ประเด็นความสัมพันธ์ระหว่างประเทศ ฉบับที่ D46 25 ก.ย. 68	วิทยาลัยการทัพบก
ประเด็น ประเทศจีน	จีนเสนอพันธมิตรระหว่างประเทศปราบปรามการฉ้อโกงโทรคมนาคม-ไซเบอร์: บทบาท ความท้าทาย และโอกาส
ประเด็นสำคัญ	- จุดมุ่งหมายและเป้าหมายเชิงกลยุทธ์ - จุดแข็งและโอกาส - อุปสรรคและข้อท้าทาย - ข้อเสนอแนะสำหรับประเทศไทย - ความเสี่ยงที่อาจเกิดขึ้นหากไม่จัดการอย่างระมัดระวัง

จากข่าวกระทรวงความมั่นคงสาธารณะของจีนเสนอให้มีการสร้างพันธมิตรระหว่างประเทศเพื่อปราบปรามการฉ้อโกงทางโทรคมนาคมและไซเบอร์ แนวคิดดังกล่าวได้รับการนำเสนอในการประชุมย่อยของการประชุมความร่วมมือด้านความมั่นคงสาธารณะระดับโลก (Conference of Global Public Security Cooperation Forum) ประจำปี 2568 ณ เมืองเหลียนอวิ๋นกัง ในมณฑลเจียงซูทางตะวันออกของจีน ระหว่างวันที่ 16-18 ก.ย. 68

ในช่วงหลายปีที่ผ่านมา ปัญหาการฉ้อโกงโทรคมนาคมและอาชญากรรมไซเบอร์ข้ามพรมแดนได้ทวีความซับซ้อนและขยายตัวอย่างรวดเร็ว ไม่เพียงแต่กระทบต่อประชาชนทั่วไปที่ตกเป็นเหยื่อโดยตรงเท่านั้น แต่ยังส่งผลกระทบต่อเสถียรภาพของระบบความมั่นคง การแลกเปลี่ยนข้อมูลระหว่างประเทศ และเศรษฐกิจโลก แม้แต่รัฐบาลที่มีทรัพยากรเข้มแข็งและเทคโนโลยีสูงก็ยังประสบปัญหาในการรับมือ

ล่าสุด กระทรวงความมั่นคงสาธารณะของจีนได้เสนอแนวคิดจัดตั้ง พันธมิตรระหว่างประเทศ (International Alliance) เพื่อรวมพลังในการปราบปรามการฉ้อโกงทางโทรคมนาคมและไซเบอร์ โดยเน้นการทำงานร่วมกันของประเทศต่าง ๆ ในด้านกฎหมาย การบังคับใช้กฎหมาย การแลกเปลี่ยนข้อมูล และการจัดตั้งกลไกประสานงานที่มีประสิทธิภาพมากขึ้น

แนวคิดการตั้งพันธมิตรระหว่างประเทศของจีนมีต้นตอมาจากการตระหนักว่า “การฉ้อโกงโทรคมนาคมและไซเบอร์” เป็นปัญหาที่ไม่สามารถแก้ไขได้โดยแต่ละประเทศเพียงลำพัง สถานการณ์ที่ผู้หลอกลวงใช้เครือข่ายข้ามพรมแดนเพื่อหลบเลี่ยงกฎหมายในประเทศหนึ่งแล้วใช้ทรัพยากรจากประเทศอื่น ผสมกับช่องโหว่ทางกฎหมายและการบังคับใช้กฎหมายที่แตกต่างกัน เป็นปัจจัยสำคัญที่ทำให้การปราบปรามแบบ “เดี่ยว” ได้ผลไม่

