ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์สำหรับประเทศไทย

Cyber Threats Management Strategy for Thailand

พงษ์ศักดิ์ ผกามาศ[1], ชัยวัฒน์ ประสงค์สร้าง[2],
เศรษฐชัย ชัยสนิท[3], ชูเกียรติ ช่วยเพชร[4] และ ราชิต อรุณรังษี[5]
มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์[1,2] มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี[3]
สำนักงานวิจัยและพัฒนาการทางทหารกองทัพบก[4]
กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร[5]

บทคัดย่อ

บทความนี้นำเสนอยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์สำหรับประเทศไทย โดยมีวัตถุประสงค์เพื่อ 1) ศึกษารูปแบบ วิธีการ การประเมินสถานการณ์ และปัญหาของภัยคุกคามด้านไซเบอร์ 2) ศึกษาผลกระทบของภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงแห่งชาติ และ 3) นำเสนอยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์สำหรับประเทศไทย การวิจัยนี้ใช้ระเบียบวิธีวิจัยเชิงคุณภาพโดยเน้นการศึกษาเฉพาะประเด็นที่นำไปสู่การกำหนดยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ กลุ่มเป้าหมาย ได้แก่ 1) หน่วยงานด้านความมั่นคงของรัฐ 2) ผู้บริหารระดับกระทรวงที่เกี่ยวข้อง 5 กระทรวง 3) ผู้บริหาร/ผู้นำท้องถิ่น 4) หน่วยงานภาคเอกชน 5) ภาคประชาชน 6) เจ้าหน้าที่ด้านการข่าวที่เชี่ยวชาญระบบไอซีที 7) เจ้าหน้าที่ทหารที่รับผิดชอบด้านภัยคุกคามด้านไซเบอร์ 8) ผู้ปฏิบัติงานที่เกี่ยวข้องกับระบบเครือข่ายอินเตอร์เน็ต 9) ผู้ทรงคุณวุฒิจากหน่วยงานความมั่นคงด้านไซเบอร์กองทัพไทย และ 10) ผู้เชี่ยวชาญด้านวิศวกรรมระบบไอซีทีและโลกไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ รวมกลุ่มเป้าหมายทั้งสิ้น 79 คน โดยกลุ่มเป้าหมายได้มาจากการเลือกในลักษณะจำเพาะเจาะจง เครื่องมือที่ใช้ในการวิจัย คือ แบบสัมภาษณ์แบบไม่มีโครงสร้าง การวิเคราะห์และสังเคราะห์ข้อมูลตามหลักการวิจัยเชิงคุณภาพโดยวิธีพรรณนาเชิงวิเคราะห์ การตรวจสอบข้อมูลโดยวิธีการสามเส้าด้านข้อมูล และการยืนยันร่างยุทธศาสตร์โดยการสัมมนาอิงผู้เชี่ยวชาญ

ผลการวิจัยพบว่า กระบวนการใช้โลกไซเบอร์ในการสร้างความไม่สงบสุขมีหลายวิธี เช่น การใช้เครือข่ายสังคมออนไลน์เพื่อการบ่อนทำลายความน่าเชื่อถือของเจ้าหน้าที่รัฐ การปฏิบัติการจิตวิทยา และการโฆษณาชวนเชื่อของกลุ่มผู้ไม่หวังดี การสร้างกระแสข่าวในเชิงลบและการสร้างความขัดแย้งต่อประชาชน การก่อวินาศกรรมโดยใช้เครือข่ายอินเตอร์เน็ตเป็นมัชฌิม

โดยมีแนวโน้มจะปฏิบัติการในรูปแบบอื่นๆ เพิ่มมากขึ้น นอกจากนี้ใช้ระบบการติดต่อสื่อสารผ่านแอพพลิเคชั่นเพื่อหลบเลี่ยงการตรวจจับและติดตามโดยเจ้าหน้าที่รัฐ เหล่านี้ล้วนสร้างผลกระทบโดยตรงต่อความมั่นคงแห่งชาติแทบทั้งสิ้น ยุทธศาสตร์การจัดการภัยคุกคามด้าน ไซเบอร์สำหรับประเทศไทย ประกอบด้วย 7 ยุทธศาสตร์ ได้แก่ 1) การจัดโครงสร้างพื้นฐานของประเทศไทยสำหรับใช้ในการจัดการกับภัยคุกคามด้านไซเบอร์ 2) การสร้างการตระหนักรู้โลกไซเบอร์ให้กับประชาชน 3) การพัฒนาความก้าวหน้าด้านไซเบอร์ 4) การส่งเสริมความร่วมมือด้านไซเบอร์ระหว่างภาครัฐ ภาคเอกชน และภาคประชาชน 5) การกำหนดใช้กฎหมายด้านไซเบอร์และการบังคับใช้กับประชาชน 6) การใช้การบูรณาการร่วมกันเพื่อแบ่งปันข้อมูลข่าวสาร และ 7) การรับรู้ด้านไซเบอร์เพื่อการป้องกัน การยับยั้ง และการโจมตี สำหรับประเทศไทยควรใช้ยุทธศาสตร์และมาตรการรองรับการจัดการกับภัยคุกคามในโลกไซเบอร์ให้มีประสิทธิภาพ คุณภาพ และความเข้มแข็งอย่างต่อเนื่อง เพื่อเสริมสร้างความมั่นคงปลอดภัยด้านไซเบอร์ให้กับประเทศชาติต่อไป

คำสำคัญ : ยุทธศาสตร์, ภัยคุกคามด้านไซเบอร์

Abstract

This article presents a strategy for managing cyber threats for Thailand, with the following objectives: 1) study the model of the situation assessment method in Thailand; 2) study the impact of cyber threats on national security; and 3) present a cyber threats management strategy for Thailand. This research uses qualitative research methodology by study focused on specific issues leading to the establishment of cyber threat management strategies in Thailand. Target groups include: 1) state security agencies; 2) ministries concerned 5 ministry 3) local administrators/leaders; 4) private sector organizations; 5) people in Thailand; 6) news officers threatened of cyber threats; 7) military officers threatened of cyber threats; 8) people involved in internet network; 9) experts from the cyber security department, Thai Army Headquarters; and 10) ICT and cyber security experts in the southern region Thailand. The total target groups of 79 people came from a specific selection. The research tools were unstructured interviews. Analysis and synthesis of data based on qualitative research. Analysis and synthesis of qualitative research data by means of

analytical descriptive method, Validate data using data triangulation technique and confirm the strategy by using connoisseurship approach.

The research found that in Thailand, there is a cybercrime process to create a variety of disturbances. Like using social networks to undermine the credibility of government officials. Including the psychological operations and propaganda of the poor. Creating negative news and creating conflicts with the people. Sabotage using the Internet is mediocre. There are likely to be other types of operations. In addition, the system uses communication through the application to avoid detection and tracking by government officials. These have made a direct impact on national security. Strategies for managing cyber threats for Thailand consist of 7 strategies: 1) Thailand's infrastructure for dealing with cyber threats; 2) creating cyber awareness for the people; 3) development of cyber security; 4) promotion of cyber-cooperation between the public, private and public sectors; 5) enforcement of cyber law and enforcement with the people; 6) use of mutual Integration to share information and 7) cyber awareness for prevention, inhibition and attack. For Thailand, strategies and measures to address cyber threats should be implemented to ensure consistency, quality and consistency. In order to strengthen cyber security of the country.

Keywords : Strategy, Cyber Threats.

กล่าวนำ

ปัจจุบันระบบเทคโนโลยีสารสนเทศและการสื่อสารหรือระบบไอซีที (Information and Communication Technology : ICT) มีประโยชน์ต่อการพัฒนาประเทศให้เจริญก้าวหน้า โดยเป็นเรื่องที่เกี่ยวกับวิถีความเป็นอยู่ของสังคมสมัยใหม่ ก่อให้เกิดการเปลี่ยนแปลงวิถีชีวิตรวมถึงกลายเป็นสิ่งสำคัญและจำเป็นในการปฏิบัติงานของทุกองค์กรไม่ว่าจะเป็นการดำเนินธุรกิจ อุตสาหกรรม การให้บริการโทรคมนาคม การท่องเที่ยว การทหาร และการศึกษา เป็นต้น หรือกล่าวได้ว่าโลกเข้าสู่สังคมฐานความรู้ (Knowledge-based Society) ที่มีการเชื่อมโยงข้อมูลเป็นระบบเครือข่าย โดยเฉพาะอย่างยิ่งเครือข่ายอินเตอร์เน็ตได้ถูกนำมาใช้อย่างแพร่หลายในทุกบริบทของสังคม (พงษ์ศักดิ์ ผกามาศ, 2553) อีกทั้งโครงสร้างพื้นฐานวิกฤต (Critical Infrastructure) ที่อยู่รอบตัวเรา เช่น ระบบไฟฟ้า น้ำประปา การคมนาคมขนส่ง ระบบธนาคาร และระบบสื่อสารโทรคมนาคม ล้วนมีการเชื่อมต่อกับเครือข่ายอินเตอร์เน็ตแทบทั้งสิ้น การแพร่หลายของเครือข่ายนี้

ได้เปลี่ยนวิถีการดำรงชีวิตของมนุษย์แทบทุกด้าน เช่น การใช้เว็บไซต์ การรับส่งอีเมล์ การซื้อขายสินค้าไปจนถึงการทำธุรกรรมทางอิเล็กทรอนิกส์ เช่น ระบบ Internet Banking ระบบ GFMIS ของรัฐบาล และระบบการชำระภาษี เป็นต้น แนวโน้มในอนาคตของมนุษยชาติย่อมหลีกเลี่ยงไม่ได้กับการใช้งานระบบเครือข่ายสากล (Universal Network) ที่เพิ่มมากขึ้น ตามการเปลี่ยนแปลงทั้งทางด้านวิทยาศาสตร์และเทคโนโลยี รวมถึงการเชื่อมโยงกันระหว่างประเทศในโลกยุคเศรษฐกิจดิจิทัล (Digital Economy)

พัฒนาการและการเปลี่ยนแปลงของระบบไอซีทีได้ส่งผลกระทบต่อกิจการและการดำเนินงานทางการเมือง การทหาร เศรษฐกิจ และสังคมจิตวิทยาของทุกประเทศในโลกเป็นอย่างมาก ผลจากการพัฒนาด้านวิทยาศาสตร์และเทคโนโลยีในหลายทศวรรษที่ผ่านมาทำให้เกิดการปฏิวัติสารสนเทศ (Information Revolution) ซึ่งเกี่ยวข้องกับการประมวลผลและกระจายสารสนเทศอย่างกว้างขวางจนนำมาสู่การพัฒนาในสาขาคอมพิวเตอร์และการติดต่อสื่อสารอย่างก้าวกระโดดจนก่อให้เกิดพื้นที่มิติใหม่ที่เรียกว่า “โลกไซเบอร์” (Cyberspace) ด้วยเหตุนี้ความมั่นคงแห่งชาติ (National Security) จึงได้รับผลกระทบจากการปฏิวัติและปรากฏการณ์ของโลกไซเบอร์นี้โดยตรง เห็นได้จากมีผู้กล่าวถึง “ความมั่นคงด้านไซเบอร์” (Cyber Security) ในบริบทของความมั่นคงแห่งชาติมากขึ้น อีกทั้งยังมีผู้กล่าวถึงคุณลักษณะของโลกไซเบอร์ ความล่อแหลมที่มีอยู่ภายใน ภัยคุกคามที่เป็นไปได้ด้านไซเบอร์ รวมถึงประเด็นที่เกี่ยวข้องกับการป้องกัน (Defense) การยับยั้ง (Deterrence) และการโจมตี (Attack) ในโลกไซเบอร์มากขึ้น (Raphael Satter, 2017) แม้ว่าในปัจจุบันจะยังไม่มีหลักเกณฑ์ที่แน่นอนและชัดเจนที่จะกำหนดได้ว่า “การโจมตีด้านไซเบอร์เป็นอาชญากรรม” ในขณะเดียวกันยังไม่มีกลไกทางกฎหมายระหว่างประเทศใดที่จะสามารถระบุและควบคุมความสัมพันธ์ระหว่างรัฐในโลกไซเบอร์นี้ได้ ดังนั้นนานาอารยะประเทศรวมถึงประเทศไทยยังคงต้องค้นหารูปแบบและวิธีการที่เหมาะสมในการจัดการกับภัยคุกคามนี้อย่างต่อเนื่องจนถึงปัจจุบัน ทั้งนี้เพื่อให้เกิดความมั่นคงในการใช้ประโยชน์จากระบบไอซีทีเพื่อการพัฒนาประเทศชาติอย่างแท้จริง (Wikipedia, 2018)

ด้วยเหตุนี้ ในโลกที่เต็มไปด้วยความขัดแย้งทางการเมือง หากคู่กรณีมุ่งที่จะบรรลุจุดมุ่งหมาย (Ends) ของตน โดยไม่สนใจว่าจะใช้เครื่องมือ (Means) อะไรแล้ว การทำสงครามไซเบอร์จึงเป็นเครื่องมือที่ง่ายและเหมาะสมมากที่สุด หากพวกเขาต้องการทำสงครามในกรอบของกฎหมายระหว่างประเทศที่มีอยู่ในปัจจุบัน อย่างไรก็ตาม การใช้อาวุธด้านไซเบอร์กับฝ่ายตรงข้ามย่อมสุ่มเสี่ยงต่อการถูกโจมตีกลับเช่นเดียวกัน เพราะคงไม่มีฝ่ายใดที่จะยอมให้ฝ่ายตรงข้ามเป็นฝ่ายโจมตีได้ฝ่ายเดียว แต่ละฝ่ายต่างก็สามารถโจมตีอีกฝ่ายหนึ่งได้ทุกเมื่อ โดยอาศัยบุคลากรที่มีขีดความสามารถและระบบเครือข่ายที่มีอยู่ ทั้งนี้ก็เนื่องมาจากแต่ละฝ่ายสามารถเข้าถึงเครือข่ายจากที่ใดก็ได้ในโลกนี้เพื่อการเฝ้าติดตาม การค้นหาช่องโหว่ของระบบ การโจมตีต่อระบบ การแอบฝัง

โปรแกรมจารกรรมข้อมูล (Spyware) แสวงประโยชน์จากการใช้ช่องโหว่ของโปรแกรมควบคุมเครือข่ายและการทำงานของระบบ (Botnet) รวมถึงแพร่ระบาดโปรแกรมไม่พึงประสงค์ (Malware) เพื่อสร้างความเสียหายต่อระบบอีกฝ่ายหนึ่งได้ตลอดเวลา ทำให้ป้องกันได้ยาก หรือเฝ้าระวังและติดตามฝ่ายตรงข้าม (P.W. Singer and Allan Friedman, 2014: 6-10) ฉะนั้น การกระทำที่เป็นอันตรายต่อระบบเครือข่ายเหล่านี้ ถือเป็นภัยคุกคามรูปแบบใหม่ที่เรียกว่า “ภัยคุกคามด้านไซเบอร์” (Cyber Threats) ซึ่งอาจเกิดจากการกระทำในระดับบุคคล องค์กร หรือรัฐก็ได้ ในระดับบุคคล การกระทำเช่นนี้ถือเป็นการก่ออาชญากรรมบนโลกไซเบอร์ (Cyber Crimes) ทั้งที่เกิดจากพวกมือสมัครเล่น พวกลองวิชา รวมไปถึงพวกไม่เพียงแต่หวังล้วงหรือขโมยข้อมูลเท่านั้น แต่อาจลามไปถึงการทำลายล้าง หรือสร้างความเสียหายต่อทรัพย์สินของเป้าหมาย หรือสร้างอันตรายและผลกระทบต่อชีวิตประชาชนทั่วไปด้วยก็ได้ อย่างไรก็ตาม กลุ่มที่กระทำโดยมีอุดมการณ์หรือวัตถุประสงค์ทางการเมือง อาจเรียกการกระทำเช่นนี้ได้ว่าเป็น “ภัยการก่อการร้ายทางโลกไซเบอร์” ภัยคุกคามเหล่านี้อาจมิได้กระทำโดยกลุ่มบุคคลหรือผู้ก่อการร้ายด้านไซเบอร์ตามลำพัง เพราะการกระทำของบุคคลเหล่านี้อาจมีองค์การหรือรัฐอยู่เบื้องหลังหรือให้การสนับสนุนก็ได้ ทั้งนี้เพื่อบรรลุเป้าหมายทางยุทธศาสตร์ในการสร้างความเสียหายต่อโครงสร้างพื้นฐานและส่งผลกระทบต่อความมั่นคงแห่งชาติฝ่ายตรงข้าม โดยเฉพาะในด้านผลประโยชน์ทางการเมือง เศรษฐกิจ สังคมจิตวิทยา ทรัพยากรธรรมชาติและสิ่งแวดล้อม เป็นต้น (พล.ต.ฤทธี อินทราวุธ, 2561: 1-3)

