Graduate Review of Political Science and Public Administration Journal Vol. 4 No. 1 (2025): 29-60

การประกอบสร้างความมั่นคงปลอดภัยไซเบอร์ในอาเซียน: ระบอบแห่งความร่วมมือและความเป็นปฏิปักษ์[1]

ปวเรศ แผ่แสงจันทร์[2] และเอกลักษณ์ ไชยภูมี[3]

วันที่รับบทความ: 10 กุมภาพันธ์ 2568; วันที่แก้ไขล่าสุด: 22 มิถุนายน 2568; วันที่ตอบรับตีพิมพ์: 23 มิถุนายน 2568

บทคัดย่อ

งานวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาตัวแสดงที่เกี่ยวข้องกับการสร้างระบอบความมั่นคงปลอดภัยไซเบอร์ในภูมิภาคอาเซียน (ASEAN) และเพื่อศึกษาปัจจัยและที่มาของการบังคับใช้และการค้ำจุนระบอบความมั่นคงปลอดภัยไซเบอร์ใน ASEAN ผ่านวิธีการวิจัยเชิงคุณภาพด้วยการวิจัยทางเอกสาร โดยจากผลการวิจัยพบว่า ปัจจัยหลักที่เกี่ยวข้องกับกระบวนการสร้างระบอบความมั่นคงปลอดภัยไซเบอร์ในอาเซียน คือ ตัวแสดงที่สร้างความมั่นคง ได้แก่ รัฐสมาชิกอาเซียน องค์การระหว่างประเทศ และองค์การภาคประชาสังคม ซึ่งทำหน้าที่ในการกำหนดถึงสิ่งที่เป็นภัยคุกคามต่อความมั่นคงของภูมิภาค มีอิทธิพลต่อวาทกรรมด้านความมั่นคง และกำหนดแนวทางการแก้ไขปัญหาด้านความมั่นคงปลอดภัยทางไซเบอร์ของอาเซียน และอีกปัจจัยหนึ่ง คือ การตระหนักต่อภัยคุกคามที่มีร่วมกัน ซึ่งในกรณีนี้คือ ภัยคุกคามทางไซเบอร์ซึ่งเป็นประเด็นที่มีลักษณะข้ามชาติ มีการพัฒนาอยู่เสมอ และกลายเป็นภัยคุกคามที่สร้างผลกระทบต่ออาเซียนทั้งในแง่ของเศรษฐกิจและสังคม รวมถึงสร้างผลกระทบสืบเนื่องให้เกิดภัยคุกคามต่อความมั่นคงด้านอื่นๆ ทำให้อาเซียนจำเป็นต้องพัฒนาความร่วมมือในรูปแบบต่างๆ และทำให้เกิดระบอบความมั่นคงปลอดภัยไซเบอร์ของอาเซียนขึ้นมา อย่างไรก็ตาม ระบอบความมั่นคงปลอดภัยไซเบอร์อาเซียน ไม่ได้มีเพียงแค่ความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ แต่แฝงไว้ด้วยความเป็นปฏิปักษ์ด้านความมั่นคงปลอดภัยไซเบอร์ด้วยเช่นกัน ซึ่งเกิดขึ้นมาได้จากหลายปัจจัย ได้แก่ ความแตกต่างในการตีความ ความแตกต่างในการพัฒนา ความขัดแย้งทางการเมือง และบทบาทของมหาอำนาจภายนอกภูมิภาค โดยข้อเสนอแนะของงานวิจัยชิ้นนี้คือ อาเซียนมีความจำเป็นที่จะต้องมีแนวทางร่วมกันในการปรับตัวเพื่อรักษาความมั่นคงและเสถียรภาพ เพื่อให้ระบอบความมั่นคงปลอดภัยไซเบอร์ที่อาเซียนสถาปนาขึ้นสามารถพัฒนาและเติบโตต่อไปได้อย่างมั่นคง เข้มแข็ง และยั่งยืน ทั้งนี้ ผู้ที่มีความสนใจสามารถต่อยอดงานวิจัยชิ้นนี้ โดยศึกษาตัวแสดงที่สร้างความมั่นคงแบบเจาะลึกรายประเทศ หรือศึกษาตัวแสดงมหาอำนาจว่าได้เข้ามามีอิทธิพลและบทบาทในภูมิภาคอาเซียนอย่างไร

คำสำคัญ ความมั่นคงปลอดภัยไซเบอร์, อาเซียน, กระบวนการสร้างความมั่นคง, ความร่วมมือ, ความเป็นปฏิปักษ์

---

[1] บทความวิจัยเรื่องนี้เป็นส่วนหนึ่งของการศึกษาค้นคว้าอิสระ เรื่อง “การพัฒนาระบอบความมั่นคงปลอดภัยไซเบอร์ในภูมิภาคอาเซียน” หลักสูตรรัฐศาสตรมหาบัณฑิต สาขาวิชารัฐศาสตร์ มหาวิทยาลัยเกษตรศาสตร์

[2] คณะสังคมศาสตร์ มหาวิทยาลัยเกษตรศาสตร์ กรุงเทพฯ 10900 อีเมล: pavarate.p@ku.th

[3] คณะสังคมศาสตร์ มหาวิทยาลัยเกษตรศาสตร์ กรุงเทพฯ 10900 อีเมล: akekalak.c@ku.th

ASEAN Cybersecurity Securitization: Regime of Cooperation and Enmity[4]

Pavarate Phaesaengchan[5] and Akekalak Chaipumee[6]

Received: 10 February 2025; Revised: 22 June 2025; Accepted: 23 June 2025

Abstract

This research aims to examine the key actors involved in the construction of the cybersecurity regime in the ASEAN region, as well as to study the factors and origins that drive the enforcement and maintenance of this regime. The study employs qualitative research through documentary analysis. The findings reveal that the main factors contributing to the construction of the ASEAN cybersecurity regime include securitizing actors such as ASEAN member states, international organizations, and civil society organizations. These actors play a crucial role in defining what constitutes a threat to regional security, influencing security discourse, and shaping ASEAN's approach to addressing cybersecurity issues. Another key factor is the shared awareness of mutual threats, specifically, cyber threats which are transnational in nature, constantly evolving, and have significant impacts on both the economic and social dimensions of ASEAN. These threats also have cascading effects on other aspects of regional security, necessitating the development of various forms of cooperation within ASEAN and leading to the formation of the ASEAN cybersecurity regime. However, the ASEAN cybersecurity regime is not solely characterized by cooperation; it also embodies elements of cybersecurity enmity. This enmity arises from several factors, including the difference in interpretation, developmental disparities, political conflicts, and the involvement of external superpowers. The study suggests that ASEAN must develop a common approach to adapt in order to preserve regional security and stability, thus enabling its cybersecurity regime to grow in a stable, resilient, and sustainable manner. Future research can expand on this work by conducting in-depth studies of securitizing actors at the national level or by

[4] This research article is based on independent study, "Developing Cyber Security Regime in ASEAN". This thesis submitted in partial fulfillment of the requirements for the degree of Master of Arts in Political Science, Kasetsart University.

[5] Faculty of Social Sciences, Kasetsart University, Bangkok 10900. E-mail: pavarate.p@ku.th

[6] Faculty of Social Sciences, Kasetsart University, Bangkok 10900. E-mail: akekalak.c@ku.th

analyzing how external superpowers exert influence and play roles within the ASEAN's cybersecurity landscape.

Keywords Cybersecurity, ASEAN, Securitization, Cooperation, Enmity

1. บทนำ

อาเซียนเป็นหนึ่งในภูมิภาคที่มีจำนวนปริมาณผู้ใช้งานอินเทอร์เน็ตเติบโตเร็วที่สุดในโลก และมีประชากรกว่าครึ่งหนึ่งภายในภูมิภาคอาเซียนเป็นผู้ใช้สื่อสังคมออนไลน์ (Social Media) ทำให้อาเซียนเป็นหนึ่งในตลาดสังคมออนไลน์อันดับหนึ่งของโลก ซึ่งลักษณะของสังคมดิจิทัลในภูมิภาคก็ได้นำมาซึ่งผลประโยชน์ในทางเศรษฐกิจจำนวนมหาศาล โดยในเบื้องต้น มีการคาดการณ์ว่าภายในปี พ.ศ. 2568 (ค.ศ. 2025) จะมีปริมาณการซื้อขายสินค้าออนไลน์เพิ่มมากขึ้นเป็น 6 เท่า หรือมีมูลค่าประมาณ 200 พันล้านเหรียญสหรัฐ (Brandon, 2018)

การเติบโตดังกล่าวเป็นผลดีในแง่ของการเจริญเติบโตทางเศรษฐกิจของภูมิภาค แต่ทว่า สิ่งที่ตามมาจากการเติบโตอย่างรวดเร็วของผู้ใช้งานอินเทอร์เน็ต ไม่ได้มีเพียงการเกิดขึ้นของวิถีชีวิตสังคมออนไลน์ และความรุ่งเรืองของเศรษฐกิจดิจิทัลในภูมิภาคอาเซียนแต่เพียงอย่างเดียว แต่ยังได้ทำให้ภูมิภาคอาเซียนไม่อาจที่จะหลีกเลี่ยงที่จะต้องเผชิญหน้ากับภัยคุกคามความมั่นคงรูปแบบใหม่ (Non-traditional Threat) ที่ใช้งานเทคโนโลยีอินเทอร์เน็ตและคอมพิวเตอร์เป็นช่องทางหลักในการโจมตี นั่นคือ ภัยคุกคามทางไซเบอร์ (Cyber Threat) รวมไปถึงการก่ออาชญากรรมทางไซเบอร์ (Cyber Crime) อันเป็นปัญหาความมั่นคงที่มีลักษณะข้ามชาติหรือข้ามพรมแดน ซึ่งประเทศในภูมิภาคอาเซียนหลายประเทศได้รับผลกระทบจากภัยดังกล่าว โดยพบว่ามีเว็บไซต์ของกลุ่มประเทศสมาชิกอาเซียนประมาณ 270 แห่งได้ถูกโจมตีด้วยมัลแวร์ (Malware) และปรากฏข้อมูลว่าเซิร์ฟเวอร์กว่า 8,800 เครื่อง ถูกใช้เป็นเครื่องควบคุมและสั่งการมัลแวร์สำหรับใช้ในการโจมตีอีกด้วย เช่น กรณีการแพร่ระบาดของมัลแวร์ วอนนาคราย (WannaCry) เมื่อปี พ.ศ. 2560 (ค.ศ. 2017) ซึ่งเป็นการโจมตีผ่านระบบอีเมล (E-mail) เพื่อเรียกค่าไถ่ข้อมูลจากเจ้าของข้อมูล โดยปรากฏข้อมูลว่าประเทศไทยก็เป็นประเทศที่ตกเป็นเหยื่อและได้รับความเสียหายจากการโจมตีดังกล่าวเช่นเดียวกัน (ไทยพีบีเอส, 2560)

ด้วยเหตุนี้ เพื่อเป็นการตอบสนองและรับมือกับภัยคุกคามต่อความมั่นคงทางไซเบอร์ที่มีเพิ่มมากขึ้นเรื่อยๆ ในภูมิภาค ทำให้ประเทศสมาชิกอาเซียนจึงได้ริเริ่มสร้างแนวทางป้องกันภัยคุกคามทางไซเบอร์ภายในประเทศของตน ตลอดจนได้ขยายขอบเขตของความร่วมมือทั้งภายในประเทศและระหว่างประเทศกับรัฐอื่นๆ เพื่อสร้างกลไกในการรับมือและตอบสนองต่อภัยคุกคามรูปแบบใหม่ ซึ่งในกรณีนี้ คือ ภัยคุกคามต่อความมั่นคงทางไซเบอร์ เพราะภัยคุกคามทางไซเบอร์ได้กลายเป็นภัยคุกคามที่สร้างผลกระทบต่อความมั่นคงทั้งในรูปแบบดั้งเดิมและรูปแบบใหม่ของแต่ละประเทศอย่างไม่อาจควบคุมได้ นอกจากจะมีลักษณะข้ามชาติและยากที่จะป้องกันแล้ว ภัยคุกคามดังกล่าวยังมีความก้าวหน้าในการพัฒนาอย่างรวดเร็ว ดังนั้น นอกจากการที่แต่ละประเทศจะเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ของตัวเองแล้ว ยังมีความจำเป็นต้องประสานความร่วมมือและแลกเปลี่ยนความร่วมมือกับประเทศอื่นๆ เพื่อรับมือกับภัยคุกคามดังกล่าว

ทั้งนี้ การประสานความร่วมมือเพื่อตอบสนองต่อภัยคุกคามทางไซเบอร์ที่เกิดขึ้นภายในภูมิภาคอาเซียนก็ไม่ควรเป็นเพียงแค่การดำเนินการในลักษณะความร่วมมือระยะสั้นเพื่อแก้ไขปัญหาเฉพาะหน้าเท่านั้น แต่จำเป็นต้องคำนึงและพิจารณาถึงการวางรากฐาน หรือสถาปนากลไกความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ในระยะยาวของภูมิภาคเพื่อการรับมือกับภัยคุกคามในอนาคตและเตรียมความพร้อมในการรับมือกับภัยคุกคามรูปแบบต่างๆ ได้อย่างยั่งยืน อย่างไรก็ตาม การสถาปนาหรือพัฒนากลไกความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ในภูมิภาคอาเซียนก็อาจมีทั้งจุดเด่นและจุดด้อย ซึ่งเป็นผลมาจากแนวทางการดำเนินงานและข้อจำกัดอันเกิดมาจากรูปแบบการรวมกลุ่มของประเทศสมาชิกอาเซียน ด้วยเหตุนี้ จึงนำไปสู่ประเด็นปัญหาที่สำคัญของการวิจัย คือ อะไรคือปัจจัยที่เกื้อหนุนและเป็นอุปสรรคต่อภูมิภาคอาเซียน ในการพัฒนากลไกในการสถาปนาระบอบความมั่นคงปลอดภัยไซเบอร์ในภูมิภาค โดยจากการศึกษาพบว่า ระบอบความมั่นคงปลอดภัยไซเบอร์อาเซียนมีปัจจัยสำคัญคือ ตัวแสดงที่มีบทบาทในการประกอบสร้างความมั่นคงปลอดภัยไซเบอร์ ซึ่งมีอิทธิพลต่อแนวทางการกำหนดนโยบาย การบังคับใช้ และการค้ำจุนระบอบความมั่นคงปลอดภัยไซเบอร์ในภูมิภาคอาเซียน

2. วัตถุประสงค์ของการศึกษา

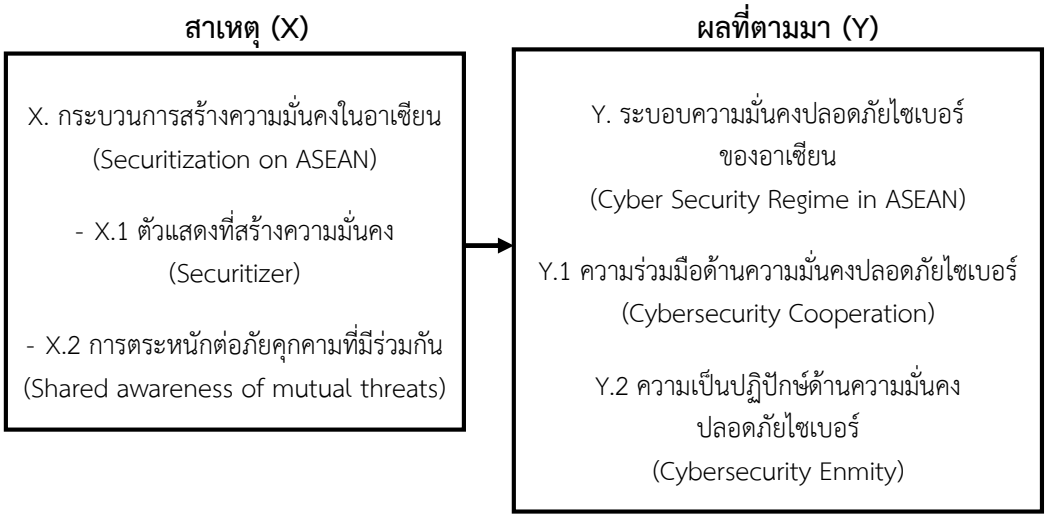
(1) เพื่อศึกษาตัวแสดงที่เกี่ยวข้องกับการสร้างระบอบความมั่นคงปลอดภัยไซเบอร์ในภูมิภาคอาเซียน

(2) เพื่อศึกษาปัจจัยและที่มาของการบังคับใช้และการค้ำจุนระบอบความมั่นคงปลอดภัยไซเบอร์ในภูมิภาคอาเซียน

