แนวทางการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศไทย

โดย

พลเรือตรี วิโรจน์ ธันวรักษ์กิจ

เจ้ากรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ

กองทัพเรือ

นักศึกษาวิทยาลัยป้องกันราชอาณาจักร

หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ ๕๖

ประจำปีการศึกษา พุทธศักราช ๒๕๕๖ - ๒๕๕๗

บทคัดย่อ

เรื่อง แนวทางการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศไทยในอนาคต

ลักษณะวิชา วิทยาศาสตร์และเทคโนโลยี

ผู้วิจัย พล.ร.ต.วิโรจน์ ธันวรักษ์กิจ ร.น. **หลักสูตร** วปอ. **รุ่นที่** ๕๖

การวิจัยการดำเนินการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศไทย ได้กำหนดวัตถุประสงค์หลักไว้เพื่อศึกษา วิเคราะห์ เปรียบเทียบ แนวทางในการรักษาความมั่นคงปลอดภัยทางสารสนเทศ และเสนอแนะแนวทางที่เหมาะสมในการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศไทยในอนาคต

จากการศึกษาวิจัยค้นคว้าแหล่งข้อมูลทั้งในและต่างประเทศ พบว่า ประเทศไทยมีกระทรวงที่เกี่ยวข้องกับงานด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศหลายกระทรวง โดยการดำเนินการในภาพรวมยังขาดการบูรณาการงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางสารสนเทศ เป็นการดำเนินการแบบเอกเทศทั้งในระดับนโยบายและระดับปฏิบัติการ ทำให้ขาดศักยภาพในการดำเนินการรับมือกับภัยคุกคามรูปแบบต่างๆ บุคลากรมีจำนวนจำกัด จำเป็นต้องส่งเสริมสร้างนักวิจัยอย่างเร่งด่วน นอกจากนี้ช่องทางการเชื่อมต่อเครือข่ายอินเทอร์เน็ตภายในประเทศกับเครือข่ายอินเทอร์เน็ตต่างประเทศผ่านหน่วยงานรัฐ ผู้ให้บริการอินเทอร์เน็ตทั้งภาครัฐและเอกชน มีเป็นจำนวนมาก ดังนั้นการตรวจสอบและสกัดกั้นข้อมูลการจราจรทางอินเทอร์เน็ตตามกฎหมาย การควบคุมข้อมูลที่ผิดกฎหมายหรือมีผลกระทบต่อความมั่นคง รวมทั้งการป้องกันการโจมตีทางไซเบอร์ จึงทำได้ค่อนข้างยาก

ผลการวิจัยในเอกสารฉบับนี้เกี่ยวข้องกับการบูรณาการงานด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศของกระทรวงต่างๆที่เกี่ยวข้อง ทั้งนี้ได้เสนอแนะให้ สมช.เป็นหน่วยหลักรับผิดชอบในการดำเนินงานในภาพรวมทั้งในระยะสั้น ระยะกลาง และระยะยาว โดยผลการวิจัยเสนอแนะให้จัดตั้งหน่วยงานรักษาความมั่นคงปลอดภัยทางสารสนเทศแห่งชาติ รวมทั้งการดำเนินการในด้านอื่นๆ ควบคู่กัน เช่น การผลักดันให้มีกฎหมายควบคุมการจราจรทางอินเตอร์เน็ต การผลักดันหน่วยงาน National CERT ให้เป็นศูนย์ปฏิบัติการในระดับประเทศ การประสานความร่วมมือกับหน่วยงานต่างประเทศ เป็นต้น รวมทั้งผลักดันให้มีการจัดตั้งศูนย์รวมความเป็นเลิศด้านไซเบอร์ โดยหากหน่วยงานที่เกี่ยวข้องนำผลงานวิจัยนี้ไปใช้ประโยชน์อย่างจริงจัง และผลักดันให้เป็นวาระแห่งชาติเร่งด่วน จะเป็นประโยชน์โดยตรงกับประเทศให้มีศักยภาพและขีดความสามารถด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศ

คำนำ

เอกสารวิจัยฉบับนี้เป็นส่วนหนึ่งของการศึกษาในหลักสูตรวิทยาลัยป้องกันราชอาณาจักร รุ่นที่ ๕๖ ประจำปีการศึกษา ๒๕๕๗ ที่ให้นักศึกษาได้ค้นคว้าวิจัยในเรื่องที่สนใจ และเป็นประโยชน์ต่อหน่วยงาน ผู้วิจัยได้ทำงานในตำแหน่งเจ้ากรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ จึงมีความสนใจในแนวทางการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศ โดยข้อมูลที่สำคัญในการศึกษาวิจัยและเขียนเอกสารฉบับนี้ส่วนหนึ่งมาจากการประชุมสัมมนากับหน่วยงานต่างๆ ทั้งในและนอกกระทรวงกลาโหม ข้อมูลจากกระทรวงต่างๆ และจากแหล่งข้อมูลเปิด เช่น อินเตอร์เน็ต เป็นต้น

เนื้อหาของเอกสารวิจัยฉบับนี้ เกี่ยวข้องกับการบูรณาการงานด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศของกระทรวงต่างๆที่เกี่ยวข้อง โดยผลการวิจัยเสนอแนะให้จัดตั้งหน่วยงานรักษาความมั่นคงปลอดภัยทางสารสนเทศแห่งชาติ รวมทั้งการดำเนินการในด้านอื่นๆ ควบคู่กัน เช่น การผลักดันให้มีกฎหมายควบคุมการจราจรทางอินเตอร์เน็ต การผลักดันหน่วยงาน National CERT ให้เป็นศูนย์ปฏิบัติการในระดับประเทศ การประสานความร่วมมือกับหน่วยงานต่างประเทศ เป็นต้น โดยหากหน่วยงานที่เกี่ยวข้องนำผลงานวิจัยนี้ไปใช้ประโยชน์อย่างจริงจัง และผลักดันให้เป็นวาระแห่งชาติเร่งด่วน จะเป็นประโยชน์โดยตรงกับประเทศให้มีศักยภาพและขีดความสามารถด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศ

ผู้วิจัยขอขอบคุณคณะกรรมการที่ช่วยให้คำแนะนำและติดตามการทำงานของผู้วิจัยอย่างต่อเนื่อง ทำให้เอกสารเสร็จตามรูปแบบและเวลาที่กำหนด นอกจากนี้ผู้วิจัยขอขอบคุณผู้ให้การสนับสนุนข้อมูลและเรื่องอื่นๆ อีกหลายท่าน ทั้งที่ปรากฏและไม่ปรากฏชื่อในเอกสารนี้ ซึ่งจะทำให้เอกสารเสร็จไปได้ด้วยดี หากเอกสารวิจัยฉบับนี้มีข้อผิดพลาดประการใด ผู้วิจัยขอน้อมรับแต่โดยดี

พล.ร.ต. ร.น.

(วิโรจน์ ธันวรักษ์กิจ)

นักศึกษาวิทยาลัยป้องกันราชอาณาจักร

หลักสูตร วปอ. รุ่นที่ ๕๖

ผู้วิจัย

สารบัญ

สารบัญ (ต่อ)

บทที่ ๑

บทนำ

ความเป็นมาและความสำคัญของปัญหา

ความก้าวหน้าทางด้านเทคโนโลยีสารสนเทศได้ทำให้เกิดความเปลี่ยนแปลงของมนุษยชาติในหลาย ๆ ด้าน จนนักอนาคตศาสตร์อย่าง Alvin Toffler ตั้งทฤษฎี "คลื่นลูกที่สาม" โดย Toffler มองว่าเทคโนโลยีสารสนเทศคือคลื่นลูกที่สามของคลื่นปฏิวัติสังคมมนุษย์ต่อจากการทำการเกษตร และการปฏิวัติอุตสาหกรรม [๑] [๒] ซึ่งทฤษฎีดังกล่าวสอดคล้องกับตัวเลขทางเศรษฐกิจในปัจจุบัน ตามการจัดลำดับมูลค่าทางการตลาดของบริษัททั่วโลกในปี ๒๕๕๕ โดย Financial Time ปรากฏว่า ในรายชื่อของบริษัทที่มูลค่าทางการตลาด ๕๐ อันดับแรกของโลก มีบริษัทที่ประกอบธุรกิจเกี่ยวข้องกับเทคโนโลยีสารสนเทศมากถึง ๑๓ บริษัท [๓] และมีแนวโน้มว่ามูลค่าทางการตลาดของบริษัทเหล่านั้นจะเพิ่มขึ้นอย่างต่อเนื่องในอนาคต

นอกจากความเปลี่ยนแปลงทางด้านเศรษฐกิจแล้ว เทคโนโลยีสารสนเทศยังทำให้เกิดความเปลี่ยนแปลงทางด้านสังคมและวัฒนธรรมอย่างลึกซึ้ง การติดต่อสื่อสาร การรับและเผยแพร่ข้อมูลข่าวสาร ทัศนคติและวิธีคิด การดำเนินชีวิตประจำวันของคนในสังคมได้เปลี่ยนแปลงไปอย่างมาก โดยเฉพาะอย่างยิ่งเมื่อ Social Network ได้รับความนิยมและถูกใช้งานอย่างกว้างขวาง จนได้ชื่อว่า “สื่อใหม่” ซึ่งสามารถเข้ามาแทนที่ และมีอิทธิพลเหนือสื่อในรูปแบบเดิมที่ถือได้ว่าเป็น “ฐานันดรที่สี่” ได้ส่งผลให้สื่อเดิมต้องมีการปรับตัว และนำสื่อใหม่มาปรับใช้ให้เท่าทันความเปลี่ยนแปลงทางวัฒนธรรมที่เกิดขึ้น

เมื่อเทคโนโลยีสารสนเทศเข้ามาเกี่ยวข้องกับคนจำนวนมาก โดยตามสถิติล่าสุดประชากรในประเทศไทยเกินกว่าครึ่งสามารถเข้าถึงอินเทอร์เน็ตได้ ความเกี่ยวข้องระหว่างเทคโนโลยีสารสนเทศกับการเมืองจึงเป็นเรื่องที่หลีกเลี่ยงไม่ได้ เทคโนโลยีสารสนเทศถูกนำมาใช้เป็นเครื่องมือทั้งในทาง

---

๑ Alvin Toffler. "The Third Wave". Bantam Books. USA, 1980.

๒ Alvin Toffler. "Revolutionary Wealth". Bantam Books. USA, 2006.

๓ Financial Times."FT Global 500 2012". (Online). Available : http://www.ft.com/cms/a81f853e-ca80-11e1-89f8-00144feabdc0.pdf

สนับสนุนและต่อต้านแนวคิดทางการเมือง เหตุการณ์ทางการเมืองสำคัญในประเทศไทยและทั่วโลกในระยะเวลา ๓-๕ ปีที่ผ่านมาจึงมีความเชื่อมโยงกับเทคโนโลยีสารสนเทศ ทั้งในแง่ของการใช้เป็นเครื่องมือในการติดต่อสื่อสาร เผยแพร่ความคิด การจัดตั้ง และบริหารจัดการมวลชน ไม่ว่าจะเป็นเหตุการณ์ในช่วง เมษายน-พฤษภาคม ๒๕๕๓ ในกรุงเทพมหานคร เหตุการณ์อาหรับสปริง การรัฐประหารในประเทศอียิปต์ เป็นต้น

จากการที่เทคโนโลยีสารสนเทศเข้ามามีอิทธิพล และส่งผลกระทบต่อ เศรษฐกิจ สังคม วัฒนธรรม และการเมือง ทั้งในเชิงลึกและเชิงกว้าง ย่อมหมายถึงการมีบทบาทของเทคโนโลยีสารสนเทศในแง่ความมั่นคงของชาติโดยปริยาย ประเทศต่าง ๆ ทั่วโลกจึงให้ความสนใจในเรื่องดังกล่าว จนมีการนิยามคำว่า "Cyberwarfare" หรือ สงครามไซเบอร์ขึ้นในปี ๒๕๓๖[๔] ในปี ๒๕๕๓ กองทัพสหรัฐอเมริกาได้กำหนดให้สงครามไซเบอร์เป็น "ขอบเขตที่ห้าของการทำสงคราม" [๕] และในปีเดียวกันได้มีการจัดตั้ง U.S. Cyber Command เพื่อรับผิดชอบในส่วนของสงครามไซเบอร์ [๖]

ด้วยลักษณะเฉพาะของเทคโนโลยีสารสนเทศที่มีการเชื่อมโยงกับผู้คนจำนวนมาก และเป็นการเชื่อมโยงแบบไร้พรมแดน ทำให้ผลกระทบทางความมั่นคงที่เกิดจากเทคโนโลยีสารสนเทศจึงมีความเฉพาะตามไปด้วย มีการนำเทคโนโลยีสารสนเทศมาใช้ทั้งในสงครามตามแบบ และสงครามนอกแบบ อีกทั้งคู่ความขัดแย้งที่เกิดขึ้นก็มีได้ทั้งคู่ความขัดแย้งระหว่างรัฐกับรัฐ รัฐกับกองกำลังอิสระ รัฐกับผู้ก่อการร้าย รัฐกับประชาชน หรือแม้แต่ประชาชนกับประชาชน ซึ่งคู่ความขัดแย้งที่มีความหลากหลายเช่นนี้จะเป็นไปไม่ได้เลย หากไม่มีเทคโนโลยีสารสนเทศที่มีราคาถูก ใช้งานง่าย และสามารถสร้างผลกระทบได้ในวงกว้าง

ลักษณะของภัยคุกคามในสงครามไซเบอร์มีหลากหลายรูปแบบ และเริ่มมีปรากฏให้เห็นในห้วงเวลาหลายปีที่ผ่านมา รูปแบบที่มีมักพบเห็นมากที่สุดคือ การก่ออาชญากรรมคอมพิวเตอร์ที่เกี่ยวข้องกับระบบพาณิชย์อิเล็กทรอนิกส์ (E-Commerce) การทำธุรกรรมอิเล็กทรอนิกส์ (E-Transaction) รวมถึงการละเมิดสิทธิทรัพย์สินทางปัญญา มีการคาดการณ์ว่าความเสียหายอันเกิดจากการ

---

๔ John Arquilla and David Ronfeldt. "Cyberwar is comming!", Comparative Strategy. Vol. 12, No. 2, Spring, 1993. pp. 141-165.

๕ กระทรวงต่างประเทศสหรัฐอเมริกา. "Defending a New Domain". (Online). Available : http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain

๖ กระทรวงกลาโหมประเทศสหรัฐอเมริกา. “Special Report : The Cyber Domain”. (Online). Available : http://www.defense.gov/home/features/2013/0713_cyberdomain/

ก่ออาชญากรรมคอมพิวเตอร์ในรูปแบบต่าง ๆ ทั่วโลกมีมูลค่ารวมกันสูงถึงห้าแสนล้านเหรียญสหรัฐต่อปี ถือว่าสูงมากเมื่อเทียบกับอาชญากรรมในลักษณะอื่น ทำให้ส่งผลกระทบต่อเศรษฐกิจในวงกว้าง รัฐบาลสหรัฐอเมริกาจึงให้ความสนใจและให้ความสำคัญในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อภาคธุรกิจและเศรษฐกิจมาตั้งแต่สมัยรัฐบาลคลินตัน กรณีล่าสุดที่เกิดขึ้นในประเทศไทยคือ การขโมยข้อมูลบัตรเอทีเอ็มเพื่อลักลอบถอนเงินจากบัญชีผู้เสียหาย ทำให้เกิดความเสียหายแก่ผู้ใช้บัตรเอทีเอ็มและธนาคารจำนวนมาก และมีมูลค่าความเสียหายที่สูง

รูปแบบสงครามไซเบอร์รูปแบบหนึ่งที่เกี่ยวข้องกับความมั่นคงของรัฐโดยตรงคือ การโจรกรรมข้อมูล กรณีที่สร้างความเสียหายให้กับหลายประเทศและส่งผลกระทบเป็นวงกว้างคือ การนำข้อมูลลับของรัฐบาลหลายประเทศมาเปิดเผยโดยวิกีลีกส์ ที่มีการดำเนินการโดยกลุ่มแฮกเกอร์อิสระจากทั่วโลก ข้อมูลต่าง ๆ ล้วนได้มาจากการโจรกรรม นอกจากการโจรกรรมข้อมูลโดยแฮกเกอร์แล้ว รัฐบาลหลาย ๆ ประเทศก็ดำเนินการโจรกรรมข้อมูลของประเทศอื่น ๆ ตัวอย่างที่เห็นได้ชัดที่สุดคือ การดักฟังข้อมูลโดยรัฐบาลสหรัฐฯ ภายใต้โครงการ PRISM หรือการดักฟังการพูดคุยโทรศัพท์ผู้นำหลายประเทศ เป็นต้น เหล่านี้ล้วนกระทบต่อความมั่นคงแห่งรัฐ และความสัมพันธ์ระหว่างประเทศทั้งสิ้น

นอกจากการโจรกรรมข้อมูลแล้ว การโจมตีระบบถือเป็นภัยคุกคามอีกรูปแบบหนึ่งที่เกี่ยวข้องกับความมั่นคงของรัฐโดยตรง แม้ว่าในอดีตที่ผ่านมาจะมีความพยายามในการโจมตีระบบที่มีผลต่อความมั่นคงปลอดภัยของประเทศ อาทิ ระบบเทคโนโลยีสารสนเทศที่มีความเกี่ยวข้องกับสาธารณูปโภคพื้นฐาน ระบบเทคโนโลยีสารสนเทศทางการทหาร เป็นต้น แต่ก็ยังไม่มีรายงานถึงความสำเร็จในการโจมตีแต่อย่างใด อย่างไรก็ตาม ยังมีการโจมตีที่ส่งผลกระทบต่อระบบที่มีผลต่อความมั่นคงปลอดภัยของประเทศโดยทางอ้อม กรณีที่ชัดเจนที่สุดได้แก่ การโจมตีด้วยวิธี Distributed Denial of Service – DDoS ที่ใช้ช่องสัญญาณอินเทอร์เน็ตถึง ๓๐๐ Gbit/s ทำให้ส่งผลกระทบต่อการใช้งานอินเทอร์เน็ตโดยรวม ซึ่งถือว่าเป็นการโจมตีที่ส่งผลต่อระบบสาธารณูปโภคพื้นฐานรูปแบบหนึ่ง

ตัวอย่างภัยคุกคามไซเบอร์ที่ได้รับความสนใจไปทั่วโลกอีกกรณีหนึ่งคือ การโจมตีโรงงานผลิตอาวุธนิวเคลียร์ และโรงงานไฟฟ้านิวเคลียร์ด้วยไวรัสคอมพิวเตอร์ Stuxnet ลักษณะเฉพาะของกรณีดังกล่าวคือ มีการใช้ไวรัสคอมพิวเตอร์เป็นเครื่องมือในสงครามไซเบอร์จริง โดยไวรัสคอมพิวเตอร์มีขีดความสามารถในการโจมตีเฉพาะเจาะจงหน่วยงานและสามารถโจมตีเป้าหมายได้ในระดับอุปกรณ์ฮาร์ดแวร์ ซึ่งถือเป็นภัยคุกคามทางไซเบอร์ที่ควรให้ความสนใจ และให้ความระมัดระวังมากขึ้นเป็นพิเศษ โดยเฉพาะอย่างยิ่งเมื่อมีการนำสงครามที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Warfare – NCW) มาปรับใช้ในเหล่าทัพต่าง ๆ ของประเทศไทย เครื่องมือ อุปกรณ์ และระบบต่าง ๆ ที่เกี่ยวข้องอาจถูกโจมตีด้วยไวรัสคอมพิวเตอร์ได้

จากความสำคัญของเทคโนโลยีสารสนเทศและผลกระทบวงกว้างของสงครามไซเบอร์ ประเทศไทยจึงมีการจัดตั้ง “คณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ” ขึ้น[๗] โดยผู้เป็นคณะกรรมการได้รับการแต่งตั้งจากบุคลากรของหน่วยงานภาครัฐที่มีความรับผิดชอบเกี่ยวข้องกับความมั่นคงและเทคโนโลยีสารสนเทศ มีหน้าที่เป็นผู้กำหนดนโยบายและแผนแม่บทความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ปัจจุบันหน่วยงานในระดับปฏิบัติการที่มีหน้าที่รับผิดชอบเกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ คือ “ศูนย์ปฏิบัติการความมั่นคงปลอดภัยทางไซเบอร์” สังกัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร โดยมีภารกิจคือ “ปกป้องดูแลสถาบันหลักของประเทศ และประชาชน ดำเนินการติดตาม เฝ้าระวัง ตรวจสอบวิเคราะห์เว็บไซต์และข้อมูลอินเทอร์เน็ตที่ไม่เหมาะสมหรือผิดกฎหมายต่างๆ อันเป็นการสนับสนุนการปฏิบัติหน้าที่ของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และหน่วยงานที่เกี่ยวข้องให้ปฏิบัติงานได้อย่างมีประสิทธิภาพ”

ทางด้านการป้องกันและปราบปราบอาชญากรรมคอมพิวเตอร์ หน่วยงานที่มีความเกี่ยวข้องโดยตรงคือ กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ปอท.) ที่มีภารกิจและความรับผิดชอบด้านการอำนวยความยุติธรรม ป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมที่เกี่ยวข้องกับเทคโนโลยี โดยการปฏิบัติหน้าที่ของ ปอท. เป็นไปในลักษณะเชิงรับที่ต้องรับเรื่องร้องเรียน ไม่ได้เป็นหน่วยงานทางด้านความมั่นคงที่สามารถปฏิบัติหน้าที่ในเชิงรุกได้

องค์กรที่มีส่วนในการป้องกันอาชญากรรมคอมพิวเตอร์อีกองค์กรหนึ่งคือ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) โดยมีภารกิจหลักคือ พัฒนา ส่งเสริมและสนับสนุนการทำธุรกรรมทางอิเล็กทรอนิกส์ของประเทศ ให้เป็นไปตามความต้องการ โครงสร้างพื้นฐานสารสนเทศที่เอื้อต่อการทำธุรกรรมทางอิเล็กทรอนิกส์ และธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ ตลอดจนการมีมาตรฐานเทคโนโลยีสารสนเทศ และการสื่อสารที่มีความมั่นคงปลอดภัยและน่าเชื่อถือ

จากภารกิจของแต่ละหน่วยงานจะเห็นได้ว่าหน่วยงานรัฐที่มีอยู่ ยังไม่สามารถป้องกันภัยคุกคามไซเบอร์ได้อย่างมีประสิทธิภาพ และมีประสิทธิผล เนื่องจากภารกิจ นโยบายของแต่ละหน่วยงานยังไม่มีการบูรณาการ และไม่สอดรับซึ่งกันและกัน ดังนั้นเพื่อป้องกัน แก้ปัญหา และบรรเทาผลกระทบ

---

๗ คำสั่งสำนักนายกรัฐมนตรี ที่ ๗๖/๒๕๕๕ เรื่อง แต่งตั้งคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Committee)

อันเกิดจากภัยคุกคามทางไซเบอร์ในลักษณะเชิงรุกแบบบูรณาการ การกำหนดแนวทางการรักษาความมั่นคงปลอดภัยทางสารสนเทศจึงมีความจำเป็นอย่างยิ่ง โดยต้องมีการกำหนดนโยบายทางด้านความปลอดภัย และทางด้านความมั่นคงทางสารสนเทศในภาพรวมของประเทศ มีการประสานงานกับหน่วยงานที่เกี่ยวข้องกับความมั่นคง หรือเกี่ยวข้องกับเทคโนโลยีสารสนเทศ ทั้งหน่วยงานภาครัฐ ภาคเอกชน องค์กรอิสระ และหน่วยงานความมั่นคงไซเบอร์ต่างประเทศ อีกทั้งต้องมีการควบคุม กำกับดูแลการปฏิบัติให้เป็นไปตามนโยบาย

เนื่องจากความมั่นคงปลอดภัยทางสารสนเทศเกี่ยวข้องกับองค์ความรู้หลากหลายด้าน และองค์ความรู้เหล่านั้นเป็นเครื่องมือที่สำคัญที่สุดในการรักษาความมั่นคงปลอดภัย การกำหนดแนวทางในการรวบรวมความรู้ สนับสนุนการสร้างความรู้ เผยแพร่ความรู้ และสนับสนุนให้มีการนำความรู้ไปใช้งาน ถือเป็นองค์ประกอบหนึ่งที่ทำให้การรักษาความมั่นคงปลอดภัยในภาพรวมเกิดประสิทธิภาพและประสิทธิผลสูงสุด ดังนั้น ผู้วิจัยจึงเห็นว่าควรที่จะศึกษาและวิจัยเพื่อให้ได้แนวความคิดในการกำหนดแนวทางการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศไทย รวมถึงการสร้างองค์ความรู้เพื่อช่วยให้หน่วยงานสามารถพัฒนาและเสริมสร้างขีดความสามารถในการตอบสนองภัยคุกคามทางไซเบอร์ในทุกรูปแบบได้อย่างมีประสิทธิภาพ และใช้ในการปรับบทบาทและโครงสร้างของหน่วยรับผิดชอบหลักเพื่อให้สามารถบูรณาการการปฏิบัติงานได้อย่างแท้จริง

วัตถุประสงค์ของการวิจัย

๑. เพื่อศึกษาวิเคราะห์ ปัญหา สาเหตุและผลกระทบที่เกิดจากภัยคุกคามทางไซเบอร์ต่อความมั่นคงปลอดภัยในด้านต่าง ๆ เช่น เศรษฐกิจ สังคม วัฒนธรรม การเมือง และการทหารเป็นต้น

๒. เพื่อศึกษา วิเคราะห์ เปรียบเทียบ แนวทางต่าง ๆ ในการรักษาความมั่นคงปลอดภัยทางสารสนเทศ

๓. เพื่อเสนอแนะแนวทางที่เหมาะสมในการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศไทยในอนาคต

ขอบเขตการวิจัย

ศึกษา วิเคราะห์บทบาท และผลกระทบของเทคโนโลยีสารสนเทศต่อความมั่นคงด้านเศรษฐกิจ สังคม วัฒนธรรม การเมืองและอื่น ๆ ที่สำคัญของประเทศไทย ประเทศที่มีความก้าวหน้าทางเทคโนโลยีสารสนเทศ และประเทศที่มีอิทธิพลทางการทหาร รวมถึงศึกษาแนวทาง ขั้นตอนการดำเนินการ และอุปสรรคข้อขัดข้อง ในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ สังเคราะห์ให้ได้

แนวทางในการป้องกัน ต่อต้าน และบรรเทาผลกระทบที่เกิดจากภัยคุกคามทางสารสนเทศของประเทศไทยในอนาคต

วิธีดำเนินการวิจัย

๑. ดำเนินการวิจัยเชิงคุณภาพ โดยรวบรวม ศึกษา และวิเคราะห์ข้อมูลที่ได้จากการศึกษาค้นคว้าจากแหล่งต่าง ๆทั้งในประเทศ และต่างประเทศ

๒. ศึกษาแนวทาง ขั้นตอนการดำเนินการ อุปสรรค ข้อขัดข้องการรักษาความมั่นคงปลอดภัยทางสารสนเทศของหน่วยงานต่าง ๆ ในประเทศไทยในปัจจุบัน

๓. ศึกษาแนวทาง และวิเคราะห์เปรียบเทียบ แนวทางการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศต่าง ๆ

๔. วิเคราะห์เพื่อหาข้อสรุป แนวทางการรักษาความมั่นคงปลอดภัยทางสารสนเทศในระยะสั้น ระยะกลาง และระยะยาว เพื่อป้องกัน ต่อต้าน และบรรเทาผลกระทบที่เกิดจากภัยคุกคามทางไซเบอร์ให้เกิดประสิทธิภาพ และประสิทธิผลสูงสุด

ประโยชน์ที่ได้รับจากการวิจัย

๑. จะทำให้ได้แนวทางในการปรับปรุงกระบวนการและรูปแบบในการกำหนดอำนาจหน้าที่ของหน่วยงานต่าง ๆ ซึ่งจะช่วยให้หน่วยงานสามารถพัฒนาและเสริมสร้างขีดความสามารถในการตอบสนองภัยคุกคามทางไซเบอร์ในทุกรูปแบบได้อย่างมีประสิทธิภาพ

๒. ได้แนวทางในการปรับบทบาทและโครงสร้างของหน่วยรับผิดชอบหลัก เพื่อให้สามารถบูรณาการการปฏิบัติงานได้อย่างแท้จริง

บทที่ ๒
การดำเนินการด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศ

แนวคิดของการรักษาความมั่นคงปลอดภัยทางสารสนเทศ

ความมั่นคงปลอดภัยทางสารสนเทศ คือ การป้องกันสารสนเทศและองค์ประกอบอื่นที่เกี่ยวข้อง ทั้งนี้การรักษาความปลอดภัยทางข้อมูลสารสนเทศ คือ ผลที่เกิดขึ้นจากการใช้ระบบของนโยบายและ/หรือ ระเบียบปฏิบัติที่ใช้ในการพิสูจน์ทราบ ควบคุม และป้องกันการเปิดเผยข้อมูล (ที่ได้รับคำสั่งให้มีการป้องกัน) โดยไม่ได้รับอนุญาต โดยแนวคิดหลักของความมั่นคงปลอดภัยทางสารสนเทศ ประกอบด้วย

๑. ความลับ (Confidentiality) เป็นการรับประกันว่าผู้มีสิทธิ์และได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลได้ โดยองค์กรต้องมีมาตรการป้องกันการเข้าถึงสารสนเทศที่เป็นความลับ เช่น การจัดประเภทของสารสนเทศ การรักษาความปลอดภัยให้กับแหล่งจัดเก็บข้อมูล กำหนดนโยบายรักษาความมั่นคงปลอดภัยและนำไปใช้ให้การศึกษาแก่ทีมงานความมั่นคงปลอดภัยและผู้ใช้ ภัยคุกคามที่เพิ่มมากขึ้นในปัจจุบัน มีสาเหตุมาจากความก้าวหน้าทางเทคโนโลยี ประกอบกับความต้องการความสะดวกสบายในการสั่งซื้อสินค้าของลูกค้า โดยการยอมให้สารสนเทศส่วนบุคคลแก่เว็บไซต์ เพื่อสิทธิ์ในการทำธุรกรรมต่าง ๆ โดยลืมไปว่าเว็บไซต์เป็นแหล่งข้อมูลที่สามารถขโมยสารสนเทศไปได้ไม่ยากนัก

๒. ความสมบูรณ์ (Integrity) หมายถึง ความครบถ้วน ถูกต้อง และไม่มีสิ่งแปลกปลอม สารสนเทศที่มีความสมบูรณ์ จึงเป็นสารสนเทศที่นำไปใช้ประโยชน์ได้อย่างถูกต้องครบถ้วน สารสนเทศจะขาดความสมบูรณ์ ก็ต่อเมื่อสารสนเทศนั้นถูกนำไปเปลี่ยนแปลง ปลอมปนด้วยสารสนเทศอื่น ถูกทำให้เสียหาย ถูกทำลาย หรือถูกกระทำในรูปแบบอื่น ๆ เพื่อขัดขวางการพิสูจน์การเป็นสารสนเทศจริง

๓. ความพร้อมใช้ (Availability) หมายถึง สารสนเทศจะถูกเข้าถึงหรือเรียกใช้งานได้อย่างราบรื่น โดยผู้ใช้หรือระบบอื่นที่ได้รับอนุญาตเท่านั้น หากเป็นผู้ใช้หรือระบบที่ไม่ได้รับอนุญาตการเข้าถึงหรือเรียกใช้งานจะถูกขัดขวางและล้มเหลวในที่สุด

๔. ความถูกต้องแม่นยำ (Accuracy) หมายถึง สารสนเทศต้องไม่มีความผิดพลาด และต้องมีค่าตรงกับความคาดหวังของผู้ใช้เสมอ เมื่อใดก็ตามที่สารสนเทศมีค่าผิดเพี้ยนไปจากความคาดหวังของผู้ใช้ ไม่ว่าจะเกิดจากการแก้ไขด้วยความตั้งใจหรือไม่ก็ตาม เมื่อนั้นจะถือว่าสารสนเทศ “ไม่มีความถูกต้องแม่นยำ”

๕. เป็นของแท้ (Authenticity) หมายถึง สารสนเทศที่ถูกจัดทำขึ้นจากแหล่งที่ถูกต้อง ไม่ถูกทำซ้ำโดยแหล่งอื่นที่ไม่ได้รับอนุญาต หรือแหล่งที่ไม่คุ้นเคยและไม่เคยทราบมาก่อน

๖. ความเป็นส่วนตัว (Privacy) หมายถึง สารสนเทศที่ถูกรวบรวม เรียกใช้ และจัดเก็บโดยองค์กร จะต้องถูกใช้ในวัตถุประสงค์ที่ผู้เป็นเจ้าของสารสนเทศรับทราบ ณ ขณะที่มีการรวบรวมสารสนเทศนั้น มิฉะนั้นจะถือว่าเป็นการละเมิดสิทธิส่วนบุคคลด้านสารสนเทศ

นอกจากนี้คณะกรรมการด้านความมั่นคงโทรคมนาคมและระบบสารสนเทศแห่งชาติ (NSTISSC : Nation Security Telecommunications and Information Systems Security) ได้กำหนดแนวคิดความมั่นคงปลอดภัยทางสารสนเทศขึ้นมา ต่อมาได้กลายเป็นมาตรฐานการประเมินความมั่นคงทางระบบสารสนเทศ โดยสิ่งสำคัญในการดำเนินงานความมั่นคงปลอดภัยทางสารสนเทศนั้นนอกจากจะมีความคิดหลักในด้านต่างๆ แล้วยังรวมถึงการกำหนดนโยบายการปฏิบัติงาน การให้การศึกษา และเทคโนโลยีที่จะนำมาใช้เป็นกลไกควบคุมและป้องกัน ที่ต้องเกี่ยวข้องกับการจัดการความมั่นคงปลอดภัยทางสารสนเทศด้วย

ประเทศที่ให้ความสำคัญเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางสารสนเทศ

โดยภาพรวมเทคโนโลยีสารสนเทศเป็นองค์ความรู้ใหม่ที่เพิ่งเกิดขึ้นใน ช่วงสงครามโลกครั้งที่สอง (พ.ศ. ๒๔๗๘ ถึง พ.ศ. ๒๔๘๘) หลังจากที่มีการคิดค้นเครื่องคอมพิวเตอร์ และระบบคอมพิวเตอร์เพื่อใช้ทางการทหาร[๑] และองค์ความรู้ด้านนี้ได้ขยายขอบเขตออกไปอย่างกว้างขวางขึ้นเมื่ออินเตอร์เน็ตเริ่มถูกนำมาใช้งานตั้งแต่ยุคสงครามเย็น[๒] ข้อสังเกตที่น่าสนใจอย่างหนึ่งคือทั้งคอมพิวเตอร์และอินเตอร์เน็ตมีจุดเริ่มต้นเพื่อใช้งานทางด้านการทหารเช่นเดียวกัน แล้วต่อมา จึงได้มีการนำมาประยุกต์ใช้งานในด้านอื่นภายหลัง

แม้จะเป็นองค์ความรู้ใหม่แต่เทคโนโลยีสารสนเทศถูกนำมาประยุกต์ใช้ในบริบทต่าง ๆ ของสังคมทำให้กลายเป็นเทคโนโลยีที่มีความสำคัญและมีความจำเป็น กระทั่งเข้ามามีบทบาทด้านความมั่นคงทั้งในแง่ของการนำมาใช้งาน และการรักษาความมั่นคงปลอดภัยทางสารสนเทศในเวลาต่อมา การปรับตัวของหน่วยงานทางด้านความมั่นคงในหลายประเทศทั่วโลกรวมถึงประเทศไทย

---

๑ Paul E. Ceruzzi, “Computing: A Concise History (MIT Press Essential Knowledge)”, The MIT Press, June 15, 2012, USA

๒ Johnny Ryan, “A History of the Internet and the Digital Future”, Reaktion Books, 2013, USA

เพื่อให้รู้เท่าทันองค์ความรู้ใหม่นี้มีความช้าเร็วแตกต่างกัน ขึ้นอยู่กับความสำคัญของเทคโนโลยีสารสนเทศต่อประเทศนั้น ๆ รวมถึงความพร้อมของหน่วยงานทางด้านความมั่นคง ทั้งในแง่ของบุคลากร การถือครองเทคโนโลยีและงบประมาณ สำหรับประเทศไทย หากนำจำนวนประชากรที่เข้าถึงอินเตอร์เน็ตมาเป็นตัวชี้วัดการเข้าถึงเทคโนโลยีสารสนเทศ โดยจำนวนประชากรในประเทศไทยสามารถเข้าถึงอินเตอร์เน็ตได้เกินกว่าร้อยละ ๑๐ ของจำนวนประชากรทั้งหมดเป็นครั้งแรกเมื่อปี ๒๕๔๗ และเกินกว่าร้อยละ ๕๐ ในปี ๒๕๕๖ ตามลำดับ[๓] เมื่อเปรียบเทียบกับประชากรในประเทศสหรัฐอเมริกาที่ประชากรกว่าร้อยละ ๕๑ สามารถเข้าถึงอินเตอร์เน็ตได้ตั้งแต่ปี ๒๕๔๓[๔] จะเห็นได้ว่าการเข้าถึงเทคโนโลยีสารสนเทศของประชากรไทยตามหลังสหรัฐอเมริกากว่าสิบปี หรือกล่าวอีกนัยหนึ่งคือ เทคโนโลยีสารสนเทศมีความสำคัญ และจำเป็นต่อประชากรของสหรัฐอเมริกามากกว่าประเทศไทยอย่างมาก ดังนั้น สหรัฐอเมริกาจึงเป็นประเทศหนึ่งที่มีความตื่นตัวและให้ความสำคัญกับความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศอย่างมาก สหรัฐอเมริกาจึงมีการจัดตั้งหน่วยงานความมั่นคงปลอดภัยทางสารสนเทศขึ้นหลายหน่วยงาน นอกจากสหรัฐอเมริกาแล้ว ยังมีอีกหลายประเทศที่ให้ความสำคัญกับความมั่นคงปลอดภัยทางสารสนเทศ เช่น มีการตั้งหน่วยงานความมั่นคงปลอดภัยทางสารสนเทศขึ้นมาเป็นการเฉพาะ การศึกษาแนวคิดและแนวทางในการตั้งหน่วยงานความมั่นคงปลอดภัยทางสารสนเทศของต่างประเทศ ถือเป็นแหล่งข้อมูลสำคัญในการวางแนวทางการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศไทยในอนาคต

ทั้งนี้การศึกษาแนวทางของต่างประเทศเพียงอย่างเดียวยังไม่สามารถนำมากำหนดแนวทางการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศไทยในอนาคตได้ หากไม่ทำความเข้าใจโครงสร้างองค์กรและภารกิจขององค์กรที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางสารสนเทศในประเทศไทย โดยในบทนี้จะมีการศึกษาการดำเนินการขององค์กรที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางสารสนเทศ และการประสานงานระหว่างองค์กรในประเทศไทย และระหว่างองค์กรในประเทศไทยกับองค์กรต่างประเทศ

การศึกษาข้อมูล ทำความเข้าใจแนวคิดการดำเนินการด้านความมั่นคงปลอดภัยทางสารสนเทศของแต่ละประเทศ จะช่วยให้เห็นภูมิทัศน์ของสถานการณ์ภัยคุกคามในปัจจุบันได้กว้างขึ้น ทั้งยังช่วยให้เข้าใจความสัมพันธ์ระหว่างประเทศในด้านการรักษาความมั่นคงปลอดภัยทาง

---

๓ Internet Information Research Network Technology Lab, “สรุปสถิติเครือข่ายอินเตอร์เน็ต”. (Online). Available : http://internet.nectec.or.th/webstats/home.iir, ๒๐๑๔

๔ U.S. Census Bureau, “Computer and Internet Use in the United States”. (Online). Available : http://www.census.gov/prod/2013pubs/p20-569.pdf, 2013

สารสนเทศอีกด้วย สิ่งเหล่านี้ล้วนเป็นข้อมูลพื้นฐานที่จะนำไปวิเคราะห์ ทำความเข้าใจในเรื่องอื่นต่อไป ซึ่งกลุ่มประเทศที่น่าสนใจได้แก่ สหรัฐอเมริกา สาธารณรัฐประชาชนจีน สหพันธ์สาธารณรัฐเยอรมนี สาธารณรัฐประชาธิปไตยประชาชนเกาหลี สาธารณรัฐเกาหลี และสหพันธ์รัฐรัสเซีย

๑. สหรัฐอเมริกา

ด้วยความสำคัญของเทคโนโลยีสารสนเทศต่อสหรัฐอเมริกาในด้านเศรษฐกิจ สังคม การเมือง และทางการทหาร สหรัฐอเมริกาถือเป็นประเทศที่มีความตื่นตัวด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศมากที่สุดประเทศหนึ่ง การรักษาความมั่นคงปลอดภัยทางสารสนเทศถูกกำหนดให้เป็นหนึ่งในยุทธศาสตร์ในการป้องกันประเทศ[๕] และทางการทหารของกองทัพสหรัฐอเมริกา[๖] และได้เพิ่มความสำคัญของการรักษาความมั่นคงปลอดภัยทางสารสนเทศมากขึ้น[๗] ภาพสะท้อนที่เห็นได้ชัดอย่างหนึ่งคือการตั้งหน่วยงานทางความมั่นคงที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางสารสนเทศของสหรัฐอเมริกา ซึ่งจะกล่าวถึงในหัวข้อ “องค์กร บทบาท หน้าที่ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางสารสนเทศของต่างประเทศ” ต่อไป

ในด้านหนึ่งสหรัฐอเมริกามีความต้องการป้องกันระบบโทรคมนาคม และเทคโนโลยีสารสนเทศของตนเองจากการภัยคุกคามทางสารสนเทศ[๘] แต่ในอีกด้านหนึ่งสหรัฐอเมริกามีแนวทางที่จะใช้เทคโนโลยีสารสนเทศเป็นเครื่องมือสนับสนุนการปฏิบัติการทางทหาร เช่น การผนวกเทคโนโลยีสารสนเทศกับอาวุธยุทโธปกรณ์ การใช้อากาศยานไร้คนขับร่วมกับเทคโนโลยีสารสนเทศในการลาดตระเวนหาข่าว เป็นต้น และยิ่งไปกว่านั้นสหรัฐอเมริกามองว่าเทคโนโลยีสารสนเทศยังสามารถนำมาประยุกต์ใช้เป็นปฏิบัติการทางทหารในเชิงรุกที่สามารถสร้างความ

---

๕ US-CERT, “The National Strategy to Secure Cyberspace”. (Online). Available : https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf, 2003

๖ กระทรวงกลาโหม สหรัฐอเมริกา, “Department of Defense Strategy for Operating in Cyberspace”. (Online). Available : http://www.defense.gov/news/d20110714cyber.pdf, 2011

๗ The New York Times, “U.S. Weighs Its Strategy on Warfare in Cyberspace”. (Online).Available:http://www.nytimes.com/2011/10/19/world/africa/united-states-weighs-cyberwarfare-strategy.html?_r=0, 2011

๘ Home Land Security, “National Cyber Incident Response Plan”. (Online). Available:http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf, 2009

เสียหายได้จริง ทั้งนี้การปฏิบัติการทางทหารในการรักษาความมั่นคงปลอดภัยทางสารสนเทศของกองทัพสหรัฐอเมริกาจะกล่าวถึงในหัวข้อ **"เหตุการณ์สำคัญอันเกี่ยวเนื่องกับการรักษาความมั่นคงปลอดภัยทางสารสนเทศ และการดำเนินการตอบโต้โดยหน่วยงานภาครัฐ"** ต่อไป

นอกจากการปรับตัวทางด้านความมั่นคงและทางการทหารแล้ว สหรัฐอเมริกายังมีการปรับตัวทางด้านอื่น ๆ ควบคู่กันไปอีกด้วย เช่น ทางด้านกฎหมายมีการออกกฎหมายที่มีชื่ออย่างไม่เป็นทางการว่า "Kill Switch Bill" ซึ่งเป็นกฎหมายที่ให้อำนาจประธานาธิบดีในการควบคุมอินเตอร์เน็ตในสถานการณ์ฉุกเฉิน[๙] และให้ความคุ้มครองโครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศในฐานะทรัพย์สมบัติของภาครัฐ กฎหมายฉบับนี้ถูกเสนอเข้าสภาสูงของสหรัฐอเมริกาใน ๑๔ มิ.ย.๕๓ โดยสมาชิกวุฒิสภาสามคนคือ วุฒิสมาชิก Joe Lieberman วุฒิสมาชิก Susan Collins และวุฒิสมาชิก Thomas Carper และเป็นกฎหมายที่ถูกวิพากษ์วิจารณ์จากสื่อสำนักต่าง ๆ อย่างกว้างขวาง

ความเคลื่อนไหวของรัฐบาลสหรัฐอเมริกาอีกหนึ่งโครงการที่ได้รับความสนใจจากสื่อและประชาชนทั่วโลกรวมถึงประชาชนของประเทศสหรัฐอเมริกาเอง คือโครงการ PRISM[๑๐] ที่กำกับดูแลโดย National Security Agency (NSA) ในโครงการนี้รัฐบาลสหรัฐอเมริกาโดย NSA มีความพยายามรวบรวมข้อมูลและข่าวกรองจากการใช้งานอินเตอร์เน็ตทั่วโลก เพื่อใช้ในการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศสหรัฐอเมริกา รวมถึงการต่อต้านการก่อการร้าย ทั้งนี้โครงการ PRISM ถูกวิพากษ์วิจารณ์อย่างมาก โดยเฉพาะในแง่มุมของการละเมิดความเป็นส่วนตัว เมื่อมีการเปิดเผยว่า เจ้าหน้าที่ในโครงการสามารถเข้าถึงข้อมูลของประชาชนโดยทั่วไปที่ใช้บริการจากผู้ให้บริการทางอินเตอร์เน็ตรายใหญ่หลายราย[๑๑] เช่น Google Facebook Microsoft Yahoo และ Apple เป็นต้น ไม่เพียงแต่หน่วยงานภาครัฐถูกวิพากษ์วิจารณ์ ผู้ให้บริการทางอินเตอร์เน็ตที่ให้ความร่วมมือกับโครงการยังได้รับผลกระทบทั้งทางด้านความน่าเชื่อถือในการให้บริการ และรายได้ของบริษัท

---

๙ Huffington Post, "Internet 'Kill Switch' Would Give President Power To Shut Down The Web". (Online).Available: http://www.huffingtonpost.com/2010/06/17/internet-kill-switch-woul_n_615923.html, 2011

๑๐ Washington Post, "NSA slides explain the PRISM data-collection program". (Online).Available:http://www.washingtonpost.com/wpsrv/special/politics/prism-collection-documents/, 2013

๑๑ The Guardian, "NSA Prism program taps in to user data of Apple, Google and others".(Online).Available:http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data, 2013

ในด้านทรัพยากรบุคคล แม้ว่าสหรัฐอเมริกาเป็นประเทศที่เป็นแหล่งรวมบุคลากรทางด้านเทคโนโลยีสารสนเทศเป็นจำนวนมาก ทั้งนี้จากการเปิดเผยของ James Gosler ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยทางสารสนเทศได้ระบุว่า ตามการคาดการณ์ของเขามีผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยทางสารสนเทศที่มีคุณวุฒิเพียงพออยู่ประมาณ ๑,๐๐๐ คน ในสหรัฐอเมริกา แต่ความต้องการผู้เชี่ยวชาญด้านนี้อยู่ที่ ๒๐,๐๐๐ ถึง ๓๐,๐๐๐ คน[๑๒] กระทั่งมีการเรียกร้องและขอความร่วมมือโดย Michael Hayden อดีตรองผู้อำนวยการสำนักงานข่าวกรองแห่งชาติสหรัฐอเมริกา (Office of the Director of National Intelligence) ให้บรรดาบุคลากรทางด้านเทคโนโลยีสารสนเทศที่เข้าร่วมการประชุม Black Hat computer security conference ในเดือน มิ.ย.๕๓ ให้ "ปฏิรูปสถาปัตยกรรมความมั่นคงปลอดภัยของอินเตอร์เน็ต"[๑๓] โดย Michael Hayden ระบุว่า "พวกคุณทำให้โลกไซเบอร์กลายเป็นที่ราบเยอรมันเหนือ"[๑๔] ทั้งนี้ไม่มีการระบุอย่างเป็นทางการว่ารัฐบาลสหรัฐอเมริกามีโครงการเสริมสร้างศักยภาพของบุคลากรด้านความมั่นคงปลอดภัยทางสารสนเทศเป็นพิเศษ เท่าที่ได้รับการเปิดเผยข้อมูล มีเพียงการร่วมกลุ่มกันของผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยทางสารสนเทศและแฮกเกอร์กันอย่างหลวม ๆ ผ่านการตั้งกลุ่มและสังคมออนไลน์ในอินเตอร์เน็ต และการพบปะกันผ่านการประชุมด้านความมั่นคงปลอดภัยทางสารสนเทศเท่านั้น

๒. สาธารณรัฐประชาชนจีน

ในช่วงสองทศวรรษที่ผ่านมาหลังจากที่มีนโยบายเปิดประเทศและปฏิรูปเศรษฐกิจแบบตลาดเสรี โดยประธานาธิบดี เติ้ง เสี่ยว ผิง จีนมีอัตราการเจริญเติบโตทางเศรษฐกิจที่สูงมากและเริ่มเข้ามามีบทบาทบนเวทีโลกในด้านต่าง ๆ มากขึ้น โดยเฉพาะอย่างยิ่งทางด้านเศรษฐกิจ[๑๕] ทั้งนี้ด้วยนโยบายทางด้านการเมืองของจีน ที่มีระบอบการปกครองแบบพรรคเดียวโดยพรรคคอมมิวนิสต์ และไม่มีนโยบายสนับสนุนเสรีภาพในการแสดงความคิดเห็น อีกทั้งการดำเนิน

---

๑๒ สำนักข่าว NPR, "Cyberwarrior Shortage Threatens U.S. Security". (Online).Available:http://www.npr.org/templates/story/story.php?storyId=128574055, 2010

๑๓ สำนักข่าว CNET, "U.S. military cyberwar: What's off-limits?". (Online).Available:http://news.cnet.com/8301-31921_3-20012121-281.html, 2010

๑๔ ที่ราบเยอรมันเหนือเป็นพื้นที่ราบที่กว้างใหญ่ อยู่ทางตอนเหนือของสหพันธ์สาธารณรัฐเยอรมนี ด้วยลักษณะทางภูมิศาสตร์ที่ให้พื้นที่ดังกล่าวถูกใช้เป็นพื้นที่เริ่มต้นในการเข้าโจมตีพื้นที่อื่น ๆ ของภาคพื้นยุโรปตะวันตกได้ง่าย - ผู้เขียน

๑๕ Dahlman, Carl J.; Aubert, Jean-Eric, "China and the Knowledge Economy: Seizing the 21st Century. WBI Development Studies", ๓๐ ม.ค. ๒๕๕๑, World Bank Publications

นโยบายทางการทหารที่แข็งกร้าวของจีน ด้วยขนาดของกองทัพที่ยิ่งใหญ่ทำให้จีนเป็นประเทศที่ถูกจับตามองจากประเทศเสรีนิยมอย่างใกล้ชิด โดยเฉพาะอย่างยิ่งจากสหรัฐอเมริกา

แม้ว่าจะไม่มีการเปิดเผยข้อมูลอย่างเป็นทางการ และการเข้าถึงข้อมูลเกี่ยวกับกองทัพของจีนเป็นไปด้วยความยากลำบาก แต่มีหลักฐานบ่งชี้ว่า จีนมีการพัฒนาขีดความสามารถด้านเทคโนโลยีสารสนเทศของตนเองอยู่ตลอดเวลา และมีความพร้อมทางด้านสงครามไซเบอร์สูง[๑๖] และหลักฐานยังบ่งชี้อีกว่ามีการลอบโจรกรรมข้อมูลของหน่วยงานภาครัฐและเอกชนในสหรัฐอเมริกา และอินเดียจากระบบเครือข่ายในประเทศจีน[๑๗] แต่ด้วยลักษณะเฉพาะของระบบเครือข่ายและอินเตอร์เน็ต จึงเป็นเรื่องที่พิสูจน์ได้ยากว่าการโจรกรรมดังกล่าวกระทำโดยรัฐบาลจีนหรือองค์กรเอกชนที่สนับสนุนโดยรัฐบาลจีน ในทางกลับกันมีการเปิดเผยจาก Edward Snowden อดีตเจ้าหน้าที่และผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยทางสารสนเทศของ NSA ว่า รัฐบาลสหรัฐอเมริกามีการจัดตั้งกลุ่มแฮกเกอร์ในการโจมตีระบบสารสนเทศของหน่วยงานภาครัฐ เอกชน รวมถึงมหาวิทยาลัยในประเทศจีนตั้งแต่ปี ๒๕๕๒[๑๘]

ด้วยขีดความสามารถทางด้านสงครามไซเบอร์ ทางเศรษฐกิจ ทางการทหาร และการดำเนินนโยบายอันแข็งกร้าวของจีนทำให้ Duncan Gardham ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยทางสารสนเทศมองว่า ปัจจุบันกำลังเข้าสู่ยุคสงครามเย็นทางไซเบอร์ (Cyber Cold War) ที่มีจีนและรัสเซียเป็นคู่ขัดแย้งสำคัญของประเทศโลกเสรีนิยม[๑๙]

---

๑๖ Jason Fritz, “How China will use cyber warfare to leapfrog in military competitiveness”. Culture Mandala: The Bulletin of the Centre for East-West Cultural and Economic Studies, Vol. 8, Iss. 1. (Online).Available:http://epublications.bond.edu.au/cgi/viewcontent.cgi?article=1110&context=cm, 2008

๑๗ The Washington Post, “Report on ‘Operation Shady RAT’ identifies widespread cyber-spying”,.(Online).Available:http://www.washingtonpost.com/national/national-security/report-identifies-widespread-cyber-spying/2011/07/29/gIQAoTUmqI_story.html, 2008

๑๘ The Japan Times, “Snowden says U.S. hacking targets China; NSA points to thwarted attacks”.(Online).Available:http://www.japantimes.co.jp/news/2013/06/14/world/u-s-hacking-effort-targets-china-snowden/#.UwcP0PgvAsk, 2013

๑๙ The Telegraph, “http://www.telegraph.co.uk/technology/news/5637243/Hackers-recruited-to-fight-new-cold-war.html”.(Online).Available : http://www.telegraph.co.uk/technology/news/5637243/Hackers-recruited-to-fight-new-cold-war.html, 2009

๓. สหพันธ์สาธารณรัฐเยอรมนี

เยอรมนีเป็นประเทศที่มีสภาพเศรษฐกิจที่ดี และมีพื้นฐานทางเศรษฐกิจที่เข้มแข็ง จนสามารถพูดได้ว่าเยอรมนีเป็นผู้นำทางเศรษฐกิจในสหภาพยุโรป รัฐบาลเยอรมนีให้ความสำคัญต่ออุตสาหกรรมอิเล็กทรอนิกส์และเทคโนโลยีสารสนเทศมาโดยตลอด และเมื่อเทคโนโลยีสารสนเทศเข้ามามีบทบาทในวิถีชีวิตของคนเยอรมันมากขึ้นเรื่อย ๆ รัฐสภาเยอรมนีนำโดยพรรคกรีน (Die Gruene) จึงตระหนักรู้ถึงความสำคัญของสันติภาพในโลกสารสนเทศ และมีการพูดถึง "นโยบายสันติภาพทางไซเบอร์" (Cyber Friedenpolitik) ครั้งแรกในรัฐสภาเยอรมนีในปี ๒๕๔๔ โดยสมาชิกสภาผู้แทนราษฎรพรรคกรีน Winfried Nachtwei[๒๐] จากนั้นเยอรมนีก็มีพัฒนาการด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศมาอย่างต่อเนื่อง กระทั่งได้มีการก่อตั้ง "ศูนย์ความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ" หรือ Nationales Cyber-Abwehrzentrum (NCAZ) ขึ้นในปี ๒๕๔๔[๒๑]

จากการเปิดเผยของ Gerhard Schindler ประธานศูนย์ข่าวกรองเยอรมนี (Bundes-nachrichtendienst) มีการโจมตีทางไซเบอร์ต่อเจ้าหน้าที่ภาครัฐของเยอรมนีเฉลี่ยวันละ ๕ กรณี[๒๒] การโจมตีส่วนมากมาจากประเทศจีน และเป็นการโจรกรรมข้อมูลที่ไม่สร้างความเสียหายมากนัก ทั้งนี้ Gerhard Schindler สันนิษฐานว่าข้อมูลที่ถูกโจรกรรมอาจถูกนำมาใช้ในการโจมตีหน่วยงานภาครัฐและหน่วยงานทางทหารของเยอรมนีต่อไปในอนาคต เนื่องจากเยอรมนีมีข้อจำกัดทางด้านงบประมาณ ทำให้ไม่สามารถเก็บรวบรวมข้อมูลที่ได้จากการจราจรบนอินเตอร์เน็ตได้มากเพียงพอต่อการการรักษาความมั่นคงปลอดภัยทางสารสนเทศ ในปี ๒๕๕๖ Hans-Peter Friedrich รัฐมนตรีว่าการกระทรวงมหาดไทยเยอรมนี ได้อนุมัติงบประมาณเป็นเงิน ๑๐๐ ล้านยูโร หรือประมาณ ๔,๔๐๐ ล้านบาท ซึ่งเป็นงบประมาณสูงสุดที่สามารถอนุมัติได้ตามกฎหมาย เพื่อใช้ในการ

---

๒๐ Manager Magazin, Cyber-Krieg: Virtuelle weiße Fahne .(Online).Available: http://www.manager-magazin.de/it/artikel/0,2828,141195,00.html, 2010

๒๑ กระทรวงมหาดไทย สหพันธรัฐเยอรมนี, "BMI-Cyberabwehrzentrum". (Online).Available:http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/ITCybersicherheit/Cybersicherheitsstrategie/Cyberabwehrzentrum/ cyberabwehrzentrum_node.html

๒๒ Der Spiegel, "Cyber Menace: Digital Spying Burdens German-Chinese Relations".(Online).Available:http://www.spiegel.de/international/world/digital-spying-burdburdens-german-relations-with-beijing-a-885444-2.html, 2013

รวบรวมข้อมูลการจราจรบนอินเตอร์เน็ตจากเดิมทำได้ร้อยละ ๕ ของปริมาณข้อมูลทั้งหมด ให้เป็นร้อยละ ๒๐ ของปริมาณข้อมูลทั้งหมด[๒๓]

ในอีกด้านหนึ่ง เนื่องจากประชาชนชาวเยอรมันมีความตื่นตัวทางด้านการเมืองที่สูง และให้ความสำคัญกับสิทธิความเป็นส่วนตัวเป็นอย่างมาก ทำให้โครงการเก็บรวบรวมข้อมูลการจราจรอินเตอร์เน็ตถูกวิพากษ์วิจารณ์ในวงกว้าง

๔. สาธารณรัฐประชาธิปไตยประชาชนเกาหลี

เกาหลีเหนือถือเป็นประเทศยากจนที่ปกครองโดยเผด็จการตระกูลคิม มายาวนานสามชั่วคน อันได้แก่ คิม อิล-ซ็อง (๒๘ ธ.ค.๑๕ – ๘ ก.ค.๓๗) คิม จ็อง-อิล (๘ ก.ค.๓๗ – ๑๗ ธ.ค. ๕๓) และคิม จ็อง-อึน (๑๗ ธ.ค.๕๓ ถึงปัจจุบัน) รวมระยะเวลากว่า ๔ ทศวรรษ ด้วยระบบเศรษฐกิจแบบปิดกอปรกับสภาพภูมิอากาศและภูมิประเทศ ทำให้เกาหลีเหนือไม่สามารถผลิตอาหารให้เพียงพอกับความต้องการของคนภายในประเทศได้ เป็นผลให้เกิดสภาวะขาดแคลนอาหาร และมีประชาชนจำนวนมากต้องเสียชีวิตจากการขาดแคลนอาหาร[๒๔] [๒๕]ด้วยเหตุนี้เกาหลีเหนือจึงจำเป็นต้องรับความช่วยเหลือทางด้านสิทธิมนุษยชนจากต่างประเทศบ่อยครั้ง[๒๖]

---

๒๓ สำนักข่าว Kazinform, “Germany to invest 100 million euros on internet surveillanc”.(Online).Available:http://www.inform.kz/eng/article/2567203, 2013

๒๔ New York Daily News, “New reports of starving North Koreans resorting to cannibalism come amid renewed tensions between Pyongyang and Washington” .(Online).Available:http://www.nydailynews.com/news/world/report-starving-north-korean-father-resorts-cannibalism-article-1.1250773, 2013

๒๕ The Huffington Post, “North Korea Hunger: Millions Of Children Deprived Of Food, Medicine, Health Care”.(Online).Available:http://www.huffingtonpost.com/2012/06/12/north-korea-hunger_n_1589029.html, 2011

๒๖ The Huffington Post, “North Korea Food Aid Approved By UN Food Body ” .(Online).Available:http://www.huffingtonpost.com/2013/06/08/north-korea-food-aid-_n_3406941.html, 2013

ตามข้อสันนิษฐานของ Richard A. Clark และ Robert Knake สาเหตุหนึ่งที่เกาหลีเหนือมีการทดลองอาวุธนิวเคลียร์ในปี ๒๕๔๙[๒๗] และปี ๒๕๕๒[๒๘] นอกจากจะเป็นการประกาศแสนยานุภาพทางการทหาร ข่มขู่ประเทศเพื่อนบ้านอย่างเกาหลีใต้ ญี่ปุ่น รวมถึงประเทศที่เป็นขั้วตรงข้ามอย่างสหรัฐอเมริกาแล้ว เป้าหมายอีกอย่างหนึ่งของเกาหลีเหนือก็เพื่อเรียกร้องให้องค์กรระหว่างประเทศให้ความช่วยเหลือกับเกาหลีเหนือในด้านต่างๆ และผลที่มักได้รับคือ ทรัพย์สินที่ได้จากการช่วยเหลือเพื่อใช้ในการบริหารประเทศโดยรัฐบาลเผด็จการต่อไป[๒๙]

เมื่อยุคแห่งข้อมูลข่าวสารและโลกดิจิตอลได้เริ่มขึ้น เกาหลีเหนือได้หันมาให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยทางสารสนเทศควบคู่กับการพัฒนาอาวุธนิวเคลียร์อย่างจริงจัง มีการตั้งหน่วยงานที่มีภารกิจในการโจมตีด้านไซเบอร์โดยเฉพาะ หน่วยงานนั้นประกอบด้วย “หน่วย ๑๑๐” “หน่วย ๑๒๑” และ “หน่วย ๒๐๔” รวมมีผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยทางสารสนเทศ และแฮกเกอร์กว่า ๓,๐๐๐ คน และมีการสร้างบุคลากรด้านนี้ด้วยการคัดเลือกนักเรียนที่มีผลการเรียนดีตั้งแต่จบประถม ให้เข้าเรียนในหลักสูตรด้านอิเล็กทรอนิกส์และเทคโนโลยีสารสนเทศเฉพาะทาง ในระดับมัธยมต้นจนถึงมหาวิทยาลัย บุคลากรเหล่านี้เมื่อจบการศึกษานอกจากจะทำงานให้กับหน่วยงานด้านสงครามไซเบอร์ที่กล่าวถึงในข้างต้น ผู้ที่ได้รับการคัดเลือกบางคนยังได้รับมอบหมายให้ปฏิบัติภารกิจแทรกซึม และบ่อนทำลายทางด้านไซเบอร์ในประเทศเพื่อนบ้านอย่างญี่ปุ่นและเกาหลีใต้อีกด้วย[๓๐]

