SSC Focus

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

ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ
กองบัญชาการกองทัพไทย

บทความวิเคราะห์สถานการณ์ยุทธศาสตร์และความมั่นคงของประเทศ ฉบับที่ ๕/๖๙

Q-Day: หมุดหมายควอนตัมกับความท้าทายใหม่ของความมั่นคงไทย

Q-Day หรือที่เรียกอีกชื่อว่า Y2Q (Year to Quantum) คือ วันที่เปรียบเสมือน "จุดพลิกผันทางไซเบอร์" เมื่อคอมพิวเตอร์ควอนตัมพัฒนาจนมีขีดความสามารถสูงพอที่จะเจาะและทำลายระบบเข้ารหัสลับ (Cryptography) ที่โลกใช้อยู่ในปัจจุบันได้สำเร็จ ซึ่งรัฐบาลสหรัฐฯ โดยเฉพาะกระทรวงความมั่นคงแห่งมาตุภูมิ (DHS) สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (NIST) และสำนักงานความมั่นคงแห่งชาติ (NSA) กำลังให้ความสำคัญกับเรื่องนี้ในระดับ "ภัยคุกคามความมั่นคงแห่งชาติขั้นสูงสุด"

ทำไม Q-Day ถึงเป็นภัยคุกคามวิกฤต?

ในปัจจุบันระบบความปลอดภัยดิจิทัลเกือบทั้งหมดตั้งแต่ธุรกรรมธนาคาร โครงสร้างพื้นฐานพลังงาน ไปจนถึงข้อมูลทางการทหารล้วนพึ่งพาระบบเข้ารหัสแบบ Public-Key Cryptography เช่น RSA และ ECC ซึ่งหากมีการเจาะระบบด้วยคอมพิวเตอร์ดั้งเดิมการสุ่มถอดรหัส RSA ต้องใช้เวลานับพันปี แต่สำหรับ Cryptographically Relevant Quantum Computer (CRQC) ซึ่งเป็นเครื่องคอมพิวเตอร์ควอนตัมที่มีขนาดใหญ่ และมีจำนวนคิวบิต (Qubits) คุณภาพสูงมากจนสามารถประมวลผลอัลกอริทึมเพื่อ "เจาะและถอดรหัส" (Break Cryptography) จาก RSA/ECC ได้ในเวลาเพียงไม่กี่นาที ส่งผลกระทบให้ลายเซ็นดิจิทัล ใบรับรอง SSL/TLS การยืนยันตัวตน และข้อมูลความลับที่ส่งผ่านอินเทอร์เน็ตทั้งหมดจะไม่ปลอดภัยและหมดความน่าเชื่อถือลงทันที

ทั้งนี้ CRQC เป็น "หมุดหมายทางเทคโนโลยี" (Milestone) ของการพัฒนาในสาย Quantum Computing ที่มุ่งเน้นใน ๓ ประเด็นหลัก คือ (๑) ข้ามผ่านยุค NISQ (Noisy Intermediate-Scale Quantum) ที่คอมพิวเตอร์ควอนตัมขนาดกลางยังมีสัญญาณรบกวนหรือข้อผิดพลาดสูง ไปสู่ยุค Fault-Tolerant Quantum Computing ที่คอมพิวเตอร์ควอนตัมมีความแม่นยำสูง อนึ่งในปัจจุบันที่เครื่องควอนตัมยังมีคิวบิตน้อย (หลักร้อยถึงหลักพัน) และมีอัตราความผิดพลาดสูง จึงสามารถใช้แก้โจทย์ทางวิทยาศาสตร์บางอย่างได้ แต่ยังไม่สามารถถอดรหัสลับที่มีอัลกอริทึมสูงได้ (๒) ยุค CRQC เครื่องควอนตัมมีความแม่นยำสูง เนื่องจากใช้เทคโนโลยี Quantum Error Correction (QEC) เพื่อรวมคิวบิตกายภาพ (Physical Qubits) นับล้านตัว ให้กลายเป็น Logical Qubits ที่เสถียรและไร้ข้อผิดพลาดจำนวนหลายพันตัว และ (๓) การรัน Shor's Algorithm (อัลกอริทึมควอนตัมที่คิดค้นโดย Peter Shor ในปี ๑๙๙๔) เป็นหัวใจสำคัญที่ทำให้ควอนตัมคอมพิวเตอร์กลายเป็น CRQC

