ภัยคุกคามทางไซเบอร์กับกฎหมายไซเบอร์ไทย

โดย นายเสมอ นิ่มเงิน
ผู้เชี่ยวชาญเฉพาะด้านวิชาการประชาสัมพันธ์

“ภัยคุกคามทางไซเบอร์” (Cyber Threats) เป็นภัยคุกคามที่ส่งผลกระทบในทุกภาคส่วน ไม่ว่าจะเป็นทางเศรษฐกิจ หรือความมั่นคงของประเทศ โดยในปี 2560 ประเทศไทย มีสถิติการคุกคามทางไซเบอร์ตลอดทั้งปี ผลโดยรวมทั้งหมด 3, 237 ครั้ง ในปี 2561 ตั้งแต่เดือนมกราคม ถึงเดือนพฤศจิกายน มีการคุกคามทางไซเบอร์ที่ได้บันทึกไว้ในสถิติแล้วจำนวนทั้งหมด 2,311 ครั้ง โดยการคุกคามที่มากสูงสุดเป็นอันดับหนึ่งของปีนี้คือ “ความพยายามจะบุกรุกเข้าระบบ” (Intrusion Attempts) ที่บันทึกไว้ได้จำนวน 984 ครั้ง ซึ่งมากกว่าสถิติที่บันทึกได้ตลอดปี 2560 ถึง 45 ครั้ง หรือเพิ่มขึ้นถึง 4.80% ปี 2562 จะมีเทคนิคการโจมตีแบบใหม่ที่เกิดขึ้นอีกมากมายและร้ายแรงกว่าที่เป็นอยู่

สถานการณ์ทางไซเบอร์ที่เกิดขึ้นทางรัฐบาลของประเทศไทย ได้ออกนโยบายให้บูรณาการความมั่นคงปลอดภัยทางไซเบอร์ควบคู่กับการขับเคลื่อนเศรษฐกิจดิจิทัล โดยได้จัดตั้ง “คณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ” หรือ National Cybersecurity Committee ไปเมื่อเดือนเมษายน 2561 ที่ผ่านมา ซึ่งมีนายกรัฐมนตรี หรือรองนายกรัฐมนตรีที่ได้รับมอบหมายเป็นประธาน ซึ่งเป็นหนึ่งในยุทธศาสตร์การพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมของรัฐบาล ควบคู่กับการเตรียมประกาศใช้ร่าง พ.ร.บ.รักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งจำเป็นต้องใช้มาตรการทั้งทางเทคนิคและทางกฎหมาย

ความหมายของคำว่า “ความมั่นคงปลอดภัยไซเบอร์” ในร่าง พ.ร.บ.ดังกล่าว คือ มาตรการและการดำเนินการ เพื่อปกป้อง ป้องกัน ส่งเสริมเพื่อรับมือกับสถานการณ์ด้านภัยคุกคามที่จะส่งผลต่อการให้บริการด้านระบบเครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม การให้บริการโดยปกติของดาวเทียม ระบบกิจการสาธารณูปโภคพื้นฐาน และระบบกิจการสาธารณะที่สำคัญ ซึ่งเป็นเครือข่ายในระดับประเทศ เพื่อมิให้เกิดผลกระทบต่อความมั่นคงของชาติ ความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ และความมั่นคงทางเศรษฐกิจ

นอกจากนี้ยังรวมถึงการกำกับดูแลตนเอง และการกำกับดูแลร่วมกันของบุคคล 3 ภาคส่วนของสังคม ได้แก่ ภาครัฐ ภาคเอกชน และภาคประชาสังคม ที่อาจได้รับผลกระทบจากการโจมตีทางไซเบอร์ซึ่งสามารถเกิดได้จากทั้งภายในประเทศ และจากภายนอกประเทศ จำต้องมีการประสานความร่วมมือกันอย่างเป็นระบบ โดยแต่ละฝ่ายอาจมีบทบาทสำคัญ ดังนี้

