ACADEMICTALK

แนวโน้มภัยคุกคามด้านเทคโนโลยีสารสนเทศของกองทัพไทย

The Threat Tendency on Information Technology of the Royal Thai Armed Forces

พลเอก ภาณุพล บรรณกิจโสภณ

เจ้ากรมการอุตสาหกรรมทหาร ศูนย์การอุตสาหกรรมป้องกันประเทศและพลังงานทหาร

Lieutenant General Panupol Bannagijsopol

Director-General, Defence Industry Department,
Defence Industry and Energy Centre

E-mail: ee1935@hotmail.com

บทคัดย่อ

ปัจจุบันนี้เทคโนโลยีสารสนเทศมีบทบาทอย่างกว้างขวางในทุกวงการ และเทคโนโลยีสารสนเทศกลายเป็นเครื่องมือสำคัญของการทำงานทุกด้าน นับตั้งแต่ทางด้านการทหารและความมั่นคง ตลอดจนด้านการเมืองและราชการ จึงทำให้แนวคิดด้านยุทธศาสตร์และยุทธวิธีทางทหารและความมั่นคงแบบเดิมนั้นอาจจะไม่สามารถนำมาใช้ต่อไปได้อย่างมีประสิทธิภาพในอนาคต เพราะรูปแบบภัยคุกคามมีการเปลี่ยนแปลงไป เช่น การใช้อินเทอร์เน็ตโจมตีระบบสารสนเทศขององค์กรภาครัฐ ไปจนถึงการใช้อินเทอร์เน็ตปล่อยข่าวโจมตีรัฐบาล จึงทำให้เกิดภัยคุกคามใหม่ที่เรียกว่า “การปฏิบัติการข่าวสาร” หรือ “Information Operations” ซึ่งถือได้ว่าเป็นภัยคุกคามรูปแบบใหม่ที่เกิดจากการเปลี่ยนแปลงของเทคโนโลยีและการเชื่อมต่อของโลกที่ไม่มีพรมแดน

ผลการศึกษาพบว่าภัยคุกคามนั้นเกิดได้จาก 2 แหล่ง แหล่งแรกคือการโจมตีจากภายนอก จะโจมตีผ่านเครือข่ายภายนอกที่เชื่อมต่อ ซึ่งจะต้องผ่านระบบป้องกัน หากระบบป้องกันมีประสิทธิภาพเพียงพอจะสามารถป้องกันการโจมตีนั้นได้ แต่หากการป้องกันไม่มีประสิทธิภาพเพียงพอจะทำให้สามารถโจมตีได้ถึงระบบงาน และมีผลกระทบต่อการทำงานในที่สุด ภัยคุกคามอีกแหล่งหนึ่งคือการโจมตีจากภายใน จะเห็นได้ว่าการโจมตีจากภายในนั้นอาจจะโจมตีจากภายในระบบป้องกันหรือภายในระบบงานที่อยู่หลังระบบป้องกัน จึงทำให้สามารถทำการโจมตีได้ง่าย การโจมตีชนิดนี้เป็นอันตรายมากและป้องกันได้ยาก เนื่องจากเป็นการโจมตีที่มาจากบุคคลภายในหน่วยงาน

คำสำคัญ: ภัยคุกคาม, เทคโนโลยีสารสนเทศ

ABSTRACT

At present, information technology role has increasingly become in every circle an important tool for every field such as military, national security, political and governmental. Therefore, national strategy and military strategy need to be changed according to the threat tendency on information technology of the Royal Thai Armed Forces. There has been a focus on the vulnerability of the systems to internet attacks to the governmental offices.

Research findings stated that the threat actually comes from two sources. The first source is from an external threat which is the attack from outside of the network. Secondly, the attack is from inside the network. This threat posed more danger to the system because the attacker is one who works inside the premises.

Keywords: Information Technology, National Security.

หลักการและเหตุผล

การพัฒนากองทัพให้มีความเจริญก้าวหน้า ทันโลก ทันสถานการณ์ ทันกับวิทยาศาสตร์และเทคโนโลยีใหม่ ๆ ที่ก้าวไปอย่างรวดเร็ว กองทัพจะต้องมีการปรับเปลี่ยนวัฒนธรรมขององค์กรให้สอดคล้องกับสภาพแวดล้อมที่เกิดขึ้นใหม่ ๆ ตามพลวัต (Dynamic) และวิวัฒนาการ (Evolution) ของโลกให้กับมนุษย์ ซึ่งเป็นเรื่องที่หลีกเลี่ยงไม่ได้ และเป็นเรื่องยากที่จะปรับเปลี่ยนความคิดของมนุษย์ให้มีความรู้เพื่อพัฒนาไปสู่ปัญญาและเกิดจิตสำนึกในที่สุด การเรียนรู้เพื่อจะให้รู้ทันภัยคุกคามด้านเทคโนโลยีสารสนเทศจำเป็นจะต้องมีความรู้ความเข้าใจในด้านต่าง ๆ ดังนี้

1. โครงสร้างพื้นฐาน (Infrastructure)

1.1 การโจมตีโครงสร้างพื้นฐาน (Infrastructure Attacks) ระบบโครงสร้างพื้นฐานที่สำคัญ ๆ มีความเสี่ยงสูงต่อการถูกโจมตีโดยขบวนการก่อการร้ายหรือขบวนการอื่น ๆ ได้แก่

1.1.1 การเงินการธนาคาร (Banking and Financial) ถึงแม้ส่วนใหญ่จะเป็นระบบปิด แต่ก็เป็นสิ่งที่ผู้ไม่ประสงค์ดีพยายามที่จะโจมตีอยู่เป็นประจำ

1.1.2 ระบบสื่อสารทางโทรศัพท์ (Voice Communication Systems) เป็นระบบที่ให้บริการประชาชนที่สำคัญ ซึ่งปัจจุบันใช้ระบบสารสนเทศควบคุมระบบมากยิ่งขึ้น

1.1.3 ระบบไฟฟ้า (Electrical Infrastructures) ส่วนใหญ่จะมีระบบตรวจวัด (Sensors) ที่ช่วยผู้ที่ดูแลระบบเปิด-ปิดไฟฟ้าในระบบเครือข่ายการจ่ายไฟฟ้า (Power Grid) เป็นจุดอ่อนที่สำคัญ หากมีการทำให้ระบบตรวจวัดผิดพลาด หรือทำให้ระบบเครือข่ายผิดพลาด อันจะทำให้ระบบไฟฟ้าทั้งระบบเสียหายได้

