ประเด็น เศรษฐกิจ ฉบับที่ C51 29 ตุลาคม 68	วิทยาลัยการทัพบก
ประเด็น ดาวเทียม Starlink ถูกใช้เชื่อมแก๊งคอลเซ็นเตอร์เมียนมา	การเปลี่ยนศูนย์กลางเศรษฐกิจไซเบอร์จากกัมพูชาสู่เมียนมา เมื่อ Starlink กลายเป็นโครงสร้างพื้นฐานของอาชญากรรม
ประเด็นสำคัญ	- จุดเริ่มต้นของการเปลี่ยนผ่านจากกัมพูชาสู่เมียนมา - บทบาทของ Starlink ในฐานะโครงสร้างพื้นฐานของเศรษฐกิจผิดกฎหมาย - เศรษฐกิจของคอมเพล็กซ์ KK Park และแรงงานไซเบอร์ - ผลกระทบเชิงเศรษฐกิจและภูมิรัฐศาสตร์ - มุมมองต่อประเทศไทยและอาเซียน - ความพยายามของประเทศไทย

“หรือศูนย์กลางอาชญากรรมไซเบอร์จะเปลี่ยนจากกัมพูชาเป็นพม่า” **Starlink ถูกใช้เชื่อมแก๊งคอลเซ็นเตอร์ในเมียนมา** ข้อเท็จจริงที่สะเทือนวงการความมั่นคงทางเศรษฐกิจในภูมิภาคเอเชียตะวันออกเฉียงใต้ และเปิดฉากคำถามใหม่ที่สำคัญยิ่งว่า “เทคโนโลยีที่สร้างขึ้นเพื่อเชื่อมต่อโลก อาจกลายเป็นเครื่องมือของอาชญากรรมระดับโลกได้อย่างไร” กรณีนี้มิได้เป็นเพียงประเด็นของการหลอกลวงออนไลน์ หากแต่สะท้อนการเปลี่ยนแปลงเชิงโครงสร้างของ **เศรษฐกิจดิจิทัล (Digital Economy)** ที่เทคโนโลยีสามารถ **หลุดพ้นจากอำนาจควบคุมของรัฐ (Beyond Sovereign Control)** และถูกใช้เพื่อขับเคลื่อน **เศรษฐกิจใต้ดินไซเบอร์ (Cyber Underground Economy)** ที่เชื่อมโยงข้ามพรมแดนได้อย่างไร้รอยต่อ

ในช่วงปี พ.ศ.2566–2568 ศูนย์กลางของอาชญากรรมออนไลน์ในภูมิภาคได้เปลี่ยนทิศจาก **กัมพูชา** ซึ่งเคยเป็นฐานของคอลเซ็นเตอร์สีเทาที่เชื่อมโยงกับทุนจีนและเครือข่ายคาสิโน มาสู่ **เมียนมา** ซึ่งมีภูมิรัฐศาสตร์ และสภาพการเมืองที่เปราะบางกว่ามาก พื้นที่ชายแดนอย่าง **เมืองเมียวดี (Myawaddy)** และ **ชเวโก๊กโก (Shwe Kokko)** ได้กลายเป็นฐานปฏิบัติการใหม่ของขบวนการคอลเซ็นเตอร์นับหมื่นคน ซึ่งใช้เทคโนโลยี **Starlink** เพื่อหลีกเลี่ยงการตัดสัญญาณอินเทอร์เน็ตและสร้างระบบสื่อสารส่วนตัวที่ไม่ต้องผ่านการควบคุมของรัฐใด ๆ เลย

จุดเริ่มต้นของ Starlink ในเมียนมา ดาวเทียม Starlink ถูกพัฒนาโดยบริษัท **SpaceX** ภายใต้การนำของ **Elon Musk** เพื่อให้บริการอินเทอร์เน็ตความเร็วสูงผ่านดาวเทียมแก่พื้นที่ห่างไกล โดยมีเป้าหมายในการ “เชื่อมโลกโดยไม่ทิ้งใครไว้ข้างหลัง” แต่ในเมียนมา ประเทศที่เผชิญกับความขัดแย้งทางการเมืองหลังรัฐประหารปี พ.ศ.2564 เทคโนโลยีนี้กลับถูกแปรสภาพเป็นเครื่องมือของ **อาชญากรรมข้ามชาติ** ที่รัฐไม่สามารถควบคุมได้