ดังนั้นภัยคุกคามด้านไซเบอร์จะยังคงเป็นภัยคุกคามต่อความมั่นคงตั้งแต่ระดับความมั่นคงแห่งชาติไปจนถึงระดับความมั่นคงของมนุษย์ โลกไซเบอร์ในอนาคตจะมีแนวโน้มขยายตัวเพิ่มขึ้นเป็นทวีคูณเพราะได้กลายเป็นสิ่งอำนวยความสะดวกต่อวิถีชีวิตมนุษย์ทุกคนและการทำงานประจำวันในองค์กรต่างๆ ทุกประเภท อย่างไรก็ตาม โลกไซเบอร์นี้ย่อมมีทั้งด้านที่เป็นคุณและด้านที่เป็นโทษ โดยขึ้นอยู่กับว่ามนุษย์จะใช้เพื่อวัตถุประสงค์ใด ด้วยเหตุนี้ การที่มนุษย์ได้ประโยชน์มหาศาลจากโลกไซเบอร์ก็นำมาซึ่งความท้าทายต่อการรับมือและป้องกันความเสียหายที่เกิดจากการใช้งานดังกล่าวด้วยเช่นกัน ผู้เชี่ยวชาญได้คำแนะนำให้ผู้ที่เกี่ยวข้องทางด้านระบบไอซีทีให้เปลี่ยนความคิดเรื่องความปลอดภัยบนโลกไซเบอร์เสียใหม่ โดยให้พึงคิดไว้เสมอว่า “ระบบที่ตนใช้งานอยู่จะต้องถูกโจมตีแน่นอน” จะต้องทำอย่างไรจึงจะสามารถหาวิธีรับมือได้อย่างรวดเร็วและเพื่อให้เกิดผลกระทบน้อยที่สุด เนื่องจากไม่มีระบบใดในโลกที่จะสมบูรณ์ปลอดภัย 100% การทำให้ตนเองคุ้นชินกับการถูกแฮ็คหรือถูกโจมตีจะช่วยให้สามารถรับมือกับภัยคุกคามบนโลกไซเบอร์ได้อย่างไม่หวั่นเกรง นอกจากนี้บนโลกไซเบอร์พบว่าการถูกดิสเครดิตหรือสูญเสียภาพลักษณ์ขององค์กรกลายเป็นความเสี่ยงที่ส่งผลกระทบอย่างรุนแรง เนื่องจากข่าวสารที่ปรากฏในโลกไซเบอร์สามารถแพร่กระจายอย่างรวดเร็ว และเมื่อสูญเสียความน่าเชื่อถือไปแล้วครั้งหนึ่ง การจะนำกลับคืนมานับว่าเป็นเรื่องยากมาก ตัวอย่างที่เห็นได้ชัดคือเรื่อง Single Gateway ที่ทางรัฐบาลเพียงแค่ต้องการศึกษาแนวทางเท่านั้น ยังไม่ได้วางแผนที่

จะทำแต่อย่างใด แต่กลายเป็นว่าผู้คนบนโลกไซเบอร์ต่างตื่นตัวกับเรื่องดังกล่าว และมองรัฐบาลในแง่ลบจนเกิดแคมเปญ F5 ต่อเนื่องไปถึงการตกเป็นเป้าหมายของกลุ่ม Anonymous ดังนั้นการพัฒนาศักยภาพของมนุษย์ให้รู้เท่าทันอันตราย คาดการณ์ถึงแนวโน้มในอนาคต และลงมือจัดการกับภัยคุกคามด้านไซเบอร์ซึ่งจะต้องอาศัยสรรพกำลังในระดับประชารัฐเพื่อการป้องกันและแก้ไขอย่างทันท่วงที โดยต้องไม่สร้างผลกระทบต่อความมั่นคงของประเทศชาติในอนาคต (ศูนย์พัฒนาหลักนิยมและยุทธศาสตร์, 2559)

ดังนั้นผู้วิจัยจึงดำเนินการวิจัยเรื่อง ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์สำหรับประเทศไทย ทั้งนี้เพื่อนำข้อมูลดังกล่าวมาใช้ในการกำหนดรูปแบบ แนวทาง กลไก และมาตรการต่างๆ รวมถึงข้อเสนอแนะเชิงนโยบายในการจัดการกับภัยคุกคามด้านไซเบอร์ โดยผลการวิจัยสามารถนำมาใช้ให้เป็นประโยชน์กับการรับมือกับภัยคุกคามด้านไซเบอร์เพื่อเสริมสร้างความมั่นคงและระงับปัญหาความไม่สงบโดยเฉพาะอย่างยิ่งในพื้นที่จังหวัดชายแดนภาคใต้อย่างเป็นรูปธรรม ทั้งนี้เพื่อให้การดำรงชีวิตของประชาชนในพื้นที่เป็นไปอย่างสันติสุขทั้งในระยะสั้นและระยะยาว อีกทั้งยังใช้เป็นกรอบยุทธศาสตร์ในการพัฒนาเสริมสร้างกำลังด้านไซเบอร์ให้เป็นระบบ มีระเบียบแบบแผน มีมาตรการเชิงรับและเชิงรุกที่มีประสิทธิภาพ คุณภาพ และยั่งยืน ผู้วิจัยจึงเห็นว่า “ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์สำหรับประเทศไทย” เป็นเรื่องสำคัญและผลการวิจัยนี้จะเป็นประโยชน์และสอดรับกับยุทธศาสตร์ชาติระยะ 20 ปี (พ.ศ. 2561-2580) ซึ่งอยู่ในประเด็นยุทธศาสตร์เฉพาะด้านความมั่นคงและความสัมพันธ์ระหว่างประเทศในการรักษาความมั่นคงและความสงบเรียบร้อยภายในประเทศ การนำพื้นที่จังหวัดชายแดนภาคใต้กลับสู่สันติสุขอย่างถาวร และการเตรียมรับมือกับภัยคุกคามรูปแบบใหม่ เช่น การก่อการร้ายและการโจมตีทางไซเบอร์ เป็นต้น โดยสามารถนำผลการวิจัยนี้ไปใช้ในการบริหารจัดการภัยคุกคามด้านไซเบอร์ให้มีประสิทธิผลต่อไป ทั้งนี้เพื่อเป็นหลักประกันด้านความมั่นคงแห่งชาติด้านไซเบอร์ของประเทศไทยในอนาคต

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษารูปแบบ วิธีการ การประเมินสถานการณ์ และปัญหาผลกระทบของภัยคุกคามด้านไซเบอร์
2. เพื่อศึกษาผลกระทบของภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงแห่งชาติ
3. เพื่อนำเสนอยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์สำหรับประเทศไทย

ขอบเขตของการวิจัย

การศึกษาวิจัยครั้งนี้เพื่อนำเสนอยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์สำหรับประเทศไทย โดยการศึกษา ค้นคว้า ทบทวน วิเคราะห์ และสังเคราะห์ตามระเบียบวิธีวิจัยเชิงคุณภาพโดยกำหนดขอบเขตการวิจัยได้ดังนี้

1. ขอบเขตด้านเนื้อหา เน้นการศึกษาเฉพาะประเด็นที่นำไปสู่การกำหนดยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์สำหรับประเทศไทย ได้แก่ แนวคิดเรื่องสงครามไซเบอร์ แนวคิดเรื่องความมั่นคงแห่งชาติ แนวคิดเรื่องผลประโยชน์แห่งชาติ ทฤษฎีการบริหารจัดการภาครัฐยุคใหม่ รูปแบบภัยคุกคามด้านไซเบอร์ที่ปรากฏทั่วโลกทั้งของไทยและต่างประเทศ สถานการณ์ด้านความมั่นคงและความไม่สงบที่มีสาเหตุมาจากภัยคุกคามด้านไซเบอร์ เอกสารทางวิชาการ เอกสารทางราชการของหน่วยงานที่เกี่ยวข้อง บทความวิชาการต่างๆ การสำรวจข้อมูลเชิงพื้นที่ เอกสารประกอบการบรรยายที่เกี่ยวข้อง แนวคิดของผู้ทรงคุณวุฒิ และเอกสารงานวิจัยที่เกี่ยวข้อง

2. ขอบเขตด้านพื้นที่ เน้นศึกษาเฉพาะพื้นที่จังหวัดชายแดนภาคใต้ประกอบด้วยพื้นที่ของจังหวัดปัตตานี จังหวัดนราธิวาส และจังหวัดยะลา รวมถึง 4 อำเภอของจังหวัดสงขลา ได้แก่ อำเภอเทพา อำเภอสะบ้าย้อย อำเภอจะนะ และอำเภอนาทวี

3. ขอบเขตด้านประชากร กลุ่มเป้าหมายประกอบด้วย 1) หน่วยงานด้านความมั่นคงของรัฐ จำนวน 12 คน (กองบัญชาการกองทัพไทย, กอ.รมน., สำนักข่าวกรองแห่งชาติ และสำนักงานตำรวจแห่งชาติ) 2) ผู้บริหารระดับกระทรวงที่เกี่ยวข้อง 5 กระทรวง จำนวน 10 คน 3) ผู้บริหาร/ผู้นำท้องถิ่น จำนวน 8 คน 4) หน่วยงานภาคเอกชน จำนวน 8 คน 5) ภาคประชาชน จำนวน 8 คน 6) เจ้าหน้าที่ด้านการข่าวที่เชี่ยวชาญระบบไอซีที จำนวน 8 คน 7) เจ้าหน้าที่ทหารที่รับผิดชอบด้านภัยคุกคามด้านไซเบอร์ จำนวน 8 คน 8) ผู้ปฏิบัติงานที่เกี่ยวข้องกับระบบเครือข่ายอินเตอร์เน็ต จำนวน 8 คน 9) ผู้ทรงคุณวุฒิจากหน่วยงานความมั่นคงด้านไซเบอร์กองทัพไทย จำนวน 4 คน และ 10) ผู้เชี่ยวชาญด้านวิศวกรรมระบบไอซีทีและโลกไซเบอร์ จำนวน 5 คน รวมกลุ่มเป้าหมายทั้งสิ้น 79 คน การเลือกกลุ่มเป้าหมายที่ให้ข้อมูลเป็นไปในลักษณะจำเพาะเจาะจง (Purposive Informant) เพื่อให้ได้ข้อมูลที่มีความแม่นตรงและสามารถวิเคราะห์ได้อย่างถูกต้องเหมาะสมกับแต่ละสถานการณ์และพื้นที่

ระเบียบวิธีวิจัย

การวิจัยนี้ใช้ระเบียบวิธีวิจัยเชิงคุณภาพ (Qualitative Research) โดยมีจุดมุ่งหมายเพื่อนำเสนอ “ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์สำหรับประเทศไทย” โดยการศึกษาค้นคว้าและรวบรวมข้อมูลที่เกี่ยวข้องกับภัยคุกคามทางด้านไซเบอร์และผลกระทบด้านต่างๆ จากนั้นนำข้อมูลดังกล่าวมากำหนดเป็นรูปแบบที่เหมาะสมของการจัดการกับภัยคุกคามด้านไซเบอร์ที่สามารถนำไปใช้ได้จริง รวมถึงร่างยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ที่สามารถป้องกันและแก้ไขเพื่อรับมือหรือยับยั้งความเสียหายที่จะเกิดขึ้นจากภัยคุกคามในอนาคตพร้อมข้อเสนอแนะเชิงนโยบาย โดยมีประเด็นการวิจัยต่อไปนี้

1. ด้านการเก็บรวบรวมข้อมูล เก็บข้อมูลเชิงลึกตามกระบวนการวิจัยเชิงคุณภาพโดยมีข้อมูลปฐมภูมิและทุติยภูมิ ดังนี้

1.1 ข้อมูลปฐมภูมิ (Primary) ดำเนินการโดยการสัมภาษณ์แบบเชิงลึก (In-depth Interview) ได้แก่ 1) หน่วยงานด้านความมั่นคงของรัฐ 2) ผู้บริหารระดับกระทรวงที่เกี่ยวข้อง 5 กระทรวง 3) ผู้บริหาร/ผู้นำท้องถิ่น 4) หน่วยงานภาคเอกชน 5) ภาคประชาชน 6) เจ้าหน้าที่ด้านการข่าวที่เชี่ยวชาญระบบไอซีที 7) เจ้าหน้าที่ทหารที่รับผิดชอบด้านภัยคุกคามด้านไซเบอร์ 8) ผู้ปฏิบัติงานที่เกี่ยวข้องกับระบบเครือข่ายอินเตอร์เน็ต 9) ผู้ทรงคุณวุฒิจากหน่วยงานความมั่นคงด้านไซเบอร์กองทัพไทย และ 10) ผู้เชี่ยวชาญด้านวิศวกรรมระบบไอซีทีและโลกไซเบอร์ ซึ่งกลุ่มเป้าหมายทั้งหมดได้มาจากการเลือกแบบเจาะจงโดยอาศัยความสะดวก (Convenience) ทั้งนี้กลุ่มผู้ให้ข้อมูลหลัก (Key Informants) จะครอบคลุมผู้มีส่วนเกี่ยวข้องทั้งโดยทางตรงและทางอ้อมทั้งหมดด้านภัยคุกคามด้านไซเบอร์และผู้ที่ปฏิบัติภารกิจด้านความมั่นคง

1.2 ข้อมูลทุติยภูมิ (Secondary) ได้จากเอกสารที่เกี่ยวข้อง อาทิ รายงานเหตุการณ์ความไม่สงบในพื้นที่ กฎหมาย ระเบียบ วารสาร บทความทางวิชาการ รายงานวิจัย และเอกสารสื่อสิ่งพิมพ์อิเล็กทรอนิกส์ทั้งในและต่างประเทศ รวมทั้งผลการสัมมนาและการทบทวนแนวทางการป้องกันและแก้ไขปัญหาภัยคุกคามด้านไซเบอร์ของหน่วยงานด้านความมั่นคงและกองทัพไทย รวมถึงฝ่ายพลเรือนในแต่ละกระทรวง

2. ด้านการวิเคราะห์และสังเคราะห์ข้อมูล ดำเนินการวิเคราะห์และสังเคราะห์ตามหลักการวิจัยเชิงคุณภาพ และตรวจสอบข้อมูลโดยใช้เทคนิควิธีการสามเส้าด้านข้อมูล (Data Triangulation Technique) ประกอบด้วย 1) ข้อมูลจากเอกสารและงานวิจัยที่เกี่ยวข้อง 2) ข้อมูลที่ได้จากกลุ่มเป้าหมาย และ 3) ข้อมูลจากระเบียบและกฎหมายที่เกี่ยวข้องกับความมั่นคงด้านไซเบอร์ รวมถึงการวิเคราะห์ SWOT เพื่อนำไปสู่การกำหนดประเด็นยุทธศาสตร์ในการจัดการกับภัยคุกคามด้านไซเบอร์อย่างเป็นระบบ

3. ด้านการนำเสนอผลการวิจัย ตรวจสอบ และยืนยัน (Confirmatory) ยุทธศาสตร์โดยการสัมมนาอิงผู้เชี่ยวชาญ (Connoisseurship) โดยอาศัยความรู้ ความเชี่ยวชาญ และประสบการณ์ของผู้วิจัย ร่วมกับความเห็นของผู้ทรงคุณวุฒิด้านวิศวกรรมระบบไอซีทีและโลกไซเบอร์ที่มีประสิทธิภาพ เพื่อแสดงความคิดเห็นและให้ข้อเสนอแนะ จากนั้นนำผลการตรวจสอบไปปรับปรุงกรอบยุทธศาสตร์ที่สมบูรณ์และนำเสนอแนวทางการปฏิบัติ แผนงาน โครงสร้างพื้นฐาน และมาตรการที่เกี่ยวข้องรวมถึงข้อเสนอแนะเชิงนโยบาย

4. สรุปและเขียนรายงานการวิจัยฉบับสมบูรณ์

ประโยชน์ที่ได้รับจากการวิจัย

1. ทำให้ทราบรูปแบบ วิธีการ การประเมินสถานการณ์ และปัญหาผลกระทบที่เกิดจากภัยคุกคามด้านไซเบอร์

2. ทำให้ทราบผลกระทบของภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงแห่งชาติรวมถึงแนวโน้มในอนาคต

3. ทำให้ได้ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์สำหรับประเทศไทยพร้อมข้อเสนอแนะเชิงนโยบายที่สามารถใช้ในการป้องกันและแก้ไขปัญหาภัยคุกคามด้านไซเบอร์อย่างเป็นรูปธรรม

