TRACK II MONITOR
Strategic Studies Center
National Defence Studies Institute
Royal Thai Armed Forces Headquarters
ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ
กองบัญชาการกองทัพไทย

Track II Monitor โดย ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ ฉบับที่ ๒/๖๙

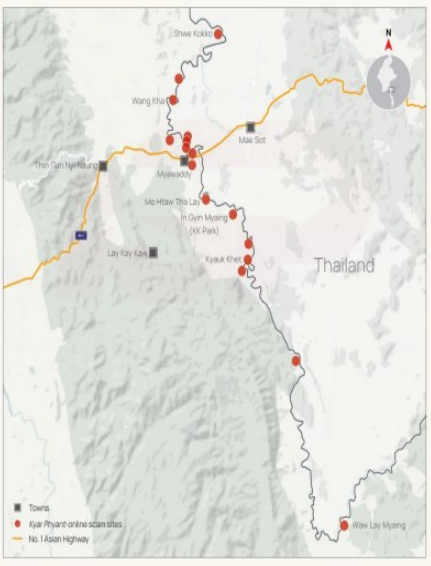
ศูนย์ Scammer ในพื้นที่ชายแดนและภัยคุกคามทางไซเบอร์ : ข้อพิจารณาด้านนโยบายสำหรับประเทศไทย

ในช่วง ๕ ปีที่ผ่านมา ศูนย์ Scammer ในเอเชียตะวันออกเฉียงใต้ได้ย้ายฐานจากกัมพูชาไปยังลาวและพื้นที่ชายแดนของเมียนมาอย่างเป็นระบบ เพื่อหลีกเลี่ยงแรงกดดันจากการบังคับใช้กฎหมายและใช้ประโยชน์จากเขตอำนาจรัฐที่อ่อนแอและความไร้เสถียรภาพทางการเมือง ประเทศไทยอยู่ศูนย์กลางของภูมิทัศน์นี้ที่เป็นทั้งทางผ่าน เป้าหมาย ที่เอื้อต่อเครือข่ายอาชญากรรมดังกล่าว ขณะที่การตอบสนองของรัฐยังเป็นเชิงรับและมีข้อจำกัดทางการเมือง เมื่อศูนย์ Scammer ขยับเข้าใกล้ชายแดนไทยมากขึ้น ความเสี่ยงต่อความมั่นคงดิจิทัล ความมั่นคงของมนุษย์และภาพลักษณ์ระหว่างประเทศของไทยจึงเพิ่มสูงขึ้นอย่างมีนัยสำคัญอีกด้วย...

การเคลื่อนย้ายและผลกระทบของศูนย์ Scammer ตามแนวชายแดน

ศูนย์ Scammer ในเอเชียตะวันออกเฉียงใต้มีการเคลื่อนย้ายอย่างเป็นระบบตามรูปแบบ “ปราบปราม–ปรับตัว–ย้ายฐาน” เพื่อตอบสนองต่อแรงกดดันจากการบังคับใช้กฎหมาย โดยอาศัยช่องโหว่ทางกฎหมาย เขตอำนาจที่เปราะบาง และการคุ้มครองจากชนชั้นนำ **เมืองสีหนุวิลล์**เป็นกรณีศึกษาสำคัญที่สะท้อนการผสมผสานระหว่างการลงทุนที่ไม่มีการควบคุมกำกับ การครอบงำรัฐโดยชนชั้นนำ และการสมรู้ร่วมคิดของเจ้าหน้าที่รัฐ ส่งผลให้ศูนย์ Scammer และการค้ามนุษย์ขยายตัวอย่างรวดเร็ว แม้จะมีการปราบปรามเป็นระยะ ๆ แต่การขาดความต่อเนื่องทำให้เครือข่ายอาชญากรรมสามารถย้ายและขยายตัวต่อไปได้ ซึ่งสะท้อนความล้มเหลวเชิงโครงสร้างของรัฐในการจัดการอาชญากรรมข้ามชาติ อย่างไรก็ตาม เมื่อกัมพูชาเผชิญแรงกดดันจากประชาคมระหว่างประเทศเพิ่มมากขึ้น และเริ่มดำเนินมาตรการปราบปรามในระดับจำกัดภายใต้แรงกดดันจากจีน กลุ่มอาชญากรรมข้ามชาติ (Transnational Organised Crime : TOC) จึงเริ่มย้ายฐานปฏิบัติการออกไป โดยระยะแรกมุ่งสู่ลาว และต่อมาเข้าสู่เมียนมา โดยเฉพาะพื้นที่ที่ได้รับผลกระทบจากสงครามกลางเมืองภายหลังรัฐประหาร

