อาเซียนกับการจัดการปัญหาอาชญากรรมไซเบอร์*

*ลัฐกา เนตรทัศน์**

บทนำ

อาเซียนเป็นภูมิภาคที่มีจำนวนผู้ใช้อินเทอร์เน็ตเติบโตเร็วที่สุดในโลก ซึ่งภายในปี พ.ศ. ๒๕๖๓ ในภูมิภาคอาเซียนจะมีผู้ใช้อินเทอร์เน็ตประมาณ ๔๘๐ ล้านคน นอกจากนี้ ภายในอาเซียนมีประชากรกว่าครึ่งหนึ่งเป็นผู้ใช้สื่อสังคมออนไลน์ (Social Media) จึงทำให้อาเซียนเป็นตลาดสังคมออนไลน์อันดับหนึ่งของโลก และจากการจัดอันดับ ๑๐ ประเทศผู้ใช้เฟซบุ๊ก (Facebook) มากที่สุดในโลก พบว่า ประเทศสมาชิกอาเซียน ๔ ได้แก่ อินโดนีเซีย ฟิลิปปินส์ เวียดนาม และไทยเป็นกลุ่มประเทศที่อยู่ในอันดับดังกล่าว อย่างไรก็ดี ลักษณะของสังคมดิจิทัลในภูมิภาคก็นำมาซึ่งผลประโยชน์ในทางเศรษฐกิจ โดยมีการคาดการณ์ว่าภายในปี พ.ศ. ๒๕๖๘ จะมียอดการใช้จ่ายออนไลน์เพิ่มขึ้นเป็น ๖ เท่า หรือประมาณ ๒๐๐ พันล้านเหรียญสหรัฐ ซึ่งเป็นผลดีในแง่ของเติบโตทางเศรษฐกิจของภูมิภาค[๑]

อย่างไรก็ตาม การเปลี่ยนแปลงไปสู่สังคมดิจิทัล (Digitalization) ก็นำมาซึ่งภัยคุกคามความมั่นคงในลักษณะของการใช้อินเทอร์เน็ตและคอมพิวเตอร์เป็นช่องทางในการโจมตี หรือที่เรียกว่าอาชญากรรมไซเบอร์ (Cyber-Crime)[๒] อันเป็นปัญหาความมั่นคงที่มีลักษณะข้ามชาติหรือข้ามพรมแดน ซึ่งประเทศในภูมิภาคอาเซียนหลายประเทศได้รับผลกระทบจากภัยดังกล่าว เห็นได้จากกรณีการปล่อยมัลแวร์วอนนาคราย (WannaCry) เมื่อปี พ.ศ. ๑๕๖๐ ซึ่งเป็นการโจมตีผ่านระบบอีเมล์ (email) เพื่อเรียกค่าไถ่ข้อมูลจากเจ้าของข้อมูล โดยปรากฏข้อมูลว่าประเทศไทยได้รับความเสียกว่า ๒๐๐ เครื่อง[๓] และประเทศฟิลิปปินส์ถูกโจมตีจากอาชญากรรมไซเบอร์ในปี พ.ศ. ๒๕๖๑ โดยส่วนใหญ่เป็นลักษณะของการฉ้อโกงทางอินเทอร์เน็ต การหลอกลวงให้ได้ไปซึ่งข้อมูลผู้ใช้ ในขณะที่อินโดนีเซียมีการฉ้อโกงทางอินเทอร์เน็ตกว่าร้อยละ ๕๐ ของคดีที่เกี่ยวข้องกับคอมพิวเตอร์ทั้งหมด[๔] นอกจากนี้ยังปรากฏข้อมูลว่าประเทศมาเลเซียถูกจัดอันดับให้เป็นประเทศที่มีความเสี่ยงต่อการก่ออาชญากรรมทางอินเตอร์เน็ตสูงเป็นอันดับ ๖ ของโลก ในขณะเดียวกัน

---

* บทความนี้เผยแพร่เมื่อวันที่ ๒๗ ธันวาคม พ.ศ. ๒๕๖๑

* นักวิเคราะห์และจัดทำข้อมูลกฎหมาย ฝ่ายอาเซียนและกิจการต่างประเทศ สำนักงานคณะกรรมการกฤษฎีกา

[๑] John J. Brandon. (2018, May 9). *Why ASEAN Needs to Invest More in Cybersecurity*. Retrieved December 26, 2018, from asiafoundation: https://asiafoundation.org/2018/05/09/why-asean-needs-to-invest-more-in-cybersecurity/

[๒] Joseph Aghatise. (2006, June). *Cybercrime definition.* Retrieved December 26, 2018, from https://www.researchgate.net/publication/265350281_Cybercrime_definition

[๓] ไทยพีบีเอส. (๑๕ พฤษภาคม ๒๕๖๐). *ไทยโดนแล้ว 200 เครื่อง มัลแวร์เรียกค่าไถ่*. เข้าถึงเมื่อ ๒๖ ธันวาคม ๒๕๖๑ จาก ไทยพีบีเอส: https://news.thaipbs.or.th/content/262480