3. สมมติฐานของการศึกษา

กลไกและระบอบความมั่นคงปลอดภัยไซเบอร์ของอาเซียนได้ถูกพัฒนาขึ้นในลักษณะมุ่งเน้นการตั้งรับ และตอบสนองต่อภัยคุกคามที่เกิดขึ้น มากกว่าดำเนินการเชิงรุกอันเป็นผลมาจากอิทธิพลของตัวแสดงที่มีบทบาทในการสร้างความมั่นคง (Securitizer) ของอาเซียน อย่างไรก็ตาม แม้ระบอบความมั่นคงปลอดภัยไซเบอร์ของอาเซียนจะเต็มไปด้วยความร่วมมือในระดับภูมิภาค แต่ก็ยังก็มีความเป็นปฏิปักษ์เกิดขึ้นระหว่างประเทศสมาชิกซึ่งเกิดจากปัจจัยสำคัญ ได้แก่ ความแตกต่างในการพัฒนา ความขัดแย้งทางการเมือง และบทบาทของมหาอำนาจภายนอก

4. กรอบแนวคิดในการทำวิจัย



5. การทบทวนวรรณกรรม

ในยุคที่ภัยคุกคามทางไซเบอร์มีลักษณะข้ามพรมแดนและซับซ้อนมากขึ้น ภูมิภาคเอเชียตะวันออกเฉียงใต้หรืออาเซียน (ASEAN) เผชิญกับความท้าทายในการสร้างระบอบความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพและมีความร่วมมือระหว่างรัฐสมาชิกมากขึ้น แม้จะมีการริเริ่มเชิงนโยบายและความพยายามทางเทคนิคเกิดขึ้นมากมายในช่วงทศวรรษที่ผ่านมา แต่การศึกษาด้านรัฐศาสตร์ที่วิเคราะห์บทบาทของ “ตัวแสดง” (Actors) และพลวัตเชิงสถาบันกลับยังมีจำนวนที่จำกัด บทความนี้มีวัตถุประสงค์เพื่อนำเสนอภาพรวมขององค์ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) ในอาเซียน พร้อมทั้งอภิปรายว่าการศึกษาตัวแสดงในกระบวนการสร้างระบอบความมั่นคงปลอดภัยไซเบอร์ของอาเซียนจะช่วยต่อยอดและสนทนากับช่องว่างทางวิชาการเดิมได้อย่างไร

วรรณกรรมที่ผ่านมาอธิบายถึงประเด็นเรื่องความมั่นคงปลอดภัยไซเบอร์ว่าเป็นประเด็นความมั่นคงในรูปแบบใหม่ หรือที่เรียกว่าความมั่นคงแบบไม่ดั้งเดิม (Non-Traditional Security) โดย Mely Caballero Anthony (2016) ได้อธิบายว่า ความมั่นคงแบบไม่ดั้งเดิม คือประเด็นความมั่นคงที่ท้าทายและส่งผลกระทบต่อความอยู่รอด ความอยู่ดีกินดีของประชาชนตลอดจนต่อรัฐ ที่เกิดขึ้นในลักษณะที่ต่างไปจากความมั่นคงแบบดั้งเดิมที่เกิดจากการใช้กำลังหรือทรัพยากรทางการทหารใดๆ และมีลักษณะข้ามชาติ รวมถึงเกิดในระยะเวลาที่สั้นและกระจายอย่างรวดเร็ว และ Robert W. Cox (1996) ได้อภิปรายว่า ความมั่นคงปลอดภัยไซเบอร์ ตลอดจนการรักษาความมั่นคงปลอดภัยทางไซเบอร์ระหว่างประเทศ เป็นประเด็นที่ดำรงอยู่และดำเนินการในฐานะโครงสร้างทางการเมืองและสังคม การระบุถึงประเด็นเรื่องความมั่นคงปลอดภัยทางไซเบอร์ระดับสากลที่ง่ายที่สุด คือการพูดถึงเรื่องของภัยคุกคามและตัวแสดงที่เป็นภัยคุกคามทางไซเบอร์

เพื่อเป็นการตอบสนองต่อประเด็นความมั่นคงแบบไม่ดั้งเดิมนี้ นักวิชาการจึงเริ่มนำแนวคิดของทฤษฎีการประกอบสร้างความมั่นคงหรือสำนักโคเปนเฮเกนมาประยุกต์ใช้กับความมั่นคงปลอดภัยทางไซเบอร์ เพื่อให้เข้าใจว่าเหตุใดภัยคุกคามจึงถูกสร้างขึ้นในลักษณะนี้ และผลลัพธ์ที่ตามมาของกระบวนการประกอบสร้างดังกล่าวคืออะไร (Hansen, 2012; Aradau, 2004) โดยนักวิชาการสำนักโคเปนเฮเกนพิจารณาประเด็นเรื่องความมั่นคงปลอดภัยไซเบอร์ในฐานะปัญหาความมั่นคงระดับชาติ (และระหว่างประเทศ) ดังนั้น จึงต้องมีกระบวนการประกอบสร้างความมั่นคง (Securitization) เพราะความมั่นคงเป็นปัจจัยสำคัญในการผลักดันประเด็นความมั่นคงให้เข้าสู่กระบวนการกำหนดนโยบาย กำหนดลักษณะของมาตรการรับมือ และสร้างแนวปฏิบัติที่สามารถนำมาใช้เพื่อต่อต้านภัยคุกคาม (Buzan, 1998)

อาเซียนเองก็เป็นหนึ่งในภูมิภาคที่ได้รับผลกระทบจากภัยคุกคามไซเบอร์ โดยการศึกษาความมั่นคงปลอดภัยไซเบอร์ในอาเซียนมีพัฒนาการที่หลากหลาย โดยมุ่งเน้นไปที่การศึกษาการจัดทำนโยบายระดับภูมิภาค เช่น ASEAN Cybersecurity Cooperation Strategy 2021-2025 ซึ่งให้ความสำคัญกับการพัฒนาโครงสร้างพื้นฐานทางไซเบอร์ การเสริมสร้างความร่วมมือระหว่างรัฐสมาชิก และการเพิ่มขีดความสามารถของบุคลากรในภูมิภาค (ASEAN, 2021) นอกจากนี้ ยังมีการศึกษาความร่วมมือระหว่างประเทศ เช่น ศูนย์ความร่วมมืออาเซียน-ญี่ปุ่น เพื่อพัฒนาบุคลากรความมั่นคงปลอดภัยไซเบอร์ (ASEAN-Japan Cybersecurity Capacity Building Centre: AJCCBC) ที่ร่วมมือกับกองทุนความร่วมมือญี่ปุ่น-อาเซียน (Japan-ASEAN Integration Fund: JAIF) ในการจัดอบรมและการแข่งขันเพื่อพัฒนาทักษะไซเบอร์ในระดับภูมิภาค (Japan-ASEAN Integration Fund, 2022)

วรรณกรรมที่ผ่านมาอภิปรายถึงลักษณะความร่วมมือของอาเซียนและข้อจำกัดของความร่วมมือในการรับมือกับภัยคุกคามไซเบอร์ เช่น Hitoshi Nasu et al. (2019) ได้อภิปรายว่า อาเซียนเป็นหนึ่งในองค์การระดับภูมิภาคแรกๆ ที่เริ่มมีส่วนร่วมในการเสริมสร้างศักยภาพด้านไซเบอร์ร่วมกันตั้งแต่ยุคเริ่มต้นของเทคโนโลยีสารสนเทศ ในขณะที่กรอบความร่วมมือด้านกฎหมายระหว่างประเทศยังคงอยู่ระหว่างการพัฒนา อาเซียนต้องรับมือกับประเด็นความมั่นคงปลอดภัยไซเบอร์ในมิติต่างๆ ภายใต้บริบทของสถานการณ์ทางสังคมและการเมืองที่มีอยู่ การแข่งขันทางภูมิรัฐศาสตร์ และช่องว่างทางดิจิทัล (Digital Divide) หรือ Caitríona H. Heinl (2013) ก็ได้ตั้งข้อสังเกตว่าความพยายามของอาเซียนในการสร้างกรอบการทำงานระดับภูมิภาคด้านความมั่นคงปลอดภัยไซเบอร์นั้น ยังคงดำเนินไปอย่างไม่เป็นระบบและขาดการบูรณาการ อันเป็นข้อบ่งชี้ถึงการขาดความเหนียวแน่นในระดับภูมิภาค ซึ่งเป็นผลมาจากสถานการณ์ทางสังคมและการเมืองที่มีอยู่เดิมของแต่ละประเทศ

วรรณกรรมอื่นๆ ในแวดวงรัฐศาสตร์ โดยเฉพาะด้านความสัมพันธ์ระหว่างประเทศ (International Relations) และความมั่นคงศึกษา (Security Studies) มีการตั้งคำถามว่า “ใคร” คือผู้มีบทบาทสำคัญในการกำหนดกฎระเบียบไซเบอร์ระดับภูมิภาค การให้ความสำคัญเฉพาะบทบาทของรัฐในฐานะตัวแสดงผู้ควบคุมนโยบายมักไม่เพียงพอ งานของ Nye (2010) และ Deibert (2013) ชี้ให้เห็นถึงความสำคัญของตัวแสดงที่ไม่ใช่รัฐ (Non-State Actors) เช่น

บริษัทเทคโนโลยี องค์กรพหุภาคี ภาคประชาสังคม และองค์การระหว่างประเทศ ในการร่วมกำหนด “norms” หรือบรรทัดฐานความมั่นคงไซเบอร์ โดยในบริบทของอาเซียน การศึกษาส่วนใหญ่มีช่องว่างสำคัญอยู่ที่การไม่สามารถอธิบายพลวัตของการสร้าง “ระบอบ” (Regime) ความมั่นคงปลอดภัยไซเบอร์ได้อย่างรอบด้าน

บทความนี้จึงได้ดำเนินการศึกษาและวิเคราะห์กระบวนการสร้างความมั่นคงในอาเซียนผ่านการศึกษาตัวแสดงที่สร้างความมั่นคง ได้แก่ รัฐสมาชิกอาเซียน องค์การระหว่างประเทศ และองค์การภาคประชาสังคม รวมถึงการตระหนักต่อภัยคุกคามที่มีร่วมกัน (Shared awareness of mutual threats) ซึ่งมีผลต่อการสถาปนาระบอบความมั่นคงปลอดภัยไซเบอร์ของอาเซียน ซึ่งเต็มไปด้วยความร่วมมือ (Cooperation) และความเป็นปฏิปักษ์ (Enmity) ด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งการศึกษาครั้งนี้สามารถตอบสนองต่อช่องว่างทางวิชาการเดิมได้หลายมิติ ทั้งการต่อยอดการวิเคราะห์เชิงเปรียบเทียบบทบาทของตัวแสดงรัฐและตัวแสดงที่ไม่ใช่รัฐ ซึ่งจะช่วยให้เราเข้าใจพัฒนาการของ “Cyber Norms” ในระดับภูมิภาคที่มีพลวัตเฉพาะของอาเซียน รวมถึงจะไปมีส่วนร่วมในการสนทนาและอธิบายว่าความร่วมมือด้านความมั่นคงปลอดภัยทางไซเบอร์ในอาเซียนไม่ได้เกิดจากการมีผลประโยชน์ร่วมกันเท่านั้น แต่ยังสะท้อนถึงอัตลักษณ์ ความเชื่อ ความไว้วางใจ หรือแม้กระทั่งความเป็นปฏิปักษ์ระหว่างรัฐสมาชิกอาเซียน นอกจากนี้ การศึกษานี้ได้เสนอความเป็นไปได้ในการท้าทาย หักล้าง หรือตั้งคำถามต่อข้อสันนิษฐานเดิมของงานศึกษาด้านรัฐศาสตร์ของอาเซียน ซึ่งมองว่าอาเซียนสามารถพัฒนาไปสู่ภูมิภาคแห่งความร่วมมือทางไซเบอร์ได้อย่างมีประสิทธิภาพ เพราะจากการศึกษาครั้งนี้พบว่าอาเซียนยังมีความแตกต่างทางนโยบาย ความไม่สมดุลทางการพัฒนาและประเด็นทางการเมืองที่ขัดขวางความร่วมมือดังกล่าว ซึ่งจะช่วยเปิดพื้นที่สำหรับการศึกษาในอนาคตให้สามารถวิเคราะห์ประเด็นด้านความมั่นคงปลอดภัยไซเบอร์ในฐานะ “การเมืองระหว่างประเทศ” ในโลกดิจิทัล

6. วิธีการศึกษา

การศึกษาวิจัยเรื่อง การพัฒนาระบอบความมั่นคงปลอดภัยไซเบอร์ในภูมิภาคอาเซียน เป็นการศึกษาวิจัยที่ใช้วิธีการวิจัยเชิงคุณภาพ (Qualitative Research) ด้วยการวิจัยทางเอกสาร (Documentary Research) โดยมีวิธีการศึกษาคือ การวิเคราะห์เอกสาร งานวิจัย บทความ เอกสารวิชาการ ตำรา และเว็บไซต์ข้อมูลของหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและเอกชน ในรูปแบบทั้งภาษาไทยและภาษาอังกฤษ โดยเพื่อให้งานวิจัยมีความครอบคลุมตรงตามวัตถุประสงค์ของการวิจัย ผู้วิจัยจึงใช้การศึกษาวิจัยเอกสารครอบคลุมทั้งเอกสารชั้นต้น (Primary Data) และเอกสารชั้นรอง (Secondary Data)

7. ผลการวิจัยและอภิปรายผล

7.1 ตัวแสดงที่เกี่ยวข้องกับการสร้างระบอบความมั่นคงปลอดภัยไซเบอร์ใน ASEAN

7.1.1 ตัวแสดงที่สร้างความมั่นคง

ความมั่นคงในภูมิภาคเอเชียตะวันออกเฉียงใต้หรืออาเซียนเป็นประเด็นที่มีความสำคัญอย่างยิ่งในบริบทของการเมืองระหว่างประเทศ โดยเฉพาะอย่างยิ่งเมื่อพิจารณาถึงการเปลี่ยนแปลงและความไม่แน่นอนที่เกิดขึ้นในหลายพื้นที่ทั่วโลก ดังนั้น การสร้างความมั่นคงในอาเซียนจึงมีความจำเป็นต้องพึ่งพาตัวแสดงที่มาทำหน้าที่แสดงบทบาทนำในการสร้างความมั่นคง ซึ่งช่วยในการกำหนดและโน้มน้าวให้ประชาชนหรือรัฐต่างๆ สามารถรับรู้ถึงภัยคุกคามต่อความมั่นคงของภูมิภาค ตัวแสดงเหล่านี้มีอิทธิพลต่อวาทกรรมด้านความมั่นคงและการกำหนดแนวทางการแก้ไขปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ของภูมิภาคอาเซียน ตลอดจนมีบทบาทในการส่งเสริมเสถียรภาพและสันติภาพในภูมิภาค โดยตัวแสดงหลักที่มีส่วนสำคัญในการสร้างความมั่นคงในอาเซียน ได้แก่ รัฐสมาชิกอาเซียน องค์การระหว่างประเทศ และองค์การภาคประชาสังคม

(1) รัฐสมาชิกอาเซียน (ASEAN Member States)