๕. สาธารณรัฐเกาหลี

ด้วยความขัดแย้งกับประเทศเพื่อนบ้านอย่างเกาหลีเหนือ อีกทั้งพัฒนาการทางด้านเศรษฐกิจ และโทรคมนาคมแบบก้าวกระโดดจนกลายเป็นประเทศที่มีระบบโครงข่ายที่รับส่ง

---

๒๗ CNN, “North Korea pledges to test nuclear-bomb” .(Online). Available: http://edition.cnn.com/2006/WORLD/asiapcf/10/03/nkorea.nuclear/index.htm?PHPSESSID=e00207818747c2c959b7677da032e02c, 2006

๒๘ BBC, “North Korea conducts nuclear test” .(Online).Available:http://news.bbc.co.uk/2/hi/asia-pacific/8066615.stm, 2008

๒๙ Richard A.Clark และ Robert Knake, “Cyber War: The Next Threat to National Security and What to Do About It”, pp 50-56, ๑๐ เม.ย. ๒๕๕๕, Ecco, USA

๓๐ Ibid, pp 55

ข้อมูลด้วยอัตราเร็วที่สุดในโลก[๓๑] เกาหลีใต้มีความพยายามอย่างมากในการพัฒนาขีดความสามารถด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศของตนเอง ด้วยการฝึกนักเรียนนายร้อยให้มีความเชี่ยวชาญด้านสงครามไซเบอร์และด้านการแฮก[๓๒] รวมถึงความร่วมมือทางด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศกับสหรัฐอเมริกา[๓๓]

แม้กระนั้นก็ตามดูเหมือนว่าขีดความสามารถด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศของเกาหลีใต้ยังไม่เพียงพอต่อการป้องกันตนเองจากภัยคุกคาม โดยเฉพาะอย่างยิ่งจากเกาหลีเหนือ ในขณะที่เกาหลีเหนือมีบุคลากรด้านสงครามไซเบอร์กว่า ๓,๐๐๐ คน เกาหลีใต้มีบุคลากรเพียง ๔๐๐ คน[๓๔] เป็นผลทำให้เกาหลีใต้ไม่อยู่ในสภาวะที่ป้องกันตนเองจากการโจมตีทางไซเบอร์ได้ ดังจะเห็นได้จากการโจมตีเครื่องคอมพิวเตอร์กว่า ๓๐,๐๐๐ เครื่องในเดือน มี.ค.๕๖ เป็นผลทำให้ธนาคารและสถานีโทรทัศน์จำนวนหนึ่งไม่สามารถให้บริการได้[๓๕] ถือว่าเป็นการโจมตีทางไซเบอร์ที่ร้ายแรงที่สุดเท่าที่เกาหลีใต้เคยประสบ

---

๓๑ The Guardian, “South Korean 5G internet move to further increase download speeds”.(Online).Available:http://www.theguardian.com/technology/2014/jan/23/south-korea-intenet-download-speeds-5g, 2013

๓๒ The Japan Times, “‘Best of the Best’: South Korea forges youth into world’s elitecyberwarriors”.(Online) Available: http : // www.japantimes.co.jp/news/2013/03/19/asia-pacific/best-of-the-best-south-korea-forges-youth-into-worlds-elite-cyberwarriors/, 2012

๓๓ สำนักข่าว Business Korea, “Korea and US Lay Institutional Foundation for Cooperation in CyberSecurity.(Online).Available:http://www.businesskorea.co.kr/article/1601/strengthened-cyber-security-korea-and-us-lay-institutional-foundation-cooperation-cyber, 2012

๓๔ The Guardian, “North Korean ‘cyberwarfare’ said to have cost South Korea £500m”.(Online).Available:http://www.theguardian.com/world/2013/oct/16/north-korean-cyber-warfare-south-korea, 2012

๓๕ USA Today, “South Korea blames North for cyberattack”. (Online).Available:http://www.usatoday.com/story/news/world/2013/07/16/korea-cyberattacks/2520017/, 2012

จากการโจมตีดังกล่าว เกาหลีใต้ได้ตอบโต้ด้วยการประกาศการซ้อมรบ Foal Eagle ร่วมกับสหรัฐอเมริกา และเร่งพัฒนายุทธศาสตร์ในการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ และเร่งติดตั้งขีปนาวุธป้องกันภัยทางอากาศ โดยได้รับการสนับสนุนจากสหรัฐอเมริกา[๓๖]

๖. สหพันธรัฐรัสเซีย

ในสมัยสงครามเย็นรัสเซียในนามของผู้นำสหภาพโซเวียตเคยเป็นประเทศที่มีความยิ่งใหญ่ และมีอิทธิพลในด้านต่าง ๆ บนเวทีโลก โดยเฉพาะอย่างยิ่งการมีอิทธิพลต่อประเทศเพื่อนบ้าน แต่หลังจากการล่มสลายของสหภาพโซเวียต ในปี ๒๕๓๔ รัสเซียมีปัญหาภายในของตนเองที่ต้องแก้มากมายโดยเฉพาะอย่างยิ่งปัญหาเศรษฐกิจ[๓๗] หลังจากการก้าวเข้าสู่อำนาจของประธานาธิบดี Vladimir Putin ในปี ๒๕๔๓ เศรษฐกิจของรัสเซียค่อย ๆ ฟื้นตัว[๓๘] ตัวเลขผลิตภัณฑ์มวลรวมในประเทศของรัสเซียเพิ่มขึ้นจาก ๒๕๙.๘ พันล้านดอลลาร์สหรัฐในปี ๒๕๔๓ เป็น ๕๙๑ พันล้านดอลล่าร์สหรัฐในปี ๒๕๔๗[๓๙] หรือเพิ่มขึ้นกว่า ๒ เท่าในเวลา ๔ ปี หลังการฟื้นตัวทางเศรษฐกิจรัสเซียพยายามเข้ามามีบทบาทและอิทธิพลในสังคมโลก โดยเฉพาะอย่างยิ่งต่อประเทศเพื่อนบ้านของตนเองในกลุ่มประเทศยุโรปตะวันออก

รัสเซียเป็นประเทศที่มีพฤติกรรมที่น่าสนใจประเทศหนึ่งในทางสงครามไซเบอร์ ในขณะที่ทางการรัสเซียไม่ได้มีการจัดตั้งหน่วย หรือมีภารกิจที่เกี่ยวข้องกับสงครามไซเบอร์อย่างเปิดเผยหรือเป็นทางการ แต่การโจมตีทางไซเบอร์สำคัญหลายครั้งที่ผู้โจมตีได้โจมตีเป้าหมายจากประเทศรัสเซีย แม้ผู้โจมตีจะไม่ได้เป็นเจ้าหน้าที่ของรัฐ แต่ก็เคยมีการยอมรับจากแฮกเกอร์ชาวรัสเซียผู้เคยโจมตีระบบคอมพิวเตอร์ของ NATO ว่าตนเองได้รับค่าจ้างจากหน่วยข่าวกรองของ

---

๓๖ สำนักข่าว Yonhap News, “S. Korean military to prepare with U.S. for cyber warfare scenarios”.(Online) Available:http://english.yonhapnews.co.kr/national/2013/04/01/20/0301000000AEN20130401004000315F.HTML, 2012

๓๗ TP Gerber และ M Hout, “More Shock than Therapy: Market Transition, Employment, and Income in Russia, 1991-1995”, 1998, American Journal of Sociology

๓๘ Center of Strategic International Studies, “Economic Change in Russia”. (Online).Available:http://csis.org/program/economic-change-russia

๓๙ TradingandEcconomics,“RussiaGDP”.(Online).Available:http”//www.tradingeconomics.com/russia/gdp

รัสเซีย (Federal Security Service – FSB) ในการปฏิบัติการดังกล่าว[๔๐] นอกจากนี้จากการรายงานของ U.S. Cyber Consequences Unit ได้ระบุว่าการโจมตีทางไซเบอร์ที่มีเป้าหมายเป็นประเทศจอร์เจียในปี ๒๕๔๙ "รัฐบาลหรือกองทัพรัสเซียมีส่วนร่วมเล็กน้อย หรือมีส่วนร่วมโดยทางอ้อมกับปฏิบัติการ"[๔๑]

องค์กร บทบาท หน้าที่ ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยทางสารสนเทศของต่างประเทศ

แม้ว่าหลายประเทศจะมีความเกี่ยวข้องกับความมั่นคงปลอดภัยทางสารสนเทศ แต่มีเพียงไม่กี่ประเทศที่จัดตั้งองค์กรที่รับผิดชอบเกี่ยวกับความมั่นคงปลอดภัยทางสารสนเทศโดยตรง โดยมากจะมอบหมายหน้าที่การรักษาความมั่นคงปลอดภัยทางสารสนเทศให้กับหน่วยงานทางความมั่นคงที่มีอยู่เดิม ทั้งนี้การดำเนินการในแนวทางดังกล่าวมักประสบปัญหาในหลายด้าน โดยเฉพาะอย่างยิ่งในด้านบุคลากร เนื่องจากเทคโนโลยีสารสนเทศ และความมั่นคงปลอดภัยทางสารสนเทศมีลักษณะเฉพาะหลายประการ โดยเฉพาะอย่างยิ่งความรวดเร็วของเหตุการณ์ ที่แตกต่างจากภัยคุกคาม หรือองค์ความรู้ด้านอื่น ดังนั้นในหลายกรณี การมอบหมายหน้าที่การรักษาความมั่นคงปลอดภัยทางสารสนเทศให้กับหน่วยงานที่ไม่ได้มีหน้าที่โดยตรง อาจทำให้การปฏิบัติงานไม่มีประสิทธิภาพและประสิทธิผลอย่างที่ควร แนวทางหนึ่งที่ช่วยเพิ่มประสิทธิภาพและประสิทธิผล ในการรักษาความมั่นคงปลอดภัยทางสารสนเทศคือการจัดตั้งองค์กรขึ้นมาเพื่อรับผิดชอบเรื่องนี้โดยเฉพาะ ในบทนี้จะกล่าวถึงองค์กรที่รับผิดชอบเกี่ยวกับความมั่นคงปลอดภัยทางสารสนเทศของแต่ละประเทศ รวมถึงบทบาท หน้าที่ ขององค์กรเหล่านั้น

๑. United States Cyber Command

United States Cyber Command (USCYBERCOM)[๔๒] เป็นหน่วยงานทางทหารของสหรัฐอเมริกาที่มีหน้าที่ "วางแผน ประสานงาน รวบรวม ประสานความสอดคล้อง และ ดำเนินการในการอำนวยการปฏิบัติการและป้องกันหน่วยงานที่เกี่ยวข้องกับสารสนเทศและระบบเครือข่าย

---

๔๐ Andrew Meier, "Black Earth", 2546, W. W. Norton & Company, ISBN 0-393-05178-1, pp 15-16.

๔๑ The Register, "Georgian cyber attacks launched by Russian crime gangs". (Online).Available:http://www.theregister.co.uk/2009/08/18/georgian_cyber_attacks/, 2008

๔๒ (Online).Available:http://www.arcyber.army.mil/org-uscc.html

นอกจากนี้ยังมีหน้าที่ในการเตรียมความพร้อม และปฏิบัติการทางทหารด้านสงครามไซเบอร์อย่างเต็มกำลังเพื่อทำให้กองทัพสหรัฐอเมริกา และพันธมิตรสามารถปฏิบัติการทางทหารได้ในทุกมิติ รวมถึงประกันอิสรภาพในการดำเนินการรักษาความมั่นคงปลอดภัยทางสารสนเทศของกองทัพสหรัฐอเมริกา และป้องกันไม่ให้ฝ่ายตรงข้ามปฏิบัติการในแบบเดียวกัน”[๔๓]

USCYBERCOM เป็นหน่วยขึ้นตรงของ United States Strategic Command[๔๔] ปัจจุบันมี พลเอก Keith B. Alexander เป็นผู้บัญชาการ มีสถานที่ตั้ง ณ เมือง Fort Meade รัฐ Maryland สหรัฐอเมริกา จุดเริ่มต้นของ USCYBERCOM เริ่มจากการตั้งหน่วยงานด้านสงครามไซเบอร์ในกองทัพอากาศสหรัฐอเมริกา ต่อมาเมื่อมีการก่อตั้งหน่วยลักษณะเดียวกันในกองทัพเรือสหรัฐอเมริกา จึงได้เกิดแนวคิดที่จะตั้งหน่วยงานกลางด้านสงครามไซเบอร์สำหรับกองทัพสหรัฐอเมริกา และ USCYBERCOM ได้ถูกก่อตั้งขึ้นในปี ๕๓ ทั้งนี้ ในการก่อตั้งได้มีข้อถกเถียงในเรื่องบทบาทหน้าที่ของ USCYBERCOM และหน่วยงานที่เกี่ยวข้องกับสงครามไซเบอร์ของสหรัฐอเมริกาที่มีอยู่แล้วอย่าง National Security Agency (NSA) ว่าจะแยกแยะออกจากกันได้อย่างไร หรือเหตุใดต้องมีการก่อตั้ง USCYBERCOM ทั้งที่ NSA มีความพร้อมทางด้านสงครามไซเบอร์อย่างมาก ทั้งทางด้านความรู้ ข้อมูล อุปกรณ์และทรัพยากรบุคคล ข้อสรุปที่ได้คือ NSA เป็นหน่วยงานที่ไม่มีกฎหมายรองรับในการปฏิบัติการทางทหาร นั่นหมายความว่า NSA ไม่สามารถปฏิบัติการในเชิงรุกนอกเหนืออาณาเขตของสหรัฐอเมริกาได้ ดังนั้นจึงต้องมีการจัดตั้งหน่วยงานทางด้านการทหารขึ้นมาโดยเฉพาะ และ NSA ควรให้การสนับสนุนหน่วยที่ก่อตั้งเท่าที่จะสามารถกระทำได้[๔๕]

การจัดโครงสร้างของ USCYBERCOM โดยภาพรวมจะแบ่งการทำงานออกเป็นสี่เหล่าทัพ (บก เรือ อากาศ นาวิกโยธิน) เช่นเดียวกับการจัดโครงสร้างกองทัพในภาพรวม และแต่ละหน่วยขึ้นตรงจะมีหมายเลขนับต่อจากหน่วยขึ้นตรงของเหล่าทัพปกติ เช่น กองเรือที่ ๑๐ หรือ กองบินที่ ๒๔ ภายใต้สังกัด USCYBERCOM เพื่อให้แต่ละส่วนสามารถสนับสนุนการทำงานของแต่ละเหล่าทัพได้เหมาะสมกับความต้องการมากที่สุด และภายใต้หน่วยขึ้นตรงของ USCYBERCOM ที่แบ่งตามเหล่าทัพแล้ว แต่ละหน่วยขึ้นตรงก็จะมีหน่วยงานย่อยที่มีลักษณะการจัดโครงสร้าง

---

๔๓ กระทรวงกลาโหม สหรัฐอเมริกา, “Cyber Command Fact Sheet”. (Online).Available:http://www.stratcom.mil/factsheets/Cyber_Command/”, 2009

๔๔ (Online).Available:http://www.stratcom.mil/

๔๕ Richard A. Clark และ Robert Knake, “Cyber War: The Next Threat to National Security and What to Do About It”, pp 62-84, ๑๐ เม.ย. ๒๕๕๕, Ecco, USA

แตกต่างกันออกไปเช่นเดียวกัน ทั้งนี้ หน่วยย่อยต่าง ๆ จะมีการทำงานกันอย่างประสานสอดคล้องผ่านการประสานงานของกองบัญชาการ USCYBERCOM[๔๖]

นอกจากหน่วยขึ้นตรงสี่หน่วยแล้ว USCYBERCOM ยังมีหน่วยพิเศษ ที่ทำหน้าที่เฉพาะอีกดังนี้

- US Army- 35Q ผู้เชี่ยวชาญเฉพาะด้านการเข้ารหัสในระบบเครือข่าย (Cryptologic Network Warfare Specialist)
- US Navy - CTN เครือข่ายนักวิเคราะห์ด้านการเข้ารหัส
- US Air Force- 1B4X1 กองกำลังป้องกันทางไซเบอร์
- US Marine Corps- 0651 นักปฏิบัติการด้านเครือข่ายแห่งนาวิกโยธิน
- US Marine Corps- เครือข่ายนักวิเคราะห์ และปฏิบัติการด้านการเข้ารหัส

๒. **National Security Agency**

National Security Agency (NSA)[๔๗] หรือสำนักงานความมั่นคงแห่งชาติเป็นหน่วยงานข่าวกรองที่มีขอบเขตหน้าที่ทั้งในและนอกประเทศ และเป็นหน่วยงานด้านข่าวกรองที่มีขนาดองค์กรที่ใหญ่ที่สุดของสหรัฐอเมริกา มีหน้าที่ในการเฝ้าระวัง ตรวจสอบ ถอดรหัสและประมวลผลข้อมูลอิเล็กทรอนิกส์ รวมถึงรักษาความมั่นคงปลอดภัยในการรับส่งข้อมูลระหว่างหน่วยงานภาครัฐของสหรัฐอเมริกา NSA มีโครงสร้างพิเศษที่แตกต่างจากหน่วยงานภาครัฐทั่วไป ที่ทำงานภายใต้การดูแลของสองหน่วยงาน กล่าวคือ กระทรวงกลาโหมสหรัฐอเมริกา และเป็นหนึ่งในสมาชิกของ United States Intelligence Community[๔๘] ภายใต้การกำกับดูแลของ Office of the Director of National Intelligence[๔๙] นอกจากนี้ NSA ยังทำงานร่วมกับหน่วยงานข่าวกรองของประเทศพันธมิตรของสหรัฐอเมริกาอย่างเยอรมันอีกด้วย[๕๐] แม้ว่าโดยบทบาทและหน้าที่ของ NSA จะไม่เกี่ยวข้อง

---

๔๖ กระทรวงกลาโหม สหรัฐอเมริกา, “Army Forces Cyber Command Headquarters StandupPlanAnnounced”.(Online).Available:http://www.defense.gov/releases/release.aspx?releaseid=13549, 2009

๔๗ (Online).Available : http://www.nsa.gov/

๔๘ (Online).Available : http://www.intelligence.gov/

๔๙ (Online).Available : http://www.dni.gov/index.php

๕๐ Laura Poitras, นิตยสาร Der Spiegel, “Ally and Target: US Intelligence Watches Germany Closely”. (Online).Available:http://www.spiegel.de/international/world/germany-is-a-both-a-partner-to-and-a-target-of-nsa-surveillance-a-916029.html, 2012

กับสงครามไซเบอร์โดยตรง แต่ด้วยภารกิจทำให้ NSA มีขีดความสามารถด้านสงครามไซเบอร์หลายด้าน ทั้งในด้านของการป้องกันภัยจากไซเบอร์ การโจรกรรมข้อมูลทางไซเบอร์และการเข้ารหัสถอดรหัสข้อมูล โดยเฉพาะอย่างยิ่งในส่วนของการเข้ารหัสและถอดรหัสข้อมูล ทำให้ NSA เป็นองค์กรที่มีพนักงานเป็นนักคณิตศาสตร์ด้านการเข้ารหัสข้อมูลมากที่สุดของโลก[๕๑]

NSA ถูกก่อตั้งขึ้นตั้งแต่ ๔ พ.ย.๒๔๙๕ หรือหลังสงครามโลกครั้งที่สองประมาณหนึ่งทศวรรษ ปัจจุบันมีพนักงานประมาณ ๔๐,๐๐๐ คน และมีสถานที่ตั้ง ณ เมือง Fort Meade รัฐ Maryland สหรัฐอเมริกา เนื่องจาก NSA อยู่ภายใต้การควบคุมของกระทรวงกลาโหมสหรัฐอเมริกา ทำให้ NSA มีผู้อำนวยการเป็นนายทหารระดับชั้นยศพลเอก ผู้อำนวยการของ NSA ปัจจุบันคือ พลเอก Keith B. Alexander[๕๒] ซึ่งดำรงตำแหน่งผู้บัญชาการ USCYBERCOM ในเวลาเดียวกัน การที่พลเอก Keith B. Alexander ดำรงทั้งสองตำแหน่งพร้อมกัน แสดงให้เห็นถึงความสัมพันธ์เกี่ยวโยงทางภารกิจและหน้าที่ระหว่าง USCYBERCOM และ NSA รวมถึงเพื่อให้การประสานสอดคล้องระหว่างทั้งสองหน่วยงานเกิดขึ้นตั้งแต่ในระดับผู้บริหารระดับสูง

โครงสร้างของ NSA ประกอบด้วยหน่วยขึ้นตรงจำนวน ๔ หน่วยงาน โดยแบ่งแยกตามประเภทงานที่แต่ละหน่วยรับผิดชอบอันประกอบด้วย

- Central Security Service (CSS) ทำหน้าที่ในการประสานงานกับ Coast Guard สหรัฐอเมริกา และเหล่าทัพต่าง ๆ ทั้งสี่เหล่าทัพอันได้แก่ กองทัพเรือ กองทัพบก กองทัพอากาศ และนาวิกโยธิน โดยจะประสานงานในส่วนของการเข้ารหัสข้อมูลเป็นหลัก
- Directorate of Operations (DO) เป็นหน่วยขึ้นตรงหลักของ NSA ที่มีหน้าที่ในการกำกับดูแล และอำนวยการการปฏิบัติงานของ NSA
- Defense Special Missile and Astronautics Center (DEFSMAC) ทำหน้าที่ในการเฝ้าระวังภัยจากขีปนาวุธ และภัยจากอวกาศ
- Intelligence and Security Command (INSCOM) ทำหน้าที่ในการควบคุม บังคับบัญชางานทางด้านข่าวกรอง และการรักษาความมั่นคงปลอดภัยทางสารสนเทศ

เมื่อพิจารณาขีดความสามารถทางไซเบอร์แล้ว NSA ถือเป็นหน่วยงานที่มีขีดความสามารถทางไซเบอร์ และมีอิทธิพลต่อความมั่นคงปลอดภัยทางสารสนเทศสูงสุดหน่วยงานหนึ่งของโครงการ PRISM จะเห็นได้ว่า NSA สามารถดักฟังและประมวลผลข้อมูลสารสนเทศที่ถูก

---

๕๑ NSA, “About NSA”. (Online).Available : http://www.nsa.gov/about/, 2008

๕๒ NSA, “Leadership”. (Online).Available : http://www.nsa.gov/about/leadership/, 2008

ส่งผ่านอินเตอร์เน็ตได้เกือบทั้งหมด โดยเฉพาะอย่างยิ่งข้อมูลเหล่านั้นถูกเก็บรักษาโดยผู้ให้บริการสัญชาติสหรัฐอเมริกา เช่น Facebook Google และ Microsoft เป็นต้น[๕๓] และจากการเปิดเผยของ Edward Snowden อดีตเจ้าหน้าที่ด้านความปลอดภัยทางสารสนเทศของ NSA ทำให้ทราบว่า NSA สามารถดักฟังโทรศัพท์ได้เกือบทั่วโลก และมีการดักฟังโทรศัพท์ของผู้นำในประเทศต่าง ๆ[๕๔] ซึ่งสร้างความไม่พอใจให้กับผู้นำเหล่านั้นเป็นอย่างมาก ล่าสุดมีการเปิดเผยข้อมูล ว่า NSA สามารถดักฟังโทรศัพท์คนอเมริกาได้ทั้งหมด[๕๕] ด้วยขีดความสามารถต่าง ๆ เหล่านี้ ทำให้ NSA ถูกจับตามองด้วยภาพลบจากทั้งพลเมืองของสหรัฐอเมริกา พลเมืองประเทศอื่น ๆ และภาครัฐของประเทศต่าง ๆ แม้แต่อดีตประธานาธิบดีสหรัฐอเมริกาอย่าง Jimmy Carter ก็มีความรู้สึกไม่ไว้วางใจ NSA และประเมินว่าตนเองถูกดักฟังจาก NSA[๕๖]

ในอีกด้านหนึ่ง NSA ก็เป็นผู้กำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยทางสารสนเทศ โดยเฉพาะอย่างยิ่งในการเข้ารหัสข้อมูล NSA Suit B[๕๗] เป็นการรวบรวมกรรมวิธีเข้ารหัสข้อมูลที่ผ่านมาตรฐานความปลอดภัยของ NSA และเป็นที่นิยมใช้ในการเข้ารหัสข้อมูลเพื่อรักษาความมั่นคงปลอดภัยทางสารสนเทศ ซึ่งประกอบด้วย

- Elliptic Curve Diffie–Hellman (ECDH)
- Secure Hash Algorithm 2 (SHA-256 and SHA-384)

---

๕๓ Timothy B. Lee, หนังสือพิมพ์ Washington Post, “Here’s everything we know about PRISM to date”. (Online).Available : http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/, 2012

๕๔ สำนักข่าว BBC, “Edward Snowden: Leaks that exposed US spy programme”. (Online).Available : http://www.bbc.com/news/world-us-canada-2312396, 2012

๕๕ หนังสือพิมพ์ Washington Post, “NSA surveillance program reaches ‘into the past’ to retrieve, replay phone calls” (Online).Available : http://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.htm, 2014

๕๖ Rebecca Shabad, สำนักข่าว The Hill, “Carter fears NSA is spying on his emails”.(Online).Available : http://thehill.com/blogs/hillicon-valley/technology/201479-carter-fears-nsa-is-spying-on-his-emails, 2014

๕๗ NSA, “Suite B Cryptography / Cryptographic Interoperability”.(Online).Available : http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml, 2014

- Advanced Encryption Standard (AES)
- Elliptic Curve Digital Signature Algorithm (ECDSA)

๓. Nationales Cyber-Abwehrzentrum

Nationales Cyber-Abwehrzentrum (NCAZ)[๕๘] เป็นหน่วยงานกลางของสหพันธ์สาธารณรัฐเยอรมนี ที่มีหน้าที่ในการป้องกันภัยจากการโจมตีทางอิเล็กทรอนิกส์และไซเบอร์ ทั้งในแง่ความมั่นคงแห่งสหพันธ์สาธารณรัฐ และความมั่นคงในทางเศรษฐกิจ รวมถึงการรักษาความมั่นคงปลอดภัยทางสารสนเทศให้กับโครงสร้างพื้นฐานของเยอรมนี[๕๙] การดำเนินการของ NCAZ จะถูกกำหนดให้สอดคล้องกับ “ยุทธศาสตร์ทางไซเบอร์สำหรับเยอรมนี”[๖๐] ข้อสังเกตจากหน้าที่ของ NCAZ ที่สำคัญประการหนึ่งคือ การรักษาความมั่นคงทางเศรษฐกิจถูกระบุเพิ่มเติมจากหน้าที่อื่น ๆ อย่างชัดเจน แตกต่างจากหน่วยงานด้านสงครามไซเบอร์ของสหรัฐอเมริกา ที่ไม่ได้กล่าวถึงการรักษาความมั่นคงทางเศรษฐกิจในหน้าที่หลักของหน่วยงาน

NCAZ ก่อตั้งขึ้นเมื่อ ๒๓ ก.พ.๕๔ เป็นหน่วยในสังกัดกระทรวงมหาดไทยของสหพันธ์สาธารณรัฐเยอรมนี ขึ้นตรงกับ Bundesamt für Sicherheit in der Informationstechnik (BSI)[๖๑] ทำให้เห็นเจตนาการจัดตั้ง NCAZ อย่างชัดเจนว่ามีขึ้นเพื่อรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับกิจการภายใน มากกว่าจะเป็นการดำเนินการทางไซเบอร์ในเชิงรุก ซึ่งแตกต่างกับสหรัฐอเมริกา โดยโครงสร้างของ NCAZ ถือเป็นหน่วยงานเฉพาะกิจ ที่ไม่สามารถดำเนินกิจการด้วยตนเอง หรือมีเจ้าหน้าที่สังกัดหน่วยโดยตรงได้ เนื่องด้วยข้อกำหนดตามกฎหมายรัฐธรรมนูญของเยอรมนี ทำให้ลักษณะดำเนินการของ NCAZ เป็นการดำเนินการร่วมระหว่างเจ้าหน้าที่จากหน่วยงานต่าง ๆ ดังนี้

---

๕๘ ศูนย์ป้องกันภัยทางไซเบอร์แห่งชาติ แปลโดยผู้เขียน

๕๙ กระทรวงมหาดไทย สหพันธ์สาธารณรัฐเยอรมนี, “Nationales Cyber-Abwehrzentrum”. (Online).Available:http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/IT- Cybersicherheit/Cybersicherheitsstrategie/Cyberabwehrzentrum/cyberabwehrzentrum_node.html

๖๐ กระทรวงมหาดไทย สหพันธ์สาธารณรัฐเยอรมนี, “Cyber Sicherheitsstrategie fuer Deutschland”.(Online).Available:http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf, 2011

๖๑ สำนักงานกลางด้านความปลอดภัยทางสารสนเทศ แปลโดยผู้เขียน

- BSI โดยเจ้าหน้าที่หลักของ NCAZ จะมาจาก BSI
- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)[๖๒]
- Bundeskiminalamt[๖๓]
- Bundesnachrichtendienst[๖๔]
- Bundespolizei[๖๕]
- Bundeswehr[๖๖]
- Zollkriminalamt[๖๗]

ด้วยลักษณะการจัดโครงสร้างที่เป็นการดำเนินการร่วม และมีจำนวนเจ้าหน้าที่ในสังกัดที่น้อย ทำให้ NCAZ ถูกวิจารณ์ว่าไม่น่าจะมีศักยภาพพอที่จะสามารถป้องกันภัยคุกคามทางไซเบอร์ให้กับสหพันธ์สาธารณรัฐเยอรมนีได้[๖๘] และหลังจากที่ NCAZ เริ่มปฏิบัติภารกิจได้ไม่นาน นักแฮกเกอร์ภายใต้ชื่อ No-Name-Crew ได้เจาะเข้าไปในเครื่องคอมพิวเตอร์แม่ข่ายของสรรพากร ซึ่งเป็นหน่วยงานที่ NCAZ รับผิดชอบดูแลความมั่นคงปลอดภัยทางสารสนเทศ การเจาะระบบดังกล่าวทำให้กลุ่มแฮกเกอร์สามารถดึงเอาข้อมูลตำบลที่เรือที่ส่งมายังสรรพากรผ่านระบบเครือข่ายไปได้[๖๙]

---

๖๒ สำนักงานกลางเพื่อการพิทักษ์ราษฎรและช่วยเหลือบรรเทาภัยพิบัติ แปลโดยผู้เขียน

๖๓ สำนักงานป้องกันและปราบปรามอาชญากรรมแห่งชาติ แปลโดยผู้เขียน

๖๔ สำนักงานข่าวกรองแห่งชาติ แปลโดยผู้เขียน

๖๕ สำนักงานตำรวจแห่งชาติ แปลโดยผู้เขียน

๖๖ กองทัพแห่งชาติ

๖๗ สำนักงานสืบสวนการกระทำความผิดทางด้านภาษีอากร

๖๘ Andreas Schwarzkopf, สถานีโทรทัศน์ Frankfurter Rundschau, “Dünner Schutz-schild. Kommentar zum Cyber-Abwehrzentrum”. (Online).Available : http://www.fr-online.de/politik/meinung/duenner-schutzschild/-/1472602/7402236/-/index.html, 2011

๖๙ Jenna Behrends, Axel Spilcker, Thomas van Zütphen, นิตยสาร FOCUS, “Angriff auf Zoll-Computer: Hacker überlisten Antiviren-Software”. (Online).Available : http://www.focus.de/digital/computer/tid-22964/angriff-auf-zoll-computer-hacker-ueberlisten-antiviren-software_aid_646219.html, 2011

การรักษาความมั่นคงปลอดภัยทางสารสนเทศของต่างประเทศ

อินเตอร์เน็ตได้กลายเป็นพื้นที่ใหม่ทางด้านเศรษฐกิจ ที่เหล่าบรรดาผู้ประกอบการ ต่างให้ความสนใจ เป็นพื้นที่สังคมออนไลน์ที่ผู้คนหลายร้อยล้านคนทั่วโลกใช้ทำกิจกรรมทางสังคมในทุกวัน แต่ในอีกด้านหนึ่งอินเตอร์เน็ตได้กลายเป็นพื้นที่ก่ออาชญากรรมและสมรภูมิทางการทหารที่มีการสู้รบอยู่เป็นเนืองนิจ ดังนั้นประเทศที่มีภัยคุกคามทางไซเบอร์สูงดังกล่าวข้างต้น นอกจากต้องเตรียมความพร้อม ด้วยการจัดตั้งหน่วยงานขึ้นมารับผิดชอบด้านความมั่นคงปลอดภัยทางสารสนเทศแล้ว การกำหนดแนวทาง การออกนโยบายเพื่อรักษาความมั่นคงปลอดภัยทางสารสนเทศถือเป็นสิ่งจำเป็นและมีความสำคัญไม่แพ้กัน

๑. สหรัฐอเมริกา

นอกจากการจัดตั้ง USCYBERCOM ขึ้นมาเพื่อปฏิบัติหน้าที่เกี่ยวกับสงครามไซเบอร์ขึ้นมาเป็นการเฉพาะ และมี NSA เป็นหน่วยงานที่มีขีดความสามารถทางสงครามไซเบอร์สูงที่ให้การสนับสนุน USCYBERCOM แล้ว สหรัฐอเมริกายังได้กำหนดให้สงครามไซเบอร์มีความสำคัญเทียบเท่ากับกองทัพทั้งสี่เหล่า[๗๐] และมีการจัดตั้งหน่วยขึ้นตรงภายใต้ USCYBERCOM ที่มีการจัดโครงสร้างเหมือนกับหน่วยขึ้นตรงทั้งสี่เหล่าทัพ เพื่อให้การสนับสนุนแต่ละเหล่าทัพเกิดประสิทธิภาพสูงสุด[๗๑]

แนวทางการรักษาความมั่นคงปลอดภัยทางสารสนเทศของสหรัฐอเมริกาจะใช้นโยบาย **"เสาห้าต้น"** (The five Pillars)[๗๒] [๗๓]เป็นหลัก โดยเสาทั้งห้าต้นนั้นประกอบด้วย

- กำหนดให้พื้นที่ Cyberspace เป็นพื้นที่สงครามที่มีความสำคัญเทียบเท่ากับพื้นที่สงครามอื่น ๆ
- เพิ่มขีดความสามารถในการป้องกันเชิงรุกสำหรับสงครามไซเบอร์

---

๗๐ United State Joint Force Command, "The Joint Operating Environment". (Oline).Available:.http://wayback.archive.org/web/20130810043238/http://www.jfcom.mil/newslink/storyarchive/ 2010/JOE_2010_o.pdf, 2011

๗๑ กระทรวงกลาโหม สหรัฐอเมริกา, "Army Forces Cyber Command Headquarters Standup Plan Announced". (Online).Available : http://www.defense.gov//releases/release.aspx?releaseid=13549, 2010

๗๒ Karen Parrish กระทรวงกลาโหม สหรัฐอเมริกา, "Lynn: Cyber Strategy's Thrust is Defensive". (Online).Available : http://www.defense.gov/news/newsarticle.aspx?id=64682, 2012

๗๓ สำนักข่าว Red Orbits, "Official: NATO Should Build A 'Cyber Shield". (Oline).Availablehttp://www.redorbit.com/news/technology/1918102/official_nato_should_build_a_cyber_shield/, 2010

• ป้องกันโครงสร้างพื้นฐานหลักสำหรับระบบโทรคมนาคมและเทคโนโลยีสารสนเทศ

• เพิ่มประสิทธิภาพในการปฏิบัติภารกิจร่วมทั้งระหว่างเหล่าทัพ และระหว่างสหรัฐอเมริกาและประเทศพันธมิตร

• รักษาความเป็นผู้นำทางด้านเทคโนโลยีสารสนเทศ

ปัจจุบันสหรัฐอเมริกาได้กำหนดให้สงครามไซเบอร์เป็น "เหตุแห่งสงคราม"[๗๔] [๗๕]ไม่ต่างจากการใช้กำลังทางทหารและอาวุธด้วยวิธีการอื่น ๆ ทำให้ใน ๑๘ ก.ย.๕๕ Harold Koh แห่งกระทรวงการต่างประเทศสหรัฐอเมริกาได้พยายามผลักดันให้มีการกำหนดในกฎหมายระหว่างประเทศว่าด้วยการโจมตีทางไซเบอร์ในฐานะการใช้กำลัง และเสนอให้มีการแก้ไขปรับปรุง "กฎการใช้กำลัง" ในกฎหมายระหว่างประเทศเพื่อมารองรับการโจมตีทางไซเบอร์ด้วย[๗๖] และมีข้อเสนอจากกระทรวงกลาโหมสหรัฐว่าควรมีการใช้อาวุธนิวเคลียร์เพื่อตอบโต้ ในกรณีที่มีการโจมตีทางไซเบอร์[๗๗] นอกจากนี้ พลเอก Keith B. Alexander ผู้บัญชาการ USCYBERCOM และผู้อำนวยการ NSA ได้เสนอการทำข้อตกลงระหว่างสหรัฐอเมริกากับรัสเซีย ในการจำกัดการโจมตีทางไซเบอร์ระหว่างสองประเทศ[๗๘]

๒. สาธารณรัฐประชาชนจีน

ข้อมูลเกี่ยวกับแนวทาง และการจัดตั้งหน่วยสำหรับการรักษาความมั่นคงปลอดภัยทางสารสนเทศของจีนไม่ได้รับการเปิดเผยต่อสาธารณะมากนัก อย่างไรก็ตามจากเหตุการณ์อันเกี่ยวข้อง

---

๗๔ ภาษาลาติน Causus Belli หมายถึง เหตุผลสำหรับการปฏิบัติแห่งสงคราม

๗๕ David E. Sanger, หนังสือพิมพ์ New York Times, "Pentagon to Consider Cyberattacks Acts of War". (Online).Available:http://www.nytimes.com/2011/06/01/us/politics/01cyber.html?_r=0, 2011

๗๖ Aram Roston, สำนักข่าว Army Times, "U.S.: Laws of war apply to cyber attacks".(Online).Available:http://www.armytimes.com/mobile/news/2012/09/dn-laws-of-war-apply-cyber-attacks-091812, 2012

๗๗ Conte, Andrew, สำนักข่าว Stripes.com "Nuke option necessary in case of massive cyberwar, report concludes".(Online).Available:http://www.stripes.com/nuke-option-necessary-in-case-of-massive-cyberwar-report-concludes-1.210515, 2013

๗๘ หนังสือพิมพ์ Post, "WSJ: U.S. Backs Talks on Cyber Warfare". (Oline).Available:http://online.wsj.com/news/articles/SB10001424052748703340904575284964215965730, 2010

กับสงครามไซเบอร์ที่ผ่านมาแสดงให้เห็นว่าจีนมีความตื่นตัวเกี่ยวกับสงครามไซเบอร์ที่สูงมาก จากการวิเคราะห์ของ Richard A. Clark[๗๙] เขาเชื่อว่าหลังจากที่จีนได้เห็นปฏิบัติการ "พายุทะเลทราย" ในสงครามอ่าวครั้งที่หนึ่ง[๘๐] ในช่วงปี ๒๕๓๓ ทำให้จีนเริ่มตระหนักถึงความสำคัญของสงครามไซเบอร์มากขึ้น ในปฏิบัติการทางทหารดังกล่าวกองทัพสหรัฐอเมริกา ได้นำเทคโนโลยีสารสนเทศมาใช้ร่วมกับอาวุธยุทโธปกรณ์อื่น ๆ ทำให้การปฏิบัติมีความเที่ยงตรง แม่นยำมากขึ้นใช้งบประมาณในภาพรวมที่น้อยลง

ก่อนหน้าปฏิบัติการพายุทะเลทราย จีนมีความพยายามในการพัฒนาขีดความสามารถกองทัพ ด้วยการเพิ่มปริมาณอาวุธ และกองกำลังทางทหาร[๘๑] เพื่อผลักดันให้ตนเองเป็นหนึ่งในมหาอำนาจทางการทหาร แต่เนื่องจากเศรษฐกิจของจีนในช่วงเวลาดังกล่าว ไม่ได้แข็งแกร่งมากนัก ทำให้จีนใช้งบประมาณสำหรับกองทัพเฉลี่ยต่อปีอยู่ที่ ๗๐,๐๐๐ ล้านดอลลาร์สหรัฐ ซึ่งคิดเป็นอัตราส่วนหนึ่งในแปดของงบประมาณกองทัพสหรัฐอเมริกา[๘๒] หลังจากปฏิบัติการพายุทะเลทราย จีนจึงมองเห็นช่องทางในการพัฒนาขีดความสามารถของกองทัพให้รวดเร็วกว่าเดิม แต่ใช้งบประมาณน้อยลงกว่าเดิม และแนวทางการพัฒนาขีดความสามารถของกองทัพจีนหลังจากนั้นจะอยู่ภายใต้กรอบนโยบาย "สงครามอสมมาตร"[๘๓] ที่จีนพยายามใช้ความรู้ และผลงานวิจัยทางด้านเทคโนโลยีสารสนเทศมาปรับใช้กับกองทัพของตนในทุก ๆ ด้าน โดยผู้เชี่ยวชาญวิเคราะห์ว่าด้วยแนวทางสงครามอสมมาตรของจีน อาจทำให้ขีดความสามารถของกองทัพจีนขึ้นมาเทียบชั้นกับขีดความสามารถกองทัพสหรัฐอเมริกาได้

---

๗๙ Richard A. Clark และ Robert Knake, "Cyber War: The Next Threat to National Security and What to Do About It", pp 62-84, ๑๐ เม.ย. ๒๕๕๕, Ecco, USA

๘๐ US History, "60a. Operation Desert Storm". (Online).Available: http://www.ushistory.org/us/60a.asp

๘๑ กระทรวงกลาโหม สหรัฐอเมริกา, "The Military Power of the People's Republic of China 2005". (Online).Available:http://www.defense.gov/news/jul2005/d20050719china.pdf, 2005

๘๒ Richard A. Clark และ Robert Knake, "Cyber War: The Next Threat to National Security and What to Do About It", pp 62-84, ๑๐ เม.ย. ๒๕๕๕, Ecco, USA

๘๓ Loro Hort, Yale Global, "The Dragon's Spear: China's Asymmetric Strategy". (Online) .Available:http://yaleglobal.yale.edu/content/dragon%E2%80%99s-spear-china%E2%80%99s-asymmetric-strategy, 2013

จากการพัฒนาขีดความสามารถทางด้านเทคโนโลยีสารสนเทศของจีนดังกล่าว จึงเป็นที่มาของการจัดตั้งหน่วย “กองทัพออนไลน์สีน้ำเงิน” ขึ้นในปี ๕๔[๙๔] ที่นอกจากจะรับผิดชอบในสงครามไซเบอร์แล้ว ยังมีส่วนร่วมในการรวบรวมข่าวกรองผ่านโลกออนไลน์อีกด้วย และจากการเปิดเผยข้อมูลทำให้ทราบว่าหน่วยงานดังกล่าว ไม่ใช่หน่วยงานแรกของกองทัพจีน ที่มีหน้าที่รับผิดชอบเกี่ยวกับสงครามไซเบอร์

ในเหตุการณ์การโจมตีทางไซเบอร์ รวมถึงการจารกรรมข้อมูลผ่านโลกไซเบอร์หลายครั้ง รัฐบาลจีนตกเป็นผู้ต้องหาทั้งในฐานะผู้สั่งการ ตัวการร่วม หรือผู้สนับสนุน และแม้ว่าหลักฐานที่บ่งชี้ถึงการอยู่เบื้องหลังของรัฐบาลจีนจะมีมากขึ้นอย่างต่อเนื่อง[๙๕] แต่จนถึงปัจจุบันยังไม่มีหลักฐานใด ๆ สามารถเชื่อมโยงเหตุการณ์เหล่านั้นกลับไปยังรัฐบาลจีนได้ และรัฐบาลจีนก็ให้การปฏิเสธมาตลอด [๙๖]

๓. สหพันธ์สาธารณรัฐเยอรมนี

การจัดตั้ง **NCAZ** ถือเป็นส่วนหนึ่งของยุทธศาสตร์การรักษาความมั่นคงปลอดภัยทางสารสนเทศของเยอรมนี[๙๗] ที่ออกโดยกระทรวงมหาดไทย โดยสาระสำคัญของแผนยุทธศาสตร์ฉบับนี้เป็นไปเพื่อป้องกันตนเองจากภัยคุกคามทางไซเบอร์ ทั้งทางด้านความมั่นคงและเศรษฐกิจ รวมถึงการป้องกันและปราบปรามอาชญากรรมที่เกี่ยวกับคอมพิวเตอร์ ซึ่งถือเป็นลักษณะที่ค่อนข้างเฉพาะเพราะในประเทศอื่น ๆ มักแยกการรักษาความมั่นคงปลอดภัยทางสารสนเทศออกจากอาชญากรรมที่เกี่ยวกับคอมพิวเตอร์ค่อนข้างชัดเจน

---

๙๔ Hannah Beech, นิตยสาร Time, “Meet China’s Newest Soldiers: An Online Blue Army”.(Online).Available:http://world.time.com/2011/05/27/meet-chinas-newest-soldiers-an-online-blue-army/, 2011

๙๕ Riley, Michael, Dune Lawrence, สำนักข่าว Bloomberg, “Hackers Linked to China’s Army Seen From EU to D.C.”. (Online).Available:http://www.bloomberg.com/news/2012-07-26/china-hackers-hit-eu-point-man-and-d-c-with-byzantine-candor.html, 2012

๙๖ สำนักข่าว Business Week, “China's Response to BusinessWeek”. (Online).Available:http://www.businessweek.com/stories/2008-04-09/chinas-response-to-businessweek, 2008

๙๗ กระทรวงมหาดไทย สหพันธ์สาธารณรัฐเยอรมนี, “Cyber Sicherheitsstrategie fuer Deutschland”.(Online).Available:http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf, 2011

ยุทธศาสตร์ดังกล่าวมีเป้าหมายและวิธีการแบ่งออกเป็น ๑๐ ประการได้ดังต่อไปนี้

๑ ป้องกันโครงสร้างทางเทคโนโลยีสารสนเทศพื้นฐานที่สำคัญ เพื่อให้ระบบเทคโนโลยีสารสนเทศในภาพรวมสามารถทำงานได้

๒ ป้องกันระบบเทคโนโลยีสารสนเทศในประเทศ

๓ เพิ่มความเข้มงวดในระบบรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศสำหรับงานรัฐกิจที่ใช้ในการบริการประชาชน

๔ ตั้ง NCAZ

๕ ตั้งสภารักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศแห่งชาติ

๖ เพิ่มมาตรการการป้องกันและปราบปรามอาชญากรรมทั้งในและนอกโลกไซเบอร์

๗ การทำงานร่วมกับหน่วยงานด้านความปลอดภัยทางสารสนเทศทั้งในสหภาพยุโรปและทั่วโลกอย่างมีประสิทธิผล

๘ การนำเทคโนโลยีสารสนเทศที่น่าเชื่อถือและไว้ใจได้มาใช้งาน

๙ เพิ่มขีดความสามารถบุคคลากรในหน่วยงานภาครัฐ

๑๐ การพัฒนาและนำอุปกรณ์ป้องกันภัยทางเทคโนโลยีสารสนเทศมาใช้งาน

เหตุการณ์สำคัญอันเกี่ยวเนื่องกับการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศต่างๆ

ยิ่งเทคโนโลยีสารสนเทศมีความสำคัญมากขึ้นเพียงใด ปฏิบัติการทางสงครามไซเบอร์หรือเหตุการณ์ที่เกี่ยวเนื่องกับสงครามไซเบอร์ก็ยิ่งมีความถี่ในการเกิดเหตุการณ์ และผลกระทบที่เกิดขึ้นก็ยิ่งทวีความรุนแรงมากขึ้นเท่านั้น ทั้งฝ่ายรุกและฝ่ายตั้งรับต้องพัฒนาขีดความสามารถของฝ่ายตนเองตลอดเวลา เพื่อเตรียมความพร้อมในการตอบโต้อีกฝ่ายอยู่เสมอ ข้อแตกต่างสำคัญของสงครามไซเบอร์ที่แตกต่างจากสงครามอื่น คือ อัตราเร็วของการเปลี่ยนแปลงเทคโนโลยี ในการวิจัยและพัฒนาเพื่อให้ได้เทคโนโลยีทางด้านการทหารใหม่ ๆ เพื่อนำมาทดแทนเทคโนโลยีเดิม โดยปกติแล้วจะใช้เวลาหลายปี หรืออาจเป็นทศวรรษ แต่ในทางเทคโนโลยีสารสนเทศ ช่วงระยะเวลาไม่กี่เดือนมีเทคโนโลยีใหม่เกิดขึ้นมากมาย และอาจทำให้เทคโนโลยีที่ทันสมัยที่สุดก่อนหน้ากลายเป็นเทคโนโลยีที่ล้าสมัยไปพร้อมกัน การเตรียมความพร้อมและติดตามสถานการณ์และเหตุการณ์ทางสงครามไซเบอร์จึงเป็นเรื่องที่สำคัญยิ่ง

ในบทนี้จะรวบรวมและสรุปเหตุการณ์สำคัญที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางสารสนเทศที่เกิดขึ้นในประเทศต่าง ๆ รวมถึงแนวทาง และการดำเนินการตอบโต้โดยหน่วยงานภาครัฐของประเทศนั้นๆ เพื่อเป็นข้อมูลในการศึกษาและวิเคราะห์แนวทางในการรักษาความมั่นคงปลอดภัยทางสารสนเทศในประเทศไทยต่อไป

๑. ปฏิบัติการ Orchard การโจมตีซีเรียโดยกองทัพอิสราเอล

ภายใต้ความสัมพันธ์ที่ไม่สู้ดีนักระหว่างอิสราเอลกับซีเรียนับตั้งแต่การก่อตั้งประเทศอิสราเอลกระทั่งปัจจุบัน มีการสู้รบและโจมตีระหว่างสองประเทศนับครั้งไม่ถ้วน แต่ครั้งที่น่าสนใจและอาจมีความเกี่ยวพันกับสงครามไซเบอร์มากที่สุด คือ ปฏิบัติการ Orchard [๘๘] ที่เครื่องบิน F 15I จำนวน ๑๐ ลำจากฝูงบินที่ ๖๙ ของกองทัพอากาศอิสราเอล ได้เข้าไปทิ้งระเบิดยังอาคารหลังหนึ่งในประเทศซีเรีย เมื่อ ๖ ก.ย. ๒๕๕๐ ทางการอิสราเอลได้ให้เหตุผลในการทิ้งระเบิดดังกล่าวในภายหลังว่า อิสราเอลมีข้อมูลข่าวกรองที่บ่งชี้ว่าทางการซีเรียมีความพยายามในการผลิตเตาปฏิกรณ์นิวเคลียร์เพื่อใช้ในการผลิตอาวุธนิวเคลียร์

ปฏิบัติการดังกล่าวหากพิจารณาในเบื้องต้นแทบจะไม่พบความเกี่ยวเนื่องกับสงครามไซเบอร์ใด ๆ ทั้งนี้เมื่อพิจารณาข้อเท็จจริงที่ว่า เครื่องบินรบของอิสราเอลสามารถบินเข้าทำลายเป้าหมายโดยไม่ถูกตรวจพบจากเรดาร์ตรวจการณ์ทางอากาศ และกองบัญชาการควบคุมภาคพื้นดินของซีเรีย โดยที่เครื่องบินรบที่ปฏิบัติภารกิจในครั้งนี้ไม่มีเครื่องบินลำใดที่เป็นเครื่องบินล่องหน (Stealth Aircraft) และจากการตรวจสอบของซีเรียก็ไม่พบความบกพร่องในการปฏิบัติหน้าที่ของเจ้าหน้าที่ที่เกี่ยวข้องกับเรดาร์ตรวจการณ์ทางอากาศแต่อย่างใด

ตามข้อสันนิษฐานของ Richard A. Clark และ Robert Knake [๘๙] และ บริษัท Airforce Technology [๙๐] [๙๑]การที่เครื่องบินรบของอิสราเอลสามารถหลุดรอดการตรวจพบของเรดาร์ตรวจการณ์ไปได้ ย่อมหมายถึงการที่ระบบรักษาความมั่นคงปลอดภัยทางสารสนเทศที่แน่นหนาของซีเรียถูกเจาะและมีแนวทางที่เป็นไปได้ ๓ ประการคือ

๑. การส่งซอฟท์แวร์จำพวก ไวรัส มัลแวร์ โทรจัน หรืออื่น ๆ เข้าไปรบกวนการทำงานของเรดาร์ตรวจการณ์ซีเรีย รวมถึงสร้างเป้าลวงบนหน้าจอเรดาร์เพื่อไม่ให้เจ้าหน้าที่ของซีเรียเกิดความสงสัย ทำโดยส่งสัญญาณที่มีซอฟท์แวร์ที่ใช้ในการโจมตีด้วยอากาศยานตรวจการณ์

---

๘๘ The Gaurdian “Was Israeli raid a dry run for attack on Iran?”. (Online).Available:http://www.theguardian.com/world/2007/sep/16/iran.israel, 2007

๘๙ Richard A. Clark และ Robert Knake, “Cyber War: The Next Threat to National Security and What to Do About It”, pp 19-30, ๑๐ เม.ย. 2555, Ecco, USA

๙๐ Airforce-Technology, “The Israeli 'E-tack' on Syria – Part I”. (Online).Available:http://www.airforce-technology.com/features/feature1625, 2008

๙๑ Airforce-Technology, “The Israeli 'E-tack' on Syria – Part II”. (Online).Available:http://www.airforce-technology.com/features/feature1669, 2008

ไร้คนขับ (Unmanned Air Vehicle – UAV) ของอิสราเอลไปยังเรดาร์ตรวจการณ์ของซีเรีย ซึ่งแนวคิดดังกล่าวสอดคล้องกับโครงการ “Senior Suter” [๙๒] ที่มีการเปิดเผยไม่นานหลังการปฏิบัติการ

๒. อิสราเอลส่งสายลับเข้าไปยังซีเรีย เพื่อติดตั้งซอฟท์แวร์ประเภท Trapdoor หรือ Backdoor[๙๓] ลงในซอฟท์แวร์ควบคุมระบบของซีเรีย และเมื่อถึงเวลาที่กำหนด Trapdoor จะปล่อยซอฟท์แวร์อีกตัวออกมา เพื่อไปรบกวนหรือทำลายระบบของซีเรีย หรือเพื่อเปิดช่องให้แฮกเกอร์ของอิสราเอลเข้ามาปฏิบัติภารกิจทางไซเบอร์ก่อนที่เครื่องบินจะโจมตีเพียงเล็กน้อย

๓. มีการส่งสายลับเพื่อลักลอบตัดสายไฟเบอร์ออพติก ที่ใช้ในการเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ของกองทัพซีเรีย แล้วพ่วงสายไฟเบอร์ออพติกดังกล่าวกับระบบเครือข่ายของแฮกเกอร์อิสราเอล และเมื่อถึงเวลาจะมีการส่งซอฟท์แวร์ทำลายระบบควบคุมอากาศยานของซีเรียผ่านเครือข่ายไฟเบอร์ออพติกดังกล่าว แม้ว่าแนวทางนี้จะเป็นแนวทางที่เป็นไปได้น้อยที่สุดในสามแนวทาง เนื่องจากการตัดและพ่วงสายไฟเบอร์ออพติกโดยที่ผู้ใช้งานไม่รู้ตัว เป็นเรื่องที่ทำได้ยาก ต้องใช้อุปกรณ์ ความเชี่ยวชาญ และเทคนิคขั้นสูง ทั้งนี้ใช่ว่าจะเป็นเรื่องที่เป็นไปไม่ได้

ทั้งสามประการข้างต้นเป็นข้อสันนิษฐานที่ยังไม่ได้รับการพิสูจน์ทั้งสิ้น เนื่องจากประเด็นที่ได้รับความสนใจในกรณีนี้เป็นเรื่องของการผลิตอาวุธนิวเคลียร์ และความขัดแย้งระหว่างประเทศในแถบตะวันออกกลางมากกว่าประเด็นทางด้านสงครามไซเบอร์ แต่เป็นเหตุการณ์ที่ทำให้เห็นได้อย่างชัดเจนว่า สงครามไซเบอร์เริ่มมีความสัมพันธ์กับสงครามด้านอื่นมากขึ้น และประเทศที่อยู่ภายใต้สภาวะความขัดแย้งอย่างอิสราเอลก็ให้ความสนใจกับสงครามไซเบอร์ไม่แตกต่างจากสงครามด้านอื่นหลังจากข่าวการโจมตีได้ถูกเผยแพร่ผ่านสื่อไปทั่วโลก ประธานาธิบดีซีเรีย บาชาร์ อัล อัสสัด ได้ออกมาให้การปฏิเสธเรื่องการผลิตอาวุธนิวเคลียร์โดยอ้างว่า “เป็นไปได้อย่างไรที่อาคารผลิตอาวุธนิวเคลียร์จะไม่มีขีปนาวุธพื้นสู่อากาศเพื่อการป้องกันตนเอง” [๙๔] ภายหลัง Wikileaks ได้เปิดเผยข้อมูลว่า หลังจากที่มีการโจมตี รัฐบาลซีเรียได้มีการเตรียมความพร้อมขั้นสูงสุดเพื่อยิงขีปนาวุธระยะไกลที่มีหัวจรวดเคมี แต่เนื่องจากซีเรียกลัวว่าอิสราเอลจะตอบโต้ซีเรียด้วยอาวุธ

---

๙๒ David A. Fulghum, Michael A. Dornheim, and William B. Scott. “Black Surprises”, ๕ ต.ค. ๒๕๕๐, Aviation Week and Space Technology.