1.1.4 ระบบประปา (Water Resources) เป็นระบบที่ให้บริการประชาชนที่สำคัญ และสำคัญต่อกระบวนการผลิตสินค้าต่าง ๆ ซึ่งปัจจุบันใช้ระบบสารสนเทศควบคุมระบบมากยิ่งขึ้น

1.1.5 ระบบส่งน้ำมันและก๊าซ (Oil and Gas) ที่มีการส่งทางท่อจะใช้ระบบการตรวจวัดในการควบคุมระยะไกล การถูกโจมตีจะทำความเสียหายต่อภาคเศรษฐกิจ เช่น การผลิตและการขนส่งที่ใช้น้ำมันหรือก๊าซ

2.2 การป้องกันระบบสารสนเทศที่ใช้ในการควบคุมโครงสร้างพื้นฐาน ควรมีการป้องกันดังนี้

2.2.1 ระบบปฏิบัติการควรมีการปรับปรุงให้ทันสมัยอยู่เสมอ

2.2.2 บังคับการใช้นโยบายระบบรหัสผ่านที่เข้มงวด

2.2.3 เมื่อผู้ดูแลระบบเลิกใช้ระบบควรทำกระบวนการออกจากระบบอยู่เสมอ

2.2.4 โปรแกรมบริการต่าง ๆ ที่ไม่มีความจำเป็นควรจะปิดการใช้งาน

2.2.5 ต้องติดตั้งโปรแกรมป้องกันไวรัสและปรับปรุงให้ทันสมัยอยู่เสมอ

2.2.6 ติดตั้งระบบตรวจจับการบุกรุก (IDS: Intrusion Detection) และกำแพงป้องกัน (Firewalls)

3.3 แผนการป้องกันระดับชาติ (The Nation Protection Plan) ของสหรัฐฯ

สหรัฐฯ มีแนวคิดในการจัดทำแผนป้องกันระดับชาติ โดยพิจารณาย่านของความเสี่ยง (The Risks Range) ที่เกี่ยวข้องกับความมั่นคงของชาติที่จะต้องพิจารณาถึงภัยคุกคามที่มีอยู่ จุดอ่อนของโครงสร้าง

พื้นฐานที่วิกฤต (Critical Infrastructures) จากการโจมตีจากไซเบอร์ (Cyber Attacks) และจากการปฏิบัติการสารสนเทศ (Information Operations) เพื่อเป็นการป้องกันและรับประกันความมั่นใจและความมั่นคงของโครงสร้างพื้นฐานที่วิกฤต

ปัจจุบันข้อมูลที่มีค่านั้นถูกเก็บไว้บนสื่ออิเล็กทรอนิกส์ของแต่ละหน่วยงาน ไม่ได้เก็บไว้อย่างปลอดภัยในรัฐบาล ซึ่งเป็นเป้าหมายที่จะถูกโจมตี ทั้งเป้าหมายที่มีค่าของรัฐบาลทางทหารและพลเรือน ดังนั้นจึงต้องมีการพัฒนาวิถีทางหรือเครื่องมือ (Means) ที่จะทำให้ลดความเสี่ยงนั้น

กลไกหรือเครื่องมือในการป้องกันระดับชาติที่สำคัญที่เราต้องออกแบบและสร้างการป้องกันรักษาความมั่นคงปลอดภัย ทั้งในรูปแบบของคณะกรรมการเพื่อความมั่นคงของชาติ และสถาบันบังคับใช้กฎหมาย (National Security Committee and Law Enforcement Institutions) มีรายละเอียดดังนี้

3.3.1 กฎหมายของชาติ (National Law) เพื่อป้องกันภายในประเทศจากอาชญากรรมซึ่งอาจจะมาจากอาชญากรรมคอมพิวเตอร์ หรืออาชญากรรมอื่น ๆ ที่เกี่ยวข้อง

3.3.2 กระทรวงกลาโหมและกองทัพเพื่อป้องกันภัยคุกคามจากภายนอก

3.3.3 ข่าวกรองของชาติ (Nation's Intelligence Agencies) เพื่อสนับสนุนข่าวที่เป็นสิ่งบอกเหตุ เจตนารมณ์ และขีดความสามารถของผู้รุกรานและทำการแจ้งเตือนล่วงหน้า

ตามที่เราทราบกันดีว่าการใช้เทคโนโลยีสารสนเทศมีความเสี่ยง แต่พึงเข้าใจว่าเรามีความจำเป็นที่จะต้องใช้เพื่อขับเคลื่อนเศรษฐกิจและความมั่นคงของชาติ ดังนั้น เราจึงควรสร้างกำแพงป้องกันทั้งกายภาพและในโลกเครือข่ายคอมพิวเตอร์ไว้ให้พร้อม

2 ภัยคุกคามด้านสารสนเทศในปัจจุบัน

2.1 หนอนอิเล็กทรอนิกส์

เป็นการเปรียบเทียบพฤติกรรมการดำเนินการของโปรแกรมคอมพิวเตอร์ที่แพร่ขยายพันธุ์กระจายตัวเองอย่างอัตโนมัติ การแพร่กระจายจะเกิดการแบ่งตัว หรือสร้างตัวเองเป็นจำนวนมหาศาล โดยโปรแกรมหนอนอิเล็กทรอนิกส์นี้จะเริ่มเจาะและฝังตัวเองที่เครื่องคอมพิวเตอร์เครื่องใดเครื่องหนึ่งในเครือข่ายก่อน จากนั้นจึงจะเจาะซ่อนตัวเองภายใน โดยฝังไปกับข้อมูลอื่น ๆ เพื่อหลบหลีกการค้นหาทำลาย เมื่อใดที่ยึดที่มั่นได้แล้วก็จะเริ่มแบ่งตัว โดยคัดลอกตัวเองไปยังที่ต่าง ๆ ในเครื่อง ซึ่งอาจจะกลายพันธุ์เพื่อให้มีหลากหลายรูปแบบ พฤติกรรมการทำลายระบบก็ขึ้นอยู่กับผู้ออกแบบหนอนนั้นว่าจะให้หนอนทำลายสิ่งไหน หนอนอิเล็กทรอนิกส์นั้นสามารถเจาะเข้าสู่ระบบได้หลายช่องทางดังนี้

