การวิเคราะห์และพัฒนาขีดความสามารถการปฏิบัติการสงคราม ไซเบอร์ของประเทศไทย

โดย

พลเรือตรี อรัญ นำผล
รองเจ้ากรมข่าวทหาร
กรมข่าวทหาร

นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ ๕๖
ประจำปีการศึกษา พุทธศักราช ๒๕๕๖ – ๒๕๕๗

บทคัดย่อ

เรื่อง **การวิเคราะห์และพัฒนาขีดความสามารถการปฏิบัติการสงครามไซเบอร์ของประเทศไทย (Analysis and Development of Cyber Warfare Capability of Thailand)**

ลักษณะวิชา **วิทยาศาสตร์และเทคโนโลยี**

ผู้วิจัย **พลเรือตรี อรัญ นำผล** **หลักสูตร วปอ.** **รุ่นที่ ๕๖**

ระบบสารสนเทศและเครือข่ายสารสนเทศ มีบทบาทมากต่อบุคคล สังคม หรือหน่วยงาน ระบบสารสนเทศและเครือข่ายสารสนเทศได้ถูกนำมาใช้เพิ่มประสิทธิภาพในการทำงานของภาคพลเรือน ทหาร และหน่วยงานราชการ เพื่อเพิ่มความรวดเร็วในการติดต่อสื่อสาร การจัดการระบบโครงสร้างพื้นฐานขนาดใหญ่และมีความสลับซับซ้อน รวมถึงเพิ่มความรวดเร็วของกระบวนการตัดสินใจ อย่างไรก็ตามการนำระบบสารสนเทศและเครือข่ายสารสนเทศมาใช้ รวมถึงการพึ่งพาว่าระบบจะทำงานอย่างมีประสิทธิภาพ กลับเป็นการเพิ่มความเสี่ยงให้กับการปฏิบัติการ หากระบบและเครือข่ายไม่สามารถทำงานได้ ทั้งจากความผิดพลาดที่ตัวระบบเองหรือการถูกโจมตีทางไซเบอร์ เนื่องจากองค์ประกอบของไซเบอร์สเปซ (Cyberspace) ที่ประกอบด้วยระบบสารสนเทศ เครือข่ายสารสนเทศ คอมพิวเตอร์ ซอฟแวร์ ฐานข้อมูล และอื่นๆ โดยเฉพาะเครือข่ายสารสนเทศที่ผู้ประสงค์ร้าย (Hackers) ใช้เป็นช่องทางในการโจมตี

การเป็นเป้าหมายของการโจมตีเป็นสิ่งที่หลีกเลี่ยงยาก และการโจมตีมีการพัฒนาความสลับซับซ้อนมากยิ่งขึ้น จึงมีความจำเป็นต้องวิเคราะห์และพัฒนาขีดความสามารถการปฏิบัติการสงครามไซเบอร์ของประเทศ ทั้งด้านการป้องกันหรือขีดความสามารถเชิงรับ และขีดความสามารถในการโจมตีหรือขีดความสามารถเชิงรุก โดยที่วิธีดำเนินการวิจัยเป็นการวิจัยเชิงคุณภาพ ด้วยการรวบรวมและวิเคราะห์ข้อมูลจากเอกสารที่เกี่ยวข้องรวมทั้งการสัมภาษณ์ผู้เชี่ยวชาญด้าน Computer Security หรือ Cyber Security

ผลการวิจัยพบว่าศักยภาพด้านสงครามไซเบอร์ของประเทศไทยในปัจจุบัน เป็นการดำเนินการแบบแยกส่วน เพื่อรองรับภารกิจของแต่ละกระทรวง หรือหน่วยงาน ไม่บูรณาการกัน ทำให้ขาดศักยภาพในการดำเนินการสงครามไซเบอร์ทั้งในทางรุก และในทางรับ สำหรับนโยบายด้านความมั่นคงแห่งชาติยังไม่มีแนวทางสงครามไซเบอร์เป็นการเฉพาะ แต่ก็มีการตระหนักถึงภัยคุกคามที่เปลี่ยนแปลงไป

การพัฒนาขีดความสามารถการปฏิบัติการสงครามไซเบอร์ของประเทศไทยที่สำคัญมีดังนี้

๑. จัดให้มีหน่วยงานความมั่นคงด้านสงครามไซเบอร์กลางเป็นการเฉพาะ เช่น National Cyber Security Agency และ National Cyber Security Committee เพื่อกำหนดนโยบายด้านสงครามไซเบอร์ที่ชัดเจนและเป็นการเฉพาะ

๒. ยกระดับความรู้ความสามารถของบุคลากรในสายวิชาชีพความมั่นคงปลอดภัยสารสนเทศ ให้อยู่ในระดับสากล รวมทั้งการสร้างเส้นทางความก้าวหน้าในสายอาชีพ พร้อมค่าตอบแทนที่เหมาะสม

๓. ปลูกจิตสำนึกด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในองค์กร ประชาชน โดยเฉพาะเยาวชน

๔. ปรับปรุงกฎหมาย ระเบียบ ข้อปฏิบัติ ให้ทันสมัย รวมถึงอาจจะต้องมีการออกกฎหมายที่รองรับการปฏิบัติของเจ้าหน้าที่ด้านความมั่นคงในการดำเนินการด้านไซเบอร์ เช่น การรองรับการดักจับและตรวจสอบข้อมูลอย่างถูกกฎหมาย (Lawful Interception)

๕. มีกฎหมายที่รองรับแนวความคิดด้านการทำ National Cyber Gateway หรือการเพิ่มขีดความสามารถในการตรวจสอบการกระทำผิดทางไซเบอร์ การโจมตีทางไซเบอร์ กับทุกเส้นทางการเชื่อมต่อเครือข่ายอินเทอร์เน็ตในประเทศกับต่างประเทศ

๖. สนับสนุนการวิจัยและพัฒนาโดยเฉพาะด้านซอฟต์แวร์ เช่น ระบบจำลองยุทธ์ทางสงครามไซเบอร์ (Cyber Security Simulator)

๗. แสวงความร่วมมือกับประเทศเพื่อนบ้านในภูมิภาค หรือกับประเทศพันธมิตรที่มีความรู้ ความสามารถ และประสบการณ์

คำนำ

ไซเบอร์สเปซ (Cyberspace) เป็นโลกเสมือนที่มีบทบาทมากต่อบุคคล สังคม และหน่วยงาน ปัจจุบันไซเบอร์สเปซเป็นส่วนสำคัญของระบบงานในองค์กร ในชีวิตประจำวัน ด้วยความสำคัญนี้ ไซเบอร์สเปซจึงเป็นเป้าหมายของการถูกโจมตีจากผู้ไม่หวังดีเพื่อผลประโยชน์ต่างๆ การเป็นเป้าหมายของการโจมตีเป็นสิ่งที่หลีกเลี่ยงยาก และการโจมตีมีการพัฒนาความสลับซับซ้อนมากยิ่งขึ้น จึงมีความจำเป็นต้องวิเคราะห์และพัฒนาขีดความสามารถการปฏิบัติการสงครามไซเบอร์ของประเทศ ทั้งด้านการป้องกันหรือขีดความสามารถเชิงรับ และขีดความสามารถในการโจมตีหรือขีดความสามารถเชิงรุก

การวิจัยเพื่อให้ทราบถึงศักยภาพด้านสงครามไซเบอร์ของประเทศไทยในปัจจุบัน จึงมีความจำเป็นเพื่อให้การกำหนดแนวทางการพัฒนามีความเหมาะสมและสอดคล้องกับสภาพแวดล้อมตลอดจนเพื่อให้การใช้ประโยชน์จากระบบสารสนเทศและเครือข่ายสารสนเทศของไทย มีความมั่นคงปลอดภัยและบรรลุวัตถุประสงค์ตามที่กำหนด

ผู้วิจัยได้เลือกหัวข้อนี้เพื่อทำเอกสารวิจัยส่วนบุคคล เนื่องมาจากเป็นเรื่องน่าสนใจเป็นประเด็นปัญหาที่เกี่ยวกับความมั่นคงแห่งชาติด้านวิทยาศาสตร์และเทคโนโลยี จึงหวังว่าผลการวิจัยจะเป็นประโยชน์ นำไปใช้กำหนดเป็นยุทธศาสตร์ชาติได้อย่างเหมาะสม สอดคล้องกับสถานการณ์ปัจจุบันและเป็นแนวทางในการพัฒนาในอนาคต

พล.ร.ต. ร.น.

(อรัญ นำผล)
นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตร วปอ. รุ่นที่ ๕๖
ผู้วิจัย

สารบัญ

สารบัญ (ต่อ)

สารบัญแผนภาพ

บทที่ ๑

บทนำ

ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันระบบสารสนเทศและเครือข่ายสารสนเทศ มีบทบาทมากทั้งต่อบุคคล สังคม หรือหน่วยงาน ระบบสารสนเทศและเครือข่ายสารสนเทศได้ถูกนำมาใช้เพิ่มประสิทธิภาพในการทำงานทั้งภาคพลเรือน ทหาร และหน่วยงานราชการ โดยระบบสารสนเทศและเครือข่ายสารสนเทศเหล่านี้ถูกนำมาใช้เพื่อเพิ่มความรวดเร็วในการติดต่อสื่อสาร การจัดการระบบโครงสร้างพื้นฐานที่มีขนาดใหญ่และมีความสลับซับซ้อน รวมถึงเพิ่มความรวดเร็วของกระบวนการตัดสินใจ ทำให้กระบวนการทำงานมีประสิทธิภาพมากยิ่งขึ้น ก่อให้เกิดการพัฒนาในภาพรวมอย่างก้าวกระโดดทางด้านเศรษฐกิจ การเมือง การทหาร และสังคม จนมีคำกล่าวว่าการเข้ามามีบทบาทของระบบสารสนเทศและเครือข่ายสารสนเทศเป็นการปฏิวัติยุคที่ ๓ คือ การปฏิวัติทางด้านเทคโนโลยีข้อมูลข่าวสาร (Information Technology Revolution) ซึ่งต่อเนื่องมาจากการปฏิวัติยุคที่ ๑ หรือการปฏิวัติทางเกษตรกรรม (AgriculturalRevolution) และการปฏิวัติยุคที่ ๒ หรือการปฏิวัติทางอุตสาหกรรม (Industrial Revolution) อย่างไรก็ตามการนำระบบสารสนเทศและเครือข่ายสารสนเทศมาใช้มากขึ้น รวมถึงการพึ่งพาว่าระบบจะทำงานอย่างมีประสิทธิภาพ กลับเป็นการเพิ่มความเสี่ยงให้กับการปฏิบัติการหากระบบและเครือข่ายไม่สามารถทำงานได้ ทั้งจากความผิดพลาดที่ตัวระบบเองหรือการถูกโจมตีทางไซเบอร์ (Cyber Attack) จากฝ่ายตรงข้าม เนื่องจากองค์ประกอบของไซเบอร์สเปซ (Cyber Space) ที่ประกอบด้วยระบบสารสนเทศเครือข่ายสารสนเทศ คอมพิวเตอร์ ซอฟแวร์ ฐานข้อมูล และอื่นๆ โดยเฉพาะเครือข่ายสารสนเทศที่ผู้ประสงค์ร้าย (Hackers) ใช้เป็นช่องทางในการโจมตี

การที่ระบบสารสนเทศและเครือข่ายสารสนเทศถูกนำมาใช้ประโยชน์ และมีความสำคัญมากขึ้นในกระบวนการการทำงานต่างๆ ส่งผลให้ระบบสารสนเทศและเครือข่ายสารสนเทศเหล่านี้กลายเป็นเป้าหมายของการโจมตีและการใช้ประโยชน์ในทางที่ไม่เหมาะสม ทั้งจากผู้ไม่หวังดีและศัตรูฝ่ายตรงข้าม โดยเฉพาะระบบสารสนเทศและเครือข่ายสารสนเทศที่เกี่ยวข้องกับโครงสร้างพื้นฐานหลักของชาติ (National Critical Infrastructure) การโจมตีทางไซเบอร์มีความแตกต่างจากการโจมตีของสงครามตามรูปแบบ (Traditional Warfare) แต่ผลจากการโจมตีเหมือนกัน คือทำให้ขีดความสามารถของฝ่ายตรงข้ามลดลง เช่น การเปรียบเทียบการโจมตีทางอากาศกับซอฟท์แวร์ประสงค์ร้ายหรือ มัลแวร์ (Malicious Software: Malware) การโจมตีทางอากาศเป็นการทำลายสิ่งปลูกสร้างทางกายภาพ เช่น สนามบิน หอควบคุมการบิน ฯลฯ ส่วนมัลแวร์ทำให้ระบบ

ควบคุมการบิน (Air Traffic ControlSystem) ที่ทำงานด้วยคอมพิวเตอร์ เชื่อมโยงระบบย่อยต่างๆ เข้าด้วยกันด้วยเครือข่ายสารสนเทศเป็นอัมพาตไม่สามารถใช้งานได้ ผลของการโจมตีทางอากาศหรือมัลแวร์ ต่างก็ทำให้สนามบินไม่สามารถใช้งานได้ หรืออีกตัวอย่างที่เป็นข่าวกล่าวถึงมากในวงการสงครามไซเบอร์ ได้แก่ ความขัดแย้งระหว่างอิหร่านกับนานาชาติ กรณีการพัฒนาขีดความสามารถด้านนิวเคลียร์ ที่ถูกมองว่าไม่ใช่การพัฒนาด้านพลังงานแต่เป็นการพัฒนาด้านอาวุธนิวเคลียร์ทำลายล้างสูง จนถูกโจมตีด้วยอาวุธทางไซเบอร์หรือซอฟท์แวร์ประสงค์ร้าย ชื่อ Stuxnet ทำให้โครงการพัฒนาดังกล่าวต้องหยุดชะงักลงทันที โปรแกรมมัลแวร์ Stuxnet ขนาดครึ่งเมกกะไบต์มีอำนาจทำลายล้างเท่าการโจมตีทางอากาศด้วยเครื่องบินโจมตีด้วยขีปนาวุธเลยทีเดียว จากการวิเคราะห์ของผู้เชี่ยวชาญด้านการรักษาความปลอดภัยเชื่อกันว่ามัลแวร์ Stuxnet ได้รับการพัฒนาร่วมกันโดยประเทศอิสราเอลและประเทศสหรัฐอเมริกา

เมื่อ ค.ศ.๑๙๔๘ Hans Morgenthau กล่าวว่า ความมั่นคงของชาติ ขึ้นอยู่กับความสงบเรียบร้อยตามแนวชายแดนกับประเทศเพื่อนบ้าน หลังเหตุวินาศกรรม ๑๑ กันยายน ๒๕๔๔ (๙/๑๑) นักยุทธศาสตร์ทางการทหารเห็นว่าการก่อการร้ายเป็นภัยคุกคามต่อความมั่นคงของชาติที่สำคัญ แต่ปัจจุบันการโจมตีทางไซเบอร์เป็นภัยคุกคามต่อความมั่นคงของชาติในระดับต้นๆ

โลกของไซเบอร์สเปซมีความกว้างใหญ่ ไม่มีพรมแดนแบ่งแยก มีความรวดเร็วเทียบเท่าความเร็วของแสง ตลอดจนไซเปอร์สเปซเชื่อมโลกทั้งโลกเข้าด้วยกัน ดังนั้นผลกระทบจากการโจมตีทางไซเบอร์จึงขยายตัวจากประเทศหนึ่งไปยังอีกประเทศหนึ่งอย่างรวดเร็ว การเตรียมความพร้อมเพื่อรองรับการโจมตีทางไซเบอร์จึงต้องประกอบการเตรียมความพร้อมภายในประเทศ ตลอดจนการแสวงความร่วมมือกับประเทศเพื่อนบ้านในภูมิภาค เช่น ประชาคมอาเซียน (Asean Community – AC) หรือกับประเทศพันธมิตรที่มีความรู้ ขีดความสามารถ และประสบการณ์ เช่น สหรัฐอเมริกา และประเทศในสหภาพยุโรป เป็นต้น

ตราบใดที่ระบบสารสนเทศและเครือข่ายสารสนเทศถูกนำมาใช้งาน การเป็นเป้าหมายของการโจมตีเป็นสิ่งที่หลีกเลี่ยงได้ยาก เนื่องจากปรัชญาการออกแบบของเครือข่ายสารสนเทศที่เน้นเรื่องการเข้าถึง (Accessibility) และในขณะที่การโจมตีมีการพัฒนาความสลับซับซ้อนมากยิ่งขึ้น จึงมีความจำเป็นที่ต้องวิเคราะห์และพัฒนาขีดความสามารถการปฏิบัติการสงครามไซเบอร์ของประเทศทั้งด้านการป้องกันหรือขีดความสามารถเชิงรับ และขีดความสามารถในการโจมตีหรือขีดความสามารถเชิงรุก เพื่อให้การใช้ประโยชน์จากระบบสารสนเทศและเครือข่ายสารสนเทศของไทย มีความมั่นคงปลอดภัยและมีประสิทธิภาพ ส่งเสริมให้เกิดการพัฒนาในด้านต่างๆ สามารถแข่งขันกับประชาคมโลกได้

วัตถุประสงค์ของการวิจัย

๑. เพื่อศึกษาหลักการ แนวทาง เทคโนโลยี และการพัฒนาขีดความสามารถด้านการปฏิบัติการสงครามไซเบอร์ของหน่วยงานต่างๆ ของไทย และของต่างประเทศ

๒. เพื่อวิเคราะห์และประเมินศักยภาพด้านสงครามไซเบอร์ของประเทศไทย

๓. เพื่อเสนอแนวทางการพัฒนาขีดความสามารถด้านการปฏิบัติการสงครามไซเบอร์ของประเทศไทย

ขอบเขตของการวิจัย

การวิจัยครั้งนี้จะศึกษาและวิเคราะห์ ถึงปัญหาที่เกิดขึ้นกับการใช้ข้อมูลและระบบสารสนเทศในประเทศไทย โดยเฉพาะอย่างยิ่ง ระบบสารสนเทศเพื่อการบริหาร รวมถึงเทคโนโลยี และเทคนิค ที่เกี่ยวข้องกับการป้องกันและการโจมตีทางไซเบอร์ต่อข้อมูลและระบบสารสนเทศดังกล่าว ตลอดจนแนวทางการพัฒนาขีดความสามารถด้านการปฏิบัติการสงครามไซเบอร์

วิธีดำเนินการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ โดยการรวบรวมและวิเคราะห์ข้อมูลใน ๒ ลักษณะดังนี้

๑. ข้อมูลปฐมภูมิ – การสัมภาษณ์ผู้เชี่ยวชาญด้าน Computer Security, Cyber Security รวมทั้งเจ้าหน้าที่ที่เกี่ยวข้องด้านระบบสารสนเทศของหน่วยงานราชการในไทย และหน่วยงานอื่นๆ

๒. ข้อมูลทุติยภูมิ – เอกสารที่เกี่ยวข้อง เช่น ตำรา วารสาร เอกสารทางวิชาการ เอกสารทั้งภายในและต่างประเทศ บทความ ตลอดจนการค้นคว้าทางอินเทอร์เน็ต

ประโยชน์ที่ได้รับจากการวิจัย

๑. ทำให้ทราบถึงปัญหา หรือ การถูกบุกรุกและการโจมตีทางไซเบอร์ที่มีผลกระทบต่อข้อมูลและระบบสารสนเทศ

๒. ทำให้ทราบถึงหลักการ แนวทาง และเทคโนโลยี ที่เกี่ยวข้องกับการพัฒนาขีดความสามารถด้านการปฏิบัติการสงครามไซเบอร์

๓. ทำให้ทราบศักยภาพด้านสงครามไซเบอร์ของประเทศไทย

๔. ทำให้มีข้อมูลประกอบในการพิจารณาวางแผนการพัฒนาขีดความสามารถด้านการปฏิบัติการสงครามไซเบอร์ของประเทศไทย

๕. ทำให้ทราบแนวทางการพัฒนาขีดความสามารถด้านการปฏิบัติการสงครามไซเบอร์ของประเทศไทย

คำจำกัดความ

ไซเบอร์สเปซ (Cyberspace) หมายถึงพื้นที่ว่าง ในที่นี้หมายถึง ที่ว่าง หรืออวกาศที่สร้างขึ้นด้วยระบบอิเล็กทรอนิกส์ ที่ใช้เพื่อสื่อสารติดต่อกันซึ่งสามารถติดต่อกันได้ทั่วโลกเหมือนท่องไปในอวกาศ เช่นการส่งไปรษณีย์อิเล็กทรอนิกส์ การติดต่อสื่อสารทางเสียงหรือภาพ เป็นต้นโดยทั่วไปหมายรวมถึงระบบอินเตอร์เน็ต ด้วย

สงครามไซเบอร์ (Cyber Warfare) หมายถึง การปฏิบัติการที่ใช้คอมพิวเตอร์ ระบบสารสนเทศ และเครือข่ายสารสนเทศ เป็นเครื่องมือ ของหน่วยงานด้านความมั่นคง ในการป้องกันโจมตีหรือทำลายระบบสารสนเทศของตน และโจมตีหรือทำลายระบบสารสนเทศของอีกฝ่ายหนึ่ง

บทที่ ๒
ทฤษฎีและแนวคิดที่เกี่ยวข้องกับสงครามไซเบอร์

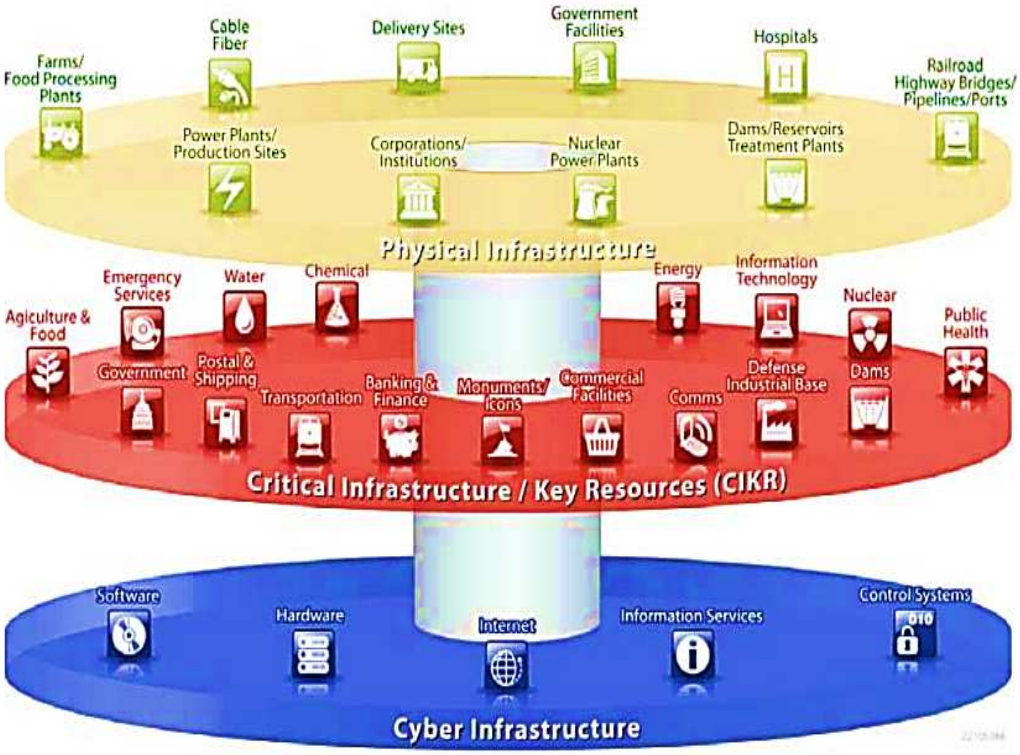
กล่าวนำ

เป็นที่ทราบกันดีว่าสงครามไซเบอร์เป็นสงครามรูปแบบใหม่ที่มีรูปแบบการโจมตี ตลอดจนแนวคิดและทฤษฎีที่แตกต่างจากสงครามแบบดั้งเดิม สงครามไซเบอร์มีความสลับซับซ้อน มีการพัฒนาและเปลี่ยนแปลงควบคู่ไปกับเทคโนโลยีสารสนเทศและการสื่อสาร งานวิจัยในบทนี้จะกล่าวถึงรูปแบบการโจมตีของสงครามไซเบอร์ แนวคิดการปฏิบัติการสงครามไซเบอร์ นโยบาย หลักการ และกฎหมายที่เกี่ยวข้องกับสงครามไซเบอร์ของประเทศไทย หน่วยงานที่เกี่ยวข้องกับการปฏิบัติการสงครามไซเบอร์ ตลอดจนหลักการกำหนดขีดความสามารถเพื่อรองรับสงครามไซเบอร์ของประเทศไทยในอนาคต

แนวความคิดการโจมตีทางไซเบอร์

การโจมตีทางไซเบอร์หมายถึงการดำเนินการเชิงรุกโดยบุคคล กลุ่มบุคคล หรือองค์กร ด้วยการใช้เครื่องมือโจมตีเพื่อใช้ขโมย เปลี่ยนแปลง หรือทำลาย และมีเป้าหมายต่อจุดอ่อนของเครื่องคอมพิวเตอร์ เครือข่ายคอมพิวเตอร์ ข้อมูล ระบบสารสนเทศ รวมถึงอุปกรณ์อื่นๆ ที่เชื่อมต่อกับเครือข่ายสารสนเทศ โดยเฉพาะหากเป้าหมายเหล่านี้เป็นระบบที่มีความสำคัญ ดังเช่นระบบในแผนภาพที่ ๒-๑ การโจมตีดังกล่าวมีผลกระทบเป็นอย่างมากต่อการขับเคลื่อนของประเทศ ทั้งทางด้าน เศรษฐกิจ สังคม และการเมือง

แผนภาพที่ ๒-๑ระบบสารสนเทศที่สำคัญ แบ่งตามชนิดโครงสร้าง[๑]



การโจมตีทางไซเบอร์มีหลายประเภท แต่สามารถแบ่งได้การโจมตีจากภายใน และการโจมตีจากภายนอก

๑. การโจมตีจากภายใน (Insider Attack/ CINDER[๒]) หมายถึงการโจมตีทางไซเบอร์จากบุคคล หรือกลุ่มบุคคลในองค์กร ที่เป็นเจ้าของเครื่องคอมพิวเตอร์ เครือข่ายคอมพิวเตอร์ ข้อมูล ระบบสารสนเทศ อุปกรณ์อื่นๆ ที่เชื่อมต่อกับเครือข่ายสารสนเทศ รวมถึงตัวบุคคลผู้ใช้ระบบดังกล่าว บุคคลหรือกลุ่มบุคคลดังกล่าวสามารถเข้าถึงระบบได้จากภายในโดยอาจจะมีสิทธิ์ในการเข้าถึงระบบหรือข้อมูล แต่ใช้สิทธิ์ดังกล่าวอย่างไม่ถูกต้อง ซึ่งการเข้าถึงดังกล่าวจะไม่ถูกมองว่าเป็นการโจมตีโดยระบบที่ใช้ตรวจสอบการบุกรุกโจมตีทางระบบสารสนเทศ (Intrusion Detection System: IDS) การโจมตีจากภายในจะถือว่ามีผลเกิดขึ้นก็เมื่อเกิดความเสียหายจากการเปิดเผยข้อมูลที่ตัวเองมีสิทธิ์เข้าถึงโดยไม่ได้รับอนุญาต ซึ่งปัญหาดังกล่าวนี้เป็นปัญหาที่เกิดต่อเนื่องตั้งแต่เริ่มมีการใช้ระบบคอมพิวเตอร์ในกระบวนการทำงานในทศวรรษที่ ๑๙๘๐ โดยมีการวิเคราะห์ถึงปัญหาดังกล่าวโดยหน่วยงานที่ทำหน้าที่กำหนดมาตรฐาน

---

[๑] กองทัพอากาศสหรัฐอเมริกา,Air Force Doctrine Document 3-12: Cyberspace Operations, 15 July 2010

[๒] DARPA: Information Innovation Office, Cyber-Insider Threat (CINDER), URL: http://www.darpa.mil/Our_Work/I2O/Programs/Cyber-Insider_Threat_%28CINDER%29.aspx เข้าถึงเมื่อ ๒๖ ก.พ.๕๗

ของสหรัฐฯ (National Institute of Standards and Technology: NIST) ว่าการโจมตีภายใน[๓] เป็นปัญหาที่เกิดจากการที่กระบวนการควบคุมนั้นไม่สอดคล้องกับนโยบายด้านการรักษาความมั่นคงปลอดภัยขององค์กรทำให้ผู้ใช้ทั่วไปสามารถหลีกเลี่ยงนโยบายด้านการรักษาความมั่นคงปลอดภัยได้ ผู้ดูแลระบบไม่สามารถบังคับใช้มาตรการการรักษาความปลอดภัยเนื่องจากกระบวนการควบคุมนั้นไม่ครอบคลุม อีกทั้งยังไม่สามารถตรวจสอบการละเมิดนโยบายและมาตรการการรักษาความปลอดภัยเนื่องจากไม่มีกระบวนการตรวจสอบที่เหมาะสม และถึงแม้ว่ามีกระบวนการตรวจสอบที่เหมาะสม ปริมาณข้อมูลที่มากจะทำให้ผู้ที่รับผิดชอบไม่สามารถค้นหาการละเมิดนโยบายด้านการรักษาความมั่นคงปลอดภัยได้

๒. การโจมตีจากภายนอก (Outsider Attack) เป็นการเข้าถึงโดยไม่ได้รับอนุญาตโดยอาศัยจุดอ่อนของเครื่องคอมพิวเตอร์ เครือข่ายคอมพิวเตอร์ ข้อมูล ระบบสารสนเทศ อุปกรณ์อื่นๆ ที่เชื่อมต่อกับเครือข่ายสารสนเทศ รวมถึงตัวผู้ใช้ระบบดังกล่าว โดยการโจมตีอาจจะมีได้ตั้งแต่การติดตั้งมัลแวร์บนเครื่องคอมพิวเตอร์ไปจนถึง ทำลายระบบสารสนเทศที่เป็นโครงสร้างพื้นฐาน ซึ่งจะส่งผลกระทบเป็นวงกว้างต่อประเทศได้ นอกจากนี้ปัจจุบันการโจมตีทางไซเบอร์ยังพัฒนาให้มีขีดความสามารถและความซับซ้อนเพิ่มมากขึ้น

การโจมตีทางไซเบอร์ทั้งภายในและภายนอกนั้น มีเทคนิคที่ใช้ในการโจมตีหลายประเภท ซึ่งขึ้นอยู่กับว่าผู้โจมตีต้องการโจมตีที่ เครื่องคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูล เครือข่าย หรือ คน โดยสามารถแบ่งชนิดการโจมตีได้ดังนี้

๑. การโจมตีที่ตัวเครื่องคอมพิวเตอร์ และระบบสารสนเทศ เป็นการอาศัยจุดอ่อนของซอฟท์แวร์ระบบปฏิบัติการ และซอฟท์แวร์โปรแกรมที่ทำงานบนเครื่องดังกล่าว ในการเข้าโจมตีและควบคุมเครื่อง โดยจุดอ่อนดังกล่าวเกิดจากการพัฒนาซอฟท์แวร์แบบไม่คำนึงถึงความปลอดภัย ทำให้เกิดช่องโหว่ (Vulnerabilities) หรือบั๊ก (Software Bug) ที่สามารถโจมตีได้ เช่น Buffer Overflow[๔], Heap overflow[๕] , Stack Overflow[๖] หรือ Format String Attack[๗]

๒. การโจมตีที่เครือข่าย โจมตีที่จุดอ่อน ซึ่งก็คือเครือข่ายเป็นเส้นทางที่ใช้ในการติดต่อสื่อสาร การส่งผ่านข้อมูล โดยรูปแบบการโจมตีส่วนใหญ่จะเป็นการลักลอบดักรับข้อมูล เช่น การดักฟังการติดต่อสื่อสาร (Wiretapping) การหลอกลวงแบบ Man-In-the-Middle (แผนภาพที่ ๒-๒) ให้ผู้ที่ถูกโจมตีคิดว่าการติดต่อสื่อสารเป็นการติดต่อสื่อสารระหว่างต้นทางกับปลายทางจริง แต่ในความเป็นจริงเป็นการติดต่อสื่อสารผ่านผู้ทำการโจมตีเป็นตัวกลาง นอกจากนี้ยังมีการโจมตีแบบที่ทำให้ผู้ที่ถูกโจมตีไม่สามารถให้บริการได้ที่เรียกว่า Denial of Service (DoS)

---

[๓] NIST, Trends for the future: Insider Threats, URL: http://csrc.nist.gov/publications/nistir/threats/subsubsection3_4_4_2.html, เข้าถึงเมื่อ ๒๖ ก.พ.๕๗

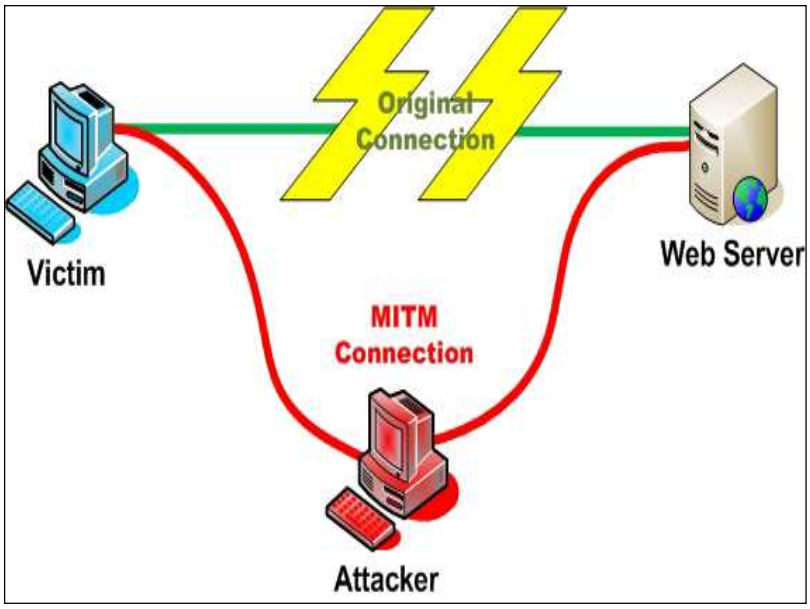
[๔] Wikipedia, “Buffer overflow”, URL: http://en.wikipedia.org/wiki/Buffer_overflow เข้าถึงเมื่อ ๒๗ ก.พ.๕๗

[๕] Wikipedia, “Heap overflow”, URL: http://en.wikipedia.org/wiki/Heap_overflow เข้าถึงเมื่อ ๒๗ ก.พ.๕๗

[๖] Wikipedia, “Heap overflow”, URL:http://en.wikipedia.org/wiki/Stack_overflow เข้าถึงเมื่อ ๒๗ ก.พ.๕๗

[๗] Wikipedia, “Uncontrolled format string”, URL: http://en.wikipedia.org/wiki/Format_string_attack เข้าถึงเมื่อ ๒๗ ก.พ.๕๗

แผนภาพที่ ๒-๒ ภาพแสดงการโจมตีแบบ Man in the Middle



๓. การโจมตีที่คน เป็นการโจมตีโดยอาศัยจุดอ่อนของคน ซึ่งเป็นที่ยอมรับกันว่าเป็นจุดอ่อนของวงจรการรักษาความปลอดภัย[๘] โดยการโจมตีแบบนี้เรียกว่าการโจมตีแบบวิศวกรรมสังคม (Social Engineering[๙]) ซึ่งเป็นเทคนิคการหลอกลวงโดยใช้หลักการพื้นฐานทางจิตวิทยาเพื่อให้เหยื่อเปิดเผยข้อมูล ซึ่งบางครั้งอาจไม่จำเป็นต้องใช้เทคโนโลยีเข้ามาเกี่ยวข้องเลย ผู้ที่ตกเป็นเหยื่อของ Social Engineering อาจจะตกเป็นเหยื่อโดยความตั้งใจหรือไม่ตั้งใจของผู้ไม่หวังดีก็ได้ กล่าวคือ ถ้าผู้ไม่หวังดีมีเป้าหมายเฉพาะเจาะจง เช่น ต้องการข้อมูลความลับขององค์กรใดองค์กรหนึ่ง เหยื่อในที่นี้ก็มักจะเป็นผู้ที่มีสิทธิในการเข้าถึงข้อมูลความลับขององค์กรนั้น แต่หากเป้าหมายของผู้ไม่หวังดีเป็นแบบที่ไม่ได้เจาะจงเหยื่อ เช่น ต้องการรหัสบัตรเครดิต หรือบัญชีผู้ใช้และรหัสผ่านของบริการต่าง ๆ ของใครก็ได้ เหยื่อของผู้ไม่หวังดีนี้จะเป็นใครก็ตามซึ่งหลงเชื่อการหลอกลวงนั้น

---

[๘] Forbes.com, “Humans: The Weakest Link In Information Security”, URL: http://www.forbes.com/sites/ciocentral/2011/11/03/humans-the-weakest-link-in-information-security/ เข้าถึงเมื่อ ๒๗ ก.พ.๕๗

[๙] วิศัลย์ ประสงค์สุข และคณะ, “Social Engineering”, ThaiCERT, URL: https://www.thaicert.or.th/papers/general/2012/pa2012ge017.html เข้าถึงเมื่อ ๒๗ ก.พ.๕๗

รูปแบบการโจมตีทางไซเบอร์

การโจมตีทางไซเบอร์ดำเนินการโดยผู้ไม่หวังดีมีหลากหลายรูปแบบดังนี้

๑. โปรแกรมมัลแวร์ (Malicious Software – Malware) เช่น Virus, Worm, Trojan Horse, SQL Injection, Spyware

๒. Spoofing

๓. Denial – of - Service (DOS)

๔. Phishing

๕. Evil Twins

๖. Pharming

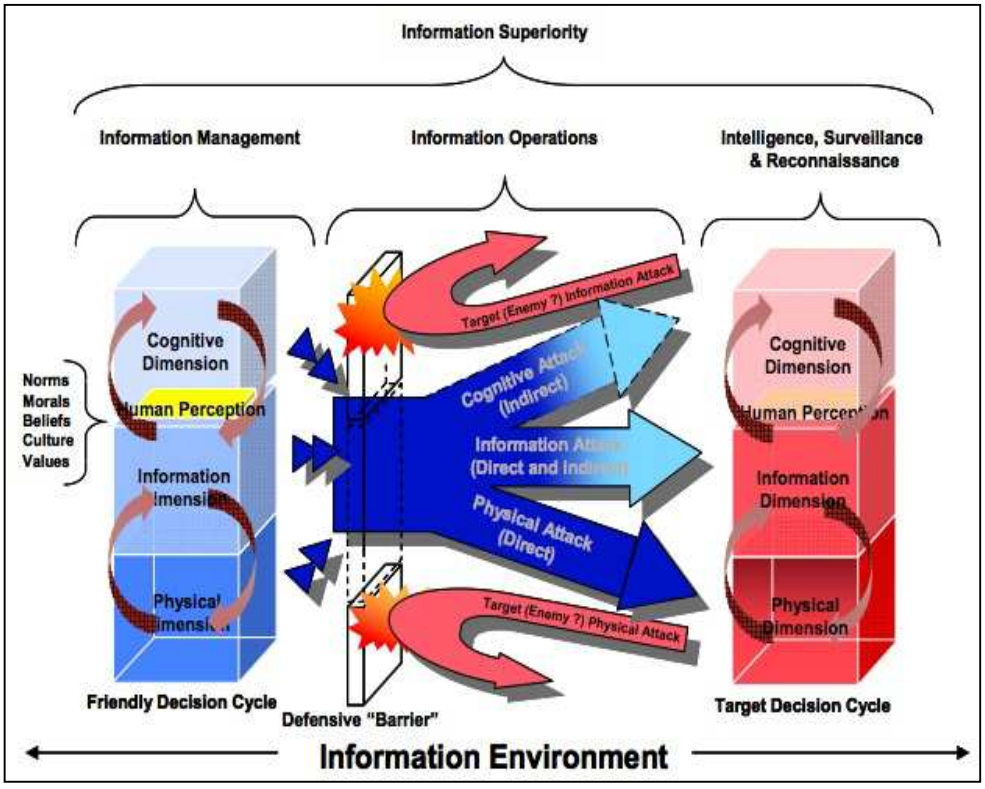
๗. Social Engineering

๘. Advanced Persistent Threats (APT)

แนวคิดการปฏิบัติการสงครามไซเบอร์

หลักนิยมด้านการปฏิบัติการข่าวสาร

แผนภาพที่ ๒-๓ แนวความคิดการปฏิบัติการข่าวสาร

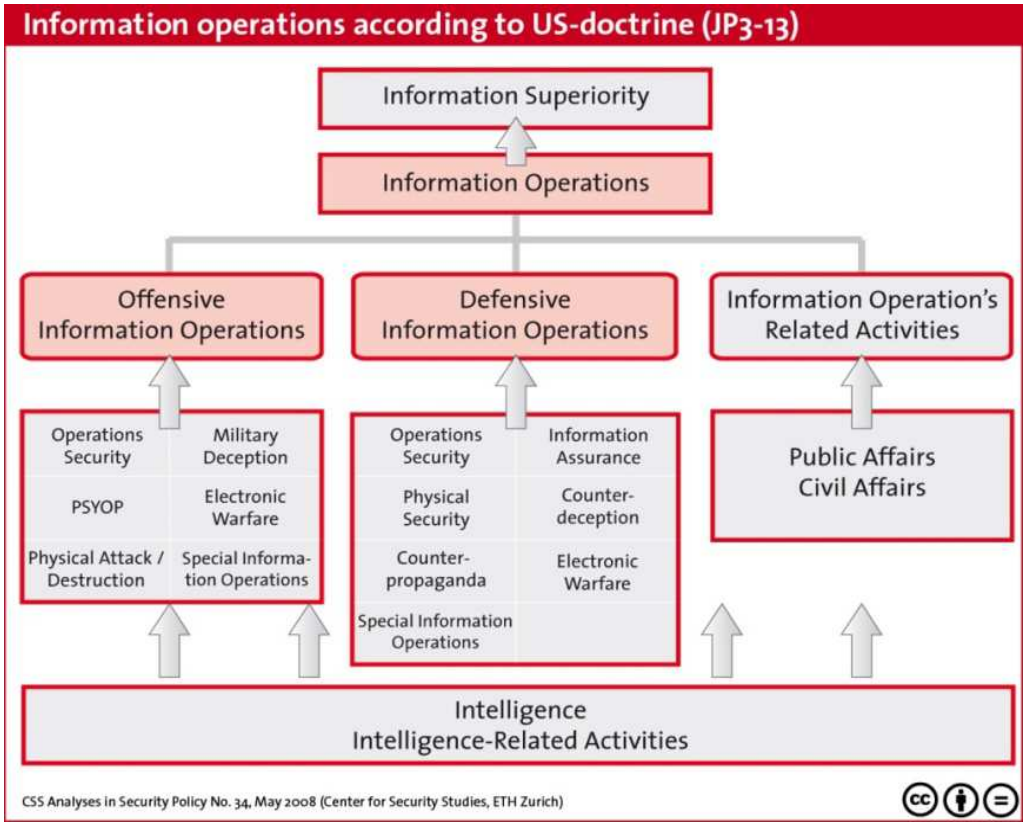


การปฏิบัติการข่าวสาร (Information Operations: IOs) เป็นหลักการที่ กห.สหรัฐฯ ได้ริเริ่มพัฒนาเมื่อปี พ.ศ.๒๕๔๖ (ค.ศ.๒๐๐๓) โดยเป็นการบูรณาการสงครามควบคุมบังคับบัญชา (Command and Control Warfare) และสงครามข้อมูลข่าวสาร (Information Warfare) เข้าด้วยกัน เนื่องจากสหรัฐฯ เห็นว่าความเหนือกว่าทางเทคโนโลยีหรือข่าวสารนั้น ยังไม่เพียงพอต่อการเอาชนะข้าศึกได้อย่างเบ็ดเสร็จ แต่ปัจจัยสำคัญในด้านความเชื่อและศรัทธา หรือจิตวิญญาณนั้น มีผลมากกว่า ซึ่งจะช่วยให้นำไปสู่ความสำเร็จตามปรัชญาของซุน วู ที่ว่าไว้คือ “ชนะโดยไม่ต้องรบ”