อาเซียนประกอบด้วยรัฐสมาชิก 10 ประเทศ ได้แก่ บรูไน กัมพูชา อินโดนีเซีย ลาว มาเลเซีย พม่าหรือเมียนมา ฟิลิปปินส์ สิงคโปร์ ไทย และเวียดนาม ซึ่งทั้ง 10 ประเทศต่างก็มีบทบาทสำคัญในการส่งเสริมการประกอบสร้างความมั่นคงของอาเซียน เนื่องจากรัฐสมาชิกอาเซียนแต่ละประเทศมีการดำเนินนโยบายภายในประเทศที่เสริมสร้างความมั่นคง อาทิ การพัฒนากองทัพ การป้องกันการก่อการร้าย การต่อต้านอาชญากรรมข้ามชาติ ตลอดจนการรับมือกับภัยคุกคามทางไซเบอร์ เช่น ประเทศไทยที่ได้มีการพัฒนาพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และดำเนินการจัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ประเทศสิงคโปร์ที่ได้มีการจัดทำพระราชบัญญัติด้านความมั่นคงปลอดภัยไซเบอร์ และจัดตั้งศูนย์ความเป็นเลิศด้านความมั่นคงปลอดภัยไซเบอร์อาเซียน-สิงคโปร์ (ASEAN-Singapore Cybersecurity of Excellence) และประเทศอินโดนีเซียที่ได้จัดตั้งสำนักงานความมั่นคงไซเบอร์และการเข้ารหัสแห่งชาติ ซึ่งนโยบายด้านความมั่นคงของแต่ละประเทศมักสอดคล้องกับนโยบายของประเทศอื่นในภูมิภาคแบบภาพรวม เพราะรัฐสมาชิกอาเซียนมักจะดำเนินการใช้กลไกการทูตเชิงป้องกัน (Preventive Diplomacy) ผ่านการเจรจาและการพบปะหารือในเวทีต่างๆ เพื่อแลกเปลี่ยนข้อมูลระหว่างกัน โดยมีเวทีสำคัญในการหารือประเด็นเรื่องความมั่นคงปลอดภัยไซเบอร์ของรัฐสมาชิกอาเซียน อาทิ การประชุมรัฐมนตรีอาเซียนด้านดิจิทัล (ASEAN Digital Ministers Meeting: ADGMIN) และการประชุมคณะกรรมการประสานงานด้านความมั่นคงปลอดภัยไซเบอร์อาเซียน (ASEAN Cybersecurity Coordinating Committee หรือ ASEAN Cyber – CC) ซึ่งได้ช่วยส่งเสริมให้พื้นที่ทางไซเบอร์ของอาเซียนอยู่บนพื้นฐานของกฎหมายและความร่วมมือในการดำเนินงานโดยความสมัครใจ (Ghosh, 2019) ด้วยเหตุนี้ รัฐสมาชิกอาเซียนจึงเป็นตัวแสดงหลักที่มีบทบาทสำคัญในการสร้างความมั่นคงในภูมิภาคเอเชียตะวันออกเฉียงใต้ ด้วยการดำเนินนโยบาย

และการสร้างความร่วมมือในด้านต่างๆ ทั้งด้านการทหาร การเมือง เศรษฐกิจ และสังคม ซึ่งการมีส่วนร่วมของรัฐสมาชิกอาเซียนก็จะช่วยส่งเสริมให้เกิดเสถียรภาพ และสันติภาพภายในภูมิภาค

อย่างไรก็ตาม แต่ละประเทศสมาชิกอาเซียนก็มี “ระบอบ” ที่แตกต่างกัน ทำให้มีมุมมองหรือการรับรู้ (Perceive) ต่อประเด็นปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ที่แตกต่างกัน โดยประเทศที่มีระบอบการปกครองแบบเผด็จการหรือกึ่งเผด็จการ มักมุ่งเน้นการควบคุมข้อมูลข่าวสารและป้องกันภัยคุกคามที่อาจส่งผลกระทบต่อความมั่นคงของรัฐตน เช่น การจัดการกับข้อมูลที่อาจนำไปสู่ความไม่สงบภายในประเทศ การปราบปรามความคิดเห็นที่วิพากษ์วิจารณ์รัฐบาล และการออกกฎหมายควบคุมการใช้อินเทอร์เน็ต อาทิ เมียนมา ซึ่งได้มีการบังคับใช้กฎหมายความมั่นคงทางไซเบอร์ฉบับใหม่ โดยตั้งเป้าไปที่การควบคุมเสรีภาพในการแสดงความคิดเห็นทางดิจิทัล มีบทลงโทษผู้ที่ใช้บริการ VPN หรือเครือข่ายส่วนตัวเสมือน (Virtual Private Network) ซึ่งเป็นช่องทางสำคัญในการระดมทุนของกลุ่มต่อต้านรัฐประหาร การแชร์ข้อมูลสิ่งที่เกิดขึ้นภายในประเทศ ไปจนถึงการวิพากษ์วิจารณ์รัฐบาลเมียนมาในพื้นที่อินเทอร์เน็ต (The Irrawaddy, 2022) ในขณะที่ประเทศที่มีระบอบประชาธิปไตย มักให้ความสำคัญกับการสร้างสมดุลระหว่างเสรีภาพในการแสดงความคิดเห็นและการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยสนับสนุนการมีส่วนร่วมของทั้งองค์การนานาชาติและภาคประชาสังคมในการพัฒนากฎหมาย อาทิ กฎหมายคุ้มครองข้อมูลส่วนบุคคลของอินโดนีเซีย (PDP Law) ซึ่งได้มีการปรับใช้หลักการมาจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป หรือ General Data Protection Regulation (GDPR) (ASEAN Briefing, 2024)

(2) องค์การระหว่างประเทศ (International Organizations)

นอกเหนือจากความร่วมมือระหว่างรัฐสมาชิก อาเซียนยังมีความร่วมมือกับองค์การระหว่างประเทศหลายแห่ง ซึ่งมีส่วนช่วยสนับสนุนการสร้างความมั่นคงในภูมิภาค ทั้งในด้านการป้องกันและแก้ไขปัญหาความขัดแย้ง และการรับมือภัยคุกคามรูปแบบใหม่ อย่างภัยคุกคามทางไซเบอร์ นอกจากนี้ อาเซียนยังมีกลไกความร่วมมือกับประเทศนอกภูมิภาค เช่น จีน ญี่ปุ่น เกาหลีใต้ สหรัฐอเมริกา และรัสเซีย ผ่านเวทีเจรจาต่างๆ เช่น การประชุมสุดยอดเอเชียตะวันออก (East Asia Summit: EAS) และกรอบการประชุมอาเซียนว่าด้วยความร่วมมือด้านการเมืองและความมั่นคงในภูมิภาคเอเชีย - แปซิฟิก (ASEAN Regional Forum: ARF) ซึ่งล้วนแล้วแต่ก็มีบทบาทสำคัญในการสนับสนุนเสถียรภาพในภูมิภาค โดยตัวอย่างองค์การระหว่างประเทศที่เกี่ยวข้องกับการสร้างความมั่นคงปลอดภัยทางไซเบอร์ของอาเซียน อาทิ องค์การสหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union: ITU) ซึ่งเป็นหนึ่งในคู่เจรจาของ ADGMIN สนับสนุนอาเซียนในด้านการพัฒนานโยบายไซเบอร์ระดับชาติ และเป็นองค์การที่ดำเนินการจัดทำดัชนีความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index) องค์การตำรวจอาชญากรรมระหว่างประเทศ (INTERPOL) ซึ่งมีบทบาทในการประสานงานกับตำรวจประเทศสมาชิกอาเซียน รวมถึงสนับสนุนการสืบสวนคดีอาชญากรรมไซเบอร์ระดับนานาชาติ และองค์การ Asia-Pacific Computer Emergency

Response Team (APCERT) ซึ่งทำหน้าที่สนับสนุนการแลกเปลี่ยนข้อมูลการโจมตีไซเบอร์และการประสานงานกรณีฉุกเฉินในภูมิภาคเอเชียแปซิฟิก โดยมีหลายประเทศอาเซียน เช่น สิงคโปร์ ไทย มาเลเซีย และอินโดนีเซีย เป็นสมาชิก

ด้วยเหตุนี้ จึงกล่าวได้ว่า องค์การระหว่างประเทศ เป็นหนึ่งในตัวแสดงที่มีบทบาทสำคัญในการสร้างความมั่นคงในภูมิภาคเอเชียตะวันออกเฉียงใต้ ผ่านการสนับสนุนและความร่วมมือในด้านต่างๆ ทั้งในระดับ ทวิภาคีและพหุภาคี องค์การระหว่างประเทศมีบทบาทสำคัญในการส่งเสริมความมั่นคงในอาเซียนผ่านการสนับสนุนด้านต่างๆ เช่น การพัฒนาเศรษฐกิจ การส่งเสริมสิทธิมนุษยชน การแก้ไขปัญหาความขัดแย้ง และการเสริมสร้างศักยภาพทางการทหาร การมีส่วนร่วมขององค์การระหว่างประเทศช่วยเสริมสร้างเสถียรภาพและสันติภาพในภูมิภาคอาเซียน และเป็นกลไกสำคัญในการสร้างความร่วมมือระหว่างประเทศสมาชิกในการรับมือกับความท้าทายและโอกาสที่เกิดขึ้นในภูมิภาคและในระดับโลก โดยองค์การระหว่างประเทศที่มีบทบาทสำคัญที่สุดในภูมิภาคนี้ ได้แก่ สมาคมประชาชาติแห่งเอเชียตะวันออกเฉียงใต้ (Association of Southeast Asian Nations หรือเรียกโดยย่อว่า ASEAN)

สมาคมประชาชาติแห่งเอเชียตะวันออกเฉียงใต้ หรืออาเซียนมีบทบาทสำคัญในการส่งเสริมและประสานงานเพื่อสร้างความมั่นคงในภูมิภาคเอเชียตะวันออกเฉียงใต้ โดยทำหน้าที่เป็นศูนย์กลางในการจัดการและประสานงานด้านนโยบายและกิจกรรมต่างๆ ของอาเซียน เพื่อให้รัฐสมาชิกสามารถดำเนินการตามพันธกรณีและข้อตกลงร่วมกันได้อย่างมีประสิทธิภาพ โดยอาเซียนได้กำหนดให้อาชญากรรมไซเบอร์เป็นภัยคุกคามความมั่นคงที่เป็นส่วนหนึ่งของอาชญากรรมข้ามชาติที่สำคัญภายใต้ประชาคมการเมืองและความมั่นคงของอาเซียน และประเด็นเรื่องความมั่นคงปลอดภัยไซเบอร์ได้ถูกจัดให้เป็นวาระสำคัญภายใต้การประชุมระดับรัฐมนตรีอาเซียนว่าด้วยอาชญากรรมข้ามชาติ (ASEAN Ministerial Meeting on Transnational Crime: AMMTC) และการประชุมรัฐมนตรีอาเซียนด้านดิจิทัล (ADGMIN) รวมถึงได้มีการจัดตั้งคณะกรรมการประสานงานด้านความมั่นคงปลอดภัยไซเบอร์ (ASEAN Cyber – CC) เพื่อเป็นตัวการประสานงานด้านความมั่นคงปลอดภัยไซเบอร์ระหว่างกรอบการประชุมต่างๆ ของอาเซียนอีกด้วย (ASEAN Secretariat, n.d.)

พื้นที่การประชุมของอาเซียน ได้กลายเป็นเวทีสำคัญในการหารือเกี่ยวกับภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ของทหาร โดยเฉพาะอย่างยิ่งผ่านการจัดการประชุมรัฐมนตรีกลาโหมอาเซียน (ASEAN Defence Ministers' Meeting) หรือ ADMM ซึ่งนิยมจัดควบคู่ไปกับการประชุมหารือกับประเทศมหาอำนาจนอกภูมิภาคอาเซียนด้วย แม้จะมีรากฐานความร่วมมือด้านความมั่นคงปลอดภัยมาจากที่ระบุไว้ในแถลงการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ของ ARF เมื่อปี ค.ศ. 2006 (ARF Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyber Space) แต่แถลงการณ์ว่าด้วยความร่วมมือในการสร้างความมั่นคงปลอดภัยไซเบอร์ของ ARF เมื่อปี ค.ศ. 2012 (ARF Statement on Cooperation in Ensuring Cyber Security) ก็เป็นการยอมรับโดยปริยายถึงความสัมพันธ์ที่เพิ่มขึ้นระหว่างพื้นที่ไซเบอร์สเปซกับข้อห่วงกังวลด้านความมั่นคงของชาติ เมื่อเดือน

สิงหาคม 2013 ณ การประชุมรัฐมนตรีกลาโหมอาเซียนกับรัฐมนตรีกลาโหมประเทศคู่เจรจา (ASEAN Defence Ministers' Meeting-Plus) หรือ ADMM-Plus ครั้งที่ 2 รัฐมนตรีกลาโหมของอาเซียนและประเทศคู่เจรจา 8 ประเทศได้หารือกันถึงบทบาทของภาคกลาโหมในการจัดการกับภัยคุกคามด้านความปลอดภัยที่ไม่ใช่แบบดั้งเดิมที่เกิดขึ้นใหม่ รวมถึงความมั่นคงปลอดภัยไซเบอร์ และต่อมาในเดือนพฤษภาคม ค.ศ. 2016 รัฐมนตรีกลาโหมอาเซียนได้รับรองเอกสารแนวคิดเกี่ยวกับการจัดตั้งคณะทำงานผู้เชี่ยวชาญ ADMM - Plus ด้านความมั่นคงปลอดภัยไซเบอร์ (Concept Paper on the Establishment of the ADMM - Plus Experts' Working Group on Cyber Security) ซึ่งมุ่งเน้นเฉพาะประเด็นด้านความมั่นคงปลอดภัยทางไซเบอร์ที่เกี่ยวข้องกับภาคกลาโหมและการทหาร (ASEAN Regional Forum, 2006, 2012)

อาเซียนยังมีบทบาทนำในการเป็นสื่อกลางขยายความร่วมมือด้านความมั่นคงปลอดภัยทางไซเบอร์ระหว่างประเทศสมาชิกอาเซียนกับประเทศคู่เจรจาอีกหลายประเทศ โดยเฉพาะอย่างยิ่งความร่วมมือกับสาธารณรัฐประชาชนจีน ญี่ปุ่น และสาธารณรัฐเกาหลี โดยได้มีการจัดการประชุมระดับรัฐมนตรีอาเซียน+3 ด้านอาชญากรรมข้ามชาติ (AMMTC+3) เพื่อเป็นเวทีให้ที่ประชุมได้ร่วมกันแลกเปลี่ยนมุมมองและแนวทางในการพัฒนาความร่วมมือเพื่อร่วมกันจัดการปัญหาอาชญากรรมข้ามชาติในภูมิภาค ทั้งในด้านข้อมูลข่าวสาร ประสบการณ์ และการปฏิบัติจริง รวมถึงสนับสนุนการพัฒนาศักยภาพของหน่วยงานด้านการบังคับใช้กฎหมายของประเทศสมาชิกอาเซียน นอกจากนี้ อาเซียนได้สร้างความร่วมมือในระดับทวิภาคีกับประเทศคู่เจรจาเพื่อให้เกิดการหารือกันอย่างใกล้ชิดในประเด็นเกี่ยวกับการจัดการปัญหาอาชญากรรมไซเบอร์ ตัวอย่างที่ชัดเจนคือ ความร่วมมือระหว่างอาเซียนกับญี่ปุ่น โดยได้มีการจัดตั้งศูนย์ความร่วมมืออาเซียน-ญี่ปุ่นเพื่อพัฒนาบุคลากรด้านความมั่นคงทางไซเบอร์ตามมติของที่ประชุมรัฐมนตรีอาเซียนด้านโทรคมนาคมและเทคโนโลยีสารสนเทศกับญี่ปุ่น นอกจากนี้ ทั้งสองฝ่ายได้ร่วมกันออกแถลงการณ์ร่วมเพื่อส่งเสริมความร่วมมือด้านการต่อต้านการก่อการร้าย และอาชญากรรมข้ามชาติ พร้อมทั้งยืนยันว่าจะส่งเสริมความมั่นคงปลอดภัยของการใช้เทคโนโลยีสารสนเทศและการสื่อสาร และต่อต้านอาชญากรรมไซเบอร์ในทุกรูปแบบ (ASEAN-Japan Cybersecurity Capacity Building Centre, 2023)

อาเซียนยังได้มีการดำเนินการจัดทำตราสารอาเซียน และเอกสารความร่วมมือต่างๆ เพื่อส่งเสริม การรับมือกับปัญหาภัยคุกคามต่อความมั่นคงปลอดภัยทางไซเบอร์ "อาเซียน" ในฐานะองค์การที่ประกอบด้วยรัฐสมาชิก ได้กลายเป็นผู้มีอำนาจตัดสินใจในการริเริ่ม อนุมัติ และลงนามในตราสารและเอกสารความร่วมมือต่างๆ โดยมีสำนักเลขาธิการอาเซียน ทำหน้าที่เป็นกลไกสนับสนุนหลักในการประสานงาน อำนวยความสะดวก จัดทำร่างเอกสาร (ในบางกรณี) และเก็บรักษาเอกสารเหล่านั้น เพื่อให้กระบวนการทำงานของอาเซียนเป็นไปอย่างราบรื่นและมีประสิทธิภาพ ซึ่งตัวเอกสารก็มีทั้งในรูปแบบปฏิญญา ยุทธศาสตร์ความร่วมมือ และข้อเสนอแนะหรือแนวทางของประเทศสมาชิกอาเซียนเพื่อรับมือกับปัญหาภัยคุกคามทางไซเบอร์ โดยตัวอย่างเอกสารที่สำคัญ อาทิ ปฏิญญาอาเซียนว่าด้วยการป้องกันและต่อต้านอาชญากรรมไซเบอร์ (ASEAN Declaration to Prevent and Combat Cybercrime) ซึ่งมี

วัตถุประสงค์ในการสนับสนุนกรอบการทำงานระดับภูมิภาคเพื่อสร้างความร่วมมือระหว่างประเทศสมาชิกอาเซียนและกำหนดแผนปฏิบัติการระดับชาติในการป้องกันและต่อต้านอาชญากรรมทางไซเบอร์ ยกระดับความร่วมมือระหว่างอาเซียนและประเทศคู่เจรจา รวมทั้งหน่วยงานและองค์กรที่เกี่ยวข้องทั้งในระดับภูมิภาคและนานาชาติ เช่น องค์การตำรวจสากล นอกจากนี้ ปฏิญญาดังกล่าวยังมีวัตถุประสงค์ในการเสริมสร้างความมั่นคงทางเทคโนโลยี และการพัฒนาขีดความสามารถของอาเซียนในการต่อสู้กับอาชญากรรมทางไซเบอร์ (ASEAN Secretariat, 2017) และอีกหนึ่งเอกสารที่มีความสำคัญ ได้แก่ ยุทธศาสตร์ความร่วมมืออาเซียนด้านความมั่นคงปลอดภัยไซเบอร์ ค.ศ. 2021-2025 (ASEAN Cybersecurity Cooperation Strategy 2021-2025) ซึ่งมีวัตถุประสงค์เพื่อมุ่งสนับสนุนการจัดตั้งระเบียบพหุภาคี โดยใช้กฎเกณฑ์เป็นฐานสำหรับโลกไซเบอร์ที่เปิดกว้าง มีความปลอดภัย มีเสถียรภาพ เข้าถึงได้ มีความเชื่อมโยงและสันติ ผ่านการนำบรรทัดฐานของรัฐ ในเรื่องความรับผิดชอบบนโลกไซเบอร์ไปปฏิบัติอย่างเป็นรูปธรรม การสร้างมาตรการความไว้เนื้อเชื่อใจ รวมถึงการส่งเสริมความร่วมมือระหว่างประเทศสมาชิกอาเซียน และอาเซียนกับคู่เจรจาในการพัฒนาศักยภาพของบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ (ASEAN Secretariat, n.d.)