ภายหลังจากรัฐบาลทหารเมียนมาจำกัดการสื่อสารอินเทอร์เน็ตเพื่อควบคุมพื้นที่ต่อต้าน กลุ่มทุนเถื่อนและกองกำลังชาติพันธุ์กลับลักลอบนำเข้า **จานรับสัญญาณ Starlink** เพื่อสร้างเครือข่ายสื่อสารอิสระที่ไม่ต้องพึ่งระบบโทรคมนาคมภายในประเทศ การสืบสวนในปี พ.ศ.2567 โดยองค์กรสื่อระหว่างประเทศและหน่วยงานไซเบอร์ของสหรัฐฯ พบว่า **สัญญาณ Starlink เริ่มถูกใช้งานในเขตชายแดนเมียนมา–ไทย** โดยเชื่อมโยงกับคอมเพล็กซ์

เศรษฐกิจผิดกฎหมายชื่อ **KK Park** และ **Shwe Kokko Zone** ซึ่งอยู่ภายใต้การคุ้มครองของกองกำลังกะเหรี่ยง BGF

ในเดือน **มีนาคม พ.ศ.2568** เจ้าหน้าที่ไทยสามารถตรวจยึดอุปกรณ์ Starlink กว่า **38 ชุด** ที่กำลังถูกขนผ่านจังหวัดตากไปยังฝั่งเมียนมา และต่อมาในเดือนตุลาคมปีเดียวกัน ทางการเมียนมาพบ **จานดาวเทียม Starlink 30 ชุด** ภายใน KK Park พร้อมแรงงานกว่า **2,000 คน** ที่ถูกบังคับให้ทำงานในระบบคอลเซ็นเตอร์ การค้นพบนี้ยืนยันว่าเทคโนโลยีที่ถูกออกแบบมาเพื่อสร้างการเข้าถึงอินเทอร์เน็ตอย่างเสรี ได้กลายเป็น “**โครงสร้างพื้นฐานของเศรษฐกิจเงา (Shadow Infrastructure)**” อย่างสมบูรณ์ในภูมิภาค

การย้ายศูนย์กลางจากกัมพูชาสู่เมียนมา ระหว่างปี พศ. 2564-2566 **กัมพูชา** เป็นจุดศูนย์กลางของ **อุตสาหกรรมคอลเซ็นเตอร์หลอกลวง** และ **คาสิโนออนไลน์** ที่มีมูลค่าหลายหมื่นล้านดอลลาร์ โดยเฉพาะในเมือง **สีหนุวิลล์** และ **โพธิ์ไผ่** แต่เมื่อสหรัฐฯ และสหภาพยุโรปเริ่มออกมาตรการคว่ำบาตรต่อบริษัทที่เกี่ยวข้องกับเครือข่าย **Huione Group** และทุนใกล้ชิดตระกูลฮุน เซน กัมพูชาจึงเผชิญแรงกดดันทางการทูตและเศรษฐกิจอย่างหนัก รัฐบาล **ฮุน มาเนต** จำเป็นต้องสร้างภาพลักษณ์การปฏิรูปด้วยการจับกุมแรงงานผิดกฎหมาย ปิดคาสิโน และตั้งคณะกรรมาธิการต่อต้านอาชญากรรมไซเบอร์ระดับชาติ

ในเชิงโครงสร้างการเมืองภายในกัมพูชาเอง การอ่อนแรงของ **ตระกูลฮุน** คือจุดเปลี่ยนสำคัญที่เร่งให้เกิด “การย้ายฐานเศรษฐกิจใต้ดิน” จากเมือง **สีหนุวิลล์** และ **โพธิ์ไผ่** มายังพื้นที่ **เมียวดี** ของเมียนมา ภายหลังแรงกดดันจากนานาชาติให้รัฐบาลฮุน มาเนตกวาดล้าง **ทุนสีเทา** ที่เกี่ยวข้องกับเครือข่ายฟอกเงินและคอลเซ็นเตอร์ข้ามชาติ รัฐบาลพนมเปญจำต้องปฏิบัติตามเพื่อรักษาความสัมพันธ์ทางเศรษฐกิจกับตะวันตก ส่งผลให้กลุ่มทุนเถื่อนซึ่งเคยมีอิทธิพลในกัมพูชาเริ่มเคลื่อนย้ายการดำเนินงานไปยังพื้นที่ที่รัฐควบคุมได้ยากกว่า เช่น **เขตชายแดนเมียนมา–ไทย** การปราบปรามครั้งนั้น แม้ช่วยฟื้นภาพลักษณ์ของรัฐบาล แต่กลับกลายเป็นการเปิดทางให้ “เศรษฐกิจเงา” ย้ายสู่พื้นที่ **ไร้อำนาจรัฐควบคุม (Lawless Zone)** อย่างสมบูรณ์

