชาคมข้อมูลข่าวสารโดยภาพรวม มาจากความตระหนักในความเสี่ยงและภัยคุกคามในระดับบุคคล ที่จะปรับพฤติกรรมและการปฏิบัติของตนให้สอดคล้องกับแนวทางการรักษาความปลอดภัย นอกจากให้ดำเนินการเพิ่มจำนวนผู้เชี่ยวชาญ และให้ผนวกรวมการอบรมด้านรักษาความปลอดภัยสารสนเทศเข้าไปในทุกการอบรมที่เกี่ยวข้องและรวมไปถึงการศึกษาภาคปกติด้วย

๗.๙ นโยบายความมั่นคงปลอดภัยไซเบอร์ที่ดี ต้องพัฒนามาจากการมีความสัมพันธ์และความร่วมมืออันใกล้ชิดกับพันธมิตรระดับนานาชาติ ซึ่งให้ความสำคัญกับพันธมิตรใกล้ชิด คือ สหราชอาณาจักร กับเยอรมัน เป็นอันดับแรก ลำดับถัดมาได้แก่ กลุ่มประเทศยุโรป ซึ่งฝรั่งเศสเองได้สนับสนุนการกำหนดนโยบายระดับกลุ่มประเทศยุโรปซึ่งมีเป้าหมายเพิ่มความแข็งแกร่งให้กับการปกป้องระบบโครงสร้างพื้นฐานแห่งรัฐและระบบเครือข่ายการสื่อสารอิเล็กทรอนิกส์ให้รอดพ้นจากการโจมตีทางไซเบอร์

วิเคราะห์ประเด็นสำคัญจากการป้องกันไซเบอร์ของต่างประเทศ

สามารถสรุปประเด็นสำคัญในการดำเนินการป้องกันไซเบอร์ของต่างประเทศที่น่าสนใจเพื่อใช้ในการวิเคราะห์ได้จำนวน ๙ ประเด็น ดังนี้

๑. มีการจัดตั้งหน่วยรับผิดชอบด้านไซเบอร์ขึ้นมาโดยเฉพาะ ในบางประเทศได้จัดตั้งหน่วยขึ้นใหม่หรือปรับปรุงจากหน่วยที่มีอยู่เดิม

๒. พัฒนาศักยภาพการตอบสนองภัยจากไซเบอร์โดยการกำหนดนโยบายและการพัฒนาทางเทคนิค

๓. ให้มีการประสานความร่วมมือทั้งในประเทศและต่างประเทศ

๔. ให้มีการสร้างความตระหนัก โดยให้มีไซเบอร์ร่วมอยู่ในทุกกิจกรรมที่ปฏิบัติ

๕. ให้มีการวิจัยและพัฒนา เพื่อพึ่งพาตนเอง

๖. รัฐมีอำนาจตรวจสอบเนื้อหาหรือเข้าควบคุมเหตุฉุกเฉินทางไซเบอร์

๗. กำหนดกฎหมาย ระเบียบ มาตรฐานด้านไซเบอร์

๘. ปกป้องโครงสร้างพื้นฐาน โดยเฉพาะโครงสร้างพื้นฐานด้านสาธารณูปโภค

๙. มีการดำเนินการเชิงรุก

ตารางที่ ๔ - ๑ ประเด็นสำคัญการป้องกันไซเบอร์ของต่างประเทศ

การดำเนินการ	USA	Thai NCS	Australia	Japan	China	ROK	French
๑. จัดหน่วยรับผิดชอบโดยตั้งขึ้นใหม่หรือปรับปรุงจากเดิม		✓	✓	✓	✓	✓	
๒. พัฒนาศักยภาพการตอบสนองภัยจากไซเบอร์ทั้งนโยบายและเทคนิค	✓	✓	✓	✓	✓	✓	✓
๓. ให้มีการประสานความร่วมมือทั้งในและต่างประเทศ	✓	✓	✓	✓		✓	✓
๔. ให้สร้างความตระหนัก โดยให้มีไซเบอร์ร่วมอยู่ในทุกกิจกรรม	✓	✓	✓	✓			✓
๕. ให้มีการวิจัยและพัฒนา เพื่อพึ่งพาตนเอง	✓	✓		✓			✓
๖. รัฐมีอำนาจตรวจสอบเนื้อหาหรือเข้าควบคุมเหตุฉุกเฉินทางไซเบอร์	✓						✓
๗. กำหนดกฎหมาย ระเบียบมาตรฐานด้านไซเบอร์	✓	✓					✓
๘. ปกป้องสาธารณูปโภคพื้นฐาน	✓	✓		✓			✓
๙. ดำเนินการเชิงรุก	✓				✓		✓

วิเคราะห์ลักษณะภัยคุกคามจากสงครามไซเบอร์ของต่างประเทศ

สามารถวิเคราะห์และสรุปลักษณะภัยคุกคามจากสงครามไซเบอร์ที่ต่างประเทศได้รับผลกระทบ ดังนี้

๑. การโจมตีในไซเบอร์สามารถโจมตีและสร้างผลเสียหายมากกระทบในวงกว้างได้อย่างรวดเร็ว

๒. ตรวจจับได้ยาก ไม่สามารถระบุที่ตั้งและตัวตนได้โดยง่าย

๓. สามารถปฏิบัติการได้จากทั่วโลก ลมฟ้าอากาศไม่มีผลกระทบเพราะอยู่ในเครือข่าย

๔. เป้าหมายของการโจมตีมีหลากหลายและจำนวนมากขึ้นทุกขณะ

๕. จุดอ่อนของฝ่ายเรามีมากไม่สามารถป้องกันหรือปิดได้หมด จำนวนการโจมตีไม่ใช่ปัจจัยแห่งความสำเร็จเพราะหากโจมตีจุดอ่อนที่ใช่เพียงครั้งเดียวก็สามารถทำลายได้

๖. การโจมตีใช้ทรัพยากรน้อย (ลงทุนน้อย) และสามารถหาเครื่องมือได้ทั่วไปในอินเทอร์เน็ต

๗. ต้องใช้ผู้เชี่ยวชาญทั้งในการโจมตีและการป้องกัน ซึ่งหาได้ยาก

วิเคราะห์ภัยคุกคามไซเบอร์ที่มีผลกระทบต่อความมั่นคงของชาติ

ปัจจุบันภัยคุกคามด้านไซเบอร์ไม่ได้มีผลเฉพาะต่อระบบสารสนเทศที่เชื่อมโยงผ่านระบบเครือข่าย หรือออนไลน์อีกต่อไป แต่ยังส่งผลกระทบต่อระบบโครงสร้างพื้นฐานต่าง ๆ ที่สำคัญในทุกภาคส่วน รวมถึงในระดับชาติ รัฐบาล หน่วยงานราชการ ผู้ประกอบการภาครัฐ และเอกชนจึงจำเป็นต้องมีความตื่นตัว และตระหนักถึงภัยดังกล่าว แม้ระบบต่าง ๆ ที่ใช้ในการดำเนินงานจะเป็นระบบปิดหรือออฟไลน์ แต่ก็ไม่อาจสามารถไว้วางใจในเรื่องดังกล่าวได้ ดังกรณีศึกษาต่าง ๆ ที่ได้เกิดขึ้นมาเป็นระยะ อาทิ เหตุภัยคุกคามทางไซเบอร์ที่เป็นข่าวใหญ่ ดังเหตุการณ์ในปี พ.ศ. ๒๕๕๓ ได้แก่ Stuxnet ซึ่งมุ่งการโจมตีไปยังระบบคอมพิวเตอร์ที่ติดตั้งภายในโรงงานอุตสาหกรรม หรือโรงไฟฟ้า/โรงไฟฟ้านิวเคลียร์ของอิหร่าน ซึ่งเป็นส่วนหนึ่งของระบบ SCADA (Supervisory Control and Data Acquisition) อันมีหน้าที่ในการควบคุมกระบวนการต่าง ๆ ภายในโรงงานอุตสาหกรรม เหตุการณ์ Night Dragon ในปี พ.ศ. ๒๕๕๒ – ๒๕๕๔ ซึ่งเป็นการเจาะระบบและโจรกรรมข้อมูลจากบริษัทพลังงานและปิโตรเคมีของชาติตะวันตก หรือ เหตุการณ์ในปี พ.ศ. ๒๕๕๒ ซึ่งสถาบันการเงินของประเทศสาธารณรัฐเกาหลี ถูกโจมตีด้วยเทคนิค Distribute Denial of Service (DDoS) ส่งผลให้ไม่สามารถทำธุรกรรมทางการเงินได้ และ พ.ศ. ๒๕๕๖ ก็ถูกไวรัสโจมตีสถานีโทรทัศน์และธนาคารและลบข้อมูลจนเป็นเหตุให้ต้องหยุดการให้บริการ

สำหรับประเทศไทย แผนแม่บทเทคโนโลยีสารสนเทศ ฉบับที่ ๓ พ.ศ. ๒๕๕๗ – ๒๕๖๑ ของประเทศไทย ได้คำนึงถึงการพัฒนาทางเทคโนโลยีสารสนเทศมีการเปลี่ยนแปลงไปอย่างรวดเร็ว เช่น การใช้การสื่อสารความเร็วสูงด้วยเทคโนโลยีไร้สายและคลาวด์ นอกจากนี้การใช้คอมพิวเตอร์ โทรศัพท์เคลื่อนที่ อินเทอร์เน็ต ที่ใช้ในการติดต่อสื่อสารหรือการทำธุรกรรมต่างๆ ทั้งในภาครัฐและเอกชนนับวันยิ่งมีแนวโน้มเพิ่มสูงขึ้น จึงทำให้มีการกระทำความผิดที่อาศัยกลไกความก้าวหน้าทางเทคโนโลยีในการสร้างความเสียหาย ไม่ว่าจะในรูปแบบการก่อการร้ายหรือการกระทำที่มีผลกระทบต่อความมั่นคงของรัฐ การกระทำที่มีผลต่อโครงสร้างพื้นฐานของประเทศ รวมถึงการสร้างความตื่นตระหนกกับประชาชนหรือภัยคุกคามต่อสิทธิความเป็นส่วน จึงได้ให้ความสำคัญความเสี่ยงด้านไซเบอร์ที่กระทบต่อความมั่นคงของชาติ โดยให้ความสำคัญในเรื่องต่อไปนี้

๑. การพัฒนาหลักกฎหมาย มาตรฐาน ระเบียบและวิธีการด้าน เทคโนโลยีสารสนเทศ ได้แก่ การผลักดันกฎหมายที่อยู่ระหว่างการพิจารณา มาตรฐาน ระเบียบ และการบริการอิเล็กทรอนิกส์ภาครัฐ เป็นต้น เนื่องจากอาชญากรรมไซเบอร์ และการคุกคามต่อโครงสร้างพื้นฐานที่วิกฤตและทรัพยากรสำคัญ มีแนวโน้มความรุนแรงเพิ่มขึ้น การพัฒนาด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับประเทศ จึงมีความสำคัญ รวมทั้งการสร้างโลกไซเบอร์ที่ปลอดภัยต่อการใช้ งาน โดยส่งเสริมการนำมาตรฐานระดับสากลเข้ามาใช้ในหน่วยงานภาครัฐและเอกชน สร้างความตระหนักให้กับประชาชนโดยการจัดให้มีหลักสูตรมาตรฐาน ส่งเสริมการพัฒนาบุคลากรมืออาชีพด้านรักษาความปลอดภัยไซเบอร์ ความร่วมมือระหว่างภาครัฐและเอกชน ผลักดันให้มีผู้บริหารที่เกี่ยวข้องกับด้านการรักษาความปลอดภัยไซเบอร์ สนับสนุนแนวทางการให้ความเป็นส่วนตัวของประชาชนโดยให้มีดุลยภาพระหว่างความเป็นส่วนตัวและความมั่นคง

๒. การส่งเสริมให้เกิดการประสานงานกับหน่วยงานต่างประเทศ ในการเข้าถึงข้อมูลของภัยคุกคามไซเบอร์เพื่อการรับมือทันต่อสถานการณ์ สร้างกลไกให้เกิดความร่วมมือประสานงานระหว่างภาครัฐและผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider) ในการเข้าถึงข้อมูลภัยคุกคามไซเบอร์ ผลักดันให้เกิดการแก้กฎหมายเพื่อให้ได้รับความร่วมมือจากผู้ให้บริการอินเทอร์เน็ต เพื่อที่จะทำให้การรับมือภัยคุกคามที่ประสิทธิภาพยิ่งขึ้น ต้องกำหนดให้มีหน่วยงานที่มีอำนาจทางกฎหมายในการตอบสนองต่อภัยคุกคามไซเบอร์ได้อย่างมีประสิทธิภาพ ผลักดันให้หน่วยงานที่เกี่ยวข้องเกิดการวิจัยและพัฒนาเทคโนโลยีที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในการป้องกันประเทศ