2.1.1 การเจาะผ่านประตูเข้าออกของข้อมูลซึ่งเรียกว่าพอร์ต (Port) ปกติอุปกรณ์คอมพิวเตอร์ที่เชื่อมต่อเครือข่ายจะมีประตูเข้าออกของข้อมูลได้ถึง 65.536 ประตู ซึ่งบางประตูเป็นช่องทางบริการที่มีการกำหนดไว้ชัดเจน เช่น ประตูสำหรับรับส่งจดหมายอิเล็กทรอนิกส์ ประตูสำหรับรับส่งข้อมูลเว็บเพจ (Webpage) เป็นต้น เมื่อประตูมีมากแต่ละประตูใช้บริการเฉพาะ เช่น การเล่นเกมออนไลน์ การพูดคุยบนเครือข่าย ประตูเหล่านี้จึงมีข้อมูลวิ่งเข้าออกอยู่ตลอดเวลา บางประตูก็ใช้งานเฉพาะที่ผู้ใช้โดยทั่วไปอาจจะไม่รู้ ผู้ออกแบบหนอนอิเล็กทรอนิกส์จึงต้องตรวจสอบหาช่องประตูเหล่านี้ว่าช่องไหนมีจุดอ่อน และเจาะผ่านประตูช่องนั้นเข้าไป

2.1.2 สาเหตุจากจุดอ่อนของระบบปฏิบัติการ (Operation System) เช่น ระบบปฏิบัติการวินโดว์ส (Windows System) ปัจจุบันระบบปฏิบัติการมีความซับซ้อนขึ้นมาก ซึ่งผู้ผลิตอาจจะสร้างจุดอ่อนไว้โดยไม่ได้ตั้งใจ เมื่อผู้ไม่หวังดีตรวจพบจุดอ่อนจึงสร้าง

หนอนอิเล็กทรอนิกส์เจาะเข้าช่องทางนั้น เมื่อผู้ผลิตทราบจึงทำการแก้ไขจุดอ่อน และออกตัวแก้ไขออกมาภายหลัง ดังนี้แล้วเราจึงควรปรับปรุงระบบปฏิบัติการอยู่เสมอ ๆ

2.2 โปรแกรมสายลับหรือสปายแวร์ (Spy Ware)

เป็นโปรแกรมที่ถูกติดตั้งเพื่อคอยเฝ้าดูการทำงานของเครื่องคอมพิวเตอร์ และพฤติกรรมการใช้งานของผู้ที่เป็นเจ้าของเครื่องหรือผู้ใช้งาน โดยเฉพาะอย่างยิ่งเมื่อมีการเชื่อมโยงกับเครือข่ายอินเทอร์เน็ต กำลังกลายเป็นโปรแกรมที่ระบาดอยู่ทั่วไปในระบบอินเทอร์เน็ต เพื่อล้วงข้อมูลส่วนบุคคลที่ดาวน์โหลด (Download) ข้อมูล หรือโปรแกรมฟรีผ่านอินเทอร์เน็ต กำลังเป็นปัญหาที่ทวีความรุนแรงเพิ่มขึ้นอย่างต่อเนื่อง แม้ว่าเครื่องที่ถูกสปายแวร์ติดตั้งอยู่จะไม่ทำให้ระบบปฏิบัติการหรือระบบงานเสียหาย แต่สปายแวร์จะเข้าไปล้วงความลับและนำข้อมูลต่าง ๆ ของผู้ใช้ออกไปยังคนภายนอก ผู้เชี่ยวชาญด้านซอฟต์แวร์ด้านการรักษาความปลอดภัยระบุว่า มีโปรแกรมมากกว่า 75,000 โปรแกรมที่เป็นสปายแวร์ โดยโปรแกรมเหล่านี้สามารถดึงเอาพฤติกรรมการใช้อินเทอร์เน็ต ขโมยรหัสผ่าน บันทึกการกดคีย์บอร์ด หรือแม้กระทั่งขโมยหมายเลขบัตรเครดิต หรือบัตรประชาชนของผู้ใช้เครื่องนั้น ๆ วิธีการป้องกันคือผู้ใช้อินเทอร์เน็ตไม่ควรดาวน์โหลดเพลงหรือซอฟต์แวร์แปลก ๆ มาลงในเครื่อง และควรติดตั้งเครื่องมือในการตรวจหาสปายแวร์ (Anti-Spy Ware)

2.3 สแปมเมล์หรือจดหมายอิเล็กทรอนิกส์ขยะ (Spam Mail)

เป็นจดหมายอิเล็กทรอนิกส์ที่มีลักษณะเหมือน ๆ กันและมีการส่งต่อตัวเองไปบนอินเทอร์เน็ตเป็นจำนวนมาก ซึ่งจะส่งไปยังผู้ที่ไม่เคยรับ สแปมเมล์ส่วนมากจะเป็นพวกเกี่ยวกับธุรกิจ โฆษณา หรือพวกสื่อลามก มีรูปแบบไม่แน่นอน และมีรูปแบบที่ออกแนวเชิญชวนน่าสงสัย เช่น วิธีที่จะทำให้รวยเร็ว หรือเกี่ยวกับภาพโป๊หรือเรื่องลามก สแปมเมล์มีอยู่ด้วยกัน 2 แบบ โดยแบบแรกจะกระจายไปตามกระดานข่าวเว็บบอร์ด โดยจะเขียนข้อความซ้ำ ๆ กัน ซึ่งข้อความไม่เกี่ยวข้องกับหัวข้อในเว็บบอร์ดนั้นเลย สแปมเมล์อีกรูปแบบหนึ่งคือส่งจดหมายอิเล็กทรอนิกส์ไปยังผู้รับโดยตรง โดยผู้รับนั้นไม่เคยรู้จักผู้ส่งเลย โดยสแปมเมล์จะทำการค้นหาที่อยู่ของจดหมายอิเล็กทรอนิกส์จากแหล่งต่าง ๆ ไม่ว่าจะจากเว็บบอร์ดต่าง ๆ ที่ไปเขียนข้อมูลไว้ หรือจากการสมัครสมาชิกต่าง ๆ หรือจากแหล่งอื่น