การปฏิบัติการข่าวสาร คือการบูรณาการการปฏิบัติทางทหารสาขาต่างๆ เข้าด้วยกัน ประกอบด้วยการปฏิบัติการทางยุทธการ การปฏิบัติการด้านมวลชน (Public Affairs) การปฏิบัติการจิตวิทยา (Psychological Operations) ร่วมกับการปฏิบัติการสารสนเทศ เช่นการโจมตีเครือข่ายคอมพิวเตอร์ (Computer Network Attack) เพื่อทำให้มีอิทธิพล ทำลาย ลดประสิทธิภาพ ต่อกระบวนการควบคุมบังคับบัญชา และการตกลงใจของฝ่ายตรงข้าม ทั้งที่กระทำโดยมนุษย์และระบบคอมพิวเตอร์ รวมทั้งดำเนินการป้องกันการกระทำของฝ่ายตรงข้ามต่อฝ่ายเราในลักษณะเดียวกัน ดังนั้น การปฏิบัติการข่าวสารจึงเป็นการปฏิบัติการทั้งเชิงรับและเชิงรุกทั้งในยามสงบ (Peace) ยามวิกฤต (Crisis) และยามสงคราม (Hostilities) และยังเกี่ยวข้องกับการปฏิบัติการ

ในทุกระดับ ตั้งแต่ระดับยุทธศาสตร์ ระดับยุทธการ ลงไปจนถึงระดับยุทธวิธี โดยสามารถแบ่งสาขาปฏิบัติการสำหรับการปฏิบัติการข่าวสารออกได้เป็น ๓ ส่วนดังนี้

แผนภาพที่ ๒-๔ องค์ประกอบขีดความสามารถที่ต้องการในการปฏิบัติการข่าวสาร



๑. **สาขาปฏิบัติการหลัก** ประกอบด้วยการปฏิบัติการ ๕ ปฏิบัติการ ได้แก่

๑.๑ การปฏิบัติการจิตวิทยา (Psychological Operations: PSYOP) คือการปฏิบัติเพื่อนำข้อมูล/ข่าวสารที่ได้เลือกไว้ให้แก่ผู้รับ โดยต้องการให้เกิดผลทางอารมณ์ การจูงใจ และความมีเหตุผล มีการใช้ในทุกระดับ ทั้งยุทธศาสตร์ ยุทธการ และยุทธวิธี ในระดับยุทธศาสตร์ อาจจะดำเนินการด้วยรูปแบบทางการเมืองหรือการทูต เช่น การประกาศหรือแถลงการณ์ ในระดับยุทธการ สามารถกระทำได้โดยการแจกใบปลิว การกระจายเสียงหรือสื่ออื่นๆ เช่น ระบบเครือข่าย ในระดับยุทธวิธี เช่น การกระจายเสียงเพื่อเพิ่มความหวาดกลัว เป็นต้น

๑.๒ การลวงทางทหาร (Military Deception: MILDEC) เป็นการปฏิบัติเพื่อให้ผู้มีหน้าที่ตัดสินใจของฝ่ายตรงข้ามมีความคิดที่ไม่ถูกต้อง เกี่ยวกับขีดความสามารถหรือความตั้งใจของฝ่ายเรา การปฏิบัติการลวงนี้ขึ้นกับการปฏิบัติการข่าว ในการกำหนดเป้าหมายการลวงที่เหมาะสมด้วย ทั้งนี้ เพื่อช่วยให้เรื่องที่สร้างขึ้นนั้นมีความน่าเชื่อถือมากขึ้น

๑.๓ การรักษาความปลอดภัยในการปฏิบัติการ (Operation Security; OPSEC) คือกระบวนการในการวางแผนและปฏิบัติ เพื่อให้ได้มาและดำรงรักษาไว้ซึ่งความลับที่สำคัญ เกี่ยวกับขีดความสามารถการปฏิบัติ และเจตนารมณ์ที่แท้จริงของฝ่ายเรา

๑.๔ การสงครามอิเล็กทรอนิกส์ (Electronic Warfare: EW) เป็นการปฏิบัติทางทหารที่เกี่ยวกับการใช้/การควบคุมคลื่นแม่เหล็กไฟฟ้า เริ่มตั้งแต่การกระทำเพื่อป้องกันระบบของฝ่ายเรา จนถึงการตอบโต้/โจมตีระบบของฝ่ายตรงข้าม การปฏิบัตินี้ไม่จำกัดเฉพาะคลื่นวิทยุหรือคลื่นเรดาร์เท่านั้น แต่ยังรวมถึงคลื่นอื่นๆ ด้วย เช่นอินฟาเรด เป็นต้น ซึ่งอาจนำมาใช้ทำงานเกี่ยวกับสงครามอิเล็กทรอนิกส์ด้วย

๑.๕ การปฏิบัติการเครือข่ายคอมพิวเตอร์ (Computer NetworkOperation: CNO) เป็นการปฏิบัติเพื่อทำลายหรือลดศักย์ของข้อมูล/ข่าวสาร ในเครือข่ายคอมพิวเตอร์ของฝ่ายตรงข้าม รวมทั้งป้องกันระบบของฝ่ายเราด้วย

๒. **สาขาการปฏิบัติการสนับสนุน** เป็นการปฏิบัติการที่ช่วยให้การปฏิบัติการหลักมีประสิทธิภาพมากยิ่งขึ้น ประกอบด้วยการปฏิบัติการ ๕ ปฏิบัติการ ได้แก่

๒.๑ การรักษาความปลอดภัยข่าวสาร (Information Assurance: IA) เป็นมาตรการที่ใช้เพื่อปกป้องและป้องกันข่าวสาร รวมทั้งระบบข่าวสาร โดยการทำให้เกิดความมั่นใจในการใช้ประโยชน์ได้ ความสมบูรณ์ การรับรองความลับเฉพาะ และไม่เกิดการปฏิเสธของข่าวสารและระบบข่าวสาร ซึ่งรวมถึงการเตรียมการสำหรับการฟื้นฟูระบบข่าวสาร

๒.๒ การรักษาความปลอดภัยทางกายภาพ (Physical Security) เป็นการรักษาความปลอดภัยในส่วนที่เกี่ยวข้องมาตรการด้านวัตถุที่กำหนดขึ้นเพื่อป้องกันมิให้มีการเข้าถึงยุทธภัณฑ์ สิ่งอำนวยความสะดวก วัสดุ และเอกสารต่างๆ โดยไม่ได้รับอนุมัติ และเพื่อป้องกันสิ่งเหล่านี้ให้รอดพ้นจากการจารกรรม การก่อวินาศกรรม การก่อความเสียหาย และการโจรกรรม

๒.๓ การโจมตีทางกายภาพ (Physical Attack) เป็นการโจมตีทางด้านวัตถุ กำลังพล สิ่งอำนวยความสะดวก หรือยุทโธปกรณ์ เพื่อลดหรือทำลายขีดความสามารถของฝ่ายตรงข้าม

๒.๔ การต่อต้านข่าวกรอง (Counter Intelligence: CI) เป็นการรวบรวมข่าวสาร และการดำเนินกิจกรรม เพื่อป้องกันการจารกรรม กิจกรรมข่าวกรองอื่นๆ การก่อวินาศกรรม หรือการลอบสังหารที่ดำเนินการโดยหรือในนามของรัฐบาล หรือหน่วยงานต่างประเทศ

๒.๕ การภาพการรบ (Combat Camera: COMCAM) เป็นเอกสารข่าวสารทางทัศนะที่ครอบคลุมทั่วทั้งประเทศ การปฏิบัติการทางอากาศ ทางทะเล และภาคพื้นดิน ของกองทัพ ในการปฏิบัติการรบและการสนับสนุนการรบ และในกิจกรรมการฝึกยามปกติที่เกี่ยวข้อง เช่น การฝึก การจำลองยุทธ์ และการปฏิบัติต่างๆ

๓. **สาขาการปฏิบัติการที่เกี่ยวข้อง** เป็นการปฏิบัติการตามภารกิจและหน้าที่ทางทหาร ซึ่งต้องปฏิบัติโดยประสานสอดคล้องกับการปฏิบัติการหลักและการปฏิบัติการสนับสนุนเสมอ เพื่อช่วยให้การปฏิบัติการข่าวสารสามารถบรรลุเป้าประสงค์ที่ตั้งไว้ ประกอบด้วยการปฏิบัติการ ๓ ปฏิบัติการ ได้แก่

๓.๑ การประชาสัมพันธ์ (Public Affairs: PA) เป็นกิจกรรมด้านประชาสนเทศ ข่าวสารของหน่วยบัญชาการ และชุมชนสัมพันธ์ ที่มุ่งกระทำต่อสาธารณชน ทั้งภายในและภายนอก ที่สนใจในกระทรวงกลาโหม

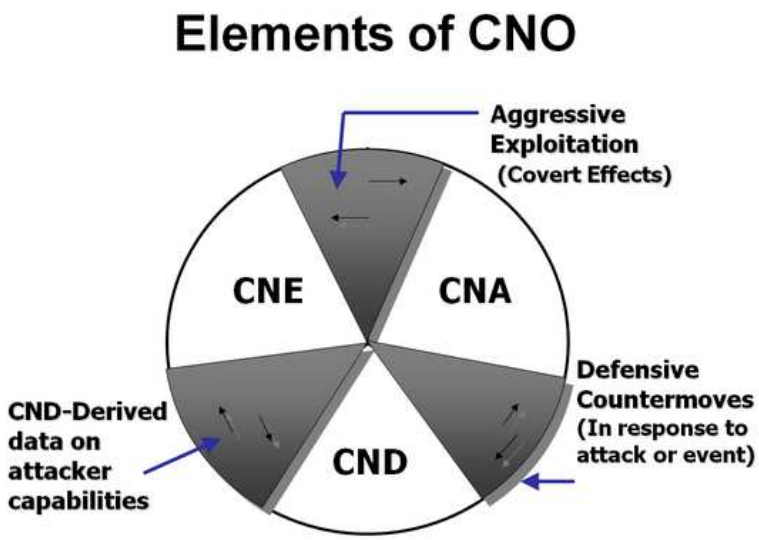
๓.๒ การกิจการพลเรือน (Civil-Military Operations: CMO) เป็นกิจกรรมที่ได้วางแผนไว้เพื่อสนับสนุนการปฏิบัติการทางทหาร ซึ่งสัมพันธ์กัน ระหว่างกำลังทหารกับเจ้าหน้าที่พลเรือน และกับประชาชน รวมทั้งเสริมสร้างความรู้สึก ทัศนคติ หรือพฤติกรรมที่ดี ต่อกลุ่มที่เป็นกลาง กลุ่มเดียวกัน หรือกลุ่มที่ไม่เป็นมิตร

๓.๓ การต่างประเทศฝ่ายทหาร (Defense Support to Public Diplomacy: DSPD) เป็นกิจกรรมและมาตรการที่ใช้โดยส่วนต่างๆ ภายในกระทรวงกลางโหม เพื่อสนับสนุน และอำนวยความสะดวกต่อความพยายามทางการทูตสาธารณะของรัฐบาล

แนวความคิดการปฏิบัติการเครือข่ายคอมพิวเตอร์

แนวความคิดด้านการปฏิบัติการสงครามสารสนเทศ เป็นแนวความคิดที่มองว่าข้อมูลข่าวสารเป็นทรัพยากรสำคัญต่อการทำงาน หรือปฏิบัติภารกิจ ยิ่งมีข้อมูลมากเท่าไหร่ ก็ยิ่งสามารถตัดสินใจ ทำงาน และปฏิบัติภารกิจได้ถูกต้องมากยิ่งขึ้น และในปัจจุบันข้อมูลข่าวสารต่างๆ ถูกปรับให้อยู่ในรูปแบบดิจิตอล จัดเก็บในระบบสารสนเทศ และสามารถเข้าถึงได้ผ่านอุปกรณ์ที่เชื่อมต่อกับเครือข่ายสารสนเทศ การปฏิบัติการสงครามสารสนเทศ จึงเป็นการกระทำเพื่อให้ได้มาซึ่งความเหนือกว่าของข้อมูลข่าวสาร และปฏิเสธการใช้ประโยชน์จากข้อมูลข่าวสารในรูปแบบดิจิตอลในระบบสารสนเทศของฝ่ายตรงข้าม

แผนภาพที่ ๒ - ๕ องค์ประกอบของขีดความสามารถด้านการปฏิบัติการเครือข่ายคอมพิวเตอร์



แนวความคิดด้านการปฏิบัติการสงครามสารสนเทศ ปัจจุบันได้รับความสำคัญในการปฏิบัติการทางทหาร ดังจะเห็นได้จากหลักการปฏิบัติการข่าวสาร (Information Operations) ซึ่งแนวความคิดด้านการปฏิบัติการสงครามสารสนเทศ ถูกกำหนดเป็นขีดความสามารถหลักที่จำเป็นต้องมี คือ ขีดความสามารถด้านการปฏิบัติการเครือข่ายคอมพิวเตอร์ (Computer Network Operations) รายละเอียดตามแผนภาพที่ ๒-๕

การดำเนินการปฏิบัติการสงครามสารสนเทศ ประกอบด้วยการดำเนินการ ๓ ส่วน ดังนี้

๑. การปฏิบัติการโจมตี เป็นการปฏิบัติการทางรุก โดยใช้เครือข่ายสารสนเทศ ในการ ขัดขวาง ปฏิเสธ ลิดรอน หรือ ทำลายข้อมูลข่าวสารที่ถูกเก็บอยู่ในระบบสารสนเทศ อุปกรณ์ที่เชื่อมต่อกับเครือข่ายสารสนเทศของฝ่ายตรงข้าม หรือตัวเครือข่ายสารสนเทศของฝ่ายตรงข้าม ซึ่งส่งผลให้ฝ่ายตรงข้ามไม่สามารถใช้ประโยชน์จากข้อมูลข่าวสาร ระบบสารสนเทศ และเครือข่ายสารสนเทศในการปฏิบัติภารกิจ และอาจส่งผลกระทบต่อภารกิจของฝ่ายตรงข้ามในที่สุด

๒. การปฏิบัติการป้องกัน เป็นการปฏิบัติการทางรับ โดยการป้องกัน ดำรงรักษาขีดความสามารถในการใช้ประโยชน์จากข้อมูลข่าวสารที่ถูกเก็บอยู่ในระบบสารสนเทศ อุปกรณ์ที่เชื่อมต่อกับเครือข่ายสารสนเทศของฝ่ายเรา จากการปฏิบัติการโจมตีของฝ่ายตรงข้าม การดำเนินการป้องกันประกอบด้วยขั้นตอนการ ตรวจสอบ วิเคราะห์ และตรวจจับการบุกรุกโจมตี หรือการเข้าถึงข้อมูลข่าวสาร หรือระบบสารสนเทศโดยไม่ได้รับอนุญาต

๓. การปฏิบัติการใช้ประโยชน์จากข้อมูลและระบบสารสนเทศ เป็นการปฏิบัติการที่สร้างขีดความสามารถในการหาข่าว หรือข้อมูลที่เกี่ยวข้องกับ ระบบสารสนเทศ หรือเครือข่ายสารสนเทศของฝ่ายตรงข้าม เพื่อใช้ประโยชน์ในการโจมตีในอนาคต ตัวอย่างของการดำเนินการเช่น การเจาะระบบเพื่อฝังตัวและคอยเก็บรวมข้อมูล การใช้งาน การติดต่อสื่อสาร เป็นต้น

นโยบาย หลักการ และ กฎหมายที่เกี่ยวข้องกับสงครามไซเบอร์ของประเทศไทย

ในส่วนนี้จะกล่าวถึง นโยบาย หลักการ แนวทาง และกฎหมาย ที่จำเป็นต้องมีการพิจารณาในการกำหนดแนวทางการพัฒนาขีดความสามารถด้านการปฏิบัติการสงครามสารสนเทศของประเทศไทย

๑. นโยบายรัฐบาล

นโยบายของรัฐบาล ซึ่งนางสาวยิ่งลักษณ์ ชินวัตร นายกรัฐมนตรี ได้แถลงต่อรัฐสภา เมื่อวันที่ ๒๓ ส.ค.๕๔ ในส่วนของความมั่นคงแห่งรัฐมีส่วนที่เกี่ยวข้องกับการปฏิบัติการสงครามสารสนเทศ ดังนี้

๑.๑ พัฒนาและเสริมสร้างศักยภาพของกองทัพและระบบป้องกันประเทศ ให้มีความพร้อมในการพิทักษ์รักษาเอกราช อธิปไตย ความมั่นคง และผลประโยชน์แห่งชาติ สนับสนุนให้กองทัพมีโครงสร้างที่เหมาะสมและมีความทันสมัยส่งเสริมกิจการอุตสาหกรรมป้องกันประเทศให้สามารถบูรณาการขีดความสามารถของภาครัฐและเอกชนให้เป็นเอกภาพ นำไปสู่การพึ่งพาตนเองได้ในการผลิตอาวุธยุทโธปกรณ์ได้เองสนับสนุนสิทธิและหน้าที่กำลังพลของกองทัพเพื่อให้เป็นทหารอาชีพในระบอบประชาธิปไตย และสามารถผนึกกำลังกับประชาชนให้มีส่วนร่วมในการรักษาความมั่นคงของประเทศ รวมทั้งกำหนดเป็นบทบาทของทหารในการช่วยเหลือประชาชน โดยเฉพาะอย่างยิ่งกรณีเกิดภัยพิบัติร้ายแรง ขณะเดียวกันจะปรับปรุงสวัสดิการของกำลังพลทุกระดับให้มีมาตรฐานการดำรงชีวิตที่ดียิ่งขึ้น

๑.๒ พัฒนาระบบการเตรียมพร้อมแห่งชาติ โดยเน้นการบริหารวิกฤตการณ์เพื่อรับมือภัยคุกคามด้านต่างๆ ทั้งที่เกิดจากภัยธรรมชาติและภัยที่มนุษย์สร้างขึ้นที่มากขึ้น โดยมุ่งระดมสรรพกำลังจากทุกภาคส่วนให้สามารถดำเนินงานร่วมกันอย่างมีประสิทธิภาพ เพื่อป้องกัน แก้ไข บรรเทา และฟื้นฟูความเสียหายของชาติที่เกิดจากภัยต่าง ๆ รวมถึงให้ความสำคัญในการเตรียมพร้อมเพื่อเผชิญกับปัญหาความมั่นคงในรูปแบบใหม่ในทุกด้าน ได้แก่ ด้านพลังงาน ด้านสิ่งแวดล้อม ความมั่นคงของมนุษย์อาชญากรรมข้ามชาติ การก่อการร้าย และอุบัติภัย ทั้งนี้ เพื่อให้มีความพร้อมรับมือกับความเปลี่ยนแปลงของประเด็นปัญหาด้านความมั่นคงในยุคโลกาภิวัตน์

๒. นโยบายความมั่นคงแห่งชาติ

ตามการวิเคราะห์สภาพแวดล้อมด้านความมั่นคงในนโยบายความมั่นคงแห่งชาติ พ.ศ.๒๕๕๐ – ๒๕๕๔ พบว่าปัจจุบัน ปัญหาด้านความมั่นคงมีแนวโน้มเปลี่ยนแปลงไปจากภัยในรูปแบบเดิม ซึ่งส่วนใหญ่หมายถึงความขัดแย้งระหว่างรัฐ เปลี่ยนแปลงเป็นภัยต่อความมั่นคงรูปแบบใหม่ ทั้งการก่อการร้ายสากล อาชญากรรมข้ามชาติ ซึ่งระบบสารสนเทศเข้ามามีบทบาทสำคัญต่อภัยคุกคามด้านความมั่นคงทั้งหมด ทั้งในด้านการถูกนำมาใช้ประโยชน์ในการกระทำการ และการตกเป็นเป้าหมายการโจมตีจากภัยคุกคามดังกล่าว ซึ่งในปัจจุบันสภาพสังคม โครงสร้างเศรษฐกิจ การดำเนินงานของหน่วยงานราชการ ล้วนแล้วแต่พึ่งพาการใช้งานระบบสารสนเทศ ในการเพิ่มประสิทธิภาพการทำงาน การเพิ่มความรวดเร็วในการติดต่อสื่อสาร การเพิ่มความถูกต้องและรวดเร็วในกระบวนการตัดสินใจ ส่งผลให้ระบบสารสนเทศเหล่านี้มีความสำคัญ และมีความเสี่ยงต่อกระบวนการทำงานหากไม่สามารถใช้งานได้ ส่งผลให้มีความจำเป็นต้องเตรียมความพร้อมแห่งชาติ เพื่อรองรับภัยคุกคามดังกล่าว เพื่อรักษาไว้ซึ่งการต่อเนื่องในการดำเนินการของหน่วยงานที่เกี่ยวข้อง อันจะส่งผลความสำเร็จในการรักษาผลประโยชน์แห่งชาติ โดยนโยบายความมั่นคงแห่งชาติในส่วนที่เกี่ยวข้องกับการปฏิบัติการสงครามไซเบอร์ ดังนี้

๒.๑ การเสริมสร้างและพัฒนาศักยภาพการป้องกันประเทศ โดยสนับสนุนให้กองทัพมีระบบอาวุธและระบบการแจ้งเตือนภัยทางทหาร และการพัฒนาศักยภาพของชาติในการป้องกันประเทศ เพื่อเตรียมรับสถานการณ์ที่ไม่แน่นอน ด้วยการส่งเสริมการวิจัยและพัฒนาอุตสาหกรรมป้องกันประเทศ การมีส่วนน่วมระหว่างกองทัพกับหน่วยงานวิจัยของภาครัฐ องค์กร สถาบันวิจัย และสถาบันการศึกษาด้านเทคโนโลยีของภาครัฐและเอกชน ทั้งในประเทศและต่างประเทศ พร้อมทั้งจัดงบประมาณสนับสนุนการพัฒนาอย่างเพียงพอและต่อเนื่อง รวมทั้งมีกรอบยุทธศาสตร์การพัฒนาที่ชัดเจน

๒.๒ การพัฒนาศักยภาพของชาติในการป้องกันประเทศ ด้วยการผนึกกำลังจากทุกฝ่าย ทั้งภาครัฐ ภาคเอกชน และภาคประชาชน เข้าด้วยกันอย่างเป็นระบบในการรักษาความสงบเรียบร้อยและความมั่นคงของชาติ

๒.๓ การพัฒนาความร่วมมือทางทหารและความเข้าใจอันดีกับกองทัพของประเทศเพื่อนบ้านและกลุ่มอาเซียนรวมทั้งมิตรประเทศอื่นๆ ในทุกระดับในการรักษาผลประโยชน์ร่วมกัน โดยสอดคล้องกับนโยบายต่างประเทศ รวมทั้งสนับสนุนภารกิจในการรักษาสันติภาพของโลกภายใต้กรอบของสหประชาชาติ ตลอดจนมีส่วนร่วมบรรเทาภัยพิบัติทางธรรมชาติในภูมิภาค

๒.๔ ปรับปรุง พัฒนานโยบาย และแผนรองรับให้สอดรับกับภัยด้านสาธารณภัยและภัยด้านความมั่นคงที่เปลี่ยนแปลงไป เพื่อเพิ่มขีดความสามารถในการป้องกันภัย ระงับภัย บรรเทาภัย และฟื้นฟูภายหลังจากการเกิดภัย รวมทั้งให้มีแผนปฏิบัติการ มาตรการ ในการเตรียมพร้อมของหน่วยงาน

โดยประสานและเชื่อมโยงระหว่างหน่วยงานพลเรือน ทหาร และภาคประชาชน ในการบริหารจัดการภัยได้อย่างมีประสิทธิภาพและทันเวลา โดยเน้นการเข้าถึงพื้นที่เป้าหมายได้อย่างทันท่วงที

๒.๕ เสริมสร้างความรู้ ความเข้าใจ และทักษะของเจ้าหน้าที่ปฏิบัติงาน ภาคประชาชน และองค์กรเครือข่ายต่างๆ โดยเฉพาะในพื้นที่ที่มีความเสี่ยงข้องภัย โดยให้มีการฝึกซ้อมแผนเป็นระยะตามเหมาะสม

๒.๖ ให้มีระบบการบริหารจัดการภัยอย่างมีเอกภาพ ประสิทธิภาพ และทันเหตุการณ์ โดยกำหนดหน่วยงานและผู้รับผิดชอบ เพื่อเสริมสร้างการบัญชาการเหตุการณ์ที่ชัดเจน

๒.๗ ส่งเสริมและประสานความร่วมมือกับต่างประเทศ เพื่อส่งเสริมประสิทธิภาพของประเทศในการบริหารจัดการภัย รวมทั้งสนับสนุนให้หน่วยงานที่เกี่ยวข้องต่างปฏิบัติภารกิจช่วยเหลือแก่ประเทศต่างๆ ที่ได้รับผลกระทบจากภัยพิบัติ อันจะเป็นการแลกเปลี่ยนประสบการณ์และความรู้ และการมีส่วนร่วมในการแก้ไขปัญหาของประชาคมโลก

๒.๘ เตรียมความพร้อมระยะยาวให้กับสังคมไทย ได้ตระหนักและตื่นตัวในการรับรู้และเรียนรู้ถึงธรรมชาติของการก่อการร้าย รวมทั้งรู้เท่าทันการเคลื่อนสังคม และความมั่นคงของประเทศ โดยสนับสนุนการเผยแพร่ข้อมูล และการมีส่วนร่วมของประชาชนในเรื่องการระวังป้องกันการก่อการร้ายอย่างเหมาะสมในทุกภาคส่วน

๓. นโยบายการเปลี่ยนแปลงไปสู่การเป็นรัฐบาลอิเล็กทรอนิกส์ (Smart Government)

เป็นส่วนหนึ่งของยุทธศาสตร์ Smart Thailand ซึ่งเป็นยุทธศาสตร์ที่ต้องการเชื่อมโยงการทำงานของทุกภาคส่วนเข้าด้วยกัน โดยเน้น ๔ กลยุทธ์หลัก ได้แก่ ๑. การเพิ่มขีดความสามารถในการแข่งขันของประเทศ ๒. การลดความเหลื่อมล้ำ ๓. การส่งเสริมการเติมโตที่เป็นมิตรต่อสิ่งแวดล้อม และ ๔. การสร้างสมดุลและปรับระบบบริหารจัดการภายในภาครัฐ โดยเน้นการบริหารจัดการ ทั้งระบบ กำลังคน และงบประมาณ นโยบาย Smart Government เป็นการดำเนินการให้เกิดการพัฒนาโครงสร้างพื้นฐานให้ครอบคลุมพื้นที่ทั่วประเทศ และการพัฒนาบริการภาครัฐฝ่ายระบบเทคโนโลยีสารสนเทศ เพื่อสร้างโอกาสให้กับประชาชนสามารถเข้าถึงบริการได้อย่างทั่วถึงและเท่าเทียม โดยการพัฒนาเครือข่ายอินเทอร์เน็ตความเร็วสูงของประชาชนในเขตเมืองและชนบท และการพัฒนาและปรับปรุงเครือข่ายข้อมูลภาครัฐ Government Information Network: GIN ให้มีประสิทธิภาพ มีการบูรณาการข้อมูลภาครัฐโดยมีการวางโครงของข้อมูลเพื่อเอื้อต่อการเชื่อมโยงทุกรูปแบบ และต่อยอดสร้างเครือข่ายเป็น Super GIN และ Smart Cloud ต่อไปซึ่งเป็นการสร้างโครงสร้างพื้นฐานด้านระบบสารสนเทศ ให้หน่วยงานภาครัฐสามารถใช้ประโยชน์ร่วมกัน รวมทั้งการกำหนดมาตรฐานด้านการรักษาความปลอดภัย พร้อมทั้งจัดหาอุปกรณ์ในการตรวจสอบเฝ้าระวังด้านความปลอดภัย ที่จะช่วยให้ระบบอิเล็กทรอนิกส์ของไทยมีความมั่นคงปลอดภัยมากยิ่งขึ้น

๔. นโยบายความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ

จากการศึกษาแนวโน้มด้านความมั่นคงปลอดภัยไซเบอร์และการประเมินความพร้อมด้านต่างๆ ที่มีส่วนสำคัญต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย เมื่อประกอบเข้ากับการศึกษาบริบทด้านแนวทางการพัฒนาประเทศไทยจากแผนระดับชาติที่เกี่ยวข้อง สามารถกำหนดเป้าหมายและยุทธศาสตร์ การรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย ได้ดังนี้

๔.๑ เป้าหมายหลัก

๔.๑.๑ สังคมมีวัฒนธรรมการตระหนักถึงความเสี่ยง (Risk-Aware Culture) จากการใช้งานบนโลกไซเบอร์ และประชาชนมีความรู้และทักษะในการใช้ประโยชน์จากโลกไซเบอร์ได้อย่างมั่นคงปลอดภัย

๔.๑.๒ มีการกำกับดูแลการใช้งานบนโลกไซเบอร์ให้มีความมั่นคงปลอดภัย โดยคำนึงถึงสิทธิเสรีภาพของประชาชน

๔.๑.๓ มีขีดความสามารถในการตอบสนองภัยคุกคามทางไซเบอร์ในทุกรูปแบบอย่างมีประสิทธิภาพ (คน กระบวนการ เครื่องมือ) เพื่อรักษาเสถียรภาพทางเศรษฐกิจ ความมั่นคงแห่งชาติ และคุณภาพชีวิตของประชาชน

๔.๑.๔ มีความคุ้มครองข้อมูลส่วนบุคคล (Privacy) และข้อมูลแสดงตัวตน (Identity) และมีการรักษาความมั่นคงปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ในทุกภาคส่วน

๔.๑.๕ มีความร่วมมือทั้งระหว่างองค์กรภายในประเทศ และองค์กรระหว่างประเทศเพื่อเสริมศักยภาพการรักษาความมั่นคงปลอดภัยไซเบอร์ ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์

๔.๒ ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์

จากการวิเคราะห์จุดแข็ง - จุดอ่อน และโอกาส - ภัยคุกคาม (SWOT Analysis) ด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย พบว่าประเทศไทยมีจุดอ่อนที่ควรแก้ไขและภัยคุกคามที่ควรป้องกันโดยเร่งด่วน จึงสามารถกำหนดยุทธศาสตร์แบบเชิงรับ เพื่อมุ่งเน้นปัจจัยสำคัญที่จะช่วยลดหรือขจัดจุดอ่อน โดยมียุทธศาสตร์ ๘ ด้าน ดังนี้

๔.๒.๑ ยุทธศาสตร์ที่ ๑ การบูรณาการการจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศ (Cybersecurity Management Integration) โดยการวางโครงสร้างบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศที่มีความชัดเจนในบทบาทหน้าที่ ดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และประสานงานกับผู้ที่รับผิดชอบงานด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของหน่วยงานอื่นๆ การดำเนินการเรื่องตรวจสอบและประเมินผล การประเมินความเสี่ยงของระบบสารสนเทศในระดับประเทศ การพัฒนาบุคลากร การวิจัยและพัฒนา และการเตรียมความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยมีกลไกลประสานเชื่อมโยงกับคณะกรรมการนโยบายระดับชาติที่เกี่ยวข้องโดยมีเป้าหมายดังนี้

๔.๒.๑.๑ มีหน่วยงานกลาง (National Cybersecurity Organization) ที่เป็นหลักในการรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยมีบทบาทในการประสานความร่วมมือในการส่งเสริม สนับสนุน มีอำนาจสั่งการ ลงโทษ (ตามกลไกการดำเนินงานของรัฐ) รองรับ กำกับ

ตรวจสอบ ประเมิน มีความสามารถในการพัฒนา วิจัย และเตรียมความพร้อม ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งอาจเป็นหน่วยงานที่จัดตั้งขึ้นมาใหม่ เป็นหน่วยงานที่มีอยู่แล้ว หรือเป็นความร่วมมือที่เป็นลายลักษณ์อักษร และเป็นรูปธรรม

๔.๒.๑.๒ มีโครงสร้างการบริหารการรักษาความมั่นคงปลอดภัยระดับชาติ พร้อมบทบาทหน้าที่ที่ชัดเจน ของบุคคลหรือหน่วยงานที่เกี่ยวข้อง และขั้นตอนการดำเนินงาน พร้อมแผนการดำเนินงานและงบประมาณที่สอดคล้องกับเป้าหมายของกรอบนโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ที่เป็นที่ยอมรับของหน่วยงานที่เกี่ยวข้อง

๔.๒.๑.๓ ส่งเสริมให้มีการรักษาความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศ (Information Asset) ทั้งระดับองค์กร และระดับประเทศ โดยใช้กลไกการจัดชั้นความลับเป็นหลักในการจำแนกประเภทของทรัพย์สินสารสนเทศแล้วจึงกำหนดแนวทางการบริหารจัดการทรัพย์สินสารสนเทศแต่ละประเภทตามระดับความเสี่ยง (Information Classification and Security Clearance)

๔.๒.๑.๔ การให้บริการของภาครัฐและหน่วยงานที่เป็นโครงสร้างพื้นฐานสำคัญที่เทคโนโลยีของการให้บริการมีผลสำคัญต่อความมั่นคงปลอดภัยของสารสนเทศหรือระบบสารสนเทศ ให้ปฏิบัติตามหลัก CIA เช่นการบริการ Outsource/Cloud

๔.๒.๒ ยุทธศาสตร์ที่ ๒ การสร้างศักยภาพในการตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Emergency Readiness) สร้างความพร้อมเชิงรับและเชิงรุกในการรับมือภัยคุกคามโดยมีเป้าหมายดังนี้

๔.๒.๒.๑ ประเทศไทยมีเครื่องมือ บุคลากร และสถานที่ พร้อมใช้งานสำหรับการเฝ้าระวังและรับมือภัยคุกคามด้านไซเบอร์ ทั้งที่มาจากภายในประเทศและภายนอกประเทศ โดยทำงานได้ทั้งเชิงรับ และเชิงรุก และสามารถจำกัดความเสียหายจากการโจมตีบนไซเบอร์ได้ทันเวลาโดยไม่กระทบต่อเสถียรภาพทางเศรษฐกิจและความมั่นคงของประเทศ

๔.๒.๒.๒ ให้มีหน่วยงานที่ดำเนินการเป็นศูนย์บัญชาการสำหรับผู้บริหารประเทศ ซึ่งมีการดำเนินการทั้งด้านการทหารและพลเรือน

๔.๒.๓ ยุทธศาสตร์ที่ ๓ การปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (National Critical Information Infrastructure Protection) ปกป้องโครงสร้างพื้นฐานสำคัญของประเทศและระบบสารสนเทศที่เกี่ยวข้อง ให้สามารถดำเนินการได้อย่างต่อเนื่องโดยมีเป้าหมายดังนี้

๔.๒.๓.๑ มีการกำหนดหลักเกณฑ์การเป็นโครงสร้างพ้นฐานสำคัญของประเทศและรณรงค์ให้หน่วยงานหรือองค์กรที่เป็นโครงสร้างพื้นฐานสำคัญของประเทศตระหนักรู้ถึงความสำคัญและความเสี่ยงของตนเอง

๔.๒.๓.๒ ส่งเสริมให้หน่วยงานหรือองค์กรที่เป็นโครงสร้างพื้นฐานสำคัญแต่ละกลุ่มอุตสาหกรรมร่วมกันจัดทำนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ โดยคำนึงถึงความสอดคล้องกับกฎหมาย/กฎระเบียบ/พันธะกรณีระหว่างประเทศ/มาตรฐานสากล ที่เกี่ยวข้องของกลุ่มอุตสาหกรรมนั้นๆ

๔.๒.๓.๓ ส่งเสริมให้หน่วยงานหรือองค์กรที่เป็นโครงสร้างพื้นฐานสำคัญมีการวิเคราะห์ความเสี่ยง มีการจัดทำแผนบริหารจัดการความเสี่ยง และมีการดำเนินการจัดการความเสี่ยงที่เกี่ยวกับภัยคุกคามไซเบอร์รวมทั้งมีการทำ BCM (Business Continuity Management)

๔.๒.๓.๔ มีการตรวจสอบและประเมินระดับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของโครงสร้างพื้นฐานสำคัญของประเทศตามเงื่อนไขของกฎหมาย (มาตรา ๖ ในพระราชกฤษฎีกา ว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๕๓)

๔.๒.๓.๕ หน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ จะต้องบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศอันเป็นที่น่าเชื่อถือและยอมรับได้ในระดับสากลและมาตรฐานเฉพาะอุตสาหกรรม

๔.๒.๔ ยุทธศาสตร์ที่ ๔ การประสานความร่วมมือระหว่างภาครัฐและเอกชนเพื่อความมั่นคงปลอดภัยไซเบอร์ (Public-Private Partnership) ทำงานร่วมกันระหว่างภาครัฐและเอกชนในการสร้างขีดความสามารถในการตอบสนองภัยคุกคามทางไซเบอร์ในทุกรูปแบบได้อย่างมีประสิทธิภาพ (คน กระบวนการ เครื่องมือ) เพื่อรักษาเสถียรภาพทางเศรษฐกิจ ความมั่นคงแห่งชาติ และคุณภาพชีวิตของประชาชนโดยมีเป้าหมายดังนี้

๔.๒.๔.๑ มีความร่วมมือแบบ PPP เพื่อส่งเสริมให้ผู้พัฒนาผลิตภัณฑ์/บริการ มีความรู้ ทักษะ และความตระหนักในการพัฒนาผลิตภัณฑ์และบริการอย่างมั่งคงปลอดภัย

๔.๒.๔.๒ ส่งเสริมให้ทุกภาคส่วนทั้งภาครัฐ เอกชน และประชาชนใช้ซอฟท์แวร์อย่างถูกต้องตามกฎหมาย เพื่อจะได้รับการแก้ไขปัญหาด้านความปลอดภัยจากผู้ผลิตอย่างสม่ำเสมอ

๔.๒.๔.๓ มีความร่วมมือด้านการแลกเปลี่ยนข้อมูลภัยคุกคามด้านไซเบอร์เพื่อนำไปใช้ในการรักษาความมั่นคงปลอดภัยไซเบอร์

๔.๒.๔.๔ มีนโยบายการบ่มเพาะและสนับสนุนผู้ประกอบการด้าน Cybersecurity ให้มีความพร้อมสู่การให้ความร่วมมือในรูปแบบ PPP ได้อย่างยั่งยืน

๔.๒.๔.๕ มีความร่วมมือในด้านการยืมตัวบุคลากรระหว่างหน่วยงาน

๔.๒.๔.๖ ให้มีกลไกหรือมาตรการ เพื่อกระตุ้นให้เกิดความร่วมมือระหว่างภาครัฐและเอกชน เช่นมาตรการทางภาษี หรือการให้ทุน