การปราบปรามเหล่านี้ทำให้กัมพูชาไม่เหมาะแก่การเป็นฐานปฏิบัติการอีกต่อไป เครือข่ายทุนสีเทาจึง **ย้ายฐานเข้าสู่เมียนมา** ที่อยู่ในภาวะ “รัฐล้มเหลวกึ่งสมบูรณ์” และมีกองกำลังท้องถิ่นที่สามารถเจรจาผลประโยชน์ได้โดยตรงโดยไม่ต้องผ่านรัฐบาลกลาง พื้นที่อย่าง **เมียวดี** จึงกลายเป็นจุดยุทธศาสตร์ใหม่ของเศรษฐกิจผิดกฎหมาย เพราะมีทั้งแรงงานราคาถูกจากหลายประเทศ เส้นทางขนส่งสะดวก และที่สำคัญคือมีการเข้าถึง **Starlink** ซึ่งให้บริการอินเทอร์เน็ตความเร็วสูงโดยไม่ต้องผ่านโครงสร้างพื้นฐานของรัฐใ ด **กลไกทางเศรษฐกิจของคอมเพล็กซ์ KK Park** ในทางเศรษฐศาสตร์การเมือง คอมเพล็กซ์อย่าง **KK Park** ถือเป็นตัวอย่างของ “**เศรษฐกิจขนาน (Parallel Economy)**” ที่ดำเนินงานเหมือนภาคธุรกิจปกติแต่ไร้การเก็บภาษีและไม่อยู่ภายใต้กฎหมายรัฐ มีการแบ่งงานเป็นฝ่ายบุคคล ฝ่ายเทคนิค ฝ่ายการเงิน และฝ่ายสื่อสาร แต่ละฝ่ายทำหน้าที่หลอกลวงเหยื่อผ่านสื่อสังคมออนไลน์และแพลตฟอร์มการลงทุนเสมือนจริง

เทคโนโลยีกับภูมิรัฐศาสตร์ การแพร่ขยายของ Starlink ในเมียนมาสะท้อนถึงการเกิดขึ้นของ **“อำนาจทางเทคโนโลยีเหนือรัฐ (Supranational Technological Power)”** อย่างชัดเจน เทคโนโลยีที่ไม่ได้อยู่ภายใต้การอนุญาตของรัฐบาลสามารถสร้างระบบสื่อสารและเศรษฐกิจคู่ขนานได้โดยสมบูรณ์ ก่อให้เกิด **“รัฐดิจิทัลเทียม (Digital Pseudo-State)”** ที่มีกฎหมายและระบบเศรษฐกิจของตนเอง

ในเดือนกรกฎาคม พ.ศ.2568 วุฒิสมาชิก **Maggie Hassan** ของสหรัฐฯ ส่งหนังสือถึง **Elon Musk** เพื่อขอให้ยุติการให้บริการ Starlink ในเมียนมา หลังพบว่ามีส่วนเกี่ยวข้องกับอาชญากรรมไซเบอร์และการค้ามนุษย์ดิจิทัล ส่งผลให้ตั้งแต่เดือนสิงหาคม - กันยายน 2568 กองทัพเมียนมา และกองกำลังพันธมิตร เช่น **BGF (Border Guard Force)** ได้เริ่ม **“ปฏิบัติการกวาดล้างเชิงสัญลักษณ์”** ในพื้นที่เศรษฐกิจ KK Park และชเวโก๊กโก โดยมีการจับกุมแรงงานต่างชาติหลายพันคน ยึดอุปกรณ์สื่อสารกว่า 200 ชุด และประกาศ “ปิดชั่วคราว” พื้นที่ที่พบการใช้งาน Starlink โดยไม่ได้รับอนุญาต

