TRACK II MONITOR

Strategic Studies Center
National Defence Studies Institute
Royal Thai Armed Forces Headquarters

ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ
กองบัญชาการกองทัพไทย

Track II Monitor โดย ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ ฉบับที่ ๕/๖๕ (๑ – ๑๕ ธ.ค.๖๔)

ยุทธศาสตร์ไซเบอร์ฉบับใหม่ของรัฐบาลสหราชอาณาจักร

ยุทธศาสตร์ไซเบอร์แห่งชาติฉบับใหม่ของสหราชอาณาจักร ได้เปิดตัวเมื่อวันพุธที่ ๑๕ ธ.ค.๖๔ ที่ผ่านมา โดยศูนย์ความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ (National Cyber Security Centre: NCSC) หลังจากได้ประกาศใช้ยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ๒๐๑๖-๒๐๒๑ มาแล้ว ไซเบอร์ยังคงเป็นปัญหาเร่งด่วนกว่าที่เคยเป็นที่ต้องให้ความสำคัญในยุคของการแข่งขันพลังอำนาจทางไซเบอร์

ยุทธศาสตร์ไซเบอร์แห่งชาติฉบับใหม่นี้ ได้กำหนดทิศทางข้างหน้าในอนาคตของสหราชอาณาจักรอย่างไร

๕ ปีที่ผ่านมา สหราชอาณาจักรได้ใช้ยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ๒๐๑๖-๒๐๒๑ (UK's National Cyber Security Strategy 2016-2021) ได้เห็นการพัฒนาที่สำคัญหลายอย่าง จากความพยายามยับยั้งมิให้รัฐ เช่น รัสเซีย และจีน ใช้ปฏิบัติการทางไซเบอร์ในการขโมยความลับ การโจมตีฝ่ายตรงข้าม และบ่อนทำลายความเชื่อมั่นในกระบวนการประชาธิปไตย ซึ่งผลของความพยายามยับยั้งในการปฏิบัติการจารกรรมทางไซเบอร์ซึ่งยับยั้งได้เพียงเล็กน้อยเท่านั้น ในขณะที่อาชญากรรมทางไซเบอร์ที่ภาคธุรกิจต้องเผชิญมีมากขึ้นกว่าแต่ก่อนที่เคยมีมาจากการระบาดของ Ramsomware ที่เกิดขึ้นทั่วโลกอย่างต่อเนื่อง ส่งผลต่อการดำเนินงานของหลาย ๆ ธุรกิจจำนวนมาก และส่งผลกระทบต่อการให้บริการสาธารณะที่สำคัญต้องหยุดชะงักลงชั่วคราว

ปัญหาคำถามในเชิงยุทธศาสตร์ว่า บทบาทของ Huawei ในโครงสร้างพื้นฐาน 5G ในสหราชอาณาจักร ชี้ให้เห็นถึงการพึ่งพาเทคโนโลยีจากจีนที่มีเพิ่มขึ้น และความท้าทายด้านความปลอดภัย โดยเฉพาะอย่างยิ่ง เมื่อประเทศมหาอำนาจอย่างจีนกำลังพยายามมองหารูปแบบในอนาคตของอินเทอร์เน็ตในแนวทางที่ขัดแย้งกับค่านิยมประชาธิปไตยของสหราชอาณาจักรและเหล่าพันธมิตร ดังนั้นเป็นเวลาที่เหมาะสมสำหรับสหราชอาณาจักรแล้วที่จะวางเป้าหมายใหม่ไปสู่โลกไซเบอร์ ยุทธศาสตร์ไซเบอร์ปี ๒๐๑๖ ได้แสดงให้เห็นถึงการเปลี่ยนแปลงที่สำคัญต่อแนวทางการเข้าไปแทรกแซงโดยรัฐบาลมากขึ้นทั่วทั้งกระบวนการตั้งแต่การตรวจจับและตอบสนองต่อภัยคุกคามทางไซเบอร์ไปจนถึงการสร้างทักษะทางไซเบอร์ การส่งเสริมนวัตกรรมไซเบอร์และการส่งเสริมการเติบโตในภาคธุรกิจด้านไซเบอร์ของสหราชอาณาจักร ส่วนยุทธศาสตร์ไซเบอร์ฉบับใหม่นี้ได้แสดงให้เห็นถึงการยกระดับความต่อเนื่องจากเดิมให้มีความสมเหตุสมผล และยังประกอบไปด้วยการเปลี่ยนแปลงอีกหลายปัจจัย อธิบายได้ว่าเป็นยุทธศาสตร์ไซเบอร์ที่มีความครอบคลุมมากขึ้น ซึ่งมุ่งเน้นไปที่การตอบสนองของทั้งสังคมโดยรวม และเป็นยุทธศาสตร์ที่ดำเนินการต่อด้วยการทบทวนแบบบูรณาการโดยการวางกรอบปัญหาในคำที่เรียกว่า “พลังอำนาจทางไซเบอร์” ที่เป็นมากกว่ายุทธศาสตร์ที่ครอบคลุม