๓. การสร้าง ความตระหนัก ให้กับประชาชนและเยาวชนของชาติ การจัดตั้งหน่วยงานเพื่อตอบสนองต่อภัยคุกคามไซเบอร์แบบเร่งด่วน ที่สามารถประสานงานเชื่อมโยงกับหน่วยงานที่เกี่ยวข้องได้ การสนับสนุนให้สถาบันการศึกษาจัดทำหลักสูตรด้านรักษาความปลอดภัยไซเบอร์ เป็นต้น

วิเคราะห์การป้องกันไซเบอร์ของประเทศไทย

๑. มีการจัดตั้งคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ซึ่งหน่วยที่เกี่ยวข้องจะต้องดำเนินการให้สอดคล้องและรองรับการดำเนินการด้านไซเบอร์ในระดับชาติต่อไป

๒. มีการกำหนดกรอบนโยบายความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ซึ่งจะทำให้การดำเนินการด้านไซเบอร์ของประเทศไทยมีเอกภาพและเป็นไปในทิศทางเดียวกัน

๓. มีการร่างกฎหมายที่เกี่ยวกับการจัดตั้งหน่วยงานด้านความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

๔. มีการร่างกฎหมายเกี่ยวกับการสนับสนุนเศรษฐกิจดิจิทัล และกฎหมายที่เกี่ยวข้องกับเศรษฐกิจ แต่ยังไม่มีกฎหมายไซเบอร์ด้านความมั่นคง

วิเคราะห์ปัญหาการป้องกันไซเบอร์ของกระทรวงกลาโหม

จากการศึกษาและวิเคราะห์ภารกิจการจัดหน่วยงานไซเบอร์ของประเทศไทยในปัจจุบัน ลักษณะการปฏิบัติงาน กิจกรรมที่แต่ละหน่วยปฏิบัติ การประสานงานระหว่างกระทรวงกลาโหม กับหน่วยงานไซเบอร์ในประเทศไทย สามารถสรุปปัญหาการดำเนินการด้านไซเบอร์ของกระทรวงกลาโหมได้ดังนี้

๑. กระทรวงกลาโหมยังขาดนโยบายและยุทธศาสตร์ด้านไซเบอร์ที่ชัดเจนและยังไม่ได้กำหนดหลักนิยมในการปฏิบัติเกี่ยวกับไซเบอร์

๒. ขาดการฝึกอบรมและการพัฒนาผู้นำด้านไซเบอร์ที่จะสร้างหน่วยให้มีความพร้อมรับมือกับภัยคุกคามไซเบอร์และพร้อมที่จะปฏิบัติภารกิจทางไซเบอร์

๓. หน่วยไซเบอร์ที่จัดตั้งขึ้นของแต่ละหน่วยขึ้นตรงกระทรวงกลาโหมในปัจจุบัน ต่างก็มีขีดความสามารถในการป้องกันไซเบอร์ของตนเองได้ระดับหนึ่ง แต่ยังขาดขีดความสามารถเชิงรุกและการเข้าควบคุม (Exploit) ไซเบอร์ของฝ่ายตรงข้าม

๔. หน่วยในกระทรวงกลาโหมมีการใช้ไซเบอร์เพิ่มขึ้น เช่น การดำเนินการเพื่อนำไปสู่การปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Operations) แต่การป้องกันไซเบอร์ยังไม่ดีพอที่จะรับมือกับภัยคุกคามระดับสูงมาก เช่น APT เป็นต้น

๕. ยังไม่มีการสนธิส่วนอำนวยการร่วมกัน (Integrating staff element) ในการทำงานด้าน ไซเบอร์ภายในกระทรวงกลาโหม ซึ่งยังอยู่ในลักษณะต่างคนต่างทำเพื่อปกป้องรักษาเครือข่ายของตนเอง แต่การทำงานด้านไซเบอร์นั้นต้องใช้การทำงานในลักษณะเครือข่ายทำงานร่วมกัน

๖. ขาดแคลนผู้เชียวชาญ เป็นปัญหาที่สำคัญมากเพราะผู้เชี่ยวชาญไม่สามารถจะจัดหามาได้ง่าย แต่ละคนต้องใช้เวลาสั่งสมความรู้ ประสบการณ์ และเอกชนให้ค่าตอบแทนที่มากกว่าราชการจึงมีสมองไหลบางส่วนและหาคนที่จะมาสมัครทำงานกับราชการได้ยาก

๗. ขาดกฎการใช้กำลังหรือการเข้าปฏิบัติการ (Rule of Engagement) ของทหาร และระหว่างพลเรือนกับทหาร

๘. ขาดการประสานงานความร่วมมือในทุก ๆ ด้านกับหน่วยงานภายนอกกระทรวงกลาโหม และหน่วยงานของต่าง ๆ ประเทศอย่างต่อเนื่องและสร้างสรรค์ผลผลิต

แนวทางการจัดทำยุทธศาสตร์การป้องกันไซเบอร์กระทรวงกลาโหม

กรอบแนวคิดที่ใช้เป็นแนวทางการจัดทำยุทธศาสตร์ สำหรับประเทศไทยนั้น ส่วนใหญ่จะใช้ กรอบแนวคิดที่ว่าด้วยองค์ประกอบสามด้าน คือ คน (People) กระบวนการ (Process) และ เทคโนโลยี (Technology) หรือ เครื่องมือ ทั้งหมดนี้ต้องนำมาพิจารณาอย่างผสมผสานกัน โดยมียุทธศาสตร์ (Strategy) เป็นแนวทางการขับเคลื่อนในระดับองค์กร โดยการพัฒนาจะต้องคำนึงถึงทั้งสามด้านให้มีความสมดุลกัน

แผนภาพ ๔ – ๑ องค์ประกอบสามด้านในการจัดทำยุทธศาสตร์

กระทรวงกลาโหมสหรัฐอเมริกา ได้นำกรอบแนวคิดการบริหารจัดการ ศักยภาพด้านไซเบอร์ของกองทัพมาใช้ รวมทั้งแนะนำให้ชาติพันธมิตรได้นำไปประยุกต์ใช้ เพื่อให้การบริหารจัดการเป็นไปโดยครบถ้วน รอบด้าน และสะดวกต่อการพิจารณาและประเมินผล ช่วยให้การแก้ไขปัญหาที่อาจเกิดขึ้นระหว่างการดำเนินการให้เป็นไปอย่างรวดเร็วยิ่งขึ้น โดยประกอบด้วยเรื่อง DOTMLPF-P ซึ่งย่อมาจาก Doctrine (หลักนิยม), Organization (การจัดการองค์กร), Materiel (เครื่องมือทางทหาร), Leadership and Education (การพัฒนาความรู้ของผู้นำหน่วย), Personnel (การจัดการกำลังพล), Facilities (การผลิตเครื่องมือหรือสิ่งอำนวยความสะดวกเพื่อใช้งานได้เอง), Policy (นโยบายหรือแนวทางปฏิบัติ) โดยมีรายละเอียดดังต่อไปนี้

แผนภาพ ๔ – ๒ กรอบแนวคิดการบริหารจัดการศักยภาพด้านไซเบอร์ของกองทัพสหรัฐอเมริกา

หลักนิยม (Doctrine) หมายถึง วิธีการซึ่งได้รับการพิสูจน์แล้วว่า “ดี” เหมาะสมสำหรับการนำไปปฏิบัติในการปฏิบัติการ หากดำเนินการตามแล้วเชื่อได้ว่าจะประสบความสำเร็จ ซึ่งหลักนิยมเป็นสิ่งที่ได้มาจากการรวบรวม และวิเคราะห์จากบทเรียนการรบต่าง ๆ เพื่อให้เป็นแนวทางปฏิบัติที่พร้อมนำไปใช้

การจัดองค์กร (Organization) หมายถึง วิธีการจัดการองค์กร โดยมีการจัดแบ่งออกเป็นองค์ประกอบย่อย ๆ ซึ่งมีขอบเขตอำนาจหน้าที่ที่รับผิดชอบกำกับ และมีพันธกิจที่มีต่อองค์กร

การฝึกอบรม (Training) หมายถึง การเตรียมการให้บุคคลากรทุกระดับ ได้มีความรู้ ทักษะ ประสบการณ์ที่จำเป็นสำหรับการปฏิบัติงานตามขอบเขตอำนาจหน้าที่ของตน ทั้งนี้รวมทั้งการฝึกในระดับหน่วย เช่น หมู่ ตอน หมวด กองร้อย กองพัน กรม หรือตามรูปแบบการจัดที่เป็นเฉพาะของแต่ละเหล่าทัพ

เครื่องมือทางทหาร (Materiel) หมายถึง การมีเครื่องมือที่เป็นเฉพาะของทหารซึ่งมีความจำเป็นต้องใช้ในการปฏิบัติงาน การมีเครื่องมือที่จำเป็นอย่างเพียงพอย่อมส่งผลถึงประสิทธิภาพและประสิทธิผลของการปฏิบัติงาน

การพัฒนาความรู้ของผู้นำหน่วย (Leadership and Education) หมายถึง การเตรียมการให้ความรู้แก่ผู้นำหน่วยอย่างเหมาะสมแก่ผู้นำทุกระดับ เพื่อให้ได้รับทราบขอบเขตบทบาทอำนาจหน้าที่ที่ตนมีต่อองค์กรและผู้ใต้บังคับบัญชา รวมทั้งต่อภารกิจที่อยู่ในความรับผิดชอบ

การจัดการกำลังพล (Personnel) หมายถึง การสร้าง ใช้ บำรุงรักษา พัฒนากำลังพลอย่างเป็นระบบ เพื่อให้ได้กำลังในแต่ละระดับแต่ละหน้าที่ อย่างเหมาะสมทั้งด้านปริมาณและคุณภาพและโดยต่อเนื่อง รวมทั้งการสร้างแรงจูงใจให้มีทัศนคติที่ดีต่อการปฏิบัติงานเพื่อองค์กร

การพัฒนาเครื่องมือหรือสิ่งอำนวยความสะดวกเพื่อใช้งานได้เอง (Facilities) หมายถึง การที่สามารถพัฒนาสิ่งอำนวยความสะดวกแก่การปฏิบัติทางทหารขึ้นได้เอง เช่น การมีหน่วยงานวิจัยและพัฒนา หรือหน่วยงานด้านอุตสาหกรรมป้องกันประเทศ เป็นต้น ซึ่งนอกจากเป็นพึ่งพาตนเองแล้ว ยังเป็นการส่งเสริมและรักษาองค์ความรู้ด้านการผลิตและการนำไปใช้งานที่จำเป็นในการปฏิบัติภารกิจทางทหาร ให้คงอยู่กับองค์กรได้อีกด้วย

นโยบาย (Policy) หมายถึง การที่มีนโยบายหรือแนวทางปฏิบัติเพื่อให้องค์กรรวมทั้งองค์ประกอบต่าง ๆ ขององค์การให้ยึดถือปฏิบัติตาม ให้เป็นไปในแนวทางเดียวกันและโดยสอดคล้องกันโดยตลอดทั้งองค์กร

การกำหนดวัตถุประสงค์และยุทธศาสตร์การป้องกันไซเบอร์กระทรวงกลาโหม

จากการศึกษาและวิเคราะห์จากบทที่ผ่านและในบทนี้ เมื่อพิจารณาประเด็นสำคัญในการป้องกันไซเบอร์ของต่างประเทศ และภัยคุกคามจากไซเบอร์โดยทั่วไป รวมถึงภัยคุกคามจากสงครามไซเบอร์ ที่มีผลกระทบที่จะเกิดขึ้นกับประเทศไทยและกระทรวงกลาโหม เมื่อนำมาพิจารณาร่วมกับ ขีดความสามารถและปัญหาการดำเนินการด้านไซเบอร์ของกระทรวงกลาโหม สามารถกำหนดเป็น**วัตถุประสงค์การป้องกันไซเบอร์กระทรวงกลาโหม** ได้ดังนี้