๔.๒.๕ ยุทธศาสตร์ที่ ๕ การสร้างความตระหนักและรอบรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Capacity and Capability Building) พัฒนาบุคลากรในบทบาทต่างๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ (ประชาชน ผู้เชี่ยวชาญเฉพาะทาง และผู้รักษากฎหมาย) และสร้างวัฒนธรรมการรักษาความมั่นคงปลอดภัยไซเบอร์โดยมีเป้าหมายดังนี้

๔.๒.๕.๑ จัดทำมาตรฐานวิชาชีพเพื่อยกระดับความรู้ความสามารถของบุคลากรในสายวิชาชีพความมั่นคงปลอดภัยสารสนเทศ ให้อยู่ในระดับสากล และสร้างเส้นทางความก้าวหน้าในสายอาชีพ พร้อมค่าตอบแทนที่เหมาะสมกับระดับความรู้ความสามารถ

๔.๒.๕.๒ พัฒนากระบวนการรับรองและการกำกับดูแลมาตรฐานวิชาชีพภายในประเทศ เพื่อลดค่าใช้จ่าย พร้อมสร้างความยอมรับการรับรองมาตรฐานดังกล่าว

๔.๒.๕.๓ พัฒนาบุคลากรของหน่วยงานภาครัฐให้มีจำนวนที่เพียงพอและยกระดับความรู้ความสามารถของบุคลากรให้มีความรู้ ความเข้าใจเกี่ยวกับภัยคุกคามไซเบอร์ และสามารถปฏิบัติงานโดยรักษาความมั่นคงปลอดภัยไซเบอร์ได้ตามกฎหมาย

๔.๒.๕.๔ ส่งเสริมและพัฒนาให้บุคลากรในกระบวนการยุติธรรม เช่น ตำรวจ พนักงานเจ้าหน้าที่ อัยการ ผู้พิพากษา ราชทัณฑ์ เจ้าหน้าที่ตรวจพิสูจน์พยานหลักฐาน ผู้เชี่ยวชาญ มีความรู้ความเข้าใจเกี่ยวกับภัยคุกคามไซเบอร์ ในการบังคับใช้กฎหมายที่เกี่ยวข้องอย่างต่อเนื่อง

๔.๒.๕.๕ ให้ความรู้อย่างต่อเนื่องและให้องค์ความรู้ที่เข้าถึงได้แก่ประชาชน เพื่อให้มีความตระหนักในความเสี่ยงต่างๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

๔.๒.๕.๖ เพิ่มหลักสูตรการศึกษาตั้งแต่ระดับประถมจนถึงระดับอุดมศึกษา รวมทั้งพัฒนาครูผู้สอน ให้มีความเข้าใจเกี่ยวกับภัยคุกคามไซเบอร์และวิธีการป้องกัน เพื่อให้สามารถนำไปปลูกจิตสำนึกด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิผล ตลอดจนนำไปประยุกต์ใช้กับการใช้งานบนโลกไซเบอร์ได้

๔.๒.๕.๗ ให้มีหน่วยงานที่รับผิดชอบด้านการพัฒนาบุคลากรในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๔.๒.๖ ยุทธศาสตร์ที่ ๖ การพัฒนาระเบียบและกฎหมายเพื่อความมั่นคงปลอดภัยไซเบอร์ (Legal Measures) ปรับปรุงกฎหมายให้ทันสมัย บังคับใช้ได้ มีแนวทางปฏิบัติตามกฎหมายที่ชัดเจนและสอดคล้องกับหลักกฎหมาย/แนวปฏิบัติสากลโดยมีเป้าหมายดังนี้

๔.๒.๖.๑ มีการปรับปรุง/จัดทำกฎหมายเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ เช่นกฎหมายที่เกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ กฎหมายเกี่ยวกับผู้กระทำความผิดทางคอมพิวเตอร์ต่างแดน กฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล ให้สอดคล้องกับหลักสากล มีบทลงโทษ และบังคับใช้ได้

๔.๒.๖.๒ จัดทำกฎหมายลำดับรอง เพื่อให้สามารถบังคับการใช้ให้เป็นไปตามกฎหมายได้

๔.๒.๗ ยุทธศาสตร์ที่ ๗ การวิจัยและพัฒนาเพื่อความมั่นคงปลอดภัยไซเบอร์ (Research and Development) มีกลไกสร้างความเป็นเลิศด้านการวิจัย และพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์เพื่อให้ประเทศพึ่งพาตัวเองได้อย่างยั่งยืนโดยมีเป้าหมายดังนี้

๔.๒.๗.๑ มีหน่วยงานที่มีหน้าที่หลักโดยเฉพาะในการวิจัยและพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์ (National ICT Academy)

๔.๒.๗.๒ มีแผนงานวิจัยและพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์พร้อมแผนด้านงบประมาณ

๔.๒.๗.๓ มีเครือข่ายความร่วมมือในการวิจัยและพัฒนากับหน่วยงานอื่นทั้งภาครัฐ เอกชน สถาบันการศึกษา สถาบันวิจัย ทั้งในและต่างประเทศ

๔.๒.๗.๔ จัดทำหลักเกณฑ์มาตรฐานต่างๆ สำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อช่วยให้การบริหารจัดการความมั่นคงปลอดภัยไซเบอร์เป็นไปในทิศทางเดียวกับภายใต้หลักเกณฑ์ของรัฐ

๔.๒.๘ ยุทธศาสตร์ที่ ๘ การประสานความร่วมมือระหว่างประเทศ เพื่อความมั่นคงปลอดภัยไซเบอร์ (International Cooperation) เป็นพันธมิตรที่น่าเชื่อถือในเครือข่ายการรักษาความมั่นคงปลอดภัยไซเบอร์ระหว่างประเทศโดยมีเป้าหมายดังนี้

๔.๒.๘.๑ มีเครือข่ายความร่วมมือระหว่างประเทศ สามารถแลกเปลี่ยนข้อมูลข่าวสาร และปฏิบัติการร่วมกันในการเฝ้าระวังและรับมือภัยคุกคามไซเบอร์

๔.๒.๘.๒ มีการพัฒนาขีดความสามารถที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยการแลกเปลี่ยนบุคลากรในการร่วมปฏิบัติงาน หรือการวิจัยและพัฒนา และโดยการอบรม ฝึกงาน และดูงาน

๕. กฎหมายและระเบียบที่เกี่ยวข้อง

๕.๑ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ เป็นกฎหมายที่ถูกตราขึ้นเพราะในปัจจุบันระบบคอมพิวเตอร์ได้เป็นส่วนสำคัญของการประกอบกิจการและการดำรงชีวิตของมนุษย์ หากมีผู้กระทำด้วยประการใดๆ ให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใดๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ หรือใช้ระบบคอมพิวเตอร์เพื่อเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือมีลักษณะอันลามกอนาจาร ย่อมก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน สมควรกำหนดมาตรการเพื่อป้องกันและปราบปรามการกระทำดังกล่าว เช่นการเก็บข้อมูลการจราจรทางอินเทอร์เน็ต (Traffic Log)

ซึ่งใช้เป็นหลักฐานหรือข้อมูลในการตรวจจับการกระทำความผิด และการกำหนดบทลงโทษผู้กระทำความผิดตามที่กำหนดไว้ใน พ.ร.บ. นี้

๕.๒ พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๔๔ เป็นกฎหมายที่ตราขึ้นเพื่อรองรับการนำระบบเทคโนโลยีสารสนเทศเข้ามาใช้ในการดำเนินกิจกรรมในทางแพ่งและพาณิชย์ รวมถึงการดำเนินงานของรัฐที่ใช้วิธีการทางอิเล็กทรอนิกส์ และอาจมีลักษณะเฉพาะที่ต่างไปจากระบบกระดาษ โดยเป็นกฎหมายที่ตราขึ้นเสริมหรือใช้ประกอบกับกฎหมายทุกฉบับที่ใช้บังคับอยู่ในปัจจุบัน เพื่อรองรับนิติสัมพันธ์ที่เกิดขึ้นในรูปของข้อมูลอิเล็กทรอนิกส์ โดยกฎหมายฉบับนี้ตราอยู่บนหลักการพื้นฐานสำคัญ ๒ ประการ คือ หลักความเท่าเทียมกัน (Functional Equivalent Approach) ซึ่งหมายถึงความเท่าเทียมกันระหว่างการใช้ข้อความที่อยู่ในรูปของกระดาษกับข้อความที่อยู่ในรูปข้อมูลอิเล็กทรอนิกส์ และหลักความเป็นกลางทางเทคโนโลยีและความเป็นการของสื่อ (Technology Neutrality/ Media Neutrality) ซึ่งหมายความว่ากฎหมายจะต้องเปิดกว้างเพื่อรอบรับการติดต่อสื่อสารด้วยวิธีการทางอิเล็กทรอนิกส์ทุกรูปแบบทั้งที่มีอยู่ในปัจจุบันและที่จะมีการพัฒนาขึ้นในอนาคต

หน่วยงานที่เกี่ยวข้องกับการปฏิบัติการสงครามไซเบอร์ของไทย

๑. หน่วยงานภาครัฐ (ภาคพลเรือน)

๑.๑ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

๑.๒ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

๑.๓ สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

๑.๔ สำนักป้องกันและปราบปรามการกระทำผิดทางเทคโนโลยีสารสนเทศ

๑.๕ กองบังคับการปราบปรามการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี

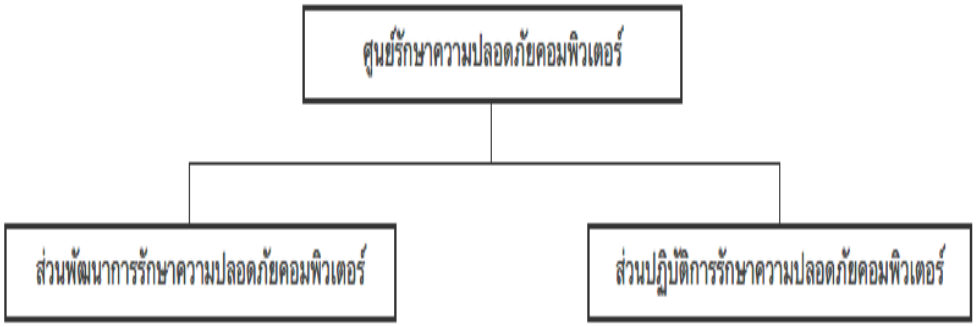
๑.๖ สำนักงานสภาความมั่นคงแห่งชาติ

๑.๗ สำนักข่าวกรองแห่งชาติ

๒. หน่วยงานความมั่นคง ได้มีการดำเนินการเกี่ยวกับด้านไซเบอร์อย่างต่อเนื่อง โดยมีการประสานงานกับหน่วยงานพลเรือนที่เกี่ยวข้อง รวมถึงภาคเอกชน การดำเนินการภายใน ได้มีการจัดประชุมสัมมนาสร้างความตระหนักให้กับกำลังพลเป็นประจำ รวมถึงมีการสร้างประชาคมความมั่นคงปลอดภัยไซเบอร์ เพื่อสร้างความร่วมมือระหว่างหน่วยงาน โดยหน่วยงานด้านไซเบอร์สังกัดกระทรวงกลาโหม ที่รับผิดชอบด้านการปฏิบัติการสงครามไซเบอร์ ในปัจจุบันสรุปได้ดังนี้

๒.๑ สำนักงานปลัดกระทรวงกลาโหม มีศูนย์รักษาความปลอดภัยคอมพิวเตอร์ กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม (ศรค.ทสอ.กห.) ซึ่งมีหน้าที่พิจารณา เสนอความเห็น วางแผน อำนวยการ ประสานงาน กำกับการและดำเนินการเกี่ยวกับการรักษาความปลอดภัยคอมพิวเตอร์และการสงครามสารสนเทศของกระทรวงกลาโหม รวมทั้งปฏิบัติงานอื่นตามที่ได้รับมอบหมาย และมีโครงสร้างหน่วยตามแผนภาพที่ ๒-๖

แผนภาพที่ ๒ - ๖ โครงสร้างการจัดส่วนราชการ ศรค.ทสอ.กห.



๒.๒ กองบัญชาการกองทัพไทย มีหน่วยงานที่เกี่ยวข้องดังนี้

๒.๒.๑ กองรักษาความปลอดภัยสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศ กรมการสื่อสารทหาร ซึ่งมีโครงสร้างหน่วยงานดังแผนภาพที่ ๒-๗ มีภารกิจหน้าที่ในการป้องกัน เฝ้าระวัง ตรวจสอบ วิเคราะห์ ทดสอบ ประเมินผล แจ้งเตือน ตอบสนองเหตุการณ์ที่เกี่ยวข้องกับภัยคุกคามทางสารสนเทศ การบุกรุกระบบ การกระทำที่ละเมิด กฎหมาย กฎระเบียบ ข้อบังคับที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ รวมถึงมีหน้าที่เกี่ยวกับการพัฒนาบุคลากร การสร้างความตระหนักรู้เกี่ยวกับการรักษาความปลอดภัยระบบสารสนเทศให้กับกำลังพลของกองบัญชาการกองทัพไทย การพัฒนาระบบงาน กระบวนงาน การบริหารจัดการระบบสารสนเทศ ในกองบัญชาการกองทัพไทย

แผนภาพที่ ๒ - ๗ โครงสร้างศูนย์เทคโนโลยีสารสนเทศ กรมการสื่อสารทหาร

๒.๒.๒ กองปฏิบัติการสงครามเครือข่ายคอมพิวเตอร์ สำนักปฏิบัติการ กรมยุทธการทหาร กองบัญชาการกองทัพไทย มีโครงสร้างหน่วยงานตามแผนภาพที่ ๒ - ๘ ตั้งขึ้นตามมติสภากลาโหมครั้งที่ ๕/๒๕๕๖ เรื่องภัยคุกคามด้านไซเบอร์ โดยกำหนดให้ บก.ทท. นำข้อมูลไปศึกษาและพิจารณาแนวทางการดำเนินการจัดตั้งหน่วยไซเบอร์ขึ้นมารับผิดชอบภัยคุกคามด้านไซเบอร์เป็นการเฉพาะ ซึ่ง บก.ทท. ได้ปรับโครงสร้างและตั้งกองปฏิบัติการสงครามเครือข่ายคอมพิวเตอร์โดยมีหน้าที่พิจารณาเสนอความเห็น นโยบาย วางแผน อำนวยการ ประสานงาน บูรณาการ กำกับดูแล และปฏิบัติการสงครามเครือข่าย ทั้งเชิงรับ และเชิงรุก โดยมีขอบเขตความรับผิดชอบและหน้าที่ที่สำคัญประกอบด้วย พิจารณาเสนอความเห็น นโยบาย วางแผน อำนวยการ ประสานงาน และกำกับดูแลการปฏิบัติ การต่างๆ ที่เกี่ยวข้องกับสงครามเครือข่าย ทั้งเชิงรับ และเชิงรุก การดำเนินการปฏิบัติการสงครามเครือข่ายคอมพิวเตอร์ ได้ทั้งเชิงรับ (Defense) และ เชิงรุก (Offense) และการดำเนินการบูรณาการการปฏิบัติงานระหว่างหน่วยงานหรือบุคลากรต่างๆ ที่มีความเชี่ยวชาญ และ มีเครื่องมือหรือยุทโธปกรณ์ต่างๆ ที่เกี่ยวข้องกับการปฏิบัติการสงครามเครือข่ายในทุกมิติ

แผนภาพที่ ๒ - ๘ โครงสร้างกองสงครามเครือข่าย ยก.ทหาร

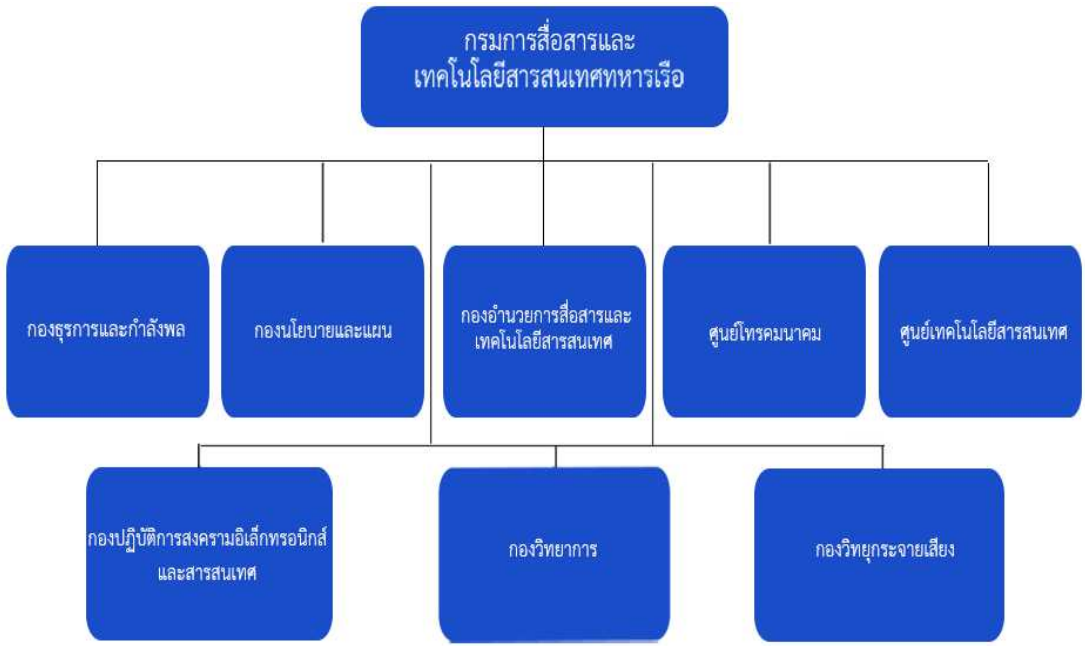
๒.๓ กองทัพบก มีกองการสงครามสารสนเทศ ศูนย์เทคโนโลยีทางทหาร กรมการทหารสื่อสาร รับผิดชอบ โดยมีโครงสร้างหน่วยงานแผนภาพที่ ๒ - ๙ ซึ่ง กองทัพบก (อยู่ระหว่างการปรับโครงสร้าง โดยในอนาคตงานด้านการปฏิบัติการสงครามไซเบอร์จะมีหน่วยงานรับผิดชอบเฉพาะดังแผนภาพที่ ๒ - ๑๐) มีหน้าที่ และความรับผิดชอบ ในการวางแผน อำนวยการ ประสานงาน กำกับการแนะนำ ดำเนินการวิจัยและพัฒนาเกี่ยวกับ การดำเนินกรมวิธีด้วยระบบคอมพิวเตอร์ เพื่อสนับสนุนการบริหารในยามปกติ ตลอดจนให้การสนับสนุนระบบควบคุมบังคับบัญชา และเทคโนโลยีคอมพิวเตอร์ของกองทัพบก รวมถึงการปฏิบัติการไซเบอร์/ข่าวสาร และภัยคุกคามที่เกี่ยวข้อง การรักษาความปลอดภัยไซเบอร์ของ ทบ. การกู้คืนระบบให้ใช้งานได้การสร้างความร่วมมือทางทางด้านไซเบอร์และสารสนเทศกับหน่วยราชการและองค์กรภายนอก ทบ.ทั้งในประเทศ และระหว่างประเทศ และการวิจัยพัฒนาและการฝึกศึกษาด้านเทคโนโลยีสารสนเทศของ ทบ.

แผนภาพที่ ๒ - ๙ โครงสร้างกองศูนย์เทคโนโลยีทางทหาร กรมการทหารสื่อสาร กองทัพบก (ปัจจุบัน)

แผนภาพที่ ๒ - ๑๐ โครงสร้างกองศูนย์เทคโนโลยีทางทหาร (อยู่ระหว่างเสนอปรับโครงสร้าง)

๒.๔ กองทัพเรือ มีกองปฏิบัติการสงครามอิเล็กทรอนิกส์และสารสนเทศ กรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ เป็นหน่วยงานรับผิดชอบ โดยมีโครงสร้างตามแผนภาพที่ ๒ - ๑๑ มีหน้าที่กำกับการและดำเนินการเกี่ยวกับสงครามสารสนเทศ การรหัสข้อมูลสารสนเทศของกองทัพเรือ เตรียมการปฏิบัติการสงครามสารสนเทศต่อฝ่ายตรงข้าม รวบรวมข้อมูลข่าวสารและเป็นศูนย์รับแจ้งเหตุด้านความปลอดภัย เผยแพร่และแจกจ่ายข้อมูลด้านการสงครามสารสนเทศให้หน่วยที่เกี่ยวข้อง

แผนภาพที่ ๒ - ๑๑ โครงสร้างกองปฏิบัติการสงครามอิเล็กทรอนิกส์และสารสนเทศ สสท.ทร.



๒.๕ กองทัพอากาศมีกองสงครามอิเล็กทรอนิกส์และสารสนเทศ กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ เป็นหน่วยงานรับผิดชอบ โดยมีโครงสร้างตามแผนภาพที่ ๒ - ๑๒ ซึ่งที่ผ่านมามีการดำเนินการเกี่ยวกับการพัฒนาขีดความสามารถด้านสงครามไซเบอร์ใน ๓ ส่วน คือ ด้านการกำหนดและปรับปรุงระเบียบ นโยบาย แนวทางการปฏิบัติ การพัฒนาด้านเทคโนโลยี การพัฒนาด้านบุคลากร

แผนภาพที่ ๒ - ๑๒ โครงสร้างกองสงครามอิเล็กทรอนิกส์และสารสนเทศ สอ.ทอ.

หลักการกำหนดขีดความสามารถด้านสงครามไซเบอร์

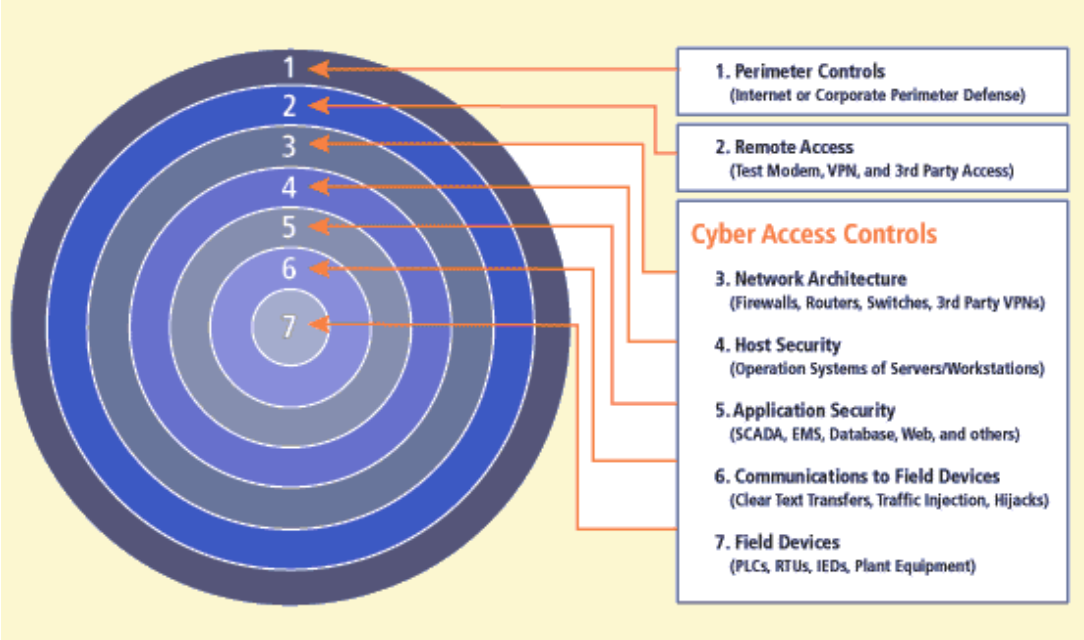
๑. เทคนิคการป้องกันภัยแบบเชิงลึก (Defense-in-Depth)

เทคนิคการป้องกันภัยแบบเชิงลึก[๑๐] เป็นแนวความคิดที่ต่างจากการป้องกันภัยทางระบบแบบเดิมที่เรียกว่าการป้องกันทางเข้าออกแบบขอบนอก (Perimeter Defense) ซึ่งเป็นการป้องกันระบบสารสนเทศการบุกรุกโจมตีภายนอก (External Attack) ทั้งจากผู้ไม่หวังดีหรือจากซอฟท์แวร์ประสงค์ร้ายต่างๆ (Malware) ทั้งนี้เพราะการโจมตีระบบที่สำเร็จและสำคัญส่วนใหญ่ ไม่ได้มาจากภายนอก แต่เกิดขึ้นภายในขอบเขตที่ได้รับการป้องกัน รวมถึงการที่ขอบเขตมีรูรั่วทั้งที่เกิดโดยไม่ได้ตั้งใจ หรือเกิดจากความประมาท มักง่ายของผู้ใช้ เช่นการนำอุปกรณ์เครือข่ายไร้สายมาต่อเชื่อมเข้ากับเครือข่ายหลักทำให้ผู้ไม่หวังดีสามารถเข้าถึงเครือข่ายและระบบสารสนเทศได้จากภายนอก หลักการป้องกันเชิงลึกจะเน้นการดำเนินการดังต่อไปนี้

---

[๑๐] Joel Snyder, Six Strategies for Defense-in-Depth, Securing the Network from the Inside Out

แผนภาพที่ ๒ - ๑๓ แนวความคิดการป้องกันภัยแบบเชิงลึก (Defense-in-Depth)



๑.๑ การปรับระบบและเครือข่ายจากเครือข่ายในลักษณะเชิงเดี่ยว (Single Homogeneous Zone) ที่เหมือนกันทั้งหมด กล่าวคือใช้อุปกรณ์ ซอฟท์แวร์ แบบเดียวกันทั้งหมด ซึ่งหากเกิดจุดอ่อนหรือช่องโหว่ทางด้านความปลอดภัยกับอุปกรณ์หรือซอฟท์แวร์ดังกล่าว ระบบทั้งระบบจะเกิดความเสี่ยงต่อการถูกโจมตี

๑.๒ การปรับสิทธิการเข้าถึงของผู้ใช้งาน จากการอนุญาตให้ผู้ใช้งานทุกคนมีสิทธิการเข้าถึงระบบเหมือนกันเป็นการให้สิทธิกับผู้ใช้ขั้นต่ำที่สุด (Least Privilege) ที่ผู้ใช้สามารถปฏิบัติงานที่ตนรับผิดชอบได้

๑.๓ การปรับปรุงเครือข่ายให้มีขีดความสามารถป้องกันภายในและมีการแบ่งพื้นที่ภายในเป็นส่วนๆ (Internal Perimeterization and Defense) ซึ่งแยกระบบสารสนเทศที่สำคัญออกจากระบบสารสนเทศอื่นๆ โดยใช้เทคนิคที่เรียกว่า DMZ: Demilitarized Zone ทำให้ผู้ที่ไม่มีสิทธิเข้าถึงระบบสารสนเทศดังกล่าวไม่สามารถเข้าถึงระบบได้

๑.๔ การมีกฎ ระเบียบ และข้อปฏิบัติที่จำเป็นชัดเจน (Regulatory Requirements) ซึ่งจะช่วยกำหนดแนวทางการใช้งานระบบสารสนเทศ และเครือข่ายสารสนเทศ อย่างปลอดภัย และมีบทลงโทษที่ชัดเจนหากมีการกระทำที่ละเมิด กฎ ระเบียบ และข้อปฏิบัติดังกล่าว นอกจากนี้ยังช่วยให้ผู้ดูแลระบบหรือผู้ที่เกี่ยวข้อง มีแนวทางในการดำเนินการเพื่อการแก้ไขปัญหาที่อาจจะเกิดขึ้นอย่างชัดเจน

๑.๕ การมีการจัดเก็บข้อมูลการใช้งาน การจราจร และมีการตรวจสอบข้อมูลดังกล่าว (Logging and Auditing) เพื่อเป็นการตรวจสอบเพิ่มเติม นอกเหนือจากการใช้ระบบป้องกันการโจมตีว่ามีการดำเนินการที่ละเมิด กฎ ระเบียบ และข้อปฏิบัติ หรือมีการโจมตีระบบที่ระบบป้องกันไม่สามารถตรวจจับได้หรือไม่ อีกทั้งยังเป็นหลักฐานทางกฎหมาย ที่เจ้าหน้าที่รัฐที่มีหน้าที่เกี่ยวข้องกับการรักษาความปลอดภัยระบบสารสนเทศอาจร้องขออีกด้วย

๑.๖ การปรับปรุงอุปกรณ์หรือซอฟท์แวร์ให้ทันสมัยและมีช่องโหว่น้อยที่สุด (Devices and Software Hardening) เป็นการดำเนินการที่จะลดโอกาสหรือพื้นที่ผิวที่มีโอกาสถูกโจมตี (Reduce Surface Area of Attack) การดำเนินการดังกล่าวจะต้องทำอย่างต่อเนื่องและเป็นระบบ ในทุกอุปกรณ์ในระบบตั้งแต่เครื่องแม่ข่าย (Server) ไปจนถึงอุปกรณ์ปลายทาง (Endpoint Devices)

๑.๗ มีการจัดทำและดำเนินการตามแผนกู้ระบบฉุกเฉิน และแผนการจัดการกับความเสียหายของระบบ เพื่อการมีช่องทางสำรองให้กับระบบสารสนเทศและเครือข่ายสารสนเทศ (Business Continuity Planning/ Disaster Recovery Planning) ซึ่งจะทำให้การดำเนินการหรือการปฏิบัติการเป็นไปได้อย่างต่อเนื่อง การดำเนินการนี้อาจจะเป็นการตั้งศูนย์ปฏิบัติการ หรือศูนย์ข้อมูลสำรอง ซึ่งจะทำงานได้ทันทีที่ ระบบสารสนเทศหลักเกิดความเสียหายไม่สามารถใช้งานได้

การดำเนินการทั้ง ๗ ประการข้างต้น จะช่วยให้ระบบสารสนเทศและเครือข่ายสารสนเทศมีความปลอดภัยมากยิ่งขึ้น การป้องกันภัยแบบเชิงลึกไม่ใช่การมีอุปกรณ์หรือเครื่องมือเป็นชิ้นๆ แต่เป็นการมีสถาปัตยกรรมความปลอดภัยที่ต้องการระบบสารสนเทศและเครือข่ายสารสนเทศที่มีขีดความสามารถในการรับรู้และเฝ้าระวัง และสามารถปกป้องตัวเองได้ ซึ่งโดยสรุปแล้วการป้องกันภัยแบบเชิงลึกเป็นแนวทางเชิงรุก ที่เน้นการมีแนวความคิดเกี่ยวกับการออกแบบระบบรักษาความปลอดภัยจากภายในไปสู่ภายนอก ซึ่งจะช่วยป้องกันทั้งการโจมตีจากภายนอกและการโจมตีจากภายใน และเป็นกระบวนการที่ต้องมีการดำเนินการอย่างต่อเนื่อง

๒. วิธีการปฏิบัติที่เป็นเลิศเกี่ยวกับการรักษาความปลอดภัยระบบสารสนเทศ (Information Security Best Practices)

เป็นแนวทางการปฏิบัติที่ได้รับการยอมรับแล้วว่าเป็นแนวทางที่ดีที่สุดในการดำเนินการเพื่อให้ได้มาซึ่งความปลอดภัยระบบสารสนเทศ วิธีการปฏิบัติที่เป็นเลิศที่เกี่ยวข้องกับการรักษาความปลอดภัยระบบสารสนเทศแบ่งได้ดังนี้

๒.๑ วิธีการปฏิบัติที่เป็นเลิศสำหรับเจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศ เป็นแนวทางที่เกี่ยวข้องกับเจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศซึ่งการจะรักษาความปลอดภัยระบบสารสนเทศได้อย่างมีประสิทธิภาพ จำเป็นต้องมีการกำหนดหน้าที่และผู้รับผิดชอบ รวมถึงต้องมีการกำหนดขีดความสามารถของผู้ที่จะมาปฏิบัติหน้าที่เป็นเจ้าหน้าที่ดังกล่าว ซึ่งหากหน่วยงานหรือองค์กรมีการจัดคนที่ไม่มีความสามารถมาปฏิบัติหน้าที่ นั่นเป็นการแสดงให้เห็นว่าหน่วยงานหรือองค์กรนั้นไม่ให้ความสำคัญกับการรักษาความปลอดภัยระบบสารสนเทศ

๒.๒ วิธีการปฏิบัติที่เป็นเลิศเกี่ยวกับการกำหนดแนวทางการใช้งานระบบสารสนเทศ ซึ่งเป็นแนวทางที่แจ้งให้ผู้ใช้งานระบบสารสนเทศทราบว่า ตนมีสิทธิและหน้าที่ สามารถใช้งานระบบสารสนเทศได้อย่างไรบ้าง อะไรเป็นข้อปฏิบัติ อะไรเป็นข้อห้าม

๒.๓ วิธีการปฏิบัติที่เป็นเลิศเกี่ยวกับการปรับปรุงซอฟท์แวร์ จากที่กล่าวไปแล้วว่าการป้องกันแบบเชิงลึกจำเป็นที่จะต้องมีการดำเนินการเกี่ยวกับการปรับปรุงอุปกรณ์และซอฟท์แวร์ให้ทันสมัยและมีช่องโหว่ให้น้อยที่สุด อย่างไรก็ตามการดำเนินการดังกล่าว หากไม่มีแนวทางที่ชัดเจน อาจส่งผลกระทบกับการทำงานของระบบสารสนเทศได้ เช่นหลังการปรับปรุงซอฟท์แวร์ ซอฟท์แวร์อาจไม่ทำงานตามที่ได้ถูกโปรแกรมไว้ เป็นต้น ดังนั้นจึงจำเป็นต้องมีแนวทางในการปฏิบัติหากเกิดปัญหาดังกล่าวขึ้น

๒.๓ วิธีการปฏิบัติที่เป็นเลิศเกี่ยวกับการรักษาความปลอดภัยทางกายภาพ แม้ว่าระบบสารสนเทศจะถูกเข้าถึงและใช้งานผ่านทางเครือข่ายสารสนเทศ แต่ความปลอดภัยทางกายภาพของอุปกรณ์เครื่องแม่ข่ายที่ให้บริการก็เป็นสิ่งที่จำเป็นจะต้องคำนึงถึง เช่นการมีการตรวจสอบและจำกัดสิทธิการเข้าถึงตัวอุปกรณ์ โดยการใช้ประตู การตรวจสอบการเข้าถึงทางกายภาพด้วยกล้องวงจรปิดเป็นต้น

๒.๔ วิธีการปฏิบัติที่เป็นเลิศเกี่ยวกับการจัดประเภทข้อมูลและเอกสาร และแนวทางการเก็บข้อมูลและเอกสาร เป็นแนวทางที่ใช้ในการกำหนดประเภทของข้อมูล แยกประเภทข้อมูลที่มีความสำคัญและเป็นความลับ ออกจากข้อมูลทั่วไปที่สามารถเปิดเผยได้ รวมถึงยังกำหนดแนวทางการจัดเก็บและระยะเวลาการจัดเก็บข้อมูลประเภทต่างๆ เพื่อประโยชน์ในการใช้งานและประโยชน์ในทางกฎหมาย

๒.๕ วิธีการปฏิบัติที่เป็นเลิศเกี่ยวกับการตั้งรหัสผ่าน เป็นแนวทางที่กำหนดขึ้นเพื่อให้ผู้ใช้ระบบสารสนเทศ กำหนดรหัสผ่านเข้าใช้ระบบสารสนเทศในสิทธิของตน เป็นไปด้วยความปลอดภัย เช่นต้องมีการตั้งรหัสผ่านที่ประกอบด้วยตัวอักษรใหญ่ เล็ก และตัวเลข โดยมีความยาวไม่ต่ำกว่า ๘ ตัวอักษร เป็นต้น ทั้งนี้จากการวิจัยพบว่าหากตั้งรหัสผ่านโดยไม่มีกฎเกณฑ์แล้ว ผู้ใช้ส่วนใหญ่จะตั้งรหัสที่จำง่าย แต่ก็มีความเสี่ยงต่อการคาดเดาได้ง่ายเช่นเดียวกัน

๒.๖ วิธีการปฏิบัติที่เป็นเลิศเกี่ยวกับการใช้เครือข่ายไร้สาย เป็นการกำหนดแนวทางที่ชัดเจนและยอมรับได้ในการใช้งานเครือข่ายไร้สายสำหรับการต่อเชื่อมกับเครือข่ายหลัก เพื่อเข้าถึงระบบสารสนเทศได้อย่างปลอดภัย

๒.๗ วิธีการปฏิบัติที่เป็นเลิศเกี่ยวกับการอบรมสร้างความตระหนักรู้ด้านความปลอดภัยระบบสารสนเทศของผู้ใช้งานระบบ เป็นแนวทางการสร้างความตระหนักรู้ถึงภัยต่อระบบสารสนเทศ และความเสี่ยง รวมถึงแนวทางการปฏิบัติอย่างปลอดภัยให้กับผู้ใช้งานระบบ

๒.๘ วิธีการปฏิบัติที่เป็นเลิศเกี่ยวกับการวางแผนฉุกเฉิน เป็นแนวทางในการปฏิบัติหากเกิดเหตุฉุกเฉินด้านความปลอดภัยกับระบบสารสนเทศขึ้น เช่นเมื่อถูกโจมตีทางระบบสารสนเทศจะต้องมีแนวทางในการดำเนินการอย่างไร

วิธีการปฏิบัติที่เป็นเลิศต่างๆ ที่กล่าวถึงไปนั้น เป็นแนวทางที่สามารถนำมาประยุกต์ใช้เพื่อเพิ่มขีดความสามารถในการรักษาความปลอดภัยระบบสารสนเทศได้

๓. การตรวจสอบหาจุดอ่อนของระบบ (Vulnerability Assessment: VA) และการทดสอบเจาะระบบ (Penetration Testing: PENTEST)

๓.๑ การตรวจสอบหาจุดอ่อนของระบบเป็นกระบวนการตรวจสอบ ค้นหา และจัดลำดับความสำคัญของจุดอ่อนหรือช่องโหว่ในระบบสารสนเทศ และซอฟท์แวร์ ซึ่งจุดอ่อนดังกล่าวอาจถูกฝ่ายตรงข้ามหรือผู้ไม่หวังดี ใช้ประโยชน์ในการได้มาซึ่งข้อมูล การควบคุมระบบ การลิดรอน ขัดขวาง หรือทำลาย ข้อมูล หรือการทำงานของระบบ ซึ่งจะส่งผลกระทบต่อการปฏิบัติงานซึ่งต้องอาศัยระบบสารสนเทศดังกล่าว การทำการตรวจสอบหาจุดอ่อนของระบบจะช่วยให้เราสามารถลดความเสี่ยงจากการที่ระบบสารสนเทศจะถูกโจมตี ด้วยการแก้ไขจุดอ่อน หรือการหาแนวทางการดำเนินการเพื่อลดผลกระทบหากจุดอ่อนดังกล่าวถูกโจมตี ขั้นตอนการดำเนินการตรวจสอบหาจุดอ่อนของระบบคล้ายคลึงกับเทคนิคการวิเคราะห์ความเสี่ยงคือ

๓.๑.๑ ระบุทรัพย์สินหรือสิ่งอุปกรณ์ที่มีความสำคัญในระบบสารสนเทศ

๓.๑.๒ จัดลำดับความสำคัญของทรัพย์สินหรือสิ่งอุปกรณ์ในระบบ

๓.๑.๓ ตรวจสอบหาจุดอ่อนของทรัพย์สินหรือสิ่งอุปกรณ์ในระบบ

๓.๑.๔ ระบุแนวทางการแก้ไขจุดอ่อนหรือแนวทางการลดผลกระทบจากจุดอ่อนนั้นถูกโจมตี

๓.๒ การทดสอบเจาะระบบ เป็นขั้นตอนการดำเนินการที่ต่อเนื่องจากการตรวจสอบหาจุดอ่อนของระบบ คือเป็นขั้นตอนที่ยืนยันว่าจุดอ่อนที่ถูกตรวจพบในขั้นตอนการตรวจสอบหาจุดอ่อนนั้น มีผลกระทบต่อระบบจริง การทดสอบเจาะระบบแบ่งเป็น ๒ ประเภทดังนี้

๓.๒.๑ Black-Box เป็นการทดสอบเจาะระบบ โดยที่ผู้ทำการทดสอบไม่ได้รับข้อมูลรายละเอียดของระบบ ผู้ทดสอบจะต้องดำเนินวิธีการค้นหา และเก็บข้อมูลของระบบเอง และใช้ข้อมูลที่รวบรวมได้ดังกล่าวในการพยายามเจาะระบบ ซึ่งลักษณะนี้จะคล้ายกับผู้โจมตีเป็นบุคคลภายนอก ซึ่งไม่มีข้อมูลของระบบทำการโจมตีระบบ

๓.๒.๒ White-Box เป็นการทดสอบเจาะระบบ โดยที่ผู้ทำการทดสอบทราบรายละเอียดของระบบ ทำให้สามารถวิเคราะห์จุดอ่อนของระบบได้ง่ายกว่า แต่อาจจะไม่เหมือนสถานการณ์จริงเพราะในความเป็นจริง ผู้ที่ทำการโจมตีระบบมักจะไม่ทราบข้อมูลของระบบมากนัก