๙๓ เป็นซอฟท์แวร์ประเภทหนึ่งที่จะถูกฝังลงไปในระบบ หรือในซอฟท์แวร์อื่น ๆ เพื่อเปิดช่องทางให้ผู้อื่นเข้ามาใช้งานระบบด้วยช่องทางอื่น นอกจากช่องทางปกติ

๙๔ Reuters, “Assad says facility Israel bombed not nuclear-paper”. (Oline).Available:http://web.archive.org/web/20121105015114/http://www.reuters.com/article/latestCrisis/idUSL27399094, 2008

นิวเคลียร์จึงได้ระงับการใช้ขีปนาวุธดังกล่าว [๙๕] จากการเข้าตรวจพื้นที่เมื่อ ๑๙ พ.ย.๕๑ โดยทบวงการพลังงานปรมาณูระหว่างประเทศ (International Atomic Energy Agency – IAEA) ได้ข้อสรุปว่าหลักฐานไม่เพียงพอที่จะบ่งชี้ว่ามีเตาปฏิกรณ์นิวเคลียร์ในอาคารดังกล่าว แต่สามารถตรวจพบข้อมูลที่โยงไปถึงการเก็บรักษาแร่ยูเรเนียมในอาคารดังกล่าวได้อย่างมีนัยสำคัญ [๙๖]

๒. การโจมตีทางไซเบอร์ในเอสโทเนีย

ตั้งแต่ ๒๗ เม.ย.๕๐ เว็บไซต์ของหน่วยงานสำคัญของประเทศเอสโทเนียเริ่มถูกโจมตีจากผู้บุกรุกไม่ทราบฝ่าย [๙๗] หน่วยงานที่ได้รับผลกระทบจากการโจมตีครั้งนี้ได้แก่ รัฐสภาของประเทศเอสโตเนีย ธนาคาร กระทรวงต่าง ๆ ของประเทศเอสโทเนีย และ สถานีโทรทัศน์ นอกจากเว็บไซต์ของหน่วยงานได้รับผลกระทบแล้ว การให้บริการทางออนไลน์ของหน่วยงานที่ถูกโจมตียังต้องสะดุดหยุดลงอีกด้วย ทำให้เกิดผลกระทบทางด้านเศรษฐกิจของเอสโทเนียอย่างเป็นวงกว้าง

การโจมตีดังกล่าวใช้แนวทางการโจมตีที่เรียกว่า Distributed Denial-of-Service (DDoS) [๙๘] ผู้โจมตีด้วยวิธีการนี้จะใช้วิธีร้องขอบริการจำนวนมากไปยังเครื่องแม่ข่ายที่เป็นเป้าหมายจนทำให้เครื่องแม่ข่ายเป้าหมายไม่สามารถทำงานได้ตามปกติ เพื่อเพิ่มประสิทธิภาพการโจมตี และหลบหลีกการตรวจจับของอุปกรณ์เครือข่ายรวมถึงอุปกรณ์รักษาความปลอดภัย ผู้โจมตีจะกระจายการโจมตีเครื่องเป้าหมายจากเครื่องคอมพิวเตอร์จำนวนมากทั่วโลก วิธีที่ใช้ในการกระจายการโจมตีคือ การปล่อยไวรัส มัลแวร์ โทรจัน หรืออื่น ๆ ไปยังเครื่องคอมพิวเตอร์ของผู้ใช้งานทั่วไป เมื่อเครื่อง

---

๙๕ Bergman, Ronen, “WikiLeaks: Syria aimed chemical weapons at Israel”. (Online).Available:http://web.archive.org/web/20121024195544/http://www.ynetnews.com/articles/0,7340,L-4056748,00.html, 2011

๙๖ ทบวงการพลังงานปรมาณูระหว่างประเทศ, “Implementation of the NPT Safeguards Agreement in the Syrian Arab Republic”.(Online).Available:http://www.isis-online.org/publications/syria/IAEA_Report_Syria_19Nov2008.pdf, 2008

๙๗ International Affair Review by The George Washington University's Elliott School of International Affairs, “Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security”. (Online).Available:http://www.iar-gwu.org/node/65, 2009

๙๘ Handley, et al., “Internet Denial-of-Service Considerations”, Network Working Group Request for Comments: 4732. (Online).Available:http://tools.ietf.org/html/rfc4732, 2006

คอมพิวเตอร์ถูกโจมตีด้วยซอฟท์แวร์ประสงค์ร้ายจากผู้โจมตี ผู้โจมตีสามารถควบคุมเครื่องคอมพิวเตอร์เหล่านั้นได้ผ่านระบบเครือข่ายโดยที่เจ้าของคอมพิวเตอร์ไม่รู้ตัว จากนั้นผู้โจมตีจะใช้คอมพิวเตอร์ดังกล่าวเป็นเครื่องมือในการโจมตีเป้าหมายต่อไป คอมพิวเตอร์ที่ถูกใช้เป็นเครื่องมือมีชื่อเรียกเฉพาะว่า Zombies [๙๙]

แนวทางการโจมตีด้วยวิธี DDoS แตกต่างจากการโจมตีด้วยวิธีการอื่นตรงที่ ผู้โจมตีไม่ได้ใช้ช่องว่างทางความมั่นคงความปลอดภัยของเครื่องเป้าหมายเป็นช่องทางในการโจมตี สำหรับเครื่องแม่ข่ายที่เป็นเป้าหมาย การร้องขอใช้บริการเป็นการร้องขอโดยทั่วไป ไม่แตกต่างจากการร้องขอปกติ แต่มีจำนวนมากจนเครื่องแม่ข่ายไม่สามารถทำงานได้ แต่ช่องว่างทางความมั่นคงความปลอดภัยที่ถูกใช้กลับเป็นของเครื่อง Zombies ที่หน่วยงานต่าง ๆ ไม่สามารถควบคุมได้ ดังนั้น DDoS จึงได้กลายเป็นการโจมตีที่น่ากลัวสำหรับหลายหน่วยงาน จนหน่วยงานทางความมั่นคงปลอดภัยที่เกี่ยวข้องกับเหตุการณ์ ต้องหันมาทบทวนมาตรการในการรักษาความมั่นคงปลอดภัยจากการโจมตีทางไซเบอร์ [๑๐๐]

แม้ว่าทางการเอสโทเนียจะไม่สามารถหาตัวผู้กระทำผิดจากเหตุการณ์ในครั้งนี้ได้ แต่การโจมตีเกิดขึ้นพร้อมกับเหตุการณ์ความไม่สงบในกรุงทัลลิน [๑๐๑] เมืองหลวงของประเทศเอสโทเนีย อันเนื่องมาจากการย้ายรูปปั้นทองเหลืองอันเป็นอนุสรณ์ทางการทหารตั้งแต่สมัยสหภาพโซเวียต เหตุการณ์ดังกล่าวมีชื่อเรียกอย่างไม่เป็นทางการว่า “ราตรีแห่งรูปปั้นทองเหลือง” หรือ “Bronze Night” จากเหตุการณ์ความไม่สงบนี้ ทำให้เกิดความขั้นแย้งขึ้นระหว่างประเทศเอสโทเนียและประเทศรัสเซีย [๑๐๒] และนำไปสู่การกล่าวหาประเทศรัสเซียโดยรัฐบาลเอสโทเนีย ว่า

---

๙๙ Tom Spring, “Spam Slayer: Slaying Spam-Spewing Zombie PCs”, PC World, ๒๐ มิ.ย. ๔๘

๑๐๐ Robert McMillan, “NATO to set up cyber warfare center ” , IDG News Service. (Online).Available:http://www.networkworld.com/news/2008/051508-nato-to-set-up-cyber.html, 2008

๑๐๑ Regnum news agency, “The 'Bronze Night' cost Estonia over 4mn euro”. (Online).Available:http://www.regnum.ru/english/862457.html, 2007

๑๐๒ Alexander Daniel, “Russian Historian: The problem is how to live together if the two peoples have such a different memory”.(Online).Available:REGNUM News Agency , http://pda.regnum.ru/news/issues/823273.html, 2007

รัสเซียเป็นต้นเหตุของการโจมตีทางไซเบอร์ที่เกิดขึ้น [๑๐๓] ทั้งนี้ทางรัฐบาลรัสเซียได้ออกมาปฏิเสธข้อกล่าวหาดังกล่าว จากการสอบสวนแม้มีหลักฐานบ่งชี้ว่า การโจมตีมีจุดเริ่มต้นจากประเทศรัสเซีย และมีแฮกเกอร์ชาวรัสเซียออกมายอมรับว่าตนเป็นผู้อยู่เบื้องหลังการโจมตี [๑๐๔] แต่ไม่มีหลักฐานที่แน่นหนาพอที่จะบอกได้ว่ารัฐบาลรัสเซียมีความเกี่ยวข้องกับการโจมตี [๑๐๕]

๓. การโจมตีทางไซเบอร์ช่วงสงครามระหว่างรัสเซียและจอร์เจีย

ในช่วงวันที่ ๗-๑๖ ส.ค. ๒๕๕๑ ได้เกิดสงครามระหว่างรัสเซียและจอร์เจียขึ้น[๑๐๖] โดยมีสาเหตุเริ่มต้นมาจากความขัดแย้งระหว่างจอร์เจีย และเซาท์ออสเซเตีย [๑๐๗] โดยจอร์เจียได้ส่งกองกำลังทหารจำนวนมากเพื่อเข้ายึดพื้นที่เซาท์ออสเซเตียมาเป็นของตน เนื่องจากรัสเซียเป็นพันธมิตรกับเซาท์ออสเซเตียและเป็นเพียงไม่กี่ประเทศที่ให้การรับรองเซาท์ออสเซเตียในฐานะรัฐ จึงได้ส่งกำลังทหารเข้าสนับสนุนเซาท์ออสเซเตีย และตอบโต้จอร์เจีย

ในระหว่างสงครามเว็บไซต์ของสำนักข่าว Osinform Information Agency [๑๐๘] และเว็บไซต์ของสถานีวิทยุ OSRadio ซึ่งเป็นของเซาท์ออสเซเตียได้ถูกโจมตี โดยผู้โจมตีได้เปลี่ยนเนื้อหาในเว็บไซต์ที่เป็นเนื้อหาสนับสนุนรัฐบาลรัสเซีย และเซาท์ออสเซเตีย ให้เป็นเนื้อหาของสถานีโทรทัศน์ AlaniaTV [๑๐๙] ซึ่งได้รับการสนับสนุนจากรัฐบาลจอร์เจีย [๑๑๐] หลังจากนั้นไม่นาน เว็บไซท์ของ

---

๑๐๓ Arthur Bright, “Estonia accuses Russia of 'cyberattack'”, The Christian Science Monitor. (Online).Available: http://www.csmonitor.com/2007/0517/p99s01-duts.html, 2007

๑๐๔ Noah Shachtman, “Kremlin Kids: We Launched the Estonian Cyber War”, Wired. (Online).Available: http://www.wired.com/dangerroom/2009/03/pro-kremlin-gro/, 2009

๑๐๕ สำนักข่าว Ria Novosti, “Estonia has no evidence of Kremlin involvement in cyber attacks”.(Online).Available:http://en.ria.ru/world/20070906/76959190.html, 2007

๑๐๖ Foreign Affairs “The Five-Day War Managing Moscow After the Georgia Crisis”.(Online).Available:http://www.foreignaffairs.com/articles/64602/charles-king/the-five-day-war, 2008

๑๐๗ เซาท์ออสเซเตีย เป็นดินแดนบนชายฝั่งตะวันออกของทะเลดำ และเป็นที่ตั้งของสาธารณรัฐเซาท์ออสซีเชีย ซึ่งเป็นประเทศที่มีอยู่เพียงไม่กี่ประเทศเท่านั้นที่ให้การรับรอง ได้แก่ รัสเซีย เวเนซุเอลา นิการากัว นาอูรู อับฮาเซีย และทรานส์นิสเตรีย

๑๐๘ สำนักข่าว Osinform Information Agency, http://www.osinform.ru/

๑๐๙ สถานีโทรทัศน์ AlaniaTV.(Online).Available: http://www.iptv.ge/en/alania-tv-live

๑๑๐ สำนักข่าว Civil.ge,“S.Ossetian News Sites Hacked”. (Online).Available:http://www.civil.ge/eng/article.php?id=18896, 2008

รัฐสภาและกระทรวงต่างประเทศจองจอร์เจียได้ถูกโจมตี มีการเปลี่ยนรูปของ Mikheil Saakashvili ประธานาธิบดีของจอร์เจียในขณะนั้น เป็นรูปของ อัลดอร์ฟ ฮิตเลอร์ จอมเผด็จการแห่งอาณาจักรไรช์เยอรมันที่สาม [๑๑๑] รวมถึงการโจมตีเว็บไซต์สัญชาติจอร์เจียทั้งของภาครัฐและเอกชนอื่น ๆ อีกจำนวนมาก ด้วยเทคนิคการโจมตีแบบ DDoS [๑๑๒]

สำนักข่าว Day.az สัญชาติอาเซอร์ไบจานอ้างว่าการโจมตีดังกล่าวกระทำโดยหน่วยงานข่าวกรองของรัสเซีย [๑๑๓] ทั้งนี้รัฐบาลรัสเซียได้ออกมาปฏิเสธข้อกล่าวหาดังกล่าว โดยอ้างว่าการโจมตีดังกล่าวอาจเป็นการกระทำของปัจเจกบุคคลที่ไม่เกี่ยวข้องกับรัฐบาลรัสเซีย [๑๑๔]

เพื่อแก้ไขปัญหาการให้บริการของเว็บไซต์ที่ถูกโจมตี รัฐบาลของประเทศเอสโตเนียและโปแลนด์ ได้เสนอความช่วยเหลือโดยการให้เว็บไซต์ที่ถูกโจมตีฝากข้อมูลเพื่อให้บริการบนเครื่องแม่ข่ายสำรองที่ทางรัฐบาลของทั้งสองประเทศได้จัดเตรียมไว้ให้ [๑๑๕]

๔. ไวรัส Stuxnet

Stuxnet เป็นไวรัสคอมพิวเตอร์ [๑๑๖] ชนิดหนึ่งที่ถูกตรวจพบในปี ๒๕๕๓ ความแตกต่างสำคัญของ Stuxnet กับไวรัสคอมพิวเตอร์โดยทั่วไปคือ Stuxnet ถูกออกแบบขึ้นมาเพื่อใช้โจมตีเป้าหมายทางกายภาพที่มีความเฉพาะเจาะจงเป็นอย่างมาก โดยเป้าหมายที่ว่าคือ เครื่องหมุนเหวี่ยง

---

๑๑๑ Gregg Keizer . “Cyber attacks knock out Georgia's Internet presence” .(Online).Available:mis-asia.com/news/articles/cyber-attacks-knock-out-georgias-internet-presence, 2008

๑๑๒ Markoff John, “Before the Gunfire, Cyberattacks” .(Online).Available:http://www.nytimes.com/2008/08/13/technology/13cyber.html?em, 2008

๑๑๓ สำนักข่าวToday.az, “Russian intelligence services undertook large scale attack against Day.Az server” .(Online).Available:http://www.today.az/news/politics/46885.html, 2008

๑๑๔ Markoff John, “Before the Gunfire, Cyberattacks” .(Online).Available:http://www.nytimes.com/2008/08/13/technology/13cyber.html?em, 2008

๑๑๕ Jeremy Kirk สำนักข่าว CNET, “Update: Estonia, Poland help Georgia fight cyberattacks”.(Online).Available:http://www.computerworld.com/s/article/9112399/Update_Estonia_Poland_help_Georgia_fight_cyberattacks, 2008

๑๑๖ ไวรัสคอมพิวเตอร์ คือ โปรแกรมคอมพิวเตอร์ที่บุกรุกเข้าไปในเครื่องคอมพิวเตอร์โดยไม่ได้รับความยินยอมจากผู้ใช้ ส่วนมากมักจะมีประสงค์ร้ายและสร้างความเสียหายให้กับระบบของเครื่องคอมพิวเตอร์นั้นๆUpdate: Estonia, Poland help Georgia fight cyberattacks

สำหรับสกัดสารกัมมันตภาพรังสีใช้ในอาวุธนิวเคลียร์ [๑๑๗] ที่ตั้งในโรงงานผลิตอาวุธนิวเคลียร์แห่งหนึ่งในประเทศอิหร่าน [๑๑๘] ผลจากการโจมตีดังกล่าวทำให้ขีดความสามารถกว่าร้อยละ ๒๐ ของเครื่องมือดังกล่าวไม่สามารถใช้งานได้ โดย Stuxnet ใช้ความเฉพาะเจาะจงของซอฟท์แวร์ควบคุมการทำงานของเครื่องหมุนเหวี่ยงที่ผลิตโดย Siemens ในการระบุเป้าหมาย [๑๑๙] และเป็นการโจมตีซอฟท์แวร์ในระดับของซอฟท์แวร์ควบคุมอุปกรณ์อิเล็กทรอนิกส์ ซึ่งถือว่าเป็นการโจมตีในระดับที่ลึกกว่าการโจมตีด้วยไวรัสบนเครื่องคอมพิวเตอร์ทั่วไปมาก และถือว่าเป็นการโจมตีทางไซเบอร์ครั้งแรก ๆ ที่สร้างความเสียหายโดยตรงต่ออุปกรณ์หรือเครื่องมือที่เกี่ยวข้องกับการทหาร

แม้ว่าจะไม่มีหลักฐานใดที่สามารถโยงกลับไปยังผู้พัฒนาไวรัสได้ แต่จากการวิเคราะห์ของผู้เชี่ยวชาญด้านความปลอดภัยคอมพิวเตอร์ระบุว่า Stuxnet เป็นไวรัสคอมพิวเตอร์ที่มีความซับซ้อนมากที่สุดตัวหนึ่งของโลก และอาจเรียกได้ว่าเป็นไวรัสคอมพิวเตอร์แห่งศตวรรษ [๑๒๐] ที่ต้องใช้ระยะเวลาในการพัฒนาไม่ต่ำว่าหกเดือน ใช้ผู้เชี่ยวชาญระดับสูงด้านการพัฒนาซอฟท์แวร์และความปลอดภัยคอมพิวเตอร์ประมาณ ๕-๓๐ คน และใช้ช่องว่างทางความปลอดภัยคอมพิวเตอร์ที่ไม่มีการเปิดเผยที่ใดมาก่อน เป็นช่องทางในการโจมตี [๑๒๑] ดังนั้น จึงมีการคาดการณ์กันว่า ผู้ที่อยู่เบื้องหลังการพัฒนา Stuxnet ต้องมีต้นทุนทั้งทางด้านวิชาการ ต้นทุนทางการเงิน และต้นทุน

---

๑๑๗ หมุนเหวี่ยงสำหรับสกัดสารกัมมันตภาพรังสีที่ใช้ในอาวุธนิวเคลียร์ หรือ Zippe-type centrifuge เป็นเครื่องมือที่ใช้สกัดกัมมันตภาพรังสีที่มีเลขไอโซโทปที่ต้องการจากแร่ธาตุต้นกำเนิด

๑๑๘ Michael Kelley, สำนักข่าว Business Insider, “The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought”. (Online).Available:http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11, 2013

๑๑๙ Gregg Keizer, สำนักข่าว InfoWorld. “Is Stuxnet the 'best' malware ever?”.(Online).Available:http://www.infoworld.com/print/137598, 2010

๑๒๐ สำนักข่าว News ORF.at, “Der Hack des Jahrhunderts” (เยอรมัน). (Online).Available:http://www.orf.at/stories/2016646/2016647/, 2010

๑๒๑ Josh Halliday, สำนักข่าว The Guardian, “Stuxnet worm is the 'work of a national government agency”.(Online).Available:http://www.guardian.co.uk/technology/2010/sep/24/stuxnet-worm-national-agency, 2008

ทรัพยากรบุคคลที่สูงมาก จึงมีความเป็นไปได้อย่างสูงที่การโจมตีได้รับการสนับสนุนจากภาครัฐของประเทศใดประเทศหนึ่ง [๑๒๒]

จากหลักฐานที่ปรากฏ Stuxnet เริ่มทำงานอย่างช้าที่สุดตั้งแต่ ๑๕ พ.ย.๕๐ และมีหลักฐานบางส่วนบ่งชี้ว่า Stuxnet ได้ลงทะเบียนไว้กับ Botnet [๑๒๓] ตั้งแต่ ๓ พ.ย.๔๘ และถูกตรวจพบโดย Sergej Ulasen ผู้เชี่ยวชาญความปลอดภัยชาวเบลารุสในปี ๒๕๕๓ [๑๒๔] โดยคาดว่าการแพร่กระจายของไวรัสเกิดขึ้นครั้งแรกจากการใช้งานอุปกรณ์ USB Flash Drives ผ่านระบบปฏิบัติการ Windows ที่ใช้บนเครื่องคอมพิวเตอร์ทั่วไป ก่อนที่จะแพร่กระจายผ่านระบบเครือข่ายไปยังอุปกรณ์อื่น ๆ ที่ใช้ระบบปฏิบัติการ WinCC [๑๒๕] ที่เป็นระบบปฏิบัติการเฉพาะที่ใช้ในเครื่องหมุนหวี่ยงต่อไป [๑๒๖]

จากการวิเคราะห์ของ Ralph Langner ผู้เชี่ยวชาญด้านความปลอดภัยคอมพิวเตอร์ [๑๒๗] Stuxnet มีที่มาที่มีความเป็นไปได้มากที่สุดสามแนวทางได้แก่

๑) ได้รับการสนับสนุนจากกองทัพอิสราเอล โดยการวิเคราะห์จากคำว่า “Myrtus” ซึ่งเป็นคำที่ปรากฏอยู่ในตัวซอฟท์แวร์ Stuxnet หลายจุด และคาดว่าจะเป็นคำที่ทีมงานผู้พัฒนา

---

๑๒๒ สำนักข่าว News ORF.at, “Der Hack des Jahrhunderts” (เยอรมัน). (Online).Available:http://www.orf.at/stories/2016646/2016647/, 2010

๑๒๓ Botnet คือซอฟท์แวร์หุ่นยนต์ หรือซอฟท์แวร์ที่ทำงานอัตโนมัติ โดยจะเน้นการทำงานบนระบบเครือข่ายตามหน้าที่ที่ได้รับมอบหมาย เช่น Google ใช้ Botnet ในการดึงเนื้อหาจากเว็บไซต์ต่าง ๆ มาประมวลผลในการค้นหาข้อมูล

๑๒๔ Jim Finkle, สำนักข่าวรอยเตอร์, “Researchers say Stuxnet was deployed against Iran in 2007”.(Online).Available:http://www.reuters.com/article/2013/02/26/us-cyberwar-stuxnet-idUSBRE91P0PP20130226, 2013

๑๒๕ ระบบปฏิบัติการ Windows Control Center ที่ผลิตโดย Simens ใช้ในอุปกรณ์อิเล็กทรอนิกส์เพื่อควบคุมการทำงานของอุปกรณ์อิเล็กทรอนิกส์อื่น ๆ.(Online).Available: http://www.automation.siemens.com/mcms/human-machine-interface/de/visualisierungssoftware/scada-wincc/Seiten/Default.aspx

๑๒๖ Ralph Langner , “Ralph's Step-By-Step Guide to Get a Crack at Stuxnet Traffic and Behaviour” .(Online).Available:http://www.langner.com/en/2010/09/14/ralphs-step-by-step-guide-to-get-a-crack-at-stuxnet-traffic-and-behavior/, 2010

๑๒๗ Ibid

ซอฟท์แวร์ใช้เรียก Stuxnet ในระหว่างการพัฒนา “Myrtus” เป็นคำภาษาฮีบรู (ภาษาราชการของอิสราเอล) ที่ใช้กล่าวถึงกษัตริย์เอสเธอร์ในคำภีร์ไบเบิล อย่างไรก็ตามมีผู้เชี่ยวชาญบางคนมองว่าแนวทางนี้เป็นเพียงทฤษฎีสมคบคิดแบบหนึ่งเท่านั้น เพราะคำว่า “Myrtus” อาจไม่ได้นำไปสู่อะไรเลย แต่ในอีกด้านหนึ่ง มีการเปิดเผยจากสมาชิกคนหนึ่งในชุมชนข่าวกรองแห่งสหรัฐอเมริกา (United States Intelligence Community) [๑๒๘] ว่า Unit 8200 [๑๒๙] หน่วยงานด้านความมั่นคงของอิสราเอลได้เคยทดลองหาช่องโหว่ในเครื่องหมุนเหวี่ยงที่ผลิตโดย Siemens และมีการใช้งานในโรงงานสกัดสารกัมมันตภาพรังสีในปากีสถาน [๑๓๐] นอกจากนี้หนังสือพิมพ์ท้องถิ่นของอิสราเอล Haaretz ยังเคยรายงานถึงวิดีโอที่ Gabi Aschkenasi เสนาธิการกองทัพอิสราเอล ได้อ้างถึงความสำเร็จในการโจมตีซีเรีย และความสำเร็จของ Stuxnet ในขณะที่เขาดำรงตำแหน่ง [๑๓๑]

๒. ได้รับการสนับสนุนจากสหรัฐอเมริกา จากหนังสือเรื่อง “Confront and Conceal: Obama’s Secret Wars and Surprising Use of American Power” โดย David E. Sanger [๑๓๒] ได้ระบุว่าโครงการ Stuxnet ได้เริ่มขึ้นในสมัยประธานาธิบดี George W. Bush และได้รับการสนับสนุนต่อเนื่องมาถึงในสมัยของประธานาธิบดี Barack Obama โดยใช้ชื่อโครงการว่า “Operation Olympic Games” โดยในหนังสือได้กล่าวถึงความร่วมมือระหว่างผู้เชี่ยวชาญของสหรัฐอเมริกา และอิสราเอล และได้รับความดูแลรวมถึงการอนุมัติโครงการในทุกขั้นตอนโดยประธานาธิบดี Barack Obama

---

๑๒๘ ชุมชนหน่วยงานด้านข่าวกรองของสหรัฐกาที่ประกอบหน่วยงานด้านข่าวกรองของรัฐบาลสหรัฐอเมริกา อย่างน้อย ๑๖ หน่วยงาน เช่น CIA, NSA เป็นต้น

๑๒๙ Unit 8200 เป็นหน่วยงานของรัฐบาลอิสราเอล มีขอบเขตรับผิดชอบด้านการสื่อสารและสารสนเทศ รวมถึงความมั่นคงทางด้านอิเล็กทรอนิกส์และไซเบอร์, http:// www.businessinsider.com/israelis-bugged-the-us-for-the-nsa-2013-6

๑๓๐ John Markoff, สำนักข่าว New York Times, “A Silent Attack, but Not a Subtle One” .(Online).Available:http://www.nytimes.com/2010/09/27/technology/27virus.html, 2010

๑๓๑ Richard Silverstein, “Ashkenazi Video Admits IDF Bombed Syrian Nuclear Reactor and Created Stuxnet” .(Online).Available:http://www.richardsilverstein.com/tikun_olam/2011/02/14/ashkenazi-video-claims-idf-responsibility-for-bombing-syrian-nuclear-reactor-and-stuxnet/, 2011

๑๓๒ David E. Sanger, “Obama Order Sped Up Wave of Cyberattacks Against Iran.”, The New York Times, ๑ มิ.ย. ๕๕, พิมพ์ครั้งที่ ๑

และคาดว่านายพล James E. Cartwright จะเป็นผู้ริเริ่มความคิดโครงการ Stuxnet และนำข้อมูลเกี่ยวกับโครงการไปให้หนังสือพิมพ์ New York Times เพื่อเปิดเผยโครงการ [๑๓๓]

๓. ความร่วมมือระหว่างประเทศ จากการรายงานของสถานีโทรทัศน์อิสราเอล PressTV ใน ๑๖ ม.ค.๕๔ ได้อ้างถึงบทความจากหนังสือพิมพ์ New York Times ใน ๑๕ ม.ค.๕๔ ว่า Stuxnet เป็นโครงการที่เกิดขึ้นโดยความร่วมมือของผู้เชี่ยวชาญจาก สหรัฐอเมริกา สหราชอาณาจักร อิสราเอล และเยอรมนี และมี Siemens ให้การสนับสนุนในการพัฒนาซอฟท์แวร์ [๑๓๔] [๑๓๕]

เป้าหมายในการพัฒนา Stuxnet นอกจากจะเป็นเรื่องของการโจมตีโรงงานผลิตอาวุธนิวเคลียร์จากที่ได้เห็นจากหลักฐานเชิงประจักษ์แล้ว ยังมีการคาดการณ์กันว่า Stuxnet ถูกพัฒนาขึ้นมาเพื่อทดลองโจมตีอุปกรณ์อิเล็กทรอนิกส์ที่ใช้ในการควบคุมการทำงานอื่น ๆ อีกด้วย โดยเฉพาะอย่างยิ่งอุปกรณ์ควบคุมสำหรับการให้บริการด้านสาธารณูปโภคพื้นฐาน เช่น การผลิตไฟฟ้า น้ำประปา เป็นต้น รวมไปถึงอุปกรณ์อิเล็กทรอนิกส์ที่ใช้ในโรงงานอุตสาหกรรม [๑๓๖] และนี่ถือเป็นภัยคุกคามรูปแบบใหม่ที่หน่วยงานด้านความมั่นคงต้องรับมือภัยคุกคามที่ไม่ได้มาในรูปของอาวุธยุทโธปกรณ์ แต่มาในรูปชุดคำสั่ง แต่สามารถสร้างความเสียหายไม่ต่างจากเครื่องบินขับไล่ทิ้งระเบิด

๕. การหลุดของข้อมูลโทรเลขจากสถานทูตสหรัฐอเมริกาประจำประเทศต่าง ๆ

เหตุการณ์หนึ่งที่ได้รับความสนใจจากรัฐบาลหลายประเทศ ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยทางสารสนเทศ รวมถึงแฮกเกอร์จากทุกมุมโลกเป็นอย่างมากเหตุการณ์หนึ่ง คือ การหลุด

---

๑๓๓ Andreas Wilkens, สำนักข่าวออนไลน์ Heisse.de, “Stuxnet: Berichte über weiteren Geheimnisverrats-Fall in den USA.” .(Online).Available:http://heise.de/-1902235, 2013

๑๓๔ William J. Broad, John Markoff, David E. Sanger, “Israel Tests on Worm Called Crucial in Iran Nuclear Delay.”, New York Times online.(Online).Available:http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html**,** 2011

๑๓๕ สถานีโทรทัศน์ Press TV, “Stuxnet, US-Israeli bid against Iran”, ๑๖ ม.ค.๒๕๕๔

๑๓๖ Sandro Gaycken, สำนักข่าว Die Zeit, “Wer war’s? Und wozu?”. (Online).Available:http://www.zeit.de/2010/48/Computerwurm-Stuxnet?page=all, 2010

ของข้อมูลโทรเลขจากสถานทูตสหรัฐอเมริกา [๑๓๗] [๑๓๘] ประจำประเทศต่าง ๆ และข้อมูลที่หลุดออกมา ได้ถูกนำเผยแพร่ในเว็บไซต์ WikiLeaks [๑๓๙] แม้โดยตัวเหตุการณ์จะไม่ถือว่าเป็นเหตุการณ์ที่เป็นสงครามไซเบอร์โดยตรง แต่มีความเกี่ยวโยงกับสงครามไซเบอร์ย่อย ๆ อีกหลายเหตุการณ์ เกี่ยวโยงกับความมั่นคงของหลายประเทศ รวมถึงความสัมพันธ์ระหว่างประเทศ และเป็นเหตุการณ์ที่ทำให้รัฐ หน่วยงานความมั่นคง รวมถึงนักวิชาการด้านรัฐศาสตร์ ต้องหันมาทบทวนในประเด็นที่ว่าด้วย บทบาทของรัฐที่ควรมีต่อประชาชน ความสัมพันธ์ระหว่างรัฐกับประชาชน และรัฐกับรัฐ ดังที่เคยปรากฏในทฤษฎีคลื่นลูกที่สามของ Alvin Toffler [๑๔๐] [๑๔๑]

การเผยแพร่ข้อมูลโทรเลขผ่าน Wikileaks ภายใต้นามเรียกขาน “Cablegate” ได้เริ่มขึ้นตั้งแต่ ๒๘ พ.ย. ๕๓ โดย Wikileaks จะทะยอยเปิดเผยข้อมูลที่มีจนกระทั่งปัจจุบัน ข้อมูลที่เปิดเผยเป็นโทรเลขภายในของหน่วยงานภาครัฐของสหรัฐอเมริกา ในตั้งแต่ปี ๒๕๓๙ จนถึงปี ๒๕๕๓ จำนวนรวมทั้งสิ้น ๒๕๑,๒๘๗ ฉบับ [๑๔๒] โดยเป็นโทรเลขชั้นความลับ ๑๕,๖๕๒ ฉบับ และเป็นโทรเลขชั้นปกปิด จำนวน ๑๐๑,๗๘๔ ฉบับ มีการสืบทราบในภายหลังว่าโทรเลขดังกล่าวได้ถูกลักลอบออกจากสถานทูตโดยพลทหาร Bradley Manning ในขณะที่เขาประจำการที่ประเทศอิรัก [๑๔๓] [๑๔๔]

---

๑๓๗ โทรเลข หรือ cable เป็นข้อมูลที่สถานทูตสหรัฐอเมริกาประจำประเทศต่าง ๆ ต้องรายงานข้อมูลต่าง ๆ ทั้งทางด้านการทูต การข่าว สถานการณ์ทางการเมืองของประเทศนั้น ๆ กลับไปยังรัฐบาลกลางสหรัฐอเมริกา ณ กรุง Washington

๑๓๘ JOSHUA E. Keating, “Why Do Diplomats Still Send Cables? In: Foreign Policy.”.(Online).Available:http://www.foreignpolicy.com/articles/2010/11/29/why_do_diplomats_still_send_cables, 2010

๑๓๙ (Online).Available:http://www.wikileaks.org/

๑๔๐ Alvin Toffler, “The Third Wave”, Bantam Books, 1980, USA

๑๔๑ Alvin Toffler, “Revolutionary Wealth”, Bantam Books, 2006, USA

๑๔๒ Wikileaks, “Secret US Embassy Cables” .(Online).Available:http://wikileaks.org/cablegate.html

๑๔๓ Kim Zetter, Kevin Poulsen, “State Department Anxious About Possible Leak of Cables to Wikileaks”, นิตยสาร Wired.(Online).Available:http://www.wired.com/threatlevel/2010/06/state-department-anxious/, 2010

๑๔๔ WikiLeaks, “Allegations in Wired that we have been sent 260,000 classified US embassy cables are, as far as we can tell, incorrect”. (Online). Available:https://www.twitter.com/#!/wikileaks/status/15612005016, 2010

และต่อมาเขาได้ถูกพิพากษาจำคุก ๓๕ ปีจากการกระทำดังกล่าว [๑๔๕]

โดยเนื้อหาในโทรเลขแบ่งออกเป็นหัวข้อต่าง ๆ ตามที่ทางกระทรวงการต่างประเทศสหรัฐอเมริกากำหนด [๑๔๖] แต่หัวข้อที่ได้รับความสนใจ และส่งผลกระทบมากที่สุดเป็นเรื่องเกี่ยวกับรวบรวมข้อมูลสถานการณ์ทางการเมืองภายในประเทศ การรายงานและการวิเคราะห์ประเมินพฤติกรรมของนักการเมืองของประเทศนั้น ๆ รวมถึงข้อมูลเชิงลึกที่ได้จากการพบปะพูดคุยระหว่างเจ้าหน้าที่จากสถานทูตสหรัฐอเมริกากับนักการเมือง และบุคลากรที่เกี่ยวข้อง ซึ่งข้อมูลที่ถูกเปิดเผยมีข้อมูลที่เกี่ยวข้องกับประเทศไทยรวมอยู่ด้วย [๑๔๗]

เนื้อหาที่อยู่ในโทรเลขถูกวิพากวิจารณ์จากรัฐบาลหลายประเทศ เช่น Steven Vanackere รัฐมนตรีกระทรวงต่างประเทศเบลเยี่ยมได้กล่าวถึงว่า “เป็นความสับสนระหว่างการทูตและการจารกรรมข้อมูล” [๑๔๘] เป็นต้น แต่ในขณะเดียวกันการเปิดเผยข้อมูลของ Wikileaks ก็ถูกวิพากวิจารณ์จากหลายประเทศเช่นเดียวกัน เช่น Guido Westerwelle รัฐมนตรีกระทรวงต่างประเทศสหพันธสาธารณรัฐเยอรมนีได้ให้สัมภาษณ์ทางโทรทัศน์ช่อง ARD ว่า “เรื่องทั้งหมด เป็นการกระทำที่ผิดกฎหมายและเป็นอาชญากรรม โดยการหารายได้ด้วยการนำข้อมูลมาเปิดเผย” [๑๔๙] เป็นต้น

ผลจากการเผยแพร่ข้อมูลของ Wikileaks ทำให้รัฐบาลของหลายประเทศโดยเฉพาะอย่างยิ่งสหรัฐอเมริกา ต้องการนำผู้รับผิดชอบ และผู้ดูแลระบบของ Wikileaks มาดำเนินคดีในประเทศของตนเอง บุคคลผู้ที่ได้รับความสนใจที่สุดในบรรดาผู้ที่เกี่ยวข้องกับ Wikileaks คือ Julian

---

๑๔๕ Julie Tate, หนังสือพิมพ์ Washington Posts, “Judge sentences Bradley Manning to 35 years”.(Online).Available:http://www.washingtonpost.com/world/national-security/judge-to-sentence-bradley-manning-today/2013/08/20/85bee184-09d0-11e3-b87c-476db8ac34cd_story.html, 2013

๑๔๖ กระทรวงการต่างประเทศสหรัฐอเมริกา, “U.S.Department of State Foreign Affairs Manual Volume 5 Handbook 3 TAGS/Terms Hanbook”. (Online). Available:http://www.state.gov/documents/organization/8925.4.pdf

๑๔๗ Wikileaks, “Category:Thailand” https://wikileaks.org/wiki/Category:Thailand

๑๔๘ Carsten Lißmann, Karsten Polke-Majewski, Kai Biermann, Lisa Caspari, “Wikileaks: Was die geheimen Dokumente verraten.”, หนังสือพิมพ์ Die Zeit. (Online).Available:http://www.zeit,de/politik/ausland/2010-11/wikileaks-usa-diplomatische-dokumente ? page=all, 2010

๑๔๙ รายการ Tagesschau สถานีโทรทัศน์ ARD. (Online).Available:http://tagesschau.vo.llnwd.net/d3/video/2010/1129/TV-20101129-1705-2501.webl.h264.mp4, 2010

Assange แฮกเกอร์และนักเคลื่อนไหวชาวออสเตรเลียผู้ก่อตั้งและผู้ดูแลด้านความปลอดภัยให้กับ Wikileaks [๑๕๐] ซึ่งในความเห็นของ Peter Ralphs นายทหารชั้นพันโทในกองทัพสหรัฐอเมริกามองว่า Julia Assange คือ **"ผู้ก่อการร้ายทางไซเบอร์"** ที่ควรถูกจับตาย [๑๕๑] แม้ว่าสหรัฐอเมริกาต้องการใช้คดีของ Bradley Manning มาเชื่อมโยงกับ Julian Assange เพื่อออกหมายจับเขาในฐานะผู้ร้ายข้ามแดน แต่ก็มีหลักฐานไม่เพียงพอ [๑๕๒] สหรัฐอเมริกาจึงพยายามขอความร่วมมือกับประเทศอื่น ๆ ในการส่งตัวเขาไปให้สหรัฐอเมริกา [๑๕๓] แต่จนถึงปัจจุบันก็ยังไม่มีการจับกุมและดำเนินคดีกับเขาในฐานะผู้ก่อตั้ง Wikileaks แต่อย่างใด จะมีก็เพียงแต่การแจ้งข้อหากระทำชำเราผู้เยาว์ในประเทศสวีเดน [๑๕๔] และนำไปสู่การจับกุมเขาด้วยข้อหาดังกล่าวในประเทศอังกฤษ [๑๕๕] แต่หลังจากการพิจารณาคดีในชั้นศาล เขาก็ได้รับการปล่อยตัว [๑๕๖] เนื่องจาก Julian Assange รู้ว่าตนเองเป็นเป้าหมายในการจับกุมของนานาประเทศ และอาจถูกฆาตกรรม เขาจึงได้เตรียมแผนการโดยการเข้ารหัสข้อมูลบางส่วนที่ยังไม่ได้เปิดเผย แล้วส่งไปให้เครือข่ายนักข่าว นักหนังสือพิมพ์ทั่วโลก โดยเขาอ้างว่า ทันทีที่เขาถูก

---

๑๕๐ Raffi Khatchadourian, หนังสือพิมพ์ New Yorker, "No Secrets. Julian Assange's mission fortotaltransparencccy" .(Online).Available:http://www.newyorker.com/reporting/2010/06/07/100607fa_fact_khatchadourian?currentPage=all, 2010

๑๕๑ Peter Ralphs, "People OK with murdering Assange". (Online).Available:, https://web.archive.org/web/20110119070538/http://www.peopleokwithmurderingassange.com/?q=8, 2011

๑๕๒ Andy Park, สำนักข่าว SBS, "US dismisses 'evidence' of Assange grand jury".(Online).Available:http://www.sbs.com.au/news/article/2013/02/26/us-dismisses-evidence-assange-grand-jury, 2013

๑๕๓ Philip Shenon, สำนักข่าว The Daily Beast, "U.S. Urges Allies to Crack Down on WikiLeaks".(Online).Available:http://www.thedailybeast.com/blogs-and-stories/2010-08-10/a-western-crackdown-on-wikileaks, 2010

๑๕๔ สำนักข่าว BBC, " Timeline: sexual allegations against Assange in Sweden". (Online).Available: http://www.bbc.com/news/world-europe-11949341, 2012

๑๕๕ Marcel Rosenbach, Holger Stark, นิตยสาร Der Spiegel, "Vergewaltigungsvorwurf: Britische Polizei setzt Julian Assange fest".(Online).Available:http://www.spiegel.de/politik/ausland/vergewaltigungsvorwurf-britische-polizei-setzt-julianassange-fest-a-733200.html, 2010

๑๕๖ นิตยสาร Der Spiegel, "Gerichtsverhandlung: WikiLeaks-Gründer Assange kommt frei" .(Online).Available:http://www.spiegel.de/politik/ausland/0,1518,735044,00.html, 2010

จับกุมตัว หรือถูกฆาตกรรม ข้อมูลต่าง ๆ เหล่านี้จะถูกเผยแพร่ทันที [๑๕๗] ปัจจุบัน Julian Assange ยังคงถือเป็นบุคคลที่เป็นภัยต่อความมั่นคงทางไซเบอร์ของสหรัฐอเมริกา

จากการที่ Wikileaks ได้เผยแพร่ข้อมูลโทรเลขของสถานทูตสหรัฐอเมริกา ส่งผลให้ผู้ให้บริการที่เกี่ยวข้องกับ Wikileaks เช่น Mastercard, PayPal, Amazon ถูกกดดัน และถูกโจมตีด้วยกระบวนการ DDoS จนทำให้ต้องถอนการให้บริการของตนเองแก่ Wikileaks [๑๕๘] ทันทีที่ Wikileaks ถูกถอนบริการ แฮกเกอร์และผู้ดูแลระบบจำนวนมากได้เสนอความช่วยเหลือเครื่องแม่ข่ายสำรองให้แก่ Wikileaks [๑๕๙] และตามมาด้วยมาตรการตอบโต้ของแฮกเกอร์ชั้นแนวหน้าทั่วโลกรวมถึงกลุ่ม Anonymous [๑๖๐] ภายใต้ชื่อปฏิบัติการ “Operation Payback” โดยแฮกเกอร์เหล่านั้นได้ใช้วิธีการ DDoS โจมตีผู้ให้บริการที่ปฏิเสธการให้บริการแก่ Wikileaks และหน่วยงานอื่น ๆ ที่เกี่ยวข้องกับการปฏิเสธบริการแก่ Wikileaks [๑๖๑] ซึ่งเป็นการโจมตีทางไซเบอร์ครั้งสำคัญครั้งหนึ่งและเป็นเหตุทำให้การบริการด้านอินเตอร์เนตจำนวนมากทั่วโลกเกิดปัญหา เพื่อป้องกันการโจมตีเครื่องแม่ข่าย และตัดการพึ่งพาผู้ให้บริการเครื่องแม่ข่าย Wikileaks ได้เช่าบังเกอร์ใต้ดินใกล้กรุงสต็อกโฮล์มประเทศสวีเดน ที่ถูกสร้างขึ้นมาเพื่อป้องกันภัยจากอาวุธนิวเคลียร์ในการเก็บรักษาเครื่องแม่ข่ายของตนเอง [๑๖๒] แนวทางดังกล่าวเป็นแนวทางการป้องกันภัยทางไซเบอร์ที่ได้รับความสนใจและกล่าวถึงอย่างมาก

---

๑๕๗ Ian Drury, สำนักข่าว The Daily Mail, “WikiLeaks founder Julian Assange 'will release poison pill of damaging secrets if killed or arrested"”.(Online).Available:http://www.dailymail.co.uk/news/article-1335888/WikiLeaks-Julian-Assange-release-damaging-secrets-killed-arrested.html, 2010

๑๕๘ Leslie Horn, นิตยสาร PC Magazine, “WikiLeaks Supporter 'Operation Payback' Targets PayPal, Amazon” .(Online).Available:http://www.pcmag.com/article2/0,2817,2374090,00.asp, 2010

๑๕๙ Stand Schroeder, สำนักข่าว Mashable, “WikiLeaks Now Has Hundreds of Mirrors” .(Online).Available:http://mashable.com/2010/12/05/wikileaks-mirrors/

๑๖๐ http://www.anonymoushackers.org/

๑๖๑ Leslie Horn, นิตยสาร PC Magazine, “WikiLeaks Supporter 'Operation Payback' Targets PayPal, Amazon” .(Online).Available:http://www.pcmag.com/article2/0,2817,2374090,00.asp, 2010

๑๖๒ John E Dunn, สำนักข่าว Techworld, “Wikileaks servers move to nuclear bunker under Stockholm”.(Online).Available:http://news.techworld.com/security/3237681/wikileaks-servers-move-to-nuclear-bunker-under-stockholm/, 2010

แม้ว่าหน่วยงานรัฐส่วนมากจะมีท่าทีด้านลบ ต่อทั้งการดำเนินการของสถานทูต และหน่วยงานภาครัฐของสหรัฐอเมริกา และทั้งการเผยแพร่ข้อมูลของ Wikileaks แต่ในอีกด้านหนึ่งนักข่าวและกลุ่มนักเคลื่อนไหวทั่วโลกตื่นเต้น และให้ความสำคัญกับการเผยแพร่ข้อมูลของ Wikileaks ดังจะเห็นได้จากการให้รางวัลแก่ Julian Assange โดยสำนักข่าวและหน่วยงานด้านสิทธิมนุษยชนต่าง ๆ [๑๖๓ ๑๖๔ ๑๖๕] รวมถึงการยกให้ Wikileaks เป็นแรงบัลดาลใจให้กับประชาชนในประเทศแถบตะวันออกกลางในการลุกขึ้นมาต่อสู้กับอำนาจเผด็จการจนเกิดปรากฏการณ์ Arab Spring [๑๖๖]

กรณีการหลุดของข้อมูลโทรเลขและ Wikileaks ในด้านหนึ่งทำให้เกิดการถกเถียงกันอย่างกว้างขวางในกระเด็น ความสมดุลระหว่างความมั่นคงแห่งรัฐ และสิทธิความเป็นส่วนตัว รวมถึงสิทธิในการรับรู้ข่าวสารของประชาชน นักเคลื่อนไหวฝ่ายเสรีนิยมมักตั้งคำถามต่อหน่วยงานรัฐในเรื่องดังกล่าว ในขณะที่รัฐเองก็มีหน้าที่ในการรักษาความมั่นคง ในอีกด้านหนึ่ง ความมั่นคงทางสารสนเทศ และความมั่นคงทางด้านการข่าวของประเทศที่ลงทุนทางการทหารด้วยงบประมาณมหาศาลอย่างสหรัฐอเมริกา กำลังถูกท้าทายอย่างหนักจากเหล่าแฮกเกอร์หนักเคลื่อนไหวที่สนับสนุน Wikileaks เป็นหลักฐานเชิงประจักษ์ที่แสดงให้เห็นว่า ในสงครามไซเบอร์งบประมาณและทรัพยากรด้านต่าง ๆ ไม่ได้เป็นจุดชี้ขาดสำคัญเสมอไป

๖. การโจมตีทางไซเบอร์ในประเทศเกาหลีใต้

ในช่วงเดือน มิ.ย. ๕๒ เว็บไซต์ของหน่วยงานราชการ ธนาคาร และบริษัททางด้านการเงินของเกาหลีใต้ รวมถึงสหรัฐอเมริกาหลายแห่งได้ถูกโจมตีด้วยกรรมวิธี DDoS จาก Botnet

---

๑๖๓ สำนักข่าว NTD, “Freedom of Expression Awards in London”. (Online). Available:http://english.ntdtv.com/?c=150&a=2858, 2008

๑๖๔ องค์กรสิทธิมนุษยชนระหว่างประเทศ Amnesty, “Amnesty Media Awards Shortlist 2009”.(Online).Available:https://amnesty.org.uk/press-releases/media-awards-2009-shortlists-announced, 2009

๑๖๕ Ray McGovern, “Julian Assange Was Given Sam Adams Award for Integrity in 2010”.(Online).Available:http://warisacrime.org/content/julian-assange-was-given-sam-adams-award-integrity-2010, 2012

๑๖๖ Peter Walker, สำนักข่าว The Gaurdian, “Amnesty International hails WikiLeaks and Guardian as Arab spring 'catalysts'". (Online).Available:http://www.theguardian.com/world/2011/may/13/amnesty-international-wikileaks-arab-spring, 2011.

ที่ถูกปล่อยออกมาจากเครื่องคอมพิวเตอร์ที่เป็น Zombies อีกทอดหนึ่ง [๑๖๗] เครื่องคอมพิวเตอร์ Zombies ที่ใช้เป็นเครื่องมือในการโจมตีคาดว่ามีปริมาณระหว่าง ๒๐,๐๐๐ ถึง ๑๖๖,๐๐๐ เครื่อง[๑๖๘] [๑๖๙] การโจมตีเกิดขึ้นเป็นระลอกใหญ่ ๆ รวมสามระลอก โดยมีการคาดการณ์กันว่า ผู้ที่อยู่เบื้องหลังการโจมตีครั้งนี้คือเกาหลีเหนือ [๑๗๐] และในการโจมตีทางไซเบอร์ครั้งนี้เริ่มมีการพูดถึงหน่วยงานทางด้านไซเบอร์ของเกาหลี ที่มีชื่อว่า “หน่วย ๑๑๐” “หน่วย ๑๒๑” และ “หน่วย ๒๐๔” ต่อสาธารณชนเป็นครั้งแรก [๑๗๑]

หลังจากการโจมตีทางไซเบอร์ในปี ๕๒ เกาหลีใต้ถูกโจมตีทางไซเบอร์อีกครั้งในเดือน มี.ค. ๕๔ ด้วยวิธีการที่คล้ายคลึงกับการโจมตีในปี ๕๒ โดยเป้าหมายในการโจมตีครั้งนี้เป็นเว็บไซต์ของหน่วยงานรัฐบาล และบริษัทขนาดใหญ่ของเกาหลีใต้ [๑๗๒] และเช่นเดียวกับการถูกโจมตีในครั้งก่อน เกาหลีเหลือถูกกล่าวหาว่าอยู่เบื้องหลังในการโจมตี

ในวันที่ ๒๐ มี.ค. ๕๖ เกาหลีใต้ถูกโจมตีทางไซเบอร์อีกครั้ง ในครั้งนี้แตกต่างจากการถูกโจมตีในสองครั้งก่อนหน้า ที่เป้าหมายเป็นเว็บไซต์ ในครั้งนี้ระบบเครือข่าย และเครื่องคอมพิวเตอร์ของสถานีโทรทัศน์หลายช่อง รวมถึงธนาคารจำนวนหนึ่งของเกาหลีใต้ ได้ถูกโจมตีทางไซเบอร์

---

๑๖๗ สำนักข่าว BBC, “New 'cyber attacks' hit S Korea”.(Online).Available:http://news.bbc.co.uk/1/hi/world/asia-pacific/8142282.stm, 2009

๑๖๘ Thomas Claburn, สำนักข่าว InformationWeek, “Cyber Attack Code Starts Killing Infected PCs”.(Online).Available:http://www.informationweek.com/news/showArticle.jhtml?article ID=218401559, 2009

๑๖๙ Martyn Williams, สำนักข่าว IDG News Service, “UK, not North Korea, source of DDOS attacks, researcher says” .(Online).Available:http://www.networkworld.com/news/2009/071409-uk-not-north-korea-source.html?ap1=rcb, 2009

๑๗๐ สำนักข่าว Financial Times, “Pyongyang blamed as cyber attack hits S Korea”.(Online).Available:http://www.ft.com/cms/s/0/61bc6d22-6c1f-11de-9320-00144feabdc0.html, 2009

๑๗๑ สำนักข่าว The Gaurdian, “North Korea launched cyber attacks, says south” .(Online).Available:http://www.theguardian.com/world/2009/jul/11/south-korea-blames-north-korea-cyber-attacks, 2009

๑๗๒ สำนักข่าว BBC, “South Korea hit by cyber attacks”.(Online).Available:http://www.bbc.com/news/technology-12646052, 2011

จนไม่สามารถให้บริการได้ [๑๗๓] หนึ่งในการให้บริการที่ได้รับผลกระทบคือตู้ ATM ผลจากการโจมตีทางไซเบอร์ทำให้กระทรวงกลาโหมเกาหลีใต้ได้เพิ่มระดับการระวังภัยทางไซเบอร์ขึ้นไปในระดับสามจากห้าระดับ เกาหลีเหนือถูกตกเป็นจำเลยอีกครั้งในฐานะผู้อยู่เบื้องหลังการโจมตี แม้ว่าหมายเลขไอพี [๑๗๔] ของผู้โจมตีจะเป็นหมายเลขไอพีของประเทศจีนก็ตาม[๑๗๕] แต่ก็มีการสันนิษฐานว่า หน่วยงานด้านสงครามไซเบอร์ของเกาหลีเหนือได้ใช้ไอพีที่ตรวจพบ เป็นข้อมูลอำพรางตัวตนที่แท้จริงของผู้โจมตี

จากแนวโน้มของความรุนแรงในการโจมตีที่มากขึ้นเรื่อย ๆ ทำให้เกาหลีใต้ตระหนักถึงภัยคุกคามทางไซเบอร์ที่ตนเองประสบ ทั้งนี้เกาหลีใต้ไม่ได้เป็นรัฐเผด็จการจึงไม่สามารถจัดสรรทรัพยากร รวมถึงอนุมัติงบประมาณเพื่อทุ่มเทให้กับการรักษาความมั่นคงปลอดภัยทางสารสนเทศได้ตามอำเภอใจของรัฐบาลและหน่วยงานความมั่นคง ดังนั้น แม้ว่าเกาหลีใต้จะเป็นประเทศที่มีความก้าวหน้าทางด้านเทคโนโลยีโทรคมนาคมและสารสนเทศมากที่สุดประเทศหนึ่งของโลก แต่ก็มีสถานการณ์ที่เป็นรองเกาหลีเหนือในด้านขีดความสามารถทางสงครามไซเบอร์ และดูเหมือนว่าสมรภูมิในสงครามไซเบอร์จะมีความสำคัญมากขึ้น และทวีความรุนแรงมากขึ้นทุกขณะ

องค์กร บทบาทหน้าที่ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางสารสนเทศของไทย

ความตื่นตัวของหน่วยงานภาครัฐในประเทศไทยต่อภัยคุกคามทางสารสนเทศและสงครามไซเบอร์ เกิดขึ้นพร้อม ๆ กับการพัฒนาขีดความสามารถทางเทคโนโลยีสารสนเทศและความแพร่หลายในการนำเทคโนโลยีสารสนเทศมาใช้งาน ทั้งในภาครัฐและเอกชน ทำให้รัฐบาลไทยได้แต่งตั้ง คณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Committee : NCSC) ซึ่งมีนายกรัฐมนตรีเป็นประธาน และหน่วยงานที่เกี่ยวข้องด้านความมั่นคง

---

๑๗๓ Tania Branigan, สำนักข่าว The Gaurdian, “South Korea on alert for cyber-attacks after major network goes down: Computer systems of banks and broadcasters are interrupted, with fingers immediately pointed at North Korea”.(Online).Available:http://www.guardian.co.uk/world/2013/mar/20/south-korea-under-cyber-attack, 2013

๑๗๔ หมายเลขไอพี คือ ฉลากหมายเลขที่กำหนดให้แก่อุปกรณ์แต่ละชนิด (เช่นคอมพิวเตอร์ เครื่องพิมพ์) ที่มีส่วนร่วมอยู่ในเครือข่ายคอมพิวเตอร์หนึ่ง ๆ ที่ใช้อินเทอร์เน็ตโพรโทคอลในการสื่อสาร

๑๗๕ สำนักข่าว BBC, “China IP address link to South Korea cyber-attack”.(Online). Available:http://www.bbc.co.uk/news/world-asia-21873017, 2013

กระบวนการยุติธรรม และด้านเศรษฐกิจ ร่วมเป็นกรรมการฯ โดยมีหน้าที่หลักในการจัดทำนโยบายความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อให้ประเทศไทยมีขีดความสามารถในการปกป้อง ป้องกัน รับมือ และลดความเสี่ยงจากสถานการณ์ด้านภัยคุกคามในไซเบอร์ ที่กระทบต่อความมั่นคงของชาติ ทั้งจากภายในและภายนอกประเทศ ครอบคลุมถึงความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ และความมั่นคงทางเศรษฐกิจ ตลอดจนติดตามและประเมินผลการปฏิบัติที่เกี่ยวข้อง เพื่อให้เกิดการบูรณาการการทำงานของหน่วยงานต่างๆ ที่เกี่ยวข้อง อันจะก่อให้เกิดประสิทธิภาพและประสิทธิผลในการบริหารจัดการความมั่นคงปลอดภัยทางสารสนเทศ สอดคล้องกับแนวทางการจัดการด้านเทคโนโลยีสารสนเทศและการสื่อสารของประชาคมอาเซียน โดยมียุทธศาสตร์หลัก ๓ ด้านคือ[๑๗๖]

๑) การบูรณาการจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศ โดยการวางโครงสร้างบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศที่มีความชัดเจนในบทบาทหน้าที่ดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และประสานงานกับผู้ที่รับผิดชอบงานด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของหน่วยงานอื่นๆ การดำเนินการเรื่องตรวจสอบและประเมินผล การประเมินความเสี่ยงของระบบสารสนเทศในระดับประเทศ การพัฒนาบุคลากร การวิจัยและพัฒนา และการเตรียมความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยมีกลไกประสานเชื่อมโยงกับคณะกรรมการนโยบายระดับชาติที่เกี่ยวข้องโดยมีเป้าหมายดังนี้

๑.๑ มีหน่วยงานกลาง (National Cybersecurity Organization)ที่เป็นหลักในการรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยมีบทบาทในการประสานความร่วมมือในการส่งเสริม สนับสนุน มีอำนาจสั่งการ ลงโทษ (ตามกลไกการดำเนินงานของรัฐ) รองรับ กำกับ ตรวจสอบ ประเมิน มีความสามารถในการพัฒนา วิจัย และเตรียมความพร้อม ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งอาจเป็นหน่วยงานที่จัดตั้งขึ้นมาใหม่ เป็นหน่วยงานที่มีอยู่แล้ว หรือเป็นความร่วมมือที่เป็นลายลักษณ์อักษร และเป็นรูปธรรม

๑.๒ มีโครงสร้างการบริหารการรักษาความมั่นคงปลอดภัยระดับชาติ พร้อมบทบาทหน้าที่ที่ชัดเจน ของบุคคลหรือหน่วยงานที่เกี่ยวข้อง และขั้นตอนการดำเนินงาน พร้อมแผนการดำเนินงานและงบประมาณที่สอดคล้องกับเป้าหมายของกรอบนโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ที่เป็นที่ยอมรับของหน่วยงานที่เกี่ยวข้อง

---

๑๗๖ พันเอก ฤทธี อินทราวุธ, “สงครามไซเบอร์สิ่งท้าทายความร่วมมือในอนาคตของอาเซียน (Cyber Warfare : A Challenge of ASEAN Cooperation in Future)”. (Online).Available:http://km.rta.mi.th/newkm/index.php/menu-km6/30-cyber-warfare, 2013

๑.๓ ส่งเสริมให้มีการรักษาความมั่นคงปลอดภัยของทรัพย์สินสารสนเทศ (Information Asset) ทั้งระดับองค์กร และระดับประเทศ โดยใช้กลไกการจัดชั้นความลับเป็นหลักในการจำแนกประเภทของทรัพย์สินสารสนเทศ แล้วจึงกำหนดแนวทางการบริหารจัดการทรัพย์สินสารสนเทศ แต่ละประเภทตามระดับความเสี่ยง (Information classification and security clearance)

๑.๔ การให้บริการของภาครัฐและหน่วยงานที่เป็นโครงสร้างพื้นฐานสำคัญที่เทคโนโลยีของการให้บริการมีผลสำคัญต่อความมั่นคงปลอดภัยของสารสนเทศหรือระบบสารสนเทศ ให้ปฏิบัติตามหลัก CIA เช่นการบริการ outsource/cloud

๒) การสร้างศักยภาพในการตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์สร้างความพร้อมเชิงรับและเชิงรุกในการรับมือภัยคุกคามโดยมีเป้าหมายดังนี้

๒.๑ ประเทศไทยมีเครื่องมือ บุคลากร และสถานที่ พร้อมใช้งานสำหรับการเฝ้าระวังและรับมือภัยคุกคามด้านไซเบอร์ ทั้งที่มาจากภายในประเทศและภายนอกประเทศ โดยทำงานได้ทั้งเชิงรับ และเชิงรุก และสามารถจำกัดความเสียหายจากการโจมตีบนไซเบอร์ได้ทันเวลาโดยไม่กระทบต่อเสถียรภาพทางเศรษฐกิจและความมั่นคงของประเทศ

๒.๒ ให้มีหน่วยงานที่ดำเนินการเป็นศูนย์บัญชาการสำหรับผู้บริหารประเทศ ซึ่งมีการดำเนินการทั้งด้านการทหารและพลเรือน

๓) การป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ ปกป้องโครงสร้างพื้นฐานสำคัญของประเทศและระบบสารสนเทศที่เกี่ยวข้อง ให้สามารถดำเนินการได้อย่างต่อเนื่อง โดยมีเป้าหมายดังนี้

๓.๑ มีการกำหนดหลักเกณฑ์การเป็นโครงสร้างพื้นฐานสำคัญของประเทศ และรณรงค์ให้หน่วยงานหรือองค์กรที่เป็นโครงสร้างพื้นฐานสำคัญของประเทศตระหนักรู้ถึงความสำคัญและความเสี่ยงของตนเอง

๓.๒ ส่งเสริมให้หน่วยงานหรือองค์กรที่เป็นโครงสร้างพื้นฐานสำคัญแต่ละกลุ่มอุตสาหกรรมร่วมกันจัดทำนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ โดยคำนึงถึงความสอดคล้องกับกฎหมาย/กฎระเบียบ/พันธะกรณีระหว่างประเทศ/มาตรฐานสากล ที่เกี่ยวข้องของกลุ่มอุตสาหกรรมนั้นๆ

๓.๓ ส่งเสริมให้หน่วยงานหรือองค์กรที่เป็นโครงสร้างพื้นฐานสำคัญมีการวิเคราะห์ความเสี่ยง มีการจัดทำแผนบริหารจัดการความเสี่ยง และมีการดำเนินการจัดการความเสี่ยงที่เกี่ยวกับภัยคุกคามไซเบอร์รวมทั้งมีการทำ BCM (Business Continuity Management)

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

๓.๕ หน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ จะต้องบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศอันเป็นที่น่าเชื่อถือและยอมรับได้ในระดับสากลและมาตรฐานเฉพาะอุตสาหกรรม

และยุทธศาสตร์รองอีก ๕ ด้าน ได้แก่

๑) การประสานความร่วมมือระหว่างภาครัฐและเอกชนเพื่อความมั่นคงปลอดภัยไซเบอร์ ทำงานร่วมกันระหว่างภาครัฐและเอกชนในการสร้างขีดความสามารถในการตอบสนองภัยคุกคามทางไซเบอร์ในทุกรูปแบบได้อย่างมีประสิทธิภาพ (คน กระบวนการ เครื่องมือ) เพื่อรักษาเสถียรภาพทางเศรษฐกิจ ความมั่นคงแห่งชาติ และคุณภาพชีวิตของประชาชน โดยมีเป้าหมายดังนี้

๑.๑ มีความร่วมมือแบบ PPP เพื่อส่งเสริมให้ผู้พัฒนาผลิตภัณฑ์/บริการ มีความรู้ ทักษะและความตระหนักในการพัฒนาผลิตภัณฑ์และบริการอย่างมั่งคงปลอดภัย

๑.๒ ส่งเสริมให้ทุกภาคส่วนทั้งภาครัฐ เอกชน และประชาชน ใช้ซอฟท์แวร์อย่างถูกต้องตามกฎหมาย เพื่อจะได้รับการแก้ไขปัญหาด้านความปลอดภัยจากผู้ผลิตอย่างสม่ำเสมอ

๑.๓ มีความร่วมมือด้านการแลกเปลี่ยนข้อมูลภัยคุกคามด้านไซเบอร์เพื่อนำไปใช้ในการรักษาความมั่นคงปลอดภัยไซเบอร์

๑.๔ มีนโยบายการบ่มเพาะและสนับสนุนผู้ประกอบการด้าน Cybersecurity ให้มีความพร้อมสู่การให้ความร่วมมือในรูปแบบ PPP ได้อย่างยั่งยืน

๑.๕ มีความร่วมมือในด้านการยืมตัวบุคลากรระหว่างหน่วยงาน (Secondment)

๑.๖ ให้มีกลไกหรือมาตรการ เพื่อกระตุ้นให้เกิดความร่วมมือระหว่างภาครัฐและเอกชน เช่นมาตรการทางภาษี หรือการให้ทุน

๒) การสร้างความตระหนักและรอบรู้ด้านความมั่นคงปลอดภัยไซเบอร์ พัฒนาบุคลากรในบทบาทต่างๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ (ประชาชน ผู้เชี่ยวชาญเฉพาะทาง และผู้รักษากฎหมาย) และสร้างวัฒนธรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยมีเป้าหมายดังนี้

๒.๑ จัดทำมาตรฐานวิชาชีพเพื่อยกระดับความรู้ความสามารถของบุคลากรในสายวิชาชีพความมั่นคงปลอดภัยสารสนเทศ ให้อยู่ในระดับสากล และสร้างเส้นทางความก้าวหน้าในสายอาชีพ พร้อมค่าตอบแทนที่เหมาะสมกับระดับความรู้ความสามารถ

๒.๒ พัฒนากระบวนการรับรองและการกำกับดูแลมาตรฐานวิชาชีพภายในประเทศเพื่อลดค่าใช้จ่าย พร้อมสร้างความยอมรับการรับรองมาตรฐานดังกล่าว

๒.๓ พัฒนาบุคลากรของหน่วยงานภาครัฐให้มีจำนวนที่เพียงพอ และยกระดับความรู้ความสามารถของบุคลากรให้มีความรู้ ความเข้าใจเกี่ยวกับภัยคุกคามไซเบอร์ และสามารถปฏิบัติงานโดยรักษาความมั่นคงปลอดภัยไซเบอร์ได้ตามกฎหมาย