๑. การดำเนินการด้านไซเบอร์ทั้งปวงต้องมีหน่วยรับผิดชอบทั้งทางด้านนโยบายและยุทธศาสตร์ และการปฏิบัติ ที่ชัดเจนมีเอกภาพเป็นไปในทิศทางเดียวกัน มีกำลังพลที่เชี่ยวชาญพร้อมปฏิบัติงาน

๒. ไซเบอร์ของกระทรวงกลาโหมต้องพร้อมใช้งานตลอดเวลา มีความเชื่อถือได้ มีการรักษาความลับที่ดี

๓. หากมีการโจมตีจากฝ่ายตรงข้ามต้องสามารถป้องกันและทำลายการโจมตีได้อย่างรวดเร็วก่อนที่จะมีการโจมตีเข้ามาในไซเบอร์ของกระทรวงกลาโหมประเทศ

๔. สร้างเครือข่ายความร่วมมือ สร้างพลังร่วม ร่วมกันดำเนินการ ประสานกับทุกภาคส่วนทั้งในประเทศและต่างประเทศ

การกำหนดยุทธศาสตร์การป้องกันไซเบอร์กระทรวงกลาโหม

วัตถุประสงค์การป้องกันไซเบอร์กระทรวงกลาโหมข้างต้น คือ เป้าหมาย (Ends) หรือความต้องการให้เกิด โดยจะต้องมีการกำหนดยุทธศาสตร์การป้องกันไซเบอร์กระทรวงกลาโหม คือ

วิธีหรือหนทางปฏิบัติ (Ways) และมีเครื่องมือสนับสนุน (Means) ต่อไป โดยนำปัจจัยอื่น ๆ เพิ่มเติมมาพิจารณาด้วย ดังรูป

แผนภาพที่ ๔ – ๓ ปัจจัยอื่น ๆ ในการพิจารณากำหนดยุทธศาสตร์ไซเบอร์กระทรวงกลาโหม

๑. ข้อจำกัดทางทรัพยากรของกระทรวงกลาโหม

๑.๑ ทรัพยากรบุคคลและงบประมาณ มีจำกัด

๑.๒ เป็นผู้บริโภคเทคโนโลยีมากกว่าเป็นผู้ผลิตเทคโนโลยี

๑.๓ การปฏิบัติงานด้านไซเบอร์ของหน่วยงานภาครัฐ ดำเนินการตามขอบเขตภารกิจของตน ซึ่งเป็นขอบเขตที่จำกัด

๑.๔ การผนึกกำลังเพื่อปฏิบัติการ ต้องมีหน่วยงานจัดการให้เกิดการประสานสอดคล้อง และมีแผน/ข้อตกลง/ซักซ้อม ในการดำเนินการร่วมกัน

๒ สภาวะแวดล้อมทางยุทธศาสตร์

๒.๑ ภัยคุกคามเกิดขึ้นอยู่เสมอ ส่วนที่ตรวจพบควบคุมได้ แต่ภัยคุกคามที่แฝงอยู่และยังไม่ถูกตรวจพบอาจมีอยู่ การโจมตีทางไซเบอร์เต็มรูปแบบอาจเกิดได้ทุกเมื่อ

๒.๒ ประสิทธิภาพการรบ ปัจจุบันมีการพึ่งพาไซเบอร์ในระดับหนึ่ง แต่มีการพึ่งพาเพิ่มมากขึ้นเรื่อย ๆ ตามการใช้การปฏิบัติการที่มีเครือข่ายเป็นศูนย์กลาง

๒.๓ การจัดการสภาวะแวดล้อมด้านไซเบอร์ของกระทรวงกลาโหม เช่น กฎหมาย หลักนิยม กฎการใช้กำลัง ยังไม่รองรับ

๒.๔ ความความหวังของระดับรัฐบาลต่อกระทรวงกลาโหม ในการดำเนินการต่อวิกฤติการไซเบอร์ระดับชาติ มีสูง

๓ เทคโนโลยีด้านไซเบอร์

๓.๑ เทคนิค วิธีการ รูปแบบการโจมตี แทรกซึม หลอกลวง พัฒนาอย่างรวดเร็ว การที่จะทำให้มีสถานภาพที่เท่าทันเทคโนโลยีอยู่เสมอ การใช้เทคโนโลยีปกป้องอาจมีมูลค่าสูงกว่ามูลค่าของทรัพย์สินที่ปกป้อง

๓.๒ การเป็นผู้บริโภคเทคโนโลยีด้านไซเบอร์ ทำให้กระทรวงกลาโหม ต้องตัดสินใจที่จะใช้ยุทธศาสตร์ที่ใช้ความเชี่ยวชาญของคน เพื่อให้พัฒนาได้อย่างต่อเนื่องไม่จำกัด และทันกับการพัฒนาไซเบอร์ที่พัฒนาไปอย่างรวดเร็ว และการผลิตเทคโนโลยีใช้เองได้ จะช่วยเพิ่มทางเลือกให้มากขึ้น

๓.๓ การมีข้อจำกัดในการได้มาและใช้งานเทคโนโลยี มีผลต่อความเสี่ยงหรือมีความล่อแหลมต่อการขยายผลของความเสียหาย หากไม่สามารถจัดหาได้ทันการ

๔ พันธมิตร มิตรประเทศ สถาบันระหว่างประเทศ

๔.๑ ประเทศไทยมีหน่วยงานที่ดำเนินการเกี่ยวกับไซเบอร์สเปซของประเทศ ทั้งภาครัฐ รัฐวิสาหกิจ เอกชน แต่ยังอยู่ในขอบเขตที่จำกัดและยังไม่มีเอกภาพ จำเป็นต้องพึ่งพิงต่างมิตรประเทศและสถาบันระหว่างประเทศ

๔.๒ การมีความสัมพันธ์กับหน่วยงานภาครัฐที่เกี่ยวข้องในประเทศ และชาติพันธมิตรยังไม่เหนี่ยวแน่น

๔.๓ ข้อตกลงหรือแผนงานในการปฏิบัติงานร่วมกัน ที่เป็นส่วนหนึ่งของแผนระดับชาติ ปัจจุบันยังไม่มีข้อตกลงหรือแผนงานแต่อย่างใด

ยุทธศาสตร์การป้องกันไซเบอร์กระทรวงกลาโหม

เมื่อพิจารณาวัตถุประสงค์การป้องกันไซเบอร์กระทรวงกลาโหม ร่วมกับ ปัจจัยแวดล้อม ปัญหาการดำเนินการและขีดความสามารถด้านไซเบอร์ของกระทรวงกลาโหม ทำให้ทราบถึงสิ่งที่เป็นอุปสรรค ข้อจำกัด หรือสนับสนุนต่อวัตถุประสงค์การป้องกันไซเบอร์กระทรวงกลาโหม สิ่งที่เป็นปัจจัยสนับสนุนจะทำให้ยุทธศาสตร์การป้องกันไซเบอร์กระทรวงกลาโหมประสบความสำเร็วได้ง่าย ส่วนที่เป็นอุปสรรคเป็นข้อพิจารณาแก้ไขข้อจำกัดนั้น เมื่อประมวลทั้งหมดแล้วจึงสามารถพิจารณากำหนดเป็นยุทธศาสตร์การป้องกันไซเบอร์กระทรวงกลาโหม ได้ดังนี้

ยุทธศาสตร์ที่ ๑ การเสริมสร้างศักย์ภาพด้านไซเบอร์ของกระทรวงกลาโหม ให้มีความพร้อมในการรับมือกับภัยคุกคาม

ยุทธศาสตร์ที่ ๒ การป้องกันไซเบอร์ ให้มีความปลอดภัยพร้อมใช้งาน เชื่อถือได้ มีการรักษาความลับ และไม่ให้เป็นจุดอ่อนหรือจุดล่อแหลมต่อการปฏิบัติภารกิจ เพื่อให้การปฏิบัติการทางทหารมีเสรีและเพิ่มมิติในการปฏิบัติ

ยุทธศาสตร์ที่ ๓ การป้องกันไซเบอร์เชิงรุก เพื่อทำการรบกวน ขัดขวาง ทำลายการโจมตีทางไซเบอร์ของผู้ไม่ประสงค์ดีก่อนที่จะเริ่มขึ้น จำกัดเสรีในการปฏิบัติของผู้ไม่ประสงค์ดีด้วยการเฝ้าตรวจ การหาข่าวทางไซเบอร์อย่างต่อเนื่อง และเข้าปฏิบัติการทันทีเมื่อมีข้อบ่งชี้ว่าจะมีการปฏิบัติการใด ๆ ที่จะเป็นอันตรายต่อฝ่ายเรา

ยุทธศาสตร์ที่ ๔ การผนึกกำลังด้านไซเบอร์ ในการป้องกันไซเบอร์ และการป้องกันไซเบอร์เชิงรุก การมีส่วนร่วมในการบริหารจัดการการปฏิบัติการไซเบอร์ของชาติอย่างมีเอกภาพตั้งแต่ภาวะปกติจนถึงภาวะสงคราม โดยผนึกกำลังทั้งภาครัฐ ภาคเอกชน และภาคประชาชน รวมทั้งประสานความร่วมมือกับมิตรประเทศ

แนวความคิดทางยุทธศาสตร์การป้องกันไซเบอร์กระทรวงกลาโหม

เพื่อให้การดำเนินการตามยุทธศาสตร์การป้องกันไซเบอร์กระทรวงกลาโหมแต่ละยุทธศาสตร์ที่ได้กำหนดไว้ข้างต้น ให้มีประสิทธิภาพและประสิทธิผลจึงกำหนดรายละเอียดแยกตามเป้าหมาย (Ends) วิธีการ (Ways) และเครื่องมือ (Means) ได้ดังนี้

๑. ยุทธศาสตร์ที่ ๑ การเสริมสร้างศักย์ภาพด้านไซเบอร์ของกระทรวงกลาโหมให้มีความพร้อมในการรับมือกับภัยคุกคาม

๑.๑ เป้าหมาย

๑.๑.๑ มีหน่วยงานรับผิดชอบหลักด้านไซเบอร์ของกระทรวงกลาโหมที่ครอบคลุมทั้งในระดับนโยบายและยุทธศาสตร์ และระดับปฏิบัติการ

๑.๑.๒ มีบุคลากรด้านไซเบอร์ของกระทรวงกลาโหมที่เพียงพอ

๑.๑.๓ มีเครื่องมือ เทคโนโลยี หลักนิยาม และมาตรฐานด้านไซเบอร์ของกระทรวงกลาโหม

๑.๒ วิธีการ

๑.๒.๑ จัดตั้งหน่วยใหม่ โดยปรับโครงสร้างการจัดหน่วยที่มีอยู่แล้ว และเพิ่มเติมใหม่บางส่วน และบูรณาการ การทำงานร่วมกันภายในกระทรวงกลาโหม

๑.๒.๒ จัดหาบุคลากร การจัดการฝึกอบรม และส่งบุคลากรไปฝึกอบรมด้านไซเบอร์

๑.๒.๓ วางแผนและจัดหายุทโธปกรณ์ เทคโนโลยี กำหนดมาตรฐาน และพัฒนาเทคนิคการรักษาความปลอดภัยไซเบอร์

๑.๒.๔ จัดการฝึกจำลองสถานการณ์ไซเบอร์ประจำปี

๑.๓ เครื่องมือ

๑.๓.๑ กฎหมาย ระเบียบคำสั่ง กระทรวงกลาโหม

๑.๓.๒ การฝึกอบรม การประชุมสัมมนาระดมสมอง

๑.๓.๓ ระบบจำลองสถานการณ์ด้านไซเบอร์

๒. ยุทธศาสตร์ที่ ๒ การป้องกันไซเบอร์ ให้มีความปลอดภัยพร้อมใช้งาน เชื่อถือได้ มีการรักษาความลับ และไม่ให้เป็นจุดอ่อนหรือจุดล่อแหลมต่อการปฏิบัติภารกิจ เพื่อให้การปฏิบัติการทางทหารมีเสรีและเพิ่มมิติในการปฏิบัติ

๒.๑ เป้าหมาย

๒.๑.๑ ปกป้องทรัพยากรสารสนเทศของกระทรวงกลาโหม ทั้งที่ระบบควบคุมบังคับบัญชา และระบบสารสนเทศเพื่อการบริหารราชการทั่วไป ได้แก่ ข้อมูล ระบบสารสนเทศ และองค์ประกอบสนับสนุน