แต่ในความเป็นจริง การกวาดล้างดังกล่าวมีลักษณะ **“เชิงสื่อและเชิงการเมือง”** มากกว่าการทำลายโครงสร้างอาชญากรรมอย่างแท้จริง เพราะรายงานจากสำนักข่าวสากล เช่น *Reuters* และ *The Irrawaddy* ระบุว่า เครือข่ายคอลเซ็นเตอร์เพียงเปลี่ยนจุดปฏิบัติการจาก KK Park ไปยังพื้นที่อื่นภายใต้การคุ้มครองของกองกำลังชาติพันธุ์ เช่น KNU และ DKBA ซึ่งยังไม่อยู่ในอำนาจของรัฐ

ในเชิงภูมิรัฐศาสตร์ สหรัฐฯ มองกรณีนี้ผ่านกรอบ **เศรษฐกิจภูมิรัฐศาสตร์ (Geo-economic Strategy)** ที่เทคโนโลยีไม่ได้เป็นเพียงสินค้าหรือบริการ แต่เป็น “เครื่องมือกำหนดอำนาจระหว่างประเทศ” การปล่อยให้ Starlink ถูกใช้ในกิจกรรมผิดกฎหมายเท่ากับเปิดช่องให้คู่แข่งเชิงยุทธศาสตร์ เช่น จีนหรือรัสเซีย ใช้ประเด็นนี้โจมตีสหรัฐฯ ว่าไม่สามารถควบคุมเทคโนโลยีของตนเองได้ เบื้องหลังของการเปลี่ยนแปลงดังกล่าวยังสะท้อน **“สมการอำนาจระหว่างมหาอำนาจ”** ที่ซับซ้อนยิ่งขึ้น เมื่อ **จีน** ซึ่งเป็นผู้สนับสนุนหลักของรัฐบาลฮุน เซนมายาวนาน เริ่มแสดงความไม่พอใจต่อผลงานของ **ฮุน มาเนต** ที่ไม่สามารถควบคุมปัญหาทุนสีเทาและความขัดแย้งชายแดนกับไทยได้ตามที่คาดหวัง ขณะเดียวกัน **สหรัฐฯ** และพันธมิตรตะวันตกกลับหนุนหลัง **สม รังสี** ผู้นำฝ่ายค้านพลัดถิ่น ซึ่งเตรียมจัดตั้ง **“รัฐบาลกัมพูชาอิสระ 23 ตุลาคม”** ที่กรุงปารีส จีนจึงปรับยุทธศาสตร์ด้วยการเปิดเกมใหม่ สนับสนุน **เจ้านโรดม จักราวุธ** ผู้นำพรรคฟุนซินเปก ซึ่งมีสายสัมพันธ์กับราชวงศ์และมีท่าทีประนีประนอมมากกว่า ฮุน มาเนต กลายเป็น **“ไพ่ลับ”** ที่ถูกวางตัวไว้เพื่อรักษาอิทธิพลในกัมพูชาโดยไม่ต้องพึ่งระบอบเดิม การเปลี่ยนขั้วนี้สะท้อนว่า ปัญหา **อาชญากรรมไซเบอร์** และ **ทุนสีเทา** ไม่ได้เป็นเพียงปรากฏการณ์อาชญากรรม แต่เป็นเครื่องมือในเกม **ภูมิรัฐศาสตร์เทคโนโลยี (Techno-Geopolitics)** ระหว่างมังกรและอินทรีที่กำลังแข่งขันกันครอบงำโครงสร้างอำนาจในเอเชียตะวันออกเฉียงใต้

ไทยและอาเซียนในเงาเศรษฐกิจไซเบอร์ ประเทศไทยกำลังเผชิญกับความเสี่ยงเชิงโครงสร้างจากการที่พื้นที่ชายแดนเชื่อมโยงโดยตรงกับศูนย์กลางอาชญากรรมไซเบอร์ในเมียนมา โดยเฉพาะในจังหวัดตากและอำเภอแม่สอด ที่กลายเป็นเส้นทางลำเลียงอุปกรณ์และแรงงาน รวมทั้งเป็นช่องทางหมุนเวียนเงินผ่านระบบ**บัญชีม้า** และ**คริปโต** การที่ระบบการเงินไทยมีความมั่นคงสูงแต่ยังขาดกลไกตรวจสอบข้ามพรมแดนอย่างมีประสิทธิภาพ ทำให้ไทยกลายเป็น **“ศูนย์กลางทางการเงินของอาชญากรรมโดยไม่ตั้งใจ”**