ผลการวิจัยและการวิเคราะห์ข้อมูล

ผลการศึกษาพบว่ารูปแบบภัยคุกคามด้านไซเบอร์ที่เกิดขึ้นในประเทศไทยปรากฏผลดังประเด็นต่อไปนี้

1. รูปแบบของภัยคุกคามด้านไซเบอร์ในประเทศไทย

1.1 รูปแบบของภัยคุกคามด้านไซเบอร์ที่พบในประเทศไทยในความคิดเห็นของหน่วยงานด้านความมั่นคงของรัฐ ผู้บริหารระดับกระทรวงที่เกี่ยวข้อง 5 กระทรวง และผู้บริหาร/ผู้นำท้องถิ่นสามารถสรุปได้ว่ามีรูปแบบที่ปรากฏดังนี้

1.1.1 รูปแบบของการสร้างข้อมูล การสร้างข้อมูลเป็นรูปแบบปกติของการนำเสนอข้อมูลข่าวสารในยุคปัจจุบัน จะสังเกตได้ว่ามีการนำระบบไซเบอร์และเครือข่ายสังคมออนไลน์มาใช้สร้างและเผยแพร่ข้อมูลข่าวสารมากขึ้นเรื่อยๆ โดยอาจจะมากกว่าการใช้กำลัง ทั้งมีการแฮกหรือการเจาะข้อมูลของส่วนงานราชการและหน่วยงานทางความมั่นคง (กอ.รมน.) เมื่อบุกรุกได้จะมีการเปลี่ยนหน้าตาโฮมเพจและอ้างว่าสามารถที่จะเจาะข้อมูลของหน่วยงานราชการได้สำเร็จและแจ้ง

ให้กับแนวร่วมว่าได้ทำตามเป้าหมายเรียบร้อยผ่านทางเครือข่ายออนไลน์วิธีใดวิธีหนึ่ง เป็นต้น (นงรัตน์ สายเพชร, 2556: 18) จากการวิเคราะห์ของผู้รับผิดชอบด้านความมั่นคงพบว่าอาจเป็นการเชื่อมโยงกับการเมืองหรือการก่อกวนให้เกิดความหวาดระแวงระหว่างเจ้าหน้าที่รัฐและประชาชนนั่นเอง

1.1.2 รูปแบบของการบิดเบือนข้อมูล มีการตรวจพบโฆษณาชวนเชื่อและมีการโจมตีในประเด็นการเผยแพร่ข่าวสารโดยมีการนำสื่อสังคมออนไลน์ เช่น เฟสบุ๊ก ไลน์ ทวิตเตอร์ และบล๊อกอื่นๆ มาใช้ในการหาแนวร่วมซึ่งมีการขยายช่องทางการสื่อสารตลอดเวลา โดยเมื่อทาง การตรวจสอบได้จะมีการเปลี่ยนรูปแบบของสื่อออนไลน์ไปได้ใช้ช่องทางอื่นไม่มีที่สิ้นสุด มีการใช้จิตวิทยาโดยเน้นการสร้างความเข้าใจผิดๆ ให้ประชาชนเข้าใจผิดหรือเกิดความรู้สึกขัดแย้งกับการทำงานของรัฐบาลตลอดจนหน่วยงานทางความมั่นคงอื่นๆ เช่น หากเจ้าหน้าที่จับผู้ต้องสงสัยในพฤติกรรมบางกลุ่มจะมีการเผยแพร่ข้อมูลผ่านทางช่องทางต่างๆ ว่าจับผิดตัว มีการกล่าวหาใส่ร้ายป้ายสีรวมถึงการสร้างความขัดแย้งกันระหว่างกลุ่มประชาสังคม ตลอดจนการนำประเด็นทางการเมืองมาเชื่อมโยงและขยายผลให้ไปสู่การสร้างสถานการณ์แห่งความรุนแรงดังเหตุการณ์ที่เกิดขึ้นในหลายๆ ครั้งในพื้นที่จังหวัดชายแดนภาคใต้

1.1.3 รูปแบบของการชักชวน รูปแบบนี้จะปรากฏให้เห็นผ่านสื่อสังคมออนไลน์ประเภทต่างๆ โดยเฉพาะอย่างยิ่งกลุ่มของไอเอส (IS) ที่มีการเผยแพร่แนวคิดและความรุนแรงโดยการหาแนวร่วมเพื่อเชิญชวนให้ไปร่วมรบในประเทศซีเรียหรือบริเวณต่างๆ ที่เกิดความรุนแรงบนโลก โดยมีการตรวจพบจากเจ้าหน้าที่ด้านความมั่นคงว่าการชักชวนและโจมตีในประเด็นการเผยแพร่ข่าวสารเกี่ยวกับประเด็นการชักชวนนี้เสมอมาตั้งแต่อดีตจนถึงปัจจุบัน

ปัจจุบันจะเห็นว่ากลุ่มผู้บริโภคข้อมูลข่าวสารโดยใช้ระบบอินเตอร์เน็ตและเครือข่ายสังคมออนไลน์มีด้วยกันทั้งสิ้น 6 กลุ่ม ได้แก่ กลุ่มขบวนการก่อการร้าย กลุ่มภาคประชาสังคม กลุ่มสื่อสารมวลชน กลุ่มสื่อทางเลือก กลุ่มสื่อสารสังคมออนไลน์ และกลุ่มภาคประชาชน จากการติดตามพฤติกรรมการใช้งานสื่อสังคมออนไลน์ เช่น เฟสบุ๊ก ทวิตเตอร์ และไลน์ ของทุกกลุ่มพบว่ามีการสร้างข้อมูลและบิดเบือนข้อมูลอยู่ตลอดเวลา เมื่อเจ้าหน้าที่ฝ่ายความมั่นคงตรวจพบมากขึ้นจะมีการปรับมาใช้ Telegram Messenger แทนในบางโอกาส รวมถึงมีการขยายผลหากมีการจับได้โดยการใช้การติดตามย้อนหลังจากอุปกรณ์ที่ยึดมาได้เพื่อนำไปสู่การจับกุมขบวนการก่อการร้ายต่อไป

1.2 รูปแบบของภัยคุกคามด้านไซเบอร์ที่พบในประเทศไทยในความคิดเห็นของเจ้าหน้าที่ระดับปฏิบัติการด้านความมั่นคงรวมถึงเจ้าหน้าที่ทหารที่รับผิดชอบด้านภัยคุกคามของสำนักปฏิบัติการข่าวสาร สามารถสรุปได้ว่ามีรูปแบบที่ปรากฏดังนี้

1.2.2 ลักษณะการโจมตีเน้นการโจมตีโดยมีรูปแบบเป็นกลุ่มขบวนการก่อการร้ายที่หวังผลทำให้เกิดความเสียหายต่อหน่วยงานของภาครัฐ ปฏิบัติการด้วยการสร้างระบบข้อมูลข่าวสารอันเป็นเท็จและขยายผลผ่านเครือข่ายสังคมออนไลน์รูปแบบต่างๆ

1.2.2 ช่วงปี พ.ศ. 2550-2561 ได้มีบุคคลภายนอกเข้ามาเจาะข้อมูลโดยพยายามเข้ามาผ่านระบบไฟล์วอล (File Wall) แต่ทางเจ้าหน้าที่ของรัฐยังไม่ทราบว่าได้นำข้อมูลใดออกไปได้มากน้อยเพียงใด หลังจากนั้นได้มีการสร้างระบบการป้องกันมากยิ่งขึ้น ดังนั้นจึงกล่าวได้ว่าเป็นรูปแบบที่ใช้บุคคลภายนอกผู้เชี่ยวชาญด้านระบบไอซีทีเป็นคนดำเนินการ

1.2.3 รูปแบบสายลับจากภายนอกเข้ามาขโมยข้อมูลโดยเข้ามารับราชการหรือบรรจุเข้าปฏิบัติราชการและอาจเข้ากลุ่มเครือข่ายสังคมออนไลน์ของเจ้าหน้าที่รัฐเพื่อนำข้อมูลภายในออกไปสู่กลุ่มเป้าหมายหรือขบวนการก่อการร้าน จากการตรวจสอบของเจ้าหน้าที่ว่าทราบเรื่องเนื่องจากเคยเกิดเหตุการณ์ปะทะกันและเข้าตรวจค้นพื้นที่จึงพบฮาร์ดดิสก์เป็นข้อมูลภายใน 351 ที่สามารถหลุดออกไปได้

1.2.4 รูปแบบจากบุคคลภายในองค์กรนำข้อมูลข่าวสารออกไปโดยทั้งตั้งใจและความรู้เท่าไม่ถึงการณ์หรือคนภายในออกไปเผยแพร่ข้อมูลเองในเครือข่ายสังคมออนไลน์โดยมิได้คำนึงถึงผลกระทบที่จะตามมาในอนาคต

1.3 รูปแบบของภัยคุกคามด้านไซเบอร์ที่พบในประเทศไทยในความคิดเห็นของนักวิชาการและผู้เชี่ยวชาญด้านระบบไอซีทีซึ่งเป็นเจ้าหน้าที่ด้านความมั่นคง สามารถสรุปได้ว่ามีรูปแบบที่ปรากฏดังนี้

1.3.1 รูปแบบของภัยคุกคามส่วนมากเป็นการใช้สื่อในการกระจายข่าว การสร้างเพจเพื่อบิดเบือนข่าวสารข้อมูล ปลุกปั่นและสร้างกระแสทั้งทางที่ดีและไม่ดี การสร้างเครือข่ายสังคมเฉพาะกลุ่ม และการนำแนวคิดกระจายลงสู่พื้นที่ให้ประชาชนในพื้นที่มากที่สุดโดยผ่านสื่อต่างๆ รวมถึงเครือข่ายสังคมออนไลน์

1.3.2 รูปแบบของภัยคุกคามที่ปรากฏมี 3 รูปแบบ คือ 1) การสร้างข่าวขึ้นใหม่รายวัน 2) ข่าวจริงแต่บิดเบือนข่าวปัจจุบัน และ 3) นำข่าวเก่ามานำเสนอซ้ำ เพื่อนำเสนอข่าวออกไปในทางลบโดยผ่านสื่อต่างๆ รวมถึงเครือข่ายสังคมออนไลน์ การสร้างความขัดแย้งระหว่างกลุ่มการเมืองและผลประโยชน์ และการสร้างความเกลียดชังให้ประชาชนไม่ไว้วางใจเจ้าหน้าที่ของรัฐ

1.3.3 รูปแบบการเข้าเจาะข้อมูลโดยเป็นการดึงข้อมูลออกไป หลังจากนั้นมีการเปลี่ยนภาพในโฮมเพจหรือในเว็บไซต์ให้เป็นภาพการ์ตูน บางครั้งจัดว่าเป็นการโจมตีแต่ไม่พบเป็นการจารกรรมข้อมูลโดยตรง แต่เป็นการเข้ามาตรวจสอบดูการเคลื่อนไหวของหน่วยงานของรัฐเท่านั้น จากข้อมูลเชิงลึกของสำนักข่าวกรองแห่งชาติพบว่ามีการจารกรรมข้อมูลออกไปครั้งหนึ่งปี

พ.ศ. 2558 โดยเว็บไซต์ของสำนักข่าวกรองที่ใช้ในการรายงานข่าวไม่สามารถตรวจสอบได้ว่ามีการนำข้อมูลออกไปได้มากน้อยเพียงใด

1.3.4 รูปแบบเฉพาะกิจ เช่น การพยายามจารกรรมและเจาะเข้าระบบฐานข้อมูลขบวนการก่อการร้าย ซึ่งระบบดังกล่าวจะเป็นการเก็บข้อมูลรายงานข่าวการเคลื่อนไหวของขบวนการ โดยเปรียบเหมือนการลองของโดยไม่ได้เน้นโจมตี อีกทั้งมีการใช้สายลับโดยให้บุคคลมาสมัครรับราชการในหน่วยงานด้านความมั่นคงและเมื่อเข้ามาได้จะหาวิธีการรายงานข้อมูลให้ขบวนการได้ทราบความเคลื่อนไหวและมีการนำข้อมูลออกไปสู่ภายนอก

1.4 รูปแบบของภัยคุกคามด้านไซเบอร์ที่พบในประเทศไทยในความคิดเห็นของหน่วยงานภาคเอกชนและภาคประชาชน สามารถสรุปได้ว่ามีรูปแบบที่ปรากฏดังนี้

1.4.1 การเผยแพร่หรือแชร์ข้อมูลข่าวสารในลักษณะการบิดเบือนทางสื่อสังคมออนไลน์ชนิดต่างๆ โดยไม่รู้ที่มาและแชร์กันไปทั่ว ซึ่งทำให้เกิดการแชร์ต่อโดยไม่มีคัดกรองและข้อมูลข่าวสารเหล่านั้นย่อมแพร่กระจายได้อย่างรวดเร็ว

1.4.2 หากมีการได้รับข่าวสารใดๆ จะมีการแจ้งต่อกันในหมู่เพื่อน แต่จะมีการวิเคราะห์ดูความเป็นมาและพิจารณาก่อนเพื่อการป้องกันข่าวลวง และมักจะมีคำกล่าวที่ว่า “เหตุการณ์ที่จริงมักจะไม่ค่อยมีการแชร์กัน”

1.4.3 การเผยแพร่ข้อมูลข่าวสารบางอย่าง ถ้ารู้จักกันเป็นการส่วนตัวมักจะมีการเตือนกันว่าให้พิจารณาข้อมูลก่อนเผยแพร่ เพราะอาจเป็นการโฆษณาชวนเชื่อหรือการสร้างข่าวเท็จในน่าเชื่อถือก็เป็นได้

1.4.4 หน่วยงานภาคเอกชนและภาคประชาชน ยังไม่เคยเห็นมาตรการทางกฎหมายว่าสามารถดำเนินการกับผู้บิดเบือนข่าวสารผ่านสื่อสังคมออนไลน์ได้อย่างไร ระดับการใช้งานที่เหมาะสมเป็นอย่างไร อะไรคือข้อพิจารณาในการเผยแพร่ข้อมูลข่าวสารที่ถูกต้องในการดำรงชีวิตของประชาชน

2. วิธีการของภัยคุกคามด้านไซเบอร์ในประเทศไทย

2.1 วิธีการของภัยคุกคามด้านไซเบอร์ที่พบในประเทศไทยในความคิดเห็นของหน่วยงานด้านความมั่นคงของรัฐ ผู้บริหารระดับกระทรวงที่เกี่ยวข้อง 5 กระทรวง และผู้บริหาร/ผู้นำท้องถิ่นสามารถสรุปได้ว่ามีวิธีการที่ปรากฏดังนี้

2.1.1 วิธีการโจมตียังไม่ปรากฏเด่นชัดเนื่องจากยังไม่มีหน่วยงานใดออกมายืนยันว่าภัยคุกคามนี้มีขั้นตอนกระบวนการทางวิชาการอย่างไร ปรากฏเพียงแค่การสร้างข่าวสาร การแพร่กระจาย และการโต้ตอบกันผ่านสื่อสังคมออนไลน์รูปแบบต่างๆ

2.1.2 เจ้าหน้าที่ใช้สมาร์ตโฟนและแอพพลิเคชั่นต่างๆ อย่างแพร่หลาย มีความรู้เท่าไม่ถึงการณ์ของเจ้าหน้าที่บางคนซึ่งมีการนำเอกสารชั้นความลับไปเผยแพร่บนเว็บไซต์ โดยอาจเป็นละเมิดการรักษาความปลอดภัยข้อมูลทางราชการและรวมถึงสิทธิส่วนบุคคล ทำให้บุคคลที่ไม่มีหน้าที่ได้รับทราบข่าวสารนั้นไปด้วย (ปริญญา หอมเอนก, 2560: 1-3) เหตุการณ์นี้อาจเป็นการคาดไม่ถึงหรือมองไม่รอบด้านของฝ่ายความมั่นคงซึ่งโดยปกติแต่ละหน่วยมีมาตรการทั้งระดับบุคคลและระดับหน่วยที่กำกับดูแลการให้ข้อมูลข่าวสารอยู่แล้ว

2.2 วิธีการของภัยคุกคามด้านไซเบอร์ที่พบในประเทศไทยใต้ในความคิดเห็นของเจ้าหน้าที่ระดับปฏิบัติการด้านความมั่นคงรวมถึงเจ้าหน้าที่ทหารที่รับผิดชอบด้านภัยคุกคามของสำนักปฏิบัติการข่าวสาร สามารถสรุปได้ว่ามีวิธีการที่ปรากฏดังนี้