การล่มสลายของธรรมาภิบาลในบางพื้นที่ของ**เมียนมา**และการเกิดเขตปกครองตนเองของกลุ่มติดอาวุธ ทำให้เกิดความคลุมเครือด้านเขตอำนาจและแรงจูงใจทางเศรษฐกิจ จนพื้นที่เหล่านี้กลายเป็น แหล่งหลบภัยของขบวนการ Scammer คริปโตสแกม และขบวนการบังคับใช้แรงงานทาสเพื่อการฉ้อโกงออนไลน์ในเมียนมา โดยมีเมืองเล่าก์ก่ายเป็นศูนย์กลางสำคัญหลังปฏิบัติการ ๑๐๒๗ และแรงกดดันจากจีน เครือข่ายอาชญากรรมได้ย้ายฐานจากรัฐฉานเหนือสู่รัฐกะเหรี่ยงอย่างเป็นระบบ โดยเฉพาะเมืองชเวก๊กโก่ (Shwe Kokko) ภายใต้การคุ้มครองของกองกำลังแห่งชาติกะเหรี่ยง (Karen National Army : KNA) หรือกองกำลังพิทักษ์ชายแดน (Border Guard Force : BGF)



Source: ISP-Myanmar (2025) Scam Cancer in Myanmar, ISP-Myanmar. Available at: https://ispmyanmar.com/scam-cancer-in-myanmar/ (Accessed: 4 July 2025). Sriyai, S. “Hammerli”. (อ้างถึงใน Sriyai, 2025)

การย้ายฐานดังกล่าวเป็นยุทธศาสตร์ที่เลือกพื้นที่ซึ่งหลักนิติธรรมอ่อนแอและมีการคุ้มครองจากกองกำลังติดอาวุธ เอื้อต่อการค้ามนุษย์และการเงินข้ามพรมแดน โดยเฉพาะตามแนวชายแดนไทย–เมียนมา ขณะเดียวกัน ผลกระทบด้านมนุษยธรรมทวีความรุนแรง เหยื่อจากหลายประเทศถูกหลอก ค้ามนุษย์ และบังคับใช้แรงงานในอุตสาหกรรมหลอกลวงมูลค่าหลายพันล้านดอลลาร์ สะท้อนจุดอ่อนเชิงโครงสร้างของธรรมาภิบาลในภูมิภาคและความจำเป็นเร่งด่วนของความร่วมมือข้ามพรมแดนอย่างจริงจัง

ข้อจำกัดและจุดอ่อนภายในประเทศของไทย

ประเทศไทยมีพรมแดนติดกับเมียนมายาวถึง ๒,๔๑๖ กิโลเมตร และมีลักษณะโปร่ง เปิด ทำให้ได้รับผลกระทบจากปฏิบัติการหลอกลวงมากขึ้นทั้งทางตรงและทางอ้อม ในด้านหนึ่ง ไทยเป็นทางผ่านและศูนย์กลางด้านโลจิสติกส์ เป็นเส้นทางสำหรับการค้ามนุษย์และการฟอกเงิน ขณะเดียวกัน ประชากรไทยจำนวนมากได้รับผลกระทบจากการค้ามนุษย์และเป็นเป้าหมายหลักของขบวนการหลอกลวงเหล่านี้