(3) องค์การภาคประชาสังคม (Civil Society Organizations: CSOs)

องค์การภาคประชาสังคมที่มีบทบาทนำในภูมิภาคอาเซียน ประกอบด้วย องค์การพัฒนาเอกชน (NGOs) รวมไปถึงกลุ่มนักวิชาการ สื่อมวลชน และกลุ่มประชาชนทั่วไป ซึ่งได้เข้ามามีส่วนร่วมในการส่งเสริมความมั่นคงของภูมิภาค ผ่านการสร้างความตระหนักรู้เกี่ยวกับประเด็นต่างๆ เช่น สิทธิมนุษยชน ความเท่าเทียมทางเพศ การพัฒนาเศรษฐกิจและสังคม การจัดการทรัพยากรธรรมชาติ หรือการแก้ไขปัญหาความขัดแย้งในระดับท้องถิ่นและระดับภูมิภาค ตลอดจนความมั่นคงปลอดภัยไซเบอร์ โดยองค์การภาคประชาสังคมทำงานควบคู่กับภาครัฐ องค์การระหว่างประเทศ และชุมชนท้องถิ่นในการเสริมสร้างความมั่นคงทั้งในด้านการเมือง สังคม และเศรษฐกิจ การมีส่วนร่วมของภาคประชาสังคมช่วยให้ประชาชนมีส่วนร่วมในการกำหนดทิศทางของนโยบายความมั่นคง และเป็นกลไกในการตรวจสอบและถ่วงดุลอำนาจของรัฐ กล่าวได้ว่า องค์การภาคประชาสังคมได้เข้ามามีบทบาทหลักในการส่งเสริมความมั่นคงในอาเซียนหลายประการ

องค์กรภาคประชาสังคมเข้ามามีบทบาทสำคัญในการส่งเสริมความมั่นคงปลอดภัยทางไซเบอร์ในภูมิภาคอาเซียน โดยมุ่งเน้นการให้ความรู้ การฝึกอบรม และการสนับสนุนด้านความปลอดภัยดิจิทัลแก่เยาวชน กลุ่มเปราะบาง และบุคลากรภาคประชาสังคม โดยมีตัวอย่างการดำเนินงานขององค์กรภาคประชาสังคม อาทิ มูลนิธิอาเซียน (ASEAN Foundation) ซึ่งได้ริเริ่มโครงการ ASEAN Cybersecurity Skilling Programme ร่วมกับ Microsoft โดยมีเป้าหมายเพื่อให้ความรู้ด้านความปลอดภัยทางไซเบอร์ในระดับเบื้องต้นแก่เยาวชนในกลุ่มประเทศอาเซียน โดยเฉพาะอย่างยิ่งกลุ่มเยาวชนที่ขาดโอกาสในการเข้าถึงเทคโนโลยี เช่น เยาวชนชนเผ่า เยาวชนผู้พิการ เยาวชนจากชุมชนแออัด และเยาวชนผู้มีความหลากหลายทางเพศ (LGBT) เพื่อเสริมสร้างความรู้และทักษะด้านความปลอดภัย

ไซเบอร์ในยุคดิจิทัลที่เชื่อมโยงกันอย่างกว้างขวาง (ASEAN Foundation, 2023) หรือ UN Women และ UN University Institute in Macau (UNU Macau) ซึ่งได้ร่วมกันพัฒนาโมดูลการเรียนรู้ออนไลน์ด้านความมั่นคงปลอดภัยทางดิจิทัลสำหรับองค์กรภาคประชาสังคมหญิงและผู้ปกป้องสิทธิมนุษยชนหญิงในภูมิภาคเอเชียตะวันออกเฉียงใต้ โดยมุ่งเน้นการเสริมสร้างความรู้และทักษะด้านความมั่นคงปลอดภัยทางดิจิทัล เพื่อปกป้องสตรีและบุคคลที่มีอัตลักษณ์ทางเพศหลากหลายจากภัยคุกคามออนไลน์ (Albahri, 2023) นอกจากนี้ องค์การภาคประชาสังคมยังมีอิทธิพลในการกำหนดมาตรฐานด้านเทคนิคและส่งเสริมนโยบายที่คำนึงถึงสิทธิมนุษยชน ซึ่งอาจขัดแย้งกับแนวทางของบางรัฐสมาชิกที่เน้นการควบคุมมากกว่าความโปร่งใส (Tan, 2022)

จะเห็นได้ว่า ความมั่นคงในภูมิภาคอาเซียนไม่ได้เกิดขึ้นจากการกระทำของรัฐใดรัฐหนึ่งเพียงอย่างเดียว แต่เป็นผลจากความร่วมมือของตัวแสดงหลากหลายกลุ่ม ตั้งแต่รัฐสมาชิกอาเซียน องค์การระหว่างประเทศ ไปจนถึงองค์การภาคประชาสังคม การสร้างความมั่นคงในภูมิภาคจึงต้องอาศัยการมีส่วนร่วมของทุกฝ่ายอย่างต่อเนื่อง การส่งเสริมความร่วมมือ การสื่อสาร และการแก้ไขปัญหาร่วมกันจะช่วยให้อาเซียนเป็นภูมิภาคที่มั่นคงและเจริญรุ่งเรืองต่อไป

7.1.2 การตระหนักต่อภัยคุกคามที่มีร่วมกัน

การตระหนักต่อภัยคุกคามที่มีร่วมกันเป็นประเด็นที่มีความสำคัญอย่างยิ่งเพราะแต่ละประเทศสมาชิกอาเซียนมีการรับรู้ภัยคุกคามทางไซเบอร์ที่แตกต่างกันไป เช่น สิงคโปร์มีความกังวลเป็นอย่างมากเกี่ยวกับการโจมตีทางไซเบอร์ที่มุ่งเป้าหมายไปที่ระบบสาธารณูปโภคคมนาคมขนส่ง โรงพยาบาล และโครงสร้างพื้นฐานที่สำคัญต่างๆ เพราะสิงคโปร์มีสถานะเป็นศูนย์กลางด้านการเงิน การบิน และการเดินเรือข้ามพรมแดน (Ghosh, 2019) ทำให้สิงคโปร์นิยามความมั่นคงปลอดภัยไซเบอร์ว่า เป็นสภาวะที่คอมพิวเตอร์หรือระบบคอมพิวเตอร์ได้รับการป้องกันจากการเข้าถึงหรือโจมตีโดยไม่ได้รับอนุญาต ในขณะที่ประเทศสมาชิกอาเซียนอื่นอย่างเวียดนามนิยามประเด็นเรื่องความมั่นคงปลอดภัยไซเบอร์ว่าเป็นเนื้อหาและการโต้ตอบระหว่างผู้ใช้งานบนพื้นที่ไซเบอร์ เป็นผลให้กฎหมายความมั่นคงปลอดภัยไซเบอร์ของเวียดนามที่ประกาศใช้ในปี ค.ศ. 2018 ได้กำหนดให้แพลตฟอร์มโซเชียลมีเดียต้องลบเนื้อหาที่ผิดกฎหมายภายใน 24 ชั่วโมง รวมถึงการโฆษณาชวนเชื่อต่อต้านรัฐ และเนื้อหาที่ไม่ถูกต้องใดๆ ที่อาจรบกวนความสงบเรียบร้อยของประชาชนหรือก่อให้เกิดความลำบากต่อเจ้าหน้าที่รัฐ (Agence France-Presse, 2024)

โดยแต่ละประเทศก็มีตัวแสดงที่ทำหน้าที่สร้างหรือกำหนดประเด็นที่เป็นความมั่นคงหรือรักษาความมั่นคงที่แตกต่างกันไป เช่น ในไทย สิงคโปร์ และอินโดนีเซียมีการพัฒนาหน่วยงานหลักที่ทำหน้าที่เป็นสำนักงานด้านความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ในขณะที่บางประเทศได้กำหนดให้เรื่องความมั่นคงปลอดภัยไซเบอร์เป็นภารกิจย่อยของกระทรวงที่มีอยู่แล้ว เช่น ฟิลิปปินส์ กำหนดให้เป็นภารกิจของกระทรวงสารสนเทศและการสื่อสาร กัมพูชาและลาวกำหนดให้เป็นภารกิจของกระทรวงไปรษณีย์และโทรคมนาคม และเวียดนามกำหนดให้เป็นภารกิจของกระทรวงความมั่นคงสาธารณะ ความแตกต่างในการตีความส่งผลต่อการออก

นโยบายหรือแนวทางการรับมือที่แตกต่างกัน โดยกฎหมายหรือพระราชบัญญัติรักษาความปลอดภัยทางไซเบอร์ของประเทศไทย สิงคโปร์ และเวียดนาม มีรายละเอียดที่แตกต่างกันอย่างเห็นได้ชัดทั้งในเรื่องของเป้าหมายของนโยบาย หน่วยงานที่เกี่ยวข้อง ระดับของภัยคุกคามไซเบอร์ การรักษาความมั่นคงปลอดภัยไซเบอร์ และบทลงโทษ (Gohwong, 2019) อย่างไรก็ตาม ถึงแม้ว่าแต่ละประเทศจะมีการวางนโยบายและการกำกับดูแลเรื่องความมั่นคงปลอดภัยทางไซเบอร์ภายในประเทศที่แตกต่างกัน แต่ก็สามารถแลกเปลี่ยนข้อมูลนโยบายระหว่างกัน เพื่อสร้างความเข้าใจที่ตรงกันได้ ผ่านพื้นที่อย่างการประชุมระดับรัฐมนตรีอาเซียนด้านความมั่นคงทางไซเบอร์ หรือความร่วมมือระหว่างหน่วยงาน Computer Emergency Response Team (CERT) ของแต่ละประเทศ

องค์การระหว่างประเทศอย่างอาเซียนเองก็ได้เข้ามามีบทบาทสำคัญในการสร้างความเข้าใจระหว่างประเทศสมาชิกอาเซียน เพื่อส่งเสริมให้เกิดความตระหนักต่อภัยคุกคามที่มีร่วมกัน ทั้งผ่านกรอบการประชุมที่มีอยู่ของอาเซียน และการดำเนินการพัฒนาโครงการและกลไกความร่วมมือระดับภูมิภาคสำหรับประเทศสมาชิกอาเซียน เช่น การจัดตั้งศูนย์ความร่วมมืออาเซียน-ญี่ปุ่น เพื่อพัฒนาบุคลากรความมั่นคงปลอดภัยไซเบอร์ (AJCCBC) เพื่อสร้างองค์ความรู้และพัฒนาศักยภาพให้กับบุคลากรของประเทศสมาชิกอาเซียนในการรับมือกับภัยคุกคามทางไซเบอร์ (ASEAN-Japan Cybersecurity Capacity Building Centre, 2023)

องค์การภาคประชาสังคม (CSOs) ก็เข้ามามีบทบาทสำคัญในการส่งเสริมความตระหนักรู้ ความร่วมมือ และการสร้างขีดความสามารถในการรับมือกับภัยคุกคามทางไซเบอร์ในอาเซียน โดยได้ทำหน้าที่เป็นทั้งผู้ให้ความรู้ ผู้เฝ้าระวัง และผู้สนับสนุนด้านนโยบายเพื่อทำให้ภูมิภาคมีความพร้อมและความปลอดภัยมากยิ่งขึ้นจากภัยคุกคามทางไซเบอร์ โดยตัวอย่างการดำเนินงานของ CSOs ในภูมิภาคอาเซียน อาทิ ASEAN Youth Organization (AYO) ที่ได้จัดโครงการฝึกอบรมและสัมมนาเกี่ยวกับการป้องกันภัยคุกคามทางไซเบอร์สำหรับเยาวชน (ASEAN Youth Organization, 2023) และ Southeast Asia Freedom of Expression Network (SAFEnet) ที่ให้คำแนะนำและฝึกอบรมเกี่ยวกับความปลอดภัยทางไซเบอร์แก่ผู้สื่อข่าว นักปกป้องสิทธิมนุษยชน และประชาชนทั่วไป (The Southeast Asia Freedom of Expression Network, 2024)

การตระหนักถึงภัยคุกคามร่วมกันจึงถือได้ว่าเป็นปัจจัยสำคัญที่นำไปสู่การสร้างความมั่นคงในภูมิภาคอาเซียน การที่ทุกรัฐสมาชิกอาเซียนมองเห็นถึงภัยคุกคามที่ส่งผลกระทบต่อทุกฝ่ายอย่างเท่าเทียม จะช่วยทำให้เกิดความร่วมมือที่มีประสิทธิภาพในการรับมือกับปัญหาระหว่างประเทศสมาชิกอาเซียน ส่งเสริมการพัฒนากลไกการรับมือกับภัยคุกคามรูปแบบใหม่ ตลอดจนเสริมสร้างความเข้าใจและความเชื่อมั่นระหว่างกัน

7.2 ความร่วมมือและความเป็นปฏิปักษ์ในระบอบความมั่นคงปลอดภัยไซเบอร์ของอาเซียน

ความมั่นคงปลอดภัยไซเบอร์เป็นประเด็นที่มีความสำคัญมากขึ้นในยุคดิจิทัล เนื่องจากการพึ่งพาเทคโนโลยีสารสนเทศและการสื่อสารที่เติบโตขึ้นอย่างรวดเร็วทำให้ภูมิภาคอาเซียนตกเป็นหนึ่งในเป้าหมายหลักของภัยคุกคามทางไซเบอร์ ทำให้อาเซียนตระหนักถึงความจำเป็นในการเสริมสร้างความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ระหว่างประเทศสมาชิก เพื่อป้องกันและลดความเสี่ยงจากการโจมตีทางไซเบอร์ที่อาจส่งผลกระทบต่อเศรษฐกิจ สังคม และความมั่นคงของภูมิภาค ด้วยเหตุนี้ อาเซียนจึงพยายามสถาปนาให้เกิดระบอบความมั่นคงปลอดภัยไซเบอร์ของอาเซียน (ASEAN Cybersecurity Regime) กล่าวคือ อาเซียนพยายามสร้างให้เกิดกลไกและความร่วมมือระหว่างประเทศสมาชิกอาเซียนในการป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์ โดยมีเป้าหมายเพื่อเสริมสร้างความมั่นคงปลอดภัยทางดิจิทัลและการป้องกันการโจมตีทางไซเบอร์ที่อาจกระทบต่อระบบเศรษฐกิจและสังคมของภูมิภาค ความร่วมมือนี้ครอบคลุม ทั้งการแลกเปลี่ยนข้อมูล การพัฒนาขีดความสามารถด้านไซเบอร์ การฝึกอบรม และการพัฒนากฎระเบียบและมาตรฐานความมั่นคงปลอดภัยไซเบอร์ร่วมกัน เพื่อเสริมสร้างภูมิคุ้มกันทางไซเบอร์ในภูมิภาคอาเซียน อย่างไรก็ตาม ภายใต้ระบอบความมั่นคงปลอดภัยไซเบอร์ของอาเซียนก็ทำให้เกิดทั้งการประสานงานและความขัดแย้ง จนทำให้เกิดทั้งความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ และความเป็นปฏิปักษ์ด้านความมั่นคงปลอดภัยไซเบอร์