2.2.1 การเจาะข้อมูลยังไม่พบแต่พบการแฝงตัวว่าเป็นเจ้าหน้าที่รัฐแล้วเข้ากลุ่มไลน์และเฟสบุ๊คที่ประกอบด้วยชาวบ้านและเจ้าหน้าที่รัฐหรือเข้ามาดำเนินการขโมยข้อมูล โดยติดตามว่าใครเป็นเจ้าหน้าที่บ้าง เมื่อเจ้าหน้าที่พิสูจน์ทราบมีการรายงานไปยังไลน์และเฟสบุ๊คเพื่อให้สลายกลุ่มหรือปิด

2.2.2 มีการนำข้อมูลสารสนเทศทั้งในส่วนราชการและภาคเอกชนไปใช้ในการใส่ร้ายป้ายสี การยั่วยุปลุกปั่น และสร้างความขัดแย้งทางศาสนา โดยการเผยแพร่และสร้างภาพให้เจ้าหน้าที่รัฐเกิดความเสียหายและกระทำผิดต่อประชาชน

2.2.3 ปัจจุบันยังไม่มีการเชื่อมโยงกับศูนย์ไซเบอร์ทั้งในระดับชุมชนและระดับหน่วยงานโดยเฉพาะอย่างยิ่งหน่วยงานด้านความมั่นคง โดยยังไม่มีเจ้าภาพรับผิดชอบหรือไม่มีตัวกลางด้านไซเบอร์และด้านศูนย์ดำเนินการข้อมูล (Information Operation : IO)

2.2.4 ผู้ประกอบวิชาชีพอาจารย์และประชาชนหลากหลายสาขาอาชีพได้นำข้อมูลข่าวสารไปบิดเบือนหลายๆ ครั้ง โดยเจ้าหน้าที่มีการประชุมติดตามและมีการตรวจสอบติดตามผ่านทางสื่อสังคมออนไลน์เช่นกัน อีกทั้งผู้ประสานงานสายข่าวได้มีการสร้างบัญชีปลอมขึ้นเพื่อการตรวจหาข่าวโดยมีสถานะอำพลางตัวตนเพื่อให้เข้าถึงแหล่งข่าว และในที่สุดจะนำไปสู่การค้นหาแหล่งที่มาของขบวนการก่อการร้ายต่อไป

2.2.5 มีการส่งข่าวสารมีลักษณะบิดเบือนโดยผ่านทางอีเมล์ในลักษณะลูกโซ่ นั่นคือเมื่อผู้ใดได้รับข้อมูลข่าวสารแล้วก็จะดำเนินการส่งต่อให้ผู้เป็นสมาชิกและไม่เป็นสมาชิกของกลุ่มก่อการร้ายในทันทีโดยไม่ได้ปรึกษาหารือกับหน่วยงานราชการก่อนว่าข้อมูลข่าวสารนี้มีที่มาที่ไปอย่างไร น่าเชื่อถือหรือไม่ และมีเป้าประสงค์ใด

2.2.6 หากมีสื่อสังคมออนไลน์ที่บิดเบือนจาก YouTube จะมีการสรุปหาการเชื่อมโยงและรายงานไปยังหน่วยงานระดับสูงกว่าเพื่อดำเนินการต่อไป โดยในส่วนการสั่งปิดจะต้องส่งไปยัง

กระทรวงไอซีที แต่ถ้าเป็นเฟสบุ๊คจะเฝ้าระวังโดยการแฝงตัวแทนเพื่อการติดตามข้อมูลและพฤติกรรมอย่างใกล้ชิดและรายงานผลให้ผู้บังคับบัญชาทราบตามลำดับต่อไป

2.3 วิธีการของภัยคุกคามด้านไซเบอร์ที่พบในประเทศไทยในความคิดเห็นของนักวิชาการและผู้เชี่ยวชาญด้านระบบไอซีทีซึ่งเป็นเจ้าหน้าที่ด้านความมั่นคง สามารถสรุปได้ว่ามีวิธีการที่ปรากฏดังนี้

2.3.1 ภัยคุกคามทางออนไลน์นับว่ามีความรุนแรงและเพิ่มขึ้น เนื่องจากเยาวชนไม่รู้เท่าทันสื่อและข้อมูลข่าวสาร ทำให้เป็นช่องทางในการชักชวนเข้าสู่ส่วนหนึ่งของกระบวนการก่อการร้ายได้

2.3.2 การแจ้งข่าวสารหรือการโต้ตอบข่าวสารของทางภาครัฐค่อนข้างล่าช้าทำให้ไม่ทันการณ์หรือเป็นสถานะผู้ตามอยู่เสมอ

2.3.4 การใช้สื่อสังคมออนไลน์ในการบิดเบือนข่าวสาร โดยมีทั้งข่าวที่เป็นความจริงและความจริงที่บิดเบือนเพื่อประโยชน์บางอย่าง เนื่องจากสื่อสังคมออนไลน์ไม่มีการควบคุมหรือควบคุมยาก วิธีการแก้ไขจากทางการคือทางการจะต้องใช้ความจริงที่จริงกว่า

2.3.5 เดิมสื่อถูกควบคุมโดยภาครัฐ แต่ปัจจุบันการเผยแพร่ข้อมูลเปลี่ยนไปโดยเทคโนโลยีและไม่มีการควบคุมกลั่นกรอง ทำให้การบิดเบือนและการกระจายข้อมูลข่าวสารไปในวงกว้างและง่ายขึ้นรวมถึงการควบคุมทำได้ยากอีกด้วย

2.4 วิธีการของภัยคุกคามด้านไซเบอร์ที่พบในประเทศไทยในความคิดเห็นของหน่วยงานภาคเอกชนและภาคประชาชน สามารถสรุปได้ว่ามีวิธีการที่ปรากฏดังนี้

2.4.1 การใช้เทคโนโลยีในการก่อการร้ายมีมากยิ่งขึ้น เช่นแต่เดิมใช้การกดระเบิดแต่ปัจจุบันใช้สมาร์ตโฟน และในอนาคตอาจเกิดการใช้เทคโนโลยีอื่นๆ มาร่วมด้วยมากขึ้น ส่งผลให้สถานการณ์อันตรายมากขึ้นเนื่องจากการก่อเหตุมีความแม่นยำมากยิ่งขึ้น

2.4.2 สมาชิก NGO หลายคนไม่สนับสนุนการทำงานของภาครัฐและนำข้อมูลข่าวสารไปบิดเบือนจนสร้างความเสียหายให้กับประเทศชาติ ควรนำพระราชบัญญัติคอมพิวเตอร์ฯ มาใช้อย่างจริงจังซึ่งความเสียหายกับประเทศชาติอาจจะลดลง

3. การประเมินสถานการณ์ภัยคุกคามด้านไซเบอร์ในประเทศไทย

3.1 การประเมินสถานการณ์ภัยคุกคามด้านไซเบอร์ในประเทศไทยในความคิดเห็นของหน่วยงานด้านความมั่นคงของรัฐ ผู้บริหารระดับกระทรวงที่เกี่ยวข้อง 5 กระทรวง และผู้บริหาร/ผู้นำท้องถิ่น สามารถสรุปได้ว่ามีกระบวนการประเมินที่ปรากฏดังนี้

3.1.1 การตรวจจับและการติดตามผู้โพสต์ข้อความและข้อมูลข่าวสาร วิเคราะห์ รวบรวม บันทึกจับกุมจากทีมข่าวเปิด และรายงานผลซึ่งมีการเปลี่ยนรูปแบบเสมอถ้ามีการจับได้

แต่ทางการมีการนำอุปกรณ์มาใช้ในการตรวจจับมากขึ้นโดยเฉพาะฮาร์ดแวร์พิเศษ โดยยังไม่มีการใช้ Sniffer แต่มีการตรวจสอบจากเครื่องมือสื่อสารที่ยึดได้และมีการสร้างการวิเคราะห์เชื่อมโยง (Link Analyze)

3.1.2 การประเมินสถานการณ์ยังไม่มีรูปแบบแน่นอนตายตัว เนื่องจากส่วนงานที่รับผิดชอบด้านไซเบอร์ระดับประเทศยังมีลักษณะไม่เป็นรูปธรรม หน่วยงานที่รับผิดชอบในพื้นที่ก็พยายามเรียนรู้และพัฒนาขีดความสามารถของการตรวจจับเพิ่มขึ้นเรื่อยๆ มีการประชุมร่วมกันแบ่งปันข้อมูลข่าวสารระหว่างหน่วยงานต่างๆ ของจังหวัดชายแดนภาคใต้อยู่เสมอ หากไม่มีมาตรการที่เหมาะสมควรดำเนินการเชิงรับต่อไป

3.2 การประเมินสถานการณ์ภัยคุกคามด้านไซเบอร์ที่พบในประเทศไทยในความคิดเห็นของเจ้าหน้าที่ระดับปฏิบัติการด้านความมั่นคงรวมถึงเจ้าหน้าที่ทหารที่รับผิดชอบด้านภัยคุกคามของสำนักปฏิบัติการข่าวสาร สามารถสรุปได้ว่ามีกระบวนการประเมินที่ปรากฏดังนี้

3.2.1 เจ้าหน้าที่ประเมินว่าทีมข่าวเปิดเปรียบเสมือนการลาดตระเวนทางไซเบอร์ ดังนั้นจะต้องดำเนินการด้วยมาตรการเชิงรุกอย่างต่อเนื่องเพื่อให้รู้เท่าทันขบวนการก่อการร้ายที่มาอย่างไร้รูปแบบ ประกอบกับการสนับสนุนจากหน่วยงานภาครัฐอย่างเป็นระบบจะช่วยให้การทำงานมีประสิทธิภาพมากขึ้น

3.2.2 การคุกคามและการสร้างความเสียหายมีมากขึ้นเรื่อยๆ จากการใช้งานไซเบอร์รูปแบบต่างๆ เจ้าหน้าที่ต้องตระหนักว่าสื่อสังคมออนไลน์ต่างๆ ล้วนไม่มีความปลอดภัย ดังนั้นต้องมีกระบวนการสร้างความตระหนักด้านความปลอดภัยไซเบอร์ให้มากขึ้นโดยการสร้างความรับรู้ด้านต่างๆ ที่เกี่ยวข้องทุกมิติ การมีส่วนร่วมในการจัดการ และการใช้มาตรการทางกฎหมายหากมีการตรวจพบ

3.2.3 ปัจจุบันฝ่ายทหารและหน่วยงานด้านความมั่นคงอื่นก็มีการใช้งานสื่อสังคมออนไลน์ เช่น เฟสบุ๊ก ไลน์ ทวิตเตอร์ และบล็อกเกอร์ ในการทำลายฝ่ายตรงข้ามเช่นกัน เรียกได้ว่าเป็นการใช้ข้อมูลข่าวสารเพื่อประโยชน์ในงานด้านการข่าวและการตรวจจับหรือเฝ้าระวังผู้บุกรุกผ่านระบบไอซีที ดังนั้นจึงควรมีเครื่องมือจับ IP address ของเครื่องที่บิดเบือนข่าวสารจะก่อให้เกิดความสะดวกในการทำงานมากขึ้น

3.2.4 เนื่องจากในฝ่ายทหารและตำรวจรวมถึงหน่วยงานที่เกี่ยวข้องด้านความมั่นคงยังไม่มีศูนย์ทางไซเบอร์ที่ทันสมัย โดยเฉพาะอย่างยิ่งในสามจังหวัดชายแดนภาคใต้มีความต้องการใช้มาก เนื่องจากมีการนำสื่อสังคมออนไลน์มาบิดเบือนเป็นประจำ ควรมีการนำคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) มาช่วยและบูรณาการในเรื่องการตัดสินใจอย่างเป็นรูปธรรม

3.2.5 ประเทศไทยยังไม่มีกฎหมายควบคุมอุปกรณ์อิเล็กทรอนิกส์ โดยเฉพาะเจ้าหน้าที่นโยบายความปลอดภัยทางกายภาพ ไม่มีกฎหมายการจัดการส่งข้อมูลผ่านสื่ออิเล็กทรอนิกส์ซึ่งยังไม่มีการเข้ารหัส ดังนั้นสื่อสังคมออนไลน์สามารถทำให้เข้าถึงประชาชนเป้าหมายได้มากขึ้นและสามารถนำสื่อกลับมาใช้ใหม่ได้ ทำให้เกิดการกระจายข่าวสารที่ผิดพลาดได้อย่างต่อเนื่องซึ่งไม่ส่งผลดีต่อการสร้างความสงบสุขให้กับประชาชน

3.3 การประเมินสถานการณ์ภัยคุกคามด้านไซเบอร์ที่พบในประเทศไทยในความคิดเห็นของนักวิชาการและผู้เชี่ยวชาญด้านระบบไอซีทีซึ่งเป็นเจ้าหน้าที่ด้านความมั่นคง สามารถสรุปได้ว่ามีกระบวนการประเมินที่ปรากฏดังนี้

3.3.1 ในพื้นที่จังหวัดชายแดนภาคใต้ รูปแบบของสถานการณ์ที่เกิดขึ้นพบว่าชาวบ้านจะเชื่อผู้นำทางศาสนามากกว่าฝ่ายปกครอง ดังนั้นจึงปรากฏภาพที่ไม่เหมาะสมและมีโอกาสกระจายผ่านออนไลน์ได้ง่ายและเร็ว เนื่องจากหากเกิดเหตุแล้วประชาชนหรือมูลนิธิอาจไปถึงก่อนทำให้ภาพแห่งความรุนแรงหลุดไปก่อน

3.3.2 หน่วยงานมีการติดตามข้อมูลข่าวสารทางสื่อสังคมออนไลน์และมีการประชุมกลั่นกรองเพื่อส่งต่อไปกระทรวงไอซีทีเพื่อปิดเว็บไซต์ และขั้นต่อไปจะต้องส่งฟ้องศาล แต่หากเป็นเว็บไซต์ต่างประเทศต้องติดต่อผ่านกระทรวงต่างประเทศ

3.3.3 มีทีมทำ IO ที่จัดตั้งมาสำหรับการตอบโต้ข่าวบิดเบือนผ่านสื่อสังคมออนไลน์ดังเช่นเหตุการณ์จับคนขับรถโรงเรียน ข่าวออกไปว่าตำรวจไปล้อมจับรถตู้ นักเรียนที่อยู่ในรถได้รับความเดือนร้อน ร้องไห้ตกใจ และทำเกินกว่าเหตุ แต่ในความเป็นจริงคนขับมีหมายจับและขับมาเจอด่านจึงมีการเชิญตัวไปและรับส่งนักเรียนอย่างเรียบร้อยโดยไม่มีการกระทำเกินกว่าเหตุ ผลที่ปรากฏทำให้ภาพลักษณ์ของเจ้าหน้าที่รัฐเสียหายมากในสานตาประชาชนและยังสามารถเป็นชนวนให้เกิดความขัดแย้งได้เพิ่มขึ้นอีก

3.4 การประเมินสถานการณ์ภัยคุกคามด้านไซเบอร์ที่พบในประเทศไทยในความคิดเห็นของหน่วยงานภาคเอกชนและภาคประชาชน สามารถสรุปได้ว่ามีกระบวนการประเมินที่ปรากฏดังนี้

3.4.1 ภัยคุกคามนี้นับเป็นภัยคุกคามที่อันตรายร้ายแรง จะต้องมีการประชาสัมพันธ์ให้ทุกภาคส่วนรับรู้และเรียนรู้อย่างต่อเนื่องทั้งทางสื่อสังคมออนไลน์เองและการลงพื้นที่ทำความเข้าใจกับประชาชน

3.4.2 เจ้าหน้าที่รัฐจะจัดการกับปัญหาสื่อสังคมออนไลน์ที่มีลักษณะสร้างความรุนแรงเหล่านี้ได้ยากขึ้น เพราะบางส่วนอาจคิดว่าเป็นเครื่องมือของเจ้าหน้าที่รัฐ

3.4.3 การประเมินสถานการณ์ควรมีการประเมินอย่างสม่ำเสมอ แต่หากมีเหตุการณ์สำคัญจะมีการออกหนังสือชี้แจงและหากเล็กน้อยจะไม่ตอบโต้ ประชาชนส่วนใหญ่มีการคิดวิเคราะห์ก่อนเมื่อได้รับข้อมูลข่าวสารที่ไม่ชัดเจนและจะไม่เผยแพร่ต่อถ้ายังไม่มั่นใจ

4. ผลกระทบของภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงแห่งชาติรวมถึงแนวโน้มในอนาคต

4.1 ผลกระทบของภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงแห่งชาติรวมถึงแนวโน้มในอนาคตในความคิดเห็นของหน่วยงานด้านความมั่นคงของรัฐ ผู้บริหารระดับกระทรวงที่เกี่ยวข้อง 5 กระทรวง และผู้บริหาร/ผู้นำท้องถิ่น สามารถสรุปได้ว่ามีผลกระทบที่ปรากฏดังนี้