๒.๔ ส่งเสริมและพัฒนาให้บุคลากรในกระบวนการยุติธรรม เช่นตำรวจ พนักงานเจ้าหน้าที่ อัยการ ผู้พิพากษา ราชทัณฑ์ เจ้าหน้าที่ตรวจพิสูจน์พยานหลักฐาน ผู้เชี่ยวชาญ มีความรู้ความเข้าใจเกี่ยวกับภัยคุกคามไซเบอร์ ในการบังคับใช้กฎหมายที่เกี่ยวข้องอย่างต่อเนื่อง

๒.๕ ให้ความรู้อย่างต่อเนื่องและให้องค์ความรู้ที่เข้าถึงได้แก่ประชาชน เพื่อให้มีความตระหนักในความเสี่ยงต่างๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

๒.๖ เพิ่มหลักสูตรการศึกษาตั้งแต่ระดับประถมจนถึงระดับอุดมศึกษา รวมทั้งพัฒนาครูผู้สอน ให้มีความเข้าใจเกี่ยวกับภัยคุกคามไซเบอร์และวิธีการป้องกัน เพื่อให้สามารถนำไปปลูกจิตสำนึกด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิผล ตลอดจนนำไปประยุกต์ใช้กับการใช้งานบนโลกไซเบอร์ได้

๒.๗ ให้มีหน่วยงานที่รับผิดชอบด้านการพัฒนาบุคลากรในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๓) การพัฒนาระเบียบและกฎหมายเพื่อความมั่นคงปลอดภัยไซเบอร์ ปรับปรุงกฎหมายให้ทันสมัย บังคับใช้ได้ มีแนวทางปฏิบัติตามกฎหมายที่ชัดเจน และสอดคล้องกับหลักกฎหมาย/แนวปฏิบัติสากล โดยมีเป้าหมายดังนี้

๓.๑ มีการปรับปรุง/จัดทำกฎหมายเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ เช่น กฎหมายที่เกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ กฎหมายเกี่ยวกับผู้กระทำความผิดทางคอมพิวเตอร์ต่างแดน กฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล ให้สอดคล้องกับหลักสากล มีบทลงโทษ และบังคับใช้ได้

๓.๒ จัดทำกฎหมายลำดับรอง เพื่อให้สามารถบังคับการใช้ให้เป็นไปตามกฎหมายได้

๔) การวิจัยและพัฒนาเพื่อความมั่นคงปลอดภัยไซเบอร์ มีกลไกสร้างความเป็นเลิศด้านการวิจัย และพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์เพื่อให้ประเทศพึ่งพาตัวเองได้อย่างยั่งยืน โดยมีเป้าหมายดังนี้

๔.๑ มีหน่วยงานที่มีหน้าที่หลักโดยเฉพาะในการวิจัยและพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์ (National ICT Academy)

๔.๒ มีแผนงานวิจัยและพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์พร้อมแผนด้านงบประมาณ

๔.๓ มีเครือข่ายความร่วมมือในการวิจัยและพัฒนากับหน่วยงานอื่น ทั้งภาครัฐ เอกชน สถาบันการศึกษา สถาบันวิจัย ทั้งในและต่างประเทศ

๔.๔ จัดทำหลักเกณฑ์มาตรฐานต่างๆ สำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อช่วยให้การบริหารจัดการความมั่นคงปลอดภัยไซเบอร์เป็นไปในทิศทางเดียวกับภายใต้หลักเกณฑ์ของรัฐ

๕) การประสานความร่วมมือระหว่างประเทศเพื่อความมั่นคงปลอดภัยไซเบอร์ เป็นพันธมิตรที่น่าเชื่อถือในเครือข่ายการรักษาความมั่นคงปลอดภัยไซเบอร์ระหว่างประเทศ โดยมีเป้าหมายดังนี้

๕.๑ มีเครือข่ายความร่วมมือระหว่างประเทศ สามารถแลกเปลี่ยนข้อมูลข่าวสาร และปฏิบัติการร่วมกันในการเฝ้าระวังและรับมือภัยคุกคามไซเบอร์

๕.๒ มีการพัฒนาขีดความสามารถที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยการแลกเปลี่ยนบุคลากรในการร่วมปฏิบัติงาน หรือการวิจัยและพัฒนา และโดยการอบรม ฝึกงาน และดูงาน

โดยรัฐบาลจะนำยุทธศาสตร์ทั้ง ๘ ด้านนี้เป็นกรอบการพัฒนาความมั่นคงปลอดภัยไซเบอร์สำหรับประเทศไทยในอีก ๕ ปีข้างหน้า โดยมอบหมายให้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ. (ETDA) เป็นฝ่ายเลขานุการฯ โดยมีความร่วมมือทางด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศ ซึ่งทาง สพธอ. ได้มีการจัดทำความร่วมมือ/บันทึกความเข้าใจ (MOU) มีระยะเวลา ๕ ปี โดยมีกรอบความร่วมมือในด้านการเผยแพร่ข่าวสารทางด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศ การถ่ายโอนองค์ความรู้ การแลกเปลี่ยนข่าวสาร การแลกเปลี่ยนทรัพยากร องค์ความรู้ต่างๆ การสร้างขีดความสามารถทางด้านนิติวิทยาศาสตร์ทางดิจิตอลให้เพิ่มขึ้น และการพัฒนามาตรฐานด้านนิติวิทยาศาสตร์ทางดิจิตอล (Digital Forensics) สำหรับอาเซียน มีแนวทางสนับสนุนการรักษาความมั่นคงปลอดภัยทางสารสนเทศในด้านการสร้างเครื่องมือในการรักษาความปลอดภัยข่าวสาร การประชาสัมพันธ์สร้างความตระหนักและการฝึกอบรมอย่างต่อเนื่อง

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ. ซึ่งทำงานร่วมกับ สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ หรือ ธอ. กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เป็นหน่วยงานหลักที่ทำหน้าที่ดำเนินการพัฒนาส่งเสริม และสนับสนุนการทำธุรกรรมทางอิเล็กทรอนิกส์ให้มีความน่าเชื่อถือ สพธอ. ทำหน้าที่สนับสนุนคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ที่มีบทบาทเชิงรุกในการสร้างความมั่นคงปลอดภัยทางสารสนเทศ เพื่อลดความเสี่ยงของภาครัฐและเอกชน ในการดำเนินการต่างๆ ทางออนไลน์ อีกทั้งยังมีการประสานการทำงานอย่างใกล้ชิดกับสำนักป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร กลุ่มงานตรวจสอบและวิเคราะห์การกระทำความผิดทางเทคโนโลยี กองบังคับการสนับสนุนทางเทคโนโลยี และกองบังคับการปราบปรามการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี สำนักงานตำรวจแห่งชาติ รวมทั้งร่วมผนึกกำลังกับสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ ที่ขานรับนโยบายคุ้มครองและปกป้องผู้บริโภคทางออนไลน์ของ

คณะกรรมการ กสทช. ด้วยเหตุนี้ สพธอ. จึงมีอีกบทบาทในการสนับสนุน คณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติที่มีบทบาทในการดูแลความมั่นคงปลอดภัยจากภัยคุกคามด้านไซเบอร์ (Cyber security Threat) ซึ่งมีรูปแบบที่เปลี่ยนแปลงไปจากอดีตและมีความซับซ้อนมากขึ้น อีกทั้งยังเป็นภัยคุกคามที่สามารถโจมตีได้จากทุกทิศทาง ซึ่งส่งผลกระทบและสร้างความเสียหายให้กับผู้ให้บริการและผู้ใช้บริการเป็นจำนวนมาก จึงเป็นเหตุให้การรับมือและจัดการภัยคุกคามระบบคอมพิวเตอร์ จำเป็นต้องมีการประสานงานร่วมกับหน่วยงานทั้งในประเทศและต่างประเทศเพื่อแก้ปัญหาให้เร็วที่สุด ดังนั้น สพธอ. จึงได้ผลักดันการทำงานเชิงรุกของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทยหรือไทยเซิร์ต (ThaiCERT) ให้ทำหน้าที่เป็นกลไกหลักของประเทศด้านความมั่นคงปลอดภัยของสังคมออนไลน์ และมีการประสานความร่วมมือกับเครือข่าย และหน่วยงานเซิร์ต (CERT/Computer Emergency Response Team) ของต่างประเทศ

ทั้งนี้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย มีภาระหน้าที่หลักเพื่อตอบสนองและจัดการกับเหตุการณ์ความมั่นคงปลอดภัยคอมพิวเตอร์ (Incident Response) และให้การสนับสนุนที่จำเป็น ให้คำแนะนำในการแก้ไขภัยคุกคามความมั่นคงปลอดภัยทางด้านคอมพิวเตอร์ รวมทั้งติดตามและเผยแพร่ข่าวสารและเหตุการณ์ทางด้านความมั่นคงปลอดภัยทางด้านคอมพิวเตอร์ต่อสาธารณชน ตลอดจนทำการศึกษาและพัฒนาเครื่องมือและแนวทางต่างๆ ในการปฏิบัติเพื่อเพิ่มความมั่นคงปลอดภัยในการใช้คอมพิวเตอร์และเครือข่ายอินเทอร์เน็ต ไทยเซิร์ตเป็นที่ปรึกษาทางด้านเทคนิคของไทยฮอตไลน์ในการสืบเสาะต้นตอ วิเคราะห์เนื้อหา และการแก้ไขปัญหาด้านความมั่นคงปลอดภัยระบบคอมพิวเตอร์

กลุ่มงานตรวจสอบและวิเคราะห์การกระทำความผิดทางเทคโนโลยี กองบังคับการสนับสนุนทางเทคโนโลยี (บก.สสท.) สำนักงานตำรวจแห่งชาติ ทำหน้าที่ให้บริการในการตรวจจับการสืบสวน และแก้ไขปัญหาทางคดีเทคโนโลยีสารสนเทศและการสื่อสารที่เกิดขึ้น และป้องกันการบุกรุกทางเครือข่ายของระบบสารสนเทศและการสื่อสาร รวมถึงสนับสนุนผู้ใช้งานและหน่วยงานอื่นๆ ทางด้านคดีเทคโนโลยีสารสนเทศและการสื่อสาร

กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) เป็นหน่วยงานบังคับใช้กฎหมายที่มุ่งเน้นการอำนวยความยุติธรรม ป้องกันปราบปรามอาชญากรรมทางเทคโนโลยีและบริการประชาชน อย่างมีมาตรฐานสากล เพื่อให้เกิดความสงบเรียบร้อย มั่นคง แก่ประชาชน สังคมและประเทศชาติ มีอำนาจหน้าที่และความรับผิดชอบเกี่ยวกับการรักษาความสงบเรียบร้อย ป้องกันและปราบปรามอาชญากรรมที่เกี่ยวกับเทคโนโลยี สืบสวนสอบสวน ปฏิบัติงานตามประมวลกฎหมาย วิธีพิจารณาความอาญา และตามกฎหมายอื่นที่เกี่ยวกับระบบคอมพิวเตอร์ บก.ปอท. กับไทยฮอตไลน์ ร่วมมือกันในการจัดการกับเนื้อหาผิดกฎหมาย/

เป็นอันตรายบนอินเทอร์เน็ต โดยทางไทยฮอตไลน์ได้นำส่งคดีที่ได้รับแจ้งไปยัง บก.ปอท. เพื่อดำเนินการตามขั้นตอนกฎหมาย ไม่ว่าจะเป็นการจับกุม หรือปิดเว็บไซต์ และร่วมมือกับไทยฮอตไลน์เป็นการเฉพาะในการจัดการกับเนื้อหาการละเมิดเด็ก

สำนักป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (Ministry of Information and Communication Technology: MICT) กระทรวงไอซีที เป็นองค์กรหลักในการพัฒนาและบูรณการระบบเทคโนโลยีสารสนเทศและการสื่อสารของประเทศไทย เพื่อให้ประชาชนเข้าถึงการใช้ประโยชน์จากเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพ สำนักป้องกันฯ มีอำนาจในการใช้กฎหมายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 จึงเกี่ยวข้องโดยตรงกับการจัดการผู้กระทำความผิดโดยใช้อินเทอร์เน็ตเป็นเครื่องมือ

ด้านวงการทหาร นายกรัฐมนตรี/รัฐมนตรีว่าการกระทรวงกลาโหม ได้อนุมัติหลักการจัดตั้งศูนย์ปฏิบัติการไซเบอร์กลาโหม (Cyber Operations Center) ขึ้น และกองบัญชาการกองทัพไทย กองทัพบก กองทัพเรือ และกองทัพอากาศ เตรียมการจัดตั้งหน่วยงานด้านไซเบอร์โดยตรง เพื่อขึ้นมารองรับการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยของประเทศ จากภัยคุกคามด้านไซเบอร์ที่ส่งผลกระทบต่อความมั่นคงของชาติ ทั้งจากภายในและภายนอกประเทศ ครอบคลุมถึงความมั่นคงทางด้านการทหาร และความสงบเรียบร้อยภายในประเทศ โดยศูนย์ปฏิบัติการไซเบอร์กลาโหมมีแนวคิดจะเป็นแกนหลัก ในด้านการพัฒนาบุคลากรด้านนี้ให้กับกำลังพลสังกัดกระทรวงกลาโหม โดยจะมีห้องปฏิบัติการสำหรับการฝึกปฏิบัติด้านสงครามไซเบอร์ (Cyber Warfare) รวมถึงการสร้างภาคี เครือข่าย ประชาคม ทั้งภาครัฐและเอกชน เพื่อเสริมสร้างศักยภาพของประเทศด้านไซเบอร์ในการรับมือกับภัยคุกคามด้านไซเบอร์ (ปัจจุบันยังไม่มีการดำเนินการ)

กฎหมายและระเบียบที่เกี่ยวข้อง

แม้ว่าเทคโนโลยีสารสนเทศจะถูกนำมาใช้งานในสังคมอย่างกว้างขวาง ความเข้าใจในสิ่งแวดล้อมของการทำงานของระบบข้อมูลสารสนเทศ นโยบายและกลยุทธในการป้องกันภัยคุกคามข้อมูล อุปกรณ์ เครื่องมือทางเทคนิค โปรแกรมป้องกันภัยข้อมูล และระบบการทำงานต่าง ๆ ขององค์กรหนึ่ง ๆ เพียงลำพัง คงไม่เพียงพอที่จะป้องกันภัยดังกล่าวได้อย่างครอบคลุมและยั่งยืน หากแต่รัฐจำเป็นต้องออกกฎเกณฑ์ หรือกำหนดมาตรการทางกฎหมายเพื่อคุ้มครองทั้งระบบและข้อมูล และเพื่อจัดการหรือปราบปรามการกระทำใด ๆ ที่ถือเป็นภัยคุกคามต่อระบบสารสนเทศ จัดตั้งองค์กรที่มีภารกิจ หรือดูแลด้านนี้โดยเฉพาะ สำหรับประเทศไทยมีกฎหมายที่เกี่ยวข้องดังนี้

๑. พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ เป็นกฎหมายที่ถูกตราขึ้นเพราะในปัจจุบันระบบคอมพิวเตอร์ได้เป็นส่วนสำคัญของการประกอบกิจการและการดำรงชีวิตของมนุษย์ หากมีผู้กระทำด้วยประการใดๆ ให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตาม

คำสั่งที่กำหนดไว้□หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้□ หรือใช้วิธีการใด ๆ เข้าล่วงรู้□ข้อมูล แก้□ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบคอมพิวเตอร์โดยมิชอบ หรือใช้ระบบคอมพิวเตอร์เพื่อเผยแพร่□ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือมีลักษณะอันลามกอนาจาร ย่□อมก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมทั้งความสงบสุขและศีลธรรมอันดีของประชาชน สมควรกำหนดมาตรการเพื่อป้องกันและปราบปรามการกระทำดังกล่าว เช่นการเก็บข้อมูลการจราจรทางอินเทอร์เน็ต (Traffic Log) ซึ่งใช้เป็นหลักฐานหรือข้อมูลในการตรวจจับการกระทำความผิด และการกำหนดบทลงโทษผู้กระทำความผิดตามที่กำหนดไว้ใน พ.ร.บ. นี้

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

ความร่วมมือกับองค์กรระหว่างประเทศ

เนื่องจากการปฏิบัติการในเรื่องความมั่นคงปลอดภัยทางสารสนเทศไม่มีข้อจำกัดทางด้านสถานที่ ไม่มีข้อจำกัดในเรื่องพรมแดน ดังนั้นการร่วมมือกับองค์กรระหว่างประเทศจึงมีความสำคัญอย่างยิ่งต่อการรักษาความมั่นคงปลอดภัยทางสารสนเทศ

๑. ความร่วมมือระหว่างประเทศสมาชิกอาเซียน

การรวมตัวของประเทศในแถบเอเชียตะวันออกเฉียงใต้รวมทั้งประเทศไทยเป็นประชาคมเศรษฐกิจอาเซียน (ASEAN Economics Community : AEC)[๑๗๗] แม้ว่าในด้านหนึ่งจะมีเป้าหมายหลักคือการร่วมมือกันเพื่อพัฒนาเศรษฐกิจ และเพิ่มอำนาจต่อรองให้กับประเทศสมาชิก และจะมีการเปิดเป็นเขตเศรษฐกิจพิเศษใน ม.ค.๕๘ แต่ในอีกด้านหนึ่ง ความร่วมมือระหว่างประเทศสมาชิกในด้านอื่น ๆ ก็เป็นสิ่งที่ไม่สามารถปฏิเสธได้

---

๑๗๗ Association of South East Asian Nations, “ASEAN Economic Community”.(Online).Available:http://www.asean.org/communities/asean-economic-community

ก่อนที่จะมีการรวมตัวกันเป็นประชาคมเศรษฐกิจอาเซียน ประเทศสมาชิกในกลุ่มอาเซียนได้มีความร่วมมือกันทางการทหารมาโดยตลอด และที่เห็นเป็นรูปธรรมชัดเจนที่สุดคือ ประชุมรัฐมนตรีกลาโหมแห่งอาเซียน (ASEAN Defence Ministers Meeting : ADMM)[๑๗๘] ที่มีขึ้นครั้งแรกในปี ๒๕๔๘ และมีการจัดอย่างต่อเนื่อง และล่าสุดมีการจัดขึ้น ณ กรุงพนมเปญ ประเทศกัมพูชาในปี ๒๕๕๕ การประชุมรัฐมนตรีกลาโหมแห่งอาเซียนถือเป็นการประชุมทางการทหารระดับสูงสุดของประเทศสมาชิกในกลุ่มอาเซียน ในการประชุมจะมีการแลกเปลี่ยนความคิดเห็นและมุมมองทางการทหารต่อสถานการณ์และประเด็นที่ได้รับความสนใจในปัจจุบัน เป้าหมายของการประชุมมีขึ้นเพื่อ เพิ่มความเชื่อใจ ความเข้าใจ ในมุมมองด้านความมั่นคงของประเทศสมาชิก รวมถึงการเพิ่มความโปร่งใสและเปิดเผยในการดำเนินการด้านความมั่นคงของประเทศสมาชิก ในด้านหนึ่งในการประชุมรัฐมนตรีกลาโหมแห่งอาเซียนที่ผ่านมา ยังไม่มีการพูดถึงสงครามไซเบอร์ระหว่างประเทศสมาชิกอย่างเป็นรูปธรรม แต่ในอีกด้านหนึ่งก็ปรากฏความร่วมมือทางด้านสงครามไซเบอร์ระหว่างประเทศสมาชิกในอาเซียนกับประเทศญี่ปุ่น[๑๗๙]

การกล่าวถึงสงครามไซเบอร์ระหว่างประเทศสมาชิกในอาเซียน ปรากฏอย่างเป็นรูปธรรมครั้งแรกที่การสัมมนานานาชาติ “สงครามไซเบอร์ สิ่งท้าทายความร่วมมือในอนาคตของอาเซียน”[๑๘๐]โดยในการสัมมนาดังกล่าวได้ข้อสรุปที่เป็นสาระสำคัญในการสร้างความตระหนักและการเตรียมการด้านไซเบอร์ เพื่ออนาคตของกลุ่มประเทศประชาคมอาเซียนในอนาคต ๙ ข้อดังนี้[๑๘๑]

๑. จะต้องเข้าใจธรรมชาติของภัยคุกคามทางด้านไซเบอร์ ซึ่งมีความซับซ้อนและรวดเร็ว อาเซียนจะต้องก้าวไปให้ทัน

---

๑๗๘ Association of South East Asian Nations, “ASEAN Defence Ministers Meeting”.(Online).Available:http://www.asean.org/communities/asean-political-security-community/category/asean-defence-ministers-meeting-admm

๑๗๙ Corey Wallace, Japan Security Watch, “Japan-ASEAN Summit on cyberwarfare countermeasures” .(Online).Available:http://jsw.newpacificinstitute.org/?p=5120, 2012

๑๘๐ มหาวิทยาลัยพระจอมเกล้าธนบุรี, “การสัมมนานานาชาติ เรื่อง 'สงครามไซเบอร์สิ่งท้าทายความร่วมมือในอนาคตของอาเซียน'”.(Online).Available:http://www2.kmutt.ac.th/news/newsdetail.aspx?ref=201303001479, 2013

๑๘๑ พันเอก ฤทธิ อินทราวุธ, “สงครามไซเบอร์สิ่งท้าทายความร่วมมือในอนาคตของอาเซียน (Cyber Warfare : A Challenge of ASEAN Cooperation in Future)”. (Online).Available:http://km.rta.mi.th/newkm/index.php/menu-km6/30-cyber-warfare, 2013

๒. การโจมตีทางด้านไซเบอร์กับกลุ่มประเทศสมาชิกในอาเซียน จะก่อให้เกิดความเสียหาย ดังนั้นภาคีต้องพัฒนาศักยภาพพื้นฐานในด้านนี้ให้มาก เพื่อการเตรียมความพร้อมในการรับมือกับภัยคุกคามที่จะเกิดขึ้น

๓. ภัยคุกคามประเภท APT (Advanced Persistent Threat) จะมีความซับซ้อนมากขึ้น และจะเกิดขึ้นเนื่องจากผลประโยชน์ทางด้านการเมือง และด้านเศรษฐกิจ

๔. ความร่วมมือในงานด้านไซเบอร์ ระหว่างภาครัฐกับเอกชนจะเพิ่มมากขึ้น เพื่อก้าวให้ทันกับพัฒนาการของภัยคุกคามที่ขยายตัวอย่างรวดเร็ว

๕. การเพิ่มขีดความสามารถในการวิจัยและพัฒนาในงานด้านไซเบอร์ จะสร้างเสริมศักยภาพของประเทศ

๖. การสร้างความตระหนักในภัยคุกคามด้านไซเบอร์ โดยภาคีในกลุ่มอาเซียนจะสร้างความเป็นหุ้นส่วนร่วมกัน มีมาตรการรับมือ และข้อเสนอแนะต่างๆ ร่วมกัน

๗. การจัดตั้งชุดเผชิญเหตุฉุกเฉินด้านไซเบอร์ของประชาคมอาเซียน ASIAN CERT (CERT : Community Emergency Response Teams) เพื่อการแลกเปลี่ยนข้อมูล การแจ้งเตือน และการสื่อสารกันระหว่างภาคี หากสมาชิกในกลุ่มถูกภัยคุกคามด้านไซเบอร์จะได้รับประโยชน์

๘. การติดตั้งระบบป้องกันภัยคุกคามทางไซเบอร์ OSCAR ซึ่งเป็นระบบ ฯ ที่กระทรวงกลาโหมอิสราเอล ใช้งานอยู่ โดยนำระบบต่างๆ มารวมกัน และมีศูนย์กลางในการควบคุม เพื่อทำให้ประเทศสมาชิกสามารถทราบว่า หน่วยงานใดในกลุ่มถูกโจมตี โดยสมาชิกในกลุ่มจะทราบทั่วกันทันที สามารถแลกเปลี่ยนข่าวกรอง ทราบรูปแบบ Pattern ของการโจมตี และร่องรอยของการโจมตี เป็นต้น

๙. การติดตั้งระบบ ADS (Advance Detection Systems) ซึ่งเป็นระบบตรวจสอบ Malware ไม่เพียงแต่ตรวจจับ Malware ที่เป็นไฟล์ภายนอกเท่านั้น ADS ยังสามารถตรวจสอบระบบควบคุมและสั่งการของ Malware ด้วย เช่น การตรวจสอบไฟล์ PDF ซึ่งระบบตรวจสอบทั่วไปไม่สามารถทราบว่าในไฟล์ PDF มี Malware ฝังตัวอยู่ แต่ ADS สามารถตรวจสอบเข้าไปในโครงสร้างของไฟล์ได้ โดยจะวิเคราะห์ระบบควบคุมและสั่งการ ดังนั้นไม่ว่าจะมีสิ่งแปลกปลอมใด ระบบ ADS สามารถตรวจสอบได้ทั้งหมด

นอกจากความร่วมมือด้านการป้องกันภัยคุกคามทางทางสารสนเทศแล้ว ประเทศสมาชิกในกลุ่มอาเซียน ยังมีความร่วมมือทางด้านการป้องกัน “อาชญากรรมไซเบอร์”[๑๘๒] อีกด้วย ซึ่งความร่วมมือดังกล่าว มีหลายส่วนที่มีความเกี่ยวโยงกับป้องกันภัยคุกคามทางสารสนเทศ

---

๑๘๒ สภาแห่งสหภาพยุโรป, “ASEAN’s Cooperation on Cybersecurity and against Cybercrime”

๒. ความร่วมมือระหว่างไทยและญี่ปุ่น

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (ไอซีที) ของไทยโดย น.อ.รศ. ดร.ประสงค์ ปราณีตพลกรัง ที่ปรึกษารัฐมนตรีว่ากระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเคยลงนามบันทึกข้อตกลงความร่วมมือ “การป้องกันภัยคุกคามไซเบอร์” ระหว่างสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) กระทรวงไอซีที ประเทศไทย และสำนักงานสารสนเทศและการสื่อสาร (Information and Communication Bureau : ICB) กระทรวงการปกครองและการสื่อสารในประเทศ ประเทศญี่ปุ่น เพื่อให้ทั้ง 2 ประเทศได้แลกเปลี่ยนข้อมูล ความรู้ ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัย และรูปแบบการโจมตีระบบหรือเครือข่ายสารสนเทศจากซอฟต์แวร์ไม่พึงประสงค์ อีกทั้งยังสามารถแจ้งเตือนเมื่อมีเหตุต้องสงสัยว่าจะมีภัยคุกคามจากซอฟต์แวร์ไม่พึงประสงค์ด้วย[๑๘๓]

สรุป

ในบทนี้ได้กล่าวถึงความเป็นมาในอดีต และมุมมองของประเทศต่าง ๆ ที่มีต่อสงครามไซเบอร์ ซึ่งเป็นที่มาของการจัดตั้งองค์กร และโครงสร้างขององค์กร รวมถึงการดำเนินการด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศ และการออกนโยบายในการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศนั้น ๆ นอกจากนี้ยังได้มีการรวบรวมเหตุการณ์สำคัญอันเกี่ยวเนื่องกับสงครามไซเบอร์ และการดำเนินการตอบโต้โดยหน่วยงานภาครัฐ จากเหตุการณ์เหล่านี้ ทำให้เห็นว่าแนวโน้มของภัยคุกคามทางไซเบอร์จะทวีความรุนแรงมากขึ้น มีเหตุเกิดบ่อยครั้งขึ้น และส่งผลกระทบต่อภาคส่วนต่าง ๆ นอกโลกไซเบอร์มากขึ้น

การดำเนินการรับมือกับภัยคุกคามด้านไซเบอร์ของประเทศไทยนั้นรับผิดชอบโดยหลายกระทรวงและหน่วยงาน ได้แก่ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงกลาโหม กระทรวงวิทยาศาสตร์และเทคโนโลยี สำนักงานตำรวจแห่งชาติ เป็นต้น ทำให้ขาดการบูรณาการงานในภาพรวมของการดำเนินการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางสารสนเทศ ในขณะที่องค์กรในต่างประเทศ เช่น สำนักงานความมั่นคงแห่งชาติ (National Security Agency : NSA) ของประเทศสหรัฐอเมริกา เป็นหน่วยงานข่าวกรองที่มีขอบเขตหน้าที่ทั้งในและนอกประเทศ และเป็นหน่วยงานด้านข่าวกรองที่มีขนาดองค์กรที่ใหญ่ที่สุดของสหรัฐอเมริกา มีหน้าที่ในการเฝ้าระวัง ตรวจสอบ ถอดรหัสและประมวลผลข้อมูลอิเล็กทรอนิกส์

---

๑๘๓ เว็บไซต์รัฐบาลไทย, “ก.ไอซีที หนุนความร่วมมือไทย-ญี่ปุ่น ต้านภัยคุมคามทางไซเบอร์”.(Online).Available:http://www.thaigov.go.th/th/news-ministry/2012-08-15-09-45-26/item/75223, 2012

รวมถึงรักษาความมั่นคงปลอดภัยในการรับส่งข้อมูลระหว่างหน่วยงานภาครัฐของสหรัฐอเมริกา NSA มีขีดความสามารถด้านสงครามไซเบอร์หลายด้าน ทั้งในด้านของการป้องกันภัยจากไซเบอร์ การโจรกรรมข้อมูลทางไซเบอร์และการเข้ารหัส ถอดรหัสข้อมูล โดยเฉพาะอย่างยิ่งในส่วนของการเข้ารหัสและถอดรหัสข้อมูล จึงทำให้สามารถเห็นความแตกต่างในการดำเนินการรักษาความมั่นคงปลอดภัยทางสารสนเทศของต่างประเทศ เมื่อเปรียบเทียบกับประเทศไทย

ข้อมูลต่าง ๆ เหล่านี้จะเป็นข้อมูลพื้นฐานสำคัญ และองค์ประกอบที่จะขาดไม่ได้ในการวิเคราะห์ และสังเคราะห์แนวทางการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศไทยในอนาคตต่อไป

บทที่ ๓
ภัยคุกคามรูปแบบต่าง ๆ ที่มีผลกระทบต่อความมั่นคงปลอดภัยทางสารสนเทศและแนวทางการดำเนินการของต่างประเทศ

คลื่นลูกที่สาม การปฏิวัติระบบเศรษฐกิจเชิงนามธรรมผ่านโลกไร้พรมแดน

ภัยคุกคามที่มีผลกระทบต่อความมั่นคงปลอดภัยทางสารสนเทศ เป็นภัยคุกคามที่เกี่ยวข้องกับเทคโนโลยีที่เกิดขึ้นใหม่อย่างอินเตอร์เน็ต และเทคโนโลยีสารสนเทศโดยตรง เนื่องจากเป็นเทคโนโลยีดังกล่าวที่ค่อนข้างใหม่ ทำให้องค์ความรู้ที่เกี่ยวข้องยังคงถูกจำกัดอยู่ในวงแคบผู้เชี่ยวชาญทางด้านเทคนิคโดยเฉพาะอย่างยิ่งผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยทางสารสนเทศยังคงมีปริมาณจำกัด และมีความต้องการในตลาดแรงงานเป็นอย่างมาก[๑] นอกจากนี้องค์ความรู้ที่เกี่ยวข้องอื่น ๆ เช่น เทคโนโลยีสารสนเทศกับความเปลี่ยนแปลงด้านเศรษฐกิจ สังคม การเมือง การทหาร สื่อสารมวลชน และวัฒนธรรม เป็นต้น ในด้านหนึ่งแม้ว่าองค์ความรู้เหล่านี้กำลังมีบทบาทต่อกระแสโลกโดยรวมมากขึ้นเรื่อย ๆ แต่ในอีกด้านหนึ่งองค์ความรู้เหล่านี้เพิ่งได้รับความสนใจ และมีการศึกษาค้นคว้าอย่างจริงจังในช่วงไม่กี่ปีที่ผ่านมาในการวิเคราะห์ภัยคุกคามที่มีผลกระทบต่อความมั่นคงปลอดภัยทางสารสนเทศ ไม่สามารถอาศัยเฉพาะความรู้ทางด้านเทคนิค และความรู้ทางด้านความมั่นคงแต่เพียงลำพังได้ ในบทนี้จะรวบรวมและวิเคราะห์องค์ความรู้ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศในด้านต่าง ๆ ที่เกี่ยวข้อง เพื่อใช้ในการสังเคราะห์หาแนวทางการรักษาความมั่นคงปลอดภัยทางสารสนเทศ

ทฤษฎี "คลื่นลูกที่สาม"[๒] [๓]เป็นทฤษฎีทางเศรษฐศาสตร์ ที่นักเศรษฐศาสตร์ และนักอนาคตศาสตร์ Alvin Toffler ได้ตั้งขึ้นมาเพื่อใช้อธิบายลักษณะทางเศรษฐกิจของสังคมโลกตั้งแต่จุดเริ่มต้นของประวัติศาสตร์มนุษย์จนกระทั่งปัจจุบัน นอกจากนั้น Toffler ยังใช้ทฤษฎีดังกล่าวในการทำนายทิศทางและอนาคตของเศรษฐกิจโลก และที่ผ่านมาก็เป็นที่ประจักษ์แน่ชัดว่าทฤษฎีคลื่นลูกที่สามสามารถทำนายสภาวะเศรษฐกิจโลกได้อย่างถูกต้องแม่นยำ และจนถึงปัจจุบันอาจกล่าวได้ว่าทฤษฎี

---

๑ สำนักข่าว Net-Security, "Lack of computer security experts weighs heavy on U.S. cyber defense",.(Online).Available:http://www.net-security.org/secworld.php?id=9611, 2010

๒ Alvin Toffler, "The Third Wave", Bantam Books, 1980, US

๓ Alvin Toffler, "Revolutionary Wealth", Bantam Books, 2006, US

คลื่นลูกที่สามอาจเป็นทฤษฎีทางเศรษฐศาสตร์เพียงทฤษฎีเดียวที่สามารถอธิบายความสัมพันธ์ระหว่างเทคโนโลยีสารสนเทศ กับเศรษฐกิจโลก และความสัมพันธ์ระหว่างประเทศ ในยุคปัจจุบันได้อย่างครบถ้วน ครอบคลุมและแม่นยำ ทฤษฎีคลื่นลูกที่สามได้แยกสังคมโลกตามนัยยะแห่งการพัฒนาออกเป็น ๓ ยุค ได้แก่

๑. คลื่นลูกที่หนึ่ง สังคมการเกษตร

เกิดจากการปฏิวัติเกษตรกรรมเมื่อ ๑๐,๐๐๐ ปีก่อน[๔] ในช่วงปลายยุคหินใหม่มนุษย์ในยุคนั้นได้เปลี่ยนวิถีชีวิตจากการเร่ร่อน ล่าสัตว์ และเก็บพืชผลไม้ป่าเป็นอาหาร มาเป็นการเริ่มเพาะปลูกและเลี้ยงสัตว์ ตั้งหมู่บ้านอาศัยอยู่เป็นหลักแหล่ง อารยะธรรมเริ่มแรกของมนุษย์จึงเริ่มปรากฏขึ้นเมื่อราว ๓,๐๐๐ ปีก่อนคริสตกาลในดินแดนเมโสโปเตเมีย[๕] เกิดจากการปฏิวัติเกษตรกรรมดังกล่าวทำให้สังคมมนุษย์ที่รู้จักการทำการเกษตรมีเวลาว่างมากขึ้น ไม่จำเป็นต้องใช้เวลาเกือบทั้งหมดในการหาของป่าล่าสัตว์เพื่อใช้ในการดำรงชีวิต อีกทั้งสามารถคาดการณ์เวลาในการเก็บเกี่ยวผลผลิตทางการเกษตรได้ถูกต้องแม่นยำขึ้น ด้วยเหตุและปัจจัยทางด้านเวลาและความมั่งคั่ง ทำให้เกิดวิวัฒนาการทางวัฒนธรรม การสร้างและพัฒนาความรู้หลากหลายสาขา ในหลากหลายภูมิภาคทั่วโลก ดังนั้นในยุคคลื่นลูกที่หนึ่ง ผู้ที่ได้เปรียบด้านการผลิตทางการเกษตรย่อมหมายถึงความได้เปรียบทางด้านอื่นที่ตามมา

ภูมิภาคที่ได้เปรียบทางด้านเศรษฐกิจเริ่มมีการขยายขอบเขตพื้นที่ของตนเอง เพื่อเพิ่มพื้นที่ทางการเกษตรและแรงงานซึ่งเป็นปัจจัยพื้นฐานในการผลิตทางการเกษตร แนวคิดดังกล่าวได้ขยายตัวออกไปจนกลายเป็นการสร้างอาณาจักรในแต่พื้นที่ในที่สุด พัฒนาการด้านการเพิ่มผลผลิตการเกษตร การคิดค้นพัฒนาเทคโนโลยีองค์ความรู้ด้านต่าง ๆ เพื่อให้อาณาจักรของตนเอง มีข้อได้เปรียบสามารถเห็นได้จากความเปลี่ยนแปลงของอาณาจักรในประวัติศาสตร์โลกตั้งแต่ ๓,๐๐๐ ปีก่อนคริสตกาล กระทั่งมาถึงจุดผกผันสำคัญคือยุคฟื้นฟูศิลปวิทยาการ หรือเรอเนสซองส์ (Renaissance) ในยุโรป ทำให้ศิลปวิทยาการแขนงต่างๆ ของกรีกและโรมันแพร่หลายไปอย่างรวดเร็ว ยุโรปเริ่มเข้าสู่ยุคแห่งการสำรวจค้นพบทางทะเล และได้เกิดยุคล่าอาณานิคมในที่สุด[๖]

---

๔ G. C. Hillman, "Late Pleistocene changes in wild plant-foods available to hunter-gatherers of the northern Fertile Crescent: Possible preludes to cereal cultivation", UCL Books, London, pp.159-203, พ.ศ.๒๕๓๙

๕ Richard Bulliet, Pamela Kyle Crossley, Daniel Headrick, Steven Hirsch, Lyman Johnson, David Northup (2010-01-01), "The Earth and Its Peoples: A Global History", Cengage Learning, ๑ ม.ค. ๕๓

๖ David Arnold "The Age of Discovery, 1400–1600", Routledge, ๑๖ มิ.ย. ๕๔

๒. คลื่นลูกที่สอง การปฏิวัติอุตสาหกรรม

เริ่มต้นจากการปฏิวัติอุตสาหกรรมซึ่งมีภูมิหลังมาจาก "ยุคแห่งแสงสว่างทางปัญญา" (Age of Enlightenment)[๗] หรือ "ยุคแห่งเหตุผล" (Age of Reason) ในคริสต์ศตวรรษที่ 18 ที่พัฒนามาจาก "การปฏิวัติทางวิทยาศาสตร์" (Scientific Revolution)[๘] ที่เกิดขึ้นก่อนหน้านี้ ปัญญาชนในยุคนี้ปฏิเสธความคิดความเชื่อที่เกิดจากศรัทธาในศาสนาของยุคกลาง นิยมการค้นหาความจริงโดยหลักของเหตุและผล มองโลกในแง่ดี เชื่อมั่นในความก้าวหน้าของมนุษย์ นำความคิดเชิงวิทยาศาสตร์ไปอธิบายปัญหาสังคม จนนำไปสู่ความรู้ทางด้านสังคมศาสตร์ ซึ่งเป็นช่วงเวลาไล่เลี่ยกับยุคจักรวรรดินิยมและการปฏิวัติอุตสาหกรรม โดยมีไอน้ำและไฟฟ้าเป็นพลังขับเคลื่อนที่สำคัญ[๙]

การปฏิวัติอุตสาหกรรม (Industrial Revolution)[๑๐] ตอนกลางคริสต์ศตวรรษที่ ๑๘ นับเป็นเหตุการณ์สำคัญทางเศรษฐกิจ สังคม และการเมืองของโลก การปฏิวัติอุตสาหกรรมได้นำไปสู่การให้ความสำคัญในเรื่องผลิตผลและประสิทธิภาพของสิ่งที่เรียกกว่า "การทำลายที่สร้างสรรค์"[๑๑] ซึ่งนำมาซึ่งปัญหาต่างๆ หลายประการ ขณะเดียวกันก็ให้ความสะดวกสบายและความเจริญก้าวหน้าแก่มนุษย์จวบจนทุกวันนี้ แบบแผนการทำงานในโรงงานยังเข้ามาแทนที่อุตสาหกรรมในครัวเรือน[๑๒] ซึ่งต้องนำงานมาส่งให้แรงงาน อันทำให้รูปแบบของสินค้า แรงงาน และสถานที่ทำงานเปลี่ยนแปลงไป โดยอาศัยพลังงานและเทคโนโลยีใหม่ๆ อาทิ ถ่านหิน และไอน้ำในช่วงการ

---

๗ Edward Grant, "The Foundations of Modern Science in the Middle Ages: Their Religious, Institutional, and Intellectual Contexts", Cambridge University Press, พ.ศ. ๒๕๓๙

๘ Andrew Atkeson, Patrick J. Kehoe, The Transition to a New Economy After the Second Industrial Revolution", Proceedings, Federal Reserve Bank of San Francisco, issue Nov., ธ.ค. ๕๔

๙ N. F. R. Crafts, "British economic growth during the industrial revolution", Clarendon Press (Oxford Oxfordshire and New York), พ.ศ. ๒๕๒๘

๑๐ Joseph A. Schumpeter, "Capitalism, Socialism and Democracy", (New York: Harper, 1975), pp. 82-85, เผยแพร่ครั้งแรก พ.ศ. ๒๔๘๕

๑๑ P Mantoux, "The industrial revolution in the eighteenth century: An outline of the beginnings of the modern factory system in England", Metuen & CO LTD, เผยแพร่ครั้งแรก พ.ศ. ๒๕๐๔

๑๒ M.C. Jensen, "The modern industrial revolution, exit, and the failure of internal control systems", the Journal of Finance, Wiley Online Library, พ.ศ.๒๕๓๖

ปฏิวัติอุตสาหกรรมครั้งแรก มาเป็นพลังงานไฟฟ้า เคมี และน้ำมันในช่วงปฏิวัติอุตสาหกรรมครั้งที่ 2 [๑๓] รวมทั้งการประดิษฐ์คิดค้น วิทยุ โทรเลข โทรศัพท์ แม้กระทั่งระบบอิเล็กทรอนิกส์ในปัจจุบันการปฏิวัติอุตสาหกรรมที่เปลี่ยนแปลงต่อระบบการทำงานส่งผลกระทบต่อชีวิตมนุษย์แทบทุกด้าน

จากความแตกต่างด้านภูมิประเทศ ภูมิอากาศ รวมไปถึงเบื้องหลังทางประศาสตร์ในแต่ละภูมิภาคจึงทำให้คลื่นแห่งความเปลี่ยนแปลงแต่ละลูกมาถึงไม่พร้อมกัน ในขณะที่ภาคพื้นยุโรปเริ่มมีแนวคิดเรื่องรัฐและประเทศมาปรับใช้ตั้งแต่ตอนกลางคริสต์ศตวรรษที่ ๑๘ เป็นผู้นำการปฏิวัติอุตสาหกรรม และก้าวเข้าสู่คลื่นลูกที่สอง ภูมิภาคอื่นของโลกโดยเฉพาะอย่างยิ่งภูมิภาคในแถบเอเชียส่วนใหญ่ยังคงอยู่ในคลื่นลูกที่หนึ่งที่ขับเคลื่อนเศรษฐกิจด้วยการเกษตร และมีการปกครองแบบอาณาจักร หรือยิ่งไปกว่านั้นในแอฟริกา และโลกใหม่อย่างอเมริกาและออสเตรเลียการผลิตแบบการเกษตรหรือการมาของคลื่นลูกที่หนึ่งยังไม่ลงหลักปักฐานด้วยซ้ำ จากความเหลื่อมล้ำได้นำไปสู่การล่าอาณานิคม และในขณะเดียวกันการล่าอาณานิคมก็เป็นแรงผลักดันให้แต่ละภูมิภาคพัฒนาตนเองเพื่อเป็นประเทศอุตสาหกรรมอย่างรวดเร็ว หลายประเทศ เช่น ญี่ปุ่น เกาหลี ไต้หวัน สิงคโปร์ ประสบความสำเร็จในการพัฒนาตนเองให้ทัดเทียมประเทศตะวันตก แต่ประเทศส่วนใหญ่ยังคงตกอยู่ในกับดักของความพยายามที่จะเป็นประเทศอุตสาหกรรม

๓. คลื่นลูกที่สาม เศรษฐกิจบริการและยุคเทคโนโลยีสารสนเทศ

เป็นยุคสมัยแห่งเทคโนโลยีระดับสูง เป็นคลื่นลูกใหม่แทนที่คลื่นลูกเก่าที่กำลังมีอิทธิพลต่อสังคม เศรษฐกิจ และการเมืองของโลกปัจจุบัน เริ่มด้วยการปฏิวัติอุตสาหกรรมเหล็กกล้า รถยนต์ และเครื่องบิน ซึ่งขยายตัวเต็มที่หลังสงครามโลกครั้งที่ ๒ ปัจจุบันกลุ่มประเทศอุตสาหกรรมชั้นนำ เช่น สหรัฐอเมริกา อังกฤษ เยอรมนี และญี่ปุ่น กำลังแปรสภาพจากสังคมเศรษฐกิจอุตสาหกรรม (Industrial Economy) ไปเป็นสังคมเศรษฐกิจบริการ (Service Economy) [๑๔] มากขึ้นเรื่อยๆ โดยเป็นการผลิตที่ใช้สารสนเทศเพิ่มขึ้น และใช้นโยบายกีดกันการค้าเข้าแทนที่นโยบายการค้าเสรีที่เคยใช้มาก่อน รวมทั้งใช้นโยบายเสรีนิยมทางการเงิน (Financial Liberalize) [๑๕] ทำให้ทุนและ

---

๑๓ J. Gershuny, I. Miles, "The new service economy: the transformation of employment in industrial societies", F. Pinter (London), พ.ศ.๒๕๒๖

๑๔ A. Demirgüç-Kunt, E. Detragiache, "Financial liberalization and financial fragility", The World Bank Development Research Group and International Monetary Fund Research Department, พ.ศ.๒๕๔๑

๑๕ A.Demirgüç-Kunt, E.Detragiache "Financial liberalization and financial fragility" The World Bank Development Research Group and International Monetary Fund Research Department พ.ศ.๒๕๔๑

เงินตรากลายเป็นปัจจัยการผลิตที่ไร้เชื้อชาติและสัญชาติ และสามารถเคลื่อนย้ายระหว่างประเทศโดยเสรี โดยอาศัยความก้าวหน้าของเทคโนโลยีสารสนเทศ ทำให้การลงทุนซื้อขายหลักทรัพย์ระหว่างประเทศมีความสำคัญแซงหน้าการลงทุนโดยตรง

ธุรกิจการเงินและธุรกิจหลักทรัพย์ระหว่างประเทศเข้าไปถือหุ้นในบรรษัทระหว่างประเทศ ตลาดการเงินระหว่างประเทศจึงเชื่อมโยงกับตลาดการผลิตระหว่างประเทศ [๑๖] อันเป็นปรากฏการณ์ซึ่งไม่เคยมีมาก่อนในช่วงก่อนสงครามโลกครั้งที่สอง

ในยุคนี้เองที่เกิดการเปลี่ยนแปลงอย่างถึงรากถึงโคนของสังคมโลกดังจะเห็นได้ว่าในจุดเริ่มต้นของคลื่นลูกที่สาม คือประมาณ ๒๐ ปีที่แล้วสังคมคอมมิวนิสต์ก็มีอันล้มครืนลงและเป็นจุดสิ้นสุดของสงครามเย็น ระบบสารสนเทศได้นำไปสู่การเปลี่ยนแปลงสังคมโลกจากยุคสงครามเย็นไปสู่ยุคหลังสงครามเย็นและวันนี้ได้ขยายไปสู่ปรากฏการณ์ ฤดูใบไม้ผลิอาหรับ (Arab Spring)[๑๗] อันนำไปสู่การพังทลายของระบบการเมืองที่ปิดกั้นหลายแห่งไม่ว่าจะเป็น อียิป ตูนีเซีย ลิเบีย และส่งผลกระทบเป็นลูกโซ่ในลักษณะของกลุ่ม "tea party"[๑๘] กลุ่ม "Indignado"[๑๙] และกลุ่ม "Occupy Wall Street"[๒๐] นอกจากนั้นยังนำไปสู่พลังที่สูงขึ้นของพรรคฝ่ายค้านทำให้รัฐบาลต้องลดการผูกขาดลงไปไม่ว่าจะเป็นสิงคโปร์ มาเลเซีย[๒๑] และขณะนี้พลังดังกล่าวได้แผ่ไปสู่ทุกอณูของสังคมโลกซึ่งนำไปสู่การเปลี่ยนอย่างที่ไม่เคยเห็นมาก่อน

---

๑๖ I. Wallerstein, "Dependence in an interdependent world: the limited possibilities of transformation within the capitalist world economy", African Studies Review, พ.ศ.๒๕๑๗

๑๗ L. Anderson, "Demystifying the Arab Spring: parsing the differences between Tunisia, Egypt, and Libya", สถาบันวิจัย HeinOnline, พ.ศ.๒๕๕๔

๑๘ V. Williamson, T. Skocpol, J. Coggin, "The Tea Party and the remaking of Republican conservatism", Perspectives on Politics, Cambridge University Press, พ.ศ.๒๕๕๔

๑๙ Georgina Blakeley, "Los Indignados: a movement that is here to stay", เว็บไซต์ OpenDemocracy.org,.(Online).Available:http://www.opendemocracy.net/georgina-blakeley/los-indignados-movement-that-is-here-to-stay, 2012

๒๐ J. Dean, "Occupy Wall Street", นิตยสาร Arena Magazine (Fitzroy, Vic), . http://search.informit.com.au/documentSummary;dn=320210167087043;res=IELHSS, 2011-2012

๒๑ D. Slater, "Strong-state democratization in Malaysia and Singapore", Journal of Democracy, Volume 23, Number 2, pp. 19-33, เม.ย.๕๕

พลังคลื่นลูกที่สาม ทำให้รัฐชาติที่ตั้งอยู่บนอธิปไตยของชาติเริ่มถูกกัดกร่อน รัฐชาติไม่สามารถปกป้องอธิปไตยทางการเมืองได้เช่นสมัยก่อน[๒๒] รัฐชาติจำเป็นต้องเปิดเสรีเพื่อรองรับกับการเปลี่ยนแปลงที่ไม่สามารถปิดกั้นได้และนำไปสู่ความจำเป็นในการถ่วงดุลไม่ให้ปลาใหญ่กินปลาเล็กในบริบทของโลกเสรีการรวมกลุ่มเขตการค้าเสรีและประชาคมเศรษฐกิจต่าง ๆ จึงเป็นปรากฏการณ์ของการถ่วงดุลในโลกแห่งความยุ่งเหยิงในยุคคลื่นลูกที่สาม

อินเตอร์เนต เครื่องมือสื่อสารทางทหารที่กลายเป็นพื้นที่ทางเศรษฐกิจและสมรภูมิ

ศาสตราจารย์ทางเศรษฐศาสตร์ชาวออสเตรีย Joseph Schumpeter ได้กล่าวถึงพัฒนาการของเศรษฐกิจโลกไว้ว่า การที่เศรษฐกิจในยุโรปและอเมริกาสามารถขยายตัวอย่างรวดเร็วจนส่งให้ทั้งสองแผ่นดินนี้ก้าวขึ้นเป็นมหาอำนาจของโลกได้นั้น ปัจจัยสำคัญที่สุด คือ การสร้างนวัตกรรมใหม่ ให้เกิดขึ้นในระบบเศรษฐกิจ โดย Schumpeter ยกตัวอย่างการขยายทางรถไฟของสหรัฐอเมริกาในช่วงคริสต์ศตวรรษที่ ๑๙ มีผลทำให้เกิดการขยายตัวทางการค้าและการเจริญเติบโตของเมืองไปพร้อม ๆ กัน Schumpeter อธิบายปรากฏการณ์ดังกล่าวนี้ว่าเมื่อประดิษฐ์กรรมใหม่ ๆ ที่ถูกสร้างขึ้นมานี้เริ่มเป็นที่ถูกอกถูกใจของผู้คนแล้ว มันจะส่งผลให้กลไกตลาดเริ่มทำงานและจัดสรรทรัพยากรในรูปแบบใหม่ผ่านการกำหนดราคาตลาดและเมื่อสิ่งเหล่านี้ได้รับการยอมรับมากขึ้นเรื่อย ๆ ก็จะเข้าไปเปลี่ยนแปลงวิถีชีวิตและการทำงานของผู้คนทั้งโลกในที่สุด และเขาเรียกนวัตกรรมใหม่นี้ว่าเป็น "พลังทำลายแห่งการสร้างสรรค์"[๒๓] [๒๔]เช่น เมื่อโทรศัพท์มือถือรวมไปถึงอีเมล์เข้ามาโทรเลขจึงถูกลดบทบาทลง เนื่องจากนวัตกรรมใหม่ที่ถูกสร้างสรรค์ขึ้นมานี้ได้เข้าไปแทนที่และทำลายนวัตกรรมเดิมลง

คอมพิวเตอร์ถือเป็นพลังทำลายแห่งการสร้างสรรค์อย่างหนึ่ง ตามความหมายของ Shumpeter การพัฒนาขีดความสามารถของคอมพิวเตอร์ตั้งแต่ทศวรรษ ๑๙๗๐[๒๕] เป็นต้นมา ทำให้คอมพิวเตอร์กลายเป็นเครื่องมือที่เข้าไปทดแทนเครื่องมืออื่น ๆ รวมถึงการทำงานบางอย่างโดย

---

๒๒ Samuel P. Huntington, "The Third Wave: Democratization in the Late 20th Century", University of Oklahoma Press, พ.ศ. ๒๕๓๖

๒๓ Creative Destruction

๒๔ Joseph A. Schumpeter, "Capitalism, Socialism and Democracy", (New York: Harper, 1975), pp. 82-85, เผยแพร่ครั้งแรก พ.ศ. ๒๔๘๕

๒๕ M. Campbell-Kelly, W. Aspray, "A History of the Information Machine", พิพิทธภัณฑ์คอมพิวเตอร์ ((Online).Available:http://www.computinghistorymuseum.org/), (Online).Available:http://www.computinghistorymuseum.org/bookinfo/text3.pdf, 2004

แรงงานในอดีต และคอมพิวเตอร์ได้กลายเป็นธุรกิจสำคัญในพื้นที่เศรษฐกิจโลก การเข้ามาของผู้เล่นหน้าใหม่อย่าง IBM Microsoft และ Apple ได้เปลี่ยนภูมิทัศน์ทางเศรษฐกิจโลกไปโดยสิ้นเชิง[๒๖] ผู้เล่นเหล่านี้ได้กลายเป็นผู้กำหนดทิศทางอุตสาหกรรมจำนวนมากทั่วโลกอย่างมีนัยสำคัญ โดยปกติแล้วการเข้ามาเป็นผู้เล่นหน้าใหม่ในโลกธุรกิจและอุตสาหกรรมเป็นเรื่องที่ไม่ง่ายนัก แต่บริษัทเหล่านี้มีข้อเสนอทางการตลาดที่สำคัญและปฏิเสธไม่ได้ คือ นวัตกรรมและเทคโนโลยีชั้นสูงที่สามารถลดขั้นตอนการทำงานและต้นทุนในกิจกรรมทางเศรษฐกิจรวมถึงการผลิตในอุตสาหกรรมอื่นได้

ลำพังการทำงานของเครื่องคอมพิวเตอร์แต่ละเครื่อง ที่ทำงานเป็นเอกเทศ ยังทรงพลังถึงขั้นเปลี่ยนแปลงภูมิทัศน์ทางเศรษฐกิจได้ทั้งโลก การเชื่อมโยงคอมพิวเตอร์จำนวนมากให้ทำงานร่วมกันจนเกิดเป็นเครือข่ายคอมพิวเตอร์จึงยิ่งทวีพลังทำลายแห่งการสร้างสรรค์ และเมื่อเครือข่ายคอมพิวเตอร์ทั่วโลกเชื่อมต่อถึงกันจนกลายเป็นเครือข่ายคอมพิวเตอร์ที่ใหญ่ที่สุดในโลกอย่างอินเตอร์เน็ต จึงเกิดการปฏิวัติเศรษฐกิจโลกครั้งยิ่งใหญ่ที่สุดของโลกอีกครั้งหนึ่งหลังการปฏิวัติอุตสาหกรรม และเป็นจุดเริ่มต้นของคลื่นลูกที่สามดังที่กล่าวไปแล้ว

อินเตอร์เน็ตกำเนิดขึ้นครั้งแรกในประเทศสหรัฐอเมริกา เมื่อ พ.ศ. ๒๕๑๒ โดยกระทรวงกลาโหมสหรัฐอเมริกา มีวัตถุประสงค์ คือ เพื่อให้มีระบบเครือข่ายที่ไม่มีวันตายแม้จะมีสงคราม ระบบการสื่อสารถูกทำลาย หรือตัดขาด แต่ระบบเครือข่ายแบบนี้ยังทำงานได้ซึ่งระบบดังกล่าวจะใช้วิธีส่งข้อมูลในรูปของคลื่นไมโครเวฟ ฝ่ายวิจัยขององค์กรจึงได้จัดตั้งระบบเน็ตเวิร์กขึ้นมา เรียกว่า ARPAnet (Advance Research Project Agency net) [๒๗] ซึ่งประสบความสำเร็จและได้รับความนิยมในหมู่ของหน่วยงานทหาร องค์กร รัฐบาล และสถาบันการศึกษาต่างๆ เป็นอย่างมาก

การเชื่อมต่อในภาพแรกแบบเดิม ถ้าระบบเครือข่ายถูกตัดขาด ระบบก็จะเสียหายและทำให้การเชื่อมต่อขาดออกจากกัน แต่ในเครือข่ายแบบใหม่ แม้ว่าระบบเครือข่ายหนึ่งถูกตัดขาดเครือข่ายก็ยังดำเนินไปได้ไม่เสียหาย เพราะโดยตัวระบบก็หาช่องทางอื่นเชื่อมโยงกันจนได้ในระยะแรก เมื่อ ARPA Net ประสบความสำเร็จ ก็มีองค์กรมหาวิทยาลัยต่างๆให้ความสนใจเข้ามาร่วมในโครงข่ายมากขึ้น โดยเน้นการรับส่งจดหมายอิเล็กทรอนิกส์ (Email) ระหว่างกันเป็นหลัก ต่อมาก็ได้ขยายการบริการไปถึงการส่งแฟ้มข้อมูลข่าวสารและส่งข่าวสารความรู้ทั่วไป แต่ไม่ได้ใช้ในเชิงพาณิชย์ เน้นการให้บริการด้านวิชาการเป็นหลัก

---

๒๖ M.C. Jensen, "The modern industrial revolution, exit, and the failure of internal control systems", the Journal of Finance, Wiley Online Library, พ.ศ.๒๕๓๖

๒๗ P. Barbaroux, "Identifying collaborative innovation capabilities within knowledge-intensive environments: Insights from the ARPANET project", European Journal of Innovation Management, พ.ศ. ๒๕๕๕

อินเตอร์เน็ตได้กลายเป็นเครื่องมือทางการสื่อสารที่สำคัญที่สุดของผู้คนทั่วโลก เนื่องจากมีราคาถูก สามารถใช้งานได้หลากหลายรูปแบบ ทำให้อินเตอร์เน็ตได้รับความนิยมจากผู้คนทั่วโลกอย่างรวดเร็ว ปัจจุบันทั่วโลกมีผู้ใช้งานอินเตอร์เน็ตประมาณ ๓ พันล้านคน[๒๘] โดยในประเทศไทยประชากรกว่าครึ่งสามารถเชื่อมต่อกับอินเตอร์เน็ตได้ [๒๙] ในตลอดช่วงพัฒนาการของอินเตอร์เน็ตนั้น สามารถแบ่งได้เป็นสามยุคด้วยกันได้แก่ จำนวนผู้ใช้งานอินเตอร์เน็ตทั่วโลก พ.ศ. ๒๕๓๔-๒๕๕๔ (ค.ศ.๑๙๙๓ - ๒๐๑๓)[๓๐]

๑. **Internet 1.0**

ยุคแรกเป็น ยุคของการเชื่อมต่อเพื่อการสื่อสารระหว่างบุคคล (Human-to-Human Communication) ในยุคนี้พัฒนาการของอินเตอร์เน็ตจะเป็นเพื่อการสื่อสารระหว่างบุคคลที่ใช้อุปกรณ์คอมพิวเตอร์ที่เชื่อมต่อกับอินเตอร์เน็ต เทคโนโลยีที่สำคัญที่พัฒนาใช้งานกับอินเตอร์เน็ตเพื่อการสื่อสารในยุคนี้ได้แก่ จดหมายอิเล็กทรอนิกส์ที่ยังมีการใช้งานในปัจจุบันและ ยูสเน็ต (UseNet) [๓๑] ที่ได้รับความนิยมลดลงและถูกทดแทนด้วยเทคโนโลยีอื่น

๒. **Internet 2.0**

ยุคต่อมาเป็นยุคของการเชื่อมต่อเพื่อสื่อสารระหว่างบุคคลกับคอมพิวเตอร์ (Human-to-Computer Communication) เทคโนโลยีสำคัญที่พัฒนาขึ้นเพื่อใช้งานอินเตอร์เน็ตในยุคนี้ได้แก่ เว็บ (Web หรือ World Wide Web) เว็บเปิดโอกาสให้บุคคลสามารถเข้าใช้คอมพิวเตอร์เพื่อทำงานใดงานหนึ่งจากระยะไกลได้ผ่านกระบวนการใช้งานที่เป็นมาตรฐานเดียวกัน ก่อนหน้าเทคโนโลยีเว็บ การใช้งานคอมพิวเตอร์จากระยะไกลจะเป็นการใช้งาน "เครื่องคอมพิวเตอร์" เพื่อทำงานด้วยเทคโนโลยีเว็บทำให้การใช้งานคอมพิวเตอร์จากระยะไกลเป็นการใช้งาน "ระบบงาน" เพื่อทำงานนอกจากนี้เว็บยังเปิดโอกาสให้ผู้ใช้ได้ใช้วิธีการใช้งานเดียวกันผ่านโปรแกรมประเภทเว็บบราวเซอร์ (Web Browser) เพื่อใช้ "ระบบงาน" โดยผู้ใช้ไม่จำเป็นต้องรู้ "ที่อยู่เครื่องคอมพิวเตอร์" เพียงแต่รู้ "ที่อยู่ของระบบงาน" เท่านั้น แม้ว่าที่อยู่ของเครื่องจะแฝงอยู่ในที่อยู่ของ

---

๒๘ (Online).Available:http://www.internetlivestats.com/internet-users/

๒๙ หนังสือพิมพ์ Bangkok Post "Half of Thais now on the internet" (Online). Available:http://www.bangkokpost.com/news/local/373333/half-of-thais-now-on-the-ternet, 2013

๓๐ (Online).Available:http://www.internetlivestats.com/internet-users/

๓๑ M. Hauben, R. Hauben, "Netizens: On the history and impact of Usenet and the Internet", Netizens, Volume 3, Number 7, ๖ มิ.ย.๔๑

