# แนวทางการพัฒนากองทัพไทยด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

# Thai Military Development Guidelines on Cyber Security

**บทความวิชาการ**

**อรรคเดช ประทีปอุษานนท์** [๑]
Akradej Prateapusanond [๑]
**ธาราทิพย์ กัลยาณมิตร** [๒]
Tharathip Kalyanamitra [๒]

**บทคัดย่อ**

สถานการณ์และการเปลี่ยนแปลงของโลกอย่างรวดเร็วในปัจจุบัน ส่งผลต่อความมั่นคงของนานาประเทศในหลายมิติ รวมทั้งประเทศไทยมีสิ่งบ่งชี้ว่าความมั่นคงของชาติได้รับผลกระทบจากไซเบอร์ในหลายระดับ ตั้งแต่รูปแบบที่มีผลกระทบต่อการใช้ชีวิตประจำวันของประชาชน ความน่าเชื่อถือทางเศรษฐกิจ สังคม การเมือง รวมไปถึงสภาวะแวดล้อมรอบตัวเราล้วนแต่ส่งผลต่อความสงบเรียบร้อยและความมั่นคงในประเทศ โดยจะใช้ในลักษณะการจารกรรม การก่อการร้าย รวมทั้งใช้เป็นเครื่องมือในการก่อกวนหรือทำลายความสงบเรียบร้อยของประเทศฝ่ายตรงข้าม ความตระหนักถึงศักยภาพของไซเบอร์ต่อความมั่นคงของชาตินั้นเกิดขึ้นอย่างกว้างขวางทั่วโลก ซึ่งหลายประเทศพยายามสร้างและพัฒนาขีดความสามารถทางไซเบอร์ เพื่อบ่งชี้ว่าประเทศของตนมีศักยภาพที่ก่อให้เกิดความได้เปรียบและความสามารถในการแข่งขันด้านต่าง ๆ แต่ยิ่งมีความก้าวหน้าและพึ่งพาไซเบอร์มากเพียงใด ยิ่งเพิ่มโอกาสเสี่ยงที่จะเกิดเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงของชาติจากไซเบอร์มากขึ้นอย่างหลีกเลี่ยงไม่ได้

การศึกษาครั้งนี้มีวัตถุประสงค์เพื่อศึกษาสภาพแวดล้อมของภัยคุกคามความมั่นคงด้านไซเบอร์ และให้ข้อเสนอแนะแนวทางการพัฒนากองทัพไทยด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยทำการศึกษาจากข้อมูลทุติยภูมิอันได้แก่ เอกสารวิชาการที่มีอยู่แล้ว และได้ทำการสัมภาษณ์เชิงลึกกับผู้ที่ปฏิบัติงานจริงทางด้านไซเบอร์ภายในกองทัพไทย โดยผลการศึกษาพบว่า ในระดับนโยบายควรสร้างความร่วมมือทางไซเบอร์ระหว่างประเทศทั้งในระดับภูมิภาคอาเซียน

---

[๑] ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ
Strategic Studies Center, National Defence Studies Institute, RTArF-HQ
E-mail: akradej@gmail.com

[๒] กองศึกษาวิจัยทางยุทธศาสตร์และความมั่นคง ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ
Strategic and Research Studies Division, Strategic Studies Center, National Defence Studies Institute, RTArF-HQ
E-mail: tharathip.th@gmail.com

ควรกำหนดนโยบายรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ควรเชื่อมโยงการทำงานด้านไซเบอร์ในภาพรวมทั้งการปฏิบัติยามปกติและการปฏิบัติในสถานการณ์จริง และควรบรรจุเรื่องไซเบอร์เข้าไปอยู่ในแผนป้องกันประเทศ ในขณะที่ระดับปฏิบัติควรมีการสร้างเครือข่ายไซเบอร์ในภาพรวม ควรได้รับการสนับสนุนจากหน่วยงานที่เกี่ยวข้อง ควรผลิตซอฟต์แวร์/ฮาร์ดแวร์ทางไซเบอร์ขึ้นใช้เอง ควรมีการฝึกร่วมกันระหว่างหน่วยงานด้านไซเบอร์ของกองทัพ ควรนำเรื่องไซเบอร์บรรจุเป็นวิชาในหลักสูตรโรงเรียนทหารทุกระดับ ทุกเหล่าทัพ ควรเตรียมความพร้อมในการตอบสนองต่อสถานการณ์ฉุกเฉินได้ทันท่วงที และฟื้นคืนระบบกลับสู่ภาวะปกติโดยเร็วที่สุด ควรมีการแบ่งปันข้อมูลระหว่างหน่วยงานในประเด็นที่เกี่ยวข้องกับไซเบอร์ ควรผลิตและพัฒนาบุคลากรด้านไซเบอร์ หน่วยงานทางด้านไซเบอร์ควรมีกระบวนการรับมือกับภัยคุกคามด้านไซเบอร์หลายรูปแบบ และควรสร้างความตระหนักรู้ให้แก่กำลังพลและประชาชนทั่วไป

**คำสำคัญ:** การพัฒนากองทัพไทย, ความมั่นคงปลอดภัยทางไซเบอร์

## Abstract

Today's rapid changes of the global situation inevitably affect the international security in many dimensions. In Thailand, there are numerous indications that national security is affected by cyber at different levels, starting with a pattern affecting the general public's daily lives, the public confidence in the reliability of a country's economic and socio-political systems as well as the other environmental settings around us. Also, cyber has had a disastrous effect on a state's peace and security as it is used in espionage and terrorism as well as a possible tool to disrupt or destroy peace and order in the targeted country. Thus awareness of the potential of cyber security to national security is widespread worldwide. Many countries are trying to build and develop cyber capabilities creating their competitive advantages and cyber potential. However, it seems that the more advanced technology is and the greater degree of a state's dependency on cyberspace inevitably increase the greater the risk of cyber-incidents, as well as the greater the risk of national security being compromised.

This study aims to examine the present environments of cyber security threats and offer recommendations on the development of the Thai military's cyber security by means of analyzing secondary including existing academic papers and in-depth interviews with those who have actual cyber-related work experience with in the Thai Armed Forces. The study found that at the policy level, international cooperation in the ASEAN region should be established; the National Cyber Security Policy should be developed. Virtual connections and possible cyber activities should be linked and properly integrated to generate the overview operations pictures of both general situations and critical activities; the national defense should plan to cover more cyber aspects; at the operational

level, virtual networks in cyberspace should be built and supported by the relevant agencies; own software/hardware should be developed and materialized; joint training and training exercises should be conducted regularly the military cyber agencies. Cyber subjects should be included in all military curriculum and courses; Emergency response and readiness be prepared and rehearsed so as to respond to emergency situations promptly and restore the system back to normal as soon as possible. Cyber-related information and issues should be shared between and among relevant agencies; personnel for cyber should be recruited and developed persistently; Cyber agencies should be prepared and readied for a variety of cyber threats; and cyber security awareness should be raised regularly for the army and the general public.