๒.๑.๒ ปกป้องสิทธิการเข้าถึงทรัพยากรสารสนเทศของกระทรวงกลาโหม ทั้งที่ระบบควบคุมบังคับบัญชา และระบบสารสนเทศเพื่อการบริหารราชการทั่วไป

๒.๑.๓ ป้องกันการจารกรรมและการก่อวินาศกรรมทางไซเบอร์

๒.๒ วิธีการ

๒.๒.๑ ปรับปรุงหรือลดขอบเขตการเชื่อมต่อไซเบอร์ของกระทรวงกลาโหม ให้มีเท่าที่จำเป็นต้องใช้และป้องกันได้ เพื่อการใช้อย่างเกิดประโยชน์และสอดคล้องกัน

๒.๒.๒ การบริหารจัดการสิทธิการเข้าถึงไซเบอร์ของกระทรวงกลาโหม และการเปิดเผยข้อมูลตัวตนหรือทรัพยากรทางสารสนเทศของกระทรวงกลาโหม

๒.๒.๓ สร้างความตระหนักและกำกับดูแะผู้ใช้ระบบไซเบอร์ให้อยู่ใน กฎ ระเบียบ ข้อบังคับและมาตรฐานที่กำหนด เพื่อลดความเสี่ยงของภัยคุกคามไซเบอร์

๒.๒.๔ เฝ้าตรวจ ควบคุม และกำจัดภัยคุกคามไซเบอร์ที่ตรวจพบ

๒.๒.๕ ทดสอบการเจาะระบบอย่างสม่ำเสมอ

๒.๒.๖ จัดหาและพัฒนาเทคโนโลยีไซเบอร์ด้านการทหารที่ทันสมัยก้าวหน้า

๒.๓ เครื่องมือ

๒.๓.๑ ระดับนโยบาย ได้แก่ คณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และระดับปฏิบัติ ได้แก่ ชุดตอบสนองภัยคุกคามไซเบอร์กระทรวงกลาโหม (MODCSIRT) ชุดปฏิบัติงานข้อมูลข่าวสารด้านไซเบอร์กระทรวงกลาโหม ศูนย์นิติวิทยาดิจิตอลกระทรวงกลาโหม สถาบันหรือหลักสูตรอบรมไซเบอร์มาตรฐานกระทรวงกลาโหม

๒.๓.๒ กฎหมาย หรือข้อตกลงความร่วมมือทุกรูปแบบ ที่เอื้อต่อการป้องกันไซเบอร์ของกระทรวงกลาโหม

๒.๓.๓ วิจัยและพัฒนาเทคโนโลยีเชิงตรวจจับ ป้องกัน ลวง เช่น การเข้าและถอดรหัส หรือระบบที่จัดทำขึ้นเพื่อลวงให้มีการบุกรุก เป็นต้น

๒.๓.๔ พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมอิเล็กทรอนิกส์ พ.ศ.๒๕๕๓ และกฎระเบียบหรือกระบวนการของกระทรวงกลาโหม ที่สนับสนุนกฎหมายดังกล่าว

๓. ยุทธศาสตร์ที่ ๓ การป้องกันไซเบอร์เชิงรุก เพื่อทำการรบกวน ขัดขวาง ทำลายการโจมตีทางไซเบอร์ของผู้ไม่ประสงค์ดีก่อนที่จะเริ่มขึ้น จำกัดเสรีในการปฏิบัติของผู้ไม่ประสงค์ดีด้วยการเฝ้าตรวจ การหาข่าวทางไซเบอร์อย่างต่อเนื่อง และเข้าปฏิบัติการทันทีเมื่อมีข้อบ่งชี้ว่าจะมีการปฏิบัติการใด ๆ ที่จะเป็นอันตรายต่อฝ่ายเรา

๓.๑ เป้าหมาย

๓.๑.๑ จำกัดเสรีการใช้ไซเบอร์ของฝ่ายตรงข้าม ในด้านยุทธการ การข่าวกรอง และการปฏิบัติการข่าวสารไซเบอร์

๓.๑.๒ รบกวน ขัดขวาง ทำลายการโจมตีทางไซเบอร์ของฝ่ายตรงข้าม

๓.๒ วิธีการ

๓.๒.๑ จัดทำทำเนียบกำลังรบ บัญชีเป้าหมาย การแทรกซึมทางไซเบอร์

๓.๒.๒ กำหนดเป้าหมายและเฝ้าติดตามความเคลื่อนไหว ของกิจกรรมทางตรงหรืออ้อมที่มีผลต่อขีดความสามารถด้านไซเบอร์ของฝ่ายตรงข้าม รวมถึงการปฏิบัติการ ไซเบอร์ของฝ่ายตรงข้ามตั้งแต่ยามที่การโจมตียังไม่เกิดขึ้น

๓.๒.๓ สร้าง พัฒนา ใช้งาน ดำรงรักษาขีดความสามารถในด้านการแทรกซึมหรือลวงล่อทางสังคมไซเบอร์ กลวิธีการโจมตี ซึ่งปฏิบัติส่วนหนึ่งของการเตรียมการรบและในการรบ

๓.๓ เครื่องมือ

๓.๓.๑ ระดับนโยบาย ได้แก่ คณะกรรมการการป้องกันไซเบอร์กระทรวงกลาโหม ระดับปฏิบัติ ได้แก่ ศูนย์อำนวยการยุทธไซเบอร์ ชุดตอบสนองภัยคุกคามไซเบอร์กระทรวงกลาโหม (MODCSIRT) ชุดปฏิบัติการข่าวสารไซเบอร์ สถาบันฝึกอบรมและมาตรฐานไซเบอร์กระทรวงกลาโหม

๓.๓.๒ กฎหมาย หรือข้อตกลงความร่วมมือทุกรูปแบบที่เอื้อต่อกระทรวงกลาโหมในการจำกัดเสรีการปฏิบัติในไซเบอร์ของฝ่ายตรงข้าม

๓.๓.๓ วิจัยและพัฒนาอาวุธไซเบอร์ที่มีผลทางยุทธศาสตร์ และยุทธวิธีการโจมตี แทรกซึม ลวง หาข่าว ปล่อยข่าว

๓.๓.๔ การประชุมระดับนโยบาย การซ้อมรับมือภัยคุกคามไซเบอร์ การฝึกร่วมของระดับปฏิบัติ

๓.๓.๕ หลักนิยม กฎการใช้กำลัง หลักการดำเนินกลยุทธ หลักการแทรกซึม และหลักการหรือกฎระเบียบใดๆ ที่สนับสนุนตามรายละเอียดที่กำหนดไว้วิธีการ

๔. ยุทธศาสตร์ที่ ๔ การผนึกกำลังด้านไซเบอร์ ในการป้องกันไซเบอร์และการป้องกันไซเบอร์เชิงรุก การมีส่วนร่วมในการบริหารจัดการการปฏิบัติการไซเบอร์ของชาติอย่างมีเอกภาพตั้งแต่ภาวะปกติจนถึงภาวะสงคราม โดยผนึกกำลังทั้งภาครัฐ ภาคเอกชน และภาคประชาชน รวมทั้งประสานความร่วมมือกับมิตรประเทศ

๔.๑ เป้าหมาย ผนึกกำลังและความร่วมมือ เพื่อการป้องกันไซเบอร์ระดับชาติและระดับนานาชาติ ในการป้องกันและการป้องกันไซเบอร์เชิงรุก ของกระทรวงกลาโหม และของประเทศไทย

๔.๑.๑ กระทรวงกลาโหม หน่วยงานภาครัฐ หน่วยงานภาคเอกชน รัฐวิสาหกิจหรือภาคเอกชนที่ให้บริการระบบสาธารณูปโภคพื้นฐานสำคัญของรัฐ หน่วยงานให้บริการประชาชน หน่วยงานให้บริการทางการเงิน ผู้ให้บริการเชื่อมต่ออินเทอร์เน็ต สถาบันการศึกษา

๔.๑.๒ กระทรวงกลาโหม สถาบันการศึกษา รัฐบาลหรือกระทรวงกลาโหมชาติพันธมิตร

๔.๒ วิธีการ

๔.๒.๑ ร่วมกันปฏิบัติการไซเบอร์ในขอบเขตรับผิดชอบ ในฐานะเป็นส่วนหนึ่งของการปฏิบัติระดับชาติในยามปกติ และตามขอบเขตที่กำหนดเพิ่มเติมในยามวิกฤติ

๔.๒.๒ ดำรงรักษาความสัมพันธ์ระดับประเทศที่ได้ประโยชน์ร่วมกัน ทบทวนและแสวงความสัมพันธ์ที่เป็นประโยชน์ชัดเจน

๔.๒.๓ ผลักดัน/ทำให้เครื่องมือที่ไม่มีให้เกิดขึ้น

๔.๓ เครื่องมือ

๔.๓.๑ ระดับนโยบาย ได้แก่ การประชุมระดับชาติ ระดับอาเซียน ระดับภูมิภาค คณะกรรมการการป้องกันไซเบอร์กระทรวงกลาโหม ระดับปฏิบัติ ได้แก่ ชุดตอบสนองภัยคุกคามไซเบอร์กระทรวงกลาโหม (MODCSIRT) ชุดปฏิบัติการข่าวสารไซเบอร์กระทรวงกลาโหม สถาบันฝึกอบรมและมาตรฐานไซเบอร์กระทรวงกลาโหม

๔.๓.๒ หน่วยงานภาครัฐที่เกี่ยวข้องระดับกรม กระทรวงหรือสูงกว่ากระทรวงและข้อตกลงการปฏิบัติงานร่วมกัน

๔.๓.๓ หน่วยงานให้บริการเชื่อมต่ออินเทอร์เน็ตทุกรูปแบบ บริษัทเอกชนที่เกี่ยวข้อง และข้อตกลงการปฏิบัติงานร่วมกัน

๔.๓.๔ หน่วยงานสาธารณูปโภคพื้นฐานสำคัญของรัฐ หน่วยงานบริการประชาชน หรือที่มีผลทางเศรษฐกิจ สถาบันการศึกษา และข้อตกลงการปฏิบัติงานร่วมกัน

๔.๓.๕ กฎหมายที่เอื้อต่อการผนึกกำลังป้องกันประเทศด้านไซเบอร์ของประเทศ

๔.๓.๖ แผนหรือยุทธศาสตร์การผนึกกำลังป้องกันประเทศด้านไซเบอร์แห่งชาติ และการซ้อมตามแผนดังกล่าว

สรุป

จากการวิเคราะห์พบว่าภัยคุกคามจากไซเบอร์นั้นมีอยู่ทั่วโลก มากและน้อยขึ้นอยู่กับการใช้งานไซเบอร์ในแต่ละประเทศ ในบางประเทศโดยเฉพาะประเทศมหาอำนาจจะมีการพึ่งพาไซเบอร์ในการควบคุมโครงสร้างพื้นฐาน ใช้ในระบบเศรษฐกิจการเงิน ใช้ในการปฏิบัติงานที่สำคัญของรัฐ และในการควบคุมและพัฒนาอุตสาหกรรม เป็นต้น ดังนั้นประเทศเหล่านี้ต่างให้ความสำคัญกับการดำเนินการป้องกันไซเบอร์เป็นอย่างมาก มีการจัดตั้งหน่วยงานกำกับดูแลด้านไซเบอร์โดยเฉพาะ มีการกำหนดนโยบายและยุทธศาสตร์ชัดเจน และที่สำคัญคือ ระดับผู้นำของชาติให้ความสำคัญ และถือว่าเป็นภารกิจหลักของชาติประการหนึ่ง สำหรับประเทศไทยกำลังมุ่งมั่นที่จะเดินหน้าไปสู่เศรษฐกิจดิจิทัล นั้นก็คือการใช้ไซเบอร์เป็นเครื่องมือหลักของการพัฒนาเศรษฐกิจของประเทศ ดังนั้น กระทรวงกลาโหมซึ่งถือว่าเป็นหน่วยงานหลักด้านความมั่นคงของประเทศ จึงต้องให้ความสนใจและพัฒนาศักยภาพด้านไซเบอร์ของกระทรวงกลาโหม ให้พร้อมรับมือกับภัยคุกคามไซเบอร์ที่จะมีต่อประเทศไทยในอนาคตอันใกล้นี้ การกำหนดยุทธศาสตร์การป้องกันไซเบอร์กระทรวงกลาโหมนี้ ไม่ได้มีผลเฉพาะกระทรวงกลาโหม แต่จะมีผลต่อประเทศไทยเป็นส่วนรวม เพราะฉะนั้นด้วยเหตุที่การพัฒนาบุคลากรผู้เชี่ยวชาญด้านไซเบอร์ การพัฒนาเทคโนโลยี กลยุทธและเทคนิคด้านไซเบอร์ ต้องใช้เวลาไม่สามารถกระทำได้ด้วยเวลาอันสั้น จึงต้องมีการเตรียมการล่วงหน้าทั้ง ๓ องค์ประกอบหลัก คือ คน กระบวนการ และเทคโนโลยี ไว้ก่อนที่ภัยคุกคามจะเกิดผลเสียหายต่อความมั่นคงของประเทศไทย