ทั้งความปลอดภัยทางไซเบอร์ และการดำเนินการทางไซเบอร์เชิงรุก ซึ่งได้มีการดำเนินการในขอบเขตนี้ไปบ้างแล้วในยุทธศาสตร์ไซเบอร์ ปี ๒๐๑๖ นอกจากนี้ยุทธศาสตร์ไซเบอร์ฉบับใหม่ยังเน้นในประเด็นที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ ด้วยการกำหนดนโยบายหลักทุกประเภท รวมทั้งยุทธศาสตร์การศึกษานโยบายอุตสาหกรรม การทำงานตามกฎระเบียบ แรงจูงใจและนโยบายการต่างประเทศ รวมทั้งรัฐบาลยังตระหนักถึงกลไกในหลาย ๆ อย่างที่มีความแตกต่างกันทั้งภายในและภายนอกรัฐบาล เพื่อหาวิธีแก้ปัญหา แต่ก็ไม่ใช่เรื่องง่าย แม้ว่าศูนย์ความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ (National Cyber Security Centre : NCSC) และผู้เชี่ยวชาญการกำหนดนโยบายหลักจะมีขีดความสามารถในการดำเนินการก็ตาม ซึ่งในประเด็นนี้ รัฐบาลสหราชอาณาจักรได้เล็งเห็นว่าเรื่องความปลอดภัยทางไซเบอร์ทุกภาคส่วนทั้งภาครัฐ ภาคเอกชน และพลเรือน ต้องร่วมมือและรับผิดชอบร่วมกัน โดยรัฐบาลสหราชอาณาจักรได้แต่งตั้งคณะกรรมการที่ปรึกษาไซเบอร์แห่งชาติชุดใหม่เข้ามาดำเนินการเพื่อให้ความรู้และร่วมกำหนดแนวทาง พร้อมประสานความร่วมมือความมั่นคงทางไซเบอร์ในทุกภาคส่วนระหว่างภาครัฐ ภาคเอกชน และพลเรือน อย่างเป็นรูปธรรมและมีระบบที่ชัดเจน

ในบริบทของยุทธศาสตร์ไซเบอร์ฉบับใหม่ของสหราชอาณาจักร ได้กำหนดกรอบการดำเนินการนโยบายด้านความมั่นคงปลอดภัยทางไซเบอร์ โดยแบ่งออกเป็น ๕ เสาหลัก (5 Pillars) ในการขับเคลื่อนยุทธศาสตร์ไซเบอร์ ได้แก่ (๑) การมุ่งเน้นการเป็นผู้นำในเทคโนโลยีที่สำคัญที่สุดทางไซเบอร์ (๒) การพัฒนาเสริมสร้างศักยภาพระบบนิเวศทางไซเบอร์ (Cyber Ecosytem) ในพื้นที่วิกฤตของสหราชอาณาจักร (๓) การพัฒนาเสริมสร้างศักยภาพในด้าน Microprocessors (๔) การพัฒนาเสริมสร้างศักยภาพในด้านเทคโนโลยีเชิงปฏิบัติงาน (Operational Technology : OT) และ (๕) การพัฒนาเสริมสร้างศักยภาพในด้านการเข้ารหัส (Cryptography) นอกเหนือจากนี้ ยังได้มีการกำหนดริเริ่มดำเนินการที่สำคัญบางอย่างอีก

บทสรุป

สหราชอาณาจักรได้กำหนดยุทธศาสตร์ไซเบอร์แห่งชาติฉบับใหม่นี้ มีวัตถุประสงค์เพื่อมุ่งไปสู่การเป็นผู้นำระดับโลกทางไซเบอร์ โดยใช้เครื่องมือขับเคลื่อนยุทธศาสตร์ในทุกภาคส่วนแบบบูรณาการและรับผิดชอบร่วมกันทั้งภาครัฐ ภาคธุรกิจเอกชน และพลเรือน ในประเด็นของความมั่นคงปลอดภัยทางไซเบอร์ โดยรัฐบาลสหราชอาณาจักรได้กำหนดนโยบายด้านความมั่นคงปลอดภัยทางไซเบอร์ โดยแบ่งออกเป็น ๕ เสาหลัก (5 Pillars) ในการขับเคลื่อนยุทธศาสตร์ไซเบอร์ โดยเฉพาะอย่างยิ่งในเสาหลักด้านระบบนิเวศทางไซเบอร์ (UK's Cyber Ecosytem) ที่มุ่งเน้นการเพิ่มศักยภาพในการรับมือกับสถานการณ์ที่เกี่ยวข้องกับภัยคุกคามต่อความมั่นคงทางเศรษฐกิจและความมั่นคงของชาติในรูปแบบต่าง ๆ ทางไซเบอร์ (Countering Cyber Threats) รวมทั้งการมุ่งเน้นเรื่องการเพิ่มศักยภาพความพร้อมหรือการปรับตัวเพื่อรับมือกับสถานการณ์ที่เกี่ยวข้องกับภัยคุกคามใหม่ ๆ ที่อาจเกิดขึ้นได้เสมอทางไซเบอร์ หรือที่เรียกว่า "ความพร้อมด้าน Cyber Resilience" ซึ่งจะแตกต่างกับ "Cyber Security" ที่เน้นไปในทางการป้องกันเพื่อไม่ให้เกิด

ที่มา

https://rusi.org/explore-our-research/publications/commentary/uk-governments-new-cyber-strategy-whole-society-response

ข้อเสนอแนะเพิ่มเติมกรุณาติดต่อ ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ

๖๒ ถนนวิภาวดีรังสิต แขวงดินแดง เขตดินแดง กรุงเทพฯ ๑๐๔๐๐ | ๐ ๒๒๗๕ ๕๗๑๕-๑๖

admin_info@sscthailand.org | ศูนย์ศึกษายุทธศาสตร์ : Strategic Studies Center https://www.facebook.com/sscthailand.org/