4.1.1 การสร้างทัศนคติเชิงลบต่อรัฐให้กับประชาชนส่งผลต่อความมั่นคงแห่งชาติเป็นอย่างยิ่ง โดยหากประชาชนจะไปรับข้อมูลข่าวสารอื่นที่ถูกบิดเบือนผ่านสื่อสังคมออนไลน์อย่างต่อเนื่อง ทำให้ต่อไปประชาชนอาจจะไม่เชื่อหรือไม่รับข้อมูลใดจากฝ่ายรัฐอีก และในที่สุดจะนำไปสู่ความเกลียดชังต่อเจ้าหน้าที่ของรัฐและการปรับทัศนคติให้กลับคืนมาได้นั้นทำได้ยาก

4.1.2 ผลกระทบต่อความมั่นคงแห่งชาติจะทำให้เกิดความแตกแยกของผู้คนทั้งทางด้านเชื้อชาติและศาสนา โดยเป็นการทำลายสังคมพหุวัฒนธรรมของพื้นที่นี้จนอาจนำไปสู่การแยกตัวไปเป็นเอกเทศในอนาคตการซึ่งยังไม่ได้รับการแก้ไข

4.1.3 แนวโน้มในอนาคตของภัยคุกคามด้านไซเบอร์จะยังคงเป็นปัญหาหลักที่รัฐบาลต้องดำเนินการอย่างเป็นระบบ ก่อนที่จะเกิดเหตุการณ์บานปลายจนกระทั่งรัฐบาลอาจไม่อยู่ในสถานะควบคุมได้ต่อไป นั่นคือ รัฐไม่มีเสถียรภาพและรัฐไม่มีความน่าเชื่อถือในการดำเนินการเรื่องความปลอดภัย

4.1.4 ปัญหาเรื่องภัยคุกคามด้านไซเบอร์อาจก่อให้เกิดปัญหาระหว่างประเทศได้ ถ้าไม่มีกระบวนการแก้ไขโดยความเห็นชอบสากล

4.2 ผลกระทบของภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงแห่งชาติรวมถึงแนวโน้มในอนาคตในความคิดเห็นของเจ้าหน้าที่ระดับปฏิบัติการด้านความมั่นคงรวมถึงเจ้าหน้าที่ทหารที่รับผิดชอบด้านภัยคุกคามของสำนักปฏิบัติการข่าวสาร สามารถสรุปได้ว่ามีผลกระทบที่ปรากฏดังนี้

4.2.1 ในโลกไซเบอร์มีการนำประเด็นชาติพันธ์และศาสนา เข้ามาเป็นประเด็นเพื่อการสร้างข่าวบิดเบือนและเผยแพร่สู่เครือข่ายสังคมออนไลน์ ซึ่งจะส่งผลให้เกิดความเกลียดชังขึ้นในสังคมทุกระดับชั้นโดยทำให้สังคมนั้นอยู่ร่วมกันโดยไม่มีความสงบสุข

4.2.2 ในโลกไซเบอร์และเครือข่ายสังคมออนไลน์มีการนำประเด็นในอดีตทั้งประวัติศาสตร์ที่จริงและบิดเบือนมาใช้เป็นเงื่อนไขสร้างสถานการณ์รุนแรง การสร้างความคิดความเชื่อให้เยาวชนซึ่งจะส่งผลต่ออนาคตของชาติในระยะยาว

4.2.3 ชาวบ้านต้องการความสงบแต่ไม่กล้าบอกเจ้าหน้าที่เนื่องจากไม่แน่ใจว่าเจ้าหน้าที่จะคุ้มครองได้ตลอดชีวิตหรือไม่ ดังนั้นต้องหาวิถีทางคุ้มครองความปลอดภัยของชีวิตและทรัพย์สินให้ดีขึ้นโดยอาจต้องปรับกฎหมายด้านการคุ้มครองให้เห็นเป็นประจักษ์และถูกต้องตามหลักสากล

4.2.4 หากมีปัจจัยหรือสถานการณ์ที่น่าจะมีแนวโน้มรุนแรงมากขึ้น ภาครัฐต้องระวังไม่ให้เกิดเหตุเพื่อให้ผู้ก่อการร้ายนำไปขยายผลไปสู่ความรุนแรงอื่นๆ ได้

4.3 ผลกระทบของภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงแห่งชาติรวมถึงแนวโน้มในอนาคตในความคิดเห็นของนักวิชาการและผู้เชี่ยวชาญด้านระบบไอซีทีซึ่งเป็นเจ้าหน้าที่ด้านความมั่นคง สามารถสรุปได้ว่ามีผลกระทบที่ปรากฏดังนี้

4.3.1 ในอนาคตถ้าไม่เกี่ยวข้องกับภัยคุกคามด้านไซเบอร์น่าจะมีการเกิดเหตุการณ์รุนแรงน้อยลง เนื่องจากฝ่ายผู้ก่อการร้ายอาจจะมีงบประมาณหรือผู้สนับสนุนน้อยลง

4.3.2 เหตุการณ์ความไม่สงบมักเกิดจากผลประโยชน์ของคนบางกลุ่มและเจ้าเมืองเก่าโดยมีการปลูกฝังเยาวชนรุ่นใหม่ให้เข้าใจผิดและเกลียดชังต่อรัฐบาล อย่างไรก็ตามมีคนอิสลามรุ่นใหม่ที่มีใจยอมรับได้มากขึ้น

4.3.3 แนวโน้มเกิดเหตุการณ์การสร้างข่าวสารบิดเบือนผ่านสื่อสังคมออนไลน์จะทวีความรุนแรงมากยิ่งขึ้นเนื่องจากมีการใช้ไซเบอร์มากขึ้น มีการดึงต่างประเทศเข้ามาร่วมเพื่อให้มีผู้สนับสนุนให้แยกประเทศโดยทำให้ประเทศไทยมีปัญหาในเวทีโลก

4.3.4 ปัจจุบันยังมีกระบวนการละเมิดสถาบันพระมหากษัตริย์ผ่านเครือข่ายสังคมออนไลน์อย่างต่อเนื่อง ซึ่งถือว่าเป็นภัยคุกคามด้านความมั่นคงแห่งชาติต่อสถาบันหลักของประเทศ

4.2 ผลกระทบของภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงแห่งชาติรวมถึงแนวโน้มในอนาคตในความคิดเห็นของหน่วยงานภาคเอกชนและภาคประชาชน สามารถสรุปได้ว่ามีผลกระทบที่ปรากฏดังนี้

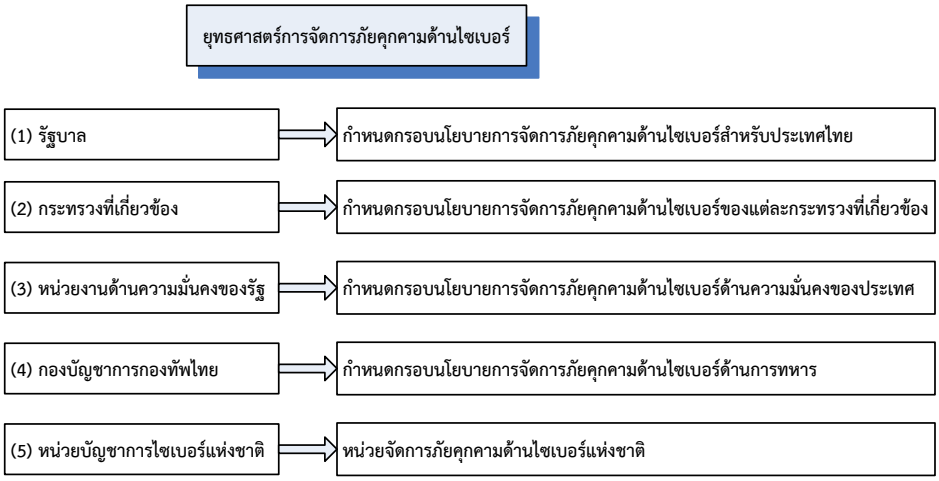
4.4.1 มาตรการป้องกันและแก้ไขของเจ้าหน้าที่รัฐยังไม่เหมาะสม ดังเช่น เมื่อผู้ต้องหาส่วนมากที่เป็นผู้ปลุกปั่นและบิดเบือนข่าวสารในสังคมออนไลน์ แต่เจ้าหน้าที่ไม่มีเครื่องมือในการหาหลักฐานอย่างเช่นการตรวจ IP Address เป็นต้น

4.4.2 ภัยคุกคามส่งผลกระทบต่อจิตใจของประชาชนอย่างหลีกเลี่ยงไม่ได้ เนื่องจากภัยคุกคามด้านไซเบอร์จะสามารถนำไปสู่ชนวนแห่งการสร้างสถานการณ์รุนแรงได้อยู่เสมอ ดังนั้นควรใช้ยุทธศาสตร์ชาติในการแก้ไขปัญหาอย่างเป็นระบบ

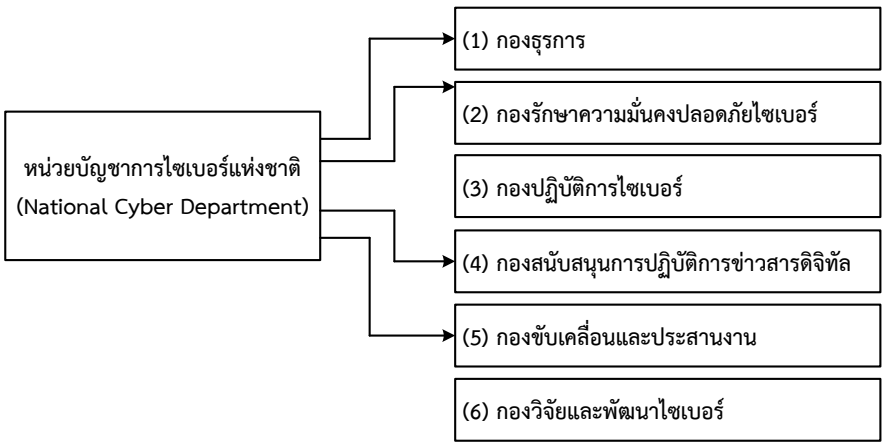
5. รูปแบบที่เหมาะสมสำหรับการจัดการภัยคุกคามด้านไซเบอร์

สำหรับประเทศไทยนั้นการกำหนดนโยบายและยุทธศาสตร์การจัดการกับภัยคุกคามด้านไซเบอร์มักเกิดขึ้นจากภาครัฐ โดยอาศัยหน่วยงานด้านความมั่นคงและกระทรวงที่เกี่ยวข้องตามที่

ปรากฏในยุทธศาสตร์ชาติระยะ 20 ปี พ.ศ. 2561-2580 โดยไม่ปรากฏประเด็นเด่นชัดที่เกี่ยวกับรูปแบบการดำเนินงาน แผนงาน และมาตรการที่เกี่ยวข้อง ซึ่งยังไม่ได้กำหนดเจ้าภาพรับผิดชอบโดยตรง จากการศึกษาข้อมูลที่เกี่ยวข้องสามารถนำเสนอรูปแบบที่เหมาะสมของการจัดการภัยคุกคามด้านไซเบอร์ในภาพรวม ซึ่งสามารถกำหนดองค์ประกอบหลักของการรักษาความมั่นคงปลอดภัยด้านไซเบอร์แห่งชาติแสดงดังภาพที่ 1



ภาพที่ 1 องค์ประกอบหลักและภารกิจของการรักษาความมั่นคงปลอดภัยด้านไซเบอร์แห่งชาติ



ภาพที่ 2 หน่วยบัญชาการไซเบอร์แห่งชาติ

ส่วนภาพที่ 2 และ 3 จะแสดงโครงสร้างของหน่วยบัญชาการไซเบอร์แห่งชาติและโครงสร้างพื้นฐานการจัดการภัยคุกคามด้านไซเบอร์ที่ประกอบด้วย 1) หน่วยบัญชาการไซเบอร์แห่งชาติ (National Cyber Department) 2) เทคโนโลยีฮาร์ดแวร์ (Hardware Technology) 3) เทคโนโลยีซอฟต์แวร์ (Software Technology) 4) เทคโนโลยีเครือข่ายความเร็วสูง (Hi-Speed Network Technology) 5) นักปฏิบัติการด้านไซเบอร์ (Cyber Operators) และ 6) รูปแบบการจัดการภัยคุกคามด้านไซเบอร์ (Cyber Treats Management Format)

ภาพที่ 3 โครงสร้างพื้นฐานการจัดการภัยคุกคามด้านไซเบอร์

ผลจากความเสียหายที่เกิดจากภัยคุกคามด้านไซเบอร์ที่ผ่านมา ทำให้รัฐบาลไทยตระหนักดีถึงผลกระทบทั้งในแง่ที่เป็นประโยชน์และโทษจากการทำสงครามไซเบอร์ โดยพยายามพัฒนาขีดความสามารถด้านการทำสงครามไซเบอร์ทั้งในเชิงรุกและการรักษาความมั่นคงปลอดภัย

ด้านไซเบอร์ เพื่อใช้เป็นมาตรการทั้งเชิงรุกและเชิงรับจากการโจมตีด้านไซเบอร์ของฝ่ายตรงข้าม (สราวุธ ปิติยาศักดิ์, 2561: 1-22) ประเด็นสำคัญของนโยบายและแนวทางด้านการทำสงครามไซเบอร์ ในส่วนกระทรวงกลาโหม กองทัพไทย และกองทัพบก มีดังนี้

(1) ควรพัฒนายุทธศาสตร์ นโยบาย และแนวทางปฏิบัติ เพื่อใช้รับมือกับภัยคุกคามด้านไซเบอร์ทุกรูปแบบ โดยอาศัยความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้องเพื่อที่จะเสริมขีดความสามารถ ผนึกกำลัง และเสริมสร้างกำลังอำนาจที่ไม่มีตัวตนในโลกไซเบอร์

(2) ควรนำกรอบยุทธศาสตร์ด้านไซเบอร์ทั้ง 3 ด้าน ไม่ว่าจะเป็นด้านการป้องกัน การป้องปราม และการผนึกกำลัง ไปดำเนินการเพื่อให้บรรลุผลสำเร็จตามยุทธศาสตร์ดังกล่าวอย่างเป็นรูปธรรม

(3) ควรเตรียมการรับมือกับภัยคุกคามด้านไซเบอร์ โดยอาศัยกรอบการดำเนินงาน 5 ขั้นตอน ดังเช่นเดียวกับพันธกิจ 5 อย่าง ที่สถาบันมาตรฐานและเทคโนโลยีแห่งสหรัฐอเมริกาใช้ (ประกอบด้วย Identify, Protect, Detect, Response และ Recovery) ซึ่งขั้นตอนเหล่านี้เป็นพื้นฐานของการรับมือกับการโจมตีด้านไซเบอร์ที่ทั่วโลกยอมรับ กล่าวคือ (1) ขั้นที่ 1 การพิสูจน์ทราบภัยคุกคาม (Identify) เพื่อระบุภัยคุกคามหรือผลกระทบที่จะเกิดขึ้นว่า เป็นภัยคุกคามอะไร และมีผลกระทบอย่างไร (2) การป้องกันภัยคุกคาม (Protect) เพื่อป้องกันระบบไม่ให้เกิดความเสียหาย (3) การตรวจจับภัยคุกคาม (Detect) เพื่อตรวจค้น สืบค้น และค้นพบให้ได้ว่าเกิดการโจมตีที่ไหน ด้วยเครื่องมืออะไร และมีเป้าหมายอยู่ที่ไหน (4) การตอบสนอง (Respond) เพื่อแก้ปัญหาที่เกิดขึ้นจากการโจมตีดังกล่าว และ (5) การคืนสภาพระบบ (Recover) เพื่อให้ระบบกลับมาใช้งานต่อไปได้ตามปกติ จากขั้นตอนดังกล่าวทำให้เห็นได้ว่าทุกหน่วยงานที่มีการใช้ระบบด้านสารสนเทศเป็นหน้าที่ของบุคลากรภายในหน่วยที่จะเป็นผู้ดำเนินการโดยอาศัยเครื่องมือที่มีอยู่ของหน่วย หลักการที่สำคัญต่อการดำเนินการตามขั้นตอนเพื่อรับมือกับภัยคุกคามด้านไซเบอร์ก็คือ “ตรวจพบให้เร็ว” “ป้องกันไว้ก่อน” “ค้นหาให้เจอ” “ตอบสนองให้ไว” และ “กู้คืนให้ได้” (Richard A. Clarke, 2017: 1-3)

