“อธิปไตยทางการสื่อสาร” ภัยคุกคามรูปแบบใหม่ ที่ประเทศไทยต้องตระหนักและเร่งสร้างเกราะป้องกัน

“ภัยคุกคามของชาติ” มิได้จำกัดอยู่เพียงการสู้รบทางทหารอีกต่อไป แต่ยังมีภัยคุกคามในรูปแบบอื่น ที่อันตรายและแยบยลกว่า เพราะเข้าถึงชีวิตประจำวันของทุกคน

ปัจจุบันประเทศไทยกำลังเผชิญกับอะไรและควรรับมืออย่างไร? เพื่อตอบคำถามและรู้เท่าทันสถานการณ์ดังกล่าว จึงได้มีการจัดงานเสวนาวิชาการ **“ความมั่นคงของชาติในโลกผันผวน: เศรษฐกิจ สังคม และภัยคุกคามรูปแบบใหม่”** โดยหลักสูตรการบริหารความมั่นคงสำหรับผู้บริหารระดับสูง รุ่นที่ 7 ณ วิทยาลัยป้องกันราชอาณาจักร (วปอ.) เมื่อวันที่ 6 มิถุนายน 2569 เพื่อแลกเปลี่ยนมุมมองเชิงยุทธศาสตร์ ท่ามกลางบริบทโลกที่เปลี่ยนแปลงอย่างรวดเร็ว โดยเฉพาะความก้าวหน้าของปัญญาประดิษฐ์ (AI) ที่ก่อให้เกิดภัยคุกคามรูปแบบใหม่ ซึ่งส่งผลกระทบโดยตรงต่อเศรษฐกิจ สังคม และความมั่นคงของประเทศ

ในการนี้ พลอากาศโท ดร.ธนพันธุ์ หร่ายเจริญ กสทช. ได้ร่วมเสวนาและให้ความเห็นว่า นอกเหนือจากภัยไซเบอร์อย่างแก๊งคอลเซ็นเตอร์หรือสแกมเมอร์ที่สร้างความเสียหายทางเศรษฐกิจมหาศาลแล้ว ยังมีภัยเงียบที่มีแนวโน้มรุนแรงยิ่งขึ้น คือ **ภัยคุกคาม “อธิปไตยทางการสื่อสาร” (Communication Sovereignty)** ซึ่งหมายถึง ***“อำนาจอิสระของรัฐหรือประชาชนในการควบคุม กำกับดูแล และปกป้องระบบสื่อสาร ข้อมูลข่าวสาร ตลอดจนโครงสร้างพื้นฐานดิจิทัล ไม่ให้ถูกครอบงำหรือแทรกแซงจากภายนอก”*** ซึ่งนับเป็นหัวใจสำคัญของความมั่นคงปลอดภัยในยุคดิจิทัล

หากเปรียบเทียบอดีต ที่ "อธิปไตย" หมายถึง การปกป้องเขตแดน ผืนดิน ผืนน้ำ และน่านฟ้า ดังนั้น “อธิปไตยทางการสื่อสาร” คือ การปกป้องเขตแดน "บนโลกไซเบอร์" ที่ไร้พรมแดน โดยที่ประเทศต้องปกป้องครอบคลุมใน 4 มิติสำคัญ ได้แก่

1. อธิปไตยทางโครงสร้างพื้นฐาน (Infrastructure Sovereignty)

- ควบคุมระบบโครงข่าย: มีอำนาจดูแลสายเคเบิลใต้น้ำ สถานีฐาน ระบบดาวเทียม และระบบคลาวด์หรือศูนย์ข้อมูล (Data Center) ภายในประเทศ
- ลดความเสี่ยงภูมิรัฐศาสตร์: ป้องกันการถูกตัดสัญญาณหรือปิดกั้นระบบ หากต้องพึ่งพาเทคโนโลยีต่างชาติทั้งหมดจะยิ่งมีความเสี่ยงสูง

2. อธิปไตยทางข้อมูล (Data Sovereignty)

- คุ้มครองข้อมูลในชาติ: จัดเก็บข้อมูลพฤติกรรม ข้อมูลส่วนบุคคล และข้อมูลความมั่นคงภายใต้กฎหมายของตนเอง เช่น Sovereign Cloud

- ลดการพึ่งพาต่างประเทศ: ป้องกันการสูญเสียอำนาจในการควบคุมและใช้ประโยชน์จาก Big Data ของคนไทยที่เกือบ 100% อยู่บนเซิร์ฟเวอร์บริษัทเทคโนโลยียักษ์ใหญ่ (Tech Giants) ข้ามชาติ

3. อธิปไตยทางกฎหมายและการกำกับดูแล (Regulatory Sovereignty)

- อำนาจบังคับใช้กฎหมาย: รัฐสามารถกำหนดกฎและหลักเกณฑ์ในการกำกับดูแลระบบและแพลตฟอร์มที่กระทำความผิดได้

- ทลายข้อจำกัดเชิงอำนาจ: ก้าวข้ามข้ออ้าง "กฎหมายเอื้อมไม่ถึง" หรือการไม่ยอมให้มีการกำกับ OTT หรือแพลตฟอร์ม เพื่อจัดการข่าวปลอม (Fake News) และเนื้อหาผิดกฎหมายอย่างมีประสิทธิภาพ