**Keywords:** Thai Military Development Guidelines, Cyber Security

**บทนำ**

ปัจจุบันเป็นยุคโลกาภิวัตน์ (Globalization) ที่การติดต่อสื่อสารไร้พรมแดน โดยการเชื่อมต่อด้วยอินเทอร์เน็ต มีอิทธิพลอย่างมากในการดำรงชีวิตประจำวัน ไม่ว่าจะเป็นการควบคุมระบบสื่อสารโทรคมนาคม ระบบไฟฟ้าธนาคาร หรือสาธารณูปโภค และระบบขนส่งของประเทศ ในขณะเดียวกันก็มีปรากฏการณ์ของอาชญากรรมอิเล็กทรอนิกส์ หรือ Cyber Crime ที่มีทั้งการล้วงข้อมูลความลับ การก่ออาชญากรรมและยักยอกทรัพย์มากขึ้น มีการใช้เทคนิคใหม่ที่เพิ่มความสลับซับซ้อนด้วยช่องทางการเข้าถึงข้อมูลที่หลากหลายยิ่งขึ้น โดยเฉพาะในเรื่อง Personal Mobile Devices ที่ใช้มือถือเชื่อมต่ออินเทอร์เน็ต การส่งข้อมูลขยะอันไม่พึงประสงค์ (Spam) การหลอกลวงผ่านสื่ออินเทอร์เน็ต (Phishing) ตลอดจนการเจาะระบบ (Hack) เพื่อเข้าถึงข้อมูลชั้นความลับ ซึ่งปัจจุบันแฮกเกอร์ (Hacker) ไม่ได้มีเป้าหมายเจาะระบบเครือข่ายธนาคารหรือผู้ให้บริการธุรกรรมออนไลน์เท่านั้น แต่ได้เปลี่ยนเป้าหมายเป็นผู้ใช้งานอินเทอร์เน็ตซึ่งเข้าถึงได้ง่ายกว่าแทน โดยอาศัยความรู้เท่าไม่ถึงการณ์ของผู้ใช้งานทั่วไปเป็นเครื่องมือ นอกจากนี้ หน่วยงานภาครัฐหรือหน่วยงานที่มีข้อมูลสำคัญ เช่น หน่วยงานทางทหาร หน่วยงานความมั่นคงปลอดภัยของประเทศ หน่วยงานด้านการเมือง หรือองค์กรธุรกิจขนาดใหญ่อาจตกเป็นเป้าหมายของการจารกรรมข้อมูลและทำลายระบบข้อมูลต่าง ๆ อีกด้วย ซึ่งเหตุการณ์และแนวโน้มที่เกิดขึ้นเหล่านี้ แสดงให้เห็นถึงลักษณะภัยคุกคามรูปแบบใหม่ที่เปลี่ยนแปลงไปสู่รูปแบบของสงครามอสมมาตร (Asymmetric Warfare) ที่ฝ่ายตรงข้าม หรือผู้ก่อการร้ายจะใช้โจมตีจุดสำคัญที่เป็นหัวใจของชาติโดยไม่จำเป็นต้องมีกำลังทางทหาร ผ่านการใช้สื่อดิจิทัล (Digital Media) และเทคโนโลยีโทรคมนาคม (Telecommunication Technology) เป็นเครื่องมือ โดยภัยคุกคามดังกล่าวนี้จะเป็นภัยคุกคามที่มีผลกระทบในระดับนานาชาติ

ในระดับภูมิภาคเอเชียตะวันออกเฉียงใต้นั้น มีความร่วมมือด้านไซเบอร์ของประเทศสมาชิกในประชาคมอาเซียน ซึ่งความมั่นคงไซเบอร์นั้นเป็นส่วนหนึ่งของความร่วมมือภายใต้เสาหลักประชาคมการเมือง-ความมั่นคง โดยกลไกหลักที่เป็นเวทีหารือและทบทวนความร่วมมือด้านความมั่นคงไซเบอร์ คือ การประชุมระดับรัฐมนตรีอาเซียนว่าด้วยอาชญากรรมข้ามชาติ (ASEAN Ministerial Meeting on Transnational Crime: AMMTC) และการประชุมเจ้าหน้าที่อาวุโสอาเซียนว่าด้วยอาชญากรรมข้ามชาติ (ASEAN Senior Officials Meeting on

Transnational Crime: SOMTC) ถึงแม้ว่าความร่วมมือในช่วงต้นจะเน้นไปที่การต่อต้านยาเสพติดเป็นสำคัญ แต่ในการประชุม AMMTC ครั้งที่ ๓ เมื่อ ต.ค.๔๔ ณ ประเทศสิงคโปร์ ที่ประชุมได้ตกลงที่จะผนวกความร่วมมือด้านความมั่นคงไซเบอร์ให้เป็นส่วนหนึ่งในแผนงานเพื่อจัดทำแผนปฏิบัติการอาเซียนเพื่อต่อต้านอาชญากรรมข้ามชาติ (ASEAN Plan of Action to Combat Transnational Crime) เป็นครั้งแรก สะท้อนถึงการตระหนักว่าอาชญากรรมข้ามชาติมิได้จำกัดอยู่เพียงอาชญากรรมที่พบเห็นได้เฉพาะหน้า เช่น การก่อการร้าย การค้ามนุษย์ หรือการค้าอาวุธสงครามเท่านั้น

ความจริงจังของภัยคุกคามทางไซเบอร์ในช่วงหลายปีที่ผ่านมา กอปรกับการตระหนักรู้ในความเชื่อมโยงระหว่างความมั่นคงไซเบอร์กับความร่วมมือด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทำให้ที่ประชุมรัฐมนตรีอาเซียนด้านโทรคมนาคมและเทคโนโลยีสารสนเทศ (ASEAN Telecommunications and IT Ministers Meeting: TELMIN) ครั้งที่ ๑๔ เมื่อ ม.ค.๕๘ ได้บรรจุประเด็นความมั่นคงไซเบอร์ลงในแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารของอาเซียน ฉบับที่ ๒ ระหว่าง ปี พ.ศ. ๒๕๕๙ - ๒๕๖๓ (ASEAN ICT Master Plan 2020) แผนแม่บทดังกล่าวได้กำหนดกลยุทธ์หลัก (Strategic Thrusts) เพิ่มเติมจากแผนแม่บทฉบับเดิม ๓ ประการ โดยหนึ่งในนั้น คือ กลยุทธ์ด้านความปลอดภัยและหลักประกันด้านข้อมูลข่าวสาร ซึ่งประกอบด้วยการพัฒนาหลักการด้านความปลอดภัยของข้อมูลระดับภูมิภาค และส่งเสริมความเข้มแข็งและประสิทธิภาพของความร่วมมือเพื่อตอบสนองต่อสถานการณ์ฉุกเฉินด้านไซเบอร์อย่างทันท่วงที โดยมีเป้าหมายเพื่อเสริมสร้างความเชื่อมั่นให้กับเศรษฐกิจดิจิทัลของอาเซียนและปรับปรุงความร่วมมือในการรับมือกับสถานการณ์ฉุกเฉินด้านไซเบอร์ของภูมิภาคให้มีประสิทธิภาพยิ่งขึ้น

ปัจจุบัน ประเทศไทยมีวิสัยทัศน์ในการบริหารประเทศ คือ “ประเทศมีความมั่นคง มั่งคั่ง ยั่งยืน เป็นประเทศพัฒนาแล้ว ด้วยการพัฒนาตามปรัชญาของเศรษฐกิจพอเพียง” โดยรัฐบาลมีภารกิจสำคัญในการขับเคลื่อนปฏิรูปประเทศด้านต่าง ๆ เพื่อปรับแก้ จัดระบบ ปรับทิศทาง และสร้างหนทางพัฒนาประเทศให้เจริญ และสามารถรับมือกับโอกาสและภัยคุกคามแบบใหม่ที่เปลี่ยนแปลงอย่างรวดเร็วโดยเฉพาะอย่างยิ่ง การมุ่งให้ความสำคัญต่อการพัฒนาเศรษฐกิจ เพื่อให้ทันต่อการขับเคลื่อนของโลกสมัยใหม่ ภายใต้วิสัยทัศน์เชิงนโยบายการพัฒนาเศรษฐกิจของประเทศไทยหรือที่เรียกกันอย่างคุ้นหูว่า “Thailand 4.0” โดยจะเป็นยุคที่เศรษฐกิจจะขับเคลื่อนด้วยนวัตกรรม (บวร เทศารินทร์, ๒๕๕๙: ๒) จากนโยบายในการขับเคลื่อนประเทศที่จะมุ่งเน้นให้มีการนำเทคโนโลยีสารสนเทศเข้ามาช่วยในการพัฒนาอาจนำมาสู่ภัยคุกคามด้านอาชญากรรมไซเบอร์ได้ เนื่องจากการเร่งการพัฒนาเกี่ยวกับอุตสาหกรรมดิจิทัลกอปรกับความสามารถในการเข้าถึงโครงข่ายไซเบอร์ของประชาชนในประเทศไทยเพิ่มขึ้นอย่างก้าวกระโดดในช่วง ๒ - ๓ ปีที่ผ่านมา ความเสี่ยงด้านภัยคุกคามไซเบอร์จึงมีสูงขึ้นหลายเท่าตัวทั้งในมิติของสังคม เศรษฐกิจ การเมือง และการทหาร และจะเป็นภัยคุกคามที่จะถูกยกระดับในเชิงยุทธศาสตร์ของประเทศอย่างหลีกเลี่ยงไม่ได้ (เศรษฐพงค์ มะลิสุวรรณ, ๒๕๕๙: ๒)