มากพอ จีนมีประสบการณ์และผลงานในเรื่องนี้อยู่แล้ว ตัวอย่างเช่น การร่วมมือกับเมียนมา ไทย ลาว และประเทศอื่น ๆ ในการจับกุมผู้ต้องสงสัยคดีฉ้อโกงโทรคมนาคมจำนวนมาก และการส่งตัวกลับประเทศต้นทางเพื่อดำเนินคดีตามกฎหมายของจีน นอกจากนี้ ยังมีรายงานว่าจากความร่วมมือระหว่างประเทศหลายแห่ง จีนสามารถจับผู้ต้องสงสัยฉ้อโกงในต่างประเทศได้ถึงประมาณ 68,000 คน และความเคลื่อนไหวล่าสุดจากการประชุมย่อย “Conference of Global Public Security Cooperation Forum” ซึ่งจีนเสนอแนวทางการจัดตั้งพันธมิตรระหว่างประเทศเพื่อรับมือกับฉ้อโกงโทรคมนาคมและไซเบอร์

จุดมุ่งหมายและเป้าหมายเชิงกลยุทธ์

1. **เสริมสร้างความร่วมมือด้านบังคับใช้กฎหมาย** (Law Enforcement Cooperation)

เพื่อให้การดำเนินคดีผู้ต้องหาฉ้อโกงที่ข้ามพรมแดนเป็นไปได้จริง ทั้งการสืบสวน การจับกุม และการส่งตัวกลับประเทศผู้เสียหายหรือผู้ถูกตั้งข้อกล่าวหา

2**. แลกเปลี่ยนข้อมูลและเทคโนโลยี**

การแจ้งเตือนเกี่ยวกับรูปแบบการหลอกลวง เทคนิคใหม่ ๆ หรือเครือข่ายอาชญากรรม รวมถึงการใช้ทรัพยากรทางเทคนิค เช่น ระบบ IP tracing, การตรวจสอบบล็อกเชน, การวิเคราะห์เครือข่ายโทรคมนาคม ฯลฯ

3. **สร้างกลไกประสานงานระหว่างประเทศ** (Coordination Mechanism)

เช่น ศูนย์ประสานงานร่วมระหว่างประเทศ (joint coordination centers) หรือ task forces ที่มีชาติที่เกี่ยวข้องสมาชิกซึ่งทำหน้าที่ประสานข้อมูล ดำเนินปฏิบัติการร่วม และติดตามผล

4. **การป้องกันและลดช่องโหว่ทรัพยากรพื้นฐาน**

ตัวอย่างเช่น การตัดน้ำ ไฟ สัญญาณอินเตอร์เน็ตในพื้นที่ที่กลุ่มอาชญากรใช้เป็นฐานปฏิบัติการ (เช่น เมียวดี ประเทศเมียนมา) ซึ่งเป็นส่วนหนึ่งของมาตรการจัดการเบื้องต้นเพื่อลดโอกาสที่กลุ่มเหล่านี้จะสามารถใช้โครงสร้างพื้นฐานเหล่านี้หลบซ่อนหรือปฏิบัติการได้อย่างยาวนาน

5. **เสนอการมีส่วนร่วมขององค์กรมาตรฐานระหว่างประเทศ**

เพื่อเสริมสร้างความชอบธรรมและลดข้อขัดแย้งที่อาจเกิดขึ้นระหว่างประเทศ เช่น กฎหมายสิทธิมนุษยชน มาตรการคุ้มครองข้อมูลส่วนบุคคล ฯลฯ

จุดแข็งและโอกาส

การผลักดันพันธมิตรระหว่างประเทศในเรื่องนี้มีจุดแข็งและโอกาสที่น่าสังเกตดังนี้

แรงจูงใจสูง: ประเทศที่ได้รับผลกระทบหนัก เช่น ประเทศในเอเชียตะวันออกเฉียงใต้ โดยเฉพาะไทย เมียนมา ลาว กัมพูชา มีความต้องการแก้ปัญหานี้อย่างจริงจัง เนื่องจากประชาชนตกเป็นเหยื่อเป็นจำนวนมากและมีความเสียหายทั้งทางเศรษฐกิจ สังคม และภาพลักษณ์ระหว่างประเทศ **ทรัพยากรและประสบการณ์ของจีน**: จีนมีระบบตำรวจไซเบอร์กว้างขวาง มีประสบการณ์จับกุมผู้กระทำผิดทั้งภายในประเทศและต่างประเทศ รวมถึงมีเทคโนโลยีและเครื่องมือที่สามารถสนับสนุนการสืบสวนข้ามพรมแดนได้ดี **การสร้างผลประโยชน์ร่วม** (Mutual Benefit): ความร่วมมือระหว่างประเทศสามารถนำไปสู่ผลประโยชน์ร่วม เช่น การฟื้นฟูความเชื่อมั่นของนักลงทุน