[๔] คม ชัด ลึก. (๒๗ มิถุนายน ๒๕๖๑). *ดึง 10 ชาติอาเซียนร่วมปราบอาชญากรไซเบอร์*. เข้าถึงเมื่อ ๒๖ ธันวาคม ๒๕๖๑ จาก คม ชัด ลึก: http://www.komchadluek.net/news/crime/332184

เว็บไซต์ของกลุ่มประเทศสมาชิกอาเซียนประมาณ ๒๗๐ แห่งได้ถูกโจมตีด้วยมัลแวร์ (malware) และปรากฏข้อมูลว่าเซิร์ฟเวอร์กว่า ๘,๘๐๐ เครื่องถูกใช้เป็นเครื่องควบคุมและสั่งการมัลแวร์สำหรับใช้ในการโจมตีอีกด้วย[๕]

ดังนั้น อาเซียนในฐานะของสถาบันหลักในภูมิภาคจึงได้ริเริ่มความร่วมมือเพื่อจัดการกับปัญหาอาชญากรรมไซเบอร์ บทความฉบับนี้จึงมีวัตถุประสงค์ในการนำเสนอความร่วมมืออาเซียนด้านการจัดการกับปัญหาดังกล่าว เพื่อเป็นประโยชน์ในการศึกษาและพัฒนาความร่วมมือต่อไป

ความร่วมมือด้านอาชญากรรมไซเบอร์

สำหรับอาเซียน อาชญากรรมไซเบอร์เป็นภัยคุกคามความมั่นคงที่ถูกกำหนดไว้ให้เป็นส่วนหนึ่งของอาชญากรรมข้ามชาติที่สำคัญภายใต้ประชาคมการเมืองและความมั่นคงของอาเซียน[๖] โดยความร่วมมือของอาเซียนด้านการจัดการปัญหาอาชญากรรมไซเบอร์สามารถแบ่งได้เป็น ๓ ลักษณะ ได้แก่ ๑) ความร่วมมือภายในอาเซียนลักษณะของการจัดประชุม ๒) ความร่วมมือในระดับพหุภาคี และ ๓) การจัดทำตราสารอาเซียน

๑) ความร่วมมือภายในอาเซียนลักษณะของการจัดประชุม

ความมั่นคงไซเบอร์ถูกจัดให้เป็นวาระสำคัญภายใต้การประชุมระดับรัฐมนตรีอาเซียนว่าด้วยอาชญากรรมข้ามชาติ (ASEAN Ministerial Meeting on Transnational Crime: AMMTC) และการประชุมเจ้าหน้าที่อาวุโสอาเซียนว่าด้วยอาชญากรรมข้ามชาติ (ASEAN Senior Officials Meeting on Transnational Crime: SOMTC) ซึ่งทั้งสองการประชุมถือได้ว่าเป็นเวทีหลักในการหารือเกี่ยวกับการพัฒนาความร่วมมือระหว่างประเทศสมาชิกอาเซียนเพื่อจัดการกับอาชญากรรมไซเบอร์ นอกจากนี้ ประเด็นเกี่ยวกับการป้องกันอาชญากรรมไซเบอร์ยังได้รับการกล่าวถึงในการประชุมรัฐมนตรีอาเซียนด้านโทรคมนาคมและเทคโนโลยีสารสนเทศ (ASEAN Telecommunications and Information Technology Ministers Meeting: TELMIN) อีกด้วย

---

[๕] ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) . (๒๕ เมษายน ๒๕๖๐). *INTERPOL รายงานคดีอาชญากรรมไซเบอร์ใน ASEAN พบเซิร์ฟเวอร์กว่า 9,000 เครื่องถูกใช้ควบคุมมัลแวร์*. เข้าถึงเมื่อ ๒๖ ธันวาคม ๒๕๖๑ จาก ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) : https://www.thaicert.or.th/newsbite/2017-04-25-02.html

[๖] อาชญากรรมสำคัญภายใต้เสาประชาคมการเมืองและความมั่นคงอาเซียน ประกอบด้วย ๑) การก่อการร้าย ๒) การค้ามนุษย์ ๓) ยาเสพติด ๔) การประมงผิดกฎหมาย ๕) การค้าอาวุธเถื่อนขนาดเล็ก ๖) อาชญากรรมทางไซเบอร์ ๗) โจรสลัด

๑.๑ การประชุมระดับรัฐมนตรีอาเซียนว่าด้วยอาชญากรรมข้ามชาติ (ASEAN Ministerial Meeting on Transnational Crime: AMMTC)