2.4 อาชญากรรมอิเล็กทรอนิกส์

สำนักงานตำรวจแห่งชาติ (www.police.go.th) ระบุว่าเทคโนโลยีสารสนเทศก่อให้เกิดประโยชน์มหาศาล แต่ในทางกลับกันกลุ่มผู้ไม่หวังดีก็ได้นำประโยชน์ของเทคโนโลยีสารสนเทศไปใช้ในทางที่ผิด ก่อให้เกิดความเสียหายทั้งทางด้านเศรษฐกิจ สังคม วัฒนธรรม และความมั่นคงของชาติ ซึ่งมีแนวโน้มที่เพิ่มขึ้นทั้งจำนวนคดีที่เกิดขึ้น และความร้ายแรง นอกจากนั้นในด้านความผิดคดีอาญาทั่วไปกลุ่มผู้กระทำผิดก็มักจะใช้เทคโนโลยีสารสนเทศมาอำนวยความสะดวกในการกระทำความผิดมากขึ้น เช่น การใช้จดหมายอิเล็กทรอนิกส์ หรือการจัดเก็บข้อมูลลูกค้า การพนัน ยาเสพติด ฯลฯ ตัวอย่างของการกระทำความผิด เช่น ผู้ขายโกงลูกค้าโดยประกาศขายโทรศัพท์มือถือราคาถูกในเว็บบอร์ด (Webboard) ของเว็บไซต์ (Website) มีชื่อเสียง ลูกค้าหลงเชื่อโอนเงินให้ไปแต่ไม่ได้รับโทรศัพท์ หรือการนัดพบส่งของแล้วปล้น ปัญหาการคัดลอกสิ่งที่มีลิขสิทธิ์ การขายบริการทางเพศผ่านอินเทอร์เน็ต หรือหลอกนัดพบแล้วแอบให้กินยานอนหลับเพื่อลักขโมยสิ่งของไป เป็นต้น

2.5 บทเรียนจากการโจมตีบนไซเบอร์ (Cyber Attack Case Studies)

จากการศึกษาพบว่ามีการเชื่อมโยงหรือมีความสัมพันธ์เกี่ยวข้องกันระหว่างที่มีความขัดแย้งต่าง ๆ เช่น ทางด้านการเมือง เศรษฐกิจ ลัทธิความ

เชื่อ จึงทำให้เกิดปฏิบัติการโจมตีบนไซเบอร์ หรือการโจมตีทางกายภาพเพิ่มขึ้น ตัวอย่างเหตุการณ์ที่เกิดขึ้น

2.5.1 ความขัดแย้งระหว่างอิสราเอลกับปาเลสไตน์ทำให้เกิดระเบิดพลีชีพเพิ่มขึ้น

2.5.2 ในปี ค.ศ. 2001 กรณีการกระทบกระทั่งระหว่างเครื่องบินตรวจการณ์ของสหรัฐฯ กับเครื่องบินรบของจีน ทำให้เกิดกลุ่มแฮกเกอร์ของจีนที่มีการรวมตัวทำการโจมตีขนาดใหญ่เป็นกลุ่มก้อน (Massive) อย่างต่อเนื่องและยาวนานเป็นอาทิตย์ต่อเป้าหมายต่าง ๆ ที่เป็นสหรัฐฯ

2.6 บทเรียนอันตรายจากบุคคลภายในองค์กร

อันตรายจากภายในเป็นอันตรายที่ร้ายแรงกว่าอันตรายจากภายนอก เพราะบุคคลภายในองค์กรสามารถเข้าถึงเครื่องคอมพิวเตอร์และฐานข้อมูลต่าง ๆ ได้โดยตรง เช่น แอบเปิดเครื่องเวลาไม่มีใครอยู่ หรือแอบเปิดช่องทางลับไว้เพื่อให้แฮกเกอร์จากภายนอกสามารถเจาะเข้าระบบได้ กรณีตัวอย่างมักจะไม่ค่อยปรากฏ เพราะหลาย ๆ หน่วยงานภาครัฐและเอกชนมักจะปกปิดความบกพร่องนี้ไว้ เนื่องจากจะส่งผลต่อชื่อเสียงของหน่วยงาน ต่อไปนี้เป็นตัวอย่างเหตุการณ์ที่เกิดขึ้น

2.6.1 พนักงานฝ่ายสารสนเทศของหน่วยบริการของทหารในสหรัฐฯ แห่งหนึ่งรู้ตัวว่ากำลังจะถูกปลด จึงแอบเข้ารหัสฐานข้อมูลสำคัญเอาไว้ ทำให้คนอื่นอ่านข้อมูลไม่ได้ และใช้เป็นข้อต่อรองในการถอดรหัส 10,000 ดอลลาร์ พร้อมคำสัญญาว่าจะไม่ฟ้องร้องเอาผิด โดยมีข้อมูลลับดังกล่าวเป็นตัวประกัน

2.6.2 โปรแกรมเมอร์ของบริษัทหนึ่งวางระเบิดเวลาด้วยโปรแกรมคอมพิวเตอร์เพื่อลบข้อมูลสำคัญทิ้งทั้งหมดหลังจากเขาลาออก เพื่อบริษัทจะได้เรียกตัวเขากลับมาแก้ไขปัญหา พร้อมกับจ่ายเงินเดือนให้มากขึ้นกว่าเดิม

2.6.3 ผู้จัดการและเสมียนของซูเปอร์มาร์เก็ตแห่งหนึ่งร่วมกันแก้ไขระบบคอมพิวเตอร์ให้โอนยอดขายบางส่วนเข้าบัญชีชั่วคราว จากนั้นในแต่ละวันก็จะหยิบเงินจากแคชเชียร์ออกมาเท่ากับจำนวนดังกล่าว แล้วลบบัญชีชั่วคราวนั้นทิ้งไปเพื่อทำลายหลักฐาน ทำเช่นนี้ 2 ปี ได้เงินกว่า 80 ล้านบาท