(1) ความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Cooperation)

ความมั่นคงปลอดภัยไซเบอร์กลายเป็นปัจจัยสำคัญในการสนับสนุนการพัฒนาของภูมิภาคอาเซียนในยุคดิจิทัล การป้องกันภัยคุกคามทางไซเบอร์ที่มีประสิทธิภาพไม่เพียงแต่ช่วยปกป้องโครงสร้างพื้นฐานสำคัญของชาติ แต่ยังช่วยเสริมสร้างความเชื่อมั่นในเศรษฐกิจดิจิทัล ปกป้องข้อมูลส่วนบุคคล และส่งเสริมความร่วมมือข้ามพรมแดน การพัฒนาความมั่นคงปลอดภัยไซเบอร์ให้แข็งแกร่งจึงกลายเป็นกุญแจสำคัญในการรับมือกับความท้าทายที่ภูมิภาคอาเซียนจำเป็นต้องเผชิญหน้าในอนาคต เนื่องจากความเสี่ยงทางไซเบอร์ เช่น การโจมตีโครงสร้างพื้นฐาน การแพร่กระจายข้อมูลเท็จ และการโจมตีทางไซเบอร์ที่มีการสนับสนุนจากรัฐกำลังเพิ่มขึ้นอย่างรวดเร็ว การมีระบบความมั่นคงไซเบอร์ที่แข็งแกร่งจะช่วยป้องกันความเสียหายทางเศรษฐกิจ การเมือง และสังคมในภูมิภาค รวมทั้งเสริมสร้างความเชื่อมั่นระหว่างประเทศสมาชิก และส่งเสริมความร่วมมือระหว่างประเทศในการตอบสนองต่อภัยคุกคามใหม่ๆ อย่างมีประสิทธิภาพ

ด้วยเหตุนี้ ตัวแสดงที่ทำหน้าที่สร้างความมั่นคง และประเด็นภัยคุกคามที่แต่ละประเทศรับรู้ (Perceived Threats) จึงเข้ามามีบทบาทสำคัญในการกำหนดแนวทาง และกระตุ้นให้เกิดความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ในภูมิภาคอาเซียน โดยเพื่อรับมือกับภัยคุกคามทางไซเบอร์ที่เพิ่มขึ้น อาเซียนจึงได้สร้างกลไกความร่วมมือหลายรูปแบบที่มุ่งเน้นในการเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ในภูมิภาค โดยสามารถแสดงความสัมพันธ์

ระหว่างตัวแสดงที่ทำหน้าที่สร้างความมั่นคง กับภัยคุกคามที่รับรู้ของอาเซียนในฐานะภูมิภาค และของแต่ละประเทศสมาชิกอาเซียน ซึ่งมีบทบาทสำคัญในการผลักดันความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ในภูมิภาคอาเซียน ให้เห็นในเบื้องต้นได้ ดังต่อไปนี้

ตารางที่ 1 ตารางอธิบาย Securitizer กับ Perceived Threats ของอาเซียน และความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ในภูมิภาค

ประเทศ	ตัวแสดงที่ทำหน้าที่สร้างความมั่นคง	ตัวอย่างประเด็นภัยคุกคามที่รับรู้	ตัวอย่างความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ในอาเซียน
อาเซียนในฐานะภูมิภาค	สำนักเลขาธิการอาเซียน, รัฐมนตรีอาเซียน, AMM, ADMM, ADMM-Plus	การโจมตีทางไซเบอร์จากรัฐ, อาชญากรรมไซเบอร์, การบิดเบือนข้อมูล, การโจมตีด้วยมัลแวร์, การหลอกลวงทางออนไลน์, การโจมตีเครือข่ายและโครงสร้างพื้นฐานที่สำคัญ, ศักยภาพและขีดความสามารถทางไซเบอร์ที่แตกต่างกันระหว่างประเทศสมาชิก	AMM: การผสานบรรทัดฐานและนโยบายทางไซเบอร์เข้ากับการอภิปรายด้านความมั่นคงระดับภูมิภาค; ADMM: โครงการความร่วมมือทางไซเบอร์, การประสานงานทางทหารเพื่อรับมือกับภัยไซเบอร์; ADMM-Plus: ความร่วมมือกับประเทศคู่เจรจา (เช่น สหรัฐฯ, จีน, ญี่ปุ่น) เพื่อพัฒนาการป้องกันทางไซเบอร์ รวมถึงการฝึกอบรม เสริมสร้างขีดความสามารถและกรอบความมั่นคงระดับภูมิภาค; การพัฒนายุทธศาสตร์ความร่วมมือด้านไซเบอร์อาเซียน, ASEAN CERT, โครงการไซเบอร์ของ ARF
สิงคโปร์	หน่วยงานของรัฐอาทิ Cyber Security Agency of Singapore (CSA), The Infocomm Media Development Authority (IMDA)	การโจมตีทางไซเบอร์ต่อโครงสร้างพื้นฐานที่สำคัญ, ภัยคุกคามต่อภาคการเงิน, การจารกรรมทางไซเบอร์ที่สนับสนุนโดยรัฐ	การจัดตั้งศูนย์ ASEAN-Singapore Cybersecurity Centre of Excellence, การส่งเสริมให้เกิดเครือข่าย ASEAN CERT การเป็นเจ้าภาพจัดการประชุมรัฐมนตรีอาเซียนด้านความมั่นคงปลอดภัยไซเบอร์ (ASEAN Ministerial Conference on Cybersecurity: AMCC)
มาเลเซีย	สภาความมั่นคงแห่งชาติ, CyberSecurity Malaysia (CSM)	อาชญากรรมไซเบอร์, การละเมิดข้อมูล, การบิดเบือนข้อมูล	การเข้าร่วม ASEAN Cyber Capacity Programme (ACCP), การเข้าร่วม ASEAN Cyber - CC

ประเทศ	ตัวแสดงที่ทำหน้าที่สร้างความมั่นคง	ตัวอย่างประเด็นภัยคุกคามที่รับรู้	ตัวอย่างความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ในอาเซียน
ไทย	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)	การจารกรรมทางไซเบอร์, การบิดเบือนข้อมูล, ภัยคุกคามต่อสถาบันการเงิน, การโจมตีจากรัฐ, การโจมตีทางไซเบอร์ต่อหน่วยงานรัฐ, มิจฉาชีพออนไลน์, การขโมยข้อมูลส่วนบุคคล	การจัดตั้งศูนย์ ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC), การทำงานและประสานงานระหว่าง ThaiCERT กับเครือข่าย ASEAN CERT การผลักดันให้เกิด ASEAN Working Group on Anti-Online Scam (WG–AS)
เวียดนาม	กระทรวงความมั่นคงสาธารณะ	การโจมตีทางไซเบอร์ที่สนับสนุนโดยรัฐ (มักเกี่ยวข้องกับจีน), อาชญากรรมไซเบอร์, การโจมตีเครือข่ายรัฐบาล	การเข้าร่วมโครงการไซเบอร์ของ ASEAN Regional Forum (ARF) และความร่วมมือกับ CERT ประเทศอื่นๆ
อินโดนีเซีย	สำนักงานความมั่นคงไซเบอร์และการเข้ารหัสแห่งชาติ (BSSN)	การก่อการร้ายทางไซเบอร์, การละเมิดข้อมูล, การบิดเบือนข้อมูล, การโจมตีจากรัฐ	การผลักดันเครือข่าย ASEAN CERT, การเข้าร่วม ASEAN Cyber Capacity Programme (ACCP)
ฟิลิปปินส์	กระทรวงสารสนเทศและการสื่อสาร (DICT)	อาชญากรรมไซเบอร์, การบิดเบือนข้อมูล, การแฮกข้อมูลฐานข้อมูลรัฐบาลและภาคเอกชน	การปฏิบัติตามยุทธศาสตร์ความร่วมมือด้านความมั่นคงไซเบอร์อาเซียน, ความร่วมมือกับ CERT ประเทศอื่นๆ
เมียนมา	กระทรวงคมนาคมและการสื่อสาร, กองทัพ	ความขัดแย้งทางไซเบอร์ภายในประเทศ, กลุ่มแฮกเกอร์, ภัยคุกคามไซเบอร์ที่เกี่ยวข้องกับการเมือง	เมียนมาเข้ามามีส่วนร่วมในการดำเนินงานของอาเซียนอย่างจำกัด; แต่ก็เข้าร่วมการประชุมต่างๆ อาทิ ASEAN Cyber - CC
บรูไน	ศูนย์รัฐบาลอิเล็กทรอนิกส์แห่งชาติ	การโจมตีทางไซเบอร์ต่อภาคการเงินและพลังงาน, อาชญากรรมไซเบอร์ทั่วไป	ความร่วมมือกับเครือข่าย ASEAN CERT, การเข้าร่วม ASEAN Cyber Capacity Programme (ACCP)
กัมพูชา	กระทรวงไปรษณีย์และโทรคมนาคม	อาชญากรรมไซเบอร์, ความไม่เพียงพอของโครงสร้างพื้นฐานทางความมั่นคง, การขาดความตระหนักด้านไซเบอร์	ความร่วมมือกับเครือข่าย ASEAN CERT, การเข้าร่วม ASEAN Cyber Capacity Programme (ACCP)
ลาว	กระทรวงไปรษณีย์และโทรคมนาคม	อาชญากรรมไซเบอร์, การขาดขีดความสามารถด้านไซเบอร์	ความร่วมมือกับเครือข่าย ASEAN CERT, การเข้าร่วม ASEAN Cyber Capacity Programme (ACCP)

จากตารางข้างต้น จะเห็นได้ว่า แต่ละประเทศสมาชิกอาเซียนมีการรับรู้ภัยคุกคามทางไซเบอร์ที่แตกต่างกันไป เช่น สิงคโปร์ มีความกังวลเป็นอย่างยิ่งต่อการโจมตีโครงสร้างพื้นฐานที่สำคัญและภาคการเงิน ในขณะที่เวียดนามเผชิญกับการโจมตีทางไซเบอร์ที่มักเกี่ยวข้องกับรัฐอื่นๆ เช่น จีน ภัยคุกคามที่หลากหลายเหล่านี้ทำให้ประเทศสมาชิกตระหนักถึงความจำเป็นในการสร้างความร่วมมือทางไซเบอร์เพื่อป้องกันภัยคุกคามที่อาจเกิดขึ้นกับระบบของแต่ละประเทศและทั้งภูมิภาค โดยแต่ละประเทศก็มีตัวแสดงที่ทำหน้าที่สร้างหรือกำหนดประเด็นที่เป็นความมั่นคง หรือรักษาความมั่นคงที่แตกต่างกันไป เช่น ในไทย สิงคโปร์ และอินโดนีเซียมีการพัฒนาหน่วยงานหลักที่ทำหน้าที่เป็นสำนักงานด้านความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ในขณะที่ หลายประเทศได้กำหนดให้ประเด็นเรื่องความมั่นคงปลอดภัยไซเบอร์เป็นภารกิจของกระทรวงที่แตกต่างกันไป เช่น ฟิลิปปินส์กำหนดให้เป็นภารกิจของกระทรวงสารสนเทศและการสื่อสาร กัมพูชาและลาวกำหนดให้เป็นภารกิจของกระทรวงไปรษณีย์และโทรคมนาคม และเวียดนาม กำหนดให้เป็นภารกิจของกระทรวงความมั่นคงสาธารณะ ซึ่งแต่ละประเทศต่างก็มีบทบาทในการวางนโยบายและกำกับดูแลเรื่องความมั่นคงไซเบอร์ภายในประเทศของตน และในขณะเดียวกัน แต่ละประเทศก็มีการส่งเสริมความร่วมมือกับประเทศอื่นๆ ในอาเซียน ผ่านกลไกความร่วมมือระดับภูมิภาค เช่น การประชุมรัฐมนตรีอาเซียนด้านความมั่นคงปลอดภัยไซเบอร์ (AMCC) และความร่วมมือระหว่าง CERT ของแต่ละประเทศ

ประเทศสมาชิกอาเซียนและตัวแสดงหลักด้านความมั่นคงของแต่ละประเทศ เช่น รัฐมนตรีอาเซียน (AMM) และรัฐมนตรีกลาโหมอาเซียน (ADMM) ได้ช่วยกันสร้างกรอบความร่วมมือในด้านนโยบายไซเบอร์ เช่น การผนวกบรรทัดฐานทางไซเบอร์เข้าสู่การอภิปรายความมั่นคงระดับภูมิภาค และการเสริมสร้างกรอบการป้องกันทางไซเบอร์ในระดับภูมิภาค เพื่อให้การรับมือต่อภัยคุกคามทางไซเบอร์สามารถเป็นไปได้อย่างเป็นระบบและมีความเชื่อมโยง โดยความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ในอาเซียนไม่ได้มีเพียงแค่การวางนโยบาย แต่ยังรวมถึงการเสริมสร้างขีดความสามารถของสมาชิก ผ่านกลไกการดำเนินงานที่ถูกสร้างขึ้น เช่น การเข้าร่วมการจัดฝึกอบรมพัฒนาทักษะความสามารถด้านความมั่นคงไซเบอร์ที่จัดขึ้นโดยศูนย์ ASEAN-Japan Cybersecurity Capacity Building Centre และศูนย์ ASEAN-Singapore Cybersecurity Centre of Excellence ตลอดจนการจัดฝึกอบรมผ่านโครงการของ ASEAN Cyber Capacity Programme (ACCP) ซึ่งต่างมีเป้าประสงค์ในการทำให้ประเทศสมาชิกอาเซียนมีศักยภาพในการป้องกันภัยไซเบอร์อย่างมีประสิทธิภาพ ตลอดจนการร่วมมือกับพันธมิตรภายนอกผ่านกลไกความร่วมมือที่มีอยู่ เช่น ADMM-Plus ซึ่งอาเซียนมีความร่วมมือกับประเทศคู่เจรจา เช่น สหรัฐฯ จีน และญี่ปุ่น ในการเสริมสร้างความมั่นคงไซเบอร์ระดับภูมิภาค การฝึกอบรมและการแลกเปลี่ยนข้อมูลด้านไซเบอร์กับประเทศคู่เจรจาเหล่านี้ จะช่วยให้ประเทศสมาชิกอาเซียนมีความเข้มแข็งในการรับมือกับภัยคุกคามที่มาจากภายนอกภูมิภาคได้มากยิ่งขึ้น (ASEAN Defence Ministers' Meeting Plus, 2016)

ทั้งนี้ เนื่องจากแต่ละประเทศมีนิยามและความเข้าใจเรื่องภัยคุกคามทางไซเบอร์ที่หลากหลายและแตกต่างกันไป ด้วยเหตุนี้ อาเซียนในฐานะภูมิภาค จึงได้เข้ามามีบทบาทสำคัญในฐานะที่เป็นตัวกลางสำหรับการประสานงานระหว่างประเทศสมาชิกอาเซียนในประเด็นต่างๆ รวมไปถึงประเด็นด้านความมั่นคงปลอดภัยไซเบอร์ โดยไม่ได้จำกัดแค่การจัดการประชุมภายใต้กรอบต่างๆ แต่อาเซียนยังได้ทำหน้าที่เป็นตัวกลางในการพัฒนาเอกสารทั้งในรูปแบบปฏิญญา ยุทธศาสตร์ความร่วมมือ และข้อเสนอแนะต่างๆ โดยรัฐมนตรีประเทศสมาชิกอาเซียนได้ร่วมให้ความเห็นชอบ “ASEAN Cybersecurity Cooperation Strategy” เป็นเอกสารหลักสำหรับกำหนดทิศทางยุทธศาสตร์การทำงานของอาเซียนและประเทศคู่เจรจาเพื่อให้บรรลุเป้าหมายของแผนแม่บทไอซีทีอาเซียน ค.ศ. 2016-2020 (ASEAN ICT Masterplan 2020: AIM 2020) ตลอดจนเป็นพื้นฐานสำหรับการพัฒนาความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์อื่นๆ ในอนาคต นอกจากนี้ อาเซียนยังมีการพัฒนามาตรฐานที่ใช้ร่วมกันในด้านความปลอดภัยของข้อมูล เช่น การจัดตั้งกลไกการแลกเปลี่ยนข้อมูลระหว่างประเทศสมาชิกเกี่ยวกับการโจมตีทางไซเบอร์และภัยคุกคามที่อาจเกิดขึ้น โดยอาเซียนได้มีการเสริมสร้างความร่วมมือระหว่างหน่วยงานด้านความมั่นคงปลอดภัยไซเบอร์ในระดับประเทศผ่านการจัดตั้งหน่วยงานเฉพาะทางอย่างการจัดตั้ง ASEAN CERT เพราะแต่ละประเทศสมาชิกอาเซียนต่างก็มีหน่วยงาน CERT ที่รับผิดชอบในการตรวจสอบและตอบสนองต่อภัยคุกคามทางไซเบอร์ภายในประเทศ ดังนั้น ASEAN CERT จะช่วยสนับสนุนการแลกเปลี่ยนข้อมูลและความร่วมมือในการจัดการกับภัยคุกคามข้ามพรมแดนได้