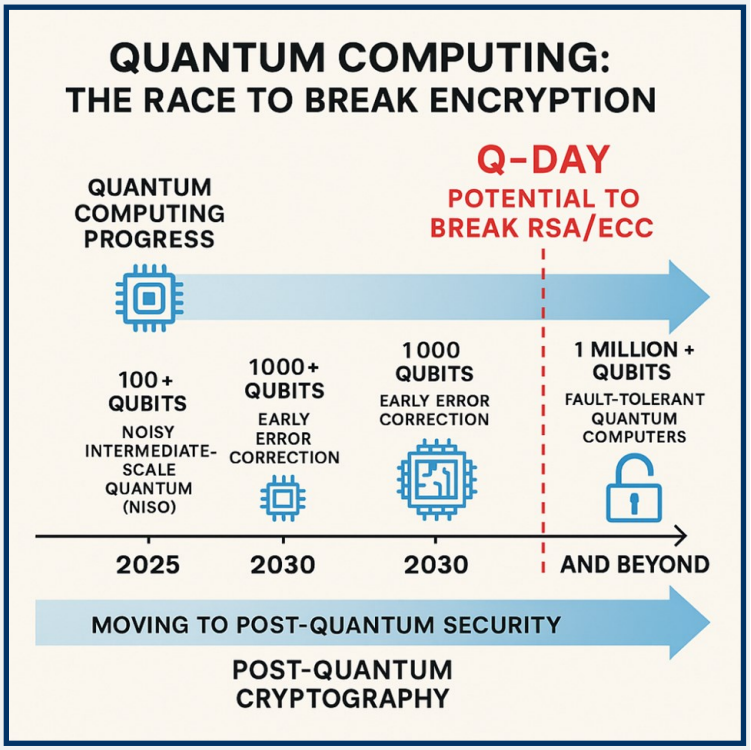
ผลกระทบหาก CRQC เกิดขึ้นจริง

เมื่อ CRQC เกิดขึ้น ระบบรักษาความปลอดภัยที่เราใช้อยู่ประจำวันจะถูกทำลายลง ส่งผลให้ระบบต่าง ๆ ที่ใช้อยู่เช่น ระบบ HTTPS / SSL / TLS ซึ่งเป็นเว็บเบราว์เซอร์, โอนเงินออนไลน์ ถูกดักจับและถอดรหัสการสื่อสารได้แบบ Real-time นอกจากนี้ระบบลายเซ็นดิจิทัล, บล็อกเชน จะถูกปลอมแปลง และสวมรอยยืนยันตัวตน และ ระบบ Encrypted Data (HNDL) ข้อมูลความลับทางการทหาร/การค้า ที่เคยถูกแฮกเกอร์กักเก็บไว้ล่วงหน้า (Harvest Now) จะถูกถอดรหัสทันที (Decrypt Later) ด้วยเหตุนี้ CRQC จึงเป็นเป้าหมายสูงสุดของทั้ง "ฝ่ายโจมตี" ที่หมายถึงประเทศมหาอำนาจและนักวิจัยที่เร่งสร้างเครื่องนี้ให้สำเร็จเป็นชาติแรก และ "ฝ่ายป้องกัน" ที่ต้องเร่งเปลี่ยนระบบไปใช้ Post-Quantum Cryptography (PQC) ให้เสร็จสิ้นก่อนที่ CRQC เครื่องแรกของโลกจะเริ่มทำงาน

Q-Day จะมาถึงเมื่อไร?