2.7 สงครามสารสนเทศกับสงครามการก่อการร้าย

เทคโนโลยีสารสนเทศที่พัฒนามาจนถึงปัจจุบันทำให้เกิดการเปลี่ยนแปลงอย่างมากมายในการทำสงคราม ทำให้อำนาจกำลังรบเพิ่มขึ้น ทำให้แนวรบเปลี่ยนไปเพราะอาวุธมีอำนาจทำลายล้างสูงขึ้น การติดต่อสื่อสารที่ฉับไวช่วยให้ทหารสามารถกระจายตัวและแทรกซึมไปในดินแดนข้าศึกได้ก่อนเกิดสงคราม สามารถกระจาย ซุ่มซ่อน และใช้อาวุธที่มีความแม่นยำสูง โดยใช้เทคโนโลยีสารสนเทศในการรวบรวมข้อมูลข่าวสาร กำหนดเป้าหมายและทำลายเป้าหมายด้วยความแม่นยำ จึงดูเหมือนว่าในยุคใหม่ กองทัพจะต้องพึ่งพาเทคโนโลยีสารสนเทศเพื่อทำให้เกิดจุดแข็ง แต่ก็เป็นจุดอ่อนรูปแบบใหม่เช่นเดียวกัน การใช้เทคโนโลยีที่ดีกว่าไม่ใช่หลักประกันว่าจะต้องชนะเสมอไป แต่คนที่รู้จักใช้เทคโนโลยีสารสนเทศทำให้เกิดประโยชน์แก่ฝ่ายตนมากที่สุดจึงจะเป็นฝ่ายชนะ เหตุการณ์ 11 ตุลาคม 2544 ที่สหรัฐอเมริกาพบว่าขบวนการก่อการร้ายอัลไกด้าใช้เทคโนโลยีสารสนเทศที่หาซื้อได้ง่าย ๆ ในปัจจุบัน เช่น การใช้โทรศัพท์มือถือ ภาพถ่ายดาวเทียม หรือภาพถ่ายที่หาซื้อได้จากอินเทอร์เน็ต การใช้อินเทอร์เน็ตประสานงาน จนทำให้สามารถสร้างความเสียหายได้อย่างมากมาย ลักษณะของกลุ่มหรือขบวนการก่อการร้ายในยุคสารสนเทศจึงมีการกระจายตัวเป็นกลุ่มเล็ก ๆ สามารถตัดสินตกลงใจด้วยตัวเองได้ สามารถสั่งการได้จากศูนย์กลางประสานกันเป็นลักษณะเครือข่ายการก่อการร้ายด้วยเทคโนโลยีสารสนเทศ เช่น อินเทอร์เน็ต โทรศัพท์มือถือ โทรศัพท์มือถือผ่านดาวเทียม เป็นต้น

2.8 ความปลอดภัยของระบบสารสนเทศในองค์กร

ในภาพรวมแล้วหมายถึงการทำให้ระบบคอมพิวเตอร์และข้อมูลสามารถใช้งานได้ตลอดเวลา และปกป้องสิทธิการเข้าถึงข้อมูลตามที่จำเป็น การรักษาความปลอดภัยระบบคอมพิวเตอร์ในองค์กรให้มีประสิทธิภาพนั้นขึ้นอยู่ความซับซ้อนในการออกแบบระบบ และเครือข่ายคอมพิวเตอร์ขององค์กรนั้น ๆ โดยในทางทฤษฎีจะต้องออกแบบระบบและเครือข่าย พร้อมวางแผนเพื่อรองรับการขยายระบบทั้งหมดก่อนที่จะวางระบบจริง แต่ในทางปฏิบัติแล้วระบบคอมพิวเตอร์จะขยายตัวตามขนาดขององค์กรและกำลังซื้อขององค์กร ทำให้การเลือกซื้อเทคโนโลยีมีความแตกต่างกัน ขึ้นอยู่กับผู้มีอำนาจในการตัดสินใจ ซึ่งทำให้มีผลกระทบต่อการรักษาความปลอดภัยของระบบคอมพิวเตอร์ขององค์กรโดยรวม

การออกแบบระบบคอมพิวเตอร์จะต้องมองถึงการขยายตัวและทิศทางการเปลี่ยนแปลงของเทคโนโลยีในระยะยาว การสนับสนุนทางด้านเทคนิค การปรับปรุงระบบอย่างสม่ำเสมอ เพื่อช่วยแก้ไขจุดอ่อนในการรักษาความปลอดภัยของระบบ เพราะแฮกเกอร์พยายามค้นหาจุดอ่อนที่จะจู่โจมและมักจะค้นพบอยู่เสมอ

การกำหนดนโยบายการรักษาความปลอดภัยระบบสารสนเทศก็มีความสำคัญเช่นเดียวกับการออกแบบระบบ ซึ่งจะต้องกำหนดให้สามารถป้องกันอันตรายจากทั้งภายนอกและภายในองค์กร นโยบายที่ควรกำหนด

2.8.1 นโยบายการรักษาความปลอดภัยเกี่ยวกับวิธีปฏิบัติของพนักงาน เช่น การให้สิทธิ์พนักงานที่เกี่ยวข้องในการเข้าใช้บริการศูนย์ข้อมูลเท่านั้น ไม่ว่าจะด้วยการใช้บัตรสมาร์ตการ์ด กุญแจประตู ระบบตรวจสอบลายนิ้วมือ หรือการติดตั้งโทรทัศน์วงจรปิดในศูนย์บริการข้อมูล การกำหนดรหัสผ่าน กำหนดให้พนักงานติดตั้งระบบป้องกันไวรัสในเครื่องของตนเอง กำหนดให้พนักงานทำการปรับปรุงระบบเครื่องของตนเองอัตโนมัติ เป็นต้น

2.8.2 การกำหนดนโยบายการรักษาความปลอดภัยเกี่ยวกับระบบคอมพิวเตอร์ เช่น การกำหนดการสำรองข้อมูลตามช่วงเวลาที่เหมาะสม การกำหนดให้มีศูนย์หรือหน่วยกู้คืนระบบที่ได้รับอันตรายจากภัยพิบัติ สำหรับองค์กรขนาดใหญ่กำหนดการตรวจสอบการรักษาความปลอดภัยระบบตามช่วงเวลาที่กำหนด มีการปรับปรุงระบบคอมพิวเตอร์และซอฟต์แวร์อยู่เสมอ กำหนดให้มีการซ่อมบำรุงฮาร์ดแวร์และซอฟต์แวร์ตามช่วงเวลาที่เหมาะสม กำหนดช่องทางบริการของระบบเท่าที่จำเป็นในการเข้าออกระบบติดตั้งระบบไฟร์วอลล์ และระบบป้องกันไวรัสตามตำแหน่งที่จำเป็น การปิดบริการของระบบเครือข่ายเท่าที่จำเป็น เป็นต้น