รายงานของ *The New York Times* ระบุว่า **เขตเศรษฐกิจพิเศษในกัมพูชา ลาว และเมียนมา ซึ่งส่วนใหญ่ตั้งอยู่ติดชายแดนไทย ถูกใช้เป็นศูนย์ปฏิบัติการของเครือข่ายคอลเซ็นเตอร์** โดยอาศัยโครงสร้างพื้นฐานไฟฟ้าและการคมนาคมของไทยในการขนส่งอุปกรณ์และแรงงาน ทั้งยังระบุว่าแรงงานจำนวนมากถูกหลอกมาทำงานในไทยก่อนถูกนำข้ามพรมแดนไปยังศูนย์หลอกลวงในเมียนมา เหตุการณ์นี้ตอกย้ำว่าไทยมิได้เป็นเพียงประเทศทางผ่าน แต่กลายเป็นส่วนหนึ่งของระบบเศรษฐกิจไซเบอร์ใต้ดินในภูมิภาคโดยปริยาย

คำถามว่า “ศูนย์กลางอาชญากรรมไซเบอร์จะเปลี่ยนจากกัมพูชาเป็นพม่าหรือไม่” คำตอบคือ “ใช่” แต่สิ่งที่สำคัญกว่าการเปลี่ยนสถานที่ คือการเปลี่ยน “**รูปแบบของอาชญากรรมจากเศรษฐกิจเงาสู่เศรษฐกิจเทคโนโลยีเต็มรูปแบบ (From Shadow to Tech Economy Crime)**” ซึ่งกำลังกลายเป็นโครงสร้างเศรษฐกิจใหม่ในภูมิภาค ผลกระทบนี้ได้แผ่ขยายมายัง **ประเทศไทยโดยตรง** ผ่านเครือข่ายการเงินและระบบเทคโนโลยีที่เชื่อมโยงกันอย่างแนบแน่น พื้นที่ชายแดน เช่น **ตากและแม่สอด** กลายเป็นทั้งทางผ่านของแรงงานและอุปกรณ์เทคโนโลยี รวมถึง **ช่องทางหมุนเวียนเงินผิดกฎหมาย** ที่ใช้บัญชีม้าและคริปโต ทำให้ไทยมีสถานะ “ศูนย์กลางทางการเงินของอาชญากรรมโดยไม่ตั้งใจ”

ประเทศไทยเองธุรกิจสแกมเมอร์และธุรกิจสีเทาก็ได้ขยายตัวอย่างรวดเร็ว จนกลายเป็นโครงสร้างเศรษฐกิจใต้ดินที่แทรกซึมทุกภาคส่วนของสังคม สร้างความเสียหายมากกว่า **1 ล้านล้านบาทต่อปี** หรือคิดเป็นร้อยละ 10 ของผลิตภัณฑ์มวลรวมในประเทศ (GDP) ซึ่งส่งผลโดยตรงต่อ **ความเชื่อมั่นของผู้บริโภค นักลงทุน และระบบการเงิน** รัฐบาลภายใต้การนำของ **นายอนุทิน ชาญวีรกูล** จึงประกาศให้การปราบปรามมิจฉาชีพออนไลน์เป็น “**วาระแห่งชาติ**” โดยมอบหมายให้ **กรมสอบสวนคดีพิเศษ (DSI)** บูรณาการร่วมกับ **สำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.)** และ **ธนาคารแห่งประเทศไทย (ธปท.)** เพื่อดำเนินการตัดเส้นทางการเงินผิดกฎหมาย ปิดบัญชีม้า และทำลายฐานปฏิบัติการข้ามชาติในพื้นที่ชายแดนกัมพูชา–เมียนมา ซึ่งกลายเป็นศูนย์กลางของเครือข่ายมิจฉาชีพระดับภูมิภาค