จากรายงานในช่วงปี ๒๐๒๓ – ๒๐๒๔ ประเทศไทยเป็นประเทศที่มีอัตราการรับสายโทรศัพท์หลอกลวงสูงที่สุดในเอเชีย และพบการฉ้อโกงทางการเงินและการขโมยข้อมูลส่วนบุคคลมากที่สุด โดยเฉพาะในกลุ่มผู้สูงอายุซึ่งได้รับผลกระทบอย่างมาก ทำให้เกิดผลกระทบทางจิตใจอย่างรุนแรงต่อกลุ่มผู้ได้รับผลกระทบดังกล่าว

ในขณะเดียวกันพื้นที่พรมแดนที่หละหลวมและการบังคับใช้กฎหมายที่กระจัดกระจาย ทำให้พื้นที่ชายแดนอย่างแม่สอด แม่สาย และด่านเจดีย์สามองค์ ยังคงเป็นเส้นทางผ่านสำคัญของการค้ามนุษย์และอาชญากรรมข้ามชาติ เหยื่อจำนวนมากถูกชักชวนผ่านโฆษณาการรับสมัครงานปลอม เดินทางผ่านกรุงเทพมหานคร และเดินทางข้ามแดนโดยไม่ผ่านจุดตรวจหรือตรวจสอบอัตลักษณ์อย่างเป็นระบบ

แม้ประเทศไทยจะมีการพัฒนาโครงสร้างพื้นฐานดิจิทัลอย่างรวดเร็ว แต่อัตราการพัฒนาด้านกฎระเบียบและการกำกับดูแลยังไม่สอดคล้องกับระดับการเชื่อมต่อของสังคม ส่งผลให้มาตรการด้านความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคลยังขาดประสิทธิภาพ ความเชื่อมั่นของประชาชนต่อระบบดิจิทัลของรัฐอยู่ในระดับต่ำจากเหตุการณ์ข้อมูลรั่วไหลอย่างต่อเนื่อง

ขณะเดียวกัน นโยบายด้าน Entertainment Complex และคาสิโนอาจยิ่งเพิ่มความเสี่ยงด้านการฟอกเงิน หากขาดกรอบการกำกับดูแลที่เข้มงวด สอดคล้องกับข้อค้นพบของสำนักงานว่าด้วยยาเสพติดและอาชญากรรมแห่งสหประชาชาติ (United Nations Office on Drugs and Crime : UNOCD) ที่ชี้ว่าคาสิโนเป็นหนึ่งในช่องทางสำคัญของขบวนการหลอกลวงในการซ่อนและโอนย้ายเงินผิดกฎหมาย

นอกจากนี้ การรู้เท่าทันดิจิทัลของประชาชน โดยเฉพาะผู้สูงอายุและประชาชนในชนบทยังอยู่ในระดับต่ำ ทำให้กลุ่มเปราะบางเหล่านี้ตกเป็นเป้าหมายของอาชญากรรมไซเบอร์ได้โดยง่าย สะท้อนถึงความจำเป็นเร่งด่วนในการเสริมสร้างความมั่นคงปลอดภัยไซเบอร์และการเสริมสร้างความรู้เท่าทันทางดิจิทัลอย่างทั่วถึง

ข้อจำกัดข้ามพรมแดนและข้อจำกัดทางการเมือง

ศูนย์ Scammer ข้ามชาติเป็นปัญหาที่ปราบปรามได้ยาก เนื่องจากเครือข่ายอาชญากรรมดำเนินการในพื้นที่บริเวณชายแดนที่ขาดการกำกับดูแล และอาศัยช่องว่างของระบบกฎหมาย เขตอำนาจศาล และเจตจำนงทางการเมือง ความร่วมมือระดับภูมิภาคจึงมีความจำเป็นอย่างยิ่ง อย่างไรก็ตาม อาเซียนยังขาดกรอบในการบังคับใช้ที่เป็นรูปธรรมและมีผลผูกพัน แม้จะมีแผนแม่บทดิจิทัลอาเซียน ๒๐๒๕ (ASEAN Digital Masterplan 2025) และอนุสัญญาอาเซียนต่อต้านการค้ามนุษย์โดยเฉพาะสตรี และเด็ก (ASEAN Convention Against Trafficking in Persons, Especially Women and Children : ACTIP) แต่การปฏิบัติจริงยังขาดความต่อเนื่อง การส่งผู้ร้ายข้ามแดนยังมีความล่าช้าและการสอบสวนร่วมเกิดขึ้นน้อยมาก