อาเซียนยังมีการนำทรัพยากรจำนวนมากมาใช้กับการเสริมสร้างความร่วมมือระหว่างหน่วยงานความมั่นคงปลอดภัยไซเบอร์ ซึ่งมีทั้งการดำเนินงานที่ผลักดันโดยรัฐสมาชิกอาเซียน องค์กรระหว่างประเทศ และความร่วมมือกับประเทศภายนอกภูมิภาคอาเซียน เช่น การดำเนินโครงการเสริมสร้างความสามารถด้านไซเบอร์อาเซียนซึ่งริเริ่มโดยสิงคโปร์ (Singapore-initiated ASEAN Cyber Capacity Program) การจัดตั้งศูนย์ความร่วมมืออาเซียน-ญี่ปุ่นเพื่อพัฒนาบุคลากรความมั่นคงปลอดภัยไซเบอร์ (AJCCBC) ด้วยทุนสนับสนุนจากประเทศญี่ปุ่น ผ่านกองทุน JAIF (Japan-ASEAN Integration Fund) ที่กรุงเทพฯ และการดำเนินงานของสิงคโปร์ผ่านหน่วยงานต่างๆ ของสิงคโปร์ อาทิ ศูนย์ความเป็นเลิศด้านความมั่นคงปลอดภัยไซเบอร์อาเซียน-สิงคโปร์ (ASEAN-Singapore Cybersecurity of Excellence) สถาบันวิจัยและฝึกอบรมด้านไซเบอร์ (Cyber Think Tank and Training Centre) และการจัดตั้งศูนย์ ASEAN Cert ณ สิงคโปร์

ภัยคุกคามทางไซเบอร์ที่เปลี่ยนแปลงอย่างรวดเร็วทำให้ประเทศสมาชิกอาเซียนต้องเน้นความร่วมมือทางด้านความมั่นคงปลอดภัยไซเบอร์มากยิ่งขึ้น การแลกเปลี่ยนข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ระหว่างประเทศ การฝึกอบรมบุคลากรและการสร้างกรอบความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้องเป็นสิ่งจำเป็นในการสร้างแนวทางป้องกันและรับมือกับภัยคุกคามที่มีความซับซ้อนและเปลี่ยนแปลงอยู่ตลอดเวลา เพราะภัยคุกคามทางไซเบอร์ที่เปลี่ยนแปลงอย่างรวดเร็วเป็นความท้าทายสำคัญที่ส่งผลต่อความมั่นคง

ปลอดภัยไซเบอร์ของทุกประเทศในอาเซียน ภูมิภาคนี้จำเป็นต้องพัฒนาขีดความสามารถในการป้องกันภัยคุกคามอย่างต่อเนื่อง ทั้งในด้านการพัฒนาบุคลากร การสร้างความร่วมมือระหว่างประเทศ การปรับปรุงนโยบาย และการปกป้องโครงสร้างพื้นฐานสำคัญ การทำเช่นนี้จะช่วยเสริมสร้างความมั่นคงทางไซเบอร์ของภูมิภาคให้แข็งแกร่งมากยิ่งขึ้น

(2) ความเป็นปฏิปักษ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Enmity)

ถึงแม้ว่าอาเซียนจะมีความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์หลายประการทั้งกับประเทศภายในภูมิภาคอาเซียนเอง กับประเทศคู่เจรจาและหน่วยงานภายนอกภูมิภาค แต่ภายใต้ระบอบความมั่นคงปลอดภัยไซเบอร์ของอาเซียน ก็ไม่ได้มีแต่ประเด็นด้านความร่วมมือ แต่ยังแฝงไว้ด้วยเรื่องของความเป็นปฏิปักษ์ ในประเด็นด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งเกิดขึ้นมาจากหลายปัจจัย เช่น ความแตกต่างในการตีความ ความแตกต่างในการพัฒนา ความขัดแย้งทางการเมือง และการมีบทบาทของมหาอำนาจภายนอก ประเทศต่างๆ อาจมองการโจมตีทางไซเบอร์หรือการแทรกแซงทางดิจิทัลเป็นภัยคุกคามต่อความมั่นคงของรัฐและอธิปไตย ส่งผลให้เกิดความขัดแย้งหรือการแข่งขันในการพัฒนาขีดความสามารถทางไซเบอร์เพื่อปกป้องข้อมูลและโครงสร้างพื้นฐานของประเทศตน การพึ่งพาเทคโนโลยีของต่างประเทศหรือการไม่สามารถสร้างมาตรฐานความมั่นคงทางไซเบอร์ร่วมกันยังเพิ่มความเสี่ยงต่อความเป็นปฏิปักษ์ระหว่างประเทศได้อีกด้วย ในยุคดิจิทัลที่เทคโนโลยีสารสนเทศและการสื่อสารมีบทบาทสำคัญในทุกด้านของชีวิตประจำวัน รวมถึงการดำเนินงานของภาครัฐและเอกชน ความมั่นคงปลอดภัยไซเบอร์กลายเป็นหัวใจสำคัญของการรักษาความมั่นคงทั้งในระดับชาติและระดับภูมิภาค อย่างไรก็ตาม ประเด็นนี้ก็สามารถกลายเป็นแหล่งกำเนิดของความเป็นปฏิปักษ์ในหลายมิติ ทั้งในด้านการเมือง เศรษฐกิจ และเทคโนโลยีของภูมิภาคอาเซียนได้เช่นเดียวกัน ซึ่งสามารถอธิบายได้จากหลายปัจจัยอภิปรายเพิ่มเติมได้ ดังนี้

หนึ่งในปัจจัยสำคัญที่สามารถก่อให้เกิดความเป็นปฏิปักษ์ คือ ความแตกต่างในการตีความ เพราะถึงแม้ว่าการตระหนักต่อภัยคุกคามร่วมกันถือได้ว่าเป็นหนึ่งในประเด็นที่มีความสำคัญที่สุดสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ของอาเซียน แต่ก็เป็นประเด็นที่ละเอียดอ่อน นั่นก็เพราะประเทศสมาชิกอาเซียนยังไม่มีความเห็นพ้องต้องกันอย่างชัดเจนต่อประเด็นด้านดิจิทัลเรื่องต่างๆ เช่น นิยามของ “พื้นที่ไซเบอร์สเปซ” ที่เกี่ยวข้องกับผลประโยชน์ของรัฐนั้น หมายถึงอะไร โดยสิงคโปร์นิยามพื้นที่นี้ว่าเป็นเทคโนโลยี (ฮาร์ดแวร์ และซอฟต์แวร์) ที่ช่วยให้เข้าถึงพื้นที่ไซเบอร์สเปซได้อย่างเสรี ซึ่งเป็นผลให้พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Act) ของสิงคโปร์ ได้นิยามความมั่นคงปลอดภัยไซเบอร์ว่าเป็นสภาวะที่คอมพิวเตอร์หรือระบบคอมพิวเตอร์ได้รับการป้องกันจากการเข้าถึงหรือโจมตีโดยไม่ได้รับอนุญาต (Ang, 2018) ในขณะที่เวียดนามนิยามพื้นที่ไซเบอร์สเปซว่าเป็นเนื้อหาและการโต้ตอบ (คำพูดและการแสดงออก) ระหว่างผู้ใช้งานพื้นที่ไซเบอร์สเปซ ซึ่งทำให้กฎหมายความมั่นคงปลอดภัยไซเบอร์ของเวียดนามที่ประกาศใช้ในปี ค.ศ. 2018 ได้กำหนดให้แพลตฟอร์มโซเชียลมีเดีย

ต้องลบเนื้อหาที่ผิดกฎหมายภายใน 24 ชั่วโมง รวมถึงการโฆษณาชวนเชื่อต่อต้านรัฐ และเนื้อหาที่ไม่ถูกต้องใดๆ ที่อาจรบกวนความสงบเรียบร้อยของประชาชนหรือก่อให้เกิดความลำบากต่อเจ้าหน้าที่รัฐ (Woollacott, 2019)

บางครั้งความแตกต่างในการตีความอาจเป็นผลที่เกิดขึ้นมาจากการรับข้อมูลที่ผิดพลาด ซึ่งเป็นผลมาจากการแพร่ระบาดของข่าวปลอม (Fake News) และข้อมูลอันเป็นเท็จทางอินเทอร์เน็ต ซึ่งบางครั้งมีเป้าหมายเพื่อก่อความไม่สงบทางสังคมและความรุนแรงภายในรัฐ หรือในบางครั้ง รัฐอาจเป็นผู้เผยแพร่ข่าวปลอมหรือข้อมูลอันเป็นเท็จเองเพื่อให้ได้ผลประโยชน์ทางการเมืองและความมั่นคงแก่รัฐตน ดังเช่น กรณีที่รัฐบาลอินโดนีเซียถูกวิพากษ์วิจารณ์ว่าอาศัยอำนาจพิเศษในช่วงที่เกิดวิกฤติการแพร่ระบาดของโควิด-19 ในการจับกลุ่มคนที่ไม่เห็นด้วยกับรัฐบาล และมีการแชร์ข่าวปลอมเพื่อให้ประชาชนสร้างความเชื่อมั่นของรัฐบาล (สุภชาติ เล็บนาค, 2020) ซึ่งถึงแม้จะเป็นการดำเนินการที่มุ่งหวังผลลัพธ์ภายในประเทศ แต่การกระจายข่าวปลอมอาจส่งผลให้เกิดการรับรู้ข้อมูลที่ไม่ถูกต้องของรัฐอื่นๆ และสร้างผลกระทบตามมาได้ เช่น การที่รัฐบาลคาดการณ์สภาวะการกระจายตัวของโรคระบาดจากประเทศข้างเคียงผิดพลาดจนไม่สามารถรับมือสถานการณ์การแพร่ระบาดเข้าประเทศตนได้ ดังนั้น ถ้าอาเซียนต้องการป้องกันไม่ให้เกิดความเข้าใจผิดและทำให้เกิดความร่วมมือในพื้นที่ไซเบอร์อย่างปราศจากความขัดแย้ง ก็จำเป็นที่จะต้องมีมาตรฐานความเข้าใจที่ตรงกัน ผ่านกลไกความร่วมมือที่มีอยู่ อาทิ การหารือเกี่ยวกับบรรทัดฐานความรับผิดชอบของรัฐบนโลกไซเบอร์ (Norms of Responsible State Behaviour in Cyberspace) ระหว่างการประชุมรัฐมนตรีอาเซียนด้านความมั่นคงปลอดภัยไซเบอร์ครั้งที่ 4 (กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, 2562)

อีกหนึ่งประเด็นสำคัญที่ทำให้เกิดความเป็นปฏิปักษ์และความขัดแย้งได้นั้น คือความไม่สมดุลในการพัฒนาด้านความมั่นคงไซเบอร์ของประเทศสมาชิกอาเซียน ในขณะที่ประเทศอย่างสิงคโปร์และมาเลเซียมีการพัฒนาเทคโนโลยีและมาตรการความปลอดภัยทางไซเบอร์ที่เข้มแข็ง ประเทศสมาชิกอื่นๆ เช่น เมียนมา ลาว และกัมพูชายังคงประสบปัญหาการขาดแคลนโครงสร้างพื้นฐานและทรัพยากรในการป้องกันภัยคุกคามทางไซเบอร์ ความแตกต่างนี้ก่อให้เกิดความตึงเครียดภายในภูมิภาค เนื่องจากประเทศที่มีศักยภาพต่ำกว่ามักตกเป็นเป้าหมายของการโจมตีทางไซเบอร์ และอาจกลายเป็นช่องโหว่ในการรักษาความปลอดภัยทางไซเบอร์ของภูมิภาคโดยรวม นอกจากความแตกต่างด้านระดับการพัฒนาเทคโนโลยีแล้ว อาเซียนยังมีความแตกต่างในเรื่องของระดับการพัฒนาเนื้อหาของกฎหมายและนโยบายของแต่ละประเทศที่ไม่ได้อยู่ในระดับที่เท่าเทียมกัน อาทิ เรื่องของการละเมิดลิขสิทธิ์บนพื้นที่ออนไลน์ ในแง่ของการบังคับใช้กฎหมาย มีเพียงสิงคโปร์และมาเลเซียเท่านั้นที่มีขั้นตอนการแจ้งเตือนและถอดเนื้อหาอย่างเป็นรูปธรรม ในขณะที่ อินโดนีเซีย ฟิลิปปินส์ ไทย และเวียดนามยังไม่มีบทบัญญัติทางกฎหมายสำหรับผู้ถือสิทธิ์ในการบังคับใช้การคุ้มครองลิขสิทธิ์โดยตรงผ่านระบบแจ้งเตือนของผู้ให้บริการอินเทอร์เน็ต (Internet service provider: ISP) แต่จำเป็นต้องดำเนินการบังคับใช้กฎหมายลิขสิทธิ์ผ่านการดำเนินคดีทางกฎหมายหรือระบบตุลาการ (Judicial System) (Sunkpho, Ramjan, & Ottamakorn, 2018)

ประเด็นความขัดแย้งกันในเรื่องอำนาจอธิปไตยและหลักการเรื่องการไม่แทรกแซงของอาเซียนเองก็สามารถกลายเป็นปัจจัยที่ส่งผลกระทบต่อการสร้างความร่วมมือด้านความมั่นคงไซเบอร์ในอาเซียน อาเซียนมีกฎบัตรที่ยึดถือหลักการไม่แทรกแซงกิจการภายในของรัฐสมาชิก ซึ่งอาจส่งผลให้การพัฒนามาตรการป้องกันภัยคุกคามทางไซเบอร์ในระดับภูมิภาคต้องพิจารณาอย่างระมัดระวัง ประเทศสมาชิกบางประเทศอาจมองว่าการแบ่งปันข้อมูลหรือการร่วมมือกันในด้านไซเบอร์เป็นการแทรกแซงอธิปไตยของตน ทำให้การสร้างกรอบความร่วมมืออย่างมีประสิทธิภาพในระดับภูมิภาคมีความซับซ้อนมากยิ่งขึ้น

สาเหตุที่เป็นเช่นนั้น สืบเนื่องมาจากการที่ภูมิภาคอาเซียนประกอบด้วยประเทศสมาชิกที่มีลักษณะทางการเมืองและเศรษฐกิจที่แตกต่างกันอย่างมาก ซึ่งเป็นผลให้หลักการสำคัญของอาเซียน เช่น การเคารพในอำนาจอธิปไตยและการไม่แทรกแซงกิจการภายในของประเทศสมาชิก กลายเป็นส่วนสำคัญในการกำหนดทิศทางของ การสร้างความร่วมมือในประเด็นต่างๆ รวมถึงความมั่นคงปลอดภัยไซเบอร์ อย่างไรก็ตาม หลักการเหล่านี้อาจกลายเป็นอุปสรรคสำคัญต่อการพัฒนาความร่วมมือด้านความมั่นคงไซเบอร์ในภูมิภาคด้วยข้อจำกัดจากหลักการไม่แทรกแซงและความยากลำบากในการกำหนดมาตรฐานร่วม การขาดการประสานงานในระดับลึก และการรักษาภาพลักษณ์และผลประโยชน์ทางการเมืองในระดับทวิภาคีและพหุภาคี