ทั้งเทคนิคการตรวจสอบหาจุดอ่อนของระบบ และการทดสอบเจาะระบบ เป็นเทคนิคที่จำเป็นในการป้องกันระบบสารสนเทศจากการโจมตีได้อย่างมีประสิทธิภาพ นอกจากนี้เทคนิคทั้ง ๒ นี้สามารถนำมาประยุกต์ใช้ในการพัฒนาขีดความสามารถเชิงรุกได้ กล่าวคือการใช้เทคนิคทั้ง ๒ ดำเนินการกับระบบสารสนเทศของฝ่ายตรงข้าม ในวิเคราะห์ ค้นหา และการเก็บข้อมูล จุดอ่อนของระบบ เพื่อสามารถใช้ประโยชน์จากจุดอ่อนของระบบนั้นในการปฏิบัติการสงครามสารสนเทศเชิงรุกกับระบบสารสนเทศของฝ่ายตรงข้ามต่อไป

๔. การตรวจสอบและสกัดกั้นข้อมูลการจราจรทางอินเทอร์เน็ตตามกฎหมาย (Lawful Interception)

การตรวจสอบและสกัดกั้นข้อมูลการจราจรทางอินเทอร์เน็ตตามกฎหมาย (Lawful Interception: LI) เป็นการตรวจสอบวิเคราะห์ข้อมูลการจราจรทางอินเทอร์เน็ต เพื่อการป้องกันระบบสารสนเทศ การรักษาความปลอดภัยไซเบอร์ ซึ่งโดยทั่วไปแล้วในระบบเครือข่ายขององค์กร เจ้าหน้าที่ผู้รับผิดชอบดูแลระบบสารสารสนเทศและเครือข่าย มีสิทธิ์เต็มที่ในการตรวจสอบข้อมูลการจราจรทางอินเทอร์เน็ตที่ผ่านเข้าและออกจากเครือข่ายองค์กรของตน ตราบใดที่ไม่นำข้อมูลส่วนบุคคลไปใช้ประโยชน์ในทางที่ผิด โดยข้อมูลการจราจรทางอินเทอร์เน็ตที่ใช้ในการตรวจสอบจะประกอบด้วยข้อมูล ๓ ประเภท ดังนี้

๔.๑ ข้อมูลสัญญาณ (Signaling data)

๔.๒ ข้อมูลเกี่ยวกับการบริหารจัดการเครือข่าย (Network Management Information)

๔.๓ ข้อมูลที่เป็นเนื้อหาที่ผู้ใช้ใช้งาน (User Content)

สำหรับเครือข่ายสาธารณะเช่นเครือข่ายอินเทอร์เน็ต โดยให้บริการผู้ให้บริการอินเทอร์เน็ตเอกชน (Internet Service Provider : ISP) นั้น โดยทั่วไปจะบริหารจัดการเครือข่ายของตนโดยใช้ข้อมูล ๒ ส่วนแรก (๔.๑ และ ๔.๒) และจะไม่ใช้ข้อมูลในส่วนที่ ๓ หรือข้อมูลเนื้อหาของผู้ใช้งาน เนื่องจากเกรงว่าจะเป็นการละเมิดกฎหมายที่เกี่ยวข้องกับความเป็นส่วนตัว

ทั้งนี้เนื่องจากการกระทำความผิดในปัจจุบันผ่านทางเครือข่ายสารสนเทศ พบว่ามีปัญหาการตรวจจับและควบคุมไม่ให้การกระทำความผิดเพิ่มมากขึ้น ทำได้ยากและใช้เวลานาน การค้นหาเว็บไซต์ที่เผยแพร่ข้อมูลที่ผิดกฎหมาย เช่นการหมิ่นสถาบันพระมหากษัตริย์ฯ การปลุกระดมทางการเมืองให้เกิดความขัดแย้ง แล้วทำการปิดกั้นเว็บไซต์ดังกล่าวซึ่งใช้ระยะเวลานานเมื่อดำเนินการตามกระบวนการกฎหมาย พบว่าไม่ได้ช่วยลดความเสียหายที่เกิดขึ้น รวมทั้งการจับกุมผู้กระทำความผิดเป็นไปได้ยากเนื่องจากมีการใช้เทคโนโลยีในการซ่อนพลางแหล่งที่มาของผู้กระทำความผิด ดังนั้นการตรวจสอบข้อมูลเนื้อหาผู้ใช้ ระหว่างที่มีการกระทำความผิดจึงเป็นช่องทางตรวจจับการกระทำความผิด รวมทั้งจะช่วยลดระยะเวลาการดำเนินการปิดกั้นลงได้ ซึ่งการทำ LI หลายประเทศให้การยอมรับและมีกฎหมายรองรับ เช่น Convention on Cybercrime[๑๑]

ซึ่งเป็นสนธิสัญญาที่เกี่ยวกับแนวทางการดำเนินการกับอาชญากรรมทางไซเบอร์ ซึ่งมีการดำเนินการทำ LI อยู่ด้วย ในสหรัฐฯ ก็มีกฎหมายที่ให้อำนาจหน่วยงานรัฐในการทำ LI เช่น Omnibus Crime Control and Safe Streets Act[๑๒], Foreign Intelligence Surveillance Act[๑๓] และ Patriot Act[๑๔] เป็นต้น อย่างไรก็ตาม การมีกฎหมายรองรับการทำ LI นั้นจำเป็นต้องคำนึงถึงความเสี่ยงที่อาจจะเกิดขึ้น เช่นการทราบถึงข้อมูลที่เป็น

---

[๑๑] Council of Europe, "Convention on Cybercrime", URL: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm เข้าถึงเมื่อ ๑๐ มิ.ย.๕๗

[๑๒] The United States Department of Justice, "Civil Rights Division Title III of the Civil Rights Act of 1964", URL: http://www.justice.gov/crt/about/spl/42usc3789d.php เข้าถึงเมื่อ ๑๐ มิ.ย.๕๗

[๑๓] Federal Judicial Center, "Foreign Intelligence Surveillance Court", URL: http://www.fjc.gov/history/home.nsf/page/courts_special_fisc.html เข้าถึงเมื่อ ๑๐ มิ.ย.๕๗

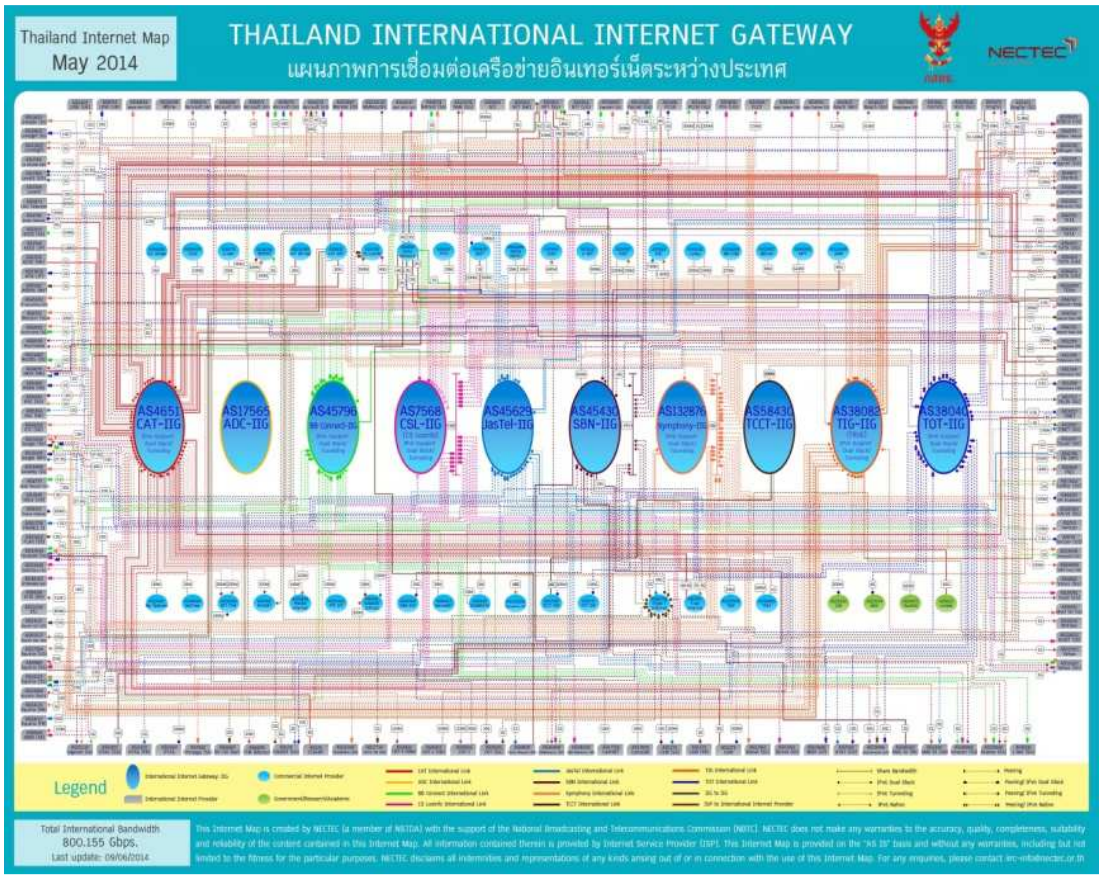
[๑๔] Department of Justice, "What is the USA Patriot", URL: http://www.justice.gov/archive/ll/highlights.htm เข้าถึงเมื่อ ๑๐ มิ.ย.๕๗

ความลับส่วนบุคคล ซึ่งอาจจะละเมิดกฎหมายอื่นที่สูงกว่าเช่นกฎหมายรัฐธรรมนูญ ดังนั้นจึงจำเป็นต้องกำหนดกฎเกณฑ์สำหรับหน่วยงานรัฐในการใช้ประโยชน์จากข้อมูลที่ได้จากการทำ LI เพื่อใช้สำหรับงานด้านความมั่นคงเท่านั้น และมีมาตรการสำหรับตรวจสอบการดำเนินการของหน่วยงานรัฐที่ทำ LI เพื่อให้เกิดความโปร่งใส และให้เกิดความไว้วางใจของประชาชน และไม่เกิดเหตุการณ์ที่หน่วยงานรัฐใช้ข้อมูลจาก LI เกินขอบเขตอย่างที่เกิดขึ้นในสหรัฐฯ ซึ่งจะกล่าวถึงในบทที่ ๓ ต่อไป

๕. ไซเบอร์เกตเวย์แห่งชาติ (National Cyber Gateway)

ปัจจุบันช่องทางการเชื่อมต่อเครือข่ายอินเทอร์เน็ตภายในประเทศ กับเครือข่ายอินเทอร์เน็ตต่างประเทศผ่านหน่วยงานรัฐ ผู้ให้บริการอินเทอร์เน็ตทั้งภาครัฐ และเอกชน มีเป็นจำนวนมากตามแผนภาพแผนภาพที่ ๒ - ๑๔

แผนภาพที่ ๒ - ๑๔ แผนภาพการเชื่อมต่อเครือข่ายอินเทอร์เน็ตระหว่างประเทศ[๑๕]



[๑๕] Internet Information Research Network Technology Lab, NECTEC, “Thailand International Gateway”, URL: http://internet.nectec.or.th/webstats/internetmap.current.iir?Sec%3Dinternetmap_current ข้าถึงเมื่อ ๑ ก.ค.๕๗

ดังนั้นการตรวจสอบการกระทำความผิด การทำ Lawful Interception การควบคุมการเผยแพร่ข้อมูลที่ผิดกฎหมายหรือมีผลกระทบต่อความมั่นคง รวมทั้งการป้องกันการโจมตีทางไซเบอร์ ทำได้ยาก หรือหากใช้กระบวนการของกฎหมายแจ้งให้ทุกผู้ให้บริการดำเนินการ ก็จะมีความล่าช้า จึงเริ่มมีแนวความคิดการทำไซเบอร์เกตเวย์แห่งชาติ (National Cyber Gateway) ขึ้น[๑๖] โดยกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารมีแผนที่จะจัดตั้งศูนย์สำหรับ ดำเนินการจัดตั้งไซเบอร์เกตเวย์แห่งชาติขึ้น เพื่อแก้ปัญหาการกระทำความผิดผ่านทางระบบสารสนเทศ รวมถึงดำเนินการปิดกั้นข้อมูลที่ต่อให้เกิดผลกระทบต่อความมั่นคงของชาติขึ้น โดยจะร่วมมือกับกองทัพบก คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) สำนักงานตำรวจแห่งชาติ และสำนักข่าวกรองแห่งชาติ รวมถึงผู้ให้บริการอินเทอร์เน็ตทั้งภาครัฐและเอกชน โดยมีจุดประสงค์เพื่อเพิ่มขีดความสามารถในการตรวจสอบ และควบคุมการกระทำความผิด และยังเพิ่มขีดความสามารถในการป้องกันการโจมตีทางไซเบอร์ในอนาคตอีกด้วย

---

[๑๖] Bangkok Post, “ICT plans national gateway to curb abuse of internet”, URL: http://www.bangkokpost.com/news/politics/412124/ict-plans-national-gateway-to-curb-abuse-of-internet เข้าถึงเมื่อ ๑๐ มิ.ย.๕๗

บทที่ ๓
การโจมตีทางไซเบอร์จากอดีตถึงปัจจุบัน

กล่าวนำ

การโจมตีทางไซเบอร์เกิดขึ้นพร้อมๆ กับการเกิดขึ้นของโลกไซเบอร์ ทั้งจากความตั้งใจและไม่ได้ตั้งใจของผู้กระทำ ผู้กระทำการโจมตีซึ่งปัจจุบันเรียกกันโดยทั่วไปว่า “แฮกเกอร์” (Hacker) ในยุคเริ่มต้นมีความสลับซับซ้อนน้อย เมื่อโลกไซเบอร์ได้พัฒนาไปตามกาลเวลา โลกไซเบอร์มีความสลับซับซ้อนมากขึ้น แฮกเกอร์ก็ได้พัฒนาตาม จนในปัจจุบันแฮกเกอร์มีความเชี่ยวชาญมาก สามารถสร้างความเสียหายให้กลับระบบสารสนเทศเกินกว่าที่เราจะจินตนาการได้

การบุกรุกและโจมตีทางไซเบอร์จากอดีตถึงปัจจุบัน

เมื่อวัน ๒ พฤศจิกายน ค.ศ.๑๙๘๘ (พ.ศ.๒๕๓๑) นาย Robert Morris, Jr. ซึ่งเป็นนิสิต ศึกษาอยู่คณะวิทยาศาสตร์คอมพิวเตอร์มหาวิทยาลัย Cornell ประเทศสหรัฐฯ ได้พัฒนาโปรแกรม ที่มีขีดความสามารถในการขยายพันธุ์ด้วยตัวเอง (Self - Replicate) และสามารถแพร่ระบาดด้วยตัวเอง (Self - Propagate) โดยได้ทดลองปล่อยสู่เครือข่ายอินเทอร์เน็ตถือเป็นหนอนอินเทอร์เน็ต และมัลแวร์ตัวแรกของโลก ที่มีการแพร่ระบาด[๑] ในวงกว้างและนับเป็นการตัวอย่างโจมตีทางไซเบอร์ครั้งแรกๆ ของโลก หลังจากนั้นมัลแวร์และการโจมตีทางไซเบอร์ก็มีวิวัฒนาการอย่างต่อเนื่อง พร้อมกับการเปลี่ยนแปลงจุดมุ่งหมายของการโจมตี จากเดิมที่ใช้เป็นการแสดงความสามารถของผู้โจมตีหรือพัฒนามัลแวร์ว่ามีความเข้าใจการทำงานของระบบรวมถึงรู้ถึงจุดอ่อนต่างๆ ของระบบ เปลี่ยนเป็นการใช้ประโยชน์จากจุดอ่อนในการเข้าโจมตีเพื่อผลประโยชน์อย่างใดอย่างหนึ่ง เช่น ผลประโยชน์ทางด้านการเงิน หรือการใช้เป็นเครื่องมือในการโจมตีทางไซเบอร์ระหว่างประเทศ โดยตัวอย่างการโจมตีทางด้านไซเบอร์ที่จะกล่าวถึงต่อไปในบทนี้ จะแสดงให้เห็นถึงความเปลี่ยนแปลงความซับซ้อนในรูปแบบของการโจมตีทางไซเบอร์ จุดมุ่งหมายของการโจมตีที่เปลี่ยนแปลงไป จนถึงความเสี่ยงของการโจมตีทางไซเบอร์ต่อระบบสารสนเทศและเครือข่ายสารสนเทศของหน่วยงานราชการและหน่วยงานที่รับผิดชอบเกี่ยวกับโครงสร้างพื้นฐานหลักของชาติ (National Critical Infrastructure)

---

[๑] “The Robert Morris Internet Worm”, URL: http://groups.csail.mit.edu/mac/classes/6.805/articles/morris-worm.html เข้าถึงเมื่อ ๗ มี.ค.๕๗

๑. การโจมตีทางไซเบอร์ยุคแรก

การโจมตีทางไซเบอร์ในยุคแรกกระทำที่จุดอ่อนของการออกแบบและการทำงานของระบบ โดยมีรายละเอียดพอสังเขปดังนี้

๑.๑ การโจมตีด้วยไวรัสคอมพิวเตอร์และมัลแวร์ยุคแรก

ไวรัสคอมพิวเตอร์ ถูกเรียกเลียนแบบไวรัส ที่เป็นสิ่งมีชีวิต แต่เป็นคำเรียกแบบย่อของโปรแกรมคอมพิวเตอร์ที่สามารถสำเนาตัวเอง โดยมีประวัติความเป็นมาดังนี้

๑.๑.๑ ในปี พ.ศ. ๒๕๐๕ (ค.ศ. ๑๙๖๒) ทีมวิศวกรของ Bell Telephone Laboratories ได้สร้างเกมชื่อว่า "Darwin" ถือเป็นโปรแกรมคอมพิวเตอร์ตัวแรกที่มีรูปแบบของไวรัส โดยฝังตัวอยู่ในหน่วยความจำ เกมนี้ใช้คำศัพท์บางอย่างที่มีคำว่า "Supervisor" มีลักษณะที่กำหนดกฎเกณฑ์การต่อสู้ระหว่างผู้เข้าแข่งขัน โปรแกรม Darwin นี้มีความสามารถที่จะวิจัยสภาพแวดล้อมของมัน ทำสำเนา และทำลายตัวเองได้ จุดประสงค์หลักของเกมนี้ก็คือลบโปรแกรมทั้งหมดที่คู่แข่งเขียนและครอบครองสนามรบ

๑.๑.๒ ต้นปี พ.ศ. ๒๕๑๓ (ค.ศ. ๑๙๗๐) มีการตรวจพบไวรัส Creeper ในเครือข่าย APRAnet ของทหารอเมริกา ถือเป็นต้นแบบไวรัสคอมพิวเตอร์ในปัจจุบัน โปรแกรม Creeper สามารถเข้าครอบครองเครือข่ายผ่านโมเด็มและส่งสำเนาตัวเองไปที่ฝั่ง Remote ไวรัสนี้ทำให้คนรู้ว่าติดไวรัสด้วยการ Broadcast ข้อความ "I'M THE CREEPER ... CATCH ME IF YOU CAN"

๑.๑.๓ ปี พ.ศ. ๒๕๑๗ (ค.ศ. ๑๙๗๔) โปรแกรมชื่อ "Rabbit" โผล่ขึ้นมาบนเครื่องเมนเฟรมที่เรียกชื่อนี้เพราะมันไม่ได้ทำอะไรนอกจากสำเนาตัวเองอย่างรวดเร็วไปในระบบเก็บข้อมูลชนิดต่างๆ Rabbit นี้ได้ดึงทรัพยากรของระบบมาใช้อย่างมาก ทำให้การทำงานกระทบอย่างรุนแรงจนอาจทำให้ระบบทำงานผิดพลาดได้

๑.๑.๔ ปี พ.ศ. ๒๕๒๕ (ค.ศ. ๑๙๘๒) มีการตรวจพบไวรัสชื่อ "Elk Cloner" นั้นเป็นคอมพิวเตอร์ไวรัสบนเครื่องคอมพิวเตอร์ส่วนบุคคลตัวแรก ซึ่งแพร่กระจาย คือในวงที่กว้างออกไปกว่าภายในห้องทดลองที่สร้างโปรแกรม โปรแกรมนี้ถูกเขียนขึ้นโดย Rich Skrenta โดยไวรัสนี้จะติดไปกับระบบปฏิบัติการ Apple DOS 3.3 ผ่านทาง Boot Sector ของฟล็อปปี้ดิสก์ ณ เวลานั้นผลของมันทำให้ผู้ใช้คอมพิวเตอร์บางคนนึกว่าไวรัสคอมพิวเตอร์เกิดจากมนุษย์ต่างดาว เพราะทำให้การแสดงภาพที่จอกลับหัวทำตัวอักษรกะพริบขึ้นข้อความต่างๆ ออกมา

๑.๑.๕ ปี พ.ศ. ๒๕๒๖ (ค.ศ. ๑๙๘๓) Len Adleman แห่งมหาวิทยาลัย Lehigh ตั้งคำว่า "Virus" ว่าเป็นโปรแกรมคอมพิวเตอร์ที่ทำสำเนาตัวเองได้ และในปี พ.ศ.๒๕๒๗ ใน Information Security Conference ครั้งที่ ๗ Fred Cohen ได้ให้คำจำกัดความของคำ "Computer Virus" ว่าเป็นโปรแกรมที่สามารถติดต่อไปยังโปรแกรมอื่นโดยการแก้ไขโปรแกรมเดิมเพื่อแพร่ขยายตัวเอง

๑.๑.๖ เดือนพฤศจิกายน พ.ศ. ๒๕๒๖ (ค.ศ. ๑๙๘๓) Fred Cohen บิดาแห่งไวรัสศาสตร์ (Virology) ได้ใช้คอมพิวเตอร์ VAX 11/750 สาธิตว่าโปรแกรมไวรัสสามารถฝังตัวเข้าไปใน Object อื่นได้

๑.๑.๗ ปี พ.ศ. ๒๕๒๙ (ค.ศ. ๑๙๘๖) ไวรัสตัวคอมพิวเตอร์รุ่นแรกๆ สร้างโดยโปรแกรมเมอร์ อายุ ๑๙ ปี ชาวปากีสถาน ชื่อ Basit Farooq และพี่ชายชื่อ Amjad เรียกชื่อ "Brain" ที่มีเป้าหมายไปที่เครื่องคอมพิวเตอร์ IBM Compatible ด้วยเหตุผลที่ว่าต้องการรู้ระดับของซอฟต์แวร์เถื่อนในประเทศตัวเอง แต่โชคไม่ดีที่การทดลองนี้หลุดออกมานอกประเทศ

๑.๑.๘ ปี พ.ศ. ๒๕๒๙ (ค.ศ. ๑๙๘๖) โปรแกรมเมอร์ชาวเยอรมันชื่อ Ralf Burger พบวิธีตรวจจับโปรแกรมที่สำเนาตัวเองโดยการเพิ่มรหัสคำสั่งบางตัวเข้าไปในไฟล์ .COM โดยชุดโปรแกรมที่ใช้ทดลองชื่อ Virdem ถูกนำมาแสดงในเดือนธันวาคม ที่ Hamburg เป็นเวทีที่เหล่า Hacker ที่ชำนาญในการเจาะระบบ VAX/VMS มารวมตัวกันชื่อ "Chaos Computer Club"

๑.๑.๙ ปี พ.ศ. ๒๕๓๐ (ค.ศ. ๑๙๘๗) เกิดไวรัสระบาดที่กรุงเวียนนา ประเทศออสเตรีย เป็นไวรัสที่ทำลายคอมพิวเตอร์ส่วนบุคคลตัวแรกที่ทำงานเต็มระบบ ส่งผลกระทบไปเกือบทั่วโลก ที่มาของไวรัสนี้เป็นประเด็นถกเถียงกันมาก เพราะคนที่อ้างว่าเป็นคนเขียนคือ Franz Svoboda แต่เมื่อสืบไปจึงพบว่าเขารับมาจาก Ralf Burger ซึ่งก็อ้างว่ารับมาจาก Svoboda เดิมชื่อไวรัสคือ "lovechild" แต่เพราะไม่สามารถหาคนให้กำเนิดได้จึงถูกเรียกอย่างเป็นทางการว่า "Orphan" (ลูกกำพร้า)

๑.๑.๑๐ ปี พ.ศ. ๒๕๓๐ (ค.ศ. ๑๙๘๗) เดือนธันวาคม เกิดการระบาดของไวรัสครั้งแรกในเครือข่ายคอมพิวเตอร์ ชื่อ "Christmas Tree" โดยที่ไวรัสนี้มาจากเครือข่าย Bitnet ของมหาวิทยาลัย Western University ประเทศเยอรมนี และแพร่ไปยัง European Academic Research Network (EARN) และต่อเข้าไป เครือข่าย IBM-Vnet เครื่องคอมพิวเตอร์ที่ติดไวรัสจะแสดงผลที่หน้าจอเป็นรูปต้นคริสต์มาสต์ และส่งไปให้ผู้ใช้อื่นๆในเครือข่ายด้วย

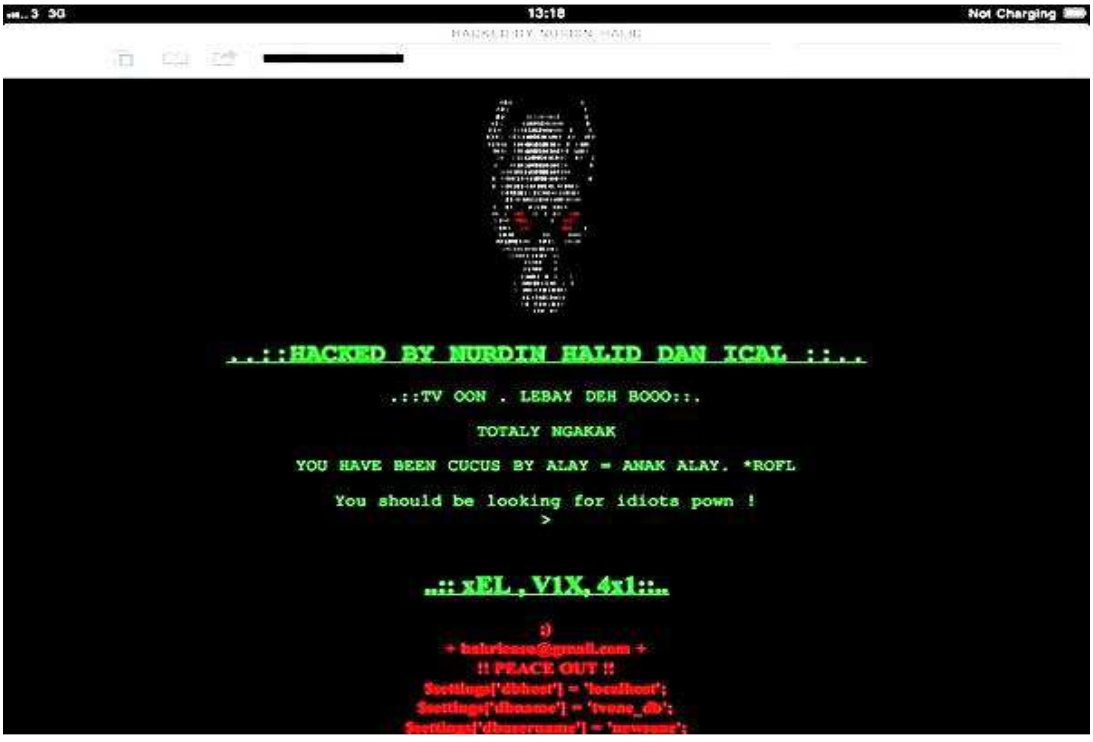
๑.๑.๑๑ ปี พ.ศ. ๒๕๓๑ (ค.ศ. ๑๙๘๘) Peter Norton นักเขียนโปรแกรมที่มีชื่อเสียง ผู้ก่อตั้งบริษัท Symantec ได้ออกมาประกาศว่าไวรัสคอมพิวเตอร์เป็นเรื่องไร้สาระ โดยเปรียบว่าเป็นแค่จระเข้ที่อยู่ในท่อระบายน้ำเสียในนิวยอร์ก สามารถกำจัดได้โดยไม่ยาก Peter Norton เป็นผู้เริ่มต้นเขียนโปรแกรม Norton-AntiVirus

๑.๑.๑๒ ปี พ.ศ. ๒๕๓๑ (ค.ศ. ๑๙๘๘) เดือนพฤศจิกายน มีหนอนเครือข่ายชื่อ "Morris" ระบาดอย่างรวดเร็ว ทำให้คอมพิวเตอร์กว่า ๖,๐๐๐ เครื่องในสหรัฐอเมริกา รวมทั้งในเครื่องคอมพิวเตอร์ของ NASA ด้วย ไม่สามารถใช้งานได้ โดยที่หนอนเครือข่าย Morris นี้จะสำเนาตัวเองไปที่เครือข่ายอื่นอย่างไม่จำกัดทำให้เครือข่ายรับไม่ไหวจนล่ม (Crash) ไปในที่สุด การระบาดของหนอนเครือข่ายครั้งนั้นทำให้สูญเสียเป็นมูลค่ากว่า ๙๖ ล้านดอลลาร์สหรัฐ

๑.๒ Website Defacement[๒]

Website Defacement หรือการลักลอบเปลี่ยนแปลงหน้าเว็บไซต์ เป็นการโจมตีทางไซเบอร์ที่ตัวซอฟท์แวร์ที่ให้บริการหน้าเว็บ (Web Server) โดยอาศัยจุดอ่อนของการของซอฟท์แวร์ระบบปฏิบัติการ หรือการตั้งค่า ในการได้สิทธิ์เข้าไปแก้ไขข้อมูลที่ให้บริการบน Web Server นั้น ทั้งนี้เนื่องจากเว็บไซต์ถูกใช้เป็นเครื่องมือที่สำคัญของหน่วยงานต่างๆในการสื่อสาร ประชาสัมพันธ์ หรือให้บริการออนไลน์ต่างๆกับผู้ใช้งานผ่านเครือข่ายอินเทอร์เน็ตสาธารณะ ด้วยลักษณะของบริการเว็บไซต์ที่เปิดให้ผู้ใช้งานสามารถเข้าถึงได้อยู่ตลอดเวลา ทำให้บริการเว็บไซต์ที่ไม่มีการรักษาความมั่นคงปลอดภัยที่ดี มีความเสี่ยงจากการถูกโจมตีจากผู้ไม่ประสงค์ดีได้อยู่ตลอดเวลาเช่นกัน โดยภัยคุกคามรูปแบบหนึ่งที่มักจะเกิดขึ้นกับบริการเว็บไซต์ คือการโจมตีเว็บไซต์เพื่อเปลี่ยนแปลงข้อมูลเผยแพร่หน้าเว็บ (Website Defacement) ซึ่งผู้โจมตีมีวัตถุประสงค์เพื่อปรับเปลี่ยนหน้าเว็บไซต์แรกของเว็บไซต์เป้าหมายหรือทั้งเว็บไซต์ จากเดิมไปเป็นหน้าเว็บไซต์ใหม่ การกระทำเช่นนี้อาจไม่ได้ก่อความเสียหายที่รุนแรงอะไรมากนัก เพียงแต่มีความต้องการเพื่อทำลายความน่าเชื่อถือของหน่วยงานเจ้าของเว็บไซต์ ซึ่งในเว็บไซต์ที่ถูกโจมตีส่วนใหญ่จะปรากฏรูปภาพหรือข้อความที่บ่งบอกถึงว่าเว็บไซต์ได้ถูกโจมตีได้สำเร็จ (รายละเอียดตามแผนภาพที่ ๓ - ๑)

แผนภาพที่ ๓ – ๑ ภาพแสดงให้เห็นถึงหน้าเว็บไซต์หลักแห่งหนึ่งที่ถูก Defacement



[๒]"ThaiCERT: รู้จักและป้องกันภัยจาก Website Defacement", URL: ttps://www.thaicert.or.th/papers/technical/2011/pa2011te004.html เข้าถึงเมื่อ ๑๕ พ.ค.๕๗

โดยรูปแบบของการโจมตีในลักษณะ Website Defacement เป็นการโจมตีที่นิยมมากที่สุดในหมู่ผู้โจมตีหรือแฮกเกอร์เนื่องจากสามารถเข้าโจมตีได้ง่ายและการโจมตีมักได้ผลทางด้านการสูญเสียความน่าเชื่อถืออย่างรวดเร็ว รวมถึงสามารถต่อยอดในการโจมตีส่วนประกอบหรือบริการอื่นๆ บนเครื่องแม่ข่ายนั้นๆ ด้วย ยิ่งหากผู้พัฒนาหรือผู้ดูแลระบบไม่มีการปิดช่องโหว่ดังกล่าวแล้ว อาจทำให้ผู้โจมตีสามารถทำความเสียหายซ้ำแล้วซ้ำเล่าจากรูปแบบเดิมๆ

๒. การโจมตีทางไซเบอร์เพื่อผลประโยชน์ทางการเงิน และข้อมูลข่าวสาร

จากพัฒนาการทางเทคโนโลยีสารสนเทศ การสื่อสารและโทรคมนาคมทำให้ระบบสารสนเทศและการสื่อสารถูกนำมาใช้ช่วยเพิ่มประสิทธิภาพ ข้อมูลที่สำคัญเช่น ข้อมูลบุคคล ข้อมูลทางด้านการเงิน จึงถูกนำเข้าสู่ระบบสารสนเทศมากยิ่งขึ้น ความสำคัญของระบบสารสนเทศมีเพิ่มมากขึ้น ส่งผลให้ระบบเหล่านี้กลายเป็นเป้าหมายของการโจมตีทางไซเบอร์ ไม่ใช่เพียงเพื่อทำลายเหมือนในยุคแรก แต่เพื่อใช้ประโยชน์ทางด้านการเงินจากระบบสารสนเทศเหล่านี้ รวมถึงข้อมูลที่อยู่ในระบบดังกล่าวด้วย โดยจากรายงานของบริษัท Kaspersky[๓] พบว่าในปี ค.ศ. ๒๐๑๓ ภัยคุกคามทางไซเบอร์ต่อด้านการเงินเพิ่มสูงขึ้น โดยการโจมตีทางไซเบอร์ที่ใช้มัลแวร์ สร้างความเสียหายเพิ่มมากขึ้น คาดว่าความเสียหายที่เกิดจากการโจมตีของมัลแวร์ทางด้านการเงินทั่วโลกกว่า ๒๘.๔ ล้านเหรียญสหรัฐ ซึ่งเพิ่มขึ้นประมาณร้อยละ ๒๘ เมื่อเทียบกับปีก่อนหน้านี้ โดยตัวอย่างของการโจมตีประเภทนี้ได้แก่

๒.๑ สปายแวร์[๔] (Spyware)

สปายแวร์เป็นคำจำกัดความของมัลแวร์ประเภทหนึ่ง ซึ่งมีลักษณะการทำงานบางอย่างโดยไม่ได้รับอนุญาตจากผู้ใช้ เช่นการแสดงภาพหรือข้อความโฆษณา การเก็บรวบรวมข้อมูลส่วนตัวของผู้ใช้ การเปลี่ยนแปลงค่าการทำงานของเครื่องคอมพิวเตอร์และระบบสารสนเทศ

จากข้อมูลพบว่าคำว่าสปายแวร์มีการเริ่มใช้ครั้งแรกในปี ค.ศ.๑๙๙๕ โดยมีความหมายถึงซอฟท์แวร์ที่ใช้ในการจารกรรม (Espionage) โดยตัวอย่างสปายแวร์ตัวแรกๆ ถูกตรวจพบและรายงานโดยโปรแกรมไฟร์วอลล์ Zone AlarmPersonal Firewall ซึ่งสามารถตรวจพบว่าโปรแกรม Reader Rabbit ซึ่งเป็นโปรแกรมเพื่อการศึกษาสำหรับเด็ก ซึ่งจำหน่ายโดยบริษัท Mattel มีการแอบส่งข้อมูลกลับไปยังบริษัทโดยที่ไม่มีการแจ้งไว้ในคำอธิบายการทำงานของโปรแกรม

โดยส่วนใหญ่สปายแวร์จะแฝงมากับซอฟท์แวร์ปกติ หรืออาศัยช่องโหว่ของระบบปฏิบัติการหรือซอฟท์แวร์บราวเซอร์ของผู้ใช้ ในการแอบเข้ามาติดตั้งบนเครื่องคอมพิวเตอร์ โดยที่ผู้ใช้ไม่รู้ตัว นอกจากนี้ในบางกรณียังอาจมีการใช้งานสปายแวร์อย่างถูกต้องในบริษัทเอกชน หน่วยงานราชการ

---

[๓] "Kaspersky Lab statistics: attacks involving finicial malware rise to 28 million in 2013", URL: http://www.kaspersky.com/about/news/virus/2014/Kaspersky-Lab-statistics-attacks-involving-financial-malware-rise-to-28-million-in-2013 เข้าถึงเมื่อ ๑๕ พ.ค.๕๗

[๔] "What is spyware?", URL: http://www.microsoft.com/security/pc-security/spyware-whatis.aspx เข้าถึงเมื่อ ๑๕ พ.ค.๕๗

ในการเก็บข้อมูลการใช้งานคอมพิวเตอร์ของผู้ใช้ในองค์กร เช่นหน่วยงานในประเทศสวิสเซอร์แลนด์และเยอรมนี ซึ่งมีกฎ ระเบียบ และกฎหมายรองรับ[๕] ให้องค์กรดังกล่าวสามารถตรวจสอบการใช้งานทรัพยากรขององค์กรตนเอง ว่าเป็นไปอย่างมีประสิทธิภาพหรือไม่

การใช้งานของสปายแวร์ก็มีวิวัฒนาการมาอย่างต่อเนื่องเช่นเดียวกับมัลแวร์ประเภทอื่น คือในยุคแรกๆ นั้นจะใช้เพื่อแสดงโฆษณาบนเครื่องคอมพิวเตอร์ของผู้ใช้ โดยที่ผู้ใช้ไม่ได้เป็นผู้เรียกดู ต่อมาเริ่มมีการใช้งานสปายแวร์ในลักษณะที่คล้ายมัลแวร์มากขึ้น โดยเน้นใช้เพื่อลักลอบเก็บข้อมูลการใช้งานอินเทอร์เน็ต ที่เรียกว่า Web Tracking โดยมีจุดประสงค์เพื่อศึกษาพฤติกรรมของผู้ใช้ และส่งโฆษณาที่ตรงกับความสนใจของผู้ใช้มากขึ้น หรือการลักลอบเก็บข้อความที่ผู้ใช้พิมพ์บนแป้นพิมพ์หรือที่เรียกว่า Key Logger สิ่งที่สปายแวร์ต่างจากมัลแวร์ชนิดอื่นคือ โดยทั่วไปแล้วสปายแวร์จะไม่แพร่กระจายตัวเอง (Self-Replicate) ในลักษณะคล้ายไวรัสคอมพิวเตอร์หรือหนอนอินเทอร์เน็ตแต่จะใช้เทคนิคเช่นแฝงมากับซอฟท์แวร์อื่นตามที่กล่าวไปแล้วข้างต้น ในปัจจุบันสปายแวร์มีจุดประสงค์การทำงานเพิ่มเติมนอกจากศึกษาพฤติกรรมของผู้ใช้ โดยมีการลักลอบเก็บข้อมูลผู้ใช้เพิ่มเติม เช่น รหัสผ่านของผู้ใช้ รวมถึงรายละเอียดส่วนตัวของผู้ใช้อื่นๆ ซึ่งอาจถูกนำไปใช้ในการลวงหรือการขโมยความเป็นตัวตน[๖] (Identity Theft) และใช้โจมตีผู้ใช้ในแง่ของการเงินได้ ซึ่ง Federal Trade Commission ซึ่งเป็นหน่วยงานซึ่งกำกับดูแลเกี่ยวกับเศรษฐกิจของสหรัฐฯ ได้ประมาณการว่ามีชาวอเมริกันกว่า ๒๗ ล้านคนเป็นเหยื่อการขโมยความเป็นตัวตน และส่งผลเสียหายกว่า สี่หมื่นแปดพันล้านเหรียญสหรัฐฯ ในภาคธุรกิจ และกว่าห้าพันล้านเหรียญสหรัฐฯ ในภาคประชาชน ตัวอย่างสปายแวร์ที่สำคัญ มีดังนี้

- Cool Web Search เป็นสปายแวร์ที่อาศัยช่องโหว่ของโปรแกรม Internet Explorer (IE) ในการติดตั้ง เมื่อติดแล้วจะปรับค่าโปรแกรม IE ให้ส่งข้อมูลการค้นหาผ่านเว็บไซต์ coolwebsearch.com พร้อมทั้งแสดงโฆษณา
- Internet Optimizer เป็นสปายแวร์ที่คอยดักจับและเปลี่ยนแปลงการใช้งานอินเทอร์เน็ตของผู้ใช้ โดยเมื่อโปรแกรมบราวเซอร์ถูกเรียกไปยังเว็บไซต์ที่ไม่มีตัวตน สปายแวร์ดังกล่าวจะแสดงโฆษณาที่มีข้อความเกี่ยวข้องกับเว็บไซต์ที่ผู้ใช้เรียก
- HuntBar หรือ Win Tools เป็นสปายแวร์ที่ติดตั้งตัวเองเป็นทูลบาร์เพิ่มเติมของโปรแกรมบราวเซอร์ ทำหน้าที่ในการเก็บข้อมูลการใช้งานอินเทอร์เน็ตของผู้ใช้ รวมถึงแอบแสดงหน้าโฆษณา