และพลเมือง สร้างสภาพแวดล้อมที่ปลอดภัยทางไซเบอร์ และลดภาระของรัฐบาลในด้านการเยียวยาผู้เสียหาย **การสนับสนุนจากองค์กรมาตรฐานระหว่างประเทศ**: การมีส่วนร่วมของ UNODC (สำนักงานว่าด้วยยาเสพติดและอาชญากรรมแห่งสหประชาชาติ) และ องค์กรต่าง ๆ สามารถช่วยเติมเต็มเรื่องกฎหมายมนุษยธรรม กฎหมายสิทธิมนุษยชน และมาตรฐานการคุ้มครองข้อมูลส่วนบุคคล **แรงกดดันสาธารณะและสื่อ**: เมื่อข่าวเกี่ยวกับแก๊งคอลเซ็นเตอร์ และการหลอกลวงที่มีผลต่อประชาชนแพร่หลายมากขึ้น ทำให้เกิดแรงกดดันทั้งภายในประเทศและระหว่างประเทศให้เจ้าหน้าที่ต้องลงมืออย่างจริงจัง

อุปสรรคและข้อท้าทาย

ถึงแม้ว่าความคิดริเริ่มนี้จะมีจุดแข็งหลายประการ แต่ก็มีอุปสรรคนานาและความท้าทายที่ต้องพิจารณาให้รอบคอบ ดังนี้: **ความแตกต่างของกรอบกฎหมายและอำนาจอธิปไตย** แต่ละประเทศมีกฎหมายเกี่ยวกับไซเบอร์ ฉ้อโกง โทรคมนาคม การค้ามนุษย์ ฯลฯ ที่แตกต่างกัน บางประเทศอาจไม่มีบทบัญญัติทางกฎหมายที่คล้ายกัน หรือมีกฎหมายที่ล้าหลังกว่านั้น ซึ่งอาจทำให้การดำเนินคดีหรือการส่งผู้ร้ายข้ามแดนทำได้ลำบาก **ปัญหาด้านสิทธิมนุษยชนและการคุ้มครองข้อมูลส่วนบุคคล** การแลกเปลี่ยนข้อมูลจำนวนมากระหว่างประเทศอาจกระทบกับสิทธิส่วนบุคคล รวมถึงอาจมีความกังวลเกี่ยวกับการใช้มาตรการ “ตัดน้ำตัดไฟ” หรือปิดอินเตอร์เน็ต ซึ่งหากไม่ระมัดระวังอาจละเมิดสิทธิขั้นพื้นฐานของประชาชน **การมีส่วนร่วมของทุกฝ่ายที่เกี่ยวข้อง**