2.9 แนวโน้มภัยคุกคามด้านการโจมตีระบบเทคโนโลยีสารสนเทศ

2.9.1 สหรัฐฯ เป็นประเทศแหล่งกำเนิดของการโจมตีเครื่องคอมพิวเตอร์ส่วนใหญ่

2.9.2 ประเทศจีนเป็นประเทศที่ตกเป็นเป้าหมายในการโจมตีแบบ Denial of Service (DoS) บ่อยที่สุด คิดเป็น 63% ของการโจมตีระบบในภูมิภาคนี้

2.9.3 ไซแมนเทคตรวจพบคอมพิวเตอร์ที่ถูกควบคุมโดยบ็อตเฉลี่ยรวมกว่า 19,095 เครื่องในแต่ละวันในแถบประเทศกลุ่มเอเชีย-แปซิฟิก และญี่ปุ่น (เอพีเจ)

2.9.4 ไซแมนเทคยังพบอีกว่ามีคอมพิวเตอร์กว่า 2,268,219 เครื่อง ในประเทศกลุ่มเอพีเจที่ถูกควบคุมโดยบ็อตในช่วงระยะเวลาหนึ่งของครึ่งหลังของปี 2549

2.9.5 ประเทศจีนมีคอมพิวเตอร์ที่ตกเป็นเหยื่อของบ็อตมากที่สุดในแถบเอพีเจคือประมาณ 71% ของคอมพิวเตอร์ที่ตกเป็นเหยื่อทั้งหมด

2.9.6 กรุงปักกิ่งมีคอมพิวเตอร์ที่ตกเป็นเหยื่อของบ็อตถึงกว่า 16% ของคอมพิวเตอร์ที่ตกเป็นเหยื่อทั้งหมดในภูมิภาคเอพีเจ

2.9.7 ผู้ใช้ตามบ้านเป็นกลุ่มเป้าหมายการโจมตีสำคัญในกลุ่มเอพีเจ คิดเป็นร้อยละ 98 ของจำนวนการโจมตีแบบเฉพาะเจาะจงทั้งหมด

2.9.8 ประเทศจีนมีปัญหาของโค้ดอันตรายมากเป็นอันดับ 1 คือ 39% เมื่อเทียบกับประเทศอื่น ๆ ในกลุ่มเอพีเจ

2.9.9 ไต้หวันเป็นประเทศที่มีปัญหาของโค้ดอันตรายต่อจำนวนผู้ใช้อินเทอร์เน็ตมากที่สุดในกลุ่มประเทศเอพีเจ

2.9.10 โทรจันเป็นโค้ดอันตรายที่แพร่ระบาดมากที่สุดในกลุ่มประเทศเอพีเจ คิดเป็น 48% ของโค้ดอันตรายทั้งหมดที่ได้รับรายงานในภูมิภาคนี้

2.9.11 โค้ดอันตรายที่ได้รับรายงานเป็นอันดับสูงสุดในกลุ่มประเทศเอพีเจคือเวิร์มที่ชื่อลุคพี (Looked.P)

2.9.12 โค้ดอันตรายตระกูลล่าสุดที่มีการแพร่ระบาดมากที่สุดในประเทศกลุ่มเอพีเจในช่วงที่ผ่านมาก็คือเวิร์มที่ชื่อเดอะสแตรชั่น (The Stration)

2.9.13 ภัยคุกคามที่มุ่งหวังขโมยข้อมูลสำคัญคิดเป็นร้อยละ 60 ของจำนวนโค้ดอันตราย 50 อันดับแรกในกลุ่มประเทศเอพีเจ

2.9.14 2 ใน 3 อันดับแรกของโค้ดอันตรายในประเทศแถบเอพีเจเป็นโค้ดสำหรับขโมยรหัสผ่านของเกมออนไลน์ และแพร่ระบาดมากที่สุดในไต้หวัน

2.9.15 โค้ดอันตรายในกลุ่มประเทศเอพีเจกว่า 60% แพร่ระบาดตัวเองผ่าน CIFS (Common Internet File System)

2.9.16 ญี่ปุ่นเป็นประเทศที่มีเว็บไซต์หลอกลวงประเภทฟิชชิ่งมากที่สุดในแถบเอพีเจ

2.9.17 19% ของเว็บไซต์ฟิชชิ่งในแถบเอพีเจมีสถานที่ตั้งอยู่ในไทเป ซึ่งถือเป็นเมืองที่มีเว็บไซต์ฟิชชิ่งมากที่สุด

2.9.18 37% ของอีเมล์ขยะทั้งหมดในภูมิภาคเอพีเจต้นกำเนิดมาจากประเทศจีน ซึ่งถือว่ามากที่สุดเมื่อเทียบกับประเทศอื่น ๆ

2.9.19 ประเทศจีนมีเหยื่อที่กลายเป็นเครื่องมือสำหรับส่งอีเมล์ขยะ (Spam Zombies) มากกว่าประเทศอื่น ๆ โดยคิดเป็นประมาณ 43%

2.9.20 กรุงโซลเป็นเมืองที่มีจำนวนของเหยื่อที่ตกเป็นเครื่องมือสำหรับส่งอีเมล์ขยะมากที่สุด คิดเป็น 14%

2.9.21 ในพื้นที่แถบเอพีเจอีเมล์ขยะคิดเป็นประมาณ 69% ของอีเมล์ทั้งหมดที่มีการรับส่งถึงกันในภูมิภาค

2.9.22 ในกลุ่ม 20 ประเทศที่มีการใช้อีเมล์ในพื้นที่แถบเอพีเจ ประเทศฟิลิปปินส์มีอัตราส่วนของอีเมล์ขยะมากที่สุดคือ 88%