(4) ควรพัฒนากำลังพลของกองทัพให้มีความรู้ความสามารถเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ เพื่อให้กำลังพลของกองทัพมีความรู้ที่ทันต่อสถานการณ์ที่เปลี่ยนแปลงไปอย่างต่อเนื่องและมีทักษะที่จำเป็นต่อการรับมือกับภัยคุกคามที่หลากหลายรูปแบบ

(5) ควรให้ความรู้และสร้างความตระหนักรู้ถึงภัยคุกคามด้านไซเบอร์ให้กับกำลังพล บุคคลในครอบครัว ญาติพี่น้อง หรือบุคคลในสถานศึกษาต่างๆ เพื่อให้ช่วยกันเฝ้าระวังและตระหนักในเรื่องของการใช้เทคโนโลยีไม่ให้พวกเขาตกเป็นเหยื่อหรือเป็นเป้าหมายของการโจมตีด้านไซเบอร์ได้ง่าย

ในฐานะปัจเจกชน โลกไซเบอร์ย่อมถือได้ว่าอาจเป็นคุณอย่างมหาศาลหรืออาจเป็นโทษอย่างอนันต์ก็ได้ อย่างไรก็ตาม ภัยคุกคามที่มาพร้อมกับประโยชน์ที่ได้จากโลกไซเบอร์นี้อาจเกิดขึ้นได้ตลอดเวลาและมีความเสี่ยงสูงกับผู้ใช้งานด้านต่างๆ ดังนั้นกำลังพลของกองทัพหรือประชาชนทั่วไปที่มีส่วนเกี่ยวข้องกับการแสวงประโยชน์จากโลกไซเบอร์พึงต้องตระหนักถึงผลกระทบที่จะเกิดขึ้นตามมา รวมถึงให้ความสำคัญกับการรักษาความปลอดภัยในโลกไซเบอร์อย่างเคร่งครัดในเบื้องต้นดังนี้

(1) ไม่ควรระบุข้อมูลส่วนตัวในการลงทะเบียนสมาชิก (Registration) ที่เกินความจำเป็นและเผยแพร่สู่สาธารณะ เช่น ชื่อ/นามสกุลจริง วันเดือนปีเกิด สถานที่เกิด ภูมิลำเนา สถานที่ทำงาน หมายเลขโทรศัพท์ และอีเมล์ เป็นต้น เพราะอาจจะถูกใช้เป็นข้อมูลอ้างอิงให้กับผู้ประสงค์ร้าย และคาดเดารหัสผ่าน (Password) ที่ใช้อยู่ได้

(2) ควรกำหนดรหัสผู้ใช้งาน (Username) และรหัสผ่านโดยปฏิบัติตามกฎการรักษาความปลอดภัยด้านสารสนเทศ ควรเปลี่ยนแปลงรหัสผ่านด้วยตนเองในภายหลังตามที่ระบบกำหนดหรือเปลี่ยนตามห้วงระยะเวลา และควรหลีกเลี่ยงการกำหนดรหัสที่เป็นชื่อ วันเดือนปีเกิด หรือรหัสอื่นๆ ที่นักเจาะระบบสามารถเดาสุ่มได้ ไม่ควรเปิดเผยรหัสผ่านให้ผู้อื่นทราบ โดยเฉพาะการให้ผู้อื่นนำรหัสผ่านของตนมาเข้าใช้งานแทน เพราะอาจมีการนำไปใช้งานในทางที่มิชอบ และไม่ควรจดบันทึกรหัสผ่านลงในบัตรอิเล็กทรอนิกส์ บัตรเครดิต และกระดาษบันทึกหรือโทรศัพท์มือถือเป็นต้น เพราะมีโอกาสสูญหายและรั่วไหลไปยังบุคคลอื่นได้

(3) ไม่ควรนำข้อมูลแผนการต่างๆ อย่างละเอียดเผยแพร่บนสื่อสาธารณะ เช่น แผนการเดินทางส่วนตัว ข้อมูลแผนที่เกี่ยวกับที่อยู่อาศัย และระบุชื่อบุคคลในรูปภาพ (ติด Tag) เพราะจะเป็นข้อมูลให้กับเหล่ามิจฉาชีพ อาจถูกนำไปใช้ในทางมิชอบ หรือส่งผลกระทบต่อกองทัพ

(4) ไม่ควรปล่อยให้เด็กใช้งานระบบคอมพิวเตอร์หรือระบบเครือข่ายโดยอิสระ โดยขาดการตรวจสอบ ควบคุม กำกับดูแลของผู้ใหญ่ เพราะเด็กอาจจะนำข้อมูลที่ไม่เหมาะสมไปเผยแพร่ด้วยความคึกคะนอง ไม่ตั้งใจ ไม่ทันคิด หรืออาจจะถูกล่อลวงไปในทางมิชอบ

(5) หลีกเลี่ยงการนำเสนอข้อมูลพฤติกรรมส่วนตัวที่ส่งผลกระทบต่อความสงบเรียบร้อยทางสังคม เช่น ภาพการดื่มสุรา สูบบุหรี่ การกระทำที่ก้าวร้าวรุนแรง และการทารุณกรรม เป็นต้น เพราะอาจจะถูกนำไปใช้เป็นเครื่องมือในทางมิชอบ หรือนำไปสู่การเลียนแบบพฤติกรรมที่ไม่ดี

(6) ไม่ใช้บริการเครือข่ายสังคมออนไลน์ที่ไม่แน่ใจในเรื่องของความปลอดภัย แต่ให้เลือกใช้งานเฉพาะกลุ่มและสมาชิกที่มีความรู้จักมักคุ้น มีความเชื่อถือไว้ใจได้ มีความปลอดภัย และมีพฤติกรรมที่เหมาะสม เพื่อป้องกันข้อมูลข่าวสารของกลุ่มและสมาชิกในกลุ่มไม่ให้ถูกเผยแพร่ไปที่อื่น

(7) ระบบงานที่มีความสำคัญควรใช้อุปกรณ์ทางชีวภาพ (Biometric Device) เช่น การสแกนลายนิ้วมือ การสแกนฝ่ามือ และการสแกนม่านตา เป็นต้น เพื่อใช้เป็นอุปกรณ์ตรวจสอบลักษณะส่วนบุคคลทางชีวภาพ และเป็นการยืนยันตัวบุคคล (Authentic) ประกอบกับการใช้รหัสผ่านเพื่ออนุญาตการเข้าใช้งานโปรแกรม ระบบงาน หรือการเข้าใช้ห้องระบบคอมพิวเตอร์

(8) การใช้งานเครือข่ายอินเตอร์เน็ตสาธารณะแบบไร้สาย (Public WiFi) หรือเครือข่ายอินเตอร์เน็ตไร้สายฟรี (Free WiFi) ผู้ใช้พึงต้องระมัดระวัง รอบคอบ และมั่นใจว่าได้ในเรื่องความปลอดภัย ไม่ควรติดตั้งระบบอินเตอร์เน็ตไร้สายฟรี เพราะจะเป็นช่องทางให้นักเจาะระบบ หรือผู้ไม่ประสงค์ดีเข้ามาใช้งานในทางมิชอบและเจาะระบบเข้าถึงข้อมูลในองค์กรได้อย่างง่ายดาย รวมถึงส่งผลต่อการทำงานและก่อปัญหาให้กับองค์กรในภาพรวมได้อีกด้วย

จากผลการศึกษาสามารถนำมาสร้างมาตรการป้องกันภัยคุกคามทางอินเตอร์เน็ตเพื่อการรักษาความมั่นคงปลอดภัยของข้อมูลข่าวสารดังนี้ (ปริญญา หอมเอนก, 2561)

1. มาตรการป้องกันภัยคุกคามทางอินเตอร์เน็ตสำหรับหน่วยงาน

1.1 ตรวจสอบและยืนยันสิทธิการเข้าระบบที่สำคัญของบัญชีผู้ใช้ให้สอดคล้องกับความจำเป็นเข้าถึงระบบและข้อมูล

1.2 เพิ่มมาตรการป้องกันเว็บไซต์สำคัญด้วยระบบการป้องกันการโจมตี เช่น Web Application Firewall หรือ DDoS

1.3 แจ้งเจ้าหน้าที่ของหน่วยงานและพนักงานให้เพิ่มความระมัดระวังในการใช้อินเตอร์เน็ตโดยหลีกเลี่ยงการเข้าเว็บไซต์ที่ไม่เหมาะสม ไม่คลิกไฟล์แนบจากผู้อื่นกรณีที่ไม่ได้ตกลงกันก่อนหรือไม่รับเมล์แนบจากคนที่ไม่รู้จัก ระมัดระวังความเสี่ยงจากการเปิดไฟล์ผ่านโปรแกรมสนทนาต่างๆ หรือช่องทางเครือข่ายออนไลน์ทุกชนิด ทั้งนี้เพื่อหลีกเลี่ยงการติดมัลแวร์

1.4 หากพบพิรุธว่าระบบถูกโจมตี เช่น ไม่สามารถเข้าใช้งานระบบ/เว็บไซต์ได้ หรือมีความล่าช้ากว่าปกติ ควรตรวจสอบข้อมูลการเข้าถึงระบบที่สำคัญ เช่น ข้อมูล Log ย้อนหลัง 30 วัน เพื่อตรวจหาความผิดปกติในการเข้าถึงข้อมูล

1.5 การตั้งค่าระบบงานที่สำคัญให้บันทึกเหตุการณ์ (Log) การเข้าใช้งานระบบไม่ต่ำกว่า 90 วัน หรือตามที่กฎหมายกำหนด

1.6 หากเป็นไปได้ ให้หน่วยงานส่งรายชื่อผู้ติดต่อ (Contact Point) กรณีเกิดเหตุภัยคุกคามด้านไซเบอร์มายังศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย : ThaiCERT (ไทยเซิร์ต) เพื่อการตรวจสอบที่ถูกต้อง

2. มาตรการป้องกันภัยคุกคามทางอินเตอร์เน็ตสำหรับประชาชนทั่วไป

2.1 เพิ่มความระมัดระวังในการใช้อินเตอร์เน็ต โดยหลีกเลี่ยงการเข้าเว็บไซต์ที่ไม่เหมาะสม เว็บผิดกฎหมาย ไม่คลิกไฟล์แนบจากผู้อื่นกรณีที่ไม่ได้ตกลงกันหรือไม่รู้จักกันมาก่อน ระมัดระวังความเสี่ยง จากการเปิดไฟล์ผ่านโปรแกรมสนทนาต่างๆ หรือช่องทางสื่อสังคมออนไลน์ เพื่อหลีกเลี่ยงการติดมัลแวร์ ซึ่งนับวันมัลแวร์จะมาจากพวกไฟล์แนบทางเครือข่ายสังคมออนไลน์เพิ่มมากขึ้น

2.2 การใช้บริการอินเตอร์เน็ต อย่าตั้งรหัสผ่านเหมือนกันทุกระบบ เพราะหากคุณโดนแฮกเกอร์เจาะระบบสำเร็จแล้ว ระบบอื่นๆ ก็อาจถูกเจาะระบบด้วยหากใช้รหัสผ่านเดียวกัน

2.3 ติดตามข้อมูลข่าวสารเกี่ยวกับความมั่นคงปลอดภัยด้านไซเบอร์ และอ่านพิจารณาข้อมูลก่อนการแชร์ข้อมูลทุกครั้ง ตลอดจนไม่ส่งต่อข้อมูลที่ไม่ได้รับการยืนยันจากผู้ที่เกี่ยวข้อง

เมื่อนำข้อมูลทุกด้านมาตรวจสอบด้วยวิธีการสามเส้าด้านข้อมูลพบว่า ข้อมูลที่ได้มาจากการศึกษาเอกสารและรายงานการวิจัยที่เกี่ยวข้อง การสัมภาษณ์ และข้อเท็จจริงที่เกิดขึ้น สามารถกล่าวได้ว่าภัยคุกคามด้านไซเบอร์เป็นภัยที่ร้ายแรงสำหรับประเทศไทย ดังนั้นจึงควรมีนโยบาย มาตรการ แผนงาน และกิจกรรมที่ต้องสอดคล้องกับนโยบายแห่งรัฐเพื่อการจัดการภัยคุกคามให้มีประสิทธิภาพต่อไป

สรุปและอภิปรายผลการวิจัย

จากผลการศึกษาวิจัยสามารถนำข้อมูลทั้งหมดมาวิเคราะห์ SWOT และกำหนดร่างยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์สำหรับประเทศไทย สามารถสรุปได้ดังนี้

วิสัยทัศน์ (Vision) : ประเทศไทยมีศักยภาพในการจัดการภัยคุกคามด้านไซเบอร์

พันธกิจ (Mission) : การพัฒนารูปแบบการจัดการภัยคุกคามด้านไซเบอร์โดยมุ่งสร้างฐานความรู้ให้กับประชาชนทุกระดับเพื่อความมั่นคงปลอดภัยด้านไซเบอร์ของประเทศไทย

วัตถุประสงค์ (Objective) :

1. เพื่อใช้เป็นยุทธศาสตร์ที่มีประสิทธิภาพในการจัดการกับภัยคุกคามด้านไซเบอร์ของประเทศไทย
2. เพื่อพัฒนาขีดความสามารถในการจัดการกับภัยคุกคามด้านไซเบอร์ของประเทศไทย
3. เพื่อเสริมสร้างความมั่นคงปลอดภัยด้านไซเบอร์และก่อให้เกิดความสงบสุขในพื้นที่ประเทศไทย

ยุทธศาสตร์ (Strategy) : ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์สำหรับประเทศไทยประกอบด้วย IADCLIP โดยมีโครงสร้างดังต่อไปนี้

ยุทธศาสตร์ที่ 1 : ยุทธศาสตร์การจัดโครงสร้างพื้นฐานของประเทศไทยสำหรับใช้ในการจัดการกับภัยคุกคามด้าน ไซเบอร์ (Infrastructure)

เป้าหมายยุทธศาสตร์ : เพื่อการจัดโครงสร้างพื้นฐานของประเทศไทยสำหรับการจัดการกับภัยคุกคามด้านไซเบอร์

แนวทางหรือมาตรการ มีดังต่อไปนี้

1. การจัดโครงสร้างพื้นฐานของประเทศไทยสำหรับใช้ในการจัดการกับภัยคุกคามด้านไซเบอร์ดังภาพที่ 3

2. การกำหนดรูปแบบการจัดการภัยคุกคามด้านไซเบอร์ที่เหมาะสมและมีประสิทธิภาพโดยคำนึงถึงความมั่นคงปลอดภัยและความสงบสุขของประชาชนอย่างเป็นด้านหลัก

ยุทธวิธีหรือแผนปฏิบัติการ มีดังต่อไปนี้

1. การนำโครงสร้างพื้นฐานไปใช้จัดตั้งเพื่อกำหนดให้เป็นโครงสร้างหลักในการจัดการภัยคุกคามด้านไซเบอร์

2. การนำรูปแบบของระบบไอซีทีเพื่อการบริหารจัดการองค์กรเพื่อความมั่นคงปลอดภัยโดยเน้นการรักษาความมั่นคงปลอดภัยตามมาตรฐานสากล

ดัชนีชี้วัดผลงาน : ระบบป้องกันภัยคุกคามด้านไซเบอร์และสถิติการบุกรุกเพื่อจารกรรมข้อมูลข่าวสาร

ผลที่คาดว่าจะได้รับตามยุทธศาสตร์ที่ 1 : ประเทศไทยมีโครงสร้างพื้นฐานสำหรับการจัดการกับภัยคุกคามด้านไซเบอร์

ยุทธศาสตร์ที่ 2 : ยุทธศาสตร์การสร้างการตระหนักรู้โลกไซเบอร์ให้กับประชาชน (Awareness)

เป้าหมายยุทธศาสตร์ : เพื่อการสร้างการตระหนักรู้โลกไซเบอร์ให้กับประชาชน

แนวทางหรือมาตรการ มีดังต่อไปนี้

1. การสนับสนุนให้ประชาชนมีการสร้างความรู้ความเข้าใจที่ดีต่อการใช้งานด้านไซเบอร์และมีการถ่ายทอดความรู้ความเข้าใจที่ดีต่อการใช้ไซเบอร์เพื่อประโยชน์ส่วนตนรวมถึงประเทศชาติรวมทั้งมีการถ่ายทอดความรู้ความเข้าใจจากรุ่นไปสู่รุ่น

2. การเผยแพร่ความรู้และประชาสัมพันธ์ให้ประชาชนมีการใช้งานด้านไซเบอร์อย่างถูกวิธีรวมทั้งตระหนักถึงผลกระทบต่อการใช้งานไซเบอร์ที่ไม่ถูกต้อง เพื่อป้องกันการนำมาใช้เป็นเครื่องมือในการก่อการร้ายในประเทศไทย