---

[๕] Basil Cupa, “Trojan Horse Resurrected: On the Legality of the Use of Government Spyware (Govware)”, LISS 2013, pp.419-428

[๖] Ecker Clint, “Massive spyware-based identity theft ring uncovered”, ArsTechnica, URL: http://arstechnica.com/news.ars/post/20050805-5175.html เข้าถึงเมื่อ ๑๕ พ.ค.๕๗

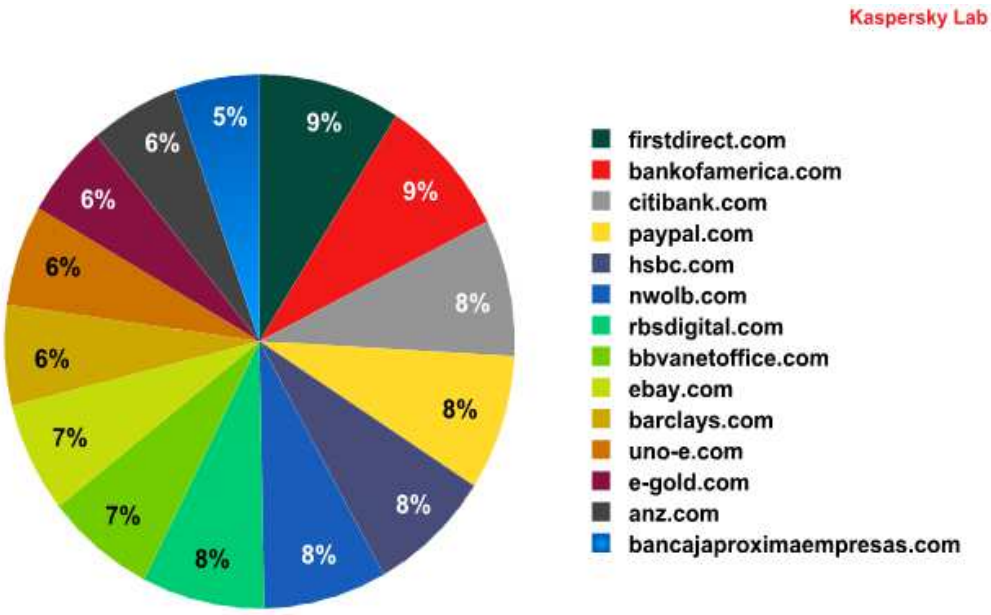
๒.๒ มัลแวร์เน้นการโจมตีด้านการเงิน

Zeus[๗] (ซุส) หรือที่รู้จักในอีกชื่อหนึ่งคือ Zbot เป็นมัลแวร์ที่โด่งดังในปี ค.ศ ๒๐๐๖ มีแหล่งกำเนิดจากยุโรปตะวันออก ถูกสร้างขึ้นเพื่อเป็นใช้เป็นเครื่องมือสำหรับอาชญากรในการขโมยข้อมูลสำคัญของผู้ใช้งานบริการสถาบันการเงินออนไลน์ ดังแสดงในแผนภาพที่ ๓ - ๒ โดเมน .com ที่ตกเป็นเป้าหมายของซุสและซุสสามารถแพร่กระจายได้หลายวิธี เช่น แนบไฟล์หรือลิงค์มากับอีเมล ฝังตัวอยู่ในช่องโหว่ของเอกสารประเภท PDF แฝงมากับอุปกรณ์บันทึกข้อมูลภายนอก (External Drive) ติดมากับซอฟต์แวร์ละเมิดลิขสิทธิ์ หรือส่งต่อลิงค์ผ่านเครือข่ายสังคมออนไลน์ (Social Network) เป็นต้น เมื่อซุสได้ติดตั้งตัวเองลงบนเครื่องคอมพิวเตอร์ของเหยื่อ เครื่องนั้นก็จะกลายเป็น Botnet ของซุสในทันที ทำให้ผู้โจมตีสามารถเข้ามาโจรกรรมข้อมูลสำคัญภายในเครื่องคอมพิวเตอร์ของเหยื่อได้ ไม่ว่าจะหมายเลขบัญชีธนาคาร รหัสผ่าน หรือข้อมูลอื่นๆนอกจากนี้ซุสยังพยายามรวบรวมข้อมูลของผู้ใช้งานที่ขโมยมาได้แล้วส่งมาเก็บไว้ที่เซิร์ฟเวอร์ของผู้โจมตี ซุสถูกขายเป็นเครื่องมือในตลาดมืด โดยมีราคาประมาณ ๓๐๐๐ – ๔๐๐๐ ดอลลาร์สหรัฐฯ จากรายงานการรับแจ้งเหตุภัยคุกคามของศูนย์ประสานงานการรักษาความมั่นคงระบบคอมพิวเตอร์ประเทศไทย (Thai CERT) ยังคงพบการแพร่กระจายของซุสที่ใช้ในการโจมตีผู้ใช้งานบริการออนไลน์ของสถาบันการเงินทั้งสถาบันการเงินในประเทศและต่างประเทศอยู่อย่างต่อเนื่อง

แผนภาพที่ ๓ – ๒ เว็บไซต์ปลอมที่สร้างขึ้นเพื่อหลอกลวงเหยื่อ

[๗] "Trojan.Zbot| Symantec", URL: http://www.symantec.com/security_response/writeup.jsp?docid=2010-011016-3514-99 เข้าถึงเมื่อ ๑๕ พ.ค.๕๗

แผนภาพที่ ๓ - ๓ โดเมน .com ที่ตกเป็นเป้าหมายของซุส



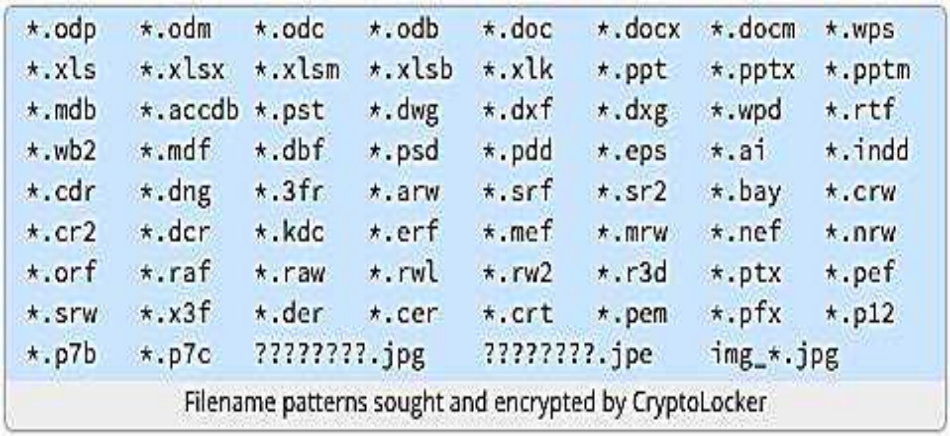
CryptoLocker[๘][๙] เป็น Ransomware บนระบบปฏิบัติการ Windows ตัวล่าสุดที่ถูกค้นพบเมื่อช่วงเดือนกันยายน พ.ศ.๒๕๕๖ ที่ผ่านมา โดยถูกเผยแพร่ผ่านทางไฟล์แนบในอีเมลหลอกลวง (ตัวอย่างที่มีผู้เคยพบ เช่น อีเมลแจ้งการติดตามพัสดุจาก Fed Ex หรือ UPS พร้อมกับแนบไฟล์ ZIP ซึ่งภายในมีไฟล์ EXE ที่ถูกปลอมแปลงว่าเป็นไฟล์ PDF) หรือผ่านทางมัลแวร์ประเภทบอตเน็ตที่เคยถูกติดตั้งลงบนเครื่องของผู้ใช้มาก่อน หลักการทำงานโดยทั่วไปของ CryptoLocker นั้น คล้ายคลึงกับ Ransomware ตัวอื่น ๆ ในอดีตที่ผ่านมา นั่นคือ ทำการเข้ารหัสลับข้อมูลไม่ว่าจะเป็นไฟล์เอกสาร รูปภาพ และไฟล์ประเภทอื่น ๆ ในเครื่องคอมพิวเตอร์ของเหยื่อ จากนั้นจะขึ้นข้อความข่มขู่ให้ผู้ใช้ทำการชำระเงินภายในเวลาที่กำหนด ก่อนที่ข้อมูลทั้งหมดจะไม่สามารถถูกถอดรหัสลับได้อีกตลอดไป ทั้งนี้ไม่ใช่เฉพาะข้อมูลในคอมพิวเตอร์ของเหยื่อเท่านั้นที่ถูกเข้ารหัสลับ แต่ข้อมูลที่แชร์ร่วมกันในระบบเครือข่ายก็ถูกเข้ารหัสลับด้วยเช่นกัน

---

[๘] "CryptoLocker", URL: http://en.wikipedia.org/wiki/CryptoLocker เข้าถึงเมื่อ ๑๕ พ.ค.๕๗

[๙] ธงชัย ศิลปวรางกูร, "CryptoLocker: เรื่องเก่าที่ถูกเอามาเล่าใหม่", URL: https://www.thaicert.or.th/papers/technical/2013/pa2013te011.html เข้าถึงเมื่อ ๑๕ พ.ค.๕๗

แผนภาพที่ ๓ - ๔ นามสกุลของไฟล์ที่ถูก CryptoLocker เข้ารหัส



*.odp	*.odm	*.odc	*.odb	*.doc	*.docx	*.docm	*.wps
*.xls	*.xlsx	*.xlsm	*.xlsb	*.xlk	*.ppt	*.pptx	*.pptm
*.mdb	*.accdb	*.pst	*.dwg	*.dxf	*.dxg	*.wpd	*.rtf
*.wb2	*.mdf	*.dbf	*.psd	*.pdd	*.eps	*.ai	*.indd
*.cdr	*.dng	*.3fr	*.arw	*.srf	*.sr2	*.bay	*.crw
*.cr2	*.dcr	*.kdc	*.erf	*.mef	*.mrw	*.nef	*.nrw
*.orf	*.raf	*.raw	*.rwl	*.rw2	*.r3d	*.ptx	*.pef
*.srw	*.x3f	*.der	*.cer	*.crt	*.pem	*.pfx	*.p12
*.p7b	*.p7c	????????.jpg		????????.jpe		img_*.jpg	

Filename patterns sought and encrypted by CryptoLocker

แผนภาพที่ ๓-๕ หน้าต่างของโปรแกรม CryptoLocker ที่ขึ้นข้อความข่มขู่ให้ผู้ใช้ชำระเงิน

พฤติกรรมที่น่าสนใจของ Crypto Locker อย่างหนึ่งหลังจากที่ติดตั้งตัวเองลงในคอมพิวเตอร์แล้ว คือการสร้างสุ่มชื่อโดเมนด้วยเทคนิค Domain Generation Algorithm เพื่อเชื่อมต่อไปยังเครื่องควบคุมและสั่งการ (Command-and-Control Server) ในการดาวน์โหลด Public Key ที่ใช้สำหรับเข้ารหัสลับ ซึ่งเทคนิคการสุ่มชื่อโดเมนเพื่อเชื่อมต่อไปยังเครื่องควบคุมและสั่งการนี้มักพบเห็นในมัลแวร์สมัยใหม่ที่แพร่ระบาดอยู่ในปัจจุบัน โดย Public Key ที่ถูกดาวน์โหลดมานั้นใช้อัลกอริทึม RSA ที่มีความยาวถึง ๒๐๔๘ bits ซึ่งด้วยสมรรถนะของคอมพิวเตอร์ในปัจจุบันยังไม่สามารถทำการสุ่มหา Private Key ที่ใช้ในการถอดรหัสลับที่มีความยาวขนาดนี้ในทางปฏิบัติได้ ทั้งนี้ RSA Public Key ดังกล่าวเป็นเพียง Key ที่ใช้ในการเข้ารหัสลับ Secret Key ที่ใช้ในการเข้ารหัสลับข้อมูลในคอมพิวเตอร์ของเหยื่อจริงๆ อีกทอดหนึ่ง โดย Secret Key ดังกล่าวใช้อัลกอริทึม AES ความยาว ๒๕๖ bits นอกจากนี้สิ่งที่น่าสนใจอีกอย่างคือช่องทางการชำระเงิน ซึ่งผู้ไม่หวังดีเปิดโอกาสให้เหยื่อสามารถชำระเงินเพื่อขอรับ Private Key ด้วย Bitcoin (ตัวย่อ: BTC) ซึ่งเป็นสกุลเงินในโลกดิจิตอลที่กำลังได้รับความนิยมอยู่ในปัจจุบัน

ทั้งนี้เมื่อต้นเดือนพฤศจิกายน พ.ศ.๒๕๕๖ มีการรายงานว่าผู้พัฒนา CryptoLocker ได้ยืดระยะเวลาให้กับผู้ใช้ที่ตกเป็นเหยื่อ ด้วยการเปิดเว็บไซต์ผ่านเครือข่าย TOR เพื่อให้บริการรับชำระเงิน โดยวิธีการชำระเงินนั้นจะเริ่มจากการให้ผู้ใช้อัพโหลดไฟล์ที่ถูกเข้ารหัสลับผ่านหน้าเว็บไซต์เพื่อทำการตรวจสอบหา Private Key ที่ใช้ในการถอดรหัสลับ โดยอ้างว่าใช้เวลาในขั้นตอนดังกล่าวประมาณ ๒๔ ชั่วโมง หลังจากเสร็จสิ้นจะมีหน้าต่างปรากฏให้ชำระเงินเป็น Bitcoin เช่นเดิม แต่มีการขึ้นราคาจากเดิม ๒ BTC เป็น ๑๐ BTC หรือเทียบเท่ากับราคาจากเดิมประมาณ ๔๖๐ USD เป็น ๒๓๐๐ USD (ข้อมูลอัตราแลกเปลี่ยน ณ วันที่ ๔ พฤศจิกายน พ.ศ.๒๕๕๖)

๓. การใช้ขีดความสามารถไซเบอร์เป็นกำลังอำนาจแห่งชาติ

๓.๑ การลักลอบดักรับและเก็บรวบรวมข้อมูลของหน่วยงานความมั่นคง

บางประเทศที่มีขีดความสามารถด้านไซเบอร์ได้ทำการลักลอบดักรับและเก็บรวบรวมข้อมูลของหน่วยงานด้านความมั่นคง ข้อมูลผู้นำประเทศ และข้อมูลอื่นๆ ทีเป็นประโยชน์ต่อตนเอง โดยการดักรับนี้ได้ดำเนินผ่านจากเครือข่ายอินเตอร์เน็ต เครือข่ายการสื่อสารโทรคมนาคม ตัวอย่างการดำเนินการในลักษณะนี้ได้รับการเปิดโปงโดยนาย Edward Snowden[๑๐] ว่าในหลายปีที่ผ่านมาทางการสหรัฐฯ ได้ลักลอบดักรับและเก็บรวบรวมข้อมูลการใช้งานระบบสื่อสารและระบบสารสนเทศโดยที่ไม่เลือกกลุ่มเป้าหมาย รวมถึงผู้นำที่เป็นมิตรประเทศของสหรัฐฯ เองด้วย ซึ่งต่อมาทางการสหรัฐฯ ได้ออกมายอมรับว่ามีการดักรบข้อมูลจริง แต่กระทำเพื่อความมั่นคงปลอดภัยของประเทศ

---

[๑๐] Bloomberg Businessweek, The Management Blog, “Edward Snowden and the NSA: A Lesson About Insider Threat”,URL: http://www.businessweek.com/articles/2013-07-03/edward-snowden-and-the-nsa-a-lesson-in-the-insider-threat เข้าถึงเมื่อ ๒๖ ก.พ.๕๗

๓.๒ การโจมตีทางไซเบอร์โดยหน่วยงานของรัฐบาล

จากรายงานของกระทรวงกลาโหมสหรัฐฯ[๑๑] และรายงานจากบริษัทที่เชี่ยวชาญด้านการรักษาความปลอดภัยระบบสารสนเทศ[๑๒] พบว่าระบบสารสนเทศของสหรัฐฯ และของชาติอื่นทั้งภาครัฐและเอกชน เป็นเป้าหมายและถูกโจมตีอย่างต่อเนื่อง (รายละเอียดตามแผนภาพที่ ๓ - ๑) โดยมีหลักฐานว่าที่มาของการโจมตีบางส่วนสามารถเชื่อมโยงกลับไปยังหน่วยงานรัฐบาลและหน่วยงานทางทหารของจีนได้ ซึ่งจีนได้ปฏิเสธการกระทำดังกล่าวและตอบโต้ว่าสหรัฐฯ ก็ได้ทำการโจมตีระบบสารสนเทศของจีนอย่างต่อเนื่อง[๑๓] ซึ่งปัญหาดังกล่าวได้เพิ่มความรุนแรง ส่งผลให้ทั้งสหรัฐฯ และจีนต้องมีการตกลงร่วมกันในการเกี่ยวกับการกำหนดแนวทางการรักษาความปลอดภัยทางไซเบอร์[๑๔] ในระหว่างที่รัฐมนตรีว่าการกระทรวงการต่างประเทศสหรัฐฯ เยือนจีนช่วงเดือน เม.ย.๕๖

ปัญหาดังกล่าวแสดงให้เห็นว่า ปัจจุบันมีชาติมหาอำนาจทั้งจีนและสหรัฐฯ ต่างมีการดำเนินการโจมตีระบบสารสนเทศ โดยหน่วยงานของรัฐจริง ทั้งนี้เพื่อการหาข่าวและข้อมูลที่สำคัญ รวมถึงการเตรียมความพร้อมในการในการโจมตีระบบสารสนเทศที่สำคัญหากเกิดสงครามหรือความขัดแย้งขึ้น

๓.๓ การโจมตีเพื่อลดขีดความสามารถทางการทหาร

ตัวอย่างการโจมตีทางไซเบอร์ในลักษณะได้ขึ้นกับโครงการพัฒนาขีดความสามารถด้านนิวเคลียร์ของประเทศอิหร่าน โดยที่ระบบสารสนเทศของโครงการพัฒนาขีดความสามารถด้านนิวเคลียร์ฯ ได้ถูกโจมตีโดยมัลแวร์ Stuxnet

มัลแวร์ Stuxnet ซึ่งถูกค้นพบครั้งแรกในช่วงเดือน มิ.ย.๕๒ เป็นตัวอย่างที่เห็นได้ชัดในปัจจุบันว่ามีการใช้ซอฟท์แวร์เป็นเครื่องมือทางไซเบอร์ในการโจมตีทำลายขีดความสามารถด้านอื่นนอกเหนือจากซอฟท์แวร์และตัวระบบสารสนเทศเอง เช่นแก้ไขเปลี่ยนแปลงซอฟท์แวร์ที่ควบคุมเครื่องจักรกลทำงานอย่างผิดปกติจนกระทั่งทำเครื่องจักรกลดังกล่าวเกิดความเสียหาย

จากการวิเคราะห์การทำงานของมัลแวร์ Stuxnet[๑๕] โดยผู้เชี่ยวชาญเกี่ยวกับมัลแวร์ พบว่า Stuxnet เป็นซอฟท์แวร์ที่มีขีดความสามารถและมีความซับซ้อนเป็นอย่างมาก ซึ่งจากขีดความสามารถ

---

[๑๑] Annual Report to Congress, Department of Defense, <http://www.defense.gov/pubs/2013_china_report_final.pdf> (10 May 2013)

[๑๒] APT1: Exposing One of China's Cyber Espionage Units, Madiant, <http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf> (10 May 2013)

[๑๓] Chinese Army: US hacks us so much, I'm amazed you can read this, The Register, <http://www.theregister.co.uk/2013/02/28/china_accuses_us_of_hacking/> (10 May 2013)

[๑๔] China, U.S. agree to work together on cyber security, SC Magazine, <http://www.scmagazine.com/china-us-agree-to-work-together-on-cyber-security/article/288948/?DCMP=EMC-SCUS_Newswire> (10 May 2013)

[๑๕] N. Falliere and others, W32.Stuxnet Dossier, February 2011. <http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/

และความซับซ้อนดังกล่าว นักวิเคราะห์ประเมินว่าการพัฒนามัลแวร์ Stuxnet ต้องได้รับการสนับสนุนทั้งทางด้านเงินทุนและเทคโนโลยีจากหน่วยงานภาครัฐ ซึ่งคาดว่าผู้พัฒนาหลักเป็นหน่วยงานภาครัฐจากประเทศอิสราเอลและสหรัฐอเมริกา โดยเป้าหมายของ Stuxnet คือการแก้ไขซอฟท์แวร์ที่ใช้ตั้งค่าอุปกรณ์ควบคุมการทำงานของเครื่องจักรที่ใช้ในกระบวนการเสริมสมรรถนะแร่ยูเรเนียม (Uranium Enrichment) ของประเทศอิหร่าน ทำให้เครื่องจักรดังกล่าวเกิดความเสียหาย และส่งผลกระทบต่อกระบวนการเสริมสมรรถนะแร่ยูเรเนียมของอิหร่านในที่สุด (รายละเอียดตามแผนภาพที่ ๓-๒)

แผนภาพที่ ๓-๖ ประธานาธิบดีอิหร่านเยี่ยมชม Natanz Uranium Enrichment Facility เมื่อวันที่ ๘ เม.ย.๕๑

การทำงานของมัลแวร์ Stuxnet เป็นตัวอย่างของการใช้ซอฟท์แวร์ในการลิดรอนทำลายระบบสารสนเทศที่เป็นโครงสร้างพื้นฐานหลักของชาติเช่น ระบบสื่อสารและโทรคมนาคม ระบบพลังงาน ระบบการเงินและเศรษฐกิจ ซึ่งมีความสำคัญและจำเป็นต่อทุกกระบวนการทำงานของชาติ ดังนั้นการรักษาความปลอดภัยระบบสารสนเทศที่เป็นโครงสร้างพื้นฐานหลักของชาติ ให้สามารถทำงานได้อย่างต่อเนื่องและปลอดภัยจากการโจมตีจึงเป็นสิ่งจำเป็นที่หน่วยงานที่รับผิดชอบจะต้องกำกับดูแล

การโจมตีทางไซเบอร์ในประเทศไทย

การโจมตีและเปลี่ยนแปลงหน้าเว็บไซต์ของหน่วยงานราชการไทย

เว็บไซต์สำนักงานปลัดสำนักนายกรัฐมนตรี (http://www.opm.go.th) ถูกโจมตีโดยทำการเปลี่ยนแปลงหน้าเว็บไซต์ เมื่อวันที่ ๘ พ.ค.๕๖ โดยมีการเปลี่ยนแปลงแก้ไขหน้าเว็บ การโจมตีก่อให้เกิดความเสียหายให้แก่ น.ส.ยิ่งลักษณ์ ชินวัตร นายกรัฐมนตรี โดยมีจุดมุ่งหมายที่จะทำลายความน่าเชื่อถือทางการเมือง โดยผลกระทบที่เกิดขึ้นตามมาคือความน่าเชื่อถือของหน่วยงานราชการถูกทำลาย เนื่องจากเว็บไซต์ดังกล่าวเป็นช่องทางที่สำนักงานปลัดสำนักนายกรัฐมนตรี (สปน.) ใช้ในการเผยแพร่ข้อมูลข่าวสารให้กับสาธารณชน

การโจมตีดังกล่าว ผู้โจมตีได้ใช้จุดอ่อนด้านความปลอดภัยที่มีในซอฟท์แวร์ระบบจัดการเนื้อหา (Content Management System: CMS) ซึ่งมีทำให้ผู้ไม่หวังดีสามารถได้สิทธิ์ในการควบคุมระบบและสามารถแก้ไขข้อมูลเช่นหน้าเว็บไซต์ได้ การที่ซอฟท์แวร์ระบบจัดการเนื้อหาถูกโจมตีจนนำไปสู่การเปลี่ยนแปลงหน้าเว็บไซต์ แสดงให้เห็นถึงความไม่รับผิดชอบของผู้ที่มีหน้าที่ในการดูแลจัดการและการรักษาความปลอดภัยของระบบและซอฟท์แวร์ที่ใช้งานจากการโจมตี และยังแสดงให้เห็นถึงความจำเป็นที่จะต้องมีการตรวจสอบและปรับปรุงซอฟท์แวร์ให้ทันสมัยอยู่เสมอ

แนวโน้มการโจมตีทางไซเบอร์[๑๖]

หลายบริษัทที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยทางไซเบอร์เช่น FireEye, Kaspersky, Microsoft, Sophos, Symantec, Trend Micro และ InfoSec Institute ได้วิเคราะห์แนวโน้มของภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ โดยสามารถสรุปเป็นหัวข้อที่น่าสนใจดังต่อไปนี้

ช่องโหว่ในซอฟต์แวร์ที่ถูกยุติการให้บริการสนับสนุน

ผลิตภัณฑ์ซอฟต์แวร์หลายตัวบริษัทผู้ผลิตจะยุติการให้บริการสนับสนุน เช่น Microsoft จะยุติการให้บริการ Windows XP และ Microsoft Office 2003 ตลอดจน Oracle จะยุติการให้บริการสนับสนุนผลิตภัณฑ์ Java 6 ซึ่งหมายความว่าจะไม่มีการแก้ไขช่องโหว่ใดๆ ในซอฟแวร์ดังกล่าวอีกต่อไปแล้วเป็นผลทำให้อาจจะมีการเผยแพร่ช่องโหว่ของผลิตภัณฑ์ดังกล่าวมากขึ้นเนื่องจากมีความเป็นไปได้ว่าผู้ไม่หวังดีจะนำช่องโหว่ที่ตนเองเคยค้นพบแต่ยังไม่เคยเผยแพร่ออกสู่สาธารณะออกมาใช้ในการโจมตีผู้อื่น

---

[๑๖] ThaiCERT: แนวโน้มภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ ปี 2557, URL: https://www.thaicert.or.th/papers/general/2013/pa2013ge013.html เข้าถึงเมื่อ ๒ มิ.ย.๕๗

มัลแวร์ที่มีความซับซ้อนมากขึ้น

ลักษณะของมัลแวร์ในอนาคตจะสามารถหลบหลีกการตรวจจับการติดต่อสื่อสารกับผู้ไม่หวังดี ได้แยบยลขึ้นหรือมีความสามารถในการลบระบบปฏิบัติการเพื่อทำลายร่องรอยหลังปฏิบัติการสำเร็จ เช่นการลบตัวระบบปฏิบัติการ Windows ทิ้งทั้งหมด ทำให้ไม่สามารถใช้งานคอมพิวเตอร์ได้

ภัยคุกคามที่เกี่ยวข้องกับโทรศัพท์มือถือ

ภัยคุกคามที่เกี่ยวข้องกับโทรศัพท์มือถือจะมีแนวโน้มเพิ่มมากขึ้นเนื่องจากจำนวนผู้ใช้โทรศัพท์มือถือที่เพิ่มขึ้น โดยการขโมย SMS ในมือถือที่ใช้ในการยืนยันตัวตน ๒ ขั้น (2-Step Verification) เช่น การขโมยรหัส OTP ที่เป็น SMS สำหรับใช้ล็อกอินบัญชีธนาคารออนไลน์จะพบเห็นได้มากขึ้นซึ่งเมื่อเดือนกรกฎาคม ๒๕๕๖ ที่ผ่านมาผู้ใช้บัญชีธนาคารออนไลน์ในประเทศไทยก็ได้ตกเป็นเป้าหมายของภัยคุกคามประเภทนี้

การโจมตีผู้ใช้ทั่วไป

เกิดจากตัวผู้ใช้ไม่ได้มีความตระหนักรู้และความเข้าใจในเรื่องความมั่นคงปลอดภัยไซเบอร์ ซึ่ง Trend Micro ได้ให้ความเห็นว่าผู้ไม่หวังดีจะโจมตีผู้ใช้โดยตรงแทนที่จะโจมตีระบบ โดยรูปแบบในการโจมตีนั้นอาจเป็นการส่งอีเมลหลอกลวงจากผู้ไม่หวังดีโดยเนื้อหาในอีเมลส่วนหนึ่งจะประกอบด้วยข้อมูลส่วนตัวของเหยื่อเพื่อสร้างความน่าเชื่อถือผู้ใช้จะถูกหลอกให้เปิดไฟล์อันตรายที่แนบมาหรือหลอกให้เข้าเว็บไซต์อันตรายที่สร้างขึ้นโดยผู้ไม่หวังดีส่งผลให้ผู้ไม่หวังดีสามารถเข้าถึงเครื่องคอมพิวเตอร์ของผู้ใช้และขโมยข้อมูลได้วิธีนี้เป็นที่นิยมเนื่องจากข้อมูลส่วนตัวของผู้ใช้อินเทอร์เน็ตมักหาได้โดยง่ายจากการที่ผู้ใช้เปิดเผยข้อมูลส่วนตัวลงบนสื่อสังคมออนไลน์เช่น Facebook โดยไม่ได้ตระหนักถึงผลกระทบต่างๆ ที่อาจตามมา

การโจมตีในระดับองค์กร

Kaspersky ได้กล่าวถึงประเภทการโจมตีทางไซเบอร์เปรียบเป็นรูปพีระมิดที่ถูกแบ่งออกเป็น ๓ ส่วน ส่วนล่างคือการโจมตีบุคคลทั่วไปโดยอาชญากรทางไซเบอร์เพื่อเงิน ส่วนกลางคือการจารกรรมข้อมูลขององค์กร รวมถึงการสอดแนมประชาชนโดยรัฐบาล และส่วนบนคือการโจมตีทางไซเบอร์จากประเทศหนึ่งไปยังประเทศอื่นๆ โดย Kaspersky ได้ให้ความเห็นว่าการโจมตีในระดับองค์กรจะมีแนวโน้มเพิ่มมากขึ้นโดยกลุ่มของผู้ที่เป็นอาชญากรทางไซเบอร์ทั่วไปหรือแม้กระทั่งผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยที่ไม่เคยมีส่วนเกี่ยวข้องกับอาชญากรรมทางไซเบอร์มาก่อนมีแนวโน้มที่จะผันตัวเองไปทำงานในลักษณะของมือปืนรับจ้างซึ่งผู้จ้างวานอาจเป็นบริษัทที่ต้องการสอดแนมข้อมูลของคู่ค้าและคู่แข่งเพื่อชิงความได้เปรียบทางด้านธุรกิจ

บทที่ ๔

การพัฒนาขีดความสามารถการปฏิบัติการสงครามไซเบอร์ของประเทศไทย

วิเคราะห์ศักยภาพด้านสงครามไซเบอร์ของประเทศไทย

นโยบายของรัฐบาลในปัจจุบัน เป็นนโยบายด้านความมั่นคงทั่วไป ยังไม่มีการออกนโยบายหรือแนวทางเฉพาะในการดำเนินการด้านสงครามไซเบอร์ การดำเนินการที่เกี่ยวข้องกับสงครามไซเบอร์ยังเป็นการดำเนินการแบบแยกส่วน เพื่อรองรับภารกิจของแต่ละกระทรวง หรือหน่วยงาน ไม่สามารถบูรณาการกันได้ ทำให้ขาดศักยภาพในการดำเนินการสงครามไซเบอร์ทั้งในทางรุก และในทางรับ และยังเป็นการสิ้นเปลืองทรัพยากรอีกด้วย นอกจากนั้น นโยบายการเปลี่ยนแปลงไปสู่การเป็นรัฐบาลอิเล็กทรอนิกส์ (Smart Government) ที่มีกลยุทธ์คือพัฒนาและปรับปรุงเครือข่ายข้อมูลภาครัฐ Government Information Network ให้มีประสิทธิภาพ มีการบูรณาการข้อมูลภาครัฐ โดยมีการวางโครงของข้อมูลเพื่อเอื้อต่อการเชื่อมโยงทุกรูปแบบ และต่อยอดสร้างเครือข่ายเป็น Super GIN และ Smart Cloud ต่อไปซึ่งเป็นการสร้างโครงสร้างพื้นฐานด้านระบบสารสนเทศ ให้หน่วยงานภาครัฐสามารถใช้ประโยชน์ร่วมกันนั้น ทำให้ระบบสารสนเทศกลายเป็นโครงสร้างพื้นฐานหลักอันหนึ่งของประเทศ เนื่องจากโครงสร้างพื้นฐานร่วมนี้ก็จะทำระบบสารสนเทศทุกกระทรวง ถูกจัดเก็บรวมในที่เดียวกัน ซึ่งทำให้เป็นจุดอ่อนหรือเป็นเป้าหมายที่สะดวกต่อการทำลายทางกายภาพ หรือการโจมตีทางเครือข่ายของฝ่ายตรงข้ามได้ง่าย

นโยบายด้านความมั่นคงแห่งชาติ ได้มีการชี้ให้เห็นภัยคุกคามที่มีการเปลี่ยนแปลงไป มองว่าระบบสารสนเทศเข้ามามีบทบาทสำคัญต่อภัยคุกคามด้านความมั่นคงทั้งหมด ทั้งในด้านที่อาจถูกนำมาใช้ประโยชน์ในการกระทำการโจมตีต่อฝ่ายตรงข้าม และระบบสารสนเทศนี้เองก็อาจตกเป็นเป้าหมายการโจมตีได้เช่นเดียวกันสำหรับแนวทางการดำเนินการด้านความมั่นคงในภาพรวมคือ พัฒนาศักยภาพของชาติในการป้องกันประเทศ ด้วยการผนึกกำลังจากทุกฝ่าย ทั้งภาครัฐ ภาคเอกชน และภาคประชาชน การพัฒนาความร่วมมือทางทหารและความเข้าใจอันดีกับกองทัพของประเทศเพื่อนบ้าน และส่งเสริมและประสานความร่วมมือกับต่างประเทศในด้านความมั่นคง ซึ่งตามแนวทางนี้ ภาครัฐก็ควรดำเนินการพัฒนาศักยภาพด้านสงครามไซเบอร์ ด้วยการผนึกกำลังจากทุกฝ่าย ทั้งภาครัฐ ภาคเอกชน ที่เกี่ยวข้องกับสงครามไซเบอร์ และจัดตั้งเครือข่ายภาคประชาชนในการร่วมมือกันเพื่อเพิ่มขีดความสามารถในด้านการปฏิบัติการสงครามไซเบอร์ได้ นอกจากนั้นยังควรร่วมมือกับกองทัพของประเทศเพื่อนบ้านในการดำเนินการป้องกันประเทศจากสงครามไซเบอร์ และส่งเสริมและประสานความร่วมมือกับประเทศอื่นๆที่มีศักยภาพในด้านสงครามไซเบอร์อีกด้วย

ศักยภาพด้านสงครามไซเบอร์ในประเทศไทย ในมุมมองจากผู้ที่เกี่ยวข้องและนักวิชาการ[๑๒๓๔] มีความเห็นตรงกันว่าขีดความสามารถด้านไซเบอร์ของประเทศไทยในเชิงรับยังอยู่ในระดับต่ำทั้งภาครัฐ (ฝ่ายพลเรือน และฝ่ายความมั่นคง) ซึ่งดูได้จากตัวชี้วัดเช่น จำนวนบุคลากร ที่มีความเชี่ยวชาญด้านไซเบอร์ที่ผ่านเกณฑ์ได้รับใบรับรองความสามารถด้านไซเบอร์เป็นการเฉพาะ ทั้งนี้สาเหตุหลักประการหนึ่งคือขาดการสนับสนุนในเชิงนโยบาย อีกตัวชี้วัดหนึ่งคือปริมาณการโจมตีทางไซเบอร์ที่มีแนวโน้มที่เพิ่มขึ้นอย่างต่อเนื่อง ตามที่หน่วยงานที่เกี่ยวข้องได้รายงาน ซึ่งได้กล่าวไปแล้วในบทที่ ๓ ซึ่งแสดงให้เห็นว่าผู้ดูแลระบบไม่ทราบหรือไม่มีความสามารถในการป้องกันการโจมตี ส่งผลให้ระบบดังกล่าวถูกนำไปใช้ประโยชน์เป็นฐานการโจมตีระบบอื่นต่อไป อย่างไรก็ตามทุกภาคส่วนมีความตื่นตัวกับเรื่องของความปลอดภัยไซเบอร์มากยิ่งขึ้น ซึ่งสามารถเห็นได้จาก จำนวนการจัดสัมมนา นิทรรศการ การแข่งขันที่เกี่ยวกับไซเบอร์ที่มีมากยิ่งขึ้น

สำหรับขีดความสามารถด้านสงครามไซเบอร์เชิงรุกก็ยังอยู่ในขั้นการเริ่มต้น การนำนโยบายดังกล่าวไปสู่การปฏิบัติก็ยังไม่มีแนวทางการดำเนินการที่ชัดเจน กฎหมายที่ออกมาเช่น พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ หรือ พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๔๔ ก็เป็นไปเพื่อรองรับการดำเนินการทางธุรกิจเป็นหลักเท่านั้น และยังขาดการบูรณาการด้านสงครามไซเบอร์ทางรับในระดับประเทศ ในขณะที่ศักยภาพทางรับแม้จะดูเหมือนว่ามีการเพิ่มเครื่องมือต่างๆมากขึ้น แต่ก็อาจไม่เพียงพอต่อการป้องกันระบบในภาพรวม เนื่องจากการขยายตัวของการใช้งานระบบสารสนเทศที่ถูกใช้เป็นเครื่องมือหลักในการดำเนินการทุกด้านของประเทศอย่างรวดเร็ว

แนวทางการพัฒนาขีดความสามารถการปฏิบัติการสงครามไซเบอร์ของประเทศไทย

จากการวิเคราะห์ศักยภาพด้านสงครามไซเบอร์ของประเทศไทยตามกล่าวข้างต้น เพื่อให้มีขีดความสามารถพร้อมสำหรับการปฏิบัติการสงครามไซเบอร์ จำเป็นต้องดำเนินการพัฒนาและดำเนินการทั้งด้านองค์บุคคล องค์วัตถุ และการบริหารจัดการ ดังนี้

<u>องค์บุคคล</u> ประเทศไทยจำเป็นต้องมีผู้เชี่ยวชาญด้านสงครามไซเบอร์ที่มีมาตรฐานสามารถปฏิบัติงานได้อย่างเพียงพอ โดยจะต้องได้รับการส่งเสริมจากภาครัฐในการผลิตบุคลากรที่มีความตระหนักรู้ด้านไซเบอร์ ไปจนถึงระดับผู้เชี่ยวชาญ โดยมีการจัดทำมาตรฐานวิชาชีพ เพื่อยกระดับความรู้ความสามารถของบุคลากรในสายวิชาชีพความมั่นคงปลอดภัยสารสนเทศ ให้อยู่ในระดับสากล

---

[๑] สุรางคณา วายุภาพ, สัมภาษณ์, ๘ มิ.ย.๕๗ (ภาคผนวก)

[๒] พล.ท. บรรเจิด เทียนทองดี, สัมภาษณ์, ๖ มิ.ย.๕๗ (ภาคผนวก)

[๓] ปริญญา หอมอเนก, สัมภาษณ์, ๔ มิ.ย.๕๗ (ภาคผนวก)

[๔] ไชยกร อภิวัฒโนกุล, สัมภาษณ์, ๔ มิ.ย.๕๗ (ภาคผนวก)

ร่วมทั้งการสร้างเส้นทางความก้าวหน้าในสายอาชีพ พร้อมค่าตอบแทนที่เหมาะสมกับระดับความรู้ความสามารถ ควบคู่กับการพัฒนากระบวนการรับรอง และการกำกับดูแลมาตรฐานวิชาชีพภายในประเทศ เพื่อลดค่าใช้จ่าย พร้อมสร้างความยอมรับการรับรองมาตรฐานดังกล่าว ในการผลิตผู้เชี่ยวชาญ อาจพัฒนาผู้เชี่ยวชาญระดับต้นจากสถาบันการศึกษาในประเทศ เช่นมหาวิทยาลัยต่างๆ และจากหน่วยงานวิจัยระดับชาติ รวมทั้งประสานความร่วมมือกับมิตรประเทศในการพัฒนาผู้เชี่ยวชาญด้านสงครามไซเบอร์

นอกจากนี้ยังต้องมีแผนการให้ความรู้อย่างต่อเนื่องและมีองค์ความรู้ที่เข้าถึงได้แก่ประชาชนทั่วไป เพื่อให้มีความตระหนักในความเสี่ยงต่างๆ ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ รวมถึงมีการปรับปรุงหลักสูตรการศึกษา ตั้งแต่ระดับประถมจนถึงระดับอุดมศึกษา โดยมีการสอดแทรกเนื้อหาที่เกี่ยวกับภัยคุกคามทางไซเบอร์และวิธีการป้องกันภัยดังกล่าวเบื้องต้น รวมทั้งมีการพัฒนาครูผู้สอน เพื่อให้สามารถปลูกจิตสำนึกด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับเยาวชนได้อย่างมีประสิทธิภาพ

<u>องค์วัตถุ</u> รัฐบาลจะต้องสนับสนุนการวิจัยและพัฒนาเทคโนโลยีที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อให้ประเทศไทยใช้เทคโนโลยีที่มีราคาถูก เพื่อให้เพียงพอกับการป้องกันประเทศจากสงครามไซเบอร์ นอกจากนั้นซอฟต์แวร์ที่วิจัยพัฒนาเองภายในประเทศจะเป็นซอฟต์แวร์ปลอดภัยจากการแฝงตัวของซอฟต์แวร์ประสงค์ร้ายจากฝ่ายตรงข้ามอีกด้วย