สำหรับการประชุมระดับรัฐมนตรีอาเซียนด้านอาชญากรรมข้ามชาติ (AMMTC) จัดการประชุมครั้งแรกเมื่อปี พ.ศ. ๒๕๔๐ แต่เดิมกำหนดให้มีการจัดประชุมทุก ๒ ปี[๗] ซึ่งในการประชุมแต่ละครั้งที่ประชุมได้ให้ความสำคัญกับปัญหาอาชญากรรมไซเบอร์ผ่านการแลกเปลี่ยนข้อมูลและประสบการณ์ร่วมกันเพื่อหาแนวทางสำหรับการจัดการกับปัญหาดังกล่าว เห็นได้จากแถลงการณ์จากการประชุม AMMTC ครั้งที่ ๓ ในปี พ.ศ. ๒๕๔๔ ที่ประชุมได้แสดงออกถึงความมุ่งมั่นที่จะร่วมมือกันในการต่อต้านอาชญากรรมข้ามชาติ โดยให้มีการร่วมมือกันระหว่างประเทศสมาชิกอาเซียนและการร่วมมือกับประเทศคู่เจรจาในการต่อต้านอาชญากรรมไซเบอร์และการก่อการร้าย[๘] นอกจากนี้ ที่ประชุมได้ตกลงที่จะกำหนดให้ความร่วมมือด้านความมั่นคงไซเบอร์เป็นส่วนหนึ่งในแผนงานเพื่อจัดทำแผนปฏิบัติการอาเซียนเพื่อต่อต้านอาชญากรรมข้ามชาติ (ASEAN Plan of Action to Combat Transnational Crime) เป็นครั้งแรก และเพื่อเป็นการส่งเสริมความร่วมมือในการต่อต้านอาชญากรรมข้ามชาติในทุกรูปแบบ ที่ประชุม AMMTC ได้ร่วมลงนามในลงนามในปฏิญญากัวลาลัมเปอร์ว่าด้วยการต่อต้านอาชญากรรมข้ามชาติ (Kuala Lumpur Declaration in Combating Transnational Crime) ในการประชุมครั้งที่ ๑๐ ณ กรุงกัวลาลัมเปอร์ ประเทศมาเลเซีย โดยส่งเสริมการบังคับใช้กฎหมายอย่างเข้มงวดและสนับสนุนบทบาทของที่ประชุมรัฐมนตรีกฎหมายอาเซียนในการประสานความร่วมมือด้านการส่งผู้ร้ายข้ามแดนในอาเซียน[๙] ทั้งนี้ ความคืบหน้าล่าสุด ที่ประชุม AMMTC ครั้งที่ ๑๒ ซึ่งจัดขึ้นเมื่อวันที่ ๓๑ ตุลาคม พ.ศ. ๒๕๖๑ ณ ประเทศเมียนมา ที่ประชุมยังคงให้ความสำคัญกับการต่อต้านอาชญากรรมไซเบอร์ โดยเน้นย้ำให้อาเซียนดำเนินการตามกรอบความร่วมมือด้านการต่อต้านอาชญากรรมข้ามชาติต่อไป เพื่อเป็นการสร้างความสามัคคีให้กับประเทศสมาชิกและสร้างความเข้มแข็งให้กับภูมิภาค[๑๐]

๑.๒ การประชุมเจ้าหน้าที่อาวุโสอาเซียนว่าด้วยอาชญากรรมข้ามชาติ (ASEAN Senior Officials Meeting on Transnational Crime: SOMTC)

---

[๗] แต่ในการประชุม AMMTC ครั้งที่ ๑๐ ที่ประชุมเห็นชอบให้จัดการประชุมขึ้นปีละหนึ่งครั้ง ตั้งแต่ปี พ.ศ. ๒๕๖๐ เป็นต้นไป

[๘] กระทรวงการต่างประเทศ. (๑๘ ตุลาคม ๒๕๔๔). *ผลการประชุมรัฐมนตรีอาเซียนด้านอาชญากรรมข้ามชาติครั้งที่ 3.* เข้าถึงเมื่อ ๒๖ ธันวาคม ๒๕๖๑ จาก อาร์วายทีไนน์: https://www.ryt9.com/s/ryt9/267415

[๙] ASEAN. (2015, September 29). *Joint Statement of the Tenth ASEAN Ministeral Meeting on Transnational Crime (10TH AMMTC).* Retrieved December 26, 2018, from https://asean.org/wp-content/uploads/2012/05/Adopted-Joint-Statement-of-the-10th-AMMTC.pdf

[๑๐] ASEAN. (2018, October 31). *Joint Statement Twelfth ASEAN Ministerial Meeting on Transnational Crime* Retrieved December 26, 26, from ASEAN: https://asean.org/storage/2012/05/Adopted-Joint-Statement-of-12th-AMMTC.pdf