ระบบงานแต่ก็ไม่ได้เป็นปัจจัยหลัก กล่าวโดยสรุปคือในมุมมองเชิงแนวความคิดแล้ว เว็บทำให้การใช้งานอินเตอร์เน็ตเปลี่ยนจากการอยู่บนพื้นฐานของ "เครื่อง" เป็น "ระบบ"

๓. **Internet 3.0**

ยุคที่สามของอินเตอร์เน็ตเป็นยุคที่กำลังจะก้าวไปสู่เป็น ยุคของการสื่อสารเพื่อการเชื่อมต่อระหว่างคอมพิวเตอร์กับคอมพิวเตอร์ (Computer-to-Computer Communication) " การเชื่อมต่อ" ในที่นี้เป็นการกล่าวถึงการเชื่อมต่อในระดับของสารสนเทศ (Information) ซึ่งเป็นการเชื่อมต่อในระดับที่สูงกว่าใน "การรับรู้ความหมาย" กว่าการเชื่อมต่อเพื่อการส่งผ่านข้อมูล (Data Communication) โดย Cloud Computing ถือเป็นจุดเริ่มต้นหนึ่งของอินเตอร์เน็ตในยุคที่สาม [๓๒]

ในยุคที่สามนี้จะเป็นยุคที่ "ระบบงาน" จะติดต่อสื่อสารกันเพื่อให้สารสนเทศซึ่งกันและกันเพื่อให้บริการแก่ผู้ใช้ กล่าวคือในมุมมองเชิงแนวความคิด (Conceptual Prospective) โดยจะเน้นการ "บริการ" สารสนเทศของตนแก่ระบบงานอื่นๆ และใช้บริการสารสนเทศจากระบบงานอื่น ๆ เพื่อประกอบเป็นบริการของตนให้แก่ผู้ใช้ ดังนั้นสิ่งที่จะเกิดขึ้นในอินเตอร์เน็ตยุคนี้จะเป็นการให้บริการระหว่างเครือข่ายในรูปแบบต่าง ๆ เช่น Software as a Service (SaaS)[๓๓] Infrastructure as a Service (IaaS)[๓๔] เป็นต้น

จะเห็นได้ว่าในยุคที่สามนี้จะมีการกล่าวถึง "บริการ" ระหว่างกันและในการติดต่อสื่อสารของข้อมูลในระบบนี้ก็ยังผ่านเทคโนโลยีพื้นฐานบางอย่างของเว็บ ดังนั้นนักการตลาดของหลายบริษัทจึงใช้คำว่า "Web Services" แทนความหมายของยุคที่สามนี้ ศัพท์ที่เป็นที่นิยมอีกคำหนึ่งที่จะแทนความหมายของยุคนี้คือ "Web 2.0" ซึ่งความหมายเชิงการตลาดมากกว่าที่จะมีความหมายเชิงเทคโนโลยี คำอธิบายในสถานะของผู้ใช้นั้นในยุคแรกของเว็บจะเป็นยุค "เว็บเพื่ออ่านอย่างเดียว" (Read-Only Web) ในยุคนี้ผู้อ่านและผู้เขียนจะแยกกันอย่างชัดเจน คนเขียนจะมีหน้าที่เขียนส่วนคนอ่านจะมีหน้าที่อ่าน ไม่ปะปนกัน ส่วนในยุคที่สองจะเป็นยุค "เว็บเพื่อการอ่านและเขียน" (Read-Write Web) ในยุคนี้ผู้อ่านและผู้เขียนจะเป็นบุคคลเดียวกัน

---

๓๒ M. Armbrust, A. Fox, R. Griffith, et. al., "A view of cloud computing", Communications of the ACM, Volume 53 Issue 4, เม.ย. ๕๓

๓๓ M.P. Papazoglou, "Service-oriented computing: Concepts, characteristics and directions", Web Information Systems Engineering, 2003. WISE 2003. Proceedings of the Fourth International Conference on, ๑๐-๑๒ ธ.ค. ๔๖

๓๔ S. Bhardwaj, L. Jain, S. Jain, "Cloud computing: A study of infrastructure as a service (IAAS)", International Journal of Engineering and Information Technology, Vol. 2 No. 1, พ.ศ. ๒๕๕๓

ในช่วงของ Internet 2.0 ความนิยมในการใช้งานอินเตอร์เน็ตแพร่กระจายไปในวงกว้าง ทำให้เกิดธุรกิจที่เกี่ยวข้องกับอินเตอร์เน็ตเกิดขึ้นมากมายโดยเฉพาะอย่างยิ่งในสหรัฐอเมริกา ธุรกิจเหล่านี้มีชื่อเรียกอย่างไม่เป็นทางการว่าธุรกิจ "ด็อทคอม" (.com) [๓๕] และมีบริษัทด็อทคอมจำนวนหนึ่งเป็นบริษัทจดทะเบียนในตลาดหลักทรัพย์อเมริกา เนื่องจากเป็นธุรกิจใหม่และมีแนวโน้มที่เป็นความต้องการของตลาดที่สูง ทำให้ราคาหุ้นของบริษัทเหล่านี้ในตลาดหลักทรัพย์สูงขึ้นอย่างต่อเนื่องตั้งแต่ พ.ศ.๒๕๓๗ จนถึง พ.ศ. ๒๕๔๓ ทำให้สภาพตลาดของ NASDAQ เพิ่มขึ้นจาก ๑,๐๐๐ จุดในปี ๒๕๓๙ ขยายตัวขึ้นเป็น ๕,๐๐๐ จุดในปี ๒๕๔๓ [๓๖] แม้ว่าบริษัทด็อทคอมจะเป็นที่นิยมในการใช้งาน แต่การทำรายได้ของบริษัทกลับไม่ชัดเจน บริษัทส่วนมากทำรายได้จากการโฆษณาบนหน้าเว็บไซต์ของตนเอง ซึ่งผลตอบแทนมักไม่คุ้มค่าและไม่แน่นอน จนเป็นที่มาของ "ฟองสบู่ด็อทคอม" [๓๗] [๓๘] เมื่อฟองสบู่ด็อทคอมได้แตกลง ทำให้ตลาดหุ้น NASDAQ ดิ่งทะยานจาก ๕,๐๐๐ จุดในปี พ.ศ. ๒๕๔๓ กลับมาสู่ ๑,๒๐๐ จุดในปี พ.ศ.๒๕๔๖ และส่งผลกระทบต่อเศรษฐกิจสหรัฐอเมริกาและเศรษฐกิจโลกจนกระทั่งปัจจุบัน สภาพตลาดหุ้น NASDAQในสหรัฐอเมริกาช่วง พ.ศ.๒๕๓๗-๒๕๕๓ (ค.ศ.๑๙๙๓-๒๐๑๐) (picture/NASDAQ.gif) วิกฤตฟองสบู่ด็อทคอมเป็นเครื่องชี้วัดความสัมพันธ์ระหว่างธุรกิจบนโลกอินเตอร์เน็ตกับเศรษฐกิจอเมริกาและเศรษฐกิจโลกในช่วง ๒๐ ปีที่ผ่านมาได้เป็นอย่างดี

นอกจากธุรกิจด็อทคอมแล้ว การค้าขายผ่านระบบอินเตอร์เน็ต หรือ e-commerce ถือเป็นแนวทางการทำธุรกิจที่สร้างมูลค่ามหาศาลในระบบเศรษฐกิจสหรัฐอเมริกาและเศรษฐกิจโลก [๓๙] แตกต่างจากธุรกิจด็อทคอมอื่น ๆ การค้าขายผ่านระบบอินเตอร์เน็ตมีผลประกอบการที่ชัดเจน และ

---

๓๕ ธุรกิจด็อทคอม เป็นธุรกิจที่ให้บริการผ่านทางอินเตอร์เน็ต ผ่านเว็บไซท์ที่มักทีชื่อโดเมนที่ลงท้ายด้วย .com จึงเป็นที่มาของชื่อ ธุรกิจด็อทคอม การให้บริการของธุรกิจด็อทคอมมักเป็นการให้บริการเชิงข้อมูลข่าวสาร ไม่ใช่การค้าขาย หรือการทำธุรกรรมผ่านอินเตอร์เน็ต

๓๖ Jorn Madslien, "Dotcom bubble burst: 10 years on", สำนักข่าว BBC,. (Online).Available: http://news.bbc.co.uk/2/hi/business/8558257.stm,

๓๗ Dot-Com Bubble

๓๘ A. Ljungqvist, W.J. Wilhelm, "IPO pricing in the dot-com bubble", The Journal of Finance, Wiley Online Library, พ.ศ. ๒๕๔๖

๓๙ C. Wymbs, "How e-commerce is transforming and internationalizing service industries", Journal of Services Marketing, พ.ศ. ๒๕๔๓

สร้างมูลค่าทางเศรษฐกิจให้กับผู้ประกอบการอย่างเป็นรูปธรรม บริษัทที่ใช้การค้าขายผ่านระบบอินเตอร์เน็ตเป็นโครงสร้างหลักในการประกอบธุรกิจอย่าง Amazon.com[๔๐] และ e-bay มีผลประกอบการที่ดีต่อเนื่องตั้งแต่ช่วงก่อนฟองสบู่ดอทคอมจนกระทั่งปัจจุบัน และมีรายได้สูงถึง ๗๕,๐๐๐ ล้านเหรียญสหรัฐอเมริกา สำหรับ Amazon.com และ ๑๕,๐๐๐ ล้านเหรียญสหรัฐอเมริกา สำหรับ e-bay[๔๑] ในปี ๒๕๕๖

โดยภาพรวมแล้วการค้าขายผ่านระบบอินเตอร์เน็ตมีมูลค่าทางการตลาดที่สูงมาก และถือว่าสำหรับประเทศที่พึ่งพาเทคโนโลยีสารสนเทศสูงอย่างสหรัฐอเมริกา การค้าขายผ่านระบบอินเตอร์เน็ตเป็นพื้นที่ทางเศรษฐกิจที่มีความสำคัญเป็นอย่างมาก จนอาจกล่าวได้ว่า ภัยคุกคามที่มีผลต่อความมั่นคงปลอดภัยของการค้าขายผ่านระบบอินเตอร์เน็ต ย่อมหมายถึงภัยคุกคามต่อระบบเศรษฐกิจของประเทศ และเป็นภัยคุกคามต่อความมั่นคงของประเทศด้วยเช่นเดียวกัน

การให้บริการอีกประเภทหนึ่งที่ถือเป็นหัวใจสำคัญในการใช้งานอินเตอร์เน็ตในภาพรวมคือ การให้บริการค้นหาผ่านอินเตอร์เน็ต หรือ Search Engine เนื่องเพราะอินเตอร์เน็ตเป็นพื้นที่ที่มีปริมาณข้อมูลอยู่มหาศาล ทำให้การเข้าถึงข้อมูลที่ผู้ใช้งานต้องการไม่ใช่เรื่องที่ง่ายนัก การให้บริการค้นหาผ่านอินเตอร์เน็ตจะช่วยให้ผู้ใช้งานค้นหาและเข้าถึงข้อมูลที่ตนเองต้องการได้สะดวกรวดเร็วขึ้น Google[๔๒] เป็นผู้ให้บริการด้านค้นหาผ่านอินเตอร์เน็ตรายแรกที่ได้รับความนิยมในการใช้งานอย่างแพร่หลายจากผู้ใช้งานอินเตอร์เน็ตทั่วโลก สืบเนื่องจากนวัตกรรมด้านการค้นหาข้อมูลที่ทำให้ผลการค้นหาตรงกับความต้องการของผู้ใช้งาน และด้วยนวัตกรรมด้านการตลาดที่นำผลการค้นหาและข้อมูลการโฆษณามาประมวลผลร่วมกันภายใต้ผลิตภัณฑ์ที่มีชื่อว่า AdWords[๔๓] ทำให้ Google สามารถสร้างรายได้จากการโฆษณาอย่างมหาศาล จนกลายเป็นบริษัทด้านเทคโนโลยีสารสนเทศที่สามารถสร้างรายได้สูงสุดบริษัทหนึ่งในสหรัฐอเมริกา ในปี ๒๕๕๖ Google สามารถสร้างรายได้สูงถึง ๕๘,๐๐๐ ล้านเหรียญสหรัฐอเมริกา นอกจากการค้นหาผ่านอินเตอร์เน็ตแล้ว

---

๔๐ สำนักข่าว Bloomberg BusinessWeek, "amazon.com inc (AMZN:NASDAQ GS)",.(Online).Available:http://investing.businessweek.com/research/stocks/earnings/earnings.asp?ticker=AMZ

๔๑ สำนักข่าว Bloomberg BusinessWeek, "ebay inc (EBAY:NASDAQ GS)", http://investing.businessweek.com/research/stocks/earnings/earnings.asp?ticker=EBAY

๔๒ (Online).Available:http://www.google.com/

๔๓ (Online).Available:http://www.google.com/adwords/

Google ยังมีบริการอื่น ๆ ที่เกี่ยวข้องกับอินเตอร์เน็ตอีกมากมาย และถือได้ว่าเป็นบริษัทที่ทรงอิทธิพลบริษัทหนึ่งในโลกอินเตอร์เน็ต

ปัจจุบันบริษัทที่ให้บริการการค้นหาผ่านอินเตอร์เน็ตเพียงไม่กี่บริษัททั่วโลก บริษัทที่สามารถแข่งขันกับ Google ได้ในตลาดการค้นหาทั่วโลกมีเพียง Microsoft ภายใต้ผลิตภัณฑ์ Bing[๔๔] นอกเหนือจากนั้นจะเป็นการให้บริการที่เน้นตลาดภูมิภาค เช่น Baidu[๔๕] เน้นการค้าหาที่เป็นภาษาจีน Yandex[๔๖] เน้นการค้าหาที่เป็นภาษารัสเซีย เป็นต้น และเนื่องจาก Google มีศูนย์ข้อมูลขนาดใหญ่ที่เก็บข้อมูลจากอินเตอร์เน็ตจำนวนมหาศาลเพื่อใช้ในการค้นหา ทำให้หลายประเทศมีความกังวลต่ออิทธิพลของ Google ต่อโลกอินเตอร์เน็ต[๔๗] และในขณะเดียวกันด้วยบทบาทของบริการค้นหาข้อมูลบนอินเตอร์เน็ต ทำให้บริษัทเหล่านี้ได้กลายเป็นจุดล่อแหลมที่จะถูกโจมตี [๔๘]

การประกอบธุรกิจบนอินเตอร์เน็ตมักมาพร้อมกับการทำธุรกรรมอิเล็กทรอนิกส์[๔๙] ที่มีทั้งในรูปแบบของการใช้งานบัตรเครดิต และการใช้บริการธนาคารอิเล็กทรอนิกส์[๕๐] ที่ช่วยอำนวยความสะดวกในการซื้อขายสินค้าและบริการผ่านอินเตอร์เน็ต ในปี พ.ศ.๒๕๕๕ มูลค่าการทำธุรกรรมทั่วโลกสูงถึง ๑ ล้านล้านเหรียญสหรัฐ[๕๑] และมีแนวโน้มที่สูงขึ้นในทุกปี ด้วยเม็ดเงินที่มหาศาลทำให้การทำธุรกรรมอิเล็กทรอนิกส์โดยเฉพาะอย่างยิ่งการใช้งานบัตรเครดิตตกเป็น

---

๔๔ (Online).Available:http://www.bing.com/

๔๕ (Online).Available:http://www.baidu.com/

๔๖ (Online).Available:http://www.yandex.com/

๔๗ สำนักข่าว The Conversations, "Google still controls your information, despite EU ruling",. (Online).Available:http://theconversation.com/google-still-controls-your-information-despite-eu-ruling-22925, 2014

๔๘ Mathew J. Schwartz, "Google Aurora Hack Was Chinese Counterespionage Operation", สำนักข่าว Dark Reading, (Online).Available:http://www.darkreading.com/attacks-and-breaches/google-aurora-hack-was-chinese-counterespionage-operation/d/d-id/1110060?

๔๙ e-transaction

๕๐ e-banking

๕๑ สำนักข่าว Internet Retailer, "Global e-commerce tops $1 trillion in 20", .(Online).Available:https://www.internetretailer.com/2013/02/05/global-e-commerce-tops-1-trillion-2012, 2013

เป้าหมายของการก่ออาชญากรรมไซเบอร์ จากรายงานของบริษัทด้านความปลอดภัย ปรากฏว่าอาชญากรรมไซเบอร์ในปี พ.ศ.๒๕๕๖ มีมูลค่าสูงถึง ๓๘๘,๐๐๐ ล้านเหรียญสหรัฐ [๕๒]

ไม่เพียงแต่ธุรกิจในภาคเอกชนเท่านั้นที่ต้องพึ่งพาอินเตอร์เน็ตในการประกอบการ หน่วยงานราชการต่าง ๆ ทั่วโลกได้หันมาให้ความสนใจกับระบบ "รัฐบาลอิเล็กทรอนิกส์"[๕๓] กันมากขึ้น เนื่องเพราะความสะดวกในการใช้งาน การเพิ่มคุณภาพในการบริการประชาชน การขยายขอบเขตในการให้บริการประชาชน และสามารถลดค่าใช้จ่ายของภาครัฐได้ ปัจจุบันประเทศไทยได้หันมาให้บริการผ่านระบบรัฐบาลอิเล็กทรอนิกส์แบบเต็มตัว ดังจะเห็นได้จากเหตุการณ์ทางการเมืองตั้งแต่ พ.ย.๕๖ ที่ผู้ชุมนุมทางการเมืองมีการปิดหน่วยงานราชการเพื่อเป็นการกดดันรัฐบาล ทั้งนี้หน่วยงานราชการส่วนมากยังคงสามารถปฏิบัติงาน และให้บริการประชาชนได้ เนื่องจากมีการทำงานผ่านระบบรัฐบาลอิเล็กทรอนิกส์ [๕๔]

จากบทบาทและความสำคัญของอินเตอร์เน็ตทั้งต่อระบบเศรษฐกิจโดยรวม ต่อภาคเอกชน ต่อการทำธุรกรรมทางด้านการเงิน และหน่วยงานภาครัฐ จนกล่าวได้ว่าความมั่นคงปลอดภัยบนอินเตอร์เน็ต ถือเป็นส่วนหนึ่งของความมั่นคงของประเทศ ไม่แตกต่างจากความมั่นคงปลอดภัยทางเศรษฐกิจอื่น ๆ และด้วยลักษณะของอินเตอร์เน็ตที่เป็นพื้นที่เปิดกว้าง ไร้พรมแดน สามารถเข้าใช้งานจากทั่วโลก ทำให้อินเตอร์เน็ตตกเป็นพื้นที่ในความสนใจ ทั้งจากอาชญากรไซเบอร์ และจากผู้รุกรานทางไซเบอร์

บริการอินเตอร์เน็ตที่ได้รับความนิยมจากผู้ใช้งานอินเตอร์เน็ตทั่วโลกในช่วงทศวรรษที่ผ่านมาคือบริการในรูปแบบที่เรียกว่า "โซเชียลเน็ตเวิร์ค"[๕๕] ที่เป็นผลจากการพัฒนา Web 2.0 ที่ผู้ใช้งานแต่ละคนเป็นมากกว่า "ผู้รับ" ข้อมูลข่าวสาร แต่เป็น "ผู้สร้าง" ข้อมูลข่าวสารในเวลาเดียวกัน นอกจากการสร้างข้อมูลข่าวสารโดยผู้ใช้งานแล้ว การปฏิสัมพันธ์ระหว่างผู้ใช้งานด้วยกันถือเป็นอีกหนึ่งองค์ประกอบสำคัญของโซเชียลเน็ตเวิร์ค และสื่อโซเชียลเน็ตเวิร์คที่ประสบความสำเร็จมักจะสร้างปฏิสัมพันธ์ระหว่างผู้ใช้ในลักษณะ "Real Time Communication" ที่ผู้ใช้งานรับข้อมูลข่าวสารจากผู้ใช้คนอื่นทันทีที่ผู้ใช้คนอื่นสร้างเนื้อหา เครื่องมือที่ทำให้การปฏิสัมพันธ์ในลักษณะดังกล่าว

---

๕๒ Norton by Symantec, “Cybercrime report”,.(Online).Available:http://uk.norton.com/cybercrimereport

๕๓ e-goverment

๕๔ หนังสือพิมพ์ผู้จัดการ, "EGA ฟุ้งภาครัฐยุคใหม่ไม่แคร์มือบ ทำงานบนคลาวด์ได้แม้ถูกยึดพื้นที่", ๒๙ พ.ย. ๕๖,

๕๕ Social Network หรือ Social Media

เกิดขึ้นได้คือโทรศัพท์เคลื่อนที่แบบ "Smart Phone" ร่วมกับการต่ออินเตอร์เน็ตด้วยระบบ 3G ทำให้ผู้ใช้สามารถใช้งานอินเตอร์เน็ตและซอฟท์แวร์โซเชียลเน็ตเวิร์คได้ทุกที่ทุกเวลา

ปัจจุบันบริการโซเชียลเน็ตเวิร์คที่ได้รับความนิยมจากผู้ใช้งานทั่วโลกได้แก่ Facebook [๕๖] Twitter[๕๗] Instagram[๕๘] LINE[๕๙] Whatsapp[๖๐] เป็นต้น จากสถิติการใช้งานทั่วโลก ในปี ๒๕๕๖ ผู้ใช้งานอินเตอร์เน็ต ๕๘% หรือ กว่า ๑,๗๐๐ ล้านคนทั่วโลกมีการใช้งานโซเชียลมีเดีย [๖๑] โดยเฉพาะอย่างยิ่ง Facebook มีปริมาณผู้ใช้งานมากถึง ๑,๓๐๐ ล้านคนทั่วโลก[๖๒] โดยในนั้นมีผู้ใช้งานจากอุปกรณ์พกพาเช่น Smart Phone หรือ Tablet ประมาณ ๑๘๙ ล้านคน [๖๓]

ด้วยลักษณะเฉพาะของโซเชียลเน็ตเวิร์คที่ข้อมูลมีความสดใหม่ มีที่มาของแหล่งข้อมูลที่หลากหลาย ไม่จำกัดเฉพาะสำนักข่าว การแพร่กระจายของข้อมูลที่รวดเร็วและกว้างขวาง ทำให้โซเชียลเน็ตเวิร์คกลายเป็นสื่อใหม่ที่มีทรงพลังและทรงอิทธิพลเทียบเท่าสื่อเดิมอย่าง โทรทัศน์ วิทยุ หนังสือพิมพ์ แม้แต่คนในวงการสื่อเดิมเองก็ให้การยอมรับ และยกให้โซเชียลเน็ตเวิร์ค

---

๕๖ (Online).Available:http://www.facebook.com/

๕๗ (Online).Available:http://www.twitter.com/

๕๘ (Online).Available:http://www.instagram.com/

๕๙ (Online).Available:http://www.line.me/

๖๐ (Online).Available:http://www.whatsapp.com/

๖๑ Statisti Brain, "Social Networking Statistics", (Online). Available:http://www.statisticbrain.com/social-networking-statistics/, 2014

๖๒ Statisti Brain, "Facebook Statistics", (Online).Available:http://www.statisticbrain.com/facebook-statistics/, 2014

๖๓ Belle Beth Cooper, "10 Surprising Social Media Statistics That Will Make You Rethink Your Social Strategy", Fast Company, (Online).Available:http://www.fastcompany.com/3021749/work-smart/10-surprising-social-media-statistics-that-will-make-you-rethink-your-social-stra

เป็น "ฐานันดร ที่ ๕"[๖๔] [๖๕]และได้เปลี่ยนมุมมองจากประชาชนในฐานะ "ผู้รับข่าว" เป็นประชาชนในฐานะ "ผู้รับและสื่อข่าว" โดย Alvin Toffler ได้ให้จำกัดความการทำหน้าที่สื่อของประชาชนในลักษณะนี้ว่า "Prosumer"[๖๖] ซึ่งเป็นการผสมคำระหว่าง Producer หรือผู้ผลิต กับ Consumer หรือผู้บริโภค ในหลายกรณีผู้สื่อข่าวมืออาชีพเองก็ได้ใช้โซเชียลเน็ตเวิร์คเป็นแหล่งข่าวปฐมภูมิของตนเอง

เหตุการณ์สำคัญที่แสดงให้เห็นถึงความทรงอิทธิพลของโซเชียลเน็ตเวิร์คคือ Arab Spring[๖๗] [๖๘]ที่จุดเริ่มต้นจากการแลกเปลี่ยนข้อมูลข่าวสารและความคิดเห็นของประชาชนตูนีเซียผ่าน Facebook จนเกิดความเคลื่อนไหวทางสังคม ทางการเมือง นำไปสู่การล้มรัฐบาลเผด็จการทหารในที่สุด ความเคลื่อนไหวทางสังคมยังคงไม่หยุดแค่เพียงในประเทศตูนิเซีย แต่ขยายวงกว้างออกไปยัง อียิปต์ ลิเบีย เยเมน บาเรน และซีเรีย รวมไปถึงการชุมนุมประท้วงรัฐบาลในประเทศ อัลจีเรีย อิรัก จอร์แดน

---

๖๔ ฐานันดรที่สี่ หมายถึง แรงขับดันหรือสถาบัน ทางสังคมหรือการเมือง ที่อิทธิพลของมันเป็นที่รับรู้ได้อย่างสม่ำเสมอหรือเป็นทางการ ซึ่งมักจะหมายถึงสื่อข่าว โดยเฉพาะสื่อข่าวสิ่งพิมพ์ (The Press) โดยฐานันดรมีที่มาจากรัฐสภาอังกฤษประกอบด้วยฐานันดรศักดิ์ทั้งสาม คือ ฐานันดรที่ 1 ประกอบด้วยสภาขุนนางอันมี พวกขุนนางสืบตระกูล ฐานันดรที่ 2 ประกอบด้วย บรรพชิต พระราชาคณะ ฐานันดรที่ 3 ประกอบด้วย สภาผู้แทนราษฎร ซึ่งคนธรรมดาได้เลือกตั้งให้เป็นแทนตนเข้าไป วันหนึ่งได้มีการประชุมในรัฐสภาอังกฤษ ได้มีสมาชิกสภาผู้แทนราษฎรคนชื่อ นายเอ็ดมันด์ เบิร์ก อภิปรายมีตอนหนึ่งที่ท่านผู้นี้ได้กล่าวขึ้นว่า..... "ในขณะที่เราทั้งหลายเป็นฐานันดรใดฐานันดรหนึ่งทั้งสามกำลังประชุมกันอยู่นี้ เราพึงคำนึงไว้ด้วยว่าบัดนี้ได้มี ฐานันดรที่ 4 เกิดขึ้นแล้ว และฐานันดรนั้นกำลังมานั่งฟังการประชุมของเราอยู่ ณ ที่นี้ด้วย" เขาก็ชี้มือไปยัง กลุ่มคนหนังสือพิมพ์ ซึ่งได้พากันมานั่งฟังการประชุม ตั้งแต่นั้นมากลุ่มผู้ประกอบอาชีพหนังสือพิมพ์จึงกล่าวว่าเป็นฐานันดรที่สี่

๖๕ หนังสือพิมพ์ คม ชัด ลึก, "ฐานันดร5+:โลกที่ทุกคนเป็นนักข่าว?",. (Online).Available:http://www.komchadluek.net/detail/20120808/137152, 2012

๖๖ Alvin Toffler, "Revolutionary Wealth", Bantam Books, 2006, USA

๖๗ C. Huang, "Role of the new media in the Arab Spring", หนังสือพิมพ์ The National,.(Online).Available:http://openlab.citytech.cuny.edu/designprocess/files/2012/08/TheNational_FacebookandTwitterKeytoArabSpringUprising.pdf, 2011

๖๘ H.H. Khondker, "Role of the New Media in the Arab Spring", Globalizations, Volume 8, Issue5,.(Online).Available:http://www.tandfonline.com/doi/abs/10.1080/14747731.2011.621287#.U0OPmab9rQo, 2011

คูเวต โมร็อกโก ซูดาน มริทันเนีย โอมาน ซาอุดิอาราเบีย จิบูติ ซาฮาร่าตะวันตก และปาเลสสไตน์ [๖๙] อาจกล่าวได้ว่า Arab Spring ถือเป็นความเคลื่อนไหวทางสังคม และทางการเมืองที่แพร่ขยายออกไปในพื้นที่เป็นวงกว้าง และส่งผลต่อประชาชนจำนวนมากที่สุดครั้งหนึ่งในประวัติศาสตร์โลก และ Arab Spring จะเกิดขึ้นไม่ได้เลยหากไร้ซึ่งโซเชียลเน็ตเวิร์ค

นอกจากคุณสมบัติในฐานะสื่อ ที่ทำให้โซเชียลเน็ตเวิร์คเป็นแหล่งข่าวที่มีความหลากหลายข้อมูล และสามารถกระจายข้อมูลข่าวสารได้อย่างรวดเร็วแล้ว คุณสมบัติที่สื่ออื่นไม่เคยมีมาก่อนคือ "การไร้การควบคุม" ซึ่งในสื่อเดิมแม้ในประเทศที่สื่อมีสิทธิเสรีภาพสูง ไม่ถูกควบคุมโดยหน่วยงานภาครัฐ แต่ก็สามารถถูกควบคุมโดยความคิดเห็นของบรรณาธิการ ผู้ประกอบการ และผู้สนับสนุนกิจการ การเป็นสื่อที่ไร้การควบคุมของโซเชียลเน็ตเวิร์คนั้นเป็นดาบสองคมที่ควรพึงระวัง ในด้านหนึ่งโซเชียลเน็ตเวิร์คเป็นเครื่องมืออันทรงพลังในการสนับสนุนสิทธิเสรีภาพในการแสดงความคิดเห็น แต่ในอีกด้านหนึ่ง ก็ทำให้คุณภาพของข้อมูลข่าวสารในโซเชียลมีเดียนั้นลดคุณภาพ และความน่าเชื่อถือลงไปด้วย และด้วยการไร้การควบคุมทำให้โซเชียลเน็ตเวิร์คกลายเป็นพื้นที่เป้าหมายในการทำ "สงครามข้อมูลข่าวสาร"[๗๐] ที่ทรงพลังไม่แพ้การเคลื่อนไหวทางสังคม

รูปแบบการก่อการร้ายในโลกเสมือนจริง

ด้วยความเจริญก้าวหน้าของระบบการติดต่อสื่อสารได้เปิดโอกาสและช่องทางให้กลุ่มก่อการร้ายอาศัยสื่ออินเตอร์เน็ตเป็นเครื่องมือในการติดต่อสื่อสาร การประสานงานและการวางแผนก่อการร้าย ก่อให้เกิดภัยคุกคามต่อความมั่นคงของประเทศต่างๆทั่วโลก โดยธรรมชาติของอินเตอร์เน็ตเป็นสถานที่ที่มีความเหมาะสมในการดำเนินกิจกรรมต่างๆขององค์กรก่อการร้าย เนื่องจากสะดวกต่อการเข้าถึง มีกฎข้อบังคับน้อย ไม่มีการตรวจสอบ หรือการควบคุมจากหน่วยงานภาครัฐ มีจำนวนของผู้ใช้งานอยู่ในปริมาณสูง การไหลของข้อมูลที่รวดเร็ว ราคาประหยัดในการดำเนินการจัดทำและดูแล และ สามารถสื่อสารได้ในระบบมัลติมีเดีย ข้อความ ภาพ เสียง ภาพเคลื่อนไหว วีดีโอ ซึ่งผู้ใช้สามารถเข้าถึงและดาวโหลดข้อมูลได้อย่างรวดเร็ว

---

๖๙ Garry Blight, Sheila Pulham, Paul Torpey, "Arab spring: an interactive timeline of Middle East protests", สำนักข่าว The Gurdian,,(Online).Available:http://www.theguardian.com/world/interactive/2011/mar/22/middle-east-protest-interactive-timeline, 2012

๗๐ Mathew Ingram, "How social media is rewriting the rules of modern warfare", เว็บไซต์ GIGAOM, http://gigaom.com/2012/11/19/how-social-media-is-rewriting-the-rules-of-modern-warfare/, 2012

การใช้งานอินเตอร์เน็ตของกลุ่มก่อการร้ายมีรูปแบบพลวัตร กล่าวคือมีการเปลี่ยนแปลงและเคลื่อนไหวอยู่ตลอดเวลา มีการเกิดขึ้นและหายไปอย่างรวดเร็วเพื่อเป็นการปกปิดและการลวงถึงวัตถุประสงค์ที่แท้จริงของกลุ่ม อย่างไรก็ตามเราสามารถระบุการใช้งานอินเตอร์เน็ตของกลุ่มก่อการร้ายได้ออกเป็น ๘ แนวทางซึ่งมีการทับซ้อนกันบางโอกาส มีการใช้งานคู่ขนานกันไปตามวัตถุประสงค์ของกลุ่ม ดังนี้ [๗๑]

๑. สงครามปฏิบัติการจิตวิทยา

การบิดเบือนข้อเท็จจริง การเผยแพร่ภัยคุกคามให้เกิดความหวาดกลัวและสิ้นหวัง เช่น การสังหารผู้สื่อข่าวชาวอเมริกันอย่างโหดเหี้ยม ภาพวิดีโอเทปที่ถูกเผยแพร่บนเว็บไซต์ของผู้ก่อการร้ายหลายๆแห่ง ผู้ก่อการร้ายสามารถสร้างความหวาดกลัวผ่านทางอินเตอร์เน็ต เพื่อผลทางจิตวิทยา ความหวาดกลัวภัยอินเตอร์เน็ต ถูกกระทำให้เกิดขึ้นจากความวิตกกังวลเกี่ยวกับการโจมตีต่อระบบคอมพิวเตอร์เครือข่ายของสายการบิน ส่งผลให้ระบบคอมพิวเตอร์ควบคุมการบินขัดข้องหรือโจมตีระบบเศรษฐกิจของชาติ โดยการเจาะระบบเข้าไปทำลายระบบคอมพิวเตอร์ของตลาดหุ้นโดยอาศัยการไหลของข้อมูลข่าวสารที่รวดเร็วและต่อเนื่อง จนทำให้สาธารณชนเชื่อว่าเหตุการณ์ดังกล่าวจะเกิดขึ้นจริง

กลุ่มอัลเคด้า ได้ผสมผสานการโฆษณาชวนเชื่อโดยอาศัยเทคโนโลยีในการสร้างรูปแบบสงครามปฏิบัติการจิตวิทยา อุสมา บิน ลาเดน และพรรคพวก มุ่งความพยายามของการสร้างการโฆษณาชวนเชื่อบน[๗๒] อินเตอร์เน็ต สถานที่ซึ่งผู้เยี่ยมชมจากทั่วโลกสามารถเข้าถึงเพื่อสร้างความเห็นใจในรูปแบบของสื่อชนิดต่างๆ เช่น ข้อความ วิดีโอเทปและ ไฟล์เสียง ภาพ และการประกาศประชาสัมพันธ์ต่าง ๆเป็นที่น่าสนใจว่า กลุ่มอัลเคด้า สามารถอ้างต่อเนื่องในเวบไซต์ ถึงการทำลายล้างตึกเวิล์ดเทรดเซ็นเตอร์ สร้างความเสียหายด้านจิตวิทยา พอๆกับการสร้างความเสียหายทางด้านกายภาพ[๗๓] ในระบบเศรษฐกิจของสหรัฐอเมริกา การโจมตีตึกแฝดดังกล่าวถือเป็นการกระทำต่อเครื่องหมายการค้าของสหรัฐอเมริกา หลักฐานที่มีประสิทธิภาพคือการอ่อนค่าลงของเงินดอลล่าร์สหรัฐอเมริกา การตกลงของตลาดหุ้น และการสูญเสียความเชื่อมั่นของระบบเศรษฐกิจ

---

๗๑ เว็บไซต์ทหารพลร่ม, "อินเตอร์เน็ตกับการก่อการร้ายสากล", ๑๐ ต.ค. ๕๒

๗๒ P.L. Bergen, "Holy war, Inc.: inside the secret world of Osama bin Laden", TOUCHSTONE Rockfeller Center, New York, U.S.A., พ.ศ. ๒๕๔๔

๗๓ Sandro Galea, Jennifer Ahern, Heidi Resnick, et.al., "Psychological Sequelae of the September 11 Terrorist Attacks in New York City", Special Article on N Engl J Med 2002

สหรัฐอเมริกาและอื่น ๆ ทั่วโลก [๗๔] นอกจากนี้ยังสามารถเผยแพร่ถึงการกระทำดังกล่าวว่าสหรัฐอเมริกาถูกโต้ตอบโดยอำนาจที่ยิ่งใหญ่จากพระเจ้า

๒. สื่อสาธารณะและการโฆษณาชวนเชื่อ

อินเตอร์เน็ตมีความสำคัญและเพิ่มโอกาสของกลุ่มก่อการร้ายที่จะแย่งชิงสาธารณะโดยคาดหวังชัยชนะเหนือสาธารณะในปัญหาและกิจกรรมที่ดำเนินอยู่ สมัยก่อนการต่อสู้ต้องพึ่งพาสื่อจำพวก วิทยุ โทรทัศน์และสื่อสิ่งพิมพ์ ซึ่งปกติแล้วยากที่กลุ่มก่อการร้ายจะเข้าถึง จนกระทั่งอินเตอร์เน็ตเกิดขึ้น ความจำกัดดังกล่าวได้หมดไป ปัจจุบันกลุ่มก่อการร้ายต่างๆได้มีเว็บไซต์ของตนเองเพื่อเผยแพร่ข่าวสาร สามารถที่จะนำเสนอและควบคุมข่าวสารได้อย่างไม่จำกัด สร้างภาพที่ยุติธรรมและโจมตีศัตรูได้ เว็บไซต์ของกลุ่มก่อการร้ายปกติแล้วจะนำใช้เทคนิคในการนำเสนอ ๓ แนวทาง

๒.๑ การกล่าวอ้างถึงความจำเป็นและไม่มีทางเลือกอื่นนอกจากใช้ความรุนแรงด้วยวิธีการนี้ จะทำให้สื่อถึงภาพองค์กรที่มีขนาดเล็ก อ่อนแอ และถูกเอารัดเอาเปรียบ

๒.๒ สร้างความชอบธรรมของการใช้ความรุ่นแรงเพื่อสมาชิกของกลุ่มจะถูกนำเสนอในฐานะของนักสู้เพื่ออิสรภาพ แรงกระตุ้นให้ต่อสู้อย่างรุ่นแรงเนื่องจากศัตรูกำลังบีบคั้นสิทธิและศักดิ์ศรีของกลุ่ม กลุ่มหรือองค์กรที่อยู่ตรงข้ามคือผู้ก่อการร้ายตัวจริง การใช้ความรุนแรงเป็นเพียงส่วนเล็กน้อยเมื่อเทียบกับสิ่งที่ถูกกระทำ กลุ่มก่อการร้ายพยายามที่จะเปลี่ยนความรับผิดชอบของความรุนแรงให้กับฝ่ายตรงข้าม ซึ่งถูกกล่าวหาว่ามีความโหดร้าย ไม่ใช้มนุษย์ และไร้ศีลธรรม

๒.๓ การสร้างภาพของการไม่ใช้ความรุนแรงในความพยายามในการแก้ไขปัญหา แม้ว่าองค์กรเหล่านี้คือองค์กรแห่งความรุ่นแรง เว็บไซต์จำนวนมากของกลุ่มเหล่านี้กล่าวอ้างถึงการค้นหาการแก้ปัญหาอย่างเสรีภาพ ซึ่งเป้าประสงค์สูงสุดคือการเจรจาทางการทูต

๓. แหล่งข้อมูล

อินเตอร์เน็ตอาจจะถูกมองในฐานะของห้องสมุดดิจิตอลขนาดใหญ่ ในโลกของอินเตอร์เน็ตเพียงอย่างเดียวก็เต็มไปด้วยข้อมูลมหาศาล และส่วนใหญ่แล้วฟรี และส่วนใหญ่ก็เป็นที่สนใจของ กลุ่มก่อการร้าย ผู้ก่อการร้ายสามารถเรียนรู้จากอินเตอร์เน็ตเกี่ยวกับเป้าหมาย เช่น ระบบการขนส่งมวลชน โรงงานนิวเคลียร์ อาคารสาธารณะ สนามบิน ท่าเรือ แม้กระทั่งมาตรการต่อต้านการก่อการร้าย Dan Verton [๗๕] อธิบายว่า กลุ่มก่อการร้ายอัลเคด้า ปฏิบัติการโดยใช้ฐานข้อมูลจากอินเตอร์เน็ตในการรวบรวมเป้าหมายที่เป็นไปได้ในสหรัฐอเมริกา กลุ่มก่อการร้ายใช้อินเตอร์เน็ต

---

๗๔ J.M. Virgo, "Economic impact of the terrorist attacks of September 11", Atlantic Economic Journal, 2001, Springer, U.S.A.

๗๕ Dan Verton, "Black Ice: The Invisible Threat of Cyber-Terrorism", McGraw-Hill Osborne Media; 1 edition, ๑๕ ส.ค.๔๖

เครื่องมือการข่าวเพื่อรวบรวมข่าวสารเกี่ยวกับเป้าหมาย เฉพาะอย่างยิ่งเป้าหมายสำคัญด้านเศรษฐกิจ ด้วยความสามารถของโปรแกรมสมัยใหม่เกื้อกูลให้สามารถศึกษาโครงสร้างจุดอ่อนของสิ่งอำนวยความสะดวกรวมทั้งการคาดการณ์ผลกระทบจากการโจมตีที่เกิดขึ้น ปัจจุบันมีเว็บไซต์จำนวนมากที่เสนอเครื่องมือในการค้นหาข้อมูล ทำให้เกื้อกูลต่อผู้ก่อการร้ายสามารถเข้าถึงข้อมูลได้อย่างสะดวก โดยใช้ความพยายามเล็กน้อยหรือลงทุนนิดหน่อย

๔. แหล่งระดมเงินทุน

การหาเงินทุนสนับสนุนการก่อการร้ายโดยอาศัยอินเตอร์เน็ตเป็นสื่อกลาง คล้ายกับเว็บไซต์ขององค์การทางการเมือง ซึ่งจัดขึ้นเพื่อหาเงินทุนจากผู้สนับสนุน ดังนั้นกลุ่มผู้ก่อการร้ายก็ได้จัดตั้งเว็บไซต์จำนวนมากขึ้นเพื่อระดมทุนจากแนวร่วมหรือผู้มีอุดมการณ์ร่วมจากทั่วโลก ซึ่งจะอยู่ในรูปของการบริจาคเพื่อกองทุนการกุศล องค์กรที่ไม่ใช่รัฐ เช่น กลุ่ม Hizb ut-Tahrir[๗๖] ใช้การบูรณาการของเว็บไซต์ เครือข่ายเชื่อมโยงทั่วโลก เพื่อขอรับการสนับสนุนเงินทุนการกุศลทางศาสนา ซึ่งผู้ศรัทธาสามารถบริจาคได้ทั้งในรูปแบบของการโอนเงินเข้าบัญชีธนาคารโดยใช้ระบบบัตรเครดิตด้วย จึงนับว่าสะดวกอย่างยิ่ง

กลุ่มก่อการร้ายจะใช้ประโยชน์จากข้อมูลส่วนบุคคลที่ใช้ในการกรอกแบบสอบถามหรือการสั่งซื้อในอินเตอร์เน็ต ซึ่งทำให้สามารถระบุกลุ่มผู้ใช้ ที่มีแนวโน้มทัศนะคติความเชื่อที่ใกล้เคียงกัน ต่อมากลุ่มบุคคลเหล่านี้จะถูกถามให้บริจาคเงินช่วยเหลือ ผ่านทางระบบอีเมล์ ซึ่งส่งมาจากตัวแทนของก่อการร้าย หรือองค์กรที่สนับสนุนการก่อการร้าย แต่ดำเนินการเปิดเผยและถูกกฎหมาย และปกติจะไม่มีหลักฐานเชื่อโยงถึงกลุ่มก่อการร้าย เช่น เงินทุนสนับสนุนขบวนการกลุ่มฮามาส จะถูกรวบรวมผ่านทางเว็บไซต์ ซึ่งถูกรัฐบาลสหรัฐอเมริกา จับกุมทรัพย์สินใน ธ.ค.๔๓[๗๗] เนื่องจากมีความเชื่อมโยงกับกลุ่มฮามาส

๕. การชักจูงสมาชิก

อินเตอร์เน็ตไม่เป็นเพียงแต่เครื่องมือในการเข้าถึงการบริจาค แต่รวมถึงการชักชวนสมาชิกใหม่โดยอาศัยการเก็บข้อมูลผู้ใช้งานที่เข้ามาเยี่ยมชมเว็บ ผู้ใช้งานซึ่งแสดงออกถึงสนใจมากที่สุดต่อกิจกรรมของกลุ่มหรือมีความเหมาะสมที่สุดต่อการดำเนินการของกลุ่มจะได้รับการติดต่อ ซึ่งส่วนใหญ่เป้าหมายที่ถูกเลือกจะเป็นคนหนุ่มสาว นอกจากนั้นยังมีข้อมูลที่ได้รับการเปิดเผย ว่ามีการใช้อินเตอร์เน็ตเป็นสื่อกลางในการโฆษณาตัวเองต่อกลุ่มก่อการร้าย เช่นกรณีของนักศึกษา Ziyad

---

๗๖ (Online).Available:http://www.hizbuttahrir.org/

๗๗ Attorney General John Ashcroft, "Prepared Remarks re: Holy Land Foundation Indictment. United States Department of Justice", Available:http (Online).://www.justice.gov/ archive/ag/ 2004/72704ag.htm, 2014

Khalil นักศึกษาชาวอียิปต์ซึ่งศึกษาอยู่ในคณะวิทยาการคอมพิวเตอร์ ณ มหาวิทยาลัย โคลัมเบีย รัฐมิสซูรี สหรัฐอเมริกา ได้ใช้อินเตอร์เน็ตเป็นสื่อในการนำเสนอตัวเองต่อกลุ่มก่อการร้าย ด้วยการจัดตั้งเว็บไซต์สนับสนุนกลุ่มฮามาส[๗๘] กิจกรรมที่เขาทำหลายอย่างผ่านระบบอินเตอร์เน็ตทำให้เขาเป็นที่สนใจของ บินลาเดนและพรรคพวก ต่อมา Khalil ได้กลายมาเป็นตัวแทนของอัลเคด้าในสหรัฐอเมริกา ทำหน้าที่ในการจัดซื้อโทรศัพท์ดาวเทียม คอมพิวเตอร์และระบบอิเล็กโทรนิกส์ในการติดต่อสื่อสาร เพื่อช่วยให้บินลาเดนสามารถติดต่อสื่อสารกับผู้สนับสนุนและลูกน้องของเขาได้ อย่างไรก็ตามโดยปกติแล้วกลุ่มก่อการร้ายจะเข้าถึงเป้าหมายที่ต้องการมากกว่าที่จะให้เป้าหมายนำเสนอตัวเอง

๖. เครือข่ายเชื่อมโยงถึงกัน

ปัจจุบันกลุ่มก่อการร้ายฮามาส และอัลเคด้า ได้ใช้อินเตอร์เน็ตเป็นสื่อกลางในการเชื่อมความสัมพันธ์และการสั่งการ และขยายการติดต่อสมาชิกกลุ่มก่อการร้ายอื่นๆ ในอนาคตกลุ่มก่อการร้ายมีแนวโน้มที่จะกระจายอำนาจในการควบคุมและสั่งการมากขึ้น โดยระบบสายสัมพันธ์ของกลุ่มก่อการร้ายผ่านระบบอินเตอร์เน็ต ซึ่งการติดต่อและการประสานงานจะกระจายเป็นไปในทิศทางระดับมากกว่าทางดิ่ง

เหตุผลที่เทคโนโลยีสื่อสารสมัยใหม่ โดยเฉพาะอย่างยิ่งอินเตอร์เน็ต สามารถเอื้อประโยชน์อย่างมากต่อกลุ่มก่อการร้ายในการจัดตั้งและดำรงสภาพของเครือข่ายเนื่องจาก ประการแรกเทคโนโลยีช่วยลดเวลาในการติดต่อสื่อสาร ทำให้สามารถติดต่อถึงกันได้อย่างเสรีและประสานงานกันอย่างมีประสิทธิภาพ ประการที่สองเทคโนโลยีมีบทบาทสำคัญในการลดค่าใช้จ่ายของการติดต่อสื่อสาร และประการที่สามการบูรณาการคอมพิวเตอร์เข้ากับการติดต่อสื่อสารส่งผลให้สามารถเพิ่มรูปแบบของการสื่อสารที่หลากหลายของข้อมูลที่สามารถแลกเปลี่ยนกันได้

อินเตอร์เน็ตไม่เพียงแต่เป็นเครื่องมือในการติดต่อระหว่างสมาชิกของกลุ่มเท่านั้น แต่ยังรวมถึงระหว่างสมาชิกของกลุ่มก่อการร้ายทั่วโลกด้วย เช่น เว็บไซต์จำนวนมากซึ่งสนับสนุนการก่อการร้ายในนามของจีฮัด โดยเว็บไซต์เหล่านี้รวมทั้งชุมชนออนไลน์ อนุญาตให้กลุ่มก่อการร้ายต่างๆทั่วโลกเช่น ปาเลสไตน์ อินโดนีเซีย อัฟกานิสถาน ตุรกี อีรัก มาเลเซีย ฟิลิปปินส์ และเลบานอน แลกเปลี่ยนข้อมูลข่าวสาร เช่นการผลิตระเบิด การชักจูงสมาชิกใหม่ และการปฏิบัติการโจมตี เป็นต้น

---

๗๘ Steven Emerson, "American Jihad: The Terrorists Living Among Us", The Free Press, New York, U.S.A., พ.ศ.๒๕๔๕

๗. แลกเปลี่ยนข้อมูลข่าวสาร

โลกของอินเตอร์เน็ตเปรียบเสมือนแหล่งรวมของของเว็บไซต์จำนวนมหาศาล ที่มีข้อมูลเกี่ยวกับการผลิตสารเคมี การผลิตวัตถุระเบิด เว็บไซต์หลายแห่งมีข้อมูล The Terrorist's Handbook[๗๙] และ The Anarchist Cookbook คู่มือสองเล่มนี้เป็นที่รู้จักกันดีว่าให้ข้อมูลและรายละเอียดในการผลิตระเบิดชนิดต่างๆ และอีกหนึ่งคู่มือคือ The Mujahadeen Poisons Handbook[๘๐] ซึ่งเขียนโดย The Mujahadeen Poisons Handbook ถูกนำเสนอบนเว็บไซต์ของกลุ่มฮามาส ให้ข้อมูลเกี่ยวกับการจัดเตรียมสารพิษ กาซพิษ และสารพิษอันตรายอื่นๆสำหรับใช้ในการโจมตี นอกจากนั้นยังมีคู่มืออีกหนึ่งเล่มที่มีชื่อเรียกว่า "The Encyclopedia of Jihad and prepared by al Qaeda" [๘๑] มีจำนวนมากกว่าหนึ่งพันหน้า นำเสนอข้อมูลผ่านเว็บไซต์ ให้ข้อมูลวิธีการปฏิบัติการเครือข่ายใต้ดิน รวมทั้งการปฏิบัติการโจมตีต่อเป้าหมาย

๘. การวางแผนและการประสานงาน

กลุ่มก่อการร้ายไม่เพียงแต่ใช้อินเตอร์เน็ตเป็นสถานที่ในการเรียนรู้วิธีการผลิตวัตถุระเบิดเพียงอย่างเดียวเท่านั้นแต่ยังรวมถึงการวางแผนและประสานความร่วมมือในการโจมตีเป้าหมายด้วย การปฏิบัติการของกลุ่มอัลเคด้าต้องพึ่งพาอินเตอร์เน็ตอย่างมากในการวางแผนและประสานงานในการโจมตีเมื่อ 9/11 เจ้าหน้าที่ FBI ของสหรัฐอเมริกา ตรวจพบข้อมูลนับพันซึ่งมีการเข้ารหัสป้องกันอย่างดีบนเว็บไซต์ของกลุ่มก่อการร้ายรวมทั้งในคอมพิวเตอร์ของ Abu Zubaydah ผู้ถูกกล่าวหาว่าอยู่เบื้องหลังเหตุการณ์โจมตี เมื่อ ๑๑ ก.ย. ข้อความแรกตรวจพบในคอมพิวเตอร์ถูกส่งออกไปเมื่อ พ.ค.๔๔ และส่งครั้งสุดท้ายเมื่อ ๘ ก.ย.๔๔ ความถี่ของข้อความสูงสุดในเดือน ส.ค. ๔๔ และเพื่อปกปิดตัวเอง กลุ่มก่อการร้ายใช้อินเตอร์เน็ตของสาธารณะ ในการส่งข่าวสารผ่านระบบอินเตอร์เน็ต [๘๒]

---

๗๙ (Online).Available:http://www.capricorn.org/~akira/home/terror.html (Online).Available:http://bnrg.cs.berkeley.edu/~randy/Courses/CS39K.S13/anarchistcookbook2000.pdf

๘๐ (Online).Available:http://dead-planet.net/chemicalterrorism/pdfs/Mujahideen_Poisons

๘๑ (Online).Available:http:// digitalcommons.liberty.edu/cgi/ viewcontent.cgi?article= 1023&context=gov_fac_pubs

๘๒ Rupert Cornwell, "The secret diary of Abu Zubaydah, from student to hardline jihadi and CIA torture",.(Online).Available:http://www.independent.co.uk/news/world/middle-east/the-secret-diary-of-abu-zubaydah-from-student-to-hardline-jihadi-and-cia-torture-8929831.html, 2013

แฮกเกอร์ ขุนพลในศตวรรษที่ ๒๑

เนื่องจากเทคโนโลยีสารสนเทศเป็นเทคโนโลยีใหม่ และต้องใช้ความรู้เฉพาะทางที่สูง การเจาะระบบหรือโจมตีระบบจึงต้องใช้ผู้ที่มีความรู้และความเชี่ยวชาญด้านความมั่นคงปลอดภัยทางสารสนเทศที่สูงด้วยเช่นกัน ผู้เชี่ยวชาญดังกล่าวมักรู้จักกันภายใต้ชื่อเรียก "แฮกเกอร์" และมักถูกมองในฐานะบุคคลลึกลับ และมีภารกิจหรือเป้าหมายในทางทำลายมากกว่าทางสร้างสรรค์ ทั้งนี้แฮกเกอร์เป็นกลุ่มผู้เชี่ยวชาญที่มีประวัติศาสตร์ยาวนานเทียบเท่ากับเทคโนโลยีสารสนเทศ และไม่ได้ถูกมองในด้านลบเสมอไป

แฮกเกอร์ในความหมายแรกเริ่มที่ถูกใช้ใน MIT Artificial Intelligence Laboratory[๘๓] ช่วงทศวรรษ ๑๙๖๐ คือ กลุ่มคนที่สามารถทำให้ซอฟท์แวร์ทำงานบางอย่างได้ มากกว่าที่ซอฟท์แวร์นั้น ๆ ถูกออกแบบเอาไว้[๘๔ ๘๕] ซึ่งเป็นความหมายในเชิงบวกมากกว่าเชิงลบ ในช่วงทศวรรษ ๑๙๗๐ แฮกเกอร์ที่ถูกกล่าวถึงมากที่สุดคนหนึ่งคือ John Drape ที่สามารถเจาะเข้าระบบโทรศัพท์สาธารณะและสามารถใช้งานโทรศัพท์ทางไกลได้โดยไม่ต้องเสียค่าใช้จ่าย [๘๖] ทั้งนี้ในชุมชนแฮกเกอร์ได้มีข้อถกเถียงเกิดขึ้นว่า การกระทำของ John Drape นั้นถือเป็นการกระทำของ "แฮกเกอร์" หรือไม่ เนื่องจากดังที่เคยปรากฏว่า กลุ่มแฮกเกอร์ในสมัยนั้นร่วมกันออกหลักการไว้ยึดถือปฏิบัติ เรียกว่า "จรรยาบรรณของแฮกเกอร์" ซึ่งประกอบด้วย

๑. หนทางเข้าสู่คอมพิวเตอร์ หรืออะไรก็ตามที่สามารถเป็นสื่อแสดงความเป็นไปของโลก ไม่ควรมีขอบเขต หรือข้อจำกัดใด ๆ ในการเข้าถึง

๒. ข้อมูลความรู้เป็นของสาธารณะที่ทุกคนสามารถเข้าถึงได้

๓. จงอย่าไว้วางใจผู้มีอำนาจ และต้องส่งเสริมการกระจายอำนาจ

๔. จงตัดสินแฮกเกอร์จากการกระทำและความสามารถของเขา ไม่ใช่ที่รูปร่าง หน้าตา วัยวุฒิ เชื้อชาติ เพศ หรือสถานะทางสังคมอื่นใด

๕. ทุกคนล้วนมีสิทธิในการสร้างสรรค์งานศิลปะ และความงามด้วยคอมพิวเตอร์

---

๘๓ (Online).Available:http://www.csail.mit.edu/

๘๔ Richard Stallman, "On Hacking", https://stallman.org/articles/on-hacking.html

๘๕ Robert Trigaux, "A history of hacking", หนังสือพิมพ์ St. Petersberg Time, (Online).Available:http://www.sptimes.com/Hackers/history.hacking.html

๘๖ John Markoff, "The Odyssey Of a Hacker: From Outlaw To Consultant", หนังสือพิมพ์ The New York Times, (Online). Available: http://www.nytimes.Com /2001/01/29/ business/the-odyssey-of-a-hacker-from-outlaw-to-consultant.html, 2001

๖. คอมพิวเตอร์สามารถเปลี่ยนแปลงชีวิตให้ดีขึ้นได้

๗. ไม่รื้อค้นข้อมูลของผู้อื่น

๘. จงใช้ข้อมูลสาธารณะ ในขณะที่ต้องคุ้มครองข้อมูลส่วนบุคคล [๘๗]

กลุ่มแฮกเกอร์กลุ่มหนึ่งที่ได้รับการยอมรับในวงกว้างยุคหลังทศวรรษ ๑๙๘๐ เป็นต้นมา และเป็นส่วนหนึ่งของการผลักดันจรรยาบรรณของแฮกเกอร์คือกลุ่มแฮกเกอร์ในโครงการโอเพนซอร์ส ต่าง ๆ [๘๘] โดยเฉพาะโครงการที่อยู่ในความดูแลของ GNU [๘๙] ซึ่งมี Richard Stallman [๙๐] เป็นผู้ก่อตั้งและผู้นำทางความคิดของโครงการ Stallman ได้รับการยอมรับในวงการพัฒนาซอฟท์แวร์ทั้งในโลกซอฟท์แวร์โอเพนซอร์สและโลกซอฟท์แวร์พาณิชย์ ในฐานะผู้ออกแบบ และพัฒนาซอฟท์แวร์ที่ริเริ่มพัฒนาซอฟท์แวร์สำคัญเช่น GCC [๙๑] และ Emacs [๙๒] ในฐานะนักกิจกรรมและนักเคลื่อนไหวทางสังคมที่ผลักดันสัญญาอนุญาตแบบ GPL [๙๓] ที่มีนัยยะของการสนับสนุนเสรีภาพผ่านซอฟท์แวร์ และที่สำคัญในฐานะแฮกเกอร์ ที่มีฝีมือหาตัวจับได้ยาก และคอยสอดส่องดูแลคุณภาพด้านความปลอดภัยของซอฟท์แวร์โอเพนซอร์สในโครงการต่าง ๆ

---

๘๗ ดู URL (Online).Available:http://www.ccc.de/hackerethics (25.10.09).