รายงาน “State of Scams in Thailand 2025” โดย Global Anti-Scam Alliance (GASA) ระบุว่า คนไทยกว่า 72% เผชิญความพยายามหลอกลวงเฉลี่ยปีละ 172 ครั้ง และกว่า 60% ของผู้ใหญ่ตกเป็นเหยื่อสำเร็จ โดย 14% สูญเงินเฉลี่ยคนละ 12,955 บาท รวมมูลค่าความเสียหายกว่า **115,000 ล้านบาทต่อปี** ตัวเลขนี้สะท้อนถึง “**ภูมิคุ้มกันไซเบอร์ที่ต่ำกว่าการเติบโตของเทคโนโลยี**” ของสังคมไทย ปัจจุบันมิจฉาชีพใช้ **AI และ Deepfake** เพื่อปลอมแปลงภาพ เสียง และตัวตนของบุคคลจริง ทำให้ประชาชนหลงเชื่อว่ากำลังติดต่อกับเจ้าหน้าที่รัฐหรือธนาคาร รูปแบบการหลอกลงทุนครองสัดส่วนสูงสุด (66%) รองลงมาคือหลอกซื้อสินค้า (63%) และหลอกสมัครงาน (53%) โดยกว่าร้อยละ 73 ของการหลอกลวงเกิดผ่านช่องทางสื่อสารยอดนิยม เช่น Facebook, SMS, Gmail, TikTok และโทรศัพท์ ซึ่งแทรกซึมทั้งในกลุ่มวัยทำงานและเยาวชน

สิ่งที่น่ากังวลคือ “**ความมั่นใจย้อนแย้ง (Confidence Paradox)**” คนไทยกว่า 76% เชื่อว่าตนสามารถแยกแยะมิจฉาชีพได้ แต่ในกลุ่มนี้กว่า 66% กลับตกเป็นเหยื่อจริง แสดงถึงช่องว่างระหว่าง

ความรู้เท่าทันกับพฤติกรรมเสี่ยง แม้ผู้เสียหาย 74% จะรายงานเหตุไปยังธนาคารหรือหน่วยงานรัฐ แต่เพียง 29% เท่านั้นที่ได้รับเงินคืนบางส่วน ขณะที่อีก 41% ไม่ได้รับการตอบสนองใด ๆ ปัญหานี้สะท้อนถึง **การขาดระบบข้อมูลกลางและการประสานงานระหว่างหน่วยงาน** ที่ยังไม่เชื่อมโยงกันครบวงจร ระบบธนาคารแบบเดิมยังเป็นช่องทางหลักของการหลอกลวง (73%) เพราะขาดมาตรการยืนยันชื่อผู้รับเงินแบบเรียลไทม์ (Confirmation of Payee) ทำให้เงินไหลเข้าสู่เครือข่ายผิดกฎหมายโดยตรวจไม่พบ

จากบริบทนี้ รัฐบาลไทยก็ได้ตระหนักถึงความจำเป็นในการสร้างกลไกความร่วมมือระดับภูมิภาค เพื่อควบคุมอาชญากรรมไซเบอร์ข้ามพรมแดนหนึ่งในหมุดหมายสำคัญคือการที่ **นาย อนุทิน ชาญวีรกูล นายกรัฐมนตรีและรัฐมนตรีว่าการกระทรวงมหาดไทย** ได้ร่วมลงนามใน **“ประกาศความสัมพันธ์ไทย–กัมพูชาเพื่อสันติภาพ” (Joint Declaration of Relations between Thailand and Cambodia for Peace)** กับ **ฮุน มาเนต** นายกรัฐมนตรีกัมพูชา เมื่อวันที่ 26 ตุลาคม 2568 ที่กรุงกัวลาลัมเปอร์ ประเทศมาเลเซีย โดยมี **อันวาร์ อิบราฮิม** นายกรัฐมนตรีมาเลเซีย และ **โดนัลด์ ทรัมป์** ประธานาธิบดีสหรัฐอเมริกา เข้าร่วมเป็นสักขีพยาน การลงนามดังกล่าวมิได้เป็นเพียงข้อตกลงทางการเมืองเพื่อยุติความตึงเครียดบริเวณชายแดน แต่ยังถือเป็น **“ข้อตกลงสันติภาพเชิงดิจิทัล” (Digital Peace Accord)** ที่วางรากฐานความร่วมมือในการปราบปรามขบวนการสแกมเมอร์ข้ามชาติ การประกาศฉบับนี้ระบุชัดถึง **มาตรการ 4 ด้าน** ได้แก่ 1) การถอนอาวุธหนักออกจากพื้นที่ชายแดน 2) การเก็บกู้วัตถุระเบิด 3) การร่วมกันปราบปรามอาชญากรรมไซเบอร์และขบวนการสแกมเมอร์ และ 4) การหาแนวทางบริหารจัดการพื้นที่ทับซ้อนอย่างสันติ