สำหรับการประชุมเจ้าหน้าที่อาวุโสอาเซียนว่าด้วยอาชญากรรมข้ามชาติ (ASEAN Senior Officials Meeting on Transnational Crime: SOMTC) เป็นอีกหนึ่งกลไกสำคัญของอาเซียนในการการจัดการปัญหาอาชญากรรมไซเบอร์ โดยมีการจัดประชุมครั้งแรกเมื่อปี พ.ศ. ๒๕๔๔ และมีสิงคโปร์เป็นประเทศที่มีบทบาทหลักในการผลักดันความร่วมมือในด้านการต่อต้านการอาชญากรรมไซเบอร์ภายใต้การประชุมดังกล่าว ในการประชุม SOMTC ครั้งที่ ๒ เมื่อวันที่ ๑๖ - ๑๗ พฤษภาคม พ.ศ. ๒๕๔๕ ณ กรุงกัวลาลัมเปอร์ ประเทศมาเลเซีย ที่ประชุมได้รับรองแผนปฏิบัติการอาเซียนเพื่อต่อต้านอาชญากรรมข้ามชาติ โดยแผนปฏิบัติการดังกล่าวได้แบ่งความร่วมมือของประเทศสมาชิกออกเป็น ๕ ประเภท ได้แก่ความร่วมมือด้านการแลกเปลี่ยนข้อมูลข่าวสาร ความร่วมมือด้านข้อกฎหมาย ความร่วมมือด้านการบังคับใช้กฎหมายความร่วมมือด้านการฝึกอบรมและการพัฒนาขีดความสามารถและความร่วมมือนอกภูมิภาค[๑๑] ต่อมาที่ประชุม SOMTC ได้มีมติให้มีการจัดตั้งคณะทำงานด้านอาชญากรรมไซเบอร์ (SOMTC Working Group on Cybercrime: SOMTC WG on CC) ขึ้นในการประชุมครั้งที่ ๑๓ ณ กรุงเวียงจันทน์ ประเทศลาว เมื่อปี พ.ศ. ๒๕๕๖[๑๒] ซึ่งคณะทำงานดังกล่าวมีบทบาทสำคัญอย่างยิ่งในหาข้อสรุปและส่งเสริมความร่วมมือระดับภูมิภาคในการรับมือภัยคุกคามไซเบอร์ตามแนวทางของแผนปฏิบัติการอาเซียนเพื่อต่อต้านอาชญากรรมข้ามชาติ โดยการประชุมครั้งแรกของคณะทำงานฯ เกิดขึ้นในเดือนพฤษภาคม พ.ศ. ๒๕๕๗ ณ ประเทศสิงคโปร์[๑๓]

๑.๓ การประชุมรัฐมนตรีอาเซียนด้านโทรคมนาคมและเทคโนโลยีสารสนเทศ (ASEAN Telecommunications and Information Technology Ministers Meeting: TELMIN)

ประเด็นเรื่องการจัดการปัญหาอาชญากรรมไซเบอร์ได้รับการกล่าวถึงในที่ประชุมรัฐมนตรีอาเซียนด้านโทรคมนาคมและเทคโนโลยีสารสนเทศ (ASEAN Telecommunications and Information Technology Ministers Meeting: TELMIN) โดยสถานะความคืบหน้าล่าสุด การประชุมรัฐมนตรีอาเซียน

---

[๑๑] ASEAN. (n.d.). *Senior Officials Meeting on Transnational Crime (SOMTC).* Retrieved December 26, 2018, from ASEAN: https://asean.org/asean-political-security-community/asean-ministerial-meeting-on-transnational-crime-ammtc/senior-officials-meeting-on-transnational-crime-somtc/

[๑๒] ปัจจุบันการประชุม SOMTC มีคณะทำงานทั้งสิ้น ๖ คณะ ดังนี้

๑. คณะทำงานด้านการค้ามนุษย์ (SOMTC Working Group on Trafficking in Persons :SOMTC WG on TIP)

๒. คณะทำงานด้านกาต่อต้านการก่อการร้าย (SOMTC Working Group on Counter Terrorism :SOMTC WG on CT)

๓. คณะทำงานด้านอาชญากรรมไซเบอร์ (SOMTC Working Group on Cybercrime: SOMTC WG on CC)

๔. คณะทำงานด้านการค้าอาวุธ (SOMTC Working Group on Arms Smuggling: SOMTC WG on AS)

๕. คณะทำงานด้านการค้าสัตว์ป่าและไม้ป่าผิดกฎหมาย (SOMTC Working Group on Illicit Trafficking of Wildlife and Timber: SOMTC WG on ITWT)

๖. หัวหน้าหน่วยงานพิเศษ (Heads of Specialist Trafficking Units: HSU)

[๑๓] ปัจจุบัน (พ.ศ. ๒๕๖๑) คณะทำงานด้านอาชญากรรมไซเบอร์ (SOMTC on CC) ได้มีการจัดประชุมขึ้นทั้งสิ้น ๕ ครั้ง โดยครั้งล่าสุดจัดขึ้นเมื่อวันที่ ๒๔ กันยายน พ.ศ. ๒๕๖๑ ณ เมืองปุตราจายา ประเทศมาเลเซีย