บทที่ ๕
สรุปและข้อเสนอแนะ

สรุปสถานการณ์และความพร้อมของกระทรวงกลาโหมด้านไซเบอร์

๑. ภัยคุกคามไซเบอร์ในปัจจุบันและอนาคตมีผลกระทบต่อความมั่นคงของประเทศ โดยเฉพาะทางด้านเศรษฐกิจและสังคม ซึ่งกระทบต่อความน่าเชื่อถือของประเทศในการทำธุรกรรมทางอิเล็กทรอนิกส์ รวมถึงผลกระทบต่อด้านการทหาร เช่น การทำให้ระบบควบคุมบังคับบัญชา ระบบอาวุธใช้งานไม่ได้ การก่อการร้ายทางไซเบอร์ เป็นต้น

๒. การดำเนินการไซเบอร์ของกระทรวงกลาโหมที่ผ่านมาและในปัจจุบัน ได้มีการจัดตั้งหน่วยงานเพื่อทำหน้าที่ในการป้องกันระบบสารสนเทศของกระทรวงกลาโหม ซึ่งสามารถป้องกันตนเองได้ในระดับหนึ่ง กระทรวงกลาโหมมีการสร้างความตระหนักให้กับส่วนราชการ กระทรวง รัฐวิสาหกิจ หน่วยงานที่รับผิดชอบโครงสร้างพื้นฐาน โดยจัดสัมมนาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ รวมถึงมีการฝึกอบรมให้กับกำลังพลของกระทรวงกลาโหม เพื่อให้กำลังพลเกิดความตระหนักถึงภัยคุกคามอย่างต่อเนื่อง สำหรับการพัฒนาบุคลากรด้านไซเบอร์ได้มีการส่งบุคลากรเข้ารับการฝึกอบรมอย่างต่อเนื่องทั้งจากภายในกระทรวงกลาโหม และจากภาคเอกชนทั้งในประเทศและต่างประเทศ ทำให้ปัจจุบันกระทรวงกลาโหม มีบุคลากรด้านไซเบอร์ประมาณ ๕๐ คน (สำรวจเมื่อปี ๒๕๕๖) ซึ่งกระทรวงกลาโหมต้องการอีกเป็นจำนวนมาก แต่เป็นที่ยอมรับกันว่าการจัดหาบุคลากรด้านนี้ทำได้ยาก และค่าใช้จ่ายแต่ละหลักสูตรมีมูลค่าสูงมาก จึงสามารถส่งไปเข้ารับการฝึกอบรมได้ปีละจำนวนไม่มากนัก รวมทั้งการสร้างผู้เชี่ยวชาญต้องใช้เวลาในการสั่งสมประสบการณ์จากการปฏิบัติเป็นเวลานาน

๓. ความพร้อมของกระทรวงกลาโหมในด้านไซเบอร์ ในปัจจุบันมีความพร้อมในเชิงรับ กล่าวคือ มีขีดความสามารถในการป้องกันระบบสารสนเทศของตนเองในระดับหนึ่ง สำหรับขีดความสามารถในการป้องกันเชิงรุก กระทรวงกลาโหมต้องใช้เวลาในการพัฒนา เนื่องจากข้อจำกัดในการจัดตั้งหน่วยใหม่ให้มารับผิดชอบงานไซเบอร์โดยเฉพาะ และงบประมาณในการพัฒนาบุคลากรและเครื่องมือของกระทรวงกลาโหม มีจำกัดเพราะต้องให้ลำดับความสำคัญเร่งด่วนทางทหาร ให้กับการจัดหาอาวุธยุทโธปกรณ์เป็นลำดับแรก จึงต้องเฉลี่ยงบประมาณตามลำดับความเร่งด่วน รวมถึงการปฏิบัติการป้องกันเชิงรุกต้องมีการออกกฎหมายหรือปรับปรุงกฎหมาย ให้อำนาจหน้าที่แก่ฝ่ายความมั่นคงสามารถปฏิบัติการได้โดยไม่ผิดกฎหมาย

ข้อเสนอแนะ

๑. กระทรวงกลาโหมควรกำหนดนโยบายและยุทธศาสตร์ด้านไซเบอร์ให้ชัดเจน เพื่อให้การดำเนินการด้านไซเบอร์ของกองทัพมีเอกภาพและเป็นไปในทิศทางเดียวกัน โดยผู้วิจัยขอเสนอยุทธศาสตร์การป้องกันไซเบอร์กระทรวงกลาโหมดังนี้

ยุทธศาสตร์การป้องกันไซเบอร์กระทรวงกลาโหม

ยุทธศาสตร์ที่ ๑ การเสริมสร้างศักย์ภาพด้านไซเบอร์ของกระทรวงกลาโหมให้มีความพร้อมในการรับมือกับภัยคุกคาม

ยุทธศาสตร์ที่ ๒ การป้องกันไซเบอร์ ให้มีความปลอดภัยพร้อมใช้งาน เชื่อถือได้ มีการรักษาความลับ และไม่ให้เป็นจุดอ่อนหรือจุดล่อแหลมต่อการปฏิบัติภารกิจ เพื่อให้การปฏิบัติการทางทหารมีเสรีและเพิ่มมิติในการปฏิบัติ

ยุทธศาสตร์ที่ ๓ การป้องกันไซเบอร์เชิงรุก เพื่อทำการรบกวน ขัดขวาง ทำลายการโจมตีทางไซเบอร์ของผู้ไม่ประสงค์ดีก่อนที่จะเริ่มขึ้น จำกัดเสรีในการปฏิบัติของผู้ไม่ประสงค์ดีด้วยการเฝ้าตรวจ การหาข่าวทางไซเบอร์อย่างต่อเนื่อง และเข้าปฏิบัติการทันทีเมื่อมีข้อบ่งชี้ว่าจะมีการปฏิบัติการใด ๆ ที่จะเป็นอันตรายต่อฝ่ายเรา

ยุทธศาสตร์ที่ ๔ การผนึกกำลังด้านไซเบอร์ ในการป้องกันไซเบอร์ และการป้องกันไซเบอร์เชิงรุก การมีส่วนร่วมในการบริหารจัดการการปฏิบัติการไซเบอร์ของชาติอย่างมีเอกภาพตั้งแต่ภาวะปกติจนถึงภาวะสงคราม โดยผนึกกำลังทั้งภาครัฐ ภาคเอกชน และภาคประชาชน รวมทั้งประสานความร่วมมือกับมิตรประเทศ

๒. ปัจจัยสนับสนุนเร่งด่วนในการเพิ่มขีดความสามารถทางด้านไซเบอร์ทั้งเชิงรับและการป้องกันเชิงรุกของกระทรวงกลาโหม

๒.๑ ให้มีการออกกฎหมายหรือปรับปรุงกฎหมาย ให้เจ้าหน้าที่ฝ่ายความมั่นคงสามารถดำเนินการทั้งเชิงรับและการป้องกันเชิงรุกได้ เพราะหากไม่มีกฎหมายให้อำนาจไว้การปฏิบัติการป้องกันเชิงรุกจะทำให้เจ้าหน้าที่ฝ่ายความมั่นคงมีความผิดตามกฎหมายทั้งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง

๒.๒ สนับสนุนการจัดตั้งหน่วยงานเฉพาะด้านไซเบอร์ ด้วยการเปิดอัตราใหม่และการบรรจุจากพลเรือน เนื่องจากข้อจำกัดในการจัดตั้งหน่วยใหม่ที่การเพิ่มอัตรากำลังพลนั้นห้ามเปิดอัตราใหม่ โดยให้ทำการปรับเกลี่ยจากอัตรากำลังพลที่มีอยู่ จึงทำให้กำลังพลที่ติดมากับอัตราเดิมไม่สามารถปฏิบัติการได้ทันทีจะต้องดำเนินการปรับสภาพให้มีความรู้ความสามารถด้านไซเบอร์ซึ่ง

การปรับสภาพจนมีขีดความสามารถต้องใช้เวลานานมากหรือบางครั้งบุคคลนั้นไม่สามารถทำได้ เพราะการพัฒนาความสามารถของกำลังพลไซเบอร์ต้องผ่านการอบรม การฝึกความเชี่ยวชาญ และเสริมสร้างประสบประการณ์ ซึ่งต้องใช้เวลาและงบประมาณสูงและมิใช่ว่าทุกคนจะพัฒนาด้านไซเบอร์ได้ ดังนั้นการบรรจุพลเรือนจึงเหมาะสมและรวดเร็วกว่า ซึ่งหน่วยที่ต้องดำเนินการจัดตั้งโดยเร่งด่วน คือ ศูนย์บัญชาการไซเบอร์กระทรวงกลาโหม และ หน่วยปฏิบัติการไซเบอร์ของกองบัญชาการกองทัพไทยและเหล่าทัพ เพื่อบูรณาการปฏิบัติการไซเบอร์ของทุกภาคส่วนทั้งฝ่ายความมั่นคง ภาครัฐ และเอกชน

๒.๓ สนับสนุนงบประมาณในการพัฒนาบุคลากรและเครื่องมือด้านไซเบอร์เป็นพิเศษ เนื่องจากงบประมาณของกระทรวงกลาโหม ต้องจัดสรรให้ความสำคัญกับอาวุธยุทโธปกรณ์เป็นลำดับแรก จึงมีงบประมาณที่จะใช้สำหรับงานด้านไซเบอร์จำนวนจำกัด ทำให้ต้องใช้เวลาในการพัฒนาขีดความสามารถด้านไซเบอร์มาก

๓. แนวความคิดในการจัดตั้งศูนย์บัญชาการไซเบอร์กระทรวงกลาโหมและหน่วยปฏิบัติการไซเบอร์ของกองบัญชาการกองทัพไทยและเหล่าทัพ เพื่อให้กระทรวงกลาโหมมีหน่วยปฏิบัติงานด้านไซเบอร์ตั้งแต่หน่วยในระดับนโยบายและยุทธศาสตร์จนถึงหน่วยปฏิบัติ ซึ่งจะช่วยสร้างพลังในการปฏิบัติงานให้เพิ่มมากขึ้น โดยปรับปรุงโครงสร้างการจัดหน่วยแปรสภาพหน่วยงานด้านไซเบอร์ของสำนักงานปลัดกระทรวงกลาโหม กองบัญชาการกองทัพไทยและเหล่าทัพที่มีอยู่แล้วและเพิ่มเติมอีกบางส่วนให้มีโครงสร้างของงานด้านไซเบอร์ภายในกระทรวงกลาโหมให้เป็นเอกภาพ เป็นไปในทิศทางเดียวกัน

๓.๑ หน้าที่ ศูนย์บัญชาการไซเบอร์กระทรวงกลาโหม ทำหน้าที่ในการกำหนดนโยบายและยุทธศาสตร์ด้านไซเบอร์ของกระทรวงกลาโหม การบูรณาการการปฏิบัติการไซเบอร์ภายในกระทรวงกลาโหม และกับทุกภาคส่วนทั้งฝ่ายความมั่นคง ภาครัฐ และเอกชน กำกับดูแลการปฏิบัติการไซเบอร์ให้มีเอกภาพประสานสอนคล้องเสริมแรงซึ่งกันและกัน

๓.๒ กำลังพล ใช้กำลังจากทหารประจำการเพื่อเป็นแกนหลักส่วนหนึ่ง กำลังส่วนที่เหลือใช้กำลังจาก ข้าราชการพลเรือนกลาโหม กำลังพลสำรอง และ การจ้างบริษัทภายนอกที่ผ่านการรับรอง (Outsource)

