**นโยบาย Cybersecurity สังคมต้องมีส่วนร่วม**

**บทความโดย ประวิทย์ ลี่สถาพรวงศา**

**กรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.)**

ในโอกาสวันสื่อสารแห่งชาติ พลอากาศเอกธเรศ ปุณศรี ประธาน กสทช. ได้เชิญคุณ Richard A. Clarke อดีตที่ปรึกษาประธานาธิบดีสหรัฐอเมริกาด้านความมั่นคง มาแลกเปลี่ยนมุมมองเรื่อง Cybersecurity เพื่อให้ประเทศไทยพร้อมรับมือภัยคุกคามทางไซเบอร์ในยุคเศรษฐกิจดิจิตัล โดยได้นำประสบการณ์ที่สหรัฐอเมริกาและประเทศต่างๆ ทั่วโลกได้เผชิญปัญหามาเป็นบทเรียนในการขับเคลื่อนนโยบาย คุณ Clarke ได้สรุปหัวใจของแนวคิดเป็น 4 ปัญหา 6 คำถาม ดังนี้

ปัญหาภัยคุกคามทางไซเบอร์แบ่งได้เป็น 4 ลักษณะ สรุปโดยย่อคือ C.H.E.W.

C คือ Cybercrime เป็นปัญหาการก่ออาชญากรรมทางไซเบอร์โดยมีวัตถุประสงค์ทางการเงิน เช่นการแฮ็คบัญชีธนาคารหรือธุรกรรมออนไลน์ต่างๆ ทำให้คนส่วนหนึ่งไม่ยอมทำธุรกรรมออนไลน์ และคิดว่าตนเองก็จะไม่ได้รับผลกระทบ แต่ในมุมมองของผู้เชี่ยวชาญ อาชญากรรมเหล่านี้เพิ่มต้นทุนต่อระบบ และระบบก็จะผลักต้นทุนนั้นให้ผู้บริโภคทุกคนไม่ว่าจะออฟไลน์หรือออนไลน์แบกรับในที่สุด ปัญหานี้จึงกระทบทุกคนอย่างหลีกเลี่ยงไม่ได้

H คือ Hacktivism เป็นการแฮ็คข้อมูลลับไม่ว่าจะของทางการหรือเอกชนแล้วนำมาเผยแพร่ต่อสาธารณะ เพื่อเปิดโปงเรื่องบางอย่างหรือสร้างความอับอายแก่เจ้าของข้อมูล รวมถึงการแฮ็คเว็บเพจแล้วเผยแพร่ข้อความของตนลงไปในเว็บเหล่านั้นเพื่อประกาศจุดยืนหรืออุดมการณ์ต่างๆ แม้เราจะป้องกันตัวเองดีเพียงใด แต่หากเป็นการสื่อสารกับปลายทาง เช่น อีเมล เมื่อปลายทางถูกแฮ็ค ข้อมูลของเราก็รั่วไหลอยู่ดี

E คือ Espionage เป็นการจารกรรมข้อมูลเพื่อนำไปใช้ประโยชน์ต่อ เช่น การเจาะข้อมูลนวัตกรรมต่างๆ การเจาะข้อมูลทางการทหาร ซึ่งในอดีตใครที่พยายามขโมยเอกสารที่มีชั้นความลับของหน่วยงานต่างๆ เท่ากับต้องบุกรุกเข้าไปในหน่วยงาน แต่ในยุคดิจิตัล แฮ็คเกอร์อาจซ่อนตัวอยู่มุมใดมุมหนึ่งของโลก แล้วเชื่อมต่อทางออนไลน์ ต้นทุนการจารกรรมจึงต่ำมาก และความเสี่ยงในการถูกจับตัวได้ก็ลดลงมาก

W คือ War หรือ Cyberwar ซึ่งเกิดขึ้นแล้ว เช่น การทำลายฐานผลิตอาวุธนิวเคลียร์โดยไม่ต้องส่งกำลังพลหรือใช้อาวุธกายภาพแม้แต่น้อย แต่เป็นการส่งคำสั่งเข้าไปให้เครื่องยนต์ทำลายตนเอง หรือแม้แต่การที่บางประเทศโจมตีทางไซเบอร์เพื่อให้ระบบสื่อสารและแหล่งพลังงานของปฏิปักษ์ล่ม แล้วใช้กำลังพลบุกยึดครองดินแดนจริงได้อย่างง่ายดาย