ด้านโทรคมนาคมและเทคโนโลยีสารสนเทศ (TELMIN) ครั้งที่ ๑๔ เมื่อเดือนมกราคม ๒๕๕๘ ที่ประชุมเห็นชอบให้รวมประเด็นความมั่นคงไซเบอร์ในแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารของอาเซียนฉบับที่ ๒ ระหว่างปี พ.ศ. ๒๕๕๙ - ๒๕๖๓ (ASEAN ICT Masterplan 2020) โดยแผนแม่บทดังกล่าวได้กำหนดยุทธศาสตร์ (Strategic Thrusts) ด้านความปลอดภัยและหลักประกันด้านข้อมูลข่าวสาร ซึ่งประกอบด้วยการพัฒนาหลักการด้านความปลอดภัยของข้อมูลระดับภูมิภาค และส่งเสริมความเข้มแข็งและประสิทธิภาพของความร่วมมือเพื่อตอบสนองต่อสถานการณ์ฉุกเฉินด้านไซเบอร์อย่างทันท่วงที โดยมีเป้าหมายเพื่อเสริมสร้างความเชื่อมั่นให้กับเศรษฐกิจดิจิทัลของอาเซียน และปรับปรุงความร่วมมือในการรับมือกับสถานการณ์ฉุกเฉินด้านไซเบอร์ของภูมิภาคให้มีประสิทธิภาพยิ่งขึ้น[๑๔]

๒) ความร่วมมือระดับพหุภาคี

๒.๑) การประชุมอาเซียนว่าด้วยความร่วมมือด้านการเมืองและความมั่นคงในภูมิภาคเอเชีย - แปซิฟิก (ASEAN Regional Forum: ARF)

การประชุม ARF เป็นเวทีที่จัดขึ้นเพื่อให้อาเซียนได้มีปฏิสัมพันธ์กับประเทศนอกภูมิภาคในการรักษาไว้ซึ่งผลประโยชน์ร่วมกัน โดยการประชุม ARF มีการดำเนินงาน ๓ ขั้นตอน ได้แก่ มาตรการเสริมสร้างความไว้เนื้อเชื่อใจ (Confidence Building Measures: CBMs) การทูตเชิงป้องกัน (Preventive Diplomacy : PD) และแนวทางเรื่องปญหาความขัดแยง (Approaches to Conflict)[๑๕]

สำหรับกลไกการทำงานด้านการต่อต้านอาชญากรรมไซเบอร์ นอกจากการประชุมหลักของ ARF ที่จัดขึ้นเป็นประจำทุกปีแล้ว ที่ประชุม ARF ได้มีการจัดประชุมเวทีเฉพาะด้าน โดยใช้ชื่อว่า การประชุมระหว่างปีกิจกรรมว่าด้วยการต่อต้านการก่อการร้ายและอาชญากรรมข้ามชาติ (ASEAN Regional Forum Inter-Sessional Meeting on Counter Terrorism and Transnational Crime: ARF ISM on CTTC) เพื่อเป็นเวทีเฉพาะสำหรับการหารือและแลกเปลี่ยนประสบการณ์ระหว่างประเทศสมาชิกในการป้องกันและปราบปรามการก่อการร้ายและการก่ออาชญากรรมไซเบอร์ อย่างไรก็ดี ภายใต้การประชุมหลักของ ARF และการประชุมระหว่างปีกิจกรรม ที่ประชุมได้ให้ความสำคัญกับประเด็นปัญหาอาชญากรรมไซเบอร์อยู่เสมอมาด้วยออกแถลงการณ์เพื่อแสดงถึงเจตนารมณ์การส่งเสริมความร่วมมือระหว่างประเทศสมาชิกด้านความมั่นคงไซเบอร์ และในปี พ.ศ. ๒๕๕๕ แถลงการณ์ของที่ประชุม ARF ระบุอย่างชัดเจนถึงเป้าหมายภายในของอาเซียนในการรับมือกับปัญหาภัยคุกคามทางไซเบอร์ รวมถึงการสร้างมาตรการส่งเสริม

---

[๑๔] Ministry of Information and Communications the S. R. of Viet Nam. (2015). *THE ASEAN ICT Masterplan 2020.* Retrieved December 27, 2018, from ASEAN: https://www.asean.org/storage/images/2015/November/ICT/15b%20--%20AIM%202020_Publication_Final.pdf

[๑๕] กองอาเซียน กรมอาเซียน. (ตุลาคม ๒๕๕๕). *การประชุมอาเซียนว่าด้วยความร่วมมือด้านการเมืองและความมั่นคงในภูมิภาคเอเชีย - แปซิฟิก (ASEAN Regional Forum – ARF).* เข้าถึงเมื่อ ๒๖ ธันวาคม ๒๕๖๑ จาก กรมบังคับคดี : http://www.led.go.th/asean/pdf/4/4-3.pdf