๘๘ โครงการโอเพนซอร์ส (Open Source Software Project) คือ วิธีการในการออกแบบ พัฒนา และแจกจ่ายสำหรับต้นฉบับของสินค้าหรือความรู้ โดยเฉพาะซอฟต์แวร์ โดยโอเพนซอร์ซถูกพิจารณาว่าเป็นทั้งรูปแบบหนึ่งในการออกแบบ และแผนการในการดำเนินการ โดยโอเพนซอร์ซเปิดโอกาสให้บุคคลอื่นนำเอาระบบนั้นไปพัฒนาได้ต่อไป

๘๙ GNU (htttp://www.gnu.org/) เป็นชื่อของโครงการพัฒนาระบบปฏิบัติการ ริเริ่มโดยริชาร์ด สตอลแมน เมื่อปี พ.ศ. ๑๙๘๔

๙๐ (Online).Available:https://stallman.org/

๙๑ GCC เป็นชุดโปรแกรมแปลโปรแกรมสำหรับแปลภาษาโปรแกรมต่าง ๆ พัฒนาโดยโครงการกนู (GNU) และแจกจ่ายเป็นซอฟต์แวร์เสรีภายใต้สัญญาอนุญาตแบบ GPL และ LGPL

๙๒ Emacs เป็นโปรแกรมคอมพิวเตอร์ที่ใช้แก้ไขข้อความ มีความสามารถหลากหลายเป็นที่นิยมในหมู่นักเขียนโปรแกรมคอมพิวเตอร์

๙๓ GPL (GNU General Public License, GNU GPL, GPL) เป็นสัญญาอนุญาตสำหรับซอฟต์แวร์เสรี ที่ได้รับความนิยมสูงที่สุดในปัจจุบัน ฉบับแรกสุดเขียนโดย ริชาร์ด สตอลล์แมน เริ่มต้นใช้กับโครงการกนู ในปี พ.ศ. ๒๕๓๔ (ค.ศ. 1991). สัญญาอนุญาตจีพีแอลในปัจจุบันเป็นรุ่นที่ ๓ นอกจากนี้มีสัญญาอนุญาตสาธารณะทั่วไปแบบผ่อนปรนของกนู หรือ แอลจีพีแอล (GNU Lesser General Public License, LGPL) ที่พัฒนาแยกออกมาจากจีพีแอลเพื่อใช้สำหรับไลบรารีซอฟต์แวร์

เมื่อพิจารณาจากจรรยาบรรณแฮกเกอร์แล้ว จะเห็นได้ว่าแฮกเกอร์ในความเข้าใจของคนโดยทั่วไป ไม่ได้หมายถึงกลุ่มคนที่เรียกตนเองว่าแฮกเกอร์ แต่กลับหมายถึงกลุ่ม "แครกเกอร์" [๖๔] หรือกลุ่มคนที่มีความสามารถเช่นเดียวกับแฮกเกอร์ แต่เน้นการทำกิจกรรมที่มีผลเสียต่อระบบคอมพิวเตอร์ หรือการกระทำที่เพื่อหวังผลประโยชน์ในทางมิชอบอย่างใดอย่างหนึ่ง ในส่วนอื่น ๆ ของเอกสารวิจัยฉบับนี้จะใช้คำว่า "แฮกเกอร์" ในความหมายของ "แครกเกอร์"

แน่นอนว่าในเหตุการณ์ทางสงครามไซเบอร์ทุกเหตุการณ์ที่เกิดขึ้น ย่อมมีแฮกเกอร์มาเกี่ยวข้องทั้งในฐานะผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศ และในฐานะผู้ปฏิบัติการโดยแฮกเกอร์ถือเป็นองค์ประกอบที่ชี้ขาดความสำเร็จหรือความล้มเหลวของการรักษาความมั่นคงปลอดภัยทางสารสนเทศ ฝ่ายที่มีแฮกเกอร์ที่มีความเชี่ยวชาญ มีความรู้ความสามารถ ย่อมมีความได้เปรียบในการปฏิบัติการในทางการป้องกันภัยคุกคามทางเทคโนโลยีสารสนเทศเองก็ต้องอาศัยแฮกเกอร์ในการให้คำแนะนำในการออกแบบและพัฒนาระบบที่สามารถป้องกันการโจมตีทางไซเบอร์ได้ ดังนั้นความมั่นคงปลอดภัยทางสารสนเทศ แฮกเกอร์จึงเปรียบได้กับ "ขุนพล" ที่เป็นผู้กำหนดชะตากรรม

ดังนั้นแฮกเกอร์จึงกลายเป็นกลุ่มคนที่เป็นที่ต้องการของหน่วยงานทางมั่นคงทางสารสนเทศในประเทศต่าง ๆ ทั้งนี้ การสร้างแฮกเกอร์ไม่สามารถสร้างได้จากระบบการศึกษาปกติด้วยข้อจำกัดสำคัญอย่างน้อย ๓ ประการคือ

๑ . ข้อจำกัดทางกฎหมาย กฎหมายในหลายประเทศรวมถึงประเทศไทย [๖๕] ถือว่าการกระทำหลายอย่างของของแฮกเกอร์เป็นการกระทำความผิดทางกฎหมายที่มีโทษทางอาญา ดังนั้นการสร้างหรือฝึกฝนแฮกเกอร์จึงมีความเสี่ยงที่จะถูกลงโทษทางกฎหมาย

๒. ข้อจำกัดด้านระบบการศึกษาและการเข้าถึงข้อมูล ระบบการศึกษาตามปกติต้องมีการกำหนดหลักสูตรที่ชัดเจนแน่นอน ทำให้กระบวนการเปลี่ยนแปลงเนื้อหาในหลักสูตรมีกระบวนการ และใช้ระยะเวลาที่ยาวนาน ซึ่งแตกต่างจากความรู้ที่จำเป็นสำหรับแฮกเกอร์มีการเปลี่ยนแปลงตลอดเวลา ทำให้ระบบการศึกษาตามปกติไม่สามารถให้ความรู้ที่จำเป็นสำหรับแฮกเกอร์ได้ กระทั่งหนังสือหรือสื่อการเรียนการสอนเองก็ไม่สามารถตามความเปลี่ยนแปลงดังกล่าวได้ ผนวกกับข้อจำกัดทางด้านกฎหมายทำให้การเข้าถึงองค์ความรู้ที่จำเป็นสำหรับแฮกเกอร์จึงกลายเป็นเฉพาะทางที่มีความลึกลับในตัวเอง

---

๖๔ Cracker

๖๕ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ มาตรา ๕-๑๑

๓. ข้อจำกัดด้านระบบ การจำลองระบบเพื่อใช้ทดลองในการโจมตี หรือป้องกันการโจมตีเป็นเรื่องที่แทบเป็นไปไม่ได้ เพราะการจำลองระบบในลักษณะดังกล่าวต้องใช้ทรัพยากรที่มากพอกับระบบจริง อีกทั้งการทดลองในระบบจริงก็อาจสร้างความเสียหายในระบบได้ ดังนั้น การหาพื้นที่ในการเรียนรู้หรือทดลองความรู้สำหรับแฮกเกอร์จึงเป็นเรื่องที่ยุ่งยาก

เนื่องจากแฮกเกอร์ไม่สามารถสร้างจากระบบการศึกษาปกติ และมีคุณค่าทางยุทธการที่สูง ทำให้แฮกเกอร์กลายเป็นที่ต้องการของหน่วยงานทางความมั่นคงปลอดภัยทางสารสนเทศเป็นอย่างมาก หลายประเทศมีความพยายามที่จะสร้างแฮกเกอร์เพื่อใช้งานทางการทหารอย่างลับ ๆ เช่น เกาหลีเหนือ และ จีน[๙๖] เป็นต้น และมีความพยายามใช้แฮกเกอร์ที่เป็นอาชญากรคอมพิวเตอร์มาปฏิบัติการทางการทหาร จึงทำให้ไม่สามารถโยงการกระทำของแฮกเกอร์เหล่านั้นกลับไปยังหน่วยงานประเทศใดได้

การกำหนดแนวทางการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศไทยในอนาคต แฮกเกอร์ถือเป็นปัจจัยสำคัญปัจจัยหนึ่งที่ต้องคำนึงถึง ทั้งในด้านการสร้างบุคคลากร การสร้างสภาพแวดล้อมให้เอื้ออำนวยในการศึกษาหาความรู้ใหม่ ๆ การออกแบบโครงสร้างองค์กรให้เหมาะสมกับการปฏิบัติงานของแฮกเกอร์

อาชญากรรมคอมพิวเตอร์ การกระทำความผิดในพื้นที่เศรษฐกิจเปิดกว้าง

คงไม่อาจปฏิเสธได้ว่า อาชญากรรมเศรษฐกิจ อาชญากรรมคอมพิวเตอร์ เรื่อยมาจนถึงอาชญากรรมไซเบอร์ หรืออาชญากรรมอินเตอร์เน็ต เหล่านี้ล้วนแล้วแต่เป็นผลพวงด้านลบที่เกิดขึ้นพัฒนา และขยายตัวมาพร้อม ๆ กับวิวัฒนาการ และความก้าวหน้าทางเทคโนโลยีในยุคข้อมูลข่าวสาร นวัตกรรมใหม่อย่างคอมพิวเตอร์ และการเชื่อมต่อระหว่างกันจนเกิดเป็นเครือข่ายขนาดเล็กและใหญ่ในช่วงปลายทศวรรษที่ ๑๙๖๐ ด้านหนึ่งถูกใช้เป็น "เครื่องมือ" ในการกระทำความผิด ในขณะที่อีกด้านหนึ่งเป็น "เป้าหมายแห่งการกระทำความผิด" ในฐานะที่เป็นอุปกรณ์ หรือช่องทางสำคัญในการเก็บรักษา และ/หรือ รับ-ส่ง "ข้อมูลข่าวสาร" สิ่งที่ในปัจจุบันดูจะเป็นทรัพย์สินที่มีค่ายิ่งกว่าทรัพย์ที่มีรูปร่างบางชนิด เช่น รถยนต์ หรือโทรศัพท์เคลื่อนที่ เสียอีก

ในบทนี้จะกล่าวถึง วิวัฒนาการของ อาชญากรรมคอมพิวเตอร์ (Computer Crime) จากอดีตเรื่อยมาจนถึงยุคของ อาชญากรรมเครือข่าย (Cyber Crime) อาชญากรรมออนไลน์ (Online Crime) หรือที่รู้จักกันในชื่อว่า อาชญากรรมอินเตอร์เน็ต (Internet Crime) ในช่วงหลายปีที่ผ่านมาได้กลายเป็นปัญหาสำคัญของหลายประเทศที่จะหาวิธีป้องกันและปราบปราม ทั้งนี้เพื่อให้ทราบถึง ที่มาและเห็นลำดับการพัฒนาเปลี่ยนแปลงเป้าหมายแห่งการกระทำความผิดจาก "นิติสมบัติ" หรือ

---

๙๖ Richard A. Clark และ Robert Knake, “Cyber War: The Next Threat to National Security and What to Do About It”, pp 50-56, 10 เม.ย. 2555, Ecco, USA

"สิ่งที่กฎหมายประสงค์จะคุ้มครอง" สิ่งหนึ่งไปสู่อีกสิ่งหนึ่ง ซึ่งเหล่านี้ล้วนเกิดขึ้นในช่วงระยะเวลาเพียงไม่กี่สิบปีเท่านั้น นอกจากนั้นบทความนี้ยังน่าจะเป็นประโยชน์ ต่อการวิเคราะห์เพื่อหาแนวโน้มของรูปแบบการกระทำความผิด และขอบเขตความเสียหายอื่น ๆ ที่อาจขยายตัวต่อไปตามวิวัฒนาการทางเทคโนโลยีในอนาคตด้วย

๑. การกระทำความผิดต่อ "สิทธิความเป็นส่วนตัว และข้อมูลส่วนบุคคล"

แม้จะมีความพยายามมานาน แต่จนถึงปัจจุบันนิยามของคำว่า "อาชญากรรมคอมพิวเตอร์" ที่ชัดเจน ครอบคลุม และเป็นเอกภาพอันเป็นที่ยอมรับกันในทางระหว่างประเทศก็ยังไม่ปรากฏ คำนิยามต่างๆที่ถูกให้ไว้ ยังคงขึ้นอยู่กับมุมมองของนักกฎหมายในแต่ละสาขา และแต่ละประเทศ อย่างไรก็ตามถ้ากล่าวถึงความหมายโดยทั่วไปที่ทำให้คนในสังคมเริ่มเข้าใจ และตระหนักถึงความเสียหายที่เกิดขึ้นจากอาชญากรรมประเภทนี้แล้ว ความหมายโดยนัยดังกล่าวเริ่มขึ้นเมื่อไม่กี่สิบปีที่ผ่านมา อันเป็นช่วงระยะเวลาที่ข้อมูลส่วนตัวของผู้คนจำนวนหนึ่งถูกบันทึก ควบคุม หรือตกอยู่ภายใต้ระบบการทำงานของเทคโนโลยีคอมพิวเตอร์

ช่วงปี ค.ศ. ๑๙๖๐ - ๑๙๗๐ นับเป็นช่วงเวลาแรก ๆ ที่เริ่มมีการชี้ให้เห็นถึงภยันตรายที่เกิดขึ้นจากเทคโนโลยีคอมพิวเตอร์[๙๗] เพราะในสมัยนั้น หลายประเทศในแถบตะวันตกใช้คอมพิวเตอร์เป็นอุปกรณ์ในการเก็บบันทึก ถ่ายทอด และเชื่อมโยงฐานข้อมูลส่วนบุคคลของประชาชนในรัฐเข้าด้วยกัน และด้วยเหตุที่มีการนำข้อมูลดังกล่าวรวบรวมไว้ภายใต้การจัดการของรัฐนี้เอง นักวิชาการจำนวนหนึ่งจึงเริ่มมองเห็นปัญหา และลงมืออภิปรายถกเถียงกันถึงประเด็นที่ว่าประชาชนอาจถูกตรวจสอบ เฝ้ามอง หรือถูกควบคุมจากรัฐได้โดยง่าย โดยข้อสังเกตส่วนใหญ่ได้รับอิทธิพลมาจาก "1984" ของ George Orwell [๙๘] นิยายการเมืองการปกครอง ที่มีเนื้อหาส่วนหนึ่งกล่าวถึงพัฒนาการทางเทคโนโลยี และพลังอำนาจใหม่ของรัฐชาติ ประเด็นสำคัญ ก็คือ แม้ในช่วงเวลาเริ่มต้น กระบวนทัศน์ ของมนุษย์ที่มีต่อคอมพิวเตอร์จะเป็นไปในเชิงบวก กล่าวคือ เป็นอุปกรณ์หรือเครื่องมือทรงพลังที่มีประโยชน์อย่างยิ่งต่อระบบการจัดการข้อมูลข่าวสารทำให้การทำงานต่าง ๆ ของมนุษย์สะดวก และรวดเร็วขึ้น แต่ในอนาคตกระบวนทัศน์นี้จะเปลี่ยนแปลงไป เพราะลักษณะการใช้เทคโนโลยีคอมพิวเตอร์ โดยเฉพาะอย่างยิ่งโดยรัฐจะเริ่มล่วงล้ำสิทธิ และเกินขอบเขตความเป็นส่วนตัวของประชาชนมากขึ้นเรื่อย ๆ ถึงกระทั่งมันอาจถูกใช้เป็นเครื่องมือควบคุมตรวจสอบพฤติกรรมพลเมืองโดยผู้ปกครองรัฐ (Big Brother)

---

๙๗ Ulrich Sieber, “Computerkriminalität und Informationsstrafrecht. Entwicklungen in der internationalen Informations- und Risikogesellschaft“, CR 1995, p. 101.

๙๘ อ่าน 1984 ภาษาอังกฤษ ออนไลน์ได้ที่ URL: (Online).Available:http://www.george-orwell.org/1984 (19.10.09).

ความเข้าใจที่มีต่อการกระทำความผิดโดยมีคอมพิวเตอร์เข้าไปเกี่ยวข้องในยุคแรก ๆ จึงยังไม่ได้มีความหมายทำนองเดียวกับ "อาชญากรรมคอมพิวเตอร์" ที่เข้าใจกันอยู่ในปัจจุบัน (อาทิ เจาะระบบ เผยแพร่โปรแกรมทำลาย หรือ เผยแพร่เนื้อหาที่เป็นความผิดกฎหมาย) แต่หมายถึง การกระทำความผิดใดๆ ที่เป็นอันตรายต่อข้อมูลข่าวสาร ซึ่งมีผลกระทบต่อระดับความลับ หรือความเป็นส่วนตัวของมนุษย์ ดังนั้น สิ่งสำคัญที่คนให้ความสนใจ และเรียกร้องให้รัฐให้ความคุ้มครองเป็นพิเศษในช่วงเวลานั้นก็คือ "ข้อมูลความลับ และข้อมูลส่วนบุคคล" โดยเฉพาะอย่างยิ่ง ความลับในทางวิชาชีพต่างๆ อาทิข้อมูลทางการแพทย์ ข้อมูลทางการเงินการธนาคาร หรือข้อมูลทางด้านคดีความ เป็นต้น "กฎหมายคุ้มครองข้อมูลส่วนบุคคล" จึงเป็นกฎหมายที่เกี่ยวข้องกับเรื่องนี้ในยุคแรกที่หลายประเทศต้องผลักดันออกมาก่อน มิใช่กฎหมายที่กำหนดฐานความผิดใหม่ เพื่อป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ อย่างที่เข้าใจอยู่ในปัจจุบัน [๙๙]

อนึ่ง การกระทำความผิดต่อข้อมูลดังกล่าวมักมีระดับของภยันตรายที่แตกต่างกันไป ขึ้นอยู่กับว่าข้อมูลที่ถูกละเมิดนั้นเป็นของใคร หรือหน่วยงานใด เช่น การจารกรรมข้อมูลข่าวสารที่เกี่ยวกับระบบความปลอดภัยของรัฐ ย่อมอันตรายกว่าการขโมยข้อมูลส่วนบุคคลบางอย่างเพื่อผู้กระทำความผิดจะนำไปใช้ข่มขู่ หรือเรียกร้องเงิน หรือผลประโยชน์อื่นใดจากเจ้าของข้อมูล คดีสำคัญ ๆ ในอดีตเกี่ยวกับการกระทำความผิดต่อข้อมูล เช่น การขโมยข้อมูลการรักษาผู้ป่วยโรคเอดส์ในประเทศแอฟริกาใต้ ซึ่งต่อมาข้อมูลนั้น ถูกส่งต่อไปยังผู้จ้างงานของผู้ป่วยจนเขาได้รับเสียหาย[๑๐๐] คดีที่บริษัท IBM ถูกฟ้องร้องเมื่อปี 1986 ว่าระบบความปลอดภัย (RACF)[๑๐๑] อาจโดนพนักงานของบริษัทตรวจสอบโดยเจ้าของไม่อนุญาต หรือ คดีจารกรรมข้อมูลทางการทหารของสหรัฐอเมริกาไปขายให้หน่วยสืบราชการลับของสหภาพโซเวียต (KGB-Case)[๑๐๒] เป็นต้น

---

๙๙ แม้จะเป็นหนึ่งในกฎหมาย **6** ฉบับในโครงการกฎหมายที่เกี่ยวกับเทคโนโลยี ปี 2000 [ดู Nectec, Dokument IT - 2000 project, URL (Online).Available:http://www.nectec.or.th/it-projects/ (19.10.09)] แต่จนถึงปัจจุบัน "กฎหมายคุ้มครองข้อมูลส่วนบุคคล" ในประเทศไทย ยังมีสถานะเป็นเพียงร่างกฎหมาย เท่านั้น

๑๐๐ ดูคดีนี้ใน Hugo van der Merwe, in: Ulrich Sieber, “International Technology Crime“, 1994, p. 423.

๑๐๑ ดูคดีนี้ใน Ulrich Sieber, “The International Handbook on Computer Crime”, 1986, p. 23.

๑๐๒ ดูคดีนี้ใน Wolfgang Bär, “Der Zugriff auf Computerdaten im Strafverfahren“, Köln/Berlin/ Bonn/München, 1992, p. 37.

๒. อาชญากรรมเศรษฐกิจ

แม้ในปัจจุบัน อาชญากรรมคอมพิวเตอร์ที่เกิดขึ้นในหลายๆกรณีเป็นความผิดในกลุ่มอื่นใด ที่อาจมีผลกระทบต่อชีวิตร่างกาย ระบบรักษาความปลอดภัย หรือเป็นภยันตรายต่อสังคมโดยรวม ซึ่งไม่ได้เกี่ยวพันกับปัญหาในทางเศรษฐกิจเลยก็ตาม แต่ในยุคสมัยหนึ่ง การกระทำความผิดที่มีคอมพิวเตอร์เข้าไปเกี่ยวข้องนี้ถูกกำหนดให้เป็นส่วนหนึ่งของ "อาชญากรรมทางเศรษฐกิจ" หรือ ที่บางคนรู้จักในนาม "White Collar Crimes" อาชญากรรมเชิ้ตขาว หรืออาชญากรรมเสื้อคอปก ที่ผู้กระทำความผิดเป็นกลุ่มคนทำงานดี แต่งตัวดี หรือมีความรู้ความสามารถ ความหมายของ อาชญากรรมทางเศรษฐกิจนั้นกินความกว้าง ครอบคลุมความผิดหลายฐาน เป็นการกระทำที่สร้างความเสียหาย ทั้งแก่เศรษฐกิจของปัจเจกชน ประเทศชาติ สังคมส่วนรวม และมีผลในการทำลายความเชื่อถือ และความมั่นคงทางเศรษฐกิจ ตัวอย่างอาชญากรรมเศรษฐกิจ เช่น ความผิดเกี่ยวกับการปลอมแปลงเงินตรา การปั่นหุ้น ความผิดเกี่ยวกับภาษีอากร ธุรกิจต่าง ๆ สถาบันการเงิน เกี่ยวกับการค้า หรือธุรกิจเงินนอกระบบ เป็นต้น

หลังจากปีค.ศ. ๑๙๖๙ ที่เทคโนโลยีอินเตอร์เน็ตเกิดขึ้นครั้งแรก นอกจากอินเตอร์เน็ตจะกลายเป็นส่วนสำคัญในการทำงานในหน่วยงานของรัฐแล้ว ผู้ประกอบธุรกิจรายใหญ่ ๆ ก็หันมาใช้ประโยชน์จากคอมพิวเตอร์ และอินเตอร์เน็ตด้วยเช่นกัน เพราะสามารถแลกเปลี่ยนข้อมูลข่าวสารระหว่างผู้ประกอบธุรกิจด้วยกันเองได้สะดวกและรวดเร็ว อย่างไรก็ตามในอีกด้านหนึ่งสิ่งนี้ก็กลายเป็นข้อดีให้กับผู้กระทำความผิดที่ต้องการจารกรรม หรือลักลอบทำซ้ำข้อมูล ไปใช้ประโยชน์ทางธุรกิจของตน หรือสร้างความเสียหายทางด้านการเงินต่อธุรกิจของผู้อื่น จากที่สมัยเดิม "อาชญากรรมเศรษฐกิจ" ไม่ได้มีเครื่องมือพิเศษเพื่อเพิ่มศักยภาพในการกระทำความผิด และมักเป็นแค่เพียงการปลอมแปลง หรือการกระทำต่อเอกสารบัญชีการเงินการธนาคาร และเอกสารอื่น ๆ อาชญากรรมเศรษฐกิจในยุคคอมพิวเตอร์ และอินเตอร์เน็ตที่ขยายขอบเขตไปสู่ความเสียหายต่อเศรษฐกิจในด้านอื่น ๆ ด้วย ก็เริ่มปรากฏตัวขึ้น

ช่วงปี ค.ศ. ๑๙๗๐ - ๑๙๘๐ การอภิปรายเพื่อหาทางแก้ปัญหาการกระทำความผิดอันเกี่ยวกับคอมพิวเตอร์ จึงไม่ได้จำกัดขอบเขตอยู่ที่ประเด็นการกระทำความผิดต่อข้อมูลข่าวสารส่วนบุคคล แต่รัฐเริ่มหันมาให้ความสนใจในประเด็นปัญหา "อาชญากรรมทางเศรษฐกิจ" ด้วย [๑๐๓] (ซึ่งจนถึงปัจจุบัน ประเด็นดังกล่าวนี้ ก็ยังคงเป็นปัญหาหลัก ๆ ในขอบเขตของอาชญากรรมคอมพิวเตอร์) ในยุคนี้ที่เริ่มมีความพยายามในการจำแนกอาชญากรรมคอมพิวเตอร์ ออกเป็นสองกลุ่มใหญ่ ๆ คือ กลุ่มความผิดที่ผู้กระทำอาศัยคอมพิวเตอร์เป็น "เครื่องมือ" และ กลุ่มความผิดที่

---

๑๐๓ Ulrich Sieber, CR 1995, อ้างแล้ว, p. 101.

ระบบคอมพิวเตอร์ และข้อมูลที่อยู่ในคอมพิวเตอร์เป็น "เป้าหมาย" ของผู้กระทำความผิด[๑๐๔] ทั้งนี้ ความผิดสำคัญ ๆ ที่เกิดขึ้นบ่อยครั้ง และได้รับความสนใจจากนักกฎหมาย รวมทั้งนักวิชาการด้านอื่น ๆ ได้แก่ การเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ (Computer manipulation), การก่อวินาศกรรมคอมพิวเตอร์ (Computer sabotage) หรือการกรรโชกทางคอมพิวเตอร์, การเข้าไปในระบบคอมพิวเตอร์โดยปราศจากอำนาจ (unauthorized access to information system) และการละเมิดลิขสิทธิ์ซอร์ฟแวร์ รวมทั้งการลักลอบขโมยผลิตภัณฑ์ดิจิตอลอื่น ๆ ที่มีลิขสิทธิ์

๒.๑ การเปลี่ยนหรือปลอมแปลงข้อมูลคอมพิวเตอร์ (Computer manipulation)

ช่วงปี ค.ศ. ๑๙๗๐ - ๑๙๘๐ การกระทำความผิดแบบนี้ จะหมายเฉพาะที่กระทำต่อระบบคอมพิวเตอร์ หรือข้อมูลที่อยู่ในคอมพิวเตอร์ตัวหลัก (Mainframe-Computer) เท่านั้น แต่เนื่องจากในสมัยต่อมา (ช่วงปี ค.ศ. ๑๙๘๐ - ๑๙๙๐) จนถึงปัจจุบัน ระบบคอมพิวเตอร์ได้รับการพัฒนาเพื่อใช้งานร่วมกับเครื่องมืออื่น ๆ ที่มีความหลากหลายมากขึ้น ดังนั้น ประเภทของความผิดที่เกิดจากการกระทำในรูปแบบนี้ จึงถูกจำแนกเพิ่มขึ้นด้วยเช่นกัน

สำหรับการปลอมแปลงข้อมูลคอมพิวเตอร์ดั้งเดิม นั้น เป้าหมายหลักของผู้กระทำความผิดยังคงอยู่ที่ บัญชีด้านการเงินการธนาคารของบริษัท และผู้ประกอบธุรกิจต่าง ๆ อาทิ การเปลี่ยนแปลงหรือบิดเบือนข้อมูลการชำระเงิน การเปลี่ยนแปลงรายรับ-รายจ่ายของบริษัท การเปลี่ยนแปลงงบดุลบัญชีบริษัท การเปลี่ยนแปลงรายการ หรือสถานภาพการเงินของธนาคาร รวมทั้งการเปลี่ยนแปลงระบบ "บัญชีเงินสะสม" ของบริษัทต่าง ๆ โดยคดีสำคัญที่เคยเกิดขึ้น เช่น คดีในประเทศเยอรมนี ปี พ.ศ. ๒๕๑๗ โปรแกรมเมอร์ของบริษัทแห่งหนึ่งทำการตกแต่งบัญชี และบิดเบือนรายรับของบริษัท ยักยอกเงินไปได้กว่า ๑๙๓,๐๐๐ ดอยช์มาร์ค และในปีเดียวกัน ธนาคาร Herstatt-Bank ประเทศเยอรมนี ถูกเปลี่ยนแปลงข้อมูลด้านงบดุลบัญชีจนต้องสูญเสียเงินไปกว่า ๑ ล้าน ดอยช์มาร์ค[๑๐๕] หรือคดีที่เกิดขึ้นปี พ.ศ. ๒๕๓๗ โดยกลุ่มผู้กระทำความผิดชาวรัสเซียร่วมกันเปลี่ยนแปลงบัญชีของโบสถ์แห่งหนึ่ง จนได้รับโอนเงินจากธนาคารประเทศสหรัฐอเมริกาจำนวนกว่าล้านเหรียญดอล์ล่าร์สหรัฐ[๑๐๖] เป็นต้น

---

๑๐๔ Rainer A von Mühlen, “Computer - Kriminalität. Gefahren und Abwehrmaßnahmen“, Neuwied/Berlin, 1973, p. 7.

๑๐๕ ดูสองคดีดังกล่าวใน Ulrich Sieber, „Computerkriminalität und Strafrecht, 1980, p. 58, 61.

๑๐๖ ดูคดีนี้ใน "Datenschutzberater", Vol. 10, 1995, p. 23.

ในช่วงกลางของทศวรรษที่ ๑๙๘๐ การปลอมแปลงข้อมูลคอมพิวเตอร์ในลักษณะของการกระทำความผิดต่อเครื่องเบิกเงินอัตโนมัติ หรือตู้เอทีเอ็ม รวมทั้งบัตรชำระเงินประเภทต่าง ๆ ที่ใช้ระบบอิเล็กทรอนิกส์ เริ่มเกิดขึ้น และขยายตัว ทั้งนี้แม้โดยปกติแล้วการกระทำความผิดที่เกี่ยวกับบัตรจ่ายเงินเหล่านี้ในแต่ละครั้ง จะสร้างความเสียหายต่อเหยื่อไม่มากนักเพราะผู้กระทำความผิดมักได้เงินไปเพียงเล็กน้อย แต่จากสถิติการกระทำความผิดที่สำรวจได้ในหลายประเทศพบว่าการปลอมแปลงข้อมูลคอมพิวเตอร์รูปแบบนี้เกิดขึ้นบ่อยครั้งกว่าการปลอมแปลงข้อมูลคอมพิวเตอร์ดั้งเดิมหลายเท่า[๑๐๗] โดยวิธีการกระทำความผิด มีตั้งแต่การขโมยบัตรชำระเงินจากเหยื่อแล้วใช้เทคนิคในการสุ่มหมายเลขเพื่อเบิกเงิน ขโมยบัตรมาเปลี่ยนแปลงรหัสโดยใช้คอมพิวเตอร์ก่อน แล้วจึงนำไปเบิกเงินจากเครื่องเอทีเอ็ม ไปจนถึงการติดตั้งเครื่องมือดักรหัสลับไว้ที่ตู้เบิกเงิน หรือใช้เครื่องดักฟังระยะไกลเพื่อบันทึกรหัสลับของผู้เสียหาย เป็นต้น อย่างไรก็ตามตามกฎหมายของบางประเทศ เช่น ประเทศเยอรมนี ถือว่าความผิดที่เกี่ยวกับบัตรอิเล็กทรอนิกส์นี้เป็นความผิดในกลุ่มเดียวกันกับความผิดฐาน "ฉ้อโกงคอมพิวเตอร์" ด้วย ทั้งนี้เพราะในขั้นตอนของการใช้บัตร (รวมทั้งรหัสต่าง ๆ ในกรณี Online-Banking อาทิ PIN จากการทำ Phishing) ของผู้อื่นเพื่อเบิกเงิน หรือใช้บริการกับระบบคอมพิวเตอร์ ย่อมมีการกระทำในลักษณะของ "การหลอกลวง" คอมพิวเตอร์ เกิดขึ้นแล้ว [๑๐๘] ปลายทศวรรษที่๑๙๘๐ ขอบเขตการกระทำความผิดการปลอมแปลงข้อมูลคอมพิวเตอร์ได้รับการพัฒนาให้กว้างขวางยิ่งขึ้นอีก ธุรกิจบริการรูปแบบอื่น ๆ ไม่เฉพาะการเงินการธนาคาร เริ่มตกเป็นเป้าหมายของผู้กระทำความผิด โดยเฉพาะอย่างยิ่ง การกระทำความผิดเกี่ยวกับ "บริการโทรศัพท์ผ่านเครือข่ายอินเตอร์เน็ต" อันที่จริงการลักใช้บริการโทรศัพท์เกิดขึ้นก่อนหน้านี้แล้ว แต่ในอดีตที่ผ่านมา (ทศวรรษที่ ๑๙๖๐)[๑๐๙] เป้าหมายของผู้กระทำความผิดส่วนใหญ่กระทำไปก็เพียงเพื่อประหยัดค่าโทรศัพท์ กับเครื่องโทรศัพท์ส่วนบุคคล หรือโทรศัพท์ในระบบธรรมดาเท่านั้น โดยเทคนิคที่นิยมในสมัยนั้น เรียกว่า วิธี "blue boxing" ด้วยเครื่องมือที่เรียกว่า "blue box" ใช้ในการตัด และควบคุมช่องส่งสัญญาณเสียง เพื่อตนจะสามารถแทรกเข้าไปใช้บริการได้โดยไม่เสียเงิน เลขหมายโทรศัพท์ที่มักถูกโจมตี มักเป็นเลขหมายโทรศัพท์ที่ให้บริการฟรีเพื่อติดต่อหน่วยประชาสัมพันธ์ของบริษัทต่าง ๆ อย่างไรก็ตาม ด้วยวิธีการดังกล่าวยังสามารถใช้ได้เฉพาะกับบริการโทรศัพท์ภายในประเทศเท่านั้น แต่นับจากที่มีนักเจาะระบบโทรศัพท์คนหนึ่ง (Telephone Hacker) คิดค้นวิธีการลักใช้โทรศัพท์ในระบบต่าง ๆ ซึ่งรวมทั้งระบบโทรศัพท์ทางไกล

---

๑๐๗ Manfred Möhrenschlager, in: Ulrich Sieber, อ้างแล้วในเชิงอรรถที่ 4, p. 200.

๑๐๘ Tröndle, Herbert / Fischer, Thomas, „Strafgesetzbuch und Nebengesetze“ , § 263a StGB, München 2008, p. 1904-1906.

๑๐๙ Ulrich Sieber, CR 1995, อ้างแล้ว, p. 102-103.

ข้ามประเทศ แล้วนำวิธีการมาเผยแพร่ การกระทำความผิดรูปแบบนี้ก็ขยายตัวอย่างรวดเร็ว จนในช่วงทศวรรษที่ ๑๙๙๐ เป็นต้นมา ธุรกิจการให้บริการโทรศัพท์ก็กลายเป็นเป้าหมายใหญ่ โดยเฉพาะอย่างยิ่งกับบริษัทผู้ให้บริการโทรศัพท์ที่วางระบบรักษาความปลอดภัย หรือเฝ้าระวังการลักใช้บริการไว้ไม่ดีพอ มูลเหตุจูงใจให้กระทำก็หลากหลายขึ้นไม่ใช่เพียงเพื่อประหยัดค่าโทรศัพท์ส่วนตัวเท่านั้น การกระทำความผิดในกลุ่มนี้มีตั้งแต่ เปลี่ยนแปลง ยักย้ายรายการ หรือบัญชีการใช้โทรศัพท์ของตนให้กลายเป็นของผู้ใช้บริการโทรศัพท์ทางอินเตอร์เน็ตคนอื่น, เจาะระบบคอมพิวเตอร์ของผู้ให้บริการ Voice-Mail-System เพื่อแอบใช้บริการ หรือใช้วิธีดักรับ หรือหลอกลวงบริษัทผู้ให้บริการเพื่อขอรหัสโทรศัพท์ของผู้ใช้บริการรายอื่น เป็นต้น

สำหรับความผิดในลักษณะนี้ ในระยะเริ่มแรกถ้อยคำที่มีปัญหาในการตีความเพื่อนำกฎหมายอาญาปกติมาใช้บังคับ ก็คือจะถือว่าระบบคอมพิวเตอร์ที่ใช้แสดงข้อมูล หรือข้อมูลอิเล็กทรอนิกส์เหล่านี้ เป็น "เอกสาร" เพื่อให้เข้ากับฐานความผิด "ปลอมแปลงเอกสาร" ได้หรือไม่ กรณีนี้ แม้นักกฎหมายส่วนหนึ่งเห็นว่า น่าจะสามารถตีความให้เป็นเอกสารได้ ทั้งนี้เพราะเป็นสิ่งที่ใช้เพื่อแสดงความหมายได้เหมือนกัน แต่ด้วยลักษณะพิเศษที่ไม่อาจจับต้องได้ของข้อมูล ไม่มีรูปร่างที่ชัดเจน อีกทั้งสามารถถูกแก้ไขเปลี่ยนแปลงได้ในเวลาอันรวดเร็ว และยากลำบากต่อการตรวจจับหรือหาร่องรอยการแก้ไขเปลี่ยนแปลง นอกจากประเทศจำนวนหนึ่งจะบัญญัติฐานความผิดขึ้นใหม่เพื่อใช้บังคับโดยเฉพาะแล้ว บางประเทศก็ใช้วิธีการแก้ไขเพิ่มเติมนิยามของคำว่า "เอกสาร" ให้มีความหมายครอบคลุมสื่ออิเล็กทรอนิกส์ด้วย

๒.๒ การเจาะระบบหรือการเข้าถึงระบบของผู้อื่นโดยปราศจากอำนาจ

การเจาะระบบคอมพิวเตอร์ หรือการเข้าถึงโดยปราศจากอำนาจนี้ ในช่วงระยะเวลาเริ่มต้น ผู้กระทำส่วนใหญ่ยังไม่ได้มีเป้าหมายในการกระทำความผิดอื่น ๆ อาทิ เจาะระบบเพื่อเข้าไปเปลี่ยนแปลงข้อมูล เพื่อหลอกลวง ทำลายระบบ หรือจารกรรมข้อมูล แต่ผู้กระทำความผิดมักต้องการเพียงทดลองเครื่องมือ หรือทดสอบความสามารถของตนในการฝ่าระบบรักษาความปลอดภัยของผู้อื่นเท่านั้น โดยคาดว่าการเจาะระบบเกิดขึ้นครั้งแรกในราวปี ๑๙๘๐ โดย Kevin Mitnick ซึ่งทำการเจาะเข้าไปในระบบคอมพิวเตอร์ของบริษัท US-Leasing [๑๑๐] ดังนั้นแต่เดิม คำว่านักเจาะระบบหรือแฮกเกอร์ จึงมิได้มีความหมายในแง่ลบเช่นในยุคปัจจุบัน เพราะนักเจาะระบบกลุ่มแรกไม่ได้ต้องการสร้างความเสียหายให้บุคคลอื่น และทั้งไม่เห็นด้วยกับนักเจาะระบบประเภทที่มุ่งสร้างความเสียหายด้านอื่น ๆ แก่ผู้อื่นด้วย

---

๑๑๐ Nicole Krüger, “Computerkriminalität nach deutschem Recht“, URL http://freenet-homepage.de/computercrime/inhalt.htm (15.09.07).

อย่างไรก็ตาม ในระยะหลัง ความผิดลักษณะนี้เกิดขึ้นบ่อยครั้ง และหลากหลายเป้าหมายมากขึ้น ทั้งนี้ทั้งจากนักเจาะระบบมืออาชีพ และแบบสมัครเล่น ความเสียหายที่เกิดขึ้นจึงอาจแตกต่างกันไป และแม้คดีส่วนใหญ่ที่เกิดขึ้นจะสร้างความเสียหายโดยตรงต่อระบบรักษาความปลอดภัยของบริษัท หรือหน่วยงานที่ถูกเจาะระบบเท่านั้น แต่หลายคดีก็สร้างความเสียหายอื่น ๆ ตามมาด้วย เมื่อปรากฏว่าผู้เจาะระบบนั้น นำเทคนิควิธีการที่ตนใช้ไปเผยแพร่ต่อยังบุคคลอื่น ซึ่งอาจนำไปใช้ในการกระทำความผิดอื่น ๆ ต่อไปได้อีก ตัวอย่างคดีสำคัญ ๆ ในอดีตที่เกิดขึ้น ได้แก่ คดีในปี 1985 ในมลรัฐ New Jersey เด็กนักเรียน ๗ คนเจาะระบบเข้าไปที่คอมพิวเตอร์ของเพนธากอน และมีรายงานว่าตั้งแต่ปี 1986 เป็นต้นมา ระบบคอมพิวเตอร์ตามหน่วยงานสำคัญ ๆ ของประเทศสหรัฐอเมริกาโดนเจาะระบบบ่อยครั้ง ดังเช่น ปี 1995 เพนธากอนรายงานว่า ระบบคอมพิวเตอร์ของหน่วยงานถูกโจมตีถึง 250,000 ครั้ง จนคาดกันว่า ข้อมูล หรือเทคนิคการเข้าถึงดังกล่าว อาจถูกนำไปขายต่อให้ KGB หรือ หน่วยรักษาความมั่นคง และหน่วยสืบราชการลับของรัสเซียด้วย[๑๑๑] และดังกล่าวมาแล้วว่า เมื่อเทคโนโลยีด้านนี้ได้รับการพัฒนา รูปแบบการกระทำความผิดก็ย่อมมีการพัฒนา และขยายตัวไปด้วย การเจาะระบบ ก็เช่นเดียวกัน ในสมัยต่อมาไม่เฉพาะแต่ระบบคอมพิวเตอร์เท่านั้นที่เป็นเป้าหมายของการกระทำความผิด แต่ระบบให้บริการอื่น ๆ อาทิ บริการโทรศัพท์ทางอินเตอร์เน็ต โทรศัพท์ทางไกล ได้กลายเป็นเป้าหมายใหญ่ของนักเจาะระบบ

ประเด็นปัญหาในทางกฎหมายสำหรับความผิดกลุ่มนี้ในช่วงเริ่มแรก ก็คือ แม้ลักษณะของการกระทำความผิดกลุ่มนี้ จะคล้ายกับความผิดฐาน "บุกรุก" ในกฎหมายอาญาเดิมก็ตาม แต่ด้วยองค์ประกอบความผิดฐานบุกรุกเดิมที่ว่า ผู้กระทำต้องมีการเข้าไปในอสังหาริมทรัพย์ของผู้อื่นทางกายภาพ จึงก่อให้เกิดปัญหาในการตีความขึ้น ทั้งนี้เป็นที่ทราบกันแล้วว่า การเข้าถึงระบบข้อมูลนั้น ผู้กระทำไม่จำเป็นต้องเข้าถึงเครื่องคอมพิวเตอร์ของผู้เสียหายโดยตรง เพียงแต่นั่งอยู่ที่หน้าจอคอมพิวเตอร์ของตน ก็อาจเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นได้ ในวงการกฎหมายส่วนใหญ่จึงตัดปัญหาการตีความในประเด็นนี้ด้วยการกำหนดฐานความผิดใหม่ขึ้นเพื่อใช้บังคับเป็นการเฉพาะ

๒.๓ การจารกรรมทางคอมพิวเตอร์ (Computer Spionage)

แม้ในระยะเริ่มแรก สถิติการกระทำความผิดในรูปแบบนี้ไม่ได้เกิดขึ้นบ่อยนักเมื่อเทียบกับการกระทำความผิดที่เกี่ยวกับคอมพิวเตอร์เรื่องอื่น ๆ แต่ถ้าเทียบกับการ "จารกรรมข้อมูลทางเศรษฐกิจ" ด้วยวิธีดั้งเดิม จะพบว่า อันตรายและความเสียหายที่เกิดจากการจารกรรมทางคอมพิวเตอร์สูงกว่าอาชญากรรมเศรษฐกิจแบบเดิม ๆ หลายเท่าตัว ทั้งนี้เนื่องจากระบบคอมพิวเตอร์กลายเป็นอุปกรณ์หลักในการจัดเก็บบันทึกข้อมูล ซึ่งมีจำนวนมหาศาล ทั้งแง่ปริมาณ และความ

---

๑๑๑ Ulrich Sieber, CR 1995, อ้างแล้ว, p. 103.

หลากหลาย ประกอบกับความทันสมัยในเรื่องเครื่องมือ และเทคนิควิธีการ ทำให้ผู้กระทำความผิดสามารถค้นหา และทำซ้ำข้อมูลเหล่านั้นได้ง่าย และรวดเร็ว โดยไม่จำเป็นต้องมีการเข้าถึงระบบคอมพิวเตอร์ทางกายภาพ วิธีการจารกรรมข้อมูลจะมีทั้งกรณีเจาะระบบเพื่อเข้าถึงฐานข้อมูลในคอมพิวเตอร์ก่อน แล้วจึงค้นหาเพื่อทำซ้ำ และการใช้เครื่องมือพิเศษดักรับข้อมูลในระหว่างการติดต่อสื่อสาร ข้อมูลส่วนใหญ่ที่ตกเป็นเป้าหมายของผู้กระทำในรูปแบบนี้ เช่น ข้อมูลการศึกษาวิจัย, ความลับทางการทหาร, ข้อมูลการประกอบธุรกิจ รวมทั้งข้อมูลเกี่ยวกับลูกค้า หรือการดักรหัสลับสำหรับใช้บริการต่าง ๆ ของผู้ใช้อินเตอร์เน็ตรายอื่น เป็นต้น โดยในระยะหลังการกระทำความผิดรูปแบบนี้จะเกิดขึ้นกับข้อมูลทางธุรกิจเสียส่วนใหญ่ ซึ่งคู่กรณีมักเป็นบริษัทคู่แข่งขันกัน

นอกจากนี้ ยังปรากฏอีกด้วยว่า หน่วยงานรัฐเองก็นำวิธีการดังกล่าวมาใช้ร่วมกับการสืบสวนการกระทำความผิด หรือในราชการลับต่าง ๆ ทำนองเดียวกับการดักฟังการสนทนาทางโทรศัพท์ของผู้ต้องสงสัยด้วย เช่น การใช้เครื่องมือ หรือโปรแกรมพิเศษ เพื่อดักรับข้อมูลที่ผู้ต้องสงสัยส่งระหว่างกันในบริการต่าง ๆ ในอินเตอร์เน็ต จนเกิดข้อถกเถียงกันว่า การกระทำของรัฐเหล่านั้น ถือเป็นเรื่องที่เกินความจำเป็น จนกลายเป็นการล่วงล้ำสิทธิของพลเมืองมากเกินไปหรือไม่ โดยเฉพาะอย่างยิ่งการกระทำโดยเจ้าหน้าที่ หรือหน่วยงานรัฐของประเทศสหรัฐอเมริกา ดังที่เคยมีการเปิดเผยรายงานในปี พ.ศ. ๒๕๓๔ แล้วพบว่า หน่วยงานรัฐดักฟังการสนทนาทางโทรศัพท์ไปกว่า ๒,๐๐๐ ครั้ง ในขณะที่มีการจับตา และควบคุมการสนทนาทางโทรศัพท์ไปกว่า ๕๔,๐๐๐ ครั้ง [๑๑๒]

ประเด็นปัญหาในทางกฎหมายสำหรับความผิดกลุ่มนี้ในช่วงเริ่มแรก ก็คือ ประเด็นการตีความว่าจะถือได้หรือไม่ว่าเป็นความผิดฐาน "ลักทรัพย์" ทั้งนี้เพราะมีการลักเอาไปซึ่งข้อมูลคอมพิวเตอร์ แต่ในที่สุดวงการกฎหมายก็ไม่อาจหาข้อยุติที่เหมาะสมได้ว่า "ข้อมูลอิเล็กทรอนิกส์" ซึ่งไม่มีรูปร่างจับต้องได้นี้ถือเป็น "ทรัพย์" ที่ลักขโมยได้หรือไม่ อีกทั้งยังติดปัญหาที่ว่า แม้ผู้กระทำความผิดจะได้ไปซึ่งข้อมูล แต่เจ้าของข้อมูลที่แท้จริงยังได้ใช้ประโยชน์จากข้อมูลนั้นอยู่ จึงไม่น่าจะเข้าองค์ประกอบความผิดฐาน "ลักทรัพย์" ที่ปกติแล้ว เจ้าของทรัพย์จะต้องถูกพรากทั้ง "กรรมสิทธิ์" และ "การครอบครอง" ทรัพย์นั้นไปด้วยในขณะเดียวกัน เพื่อตัดปัญหาเหล่านี้ ประเทศส่วนใหญ่จึงบัญญัติฐานความผิดใหม่ใช้กับการจารกรรม รวมทั้งการดักรับไว้ซึ่งข้อมูลอิเล็กทรอนิกส์ โดยเฉพาะ

๒.๔ การก่อวินาศกรรมอินเตอร์เน็ต (Computer Sabotage) และการข่มขู่ทางอินเตอร์เน็ต (Computer Blackmail)

อาจกล่าวได้ว่า การก่อวินาศกรรมคอมพิวเตอร์ (Computer sabotage) จนถึงปัจจุบัน

---

๑๑๒ Computerviren-Entwicklungsgeschichte,.(Online).Available:http://edv-stangl.com/stangl.com/8.1.html (25.10.2009).

ยังคงจัดอยู่ในกลุ่มความผิดอันเกี่ยวกับคอมพิวเตอร์ที่เกิดขึ้นบ่อยครั้ง เช่นเดียวกับการปลอมแปลงข้อมูลคอมพิวเตอร์ ซึ่งนอกจากการกระทำต่อคอมพิวเตอร์ส่วนบุคคล ด้วยวิธีปล่อยโปรแกรมทำลายต่าง ๆ เช่น ไวรัส หรือเวิร์ม เพื่อทำลายระบบ หรือข้อมูลคอมพิวเตอร์แล้ว การก่อวินาศกรรมเพื่อสร้างความเสียหายกับบริษัทใหญ่ ๆ หรือบริษัทคู่แข่งทางธุรกิจก็เพิ่มจำนวนขึ้น การกระทำความผิดในลักษณะนี้ขยายตัวมากขึ้น ภายหลังจากระบบเครือข่ายคอมพิวเตอร์ได้รับการพัฒนา ทั้งนี้เพราะผู้กระทำความผิดเขียนโปรแกรมทำลายเพียงครั้งเดียว แต่สามารถส่งต่อเผยแพร่สร้างความเสียหายให้เหยื่อได้จำนวนมาก ไวรัสที่มีเป้าหมายในการทำลายล้าง หรือเพื่อก่อวินาศกรรมตัวแรกถูกเขียนขึ้นราวปี พ.ศ.๒๕๒๙ ในชื่อ "Pakistani Brain" โดยตัวทำลายนี้มีผลต่อ Bootsector อันเป็นส่วนประกอบสำคัญของเครื่องคอมพิวเตอร์ อย่างไรก็ตาม โปรแกรมไวรัสจำนวนมาก และหลากหลายชนิด ถูกเขียนขึ้นก่อนหน้าไวรัส "Pakistani Brain" แล้ว เพียงแต่ไม่ได้ถูกนำมาใช้เพื่อเป้าหมายในการโจมตี หรือก่อวินาศกรรมโดยเฉพาะ ไวรัสตัวแรกถูกเปิดเผยในงานปริญญาเอกของ Fred Cohen ตั้งแต่ปี พ.ศ.๒๕๒๖[๑๑๓] สำหรับโปรแกรมเวิร์มที่เป็นที่รู้จักอย่างกว้างขวาง เกิดขึ้นราวปี พ.ศ.๒๕๒๘ ในชื่อ"INTERNET-Wurm" ทั้งนี้เพราะภายหลังการเผยแพร่เพียงไม่กี่วันสามารถทำลายระบบคอมพิวเตอร์ไปกว่า ๖,๐๐๐ เครื่อง และนอกจากเวิร์มแล้ว ปัจจุบันโปรแกรมทำลายอื่นๆ ก็ถูกพัฒนาออกมาอีกจำนวนมาก อาทิ โทรจัน Logic-Bomb หรือ Time-Bomb เป็นต้น การก่อวินาศกรรมคอมพิวเตอร์ นับเป็นการกระทำความผิดที่มีผลกระทบต่อระบบเศรษฐกิจโดยรวมอย่างยิ่ง ทั้งนี้เพราะในยุคสมัยดังกล่าว เทคโนโลยีคอมพิวเตอร์ ระบบการสื่อสารผ่านเครือข่ายได้กลายเป็นส่วนสำคัญทั้งต่อการประกอบธุรกิจ และชีวิตประจำวันของคนในสังคม

การก่อวินาศกรรมคอมพิวเตอร์ที่เกิดขึ้นในยุคนั้น ยังนำมาซึ่งความผิดอีกรูปแบบหนึ่งด้วย คือ การข่มขู่ทางอินเตอร์เน็ต โดยผู้เสียหายจะถูกข่มขู่ผ่านทางจดหมายอิเล็กทรอนิกส์ หรือเอกสารลับ ให้ต้องยินยอมกระทำการอย่างหนึ่งอย่างใด กรรโชก หรือรีดไถเงิน มิเช่นนั้นระบบคอมพิวเตอร์ หรือข้อมูลที่อยู่ในระบบจะถูกทำลาย หรือทำให้เสียหายจนใช้ประโยชน์ไม่ได้ นอกจากนี้ ผู้กระทำผิดอาจใช้วิธีเขียนโปรแกรมเข้ารหัสคอมพิวเตอร์ของเหยื่อเพื่อทำให้ผู้เป็นเจ้าของไม่สามารถใช้งานคอมพิวเตอร์ หรือเข้าถึงข้อมูลได้ แล้วข่มขู่ให้จ่ายเงินเพื่อแลกกับการถอดรหัสดังกล่าว เป็นต้น

ประเด็นปัญหาในทางกฎหมายในช่วงเริ่มแรก สำหรับความผิดที่เกี่ยวกับการก่อวินาศกรรมคอมพิวเตอร์นี้จะคล้ายคลึงกับ การดักรับ หรือการจารกรรมข้อมูล คือ ปัญหาเรื่องการตีความคำว่า "ทรัพย์" เพียงแต่เป็นการตีความในความผิดฐาน "ทำให้เสียทรัพย์" ไม่ใช่ "ลักทรัพย์"

---

๑๑๓ Hafner Katie / Markoff John, “Cyberpunk: Outlaws and Hackers on the Computer Frontier“, New York: Touchstone, 1991, p. 251.

เพราะผู้กระทำความผิดมิได้มุ่งหวังที่จะนำเอาข้อมูลคอมพิวเตอร์ไป คงเป็นแต่เพียงต้องการสร้างความเสียหายให้กับระบบ และข้อมูลของผู้เสียหายเท่านั้น อย่างไรก็ตามเพื่อตัดปัญหาเกี่ยวกับการตีความดังกล่าว สุดท้ายประเทศส่วนใหญ่จึงบัญญัติการกระทำความผิดฐานนี้ไว้ในกฎหมายใหม่หรือแก้ไขเพิ่มเติมกฎหมายเก่าเช่นเดียวกัน

๒.๕ การฉ้อโกงทางคอมพิวเตอร์ (Computer Frauds)

การกระทำด้วยวิธีการใด ๆ ต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ เพื่อให้ระบบนั้นทำงานหรือแสดงผลที่ผิดพลาด หรือผิดปกติไปจากเดิมหรือที่ควรจะต้องแสดง จนเป็นเหตุให้ผู้กระทำนั้นได้ประโยชน์ในทางทรัพย์สินอย่างหนึ่งอย่างใดไปโดยมิชอบด้วยกฎหมาย เช่น การสร้างโปรแกรมคอมพิวเตอร์ หรือแก้ไขเปลี่ยนแปลงโปรแกรมบางอย่างเพื่อให้คอมพิวเตอร์ปฏิบัติการตามความต้องการของตน ตัวอย่างคดีที่พบมักเกิดขึ้นในแวดวงการเงิน การธนาคารโดยผู้กระทำ ก็มักเป็นโปรแกรมเมอร์ของธนาคารนั้น ๆ เอง ซึ่งย่อมก่อให้เกิดผลกระทบต่อเศรษฐกิจโดยรวมไปด้วย

ประเด็นปัญหาในทางกฎหมายสำหรับความผิดกลุ่มนี้ เนื่องจากการ "การฉ้อโกงทางคอมพิวเตอร์" มีลักษณะสำคัญประการหนึ่งที่แตกต่างไปจากความผิดฉ้อโกงธรรมดาตามกฎหมายอาญา คือ การฉ้อโกงคอมพิวเตอร์เป็นการหลอกลวง หรือกระทำต่อระบบคอมพิวเตอร์ ในขณะที่การฉ้อโกงธรรมดาเป็นการกระทำต่อบุคคล เมื่อวัตถุเป้าหมายที่ถูกกระทำเป็นคนละสิ่งกันเพื่อตัดปัญหาความขัดแย้งในการใช้การตีความ หลายประเทศจึงมักบัญญัติฐานความผิดใหม่เพื่อใช้กับการฉ้อโกงทางคอมพิวเตอร์โดยเฉพาะ

๒.๖ การขโมย ลักลอกทำซ้ำ หรือใช้ซอร์ฟแวร์ หรือผลิตภัณฑ์ลิขสิทธิ์อื่น ๆ โดยไม่ได้รับอนุญาต

สำหรับความผิดฐานนี้ในระยะเริ่มแรก มักมีเป้าหมายอยู่ที่ "ซอร์ฟแวร์เฉพาะทาง" (Individual Software) เนื่องจากในสมัยนั้นยังมีหน่วยงานที่สามารถลงทุนกับเครื่องคอมพิวเตอร์ และโปรแกรมในจำนวนไม่มากนัก โปรแกรมใช้งานพื้นฐานอื่น ๆ จึงยังไม่ได้รับการพัฒนา โปรแกรมส่วนใหญ่ที่ผลิตออกมาคือโปรแกรมที่ถูกเขียนขึ้นตามความต้องการของผู้ว่าจ้างเป็นราย ๆ ไป โดยไม่มีจำหน่ายเป็นการทั่วไปในตลาดปกติ คดี "Inkassoprogramm" นับเป็นคดีแรก ที่ได้รับการตัดสินจากศาลประเทศเยอรมนี ให้ผู้ลักลอบทำซ้ำรับผิดในฐานละเมิดลิขสิทธิ์โปรแกรมคอมพิวเตอร์[๑๑๔] อย่างไรก็ตาม ภายหลังจากที่ความต้องการใช้คอมพิวเตอร์โดยบุคคลทั่วไปเพิ่มขึ้น เป้าหมายของการ

---

๑๑๔ Ulrich Sieber, “Bilanz eines 'Musterverfahrens'. Zu dem rechtskräftigen Abschluß des Verfahrens BGHZ 94, S. 276 (Inkassoprogramm)“, CR 1986, p. 699.

กระทำความผิดลักษณะนี้จึงเปลี่ยนไปที่ "โปรแกรมใช้งานพื้นฐาน" (Standard Software) แทน โดยเฉพาะอย่างยิ่งโปรแกรมสำหรับใช้งานด้านต่าง ๆ ในเครื่องคอมพิวเตอร์ส่วนบุคคล ทั้งนี้เพราะในช่วงต้นของการพัฒนา โปรแกรมใช้งานดังกล่าวเกือบทั้งสิ้นเป็นโปรแกรมที่มีลิขสิทธิ์ และจำหน่ายในราคาสูง ผู้ใช้ส่วนหนึ่งที่มีความสามารถทางคอมพิวเตอร์ และไม่ต้องการเสียเงินจำนวนมาก จึงพยายามหาวิธีในการลักลอบทำซ้ำโปรแกรมเหล่านั้นมาใช้แทน การกระทำความผิดในกลุ่มนี้ส่งผลกระทบต่อบริษัทผู้ผลิตซอร์ฟแวร์จำนวนมาก โดยเฉพาะอย่างยิ่งในระยะหลังที่นอกจากการลักลอบทำซ้ำ เพื่อใช้ประโยชน์ส่วนบุคคลแล้ว ยังมีการนำมาวางขายในราคาถูกกว่าซอร์ฟแวร์จริงด้วย ดั่งที่รู้จักกันในชื่อ "ซอร์ฟแวร์เถื่อน" หรือ "ซอร์ฟแวร์ผิดกฎหมาย" ซึ่งปรากฏการณ์เช่นนี้ไม่ได้เกิดเฉพาะในประเทศโลกที่สองเท่านั้น แม้แต่ในประเทศโลกที่หนึ่งซึ่งเป็นผู้ผลิต และจำหน่าย Software ลิขสิทธิ์แหล่งใหญ่อย่างสหรัฐอเมริกา ก็เกิดปัญหาเช่นกัน ในยุคหนึ่งเคยมีการรายงานว่าในประเทศสหรัฐอเมริกามีซอร์ฟแวร์เถื่อนขายอยู่ถึงราว ๔๐% ประเทศเยอรมัน ๗๖% ประเทศญี่ปุ่น ๘๑% ในขณะที่ประเทศไทยมีอัตราสูงถึง ๙๘% [๑๑๕] แม้ในช่วงกลางทศวรรษที่ ๑๙๘๐ การไล่ติดตามจับกุมผู้ขายอย่างจริงจัง จะเป็นผลให้ธุรกิจซอร์ฟแวร์เถื่อนลดลงมาก แต่เวลาเพียงช่วงไม่กี่ปีหลังจากนั้น รูปแบบการกระทำความผิดประเภทนี้ก็พัฒนาเปลี่ยนแปลงไปอีก จากเดิมที่นำซอร์ฟแวร์มาวางขายซึ่งง่ายต่อการถูกติดตามจับกุม ก็เปลี่ยนเป็นการขายผ่านทางอินเตอร์เน็ต เว็บไซท์ หรือรับสั่ง-ส่งสินค้าทางอีเมล์ เป็นต้น ทั้งนี้หมายรวมทั้งซอร์ฟแวร์เถื่อนเอง และเครื่องมือในการทำซ้ำซอร์ฟแวร์ อีกทั้งยังมีบ่อยครั้งที่ผู้จำหน่ายฮาร์ดแวร์นำซอร์ฟแวร์เถื่อนเหล่านั้นขายพร้อมหรือให้ฟรีกับลูกค้า อย่างไรก็ตาม มีการคาดการณ์ไว้เช่นกันว่า หลังจากที่ ซอร์ฟแวร์ฟรี หรือซอร์ฟแวร์ Open Source ต่าง ๆ ถูกพัฒนาขึ้น จนเริ่มได้รับความนิยมอย่างกว้างขวาง ที่สุดแล้ว การกระทำความผิดรูปแบบนี้โดยมีเป้าหมายอยู่ที่ "โปรแกรมการใช้งานคอมพิวเตอร์" คงลดจำนวนลงไปได้

"มูลค่า" ที่เพิ่มสูงขึ้นของบรรดาข้อมูลทั้งหลายในยุคข้อมูลข่าวสารเป็นสาเหตุหนึ่งที่จูงใจให้เกิดการพัฒนาวิธีการกระทำความผิด และขยายขอบเขตเป้าหมายของการกระทำออกไป ในระยะต่อมา นอกจากการลักลอบทำซ้ำ "โปรแกรมคอมพิวเตอร์" โดยไม่ได้รับอนุญาตจะเพิ่มขึ้นแล้ว ฐานข้อมูล รวมทั้งข้อมูลอื่น ๆ อาทิ ข้อมูลทางธุรกิจ ข้อมูลลูกค้า เพลง ภาพยนตร์ เกมคอมพิวเตอร์ ฯลฯ ก็ถูกลักลอบทำซ้ำเพื่อนำมาจำหน่ายต่อด้วยเช่นกัน ซึ่งแหล่งที่มาหรือฐานข้อมูลที่ถูกลักลอบทำซ้ำโดยไม่ได้รับอนุญาตดังกล่าว มีทั้งประเภทออนไลน์ (Online Database) และไม่ได้ออนไลน์ (Offline Database)

---

๑๑๕ Newsweek v. 29.06.1992, p. 44.

ประเด็นปัญหาในทางกฎหมายสำหรับความผิดกลุ่มนี้ในช่วงเริ่มแรก ก็คือ กฎหมายทรัพย์สินทางปัญญาของประเทศส่วนใหญ่ยังไม่ได้ระบุให้ความคุ้มครองกับโปรแกรมคอมพิวเตอร์ รวมทั้งฐานข้อมูลดิจิตอล จึงต้องอาศัยการตีความจากกฎหมายเดิมที่มีอยู่ หลังจากนั้นจึงได้เกิดข้อตกลง และสนธิสัญญาระหว่างประเทศเพื่อคุ้มครองข้อมูลรูปแบบใหม่เหล่านี้ และประเทศต่าง ๆ ก็ทำการแก้ไขเพิ่มเติมกฎหมายภายในของตนเพื่อให้ใช้ได้ครอบคลุม[๑๑๖] จะเห็นได้ว่า นับตั้งแต่ทศวรรษที่ ๑๙๗๐ เป็นต้นมา เมื่อกล่าวถึง "อาชญากรรมคอมพิวเตอร์" ในสมัยที่ยังรวมอยู่ในนิยามของคำว่า "อาชญากรรมทางเศรษฐกิจ" แล้ว สิ่งที่กฎหมายประสงค์จะคุ้มครองเป็นพิเศษได้ขยายจาก "ข้อมูลส่วนบุคคล และสิทธิความเป็นส่วนตัว" ไปสู่ "เศรษฐกิจโดยรวม" ของประเทศ ทั้งนี้ก็เนื่องมาจากในยุคสมัยดังกล่าวคอมพิวเตอร์เริ่มถูกนำไปใช้เพื่ออำนวยความสะดวกในการประกอบการหรือทำธุรกิจต่างๆ มากขึ้น จึงไม่เฉพาะข้อมูลส่วนบุคคลของปัจเจกชนเท่านั้น แต่ข้อมูลหลากหลายประเภท โดยเฉพาะอย่างยิ่ง ข้อมูลทางด้านการเงิน การบัญชี ลูกค้า ผลิตภัณฑ์ดิจิตอล โปรแกรมคอมพิวเตอร์ เพลง ภาพยนตร์ ล้วนแล้วแต่มีคอมพิวเตอร์เป็นเครื่องมือสำคัญในการเก็บบันทึก และประมวลผล ทั้งสิ้น

๓. อาชญากรรมไซเบอร์ หรือ อาชญากรรมอินเตอร์เน็ต

นับเนื่องจากทศวรรษที่ ๑๙๙๐ เรื่อยมาจนถึงปัจจุบัน การกระทำความผิดที่อยู่ในขอบเขตความหมายของคำว่า "อาชญากรรมคอมพิวเตอร์" มิได้จำกัดอยู่แต่เฉพาะ การละเมิดข้อมูลส่วนบุคคล หรือเฉพาะการละเมิดทรัพย์สินที่ก่อให้ความเสียหายต่อเศรษฐกิจ อีกต่อไป แต่ยังรวมความไปถึง การกระทำความผิด ต่อสิ่งที่กฎหมายประสงค์จะคุ้มครองในด้านอื่น ๆ ด้วย โดยผู้กระทำความผิดมีเป้าหมายเพื่อสร้างความเสียหายต่อประโยชน์สาธารณะ ค่านิยม แนวคิด สังคม พัฒนาการของเด็กและเยาวชน กระทั่งต่อชีวิตและร่างกาย [๑๑๗] ทั้งนี้โดยอาศัยช่องทางจากบริการที่อยู่บนเครือข่ายคอมพิวเตอร์ เอาเข้าจริงแล้ว ความผิดในยุคนี้ ก็คือ อาชญากรรมคอมพิวเตอร์รูปแบบหนึ่งเช่นกัน แต่แทนที่จะกระทำต่อ หรือใช้คอมพิวเตอร์ส่วนบุคคลเป็นเครื่องมือ กลับอาศัยระบบเครือข่ายคอมพิวเตอร์ เพื่อช่วยให้การกระทำความผิดขยายวงกว้างขึ้น สะดวกรวดเร็ว ซับซ้อนยิ่งขึ้น และที่สำคัญทำให้การติดตามตัวผู้กระทำความผิดทำได้ยากขึ้น และเพื่อจำเพาะเจาะจงให้ชัดเจน คำว่าความผิดสำคัญ ๆ ที่เริ่มปรากฏตัวขึ้นในยุคหลังการแพร่หลายของเครือข่ายคอมพิวเตอร์ โดยเฉพาะอย่างยิ่ง อินเตอร์เน็ต เรื่อยมาจนถึงปัจจุบัน ได้แก่ การเผยแพร่ข้อมูลที่ไม่ชอบด้วยกฎหมาย อาทิ ภาพลามกอนาจารเด็ก และ/หรือ เยาวชน ข้อความหมิ่นประมาทบุคคลอื่น ข้อมูลที่มีเนื้อหาในเชิงปลุกฝังความก้าวร้าว รุนแรง หรือ แนวคิดในการดูหมิ่นชนชาติอื่น การเลือกปฏิบัติ การพนันผิดกฎหมาย

---

๑๑๖ Ulrich Sieber, CR 1995, อ้างแล้ว, p. 108-109.

๑๑๗ Ulrich Sieber, CR 1995, อ้างแล้ว, p. 105.

กระทั่งการจำหน่ายอาวุธต้องห้าม เคยมีการสำรวจพบว่า เว็บไซท์ที่มีเนื้อหาเกี่ยวกับการเหยียดหยามดูหมิ่นชนชาติ สีผิว เกิดขึ้นจำนวนมากในประเทศสหรัฐอเมริกา ซึ่งกฎหมายรัฐธรรมนูญให้การคุ้มครองไว้ในฐานะที่เป็นสิทธิเสรีภาพในการแสดงความคิดเห็น[๑๑๘] เช่นเดียวกับที่เกิดขึ้นในประเทศเยอรมนี ที่แม้เว็บไซท์ที่มีเนื้อหาลักษณะดังกล่าวจะเคยถูกปิดกั้น เพราะถือเป็นความผิดตามกฎหมายอาญา[๑๑๙] ไปแล้วจำนวนมาก แต่ก็ยังคงมีการลักลอบเผยแพร่ แนวคิดในการต่อต้านแรงงานต่างชาติ ลัทธิซ้ายหรือขวาจัด ฯลฯ หรือส่งต่อกันทางอีเมล์อีกเป็นจำนวนมาก [๑๒๐] นอกจากความผิดในแง่เนื้อหาข้อมูลแล้ว ผลจากการเติบโตของ พาณิชย์อิเล็กทรอนิกส์ (E-Commerce) การทำธุรกรรมออนไลน์ รวมทั้งวิถีทางใหม่ ๆ ที่ใช้ในการติดต่อสื่อสารระหว่างกัน ยังก่อให้เกิดความผิดรูปแบบใหม่ ๆ ขึ้นอีกจำนวนมาก อาทิเช่น Phishing, Pharming, Spamming หรือ DDoS เป็นต้น

การละเมิดทรัพย์สินทางปัญญา หรือผลงานอันมีลิขสิทธิ์ ก็เป็นอีกกลุ่มความผิดหนึ่งที่ถูกพัฒนาขึ้นอีกมากภายหลังจากที่อินเตอร์เน็ตเริ่มแพร่หลาย โดยเฉพาะอย่างยิ่งเมื่อ เครื่องมือ หรือโปรแกรมที่ช่วยให้ผู้ใช้อินเตอร์เน็ตโดยทั่วไป สามารถแลกเปลี่ยน หรือแบ่งปันงานอันมีลิขสิทธิ์ (โดยไม่ได้รับอนุญาตจากเจ้าของ) ซึ่งกันและกันได้โดยตรง (ไม่ต้องผ่านตัวกลาง หรือผู้ให้บริการ)ที่เรียกว่า File-sharing- หรือ Peer-to-Peer-System ถูกพัฒนาขึ้น[๑๒๑] โปรแกรมสำคัญ และเป็นที่รู้จักตัวแรกก็คือ Napster แต่ปัจจุบันมีโปรแกรมในลักษณะเดียวกันนี้ แต่มีความสามารถเพิ่มขึ้น และทำให้สืบหาต้นต่อผู้เผยแพร่ลำบากเกิดขึ้นอีก อาทิ Bittorrent, eDonkey, Aimster, KaZaa, Freenet หรือ Gnutella เป็นต้น

๔. การกระทำความผิดอื่น ๆ

นอกจากความผิดรูปแบบใหม่ต่าง ๆ ดังกล่าวมาแล้ว การกระทำความผิดในฐานดั้งเดิมแต่มีคอมพิวเตอร์ หรือเครือข่ายคอมพิวเตอร์เข้าไปเกี่ยวข้องก็เพิ่มขึ้นเช่นกัน โดยเฉพาะอย่างยิ่ง

---

๑๑๘ "The Constitution of the United States contains provisions for the protection of individual rights, such as the right of free speech, and nothing in the Convention shall be deemed to require or to authorize legislation or other action by the United States of America incompatible with the provisions of the Constitution of the United States of America.