นอกจากนี้ ยังไม่อาจมองข้ามบทบาทการประสานงานของจีน โดยเฉพาะอย่างยิ่ง ความร่วมมือทวิภาคีระหว่างจีนกับประเทศอาเซียนที่ทวีความเข้มข้นขึ้น เช่น ปฏิบัติการร่วมจีน–กัมพูชาในการกวาดล้างศูนย์ Scammer ที่สีหนุวิลล์ และความร่วมมือระหว่างไทยกับจีนในการปราบปรามแก๊งหลอกลวงและการค้ามนุษย์ในพื้นที่เมียวดี–แม่สอด

แม้จีนจะมีบทบาทสำคัญในการประสานความร่วมมือทวิภาคีกับประเทศอาเซียนในการปราบปรามศูนย์ Scammer แต่การให้จีนเป็นผู้นำกลับก่อให้เกิดความกังวลด้านอธิปไตยประเทศภาคี อันเนื่องมาจากความไม่สมดุลเชิงอำนาจ และปัญหาความคลุมเครือด้านเขตอำนาจศาล ซึ่งทำให้เหยื่อจำนวนมากยังตกอยู่ในสภาวะสูญญากาศทางกฎหมาย และผู้กระทำผิดมีโอกาสกลับมาก่ออาชญากรรมซ้ำ

ในกรณีของไทย การตอบสนองต่อปัญหามักเป็นไปตามการคำนวณทางการเมือง พลวัตดังกล่าวสะท้อนให้เห็นถึงความล้มเหลวเชิงโครงสร้างของกรอบความร่วมมือด้านการบังคับใช้กฎหมายต่อการรับมือกับอาชญากรรมข้ามชาติยังคงขึ้นอยู่กับผลประโยชน์ของชนชั้นนำและความสะดวกทางการทูต เมื่อขาดกลไกพหุภาคีที่เป็นสถาบันอย่างเป็นทางการ การบังคับใช้กฎหมายก็จะยังคงกระจัดกระจาย เฉพาะกิจ และเปิดช่องให้ถูกแทรกแซงทางการเมืองได้ง่าย

ข้อเสนอแนะ

ประเทศไทยควรเปลี่ยนจากมาตรการเชิงรับไปสู่ยุทธศาสตร์เชิงรุกแบบองค์รวมในการรับมือภัยคุกคามจากขบวนการศูนย์ Scammer ตามแนวชายแดน โดยยึดแนวทางพหุภาคีนิยมเป็นแกนกลางเพื่อสร้างการตอบสนองเชิงระบบ ร่วมกับประเทศในภูมิภาค ควบคู่กับการเสริมสร้างขีดความสามารถภายในผ่านการยกระดับการทูตระดับภูมิภาค การกำกับดูแลดิจิทัล และกลไกคุ้มครองประชาชน เพื่อสร้างความมั่นคงอย่างยั่งยืนและมีประสิทธิภาพในระยะยาว โดยข้อเสนอแนะต่อไปนี้เรียงลำดับตามระดับความสำคัญและนัยเชิงยุทธศาสตร์ ได้แก่

๑. เป็นผู้นำจัดตั้งคณะทำงานพหุภาคีที่รวมจีน ภายใต้กรอบอาเซียนหรือยุทธศาสตร์ความร่วมมือทางเศรษฐกิจอิรวดี - เจ้าพระยา - แม่โขง (Ayeyarwady - Chao Phraya - Mekong Economic Cooperation Strategy : ACMECS) โดยประเทศไทยควรริเริ่มจัดตั้งคณะทำงานพหุภาคีว่าด้วยอาชญากรรมดิจิทัลข้ามชาติ ภายใต้กรอบอาเซียนหรือ ACMECS โดยบูรณาการจีนเข้ามาในกลไกพหุภาคี เพื่อสร้างบรรทัดฐานร่วมด้านการบังคับใช้กฎหมาย ลดการพึ่งพาการทูตแบบทวิภาคี และการกดดันจากชาติมหาอำนาจอื่นๆ