การประเมินเหตุการณ์ Q-Day (หรือ Y2Q) ในมุมมองของนักวิชาการและ Think Tanks ระดับโลกนั้น ไม่ได้มองว่าเหตุการณ์นี้คือ "วันที่ตามปฏิทิน" เพียงวันเดียวที่จะเกิดความโกลาหลขึ้นพร้อมกันทั่วโลกเหมือนความกังวลที่เกิดขึ้นเมื่อสมัย Y2K แต่มองว่าเป็น "หมุดหมายทางขีดความสามารถ" (Capability Milestone) ที่ระบบนิเวศทางไซเบอร์จะต้องเผชิญกับการเปลี่ยนแปลงแบบหน้ามือเป็นหลังมือ

ทั้งนี้จากข้อมูลของ Global Risk Institute (GRI), World Economic Forum (WEF), RAND Corporation และ Hudson Institute ระบุว่า กรอบเวลาของ Q-Day แบ่งออกเป็น ๒ มิติ คือ "วันที่เครื่องจักรทำงานได้จริง" และ "วันแห่งความเสี่ยงที่เริ่มขึ้นแล้ว" กล่าวคือ (๑) วันที่เครื่องจักรทำงานได้จริง หรือ หมุดหมายของฮาร์ดแวร์ (The Hardware Milestone) จากรายงาน Quantum Threat Timeline Report 2024 โดย Global Risk Institute (GRI) รวบรวมความเห็นจากผู้เชี่ยวชาญด้านควอนตัม ๓๒ คนทั่วโลก ระบุว่าผู้เชี่ยวชาญส่วนใหญ่



คาดการณ์ว่า คอมพิวเตอร์ควอนตัมที่ถอดรหัสลับได้ (CRQC) จะเกิดขึ้นในช่วงปี ๒๐๓๐ เป็นต้นไป อย่างไรก็ตาม จากการประเมินความเสี่ยงให้ความน่าจะเป็นถึง ๔๐% ที่เครื่องจักรนี้อาจพร้อมใช้งานก่อนปี ๒๐๓๐ สอดคล้องกับการวิเคราะห์ของ RAND Corporation และ NIST ที่ประเมินเส้นตายความเสี่ยงว่า อยู่ในช่วงต้นทศวรรษ ๒๐๓๐

(๒) วันแห่งความเสี่ยงที่เริ่มขึ้นแล้ว คือ ภัยคุกคามที่เริ่มต้นแล้วตั้งแต่วันนี้ องค์กรทั้งหมดข้างต้นเห็นตรงกันว่า จุดเริ่มต้นของ Q-Day ที่แท้จริง "กำลังเกิดขึ้นในปัจจุบัน" ผ่านยุทธศาสตร์ Harvest Now, Decrypt Later (HNDL) โดยอาชญากรไซเบอร์และหน่วยงานระดับรัฐกำลังไล่ดักเก็บข้อมูลที่ถูกเข้ารหัสลับไว้ในปัจจุบัน เพื่อรอเวลาที่จะนำไปถอดรหัสเมื่อฮาร์ดแวร์พร้อมทำงาน

ยุทธศาสตร์ "Harvest Now, Decrypt Later" (HNDL)

ยุทธศาสตร์ "Harvest Now, Decrypt Later" (HNDL) หรือหากแปลตรงตัวคือ "ดักเก็บวันนี้ ถอดรหัสวันหน้า" (บางครั้งเรียกว่า Store Now, Decrypt Later) คือ รูปแบบการโจมตีทางไซเบอร์เชิงยุทธศาสตร์ระยะยาว โดยมีเป้าหมายเพื่อช่วงชิงความได้เปรียบจากการมาถึงของคอมพิวเตอร์ควอนตัม (Q-Day) ในอนาคต ซึ่งแนวคิดนี้ได้เปลี่ยนสมมติฐานด้านความมั่นคงที่ว่า "ควอนตัมเป็นภัยคุกคามในอนาคต" ให้กลายเป็น "ภัยคุกคามที่กำลังเกิดขึ้นในปัจจุบัน"