4. อธิปไตยทางวัฒนธรรมและเนื้อหา (Content & Cultural Sovereignty)

- อิสรภาพทางความคิด: ประชาชนรับรู้ข่าวสารได้อย่างถูกต้องโดยไม่ถูกครอบงำด้วยอัลกอริทึม (Algorithm) ที่ใช้ AI ของแพลตฟอร์มต่างชาติ

- ป้องกันการครอบงำ: ลดความเสี่ยงจากการถูกป้อนข้อมูลเพื่อล้างสมอง เปลี่ยนแปลงค่านิยม หรือสร้างความแตกแยกทางการเมือง ผ่านการดำเนินงานที่แยบยลของแพลตฟอร์มในปัจจุบัน

ดังนั้น อธิปไตยทางการสื่อสาร จึงหมายถึง การที่ประเทศไม่ได้เป็นเพียง "ผู้เช่าระบบหรือผู้บริโภค" ที่ต้องยอมจำนนต่อกฎของบริษัทยักษ์ใหญ่ หากแต่ต้องมีอำนาจในการปกป้องและกำหนดทิศทางดิจิทัลด้วยตนเอง เพื่อความมั่นคงของชาติอย่างแท้จริง

เมื่อพิจารณาสถานภาพของประเทศไทย ที่ยังคงพึ่งพาเทคโนโลยีและแพลตฟอร์มต่างชาติเป็นสำคัญ ย่อมเสี่ยงต่อการถูกแทรกแซง ข้อมูลรั่วไหล และการครอบงำทางวัฒนธรรมโดยไร้ทางสู้ สถานการณ์นี้ทำให้ย้อนนึกอดีตที่ไทยเคย “สูญเสียสิทธิสภาพนอกอาณาเขต” ที่อาจไม่ต่างจากปัจจุบันที่เมื่อเกิดปัญหาบนโลกออนไลน์ รัฐกลับต้องบังคับใช้กฎหมายผ่านกระบวนการตามกฎของแพลตฟอร์มต่างชาติ เพียงเพราะเราพึ่งพาเทคโนโลยีเขา และสิ่งที่เกิดขึ้นทุกวันนี้ คือ คนไทยส่วนใหญ่ไม่ได้ถูกบังคับแต่เต็มใจมอบข้อมูลให้เอง เพื่อแลกกับการได้ใช้ประโยชน์จากบริการที่ทันสมัยและสะดวกสบาย

ระบบการสื่อสารไทยจึงมี **"ความเปราะบาง"** (Vulnerability) ซึ่งไม่ได้หมายความว่าระบบหรือสัญญาณอินเทอร์เน็ตไม่ดีพอ แต่คือการ**พึ่งพาต่างชาติเป็นสำคัญ เพราะวันนี้บริษัทยักษ์ใหญ่ไม่ได้หยุดแค่แพลตฟอร์มหรือ** OTT แต่กำลังรุกคืบให้บริการอินเทอร์เน็ตผ่านสัญญาณดาวเทียมวงโคจรต่ำยิงตรงสู่ผู้บริโภคโดยไม่ผ่านตัวแทนในประเทศ หากเป็นเช่นนั้นประเทศไทยอาจจะไม่เหลืออธิปไตยตั้งแต่ต้นน้ำยันปลายน้ำ

เพื่อป้องกันการสูญเสียอธิปไตยทางการสื่อสาร ประเทศไทยควร**ต้องสร้างภูมิป้องกันให้ประชาชนในการใช้บริการ** และ**เร่งสร้างเกราะป้องกัน**ใน 3 ด้านหลัก คือ

1. สร้างเทคโนโลยีตนเอง: สนับสนุนการพัฒนาระบบและแพลตฟอร์มภายในประเทศ เพื่อลดการพึ่งพาต่างชาติ

2. บังคับใช้กฎเกณฑ์เชิงรุก: กำหนดหลักเกณฑ์การกำกับดูแลระบบและ OTT อย่างเหมาะสม เพื่อปกป้องเด็กและเยาวชนจากการครอบงำ

3. ผนึกกำลังภูมิภาค: สร้างพันธมิตรระดับนานาชาติ เช่น กลุ่มประเทศอาเซียน เพื่อเพิ่มอำนาจต่อรองกับบริษัทยักษ์ใหญ่ข้ามชาติ

ฉบับที่ 66 /2569
12 มิถุนายน 2569

“ในอดีต ใครคุม ‘ระบบพลังงานและไฟฟ้า’ คือ ผู้กุมอุตสาหกรรมและเศรษฐกิจของชาติ แต่ปัจจุบัน ใครคุม ‘ระบบสื่อสารและข้อมูล’ คือ ผู้กุมเศรษฐกิจและสังคมที่ครอบคลุมไปถึงความคิด พฤติกรรม และอำนาจทางการเมืองของประชาชนด้วย ดังนั้น ท่านในฐานะที่เป็นผู้บริหารและผู้นำของประเทศในอนาคต ต้องช่วยมีส่วนร่วมในการสร้าง ‘เกราะป้องกัน’ ลดความเปราะบางในเรื่องนี้ เพื่อความมั่นคงของลูกหลานเราในอนาคต” พลอากาศโท ดร.ธนพันธุ์ฯ กล่าวทิ้งทาย