อย่างไรก็ดี มีข้อจำกัดด้านความเป็นไปได้เชิงปฏิบัติ ทั้งท่าทีที่ระมัดระวังของจีน ช่องว่างเชิงสถาบันจากกรณีเมียนมา และความลังเลของประเทศที่พึ่งพาการลงทุนจากจีนสูง ดังนั้นทางออกเชิงยุทธศาสตร์คือ ควรเริ่มจากการสร้าง “แกนกลางพันธมิตร (Core Coalition)” กับประเทศที่มีแนวคิดใกล้เคียง เช่น เวียดนาม มาเลเซีย และอินโดนีเซีย เพื่อเป็นแนวทางสู่ธรรมาภิบาลระดับภูมิภาคที่มีประสิทธิภาพมากขึ้น

๒. จัดตั้งสำนักงานข่าวกรองอาชญากรรมชายแดนร่วมในระดับพื้นที่ ประเทศไทยควรจัดตั้งสำนักงานข่าวกรองอาชญากรรมชายแดนร่วมในระดับพื้นที่ตามแนวชายแดนไทย–เมียนมา เพื่อบูรณาการการทำงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Agency : NCSA) ตำรวจไซเบอร์ ศุลกากร ตรวจคนเข้าเมือง และหน่วยข่าวกรอง ในการติดตามการค้ามนุษย์และศูนย์ Scammer แบบทันต่อสถานการณ์ ครอบคลุมการเฝ้าระวัง เส้นทางการเงิน และรูปแบบอาชญากรรมข้ามชาติ โดยขยายผลจากความร่วมมือกับ UNODC และกลไกอำนวยการด้านความมั่นคงชายแดนที่มีอยู่ รวมทั้งทำหน้าที่เป็น “จุดเชื่อมประสาน (Localised Nodes)” สำหรับการแจ้งเตือนและแบ่งปันข่าวกรองอย่างมีประสิทธิภาพ

๓. เสริมสร้างเกราะป้องกันทางการเงินและสถาบันต่อขบวนการหลอกลวง ประเทศไทยควรดำเนินการ ๒ แนวทางควบคู่กัน ได้แก่ (๑) การตัดวงจรทางการเงิน โดยร่วมมือกับพันธมิตรระหว่างประเทศในการติดตามและคว่ำบาตรกระแสเงินทุนผิดกฎหมายที่เชื่อมโยงกับศูนย์ Scammer กำหนดมาตรการจำกัดแบบเฉพาะเจาะจง และยกระดับการตรวจสอบสถานะลูกค้าในภาคธุรกิจความเสี่ยงสูง โดยเฉพาะโครงการลงทุนชายแดนและธุรกิจคาสิโน และ (๒) การเสริมความมั่นคงไซเบอร์ของรัฐ ผ่านการตรวจสอบภาคบังคับ โดย NCSA พร้อมเปิดเผยผลการประเมินต่อสาธารณะเพื่อสร้างความโปร่งใส และการพัฒนาแนวทางการปฏิบัติให้แก่หน่วยงานระดับจังหวัดและระดับท้องถิ่น เพื่อทำหน้าที่เป็นแนวป้องกันด่านแรกต่ออาชญากรรมดิจิทัล

ที่มา : Sriyai, S. “Hammerli”. (2025, August 19). Borderland scam centres and cyber threats: Policy considerations for Thailand (ISEAS Perspective 2025/60). ISEAS–Yusof Ishak Institute. https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2025-60-borderland-scam-centres-and-cyber-threats-policy-considerations-for-thailand-by-surachanee-hammerli-sriyai/