๓.๓ การบังคับบัญชา

๓.๓.๑ สายการบังคับบัญชา

ศูนย์บัญชาการไซเบอร์กระทรวงกลาโหม ขึ้นตรงรัฐมนตรีว่าการกระทรวงกลาโหมอีก ๑ หน่วย รับผิดชอบพื้นที่ปฏิบัติการไซเบอร์ จาก ๕ พื้นที่ปฏิบัติการ (Domain)

ได้แก่ พื้นที่ปฏิบัติการทาง บก (Land) ทะเล (Sea) อากาศ (Air) อวกาศ (Space) ไซเบอร์ (Cyberspace) ในขั้นต้น ฝากการบังคับบัญชาและทางธุรการไว้กับ สำนักงานปลัดกระทรวงกลาโหม

ศูนย์ปฏิบัติการไซเบอร์กองบัญชาการกองทัพไทยและเหล่าทัพ แต่ละหน่วยแยกขึ้นตรงต่อกองบัญชาการกองทัพไทยและเหล่าทัพ

๓.๓.๒ สายการปฏิบัติการ ใช้หลักการ “ควบคุมแบบรวมการปฏิบัติแบบแยกการ” ควบคุมแบบรวมการ โดยให้ ศูนย์บัญชาการไซเบอร์กระทรวงกลาโหม รับผิดชอบทางด้านนโยบายและยุทธศาสตร์ การบูรณาการประสานงานกับหน่วยงานทุกภาคส่วนในประเทศไทยและต่างประเทศ การบูรณาการการกำหนดเป้าหมาย การรวมพลังของการปฏิบัติการไซเบอร์ การติดตามสถานการณ์ไซเบอร์ของประเทศ (Monitor) การพัฒนาบุคลากรในภาพรวมของกระทรวงกลาโหม การพัฒนาเทคโนโลยีกระบวนการทำงานและหลักนิยม การวิจัยพัฒนาด้านไซเบอร์ รวมถึงการป้องกันเครือข่ายเทคโนโลยีสารสนเทศและการสื่อสารหลักของกระทรวงกลาโหม และของ สำนักงานปลัดกระทรวงกลาโหม

ปฏิบัติแบบแยกการ โดยให้ หน่วยปฏิบัติการไซเบอร์กองบัญชาการกองทัพไทยและเหล่าทัพ รับผิดชอบ การป้องกันเครือข่ายเทคโนโลยีสารสนเทศและการสื่อสารของตนเอง การปฏิบัติการไซเบอร์ในความรับผิดชอบ และปฏิบัติการตามนโยบายและยุทธศาสตร์ด้านไซเบอร์ของกระทรวงกลาโหม รวมถึงการรวมพลังเข้าปฏิบัติการไซเบอร์และร่วมในการปฏิบัติต่อเป้าหมายที่กำหนด

๓.๔ ร่างการจัดศูนย์บัญชาการไซเบอร์กระทรวงกลาโหม

๓.๔.๑ ส่วนบังคับบัญชา เป็นส่วนผู้บังคับบัญชา ธุรการ กำลังพล การงบประมาณการเงิน และการสนับสนุนต่าง ๆ เช่น การพัสดุ การจัดซื้อจัดจ้าง การขนส่ง ฯลฯ

๓.๔.๒ ส่วนนโยบายและแผน เป็นส่วนเสนาธิการ จัดทำนโยบายและยุทธศาสตร์ด้านไซเบอร์ของกระทรวงกลาโหม จัดทำแผนการต่าง ๆ เช่น แผนปฏิบัติการ การกำหนดเป้าหมาย การติดตามสถานการณ์ไซเบอร์ในกระทรวงกลาโหมและของประเทศ ตั้งแต่ภาวะปกติเป็นต้นไป และการอำนวยการยุทธเมื่อมีการปฏิบัติการไซเบอร์ ให้มีฝ่ายกฎหมายไซเบอร์เพื่อปกป้องการปฏิบัติการของเจ้าหน้าที่ไซเบอร์ไม่ให้เป็นกระทำที่ผิดกฎหมาย ตามที่กฎหมายของประเทศไทยและกฎหมายนานาชาติกำหนด และเสนอแนะการแก้ไขกฎหมายที่จำเป็นในการปฏิบัติงาน นอกจากนั้นมีการแยกในส่วนนโยบายและแผนการปฏิบัติการข่าวสารในไซเบอร์เป็นการเฉพาะ เพราะส่วนใหญ่จะเป็นการต่อสู้ทางความคิดในเนื้อหา (Content) ที่เกิดขึ้นในไซเบอร์ ที่ต้องใช้เนื้อหาในการต่อสู้เป็นหลัก ทั้งนี้เพื่อสนับสนุกการปฏิบัติการข่าวสารในภาพรวมด้านอื่น ๆ ของกระทรวงกลาโหมและของประเทศ โดยทำหน้าที่กำหนดนโยบายในการปฏิบัติการข่าวสารไซเบอร์ การค้นหาและกำหนด

เป้าหมายที่เป็นบุคคล กลุ่มบุคคล หรือองค์กร รวมทั้งวางแผน ในการปฏิบัติข่าวสารไซเบอร์ต่อเป้าหมาย

๓.๔.๓ ส่วนปฏิบัติการไซเบอร์ ในศูนย์บัญชาการไซเบอร์กระทรวงกลาโหมจะมีส่วนปฏิบัติการไซเบอร์ที่มีขนาดเล็กกว่าของกองบัญชาการกองทัพไทยและเหล่าทัพ จุดมุ่งหมายหลักของส่วนนี้ เพื่อทำหน้าที่ดำเนินการด้านไซเบอร์ให้กับสำนักงานปลัดกระทรวงกลาโหมและการป้องกันตนเอง โดยชุดเผชิญเหตุทำหน้าที่เป็น MODCERT ในการแก้ปัญหากับเครื่องในเครือข่ายที่ถูกโจมตีหรือติดไวรัสคอมพิวเตอร์ การศึกษาวิทยาการและการสร้างความเชี่ยวชาญด้านการปฏิบัติการไซเบอร์จากการปฏิบัติจริง รวมทั้งเป็นเจ้าภาพหลักในการผนึกกำลังด้านไซเบอร์ ซึ่งการผนึกกำลังจะไม่สามารถกระทำได้หากไม่มีเจ้าภาพที่เป็นแกนหลักในการดำเนินการที่เข้มแข็ง โดยส่วนปฏิบัติการจะรับแผนปฏิบัติการ และเป้าหมายมาจากส่วนนโยบายและแผน นำมาปฏิบัติให้เป็นไปตามแผน

การสืบสวนสอบสวน จำเป็นต้องมีหน่วยงานภายในกระทรวงกลาโหมเป็นการเฉพาะ เพราะหลักฐานทางนิติวิทยาดิจิทัลที่เกิดขึ้นในกระทรวงกลาโหม เช่น เครื่องคอมพิวเตอร์ของเจ้าหน้าที่ทางทหาร ย่อมต้องมีความลับทางทหารติดไปกับตัวเครื่อง ดังนั้นจึงไม่ควรส่งไปให้หน่วยงานนอกกระทรวงกลาโหมช่วยทำทำการสืบสวนสอบสวนให้เพราะจะทำให้ความลับรั่วไหล และเนื่องจากวิทยาการด้านนี้ต้องใช้ความรู้ ความเชี่ยวชาญ ความชำนาญ สูงมาก จึงควรเป็นศูนย์รวมวิทยาการและการปฏิบัติทางด้านนี้โดยเฉพาะ

๓.๔.๔ ส่วนวิจัยและพัฒนาไซเบอร์ เป็นส่วนวิทยาการด้านไซเบอร์โดยเฉพาะ ทำหน้าที่พัฒนาหลักสูตร การฝึกอบรม การเป็นศูนย์ฝึกจำลองยุทธหรือการจำลองสถานการณ์ไซเบอร์ของกระทรวงกลาโหมที่กองบัญชาการกองทัพไทยและเหล่าทัพรวมทั้งส่วนราชการทางด้านความมั่นคงมาใช้ในการฝึกได้และมีการจัดการฝึกผนึกกำลังด้านไซเบอร์ประจำปี มีการวิจัยและพัฒนาอุปกรณ์ด้านไซเบอร์ให้เป็นของประเทศไทยโดยเฉพาะอุปกรณ์การเข้าและถอดรหัส รวมถึงการพัฒนาหลักนิยม การกำหนดมาตรฐานด้านไซเบอร์ภายในกระทรวงกลาโหม เช่น มาตรฐานผู้ใช้คอมพิวเตอร์ในเครือข่ายสารสนเทศ ว่าต้องมีความรู้ได้รับการอบรมอะไรบ้าง ต้องปฏิบัติอะไรได้บ้าง มาตรฐานการนำเครื่องคอมพิวเตอร์มาเชื่อมต่อเครือข่ายสารสนเทศ ว่าแต่ละเครื่องต้องมีการดำเนินการอย่างไรบ้างที่จะทำให้มั่นใจได้ว่าจะมาเชื่อมต่อแล้วทำให้เครือขายสารสนเทศมีความปลอดภัย ข้อมูลข่าวสารที่ใช้รับส่งมีความถูกต้องเชื่อถือได้ มาตรฐานวิชาชีพ ว่าแต่ละตำแหน่งที่ทำงานเกี่ยวกับไซเบอร์ต้องมีวุฒิและผ่านการฝึกอบรมหลักสูตรอะไรมาแล้วบ้าง เป็นต้น

แผนภาพที่ ๕ – ๑ ร่างศูนย์บัญชาการไซเบอร์กระทรวงกลาโหม

๔. ข้อเสนอต่อรัฐบาล

กำหนดให้การดำเนินการด้านไซเบอร์เป็นวาระแห่งชาติที่เร่งด่วนโดยสนับสนุนทรัพยากรในการบูรณาการงานด้านไซเบอร์ของทั้งประเทศ ให้เป็นระบบ มีแนวทางและทิศทางไปในทางเดียวกัน มีเจ้าภาพที่ชัดเจนและเข้มแข็ง คำนึงถึงความมั่นคงของชาติในทุก ๆ ด้าน

บรรณานุกรม

ภาษาไทย

วารสารและหนังสือพิมพ์

10 อันดับภัยอินเทอร์เน็ตล่าสุดประจำปี พ.ศ. 2551 หนังสือ eLeader Thailand ประจำเดือน เดือนกุมภาพันธ์ 2551

ภาษาอังกฤษ

ฐานข้อมูลอิเล็กทรอนิกส์

หน่วยงานไซเบอร์ของต่างประเทศ. เข้าถึงได้จาก : https://en.wikipedia.org/wiki/Main_Page, 2015.

โครงการ Cyber Security Malaysia. เข้าถึงได้จาก : http://www.cybersecurity.my/en/index.html, 2015.

กฎหมายของมาเลเซียที่เกี่ยวกับไซเบอร์. เข้าถึงได้จาก : http://www.msc.com.my/cyberlaws/

การโจมตีมาเลเซีย เมื่อ มิถุนายน 2011. เข้าถึงได้จาก : http://www.gvishnu.com/operation-malaysia-anonymous-hack-malaysian-government-portal/ และ http://mobile.businessweek.com/ news/2011-06-16/malaysia-state-websites-disrupted-as-cyber-attacks-spread.html.