ความไว้เนื้อเชื่อใจระหว่างกันอย่างเป็นรูปธรรม[๑๖] นอกจากนี้ ที่ประชุมระหว่างปีกิจกรรมฯ (ARF ISM on CTTC) ได้มีการจัดทำแผนงานต่อต้านการก่อการร้ายและอาชญากรรมข้ามชาติ (ARF Work Plan on Counter Terrorism and Transnational Crime) เพื่อกำหนดกรอบการดำเนินงานให้มีความชัดเจนยิ่งขึ้น โดยแผนงานดังกล่าวได้ระบุถึงปัญหาอาชญากรรมข้ามชาติที่มีความสำคัญสูง ได้แก่ ๑) การค้ายาเสพติด ๒) การใช้อาวุธเคมี ชีวภาพ รังสี และนิวเคลียร์ ๓) ความมั่นคงทางไซเบอร์และการใช้เทคโนโลยีสารสนเทศเพื่อการก่อการร้าย ๕) การต่อต้านการเผยแพร่แนวคิดหัวรุนแรง และ ๖) การค้ามนุษย์[๑๗]

๒.๒ ความร่วมมือกับประเทศนอกภูมิภาค

นอกจากความร่วมมือภายในภูมิภาค อาเซียนได้ขยายความร่วมมือด้านความมั่นคงทางไซเบอร์กับประเทศคู่เจรจาอีกหลายประเทศ เห็นได้จากความร่วมมือกับประเทศจีน ญี่ปุ่น และเกาหลีใต้ โดยจัดเป็นการประชุมระดับรัฐมนตรีอาเซียน + ๓ ด้านอาชญากรรมข้ามชาติ (AMMTC + 3) โดยที่ประชุมได้ร่วมกันแลกเปลี่ยนมุมมองและแนวทางในการพัฒนาความร่วมมือเพื่อร่วมกันจัดการปัญหาอาชญากรรมข้ามชาติในภูมิภาค ทั้งในด้านการแลกเปลี่ยนข้อมูลข่าวสาร การแลกเปลี่ยนประสบการณ์และบทเรียนจากการปฏิบัติ รวมถึงการสนับสนุนการพัฒนาศักยภาพของหน่วยงานด้านการบังคับใช้กฎหมายของประเทศสมาชิกอาเซียน

นอกจากนี้ อาเซียนได้สร้างความร่วมมือในระดับทวิภาคีกับประเทศคู่เจรจาเพื่อให้เกิดการหารือกันอย่างใกล้ชิดในประเด็นเกี่ยวกับการจัดการปัญหาอาชญากรรมไซเบอร์ เห็นได้จากความร่วมมือระหว่างอาเซียนกับญี่ปุ่น โดยความคืบหน้าล่าสุดทั้งสองฝ่ายริเริ่มแนวคิดที่จะจัดตั้งศูนย์ความร่วมมืออาเซียน - ญี่ปุ่น เพื่อพัฒนาบุคลากรด้านความมั่นคงทางไซเบอร์ใช้ชื่อว่า ศูนย์สร้างขีดความสามารถด้านความมั่นคงทางไซเบอร์ (ASEAN-Japan Cyber-security Capacity Building Centre) ตามมติของที่ประชุมรัฐมนตรีอาเซียนด้านโทรคมนาคมและเทคโนโลยีสารสนเทศร่วมกับประเทศญี่ปุ่น[๑๘] นอกจากนี้ ทั้งสองฝ่ายได้ร่วมกันออกแถลงการณ์ร่วมเพื่อส่งเสริมความร่วมมือด้านการต่อต้านการก่อการร้ายและอาชญากรรมข้ามชาติ พร้อมทั้งยืนยันว่าจะส่งเสริมความมั่นคงปลอดภัยของการใช้เทคโนโลยีสารสนเทศและการสื่อสาร และต่อต้านอาชญากรรมไซเบอร์ในทุกรูปแบบ รวมทั้งยังร่วมกันจัดการประชุมหารือ

---

[๑๖] กองบรรณาธิการจุลสารจับตาอาเซียน. (๓๐ มิถุนายน ๒๕๕๙). *อาเซียนกับความร่วมมือด้านความมั่นคงไซเบอร์*. เข้าถึงเมื่อ ๒๖ ธันวาคม ๒๕๖๑ จาก http://aseanwatch.org/2016/06/30/current-issue-0259/

[๑๗] กรมอาเซียน กระทรวงต่างประเทศ. (๑๑ มิถุนายน ๒๕๕๘). *การประชุม ARF Inter-Sessional Meeting on Counter Terrorism and Transnational Crime ครั้งที่ ๑๓ ที่เมืองหนานหนิง*. เข้าถึงเมื่อ ๒๖ ธันวาคม ๒๕๖๑ จาก กรมอาเซียน กระทรวงต่างประเทศ: http://www.mfa.go.th/asean/th/news/2352/57011-การประชุม-ARF-Inter-Sessional-Meeting-on-Counter-T.html

[๑๘] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (๒๙ มีนาคม ๒๕๖๑). เรียกใช้เมื่อ ๒๙ ธันวาคม ๒๕๖๑ จาก สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์: https://www.etda.or.th/content/mdes-to-launch-ajccbc-this-june-in-preparation-for-cyber-attacks.html