กองทัพไทยถือเป็นหน่วยงานหลักที่มีภารกิจในด้านการรักษาความมั่นคงปลอดภัยของประเทศชาติ ดังที่ระบุไว้ในรัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ.๒๕๖๐ กล่าวคือ เมื่อเกิดเหตุหรือมีภัยคุกคามใดก็ตามเข้ามาสู่ประเทศชาติกองทัพจึงเป็นหน่วยงานแรกที่ต้องตระหนักและรับมือกับเหตุการณ์ต่าง ๆ ที่จะเกิดขึ้น เช่นเดียวกับภัยคุกคามด้านไซเบอร์ที่มีแนวโน้มทวีความรุนแรงมากยิ่งขึ้นในปัจจุบัน ตลอดถึงนโยบายในการดำเนินงานของรัฐบาลและการดำเนินชีวิตประจำวันของประชาชนไทยนั้น

ผูกติดกับเทคโนโลยีและระบบดิจิทัลมากยิ่งขึ้น จึงเป็นการสมควรที่กองทัพจะต้องตระหนักถึงความมั่นคงปลอดภัยด้านไซเบอร์อย่างจริงจัง

**สถานการณ์ความมั่นคงปลอดภัยไซเบอร์ในต่างประเทศ**

หากกล่าวถึงความรุนแรงจากไซเบอร์ที่ประเทศในประชาคมโลกได้รับผลกระทบร้ายแรง คงเป็นตัวอย่างเหตุการณ์ของการทำสงครามไซเบอร์ (Cyber Warfare) ในต่างประเทศ โดยเหตุการณ์ที่นับว่าไซเบอร์สามารถใช้เป็นอาวุธในการโจมตีฝ่ายตรงข้ามได้อย่างแท้จริง คือ เหตุการณ์การโจมตี Stuxnet 2009 - 2010 ที่โรงงานนิวเคลียร์ของอิหร่านถูกโจมตี ซึ่งคาดว่าเป็นความร่วมมือระหว่างสหรัฐฯ กับอิสราเอล โดย Stuxnet เป็นการโจมตีโรงงานนิวเคลียร์ของอิหร่านด้วยวิธีการแทรกซึมเข้าไปในระบบควบคุมและประมวลผลแบบศูนย์รวม (Supervisory Control And Data Acquisition: SCADA) ที่ใช้ในการควบคุมและดูแลโครงสร้างพื้นฐานต่าง ๆ เช่น โรงงานไฟฟ้า โรงงานประปา ระบบควบคุมการจราจร ระบบควบคุมเขื่อน ระบบควบคุมแท่นขุดเจาะน้ำมัน ซึ่งการปฏิบัติการครั้งนี้พุ่งเป้าไปที่โรงงานนิวเคลียร์โดยการปิดหรือเปลี่ยนแปลงแรงดันของเตาปฏิกรณ์นิวเคลียร์ จนส่งผลกระทบต่อขีดความสามารถทางนิวเคลียร์ของอิหร่านต้องหยุดชะงักไป บทเรียนจากเหตุการณ์นี้ทำให้ตระหนักได้ว่าระบบที่ควบคุมด้วยเครือข่ายปิด (Closed Network) ก็ไม่ปลอดภัยเสมอไป

อีกหนึ่งเหตุการณ์ที่เป็นการโจมตีครั้งสำคัญทางไซเบอร์ของโลก คือ การโจมตีทางไซเบอร์ต่อประเทศเอสโตเนีย โดยเอสโตเนียเป็นประเทศที่แยกตัวออกมาจากสหภาพโซเวียต ต่อมามีปัญหาขัดแย้งระหว่างกันเรื่องการพยายามเคลื่อนย้ายอนุสาวรีย์ Bronze Soldier ซึ่งเป็นอนุสาวรีย์ที่สงครามโซเวียตสร้างขึ้น โซเวียตจึงใช้วิธีการโจมตีทางไซเบอร์ต่อเอสโตเนียด้วยวิธีการทำดีดอส (Distributed Denial-of-Service: DDoS) ที่มีขนาดสูงสุด ประมาณ ๑๐๐ เมกะบิตต่อวินาที ผลจากการทำ DDoS ทำให้เอสโตเนียที่ใช้ระบบ IT ในการควบคุมการทำงานของ Critical infrastructure (ไฟฟ้า ประปา ธนาคาร) ร้อยละ ๘๐ ของประเทศ ทำให้สาธารณูปโภคของประเทศไม่สามารถใช้การได้นานถึง ๓ สัปดาห์ ประเมินความเสียหายทั้งสิ้นหลายพันล้านบาท

ปี พ.ศ.๒๕๕๖ นายเอ็ดเวิร์ด สโนว์เดน ได้กล่าวหาว่าสำนักงานความมั่นคงแห่งชาติ (National Security Agency: NSA) ของสหรัฐฯ ใช้ระบบ “ปริซึม” ในการสอดแนมผู้ใช้อินเทอร์เน็ต โดยสามารถเข้าถึงข้อมูลได้ทุกชนิดไม่ว่าจะเป็นอีเมล ภาพถ่าย รวมถึงการดักฟังโทรศัพท์หรือโปรแกรมติดต่อสื่อสารระหว่างกันผ่านอินเทอร์เน็ต เพื่อสืบหาข้อมูลที่เป็นภัยต่อความมั่นคงของประเทศ ทั้งนี้ สโนว์เดนยังอ้างว่าสหรัฐฯ แอบแฮกข้อมูลเครือข่ายคอมพิวเตอร์ของจีนและฮ่องกงมานานหลายปีแล้วเช่นกัน (ไทยพับลิก้า, ๒๕๕๖: ๑-๔)

ปี พ.ศ.๒๕๕๘ สถานีโทรทัศน์เตเวแซ็งก์มงด์ของฝรั่งเศสต้องระงับการออกอากาศ เนื่องจากถูกโจมตีทางไซเบอร์ กลุ่มที่เรียกตัวเองว่า ไซเบอร์กาหลิบ ซึ่งเป็นกลุ่มที่มีความสัมพันธ์กับกลุ่มที่เรียกตัวเองว่า กลุ่มรัฐอิสลาม (ไอเอส) ออกมาอ้างว่าเป็นฝีมือของตน แต่ต่อมาเจ้าหน้าที่สืบสวนพบว่าเป็นฝีมือของกลุ่มนักเจาะระบบและล้วงข้อมูลชาวรัสเซีย

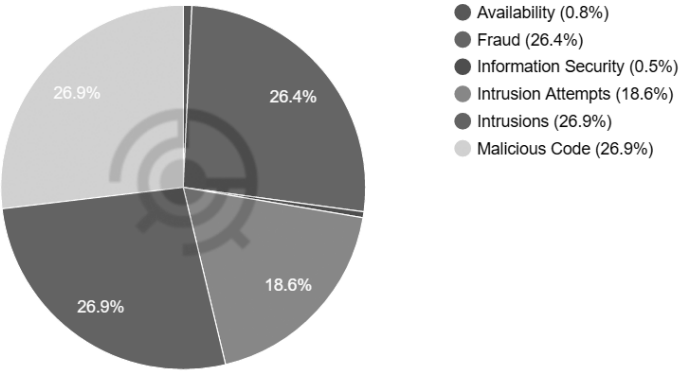
ปี พ.ศ.๒๕๕๙ นายฌอง อีฟ เล ดริยอง รัฐมนตรีว่าการกระทรวงมหาดไทยประเทศฝรั่งเศส กล่าวถึงข้อมูลภัยคุกคามทางไซเบอร์ปี ๕๙ ว่ารัฐบาลฝรั่งเศสสามารถสกัดแผนโจมตีทางไซเบอร์ที่พุ่งเป้าไปที่หน่วยงานด้านความมั่นคงในประเทศได้ถึง ๒๔,๐๐๐ ครั้ง ซึ่งแผนโจมตีดังกล่าวเพิ่มขึ้นเป็น ๒ เท่าทุกปี โดยเจ้าหน้าที่สามารถสกัดการโจมตีที่มาจากภายนอกประเทศได้หลายพันครั้ง ซึ่งรวมถึงความพยายามทำลายระบบโดรนของประเทศด้วย นอกจากนั้น นายเล ดริยอง ผู้รับผิดชอบการปรับปรุงระบบปฏิบัติการด้านความมั่นคงทางไซเบอร์ของฝรั่งเศสได้ให้ข้อมูลว่า