<u>การบริหารจัดการ</u> จะต้องบูรณาการการปฏิบัติการสงครามไซเบอร์ระหว่างหน่วยงานภาครัฐให้สามารถประสานความร่วมมือในการป้องกันได้อย่างมีประสิทธิภาพ และจัดให้มีหน่วยงานความมั่นคงด้านสงครามไซเบอร์กลางเป็นการเฉพาะ เช่น National Cyber Security Agency ที่มีโครงสร้างการบริหารงานระดับชาติ พร้อมบทบาทหน้าที่ที่ชัดเจน เพื่อการบัญชาการ การประสานความร่วมมือ กำหนดขั้นตอนการดำเนินงาน ในการส่งเสริม สนับสนุน มีอำนาจสั่งการ ลงโทษ รับรอง กำกับ ตรวจสอบ ประเมินผล เช่นเดียวกับประเทศที่ประสบผลสำเร็จในการสร้างขีดความสามารถด้านสงครามไซเบอร์ เช่น สหรัฐอเมริกา จีน เกาหลีใต้ เป็นต้น เพื่อให้การดำเนินการด้านสงครามไซเบอร์เป็นไปอย่างมีประสิทธิภาพ และมีหน่วยงานสงครามไซเบอร์ระดับเหล่าทัพเพื่อประสานการปฏิบัติอย่างใกล้ชิด อีกทั้งต้องส่งเสริมให้มีความสามารถในการวิจัย พัฒนา เตรียมความพร้อม ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงต้องมีการดำเนินการวิเคราะห์ความเสี่ยง ของทรัพย์สินสารสนเทศ ทั้งระดับองค์กร และระดับประเทศ โดยเฉพาะหน่วยงานภาครัฐและหน่วยงานที่เป็นโครงสร้างพื้นฐานสำคัญ ที่เทคโนโลยีของการให้บริการมีผลสำคัญต่อความมั่นคงปลอดภัยของระบบสารสนเทศ เพื่อให้ทราบและตระหนักถึงภัยคุกคามที่อาจจะเกิดขึ้นกับทรัพยากรดังกล่าว รวมทั้งมีการจัดเตรียมแนวนโยบายและแนวปฏิบัติ รวมถึงแผนรองรับภัยคุกคามดังกล่าวต่อไป ซึ่งแนวความคิดในการจัดตั้งหน่วยงานกลางด้านไซเบอร์นี้ ได้รับการเห็นชอบแล้วจากคณะกรรมการด้านความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Committee) ซึ่งได้กล่าวไปแล้วในบทที่ ๒

ในด้านของกฎหมาย ระเบียบ ข้อปฏิบัติ จะต้องมีการปรับปรุงให้ทันสมัยและสามารถบังคับใช้ได้จริง รวมถึงอาจจะต้องมีการออกกฎหมายที่รองรับการปฏิบัติของเจ้าหน้าที่ด้านความมั่นคงในการ

ดำเนินการด้านไซเบอร์ เช่นการรองรับการดักจับและตรวจสอบข้อมูลอย่างถูกกฎหมาย (Lawful Interception) อย่างไรก็ตามจะต้องมีความโปร่งใสในกระบวนการ และคำนึงถึงด้านความเป็นส่วนตัวของข้อมูล โดยไม่เข้าถึงข้อมูลส่วนตัวที่ไม่จำเป็น เพื่อไม่ให้เกิดปัญหาดังเช่น กรณีของหน่วยงานข่าวกรองของสหรัฐฯ (กล่าวไปแล้วในบทที่ ๓) นอกจากนี้จะต้องมีกฎหมายที่รองรับแนวความคิดด้านการทำ National Cyber Gateway หรือการเพิ่มขีดความสามารถในการตรวจสอบการกระทำผิดทางไซเบอร์ การโจมตีทางไซเบอร์กับทุกเส้นทางการเชื่อมต่อเครือข่ายอินเทอร์เน็ตในประเทศกับต่างประเทศ ซึ่งจะช่วยเพิ่มขีดความสามารถในการสามารถบังคับใช้กฎหมาย และการดำเนินการด้านไซเบอร์เพื่อความมั่นคงอย่างมีประสิทธิภาพ โดยการจัดทำ National Cyber Gateway ต้องคำนึงถึงประเด็นเรื่องเสรีภาพการต่อเชื่อม (Freedom of Connectivity) กับความสามารถการควบคุม (Controllability)

นอกจากนี้ยังต้องมีการสร้างความร่วมมือระหว่างหน่วยงานภาครัฐและภาคเอกชน (Public Private Partnership) เพื่อบูรณาการขีดความสามารถในการตอบสนองต่อภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ โดยการแบ่งปันทรัพยากร (คน กระบวนการ เครื่องมือ –People Process Technology) การแลกเปลี่ยนข้อมูลภัยคุกคามด้านไซเบอร์ การมีนโยบายสนับสนุนผู้ประกอบการด้าน Cybersecurity การมีความร่วมมือในด้านการยืมตัวบุคลากรระหว่างหน่วยงาน การมีกลไกสำหรับส่งเสริมการพัฒนาขีดความสามารถด้าน Cybersecurity ให้กับภาคเอกชน เช่นมาตรการทางภาษี หรือการให้ทุนสนับสนุน เป็นต้น

สำหรับแนวความคิดการปฏิบัติการสงครามสารสนเทศ ตามขีดความสามารถเฉพาะ ๓ ส่วน คือ ๑. การปฏิบัติการโจมตี ๒. การปฏิบัติการป้องกัน และ ๓. การปฏิบัติการใช้ประโยชน์จากข้อมูลและระบบสารสนเทศนั้น ในแต่ละส่วนมีสิ่งที่ต้องดำเนินการดังนี้

๑. การปฏิบัติการโจมตี (Offense)

<u>องค์บุคคล</u> การปฏิบัติการโจมตีจำเป็นต้องอาศัยบุคลากรที่มีความเชี่ยวชาญทางด้านเทคนิคเกี่ยวกับระบบสารสนเทศ และเครือข่ายสารสนเทศขั้นสูง สามารถใช้ความรู้ และเทคนิคต่างๆ ที่เกี่ยวข้องในการได้มาซึ่งจุดอ่อนของระบบหรือเครือข่ายสารสนเทศที่ต้องการทำการโจมตี การที่จะมีบุคลากรที่มีขีดความสามารถดังกล่าวจากบุคลากรภาครัฐแต่เพียงอย่างเดียวอาจไม่เพียงพอ นอกจากนั้น การปฏิบัติการโจมตีหากฝ่ายตรงข้ามตรวจพบและทราบว่าเป็นบุคลากรภาครัฐ ก็จะกระทบต่อความสัมพันธ์ระหว่างประเทศได้ง่าย แต่หากเกิดจากภาคประชาชนที่ร่วมเข้าเป็นเครือข่ายในการโจมตีเช่นเดียวกับกรณีเครือข่ายภาคประชาชนของประเทศจีนแล้ว จะเพิ่มขีดความสามารถในการโจมตีเป็นอย่างมาก และจะมีผลกระทบต่อความสัมพันธ์ระหว่างประเทศน้อยกว่าอีกด้วยอีกทั้งเพื่อให้เกิดประสิทธิภาพเชิงรุกมากยิ่งขึ้นควรมีการจัดหน่วยนักรบไซเบอร์ (Cyber Warrior) ในทางลับ โดยให้ กห. เป็นกำกับดูแล

<u>องค์วัตถุ</u> การปฏิบัติการโจมตีจำเป็นต้องมีเทคโนโลยีที่เหมาะสมและเพียงพอ ที่จะสามารถทำให้การปฏิบัติการดังกล่าวเป็นไปได้อย่างมีประสิทธิภาพ เครื่องมือที่ใช้ในปฏิบัติการ สามารถจัดหาได้หลายแบบ ทั้งเครื่องมือที่มีลิขสิทธิ์ และเครื่องมือที่ถูกพัฒนาขึ้นโดยอาศัยหลักการพัฒนาซอฟท์แวร์แบบเปิดเผย (Open Source) ซึ่งสามารถศึกษาและทำความเข้าใจการทำงานและสามารถสร้าง

ใช้ได้เอง อย่างไรก็ตามเครื่องมือทั้งสองแบบต่างก็มีข้อดีและข้อเสีย เช่นเครื่องมือที่มีลิขสิทธิ์จะมีราคาแพง การจัดหาอาจจะต้องใช้งบประมาณสูง แต่ส่วนใหญ่จะมีขีดความสามารถและการใช้งานที่ง่ายกว่าเครื่องมือที่เป็น Open Source เป็นต้น สำหรับเครื่องมือที่ใช้ในการโจมตี จะต้องมีขีดความสามารถในการค้นหาจุดอ่อนของระบบที่เราต้องการโจมตีได้ ดังนั้นจึงใช้เครื่องมือที่ใช้หลักการการค้นหาจุดอ่อน (Vulnerability Assessment) และเครื่องมือในการทดสอบการโจมตี (Penetration Test) ซึ่งใช้ในการรักษาความปลอดภัยของระบบได้ นอกจากเครื่องมือที่ใช้แล้ว ช่องทางหรือเครือข่าย และอุปกรณ์ประกอบอื่นๆ ก็มีความจำเป็น เช่น อาจจะต้องมีการร่วมมือกับภาคเอกชน เพื่อใช้ในการซ่อนพรางการโจมตี หรือใช้ช่องทางอื่นจากนอกประเทศในการโจมตี ยกตัวอย่างเช่นหากใช้เครือข่ายสารสนเทศของกองทัพไทยในการปฏิบัติการโจมตี หากฝ่ายตรงข้ามมีขีดความสามารถในการตรวจจับ จะพบว่าการโจมตีนี้เป็นการดำเนินการของกองทัพไทย ซึ่งอาจจะส่งผลกระทบต่อภาพลักษณ์ และความสัมพันธ์ระหว่างประเทศได้

<u>การบริหารจัดการ</u> การจะดำเนินการปฏิบัติการโจมตีได้ จะต้องมีแนวทาง หลักนิยมการดำเนินการที่ชัดเจน ทั้งนี้เนื่องจากการปฏิบัติการโจมตี ถือเป็นการบุกรุกทางคอมพิวเตอร์ ซึ่งในหลายประเทศ การดำเนินการดังกล่าว เป็นการดำเนินการที่ขัดต่อกฎหมาย ซึ่งในประเทศไทยเอง ก็มีกฎหมายที่จัดการกระทำดังกล่าวว่าเป็นการกระทำผิด และมีบทลงโทษที่ชัดเจน ทั้งทางอาญาและทางแพ่ง ดังนั้นหากไม่มีแนวทาง หรือหลักนิยม มาเป็นกรอบการดำเนินการที่ชัดเจน เจ้าหน้าที่ที่ปฏิบัติหน้าที่ในการโจมตีระบบสารสนเทศ อาจถูกดำเนินคดีตามกฎหมายได้ นอกจากนี้ในแง่ของการบริหารจัดการ การดำเนินการดังกล่าวควรมีการกำหนดโครงสร้างหน้าที่ ความรับผิดชอบให้ชัดเจน เนื่องจากการปฏิบัติการโจมตีทางระบบสารสนเทศ เป็นส่วนหนึ่งของการปฏิบัติการข่าวสาร ซึ่งมีหน่วยที่เกี่ยวข้องเป็นจำนวนมาก ควรจะต้องมีการกำหนดบทบาท และแนวทางการปฏิบัติที่สามารถทำงานได้อย่างประสานสอดคล้องกันจากทุกกระทรวงที่เกี่ยวข้อง รวมทั้งเจ้าหน้าที่ที่ดำเนินการ ควรจะได้รับการบรรจุให้ปฏิบัติงานดังกล่าวโดยอาศัยแนวทางการย้ายบรรจุที่ต่างจากข้าราชการในสายงานปกติ เนื่องจากต้องอาศัยเวลาในการพัฒนาทักษะให้สามารถปฏิบัติงานในหน้าที่ดังกล่าวได้ ในส่วนขององค์ความรู้ด้านการปฏิบัติการโจมตีจำเป็นจะต้องมีแนวทางการพัฒนาและบริหารจัดการ ให้สามารถเป็นแหล่งรวบรวมความรู้ เพื่อให้เจ้าหน้าที่ที่รับผิดชอบการปฏิบัติหน้าที่ในด้านการโจมตี สามารถใช้ประโยชน์ และต่อยอดองค์ความรู้ด้านนี้ได้อย่างต่อเนื่อง และไม่ซ้ำซ้อน

๑. การปฏิบัติการป้องกัน (Defense)

<u>องค์บุคคล</u> การปฏิบัติการป้องกันมีความต้องการบุคลากรใน ๒ ลักษณะ คือ ผู้ใช้งานระบบทั่วไป ซึ่งอาจหมายถึงประชาชนทุกคนที่ต้องมีส่วนเกี่ยวข้องหรือใช้งานระบบสารสนเทศทั้งหมด แม้ไม่จำเป็นต้องมีความรู้ทางเทคนิคเกี่ยวกับการรักษาความปลอดภัยระบบที่ตนใช้งานมากนัก แต่จะต้องมีความรู้พื้นฐานด้านการใช้งานระบบอย่างปลอดภัย รวมถึงมีความตระหนักถึงความเสี่ยง และความเสียหายที่อาจจะเกิดขึ้นกับระบบสารสนเทศ และเครือข่ายสารสนเทศ หากมีการใช้งานที่ไม่ปลอดภัย สำหรับ

บุคลากรประเภทที่ ๒ คือผู้ที่มีหน้าที่ในการดูแลรักษาความปลอดภัยของระบบ จำเป็นต้องจะต้องมีความรู้ความเชี่ยวชาญทางเทคนิค เกี่ยวกับระบบสารสนเทศและเครือข่ายสารสนเทศใน และสามารถทราบถึงจุดอ่อนหรือความเสี่ยงของระบบ โดยอาศัยเทคนิคการค้นหาและตรวจสอบจุดอ่อนของระบบ และการทดสอบการโจมตีระบบ เพื่อให้ทราบถึงแนวทางการป้องกันรักษาความปลอดภัยให้กับระบบสารสนเทศและเครือข่ายสารสนเทศดังกล่าวได้อย่างมีประสิทธิภาพ

<u>องค์วัตถุ</u> การปฏิบัติการป้องกันจำเป็นต้องมีเครื่องมือที่เหมาะสมและเพียงพอ ที่จะสามารถทำให้การปฏิบัติการดังกล่าวเป็นไปได้อย่างมีประสิทธิภาพ การจัดหาอุปกรณ์และเครื่องมือในการป้องกันรักษาความปลดภัยระบบสารสนเทศและเครือข่ายสารสนเทศ สามารถใช้เทคนิคการป้องกันภัยเชิงลึก (Defense-in-Depth) และควรวิเคราะห์ว่า โครงสร้างพื้นฐานของประเทศใดบ้างที่เป็นสุดสำคัญ หรือจุดเสี่ยงที่อาจถูกโจมตี สมควรได้รับการป้องกัน

<u>การบริหารจัดการ</u> การดำเนินการในส่วนของการป้องกันรักษาความปลอดภัยนั้น ควรมีการกำหนดแนวทางดำเนินการ ตามเทคนิคการป้องกันภัยเชิงลึก (Defense-in-Depth) ซึ่งจะสามารถกำหนดแนวทางการจัดโครงสร้างระบบสารสนเทศและเครือข่ายสารสนเทศ ได้ตามวิธีการปฏิบัติที่เป็นเลิศเกี่ยวกับการรักษาความปลอดภัย (Information Security Best Practices) ตามลำดับความสำคัญเร่งด่วน โดยมีกฎหมายบังคับให้หน่วยงานที่มีโครงสร้างพื้นฐานที่สำคัญของประเทศต้องปฏิบัติตามวิธีการปฏิบัติที่เป็นเลิศ ที่เป็นมาตรฐานสากลและสามารถลดความเสี่ยง หรือความเสียหายที่เกิดจากการถูกโจมตีได้

๓. การปฏิบัติการใช้ประโยชน์จากข้อมูลและระบบสารสนเทศ (Exploitation)

<u>องค์บุคคล</u> บุคลากรหรือเจ้าหน้าที่ที่จะทำหน้าที่ในการปฏิบัติการใช้ประโยชน์จากข้อมูลและระบบสารสนเทศ จำเป็นที่จะต้องมีความรู้ทางเทคนิคที่เกี่ยวกับระบบสารสนเทศและเครือข่ายสารสนเทศของฝ่ายตรงข้าม คล้ายกับเจ้าหน้าที่ที่ปฏิบัติการโจมตี นอกจากนี้ยังต้องมีขีดความสามารถในการวิเคราะห์ข้อมูลซึ่งอยู่ในรูปแบบภาษาต่างชาติ และมีความรู้ด้านการจารกรรม

<u>องค์วัตถุ</u> การปฏิบัติการใช้ประโยชน์จากข้อมูลและระบบสารสนเทศ จำเป็นต้องมีการดำเนินการกับข้อมูลที่รวบรวมได้อย่างต่อเนื่อง ดังนั้นจึงจำเป็นต้องมีระบบฐานข้อมูลที่สามารถรวบรวมและวิเคราะห์ข้อมูล เพื่อสามารถที่จะวิเคราะห์หาจุดอ่อนของระบบสารสนเทศและเครือข่ายสารสนเทศของฝ่ายตรงข้าม และสามารถนำข้อมูลระบบสารสนเทศ และจุดอ่อนของระบบมาจัดทำเป็นบัญชีเป้าหมายทางระบบสารสนเทศได้

<u>การบริหารจัดการ</u> จะคล้ายกับการปฏิบัติการเชิงรุก คือต้องมีแนวทางการใช้งาน และหลักนิยม เพื่อเป็นกรอบการดำเนินการที่ชัดเจนให้กับเจ้าหน้าที่ที่ปฏิบัติหน้าที่ในการใช้ประโยชน์จากข้อมูลและระบบสารสนเทศ เพื่อให้สามารถใช้เทคนิคการตรวจสอบจุดอ่อนและทดสอบการโจมตีในการเก็บรวบรวมข้อมูล รวมทั้งเจ้าหน้าที่ที่ดำเนินการ ควรจะได้รับการบรรจุให้ปฏิบัติงานดังกล่าว

บทที่ ๕
สรุปและข้อเสนอแนะ

สรุป

การที่ระบบสารสนเทศและเครือข่ายสารสนเทศถูกนำมาใช้ประโยชน์ และมีความสำคัญมากขึ้นในกระบวนการการทำงานต่างๆ ส่งผลให้ระบบสารสนเทศและเครือข่ายสารสนเทศเหล่านี้กลายเป็นเป้าหมายของการโจมตีและการใช้ประโยชน์ในทางที่ไม่เหมาะสม ทั้งจากผู้ไม่หวังดีและศัตรูฝ่ายตรงข้าม โดยเฉพาะระบบสารสนเทศและเครือข่ายสารสนเทศที่เกี่ยวข้องกับโครงสร้างพื้นฐานหลักของชาติ (National Critical Infrastructure) การโจมตีต่อระบบสารสนเทศหรือที่เรียกว่าการโจมตีทางไซเบอร์นั้นมีความแตกต่างจากการโจมตีของสงครามตามรูปแบบ (Traditional Warfare) ทั้งนี้เนื่องจากระบบสารสนเทศและเครือข่ายสารสนเทศนั้นถูกสร้างในพื้นที่เสมือนที่เรียกกันว่าไซเบอร์สเปซ(Cyberspace) โดยที่ไซเบอร์สเปซนี้มีคุณลักษณะที่สำคัญได้แก่ การมีพื้นที่ไร้พรมแดน (Borderless) การเชื่อมโยงต่อกันเป็นโครงข่าย (Connected/Networked) การปรากฏทุกหนแห่ง (Ubiquitous) การเป็นพื้นที่สาธารณะ (Public/Open) ความเร็วการเดินทางของข้อมูลเท่าความเร็วแสง (Speed of Light) และความเป็นอสมมาตร (Asymmetric) เป็นต้น แต่วัตถุประสงค์ของการโจมตีเหมือนกัน คือเพื่อลดขีดความสามารถของฝ่ายตรงข้าม โดยที่เครื่องมือหรืออาวุธที่ใช้ในการโจมตีอาจเป็นแค่ซอฟต์แวร์ขนาดเพียงครึ่งเมกะไบต์ที่อาจถูกส่งจากเครื่องคอมพิวเตอร์แบบทั่วๆไป การปฏิบัติการกระทำจากที่ไหนหรือเวลาใดก็ได้ ผลของการปฏิบัติการอาจกระทบในวงกว้างและแพร่กระจายอย่างรวดเร็วด้วย

การโจมตีทางไซเบอร์อาจเกิดจากภายในองค์กรเอง ซึ่งมีสาเหตุจากกระบวนการควบคุมไม่สอดคล้องกับนโยบายด้านการรักษาความมั่นคงปลอดภัยขององค์กร ขาดกระบวนการตรวจสอบที่เหมาะสม หรือการโจมตีทางไซเบอร์อาจเกิดจากผู้ไม่หวังดีภายนอกองค์กร เพื่อหวังผลประโยชน์จากความเสียหายของระบบสารสนเทศ ซึ่งหลักการและแนวทางการพัฒนาขีดความสามารถทางไซเบอร์เพื่อป้องกันและรับมือกับการโจมตีที่หลายประเทศใช้กัน เช่น การป้องกันภัยแบบเชิงลึก (Defense-in-Depth) การปฏิบัติตามวิธีการปฏิบัติที่เป็นเลิศที่เกี่ยวข้องกับการรักษาความปลอดภัยระบบสารสนเทศ (Information Security Best Practices) การตรวจสอบหาจุดอ่อนของระบบ (Vulnerability Assessment – VA) การทดสอบเจาะระบบ (Penetration Test – PENTEST) เป็นต้น

การโจมตีไซเบอร์จากภายนอกมีพัฒนาการที่รวดเร็ว อาจอยู่ในรูปแบบของการปล่อยไวรัส โทรจัน หรือสปายแวร์ ซึ่งเรียกรวมว่ามัลแวร์ นอกจากนั้นอาจใช้ขีดความสามารถไซเบอร์เป็นกำลัง

อำนาจแห่งชาติเช่น การลักลอบดักรับและเก็บรวบรวมข้อมูลของหน่วยงานความมั่นคง การโจมตีทางไซเบอร์โดยหน่วยงานของรัฐบาล การโจมตีเพื่อลดขีดความสามารถทางการทหาร เป็นต้น ซึ่งหน่วยงานทางทหารของสหรัฐอเมริกาได้มีการปรับตัวเพื่อรองรับภัยคุกคามใหม่นี้ โดยแนวคิดการปฏิบัติการสงครามไซเบอร์ที่บูรณาการสงครามควบคุมบังคับบัญชา (Command and Control Warfare) และสงครามข้อมูลข่าวสาร (Information Warfare) เข้าด้วยกัน ที่ประกอบด้วยการบูรณาการการปฏิบัติทางทหารสาขาต่างๆ เข้าด้วยกัน ประกอบด้วย การปฏิบัติการทางยุทธการ การปฏิบัติการด้านมวลชน (Public Affairs) การปฏิบัติการจิตวิทยา (Psychological Operations) ร่วมกับการปฏิบัติการสารสนเทศ เช่นการปฏิบัติการสงครามเครือข่าย (Computer Network Operation) ที่ประกอบด้วยการดำเนินการ ๓ ส่วน คือ การปฏิบัติการโจมตี (Computer Network Attack – CNA) เป็นการปฏิบัติการทางรุก โดยใช้เครือข่ายสารสนเทศ ในการ ขัดขวาง ปฏิเสธ ลิดรอน หรือ ทำลายข้อมูลข่าวสารที่ถูกเก็บอยู่ในระบบสารสนเทศอุปกรณ์ที่เชื่อมต่อกับเครือข่ายสารสนเทศของฝ่ายตรงข้าม ซึ่งส่งผลให้ฝ่ายตรงข้ามไม่สามารถใช้ประโยชน์จากข้อมูลข่าวสาร ระบบสารสนเทศ และเครือข่ายสารสนเทศในการปฏิบัติภารกิจ และอาจส่งผลกระทบต่อภารกิจของฝ่ายตรงข้ามในที่สุดการปฏิบัติการป้องกัน (Computer Network Defense – CND) เป็นการปฏิบัติการทางรับ โดยการป้องกัน ดำรงรักษาขีดความสามารถในการใช้ประโยชน์จากข้อมูลข่าวสารที่ถูกเก็บอยู่ในระบบสารสนเทศ อุปกรณ์ที่เชื่อมต่อกับเครือข่ายสารสนเทศของฝ่ายเราจากการปฏิบัติการโจมตีของฝ่ายตรงข้าม และการปฏิบัติการใช้ประโยชน์จากข้อมูลและระบบสารสนเทศ (Computer Network Exploitation – CNE) เป็นการปฏิบัติการที่สร้างขีดความสามารถในการหาข่าว หรือข้อมูลที่เกี่ยวข้องกับ ระบบสารสนเทศ หรือเครือข่ายสารสนเทศของฝ่ายตรงข้ามเพื่อใช้ประโยชน์ในการโจมตี หรือการปฏิบัติการทางทหารอื่นๆในอนาคต

ศักยภาพด้านสงครามไซเบอร์ของประเทศไทยในปัจจุบัน เป็นการดำเนินการแบบแยกส่วน เพื่อรองรับภารกิจของแต่ละกระทรวง หรือหน่วยงาน ไม่สามารถบูรณาการกันได้ ทำให้ขาดศักยภาพในการดำเนินการสงครามไซเบอร์ทั้งในทางรุก และในทางรับ นอกจากนั้นนโยบายการเปลี่ยนแปลงไปสู่การเป็นรัฐบาลอิเล็กทรอนิกส์ ทำให้ระบบสารสนเทศกลายเป็นโครงสร้างพื้นฐานหลักอันหนึ่งของประเทศ ระบบสารสนเทศทุกกระทรวง ถูกจัดเก็บรวมในที่เดียวกัน ทำให้เป็นจุดอ่อนหรือเป็นเป้าหมายที่สะดวกต่อการทำลายทางกายภาพ หรือการโจมตีทางเครือข่ายของฝ่ายตรงข้าม สำหรับนโยบายด้านความมั่นคงแห่งชาติยังไม่มีแนวทางสงครามไซเบอร์เป็นการเฉพาะ แต่ก็มีการตระหนักถึงภัยคุกคามที่เปลี่ยนแปลงไป แนวทางการดำเนินการด้านความมั่นคงในภาพรวมคือ การพัฒนาศักยภาพของชาติในการป้องกันประเทศด้วยการผนึกกำลังจากทุกฝ่าย ทั้งภาครัฐ ภาคเอกชน และภาคประชาชน การพัฒนาความร่วมมือทางทหารและความเข้าใจอันดีกับกองทัพของประเทศเพื่อนบ้านและส่งเสริมและประสานความร่วมมือกับต่างประเทศในด้านความมั่นคง

ศักยภาพด้านสงครามไซเบอร์ในประเทศไทย ในเชิงรับยังอยู่ในระดับต่ำ ซึ่งดูได้จากตัวชี้วัด เช่น จำนวนบุคลากรที่มีความเชี่ยวชาญด้านไซเบอร์ ปริมาณการถูกโจมตีทางไซเบอร์ที่มีแนวโน้มที่เพิ่มขึ้นอย่างต่อเนื่อง สำหรับศักยภาพสงครามไซเบอร์เชิงรุกยังอยู่ในขั้นการเริ่มต้น ซึ่งเห็นได้จากจำนวนการจัดสัมมนา นิทรรศการ การจัดกิจกรรมการการแข่งขันที่เกี่ยวกับไซเบอร์ที่มีมากยิ่งขึ้น

การพัฒนาขีดความสามารถการปฏิบัติการสงครามไซเบอร์ของประเทศไทย จำเป็นต้องดำเนินการทั้งด้านองค์บุคคล องค์วัตถุ และการบริหารจัดการ ดังนี้

Finding	**แนวทางการพัฒนา (Solution)**
นโยบายด้านความมั่นคงแห่งชาติยังไม่มีแนวทางสงครามไซเบอร์เป็นการเฉพาะ	จัดให้มีหน่วยงานความมั่นคงด้านสงครามไซเบอร์กลางเป็นการเฉพาะ เช่น National Cyber Security Agency และ National Cyber Security Committee เพื่อกำหนดนโยบายด้านสงครามไซเบอร์ที่ชัดเจนและเป็นการเฉพาะ
• หน่วยงานไม่บูรณาการ • หน่วยงานทางการทหารมีการจัดหน่วยงานเพื่อรองรับการปฏิบัติการสงครามไซเบอร์ที่ชัดเจนและมีกิจกรรมมากขึ้นและต่อเนื่อง	บูรณาการการปฏิบัติการสงครามไซเบอร์ระหว่างหน่วยงานภาครัฐ และจัดให้มีหน่วยงานความมั่นคงด้านสงครามไซเบอร์กลางเป็นการเฉพาะ เช่น National Cyber Security Agency โดยมี กห. เป็นหน่วยงานหลักในการขับเคลื่อน
ขาดแคลนผู้เชี่ยวชาญด้านไซเบอร์(Cyber Expert)	• ยกระดับความรู้ความสามารถของบุคลากรในสายวิชาชีพความมั่นคงปลอดภัยสารสนเทศ ให้อยู่ในระดับสากล รวมทั้งการสร้างเส้นทางความก้าวหน้าในสายอาชีพ พร้อมค่าตอบแทนที่เหมาะสม • พัฒนาผู้เชี่ยวชาญระดับต้นจากสถาบันการศึกษาในประเทศ • ประสานมิตรประเทศในการสร้างผู้เชี่ยวชาญ • ปรับปรุงหลักสูตรการศึกษา ตั้งแต่ระดับประถมจนถึงระดับอุดมศึกษา โดยการแทรกเนื้อหาภัยคุกคามทางไซเบอร์ • พัฒนาครูผู้สอน เพื่อให้สามารถปลูกจิตสำนึกด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับเยาวชน
Finding	**แนวทางการพัฒนา (Solution)**
ศักยภาพเชิงรับในภาพรวมยังอยู่ในระดับ	• แลกเปลี่ยนบทเรียนระหว่างองค์กร

ต่ำ ***เว้นภาคการเงินและธนาคารมีความสามารถในเกณฑ์ยอมรับได้***	● ปลูกจิตสำนึกด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในองค์กร (ยึดหลัก Information Security Best Practices) ● ปลูกจิตสำนึกด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับประชาชน โดยเฉพาะเยาวชน ● Cyber War Simulator (โดยเน้น VA + PENTEST)
ศักยภาพเชิงรุกอยู่ในขั้นการเริ่มต้น	● จัดตั้งนักรบไซเบอร์ (ในทางลับ) ● สร้างเครือข่ายภาคประชาชนที่ร่วมในการโจมตีเชิงรุก (Attack Network Base) ● พัฒนาหลักนิยมการดำเนินการปฏิบัติการทางไซเบอร์ (Cyber Warfare Doctrine) ที่ชัดเจนตามเทคนิคการป้องกันภัยเชิงลึก และตามวิธีการปฏิบัติที่เป็นเลิศเกี่ยวกับการรักษาความปลอดภัย
หลาย ISP (Multiple Gateway)	จัดทำ National Cyber Gateway
Thailand is one of the cyber-riskiest countries in the world.	● ปรับปรุงกฎหมาย ระเบียบ ข้อปฏิบัติ ให้ทันสมัย รวมถึงอาจจะต้องมีการออกกฎหมายที่รองรับการปฏิบัติของเจ้าหน้าที่ด้านความมั่นคงในการดำเนินการด้านไซเบอร์ เช่น การรองรับการดักจับและตรวจสอบข้อมูลอย่างถูกกฎหมาย (Lawful Interception) ● มีกฎหมายที่รองรับแนวความคิดด้านการทำ National Cyber Gateway หรือการเพิ่มขีดความสามารถในการตรวจสอบการกระทำผิดทางไซเบอร์ การโจมตีทางไซเบอร์ กับทุกเส้นทางการเชื่อมต่อเครือข่ายอินเทอร์เน็ตในประเทศกับต่างประเทศ
	● ส่งเสริมให้องค์กร/หน่วยงานตระหนักถึงภัยคุกคามทางไซเบอร์ โดยเริ่มตั้งแต่ขั้นออกแบบระบบ ทำความเข้าใจแนวคิด Cyber Security Defense-in-Depth
Finding	**แนวทางการพัฒนา (Solution)**
การวิจัยด้าน Cyber Security มีน้อย	● สนับสนุนการวิจัยและพัฒนาโดยเฉพาะด้าน

	ซอฟต์แวร์ เช่น ระบบจำลองยุทธ์ทางสงครามไซเบอร์ (Cyber Security Simulator) ● พิจารณาใช้เครื่องมือค้นหาจุดอ่อน และเครื่องมือในการทดสอบการโจมตี ที่ถูกพัฒนาขึ้นโดยอาศัยหลักการพัฒนาซอฟท์แวร์แบบเปิดเผย (Open Source) ● สร้างความร่วมมือระหว่างหน่วยงานภาครัฐและภาคเอกชน (Public Private Partnership) ด้านการวิจัยภัยคุกคามทางไซเบอร์
แนวโน้มการโจมตีมากขึ้น โดยไม่รู้ตัว	● สร้างความตระหนักในความเสี่ยงต่างๆ ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แก่ประชาชนทั่วไป ● มีเครื่องมือที่เหมาะสมและเพียงพอ สามารถปฏิบัติการการป้องกันภัยเชิงลึกได้ พร้อมวิเคราะห์ Critical Infrastructure ของประเทศ ● มีระบบฐานข้อมูลที่สามารถรวบรวมและวิเคราะห์ข้อมูลเพื่อวิเคราะห์หาจุดอ่อนของระบบสารสนเทศและเครือข่ายสารสนเทศของฝ่ายตรงข้าม พร้อมจัดทำเป็นบัญชีเป้าหมายทางระบบสารสนเทศ
Cyberspace: Borderless and Connected	● สร้างความร่วมมือระหว่างหน่วยงานภาครัฐและภาคเอกชน เพื่อบูรณาการขีดความสามารถในการตอบสนองต่อภัยคุกคามทางไซเบอร์ ● แสวงความร่วมมือกับประเทศเพื่อนบ้านในภูมิภาค หรือกับประเทศพันธมิตรที่มีความรู้ ความสามารถและประสบการณ์

องค์บุคคล

ผลิตผู้เชี่ยวชาญด้านสงครามไซเบอร์ที่มีมาตรฐานสามารถปฏิบัติงานได้อย่างเพียงพอ โดยการส่งเสริมจากภาครัฐ

จัดตั้งหน่วยนักรบไซเบอร์ (Cyber Warrior) ในทางลับ โดยให้ กห. เป็นกำกับดูแล เพื่อให้เกิดประสิทธิภาพเชิงรุกมากยิ่งขึ้น

มีการจัดทำมาตรฐานวิชาชีพ เพื่อยกระดับความรู้ความสามารถของบุคลากรในสายวิชาชีพความมั่นคงปลอดภัยสารสนเทศ ให้อยู่ในระดับสากล ร่วมทั้งการสร้างเส้นทางความก้าวหน้าในสายอาชีพพร้อมค่าตอบแทนที่เหมาะสมกับระดับความรู้ความสามารถ ควบคู่กับการพัฒนากระบวนการรับรองและการกำกับดูแลมาตรฐานวิชาชีพภายในประเทศ

พัฒนาผู้เชี่ยวชาญระดับต้นจากสถาบันการศึกษาในประเทศ เช่นมหาวิทยาลัยต่างๆ และจากหน่วยงานวิจัยระดับชาติ รวมทั้งประสานความร่วมมือกับมิตรประเทศในการพัฒนาผู้เชี่ยวชาญด้านสงครามไซเบอร์

มีแผนการให้ความรู้อย่างต่อเนื่องและมีองค์ความรู้ที่เข้าถึงได้แก่ประชาชนทั่วไป เพื่อให้มีความตระหนักในความเสี่ยงต่างๆ ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

ปรับปรุงหลักสูตรการศึกษา ตั้งแต่ระดับประถมจนถึงระดับอุดมศึกษา โดยมีการสอดแทรกเนื้อหาที่เกี่ยวกับภัยคุกคามทางไซเบอร์และวิธีการป้องกันภัยดังกล่าวเบื้องต้น

พัฒนาครูผู้สอน เพื่อให้สามารถปลูกจิตสำนึกด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับเยาวชนได้อย่างมีประสิทธิภาพ

สร้างเครือข่ายภาคประชาชนที่ร่วมในการโจมตีเชิงรุกเพื่อเพิ่มขีดความสามารถในการโจมตีและลดผลกระทบต่อความสัมพันธ์ระหว่างประเทศ

องค์วัตถุ

รัฐบาลสนับสนุนการวิจัยและพัฒนาเทคโนโลยีที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ โดยเฉพาะด้านซอฟต์แวร์ เช่น ระบบจำลองยุทธ์ทางสงครามไซเบอร์

พิจารณาใช้เครื่องมือค้นหาจุดอ่อน (Vulnerability Assessment) และเครื่องมือในการทดสอบการโจมตี (Penetration Test) ที่ถูกพัฒนาขึ้นโดยอาศัยหลักการพัฒนาซอฟท์แวร์แบบเปิดเผย (Open Source) ซึ่งมีราคาไม่แพง โดยร่วมมือกับภาคเอกชน เพื่อใช้ในการซ่อนพรางการโจมตี ยกตัวอย่างเช่นหากใช้เครือข่ายสารสนเทศของกองทัพไทย ในการปฏิบัติการโจมตี หากฝ่ายตรงข้ามมีขีดความสามารถในการตรวจจับ จะพบว่าการโจมตีนี้เป็นการดำเนินการของกองทัพไทย ซึ่งอาจจะส่งผลกระทบต่อภาพลักษณ์ และความสัมพันธ์ระหว่างประเทศได้

มีเครื่องมือที่เหมาะสมและเพียงพอ ที่จะสามารถทำให้การปฏิบัติการการป้องกันภัยเชิงลึก (Defense-in-Depth) ได้ พร้อมวิเคราะห์โครงสร้างพื้นฐานของประเทศ เพื่อหาสุดสำคัญ หรือจุดเสี่ยงที่อาจถูกโจมตี สมควรได้รับการป้องกัน

มีระบบฐานข้อมูลที่สามารถรวบรวมและวิเคราะห์ข้อมูล เพื่อสามารถที่จะวิเคราะห์หาจุดอ่อนของระบบสารสนเทศและเครือข่ายสารสนเทศของฝ่ายตรงข้าม และสามารถนำข้อมูลระบบสารสนเทศ และจุดอ่อนของระบบมาจัดทำเป็นบัญชีเป้าหมายทางระบบสารสนเทศได้

การบริหารจัดการ

บูรณาการการปฏิบัติการสงครามไซเบอร์ระหว่างหน่วยงานภาครัฐให้สามารถประสานความร่วมมือในการป้องกันได้อย่างมีประสิทธิภาพ และจัดให้มีหน่วยงานความมั่นคงด้านสงครามไซเบอร์กลางเป็นการเฉพาะ เช่น National Cyber Security Agency ที่มีโครงสร้างการบริหารงานระดับชาติ พร้อมบทบาทหน้าที่ที่ชัดเจน เพื่อการบัญชาการ การประสานความร่วมมือ กำหนดขั้นตอนการดำเนินงาน ในการส่งเสริมสนับสนุน มีอำนาจสั่งการ ลงโทษ รับรอง กำกับ ตรวจสอบ ประเมินผล

ปรับปรุงกฎหมาย ระเบียบ ข้อปฏิบัติ ให้ทันสมัยและสามารถบังคับใช้ได้จริง รวมถึงอาจจะต้องมีการออกกฎหมายที่รองรับการปฏิบัติของเจ้าหน้าที่ด้านความมั่นคงในการดำเนินการด้านไซเบอร์ เช่นการรองรับการดักจับและตรวจสอบข้อมูลอย่างถูกกฎหมาย (Lawful Interception)

มีกฎหมายที่รองรับแนวความคิดด้านการทำ National Cyber Gateway หรือการเพิ่มขีดความสามารถในการตรวจสอบการกระทำผิดทางไซเบอร์ การโจมตีทางไซเบอร์ กับทุกเส้นทางการเชื่อมต่อเครือข่ายอินเทอร์เน็ตในประเทศกับต่างประเทศ

มีการสร้างความร่วมมือระหว่างหน่วยงานภาครัฐและภาคเอกชน (Public Private Partnership) เพื่อบูรณาการขีดความสามารถในการตอบสนองต่อภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ โดยการแบ่งปันทรัพยากร (คน กระบวนการ เครื่องมือ–People Process Technology) การแลกเปลี่ยนข้อมูลภัยคุกคามด้านไซเบอร์ การมีนโยบายสนับสนุนผู้ประกอบการด้าน Cybersecurity การมีความร่วมมือในด้านการยืมตัวบุคลากรระหว่างหน่วยงาน การมีกลไกสำหรับส่งเสริมการพัฒนาขีดความสามารถด้าน Cybersecurity ให้กับภาคเอกชน เช่นมาตรการทางภาษี หรือการให้ทุนสนับสนุนเป็นต้น

มีแนวทาง หลักนิยม การดำเนินการปฏิบัติการทางไซเบอร์ที่ชัดเจนตามเทคนิคการป้องกันภัยเชิงลึก (Defense-in-Depth) และตามวิธีการปฏิบัติที่เป็นเลิศเกี่ยวกับการรักษาความปลอดภัย (Information Security Best Practices)