สรุป

หน่วยงานภาครัฐและเอกชนที่เกี่ยวข้อง ซึ่งปกติจะมีระบบป้องกันภัยคุกคามด้านเทคโนโลยีสารสนเทศอยู่ในระดับหนึ่งเป็นกำแพงป้องกันภัยคุกคามจากภายนอก ระบบป้องกันจะป้องกันระบบงานสารสนเทศที่มีการเชื่อมต่อกันเป็นเครือข่ายภายในหน่วยงาน เพื่อเป็นระบบเทคโนโลยีสารสนเทศที่ใช้ในการทำงานของหน่วยงาน ในส่วนนี้ถือว่าเป็นหัวใจของหน่วยงาน ความจำเป็นในการทำงานที่ต้องมีการติดต่อกับหน่วยงานภายนอก ทำให้ระบบเทคโนโลยีสารสนเทศของหน่วยงานต้องมีการเชื่อมต่อกับระบบเครือข่ายภายนอก เช่น อินเทอร์เน็ต จากแผนภาพจะเห็นว่าเครือข่ายภายนอกที่เชื่อมต่อจะต้องผ่านระบบป้องกันก่อนที่จะเข้าถึงระบบงานภายในหน่วยงาน

ภัยคุกคามนั้นเกิดได้จาก 2 แหล่ง แหล่งแรกคือการโจมตีจากภายนอก จะโจมตีผ่านเครือข่ายภายนอก

ที่เชื่อมต่อ ซึ่งจะต้องผ่านระบบป้องกัน หากระบบป้องกันมีประสิทธิภาพเพียงพอจะสามารถป้องกันการโจมตีนั้นได้ แต่หากการป้องกันไม่มีประสิทธิภาพเพียงพอจะทำให้สามารถโจมตีได้ถึงระบบงาน และมีผลกระทบต่อการทำงานในที่สุด ภัยคุกคามอีกแหล่งหนึ่งคือการโจมตีจากภายใน จะเห็นได้ว่าการโจมตีจากภายในนั้นอาจจะโจมตีจากภายในระบบป้องกันหรือภายในระบบงานที่อยู่หลังระบบป้องกัน จึงทำให้สามารถทำการโจมตีได้ง่าย การโจมตีชนิดนี้เป็นอันตรายมาก และป้องกันได้ยาก เนื่องจากเป็นการโจมตีที่มาจากบุคคลภายใน

แนวทางการบริหารจัดการต่อแนวโน้มภัยคุกคามด้านเทคโนโลยีสารสนเทศของกองทัพไทยมีดังนี้

1. กิจกรรมและแนวโน้มของภัยคุกคามด้านเทคโนโลยีสารสนเทศ

กิจกรรมภัยคุกคามด้านเทคโนโลยีสารสนเทศมีมากมาย มุ่งโจมตีและมีผลกระทบต่อระบบสารสนเทศที่เชื่อมต่อกันเป็นเครือข่าย และโดยเฉพาะระบบสารสนเทศที่เชื่อมต่อกับระบบอินเทอร์เน็ตจะเพิ่มความเสี่ยงที่จะถูกโจมตีจากสงครามสารสนเทศ กิจกรรมที่เป็นภัยคุกคามต่อระบบเทคโนโลยีสารสนเทศนั้นมีจากทั้งภายนอกและภายใน อันตรายจากภายนอกที่มาจากอินเทอร์เน็ต หรือระบบสื่อสารข้อมูลนั้น สามารถที่จะหาวิธีการป้องกันได้ ไม่ว่าอันตรายจากภายนอกจะเปลี่ยนรูปแบบการโจมตีอย่างไรก็ตามก็สามารถที่จะหาวิธีป้องกันต่าง ๆ ได้ แต่อันตรายจากภายในที่เกิดจากบุคคลภายในองค์กรที่ไม่หวังดี หรือบกพร่องในการรักษาความปลอดภัย หรือเป็นความผิดพลาดของมนุษย์ จะสร้างความเสียหายให้กับระบบสารสนเทศของหน่วยมากกว่า

แนวโน้มของภัยคุกคามด้านเทคโนโลยีสารสนเทศมีแนวโน้มที่จะเพิ่มขึ้น และมีความรุนแรงมากยิ่งขึ้น ซึ่งเกิดจากความขัดแย้งในด้านต่าง ๆ ไม่ว่าจะเป็นด้านการเมือง เศรษฐกิจ สังคม จิตวิทยา การทหาร วิทยาศาสตร์และเทคโนโลยี ที่มีการแข่งขันกันอย่างรุนแรงมากยิ่งขึ้น หรือแม้แต่เกิดจากความคึกคะนองของวัยรุ่นที่กระทำโดยไม่คำนึงถึงผลเสียหายที่จะเกิดขึ้น การทำงานในปัจจุบันและในอนาคตที่มีการเจริญเติบโตอย่างรวดเร็วนั้น มีแนวโน้มที่จะใช้ระบบสารสนเทศที่มีการเชื่อมต่อกันเป็นเครือข่าย และมีการเชื่อมต่อกับอินเทอร์เน็ตมากขึ้น และมีความจำเป็นมากยิ่งขึ้น ซึ่งก็เพิ่มแนวโน้มที่จะถูกคุกคามด้านสารสนเทศมากยิ่งขึ้น

2. ผลกระทบของภัยคุกคามด้านเทคโนโลยีสารสนเทศต่อกองทัพไทย

หน่วยงานภาครัฐและเอกชนที่สำคัญต่อความมั่นคงส่วนใหญ่เคยถูกโจมตีจากภัยคุกคามด้านเทคโนโลยีสารสนเทศ แต่ก็สามารถป้องกันแก้ไขได้โดยทำให้การทำงานหยุดชะงักเพียงเล็กน้อย ซึ่งการโจมตีส่วนใหญ่ที่เกิดขึ้นเป็นการโจมตีปกติธรรมดาที่ไม่ได้เกิดจากความขัดแย้ง แต่หากถูกโจมตีที่เกิดจากการขัดแย้งผลกระทบย่อมทำให้เกิดความเสียหายมาก เช่น ระบบไฟฟ้า ดังตัวอย่างเหตุไฟฟ้าดับที่อเมริกาและยุโรป