การแข่งขันทางอำนาจของประเทศมหาอำนาจภายนอก เช่น สหรัฐอเมริกา จีน หรือญี่ปุ่น ก็เป็นอีกปัจจัยสำคัญที่ส่งผลต่อการพัฒนาระบอบความมั่นคงปลอดภัยทางไซเบอร์ของอาเซียน ประเทศมหาอำนาจอาจสนับสนุนการพัฒนาความมั่นคงของภูมิภาคทั้งหมดโดยรวม ผ่านกลไกที่มีอยู่อย่างการประชุมรัฐมนตรีอาเซียนด้านดิจิทัลกับประเทศคู่เจรจา หรือประเทศมหาอำนาจอาจเลือกที่จะให้การสนับสนุนแค่บางประเทศที่เป็นพันธมิตร มีระบอบการปกครองที่เหมือนกัน หรือมุ่งเป้าไปที่การคานอำนาจกับมหาอำนาจอื่นที่มีอิทธิพลในภูมิภาคเหมือนกับตน ทั้งการแข่งขันและความสัมพันธ์ทางอำนาจนี้ส่งผลต่อท่าทีของประเทศสมาชิกอาเซียนในการพัฒนาความร่วมมือหรือกำหนดแนวทางการจัดการกับภัยคุกคามไซเบอร์ บางประเทศอาจได้รับการสนับสนุนทางเทคโนโลยีจากประเทศมหาอำนาจและใช้กลไกเหล่านั้นในการปกป้องตนเอง แต่ในขณะเดียวกันอาจไม่ต้องการเข้าร่วมในความร่วมมือระดับภูมิภาคอย่างเต็มที่ เพราะไม่ต้องการให้เกิดการเสียเปรียบในทางการเมืองหรือการปกครอง ยิ่งไปกว่านั้น การมีบทบาทของมหาอำนาจภายนอกภูมิภาคได้สร้างแรงกดดันต่ออาเซียนในการเลือกข้างหรือพัฒนามาตรฐานความมั่นคงไซเบอร์ที่สอดคล้องกับอำนาจภายนอก เพราะบางครั้งการเลือกเป็นพันธมิตรหรือมีแนวโน้มเอนเอียงไปทางมหาอำนาจหนึ่ง ก็อาจหมายถึงการประกาศตัวเป็นศัตรูกับอีกมหาอำนาจหนึ่ง (Waltz, 1979) กล่าวได้ว่า ประเด็นด้านความมั่นคงปลอดภัยทางไซเบอร์ส่งผลกระทบต่ออาเซียนทั้งบนพื้นที่ไซเบอร์ และบนพื้นที่ตามภูมิศาสตร์จริงของแต่ละรัฐ ความขัดแย้งทางภูมิรัฐศาสตร์ระหว่างมหาอำนาจเหล่านี้เกี่ยวข้องกับการควบคุมและการพัฒนาเทคโนโลยี เช่น 5G และการพัฒนาโครงสร้างพื้นฐานทางไซเบอร์ ทำให้อาเซียนต้องเผชิญกับความเสี่ยงในการถูกใช้เป็นเวทีสำหรับการแข่งขันด้านอำนาจระหว่างประเทศมหาอำนาจ

จนทำให้การพัฒนาความร่วมมือในอาเซียนมีความท้าทายมากยิ่งขึ้น หรือแม้กระทั่งอาจนำไปสู่ความขัดแย้งกันเองระหว่างประเทศสมาชิกอาเซียน

อาเซียนมีความแตกต่างจากกลุ่มความร่วมมือระดับภูมิภาคอื่นๆ ตรงที่ภูมิภาคอาเซียนเป็นจุดบรรจบของการแข่งขันระหว่างมหาอำนาจ โดยเฉพาะอย่างยิ่ง จีนและสหรัฐอเมริกา ซึ่งต่างก็เข้ามามีบทบาทนำในภูมิภาคอาเซียน เพราะทั้งจีนและสหรัฐฯ ต่างก็เป็นคู่ค้ารายสำคัญของประเทศสมาชิกอาเซียนส่วนใหญ่ และมีความสัมพันธ์ทางเศรษฐกิจที่ไม่อาจมองข้ามได้จากการเข้ามาลงทุนจำนวนมาก ทำให้ทั้งสองประเทศต่างก็เป็นประเทศคู่เจรจา (Dialogue Partners) ที่สำคัญมากของอาเซียน และได้เข้ามามีบทบาทสำคัญในการส่งเสริมและสนับสนุนการพัฒนาศักยภาพด้านความมั่นคงปลอดภัยทางไซเบอร์ของอาเซียน อย่างไรก็ตาม จีนและสหรัฐฯ เป็นสองมหาอำนาจที่มีแนวทางการกำกับดูแลความมั่นคงปลอดภัยทางไซเบอร์ที่แตกต่างกันอย่างชัดเจน ขณะที่จีนใช้แนวทางแบบรัฐเป็นศูนย์กลาง (State-Centric) ซึ่งให้อำนาจรัฐบาลในการควบคุมข้อมูลและการดำเนินงานด้าน ไซเบอร์ สหรัฐฯ กลับใช้แนวทางแบบตลาดเสรีและหลายภาคส่วน (Multi-Stakeholder Approach) ซึ่งให้อำนาจแก่ภาคเอกชนและภาคประชาสังคมในการกำหนดทิศทางของความมั่นคงปลอดภัยไซเบอร์ เพื่อเป็นการรับมือกับความปฏิปักษ์ที่เกิดขึ้นในบริบทนี้ อาเซียนจึงเลือกที่จะไม่เข้าข้างฝ่ายใดฝ่ายหนึ่ง แต่พยายามทำหน้าที่เป็นตัวกลาง (Broker) ระหว่างสองขั้วอำนาจ โดยอาศัยกลยุทธ์ทางการค้าและความร่วมมือระหว่างประเทศ เพื่อรักษาสมดุลทางเศรษฐกิจและความมั่นคงของตน (Van Raemdonck, 2021) แนวทางนี้สะท้อนให้เห็นว่าอาเซียนพยายามสร้าง “เอกราชทางดิจิทัล” (Digital Autonomy) เพื่อให้ประเทศสมาชิกสามารถกำหนดทิศทางด้านความมั่นคงปลอดภัยไซเบอร์ได้ด้วยตนเอง โดยไม่ต้องพึ่งพาแนวทางจากมหาอำนาจเพียงฝ่ายใดฝ่ายหนึ่ง

ประเด็นที่น่าห่วงกังวลคือความขัดแย้งที่นำไปสู่ความเป็นปฏิปักษ์อาจไม่ได้เกิดขึ้นเฉพาะระหว่างประเทศมหาอำนาจ แต่ประเทศมหาอำนาจก็อาจเป็นปฏิปักษ์กับประเทศสมาชิกอาเซียนโดยตรงได้เช่นเดียวกัน ซึ่งสิ่งนี้ปรากฏให้เห็นชัดเจนในพื้นที่ไซเบอร์สเปซทั้งในแง่ของการขยายตัวจากข้อพิพาทระหว่างประเทศสู่การโจมตีทางไซเบอร์ อาทิ การโจมตีแบบปฏิเสธบริการ (Distributed Denial-of-Service: DDoS) แบบกระจายไปยังหน่วยงานของรัฐบาลฟิลิปปินส์ที่มีความสำคัญ ซึ่งเกิดขึ้นภายหลังจากคำตัดสินของศาลอนุญาโตตุลาการถาวร (Permanent Court of Arbitration: PCA) ที่ยกเลิกการอ้างกรรมสิทธิ์ของจีนเหนือทะเลจีนใต้อย่างมีนัยสำคัญ หรือกรณีที่เครือข่ายข่าวกรองของเวียดนามถูกโจมตี จนมีการรั่วไหลของข้อมูลลับเกี่ยวกับยุทธศาสตร์ทางการทูตและการทหาร ซึ่งเกิดขึ้นหลังจากเหตุการณ์ข้อพิพาทเกี่ยวกับแท่นขุดเจาะน้ำมันของจีนในน่านน้ำที่เวียดนามอ้างสิทธิ์ในเดือนพฤษภาคม ค.ศ. 2014 (Piiparinen, 2016) แต่ถึงแม้ว่าจีนจะถูกมองว่าเป็นภัยคุกคามทางไซเบอร์ในบางกรณี แต่อาเซียนก็ไม่สามารถตัดความสัมพันธ์กับจีนได้เนื่องจากความสัมพันธ์ทางเศรษฐกิจที่แข็งแกร่ง จีนเป็นคู่ค้าหลักและแหล่งการลงทุนสำคัญในภูมิภาค ทำให้อาเซียนต้องเดินทางสายกลางระหว่างการต้องป้องกันตนเองจากภัยคุกคามทางไซเบอร์ที่มาจากจีนและการรักษาความสัมพันธ์

เชิงเศรษฐกิจกับจีน ความซับซ้อนนี้สามารถนำไปสู่ความขัดแย้งภายในอาเซียน ประเทศสมาชิกบางประเทศ เช่น สิงคโปร์ พยายามที่จะสร้างความสมดุลระหว่าง การรักษาความมั่นคงทางไซเบอร์และการเป็นมิตรกับจีน ในขณะที่บางประเทศ เช่น เวียดนามและฟิลิปปินส์ มักมีท่าทีที่แข็งกร้าวมากกว่าเนื่องจากมีประวัติเรื่องความขัดแย้งในประเด็นเรื่องทะเลจีนใต้

โดยสรุปแล้ว ความเป็นปฏิปักษ์และการแข่งขันในประเด็นความมั่นคงไซเบอร์ในอาเซียนนั้นเป็นผลสืบเนื่องมาจากความแตกต่างในการตีความ ความแตกต่างในการพัฒนา ความขัดแย้งทางการเมือง และบทบาทของมหาอำนาจภายนอก การพัฒนาความมั่นคงปลอดภัยทางไซเบอร์ในภูมิภาคอาเซียนจึงยังคงเป็นความท้าทายที่ต้องการความร่วมมืออย่างใกล้ชิดและการแก้ไขปัญหาร่วมกัน

8. สรุปผลการวิจัย

จากผลการวิจัยการพัฒนาระบอบความมั่นคงปลอดภัยไซเบอร์ในภูมิภาคอาเซียน ผู้วิจัยพบว่า ตัวแสดงหลักที่เกี่ยวข้องกับกระบวนการการสร้างระบอบความมั่นคงปลอดภัยไซเบอร์ในภูมิภาคอาเซียน สามารถแบ่งออกได้เป็น 2 ตัวแสดงสำคัญ นั่นก็คือ ตัวแสดงที่สร้างความมั่นคง และการตระหนักต่อภัยคุกคามที่มีร่วมกัน โดยสามารถอธิบายเพิ่มเติมได้ดังนี้

ตัวแสดงที่สร้างความมั่นคงเป็นตัวแสดงที่ทำหน้าที่ช่วยในการกำหนดและโน้มน้าวให้ประชาชนหรือรัฐต่างๆ สามารถรับรู้ถึงภัยคุกคามต่อความมั่นคงของภูมิภาค ตัวแสดงเหล่านี้มีอิทธิพลต่อวาทกรรมด้านความมั่นคงและการกำหนดแนวทางการแก้ไขปัญหาด้านความมั่นคงปลอดภัยทางไซเบอร์ของภูมิภาคอาเซียน ตลอดจนมีบทบาทในการส่งเสริมเสถียรภาพและสันติภาพในภูมิภาค โดยตัวแสดงหลักที่มีส่วนสำคัญในการสร้างความมั่นคงในอาเซียน ได้แก่ รัฐสมาชิกอาเซียน องค์การระหว่างประเทศ และภาคประชาสังคม

รัฐสมาชิกอาเซียนมีบทบาทที่สำคัญในการสร้างความมั่นคงในภูมิภาคผ่านการดำเนินนโยบายและการสร้างความร่วมมือในด้านต่างๆ อาทิ ด้านการทหาร การเมือง เศรษฐกิจ และสังคม ในขณะที่องค์การระหว่างประเทศเองก็มีส่วนสำคัญในการเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ในภูมิภาค ผ่านการสนับสนุนและความร่วมมือทั้งในระดับทวิภาคีและพหุภาคี องค์การระหว่างประเทศมีหน้าที่สำคัญในการเป็นตัวกลางในการเสริมสร้างความมั่นคง ด้วยการให้ความช่วยเหลือด้านการเงิน การสนับสนุนการพัฒนาโครงสร้างพื้นฐาน การช่วยแก้ไขปัญหาข้อขัดแย้ง และการส่งเสริมการพัฒนาที่ยั่งยืนระหว่างประเทศสมาชิก โดยสำนักเลขาธิการอาเซียน ถือได้ว่าเป็นองค์การระหว่างประเทศหลักที่ทำหน้าที่ในการส่งเสริมและประสานงานเพื่อสร้างความมั่นคงในภูมิภาคอาเซียน ผ่านการทำหน้าที่เป็นศูนย์กลางในการบริหารจัดการและประสานงานด้านนโยบายและกิจกรรมต่างๆ ของอาเซียน เพื่อให้รัฐสมาชิกอาเซียนสามารถดำเนินการตามพันธกรณีและข้อตกลงร่วมกันได้อย่างมีประสิทธิภาพ นอกจากนี้ ภาคประชาสังคม ก็เข้ามามีบทบาทสำคัญในการ

ส่งเสริมความมั่นคงของภูมิภาค ผ่านการสร้างความตระหนักรู้เกี่ยวกับประเด็นด้านความมั่นคง หรือเข้ามาช่วยในการแก้ไขปัญหาความขัดแย้งในระดับท้องถิ่นและระดับภูมิภาค ภาคประชาสังคมสามารถเป็นผู้ประสานงานระหว่างหน่วยงานภาครัฐ องค์การระหว่างประเทศ และชุมชนท้องถิ่น การมีส่วนร่วมของภาคประชาสังคมยังช่วยให้ประชาชนมีส่วนร่วมในการกำหนดทิศทางของนโยบายความมั่นคง และเป็นกลไกในการตรวจสอบและถ่วงดุลอำนาจของรัฐ

จากการศึกษาปัจจัยและที่มาของการบังคับใช้และการค้ำจุนระบอบความมั่นคงปลอดภัยไซเบอร์ในภูมิภาคอาเซียน ผู้วิจัยพบว่า หนึ่งในปัจจัยที่มีความสำคัญที่สุดในกระบวนการสร้างระบอบความมั่นคงในภูมิภาคอาเซียน นั่นก็คือ การตระหนักต่อภัยคุกคามที่มีร่วมกัน การที่รัฐสมาชิกอาเซียนสามารถมองเห็นถึงภัยคุกคามที่ส่งผลกระทบต่อทุกฝ่ายอย่างเท่าเทียม และมีความเข้าใจต่อประเด็นที่เป็นภัยคุกคามที่ตรงกันจะช่วยทำให้เกิดการร่วมมือและความเป็นอันหนึ่งอันเดียวกันในการรับมือกับปัญหาเหล่านั้น ไม่ว่าจะเป็นภัยคุกคามจากปัญหาความมั่นคงแบบดั้งเดิม หรือปัญหาความมั่นคงรูปแบบใหม่อย่างภัยคุกคามทางไซเบอร์

อย่างไรก็ตาม ภายใต้ระบอบความมั่นคงปลอดภัยไซเบอร์ของอาเซียนก็ทำให้เกิดทั้งการประสานงานและความขัดแย้ง จนทำให้เกิดทั้งความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ และความเป็นปฏิปักษ์ด้านความมั่นคงปลอดภัยไซเบอร์เช่นเดียวกัน ตัวแสดงที่ทำหน้าที่สร้างความมั่นคงและประเด็นภัยคุกคามที่แต่ละประเทศรับรู้ได้เข้ามามีบทบาทสำคัญในการกำหนดแนวทางและกระตุ้นให้เกิดความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ในภูมิภาคอาเซียน อาเซียนได้ตระหนักถึงความสำคัญของการร่วมมือกับประเทศและองค์การระหว่างประเทศในการเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ โดยมีการทำงานร่วมกับพันธมิตรจากภายนอก การฝึกอบรมบุคลากรด้านดิจิทัลให้ประเทศสมาชิกอาเซียน และการดำเนินการทูตเชิงป้องกัน ซึ่งถึงแม้ว่าอาเซียนจะมีความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์หลายประการทั้งกับประเทศภายในภูมิภาคอาเซียนเอง และกับประเทศคู่เจรจาตลอดจนหน่วยงานภายนอกภูมิภาค แต่ภายใต้ระบอบความมั่นคงปลอดภัยไซเบอร์ของอาเซียน ก็ยังแฝงไว้ด้วยปัจจัยเรื่องของความเป็นปฏิปักษ์ และการแข่งขันในประเด็นด้านความมั่นคงปลอดภัยทางไซเบอร์เช่นเดียวกัน ซึ่งความเป็นปฏิปักษ์และการแข่งขันนี้เกิดขึ้นมาได้จากหลายปัจจัย เช่น ความแตกต่างในการตีความ ความแตกต่างในการพัฒนา ความขัดแย้งทางการเมือง และบทบาทของมหาอำนาจภายนอก