ข้อเสนอแนะ

ทั้งนี้เนื่องจากไซเบอร์สเปซมีคุณลักษณะการมีพื้นที่ไร้พรมแดน การเชื่อมโยงต่อกันเป็นโครงข่าย การปรากฏทุกหนแห่ง การเป็นพื้นที่สาธารณะ การที่ข้อมูลถูกส่งด้วยความเร็วแสง (Speed of Light) และความเป็นอสมมาตร ทำให้ภัยคุกคามจากไซเบอร์สเปซ นับวันจะมีความสลับซับซ้อน ทวีความรุนแรงมากขึ้น เป็นภัยคุกคามที่กระทบต่อทั้งบุคคลและสาธารณะ ดังนั้นการรับมือกับภัยคุกคามรูปแบบใหม่นี้ต้องอาศัยความร่วมมือจากหลายภาคส่วนทั้งภาครัฐและภาคเอกชน การสร้างความตระหนักรู้ให้ทุกภาคส่วนมีความจำเป็นอย่างยิ่ง ตราบใดที่เทคโนโลยีสารสนเทศและการสื่อสารเป็นส่วนหนึ่งของชีวิตประจำวันของบุคคลและของหน่วยงานในทุกระดับแล้ว ไซเบอร์สเปซก็จะเข้ามาเกี่ยวข้องอย่างหลีกเลี่ยงไม่ได้

เพื่อให้การศึกษาด้านภัยคุกคามไซเบอร์สเปซมีความต่อเนื่องและครอบคลุมมากยิ่งขึ้น หัวข้อการวิจัยที่น่าสนใจและสมควรดำเนินการต่อเนื่องประกอบด้วย

๑. การศึกษารูปแบบและโครงสร้างหน่วยงานความมั่นคงด้านสงครามไซเบอร์กลางระดับชาติ หรือ National Cyber Security Agency (NCSA) ที่เหมาะสมและสอดคล้องกับการบริหารจัดการของประเทศไทย

๒. การศึกษาแนวทางการจัดทำ National Cyber Gateway ที่มีเสรีภาพในการต่อเชื่อม (Freedom of Connectivity) แต่ความสามารถควบคุม (Controllability) ได้ในมิติด้านความมั่นคง

๓. การวิจัยเพื่อศึกษาความตระหนักรู้ของประชาชนเกี่ยวกับภัยคุกคามไซเบอร์สเปซ เพื่อกำหนดแนวทางในการพัฒนาขีดความสามารถของคนในชาติต่อไป

๔. การศึกษาแนวทางการสร้างความร่วมมือระหว่างประเทศเพื่อรองรับภัยคุกคามไซเบอร์สเปซ

บรรณานุกรม

ภาษาไทย

วารสาร

กองทัพอากาศสหรัฐอเมริกา, Air Force Doctrine Document 3 – 12 : Cyberspace Operations, 15 กรกฎาคม2010

สัมภาษณ์

ไชยกร อภิวัฒโนกุล, สัมภาษณ์, ๔ มิ.ย.๕๗

ปริญญา หอมอเนก, สัมภาษณ์, ๔ มิ.ย.๕๗

พล.ท.บรรเจิด เทียนทองดี, สัมภาษณ์, ๖ มิ.ย.๕๗

สุรางคณา วายุภาพ, สัมภาษณ์, ๙ มิ.ย.๕๗

ฐานข้อมูลอิเล็คทรอนิคส์

ธงชัย ศิลปวรางกูร, “CryptoLocker: เรื่องเก่าที่ถูกเอามาเล่าใหม่”, เข้าถึงได้จาก :https://www.thaicert.or.th/papers/technical/2013/pa2013te011.html เข้าถึงเมื่อ 15 พ.ค.57

วิศัลย์ ประสงค์สุข และคณะ, “Social Engineering”, ThaiCERT, เข้าถึงได้จาก : https://www.thaicert.or.th/papers/general/2012/pa2012ge017.html เข้าถึงเมื่อ 27 ก.พ.57

วิศัลย์ ประสงค์สุข, เสฏฐวุฒิ แสนนาม และพรพรหม ประภากิตติกุล, ThaiCERT, เข้าถึงได้จาก : https://www.thaicert.or.th/papers/general/2012/pa2012ge017.html เข้าถึงเมื่อ 20 พ.ค.57

Bangkok Post, “ICT plans national gateway to curb abuse of internet”, เข้าถึงได้จาก : http://www.bangkokpost.com/news/politics/412124/ict-plans-national-gateway-to-curb-abuse-of-internet เข้าถึงเมื่อ 10 มิ.ย.57

Basil Cupa, “Trojan Horse Resurrected: On the Legality of the Use of Government Spyware (Govware)”, LISS 2013, หน้า 419-428

BloombergBusinessweek, The Management Blog, “Edward Snowden and the NSA: A Lesson About

Insider Threat", เข้าถึงได้จาก
: http://www.businessweek.com/articles/2013-07-03/edward-snowden-and-the-nsa-a-lesson-in-the-insider-threat เข้าถึงเมื่อ 26 ก.พ.57

Council of Europe, "Convention on Cybercrime", เข้าถึงได้จาก
: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htmเข้าถึงเมื่อ 10 มิ.ย.57

DARPA: Information Innovation Office, "Cyber-Insider Threat (CINDER)", เข้าถึงได้จาก
: http://www.darpa.mil/Our_Work/I2O/Programs/Cyber-Insider_Threat_%28CINDER%29.aspx เข้าถึงเมื่อ 26 ก.พ.57

Department of Defense, "Annual Report to Congress", เข้าถึงได้จาก
: http://www.defense.gov/pubs/2013_china_report_final.pdf เข้าถึงเมื่อ 20 พ.ค.57

Department of Justice, "What is the USA Patriot", เข้าถึงได้จาก
: http://www.justice.gov/archive/ll/highlights.htm เข้าถึงเมื่อ 10 มิ.ย.57

Ecker Clint, "Massive spyware-based identity theft ring uncovered", ArsTechnica, เข้าถึงได้จาก
: http://arstechnica.com/news.ars/post/20050805-5175.html เข้าถึงเมื่อ 15 พ.ค.57

Federal Judicial Center, "Foreign Intelligence Surveillance Court", เข้าถึงได้จาก
: http://www.fjc.gov/history/home.nsf/page/courts_special_fisc.html เข้าถึงเมื่อ 10 มิ.ย.57

Forbes.com, "Humans: The Weakest Link In Information Security", เข้าถึงได้จาก
: http://www.forbes.com/sites/ciocentral/2011/11/03/humans-the-weakest-link-in-information-security/ เข้าถึงเมื่อ 27 ก.พ.57

"Kaspersky Lab statistics: attacks involving finicial malware rise to 28 million in 2013", เข้าถึงได้จาก
: http://www.kaspersky.com/about/news/virus/2014/ Kaspersky-Lab-statistics-attacks-involving-financial-malware-rise-to-28-million-in-2013 เข้าถึงเมื่อ 15 พ.ค.57

Madiant,APT1: Exposing One of China's Cyber Espionage Units, เข้าถึงได้จาก
: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf เข้าถึงเมื่อ 10 พ.ค.57

N. Falliere and others, "W32.Stuxnet Dossier, February 2011", เข้าถึงได้จาก
:http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf เข้าถึงเมื่อ 10 พ.ค.57

NIST, "Trends for the future: Insider Threats", เข้าถึงได้จาก
: http://csrc.nist.gov/publications/nistir/threats/subsubsection3_4_4_2.html, เข้าถึงเมื่อ 26 ก.พ.57

SC Magazine, "China, U.S. agree to work together on cyber security", http://www.scmagazine.com/china-us-agree-to-work-together-on-cyber-security/article/288948/?DCMP=EMC-SCUS_Newswire เข้าถึงเมื่อ 10 พ.ค.57

Thai CERT, "APT ภัยคุกคามใหม่หรือแค่ชื่อใหม่ของภัยเดิม", เข้าถึงได้จาก
: https://www.thaicert.or.th/papers/technical/2011/pa2011te002.html เข้าถึงเมื่อ 20 พ.ค.57

"Thai CERT: รู้จักและป้องกันภัยจาก Website Defacement", เข้าถึงได้จาก
: https://www.thaicert.or.th/papers/technical/2011/pa2011te004.html เข้าถึงเมื่อ 15 พ.ค.57

The Register, "Chinese Army: US hacks us so much, I'm amazed you can read this", เข้าถึงได้จาก
: http://www.theregister.co.uk/2013/02/28/china_accuses_us_of_hacking เข้าถึงเมื่อ 10 พ.ค.57

"The Robert Morris Internet Worm", เข้าถึงได้จาก
: http://groups.csail.mit.edu/mac/classes/6.805/articles/morris-worm.html เข้าถึงเมื่อ 7 มี.ค.57

The United States Department of Justice, "Civil Rights Division Title III of the Civil Rights Act of 1964", เข้าถึงได้จาก: http://www.justice.gov/crt/about/spl/42usc3789d.php เข้าถึงเมื่อ 10 มิ.ย.57

"Trojan.Zbot| Symantec", เข้าถึงได้จาก
: http://www.symantec.com/security_response/writeup.jsp?docid=2010-011016-3514-99 เข้าถึงเมื่อ 15 พ.ค.57

"What is spyware?", เข้าถึงได้จาก

: http://www.microsoft.com/security/pc-security/spyware-whatis.aspx เข้าถึงเมื่อ 15 พ.ค.57

Wikipedia, "Buffer overflow", เข้าถึงได้จาก

: http://en.wikipedia.org/wiki/Buffer_overflow เข้าถึงเมื่อ 27 ก.พ.57

Wikipedia, "CryptoLocker", เข้าถึงได้จาก

: http://en.wikipedia.org/wiki/CryptoLocker เข้าถึงเมื่อ 15 พ.ค.57

Wikipedia, "Heap overflow", เข้าถึงได้จาก

: http://en.wikipedia.org/wiki/Heap_overflow เข้าถึงเมื่อ 27 ก.พ.57

Wikipedia, "Uncontrolled format string", เข้าถึงได้จาก

: http://en.wikipedia.org/wiki/Format_string_attack เข้าถึงเมื่อ 27 ก.พ.57

ภาคผนวก

ประเด็นคำถาม

๑. ท่านคิดว่าขีดความสามารถของประเทศไทยด้านสงครามไซเบอร์อยู่ในระดับใด? (ภาคเอกชน ราชการ ประชาชน อื่นๆ)

๒. ท่านคิดว่าขีดความสามารถด้านสงครามไซเบอร์ที่ประเทศไทยควรมี มีอะไรบ้าง? (เชิงรับ เชิงรุก องค์บุคคล องค์วัตถุ และการจัดการ)

๓. ท่านคิดว่าลักษณะของหน่วยงานที่รองรับด้านสงครามไซเบอร์ควรเป็นอย่างไร?

๔. ท่านคิดว่าบทบาทของภาคเอกชน และภาคการศึกษาควรมีอะไรบ้าง?

การสัมภาษณ์ผู้เชี่ยวชาญ

ผู้ถูกสัมภาษณ์ : ผศ.ดร. ม.ล. กุลธร เกษมสันต์
คณบดี คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยรังสิต

วันสัมภาษณ์ : ๙ มิถุนายน ๒๕๕๗

ประเด็นคำถามในการสัมภาษณ์

๑. ท่านคิดว่าขีดความสามารถของประเทศไทยด้านสงครามไซเบอร์อยู่ในระดับใด? (ภาคเอกชน ราชการ ประชาชน อื่นๆ)

- ในภาพรวมยังไม่พร้อมรับมือกับภัยคุกคามด้านนี้
- ประเทศไทยขากแคลนผู้เชี่ยวชาญด้านนี้
- องค์กรทุกภาคส่วนยังขากความตระหนักรู้

๒. ท่านคิดว่าขีดความสามารถด้านสงครามไซเบอร์ที่ประเทศไทยควรมี มีอะไรบ้าง? (เชิงรับ เชิงรุก องค์บุคคล องค์วัตถุ และการจัดการ)

a. ควรมีทั้งเชิงรับและเชิงรุก
b. พัฒนาคนให้มากที่สุด
c. เห็นด้วยกับมี National Cyber Security Agency และ National Cyber Security Committee
d. เห็นด้วยกับการมี National Gateway ด้าน Cyberspace
e. เห็นด้วยกับการมีกฎหมายที่ให้อำนาจเจ้าหน้าที่ในการติดตามหรือเฝ้าระวัง (Lawful Interception) โดยที่หน่วยบังคับใช้ต้องเป็นองค์กรอิสระ

๓. ท่านคิดว่าลักษณะของหน่วยงานที่รองรับด้านสงครามไซเบอร์ควรเป็นอย่างไร?

a. หลายหน่วยงานร่วมกัน เพราะว่าสงครามไซเบอร์เกี่ยวข้องกับหลายหน่วยงาน
b. มีกฎหมาย Lawful Interception ที่โปร่งใส ปลอดจากการเมือง
c. มี National Cyber Security Agency (NCSC) และ National Cyber Security Committee (NCSC) จากหลายหน่วยงาน โดยมีหน่วยงานทางการทหารเป็นหน่วยงานหลัก
d. เป็นหน่วยงานที่ชัดเจน ต้องมีความเป็นกลางและอิสระ

๔. ท่านคิดว่าบทบาทของภาคเอกชน และภาคการศึกษาควรมีอะไรบ้าง?

a. ภาคการศึกษา

- พัฒนาหลักสูตรด้าน Infosec และ Cybersec ที่เป็นสหวิทยาการ (ICT + เทคโนโลยีด้านอื่นๆ ด้วย)
- พัฒนา Certificate ที่ออกโดยมหาวิทยาลัย
- R&D ภาครัฐต้องให้การสนับสนุนมากๆ

การสัมภาษณ์ผู้เชี่ยวชาญ

ผู้ถูกสัมภาษณ์ : ดร.กิตติ โฆษะวิสุทธิ์
Vice Present, Security Management
ธนาคารกรุงเทพ จำกัด (มหาชน)

วันสัมภาษณ์ : ๙ มิถุนายน ๒๕๕๗

ประเด็นคำถามในการสัมภาษณ์

๑. ท่านคิดว่าขีดความสามารถของประเทศไทยด้านสงครามไซเบอร์อยู่ในระดับใด? (ภาคเอกชน ราชการ ประชาชน อื่นๆ)

- ในภาพรวมยังห่างจากมาตรฐานมาก (ISO, COBIT, ITIL)
- ภาคการศึกษายังสร้างคนไม่ได้ตามที่ตลาดต้องการ
- พ.ร.บ. คอมพิวเตอร์ถูกบิดเบือน ไม่ให้ความสนใจ
- ภาคการเงินมีความเข้มแข็งที่สุด
- ภาคประชาชนยังขาดความตระหนักรู้

๒. ท่านคิดว่าขีดความสามารถด้านสงครามไซเบอร์ที่ประเทศไทยควรมี มีอะไรบ้าง? (เชิงรับ เชิงรุก องค์บุคคล องค์วัตถุ และการจัดการ)

a. ควรมีทั้งเชิงรับและเชิงรุก
b. เน้นเรื่องกระบวนการ
c. เน้นเรื่อง R&D ด้าน Cyber Security ด้วยทั้ง HW and SW โดยเฉพาะด้านการเข้ารหัส
d. เชิงรับ/เชิงรุก
    - มี National Cyber Security Agency ที่เป็นรูปธรรมและทำงานได้ มีการขับเคลื่อนได้จริง ต้องคำนึง Control vs Freedom
    - อาจมีการทำ Multiple Gateway สำหรับด้านความมั่นคง และด้านธุรกิจ
e. เชิงรุก
    - มี Offensive Unit หรือ Cyber Warrior (ทางลับ) โดยได้รับการอบรมอย่างเข้มข้น
    - มีกฎหมายที่ให้อำนาจเจ้าหน้าที่ในการติดตามหรือเฝ้าระวัง (Lawful Interception) โดยที่ประชาชนให้การยอมรับ ต้องไม่อิงการเมือง หน่วยบังคับใช้กฎหมายเป็นกลางทางการเมือง

f. เชิงรับ
   - ให้ผู้ใช้ ผู้ดูแลระบบได้มีโอกาสฝึกฝนมากๆ
   - สร้างความตระหนักรู้ให้ผู้ใช้มากๆ

๓. ท่านคิดว่าลักษณะของหน่วยงานที่รองรับด้านสงครามไซเบอร์ควรเป็นอย่างไร?

a. หลายหน่วยงานร่วมกัน เพราะว่าสงครามไซเบอร์เกี่ยวข้องกับหลายหน่วยงาน
b. มีกฎหมาย Lawful Interception ที่โปร่งใส ปลอดจากการเมือง
c. มี National Cyber Security Agency (NCSC) จากหลายหน่วยงาน โดยมี กห. เป็นหน่วยงานหลัก
d. กสทช. เป็น Regulator มีหลักเกณฑ์ที่ชัดเจน ไม่กระทบความมั่นคงของชาติ

๔. ท่านคิดว่าบทบาทของภาคเอกชน และภาคการศึกษาควรมีอะไรบ้าง?

a. ภาคเอกชน
   - เป็นส่วนที่ติดตาม Know how ด้านนี้
   - ต้องพึ่งพาเอกชนด้านการจัดซื้อจัดหา
b. ภาคการศึกษา
   - พัฒนาหลักสูตรที่สอดคล้องกับความต้องการทุกระดับ (Short course และปริญญา)
   - สร้างนัก Cyber ที่มี Hand-on มากๆ
   - วิจัยร่วม มหาวิทยาลัย เอกชน ภาคราชการ (Co-Research) เช่น Cyber Game Simulation

การสัมภาษณ์ผู้เชี่ยวชาญ

ผู้ถูกสัมภาษณ์ : ดร.กิตติ โฆษะวิสุทธิ์
Vice Present, Security Management
ธนาคารกรุงเทพ จำกัด (มหาชน)

วันสัมภาษณ์ : ๙ มิถุนายน ๒๕๕๗

ประเด็นคำถามในการสัมภาษณ์

๑. ท่านคิดว่าขีดความสามารถของประเทศไทยด้านสงครามไซเบอร์อยู่ในระดับใด? (ภาคเอกชน ราชการ ประชาชน อื่นๆ)

- ทั้งภาครัฐและเอกชนขาดผู้นำระดับนโยบายในเรื่อง Cyber Security
- ทั้งภาครัฐและเอกชน มีการตื่นตัวด้านสงครามไซเบอร์มากขึ้น โดยดูจากตัวชี้วัด เช่น การจัดสัมมนา การจัดนิทรรศการ การจัดการแข่งขันการเจาะระบบ
- โดยภาพขีดความสามารถยังต่ำอยู่ ยกเว้นภาคการเงิน (เช่น ธนาคาร เนื่องจากลักษณะของงาน
- ภาคการเงินเน้นการป้องกันอย่างเดียว
- ด้านความมั่งคง ต้องพัฒนาทั้งเชิงรับ และรุก
- แต่ละภาคส่วนต่างคนต่างทำ ไม่มีการบูรณาการ
- ภาคประชาชนยังขาดความตระหนักรู้

๒. ท่านคิดว่าขีดความสามารถด้านสงครามไซเบอร์ที่ประเทศไทยควรมี มีอะไรบ้าง? (เชิงรับ เชิงรุก องค์บุคคล องค์วัตถุ และการจัดการ)

a. ควรมีทั้งเชิงรับและเชิงรุก
b. เน้นการพัฒนาบุคลากรให้มาก และต้องสอนจริยธรรมด้วย
c. สร้าง Human Network/Cyber Warrior Network
d. ทางการทหาร Cyber อาจนำมาใช้เป็นอาวุธได้
e. เน้นเรื่อง R&D ด้าน Cyber Security ด้วยทั้ง HW and SW โดยเฉพาะด้านการเข้ารหัส
f. เชิงรับ/เชิงรุก
   - มี National Cyber Security Agency ที่เป็นรูปธรรมและทำงานได้ มีการขับเคลื่อนได้จริง
   - การมี National Gateway สำหรับ Cyber Space เป็นเรื่อง Sensitive เป็นเรื่อง Security vs Privacy ต้อง Balance ให้ดี ต้องให้ประชาชนเข้าใจความจำเป็นด้านความมั่นคง

g. เชิงรุก
   - มี Offensive Unit หรือ Cyber Warrior (ทางลับ) โดยได้รับการอบรมอย่างเข้มข้น
   - มีกฎหมายที่ให้อำนาจเจ้าหน้าที่ในการติดตามหรือเฝ้าระวัง (Lawful Interception) โดยที่ประชาชนให้การยอมรับ

h. เชิงรับ
   - ให้ผู้ใช้ ผู้ดูแลระบบได้มีโอกาสฝึกฝนมากๆ
   - สร้างความตระหนักรู้ให้ผู้ใช้มากๆ

๓. ท่านคิดว่าลักษณะของหน่วยงานที่รองรับด้านสงครามไซเบอร์ควรเป็นอย่างไร?

a. หลายหน่วยงานร่วมกัน เพราะว่าสงครามไซเบอร์เกี่ยวข้องกับหลายหน่วยงาน
b. มีกฎหมาย Lawful Interception
c. มี National Cyber Security Agency (NCSC) จากหลายหน่วยงาน โดยมี กห. เป็นหน่วยงานหลัก

๔. ท่านคิดว่าบทบาทของภาคเอกชน และภาคการศึกษาควรมีอะไรบ้าง?

a. ภาคเอกชน
   - เป็นส่วนที่ติดตาม Know how ด้านนี้
   - ต้องพึ่งพาเอกชนด้านการจัดซื้อจัดหา

b. ภาคการศึกษา
   - พัฒนาหลักสูตรที่สอดคล้องกับความต้องการทุกระดับ (Short course และปริญญา)
   - สร้างนัก Cyber ที่มี Hand-on มากๆ
   - วิจัยร่วม มหาวิทยาลัย เอกชน ภาคราชการ

การสัมภาษณ์ผู้เชี่ยวชาญ

ผู้ถูกสัมภาษณ์ : พลโท บรรเจิด เทียนทองดี
เจ้ากรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม
สำนักงานปลัดกระทรวงกลาโหม

วันสัมภาษณ์ : ๖ มิถุนายน ๒๕๕๗

ประเด็นคำถามในการสัมภาษณ์

๑. ท่านคิดว่าขีดความสามารถของประเทศไทยด้านสงครามไซเบอร์อยู่ในระดับใด? (ภาคเอกชน ราชการ ประชาชน อื่นๆ)

- ทั้งภาครัฐและเอกชนขาดผู้นำระดับนโยบายในเรื่อง Cyber Security
- ทั้งภาครัฐและเอกชน มีการตื่นตัวด้านสงครามไซเบอร์มากขึ้น โดยดูจากตัวชี้วัด เช่น การจัดสัมมนา การจัดนิทรรศการ การจัดการแข่งขันการเจาะระบบ
- โดยภาพขีดความสามารถยังต่ำอยู่ ยกเว้นภาคการเงิน (เช่น ธนาคาร เนื่องจากลักษณะของงาน
- ภาคการเงินเน้นการป้องกันอย่างเดียว
- ด้านความมั่งคง ต้องพัฒนาทั้งเชิงรับ และรุก
- แต่ละภาคส่วนต่างคนต่างทำ ไม่มีการบูรณาการ
- ภาคประชาชนยังขาดความตระหนักรู้

๒. ท่านคิดว่าขีดความสามารถด้านสงครามไซเบอร์ที่ประเทศไทยควรมี มีอะไรบ้าง? (เชิงรับ เชิงรุก องค์บุคคล องค์วัตถุ และการจัดการ)

a. ควรมีทั้งเชิงรับและเชิงรุก
b. เน้นการพัฒนาบุคลากรให้มาก และต้องสอนจริยธรรมด้วย
c. สร้าง Human Network/Cyber Warrior Network
d. ทางการทหาร Cyber อาจนำมาใช้เป็นอาวุธได้
e. เน้นเรื่อง R&D ด้าน Cyber Security ด้วยทั้ง HW and SW โดยเฉพาะด้านการเข้ารหัส
f. เชิงรับ/เชิงรุก
   - มี National Cyber Security Agency ที่เป็นรูปธรรมและทำงานได้ มีการขับเคลื่อนได้จริง
   - การมี National Gateway สำหรับ Cyber Space เป็นเรื่อง Sensitive เป็นเรื่อง Security vs Privacy ต้อง Balance ให้ดี ต้องให้ประชาชนเข้าใจความจำเป็นด้านความมั่นคง

g. เชิงรุก
   - มี Offensive Unit หรือ Cyber Warrior (ทางลับ) โดยได้รับการอบรมอย่างเข้มข้น
   - มีกฎหมายที่ให้อำนาจเจ้าหน้าที่ในการติดตามหรือเฝ้าระวัง (Lawful Interception) โดยที่ประชาชนให้การยอมรับ

h. เชิงรับ
   - ให้ผู้ใช้ ผู้ดูแลระบบได้มีโอกาสฝึกฝนมากๆ
   - สร้างความตระหนักรู้ให้ผู้ใช้มากๆ

๓. ท่านคิดว่าลักษณะของหน่วยงานที่รองรับด้านสงครามไซเบอร์ควรเป็นอย่างไร?

a. หลายหน่วยงานร่วมกัน เพราะว่าสงครามไซเบอร์เกี่ยวข้องกับหลายหน่วยงาน
b. มีกฎหมาย Lawful Interception
c. มี National Cyber Security Agency (NCSC) จากหลายหน่วยงาน โดยมี กห. เป็นหน่วยงานหลัก

๔. ท่านคิดว่าบทบาทของภาคเอกชน และภาคการศึกษาควรมีอะไรบ้าง?

a. ภาคเอกชน
   - เป็นส่วนที่ติดตาม Know how ด้านนี้
   - ต้องพึ่งพาเอกชนด้านการจัดซื้อจัดหา

b. ภาคการศึกษา
   - พัฒนาหลักสูตรที่สอดคล้องกับความต้องการทุกระดับ (Short course และปริญญา)
   - สร้างนัก Cyber ที่มี Hand-on มากๆ
   - วิจัยร่วม มหาวิทยาลัย เอกชน ภาคราชการ

การสัมภาษณ์ผู้เชี่ยวชาญ

ผู้ถูกสัมภาษณ์ : พลโท บรรเจิด เทียนทองดี
เจ้ากรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม
สำนักงานปลัดกระทรวงกลาโหม

วันสัมภาษณ์ : ๖ มิถุนายน ๒๕๕๗

ประเด็นคำถามในการสัมภาษณ์

๑. ท่านคิดว่าขีดความสามารถของประเทศไทยด้านสงครามไซเบอร์อยู่ในระดับใด? (ภาคเอกชน ราชการ ประชาชน อื่นๆ)

- ทั้งภาครัฐและเอกชนขาดผู้นำระดับนโยบายในเรื่อง Cyber Security
- ทั้งภาครัฐและเอกชน มีการตื่นตัวด้านสงครามไซเบอร์มากขึ้น โดยดูจากตัวชี้วัด เช่น การจัดสัมมนา การจัดนิทรรศการ การจัดการแข่งขันการเจาะระบบ
- โดยภาพขีดความสามารถยังต่ำอยู่ ยกเว้นภาคการเงิน (เช่น ธนาคาร เนื่องจากลักษณะของงาน
- ภาคการเงินเน้นการป้องกันอย่างเดียว
- ด้านความมั่งคง ต้องพัฒนาทั้งเชิงรับ และรุก
- แต่ละภาคส่วนต่างคนต่างทำ ไม่มีการบูรณาการ
- ภาคประชาชนยังขาดความตระหนักรู้

๒. ท่านคิดว่าขีดความสามารถด้านสงครามไซเบอร์ที่ประเทศไทยควรมี มีอะไรบ้าง? (เชิงรับ เชิงรุก องค์บุคคล องค์วัตถุ และการจัดการ)

a. ควรมีทั้งเชิงรับและเชิงรุก
b. เน้นการพัฒนาบุคลากรให้มาก และต้องสอนจริยธรรมด้วย
c. สร้าง Human Network/Cyber Warrior Network
d. ทางการทหาร Cyber อาจนำมาใช้เป็นอาวุธได้
e. เน้นเรื่อง R&D ด้าน Cyber Security ด้วยทั้ง HW and SW โดยเฉพาะด้านการเข้ารหัส
f. เชิงรับ/เชิงรุก
   - มี National Cyber Security Agency ที่เป็นรูปธรรมและทำงานได้ มีการขับเคลื่อนได้จริง
   - การมี National Gateway สำหรับ Cyber Space เป็นเรื่อง Sensitive เป็นเรื่อง Security vs Privacy ต้อง Balance ให้ดี ต้องให้ประชาชนเข้าใจความจำเป็นด้านความมั่นคง

g. เชิงรุก
   - มี Offensive Unit หรือ Cyber Warrior (ทางลับ) โดยได้รับการอบรมอย่างเข้มข้น
   - มีกฎหมายที่ให้อำนาจเจ้าหน้าที่ในการติดตามหรือเฝ้าระวัง (Lawful Interception) โดยที่ประชาชนให้การยอมรับ

h. เชิงรับ
   - ให้ผู้ใช้ ผู้ดูแลระบบได้มีโอกาสฝึกฝนมากๆ
   - สร้างความตระหนักรู้ให้ผู้ใช้มากๆ

๓. ท่านคิดว่าลักษณะของหน่วยงานที่รองรับด้านสงครามไซเบอร์ควรเป็นอย่างไร?

a. หลายหน่วยงานร่วมกัน เพราะว่าสงครามไซเบอร์เกี่ยวข้องกับหลายหน่วยงาน
b. มีกฎหมาย Lawful Interception
c. มี National Cyber Security Agency (NCSC) จากหลายหน่วยงาน โดยมี กห. เป็นหน่วยงานหลัก

๔. ท่านคิดว่าบทบาทของภาคเอกชน และภาคการศึกษาควรมีอะไรบ้าง?

a. ภาคเอกชน
   - เป็นส่วนที่ติดตาม Know how ด้านนี้
   - ต้องพึ่งพาเอกชนด้านการจัดซื้อจัดหา

b. ภาคการศึกษา
   - พัฒนาหลักสูตรที่สอดคล้องกับความต้องการทุกระดับ (Short course และปริญญา)
   - สร้างนัก Cyber ที่มี Hand-on มากๆ
   - วิจัยร่วม มหาวิทยาลัย เอกชน ภาคราชการ

การสัมภาษณ์ผู้เชี่ยวชาญ

ผู้ถูกสัมภาษณ์ : พลเอก ภูดิท วีระศักดิ์
ประธานคณะอนุกรรมการความมั่นคงเครือข่าย
กสทช.

วันสัมภาษณ์ : ๙ มิถุนายน ๒๕๕๗

ประเด็นคำถามในการสัมภาษณ์

๑. ท่านคิดว่าขีดความสามารถของประเทศไทยด้านสงครามไซเบอร์อยู่ในระดับใด? (ภาคเอกชน ราชการ ประชาชน อื่นๆ)

- ในภาพรวมยังไม่พร้อมรับมือกับภัยคุกคามด้านนี้
- ภาคการเงิน โดยเฉพาะธนาคารมีความเข้มแข็งที่สุด
- แต่ในส่วนของหน่วยงานทางทหารได้เริ่มตื่นตัวมากขึ้นแล้ว
- ในภาพรวมประเทศไทยยังต้องการผู้เชี่ยวชาญด้านนี้อีกมาก

๒. ท่านคิดว่าขีดความสามารถด้านสงครามไซเบอร์ที่ประเทศไทยควรมี มีอะไรบ้าง? (เชิงรับ เชิงรุก องค์บุคคล องค์วัตถุ และการจัดการ)

a. ควรมีทั้งเชิงรับและเชิงรุก
b. โดยเฉพาะทางการทหารต้องพร้อมทั้ง 2 ด้าน
c. เห็นด้วยกับมี National Cyber Security Agency และ National Cyber Security Committee
d. เห็นด้วยกับการมี National Gateway ด้าน Cyberspace
e. เห็นด้วยกับการมีกฎหมายที่ให้อำนาจเจ้าหน้าที่ในการติดตามหรือเฝ้าระวัง (Lawful Interception) โดยที่หน่วยบังคับใช้ต้องเป็นองค์กรอิสระ

๓. ท่านคิดว่าลักษณะของหน่วยงานที่รองรับด้านสงครามไซเบอร์ควรเป็นอย่างไร?

a. หลายหน่วยงานร่วมกัน เพราะว่าสงครามไซเบอร์เกี่ยวข้องกับหลายหน่วยงาน
b. มีกฎหมาย Lawful Interception ที่โปร่งใส ปลอดจากการเมือง
c. มี National Cyber Security Agency (NCSC) จากหลายหน่วยงาน โดยมี กห. เป็นหน่วยงานหลัก
d. กสทช. เป็น Regulator มีหลักเกณฑ์ที่ชัดเจน ไม่กระทบความมั่นคงของชาติ

๔. ท่านคิดว่าบทบาทของภาคเอกชน และภาคการศึกษาควรมีอะไรบ้าง?

a. ภาคการศึกษา

- พัฒนาหลักสูตรด้าน Infosec และ Cybersec
- เน้นงาน R&D ระหว่างภาคเอกชนและภาคการศึกษา

การสัมภาษณ์ผู้เชี่ยวชาญ

ผู้ถูกสัมภาษณ์ : คุณสุรางคณา วายุภาพ
ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

วันสัมภาษณ์ : ๙ มิถุนายน ๒๕๕๗

ประเด็นคำถามในการสัมภาษณ์

๑. ท่านคิดว่าขีดความสามารถของประเทศไทยด้านสงครามไซเบอร์อยู่ในระดับใด? (ภาคเอกชน ราชการ ประชาชน อื่นๆ)

- ในภาพรวมยังไม่พร้อมรับมือกับภัยคุกคามด้านนี้
- ภาคการเงิน โดยเฉพาะธนาคารมีความเข้มแข็งที่สุด (คะแนน 5 จาก 10)
- ภาคราชการ คะแนน 3 จาก 10
- ประชาชน คะแนน 2 จาก 10

๒. ท่านคิดว่าขีดความสามารถด้านสงครามไซเบอร์ที่ประเทศไทยควรมี มีอะไรบ้าง? (เชิงรับ เชิงรุก องค์บุคคล องค์วัตถุ และการจัดการ)

a. ควรมีทั้งเชิงรับและเชิงรุก
b. พัฒนาคนให้มากที่สุด
c. เห็นด้วยกับมี National Cyber Security Agency และ National Cyber Security Committee
d. เห็นด้วยกับการมี National Gateway ด้าน Cyberspace
e. เห็นด้วยกับการมีกฎหมายที่ให้อำนาจเจ้าหน้าที่ในการติดตามหรือเฝ้าระวัง (Lawful Interception) โดยที่หน่วยบังคับใช้ต้องเป็นองค์กรอิสระ

๓. ท่านคิดว่าลักษณะของหน่วยงานที่รองรับด้านสงครามไซเบอร์ควรเป็นอย่างไร?

a. หลายหน่วยงานร่วมกัน เพราะว่าสงครามไซเบอร์เกี่ยวข้องกับหลายหน่วยงาน
b. มีกฎหมาย Lawful Interception ที่โปร่งใส ปลอดจากการเมือง
c. มี National Cyber Security Agency (NCSC) และ National Cyber Security Committee (NCSC) จากหลายหน่วยงาน โดยมีหน่วยงานทางการทหารเป็นหน่วยงานหลัก
d. เป็นหน่วยงานที่ชัดเจน ต้องไม่ซ้ำซ้อน (Single command and Powerful)

๔. ท่านคิดว่าบทบาทของภาคเอกชน และภาคการศึกษาควรมีอะไรบ้าง?

a. ภาคการศึกษา
   - พัฒนาหลักสูตรด้าน Infosec และ Cybersec ที่เป็นสหวิทยาการ (ICT + เทคโนโลยีด้านอื่นๆ ด้วย)

การสัมภาษณ์ผู้เชี่ยวชาญ

ผู้ถูกสัมภาษณ์ : นายไชยกร อภิวัฒโนกุล
ประธานบริษัท S-Generation Co., Ltd.

วันสัมภาษณ์ : ๔ มิถุนายน ๒๕๕๗

ประเด็นคำถามในการสัมภาษณ์

๑. ท่านคิดว่าขีดความสามารถของประเทศไทยด้านสงครามไซเบอร์อยู่ในระดับใด? (ภาคเอกชน ราชการ ประชาชน อื่นๆ)

- ทั้งภาครัฐและเอกชน มีขีดความสามารถด้านสงครามไซเบอร์ต่ำ โดยดูจากตัวชี้วัด เช่น
  - จำนวนผู้เชี่ยวชาญด้าน Cyber Security
  - จำนวนการเจาะระบบโดยที่ผู้ดูแลไม่ทราบว่าระบบของตัวเองถูกเจาะ และถูกใช้เป็นทางผ่านเพื่อไปโจมตี Website อื่น
- ภาคประชาชนยังขาดความตระหนักรู้

๒. ท่านคิดว่าขีดความสามารถด้านสงครามไซเบอร์ที่ประเทศไทยควรมี มีอะไรบ้าง? (เชิงรับ เชิงรุก องค์บุคคล องค์วัตถุ และการจัดการ)

a. ควรมีทั้งเชิงรับและเชิงรุก
b. เน้นการพัฒนาบุคลากรให้มาก ปัจจุบันหลายองค์กรมีเครื่องเยอะมาก แต่ใช้ไม่คุ้มค่า เพราะขาดผู้เชี่ยวชาญในการประยุกต์ใช้เครื่องมือเหล่านั้น โดยเสียงบประมาณโดยไม่จำเป็น
c. เน้นเรื่อง R&D ด้าน Cyber Security ด้วยทั้ง HW and SW
d. เชิงรับ/เชิงรุก
   - มี National Cyber Agency ที่เป็นรูปธรรมและทำงานได้
   - ควรมี Virtual National Gateway สำหรับ Cyber Space เนื่อง gateway เชิงกายภาพทำได้ยาก ช่องทางการติดต่อสื่อสารมีมาก
e. เชิงรุก
   - มี Offensive Unit หรือ Cyber Warrior (ทางลับ) โดยได้รับการอบรมอย่างเข้มข้น
   - มีกฎหมายที่ให้อำนาจเจ้าหน้าที่ในการติดตามหรือเฝ้าระวัง (Lawful Interception)
f. เชิงรับ
   - ให้ผู้ใช้ ผู้ดูแลระบบได้มีโอกาสฝึกฝนมากๆ
   - สร้างความตระหนักรู้ให้ผู้ใช้มากๆ

๓. ท่านคิดว่าลักษณะของหน่วยงานที่รองรับด้านสงครามไซเบอร์ควรเป็นอย่างไร?

a. หลายหน่วยงานร่วมกัน เพราะว่าสงครามไซเบอร์เกี่ยวข้องกับหลายหน่วยงาน

b. มีกฎหมาย Lawful Interception

c. มี National Cyber Agency

๔. ท่านคิดว่าบทบาทของภาคเอกชน และภาคการศึกษาควรมีอะไรบ้าง?

a. เน้น Public Private Partnership (PPP)

- ภาครัฐส่งเสริมให้เอกชนเข้มแข็ง
- สนับสนุนผู้ประกอบการของไทย
- สนับสนุนด้าน HW and SW เช่น โครงการ Software Park

การสัมภาษณ์ผู้เชี่ยวชาญ

ผู้ถูกสัมภาษณ์ : นายไชยกร อภิวัฒโนกุล
ประธานบริษัท S-Generation Co., Ltd.

วันสัมภาษณ์ : ๔ มิถุนายน ๒๕๕๗

ประเด็นคำถามในการสัมภาษณ์

๑. ท่านคิดว่าขีดความสามารถของประเทศไทยด้านสงครามไซเบอร์อยู่ในระดับใด? (ภาคเอกชน ราชการ ประชาชน อื่นๆ)

- ทั้งภาครัฐและเอกชน มีขีดความสามารถด้านสงครามไซเบอร์ต่ำ โดยดูจากตัวชี้วัด เช่น
  - จำนวนผู้เชี่ยวชาญด้าน Cyber Security
  - จำนวนการเจาะระบบโดยที่ผู้ดูแลไม่ทราบว่าระบบของตัวเองถูกเจาะ และถูกใช้เป็นทางผ่านเพื่อไปโจมตี Website อื่น
- ภาคประชาชนยังขาดความตระหนักรู้

๒. ท่านคิดว่าขีดความสามารถด้านสงครามไซเบอร์ที่ประเทศไทยควรมี มีอะไรบ้าง? (เชิงรับ เชิงรุก องค์บุคคล องค์วัตถุ และการจัดการ)

a. ควรมีทั้งเชิงรับและเชิงรุก
b. เน้นการพัฒนาบุคลากรให้มาก ปัจจุบันหลายองค์กรมีเครื่องเยอะมาก แต่ใช้ไม่คุ้มค่า เพราะขาดผู้เชี่ยวชาญในการประยุกต์ใช้เครื่องมือเหล่านั้น โดยเสียงบประมาณโดยไม่จำเป็น
c. เน้นเรื่อง R&D ด้าน Cyber Security ด้วยทั้ง HW and SW
d. เชิงรับ/เชิงรุก
   - มี National Cyber Agency ที่เป็นรูปธรรมและทำงานได้
   - ควรมี Virtual National Gateway สำหรับ Cyber Space เนื่อง gateway เชิงกายภาพทำได้ยาก ช่องทางการติดต่อสื่อสารมีมาก
e. เชิงรุก
   - มี Offensive Unit หรือ Cyber Warrior (ทางลับ) โดยได้รับการอบรมอย่างเข้มข้น
   - มีกฎหมายที่ให้อำนาจเจ้าหน้าที่ในการติดตามหรือเฝ้าระวัง (Lawful Interception)
f. เชิงรับ
   - ให้ผู้ใช้ ผู้ดูแลระบบได้มีโอกาสฝึกฝนมากๆ
   - สร้างความตระหนักรู้ให้ผู้ใช้มากๆ

๓. ท่านคิดว่าลักษณะของหน่วยงานที่รองรับด้านสงครามไซเบอร์ควรเป็นอย่างไร?

a. หลายหน่วยงานร่วมกัน เพราะว่าสงครามไซเบอร์เกี่ยวข้องกับหลายหน่วยงาน

b. มีกฎหมาย Lawful Interception

c. มี National Cyber Agency

๔. ท่านคิดว่าบทบาทของภาคเอกชน และภาคการศึกษาควรมีอะไรบ้าง?

a. เน้น Public Private Partnership (PPP)

- ภาครัฐส่งเสริมให้เอกชนเข้มแข็ง
- สนับสนุนผู้ประกอบการของไทย
- สนับสนุนด้าน HW and SW เช่น โครงการ Software Park

การสัมภาษณ์ผู้เชี่ยวชาญ

ผู้ถูกสัมภาษณ์ : นายปริญญา หอมอเนก
ประธานบริษัท ACIS Professional Center Co., Ltd.