ยุทธวิธีหรือแผนปฏิบัติการ มีดังต่อไปนี้

1. สร้างรูปแบบและวิธีการในการให้ความรู้ความเข้าใจโดยอาจใช้วิธีการฝึกอบรมภายในหน่วยงานหรือการถ่ายทอดความรู้โดยใช้สื่อสารมวลชน

2. ใช้สถาบันการศึกษาในการถ่ายทอดความรู้ความเข้าใจให้กับเยาวชนโดยอาจบรรจุไว้ในหลักสูตรหรือกิจกรรมเสริมหลักสูตร

3. กำหนดหลักสูตรที่เกี่ยวกับไซเบอร์ในทุกระดับเพื่อให้เยาวชนได้มีรากฐานของการศึกษาและเข้าใจต่อการใช้ไซเบอร์อย่างถูกต้อง

4. พัฒนาหลักสูตรในระดับอุดมศึกษาเพื่อพัฒนาองค์ความรู้ทางไซเบอร์ให้สามารถนำความรู้ไปใช้อย่างครอบคลุมและมีประสิทธิภาพในทุกมิติ

ดัชนีชี้วัดผลงาน : ความรู้ความเข้าใจต่อภัยคุกคามด้านไซเบอร์และรูปแบบการใช้งานด้านไซเบอร์ที่สร้างสรรค์ต่อสังคมโดยไม่ใช่การก่ออาชญากรรม

ผลที่คาดว่าจะได้รับตามยุทธศาสตร์ที่ 2 : ประชาชนของประเทศไทยมีความตระหนักรู้ต่อภัยคุกคามด้านไซเบอร์และมีรูปแบบการใช้งานที่ไม่เป็นภัยต่อผลประโยชน์และความมั่นคงของชาติ

ยุทธศาสตร์ที่ 3 : ยุทธศาสตร์การพัฒนาความก้าวหน้าด้านไซเบอร์ (Development)

เป้าหมายยุทธศาสตร์ : เพื่อการพัฒนาความก้าวหน้าด้านไซเบอร์ของประเทศไทยให้เข้าสู่มาตรฐานสากล

แนวทางหรือมาตรการ มีดังต่อไปนี้

1. การจัดตั้งหน่วยงานการพัฒนาด้านไซเบอร์เพื่อพัฒนาระบบไอซีทีและการรักษาความปลอดภัยทางไซเบอร์ข้อมูลข่าวสาร

2. จัดฝึกอบรมให้ความรู้ สนับสนุนการจัดสอบเพื่อให้บุคลากรผ่านเกณฑ์มาตรฐานสากลรวมทั้งการวิจัยสร้างองค์ความรู้ใหม่ทางด้านไซเบอร์

3. การพัฒนาบุคลากรให้มีความเชี่ยวชาญในการรักษาความมั่นคงปลอดภัยด้านไซเบอร์รวมทั้งสร้างแรงจูงใจในการจงรักภักดีและทำงานเพื่อประเทศชาติเพื่อป้องกันสมองไหลไปยังต่างประเทศ

ยุทธวิธีหรือแผนปฏิบัติการ มีดังต่อไปนี้

1. การสร้างหน่วยงานด้านความมั่นคงปลอดภัยด้านไซเบอร์ที่มีเครื่องมือและอุปกรณ์ที่ทันสมัย และพร้อมรับมือกับการป้องกัน การโจมตี และการโต้ตอบ

2. การสร้างชุดกิจกรรมฝึกอบรมกับประชาชนทุกระดับให้ทราบถึงความหมายและการรักษาความปลอดภัยทั้งข้อมูลส่วนตัวและข้อมูลส่วนรวม

3. การจัดโครงการพัฒนาบุคลากรในหน่วยงานด้านความมั่นคงของชาติให้เป็นหน้าที่ของผู้เชี่ยวชาญด้านไซเบอร์ที่มีศักยภาพสูงและพร้อมปฏิบัติการทุกรูปแบบ

4. การวิจัยและพัฒนาด้านไซเบอร์ที่เป็นประโยชน์ต่อการพัฒนาประเทศไทยและต่อต้านการก่อการร้ายด้านไซเบอร์

ดัชนีชี้วัดผลงาน : ทุกองค์กรในหน่วยงานด้านความมั่นคงของชาติรวมถึงภาคธุรกิจเอกชนมีผู้เชี่ยวชาญด้านไซเบอร์ที่มีศักยภาพสูงและงานวิจัยที่มีคุณภาพ

ผลที่คาดว่าจะได้รับตามยุทธศาสตร์ที่ 3 : ประเทศไทยมีความก้าวหน้าด้านไซเบอร์และมีรูปแบบการบริหารจัดการเทียบเท่ามาตรฐานสากล ทำให้เป็นจุดเริ่มต้นของการสร้างความสงบสุขโดยเฉพาะอย่างยิ่งในพื้นที่จังหวัดชายแดนภาคใต้

ยุทธศาสตร์ที่ 4 : ยุทธศาสตร์การส่งเสริมความร่วมมือด้านไซเบอร์ระหว่างภาครัฐ ภาคเอกชน และภาคประชาชน (Coordinate)

เป้าหมายยุทธศาสตร์ : เพื่อการสร้างความร่วมมือด้านไซเบอร์ระหว่างภาครัฐ ภาคเอกชน และภาคประชาชน

แนวทางหรือมาตรการ มีดังต่อไปนี้

1. มีการเสริมสร้างความเข้าใจร่วมกันในการกำหนด นิยาม ความหมายของภัยคุกคามด้านไซเบอร์ การก่อการร้าย และการก่อการร้ายทางไซเบอร์

2. มีการกำหนดนโยบาย แนวทาง และแผนปฏิบัติการที่รัดกุมชัดเจนเพื่อให้เกิดการแปลงแผนนั้นไปสู่กลยุทธ์และไปสู่การปฏิบัติตามวิสัยทัศน์ พันธกิจ และเป้าประสงค์ที่กำหนดไว้อย่างมีประสิทธิภาพ

3. กำหนดกลไกในการทบทวน ติดตาม และประเมินความเสี่ยงต่อการนำแผนงานไปปรับใช้เพื่อปรับแนวทางให้มีความเหมาะสมตามสถานการณ์ใหม่หรือสถานการณ์ที่แตกต่าง

ยุทธวิธีหรือแผนปฏิบัติการ มีดังต่อไปนี้

1. การใช้หน่วยบัญชาการไซเบอร์แห่งชาติเป็นศูนย์กลางเพื่อร่วมกันกำหนด นิยาม ความหมายของภัยคุกคามด้านไซเบอร์ การก่อการร้าย และการก่อการร้ายทางไซเบอร์

2. การกำหนดนโยบาย แนวทาง และแผนปฏิบัติการที่ชัดเจนเพื่อนำไปสู่การปฏิบัติตามวิสัยทัศน์ พันธกิจ และเป้าประสงค์ที่กำหนดของทุกภาคส่วนอย่างมีประสิทธิภาพและประสิทธิผล

3. การสร้างกลไกเฉพาะในการทบทวน ติดตาม และประเมินความเสี่ยงของภัยคุกคามด้านไซเบอร์ต่อการนำแผนงานไปปรับใช้อย่างมีประสิทธิภาพและประสิทธิผล

ดัชนีชี้วัดผลงาน : รูปแบบการใช้งานด้านไซเบอร์ที่มีประสิทธิภาพและประสิทธิผลทั้งในระดับองค์กรและระดับบุคคล

ผลที่คาดว่าจะได้รับตามยุทธศาสตร์ที่ 4 : ทุกภาคส่วนของประเทศไทยมีความร่วมมือในการต่อต้านการก่อการร้ายด้านไซเบอร์โดยเฉพาะอย่างยิ่งในพื้นที่จังหวัดชายแดนภาคใต้

ยุทธศาสตร์ที่ 5 : ยุทธศาสตร์การกำหนดใช้กฎหมายด้านไซเบอร์และการบังคับใช้กับประชาชน (Law and Enforcement)

เป้าหมายยุทธศาสตร์ : เพื่อการผลักดันการใช้กฎหมายสำหรับอาชญากรไซเบอร์ที่สร้างความรุนแรงในพื้นที่จังหวัดชายแดนภาคใต้

แนวทางหรือมาตรการ มีดังต่อไปนี้

1. กำหนดกฎหมาย กฎระเบียบ ขั้นตอน และแนวปฏิบัติที่เกี่ยวข้องกับการใช้ด้านไซเบอร์ ความมั่นคงปลอดภัยด้านไซเบอร์ และการต่อต้านการก่อการร้ายด้านไซเบอร์อย่างครอบคลุม

2. กำหนดแนวทางที่ชัดเจนและเหมาะสมต่อการบังคับใช้กฎหมาย พร้อมทั้งมาตรการและบทลงโทษต่อการกระทำอันเกี่ยวข้องกับก่อการร้ายด้านไซเบอร์

ยุทธวิธีหรือแผนปฏิบัติการ มีดังต่อไปนี้

1. การใช้หน่วยงานทางกฎหมายร่วมกันกำหนดกฎหมาย กฎระเบียบ ขั้นตอน และแนวปฏิบัติที่เกี่ยวข้องกับการใช้งานด้านไซเบอร์ ความมั่นคงปลอดภัยด้านไซเบอร์ และรูปแบบการต่อต้านการก่อการร้ายด้านไซเบอร์

2. การใช้หน่วยงานทางกฎหมายร่วมกันกำหนดแนวทางที่ชัดเจนและเหมาะสมต่อการบังคับใช้กฎหมาย พร้อมทั้งมาตรการและบทลงโทษต่อการกระทำอันเกี่ยวข้องกับก่อการร้ายด้านไซเบอร์

ดัชนีชี้วัดผลงาน : กฎหมาย กฎระเบียบ ขั้นตอน และแนวปฏิบัติที่เกี่ยวข้องกับการใช้ด้านไซเบอร์ที่มีประสิทธิภาพและประสิทธิผลทั้งในระดับองค์กรและระดับบุคคล

ผลที่คาดว่าจะได้รับตามยุทธศาสตร์ที่ 5 : ประเทศไทยมีกฎหมาย กฎระเบียบ ขั้นตอน และแนวปฏิบัติที่เกี่ยวข้องกับการใช้ด้านไซเบอร์ในการต่อต้านการก่อการร้ายและการสร้างความไม่สงบสุขโดยเฉพาะในพื้นที่จังหวัดชายแดนภาคใต้

ยุทธศาสตร์ที่ 6 : ยุทธศาสตร์การใช้การบูรณาการร่วมกันเพื่อแบ่งปันข้อมูลข่าวสาร (Integration)

เป้าหมายยุทธศาสตร์ : เพื่อการใช้การบูรณาการร่วมกันเพื่อแบ่งปันข้อมูลข่าวสารโดยเฉพาะอย่างยิ่งในพื้นที่จังหวัดชายแดนภาคใต้อย่างถูกวิธีและไม่ส่งผลกระทบต่อความมั่นคงแห่งชาติ

แนวทางหรือมาตรการ มีดังต่อไปนี้

1. การใช้หน่วยบัญชาการไซเบอร์แห่งชาติที่มีหน้าที่ในการกำกับดูแลและดำเนินการด้านไซเบอร์ มีการแบ่งปันข้อมูลร่วมกันเพื่อประโยชน์ของประชาชน รวมทั้งมีการบูรณาการการทำงานร่วมกัน อีกทั้งระบุโอกาส และความท้าทายในการเพิ่มขีดความสามารถของกลไกการตอบสนองต่อการก่อการร้ายรูปแบบต่างๆ

2. การสร้างฐานข้อมูลกลางเพื่อรวบรวมข้อมูลสำคัญจากทุกภาคส่วน รวมทั้งมีการควบคุมดูแลเพื่อไม่ให้ข้อมูลถูกเผยแพร่ ตลอดจนเปิดโอกาสให้ทุกหน่วยงานที่เกี่ยวข้องกับไซเบอร์สามารถดึงข้อมูลไปใช้ในทางที่ถูกต้องและเป็นประโยชน์ต่อชาติบ้านเมือง

3. การจัดตั้งสำนักข่าวกรองด้านไซเบอร์ เพื่อทำงานด้านการข่าวด้านไซเบอร์ แบ่งปันข้อมูลข่าวสาร และประสานงานความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้อง

ยุทธวิธีหรือแผนปฏิบัติการ มีดังต่อไปนี้

1. การกำหนดภารกิจและบทบาทของหน่วยบัญชาการไซเบอร์แห่งชาติในด้านการกำกับดูแลและดำเนินการด้านไซเบอร์เพื่อต่อต้านการก่อการร้ายด้านไซเบอร์

2. การสร้างฐานข้อมูลกลางโดยระดมผู้เชี่ยวชาญด้านการออกแบบและพัฒนาระบบไอซีทีที่มีศักยภาพในการสร้างฐานข้อมูลที่มีความมั่นคงปลอดภัยในระดับสูงสุด

3. การกำหนดภารกิจและบทบาทของสำนักข่าวกรองด้านไซเบอร์เพื่องานด้านการข่าวที่เกิดจากการประสานความร่วมมือกันของทุกภาคส่วน

ดัชนีชี้วัดผลงาน : หน่วยบัญชาการไซเบอร์แห่งชาติและสำนักข่าวกรองด้านไซเบอร์มีรูปแบบภารกิจที่สนับสนุนงานด้านไซเบอร์ที่ได้มาตรฐาน

ผลที่คาดว่าจะได้รับตามยุทธศาสตร์ที่ 6 : ประเทศไทยมีการใช้การบูรณาการร่วมกันเพื่อแบ่งปันข้อมูลข่าวสารที่เป็นประโยชน์เพื่อรักษาผลประโยชน์ของชาติและต่อต้านการก่อการร้ายด้านไซเบอร์

ยุทธศาสตร์ที่ 7 : ยุทธศาสตร์การรับรู้ด้านไซเบอร์เพื่อการป้องกัน การยับยั้งและการโจมตี (Perception)

เป้าหมายยุทธศาสตร์ : เพื่อให้เกิดการรับรู้ด้านไซเบอร์ทั้งการป้องกัน การยับยั้งและการโจมตีด้านไซเบอร์

แนวทางหรือมาตรการ มีดังต่อไปนี้

1. การปลูกฝังทัศนคติและแนวทางการใช้งานไซเบอร์ที่เป็นรูปธรรมเพื่อให้ประชาชนมีการรับรู้ต่อการใช้งานไซเบอร์ในทางที่ถูกต้องและไม่เป็นภัยต่อความมั่นคงของชาติ

2. การสร้างรูปแบบการมีส่วนร่วมของทุกภาคส่วน รวมทั้งวิธีการในการตระเตรียมตนเองเพื่อให้เกิดการปฏิบัติอย่างรู้เท่าทัน

ยุทธวิธีหรือแผนปฏิบัติการ มีดังต่อไปนี้

1. การกำหนดรูปแบบการปลูกฝังทัศนคติและแนวทางการใช้งานไซเบอร์ที่เป็นรูปธรรม เพื่อให้ประชาชนมีการรับรู้ต่อการใช้งานไซเบอร์ในทางที่ถูกต้องและไม่ส่งผลกระทบต่อความมั่นคงแห่งชาติ

2. การสร้างรูปแบบการมีส่วนร่วมของทุกภาคส่วน รวมทั้งวิธีการในการตระเตรียมตนเองและใช้มาตรการต่างๆ เพื่อให้เกิดการปฏิบัติอย่างรู้เท่าทัน

ดัชนีชี้วัดผลงาน : ทัศนคติในการใช้งานไซเบอร์ในทุกพื้นที่ของประเทศไทยมีประโยชน์ต่อการพัฒนาประเทศทุกมิติ

ผลที่คาดว่าจะได้รับตามยุทธศาสตร์ที่ 7 : ทุกภาคส่วนมีการรับรู้ด้านไซเบอร์เพื่อการป้องกัน การยับยั้ง และการโจมตี

ผลที่คาดว่าจะได้รับ (Outcomes) :

1. ภาครัฐมียุทธศาสตร์ที่มีประสิทธิภาพในการจัดการกับภัยคุกคามด้านไซเบอร์

2. ขีดความสามารถในการจัดการกับภัยคุกคามด้านไซเบอร์ทุกพื้นที่ของประเทศไทยเพิ่มขึ้น

3. ทำให้เกิดความมั่นคงปลอดภัยด้านไซเบอร์และก่อให้เกิดความสงบสุขในพื้นที่โดยเฉพาะอย่างยิ่งในจังหวัดชายแดนภาคใต้ของประเทศไทย