3. การใช้ระบบเทคโนโลยีสารสนเทศของหน่วยงานภาครัฐและเอกชน

หน่วยงานภาครัฐและเอกชนที่ใช้ระบบเทคโนโลยีสารสนเทศเป็นระบบสำคัญในการทำงานนั้นมีเพิ่มมากขึ้น ระบบเทคโนโลยีสารสนเทศส่วนใหญ่เชื่อมต่อกันเป็นระบบเครือข่าย ทั้งที่เป็นระบบปิดคือไม่เชื่อมต่อกับระบบอื่น ๆ ภายนอกองค์กร และระบบเปิดคือมีการเชื่อมต่อกับระบบอื่น ๆ ภายนอกองค์กร เช่น ระบบอินเทอร์เน็ต ซึ่งการเชื่อมต่อกันเป็นระบบเครือข่ายมีความจำเป็นอย่างหลีกเลี่ยงไม่ได้ในอนาคตในยุคสารสนเทศที่โลกมีการเชื่อมต่อกันเป็นเครือข่ายโยงใยติดต่อกันได้อย่างรวดเร็ว เป็นโลกโลกาภิวัตน์ที่มีการต่อสู้แข่งขันกันอย่างรุนแรง ดังนั้น หน่วยงานภาครัฐและเอกชนจึงต้องปรับตัว และมีความจำเป็นที่จะต้องใช้ระบบเทคโนโลยีสารสนเทศที่มีการเชื่อมต่อกันเป็นเครือข่าย เป็นระบบสำคัญในการทำงาน

หน่วยงานภาครัฐและเอกชนที่มีความสำคัญต่อความมั่นคงทั้ง 6 ด้าน ส่วนใหญ่จะเป็นหน่วยงานที่เกี่ยวกับโครงสร้างพื้นฐานที่สำคัญของชาติ เช่น ไฟฟ้า ประปา ระบบขนส่งคมนาคม ระบบโทรคมนาคมและการสื่อสาร เป็นต้น หน่วยงานป้องกันประเทศ และหน่วยงานอื่น ๆ ที่เกี่ยวข้อง

4. การจัดการต่อสู้ป้องกันภัยคุกคามด้านเทคโนโลยีสารสนเทศของหน่วยงานภาครัฐและเอกชน

หน่วยงานภาครัฐและเอกชนส่วนใหญ่ดูแลจัดการต่อสู้ป้องกันกันเอง ซึ่งบางครั้งชักช้า ไม่ทันการณ์ต่อภัยคุกคามรูปแบบใหม่ ๆ ที่ยังไม่เคยพบ ทำให้ไม่สามารถจัดการป้องกันได้ทัน มีหน่วยงานที่เป็นองค์กรของรัฐหรือองค์กรอิสระในการแจ้งเตือน และเสนอแนะวิธีป้องกันแก้ไข แต่ยังไม่เพียงพอในการจัดการต่อสู้ป้องกัน

5. แนวทางการปฏิบัติในการจัดการ การต่อสู้ป้องกันภัยคุกคามด้านสารสนเทศ

หน่วยงานกลางที่ทำหน้าที่ดูแลภัยคุกคามด้านสารสนเทศ ปัจจุบันเป็นองค์กรอิสระเพียงองค์กรเดียวทำหน้าที่แจ้งเตือนและเสนอแนะวิธีป้องกันแก้ไข และมีเพียงหน่วยงานของรัฐเพียงหน่วยงานเดียวที่ดูแลอาชญากรรมบนอินเทอร์เน็ตซึ่งยังไม่เพียงพอ สำหรับการดูแลหน่วยงานเกี่ยวกับความมั่นคงควรที่จะมีหน่วยงานกลางที่ทำหน้าที่ดูแล ตรวจสอบ การกำหนดมาตรฐานของระบบ การกำหนดมาตรการความปลอดภัยของหน่วยงานที่เกี่ยวข้องกับความมั่นคง หรือหน่วยงานอื่น ๆ ที่ต้องการ เพื่อให้มั่นใจได้ว่าระบบสารสนเทศที่มีความสำคัญต่อความมั่นคง ได้รับการจัดการการต่อสู้ป้องกันที่เพียงพอจากภัยคุกคามจากสงครามสารสนเทศ

6. กลยุทธ์ในการป้องกันภัยคุกคาม (Defense Strategies)

กลยุทธ์ในการป้องกันภัยคุกคามสามารถนำมาใช้เพื่อป้องกันภัยคุกคาม มีอยู่ด้วยกันหลายประเภทการเลือกกลยุทธ์มาใช้ขึ้นอยู่กับวัตถุประสงค์ของการป้องกันและความคุ้มค่าของค่าใช้จ่ายที่เกิดขึ้น

1. การป้องกันและการยับยั้ง (Prevention and Deterrence) เป็นกลยุทธ์การป้องกันภัยคุกคามมิให้เกิดขึ้น และเป็นการดำเนินการล่วงหน้าก่อนที่จะเกิดภัยคุกคาม เช่น การควบคุมการพัฒนาระบบ

2. การสืบหา (Detection) ถ้าองค์การสามารถสืบหาข้อผิดพลาดที่เกิดขึ้นในระบบได้เร็วเท่าใดก็จะช่วยลดความเสียหายที่จะเกิดขึ้นกับระบบลงได้มากขึ้นเท่านั้น

3. การกำจัด (Limitation) เป็นการจำกัดความเสียหายที่จะเกิดขึ้นจากการทำงานที่ผิดพลาดของระบบเทคโนโลยีสารสนเทศซึ่งสามารถทำไว้ก่อนล่วงหน้าได้

4. การฟื้นสภาพระบบ (Recovery) เป็นการวางแผนที่จะแก้ไขข้อบกพร่อง หรือความเสียหายที่เกิดขึ้นในระบบสารสนเทศให้รวดเร็วที่สุดเท่าที่จะทำได้

5. การแก้ไขข้อผิดพลาดให้ถูกต้อง (Correction) เป็นการแก้ไขข้อผิดพลาดที่เกิดขึ้นในการทำงานของระบบ

บรรณานุกรม

แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารกองทัพไทย และกองบัญชาการกองทัพไทย พ.ศ. 2557-2561

พันเอก ฤทธี อินทราวุธ, รองผู้อำนวยการศูนย์เทคโนโลยีทางทหาร. แนวทางการพัฒนา IT ของกองทัพเพื่อรองรับประชาคมอาเซียน