The DoD CYBER STRATEGY. เข้าถึงได้จาก : http://www.defense.gov/home/features/2015/0415_cyber-strategy/ Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

Australian Government Defence White Paper 2013. เข้าถึงได้จาก : http://www.defence.gov.au/whitepaper/2013/docs/ WP_2013_web.pdf

Defense of Japan 2013. เข้าถึงได้จาก : http://www.mod.go.jp/ e/publ/w_paper/2013.html

Chinese Military Modernization and Force Development A Western Perspective. เข้าถึงได้จาก : http://csis.org/files/publication/120621_Chinese_Military_Modernization.pdf

Republic of Korea 2010 Defense White Paper. เข้าถึงได้จาก : http://www.nti.org/media/pdfs/2010WhitePaperAll_eng.pdf?_=1340662780

Norwegian Defence 2013 FACTS and FIGURES. เข้าถึงได้จาก : https://www.bbn.gov.pl/ftp/dok/07/NOR_Norwegian_Defence_2013.pdf

French White Paper Defense and National Security 2013. เข้าถึงได้จาก : http://www.livreblancdefenseetsecurite.gouv.fr/ pdf/the_white_paper_defence_2013.pdf

DOTMLPF-P. เข้าถึงได้จาก : https://en.wikipedia.org/wiki/ DOTMLPF และ http://soldiersystems.net/2012/05/11/dotmlpf-what-is-it/

ประวัติย่อผู้วิจัย

ชื่อ	พลตรี สุทธิศักดิ์ สลักคำ
วัน เดือน ปีเกิด	๒๗ ธันวาคม พ.ศ. ๒๕๐๑
การศึกษา	โรงเรียนพิบูลวิทยาลัย พ.ศ. ๒๕๑๘
	ปริญญาตรี สาขาวิทยาศาสตร์ โรงเรียนนายร้อยพระจุลจอมเกล้า พ.ศ. ๒๕๒๕
	ปริญญาโท สาขาเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้า
	เจ้าคุณทหารลาดกระบัง พ.ศ. ๒๕๕๖
	ชั้นนายร้อยเหล่าทหารปืนใหญ่ พ.ศ. ๒๕๒๕
	ชั้นนายพันเหล่าทหารปืนใหญ่ พ.ศ. ๒๕๓๐
	โรงเรียนเสนาธิการทหารบก พ.ศ. ๒๕๓๓
	วิทยาลัยเสนาธิการทหาร พ.ศ. ๒๕๔๗
	วิทยาลัยป้องกันราชอาณาจักร พ.ศ. ๒๕๕๗
ประวัติการทำงาน	ผู้บังคับกองพันทหารปืนใหญ่ที่ ๓๐ พ.ศ. ๒๕๓๘
โดยย่อ	ผู้ช่วยผู้อำนวยการกองวางแผนการฝึก สำนักงานวางแผนการฝึกร่วมและผสม กรมยุทธการทหาร พ.ศ. ๒๕๔๑
	ผู้อำนวยการกองการศึกษา สถาบันคอมพิวเตอร์ทหาร พ.ศ. ๒๕๔๘
	ผู้อำนวยการกองนโยบายและแผน กรมการสนเทศทหาร พ.ศ. ๒๕๔๘
	ผู้อำนวยการกองแผนและวิศวกรรม ศูนย์พัฒนากิจการอวกาศกลาโหม พ.ศ. ๒๕๔๙
	ผู้อำนวยการกองแผนและวิศวกรรม กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม พ.ศ. ๒๕๕๑
	ผู้อำนวยการศูนย์รักษาความปลอดภัยคอมพิวเตอร์ กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม พ.ศ. ๒๕๕๕
	รองเจ้ากรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม พ.ศ. ๒๕๕๗
ตำแหน่งปัจจุบัน	รองเจ้ากรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม

สรุปย่อ

ลักษณะวิชา ยุทธศาสตร์, การทหาร

เรื่อง ยุทธศาสตร์การป้องกันไซเบอร์กระทรวงกลาโหม

ผู้วิจัย พลตรี สุทธิศักดิ์ สลักคำ **หลักสูตร** วปอ. **รุ่นที่** ๕๗

ตำแหน่ง รองเจ้ากรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม

ความเป็นมาและความสำคัญของปัญหา

กองทัพที่ทันสมัยในปัจจุบัน ถือว่า ไซเบอร์ (Cyber) เป็นโดเมน (Domain) หรือพื้นที่ปฏิบัติการหนึ่ง เช่นเดียวกับพื้นที่ปฏิบัติการทาง บก (Land) ทะเล (Sea) อากาศ (Air) อวกาศ (Space) ไซเบอร์ (Cyberspace) ที่มีการปฏิบัติการต่าง ๆ ในไซเบอร์ตั้งแต่ภาวะปกติไปจนถึงภาวะวิกฤติและสงคราม เนื่องจากปัจจุบันการใช้สารสนเทศมีการเชื่อมต่อออนไลน์โยงใยกันอย่างกว้างขวาง มีการใช้ประโยชน์ตั้งแต่การใช้ในชีวิตประจำวัน การใช้ในการทำงาน การใช้ควบคุมอุปกรณ์ การใช้ควบคุมโรงงาน การใช้ควบคุมโครงสร้างพื้นฐาน ซึ่งเป็นปัจจัยสำคัญของเศรษฐกิจ ไปจนถึงการใช้ในระบบควบคุมบังคับบัญชาของกองทัพ ต่างพึ่งพาและใช้สารสนเทศที่มีการเชื่อมต่อออนไลน์แทบทั้งสิ้น การเชื่อมต่ออย่างกว้างขวางนี่เอง คือคุณสมบัติของไซเบอร์ ซึ่งหากได้รับอันตรายจากภัยคุกคามไซเบอร์ย่อมจะสร้างความเสียหายให้กับความมั่นคงของชาติในที่สุด ดังนั้นจึงต้องเตรียมการไว้ให้พร้อมในการรับมือกับภัยคุกคามยุคใหม่

วัตถุประสงค์ของการวิจัย

๑. เพื่อศึกษาภัยคุกคามจากไซเบอร์ที่มีผลกระทบต่อความมั่นคงของชาติ ในส่วนที่เกี่ยวข้องกับกระทรวงกลาโหมในฐานะของหน่วยงานด้านความมั่นคง

๒. เพื่อศึกษา การป้องกันไซเบอร์ การรับมือและการเตรียมการรับมือต่อภัยคุกคามจากไซเบอร์ของต่างประเทศและประเทศไทย

๓. เสนอแนะยุทธศาสตร์การป้องกันไซเบอร์กระทรวงกลาโหม

ขอบเขตของการวิจัย

การวิจัยจำกัดขอบเขตเฉพาะข้อมูลข่าวสารที่เปิดเผยทางอินเทอร์เน็ต หรือเอกสารที่เผยแพร่โดยทั่วไปของต่างประเทศและประเทศไทย มุ่งเน้นศึกษาส่วนราชการในกระทรวงกลาโหม และหน่วยงานภาครัฐ

วิธีดำเนินการวิจัย

การวิจัยนี้เป็นการวิจัยเชิงคุณภาพ โดยศึกษาและวิเคราะห์จากข้อมูลข่าวสารที่เปิดเผยทางอินเทอร์เน็ต หรือเอกสารที่เผยแพร่โดยทั่วไป นำมาเปรียบเทียบ วิเคราะห์ข้อมูล และสังเคราะห์เป็นยุทธศาสตร์

ผลการวิจัย

๑. นโยบายระดับชาติได้กล่าวถึงไซเบอร์ใน (ร่าง)นโยบายความมั่นคงแห่งชาติ พ.ศ.๒๕๕๘ – ๒๕๖๒ ได้กำหนดนโยบายการเสริมสร้างความมั่นคงทางเทคโนโลยีสารสนเทศและไซเบอร์ เน้นการปกป้อง ป้องกันภัยคุกคามด้านไซเบอร์ สงครามไซเบอร์ การบังคับใช้กฎหมาย การพัฒนากฎหมาย การพัฒนาการสืบสวนและการป้องกันอาชญากรรมไซเบอร์ พร้อมทั้งพัฒนาศักยภาพด้านไซเบอร์ และคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ได้กำหนดกรอบนโยบายการรักษาความปลอดภัยไซเบอร์แห่งชาติ เพื่อให้ "ประเทศไทยมีความมั่นคงปลอดภัยด้านไซเบอร์เป็นที่เชื่อถือและยอมรับในระดับสากล" กล่าวถึงการบูรณาการการจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศ การมีขีดความสามารถในการตอบสนองต่อภัยคุกคามทางไซเบอร์ รวมถึงการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ

๒. ภัยคุกคามไซเบอร์ในปัจจุบันทำให้เกิดความเสียหายต่อบุคคล ต่อองค์กร ต่อสังคม ต่อเศรษฐกิจ และความมั่นคงของประเทศ รูปแบบการโจมตีมีหลากหลายและพัฒนาวิธีการใหม่ ๆ อยู่ตลอดเวลา จึงต้องมีการดำเนินการป้องกันอย่างต่อเนื่อง ในต่างประเทศรวมถึงประเทศไทย ได้ตระหนักถึงอันตรายจากภัยคุกคามไซเบอร์ ได้เริ่มดำเนินการกับไซเบอร์อย่างจริงจัง มีการจัดตั้งหน่วยงาน มีการสร้างความตระหนัก และประสานความร่วมมือระหว่างประเทศมากขึ้น แต่ภัยคุกคามไซเบอร์ยังไม่หมดไป ดังนั้นจึงจำเป็นต้องดำรงความต่อเนื่องในการดำเนินการป้องกันไซเบอร์ของประเทศและกระทรวงกลาโหมต่อไป

๒.๑ ได้ศึกษาหน่วยงานไซเบอร์ของต่างประเทศในหลาย ๆ ประเทศ ได้แก่ อิสราเอล อิหร่าน อเมริกา เยอรมัน อังกฤษ สวีเดน จีน อินเดีย สิงคโปร์ มาเลเซีย พม่า เวียดนาม พบจุดร่วมที่เหมือนกันคือ มีการกำหนดนโยบาย ยุทธศาสตร์ และหน่วยงานรับผิดชอบงานด้านไซเบอร์โดยเฉพาะ มีการออกกฎหมาย ระเบียบ ที่เกี่ยวข้อง มีการพัฒนาบุคลากรและเทคโนโลยี รวมถึงมีการประสานความร่วมมือระหว่างประเทศ

๒.๒ ได้ศึกษาหน่วยงานด้านไซเบอร์ในประเทศไทยมีหน่วยงานที่เกี่ยวข้องกับกระทรวงกลาโหมดังนี้

๒.๒.๑ หน่วยงานด้านไซเบอร์ระดับชาติ ได้แก่ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ มีหน้าที่ดำเนินการให้ธุรกรรมอิเล็กทรอนิกส์มีความปลอดภัย และทำหน้าที่เป็นเลขานุการคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และมีศูนย์ประสานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย (ThaiCERT) ทำหน้าที่ตอบสนองและจัดการกับเหตุการณ์ความมั่นคงปลอดภัยคอมพิวเตอร์ รวมทั้งการประสานงานระหว่างหน่วยงานต่างประเทศที่เป็นสมาชิกขององค์กรระดับภูมิภาค

๒.๒.๒ หน่วยงานไซเบอร์ในกระทรวงกลาโหม แบ่งเป็น <u>หน่วยรับผิดชอบด้านนโยบายและยุทธศาสตร์</u> มีศูนย์รักษาความปลอดภัยคอมพิวเตอร์ กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม ทำหน้าที่นี้โดยปริยาย <u>หน่วยรับผิดชอบการปฏิบัติ</u> ได้แก่ (๑) กองรักษาความปลอดภัยสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศทหาร (๒) กรมการสื่อสารทหาร (๓) กองปฏิบัติการสงครามเครือข่าย สำนักปฏิบัติการ กรมยุทธการทหาร (๔) ศูนย์ไซเบอร์กองทัพบก (๕) กองสงครามไซเบอร์ สำนักปฏิบัติการ กรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ (๖) กองสงครามไซเบอร์ สำนักระบบบัญชาการและควบคุม กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ

๓. วิเคราะห์ประเด็นสำคัญจากการป้องกันไซเบอร์ของต่างประเทศได้จำนวน ๙ ประเด็นที่ส่วนใหญ่ดำเนินการคือ มีการจัดตั้งหน่วยใหม่หรือปรับปรุงหน่วยเดิมให้เป็นหน่วยรับผิดชอบด้านไซเบอร์โดยเฉพาะ มีการพัฒนาศักยภาพการตอบสนองภัยคุกคามจากไซเบอร์โดยกำหนดนโยบายและพัฒนาทางเทคนิค มีการประสานความร่วมมือทั้งในประเทศและต่างประเทศ มีการสร้างความตระหนัก มีการวิจัยและพัฒนาเพื่อพึ่งพาตนเอง รัฐมีอำนาจตรวจสอบเนื้อหาหรือเข้าควบคุมเหตุฉุกเฉินทางไซเบอร์ กำหนดกฎหมาย ระเบียบ และมาตรฐานด้านไซเบอร์ปกป้องโครงสร้างพื้นฐานโดยเฉพาะสาธารณูปโภค และมีการดำเนินการเชิงรุกในบางประเทศ