กล่าวโดยสรุปได้ว่า ภัยคุกคามด้านไซเบอร์จะยังคงเป็นภัยคุกคามต่อความมั่นคงตั้งแต่ระดับความมั่นคงแห่งชาติลงไปจนถึงระดับความมั่นคงของมนุษย์และในอนาคตจะมีแนวโน้มขยายตัวเพิ่มขึ้นเป็นทวีคูณ เพราะโลกไซเบอร์ได้กลายเป็นสิ่งอำนวยความสะดวกต่อวิถีชีวิตมนุษย์และการทำงานประจำวันในองค์กรต่างๆ อย่างไรก็ตาม โลกไซเบอร์นี้ย่อมมีทั้งด้านที่เป็นคุณและด้านที่เป็นโทษ ขึ้นอยู่กับมนุษย์ว่าจะใช้มันเพื่อวัตถุประสงค์ใดและได้ประโยชน์ด้านใด ด้วยเหตุนี้การที่มนุษย์ได้ประโยชน์อย่างมหาศาลจากโลกไซเบอร์ก็นำมาซึ่งความท้าทายต่อการป้องกันความเสียหายที่เกิดจากการใช้งานดังกล่าวด้วยเช่นกัน (สำนักงานสภาความมั่นคงแห่งชาติ, 2558: 17) ดังนั้นการพัฒนาศักยภาพของมนุษย์ให้รู้เท่าทันกับอันตราย คาดการณ์ถึงแนวโน้มในอนาคต และลงมือจัดการกับภัยคุกคามในโลกไซเบอร์ จะต้องอาศัยการแลกเปลี่ยนข้อมูลระหว่างกัน เทคโนโลยีคลาวด์และการสร้างสมรรถนะและความคล่องตัวทั้งในแง่ของระบบและบุคลากร ในรูปแบบที่ทัดเทียมกับเหล่าอาชญากรด้านไซเบอร์ โดยต้องรู้เท่าทันต่อการรบกวนและโจมตีในรูปแบบต่างๆ พร้อมจะรับมือได้ทั้งในระดับนโยบาย องค์กร และปัจเจกบุคคล ด้วยเหตุนี้ การจะเอาชนะสงครามไซเบอร์ทั้งในปัจจุบันและในอนาคตได้ก็ต่อเมื่อรัฐบาล หน่วยงานด้านความมั่นคงของรัฐ กระทรวงกลาโหม และกองทัพไทย รวมถึงองค์กรอื่นๆ ที่เกี่ยวข้อง ต่างมองเห็นสถานการณ์นี้ได้อย่างชัดเจน มีการบูรณาการข้อมูลอย่างเป็นระบบ เรียนรู้ข้อมูลระหว่างกัน ตรวจจับเหตุผิดปกติ

ตอบสนองได้อย่างรวดเร็ว ใช้เครื่องมือและทรัพยากรที่มีอยู่ได้อย่างคุ้มค่าและมีประสิทธิภาพสูงสุด ในส่วนของกองทัพไทยทั้งสามเหล่าทัพควรเตรียมความพร้อมทั้งทางด้านบุคลากร การจัดหน่วยผู้เชี่ยวชาญ นักวิเคราะห์ระบบ และเครื่องมือที่ทันสมัย เพื่อการรับมือกับภัยคุกคามด้านไซเบอร์ที่มีความรุนแรง สร้างความเสียหายอย่างใหญ่หลวง และส่งผลกระทบต่อความมั่นคงของประเทศ อีกทั้งควรพัฒนาเสริมสร้างกำลังด้านไซเบอร์อย่างเป็นระบบ มีระเบียบแบบแผน ทั้งมาตรการเชิงรับและเชิงรุก ให้มีประสิทธิภาพ คุณภาพ และความเข้มแข็งอย่างต่อเนื่องและยั่งยืน เพื่อเป็นหลักประกันด้านความมั่งคงปลอดภัยด้านไซเบอร์ของประเทศต่อไป

ข้อเสนอแนะ

ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์สำหรับประเทศไทย ถือว่าเป็นเรื่องสำคัญที่ต้องดำเนินการโดยเร็วที่สุด ทั้งนี้ก็เพื่อการรักษาความมั่นคงปลอดภัยด้านไซเบอร์หน่วยงานราชการ ภาคเอกชน และภาคประชาชนให้มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้ตามปกติ ตลอดจนการระงับยับยั้งการก่อการร้ายด้านไซเบอร์ไม่ให้เกิดขึ้นในประเทศไทย ผู้วิจัยมีข้อเสนอแนะดังนี้

1. ข้อเสนอแนะเชิงนโยบาย

1.1 ก่อนที่จะนำนโยบายหรือกฎหมายฉบับใดที่เกี่ยวข้องกับโลกไซเบอร์มาประกาศใช้ รัฐบาลต้องประชาสัมพันธ์ให้ประชาชนมีความเข้าใจอย่างแท้จริง เกี่ยวกับวัตถุประสงค์ ประโยชน์ที่ประชาชนจะพึงได้รับ และผลกระทบที่จะตามมา เพื่อป้องกันการเกิดข่าวลือที่ไม่พึงประสงค์ และกระแสต่อต้านของประชาชนในสื่อสังคมออนไลน์

1.2 องค์กรและหน่วยงานทั่วไปที่มีการใช้งานในโลกไซเบอร์ ควรมีมาตรการการรักษาปลอดภัยด้านไซเบอร์ (Cyber Security Measures) สำหรับหน่วยงานของตน

1.3 ในระดับประเทศ ควรมีหน่วยงานไซเบอร์เป็นการเฉพาะที่ให้การรักษาความมั่นคงปลอดภัยด้านไซเบอร์และการบริการประชาชนในการเฝ้าระวัง แจ้งเตือนภัย และการแก้ไขปัญหา เพื่อสร้างความเชื่อมั่นและความมั่นใจในการใช้งานในโลกไซเบอร์

1.4 ควรมีกลไกในการตัดสินใจภายใต้ประเมินความเสี่ยงเพื่อให้สามารถตอบสนองต่อการโจมตีด้านไซเบอร์ของฝ่ายตรงข้ามได้อย่างเหมาะสม และ พิจารณาถึงผลกระทบที่จะตามมา รวมถึงอาศัยภาวะผู้นำของผู้บริหารในการตัดสินใจที่ไม่ใช่มุ่งเน้นในเรื่อง “การป้องกัน” มากเกินไป จนละเลยหรือเพิกเฉยต่อ “การตอบโต้” กับการโจมตีดังกล่าว

1.5 ควรกำหนดทิศทางแก้ไขปัญหาและมาตรการตอบโต้การโจมตีด้านไซเบอร์ที่เหมาะสม โดยแต่ละหน่วยงานภาครัฐจะต้องตรวจสอบดูว่า นโยบายที่กำหนดขึ้นเพื่อการป้องกันและตอบโต้ต่อการโจมตีด้านไซเบอร์ของตนสามารถปฏิบัติได้จริง มีช่องโหว่ หรือปัญหาอะไรหรือไม่ โดยนโยบายดังกล่าวจะต้องเป็นนโยบายที่สามารถดำเนินการได้ในสภาพความเป็นจริงด้วย

1.6 ควรเสริมสร้างความรู้ความเข้าใจโลกไซเบอร์แก่เจ้าหน้าที่ภาครัฐและประชาชนทั่วไป โดยมุ่งเน้นในเรื่องมาตรการป้องกันมากกว่าการบังคับใช้กฎหมายหรือระเบียบที่เข้มงวดซึ่งเป็นการแก้ไขปัญหานี้ที่ปลายเหตุ เพราะยิ่งมีกฎหมายหรือระเบียบที่เข้มงวดมากขึ้นเท่าใด คนก็จะพยายามหลีกเลี่ยงมากขึ้นเท่านั้น ดังนั้น การดำเนินนโยบายหรือการหาช่องทางในการปิดกั้นหรือตัดขาด การรับรู้ของประชาชนจากโลกไซเบอร์ในสภาพแวดล้อมของโลกในปัจจุบันจึงเป็นสิ่งที่ทำไม่ได้อีกแล้ว หรือหากกระทำได้ก็จะเป็นการฝืนมติมหาชนอย่างรุนแรง ด้วยเหตุนี้ แนวทางที่ดีที่สุดต่อการดำเนินการด้านไซเบอร์ของรัฐบาลและหน่วยงานที่เกี่ยวข้อง คือ “การสร้างความเข้าใจกับประชาชน” เพื่อให้ประชาชนไว้เนื้อเชื่อใจต่อการดำเนินงานของรัฐบาล ไม่ใช่การออกกฎหมายเพื่อใช้บังคับกับประชาชนเพียงอย่างเดียว

1.7 ควรมีกฎหมายด้านไซเบอร์เป็นการเฉพาะ เพื่อกำหนดกฎกติกาทางสังคมของโลกไซเบอร์และมาตรการป้องปรามป้องกันการละเมิดกฎหมาย โดยกฎหมายจะเป็นเครื่องมือที่สำคัญอย่างมากสำหรับการสร้างโลกไซเบอร์ที่ปลอดภัย รวมถึงการมีหน่วยงานที่สามารถบังคับใช้กฎหมายด้านไซเบอร์อย่างจริงจัง

2. ข้อเสนอแนะในการวิจัยครั้งต่อไป

2.1 ควรมีการศึกษาวิจัยการออกแบบและพัฒนาระบบรักษาความปลอดภัยด้านไซเบอร์ที่เหมาะสมกับหน่วยงานทางความมั่นคงหรือกองทัพเป็นการเฉพาะ เพื่อให้เกิดความหลากหลายและเกิดประโยชน์ในการพัฒนางานวิจัยมากยิ่งขึ้น

2.2 ควรมีการศึกษาวิจัยการพัฒนาขีดความสามารถทางด้านการรักษาความปลอดภัยด้านไซเบอร์เพื่อให้ทัดเทียมกับมาตรฐานการรักษาความปลอดภัยด้านไซเบอร์สากลและเกิดประโยชน์ในการนำไปใช้แก้ปัญหาด้านความมั่นคงของชาติต่อไป

2.3 ควรมีการศึกษาวิจัยเชิงลึกยุทธศาสตร์การสร้างระบบรักษาความปลอดภัยด้านไซเบอร์ที่เชื่อมโยงกับมาตรฐานสากล

2.4 ควรมีการศึกษาวิจัยเชิงลึกถึงแผนงานและมาตรการในการพัฒนาระบบรักษาความปลอดภัยด้านไซเบอร์ที่เกี่ยวข้องกับนวัตกรรมและเทคโนโลยีสมัยใหม่ เพื่อให้ได้รูปแบบระบบรักษาความปลอดภัยด้านไซเบอร์ของกองทัพไทยและหน่วยงานทางความมั่นคงที่ทันสมัยมากยิ่งขึ้น

2.5 ควรมีการศึกษาวิจัยและพัฒนามาตรฐานด้านการรักษาความปลอดภัยด้านไซเบอร์ที่สามารถเชื่อมโยงนโยบายแห่งรัฐกับหน่วยงานทางความมั่นคง องค์กรต่อต้านการก่อการร้าย ภาคเอกชน ภาคประชาสังคม และภาคประชาชน เพื่อให้ได้รูปแบบของระบบรักษาความปลอดภัยด้านไซเบอร์ที่มีประสิทธิภาพภายใต้มาตรฐานเดียวกัน

รายการอ้างอิง

Nongrat S. (2013). American Cyber Security. *Security Studies Journal*. No.129-130 September 2013, pp. 18. (in Thai)

นงรัตน์ สายเพชร. (2556). ความมั่นคงไซเบอร์ของสหรัฐอเมริกา (American Cyber Security). *จุลสารความมั่นคงศึกษา.* ฉบับที่ 129-130 กันยายน พ.ศ. 2556, หน้า 18.

Prinya H.A. (2018). *Cyber Security*. [online] Retrieved May 2, 2018, pp. 1-3. from https://www.acisonline.net/?page_id=797 (in Thai)

ปริญญา หอมเอนก. (2561). *Cyber Security.* [ออนไลน์] สืบค้นเมื่อ 2 พฤษภาคม 2561, หน้า 1-3. เข้าถึงได้จาก: https://www.acisonline.net/?page_id=797

Phongsak P. (2010). *ICT System and Modern Management*. Bangkok: Witty, pp. 10-11. (in Thai)

พงษ์ศักดิ์ ผกามาศ. (2553). *ระบบไอซีทีและการจัดการยุคใหม่.* กรุงเทพ: สำนักพิมพ์ Witty, หน้า 10-11.

Gen. Rittee I. (2018). *Cyber Space VS National Security*. [online] Retrieved May 3, 2018, from http://rittee1834.blogspot.com/2015/04/cyber-space-vs-national-security.html (in Thai)

พล.ต.ฤทธี อินทราวุธ. (2561). *โลกไซเบอร์กับความมั่นคงของชาติ.* [ออนไลน์] สืบค้นเมื่อ 3 พฤษภาคม 2561. เข้าถึงได้จาก: http://rittee1834.blogspot.com/2015/04/cyber-space-vs-national-security.html

Gen. Rittee I. (2018). *Army Cyber Center*. [online] Retrieved May 5, 2018, from http://rittee1834.blogspot.com/2014/10/army-cyber-center.html (in Thai)

พล.ต.ฤทธี อินทราวุธ. (2561). *ศูนย์ไซเบอร์กองทัพบก.* [ออนไลน์] สืบค้นเมื่อ 5 พฤษภาคม 2561. เข้าถึงได้จาก: http://rittee1834.blogspot.com/2014/10/army-cyber-center.html

Center for Doctrine and Strategy Development. (2016). Army and Cyber Threats. *Security Strategy Journal*. Army Training Command Department 2016, pp. 5-6. (in Thai)

ศูนย์พัฒนาหลักนิยมและยุทธศาสตร์. (2559). กองทัพบกกับภัยคุกคามด้านไซเบอร์. *จุลสารยุทธศาสตร์ด้านความมั่นคง.* กรมยุทธศึกษาทหารบก 2559, หน้า 5-6.

Office of the National Security Council, Prime Minister's Office. (2015). *National Security Policy 2015-2021*. Bangkok: Cabinet and Royal Gazette Publishing Office 2015, pp.17. (in Thai)

สำนักงานสภาความมั่นคงแห่งชาติ สำนักนายกรัฐมนตรี. (2558). *นโยบายความมั่นคงแห่งชาติ พ.ศ. 2558-2564.* กรุงเทพมหานคร : สำนักพิมพ์คณะรัฐมนตรีและราชกิจจานุเบกษา พ.ศ. 2558, หน้า 17.

The electronic government policy. (2016). *Cyber Security*. Electronic Transactions Development Agency (Public Organization). Prepared September 10, 2016. (in Thai)

ส่วนนโนบายรัฐบาลอิเล็กทรอนิกส์. (2559). *ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security).* สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน). จัดทำเมื่อวันที่ 10 กันยายน 2559.

Sarawut P. (2018). *Cyber Security*. [online] Retrieved May 4, 2018, pp. 1-22. from https://thainetizen.org/2 0 1 5 / 1 0 / digital-economy-laws-update-sarawut-kittisak/ (in Thai)

สราวุธ ปิติยาศักดิ์. (2561). *ความมั่นคงด้านไซเบอร์.* [ออนไลน์] สืบค้นเมื่อ 4 พฤษภาคม 2561, หน้า 1-22. เข้าถึงได้จาก: https://thainetizen.org/2015/10/digital-economy-laws-update-sarawut-kittisak/

P.W. Singer and Allan Friedman. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know® 1st Edition.* New York: Oxford University Press, pp. 6-10.

Raphael Satter. (2017). *What makes a cyberattack? Experts lobby to restrict the term.* [Online] Retrieved 7 July 2017, pp. 1-2. Retrieved From: https://apnews.com/2c25d7da76f4409bae7daf063c071420

Richard A. Clarke. (2017). *US Cyber Security.* [Online] Retrieved 5 May 2018, pp. 1-3. Retrieved From: https://en.wikipedia.org/wiki/Richard_A._Clarke

Wikipedia. *Cyberattack.* (2018). [Online] Retrieved 5 May 2018, pp. 1-5. Retrieved From: https://en.wikipedia.org/wiki/Cyberattack, Retrieved 5 May 2018.

ผู้เขียน

พงษ์ศักดิ์ ผกามาศ
มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์
E-mail: p_phakamach@hotmail.com

ชัยวัฒน์ ประสงค์สร้าง
มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์
E-mail: chaiwatp62@gmail.com

เศรษฐชัย ชัยสนิท
มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี
E-mail: settachai.ch@gmail.com

ชูเกียรติ ช่วยเพชร
สำนักงานวิจัยและพัฒนาการทางทหารกองทัพบก
E-mail: huanatao2132@hotmail.com

ราชิต อรุณรังสี
กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร
E-mail: auma05@icloud.com