ในช่วง ๓ ปีที่ผ่านมา การโจมตีทางไซเบอร์ในฝรั่งเศสพุ่งสูงมาก และได้กลายเป็นภัยคุกคามร้ายแรงต่อโครงสร้างพื้นฐานของประเทศ และหลังจากนี้สิ่งที่ต้องจับตาดูอย่างใกล้ชิด คือ การเลือกตั้งทั่วไปในฝรั่งเศสช่วงเดือน เม.ย. - พ.ค. ๖๐ อาจตกเป็นเป้าการโจมตีทางไซเบอร์ได้อีก (บีบีซี ไทย, ๒๕๖๐: ๑-๒)

**สถานการณ์ความมั่นคงปลอดภัยไซเบอร์ในประเทศไทย**

สถานการณ์ไซเบอร์ภายในประเทศไทยนับว่ายังไม่มีความรุนแรงมากนัก การโจมตีในลักษณะที่เป็นการทำสงครามไซเบอร์ระดับประเทศนั้นยังไม่ปรากฏเหตุการณ์ชัดเจน มีเพียงแต่เหตุการณ์ที่เว็บไซต์ของหน่วยงานต่าง ๆ ถูกโจมตีด้วยการเปลี่ยนหน้าเว็บไซต์จากบุคคลเฉพาะกลุ่ม เช่น กลุ่มพลเมืองต่อต้าน Single Gateway กลุ่มพลเมืองต่อต้าน พ.ร.บ.คอมพิวเตอร์ โดยผู้กระทำผิดหรือแฮกเกอร์กลุ่มดังกล่าวต้องการต่อต้านอำนาจของรัฐ หรือทำให้รัฐเกิดความวุ่นวายและเสียหาย นอกจากนี้ ยังมีการโจมตีอีกรูปแบบหนึ่งที่เกิดขึ้น คือ การปฏิบัติการข่าวสาร (Information Operations: IO) กล่าวคือ เป็นการเปลี่ยนแปลงข่าวสารการรับรู้ต่าง ๆ ของประชาชน เช่น การแฮกเข้าไปบนเว็บไซต์เพื่อทิ้งข้อความบางอย่างไว้ การที่หน่วยงานภาครัฐทำ IO ผลงานนายกรัฐมนตรีเป็น infografic เผยแพร่ออกไป แต่กลุ่มดังกล่าวก็ทำการเปลี่ยนแปลงด้วยการตัดต่อเป็นรูปตลกขบขัน ซึ่งถือเป็นสงคราม IO ที่เกิดขึ้น เพื่อต้องการดึงประชาชนรวมถึงสื่อต่างประเทศ ที่เลือกฝั่งชัดเจนและไม่เลือกฝั่งชัดเจนเข้ามาในสนามนี้ด้วย

จากสถิติการแจ้งเหตุภัยคุกคามด้านไซเบอร์ที่เกิดขึ้นในประเทศไทย ประจำปี พ.ศ.๒๕๕๙ โดยจำแนกประเภทภัยคุกคามออกเป็น ๙ ประเภท ตามที่กำหนดโดย The European Computer Security Incident Response Team: eCSIRT พบการแจ้งเหตุภัยคุกคามทั้งสิ้น ๓,๗๙๗ เรื่อง โดยสามารถจัดลำดับตามจำนวนเหตุภัยคุกคามที่ได้รับแจ้งออกเป็นประเภทใหญ่ ๆ ได้ ดังนี้ ภัยคุกคามส่วนใหญ่ประมาณร้อยละ ๒๖.๙ (จำนวน ๑,๐๒๐ เรื่อง) เป็นภัยคุกคามที่เกิดจากโปรแกรมหรือซอฟต์แวร์ที่ถูกพัฒนาขึ้นเพื่อส่งให้เกิดผลลัพธ์ที่ไม่พึงประสงค์กับผู้ใช้งานหรือระบบ (Malicious Code) และประมาณร้อยละ ๒๖.๙ (จำนวน ๑,๐๒๐ เรื่อง) เป็นภัยคุกคามที่เกิดกับระบบที่ถูกบุกรุก/เจาะเข้าระบบได้สำเร็จ และระบบถูกครอบครองโดยผู้ที่ไม่ได้รับอนุญาต (Intrusions) ในส่วนภัยคุกคามที่รองลงมาประมาณร้อยละ ๒๖.๔ (จำนวน ๑,๐๐๒ เรื่อง) เป็นภัยคุกคามภัยที่เกิดจากการฉ้อฉลฉ้อโกงหรือการหลอกลวงเพื่อผลประโยชน์ (Fraud) และลำดับสุดท้ายประมาณร้อยละ ๑๘.๖ (จำนวน ๗๐๖ เรื่อง) เป็นภัยคุกคามที่เกิดจากความพยายามจะบุกรุก/เจาะเข้าระบบ (Intrusion Attempts) (ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT), ๒๕๕๙: ๑-๔) ข้อมูลดังภาพที่ ๑ และตารางที่ ๑




**ภาพที่ ๑ แสดงร้อยละการแจ้งเหตุภัยคุกคามด้านไซเบอร์ที่เกิดขึ้นในประเทศไทย ประจำปี พ.ศ.๒๕๕๙**

| ประเภทภัยคุกคาม/เดือน | ม.ค. | ก.พ. | มี.ค. | เม.ย. | พ.ค. | มิ.ย. | ก.ค. | ส.ค. | ก.ย. | ต.ค. | พ.ย. | ธ.ค. | รวม |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Abusive content | ๐ | ๐ | ๐ | ๐ | ๐ | ๐ | ๐ | ๐ | ๐ | ๐ | ๐ | ๐ | **๐** |
| Availability | ๐ | ๐ | ๐ | ๐ | ๐ | ๐ | ๐ | ๐ | ๐ | ๐ | ๐ | ๒๙ | **๒๙** |
| Fraud | ๙๘ | ๙๕ | ๖๖ | ๗๓ | ๑๖๔ | ๑๒๕ | ๑๐๔ | ๕๒ | ๕๗ | ๕๕ | ๔๓ | ๗๐ | **๑,๐๐๒** |
| Information gathering | ๐ | ๐ | ๐ | ๐ | ๐ | ๐ | ๐ | ๐ | ๐ | ๐ | ๐ | ๐ | **๐** |
| Information security | ๐ | ๐ | ๐ | ๐ | ๐ | ๐ | ๐ | ๐ | ๐ | ๐ | ๒ | ๑๘ | **๒๐** |
| Intrusion Attempts | ๓๕ | ๓๙ | ๓๖ | ๖๒ | ๖๙ | ๗๐ | ๕๙ | ๘๒ | ๔๒ | ๓๕ | ๖๖ | ๑๑๑ | **๗๐๖** |
| Intrusions | ๑๗๕ | ๕๑ | ๑๒๒ | ๙๖ | ๕๓ | ๔๔ | ๑๕๘ | ๖๐ | ๙๕ | ๓๗ | ๔๐ | ๘๙ | **๑,๐๒๐** |
| Malicious code | ๙๗ | ๑๒๓ | ๘๐ | ๑๐๔ | ๑๖๘ | ๑๖๗ | ๔๙ | ๑๔ | ๗๘ | ๓๐ | ๘๙ | ๒๑ | **๑,๐๒๐** |
| Other | ๐ | ๐ | ๐ | ๐ | ๐ | ๐ | ๐ | ๐ | ๐ | ๐ | ๐ | ๐ | **๐** |
| **รวม** | **๔๐๕** | **๓๐๘** | **๓๐๔** | **๓๓๕** | **๔๕๔** | **๔๐๖** | **๓๗๐** | **๒๐๘** | **๒๗๒** | **๑๕๗** | **๒๔๐** | **๓๓๘** | **๓,๗๙๗** |