๑๑๙ § 130 StGB „Volksverhetzung".

๑๒๐ Anton Maegerle / Matthias Mletzko, "Thule-Netz". Rechtsextremistischer Mailboxen-Verbund, in: Informationsdienst Terrorismus, Extremismus, Organisierte Kriminalität, 1994, p. 1.

๑๒๑ Jan Bernd Nordemann / Andreas Dustmann, "To Peer Or Not To Peer - Urheberrechtliche und datenschutzrechtliche Fragen der Bekämpfung der Internet - Piraterie", CR 2004, p. 388.Michael Heghmanns, "Musiktauchbörsen im Internet aus strafrechtlicher Sicht", MMR 2004, p. 14.

ความผิดฐานฉ้อโกง ซึ่งเติบโตควบคู่มากับธุรกิจออนไลน์ เช่น การสั่งซื้อของผ่านอินเตอร์เน็ต แต่ไม่ได้รับสินค้านั้นภายหลังชำระเงินแล้ว หรือกลับกัน ส่งสินค้าไปแล้วแต่ไม่ได้รับการชำระเงินในภายหลัง หรือแม้กระทั่ง สั่งซื้อสินค้าอย่างหนึ่ง แต่สินค้าที่ถูกส่งมาเป็นอีกอย่าง หรืออีกคุณภาพหนึ่ง เป็นต้น

นอกจากนี้ ในระยะหลังยังพบว่า การเปลี่ยนแปลงข้อมูลทางคอมพิวเตอร์หลายคดี ผู้กระทำมิได้มุ่งหมายเพื่อผลประโยชน์ในทางทรัพย์สิน หรือสร้างความเสียหายด้านเศรษฐกิจเท่านั้น แต่มีเป้าหมายในการทำร้ายร่างกาย หรือละเมิดชีวิตของเหยื่อผู้เสียหายด้วย อาทิ การเปลี่ยนแปลงข้อมูลการรักษาหรือแก้ไขรายการให้ยาผู้ป่วยในฐานข้อมูลของโรงพยาบาล การรบกวน หรือโจมตีทำลายระบบรักษาความปลอดภัย หรือข้อมูลการบินของอากาศยาน รวมทั้งระบบสาธารณูปโภคอื่น ๆ ปัจจุบันเทคโนโลยีคอมพิวเตอร์ยังถูกนำมาใช้เพื่อสร้างเสริมประสิทธิภาพการทำงาน หรือเพื่ออำนวยความสะดวกในการติดต่อสื่อสารระหว่างอาชญากรในองค์กรอาชญากรรม รวมทั้งกลุ่มผู้ก่อการร้ายระหว่างประเทศ ตัวอย่างคดีความผิดเกี่ยวกับคอมพิวเตอร์ที่มีผลต่อชีวิตร่างกาย เกิดขึ้นในประเทศอังกฤษตั้งแต่ราวปี พ.ศ.๒๕๓๗ เมื่อแฮกเกอร์ชาวอังกฤษคนหนึ่ง เจาะระบบฐานข้อมูลของโรงพยาบาลลิเวอร์พูล เพื่อสร้างความเสียหายแก่เครื่องบันทึกข้อมูล นอกจากนี้ยังทำการเปลี่ยนแปลงข้อมูลการให้ยารักษาคนไข้เด็กอายุ ๘ ขวบรายหนึ่งด้วย แต่นางพยาบาลผู้ดูแลพบความผิดปกติของข้อมูลก่อนจึงไม่ได้เกิดอันตรายต่อเด็ก [๑๒๒]

การเปลี่ยนแปลงข้อมูลในคอมพิวเตอร์ หรือการก่อวินาศกรรมคอมพิวเตอร์ จนทำให้การประมวลผลข้อมูลผิดพลาด เคยสร้างปัญหาให้ระบบการทำงานในกองทัพหลายต่อหลายครั้งเช่นกัน จนเคยมีข้อกังวลว่า หากกองทัพไม่เร่งหาทางป้องกันระบบฐานข้อมูลเหล่านี้ให้ดีพอ ความเสียหายที่เกิดขึ้นในอนาคตอาจมิใช่แค่เพียงระบบรักษาความปลอดภัยของตนเองเท่านั้น แต่อาจร้ายแรงถึงขั้นก่อให้เกิดสงครามโดยไม่ตั้งใจ ดังที่เคยเกิดขึ้นกับกองทัพสหรัฐมาแล้วในปี พ.ศ.๒๕๓๘ ครั้งนั้นการถูกเจาะระบบเปลี่ยนแปลงข้อมูลผ่านอินเตอร์เน็ต เป็นผลให้กองทัพเรือสหรัฐส่งเรือรบไปยังสถานที่หนึ่งซึ่งผิดไปจากเป้าหมายถึง ๗ ลำ [๑๒๓]

ประเด็นทางกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางสารสนเทศ

แม้ว่าเทคโนโลยีสารสนเทศจะถูกนำมาใช้งานในสังคมอย่างกว้างขวาง ความเข้าใจในสิ่งแวดล้อมของการทำงานของระบบข้อมูลสารสนเทศ นโยบายและกลยุทธในการป้องกันภัย

---

๑๒๒ Der Spiegel Nr. 9/1994 v. 28.2.1994, p. 243

๑๒๓ Roger C. Molander / Andrew S. Riddile / Peter A. Wilson, “Strategic Information Warfare.A New From of War”, 1996, 17-22; John Arquilla / David Ronfeldt, “Cyberwar is Coming!”, Coparative Strategy, 1993, p. 141.

คุกคามข้อมูล อุปกรณ์ เครื่องมือทางเทคนิค โปรแกรมป้องกันภัยข้อมูล และระบบการทำงานต่าง ๆ ขององค์กรหนึ่ง ๆ เพียงลำพัง คงไม่เพียงพอที่จะป้องกันภัยดังกล่าวได้อย่างครอบคลุมและยั่งยืน ตราบใดที่รัฐไม่สนใจ หรือไม่เห็นความสำคัญของภัยรูปแบบนี้ที่มีมายังประชาชน องค์กร หรือหน่วยงานที่อยู่ภายใต้การปกครองของตน หากแต่รัฐจำเป็นต้องออกกฎเกณฑ์ หรือกำหนดมาตรการทางกฎหมายเพื่อคุ้มครองทั้งระบบและข้อมูล และเพื่อจัดการหรือปราบปรามการกระทำใด ๆ ที่ถือเป็นภัยคุกคามต่อระบบสารสนเทศ จัดตั้งองค์กรที่มีภารกิจ หรือดูแลด้านนี้โดยเฉพาะ รวมทั้ง รัฐจะต้องพยายามแสวงความร่วมมือ หรือจัดทำข้อตกลงระหว่างประเทศเพื่อป้องกันและปราบปรามภัยคุกคามดังกล่าวด้วย

อย่างไรก็ดี ปัจจุบันประเทศต่าง ๆ ทั่วโลก รวมทั้งประเทศไทยล้วนให้ความสำคัญกับการป้องกันภัยคุกคามความมั่นคงทางระบบสารสนเทศ และพยายามเสริมสร้างระบบรักษาความปลอดภัยไซเบอร์ให้แข็งแกร่ง โดยนอกจากหน่วยงานเฉพาะที่ตั้งขึ้นเพื่อดูแลเรื่องนี้ในประเทศตนเองแล้ว ก็ยังออกกฎหมายภายใน และทำข้อตกลงระหว่างประเทศด้วย เช่น ปัจจุบันประเทศไทยมี คณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security committee – NCSC) [๑๒๔] ซึ่งมีหน้าที่ในการจัดทำนโยบายความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อให้ประเทศไทยมีขีดความสามารถในการปกป้อง รับมือ และลดความเสี่ยงจากสถานการณ์ด้านภัยคุกคามในไซเบอร์ทั้งจากภายในและภายนอก ที่กระทบต่อความมั่นคงแห่งชาติ ครอบคลุมถึงความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ และความมั่นคงทางเศรษฐกิจ ตลอดจนติดตามและประเมินผลการปฏิบัติที่เกี่ยวข้อง เพื่อให้เกิดการบูรณาการการทำงานของหน่วยงานต่าง ๆ นอกจากนี้ยังมีการจัดทำความร่วมมือ (MOU) กับกลุ่มประเทศอาเซียนเพื่อแลกเปลี่ยนเทคโนโลยีและประสบการณ์ด้านการรักษาความปลอดภัยไซเบอร์ เป็นต้น ในระดับอาเซียนเอง ก็ได้มีการจัดตั้งชุดเผชิญเหตุฉุกเฉินด้านไซเบอร์ของประชาคมอาเซียน (ASIAN CERT) [๑๒๕] ขึ้นเพื่อแลกเปลี่ยนข้อมูล แจ้งเตือนภัย และให้ความช่วยเหลือแก่สมาชิกที่ถูกภัยคุกคาม

สำหรับในประเด็นด้านกฎหมายนั้น ปัจจุบัน ประเทศไทยมีพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ที่กำหนดให้การเข้าถึงระบบ และข้อมูลคอมพิวเตอร์

---

๑๒๔ (Online).Available:https://www.ncsc.nl/english

๑๒๕ Association of South East Asian Nations, "ASEAN Defence Ministers Meeting"(Online).Available:http://www.asean.org/communities/asean-political-security-community/ category/asean-defence-ministers-meeting-admm

ของผู้อื่น โดยปราศจากอำนาจเป็นความผิดและต้องระวางโทษ (มาตรา ๕[๑๒๖] และมาตรา ๗[๑๒๗] พรบ.คอมพิวเตอร์ฯ) นอกจากนี้ การใช้อุปกรณ์อิเล็กทรอนิกส์เพื่อดักรับข้อมูลของบุคคลอื่นโดยปราศจากอำนาจก็เป็นความผิดด้วย (มาตรา ๘ [๑๒๘] สำหรับการก่อวินาศกรรมระบบไม่ว่าด้วยวิธีการใด ๆ จะมีความผิดตามมาตรา ๑๐[๑๒๙] แต่ถ้าผู้กระทำบิดเบือนหรือเปลี่ยนแปลงข้อมูลของบุคคลอื่นก็มีความผิดตามมาตรา ๙[๑๓๐] ทั้งนี้ หากปรากฏว่า ระบบหรือข้อมูลที่ถูกกระทำหรือถูกโจมตีเหล่านั้นเป็นระบบหรือข้อมูลที่มีความสำคัญแก่ประเทศ เพราะเกี่ยวกับการรักษาความมั่นคงปลอดภัย ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจ บริการสาธารณะ หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อ

---

๑๒๖ มาตรา ๕ ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้น มิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

๑๒๗ มาตรา ๗ ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับไม่เกินสี่หมื่นบาทหรือทั้งจำทั้งปรับ

๑๒๘ มาตรา ๘ ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

๑๒๙ มาตรา ๑๐ ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

๑๓๐ มาตรา ๙ ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

ประโยชน์สาธารณะ ผู้กระทำความผิดต้องรับโทษหนักขึ้นตามมาตรา ๑๒[๑๓๑] แห่งพรบ. คอมพิวเตอร์ ฯ ในพระราชบัญญัติฉบับนี้ ยังกำหนดให้อำนาจพิเศษแก่พนักงานเจ้าหน้าที่อีกหลายประการ เพื่อค้นหา และรวบรวมพยานหลักฐานมาพิสูจน์ความผิด ไม่ว่าจะเป็น การสั่งให้ถอดรหัสคอมพิวเตอร์ การทำสำเนาข้อมูลคอมพิวเตอร์ การยึดเครื่องคอมพิวเตอร์ ฯลฯ และเพื่ออำนวยความสะดวกให้กับเจ้าพนักงาน โดยผลของกฎหมายฉบับนี้ ผู้ให้บริการอินเทอร์เน็ต และโทรคมนาคมทั้งหลาย ยังมีหน้าที่ต้องเก็บ "ข้อมูลจราจรทางคอมพิวเตอร์" หรือบรรดา Logfile ทั้งหลายไว้ไม่เกิน ๙๐ วัน โดยอาจต้องส่งมอบข้อมูลดังกล่าวหากเจ้าพนักงานร้องขอ อย่างไรก็ตาม กฎหมายฉบับนี้เป็นเพียงกฎหมายภายในเท่านั้น หรือกล่าวอีกอย่างก็คือ คงบังคับใช้ได้กับการกระทำที่เกิดขึ้นในประเทศ หรือหากจะเกิดขึ้นภายนอกประเทศ การดำเนินคดีกับผู้กระทำผิดก็จำเป็นต้องเป็นไปตามเงื่อนไขและกระบวนการอื่น ๆ อีกมากในทางระหว่างประเทศ เช่น การส่งผู้ร้ายข้ามแดน หรือข้อตกลงความร่วมมือในการสอบสวนคดีอาญา ฯลฯ จึงอาจกล่าวได้ว่าลำพังแต่เพียงกฎหมายภายใน ก็คงไม่อาจป้องกันและปราบปรามภัยคุกคามเหล่านี้ได้สมบูรณ์ หากแต่จำเป็นต้องอาศัยความร่วมมือระหว่างประเทศ ซึ่งในที่นี้หมายทั้งในระดับโลก และระดับภูมิภาคประกอบด้วย

อำนาจอธิปไตยของรัฐในโลกเสมือน

รัฐ คือ องค์ประกอบของสถาบันการปกครองและกลไกทางการเมืองโดยมีอำนาจอธิปไตยปกครองดินแดนทางภูมิศาสตร์ที่มีอาณาเขตและมีประชากรแน่นอน ตั้งแต่อดีตถึงปัจจุบัน ความสัมพันธ์ระหว่างรัฐกับประชาชนสามารถจัดแบ่งลักษณะได้ ๓ รูปแบบ คือ [๑๓๒]

---

๑๓๑ มาตรา ๑๒ ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐

(๑) ก่อให้เกิดความเสียหายแก่ประชาชน ไม่ว่าความเสียหายนั้นจะเกิดขึ้นในทันทีหรือในภายหลัง และไม่ว่าจะเกิดขึ้นพร้อมกันหรือไม่ ต้องระวางโทษจำคุกไม่เกินสิบปี และปรับไม่เกินสองแสนบาท

(๒) เป็นการกระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท ถ้าการกระทำความผิดตาม (๒) เป็นเหตุให้ผู้อื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่สิบปีถึงยี่สิบปี

๑๓๒ วิวัฒน์ เอี่ยมไพรวัน, "กฎเกณฑ์ทางการเมืองแนวใหม่ของการเมืองไทยกับความสัมพันธ์ทางอำนาจระหว่างรัฐกับประชาชน ", พ.ศ.๒๕๔๕

๑. รูปแบบความสัมพันธ์แบบผู้ปกครองกับผู้ถูกปกครอง (Ruler and Ruled)

๒. รูปแบบความสัมพันธ์แบบการปกครองโดยผู้แทน (Representative Government)

๓. รูปแบบความสัมพันธ์ของการเมืองแบบมีส่วนร่วม (Participative Politics)

จะเห็นได้ว่าในพัฒนาการระหว่างรัฐกับประชาชน รัฐ ผู้ปกครองรัฐ รวมถึงรัฐบาล ถูกลดบทบาทและความสำคัญให้เหลือน้อยลงไปเรื่อย ๆ อำนาจรัฐจะถูกกระจายไปยังประชาชนมากขึ้น ทำให้ประชนมีส่วนร่วมในการตัดสินใจในนโยบายต่าง ๆ ของรัฐมากขึ้น อีกทั้งรูปแบบของรัฐเองก็มีแนวโน้มที่จะเป็นไปในลักษณะการกระจายอำนาจมากกว่าจะเป็นการรวมศูนย์[๑๓๓ ๑๓๔]โดยเป้าหมายการกระจายอำนาจเป็นไปเพื่อความสะดวกรวดเร็วในการบริหารท้องถิ่น และเพื่อให้การดำเนินการของภาครัฐตรงตามความต้องการที่แตกต่างกันของประชากรในแต่ละท้องถิ่นให้มากที่สุด

นอกจากอำนาจรัฐจะถูกกระจายตัวไปยังประชากรของรัฐแล้ว ในภาพกว้างยังมีการรวมกลุ่มของรัฐเกิดขึ้นเพื่อผลประโยชน์ทางเศรษฐกิจและการเมือง และในการรวมกลุ่มของรัฐ แต่ละรัฐในกลุ่มรัฐต้องผ่องถ่ายอำนาจรัฐบางอย่างไปสู่กลุ่มรัฐ ตัวอย่างที่เห็นเด่นชัดที่สุดคือการรวมตัวกันเป็น "สหภาพยุโรป" ที่ประเทศสมาชิกต้องผ่องถ่ายอำนาจอธิปไตยของรัฐบางอย่างไปให้สหภาพยุโรป[๑๓๕] เช่น อำนาจอธิปไตยในการกำหนดสกุลเงิน อำนาจอธิปไตยในการผ่านเขตแดน (โดยเฉพาะอย่างยิ่งประเทศในเขต Schengen)[๑๓๖] อำนาจศาลและการออกกฎหมาย เป็นต้น

---

๑๓๓ B.C. Smith, "Decentralization : the territorial dimension of the state", Allen & Unwin, London, U.K., พ.ศ. ๒๕๒๘

๑๓๔ กระทรวงมหาดไทย, "สรุปสำหรับผู้บริหารเรื่อง การกระจายอำนาจการปกครองท้องถิ่นของประเทศไทย", สรุปสำหรับผู้บริหารเรื่อง การกระจายอำนาจการปกครองท้องถิ่นของประเทศไทย James A. Caporaso, "The European Union and Forms of State: Westphalian, Regulatory or Post-Modern?", JCMS: Journal of Common Market Studies, Volume 34, Issue 1, pages 29–52, มี.ค. ๒๕๓๙

๑๓๕ James A. Caporaso, "The European Union and Forms of State: Westphalian, Regulatory or Post-Modern?", JCMS: Journal of Common Market Studies, Volume 34, Issue 1, pages 29–52, มี.ค. ๒๕๓๙

๑๓๖ สหภาพยุโรป, "Schengen Area",. (Online).Available:http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/schengen/index_en.htm

ประชาคมเศรษฐกิจอาเซียน (AEC) ที่มีประเทศไทยเป็นประเทศสมาชิกก็มีแนวคิดเช่นเดียวกับสหภาพยุโรปในการรวมกลุ่มประเทศ [๑๓๗]

จากแนวโน้มที่เป็นปัจจัยภายในคือการจัดโครงสร้างแบบกระจายอำอาจรัฐ และจากปัจจัยภายนอกคือการจัดตั้งกลุ่มประเทศ ทำให้สามารถคาดการณ์ได้ว่าบทบาทของในอนาคตจะถูกลดทอนลง และด้วยเทคโนโลยีสารสนเทศ ที่ทำให้ประชากรทั่วโลกติดต่อกันได้อย่างไร้พรมแดน การแลกเปลี่ยนข้อมูล สินค้า ศิลปะและวัฒนธรรม เกิดขึ้นได้โดยไม่มีเขตแดนเป็นเครื่องกีดขวาง จะกลายเป็นสิ่งเร้า เร่งให้กระบวนการลดทอนอำนาจรัฐเกิดเร็วขึ้น จนในที่สุดเขตแดนในการแบ่งประเทศจะเลือนลางจนแทบมองไม่เห็น การใช้ชีวิตของคนในเขต Schengen อันประกอบด้วยประเทศต่าง ๆ ในทวีปยุโรปจำนวน ๒๖ ประเทศ ก็พอจะทำให้จินตนาการออกถึงความเลือนลางของเส้นแบ่งประเทศ ในพื้นที่ซึ่งประชาการในแต่ละประเทศสามารถเดินทางไปมาระหว่างประเทศได้ โดยไม่มีการตรวจตราใด ๆ จากภาครัฐและเมื่อถึงจุดหนึ่งแนวคิดของรัฐในฐานะ "กลไกทางการปกครอง" จะกลายสภาพไปเป็น "กลไกเพื่อการรับรองและอำนวยการ" เนื่องเพราะในสภาวะที่บทบาทของรัฐลดลงอย่างถึงที่สุด ประชากรแห่งรัฐ หรือองค์กรภาคเอกชนยังคงต้องการหน่วยงานที่สามารถรับรองความน่าเชื่อถือขององค์กรอื่น ๆ และหน่วยงานที่ให้การสนับสนุนด้านสาธารณูปโภคพื้นฐานได้ ซึ่งหน่วยงานที่เหมาะสมที่สุดคือหน่วยงานภาครัฐสภาวะอย่างหนึ่งที่ทำให้เห็นสภาวะการถูกลดอำนาจของภาครัฐมากขึ้น คือ การทำการค้าผ่านอินเตอร์เน็ตในลักษณะ e-commerce จากเดิมที่รัฐสามารถเก็บภาษีจากการค้าขายระหว่างประเทศได้จำนวนมหาศาล จากการควบคุมการขนส่งสินค้าผ่านทางท่าเรือและสนามบิน โดยบริษัทที่ต้องการนำเข้าหรือส่งออกสินค้าต้องแจ้งให้ทางภาครัฐรับรู้ แต่เมื่อเกิดกลไกทางการตลาดแบบ e-commerce ทำให้ภาครัฐควบคุมการเก็บภาษีได้ยากขึ้น การสั่งซื้อสินค้าสามารถทำได้โดยผ่านเว็บไซต์ของผู้ขาย การขนส่งสินค้าทำโดยไปรษณีย์ หรือบริษัทรับส่งสินค้า การที่ทางภาครัฐเข้าไปตรวจสอบ จะเจอกับข้อกล่าวหาในเรื่องของการละเมิดความเป็นส่วนตัว ดังนั้นหลายประเทศเริ่มมีการปรับตัวในเรื่องนี้ และมีกระบวนการป้องกันที่เป็นรูปธรรม หากไม่มีมาตรการที่เหมาะสมหรือดีพอ สภาพดังกล่าวจะทำให้รัฐสูญเสียอำนาจรัฐในเรื่องการค้าและพาณิชย์โดยปริยาย

สำหรับในหลายประเทศ สื่อถือเป็นกลไกหนึ่งที่ใช้ในการรักษาอำนาจรัฐ แม้ในประเทศที่สนับสนุนเสรีภาพสื่ออย่างเต็มที่ รัฐยังใช้สื่อเป็นเครื่องมือในการประชาสัมพันธ์และผลักดันนโยบายรัฐ มิพักต้องพูดถึงในประเทศที่เสรีภาพสื่อไม่ได้รับการคุ้มครองมากนัก สื่อมักถูกใช้เป็นเครื่องมือในการดำรงอำนาจของผู้ปกครองรัฐอย่างเต็มรูปแบบ แต่ด้วยเทคโนโลยีสารสนเทศ

---

๑๓๗ Mario Telò, "European Union and new regionalism: regional actors and global governance in a post-hegemonic era", Ashgate Publishing Limited, Berlington, U.S.A., พ.ศ. ๒๕๕๐

และโซเชียลเน็ตเวิร์ค ทำให้สื่อเดิมถูกลดบทบาทลง ประชาชนภายในรัฐสามารถมีส่วนร่วมในการสร้างเนื้อหาในสื่อใหม่หรือโซเชียลเน็ตเวิร์คมากขึ้น จนอาจเรียกว่าเสรีภาพในสื่อใหม่แทบไร้ข้อจำกัดและการควบคุม ดังนั้น ประชาชนในรัฐจึงมีเครื่องมือในการต่อรองกับผู้ปกครองในรัฐมากขึ้น โดยเฉพาะอย่างยิ่งในด้านการกำหนดและตรวจสอบนโยบายรัฐ ประชาชนสามารถรวมตัวกันเพื่อตรวจสอบกันได้ง่ายขึ้น หรือยิ่งไปกว่านั้น ในกรณีของ Arab Spring เราจะเห็นได้ว่าโซเชียลเน็ตเวิร์คกลายเป็นเครื่องมือที่สามารถล้มอำนาจรัฐหรือผู้ปกครองรัฐเสียด้วยซ้ำ

การก่อการร้ายถือเป็นอีกภัยคุกคามที่ส่งผลต่ออำนาจรัฐอย่างมาก จากในบท "การก่อการร้าย กับการการสร้างกองกำลังผ่านและในโลกเสมือนจริง" จะเห็นได้ว่า เทคโนโลยีสารสนเทศได้ถูกนำมาใช้ในกระบวนการการก่อการร้ายทั่วโลกอย่างกว้างขวาง การขาดการเตรียมพร้อมของรัฐหรือหน่วยงานความมั่นคงภายในรัฐด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศ อาจกลายเป็นช่องว่างในการโจมตีของผู้ก่อการร้าย ในขณะเดียวกัน อินเตอร์เน็ตในฐานะเครื่องมือของการก่อการร้าย ถูกนำมาใช้งานในลักษณะของการแลกเปลี่ยนข้อมูลและการติดต่อสื่อสาร การป้องกันภัยจากการก่อการร้ายในลักษณะดังกล่าวเป็นเรื่องที่ทำได้ยาก เพราะจะกระทบต่อสิทธิเสรีภาพของประชาชนในรัฐ จนถึงปัจจุบันประเทศต่าง ๆ ยังไม่มีมาตรการที่ลงตัวระหว่างการป้องกันภัยที่มาจากการก่อการร้ายผ่านอินเตอร์เน็ต และการรักษาสิทธิเสรีภาพของประชาชนในรัฐ

บทที่ ๔
แนวทางการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศไทยในอนาคต

วิเคราะห์ภัยคุกคามที่มีผลกระทบต่อความมั่นคงของประเทศ

จากเหตุการณ์สำคัญที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางสารสนเทศ และภัยคุกคามรูปแบบต่างๆ ที่กล่าวถึงในบทที่ ๒ และ ๓ สามารถจำแนกประเภทของภัยคุกคามที่มีผลกระทบต่อความมั่นคงของประเทศ ได้เป็น ๔ ประเภทใหญ่ๆ ได้แก่

๑. ภัยคุกคามต่อความมั่นคงทางเศรษฐกิจ โดยส่วนใหญ่จะเป็นภัยคุกคามที่มีผลกระทบกับเศรษฐกิจ เช่น ความผิดฐานฉ้อโกง ซึ่งเติบโตควบคู่มากับธุรกิจออนไลน์ การทำธุรกรรมทางอิเล็กทรอนิกส์ การปลอมแปลงข้อมูลทางคอมพิวเตอร์หลายคดีผู้กระทำมิได้มุ่งหมายเพื่อผลประโยชน์ในทางทรัพย์สิน หรือสร้างความเสียหายด้านเศรษฐกิจ อาชญากรรมคอมพิวเตอร์ รวมถึงการกระทำความผิดในเรื่องอื่นๆ ซึ่งจะกระทบกับความมั่นคงด้านเศรษฐกิจ

๒. ภัยคุกคามต่อสังคมและจิตวิทยา เช่น การละเมิดต่อสิทธิความเป็นส่วนตัว การขโมยข้อมูลส่วนบุคคลเพื่อผู้กระทำความผิดจะนำไปใช้ข่มขู่ หรือเรียกร้องเงิน หรือผลประโยชน์อื่นใดจากเจ้าของข้อมูล การชุมนุมทางการเมืองโดยใช้สื่อโซเชียลเน็ตเวิร์คเผยแพร่ข้อมูลข่าวสาร ส่งผลกระทบในวงกว้างต่อสังคมและจิตวิทยาของคนในประเทศ เป็นต้น

๓. ภัยคุกคามต่อความมั่นคงทางทหาร ดังจะเห็นได้จากเหตุการณ์สำคัญอันเกี่ยวเนื่องกับการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศต่างๆ ไม่ว่าจะเป็น ปฏิบัติการ Orchard การโจมตีทางไซเบอร์ของประเทศต่างๆ การทำลายเครื่องหมุนเหวี่ยงสำหรับสกัดสารกัมมันตภาพรังสีใช้ในอาวุธนิวเคลียร์โดยใช้ไวรัส Stuxnet เป็นต้น

๔. ภัยคุกคามในรูปแบบการก่อการร้าย เช่น สงครามปฏิบัติการจิตวิทยา สื่อสาธารณะและการโฆษณาชวนเชื่อ โดยอาศัยช่องทางการสื่อสารโซเชียลมีเดีย การเชื่อมโยงเครือข่ายของกลุ่มก่อการร้ายต่างๆถึงกันโดยใช้อินเตอร์เน็ต การสร้างกองกำลังในโลกเสมือนจริง เป็นต้น

ปัญหาและผลกระทบต่อการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศไทย

ปัญหาและผลกระทบต่อการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศไทยนั้น จำเป็นต้องวิเคราะห์และจำแนกประเภทของภัยคุกคามที่เกิดขึ้น และหาสาเหตุของปัญหา รวมทั้งผลกระทบที่เกิดขึ้น เพื่อหาแนวทางในการแก้ไขปัญหาให้ได้ผลเป็นรูปธรรม ดังนี้

๑. ด้านการบริหารจัดการการรักษาความมั่นคงปลอดภัย

จากการศึกษาแนวโน้มและวิเคราะห์ภัยคุกคามที่มีผลกระทบต่อความมั่นคงปลอดภัยทางสารสนเทศของประเทศ จึงทำให้ประเทศไทยได้กำหนดแนวทางการบริหารจัดการอย่างเป็นระบบเพื่อสร้างภูมิคุ้มกันด้านความมั่นคงปลอดภัยทางสารสนเทศให้มีความเข้มแข็ง โดยการดำเนินการเตรียมความพร้อมในการรับมือกับภัยคุกคามด้านสารสนเทศของประเทศที่ผ่านมานั้นรัฐบาลไทยได้มีการแต่งตั้งคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Committee : NCSC) ซึ่งมีนายกรัฐมนตรีเป็นประธาน และมีหน่วยงานที่เกี่ยวข้องด้านความมั่นคง กระบวนการยุติธรรม และด้านเศรษฐกิจ ร่วมเป็นกรรมการฯ มีหน้าที่หลักในการจัดทำนโยบายความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อให้ประเทศไทยมีขีดความสามารถในการปกป้อง ป้องกัน รับมือ และลดความเสี่ยงจากสถานการณ์ด้านภัยคุกคามในไซเบอร์ ที่กระทบต่อความมั่นคงของชาติทั้งจากภายในและภายนอกประเทศ ครอบคลุมถึงความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ และความมั่นคงทางเศรษฐกิจ นอกจากนี้ยังได้กำหนดยุทธศาสตร์หลัก ๓ ด้าน ยุทธศาสตร์รอง ๕ ด้าน เพื่อเป็นกรอบในการพัฒนาการรักษาความมั่นคงปลอดภัยทางสารสนเทศสำหรับประเทศไทยในอีก ๕ ปีข้างหน้า

อย่างไรก็ตามการดำเนินการตามยุทธศาสตร์ของคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ยังไม่ได้กำหนดหน่วยงานใดเป็นหน่วยงานหลักมารองรับการดำเนินการของคณะกรรมการดังกล่าวให้เห็นผลเป็นรูปธรรม เพื่อดำเนินการบูรณาการงานด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศให้สามารถแปลงนโยบายและยุทธศาสตร์ของคณะกรรมการฯ มาสู่การปฏิบัติได้อย่างต่อเนื่องและมีประสิทธิผล ทั้งนี้หน่วยงานต่างๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางสารสนเทศ ได้แก่ กระทรวงกลาโหม (กห.) กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (ทก.: เช่น สพธอ.และสำนักป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศ) กระทรวงวิทยาศาสตร์และเทคโนโลยี (วท.) สำนักงานตำรวจแห่งชาติ (สตช.: เช่น กลุ่มงานตรวจสอบและวิเคราะห์การกระทำความผิดทางเทคโนโลยี กองบังคับการสนับสนุนทางเทคโนโลยี (บก.สสท.) และกองบังคับการปราบปรามการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.)) และหน่วยงานด้านการวิจัย ได้แก่ กห.(สำนักงานเทคโนโลยีป้องกันประเทศ (สทป.)) วท.(ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

(NECTEC)) รวมทั้งหน่วยงานที่เกี่ยวข้องกับไซเบอร์เกตเวย์ของประเทศ ได้แก่ ทก.(ทีโอที และ กสท) ก็ยังขาดการบูรณาการงานในภาพรวมของการดำเนินการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางสารสนเทศ โดยยังเป็นการดำเนินการแบบเอกเทศทั้งในระดับนโยบายและระดับปฏิบัติการเพื่อรองรับภารกิจของแต่ละกระทรวงหรือหน่วยงานตนเองเท่านั้น ทำให้ขาดศักยภาพ ในการดำเนินการรับมือกับภัยคุกคามรูปแบบต่างๆ ไม่ว่าจะเป็นภัยคุกคามที่เกิดขึ้นในสภาวะวิกฤติของประเทศ ภัยคุกคามทั้งทางเศรษฐกิจ สังคม ทางการทหาร

ด้านวงการทหาร นายกรัฐมนตรี/รัฐมนตรีว่าการกระทรวงกลาโหม ได้อนุมัติหลักการจัดตั้ง ศูนย์ปฏิบัติการไซเบอร์กลาโหมขึ้น กองบัญชาการกองทัพไทย กองทัพบก กองทัพเรือ และกองทัพอากาศ เตรียมจัดตั้งหน่วยงานด้านไซเบอร์โดยตรง เพื่อขึ้นมารองรับการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยของประเทศ อย่างไรก็ตามยังไม่มีผลการดำเนินการใดๆ ที่เป็นรูปธรรมที่ชัดเจน เนื่องจากบุคลากรด้านไซเบอร์ของกระทรวงกลาโหมมีจำนวนจำกัด สามารถดำเนินการได้เพียงการดำเนินการในเชิงรับ การดำเนินการเชิงรุกจำเป็นต้องสร้างนักแฮกเกอร์ในระดับประเทศขึ้น รวมทั้งต้องมีห้องปฏิบัติการและเครื่องมือจำนวนมาก ซึ่งจำเป็นต้องใช้งบประมาณจำนวนมาก

หน่วยงานที่กล่าวมาแล้วทั้งหมดของไทยยังขาดการบูรณาการงานในภาพรวม ดังจะเห็นได้จากการดำเนินการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางสารสนเทศ ยังเป็นการดำเนินการแบบแยกส่วน แยกทั้งในระดับนโยบายและระดับปฏิบัติการเพื่อรองรับภารกิจของแต่ละกระทรวงหรือหน่วยงาน มีการจัดซื้ออุปกรณ์ในลักษณะต่างคนต่างทำ ทำให้ขาดศักยภาพในการดำเนินการรับมือกับภัยคุกคามรูปแบบต่างๆ จึงมีความจำเป็นต้องมีการบูรณาการงานในภาพรวมของการดำเนินการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางสารสนเทศ โดยบูรณาการทั้งในระดับนโยบายและระดับปฏิบัติการเพื่อขับเคลื่อนการดำเนินการให้ตอบสนองและสอดคล้องกับยุทธศาสตร์ของคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้อย่างต่อเนื่องและได้ประสิทธิผลสูงสุด

๒. ด้านบุคลากร

ประเทศไทยยังอยู่ในระดับต่ำทั้งภาครัฐ (ฝ่ายพลเรือน และฝ่ายความมั่นคง) และภาคเอกชน ซึ่งดูได้จากตัวชี้วัดเช่น จำนวนบุคลากร ที่มีความเชี่ยวชาญด้านไซเบอร์ ที่ผ่านเกณฑ์ได้รับใบรับรองความสามารถด้านไซเบอร์เป็นการเฉพาะ ทั้งนี้สาเหตุหลักประการหนึ่งคือขาดการสนับสนุนในเชิงนโยบาย อีกตัวชี้วัดหนึ่งคือปริมาณการโจมตีทางไซเบอร์ที่มีแนวโน้มที่เพิ่มขึ้นอย่างต่อเนื่อง ตามที่หน่วยงานที่เกี่ยวข้องได้รายงาน ซึ่งแสดงให้เห็นว่า ผู้ดูแลระบบไม่ทราบหรือไม่มีความสามารถในการป้องกันการโจมตี ส่งผลให้ระบบดังกล่าวถูกนำไปใช้ประโยชน์เป็นฐานการโจมตีระบบอื่นต่อไป

การสร้างศักยภาพของบุคลากรให้มีขีดความสามารถด้านสงครามไซเบอร์ในระดับประเทศ จำเป็นต้องได้รับการส่งเสริมทั้งในระดับนโยบายและปฏิบัติการ ต้องมีการบูรณาการทั้งด้านการบริหารจัดการบุคลากรที่มีจำนวนจำกัด รวมทั้งการส่งเสริมสร้างนักวิจัยด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศ

๓. กฎหมายและ พ.ร.บ.ที่เกี่ยวข้อง

พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ เป็นกฎหมายที่ถูกตราขึ้น เพราะในปัจจุบันระบบคอมพิวเตอร์ได้เป็นส่วนสำคัญของการประกอบกิจการและการดำรงชีวิตของมนุษย์ สำหรับ พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๔๔ เป็นกฎหมายที่ตราขึ้นเพื่อรองรับการนำระบบเทคโนโลยีสารสนเทศเข้ามาใช้ในการดำเนินกิจกรรมในทางแพ่งและพาณิชย์ รวมถึงการดำเนินงานของรัฐที่ใช้วิธีการทางอิเล็กทรอนิกส์

กฎหมายทั้งสองฉบับยังไม่สามารถรองรับภัยคุกคามด้านสงครามจิตวิทยา การเมือง รวมทั้งภัยคุกคามอื่นๆ ไม่ว่าจะเป็นทางด้านการทหาร การรับมือกับการก่อการร้าย สังคมและจิตวิทยา ดังตัวอย่างที่เห็นชัดเจนที่สุดคือการชุมนุมทางการเมืองในประเทศไทยที่ผ่านมา มีทั้งการใช้งานโซเชียลมีเดียเพื่อชักจูงให้ประชาชนเข้าร่วมการชุมนุมทางการเมือง ส่งผลกระทบโดยตรงกับความมั่นคงของประเทศ ทั้งนี้เนื่องจากการกระทำความผิดในปัจจุบันผ่านทางเครือข่ายสารสนเทศ พบว่ามีปัญหาการตรวจจับและควบคุมไม่ให้มีการกระทำความผิดเพิ่มมากขึ้น ทำได้ยากและใช้เวลานาน การค้นหาเว็บไซต์ที่เผยแพร่ข้อมูลที่ผิดกฎหมาย เช่นการหมิ่นสถาบันพระมหากษัตริย์ฯ การปลุกระดมทางการเมืองให้เกิดความขัดแย้ง แล้วทำการปิดกั้นเว็บไซต์ดังกล่าวใช้ระยะเวลานาน เมื่อดำเนินการตามกระบวนการกฎหมาย พบว่าไม่ได้ช่วยลดความเสียหายที่เกิดขึ้น รวมทั้งการจับกุมผู้กระทำความผิดเป็นไปได้ยากเนื่องจากมีการใช้เทคโนโลยีในการซ่อนพลางแหล่งที่มาของผู้กระทำความผิด ดังนั้นการตรวจสอบข้อมูลเนื้อหาผู้ใช้ในระหว่างที่มีการกระทำความผิดจึงเป็นช่องทางตรวจจับการกระทำความผิด รวมทั้งจะช่วยลดระยะเวลาการดำเนินการปิดกั้นลงได้

นอกจากนี้ช่องทางการเชื่อมต่อเครือข่ายอินเทอร์เน็ตภายในประเทศ กับเครือข่ายอินเทอร์เน็ตต่างประเทศผ่านหน่วยงานรัฐ ผู้ให้บริการอินเทอร์เน็ตทั้งภาครัฐ และเอกชน มีเป็นจำนวนมาก ดังนั้นการตรวจสอบการกระทำความผิด การทำ Lawful Interception การควบคุมการเผยแพร่ข้อมูลที่ผิดกฎหมายหรือมีผลกระทบต่อความมั่นคง รวมทั้งการป้องกันการโจมตีทางไซเบอร์ ทำได้ยาก หรือหากใช้กระบวนการของกฎหมายแจ้งให้ทุกผู้ให้บริการดำเนินการ ก็จะมีความล่าช้า

๔. โครงสร้างพื้นฐานของประเทศ

ในขณะที่อินเทอร์เน็ตกำลังเป็นเครื่องมือสำคัญสำหรับการพัฒนาความเจริญเติบโตทางเศรษฐกิจของทุกประเทศทั่วโลก และขณะเดียวกันอินเทอร์เน็ตกลายเป็นเวทีสำหรับการแลกเปลี่ยนความคิดเห็นของประชาชนในหลายประเทศทั่วโลก จากรายงานของ World Economic Forum แสดงให้เห็นว่าทั่วโลกกำลังวิตกกังวลกับภัยคุกคามด้านไซเบอร์เป็นอย่างมาก โดยภัยคุกคามด้านไซเบอร์ถูกจัดให้อยู่ในอันดับที่ ๔ ใน ๑๐ Trends ของโลก หลายประเทศรวมทั้งสหรัฐอเมริกาจึงให้ความสำคัญกับการปกป้องโครงสร้างพื้นฐานที่สำคัญของประเทศ (Critical Infrastructure Security) เพื่อให้เป็นแนวทางและมาตรฐานซึ่งครอบคลุมทั้งในระดับนโยบาย การจัดการองค์กร และ เทคโนโลยี เพื่อบริหารความเสี่ยงไซเบอร์ที่มีผลกระทบกับหน่วยงานโครงสร้างพื้นฐานสำคัญได้อย่างเหมาะสม สำหรับประเทศไทยตามยุทธศาสตร์ในข้อ ๓ กำหนด “การป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ ปกป้องโครงสร้างพื้นฐานสำคัญของประเทศและระบบสารสนเทศที่เกี่ยวข้อง” โดยมีเป้าหมายให้มีการกำหนดหลักเกณฑ์การเป็นโครงสร้างพื้นฐานสำคัญของประเทศ และรณรงค์ให้หน่วยงานหรือองค์กรที่เป็นโครงสร้างพื้นฐานสำคัญของประเทศตระหนักรู้ถึงความสำคัญและความเสี่ยงของตนเอง อย่างไรก็ตามยังไม่มีการดำเนินการกำหนดอุตสาหกรรมและระบบสาธารณูปโภคสำคัญที่เกี่ยวกับโครงสร้างพื้นฐานสำคัญของประเทศที่เป็นรูปธรรมและชัดเจน

นอกจากอุตสาหกรรมและระบบสาธารณูปโภคสำคัญที่เกี่ยวกับโครงสร้างพื้นฐานสำคัญของประเทศแล้ว จำเป็นต้องมีการดำเนินการสร้างการตรวจสอบและสกัดกั้นข้อมูลการจราจรทางอินเทอร์เน็ตตามกฎหมาย (Lawful Interception: LI) เป็นการตรวจสอบวิเคราะห์ข้อมูลการจราจรทางอินเทอร์เน็ตเพื่อการป้องกันโครงสร้างพื้นฐานสำคัญของประเทศ ซึ่งโดยทั่วไปแล้วในระบบเครือข่ายขององค์กร เจ้าหน้าที่ผู้รับผิดชอบดูแลระบบสารสารสนเทศและเครือข่ายมีสิทธิ์เต็มที่ ในการตรวจสอบข้อมูลการจราจรทางอินเทอร์เน็ตที่ผ่านเข้าและออกจากเครือข่ายองค์กรของตนตราบใดที่ไม่นำข้อมูลส่วนบุคคลไปใช้ประโยชน์ในทางที่ผิด ซึ่งที่ผ่านมาจะเห็นได้ว่าเมื่อประเทศเกิดภาวะวิกฤต เช่นการชุมนุมทางการเมือง การสื่อสารผ่านโซเชียลเน็ตเวิร์คของกลุ่มผู้ชุมนุมทางการเมือง หน่วยงานรับผิดชอบ เช่นสำนักป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศ ทก. ซึ่งมีอำนาจในการใช้กฎหมายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 กลับไม่สามารถดำเนินการใดๆได้เลย

วิเคราะห์การดำเนินการรักษาความมั่นคงปลอดภัยทางสารสนเทศของต่างประเทศ

จากปัญหาและผลกระทบต่อการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศไทยนั้น จึงจำเป็นต้องวิเคราะห์และเปรียบเทียบแนวทางในการดำเนินการของต่างประเทศเพื่อหาแนวทางในการแก้ไขปัญหาให้ได้ผลเป็นรูปธรรม ดังนี้

๑. ด้านการบริหารจัดการการรักษาความมั่นคงปลอดภัย

องค์กรในต่างประเทศ เช่น สำนักงานความมั่นคงแห่งชาติ (National Security Agency : NSA) ของประเทศสหรัฐอเมริกา เป็นหน่วยงานข่าวกรองที่มีขอบเขตหน้าที่ทั้งในและนอกประเทศ และเป็นหน่วยงานด้านข่าวกรองที่มีขนาดองค์กรที่ใหญ่ที่สุดของสหรัฐอเมริกา มีหน้าที่ในการเฝ้าระวัง ตรวจสอบ ถอดรหัสและประมวลผลข้อมูลอิเล็กทรอนิกส์ รวมถึงรักษาความมั่นคงปลอดภัยในการรับส่งข้อมูลระหว่างหน่วยงานภาครัฐของสหรัฐอเมริกา NSA มีขีดความสามารถด้านสงครามไซเบอร์หลายด้าน ทั้งในด้านของการป้องกันภัยจากไซเบอร์ การโจรกรรมข้อมูลทางไซเบอร์และการเข้ารหัส ถอดรหัสข้อมูล โดยเฉพาะอย่างยิ่งในส่วนของการเข้ารหัสและถอดรหัสข้อมูล มีกฎหมายรองรับสามารถดักฟังและประมวลผลข้อมูลสารสนเทศที่ถูกส่งผ่านอินเตอร์เน็ตได้เกือบทั้งหมด ข้อมูลเหล่านั้นถูกเก็บรักษาโดยผู้ให้บริการสัญชาติสหรัฐอเมริกา เช่น Facebook Google และ Microsoft เป็นต้น

สำหรับหน่วยงาน United States Cyber Command (USCYBERCOM) เป็นหน่วยงานทางทหารของสหรัฐอเมริกาที่มีหน้าที่ “วางแผน ประสานงาน รวบรวม ประสานความสอดคล้องและดำเนินการในการอำนวยการปฏิบัติการและป้องกันหน่วยงานที่เกี่ยวข้องกับสารสนเทศและระบบเครือข่ายนอกจากนี้ยังมีหน้าที่ในการเตรียมความพร้อม และปฏิบัติการทางทหารด้านสงครามไซเบอร์อย่างเต็มกำลังเพื่อทำให้กองทัพสหรัฐอเมริกา และพันธมิตรสามารถปฏิบัติการทางทหารได้ในทุกมิติรวมถึงประกันอิสรภาพในการดำเนินการรักษาความมั่นคงปลอดภัยทางสารสนเทศของกองทัพสหรัฐอเมริกา และป้องกันไม่ให้ฝ่ายตรงข้ามปฏิบัติการในแบบเดียวกัน” โดย USCYBERCOM เป็นหน่วยขึ้นตรงของ United States Strategic Command มีแนวคิดที่ตั้งเป็นหน่วยงานกลางด้านสงครามไซเบอร์สำหรับกองทัพสหรัฐอเมริกา เป็นหน่วยงานที่มีกฎหมายรองรับในการปฏิบัติการทางทหารสามารถปฏิบัติการในเชิงรุกนอกเหนืออาณาเขตของสหรัฐอเมริกาได้

ประเทศสหรัฐอเมริกามีบุคลากรด้านไซเบอร์จำนวนมาก จึงมีขีดความสามารถในการจัดตั้งหน่วยงาน NSA และ USCYBERCOM โดยทั้งสองหน่วยงานเป็นหน่วยงานขนาดใหญ่รับผิดชอบงานด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศสหรัฐอเมริกา รวมทั้งการปฏิบัติการทางทหารในเชิงรุกนอกเหนืออาณาเขตของสหรัฐอเมริกา

ประเทศสหพันธ์สาธารณรัฐเยอรมนี มีการก่อตั้ง “ศูนย์ความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ” หรือ Nationales Cyber-Abwehrzentrum (NCAZ) ขึ้นในปี ๒๕๔๔ เป็นหน่วยงานกลางที่มีหน้าที่ในการป้องกันภัยจากการโจมตีทางอิเล็กทรอนิกส์และไซเบอร์ ทั้งในแง่ความมั่นคงแห่งสหพันธ์สาธารณรัฐ และความมั่นคงในทางเศรษฐกิจ รวมถึงการรักษาความมั่นคงปลอดภัยทางสารสนเทศให้กับโครงสร้างพื้นฐานของเยอรมนี การดำเนินการของ NCAZ จะถูกกำหนดให้สอดคล้องกับ “ยุทธศาสตร์ทางไซเบอร์สำหรับเยอรมนี” ข้อสังเกตจากหน้าที่ของ NCAZ ที่สำคัญประการหนึ่งคือ การรักษาความมั่นคงทางเศรษฐกิจถูกระบุเพิ่มเติมจากหน้าที่อื่น ๆ อย่างชัดเจน แตกต่างจากหน่วยงานด้านสงครามไซเบอร์ของสหรัฐอเมริกา ที่ไม่ได้กล่าวถึงการรักษาความมั่นคงทางเศรษฐกิจในหน้าที่หลักของหน่วยงาน

นอกจากนี้ NCAZ เป็นหน่วยในสังกัดกระทรวงมหาดไทย ทำให้เห็นเจตนาการจัดตั้ง NCAZ อย่างชัดเจนว่ามีขึ้นเพื่อรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับกิจการภายใน มากกว่าจะเป็นการดำเนินการทางไซเบอร์ในเชิงรุก ซึ่งแตกต่างกับสหรัฐอเมริกาโดยโครงสร้างของ NCAZ ถือเป็นหน่วยงานเฉพาะกิจที่ไม่สามารถดำเนินกิจการด้วยตนเอง หรือมีเจ้าหน้าที่สังกัดหน่วยโดยตรง เนื่องด้วยข้อกำหนดตามกฎหมายรัฐธรรมนูญของเยอรมนี ทำให้ลักษณะการดำเนินการของ NCAZ เป็นการดำเนินการร่วมระหว่างเจ้าหน้าที่จากหน่วยงานต่าง ๆ ด้วยลักษณะการจัดโครงสร้างที่เป็นการดำเนินการร่วมเพื่อรับมือกับภัยคุกคามในรูปแบบต่างๆ ทำให้ NCAZ ถูกวิจารณ์ว่าไม่น่าจะมีศักยภาพพอที่จะสามารถป้องกันภัยคุกคามทางไซเบอร์ให้กับสหพันธ์สาธารณรัฐเยอรมนีได้ และหลังจากที่ NCAZ เริ่มปฏิบัติภารกิจได้ไม่นาน เครื่องคอมพิวเตอร์แม่ข่ายของสรรพากร ซึ่งเป็นหน่วยงานที่ NCAZ รับผิดชอบดูแลความมั่นคงปลอดภัยทางสารสนเทศ ถูกเจาะระบบเครือข่ายเข้าไปได้

ทั้งนี้ในการจัดโครงสร้างองค์กรของ NCAZ เพื่อรับมือกับภัยคุกคามในรูปแบบต่างๆ นั้นมีลักษณะคล้ายคลึงกับการบริหารจัดการในประเทศไทยซึ่งเกี่ยวข้องกับหลายกระทรวง ภายใต้การกำกับของคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ซึ่งมีนายกรัฐมนตรีเป็นประธาน และมีหน่วยงานที่เกี่ยวข้องด้านความมั่นคง กระบวนการยุติธรรม และด้านเศรษฐกิจ ร่วมเป็นกรรมการฯ จึงเห็นได้ว่าลักษณะการจัดโครงสร้างที่เป็นการดำเนินการเฉพาะกิจ ที่ไม่สามารถดำเนินกิจการด้วยตนเอง ยังไม่สามารถนำมาเป็นแนวทางในการแก้ไขปัญหาของประเทศไทยได้

สำหรับการจัดตั้งหน่วยสำหรับการรักษาความมั่นคงปลอดภัยทางสารสนเทศของจีนไม่ได้รับการเปิดเผยต่อสาธารณะมากนัก อย่างไรก็ตามจากเหตุการณ์อันเกี่ยวข้องกับสงครามไซเบอร์ที่ผ่านมาแสดงให้เห็นว่าจีนมีความตื่นตัวเกี่ยวกับสงครามไซเบอร์ที่สูงมาก จากการวิเคราะห์ทำให้เชื่อได้ว่าหลังจากที่จีนได้เห็นปฏิบัติการ “พายุทะเลทราย”ในสงครามอ่าวครั้งที่หนึ่ง ในช่วงปี

๒๕๓๓ ทำให้จีนเริ่มตระหนักถึงความสำคัญของสงครามไซเบอร์มากขึ้น ในปฏิบัติการทางทหารดังกล่าวกองทัพสหรัฐอเมริกา ได้นำเทคโนโลยีสารสนเทศมาใช้ร่วมกับอาวุธยุทโธปกรณ์อื่น ๆ ทำให้การปฏิบัติมีความเที่ยงตรง แม่นยำมากขึ้นใช้งบประมาณในภาพรวมที่น้อยลง

ก่อนหน้าปฏิบัติการพายุทะเลทราย จีนมีความพยายามในการพัฒนาขีดความสามารถกองทัพ ด้วยการเพิ่มปริมาณอาวุธ และกองกำลังทางทหาร เพื่อผลักดันให้ตนเองเป็นหนึ่งในมหาอำนาจทางการทหาร แต่เนื่องจากเศรษฐกิจของจีนในช่วงเวลาดังกล่าวไม่ได้แข็งแกร่งมากนัก หลังจากปฏิบัติการพายุทะเลทราย จีนจึงมองเห็นช่องทางในการพัฒนาขีดความสามารถของกองทัพให้รวดเร็วกว่าเดิม แต่ใช้งบประมาณน้อยลงกว่าเดิม และแนวทางการพัฒนาขีดความสามารถของกองทัพจีนหลังจากนั้นจะอยู่ภายใต้กรอบนโยบาย “สงครามอสมมาตร” ที่จีนพยายามใช้ความรู้ และผลงานวิจัยทางด้านเทคโนโลยีสารสนเทศมาปรับใช้กับกองทัพของตนในทุก ๆ ด้าน โดยผู้เชี่ยวชาญวิเคราะห์ว่าด้วยแนวทางสงครามอสมมาตรของจีน อาจทำให้ขีดความสามารถของกองทัพจีนขึ้นมาเทียบชั้นกับขีดความสามารถกองทัพสหรัฐอเมริกาได้

สำหรับแนวทางการพัฒนาขีดความสามารถของกองทัพจีนนั้นจะอยู่ภายใต้กรอบนโยบาย “สงครามอสมมาตร” โดยใช้ความรู้ และผลงานวิจัยทางด้านเทคโนโลยีสารสนเทศมาปรับใช้กับกองทัพของตนในทุก ๆ ด้าน ซึ่งน่าจะเป็นประโยชน์กับประเทศไทยในการรับมือกับภัยคุกคามในรูปแบบต่างๆ

จากการวิเคราะห์และเปรียบเทียบกับองค์กรในประเทศไทยกับต่างประเทศจะเห็นได้ว่าองค์กร NSA ของประเทศสหรัฐอเมริกา เป็นหน่วยงานข่าวกรองที่มีขอบเขตหน้าที่ทั้งในและนอกประเทศ มีขีดความสามารถด้านสงครามไซเบอร์หลายด้าน ทั้งในด้านของการป้องกันภัยจากไซเบอร์ การโจรกรรมข้อมูลทางไซเบอร์และการเข้ารหัส ถอดรหัสข้อมูล มีกฎหมายรองรับ สามารถดักฟังและประมวลผลข้อมูลสารสนเทศที่ถูกส่งผ่านอินเตอร์เน็ตได้เกือบทั้งหมด ดังนั้นเพื่อให้การรักษาความมั่นคงปลอดภัยทางสารสนเทศสำหรับประเทศไทยมีผลเป็นรูปธรรม จึงควรจัดตั้งหน่วยงานรักษาความมั่นคงปลอดภัยทางสารสนเทศแห่งชาติขึ้น เช่นเดียวกับ NSA ของประเทศสหรัฐอเมริกา มีหน้าที่ในการป้องกันภัยจากการโจมตีทางอิเล็กทรอนิกส์และไซเบอร์ ทั้งในแง่ความมั่นคงแห่งชาติและความมั่นคงในทางเศรษฐกิจ รวมถึงการรักษาความมั่นคงปลอดภัยทางสารสนเทศให้กับโครงสร้างพื้นฐานของประเทศ คล้ายกับหน้าที่ของหน่วยงาน NCAZ ประเทศสหพันสาธารณรัฐเยอรมนี โดยรวมการคนและเครื่องมือจากหน่วยงานต่างๆ ทั้ง ทก. กห. วท. สตช. ยธ. มท. และเป็นหน่วยขึ้นตรงกับนายกรัฐมนตรี ภายใต้การกำกับดูแลของคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติที่มีนายกรัฐมนตรีเป็นประธาน

