กรุงเทพธุรกิจ
Krungthep Turakij
Circulation: 200,000
Ad Rate: 2,400

Section: First Section/Think Digi
วันที่: จันทร์ 8 กรกฎาคม 2562
ปีที่: 32 **ฉบับที่:** 11246 **หน้า:** 10(ซ้าย)
Col.Inch: 40.52 **Ad Value:** 97,248 **PRValue (x3):** 291,744 **คลิป:** สี่สี
คอลัมน์: ThinkSecure: 'ดาวเทียม'เป้าหมายใหม่ โจมตีทางไซเบอร์

กรุงเทพธุรกิจ
ThinkSecure
นักรบ เนียมนามธรรม
กรรมการผู้จัดการ
บริษัท เอ็นฟอร์ซ ซีเคียว จำกัด

'ดาวเทียม'เป้าหมายใหม่ โจมตีทางไซเบอร์

โครงสร้างพื้นฐานทางเทคโนโลยี ตกเป็นเป้าหมายแรกในการโจมตีผู้ไม่หวังดีทางไซเบอร์เสมอมา ไม่ว่าจะเป็นระบบเครือข่ายคอมพิวเตอร์, ระบบโทรคมนาคม, ระบบ SCADA (Supervisory Control and Data Acquisition) ซึ่งเป็นส่วนหนึ่งของระบบการควบคุมอุตสาหกรรม (Industrial Control System or ICS) ที่ถูกนำไปใช้กับระบบโครงสร้างพื้นฐานในปัจจุบัน เช่น ไฟฟ้า, ประปา, ท่อก๊าซ, ระบบรถไฟฟ้าขนส่งทางราง ฯลฯ แต่ตอนนี้สิ่งที่ผู้เชี่ยวชาญด้านการรักษาความปลอดภัยทางไซเบอร์ ให้ความกังวลว่าจะตกเป็นเป้าหมายถัดไปของกลุ่มคนเหล่านั้น คือ ดาวเทียม และระบบที่เกี่ยวข้อง

โลกปัจจุบันพึ่งพาการใช้งานดาวเทียมเป็นอย่างมาก ทั้งเชิงพาณิชย์, วิทยาศาสตร์ และแน่นอน รวมถึงกิจการของทหาร ตัวอย่างเช่น ระบบการกำหนดตำแหน่งบนพื้นโลก (GPS-Global Positioning System) ที่ใช้กันทั่วไปในชีวิตประจำวัน เพื่อการนำทาง, นำร่องเรือเดินสมุทร, เครื่องบิน, การนำมาใช้งานกับรถยนต์ขับเคลื่อนอัตโนมัติ ที่จะเริ่มมีใช้งานในอนาคตอันใกล้นี้ หรือการใช้ดาวเทียมทางทหารนำวิถีขีปนาวุธ เพื่อโจมตีเป้าหมาย ด้วยการเติบโตของผู้ไม่หวังดี ที่ได้รับการสนับสนุนจากรัฐ (State Sponsored) หรือ กองทัพไซเบอร์ (Cyber Army) ในกรณีที่เกิดความขัดแย้งขึ้นระหว่างรัฐ ไม่แปลกใจว่าดาวเทียมหรือสถานีดาวเทียมจะตกเป็นเป้าหมายแรกในการโจมตี

แน่นอนว่า การโจมตีทางกายภาพต่อดาวเทียมสามารถทำได้ แต่การโจมตีทางไซเบอร์นั้นสามารถทำได้ง่ายและได้ประโยชน์มากกว่า จะเกิดอะไรขึ้นถ้าดาวเทียมสื่อสารหรือดาวเทียมสอดแนมไม่สามารถใช้งานได้ หรือว่าถ้าข้อมูลที่รับ และส่งมาจากดาวเทียมไม่สามารถเชื่อถือได้ ความสามารถในการตอบโต้ของรัฐต่อรัฐย่อมลดลงอย่างแน่นอน ตัวอย่างที่เคยเกิดขึ้นกับกองกำลังป้องกันแอตแลนติกเหนือ (NATO–North Atlantic Treaty Organization) ที่เคยถูกรบกวนสัญญาณจีพีเอสระหว่างการฝึกซ้อมรบ

หลายประเทศในโลกพยายามสร้าง หรือเพิ่มความสามารถในด้านอวกาศของตนเอง ด้วยการแข่งขันการส่งดาวเทียมไปยังวงโคจร ไม่ว่าด้วยเหตุผลทางวิทยาศาสตร์ เช่น เพื่อการสำรวจทรัพยากร สำรวจอวกาศ หรือเหตุผลทางด้านความมั่นคง เช่น การสอดแนม การกระทำดังกล่าวกลับเพิ่มโอกาสให้กับผู้ไม่หวังดีทางไซเบอร์มองเห็นดาวเทียมเหล่านั้นเป็นเครื่องมือหรือเป้าหมายในการโจมตีมากขึ้น เมื่อปีที่แล้วในงาน Black Hat Conference 2018 นักวิจัยด้านความปลอดภัยคนหนึ่งอาศัยช่องโหว่ที่พบบนอุปกรณ์ดาวเทียมในการเจาะเข้าไปในระบบ Airplane 's In-Flight Communication ได้จากทางภาคพื้นดิน ตอนนี้บางประเทศเริ่มให้ความสนใจในการสร้างความปลอดภัยให้กับระบบดาวเทียมของตัวเอง ในปี 2016 ประเทศจีนได้ปล่อยดาวเทียม Mozi (墨子) ที่ใช้การเข้ารหัสแบบควอนตัมเพื่อป้องกันการสื่อสารระหว่างกัน

เทคโนโลยีเป็นเหมือนเหรียญที่มี 2 ด้าน ขณะที่ด้านหนึ่งถูกใช้เพื่อสร้างประโยชน์ เพื่อให้ชีวิตที่ดีขึ้น แต่อีกด้านหนึ่งมันก็กลายเป็นเป้าหมายของผู้ที่ไม่หวังดีในการนำไปใช้ในทางที่จะก่อให้เกิดความเสียหายที่สูงค่ามากกว่า ดาวเทียมก็ตกอยู่ในข่ายนี้เช่นกัน โลกของการรักษาความปลอดภัยทางไซเบอร์ไม่ได้หยุดอยู่แค่เพียงบนพื้นดินอีกต่อไปแต่ครอบคลุมไปไกลถึงอวกาศแล้ว