แนวทางดังกล่าวสะท้อนวิสัยทัศน์ของรัฐบาลไทยในการใช้ **การทูตเชิงความมั่นคงไซเบอร์ (Cybersecurity Diplomacy)** เพื่อป้องกันและควบคุมภัยที่เกิดจากเทคโนโลยีดิจิทัล โดยอาศัยความร่วมมือระหว่างประเทศเพื่อนบ้านและพันธมิตรระดับโลก ขณะเดียวกันก็ยังรักษาอธิปไตยและเกียรติภูมิของชาติในมิติทางเศรษฐกิจและความมั่นคง

ความพยายามของไทยไม่ได้จำกัดอยู่ในระดับทวิภาคีเท่านั้น แต่ยังขยายไปสู่ **ความร่วมมือระดับพหุภาคี** ภายใต้องค์การสหประชาชาติ เมื่อ **นายไชยชนก ชิดชอบ** รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ได้ร่วมลงนามใน **“อนุสัญญาสหประชาชาติว่าด้วยการต่อต้านอาชญากรรมไซเบอร์” (United Nations Convention against Cybercrime)** ที่กรุงฮานอย สาธารณรัฐสังคมนิยมเวียดนาม พร้อมกับตัวแทนจาก 68 ประเทศและสหภาพยุโรป (EU) อนุสัญญาฉบับนี้มีเป้าหมายเพื่อส่งเสริมมาตรการร่วมกันในการป้องกันและปราบปรามอาชญากรรมไซเบอร์ เพิ่มประสิทธิภาพในการบังคับใช้กฎหมาย และยกระดับการแลกเปลี่ยนข้อมูลด้านเทคนิคระหว่างประเทศ โดยเฉพาะในกลุ่มประเทศกำลังพัฒนา ถือเป็นก้าวย่างสำคัญที่สะท้อนถึงจุดยืนของประเทศไทยในการยกระดับมาตรฐาน **ธรรมาภิบาลเทคโนโลยี (Tech Governance)** สู่ระดับโลก

รัฐบาลไทยยังได้กำหนดให้การแก้ปัญหาการหลอกลวงออนไลน์และการฟอกเงินผ่านบัญชีม้าเป็น **“วาระแห่งชาติ”** พร้อม **ขับเคลื่อนมาตรการเชิงรุก 3 ด้าน** ได้แก่ 1) การตัดสัญญาณโทรศัพท์และอินเทอร์เน็ตในพื้นที่ชายแดนที่เป็นช่องทางของอาชญากรรมไซเบอร์ 2) การพัฒนาฐานข้อมูลกลางเพื่อใช้ติดตามและระงับบัญชีม้าที่ใช้ในกระบวนการฟอกเงิน และ 3) การปรับปรุงกฎหมายและกระบวนการยุติธรรมเพื่อให้สอดรับกับภัยเทคโนโลยีสมัยใหม่