ดังนั้นในมิติความมั่นคง HNDL จึงเป็นภัยคุกคามระดับวิกฤต เพราะแม้ว่า Q-Day อาจจะมาถึงในอีก ๕-๑๐ ปีข้างหน้า แต่ข้อมูลความลับระดับชาติบางประเภทมี "อายุความลับ" (Shelf-life) ที่ยาวนาน ๑๐, ๒๕ หรือ ๕๐ ปี หากข้อมูลเหล่านี้ถูกถอดรหัสได้ก็จะสร้างความเสียหายทางยุทธศาสตร์อย่างประเมินค่าไม่ได้

ภาคส่วนใดที่จะได้รับผลกระทบ?

(๑) ภาคความมั่นคงแห่งชาติและข่าวกรอง (National Security & Intelligence) เป็นเป้าหมายอันดับหนึ่ง เนื่องจากข้อมูลทางทหาร เครือข่าย การสื่อสารของรัฐบาล และความลับทางการค้าขั้นสูงเป็นเป้าหมายหลักของการดักเก็บแบบ HNDL ข้อมูลเหล่านี้แม้อีก ๑๐-๒๐ ปีข้างหน้าก็ยังมีมูลค่าหรือสร้างความเสียหายทางภูมิรัฐศาสตร์ได้หากถูกเปิดเผย

(๒) โครงสร้างพื้นฐานทางยุทธศาสตร์และคริปโทเคอร์เรนซี (Strategic Infrastructure & Blockchain): ตามการประเมินของ Deloitte ระบบบล็อกเชนปัจจุบัน เช่น Ethereum ตกอยู่ในความเสี่ยงโดยตรง เนื่องจากพึ่งพาลายเซ็นดิจิทัลที่เจาะได้ด้วยควอนตัม ในขณะที่โครงสร้างพื้นฐานด้านพลังงาน ข้อมูลทรัพย์สินทางปัญญา และข้อมูลสาธารณสุขก็มีความเสี่ยงสูงที่จะถูกเจาะเพื่อเรียกค่าไถ่หรือสร้างความชะงักงันได้ด้วย

(๓) ภาคการเงินและการธนาคาร (Financial Sector): จากรายงาน Transitioning to a Quantum-Secure Economy 2022 ของ World Economic Forum และรายงานจาก Hudson Institute 2023 เน้นย้ำว่าเศรษฐกิจยุคดิจิทัลในปัจจุบันที่พึ่งพาระบบ Public-Key Cryptography ทั้งการโอนเงิน การรับรองความถูกต้องของระบบ การยืนยันตัวตนด้วยชีวมาตร และเครือข่าย SWIFT หากไม่มีการเตรียมพร้อมระบบการเงินของสหรัฐฯ ตกอยู่ในความเสี่ยงระดับวิกฤต

ประเทศไทยกับการเตรียมพร้อมสำหรับ Q-Day

เนื่องจากยุทธศาสตร์ Harvest Now, Decrypt Later (HNDL) ของต่างประเทศ ทำให้ข้อมูลการสื่อสารทางทหาร ข้อมูลการข่าวกรอง ความลับทางการทูต และฐานข้อมูลทะเบียนราษฎร์/ชีวมาตร (Biometrics) ที่กองทัพและหน่วยงานความมั่นคงไทยส่งผ่านเครือข่ายอยู่ในขณะนี้ อาจถูกดักจับและกักเก็บไว้เรียบร้อยแล้ว ดังนั้นภาคส่วนความมั่นคงและกองทัพไทยควรเตรียมความพร้อมอย่างเป็นระบบ โดยแบ่งเป็นระดับยุทธศาสตร์ และระดับการปฏิบัติการ ดังนี้