ปัญหาทั้งหมดนี้ชี้ให้เห็นความจำเป็นในการพัฒนานโยบาย Cybersecurity และมีคำถามพื้นฐาน 6 ข้อที่ต้องตอบเพื่อกำหนดนโยบายได้อย่างถูกต้อง ได้แก่

๑. การเลือกพัฒนาระบบโจมตี หรือจะพัฒนาระบบป้องกัน (Offense vs Defense) บางท่านคิดว่าอาวุธไซเบอร์ที่ทรงอานุภาพจะทำให้เราเป็นฝ่ายชนะ แต่แท้จริงแล้วภัยของการคุกคามทางไซเบอร์คือการถูกโจมตี ซึ่งเกิดขึ้นเวลาใดก็ได้ การขาดระบบป้องกันที่ดีกลับจะทำให้เราเป็นฝ่ายแพ้อย่างราบคาบ การพัฒนาระบบรับมือการโจมตีจึงควรเป็นสิ่งสำคัญลำดับแรก

๒. การปกป้องโครงสร้างพื้นฐานที่สำคัญ (Critical Infrastructure) ซึ่งรัฐมิได้ควบคุมด้วยตนเอง จะเลือกนโยบายเสรีให้ต่างคนต่างรับผิดชอบตนเอง หรือต้องมีนโยบายกำกับดูแล (Market forces vs Regulation) โครงสร้างพื้นฐานในยุคดิจิตัลล้วนเชื่อมต่อออนไลน์ และเสี่ยงต่อภัยคุกคาม เช่น ด้านการผลิตพลังงานหรือกระแสไฟฟ้า ด้านการขนส่งทั้งทางบก ทางน้ำ ทางอากาศ ด้านการเงินการธนาคาร ด้านโรงพยาบาลหรือบริการทางการแพทย์ ด้านการสื่อสาร หรือแม้กระทั่งตลาดหลักทรัพย์ ซึ่งล้วนแล้วแต่มีความสำคัญอย่างยิ่งยวด แต่การพัฒนาระบบรับมือภัยคุกคามต้องมีต้นทุน และในบางครั้งเอกชนก็เน้นการควบคุมหรือลดต้นทุนของตนเอง แต่ผลกระทบจากภัยคุกคามต่อสังคมนั้นมีมูลค่าสูงมากกว่าหลายเท่าตัว เช่น หากระบบไฟฟ้าของประเทศล่ม เท่ากับเศรษฐกิจดิจิตัลหยุดชะงัก จึงจำเป็นต้องมีการกำกับดูแล โดยการออก Smart Regulation ตามด้วยการตรวจสอบการปฏิบัติตามกติกา การทดสอบการโจมตีทางไซเบอร์ และการปรับปรุงพัฒนาระบบ

๓. การคุ้มครองความเป็นส่วนตัว หรือการคุ้มครองความปลอดภัย (Privacy vs Security) สังคมกังวลเกี่ยวกับการถูกละเมิดความเป็นส่วนตัวเพราะรัฐมักจะยกข้ออ้างเรื่อง Cybersecurity แต่หากไม่มี Cybersecurity ก็ไม่มีความเป็นส่วนตัว เพราะข้อมูลของเราจะถูกแฮ็คได้ตลอดเวลา ทั้งสองเรื่องจึงไม่ใช่คู่ตรงข้ามกัน แต่เป็นเรื่องที่ต้องคำนึงไปพร้อมกัน สังคมยอมรับได้หากการเปิดเผยข้อมูลเป็นไปตามคำสั่งศาลโดยชอบด้วยกฎหมาย แต่ภัยคุกคามนั้นต้องรับมือโดยเร็วให้ทันการณ์ จึงต้องมีการพัฒนาระบบการพิจารณาโดยศาลเฉพาะเรื่องนี้ให้ตอบสนองปัญหาได้เร็วที่สุด แทนระบบการออกหมายศาลแบบเดิม