กล่าวโดยสรุป กรณีที่ **Starlink** ถูกนำมาใช้เชื่อมโยงเครือข่ายคอลเซ็นเตอร์ในเมียนมา มิใช่เพียงเหตุการณ์อาชญากรรมไซเบอร์เฉพาะจุด แต่สะท้อน **การเปลี่ยนแปลงเชิงโครงสร้างของเศรษฐกิจดิจิทัลในภูมิภาค** ที่เทคโนโลยีซึ่งถูกออกแบบมาเพื่อ “เชื่อมต่อโลก” กลับกลายเป็น **โครงสร้างพื้นฐานของอาชญากรรม** อย่างสมบูรณ์ พื้นที่อย่าง **KK Park** และ **Shwe Kokko** ได้พัฒนาเป็นศูนย์กลางของ **เศรษฐกิจไซเบอร์ใต้ดิน** ที่ขับเคลื่อนด้วย AI, Deepfake และ Cryptocurrency โดยอาศัยระบบสื่อสารดาวเทียมที่อยู่นอกเหนืออำนาจรัฐ ผลกระทบดังกล่าวขยายสู่ **ชายแดนไทย–เมียนมา** โดยเฉพาะจังหวัดตากและแม่สอด ซึ่งกลายเป็นช่องทางสำคัญของแรงงานและทุนสีเทา ขณะที่ช่องว่างด้านการตรวจสอบข้ามพรมแดนทำให้ไทยถูกมองว่าเป็น **ศูนย์กลางทางการเงินของอาชญากรรมโดยไม่ตั้งใจ**

ความเคลื่อนไหวทางนโยบายล่าสุดของไทยแสดงให้เห็นถึงความพยายามเปลี่ยนบทบาทจาก “รัฐเหยื่อ” สู่ **“รัฐเจ้าภาพแห่งความร่วมมือไซเบอร์”** การลงนามใน **ข้อตกลงสันติภาพเชิงดิจิทัลไทย–กัมพูชา** และการเข้าร่วม **อนุสัญญาสหประชาชาติว่าด้วยการต่อต้านอาชญากรรมไซเบอร์** ถือเป็นหมุดหมายสำคัญของการสร้าง **ธรรมาภิบาลเทคโนโลยี (Tech Governance)** ในภูมิภาค มาตรการเชิงรุก เช่น การตัดสัญญาณชายแดน การติดตามบัญชีม้า และการปรับปรุงกฎหมายไซเบอร์ล้วนสะท้อนเจตนารมณ์ของไทยในการเสริมสร้าง **ความมั่นคงดิจิทัลและเศรษฐกิจดิจิทัลที่ปลอดภัยยั่งยืน** หากรัฐสามารถประสานความร่วมมือระหว่างภาครัฐ เอกชน และนานาชาติได้อย่างมีเอกภาพ ดไทยย่อมมีศักยภาพก้าวสู่การเป็น **ศูนย์กลางความร่วมมือด้านความมั่นคงไซเบอร์ของอาเซียน** ได้อย่างแท้จริง

พ.อ.หญิง นวลสมร จรวงษ์
อจ.หก.วทบ.

แหล่งอ้างอิง

1. InfoQuest. (2568, 20 ตุลาคม). *รัฐบาลทหารเมียนมาบุกทลายรังคอลเซ็นเตอร์ พบใช้ “สตาร์ลิงก์” หนุนปฏิบัติการหลอกลวง*. สืบค้นจาก https://www.infoquest.co.th/2025/538819
2. แนวหน้า. (2568, 20 ตุลาคม). *กองทัพเมียนมาบุกแหล่งสแกมเมอร์เมืองเมียวดี รวบคนงานได้ 2,200 คน พร้อมยึดสตาร์ลิงก์ 30 เครื่อง*. สืบค้นจาก https://www.naewna.com/inter/922396
3. Beech, H., & Suhartono, M. (2025, October 22). *Scam centers run on a steady supply of labor and electricity. The New York Times.* Retrieved from https://www.nytimes.com
4. เดลินิวส์. (2568, 25 มิถุนายน). *รายงาน “ยูเอ็น” เผย กัมพูชาคือศูนย์กลางแก๊ง “คอลเซ็นเตอร์” ระดับโลก*. สืบค้นจาก https://www.dailynews.co.th/news/4851638
5. ฐานเศรษฐกิจ. (2568, 21 ตุลาคม). *“ดีอี” เผยภัยสแกมเมอร์ครองแชมป์คดีอาชญากรรมไซเบอร์ไทย สูญ 1 ล้านล้านบาทต่อปี.* สืบค้นจาก https://www.thansettakij.com/economy/642188
6. ฐานเศรษฐกิจ. (2568, ตุลาคม 26). *เปิดดีลสันติภาพ “อนุทิน-ฮุนมาเนต” ไทย–กัมพูชา ร่วมปราบคอลเซ็นเตอร์ชายแดน.* สืบค้นจาก https://www.thansettakij.com/politics/642398