อาเซียน - ญี่ปุ่นว่าด้วยอาชญากรรมไซเบอร์ (ASEAN-Japan Cybercrime Dialogue) เพื่อเป็นเวทีหารือกรอบความร่วมมือและส่งเสริมศักยภาพการรับมือกับภัยคุกคามไซเบอร์ระหว่างกัน

อย่างไรก็ดี อาเซียนไม่เพียงแต่จะสร้างความร่วมมือกับประเทศคู่เจรจาในภูมิภาคเอเชียนั้น หากแต่ยังขยายความร่วมมือด้านความมั่นคงทางไซเบอร์ไปยังประเทศคู่เจรจานอกภูมิภาค อาทิ สหรัฐอเมริกา ออสเตรเลีย รัสเซีย สำหรับความร่วมมือระหว่างอาเซียนและสหรัฐฯ ภายใต้การประชุมเจ้าหน้าที่อาวุโสอาเซียน – สหรัฐฯ ครั้งที่ ๓๑ ที่จัดขึ้น ณ กรุงกัวลาลัมเปอร์ ประเทศมาเลเซีย สหรัฐฯ ยังคงยืนยันที่จะให้การสนับสนุนอาเซียนในการต่อต้านการก่อการร้ายและอาชญากรรมไซเบอร์[๑๙] ด้านความร่วมมือระหว่างอาเซียนและออสเตรเลีย เมื่อวันที่ ๑๔ กุมภาพันธ์ พ.ศ. ๒๕๖๑ มีการจัดประชุมเชิงปฏิบัติการว่าด้วยความร่วมมือระหว่างประเทศสมาชิกอาเซียนกับออสเตรเลียด้านความมั่นคงปลอดภัยทางไซเบอร์ โดยมีวัตถุประสงค์เพื่อเสริมสร้างความเข้าใจระหว่างประเทศสมาชิกอาเซียนและออสเตรเลียเกี่ยวกับกลไกและกฎหมายที่เกี่ยวข้องกับอาชญากรรมทางไซเบอร์ รวมถึงส่งเสริมความร่วมมือด้านกระบวนการยุติธรรม ตลอดจนการแลกเปลี่ยนแนวปฏิบัติเกี่ยวกับกลไกกำกับดูแลด้านไซเบอร์และปฏิบัติการรับมือกรณีที่มีการโจมตีทางไซเบอร์ในระดับภูมิภาค[๒๐] นอกจากนี้ อาเซียนและรัสเซียยังได้ริเริ่มแนวคิดที่จะจัดทำความตกลงด้านความมั่นคงทางไซเบอร์ขึ้นอันเนื่องมาจากการที่สิงคโปร์และมาเลเซียถูกโจมตีทางไซเบอร์เมื่อช่วงต้นปี พ.ศ. ๒๕๖๑ อีกด้วย[๒๑]

๓. การจัดทำตราสารอาเซียน

เพื่อเป็นการเสริมสร้างความร่วมมือในการต่อต้านอาชญากรรมทางไซเบอร์ อาเซียนได้มีการจัดทำตราสารความมั่นคงในลักษณะของปฏิญญา (Declaration) โดยที่ประชุมสุดยอดผู้นำอาเซียนครั้งที่ ๓๑ ระหว่างวันที่ ๑๓ - ๑๔ พฤศจิกายน ๒๕๖๐ ประเทศสมาชิกอาเซียนจึงได้รับรองปฏิญญาอาเซียนว่าด้วยการป้องกันและต่อต้านอาชญากรรมไซเบอร์ (ASEAN Declaration to Prevent and Combat Cybercrime) ณ กรุงมะนิลา สาธารณรัฐฟิลิปปินส์

ปฏิญญาอาเซียนว่าด้วยการป้องกันและต่อต้านอาชญากรรมไซเบอร์สนับสนุนการร่างกรอบการทำงานระดับภูมิภาคเพื่อสร้างความร่วมมือระหว่างประเทศสมาชิกและการกำหนดแผนปฏิบัติการระดับชาติในการป้องกันและต่อต้านอาชญากรรมทางไซเบอร์ รวมถึงการให้ความช่วยเหลือ

---

[๑๙] กองเศรษฐกิจ กรมอาเซียน. (๒๒ สิงหาคม ๒๕๖๑). *ความสัมพันธ์อาเซียน-สหรัฐฯ*. เข้าถึงเมื่อ ๒๖ ธันวาคม ๒๕๖๑ จาก กระทรวงต่างประเทศ: http://www.mfa.go.th/asean/contents/files/partnership-20180827-161020-142446.pdf

[๒๐] ศูนย์ข้อมูลข่าวสารอาเซียน กรมประชาสัมพันธ์. (๑๔ กุมภาพันธ์ ๒๕๖๑). *อาเซียน - ออสเตรเลียประชุมความร่วมมือด้านความมั่นคงปลอดภัยทางไซเบอร์อาเซียน*. เข้าถึงเมื่อ ๒๖ ธันวาคม ๒๕๖๑ จาก ศูนย์ข้อมูลข่าวสารอาเซียน กรมประชาสัมพันธ์: http://www.aseanthai.net/ewt_news.php?nid=7985&filename=index