**ตารางที่ ๑ ตารางแสดงสถิติภัยคุกคามทางด้านไซเบอร์ในประเทศไทย พ.ศ.๒๕๕๙**

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

จากความรุนแรงของภัยคุกคามด้านไซเบอร์ ประเทศในประชาคมโลกต่างก็แสวงหาแนวทางและวิธีการรับมือแตกต่างกันไป สำหรับประเทศไทยในเวทีความร่วมมืออาเซียน นายกรัฐมนตรีได้เข้าร่วมประชุมสุดยอดอาเซียน ครั้งที่ ๒๗ ระหว่างวันที่ ๒๐ - ๒๒ พ.ย.๕๘ ณ กรุงกัวลาลัมเปอร์ ประเทศมาเลเซีย ซึ่งการประชุมดังกล่าวนายกรัฐมนตรีได้มีข้อเสนอให้มีการจัดตั้งศูนย์ไซเบอร์อาเซียนขึ้นเพื่อรับมือกับผลกระทบทางลบจากความเชื่อมโยงและความท้าทายจากความมั่นคงรูปแบบใหม่ โดยเฉพาะอาชญากรรมไซเบอร์ (กระทรวงการต่างประเทศ, ๒๕๕๘: ๑-๔) ในระดับประเทศขณะนี้สำนักงานสภาความมั่นคงแห่งชาติกำลังดำเนินการจัดทำนโยบายรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อใช้เป็นกรอบกำหนดทิศทางการรักษาความปลอดภัยของประเทศ อันจะนำไปสู่การออก พ.ร.บ. และกฎหมายอื่น ๆ ที่เกี่ยวข้องตามมา นอกจากนั้น รองนายกรัฐมนตรีฝ่ายความมั่นคง และรัฐมนตรีว่าการกระทรวงกลาโหมได้มีนโยบายต่อภัยคุกคามด้านไซเบอร์ โดยให้เสริมสร้างขีดความสามารถการปฏิบัติการด้านไซเบอร์กระทรวงกลาโหมทั้งในด้านโครงสร้าง การจัดหน่วยระดับนโยบาย และระดับปฏิบัติ การสรรหาและการพัฒนาความรู้ให้กับบุคลากรที่จะบรรจุในอัตราของหน่วยที่เกี่ยวข้องกับการปฏิบัติงานไซเบอร์ การพัฒนาหลักนิยมและหลักการสำหรับการปฏิบัติการด้านไซเบอร์ทั้งเชิงรุก

และเชิงรับ รวมทั้งการสร้างความตระหนักรู้เกี่ยวกับภัยคุกคามด้านไซเบอร์ให้กับกำลังพลโดยทั่วไป เพื่อให้เห็นถึงความสำคัญและมีความตื่นตัวในการปฏิบัติตามมาตรการรักษาความปลอดภัยด้านไซเบอร์ (กระทรวงกลาโหม, ๒๕๖๐: ๑) เช่นเดียวกับกองบัญชาการกองทัพไทย โดยผู้บัญชาการทหารสูงสุดก็ได้มีนโยบายให้จัดตั้งและบูรณาการหน่วยงานรับผิดชอบงานด้านไซเบอร์ให้มีขีดความสามารถทั้งเชิงรุกและเชิงรับ และพัฒนาขีดความสามารถด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ทั้งด้านความมีเอกภาพ หลักนิยม กำลังพล และยุทโธปกรณ์ (กองทัพไทย, ๒๕๖๐: ๒๒)

**การดำเนินการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกองทัพไทย**

การปฏิบัติการในมิติไซเบอร์ของกองทัพไทยถือเป็นการปฏิบัติการทางทหารอย่างหนึ่งเพื่อรับมือกับภัยคุกคามรูปแบบใหม่ ซึ่งมีความสอดคล้องกับหน้าที่ของกองทัพไทยในการเตรียมกำลัง การป้องกันราชอาณาจักร และการดำเนินการเกี่ยวกับการใช้กำลังทางทหาร โดยในระดับกระทรวงกลาโหมและกองบัญชาการกองทัพไทยมีหน่วยงานสำคัญที่มีบทบาทในการดำเนินภารกิจเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ ได้แก่

**๑. ศูนย์ไซเบอร์ กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม กระทรวงกลาโหม (ศซบ.ทสอ.กห.)** ศซบ.ทสอ.กห. จัดตั้งขึ้นเมื่อ ๑ ต.ค.๕๘ ตามยุทธศาสตร์ไซเบอร์เพื่อการป้องกันประเทศ กระทรวงกลาโหม พ.ศ. ๒๕๕๘ ที่ รมว.กห. ได้อนุมัติเมื่อ ๓๐ มี.ค.๕๙ เพื่อให้เป็นหน่วยงานหลักประสานงานด้านไซเบอร์ในภาพรวมของ กห. เชื่อมโยงนโยบายด้านไซเบอร์กับระดับรัฐบาล และนำไปสู่การดำเนินการของหน่วยไซเบอร์ระดับปฏิบัติ รวมทั้งดำเนินการความร่วมมือด้านไซเบอร์กับหน่วยงานภาครัฐและภาคเอกชนที่เกี่ยวข้องทั้งในและต่างประเทศ

**๒. กองปฏิบัติการสงครามเครือข่าย สำนักปฏิบัติการ กรมยุทธการทหาร (กสค.สปก.ยก.ทหาร)** กสค.สปก.ยก.ทหาร จัดตั้งขึ้นเมื่อ พ.ค.๕๖ โดยสภากลาโหมมีมติอนุมัติให้กองทัพไทยจัดตั้งหน่วยงานรับผิดชอบทางด้านไซเบอร์ โดย กสค.สปก.ยก.ทหาร มีความรับผิดชอบหลักในการจัดการและบูรณาการการปฏิบัติทางไซเบอร์ในระดับกองทัพไทย เช่น จัดทำยุทธศาสตร์การปฏิบัติการไซเบอร์ของกองทัพไทย และมีหน้าที่รับผิดชอบในฐานะเป็นองค์ประกอบหนึ่งของศูนย์ประสานการรักษาความปลอดภัยระบบคอมพิวเตอร์กระทรวงกลาโหม (MODCERT)

**๓. กองรักษาความปลอดภัยสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร** (กรส.ศทศ.สส.ทหาร) กรส.ศทศ.สส.ทหาร มีพันธกิจในการดำเนินการตรวจสอบ วิเคราะห์ ป้องกัน กู้คืน และประเมินผลการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ จัดทำแนวทาง หลักการ ระเบียบ มาตรการ และแผนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของ บก.ทท. รวมทั้งพิจารณาเสนอแนะการดำเนินการต่อภัยคุกคามที่มีผลกระทบต่อระบบสารสนเทศของ บก.ทท. และมีหน้าที่รับผิดชอบในฐานะเป็นองค์ประกอบหนึ่งของศูนย์ประสานการรักษาความปลอดภัยระบบคอมพิวเตอร์กระทรวงกลาโหม (MODCERT)

**๔. การจัดตั้งศูนย์ไซเบอร์ทหาร** จากข้อมูลข้างต้นจะเห็นได้ว่าปัจจุบันกองบัญชาการกองทัพไทย มีหน่วยงานหลัก ที่รับผิดชอบด้านความมั่นคงปลอดภัยทางไซเบอร์อยู่ ๒ หน่วยงาน คือ กสค.สปก.ยก.ทหาร และ กรส.ศทศ.สส.ทหาร ซึ่งทั้ง ๒ หน่วยงานมีภารกิจทางด้านไซเบอร์ที่ต้องรับผิดชอบเหมือนกัน แต่มีสายการบังคับบัญชาที่แยกกันอยู่เมื่อผู้บังคับบัญชาได้เล็งเห็นถึงความเชื่อมโยงระหว่าง ๒ หน่วยงานนี้ จึงมีนโยบายให้มีการแปรสภาพ ๒ หน่วยงานดังกล่าวให้เป็น ***"ศูนย์ไซเบอร์ทหาร"*** ขึ้นตรงกับสำนักผู้บัญชาการทหารสูงสุด ซึ่งได้ทดลองปฏิบัติงานร่วมกันมาตั้งแต่ ต.ค.๕๙ และให้พร้อมปฏิบัติงานภายใน เม.ย.๖๐ นี้ โดยใช้พื้นที่อาคาร ๗ ชั้น ๑-๓ บก.ทท.