1. ภาครัฐ ต้องทำหน้าที่หลักในการเป็นตัวกลาง

เพื่อประสานความร่วมมือกับภาคเอกชนและภาคประชาสังคม โดยเฉพาะอย่างอย่างยิ่งที่เกี่ยวข้องกับความมั่นคงของชาติ เช่น กิจการธนาคาร สายการบิน สาธารณูปโภค จัดให้มีการบริหารความเสี่ยงทางเทคนิคที่ดีและต่อเนื่อง เช่น มีระบบการตั้งค่าแบบปลอดภัย มีระบบควบคุมการเข้าถึง มีระบบป้องกันชุดคำสั่งไม่พึงประสงค์ ระบบจัดการปิดช่องโหว่คอมพิวเตอร์ และมีการแบ็กอัพข้อมูลสำคัญ

2. ภาคเอกชน มีหน้าหลักที่บริหารความเสี่ยงในการจัดการทางเทคนิค

เพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ เช่นไฟร์วอลล์ขอบเขต (Boundary Firewalls) เกตเวย์ อินเทอร์เน็ต ระบบการตั้งค่าแบบปลอดภัย ระบบควบคุมการเข้าถึง เป็นต้น นอกจากนี้ หน่วยงานภาคเอกชนที่เกี่ยวข้องกับกิจการสำคัญ เช่น กิจการธนาคาร สายการบิน ต้องมีหน้าที่รายงานการโจมตีทางไซเบอร์ให้หน่วยงานของรัฐทันที เพื่อป้องกันความเสียหายอย่างทันการ

3. ภาคประชาสังคม มีหน้าที่เฝ้าระวังระบบและข้อมูลบนอินเทอร์เน็ตให้มีความมั่นคงปลอดภัย

หากพบเว็บไซต์ที่มีเนื้อหาไม่เหมาะสมหรือพบการโจมตีทางไซเบอร์ ควรรายงานต่อเจ้าหน้าที่ที่มีอำนาจในการจัดการปัญหาดังกล่าวทันที ซึ่งกฎหมายนี้ จะส่งผลดีถึงประชาชนจะได้รับการคุ้มครองสิทธิเสรีภาพในโลกไซเบอร์เสมอภาคด้วยโลกแห่งความเป็นจริง

ความคาดหวังในกฎหมายไซเบอร์ของไทย ไม่ใช่ประเด็นของการป้องกันภัยที่จะเกิดขึ้นทางไซเบอร์อย่างเดียวเท่านั้น แต่ยังมุ่งเน้นในการสร้างความร่วมมือระหว่างรัฐ ภาคเอกชน ภาคประชาสังคม ในลักษณะของการกำกับดูแลตนเอง และการกำกับดูแลร่วมกัน มากกว่าการใช้ตัวบทกฎหมาย ที่เข้มงวดเกินไป ซึ่งอาจกระทบถึงสิทธิเสรีภาพของประชาชนในการติดต่อสื่อสารได้

ภัยคุกคามทางไซเบอร์ที่เกิดขึ้น ไม่ใช่เรื่องที่เป็นแค่วิสัยทัศน์ของภาคส่วนใดภาคส่วนหนึ่งอีกต่อไป แต่เป็นประเด็นสำคัญที่ทุกภาคส่วนของสังคม ที่ต้องประสานความร่วมมือกัน เพื่อช่วยป้องกันให้เกิดผลในภาพรวม ส่งต่อความรู้เพื่อสร้างความเข้าใจ สนับสนุนกระบวนการทางเทคนิค รวมถึงกฎหมายให้เกิดผลอย่างรวดเร็วและมีประสิทธิภาพให้เท่าทันโลกที่ถูกขับเคลื่อนด้วยความก้าวหน้าทางเทคโนโลยีแบบในปัจจุบัน

อ้างอิง

1. https://www.prachachat.net/columns/news-81915
2. https://positioningmag.com/1192167
3. https://www.thaicert.or.th/statistics/statistics.html
4. https://www.thaicert.or.th/papers/general/2012/pa2012ge001.html