วันสัมภาษณ์ : ๔ มิถุนายน ๒๕๕๗

ประเด็นคำถามในการสัมภาษณ์

๑. ท่านคิดว่าขีดความสามารถของประเทศไทยด้านสงครามไซเบอร์อยู่ในระดับใด? (ภาคเอกชน ราชการ ประชาชน อื่นๆ)

- ภาครัฐ (พลเรือน และทหาร) มีขีดความสามารถด้านสงครามไซเบอร์ต่ำ ปัญหาน่าจะเกิดจากการขาดแคลนผู้เชี่ยวชาญ และการสนับสนุนจากผู้บังคับบัญชา
- ภาคเอกชน มีขีดความสามารถด้านสงครามไซเบอร์สูง โดยเฉพาะอย่างยิ่งภาคการเงินและธนาคาร
  - แต่ปัจจุบัน Hacker เจาะระบบผ่านลูกค้า เนื่องจากเจาะระบบโดยตรงไม่ได้
- ภาคประชาชนยังขาดความตระหนักรู้

๒. ท่านคิดว่าขีดความสามารถด้านสงครามไซเบอร์ที่ประเทศไทยควรมี มีอะไรบ้าง? (เชิงรับ เชิงรุก องค์บุคคล องค์วัตถุ และการจัดการ)

a. ควรมีทั้งเชิงรับและเชิงรุก
b. เชิงรับ/เชิงรุก
   - มี National Cyber Agency ที่เป็นรูปธรรมและทำงานได้
   - ควรมี National Gateway สำหรับ Cyber Space
c. เชิงรุก
   - มี Offensive Unit หรือ Cyber Warrior (ทางลับ) โดยได้รับการอบรมอย่างเข้มข้น
   - มีกฎหมายที่ให้อำนาจเจ้าหน้าที่ในการติดตามหรือเฝ้าระวัง (Lawful Interception)
d. เชิงรับ
   - ให้ผู้ใช้ ผู้ดูแลระบบได้มีโอกาสฝึกฝนมากๆ
   - สร้างความตระหนักรู้ให้ผู้ใช้มากๆ
   - ควรมี Simulation System สำหรับผู้ใช้ในหลายระดับ
   - จัดให้มีการแข่งขัน Cyber Got Talents

๓. ท่านคิดว่าลักษณะของหน่วยงานที่รองรับด้านสงครามไซเบอร์ควรเป็นอย่างไร?

a. หลายหน่วยงานร่วมกัน เพราะว่าสงครามไซเบอร์เกี่ยวข้องกับหลายหน่วยงาน

b. มีกฎหมาย Lawful Interception

c. มี National Cyber Agency

๔. ท่านคิดว่าบทบาทของภาคเอกชน และภาคการศึกษาควรมีอะไรบ้าง?

a. บทบาทของภาคเอกชนและภาคการศึกษาสำคัญ

b. ภาคการศึกษาตั้งแต่โรงเรียนจนถึงอุดมศึกษาจัดให้มีหลักสูตรด้าน Cyber Security ที่เหมาะสม

c. มี Simulation System ในหลากหลายระดับ

การสัมภาษณ์ผู้เชี่ยวชาญ

ผู้ถูกสัมภาษณ์ : นายปริญญา หอมอเนก
ประธานบริษัท ACIS Professional Center Co., Ltd.

วันสัมภาษณ์ : ๔ มิถุนายน ๒๕๕๗

ประเด็นคำถามในการสัมภาษณ์

๑. ท่านคิดว่าขีดความสามารถของประเทศไทยด้านสงครามไซเบอร์อยู่ในระดับใด? (ภาคเอกชน ราชการ ประชาชน อื่นๆ)

- ภาครัฐ (พลเรือน และทหาร) มีขีดความสามารถด้านสงครามไซเบอร์ต่ำ ปัญหาน่าจะเกิดจากการขาดแคลนผู้เชี่ยวชาญ และการสนับสนุนจากผู้บังคับบัญชา
- ภาคเอกชน มีขีดความสามารถด้านสงครามไซเบอร์สูง โดยเฉพาะอย่างยิ่งภาคการเงินและธนาคาร
  - แต่ปัจจุบัน Hacker เจาะระบบผ่านลูกค้า เนื่องจากเจาะระบบโดยตรงไม่ได้
- ภาคประชาชนยังขาดความตระหนักรู้

๒. ท่านคิดว่าขีดความสามารถด้านสงครามไซเบอร์ที่ประเทศไทยควรมี มีอะไรบ้าง? (เชิงรับ เชิงรุก องค์บุคคล องค์วัตถุ และการจัดการ)

a. ควรมีทั้งเชิงรับและเชิงรุก
b. เชิงรับ/เชิงรุก
   - มี National Cyber Agency ที่เป็นรูปธรรมและทำงานได้
   - ควรมี National Gateway สำหรับ Cyber Space
c. เชิงรุก
   - มี Offensive Unit หรือ Cyber Warrior (ทางลับ) โดยได้รับการอบรมอย่างเข้มข้น
   - มีกฎหมายที่ให้อำนาจเจ้าหน้าที่ในการติดตามหรือเฝ้าระวัง (Lawful Interception)
d. เชิงรับ
   - ให้ผู้ใช้ ผู้ดูแลระบบได้มีโอกาสฝึกฝนมากๆ
   - สร้างความตระหนักรู้ให้ผู้ใช้มากๆ
   - ควรมี Simulation System สำหรับผู้ใช้ในหลายระดับ
   - จัดให้มีการแข่งขัน Cyber Got Talents

๓. ท่านคิดว่าลักษณะของหน่วยงานที่รองรับด้านสงครามไซเบอร์ควรเป็นอย่างไร?

a. หลายหน่วยงานร่วมกัน เพราะว่าสงครามไซเบอร์เกี่ยวข้องกับหลายหน่วยงาน

b. มีกฎหมาย Lawful Interception

c. มี National Cyber Agency

๔. ท่านคิดว่าบทบาทของภาคเอกชน และภาคการศึกษาควรมีอะไรบ้าง?

a. บทบาทของภาคเอกชนและภาคการศึกษาสำคัญ

b. ภาคการศึกษาตั้งแต่โรงเรียนจนถึงอุดมศึกษาจัดให้มีหลักสูตรด้าน Cyber Security ที่เหมาะสม

c. มี Simulation System ในหลากหลายระดับ

ประวัติย่อผู้วิจัย

ชื่อ พลเรือตรี อรัญ นำผล

วัน เดือน ปีเกิด ๕ พฤศจิกายน ๒๕๐๓

การศึกษา

- โรงเรียนเตรียมทหาร
- โรงเรียนนายเรือ
- โรงเรียนเสนาธิการทหารเรือ
- วิทยาลัยการทัพเรือ
- ปริญญาตรี-โท-เอก วิศวกรรมไฟฟ้า (The Catholic University of America) ประเทศสหรัฐอเมริกา
- หลักสูตร International Defense Resource Management (Naval Postgraduate School) Monterey ประเทศสหรัฐอเมริกา

ประวัติการทำงานโดยย่อ

- ผู้อำนวยการกองอำนวยการสื่อสาร กรมสื่อสารทหารเรือ
- ผู้อำนวยการกองนโยบายและแผน กรมสื่อสารทหารเรือ
- ผู้บังคับหมวดเรือที่ ๒ กองเรือยกพลขึ้นบก กองเรือยุทธการ
- ผู้ช่วยทูตฝ่ายทหารเรือประจำสถานเอกอัครราชทูต ประจำกรุงกัวลาลัมเปอร์
- รองเจ้ากรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ

ตำแหน่งปัจจุบัน

- รองเจ้ากรมข่าวทหาร กองบัญชาการกองทัพไทย

สรุปย่อ

เรื่อง **การวิเคราะห์และพัฒนาขีดความสามารถการปฏิบัติการสงครามไซเบอร์ของประเทศไทย (Analysis and Development of Cyber Warfare Capability of Thailand)**

ลักษณะวิชา **วิทยาศาสตร์และเทคโนโลยี**

ผู้วิจัย **พลเรือตรี อรัญ นำผล** **หลักสูตร วปอ.** **รุ่นที่ ๕๖**

ความเป็นมาและความสำคัญของการวิจัย

ปัจจุบันระบบสารสนเทศและเครือข่ายสารสนเทศ มีบทบาทมากทั้งต่อบุคคล สังคม หรือหน่วยงาน ระบบสารสนเทศและเครือข่ายสารสนเทศได้ถูกนำมาใช้เพิ่มประสิทธิภาพในการทำงานทั้งภาคพลเรือน ทหาร และหน่วยงานราชการ เพื่อเพิ่มความรวดเร็วในการติดต่อสื่อสาร การจัดการระบบโครงสร้างพื้นฐานที่มีขนาดใหญ่และมีความสลับซับซ้อน รวมถึงเพิ่มความรวดเร็วของกระบวนการตัดสินใจ ทำให้กระบวนการทำงานมีประสิทธิภาพมากยิ่งขึ้น ก่อให้เกิดการพัฒนาในภาพรวมอย่างก้าวกระโดดทางด้านเศรษฐกิจ การเมือง การทหาร และสังคม จนมีคำกล่าวว่าการเข้ามามีบทบาทของระบบสารสนเทศและเครือข่ายสารสนเทศเป็นการปฏิวัติยุคที่ ๓ คือ การปฏิวัติทางด้านเทคโนโลยีข้อมูลข่าวสารซึ่งต่อเนื่องมาจากการปฏิวัติยุคที่ ๑หรือการปฏิวัติทางเกษตรกรรม และการปฏิวัติยุคที่ ๒ หรือการปฏิวัติทางอุตสาหกรรมอย่างไรก็ตามการนำระบบสารสนเทศและเครือข่ายสารสนเทศมาใช้มากขึ้น รวมถึงการพึ่งพาว่าระบบจะทำงานอย่างมีประสิทธิภาพ กลับเป็นการเพิ่มความเสี่ยงให้กับการปฏิบัติการหากระบบและเครือข่ายไม่สามารถทำงานได้ ทั้งจากความผิดพลาดที่ตัวระบบเองหรือการถูกโจมตีทางไซเบอร์เนื่องจากองค์ประกอบของไซเบอร์สเปซ (Cyberspace) ที่ประกอบด้วยระบบสารสนเทศ เครือข่ายสารสนเทศ คอมพิวเตอร์ ซอฟแวร์ ฐานข้อมูล และอื่นๆ โดยเฉพาะเครือข่ายสารสนเทศที่ผู้ประสงค์ร้าย (Hackers) ใช้เป็นช่องทางในการโจมตี

การโจมตีทางไซเบอร์มีความแตกต่างจากการโจมตีของสงครามตามรูปแบบแต่ผลจากการโจมตีเหมือนกัน คือทำให้ขีดความสามารถของฝ่ายตรงข้ามลดลง เช่น การเปรียบเทียบระหว่างการโจมตีทางอากาศกับการโจมตีด้วยซอฟท์แวร์ประสงค์ร้าย (หรือมัลแวร์) การโจมตีทางอากาศเป็นการทำลายสิ่งปลูกสร้างทางกายภาพ เช่น สนามบิน หอควบคุมการบิน ฯลฯ ส่วนมัลแวร์เป็น

การโจมตีที่ทำให้ระบบควบคุมการบินที่ทำงานด้วยคอมพิวเตอร์ เชื่อมโยงระบบย่อยต่างๆ เข้าด้วยกันด้วยเครือข่ายสารสนเทศเป็นอัมพาต ผลของการโจมตีทางอากาศหรือมัลแวร์ ทำให้สนามบินไม่สามารถใช้งานได้ หรือที่เป็นข่าวกล่าวถึงมากในวงการสงครามไซเบอร์ ได้แก่ ความขัดแย้งระหว่างอิหร่านกับนานาชาติ กรณีการพัฒนาขีดความสามารถด้านนิวเคลียร์ ที่ถูกมองว่าไม่ใช่การพัฒนาด้านพลังงานแต่เป็นการพัฒนาด้านอาวุธนิวเคลียร์ทำลายล้างสูง จนถูกโจมตีด้วยอาวุธทางไซเบอร์ ชื่อ โปรแกรมมัลแวร์Stuxnetทำให้โครงการพัฒนาดังกล่าวต้องหยุดชะงักลงทันที โปรแกรมมัลแวร์Stuxnetขนาดครึ่งเมกกะไบต์ก่อให้เกิดความเสียหายเท่าการโจมตีทางอากาศด้วยเครื่องบินโจมตีด้วยขีปนาวุธเลยทีเดียว

ตราบใดที่ระบบสารสนเทศและเครือข่ายสารสนเทศถูกนำมาใช้งาน การเป็นเป้าหมายของการโจมตีเป็นสิ่งที่หลีกเลี่ยงได้ยาก และการโจมตีมีการพัฒนาความสลับซับซ้อนมากยิ่งขึ้น จึงมีความจำเป็นที่ต้องวิเคราะห์และพัฒนาขีดความสามารถการปฏิบัติการสงครามไซเบอร์ของประเทศทั้งด้านการป้องกันหรือขีดความสามารถเชิงรับ และขีดความสามารถในการโจมตีหรือขีดความสามารถเชิงรุก เพื่อให้การใช้ประโยชน์จากระบบสารสนเทศและเครือข่ายสารสนเทศของไทยมีความมั่นคงปลอดภัยและบรรลุวัตถุประสงค์ตามที่กำหนด

วัตถุประสงค์ของการวิจัย

๑. เพื่อศึกษาหลักการ แนวทาง เทคโนโลยี และการพัฒนาขีดความสามารถด้านการปฏิบัติการสงครามไซเบอร์ของหน่วยงานต่างๆ ของไทย และของต่างประเทศ

๒. เพื่อวิเคราะห์และประเมินศักยภาพด้านสงครามไซเบอร์ของประเทศไทย

๓. เพื่อวิเคราะห์และเสนอแนวทางการพัฒนาขีดความสามารถด้านการปฏิบัติการสงครามไซเบอร์ของประเทศไทย

วิธีดำเนินการวิจัย

ดำเนินการวิจัยเชิงคุณภาพ โดยการรวบรวมและวิเคราะห์ข้อมูลใน ๒ ลักษณะดังนี้

๑. ข้อมูลปฐมภูมิ – การสัมภาษณ์ผู้เชี่ยวชาญด้าน Computer Security หรือ Cyber Security

๒. ข้อมูลทุติยภูมิ – เอกสารที่เกี่ยวข้อง เช่น ตำรา วารสาร เอกสารทางวิชาการ เอกสารทั้งภายในและต่างประเทศ บทความ ตลอดจนการค้นคว้าทางอินเทอร์เน็ต

ผลของการวิจัย

๑. หลักการพัฒนาขีดความสามารถการปฏิบัติการสงครามไซเบอร์

หลักการพัฒนาขีดความสามารถทางไซเบอร์เพื่อป้องกันและรับมือกับการโจมตีที่หลายหน่วยงานยึดเป็นแนวปฏิบัติโดยจะให้ความสำคัญที่คน กระบวนการ และเทคโนโลยี (People-Process-Technology) มีแนวทางที่สำคัญประกอบด้วย

๑.๑ การป้องกันภัยแบบเชิงลึก (Defense-in-Depth) เป็นแนวความคิดที่ต่างจากการป้องกันรูปแบบเดิมที่เรียกว่าการป้องกันทางเข้าออกแบบขอบนอก (Perimeter Defense) ซึ่งเป็นการป้องกันระบบสารสนเทศการบุกรุกโจมตีภายนอก (External Attack) ปัจจุบันการโจมตีระบบที่สำเร็จส่วนใหญ่ ไม่ได้มาจากภายนอก แต่เกิดขึ้นภายในขอบเขตที่ได้รับการป้องกัน การป้องกันภัยแบบเชิงลึกเป็นการมีสถาปัตยกรรมความปลอดภัยของระบบสารสนเทศและเครือข่ายสารสนเทศเป็นหลายชั้น (Multiple Layered) ที่มีขีดความสามารถในการรับรู้และเฝ้าระวัง และสามารถปกป้องตัวเองได้ เป็นการออกแบบระบบรักษาความปลอดภัยจากภายในไปสู่ภายนอก (Securing the Network from the Inside Out) ซึ่งจะช่วยป้องกันทั้งการโจมตีจากภายนอกและการโจมตีจากภายใน

๑.๒ การปฏิบัติตามวิธีการปฏิบัติที่เป็นเลิศที่เกี่ยวข้องกับการรักษาความปลอดภัยระบบสารสนเทศ (Information Security Best Practices) เป็นแนวทางการปฏิบัติที่ได้รับการยอมรับว่าเป็นแนวทางที่ดีที่สุดในการดำเนินการเพื่อให้ได้มาซึ่งความปลอดภัยของระบบสารสนเทศ แบ่งการปฏิบัติตามองค์ประกอบที่สำคัญได้แก่ เจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศ แนวทางการใช้งานระบบสารสนเทศ การปรับปรุงซอฟท์แวร์ การรักษาความปลอดภัยทางกายภาพ การจัดประเภทข้อมูลและเอกสาร การตั้งรหัสผ่าน การใช้เครือข่ายไร้สาย การอบรมสร้างความตระหนักรู้ด้านความปลอดภัยระบบสารสนเทศและการวางแผนฉุกเฉิน

๑.๓ การตรวจสอบหาจุดอ่อนของระบบ (Vulnerability Assessment – VA) การทดสอบเจาะระบบ (Penetration Test – PENTEST) เป็นกระบวนการตรวจสอบ ค้นหา และจัดลำดับความสำคัญของจุดอ่อนหรือช่องโหว่ในระบบสารสนเทศ และซอฟท์แวร์ ซึ่งจุดอ่อนดังกล่าวอาจถูกฝ่ายตรงข้ามหรือผู้ไม่หวังดี ใช้ประโยชน์ในการได้มาซึ่งข้อมูล การควบคุมระบบ การลิดรอนขัดขวาง หรือทำลาย ข้อมูล หรือการทำงานของระบบ การทำการตรวจสอบหาจุดอ่อนของระบบจะช่วยให้เราสามารถลดความเสี่ยงจากการที่ระบบสารสนเทศจะถูกโจมตี ด้วยการแก้ไขจุดอ่อน หรือการหาแนวทางการดำเนินการเพื่อลดผลกระทบหากจุดอ่อนดังกล่าวถูกโจมตี

๑.๔ แนวคิดการปฏิบัติการสงครามไซเบอร์ที่บูรณาการสงครามควบคุมบังคับบัญชา (Command and Control Warfare) และสงครามข้อมูลข่าวสาร (Information Warfare) เข้าด้วยกัน ที่ประกอบด้วยการบูรณาการการปฏิบัติทางทหารสาขาต่างๆ เข้าด้วยกัน ประกอบด้วยการปฏิบัติการทางยุทธการ การปฏิบัติการด้านมวลชน (Public Affairs) การปฏิบัติการจิตวิทยา (Psychological Operations)ร่วมกับการปฏิบัติการสารสนเทศ เช่นการปฏิบัติการสงครามเครือข่าย (Computer Network Operation) ที่ประกอบด้วยการดำเนินการ ๓ ส่วน คือ การปฏิบัติการโจมตี (Computer Network Attack – CNA) เป็นการปฏิบัติการทางรุก การปฏิบัติการป้องกัน (Computer Network Defense – CND) เป็นการปฏิบัติการทางรับ และการปฏิบัติการใช้ประโยชน์จากข้อมูลและระบบสารสนเทศ (Computer Network Exploitation – CNE) เป็นการปฏิบัติการที่สร้างขีดความสามารถในการหาข่าว หรือข้อมูลที่เกี่ยวข้องกับ ระบบสารสนเทศ หรือเครือข่ายสารสนเทศของฝ่ายตรงข้าม

๒. ศักยภาพด้านสงครามไซเบอร์ของประเทศไทย

ศักยภาพด้านสงครามไซเบอร์ของประเทศไทยในปัจจุบัน เป็นการดำเนินการแบบแยกส่วน เพื่อรองรับภารกิจของแต่ละกระทรวง หรือหน่วยงาน ไม่บูรณาการกัน ทำให้ขาดศักยภาพในการดำเนินการสงครามไซเบอร์ทั้งในทางรุก และในทางรับ นอกจากนั้นนโยบายการเปลี่ยนแปลงไปสู่การเป็นรัฐบาลอิเล็กทรอนิกส์ ทำให้ระบบสารสนเทศกลายเป็นโครงสร้างพื้นฐานหลักอันหนึ่งของประเทศ ระบบสารสนเทศทุกกระทรวง ถูกจัดเก็บรวมในที่เดียวกัน ทำให้เป็นจุดอ่อนหรือเป็นเป้าหมายที่สะดวกต่อการทำลายทางกายภาพ หรือการโจมตีทางเครือข่ายของฝ่ายตรงข้ามสำหรับนโยบายด้านความมั่นคงแห่งชาติยังไม่มีแนวทางสงครามไซเบอร์เป็นการเฉพาะ แต่ก็มีการตระหนักถึงภัยคุกคามที่เปลี่ยนแปลงไป แนวทางการดำเนินการด้านความมั่นคงในภาพรวมคือ การพัฒนาศักยภาพของชาติในการป้องกันประเทศ ด้วยการผนึกกำลังจากทุกฝ่าย ทั้งภาครัฐ ภาคเอกชน และภาคประชาชน การพัฒนาความร่วมมือทางทหารและความเข้าใจอันดีกับกองทัพของประเทศเพื่อนบ้านและส่งเสริมและประสานความร่วมมือกับต่างประเทศในด้านความมั่นคง

ศักยภาพด้านสงครามไซเบอร์ในประเทศไทยในเชิงรับในภาพรวมยังอยู่ในระดับต่ำ ซึ่งดูได้จากตัวชี้วัดเช่น จำนวนบุคลากรที่มีความเชี่ยวชาญด้านไซเบอร์ ปริมาณการถูกโจมตีทางไซเบอร์ที่มีแนวโน้มที่เพิ่มขึ้นอย่างต่อเนื่อง เว้นเอกชนภาคการเงินและธนาคารมีความสามารถเชิงรับอยู่ในเกณฑ์ยอมรับได้ สำหรับศักยภาพสงครามไซเบอร์เชิงรุกยังอยู่ในขั้นการเริ่มต้น ซึ่งเห็นได้จากจำนวนการจัดสัมมนา นิทรรศการ การจัดกิจกรรมการการแข่งขันที่เกี่ยวกับไซเบอร์ที่มีมากยิ่งขึ้น ตลอดจนการจัดตั้งหน่วยรับผิดชอบที่ชัดเจน โดยที่หน่วยงานทางการทหารมีการจัดหน่วยงานเพื่อรองรับการปฏิบัติการสงครามไซเบอร์ที่ชัดเจนและมีกิจกรรมด้านสงครามมากขึ้นอย่างต่อเนื่อง

๓. แนวทางการพัฒนาขีดความสามารถด้านสงครามไซเบอร์ของประเทศไทย

จากการสัมภาษณ์ผู้เชี่ยวชาญและหลักการพัฒนาขีดความสามารถการปฏิบัติการสงครามไซเบอร์ตลอดจนการวิเคราะห์ศักยภาพด้านสงครามไซเบอร์ของประเทศไทยตามกล่าวแล้วนั้น การพัฒนาขีดความสามารถการปฏิบัติการสงครามไซเบอร์ของประเทศไทย จำเป็นต้องดำเนินการตามตารางดังนี้

Finding	แนวทางการพัฒนา (Solution)
นโยบายด้านความมั่นคงแห่งชาติยังไม่มีแนวทางสงครามไซเบอร์เป็นการเฉพาะ	จัดให้มีหน่วยงานความมั่นคงด้านสงครามไซเบอร์กลางเป็นการเฉพาะ เช่น National Cyber Security Agency และ National Cyber Security Committee เพื่อกำหนดนโยบายด้านสงครามไซเบอร์ที่ชัดเจนและเป็นการเฉพาะ
● หน่วยงานไม่บูรณาการ ● หน่วยงานทางการทหารมีการจัดหน่วยงานเพื่อรองรับการปฏิบัติการสงครามไซเบอร์ที่ชัดเจนและมีกิจกรรมมากขึ้นและต่อเนื่อง	บูรณาการการปฏิบัติการสงครามไซเบอร์ระหว่างหน่วยงานภาครัฐ และจัดให้มีหน่วยงานความมั่นคงด้านสงครามไซเบอร์กลางเป็นการเฉพาะ เช่น National Cyber Security Agency โดยมี กห. เป็นหน่วยงานหลักในการขับเคลื่อน
ขาดแคลนผู้เชี่ยวชาญด้านไซเบอร์(Cyber Expert)	● ยกระดับความรู้ความสามารถของบุคลากรในสายวิชาชีพความมั่นคงปลอดภัยสารสนเทศ ให้อยู่ในระดับสากล รวมทั้งการสร้างเส้นทางความก้าวหน้าในสายอาชีพ พร้อมค่าตอบแทนที่เหมาะสม ● พัฒนาผู้เชี่ยวชาญระดับต้นจากสถาบันการศึกษาในประเทศ ● ประสานมิตรประเทศในการสร้างผู้เชี่ยวชาญ ● ปรับปรุงหลักสูตรการศึกษา ตั้งแต่ระดับประถมจนถึงระดับอุดมศึกษา โดยการแทรกเนื้อหาภัยคุกคามทางไซเบอร์ ● พัฒนาครูผู้สอน เพื่อให้สามารถปลูกจิตสำนึกด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับเยาวชน

Finding	แนวทางการพัฒนา (Solution)
ศักยภาพเชิงรับในภาพรวมยังอยู่ในระดับต่ำ ***เว้นภาคการเงินและธนาคารมีความสามารถในเกณฑ์ยอมรับได้***	● แลกเปลี่ยนบทเรียนระหว่างองค์กร ● ปลูกจิตสำนึกด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในองค์กร (ยึดหลัก Information Security Best Practices) ● ปลูกจิตสำนึกด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับประชาชน โดยเฉพาะเยาวชน ● Cyber War Simulator (โดยเน้น VA + PENTEST)
ศักยภาพเชิงรุกอยู่ในขั้นการเริ่มต้น	● จัดตั้งนักรบไซเบอร์ (ในทางลับ) ● สร้างเครือข่ายภาคประชาชนที่ร่วมในการโจมตีเชิงรุก (Attack Network Base) ● พัฒนาหลักนิยมการดำเนินการปฏิบัติการทางไซเบอร์ (Cyber Warfare Doctrine) ที่ชัดเจนตามเทคนิคการป้องกันภัยเชิงลึก และตามวิธีการปฏิบัติที่เป็นเลิศเกี่ยวกับการรักษาความปลอดภัย
หลาย ISP (Multiple Gateway)	จัดทำ National Cyber Gateway
Thailand is one of the cyber-riskiest countries in the world.	● ปรับปรุงกฎหมาย ระเบียบ ข้อปฏิบัติ ให้ทันสมัย รวมถึงอาจจะต้องมีการออกกฎหมายที่รองรับการปฏิบัติของเจ้าหน้าที่ด้านความมั่นคงในการดำเนินการด้านไซเบอร์ เช่น การรองรับการดักจับและตรวจสอบข้อมูลอย่างถูกกฎหมาย (Lawful Interception) ● มีกฎหมายที่รองรับแนวความคิดด้านการทำ National Cyber Gateway หรือการเพิ่มขีดความสามารถในการตรวจสอบการกระทำผิดทางไซเบอร์ การโจมตีทางไซเบอร์ กับทุกเส้นทางการเชื่อมต่อเครือข่ายอินเทอร์เน็ตในประเทศกับต่างประเทศ ● ส่งเสริมให้องค์กร/หน่วยงานตระหนักถึงภัยคุกคามทางไซเบอร์ โดยเริ่มตั้งแต่ขั้นออกแบบระบบ ทำความเข้าใจแนวคิด Cyber Security Defense-in-Depth

Finding	แนวทางการพัฒนา (Solution)
การวิจัยด้าน Cyber Security มีน้อย	● สนับสนุนการวิจัยและพัฒนาโดยเฉพาะด้านซอฟต์แวร์ เช่น ระบบจำลองยุทธ์ทางสงครามไซเบอร์ (Cyber Security Simulator) ● พิจารณาใช้เครื่องมือค้นหาจุดอ่อน และเครื่องมือในการทดสอบการโจมตี ที่ถูกพัฒนาขึ้นโดยอาศัยหลักการพัฒนาซอฟท์แวร์แบบเปิดเผย (Open Source) ● สร้างความร่วมมือระหว่างหน่วยงานภาครัฐและภาคเอกชน (Public Private Partnership) ด้านการวิจัยภัยคุกคามทางไซเบอร์
แนวโน้มการโจมตีมากขึ้น โดยไม่รู้ตัว	● สร้างความตระหนักในความเสี่ยงต่างๆ ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แก่ประชาชนทั่วไป ● มีเครื่องมือที่เหมาะสมและเพียงพอ สามารถปฏิบัติการการป้องกันภัยเชิงลึกได้ พร้อมวิเคราะห์ Critical Infrastructure ของประเทศ ● มีระบบฐานข้อมูลที่สามารถรวบรวมและวิเคราะห์ข้อมูลเพื่อวิเคราะห์หาจุดอ่อนของระบบสารสนเทศและเครือข่ายสารสนเทศของฝ่ายตรงข้าม พร้อมจัดทำเป็นบัญชีเป้าหมายทางระบบสารสนเทศ
Cyberspace: Borderless and Connected	● สร้างความร่วมมือระหว่างหน่วยงานภาครัฐและภาคเอกชน เพื่อบูรณาการขีดความสามารถในการตอบสนองต่อภัยคุกคามทางไซเบอร์ ● แสวงความร่วมมือกับประเทศเพื่อนบ้านในภูมิภาคหรือกับประเทศพันธมิตรที่มีความรู้ ความสามารถและประสบการณ์

หรือจากตารางข้างต้นสามารถจัดแบ่งในด้านองค์บุคคล องค์วัตถุ และการบริหารจัดการได้ดังนี้

๓.๑ องค์บุคคล

ผลิตผู้เชี่ยวชาญด้านสงครามไซเบอร์ที่มีมาตรฐานสามารถปฏิบัติงานได้อย่างเพียงพอ โดยการส่งเสริมจากภาครัฐรวมทั้งจัดตั้งนักรบไซเบอร์ (ในทางลับ)

มีการจัดทำมาตรฐานวิชาชีพ เพื่อยกระดับความรู้ความสามารถของบุคลากรในสายวิชาชีพความมั่นคงปลอดภัยสารสนเทศ ให้อยู่ในระดับสากล ร่วมทั้งการสร้างเส้นทางความก้าวหน้าในสายอาชีพ พร้อมค่าตอบแทนที่เหมาะสมกับระดับความรู้ความสามารถ ควบคู่กับการพัฒนากระบวนการรับรอง และการกำกับดูแลมาตรฐานวิชาชีพภายในประเทศ

พัฒนาผู้เชี่ยวชาญระดับต้นจากสถาบันการศึกษาในประเทศ เช่นมหาวิทยาลัยต่างๆ และจากหน่วยงานวิจัยระดับชาติ รวมทั้งประสานความร่วมมือกับมิตรประเทศในการพัฒนาผู้เชี่ยวชาญด้านสงครามไซเบอร์

มีแผนการให้ความรู้อย่างต่อเนื่องและมีองค์ความรู้ที่เข้าถึงได้แก่ประชาชนทั่วไป เพื่อให้มีความตระหนักในความเสี่ยงต่างๆ ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

ปรับปรุงหลักสูตรการศึกษา ตั้งแต่ระดับประถมจนถึงระดับอุดมศึกษา โดยมีการสอดแทรกเนื้อหาที่เกี่ยวกับภัยคุกคามทางไซเบอร์และวิธีการป้องกันภัยดังกล่าวเบื้องต้น

พัฒนาครูผู้สอน เพื่อให้สามารถปลูกจิตสำนึกด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับเยาวชนได้อย่างมีประสิทธิภาพ

สร้างเครือข่ายภาคประชาชนที่ร่วมในการโจมตีเชิงรุกเพื่อเพิ่มขีดความสามารถในการโจมตีและลดผลกระทบต่อความสัมพันธ์ระหว่างประเทศ

๓.๒ องค์วัตถุ

รัฐบาลสนับสนุนการวิจัยและพัฒนาเทคโนโลยีที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ โดยเฉพาะด้านซอฟต์แวร์ เช่น ระบบจำลองยุทธ์ทางสงครามไซเบอร์ (Cybersecurity Simulator)

พิจารณาใช้เครื่องมือค้นหาจุดอ่อน และเครื่องมือในการทดสอบการโจมตีที่ถูกพัฒนาขึ้นโดยอาศัยหลักการพัฒนาซอฟท์แวร์แบบเปิดเผย (Open Source)ซึ่งมีราคาไม่แพง โดยร่วมมือกับภาคเอกชน เพื่อใช้ในการซ่อนพรางการโจมตี ยกตัวอย่างเช่นหากใช้เครือข่ายสารสนเทศของกองทัพไทย ในการปฏิบัติการโจมตี หากฝ่ายตรงข้ามมีขีดความสามารถในการตรวจจับ จะพบว่าการโจมตีนี้เป็นการดำเนินการของกองทัพไทย ซึ่งอาจจะส่งผลกระทบต่อภาพลักษณ์ และความสัมพันธ์ระหว่างประเทศได้

มีเครื่องมือที่เหมาะสมและเพียงพอ ที่จะสามารถทำให้การปฏิบัติการการป้องกันภัยเชิงลึกได้ พร้อมวิเคราะห์โครงสร้างพื้นฐานของประเทศ เพื่อหาสุดสำคัญ หรือจุดเสี่ยงที่อาจถูกโจมตีสมควรได้รับการป้องกัน

มีระบบฐานข้อมูลที่สามารถรวบรวมและวิเคราะห์ข้อมูล เพื่อสามารถที่จะวิเคราะห์หาจุดอ่อนของระบบสารสนเทศและเครือข่ายสารสนเทศของฝ่ายตรงข้าม และสามารถนำข้อมูลระบบสารสนเทศ และจุดอ่อนของระบบมาจัดทำเป็นบัญชีเป้าหมายทางระบบสารสนเทศได้

๓.๓ การบริหารจัดการ

บูรณาการการปฏิบัติการสงครามไซเบอร์ระหว่างหน่วยงานภาครัฐให้สามารถประสานความร่วมมือในการป้องกันได้อย่างมีประสิทธิภาพ และจัดให้มีหน่วยงานความมั่นคงด้านสงครามไซเบอร์กลางเป็นการเฉพาะ เช่น National Cyber Security Agency ที่มีโครงสร้างการบริหารงานระดับชาติ พร้อมบทบาทหน้าที่ที่ชัดเจน เพื่อการบัญชาการ การประสานความร่วมมือ กำหนดขั้นตอนการดำเนินงาน ในการส่งเสริม สนับสนุน มีอำนาจสั่งการ ลงโทษ รับรอง กำกับ ตรวจสอบ ประเมินผล โดยมี กห. เป็นหน่วยงานหลักในการขับเคลื่อน

ปรับปรุงกฎหมาย ระเบียบ ข้อปฏิบัติ ให้ทันสมัยและสามารถบังคับใช้ได้จริง รวมถึงอาจจะต้องมีการออกกฎหมายที่รองรับการปฏิบัติของเจ้าหน้าที่ด้านความมั่นคงในการดำเนินการด้านไซเบอร์ เช่นการรองรับการดักจับและตรวจสอบข้อมูลอย่างถูกกฎหมาย (Lawful Interception)

มีกฎหมายที่รองรับแนวความคิดด้านการทำ National Cyber Gateway หรือการเพิ่มขีดความสามารถในการตรวจสอบการกระทำผิดทางไซเบอร์ การโจมตีทางไซเบอร์ กับทุกเส้นทางการเชื่อมต่อเครือข่ายอินเทอร์เน็ตในประเทศกับต่างประเทศ

มีการสร้างความร่วมมือระหว่างหน่วยงานภาครัฐและภาคเอกชน (Public Private Partnership) เพื่อบูรณาการขีดความสามารถในการตอบสนองต่อภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ โดยการแบ่งปันทรัพยากร (คน กระบวนการ เครื่องมือ–People Process Technology) การแลกเปลี่ยนข้อมูลภัยคุกคามด้านไซเบอร์ การมีนโยบายสนับสนุนผู้ประกอบการด้าน Cybersecurity การมีความร่วมมือในด้านการยืมตัวบุคลากรระหว่างหน่วยงาน การมีกลไกสำหรับส่งเสริมการพัฒนาขีดความสามารถด้าน Cybersecurity ให้กับภาคเอกชน เช่นมาตรการทางภาษี หรือการให้ทุนสนับสนุนเป็นต้น

มีแนวทาง หลักนิยม การดำเนินการปฏิบัติการทางไซเบอร์ที่ชัดเจนตามเทคนิคการป้องกันภัยเชิงลึก และตามวิธีการปฏิบัติที่เป็นเลิศเกี่ยวกับการรักษาความปลอดภัย

ข้อเสนอแนะ

เนื่องจากไซเบอร์สเปซมีคุณลักษณะการเป็นพื้นที่ไร้พรมแดน การเชื่อมโยงต่อกันเป็นโครงข่าย การปรากฏทุกหนแห่ง การเป็นพื้นที่สาธารณะ การที่ข้อมูลถูกส่งด้วยความเร็วแสงและความเป็นอสมมาตร ไซเบอร์สเปซเชื่อมโลกทั้งโลกเข้าด้วยกัน ดังนั้นผลกระทบจากการโจมตีทางไซเบอร์

จึงขยายตัวจากเครือข่ายสารสนเทศหนึ่งในประเทศหนึ่งไปยังเครือข่ายสารสนเทศของอีกประเทศหนึ่งอย่างรวดเร็ว ทำให้ภัยคุกคามจากไซเบอร์สเปซ นับวันจะมีความสลับซับซ้อน ทวีความรุนแรงมากขึ้น การเตรียมความพร้อมเพื่อรองรับการโจมตีทางไซเบอร์จึงประกอบการเตรียมความพร้อมภายในประเทศ ตลอดจนการแสวงความร่วมมือกับประเทศเพื่อนบ้านในภูมิภาค หรือกับประเทศพันธมิตรที่มีความรู้ ความสามารถ และประสบการณ์

ภัยคุกคามทางไซเบอร์มีผลกระทบต่อทั้งบุคคลและสาธารณะ การรับมือกับภัยคุกคามรูปแบบใหม่นี้ต้องอาศัยความร่วมมือจากหลายภาคส่วนทั้งภาครัฐและภาคเอกชน การสร้างความตระหนักรู้ให้ทุกภาคส่วนมีความจำเป็นอย่างยิ่ง ตราบใดที่เทคโนโลยีสารสนเทศและการสื่อสารเป็นส่วนหนึ่งของชีวิตประจำวันของบุคคลและของหน่วยงานในทุกระดับแล้ว ไซเบอร์สเปซก็จะเข้ามาเกี่ยวข้องอย่างหลีกเลี่ยงไม่ได้

ข้อเสนอแนะการทำวิจัยต่อไป

เพื่อให้การศึกษาด้านภัยคุกคามไซเบอร์สเปซมีความต่อเนื่องและครอบคลุมมากยิ่งขึ้น หัวข้อการวิจัยที่น่าสนใจประกอบด้วย

การศึกษารูปแบบและโครงสร้างหน่วยงานความมั่นคงด้านสงครามไซเบอร์กลางระดับชาติ หรือ National Cyber Security Agency ที่เหมาะสมและสอดคล้องกับการบริหารจัดการของประเทศไทย

การศึกษาแนวทางการจัดทำ National Cyber Gateway ที่มีเสรีภาพในการต่อเชื่อม (Freedom of Connectivity) แต่ความสามารถควบคุม (Controllability) ได้ในมิติด้านความมั่นคง

การวิจัยเพื่อศึกษาความตระหนักรู้ของประชาชนเกี่ยวกับภัยคุกคามไซเบอร์สเปซเพื่อกำหนดแนวทางในการพัฒนาขีดความสามารถของคนในชาติต่อไป

การศึกษาแนวทางการสร้างความร่วมมือระหว่างประเทศเพื่อรองรับภัยคุกคามไซเบอร์สเปซ