**แนวทางการพัฒนากองทัพไทยด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์**

สถานการณ์ปัจจุบันในระดับโลกเป็นสิ่งบ่งชี้ว่าความมั่นคงของชาติได้รับผลกระทบจากไซเบอร์ได้ในหลายลักษณะ ตั้งแต่รูปแบบที่มีผลกระทบต่อการใช้ชีวิตประจำวันของประชาชน ความน่าเชื่อถือทางเศรษฐกิจ ความสงบเรียบร้อยและความมั่นคงในประเทศ หรือใช้ในลักษณะการจารกรรม การก่อการร้าย รวมทั้งใช้เป็นเครื่องมือหนึ่งในการก่อกวนหรือทำลายความสงบเรียบร้อยของประเทศฝ่ายตรงข้าม ความตระหนักถึงศักยภาพของไซเบอร์ต่อความมั่นคงของชาตินั้นเกิดขึ้นอย่างกว้างขวางทั่วโลก หลายประเทศพยายามสร้างและพัฒนาขีดความสามารถทางไซเบอร์ เพื่อเป็นสิ่งบ่งชี้ถึงศักยภาพของประเทศที่ก่อให้เกิดความได้เปรียบและความสามารถในการแข่งขันด้านต่าง ๆ ได้แก่ การมีคุณภาพชีวิตที่ดีของประชาชน ความเข้มแข็งของพลังอำนาจแห่งชาติด้านเทคโนโลยี ความเข้มแข็งของพลังอำนาจแห่งชาติด้านการทหารที่มีความล้ำหน้าในการใช้ไซเบอร์เป็นเครื่องมือหนึ่งของการรบ หรือแม้แต่ความสามารถในการทำสงครามไซเบอร์ เป็นต้น แต่ยิ่งมีความก้าวหน้าและพึ่งพาไซเบอร์มากเพียงใด ยิ่งเพิ่มโอกาสเสี่ยงที่จะเกิดเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงของชาติจากไซเบอร์มากขึ้นอย่างหลีกเลี่ยงไม่ได้ จากข้อมูลในส่วนต่าง ๆ ที่กล่าวมาข้างต้นแสดงให้เห็นว่า มิติด้านไซเบอร์" (Cyberspace) นับเป็นมิติที่ทวีความรุนแรงมากขึ้นเรื่อย ๆ จนอาจกล่าวได้ว่าไซเบอร์เป็นความมั่นคงรูปแบบใหม่ที่ประชาคมโลกต่างให้ความสำคัญเป็นอย่างยิ่ง โดยมีลักษณะที่เปลี่ยนแปลงไปสู่รูปแบบของสงครามอสมมาตร (Asymmetric warfare) ที่ฝ่ายตรงข้ามหรือผู้ก่อการร้ายไม่จำเป็นต้องมีกำลังพลหรืออุทโธปกรณ์มาก แต่สามารถโจมตีจุดสำคัญที่เป็นหัวใจของเป้าหมายผ่านการใช้สื่อดิจิทัล (Digital media) และเทคโนโลยีโทรคมนาคม (Telecommunication technology) เป็นเครื่องมือ โดยภัยคุกคามดังกล่าวนี้จะเป็นภัยคุกคามที่มีผลกระทบในระดับนานาชาติ ซึ่งหากไม่มีการบริหารจัดการด้านไซเบอร์ที่ดีอาจนำมาสู่ปัญหาความมั่นคงที่ส่งผลกระทบหลายด้าน ไม่ว่าจะเป็นด้านการเมือง การทูต ข้อมูลสารสนเทศ เศรษฐกิจ สังคม และจิตวิทยา จากประเด็นปัญหาข้างต้น ผู้ศึกษาได้ทำการศึกษา เรื่องแนวทางการพัฒนากองทัพไทยด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขึ้น เพื่อศึกษาสภาพแวดล้อมของภัยคุกคามความมั่นคงด้านไซเบอร์ในอนาคต และให้ข้อเสนอแนะแนวทางการพัฒนากองทัพไทยด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยใช้วิธีการศึกษาจากเอกสาร และทำการสัมภาษณ์เชิงลึกกับบุคคลที่มีความเชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกองทัพไทย โดยได้ผลการศึกษาเป็นแนวทางการพัฒนากองทัพไทยด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ที่เสนอแนะต่อระดับนโยบายและระดับผู้ปฏิบัติที่มีความเกี่ยวข้องกับมิติด้านไซเบอร์ ดังมีรายละเอียดต่อไปนี้

**๑. ข้อเสนอแนะเชิงนโยบาย**

***๑.๑ การสร้างความร่วมมือทางไซเบอร์ระหว่างประเทศทั้งในระดับภูมิภาคอาเซียน และระหว่างประเทศคู่เจรจานอกภูมิภาค*** สิ่งสำคัญประการแรกที่ต้องคำนึงถึง คือ ประเทศไทยควรมีความร่วมมือและการตอบสนองต่อสถานการณ์ฉุกเฉินทางไซเบอร์ ระหว่างเครือข่ายของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (CERT) ในแต่ละประเทศ เพื่อให้สามารถทำงานร่วมกัน และตอบสนองต่อภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ อีกทั้งยังรวมถึงการแลกเปลี่ยนข้อมูลความรู้ และเทคโนโลยีที่จำเป็น ทั้งภายในภูมิภาคอาเซียนและประเทศคู่เจรจานอกภูมิภาคอื่น ๆ ตลอดถึงการวางกรอบความร่วมมือด้านไซเบอร์ระดับภูมิภาคร่วมกันอย่างจริงจัง

***๑.๒ การมีนโยบายรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ*** หัวใจสำคัญของการบริหารจัดการด้านไซเบอร์ คือ การเสริมสร้างความเข้าใจถึงบริบทและ

ความรุนแรงของภัยคุกคามด้านไซเบอร์ จนสามารถทำให้หน่วยที่เกี่ยวข้องเข้าใจบทบาทหน้าที่ของตนเองว่าจะต้องดำเนินการต่อเรื่องไซเบอร์อย่างไร ไม่ว่าจะเป็นกระทรวงกลาโหม กระทรวงมหาดไทย กระทรวงการต่างประเทศ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักงานตำรวจแห่งชาติ สำนักงานสภาความมั่นคงแห่งชาติ เป็นต้น โดยนโยบายรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ควรมีเนื้อหาที่ระบุรายละเอียดที่ลงลึกถึงการจัดตั้งหน่วยงานกลางระดับชาติที่มี Cyber Command ที่ชัดเจน

***๑.๓ การเชื่อมโยงการทำงานด้านไซเบอร์ในภาพรวมของกระทรวงกลาโหม ทั้งการปฏิบัติยามปกติและการปฏิบัติในสถานการณ์จริง*** สิ่งสำคัญที่กองทัพต้องตระหนัก คือ การเชื่อมโยงการทำงานระหว่างหน่วยไซเบอร์ในภาพรวม ไม่ว่าจะเป็น กห., บก.ทท. และเหล่าทัพ ทั้งการปฏิบัติยามปกติและการปฏิบัติในสถานการณ์จริง โดยกองทัพต้องผลักดันให้มี Cyber Command เมื่อเกิดเหตุการณ์ทางไซเบอร์ขึ้น (Cyber War) โดยตั้งฝ่ายบัญชาการรบ แล้วแยกการปฏิบัติไปยังหน่วยต่าง ๆ เพื่อความเป็นเอกภาพในการบังคับบัญชา