[๒๑] ผู้จัดการออนไลน์. (๒ สิงหาคม ๒๕๖๑). *อาเซียนเล็งทำ "ข้อตกลงความมั่นคงทางไซเบอร์" กับรัสเซีย หลังถูกแฮกหลายครั้ง*. เข้าถึงเมื่อ ๒๖ ธันวาคม ๒๕๖๑ จาก ผู้จัดการออนไลน์: https://mgronline.com/around/detail/9610000076586

ด้านผู้เชี่ยวชาญทางเทคนิคในการป้องกันและต่อต้านอาชญากรรมไซเบอร์ อันเป็นการยกระดับความร่วมมือระหว่างประเทศสมาชิกอาเซียนและประเทศคู่เจรจา รวมทั้งหน่วยงานและองค์กรที่เกี่ยวข้องทั้งในระดับภูมิภาคและนานาชาติ เช่น หัวหน้าตำรวจอาเซียน หัวหน้าตำรวจภาคพื้นยุโรป และองค์การตำรวจสากล นอกจากนี้ ปฏิญญาดังกล่าวยังมีวัตถุประสงค์ในการเสริมสร้างความมั่นคงทางเทคโนโลยี การป้องกันและความสามารถในการแก้ไขปัญหาเกี่ยวกับอาชญากรรมทางไซเบอร์ และเพื่อพัฒนาขีดความสามารถของอาเซียนในการสร้างและพัฒนาศักยภาพในการต่อสู้กับอาชญากรรมทางไซเบอร์ อย่างไรก็ตาม ปฏิญญาดังกล่าวเป็นการแสดงเจตนารมณ์ร่วมกันระหว่างประเทศสมาชิกในการสร้างความร่วมมือระหว่างกัน ในการป้องกันและต่อต้านอาชญากรรมทางไซเบอร์ในภูมิภาคอาเซียน โดยในทางกฎหมายระหว่างประเทศการจัดทำปฏิญญาในลักษณะนี้ไม่ก่อให้เกิดพันธกรณีระหว่างประเทศที่ร่วมรับรองปฏิญญา[๒๒]

บทสรุป

อาเซียนมีมาตรการสำหรับจัดการกับปัญหาอาชญากรรมไซเบอร์ ๓ ลักษณะ ได้แก่ ๑) ความร่วมมือภายในอาเซียนในลักษณะของการจัดประชุม แบ่งออกเป็นการประชุมระดับรัฐมนตรีอาเซียนว่าด้วยอาชญากรรมข้ามชาติ (ASEAN Ministerial Meeting on Transnational Crime: AMMTC) การประชุมเจ้าหน้าที่อาวุโสอาเซียนว่าด้วยอาชญากรรมข้ามชาติ (ASEAN Senior Officials Meeting on Transnational Crime: SOMTC) และการประชุมรัฐมนตรีอาเซียนด้านโทรคมนาคมและเทคโนโลยีสารสนเทศ (ASEAN Telecommunications and Information Technology Ministers Meeting: TELMIN) โดยการประชุมดังกล่าวเป็นพื้นที่ให้ประเทศสมาชิกอาเซียนได้มาแลกเปลี่ยนประสบการณ์เพื่อแสวงหาแนวปฏิบัติที่เป็นเลิศในด้านการจัดการปัญหาอาชญากรรมในภูมิภาค ๒) ความร่วมมือในระดับพหุภาคี แบ่งออกเป็นการประชุมอาเซียนว่าด้วยความร่วมมือด้านการเมืองและความมั่นคงในภูมิภาคเอเชีย - แปซิฟิก (ASEAN Regional Forum: ARF) และความร่วมมือกับประเทศคู่เจรจา อาทิ จีน ญี่ปุ่น เกาหลีใต้ สหรัฐอเมริกา ออสเตรเลีย รัสเซีย เป็นต้น และ ๓) การจัดทำตราสารอาเซียน ได้แก่ ปฏิญญาอาเซียนว่าด้วยการป้องกันและต่อต้านอาชญากรรมไซเบอร์ โดยที่ปฏิญญาดังกล่าวไม่ได้มีผลผูกพันประเทศสมาชิกที่รับรองแต่อย่างใด

[๒๒] จันทพร ศรีโพน. (๑๒ มกราคม ๒๕๖๑). *ปฏิญญาอาเซียนว่าด้วยการป้องกันและต่อต้านอาชญากรรมไซเบอร์และบทวิเคราะห์กฎหมายไทยที่เกี่ยวข้อง*. เข้าถึงเมื่อ ๒๗ ธันวาคม ๒๕๖๑ จาก Law For ASEAN: https://lawforasean.com/blog/2018/01/asean-declaration-to-prevent-and-combat-cybercrime-and-the-analysis-of-relevant-thai-laws