ในบริบทของภูมิภาคอาเซียน ความเป็นปฏิปักษ์และการแข่งขันด้านความมั่นคงปลอดภัยไซเบอร์มีความซับซ้อนและเกี่ยวพันกับหลายปัจจัย ทั้งในด้านการเมือง เทคโนโลยี และการพัฒนาทางเศรษฐกิจของแต่ละประเทศสมาชิก แม้ว่าอาเซียนจะพยายามสร้างกรอบความร่วมมือในการรับมือกับภัยคุกคามทางไซเบอร์ แต่การจัดการกับประเด็นเรื่องของความเป็นปฏิปักษ์ในภูมิภาคกลับมีความท้าทายเป็นอย่างมาก เนื่องจากความแตกต่างในระดับการพัฒนาด้านเทคโนโลยีและความสามารถในการป้องกันภัยคุกคามไซเบอร์ของแต่ละประเทศสมาชิก นอกจากนี้ อาเซียนยังต้องเผชิญหน้ากับการเข้ามามีบทบาทของ

มหาอำนาจภายนอก โดยเฉพาะอย่างยิ่ง ประเทศจีน ซึ่งเข้ามามีบทบาททั้งในด้านการส่งเสริมความร่วมมือด้านดิจิทัลผ่านการแบ่งปันความรู้และเทคโนโลยี และการจัดฝึกอบรมให้ประเทศสมาชิกอาเซียน แต่ในขณะเดียวกัน จีนก็เข้ามามีบทบาทในฐานะปฏิปักษ์ต่อการสร้างความมั่นคงปลอดภัยทางไซเบอร์ของอาเซียนในลักษณะที่ซับซ้อนและมีหลายมิติ ทั้งจากการขยายอิทธิพลทางเทคโนโลยี การใช้มาตรการควบคุมข้อมูล และการทำให้เกิดความตึงเครียดทางภูมิรัฐศาสตร์ อาเซียนจึงมีความจำเป็นที่จะต้องมีแนวทางร่วมกันในการปรับตัวเพื่อรักษาความมั่นคงและเสถียรภาพในภูมิภาคนี้ เพื่อให้ระบอบความมั่นคงปลอดภัยทางไซเบอร์ที่อาเซียนพัฒนาขึ้น สามารถเติบโตได้อย่างมั่นคง เข้มแข็ง และยั่งยืน

9. ข้อเสนอแนะสำหรับการศึกษาในอนาคต

ถึงแม้การศึกษาครั้งนี้จะได้ดำเนินการวิเคราะห์สถานะองค์ความรู้และตัวแสดงหลักในกระบวนการสร้างระบอบความมั่นคงปลอดภัยไซเบอร์ในอาเซียนไว้ในระดับหนึ่งแล้ว แต่อย่างไรก็ดี ยังมีประเด็นสำคัญอีกหลายด้านที่สามารถศึกษาเพิ่มเติมและสำรวจให้ลึกซึ้งยิ่งขึ้นในงานวิจัยในอนาคต เพื่อเสริมสร้างความเข้าใจเชิงรัฐศาสตร์เกี่ยวกับประเด็นด้านความมั่นคงปลอดภัยไซเบอร์ในระดับภูมิภาคที่มีลักษณะซับซ้อนและเปลี่ยนแปลงอย่างรวดเร็ว เช่น การศึกษาเชิงเปรียบเทียบบทบาทของรัฐสมาชิกอาเซียนด้านนโยบายไซเบอร์ โดยอาจมุ่งเน้นไปที่การวิเคราะห์ความสัมพันธ์เชิงอำนาจที่ไม่สมดุลกัน (Power Asymmetry) ระหว่างรัฐที่มีศักยภาพสูง เช่น สิงคโปร์ กับรัฐที่มีข้อจำกัดทางเทคนิค เช่น ลาวหรือเมียนมา ซึ่งการศึกษาวิจัยในมิตินี้จะช่วยอธิบายว่า ความไม่สมดุลด้านศักยภาพทางไซเบอร์มีผลต่อการกำหนดทิศทางของระบอบความมั่นคงปลอดภัยไซเบอร์ของภูมิภาคอาเซียนอย่างไร และสามารถดำเนินการศึกษาว่ารัฐที่มีศักยภาพต่ำก็สามารถมีอิทธิพลต่อการเจรจาระดับภูมิภาคได้หรือไม่ โดยการศึกษาในอนาคตสามารถให้ความสำคัญกับบริบททางการเมืองภายในประเทศสมาชิกอาเซียน เนื่องจากแนวนโยบายไซเบอร์ของรัฐแต่ละประเทศมักสะท้อนระดับประชาธิปไตยและวาระภายในของผู้นำ ตัวอย่างเช่น การใช้กฎหมายไซเบอร์ในการควบคุมการสื่อสารของภาคประชาชน หรือการจำกัดสิทธิเสรีภาพภายใต้การให้เหตุผลเรื่องของความมั่นคงแห่งชาติ หากมีการวิจัยเปรียบเทียบเชิงคุณภาพระหว่างรัฐประชาธิปไตยและรัฐอำนาจนิยมกึ่งเสรีภายในภูมิภาคอาเซียนก็จะช่วยเปิดเผยความสัมพันธ์ระหว่าง “ความมั่นคง” กับ “อำนาจ” ที่ดำรงอยู่ในระดับภายในและระดับภูมิภาคพร้อมกัน

อีกประเด็นการศึกษาที่น่าสนใจคือ การศึกษาบทบาทของตัวแสดงที่ไม่ใช่รัฐอย่างเป็นระบบมากยิ่งขึ้น ทั้งบริษัทเทคโนโลยีระดับโลก ภาคประชาสังคม ตลอดจนองค์การระหว่างประเทศ ซึ่งมีส่วนร่วมในการกำหนดมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง ซึ่งการศึกษาบทบาทของตัวแสดงที่ไม่ใช่รัฐ อาจทำให้สามารถวิเคราะห์และทำความเข้าใจรูปแบบความสัมพันธ์และการถ่ายโอนอำนาจในระดับข้ามชาติที่ไม่จำเป็นต้องพึ่งพิงเพียงแค่กลไกทางการทูตแบบดั้งเดิมเท่านั้นได้ นอกจากนี้ ยังสามารถศึกษาการกำหนดนโยบายด้านความมั่นคงปลอดภัยทางไซเบอร์ของภูมิภาคอาเซียน โดยใช้กรอบการวิเคราะห์

เปรียบเทียบกับภูมิภาคอื่น เช่น สหภาพยุโรป หรือสหภาพแอฟริกา ซึ่งอาจมีการพัฒนาโครงสร้างความร่วมมือด้านไซเบอร์ที่มีลักษณะเฉพาะของภูมิภาคตน นอกจากนี้ ยังสามารถศึกษาตัวแสดงประเทศมหาอำนาจอื่นๆ เช่น จีน และสหรัฐอเมริกา ว่าตัวแสดงประเทศมหาอำนาจสามารถเข้ามามีอิทธิพลในการสร้างความร่วมมือหรือความขัดแย้งด้านความมั่นคงปลอดภัยไซเบอร์ในอาเซียนอย่างไร โดยสรุปแล้ว ผู้วิจัยมุ่งหวังว่าการศึกษาครั้งนี้จะเป็นประโยชน์และสามารถช่วยให้ผู้ที่ต้องการศึกษาในประเด็นเรื่องความมั่นคงปลอดภัยทางไซเบอร์เชิงรัฐศาสตร์ในอนาคต สามารถใช้งานชิ้นนี้และข้อเสนอแนะข้างต้นในการพัฒนาองค์ความรู้ในด้านรัฐศาสตร์ ทั้งในเชิงแนวคิด ทฤษฎี และวิธีวิจัย พร้อมทั้งมีส่วนช่วยในการเปิดพื้นที่ให้กับการอภิปรายอย่างมีวิจารณญาณเกี่ยวกับประเด็นด้านความมั่นคง และประเด็นสมัยใหม่อย่างพื้นที่ไซเบอร์ ซึ่งมิได้ดำรงอยู่เพียงแค่ในฐานะของความก้าวหน้าในด้านเทคโนโลยี หากแต่มีความสัมพันธ์แนบแน่นกับโครงสร้างอำนาจ สถาบัน และอัตลักษณ์ทางการเมืองในเชิงรัฐศาสตร์อย่างลึกซึ้ง

เอกสารอ้างอิง

ภาษาไทย

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (2562). *กระทรวงดิจิทัลฯ ร่วมประชุม รมต. อาเซียน ด้านความมั่นคงปลอดภัยไซเบอร์ ที่สิงคโปร์ เดินหน้าบูรณาการร่วมกัน และกำหนดบรรทัดฐานความรับผิดชอบของรัฐบนโลกไซเบอร์.* กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. https://www.mdes.go.th/news/detail/1740

ไทยพีบีเอส. (2560). *ไทยโดนแล้ว 200 เครื่อง มัลแวร์เรียกค่าไถ่*. ThaiPBS. https://www.thaipbs.or.th/news/content/262480

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562. (2562). *ราชกิจจานุเบกษา*. เล่ม 136 ตอนที่ 69 หน้า 20-51.

สุภชาติ เล็บนาค. (2563*). สื่ออาเซียนเผย “Fake News” เกี่ยวกับ "โควิด-19" หลายครั้ง “รัฐ” เผยแพร่เอง.* Hfocus. https://www.hfocus.org/content/2020/04/19057

ภาษาอังกฤษ

Agence France-Presse. (2024). *Sweeping Vietnam Internet Law Comes into Force*. Voice of America. https://www.voanews.com/a/sweeping-vietnam-internet-law-comes-into-force/7913333.html

Ang, B. (2018). *Next Steps for Cyber Norms in ASEAN. S*. Rajaratnam School of International Studies (RSIS). https://www.rsis.edu.sg/rsis-publication/cens/next-steps-for-cyber-norms-in-asean/

Aradau, C. (2004). Security and The Democratic Scene: Desecuritization and Emancipation. *Journal of International Relations and Development, 7*, 388-413. https://doi.org/10.1057/palgrave.jird.1800030

ASEAN Briefing. (2024). *Indonesia's Comprehensive Personal Data Protection Law Guide.* ASEAN Briefing. https://www.aseanbriefing.com/doing-business-guide/indonesia/company-establishment/personal-data-protection-law

ASEAN Defence Ministers' Meeting Plus. (2016). *Concept Paper on the Establishment of the ADMM-Plus Experts' Working Group on Cyber Security.* ASEAN Defence Ministers' Meeting (ADMM). https://admm.asean.org/dmdocuments/Concept%20Paper%20on%20Establishment%20of%20EWG%20on%20Cyber%20Security,%20Final,%20as%20adopted%20by%20the%2010th%20ADMM.pdf

ASEAN Foundation. (2023). *ASEAN Foundation and Microsoft's Cybersecurity Skilling Programme Benefited 24,886 People in ASEAN*. ASEAN Foundation.

https://www.aseanfoundation.org/asean_foundation_and_microsoft_s_cybersecurity_skilling_programmebenefited_24_886_people_in_asean

ASEAN Regional Forum. (2006). *ASEAN Regional Forum (ARF) Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyber Space.* ASEAN Regional Forum https://cil.nus.edu.sg/wp-content/uploads/2019/02/2006-ARF-Statement-on-Cyber-Attack.pdf

ASEAN Regional Forum. (2012). *ASEAN Regional Forum (ARF) Statement by the Ministers of Foreign Affairs on Cooperation in Ensuring Cyber Security*. ASEAN Regional Forum. https://aseanregionalforum.asean.org/wp-ontent/uploads/2019/01/ARF-Statement-on-Cooperation-in-Ensuring-Cyber-Security.pdf

ASEAN Secretariat. (2017). *ASEAN Declaration to Prevent and Combat Cybercrime.* The ASEAN Secretariat. https://asean.org/asean-declaration-to-prevent-and-combat-cybercrime/

ASEAN Secretariat. (n.d.). *Cyber Security.* The ASEAN Secretariat. https://asean.org/our-communities/asean-political-security-community/peaceful-secure-and-stable-region/cyber-security/ASEAN

ASEAN Youth Organization. (2023). *ASEAN Cybersecurity Skilling Programme*. ASEAN Youth Organization. https://aseanyouth.net/acsp/

ASEAN-Japan Cybersecurity Capacity Building Centre. (2023). *ASEAN-Japan Cybersecurity Capacity Building Centre*. AJCCBC. https://ajccbc.ncsa.or.th/about-us/

Brandon, J. J. (2018). *Why ASEAN Needs to Invest More in Cybersecurity*. The Asia Foundation. https://asiafoundation.org/why-asean-needs-to-invest-more-in-cybersecurity/

Buzan, B. (1998). *Security: A New Framework for Analysis*. Lynne Rienner Pub.

Caballero-Anthony, M. (2016). *An Introduction to Non-Traditional Security Studies: A Transnational Approach*. Sage Publications.

Cox, R. W. (1996). *Approaches to World Order*. Cambridge University Press.

Deibert, R. J. (2013). *Black Code: Surveillance, Privacy, and the Dark Side of the Internet*. Signal.

Ghosh, N. (2019). *Singapore's Cyber Security Chief Says International Norms, Partnerships Are Key Issues*. The Straits Times. https://www.straitstimes.com/

singapore/singapores-cyber-security-chief-says-international-norms-partnerships-are-key-issues

Gohwong, S. (2019). The State of the Art of Cybersecurity Law in ASEAN. *Asian Crime and Society Review, 6*(2), 12-23. so02.tci-thaijo.org/index.php/IJCLSI/article/view/242594

Hansen, L. (2012). Reconstructing Desecuritisation: The Normative-Political in the Copenhagen School and Directions for How to Apply It. *Review of International Studies, 38*(3), 525-546. http://www.jstor.org/stable/41681477

Heinl, C. (2014). Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime. *Asia Policy, 18,* 131-159. https://dx.doi.org/10.1353/asp.2014.0026

Japan-ASEAN Integration Fund. (2022). *Enhancing Cybersecurity Skills of Professionals in ASEAN*. JAIF Management Team. https://jaif.asean.org/beneficiaries_voice/enhancing-cybersecurity-skills-of-professionals-in-asean/

Nasu, H., McLaughlin, R., Rothwell, D. R., & Tan, S. S. (2019). *The Legal Authority of ASEAN as a Security Institution*. Cambridge University Press. https://doi.org/10.1017/9781108669511

Nye, J. S. (2010). *Cyber Power*. Belfer Center for Science and International Affairs, Harvard Kennedy School. https://www.belfercenter.org/publication/cyber-power

Piiparinen, A. (2016). *China's Secret Weapon in the South China Sea: Cyber Attacks.* The Diplomat. https://thediplomat.com/2016/07/chinas-secret-weapon-in-the-south-china-sea-cyber-attacks/

Sunkpho, J., Ramjan, S., & Ootthamakorn, C. (2018). *Cybersecurity Policy in ASEAN Countries*. 17th Annual Security Conference, Information Institute Conferences. Las Vegas, NV.

The Irrawaddy. (2022). *Myanmar Junta's New Cyber Law to Jail Anyone Using VPN*. The Irrawaddy. https://www.irrawaddy.com/news/burma/myanmar-juntas-new-cyber-law-to-jail-anyone-using-vpn.html

The Southeast Asia Freedom of Expression Network. (2024). *About Us*. Southeast Asia Freedom of Expression Network. https://safenet.or.id/about-us/

Van Raemdonck, N. (2021). *Cyber Diplomacy in Southeast Asia*. EU Cyber Direct. https://eucyberdirect.eu/research/cyber-diplomacy-in-southeast-asia

Waltz, K. N. (1979). *Theory of International Politics*. Addison-Wesley.

Woollacott, E. (2019). *Days After Introduction of 'Cybersecurity' Law, Vietnam Has Facebook in Its Sights*. Forbes Magazine. https://www.forbes.com/sites/emmawoollacott/2019/01/09/days-after-introduction-of-cybersecurity-law-vietnam-has-facebook-in-its-sights/

ASEAN. (2021). *ASEAN Cybersecurity Cooperation Strategy (2021 – 2025)*. ASEAN. https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf

Tan, S. S. (2022, March 8). *ASEAN Cyber Norms Need Broad Stakeholder Engagement*. The Strategist. https://www.aspistrategist.org.au/asean-cyber-norms-need-broad-stakeholder-engagement/

Albahri, D. A. A. (2023, October 5). *Women's Civil Society and Digital Rights Groups Shape South-East Asian Digital Security Training*. UN Women Asia-Pacific. https://asiapacific.unwomen.org/en/stories/news/2023/10/womens-civil-society-and-digital-rights-groups