***๑.๔ บรรจุเรื่องไซเบอร์เข้าไปอยู่ในแผนป้องกันประเทศ*** อีกประเด็นที่สำคัญไม่แพ้กัน คือ การให้ความสำคัญในประเด็นไซเบอร์ โดยผลักดันให้เรื่องความมั่นคงทางไซเบอร์ผนวกไปบรรจุในแผนป้องกันประเทศ หรือแผนต่าง ๆ ที่จัดทำขึ้นเพื่อนำมาเป็นกรอบการปฏิบัติในกองทัพไทยและเหล่าทัพ กล่าวคือ งานด้านความมั่นคงปลอดภัยทางไซเบอร์ในปัจจุบันนั้นไม่นับว่าเป็นงานทางเทคนิค แต่นับว่าเป็นงานทางด้านยุทธการ ดังนั้น จึงต้องมีแผนต่าง ๆ มารองรับความมั่นคงปลอดภัยทางไซเบอร์

**๒. ข้อเสนอแนะเชิงปฏิบัติ**

**๒.๑ การปฏิบัติเชิงรุก**

***๒.๑.๑ การสร้างเครือข่ายไซเบอร์ในภาพรวม*** นอกจากความร่วมมือระหว่างประเทศแล้ว ความร่วมมือภายในประเทศด้านไซเบอร์ก็เป็นสิ่งสำคัญเช่นเดียวกันกล่าวคือ ความมั่นคงปลอดภัยด้านไซเบอร์นั้นอาศัยการแก้ปัญหาด้วยความร่วมมือที่เป็นทีม ไม่ว่าจะเป็นทีมของ บก.ทท. ด้านไซเบอร์ ไปสู่ทีมของ กห. ด้านไซเบอร์ และไปสู่ทีมของประเทศไทยด้านไซเบอร์ ซึ่งแต่ละทีมต้องสามารถบูรณาการการทำงานร่วมกันได้

***๒.๑.๒ การสนับสนุนของหน่วยงานที่เกี่ยวข้อง*** อีกสิ่งสำคัญที่มิติด้านไซเบอร์ต้องควรมี คือ ความร่วมมือจากหน่วยข่าวทุกองคาพยพ ไม่ว่าจะเป็น ขว., ศรภ. หรือหน่วยงานด้านการข่าวอื่น ๆ ที่ต้องคอยให้ข้อมูลความเคลื่อนไหว (Cyber Intelligence) โดยหน่วยงานด้านไซเบอร์จำเป็นต้องได้รับข้อมูลข่าวกรองที่มีความละเอียดและลงลึก ไม่ว่าจะเป็นเรื่องโครงสร้างพื้นฐานสำคัญของประเทศรอบบ้านและประเทศในภูมิภาค ข้อมูลการใช้ระบบ/เทคนิค ตลอดถึงความขัดแย้งในระดับโลก ระดับภูมิภาคหรือเจตนารมณ์ไม่ดีที่มาจากประเทศใดประเทศหนึ่ง อันจะเป็นข้อมูลสำคัญให้หน่วยงานด้านไซเบอร์ได้จัดทำแผนการบริหารจัดการกับภัยคุกคามที่อาจจะเกิดขึ้นและกระทบต่อความมั่นคงของประเทศได้

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

***๒.๑.๔ การฝึกร่วมกันระหว่างหน่วยงานด้านไซเบอร์ของกองทัพ*** โดยปกติกองทัพไทยได้มีการจัดการฝึกร่วมกันทางไซเบอร์อยู่แล้วในห้วงปกติ แต่สิ่งที่ต้องพิจารณาให้ชัดเจนยิ่งขึ้น คือ ต้องมีนโยบายกำหนดชัดเจนว่าต้องมีการฝึกร่วมทางไซเบอร์ รวมถึงเรื่องเครื่องมือที่จะเกิดขึ้นในการฝึกว่าใครจะเป็นเจ้าภาพ (Host) ในเรื่อง

เครื่องมือ เนื่องจากยุทโธปกรณ์เครื่องมือทางไซเบอร์ที่ต้องใช้ในการฝึกนั้นมีราคาสูง ตลอดถึงประเด็นเรื่องวงรอบการฝึกก็ต้องร่วมกันพิจารณาให้มีความชัดเจน

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

**๒.๒ การปฏิบัติเชิงรับ**

***๒.๒.๑ การเตรียมความพร้อมในการตอบสนองต่อสถานการณ์ฉุกเฉินได้ทันท่วงที และฟื้นคืนระบบกลับสู่ภาวะปกติโดยเร็วที่สุด (Cyber Resilience)*** กล่าวคือ กองทัพต้องเตรียมพร้อมรับมือกับความไม่ปลอดภัยและความเสี่ยงทางไซเบอร์ที่สามารถเกิดขึ้นได้ตลอดเวลา เนื่องจากความมั่นคงไซเบอร์ได้ขยับจากการรักษาความปลอดภัยไปสู่การตอบสนองต่อสถานการณ์ฉุกเฉินได้ทันท่วงที และต้องฟื้นคืนระบบให้กลับสู่ภาวะปกติโดยเร็วที่สุด (Cyber Resilience) ซึ่งภายหลังการถูกโจมตี กองทัพต้องสามารถทำให้ระบบอินเทอร์เน็ต หรือการติดต่อสื่อสารที่เป็น Network สามารถบริหารจัดการได้ โดยต้องสามารถจำกัดความเสียหายให้น้อยที่สุด ดำรงภารกิจอย่างต่อเนื่อง และฟื้นตัวให้เร็วที่สุด

***๒.๒.๒ การแบ่งปันข้อมูลระหว่างหน่วยงานในประเด็นที่เกี่ยวข้องกับไซเบอร์*** กล่าวคือ หน่วยงานต่าง ๆ ควรมีการแบ่งปันข้อมูลที่เกี่ยวข้องกับประเด็นทางไซเบอร์ เช่น กรณีการถูกแฮกระบบรถไฟฟ้าจนไม่สามารถให้บริการได้ กรณีธนาคารถูกแฮกตู้ ATM หรือกรณี รพ. หลายแห่งถูกแฮกข้อมูล ซึ่งกรณีต่าง ๆ เหล่านี้หน่วยงานที่เกี่ยวข้องควรเปิดเผย/ให้ข้อมูลกับหน่วยงานกลางทางด้านไซเบอร์ เพื่อที่จะช่วยกันอุดรอยรั่วที่เกิดขึ้นและนำมาใช้เป็นบทเรียนในครั้งต่อไป

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

***๒.๒.๔ หน่วยงานทางด้านไซเบอร์ควรมีกระบวนการรับมือกับภัยคุกคามด้านไซเบอร์หลายรูปแบบ*** การรับมือกับภัยคุกคามรูปแบบใหม่ต้องทำความเข้าใจธรรมชาติของภัยนั้น ๆ ก่อน โดยธรรมชาติของภัยคุกคามทางไซเบอร์นั้น มีการเคลื่อนไหวแบบไม่หยุดนิ่ง (Dynamic) ดังนั้น กระบวนการรับมือ คือ ต้องสามารถปฏิบัติได้ (Practical) ให้รับมือได้หลายรูปแบบ จึงสมควรต้องมีการปรับปรุงและพัฒนาการรับมือกับไซเบอร์อย่างไม่หยุดนิ่ง