๔. วิเคราะห์ลักษณะภัยคุกคามจากสงครามไซเบอร์ของต่างประเทศที่ได้รับผลกระทบ ได้แก่ การโจมตีในไซเบอร์สามารถโจมตีและสร้างผลเสียหายมากในวงกว้างได้อย่างรวดเร็ว ตรวจจับได้ยาก ระบุที่ตั้งและตัวตนได้ยาก ปฏิบัติการได้จากทั่วโลก เป้าหมายของการโจมตีมีหลากหลายและจำนวนมาก จุดอ่อนฝ่ายเรามีมากไม่สามารถป้องกันได้หมด จำนวนการโจมตีไม่ใช่ปัจจัยแห่งความสำเร็จ การโจมตีใช้ทรัพยากรน้อย (ลงทุนน้อย) สามารถหาเครื่องมือได้ทั่วไปในอินเทอร์เน็ต แต่ต้องใช้ผู้เชี่ยวชาญทั้งในการโจมตีและการป้องกัน

๕. วิเคราะห์ปัญหาการป้องกันไซเบอร์ของกระทรวงกลาโหม จากการศึกษาและวิเคราะห์ภารกิจการจัดหน่วยงานไซเบอร์ในปัจจุบัน สามารถสรุปปัญหา ได้แก่ กระทรวงกลาโหมขาดนโยบายและยุทธศาสตร์ด้านไซเบอร์ที่ชัดเจนและยังไม่ได้กำหนดหลักนิยมในการปฏิบัติเกี่ยวกับไซเบอร์ ขาดการฝึกอบรมและการพัฒนาผู้นำด้านไซเบอร์ หน่วยไซเบอร์ที่จัดตั้งขึ้น ในปัจจุบันมีขีดความสามารถในการป้องกันตนเองได้ระดับหนึ่ง แต่ยังขาดขีดความสามารถเชิงรุกและการแสวงประโยชน์ (Exploit) ในกระทรวงกลาโหมมีการใช้ไซเบอร์เพิ่มขึ้น เช่น การปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Operations) แต่การป้องกันไซเบอร์ยังไม่ดีพอ ยังไม่มีการสนธิส่วนอำนวยการร่วมกันต่างคนต่างทำเพื่อปกป้องรักษาเครือข่ายของตนเองซึ่งควรเป็นเครือข่ายการทำงานร่วมกัน ขาดแคลนผู้เชี่ยวชาญเป็นปัญหาที่สำคัญมากเพราะจัดหาได้ยากแต่ละคนต้องใช้เวลาสะสมความรู้ ประสบการณ์ เอกชนให้ค่าตอบแทนมากกว่าจึงมีสมองไหล ขาดกฎการใช้กำลัง (Rule of Engagement) ของทหารและระหว่างทหารกับพลเรือน ขาดการประสานงานความร่วมมือในทุก ๆ ด้านกับหน่วยงานภายนอกกระทรวงกลาโหมและหน่วยงานของต่างประเทศอย่างต่อเนื่องและสร้างสรรค์ผลผลิต

๖. กำหนดวัตถุประสงค์และยุทธศาสตร์การป้องกันไซเบอร์กระทรวงกลาโหมคือ การดำเนินการด้านไซเบอร์ทั้งปวงต้องมีหน่วยรับผิดชอบทั้งทางด้านนโยบายและยุทธศาสตร์ และการปฏิบัติ ที่ชัดเจนมีเอกภาพ ในทิศทางเดียวกัน มีกำลังพลที่เชี่ยวชาญพร้อมปฏิบัติงาน ไซเบอร์ต้องพร้อมใช้งานตลอดเวลา เชื่อถือได้ มีการรักษาความลับ

ที่ดี หากมีการโจมตีต้องสามารถป้องกันและทำลายการโจมตีได้อย่างรวดเร็วก่อนการโจมตีจะเริ่มขึ้น สร้างเครือข่ายความร่วมมือ สร้างพลังร่วม ร่วมกันดำเนินการ ประสานกับทุกภาคส่วนทั้งในประเทศและต่างประเทศ

๗. ยุทธศาสตร์การป้องกันไซเบอร์กระทรวงกลาโหม

ยุทธศาสตร์ที่ ๑ การเสริมสร้างศักย์ภาพด้านไซเบอร์ของกระทรวงกลาโหมให้มีความพร้อมในการรับมือกับภัยคุกคาม เพื่อให้มีหน่วยงานรับผิดชอบหลักด้านไซเบอร์ของกระทรวงกลาโหมที่ครอบคลุมทั้งในระดับนโยบายและยุทธศาสตร์ และระดับปฏิบัติการ มีบุคลากรที่เพียงพอ มีเครื่องมือ เทคโนโลยี หลักนิยาม และมาตรฐานด้านไซเบอร์ของกระทรวงกลาโหม

ยุทธศาสตร์ที่ ๒ การป้องกันไซเบอร์ ให้มีความปลอดภัยพร้อมใช้งาน เชื่อถือได้ มีการรักษาความลับและไม่ให้เป็นจุดอ่อนหรือจุดล่อแหลมต่อการปฏิบัติภารกิจ เพื่อให้การปฏิบัติการทางทหารมีเสรีและเพิ่มมิติในการปฏิบัติ มีการปกป้องทรัพยากรและการปกป้องสิทธิการเข้าถึงทรัพยากรสารสนเทศ ทั้งระบบควบคุมบังคับบัญชาและระบบสารสนเทศเพื่อการบริหารราชการทั่วไป

ยุทธศาสตร์ที่ ๓ การป้องกันไซเบอร์เชิงรุก เพื่อทำการรบกวน ขัดขวาง ทำลายการโจมตีทางไซเบอร์ของผู้ไม่ประสงค์ดีก่อนที่จะเริ่มขึ้น จำกัดเสรีในการปฏิบัติของผู้ไม่ประสงค์ดี ด้วยการเฝ้าตรวจ การหาข่าวทางไซเบอร์อย่างต่อเนื่อง และเข้าปฏิบัติการทันทีเมื่อมีข้อบ่งชี้ว่าจะมีการปฏิบัติการใด ๆ ที่จะเป็นอันตรายต่อฝ่ายเรา เพื่อจำกัดเสรีการใช้ไซเบอร์ของฝ่ายตรงข้าม ในด้านยุทธการ การข่าวกรอง และการปฏิบัติการข่าวสารไซเบอร์ มีการปฏิบัติการ รบกวน ขัดขวาง ทำลายการโจมตีทางไซเบอร์ของฝ่ายตรงข้าม

ยุทธศาสตร์ที่ ๔ การผนึกกำลังด้านไซเบอร์ ในการป้องกันไซเบอร์และการป้องกันไซเบอร์เชิงรุก การมีส่วนร่วมในการบริหารจัดการการปฏิบัติการไซเบอร์ของชาติอย่างมีเอกภาพตั้งแต่ภาวะปกติจนถึงภาวะสงคราม โดยผนึกกำลังทั้งภาครัฐ ภาคเอกชน และภาคประชาชน รวมทั้งประสานความร่วมมือกับมิตรประเทศ เพื่อผนึกกำลังและความร่วมมือเพื่อการป้องกันไซเบอร์ระดับชาติทั้งภาครัฐ ภาคเอกชน ภาคประชาชน และระดับนานาชาติ

ข้อเสนอแนะ

๑. ผู้วิจัยขอเสนอยุทธศาสตร์การป้องกันไซเบอร์กระทรวงกลาโหมดังได้กล่าวไปแล้ว

๒. ปัจจัยสนับสนุนเร่งด่วนในการเพิ่มขีดความสามารถทางด้านไซเบอร์ทั้งเชิงรับและการป้องกันเชิงรุกของกระทรวงกลาโหม ได้แก่ การออกกฎหมายหรือปรับปรุงกฎหมายให้เจ้าหน้าที่ฝ่ายความมั่นคงสามารถดำเนินการทั้งเชิงรับและการป้องกันเชิงรุกได้ และสนับสนุนการจัดตั้งหน่วยงานเฉพาะด้านไซเบอร์ ด้วยการเปิดอัตราบรรจุและการบรรจุจากพลเรือน สนับสนุนงบประมาณพัฒนาบุคลากรและเครื่องมือด้านไซเบอร์

๓. แนวความคิดในการจัดตั้งศูนย์บัญชาการไซเบอร์กระทรวงกลาโหม และหน่วยปฏิบัติการไซเบอร์ของกองบัญชาการกองทัพไทยและเหล่าทัพ เพื่อให้มีหน่วยปฏิบัติงานด้านไซเบอร์ทั้งหน่วยระดับนโยบายและ

ยุทธศาสตร์ และหน่วยปฏิบัติ โดยปรับปรุงโครงสร้างการจัดหน่วยหรือแปรสภาพหน่วยงานด้านไซเบอร์ที่มีอยู่แล้ว และเพิ่มเติมอีกบางส่วน ให้งานด้านไซเบอร์มีเอกภาพ เป็นไปในทิศทางเดียวกัน

๓.๑ ศูนย์บัญชาการไซเบอร์กระทรวงกลาโหม ทำหน้าที่กำหนดนโยบายและยุทธศาสตร์ด้านไซเบอร์ของกระทรวงกลาโหม เป็นเจ้าภาพการบูรณาการการปฏิบัติการไซเบอร์ภายในกระทรวงกลาโหมและกับทุกภาคส่วนทั้งฝ่ายความมั่นคง ภาครัฐ และเอกชน กำกับดูแลการปฏิบัติการไซเบอร์ให้มีเอกภาพประสานสอนคล้องกัน

๓.๒ กำลังพล ใช้กำลังจากทหารประจำการเพื่อเป็นแกนหลักส่วนหนึ่ง กำลังส่วนที่เหลือใช้กำลังจากข้าราชการพลเรือนกลาโหม กำลังพลสำรอง และ การจ้างบริษัทภายนอก (Outsource) ที่ผ่านการรับรอง

๓.๓ การบังคับบัญชา

๓.๓.๑ ศูนย์บัญชาการไซเบอร์กระทรวงกลาโหม เป็นหน่วยขึ้นตรงรัฐมนตรีว่าการกระทรวงกลาโหมอีก ๑ หน่วย รับผิดชอบพื้นที่ปฏิบัติการไซเบอร์ (Cyberspace Domain) ในขั้นต้น ให้เป็นหน่วยฝากการบังคับบัญชาและทางธุรการไว้กับ สำนักงานปลัดกระทรวงกลาโหม ศูนย์ปฏิบัติการไซเบอร์กองบัญชาการกองทัพไทยและเหล่าทัพ แต่ละหน่วยแยกขึ้นตรงต่อกองบัญชาการกองทัพไทยและเหล่าทัพ

๓.๓.๒ การปฏิบัติการ ใช้หลักการ “ควบคุมแบบรวมการ ปฏิบัติแบบแยกการ” โดยกำหนดให้ศูนย์บัญชาการไซเบอร์กระทรวงกลาโหม รับผิดชอบทางด้านนโยบายและยุทธศาสตร์ การบูรณาการประสานงานกับหน่วยงานทุกภาคส่วนในประเทศไทยและต่างประเทศ บูรณาการการกำหนดเป้าหมาย การผนึกกำลังของการปฏิบัติการไซเบอร์ การติดตามสถานการณ์ไซเบอร์ของประเทศ (Monitor) การพัฒนาบุคลากรในภาพรวมของกระทรวงกลาโหม การพัฒนาเทคโนโลยีกระบวนการทำงานและหลักนิยม การวิจัยพัฒนาด้านไซเบอร์ รวมถึงการป้องกันเครือข่ายเทคโนโลยีสารสนเทศและการสื่อสารหลักของกระทรวงกลาโหม และของ สำนักงานปลัดกระทรวงกลาโหม

หน่วยปฏิบัติการไซเบอร์กองบัญชาการกองทัพไทยและเหล่าทัพ รับผิดชอบ การป้องกันเครือข่ายเทคโนโลยีสารสนเทศและการสื่อสารของตนเอง การปฏิบัติการไซเบอร์ในความรับผิดชอบ และปฏิบัติการตามนโยบายและยุทธศาสตร์ด้านไซเบอร์ของกระทรวงกลาโหม

๔. ข้อเสนอต่อรัฐบาล

กำหนดให้การดำเนินการด้านไซเบอร์เป็นวาระแห่งชาติที่เร่งด่วนโดยสนับสนุนทรัพยากรในการบูรณาการงานด้านไซเบอร์ของทั้งประเทศให้เป็นระบบ มีแนวทางและทิศทางไปในทางเดียวกัน มีเจ้าภาพที่ชัดเจนและเข้มแข็ง คำนึงถึงความมั่นคงของชาติในทุก ๆ ด้าน