นอกจากรัฐแล้ว ยังมีภาคเอกชน (โทรคมนาคม ผู้ให้บริการอินเทอร์เน็ต), องค์กรไม่แสวงหาผลกำไร, ผู้เชี่ยวชาญทางเทคนิค และประชาสังคม ต้องมีบทบาทในการป้องกันและแจ้งเตือนเมื่อเกิดการกระทำผิด **ปัญหาช่องโหว่ทางภูมิศาสตร์และโครงสร้างพื้นฐาน** พรมแดนที่ยาว เชื่อมต่อระหว่างประเทศ ระบบไฟฟ้า น้ำ อินเตอร์เน็ต ที่อาจถูกนำมาใช้โดยกลุ่มอาชญากร รวมถึงการควบคุมพื้นที่ชายแดนที่บางจุดอาจอยู่ภายใต้การดูแลของภาคทหารหรือกลุ่มติดอาวุธ ฯลฯ ซึ่งทำให้ยากต่อการตรวจสอบหรือบังคับใช้กฎหมาย **ทรัพยากรและความสามารถเชิงเทคนิค** ประเทศที่มีความสามารถทางเทคโนโลยีต่ำกว่าหรือมีการบังคับใช้กฎหมายที่อ่อนแอ อาจไม่สามารถสนับสนุนการสืบสวนหรือการติดตามผู้กระทำผิดได้อย่างรวดเร็วหรือมีประสิทธิภาพ **ผลประโยชน์ทับซ้อน** (Conflicting Interests) **และประเด็นการเมืองภายใน** บางประเทศอาจมีเจ้าหน้าที่ที่เกี่ยวข้องกับวงการโทรคมนาคมหรือในเขตชายแดนที่มีผลประโยชน์ทางเศรษฐกิจที่อาจ “หาผลประโยชน์” จากการเปิดใช้งานโครงสร้างพื้นฐานให้กับกลุ่มอาชญากร หรืออาจมีการล็อบบี้จากผู้มีส่วนได้เสียที่ไม่อยากให้ความร่วมมือเข้มข้น

วิเคราะห์เชิงยุทธศาสตร์: โอกาสทางการปฏิบัติ

เพื่อให้แนวคิด “พันธมิตรระหว่างประเทศปราบปรามการฉ้อโกงโทรคมนาคม-ไซเบอร์” เป็นจริงและได้ผล ประเด็นที่ควรคำนึงถึงเป็นพิเศษมีดังนี้: **การจัดตั้งกลไกกลาง** (Central Coordination Mechanism) ควรมีองค์กรมาตรฐานกลาง ซึ่งอาจทำในรูปของ “ศูนย์ประสานงานปราบปรามฉ้อโกงโทรคมนาคม-ไซเบอร์ระหว่างประเทศ” ที่มีฐานะเป็นทั้งที่ปรึกษาและหน่วยปฏิบัติการ สนับสนุนให้ประเทศสมาชิกส่งตัวแทนมาสื่อสารกัน ร่วมกันวางนโยบาย การใช้เทคโนโลยีร่วมกัน การฝึกอบรม ฯลฯ **การทำสนธิสัญญา** (Treaties / Agreements) ที่มีผลผูกพัน หลายประเทศอาจต้องตกลงกันในระดับทางกฎหมาย เช่น สนธิสัญญาส่งผู้ร้ายข้ามแดน การแลกเปลี่ยนข้อมูลดิจิทัลโดยมีการคุ้มครองข้อมูลส่วนบุคคล และประเด็นด้านกฎหมายอาญาสากล **การ**

พัฒนามาตรฐานทางเทคนิคและการบูรณาการ เช่น การใช้บริการ IP trace-back, การสืบสวนทางดิจิทัล (digital forensics), การวิเคราะห์บล็อกเชน และการพิสูจน์ตัวตนออนไลน์ ฯลฯ โดยประเทศที่มีทรัพยากรต้องช่วยสนับสนุนประเทศที่ยังขาดทรัพยากร **การกำหนดบทลงโทษและมาตรการตอบโต้ที่ชัดเจน** เมื่อนโยบายร่วมกันเริ่มมีประสิทธิภาพ ควรกำหนดมาตรการสำหรับประเทศสมาชิกที่ไม่ให้ความร่วมมือ เช่น การจำกัดการเชื่อมโยงทางโทรคมนาคม, การระงับบริการ เป็นต้น **การมีส่วนร่วมของภาคเอกชนและประชาสังคม** ผู้ให้บริการอินเทอร์เน็ต โทรคมนาคม บริษัทโทรศัพท์มือถือ ผู้ให้บริการเครือข่าย ฯลฯ ต้องมีบทบาทในการตรวจสอบและแจ้งเตือน ความร่วมมือกับ NGO ที่ช่วยเรื่องการคุ้มครองผู้เสียหายก็สำคัญ **การสร้างความเชื่อมั่นและความโปร่งใส** ประเทศที่เข้าร่วมต้องให้ความสำคัญกับการเคารพสิทธิบุคคล ให้การเยียวยาผู้เสียหายในกรณีที่ถูกละเมิด และเปิดเผยข้อมูลความร่วมมืออย่างเหมาะสม