๔. การลงทุนด้านซอฟต์แวร์ หรือการลงทุนพัฒนาคน (Software vs People) บริษัทพัฒนาระบบรักษาความปลอดภัยไซเบอร์มักมุ่งเน้นขายระบบให้กับหน่วยงานต่างๆ แต่การซื้อซอฟท์แวร์มาใช้งานไม่สามารถรับมือภัยคุกคามได้จริง หากบุคลากรยังมีพฤติกรรมเสี่ยง ขาดความตระหนัก หรือความรู้ความเข้าใจในเรื่องนี้ จึงต้องให้ความสำคัญกับคนมากกว่าเน้นการซื้อหรือมุ่งพัฒนาระบบแล้วคิดว่าได้เตรียมการรับมือเรียบร้อยแล้ว และเราต้องค้นหาแฮ็คเกอร์ฝีมือดีแล้วเปลี่ยนให้เป็นบุคลากรด้าน Cybersecurity ของประเทศซึ่งยังขาดแคลนเป็นอย่างมาก

๕. นวัตกรรม หรือความน่าเชื่อถือ (Innovation vs Reliability) ในยุคอินเตอร์เน็ตของสรรพสิ่ง มีอุปกรณ์เชื่อมต่อออนไลน์หลายพันล้านชิ้น และจะเพิ่มเป็นหลายหมื่นล้านชิ้นในอีกสามปีข้างหน้า ที่ผ่านมามีการแฮ็คกล้องวงจรปิดนับแสนตัวเพื่อโจมตี DDoS ไปยังระบบคอมพิวเตอร์เป้าหมาย หากอุปกรณ์หลายหมื่นล้านชิ้นเสี่ยงต่อภัยคุกคาม อนาคตของเราจะเป็นอย่างไร ความเสียหายจะมากขนาดไหน

๖. การป้องกันการบุกรุก หรือความยืดหยุ่นในการรับมือการบุกรุก (Prevention of attack vs Resilience) การป้องกันการบุกรุกคือความพยายามไม่ให้ผู้โจมตีเข้าสู่ระบบได้ แต่ความยืดหยุ่นในการรับมือ คือเมื่อผู้บุกรุกเข้ามาในระบบ จะจำกัดขอบเขตของปฏิบัติการโจมตีได้ในระดับใด และหากเกิดผลกระทบแล้วจะฟื้นฟูระบบให้กลับสู่ปกติโดยเร็วได้อย่างไร เช่น การกู้ระบบไฟฟ้าของประเทศให้กลับคืนมาในเวลานับเป็นชั่วโมง ไม่ใช่เป็นวัน หรือเป็นสัปดาห์ หมายความว่าแต่ละระบบต้องมีข้อมูลสำรองและระบบสำรอง และต้องมีการฝึกซ้อมการกู้ระบบอย่างสม่ำเสมอ ไม่ต่างจากการซ้อมรับอัคคีภัยในอาคาร

นอกจากคำถามเหล่านี้แล้ว การจัดการภัยคุกคามทางไซเบอร์ ต้องเป็นความร่วมมือระหว่างประเทศ เพราะผู้โจมตีมักหลบซ่อนอยู่ในต่างประเทศ แต่ที่สำคัญที่สุดคือนโยบาย Cybersecurity ต้องได้รับการยอมรับจากสังคม ไม่ใช่การกำหนดนโยบายฝ่ายเดียวจากผู้มีอำนาจแล้วใช้บังคับกับสังคม จากประสบการณ์ที่ผ่านมาเรื่องนี้ต้องเปิดให้มีการถกเถียงสาธารณะอย่างกว้างขวาง และต้องสร้างความตระหนักและความรู้ความเข้าใจแก่สังคมอย่างจริงจัง เพื่อให้เกิดการยอมรับในมาตรการ Cybersecurity ของประเทศ แล้วการจัดการภัยคุกคามไซเบอร์จึงจะเกิดผล

หลังจากได้รับฟังมุมมองต่างๆ แล้ว เราคนไทยเองคงต้องร่วมกันหาคำตอบในเรื่องนี้อย่างเหมาะสม การไม่มีนโยบายเรื่องนี้คือหายนะของการไปสู่เศรษฐกิจดิจิตัล แต่การมุ่งบังคับโดยขาดการมีส่วนร่วมก็เป็นหายนะของสังคมและประเทศชาติเช่นกัน