***๒.๒.๕ การสร้างความตระหนักรู้ (Awareness) ให้แก่กำลังพลและประชาชนทั่วไป*** จากแนวโน้มความรุนแรงของภัยคุกคามด้านไซเบอร์ จะเห็นได้ว่าในอนาคตเทคโนโลยีจะพัฒนาและมีความก้าวหน้ามากยิ่งขึ้น โดยภัยคุกคามที่เกิดขึ้นจะมีความซับซ้อนมากขึ้นเรื่อย ๆ ซึ่งเป็นเรื่องที่แต่ละประเทศหนีไม่พ้นและต้องรับมือให้ได้ สิ่งที่กำลังพลและประชาชนทั่วไปต้องมี คือ ความตระหนักรู้ (Awareness) ต่อภัยอันตรายที่จะมาจากโลกไซเบอร์ ไม่ว่าจะเป็นการใช้อีเมล การทำธุรกรรมทางการเงิน การใช้สื่อสังคม (Social Media) ต้องใช้ด้วยความรู้เท่าทันกับภัยที่จะมาจากไซเบอร์

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

**ภาพที่ ๒ สรุปข้อเสนอแนะแนวทางการพัฒนากองทัพไทยด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์**

**บทสรุป**

โดยสรุป สถานการณ์และการเปลี่ยนแปลงของโลกอย่างรวดเร็วในปัจจุบัน ส่งผลต่อความมั่นคงของนานาประเทศในหลายมิติรวมทั้งประเทศไทย มีสิ่งบ่งชี้ว่าความมั่นคงของชาติได้รับผลกระทบจากไซเบอร์ในหลายระดับตั้งแต่รูปแบบที่มีผลกระทบต่อการใช้ชีวิตประจำวันของประชาชน ความน่าเชื่อถือทางเศรษฐกิจ สังคม การเมือง รวมไปถึงสภาวะแวดล้อมรอบตัว คุณลักษณะสำคัญประการหนึ่งของไซเบอร์ คือ สามารถแพร่กระจายอย่างรวดเร็วและไร้ซึ่งพรมแดน จึงนับเป็นภัยที่สามารถเกิดขึ้นได้ในทุกภูมิภาคทั่วโลก ประเทศไทยจึงต้องเตรียมการและใช้ศักยภาพด้านไซเบอร์ให้เป็นไปอย่างสอดคล้องกับสถานการณ์ระดับประเทศ ระดับภูมิภาค และในระดับโลกอย่างเกิดประโยชน์สูงสุด ปัจจุบันประเทศไทยมีกรอบนโยบายและกฎหมายไซเบอร์ที่เกี่ยวข้องทั้งสิ้น ๓ ฉบับ ได้แก่ (๑) ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ... (๒) ยุทธศาสตร์ไซเบอร์เพื่อการป้องกันประเทศกระทรวงกลาโหม พ.ศ.๒๕๕๘ และ (๓) แผนแม่บทไซเบอร์เพื่อการป้องกันประเทศกระทรวงกลาโหม พ.ศ.๒๕๖๐ – ๒๕๖๔ นอกจากนั้นยังมีหน่วยงานหลักที่ดำเนินการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกองทัพไทย ได้แก่ (๑) ศูนย์ไซเบอร์กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม กระทรวงกลาโหม (ศซบ.ทสอ.กห.) (๒) กองปฏิบัติการสงครามเครือข่าย สำนักปฏิบัติการ กรมยุทธการทหาร (กสค.สปก.ยก.ทหาร) และ (๓) กองรักษาความปลอดภัยสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร (กรส.ศทศ.สส.ทหาร) ซึ่งการปฏิบัติการในมิติไซเบอร์ของกองทัพไทยถือเป็นการปฏิบัติการทางทหารอย่างหนึ่งเพื่อรับมือกับภัยคุกคามรูปแบบใหม่ และสอดคล้องกับหน้าที่ของ

กองทัพไทยในการเตรียมกำลัง การป้องกันราชอาณาจักร และการดำเนินการเกี่ยวกับการใช้กำลังทางทหารในส่วน ของแนวทางการพัฒนากองทัพไทยด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่เป็นผลจากการศึกษาครั้งนี้ที่เสนอแนะต่อระดับนโยบาย ได้แก่ (๑) การสร้างความร่วมมือทางไซเบอร์ระหว่างประเทศทั้งในระดับภูมิภาคอาเซียน และระหว่างประเทศคู่เจรจานอกภูมิภาค (๒) การมีนโยบายรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (๓) การเชื่อมโยงการทำงานด้านไซเบอร์ในภาพรวมของกระทรวงกลาโหม ทั้งการปฏิบัติยามปกติและการปฏิบัติในสถานการณ์จริง และ (๔) บรรจุเรื่องไซเบอร์เข้าไปอยู่ในแผนป้องกันประเทศ ส่วนข้อเสนอแนะต่อระดับผู้ปฏิบัติที่มีความเกี่ยวข้องกับมิติด้านไซเบอร์ ได้แก่ (๑) การสร้างเครือข่ายไซเบอร์ในภาพรวม (๒) การสนับสนุนของหน่วยงานที่เกี่ยวข้อง (๓) ส่งเสริมให้หน่วยวิจัยที่เกี่ยวข้องของกองทัพผลิต Software/Hardware ทางไซเบอร์ขึ้นใช้เอง (๔) การฝึกร่วมกันระหว่างหน่วยงานด้านไซเบอร์ของกองทัพ (๕) นำเรื่องไซเบอร์บรรจุเป็นวิชาในหลักสูตรโรงเรียนทหารทุกระดับ ทุกเหล่าทัพ (๖) การเตรียมความพร้อมในการตอบสนองต่อสถานการณ์ฉุกเฉินได้ทันท่วงที และฟื้นคืนระบบกลับสู่ภาวะปกติโดยเร็วที่สุด (Cyber Resilience) (๗) การแบ่งปันข้อมูลระหว่างหน่วยงานในประเด็นที่เกี่ยวข้องกับไซเบอร์ (๘) การผลิตและพัฒนาบุคลากรด้านไซเบอร์ (๙) หน่วยงานทางด้านไซเบอร์ควรมีกระบวนการรับมือกับภัยคุกคามด้านไซเบอร์หลายรูปแบบ และ (๑๐) การสร้างความตระหนักรู้ (Awareness) ให้แก่กำลังพลและประชาชนทั่วไป

## เอกสารอ้างอิง

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

กระทรวงการต่างประเทศ. (๒๕๕๘). *ผลการประชุมสุดยอดอาเซียนครั้งที่ ๒๗ และการประชุมสุดยอดอื่น ๆ ที่เกี่ยวข้อง*.

กองทัพไทย. (๒๕๖๐). *นโยบาย ผบ.ทสส./ผบ.ศบท. ประจำปีงบประมาณ ๒๕๖๐*. (อัดสำเนา).

ไทยพับลิก้า. (๒๕๕๖). *เอ็ดเวิร์ด สโนว์เดน กับการเปิดโปง "พริซึมเกต"*. สืบค้นเมื่อ ๙ มกราคม ๒๕๖๐, จาก http://thaipublica.org/2013/06/edward-snowden-prism/

บวร เทศารินทร์. (๒๕๕๙). *ประเทศไทย ๔.๐ โมเดลเศรษฐกิจใหม่*. สืบค้นเมื่อ ๑ มกราคม ๒๕๕๙, จาก http://www.drborworn.com/articledetail.asp?id=16223

บีบีซี ไทย. (๒๕๖๐). *ฝรั่งเศสสกัดแผนโจมตีทางไซเบอร์ได้ ๒๔,๐๐๐ ครั้ง*. สืบค้นเมื่อ ๙ มกราคม ๒๕๕๙, จาก http://www.bbc.com/thai/international-38547157

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT). (๒๕๕๙). *สถิติภัยคุกคาม*. สืบค้นเมื่อ ๖ มกราคม ๒๕๖๐, จาก https://www.thaicert.or.th/statistics/statistics.html

เศรษฐพงศ์ มะลิสุวรรณ. (๒๕๕๙). *เปิดแนวคิด "เศรษฐพงศ์" ยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์*. สืบค้นเมื่อ ๒๒ พฤศจิกายน ๒๕๕๙, จาก http://www.manager.co.th/game/viewnews.aspx?NewsID=9590000070219