ข้อเสนอแนะสำหรับประเทศไทย

ประเทศไทยเป็นหนึ่งในประเทศที่อยู่ใกล้และได้รับผลกระทบอย่างชัดเจนจากเครือข่ายแก๊งคอลเซ็นเตอร์และฉ้อโกงโทรคมนาคมที่ไหลผ่านเมียนมา โดยเฉพาะทางชายแดนแม่สอด จังหวัดตาก จึงมีบทบาทสำคัญในการร่วมมือกับจีนและประเทศเพื่อนบ้าน หากไทยจะเป็นส่วนหนึ่งของพันธมิตรนี้อย่างเข้มแข็ง ควรดำเนินการดังนี้

ปรับปรุงกฎหมายในประเทศ ให้ครอบคลุมการกระทำผิดไซเบอร์และฉ้อโกงโทรคมนาคม, ส่งผู้ร้ายข้ามแดน, การจัดการทรัพย์สินที่หลบหนีหรือได้มาจากการกระทำผิด, และการคุ้มครองข้อมูลส่วนบุคคล **เสริมสร้างศักยภาพของหน่วยงานบังคับใช้กฎหมาย** โดยเฉพาะตำรวจ สำนักงานตำรวจแห่งชาติ และหน่วยงานที่เกี่ยวข้อง ให้มีเครื่องมือทางเทคนิค, บุคลากรผู้เชี่ยวชาญ, และทรัพยากรเพียงพอในการสืบสวนข้ามพรมแดน **ตั้งศูนย์ประสานงานร่วมระหว่างประเทศ** ระหว่างไทยกับจีนและเมียนมา (และอาจรวมลาว กัมพูชา) เพื่อประสานปฏิบัติการจริง, แลกเปลี่ยนข้อมูลแบบ real-time, ดำเนินการร่วมกันในการตรวจสอบเส้นทางการเงินและเครือข่ายโทรคมนาคม **ควบคุมโครงสร้างพื้นฐานที่อาจถูกนำมาใช้โดยกลุ่มอาชญากร** เช่น ตรวจสอบการให้บริการไฟฟ้า น้ำ อินเทอร์เน็ต ในพื้นที่ชายแดนที่ติดกับเมียนมา และมีการร้องเรียนเกี่ยวกับการใช้บริการเหล่านี้โดยเครือข่ายแก๊งคอลเซ็นเตอร์ **ดึงภาคเอกชนเข้ามามีส่วนร่วม** โดยเฉพาะผู้ให้บริการโทรคมนาคมและอินเทอร์เน็ต เพื่อให้มีมาตรการกรองและตรวจสอบลูกค้าหรือการใช้งานที่น่าสงสัย, ร่วมมือในการระงับบริการหรือบล็อกหมายเลขหรือโดเมนที่ถูกใช้ในการฉ้อโกง **การสร้างความร่วมมือระดับภูมิภาค** เช่น อาเซียน เพื่อให้พันธมิตรครอบคลุมประเทศที่อาจเป็นต้นทาง กลางทาง หรือตัวเชื่อมการเดินทางของผู้หลอกลวง