๑. การเตรียมความพร้อมระดับยุทธศาสตร์ (Strategic Level) ด้วยการวางโครงสร้าง นโยบาย และกรอบกฎหมายเพื่อรองรับการเปลี่ยนผ่านทางเทคโนโลยีดังนี้

๑.๑ การจัดทำ "แผนแม่บทการรักษาความปลอดภัยยุคหลังควอนตัม" (Post-Quantum Readiness Roadmap) การกำหนดเส้นตายการย้ายระบบวิกฤต (Critical Systems) ชัดเจน รวมทั้งการพิจารณาตั้งคณะทำงานร่วมระหว่าง กองบัญชาการกองทัพไทย

๑.๒ ประเมินมูลค่าและอายุความลับของข้อมูล (Data Shelf-Life Classification) โดยจำแนกข้อมูลตาม "อายุความลับ" เพื่อกำหนดลำดับความสำคัญในการปกป้อง

๑.๓ กำหนดมาตรฐานการจัดซื้อยุทโธปกรณ์ให้รองรับ PQC (Post-Quantum Cryptography) หรือมีคุณสมบัติ Crypto-Agility" และลดการพึ่งพาเทคโนโลยีสุ่มเสี่ยง

๒. การเตรียมความพร้อมระดับปฏิบัติการ (Operational Level) ด้วยการเตรียมโครงสร้างพื้นฐานไอที ระบบสื่อสาร และกำลังพลให้มีความพร้อมรับมือ

๒.๑ การสำรวจและจัดทำบัญชีทรัพย์สินเข้ารหัส (Cryptographic Inventory Audit) โดยให้ทุกเหล่าทัพทำ Inventory สแกนระบบทั้งหมด เพื่อระบุว่าใช้อัลกอริทึมใดอยู่บ้าง การเข้ารหัสอยู่ที่ในระดับ Hardware, Application หรือ Network Layer รวมทั้งระบบใดบ้างที่ไม่สามารถอัปเดตซอฟต์แวร์ได้ง่าย เพื่อเตรียมแผนการทดแทน

๒.๒ การปรับใช้ระบบเข้ารหัสแบบผสมผสาน (Hybrid Cryptography Implementation) แบบ Dual-Layer เพื่อลดความเสี่ยงด้านความเสถียรของอัลกอริทึมใหม่ด้วยการใช้การเข้ารหัสแบบเดิมซ้อนทับด้วย PQC โดยให้ทั้งระบบเดิมและ PRQC เพื่อปิดช่องโหว่และเป็นเกราะป้องกันซึ่งกันและกัน

๒.๓ การพัฒนาบุคลากรเฉพาะทาง (Human Capital & Cyber Warfare) โดยสร้างเจ้าหน้าที่ที่มีความเชี่ยวชาญด้าน Quantum-Resistant Algorithms ไม่ใช่แค่ผู้ใช้งาน (Users) แต่ต้องมีความเข้าใจในระดับสถาปัตยกรรม และการซ้อมรับมือภัยคุกคาม (Quantum Cyber Exercises) โดยจำลองสถานการณ์การโจมตีในยามที่ระบบเข้ารหัสเดิมถูกทำลาย เพื่อทดสอบความต่อเนื่องในการปฏิบัติภารกิจ ...

อ้างอิง

- Palo Alto Networks. (n.d.). What Is Q-Day? Quantum Computing and Cyber Risk. Retrieved from https://www.paloaltonetworks.com/cyberpedia/what-is-q-day
- ภูมิใจ เลขสุนทรากร. (๒๐๒๖). ความมั่นคงแห่งชาติกระแสใหม่ในยุคแห่งการพลิกผันทางยุทธศาสตร์: ผลกระทบขั้นรุนแรงจากเทคโนโลยีควอนตัม. บทความวิชาการ ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ

ก.ค.๖๙

www.sscthailand.org
sscthailand
๖๒ ถนนวิภาวดีรังสิต แขวงดินแดง เขตดินแดง กรุงเทพฯ
sscthailand