ความเสี่ยงที่อาจเกิดขึ้นหากไม่จัดการอย่างระมัดระวัง: การละเมิดสิทธิมนุษยชน หากมีการตัดไฟ ตัดอินเตอร์เน็ต หรือปิดการให้บริการในพื้นที่ประชากรอาศัยอยู่ ซึ่งอาจทำให้ประชาชนทั่วไปเดือดร้อนไม่น้อย **การใช้มาตรการที่เกินจำเป็นหรือไม่สมเหตุสมผล** เช่น บล็อกเว็บไซต์หรือโดเมนโดยไม่พิสูจน์ชัดเจนว่าเกี่ยวข้องกับการฉ้อโกง, หรือจับกุมผู้อื่นที่เพียงถูกสงสัยโดยไม่มีหลักฐานเพียงพอ **การบิดเบือนข้อมูลหรือใช้เป็นข้ออ้างทางการเมือง** บางประเทศอาจใช้การกล่าวอ้างเรื่อง “การปราบปรามอาชญากรรมโทรคมนาคม” เป็นเครื่องมือเพื่อควบคุมประชุมชนอินเทอร์เน็ต หรือจำกัดเสรีภาพต่าง ๆ **ปัญหาหลบหลีกโดยกลุ่มอาชญากร** หากกลไกดังกล่าว

ไม่รัดกุม กลุ่มฉ้อโกงอาจย้ายฐานไปยังประเทศที่บังคับใช้กฎหมายอ่อน แสวงหาช่องโหว่ใหม่ ๆ เช่น การใช้เครือข่ายกลางที่ไม่เข้มงวดเรื่องการตรวจสอบผู้ให้บริการ

การเสนอจัดตั้งพันธมิตรระหว่างประเทศของจีนเพื่อปราบปรามการฉ้อโกงโทรคมนาคมและอาชญากรรมไซเบอร์เป็นแนวคิดที่มีศักยภาพสูง เหมาะสมกับสถานการณ์โลกที่การหลบหนีการบังคับใช้กฎหมายและการใช้เครือข่ายข้ามชาติเป็นสรรพานุภาพสำคัญของบรรดากลุ่มอาชญากรหากประเทศที่เกี่ยวข้อง โดยเฉพาะประเทศไทย สามารถใช้โอกาสนี้อย่างเต็มที่ ด้วยการปฏิรูประบบกฎหมาย เสริมศักยภาพหน่วยงาน ปรับปรุงความร่วมมือระหว่างประเทศและภาคเอกชน และตั้งกลไกกลางที่มีอำนาจและความรับผิดชอบชัดเจน แนวทางนี้มีโอกาสสูงที่จะลดความเสียหายจากอาชญากรรมไซเบอร์และฉ้อโกงโทรคมนาคม รวมทั้งสร้างระบบที่ปลอดภัย ไว้วางใจได้สำหรับประชาชนและการค้า-การลงทุนระหว่างประเทศ แต่หากปล่อยให้เดินไปครึ่งทาง โดยไม่ระมัดระวังด้านสิทธิ์ หรือปล่อยให้มีผลประโยชน์ทับซ้อน หรือปล่อยให้ช่องโหว่ทางกฎหมายและโครงสร้างพื้นฐานยังคงอยู่ อาจทำให้โครงการดังกล่าวไม่บรรลุเป้าหมาย หรือแม้แต่เป็นช่องทางใหม่ให้กลุ่มอาชญากรปรับตัวและขยายอำนาจต่อไป

พ.อ. หญิง มนทิรา ยิ้มสมบุญ
อจ.หก.วทบ.

อ้างอิง

1. https://www.infoquest.co.th/news/2025 จีนเสนอสร้างพันธมิตรระหว่างประเทศต้านฉ้อโกงโทรคมนาคม-ไซเบอร์
2. https://www.xinhuathai.com/china/522944_20250706 จีน เมียนมา ไทย ยกระดับกำจัดเครือข่ายฉ้อโกงโทรคมนาคม
3. https://today.line.me/th/v3/article จีนปราบคดีฉ้อโกงโทรคมนาคมมากกว่า 1.7 ล้านคดี
4. https://www.youtube.com/watch?v=vbJpPQMg_J4 จีนเรียกร้อง 'ไทย-เมียนมา' ปราบ 'ฉ้อโกงโทรคมนาคมข้ามแดน' เข้มงวด