สำหรับการจัดตั้งหน่วยบัญชาการไซเบอร์กลาโหมที่ทำหน้าที่รับมือกับภัยคุกคามด้านการทหารเป็นหลักโดยการรับมือจะเป็นในลักษณะทั้งในเชิงรับและเชิงรุกนั้น การดำเนินการดังกล่าวมีส่วนคล้ายคลึงกับการจัดตั้ง USCYBERCOM ของประเทศสหรัฐอเมริกา อย่างไรก็ตาม เนื่องจากบุคลากรด้านไซเบอร์ของกองทัพมีจำนวนจำกัด ความพร้อมของกระทรวงกลาโหมและเหล่าทัพในการดำเนินการด้านไซเบอร์ยังมีขีดความสามารถจำกัด และงบประมาณด้านไซเบอร์ยังมีจำนวนจำกัด รวมทั้งจำเป็นต้องศึกษาข้อกฎหมายระหว่างประเทศให้ชัดเจนในการดำเนินการเชิงรุก จึงควรให้หน่วยงานรักษาความมั่นคงปลอดภัยทางสารสนเทศแห่งชาติที่เสนอแนะให้จัดตั้งขึ้น เป็นหน่วยงานหลักในการดูแลงานด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศ และกำหนดขอบเขตการดำเนินการด้านไซเบอร์เชิงรุก ให้เป็นการดำเนินการป้องกันเชิงรุก โดยเน้นการดำเนินการหาข่าวด้านไซเบอร์กับประเทศต่างๆ การสแกนหาช่องโหว่ของระบบสารสนเทศ การเก็บข้อมูลและจัดทำฐานข้อมูลทำเนียบกำลังรบด้านไซเบอร์ การจำลองการฝึกอบรมการโจมตีเครือข่ายสารสนเทศ เป็นต้น

๒. บุคลากร

ในด้านทรัพยากรบุคคล ประเทศสหรัฐอเมริกาเป็นประเทศที่เป็นแหล่งรวมบุคลากรทางด้านเทคโนโลยีสารสนเทศเป็นจำนวนมาก ทั้งนี้จากการเปิดเผยผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยทางสารสนเทศได้ระบุว่า มีผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยทางสารสนเทศที่มีคุณวุฒิเพียงพออยู่ประมาณ ๔๐,๐๐๐ คน

สำหรับประเทศจีน แม้ว่าจะไม่มีการเปิดเผยข้อมูลอย่างเป็นทางการ และการเข้าถึงข้อมูลเกี่ยวกับกองทัพของจีนเป็นไปด้วยความยากลำบาก แต่มีหลักฐานบ่งชี้ว่า จีนมีการพัฒนาขีดความสามารถด้านเทคโนโลยีสารสนเทศของตนเองอยู่ตลอดเวลา และมีความพร้อมทางด้านสงครามไซเบอร์สูง และหลักฐานยังบ่งชี้อีกว่ามีการลอบโจรกรรมข้อมูลของหน่วยงานภาครัฐและเอกชนในสหรัฐอเมริกา และอินเดียจากระบบเครือข่ายในประเทศจีน แต่ด้วยลักษณะเฉพาะของระบบเครือข่ายและอินเตอร์เน็ต จึงเป็นเรื่องที่พิสูจน์ได้ยากว่าการโจรกรรมดังกล่าวกระทำโดยรัฐบาลจีน หรือองค์กรเอกชนที่สนับสนุนโดยรัฐบาลจีน

ประเทศเกาหลีเหนือได้หันมาให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยทางสารสนเทศควบคู่กับการพัฒนาอาวุธนิวเคลียร์อย่างจริงจัง มีการตั้งหน่วยงานที่มีภารกิจในการโจมตีด้านไซเบอร์โดยเฉพาะ หน่วยงานนั้นประกอบด้วย “หน่วย ๑๑๐” “หน่วย ๑๒๑” และ “หน่วย ๒๐๔” รวมมีผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยทางสารสนเทศ และแฮกเกอร์กว่า ๓,๐๐๐ คน และมีการสร้างบุคลากรด้านนี้ด้วยการคัดเลือกนักเรียนที่มีผลการเรียนดีตั้งแต่จบประถม ให้เข้าเรียนในหลักสูตรด้านอิเล็กทรอนิกส์และเทคโนโลยีสารสนเทศเฉพาะทาง ในระดับมัธยมต้นจนถึง

มหาวิทยาลัย บุคลากรเหล่านี้เมื่อจบการศึกษานอกจากจะทำงานให้กับหน่วยงานด้านสงครามไซเบอร์ ผู้ที่ได้รับการคัดเลือกบางคนยังได้รับมอบหมายให้ปฏิบัติภารกิจแทรกซึม และบ่อนทำลายทางด้านไซเบอร์ในประเทศเพื่อนบ้านอย่างญี่ปุ่นและเกาหลีใต้อีกด้วย

สำหรับความพร้อมด้านบุคลากรของประเทศไทย ซึ่งสามารถวัดได้จากจำนวนบุคลากรที่ได้รับใบรับรองความเชี่ยวชาญในสาขาวิชาชีพด้านความมั่นคงปลอดภัยด้านสารสนเทศที่ได้รับการยอมรับในระดับสากล เช่น ใบรับรอง Certified Information System Security Professional (CISSP) ซึ่งรับรองโดย ISC ผลการสำรวจเมื่อเดือนมีนาคม พ.ศ.๒๕๕๖ พบว่าทั่วโลกมีผู้ที่ได้รับใบรับรอง CISSP ๘๕,๒๘๕ คน จาก ๑๔๔ ประเทศ ประเทศที่มีผู้เชี่ยวชาญ CISSP สูงสุดคือสหรัฐอเมริกา (๕๕,๙๒๔ คน) อันดับที่สองคือสหราชอาณาจักร (๔,๒๕๖ คน) อันดับที่สามคือแคนาดา (๔,๐๗๕ คน) อันดับที่สี่คือเกาหลีใต้ ส่วนประเทศไทย (๑๕๓ คน) อยู่ในอันดับที่ ๓๔ ของโลก และเป็นอันดับที่สามในประชาคมอาเซียน รองจากสิงคโปร์ (๑,๑๓๒ คน) และมาเลเซีย (๒๓๙ คน)

จากข้อมูลจำนวนผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยด้านสารสนเทศของประเทศในภูมิภาคอาเซียน ถึงแม้ว่าจำนวนผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยด้านสารสนเทศ ประเทศไทยอยู่ในลำดับที่ ๓ และมีจำนวนสูงกว่าหลายประเทศในภูมิภาคอยู่ก็ตาม แต่เมื่อเปรียบเทียบกับประเทศในภูมิภาคอาเซียนที่ได้รับการยอมรับว่ามีความก้าวหน้าในด้านเทคโนโลยีสารสนเทศ เช่น ประเทศสิงคโปร์ และประเทศมาเลเซีย แล้ว จำนวนผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของไทยยังมีจำนวนน้อยกว่าอยู่อย่างมีนัยสำคัญ แสดงให้เห็นถึงความท้าทายในการส่งเสริมและพัฒนาทักษะผู้เชี่ยวชาญของไทยให้เป็นที่ยอมรับและได้รับการรับรองด้านความมั่นคงปลอดภัยด้านสารสนเทศในระดับสากล เพื่อรักษาระดับความเชื่อมั่นต่อการรักษาศักยภาพในการแข่งขันกับประเทศต่าง ๆ ในภูมิภาคนี้

จากข้อมูลข้างต้นจะเห็นได้ว่า บุคลากรถือเป็นปัจจัยที่ทวีความสำคัญเมื่อเทียบกับการรักษาความมั่นคงปลอดภัยทางด้านอื่น นอกจากนี้ความรู้ความสามารถของบุคลากรก็มีความสำคัญอย่างมากเช่นเดียวกัน เนื่องจากในสงครามไซเบอร์ฝ่ายที่มีความรู้ ความเข้าใจ ความชำนาญในเทคโนโลยีสารสนเทศย่อมมีความได้เปรียบกว่าเสมอ แม้ว่าปัจจัยทางด้านอื่นจะไม่เอื้ออำนวยก็ตาม ดังนั้นการสร้างและเตรียมความพร้อมบุคลากรในประเทศไทย รวมไปถึงการสร้างและบริหารจัดการองค์ความรู้จึงเป็นสิ่งแรกที่ต้องคำนึงถึงในการรักษาความมั่นคงปลอดภัยทางสารสนเทศ

โดยองค์กรต้องตระหนักเสมือนว่าภัยคุกคามทางสารสนเทศเป็นภัยคุกคามที่มีพลวัตรสูง ดังนั้น ความรู้ของบุคลากรจึงต้องมีพลวัตรที่สูงตามลักษณะของภัยคุกคามด้วย การดำเนินการ

แก้ไขปัญหาด้านบุคลากรที่สำคัญคือให้การสนับสนุนด้านการศึกษาวิจัย ทั้งนี้ การรักษาความปลอดภัยทางเทคโนโลยีสารสนเทศ ไม่สามารถเรียนรู้และติดตามความเปลี่ยนแปลงได้จากการศึกษาในระบบการศึกษาปกติ เพราะสถาบันการศึกษาไม่สามารถปรับเปลี่ยนหลักสูตรให้ทันความเปลี่ยนแปลงที่เกิดขึ้นได้ ดังนั้น การศึกษาหาความรู้ของบุคลากรควรหาจากสถานที่ที่เป็นแหล่งกำเนิดและศูนย์กลางของสงครามทางสารสนเทศ นั่นคืออินเตอร์เน็ต โดยองค์กรต้องให้การสนับสนุนและกระตุ้น การค้นหาความรู้ และติดตามความเคลื่อนไหวเกี่ยวกับความเปลี่ยนแปลงด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ

นอกจากนี้แล้วการสร้างความร่วมมือกับหน่วยงานด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศ รวมถึงหน่วยงานด้านการศึกษา ซึ่งเป็นการเสริมสร้างขีดความสามารถของทั้งองค์กรเอง และกับหน่วยงานที่ร่วมมือ โดยเฉพาะอย่างยิ่งหน่วยงานทางด้านการศึกษา ที่มีบุคลากรที่มีคุณภาพจำนวนมาก อีกทั้งเป็นแหล่งรวมของนักศึกษาที่สามารถเข้ามาเป็นส่วนหนึ่งขององค์กรในอนาคตได้ โดยภาพรวมแล้ว การร่วมมือกับหน่วยงานทางด้านการศึกษา จะช่วยลดต้นทุนในหลายด้าน เพราะหน่วยงานการศึกษาตามปกติแล้วเป็นหน่วยงานไม่แสวงผลกำไร หรือแสวงผลกำไรในระดับที่น้อยกว่าบริษัทเอกชน และเมื่อมองในแง่ของการพัฒนาบุคลากรขององค์กรด้วยการศึกษาวิจัย หน่วยงานทางด้านการศึกษาถือว่ามีความพร้อมอย่างมาก ทั้งสิ่งอำนวยความสะดวก บุคลากร และองค์ความรู้

๓. กฎหมายและ พ.ร.บ.ที่เกี่ยวข้อง

ในขณะที่ต่างประเทศ เช่นสหรัฐอเมริกา มีการออกกฎหมายที่มีชื่ออย่างไม่เป็นทางการว่า “Kill Switch Bill” ซึ่งเป็นกฎหมายที่ให้อำนาจประธานาธิบดีในการควบคุมอินเตอร์เน็ตในสถานการณ์ฉุกเฉิน และให้ความคุ้มครองโครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศในฐานะทรัพย์สมบัติของภาครัฐ โดยตัวอย่างของหน่วยงาน NSA ซึ่งมีขีดความสามารถด้านการเข้ารหัส ถอดรหัสข้อมูล โดยมีกฎหมายรองรับสามารถดักฟังและประมวลผลข้อมูลสารสนเทศที่ถูกส่งผ่านอินเตอร์เน็ตได้เกือบทั้งหมด

สำหรับองค์กร NCAZ ประเทศสหพันสาธารณรัฐเยอรมนี ได้เพิ่มงบประมาณ เพื่อใช้ในการรวบรวมข้อมูลการจราจรบนอินเตอร์เน็ตจากเดิมทำได้ร้อยละ ๕ ของปริมาณข้อมูลทั้งหมดให้เป็นร้อยละ ๒๐ ของปริมาณข้อมูลทั้งหมด

จากที่กล่าวมาแล้วข้างต้น จึงมีความจำเป็นที่ประเทศไทยต้องมีกฎหมายรองรับในการควบคุมและสกัดกั้นข้อมูลการจราจรทางอินเตอร์เน็ตในการเผยแพร่ข้อมูลที่ผิดกฎหมายหรือมีผลกระทบต่อความมั่นคง รวมทั้งการป้องกันการโจมตีทางไซเบอร์ เพื่อปกป้องทรัพย์สินของประเทศ รวมทั้งการดำเนินการใดๆที่มีผลกระทบต่อความมั่นคง นอกจากนี้การดำเนินการควบคุม

ยับยั้งการจราจรทางอินเตอร์เน็ตในการเผยแพร่ข้อมูลที่ผิดกฎหมายหรือมีผลกระทบต่อความมั่นคง จำเป็นต้องสร้างเกตเวย์ทางอินเตอร์เน็ตของประเทศขึ้นมา เพื่อทำหน้าที่ตรวจสอบ ระงับยับยั้งการดำเนินการที่มีผลกระทบต่อความมั่นคงของประเทศ

๔. โครงสร้างพื้นฐานของประเทศ

เนื่องจากการแก้ปัญหาด้านภัยคุกคามทางไซเบอร์อย่างจริงจังต้องการแนวทางอย่างเป็นระบบเพื่อการบริหารจัดการความเสี่ยงดังกล่าวได้อย่างมีประสิทธิภาพและประสิทธิผล รัฐบาลของประเทศสหรัฐอเมริกาภายใต้การบริหารของประธานาธิบดี บารัค โอบามา ได้มอบหมายให้สถาบันมาตรฐานและเทคโนโลยีแห่งสหรัฐอเมริกา (**NIST**) ทำการพัฒนากรอบดำเนินงานเพื่อปรับปรุงความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน ระบบโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure Security) เพื่อให้เป็นแนวทางและมาตรฐาน ซึ่งครอบคลุมทั้งในระดับนโยบาย การจัดการองค์กร และ เทคโนโลยี เพื่อบริหารความเสี่ยงไซเบอร์ ที่มีผลกระทบกับหน่วยงานโครงสร้างพื้นฐานสำคัญได้อย่างเหมาะสม

NIST ได้ทำการออกเวอร์ชั่นล่าสุดของกรอบการดำเนินงาน "National Cybersecurity Framework" เมื่อวันที่ ๑๒ กุมภาพันธ์ พ.ศ.๒๕๕๗ เป็นกรอบการดำเนินงานที่ประกอบด้วยสามองค์ประกอบหลักที่เรียกว่า "Framework Core", "Framework implementation Tiers" และ "Framework Profiles" เพื่อกำหนดแนวปฏิบัติที่ดีให้นำไปใช้ในการจัดการระบบของหน่วยงานในอุตสาหกรรมที่เกี่ยวกับโครงสร้างพื้นฐานสำคัญ ครอบคลุม ๑๖ กลุ่มสำคัญ ประกอบด้วย

๑. Chemical Sector
๒. Commercial Facilities Sector
๓. Communications Sector
๔. Critical Manufacturing Sector
๕. Dams Sector
๖. Defense Industrial Base Sector
๗. Emergency Services Sector
๘. Energy Sector
๙. Financial Services Sector
๑๐. Food and Agriculture Sector
๑๑. Government Facilities Sector
๑๒. Healthcare and Public Health Sector
๑๓. Information Technology Sector

๑๔. Nuclear Reactors, Materials, and Waste Sector

๑๕. Transportation Systems Sector

๑๖. Water and Wastewater Systems Sector

องค์ประกอบของ Framework Core เพื่อนำมาใช้ในการดำเนินการร่วมกัน ประกอบด้วย

๑. หน้าที่งาน (Functions) เป็นกิจกรรมพื้นฐานด้าน ความมั่นคงปลอดภัยไซเบอร์ในระดับภาพรวม ในเอกสารนี้ จำแนกเป็น ๕ functions (IPDRR: Identify, Protect, Detect, Respond, Recover)

๒. กลุ่มงาน (Categories) เป็นกลุ่มงานที่จำแนกตามผลลัพธ์ด้านความมั่นคงปลอดภัยไซเบอร์ อาทิ การจัดการทรัพย์สิน การควบคุมการเข้าถึง

๓. กลุ่มงานย่อย (Subcategories) เป็นกลุ่มงานที่จำแนกย่อยตามผลลัพธ์เฉพาะด้านในเชิงเทคนิค และ/หรือกิจกรรมในการบริหารจัดการ

๔. ข้อมูลอ้างอิง (Informative References) เป็นส่วนที่เป็นมาตรฐาน แนวทาง และแนวปฏิบัติ ที่ใช้ในกลุ่มหน่วยงานโครงสร้างพื้นฐานสำคัญในแต่ละกลุ่ม

องค์ประกอบ Framework Core Functions แบ่งย่อยออกเป็นกรอบงานหลัก ๕ functions ซึ่งเป็นกิจกรรมงานหลักด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) ได้แก่

๑. การระบุ (Identify) เป็นขั้นตอนแรกในการศึกษาทำความเข้าใจบริบท ทรัพยากร และกิจกรรมงานสำคัญ เพื่อบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่มีต่อระบบ ทรัพย์สิน ข้อมูล และขีดความสามารถ

๒. การป้องกัน (Protect) เป็นการจัดทำและดำเนินการ ตามมาตรการป้องกันที่เหมาะสมสำหรับการให้บริการโครงสร้างพื้นฐานสำคัญ โดยมีวัตถุประสงค์เพื่อจำกัดระดับผลกระทบของเหตุการณ์ด้านความมั่นคงปลอดภัย ไซเบอร์ ครอบคลุมการฝึกอบรมและการสร้างความตระหนัก มาตรการควบคุมการเข้าถึง และมาตรการด้านความมั่นคงปลอดภัยต่าง ๆ ทั้งกระบวนการและวิธีปฏิบัติ ตลอดจนเทคโนโลยี

๓. การตรวจจับ (Detect) เป็นการจัดทำและดำเนินกิจกรรมเพื่อตรวจหาเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้น ครอบคลุมถึงกระบวนการเฝ้าระวังหรือตรวจติดตามต่อเนื่อง

๔. การตอบสนอง (Respond) เป็นการจัดทำและดำเนินกิจกรรมเพื่อตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ ครอบคลุมถึงการวางแผนรับมือ การสื่อสาร การวิเคราะห์ การลดความเสี่ยง และการปรับปรุง

๕. การคืนสภาพ (Recover) เป็นการจัดทำและดำเนินกิจกรรมตามแผนงานเพื่อรองรับการดำเนินงานต่อเนื่อง รวมถึงแผนการกู้คืนทั้งด้านขีดความสามารถและบริการให้ได้ตามที่กำหนด

จากแนวคิดกรอบดำเนินงานเพื่อปรับปรุงความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานระบบโครงสร้างพื้นฐานสำคัญ (Critical Infrastructure Security) ของประเทศสหรัฐอเมริกา นั้น ประเทศไทย ควรกำหนดกรอบการดำเนินงานดังกล่าว เพื่อให้เป็นแนวทางและมาตรฐาน ซึ่งครอบคลุมทั้งในระดับนโยบาย การจัดการองค์กร และ เทคโนโลยี เพื่อบริหารความเสี่ยงไซเบอร์ ที่มีผลกระทบกับหน่วยงานโครงสร้างพื้นฐานสำคัญได้อย่างเหมาะสม

แนวทางการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศไทยในอนาคต

จากการวิเคราะห์ภัยคุกคามและสาเหตุของปัญหารวมทั้งผลกระทบที่เกิดขึ้นในประเทศไทย และเปรียบเทียบกับต่างประเทศ เพื่อสังเคราะห์หาแนวทางการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศไทยในอนาคต จึงมีความจำเป็นต้องมีการบูรณาการงานด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศของหน่วยต่างๆ เพื่อให้สามารถรองรับการดำเนินการตามยุทธศาสตร์ของคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้อย่างเป็นรูปธรรม โดยแนวทางในการบูรณาการงานรักษาความมั่นคงปลอดภัยทางสารสนเทศแห่งชาติ มีเป้าหมายได้แก่ จัดตั้งหน่วยงานรักษาความมั่นคงปลอดภัยทางสารสนเทศแห่งชาติ เป็นหน่วยงานหลักระดับชาติรับผิดชอบงานด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศ โดยมีโครงสร้างการบริหารการรักษาความมั่นคงปลอดภัยระดับชาติ พร้อมบทบาทหน้าที่ในการประสานความร่วมมือ มีอำนาจสั่งการ ลงโทษ (ตามกลไกการดำเนินงานของรัฐ) รองรับ กำกับ ตรวจสอบ ประเมิน มีความสามารถในการพัฒนา วิจัย และเตรียมความพร้อมด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศ รวมทั้งมีศักยภาพในการตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยทางสารสนเทศ สามารถรับมือภัยคุกคามได้ทุกรูปแบบโดยเห็นควรให้ สภาความมั่นคงแห่งชาติ (สมช.) เป็นเจ้าภาพหลักในการดำเนินการ และสามารถจัดแบ่งการดำเนินการออกเป็นการดำเนินการในระยะสั้น ระยะกลาง และระยะยาว ดังนี้

๑. การดำเนินการในระยะสั้น

๑.๑ ศึกษาผลกระทบของการปรับโครงสร้างหน่วยงานต่างๆที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางสารสนเทศ ได้แก่ กห. ทก.(สพธอ.) วท. สตช. และหน่วยงานด้านการวิจัย ได้แก่ กห.(สทป.) วท.(NECTEC) รวมทั้งหน่วยงานที่เกี่ยวข้องกับเกตเวย์ของประเทศ ได้แก่ ทก.(ทีโอที และ กสท)

๑.๒ ศึกษาผลกระทบด้านกฎหมายที่เกี่ยวข้องกับการปฏิบัติการทางไซเบอร์ในเชิงรุก รวมทั้งกฎหมายเกี่ยวข้องกับการตรวจสอบการกระทำความผิดทางอินเตอร์เน็ต การควบคุมการเข้าถึงข้อมูลการจราจรทางอินเตอร์เน็ต (Lawful Interception) เพื่อใช้ในการควบคุมการเผยแพร่ข้อมูลที่ผิดกฎหมายหรือมีผลกระทบต่อความมั่นคง รวมทั้งการโจมตีทางไซเบอร์

๑.๓ สำรวจและกำหนดอุตสาหกรรมและระบบสาธารณูปโภคสำคัญที่เกี่ยวกับโครงสร้างพื้นฐานสำคัญของประเทศ (Critical Infrastructure Security) เพื่อเป็นแนวทางและมาตรฐาน ซึ่งครอบคลุมทั้งในระดับนโยบาย การจัดการองค์กรและเทคโนโลยี เพื่อบริหารความเสี่ยงด้านไซเบอร์โดยกำหนดแนวปฏิบัติที่ดีให้นำไปใช้ในการจัดการระบบของหน่วยงานในอุตสาหกรรมและระบบสาธารณูปโภคที่เกี่ยวกับโครงสร้างพื้นฐานสำคัญ ครอบคลุมกลุ่มสำคัญประกอบด้วย กลุ่มอุตสาหกรรมเคมี เขื่อนและโรงงานไฟฟ้า อุตสาหกรรมป้องกันประเทศ กลุ่มพลังงาน หน่วยงานรัฐบาล กลุ่มคมนาคมและการขนส่ง กลุ่มอาหาร กลุ่มงานด้านเทคโนโลยีสารสนเทศ กลุ่มงานด้านอาหาร กลุ่มการเงินและธนาคาร เป็นต้น

๑.๔ สำรวจบุคลากรที่มีศักยภาพด้านสงครามไซเบอร์ในระดับประเทศทั้งจากหน่วยงานราชการ กระทรวงต่างๆ หน่วยงานวิจัยที่เกี่ยวข้อง รวมทั้งจากภาคเอกชน

๒. การดำเนินการในระยะกลาง

๒.๑ ผลักดันให้มีการตรวจสอบการกระทำความผิดทางอินเตอร์เน็ต โดยมีการออกกฎหมายในการควบคุมและสกัดกั้นการเข้าถึงข้อมูลการจราจรทางอินเตอร์เน็ต (Lawful Interception) เพื่อใช้ในการควบคุมการเผยแพร่ข้อมูลที่ผิดกฎหมายหรือมีผลกระทบต่อความมั่นคง รวมทั้งการถูกโจมตีทางไซเบอร์เท่านั้น โดยร่วมกับกระทรวงยุติธรรมหรือ ยธ. และ ทก. ศึกษาและผลักดันให้มีกฎหมายในการเข้าถึงข้อมูลการจราจรทางอินเตอร์เน็ต

๒.๒ ปรับปรุงกฎหมายระหว่างประเทศเพื่อรองรับการปฏิบัติการทางไซเบอร์ในการป้องกันเชิงรุก โดยร่วมกับ ทก. ยธ.และ กห. ศึกษาและผลักดันให้มีกฎหมายการปฏิบัติการไซเบอร์ในการป้องกันเชิงรุกเพื่อรองรับการดำเนินการตามยุทธศาสตร์ของคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติในข้อ ๒ ที่กำหนด “การสร้างศักยภาพในการตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์สร้างความพร้อมเชิงรับและเชิงรุกในการรับมือภัยคุกคาม”

๒.๓ ผลักดันให้มีการทำไซเบอร์เกตเวย์แห่งชาติ (National Cyber Gateway) ขึ้นเพื่อแก้ปัญหาการกระทำความผิดผ่านทางระบบสารสนเทศ รวมถึงดำเนินการควบคุมและปิดกั้นข้อมูลที่ก่อให้เกิดผลกระทบต่อความมั่นคงของชาติขึ้น โดยจะร่วมมือกับ ทก. กห. คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) สตช. และสำนักข่าวกรองแห่งชาติ รวมถึงผู้ให้บริการอินเทอร์เน็ตทั้งภาครัฐและเอกชน สำหรับการทำไซเบอร์เกตเวย์

แห่งชาติขึ้นจำเป็นต้องบูรณาการงานเกตเวย์ของประเทศ โดยพิจารณาบังคับให้ผู้ให้บริการอินเตอร์เน็ต (ISP) ต้องเข้ามาเชื่อมต่อกับหน่วยงาน ทก.(กสท. และทีโอที) ภายใต้การกำกับดูแลของหน่วยงานรักษาความมั่นคงปลอดภัยทางสารสนเทศแห่งชาติ ที่จัดตั้งขึ้นใหม่เป็นผู้รับผิดชอบตอบสนองและจัดการกับสถานการณ์ด้านความมั่นคงปลอดภัยทางสารสนเทศ (Incident response) ของประเทศ

๒.๔ ประสานความร่วมมือ ทั้งระหว่างภาครัฐ เอกชน เพื่อความมั่นคงปลอดภัยทางสารสนเทศ ทำงานร่วมกันระหว่างภาครัฐและเอกชนในการสร้างขีดความสามารถในการตอบสนองภัยคุกคามทางทางสารสนเทศในทุกรูปแบบได้อย่างมีประสิทธิภาพ เพื่อรักษาเสถียรภาพทางเศรษฐกิจความมั่นคงแห่งชาติ รวมทั้งการประสานความร่วมมือระหว่างประเทศในการสร้างเครือข่ายการรักษาความมั่นคงปลอดภัยทางสารสนเทศ

๒.๕ ส่งเสริมและสร้างบุคลากร นักวิจัย ในทุกระดับชั้นให้มีองค์ความรู้ด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศ จนถึงระดับแฮกเกอร์

๓. การดำเนินการในระยะยาว

๓.๑ จัดตั้งหน่วยงานรักษาความมั่นคงปลอดภัยทางสารสนเทศแห่งชาติ ทำหน้าที่ดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศ และบูรณาการงานด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศกับหน่วยงานทุกภาคส่วน ทั้งฝ่ายความมั่นคง ทหาร ภาครัฐ และเอกชน โดยหน่วยงานดังกล่าวมีหน้าที่หลักในการรับมือกับภัยคุกคามสารสนเทศในทุกรูปแบบ ลักษณะเช่นเดียวกับหน่วยงาน NSA ของประเทศสหรัฐอเมริกา โดยใช้กำลังพลหลักจากหน่วยงาน ทก.(สพธอ.) และกำลังพลที่เหลือใช้กำลังพลจากข้าราชการ วท. กห. ยธ. มท. สตช. และ Outsource จากภาครัฐและเอกชน สำหรับสายการบังคับบัญชาของหน่วยงานรักษาความมั่นคงปลอดภัยทางสารสนเทศแห่งชาตินั้น กำหนดให้เป็นหน่วยขึ้นตรงกับนายกรัฐมนตรี ภายใต้การกำกับดูแลของคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติที่มีนายกรัฐมนตรีเป็นประธาน

๓.๒ ปรับโครงสร้างของศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ (Thai Computer Emergency Response Teams : ThaiCERT) ซึ่งสังกัด ทก. ให้เป็นหน่วยงานขึ้นตรงต่อหน่วยงานรักษาความมั่นคงปลอดภัยทางสารสนเทศแห่งชาติ ทำหน้าที่เป็นศูนย์ปฏิบัติการเพื่อตอบสนองและจัดการกับสถานการณ์ด้านความมั่นคงปลอดภัยทางสารสนเทศ (National CERT) และให้การสนับสนุนและคำแนะนำในการแก้ไขภัยคุกคามทางสารสนเทศที่เกิดขึ้น รวมทั้งติดตามและเผยแพร่ข่าวสารและสถานการณ์ด้านความมั่นคงปลอดภัยทางสารสนเทศ ตลอดจนทำการศึกษานโยบายและแนวทางการปฏิบัติด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศ และรับมือกับภัยคุกคามทางสารสนเทศที่เกิดขึ้น โดยโครงสร้างของศูนย์ฯ ต้องมีขีดความสามารถรองรับ

งานไซเบอร์เกตเวย์แห่งชาติ เพื่อทำหน้าที่แก้ปัญหาการกระทำความผิดผ่านทางระบบสารสนเทศ รวมถึงการปิดกั้นข้อมูลที่ก่อให้เกิดผลกระทบต่อความมั่นคงของชาติ โดยใช้บุคลากรบางส่วนจากหน่วยงาน ทก.(ThaiCERT กสท. และ ทีโอที) รวมทั้งการ Outsource จากภาครัฐ เอกชน โดยรวมการเครื่องมือที่เกี่ยวข้องกับไซเบอร์เกตเวย์ของทั้ง กสท. และทีโอที

๓.๓ จัดตั้งศูนย์รวมความเป็นเลิศด้านไซเบอร์ (Cyber security Center of Excellence) เป็นหน่วยขึ้นตรงกับหน่วยงานรักษาความมั่นคงปลอดภัยทางสารสนเทศแห่งชาติ ทำหน้าที่วิจัยและพัฒนาเพื่อความมั่นคงปลอดภัยทางสารสนเทศ และการออกแบบโครงสร้างพื้นฐานด้านสารสนเทศให้มีความมั่นคงปลอดภัย รวมทั้งการศึกษาติดตามภัยคุกคามรูปแบบใหม่ๆ ที่จะเป็นภัยคุกคามกับประเทศในอนาคต โดยกำลังพลหลักมาจากหน่วยงานวิจัยพัฒนาของหน่วยต่างๆ ที่มีศักยภาพในด้านไซเบอร์ ได้แก่ กห.(สทป.) วท.(ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ) รวมทั้งหน่วยงานภาครัฐและเอกชน

จากการวิเคราะห์ภัยคุกคามในรูปแบบต่างๆ สามารถจัดแบ่งออกได้เป็น ๔ ประเภท โดยการรับมือกับภัยคุกคามในทุกรูปแบบจำเป็นต้องศึกษาโครงสร้างองค์กร บทบาทหน้าที่ที่เกี่ยวข้องกับองค์กรในต่างประเทศและเปรียบเทียบกับประเทศไทย สำหรับแนวทางในการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศไทย จำเป็นต้องมีการบูรณาการงานในภาพรวมของหน่วยงานต่างๆ ได้แก่ ทก. กห. วท. ยธ. สตช. โดยผลการวิจัยเสนอแนะให้มีการจัดตั้งหน่วยงานรักษาความมั่นคงปลอดภัยทางสารสนเทศแห่งชาติ เช่นเดียวกับสำนักงานความมั่นคงแห่งชาติ (National Security Agency : NSA) ของประเทศสหรัฐอเมริกา รวมทั้งการดำเนินการในด้านอื่นๆ ควบคู่กัน เช่น การผลักดันให้มีกฎหมายควบคุมการจราจรทางอินเตอร์เน็ต การผลักดันหน่วยงาน National CERT ให้เป็นศูนย์ปฏิบัติการในระดับประเทศ การประสานความร่วมมือกับหน่วยงานต่างประเทศ เป็นต้น โดยหน่วยงานรักษาความมั่นคงปลอดภัยทางสารสนเทศแห่งชาติมีโครงสร้างการบริหารการรักษาความมั่นคงปลอดภัยระดับชาติ พร้อมบทบาทหน้าที่ในการประสานความร่วมมือ มีอำนาจสั่งการ ลงโทษ รองรับ กำกับ ตรวจสอบ ประเมิน มีความสามารถในการพัฒนา วิจัย และเตรียมความพร้อมด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศ รวมทั้งมีศักยภาพในการตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยทางสารสนเทศ สามารถรับมือภัยคุกคามได้ทุกรูปแบบ และเสนอแนะให้ สมช. เป็นหน่วยหลักในการดำเนินการทั้งในระยะสั้น ระยะกลาง และระยะยาว เพื่อให้ผลที่เป็นรูปธรรม

บทที่ ๕
สรุปและข้อเสนอแนะ

สรุป

การวิจัยการดำเนินการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศไทยในอนาคต ได้กำหนดวัตถุประสงค์ไว้ ๓ ประการ จากการศึกษาวิจัยค้นคว้าแหล่งข้อมูลทั้งในและต่างประเทศ นำมาวิเคราะห์หาแนวทางการดำเนินการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศไทยในอนาคตได้ นับว่าบรรลุตามวัตถุประสงค์ที่ตั้งไว้ทุกประการ ซึ่งสามารถสรุปในแต่ละวัตถุประสงค์ได้ดังนี้

วัตถุประสงค์ที่ ๑ เพื่อศึกษาวิเคราะห์ ปัญหา สาเหตุและผลกระทบที่เกิดจากภัยคุกคามทางไซเบอร์ต่อความมั่นคงปลอดภัยในด้านต่าง ๆ เช่น เศรษฐกิจ สังคม วัฒนธรรม การเมือง และการทหาร เป็นต้น

จากเหตุการณ์สำคัญที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางสารสนเทศ และภัยคุกคามรูปแบบต่างๆ ทำให้สามารถวิเคราะห์และจำแนกประเภทของภัยคุกคามที่มีผลกระทบต่อความมั่นคงของประเทศ ได้เป็น ๔ ประเภทใหญ่ๆ ได้แก่

๑. ภัยคุกคามต่อความมั่นคงทางเศรษฐกิจ

๒. ภัยคุกคามต่อสังคมและจิตวิทยา

๓. ภัยคุกคามต่อความมั่นคงทางทหาร

๔. ภัยคุกคามในรูปแบบการก่อการร้าย

จากผลวิเคราะห์ปัญหา สาเหตุและผลกระทบที่เกิดจากภัยคุกคามทางไซเบอร์ต่อความมั่นคงปลอดภัยในด้านต่าง ๆ เพื่อหาแนวทางในการแก้ไขปัญหาให้ได้ผลเป็นรูปธรรม สรุปปัญหาและผลกระทบได้ดังนี้

๑. การบริหารจัดการการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศไทย จากการตรวจสอบบทบาทและหน้าที่ของหน่วยงานต่างๆที่รับผิดชอบงานด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศไทย ได้แก่ ทก. กห. วท. ยธ. สตช. เป็นต้น สรุปได้ว่าหน่วยงานดังกล่าวยังขาดการบูรณาการงานในภาพรวมของการดำเนินการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางสารสนเทศ โดยยังเป็นการดำเนินการแบบเอกเทศทั้งในระดับนโยบายและระดับปฏิบัติการเพื่อรองรับภารกิจของแต่ละกระทรวงหรือหน่วยงานตนเองเท่านั้น ทำให้ขาดศักยภาพในการดำเนินการรับมือกับภัยคุกคามรูปแบบต่างๆ

๒. ด้านบุคลากร ขีดความสามารถด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศไทยยังอยู่ในระดับต่ำในภาครัฐ (ฝ่ายพลเรือน และฝ่ายความมั่นคง) ซึ่งดูได้จากตัวชี้วัดเช่น จำนวนบุคลากรที่มีความเชี่ยวชาญด้านไซเบอร์ จึงจำเป็นต้องมีการบูรณาการทั้งด้านการบริหารจัดการบุคลากรที่มีจำนวนจำกัด รวมทั้งการส่งเสริมสร้างนักวิจัย

๓. กฎหมายและ พ.ร.บ.ที่เกี่ยวข้อง ในปัจจุบันช่องทางการเชื่อมต่อเครือข่ายอินเทอร์เน็ตภายในประเทศกับเครือข่ายอินเทอร์เน็ตต่างประเทศผ่านหน่วยงานรัฐ ผู้ให้บริการอินเทอร์เน็ตทั้งภาครัฐและเอกชน มีเป็นจำนวนมาก ดังนั้นการตรวจสอบและสกัดกั้นข้อมูลการจราจรทางอินเทอร์เน็ต การควบคุมข้อมูลที่ผิดกฎหมายหรือมีผลกระทบต่อความมั่นคง รวมทั้งการป้องกันการโจมตีทางไซเบอร์กระทำได้ค่อนข้างยาก จึงมีความจำเป็นที่ประเทศไทยต้องมีกฎหมายรองรับในการควบคุมและสกัดกั้นข้อมูลการจราจรทางอินเตอร์เน็ตในการเผยแพร่ข้อมูลที่ผิดกฎหมายหรือมีผลกระทบต่อความมั่นคง รวมทั้งการป้องกันการโจมตีทางไซเบอร์

๔. โครงสร้างพื้นฐานของประเทศ คณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้กำหนดไว้ในยุทธศาสตร์ข้อ ๓ “การป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศปกป้องโครงสร้างพื้นฐานสำคัญของประเทศและระบบสารสนเทศที่เกี่ยวข้อง” อย่างไรก็ตามยังไม่มีการดำเนินการกำหนดอุตสาหกรรมและระบบสาธารณูปโภคสำคัญที่เกี่ยวกับโครงสร้างพื้นฐานสำคัญของประเทศที่ชัดเจน ทั้งนี้ประเทศไทยจำเป็นต้องกำหนดอุตสาหกรรมและระบบสาธารณูปโภคสำคัญของประเทศ เพื่อเป็นแนวทางและมาตรฐานครอบคลุมทั้งในระดับนโยบาย การจัดการองค์กรและเทคโนโลยี เพื่อบริหารความเสี่ยงต่อภัยคุกคามด้านไซเบอร์โดยกำหนดแนวปฏิบัติที่ดีให้นำไปใช้ในการจัดการระบบของหน่วยงานในอุตสาหกรรมและระบบสาธารณูปโภคที่เกี่ยวกับโครงสร้างพื้นฐานสำคัญ

วัตถุประสงค์ที่ ๒ เพื่อศึกษา วิเคราะห์ เปรียบเทียบ แนวทางต่าง ๆ ในการรักษาความมั่นคงปลอดภัยทางสารสนเทศ

ผลการศึกษาทำให้ทราบถึงองค์กร บทบาทหน้าที่ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางสารสนเทศ รวมทั้งการรักษาความมั่นคงปลอดภัยทางสารสนเทศของต่างประเทศ และเปรียบเทียบกับประเทศไทย โดยมุมมองของประเทศต่างๆ ที่มีต่อการรักษาความมั่นคงปลอดภัยทางสารสนเทศ เช่น สำนักงานความมั่นคงแห่งชาติ (National Security Agency : NSA) ของประเทศสหรัฐอเมริกา เป็นหน่วยงานข่าวกรองที่มีขอบเขตหน้าที่ทั้งในและนอกประเทศ และเป็นหน่วยงานด้านข่าวกรองที่มีขนาดองค์กรที่ใหญ่ที่สุดของสหรัฐอเมริกา มีหน้าที่ในการเฝ้าระวัง ตรวจสอบ ถอดรหัสและประมวลผลข้อมูลอิเล็กทรอนิกส์ รวมถึงรักษาความมั่นคงปลอดภัยในการรับส่งข้อมูลระหว่างหน่วยงานภาครัฐของสหรัฐอเมริกา NSA มีขีดความสามารถด้านสงครามไซเบอร์หลายด้าน ทั้งในด้าน

ของการป้องกันภัยจากไซเบอร์ การโจรกรรมข้อมูลทางไซเบอร์และการเข้ารหัส ถอดรหัสข้อมูล โดยเฉพาะอย่างยิ่งในส่วนของการเข้ารหัสและถอดรหัสข้อมูล มีกฎหมายรองรับสามารถดักฟังและประมวลผลข้อมูลสารสนเทศที่ถูกส่งผ่านอินเตอร์เน็ตได้เกือบทั้งหมด

เมื่อนำผลการศึกษาองค์กร บทบาทหน้าที่ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางสารสนเทศจากต่างประเทศเปรียบเทียบกับประเทศไทยแล้วจะเห็นได้ชัดเจนว่าประเทศไทยยังไม่มีการบูรณาการงานดังกล่าว ต้องพึ่งพาการดำเนินการจากหลายกระทรวงที่เกี่ยวข้อง ได้แก่ ทก. กห. วท. ยธ. สตช. กสทช. เป็นต้น จึงเป็นที่มาของการจัดตั้งองค์กร “หน่วยงานรักษาความมั่นคงปลอดภัยทางสารสนเทศแห่งชาติ” ในการรับมือกับภัยคุกคามด้านสารสนเทศในรูปแบบต่างๆ นอกจากนี้ยังได้มีการรวบรวมเหตุการณ์สำคัญอันเกี่ยวเนื่องกับการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศต่างๆ และการดำเนินการตอบโต้โดยหน่วยงานภาครัฐ จากเหตุการณ์เหล่านี้ทำให้เห็นว่าแนวโน้มของภัยคุกคามด้านสารสนเทศจะทวีความรุนแรงมากขึ้น มีเหตุเกิดบ่อยครั้งขึ้น และส่งผลกระทบในวงกว้างต่อภาคส่วนต่าง ๆ มากขึ้น

วัตถุประสงค์ที่ ๓ เพื่อเสนอแนะแนวทางที่เหมาะสมในการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศไทยในอนาคต

จากการวิเคราะห์ภัยคุกคามและสาเหตุของปัญหารวมทั้งผลกระทบที่เกิดขึ้นในประเทศไทย และเปรียบเทียบกับต่างประเทศ เพื่อสังเคราะห์หาแนวทางการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศไทยในอนาคต จึงมีความจำเป็นต้องมีการบูรณาการงานด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศของหน่วยต่างๆ เพื่อให้สามารถรองรับการดำเนินการตามยุทธศาสตร์ของคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้อย่างเป็นรูปธรรม โดยแนวทางในการบูรณาการงานรักษาความมั่นคงปลอดภัยทางสารสนเทศแห่งชาติ มีเป้าหมายได้แก่ จัดตั้งหน่วยงานรักษาความมั่นคงปลอดภัยทางสารสนเทศแห่งชาติ เป็นหน่วยงานหลักระดับชาติ รับผิดชอบงานด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศ โดยมีโครงสร้างการบริหารการรักษาความมั่นคงปลอดภัยระดับชาติ พร้อมบทบาทหน้าที่ในการประสานความร่วมมือ มีอำนาจสั่งการ ลงโทษ (ตามกลไกการดำเนินงานของรัฐ) รองรับ กำกับ ตรวจสอบ ประเมิน มีความสามารถในการพัฒนา วิจัย และเตรียมความพร้อมด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศ รวมทั้งมีศักยภาพในการตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยทางสารสนเทศ สามารถรับมือภัยคุกคามได้ทุกรูปแบบ โดยผลการวิจัยเสนอแนะให้สภาความมั่นคงแห่งชาติ (สมช.) เป็นเจ้าภาพหลักในการดำเนินการ และสามารถจัดแบ่งการดำเนินการออกเป็นการดำเนินการในระยะสั้น ระยะกลาง และระยะยาว ดังนี้

๑. การดำเนินการในระยะสั้น

เป็นการศึกษาผลกระทบของการปรับโครงสร้างหน่วยงานต่างๆที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางสารสนเทศ ได้แก่ กห. ทก.(สพธอ.) วท. สตช. และหน่วยงานด้านการวิจัย ได้แก่ กห.(สทป.) วท.(NECTEC) รวมทั้งหน่วยงานที่เกี่ยวข้องกับเกตเวย์ของประเทศ ได้แก่ ทก.(ทีโอทีและ กสท) และผลกระทบด้านกฎหมายที่เกี่ยวข้องกับการตรวจสอบการกระทำความผิดทางอินเตอร์เน็ต การเข้าถึงข้อมูลทางอินเตอร์เน็ต (Lawful Interception) เพื่อใช้ในการควบคุมการเผยแพร่ข้อมูลที่ผิดกฎหมายหรือมีผลกระทบต่อความมั่นคง นอกจากนี้ยังจำเป็นต้องสำรวจและกำหนดอุตสาหกรรมและระบบสาธารณูปโภคสำคัญที่เกี่ยวกับโครงสร้างพื้นฐานสำคัญของประเทศ (Critical Infrastructure Security) เพื่อให้เป็นแนวทางและมาตรฐาน ซึ่งครอบคลุมทั้งในระดับนโยบาย การจัดการองค์กรและเทคโนโลยี เพื่อบริหารความเสี่ยงด้านไซเบอร์

๒. การดำเนินการในระยะกลาง

เป็นการผลักดันให้มีการตรวจสอบการกระทำความผิดทางอินเตอร์เน็ต โดยมีการออกกฎหมายในการเข้าถึงข้อมูลทางอินเตอร์เน็ต (Lawful Interception) เพื่อใช้ในการควบคุมการเผยแพร่ข้อมูลที่ผิดกฎหมายหรือมีผลกระทบต่อความมั่นคงเท่านั้น และผลักดันให้มีการทำไซเบอร์เกตเวย์แห่งชาติ (National Cyber Gateway) ขึ้น เพื่อแก้ปัญหาการกระทำความผิดผ่านทางระบบสารสนเทศ รวมถึงดำเนินการปิดกั้นข้อมูลที่ต่อให้เกิดผลกระทบต่อความมั่นคงของชาติขึ้น รวมทั้งการประสานความร่วมมือ ทั้งระหว่างภาครัฐ เอกชน เพื่อความมั่นคงปลอดภัยทางสารสนเทศ ทำงานร่วมกันระหว่างภาครัฐและเอกชนในการสร้างขีดความสามารถในการตอบสนองภัยคุกคามทางทางสารสนเทศในทุกรูปแบบได้อย่างมีประสิทธิภาพ เพื่อรักษาเสถียรภาพทางเศรษฐกิจความมั่นคงแห่งชาติ รวมทั้งการประสานความร่วมมือระหว่างประเทศในการสร้างเครือข่ายการรักษาความมั่นคงปลอดภัยทางสารสนเทศ

๓. การดำเนินการในระยะยาว

เป็นการดำเนินการเพื่อให้บรรลุเป้าหมายที่ตั้งไว้ โดยจะเป็นการจัดตั้งหน่วยงานรักษาความมั่นคงปลอดภัยทางสารสนเทศแห่งชาติ ทำหน้าที่ดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศ และบูรณาการงานด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศกับหน่วยงานทุกภาคส่วน ทั้งฝ่ายความมั่นคง ทหาร ภาครัฐ และเอกชน รวมทั้งการปรับโครงสร้างของศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ (Thai Computer Emergency Response Teams : ThaiCERT) ซึ่งสังกัด ทก. ให้เป็นหน่วยงานขึ้นตรงต่อหน่วยงานรักษาความมั่นคงปลอดภัยทางสารสนเทศแห่งชาติ ทำหน้าที่เป็นศูนย์ปฏิบัติการตอบสนองและจัดการกับสถานการณ์ด้านความมั่นคง

ปลอดภัยทางสารสนเทศ (National CERT) นอกจากนี้ยังจำเป็นต้องสร้างนักวิจัย นักวิชาการที่เกี่ยวข้อง โดยเสนอแนะให้จัดตั้งศูนย์รวมความเป็นเลิศด้านไซเบอร์ (Cyber Security Center of Excellence) ขึ้นตรงกับหน่วยงานรักษาความมั่นคงปลอดภัยทางสารสนเทศแห่งชาติ ทำหน้าที่วิจัยและพัฒนาเพื่อความมั่นคงปลอดภัยทางสารสนเทศ และการออกแบบโครงสร้างพื้นฐานด้านสารสนเทศให้มีความมั่นคงปลอดภัย รวมทั้งการศึกษาติดตามภัยคุกคามรูปแบบใหม่ๆ ที่จะเป็นภัยคุกคามกับประเทศในอนาคต โดยกำลังพลหลักมาจากหน่วยงานวิจัยพัฒนาของหน่วยต่างๆ ที่มีศักยภาพในด้านไซเบอร์ ได้แก่ กห.(สทป.) วท.(ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ) รวมทั้งหน่วยงานภาครัฐและเอกชน

ข้อเสนอแนะ

การใช้ประโยชน์จากเอกสารวิจัยนี้ จะเป็นประโยชน์โดยตรงกับประเทศให้มีศักยภาพและขีดความสามารถด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศ โดยมีข้อเสนอแนะดังนี้

การกำหนดให้การรักษาความมั่นคงปลอดภัยทางสารสนเทศ เป็นวาระแห่งชาติเร่งด่วน เนื่องจากการจัดตั้งหน่วยงานรักษาความมั่นคงปลอดภัยทางสารสนเทศแห่งชาติ จำเป็นต้องมีการปฏิรูปโครงสร้างของหลายส่วนราชการ โดยเฉพาะ กห. ทก.(สพธอ.และสำนักป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศ) วท. สตช.(กลุ่มงานตรวจสอบและวิเคราะห์การกระทำความผิดทางเทคโนโลยี กองบังคับการสนับสนุนทางเทคโนโลยี (บก.สสท.) และกองบังคับการปราบปรามการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.)) และหน่วยงานด้านการวิจัย ได้แก่ กห.(สทป.) วท.(ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC)) รวมทั้งหน่วยงานที่เกี่ยวข้องกับไซเบอร์เกตเวย์ของประเทศ ได้แก่ ทก.(ทีโอที และ กสท) จึงจำเป็นต้องมีการกำหนดให้การรักษาความมั่นคงปลอดภัยทางสารสนเทศ เป็นวาระแห่งชาติที่เร่งด่วน โดยบูรณาการงานด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศของทั้งประเทศ ให้เป็นระบบ มีแนวทางและทิศทางเดียวกัน

บรรณานุกรม

ภาษาไทย

"กระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ มาตรา ๕-๑๑",พระราชบัญญัติ.

วิวัฒน์ เอี่ยมไพรวัน. กฎเกณฑ์ทางการเมืองแนวใหม่ของการเมืองไทยกับความสัมพันธ์ทางอำนาจระหว่างรัฐกับประชาชน. นนทบุรี : มหาวิทยาลัยสุโขทัยธรรมาธิราช, ๒๕๔๕.

นายกรัฐมนตรี, สำนัก. คำสั่งที่ ๗๖/๒๕๕๕ เรื่อง แต่งตั้งคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Committee).

ภาษาต่างประเทศ

Books

Arnold, David. The Age of Discovery, 1400–1600. Routledge, 2011.

Bergen, P.L. Holy war, Inc.: inside the secret world of Osama bin Laden. New York : Touchstone Rockfeller Center, 2001.

Bulliet, Richard et al. The Earth and Its Peoples: A Global History. Cengage Learning, 2010.

Ceruzzi, Paul E. Computing: A Concise History (MIT Press Essential Knowledge). USA : The MIT Press, 2012.

Clark, Richard A. and Knake, Robert. Cyber War: The Next Threat to National Security and What to Do About It. USA : Ecco, 2011.

Emerson, Steven. American Jihad: The Terrorists Living Among Us. New York : The Free Press, 2002.

Gershuny, J. and Miles, I. The new service economy: the transformation of employment in industrial societies. London : F. Pinter, 1983.

Hillman, G. C. Late Pleistocene changes in wild plant-foods available to hunter-gatherers of the northern Fertile Crescent: Possible preludes to cereal cultivation. London : UCL Books, 1996.

Katie, Hafner and John, Markoff. Cyberpunk: Outlaws and Hackers on the Computer Frontier. New York : Touchstone, 1991.

Ryan, Johnny. A History of the Internet and the Digital Future. USA : Reaktion Books, 2013.

Smith, B.C. Decentralization : the territorial dimension of the state. London : Allen & Unwin, 1985.

Telò, Mario. European Union and new regionalism: regional actors and global governance in a post-hegemonic era. Berlington : Ashgate Publishing Limited, 2007.

Toffler, Alvin. Revolutionary Wealth. USA : Bantam Books, 2006.

Toffler, Alvin. The Third Wave. USA : Bantam Books, 1980.

Journals

Armbrust, M. et al. "A view of cloud computing", Communications of the ACM. Vol. 53 Issue 4, April 2010.

Bhardwaj, S. et al. "Cloud computing: A study of infrastructure as a service (IAAS)", International Journal of Engineering and Information Technology. Vol. 2 No. 1, 2010.

Barbaroux, P. "Identifying collaborative innovation capabilities within knowledge-intensive environments: Insights from the ARPANET project", European Journal of Innovation Management. 2012.

Caporaso, James A. "The European Union and Forms of State: Westphalian, Regulatory or Post-Modern?", Journal of Common Market Studies. March 1996. p.29-52.

Dahlman, Carl J. and Aubert, Jean-Eric. “China and the Knowledge Economy: Seizing the 21st Century. WBI Development Studies”, World Bank Publications. 30 January 2008.

Fulghum, David A. et al. “Black Surprises”, Aviation Week and Space Technology. 5 October 2007.

Galea, Sandro et al. "Psychological Sequelae of the September 11 Terrorist Attacks in New York City", The New England Journal of Medicine. 2002.

Grant, Edward. “The Foundations of Modern Science in the Middle Ages: Their Religious, Institutional, and Intellectual Contexts”, Cambridge University Press, 1996.

Hauben, M. and Hauben, R. "On the history and impact of Usenet and the Internet", Netizens. Vol. 3 No. 7, 1998.

Huntington, Samuel P. "The Third Wave: Democratization in the Late 20th Century", University of Oklahoma Press. 1993.

Jensen, M.C. "The modern industrial revolution, exit, and the failure of internal control systems", the Journal of Finance. 1993.

Ljungqvist, A. and Wilhelm, W.J. "IPO pricing in the dot-com bubble", The Journal of Finance. 2003.

Sanger, David E. “Obama Order Sped Up Wave of Cyberattacks Against Iran.”, The New York Times. June 2005.

Slater, D. "Strong-state democratization in Malaysia and Singapore", Journal of Democracy. Vol. 23 No. 2, Aprill 2010. p. 19-33.

Spring, Tom. “Spam Slayer: Slaying Spam-Spewing Zombie PCs”, PC World. 20 June 2005

TP Gerber and M Hout. “More Shock than Therapy: Market Transition, Employment and Income in Russia 1991-1995”, American Journal of Sociology, 1998.

Virgo, J.M. "Economic impact of the terrorist attacks of September 11", Atlantic Economic Journal. 2001.

Wymbs, C. "How e-commerce is transforming and internationalizing service industries", Journal of Services Marketing. 2000.

Research Reports

Anderson, L. "Demystifying the Arab Spring: parsing the differences between Tunisia, Egypt and Libya". สถาบันวิจัย Hein Online, 2011.

Demirgüç-Kunt, A. and Detragiache, E. "Financial liberalization and financial fragility". The World Bank Development Research Group and International Monetary Fund Research Department, 1998.

Database on the Internet

Airforce-Technology. “The Israeli 'E-tack' on Syria – Part II”. (Online).Available:http:// www.airforce-technology.com/features/feature1669, 2008.

BBC. “North Korea conducts nuclear test”. (Online).Available:http://news.bbc.co.uk/2/hi/asia-pacific/8066615.stm, 2008.

Beech, Hannah. “Meet China’s Newest Soldiers: An Online Blue Army”. (Online). Available:http: //world. time.com/2011/05/27/meet-chinas-newest-soldiers-an-online-blue-army/, 2011.

Blakeley, Georgina. "Los Indignados: a movement that is here to stay". (Online). Available:http: // www.opendemocracy.net/georgina-blakeley/los-indignados-movement-that-is-here-to-stay, 2012.

Bright, Arthur. "Estonia accuses Russia of 'cyberattack'". (Online). Available : http://www.csmonitor.com / 2007/0517/p99s01-duts.html, 2007.

Center of Strategic International Studies. "Economic Change in Russia". (Online).Available: http://csis.org/program/economic-change-russia, 2006.

CNN. "North Korea pledges to test nuclear-bomb" .(Online). Available: http://edition.cnn.com/ 2006/WORLD/asiapcf/10/03/nkorea.nuclear/index.htm?PHPSESSID= e00207 818747c2c959b7677da032e02c, 2006.

Financial Times. "FT Global 500 2012". (Online). Available : http://www.ft.com/cms/a81f853e-ca80-11e1-89f8-00144feabdc0.pdf, 2013.

Foreign Affairs. "The Five-Day War Managing Moscow After the Georgia Crisis". (Online). Available: http://www.foreignaffairs.com/articles/64602/charles-king/the-five-day-war, 2008.

Fritz, Jason. "How China will use cyber warfare to leapfrog in military competitiveness". (Online). Available : http://epublications.bond.edu.au/cgi/viewcontent.cgi?article=1110&context=cm, 2008.

H.H. Khondker. "Role of the New Media in the Arab Spring". (Online).Available:http:// www. tandfonline.com/doi/abs/10.1080/14747731.2011.621287#.U0OPmab9rQo, 2011.

Hort, Loro. "The Dragon's Spear: China's Asymmetric Strategy". (Online) .Available:http:// yaleglobal.yale.edu/content/dragon%E2%80%99s-spear-china%E2%80%99s-asymmetric-strategy, 2013.

Ingram, Mathew. "How social media is rewriting the rules of modern warfare". (Online). Available: http://gigaom.com/2012/11/19/how-social-media-is-rewriting-the-rules-of-modern-warfare/, 2012.

Keating, Joshua E. "Why Do Diplomats Still Send Cables? In: Foreign Policy". (Online). Available: http://www.foreignpolicy.com/articles/2010/11/29/why_do_diplomats_still_send_cables, 2010.

Lawrence, Dune. "Hackers Linked to China's Army Seen From EU to D.C.". (Online). Available: http: //www.bloomberg.com/news/2012-07-26/china-hackers-hit-eu-point-man-and-d-c-with-byzantine-candor.html, 2012.

Lexander Daniel. “Russian Historian: The problem is how to live together if the two peoples have such a different memory”. (Online).Available:REGNUM News Agency , http:// pda.regnum. ru/news/issues/823273.html, 2007.

Manager Magazin. “Cyber-Krieg: Virtuelle weiße Fahne”. (Online).Available : http://www.manager-magazin.de/it/artikel/0,2828,141195,00.html, 2010.

Net-Security. "Lack of computer security experts weighs heavy on U.S. cyber defense". (Online). Available:http://www.net-security.org/secworld.php?id=9611, 2010.

New York Daily News. “New reports of starving North Koreans resorting to cannibalism come amid renewed tensions between Pyongyang and Washington”. (Online). Available:http://www.nydailynews.com/news/world/report-starving-north-korean-father-resorts-cannibalism-article-1.1250773, 2013.

NSA. “About NSA”. (Online).Available : http://www.nsa.gov/about/, 2008.

NSA. “Leadership”. (Online).Available : http://www.nsa.gov/about/leadership/, 2008.

Poitras, Laura. “Ally and Target: US Intelligence Watches Germany Closely”. (Online). Available:http://www.spiegel.de/international/world/germany-is-a-both-a-partner-to-and-a-target-of-nsa-surveillance-a-916029.html, 2012.

Post, Huffington. “Internet 'Kill Switch' Would Give President Power To Shut Down The Web”. (Online).Available : http://www.huffingtonpost.com/2010/06/17/internet-kill-switch-woul_n_ 615923.html, 2011.

Post, Washington. “NSA slides explain the PRISM data-collection program”. (Online). Available:http : //www. washingtonpost.com/wpsrv/special/politics/prism-collection-documents/, 2013.

Reuters. “Assad says facility Israel bombed not nuclear-paper”. (Oline). Available:http: //web. archive. org/web/20121105015114/http://www.reuters.com/article/latestCrisis/idUSL27399094, 2008.

Spiegel, Der. “Cyber Menace: Digital Spying Burdens German-Chinese Relations”. (Online). Available:http://www.spiegel.de/international/world/digital-spying- burdburdens-german-relations-with-beijing-a-885444-2.html, 2013.

The Conversations. "Google still controls your information, despite EU ruling". (Online).Available: http://theconversation.com/google-still-controls-your-information-despite-eu-ruling-22925, 2014.

The Guardian. “North Korean ‘cyberwarfare’ said to have cost South Korea £500m”. (Online). Available:http://www.theguardian.com/world/2013/oct/16/north-korean-cyber-warfare-south-korea, 2012.

The Guardian. “South Korean 5G internet move to further increase download speeds”. (Online). Available:http://www.theguardian.com/technology/2014/jan/23/south-korea-intenet-download-speeds-5g, 2013.

The Huffington Post. “North Korea Food Aid Approved By UN Food Body ” . \(Online).Available:http: //www.huffingtonpost.com/2013/06/08/north-korea-food-aid-_n_3406941.html, 2013.

The Huffington Post. “North Korea Hunger: Millions Of Children Deprived Of Food, Medicine, Health Care”. (Online).Available:http://www.huffingtonpost.com/2012/06/12/north-korea-hunger_n_ 1589029.html, 2011.

The Japan Times. ”Best of the Best’: South Korea forges youth into world’s elitecyberwarriors”. (Online) Available: http : // www.japantimes.co.jp/news/2013/03/19/ asia-pacific/ best-of-the-best-south-korea-forges-youth-into-worlds-elite-cyberwarriors/, 2012.

The Japan Times. “Snowden says U.S. hacking targets China; NSA points to thwarted attacks”. (Online).Available:http://www.japantimes.co.jp/news/2013/06/14/world/u-s-hacking-effort-targets-china-snowden/#.UwcP0PgvAsk, 2013

The Telegraph. “http://www.telegraph.co.uk/technology/news/5637243/Hackers-recruited-to-fight-new-cold-war.html”. (Online).Available : http://www.telegraph.co.uk/technology/news/ 5637243/ Hackers-recruited-to-fight-new-cold-war.html, 2009.

The United States Department of Defense. “Special Report : The Cyber Domain”. (Online). Available : http://www. defense.gov/home/features/2013/0713_cyberdomain. 2013.

The Washington Post. “Report on ‘Operation Shady RAT’ identifies widespread cyber- spying”. (Online). Available:http://www.washingtonpost.com/national/national-security/report-identifies-widespread-cyber-spying/2011/07/29/gIQAoTUmqI_story.html, 2008.

TradingandEcconomics. “RussiaGDP”. (Online).Available:http”// www.tradingeconomics. com/russia/gdp, 2011.

U.S. Census Bureau. “Computer and Internet Use in the United States”. (Online). Available : http:// www.census.gov /prod/2013pubs/p20-569.pdf, 2013.

USA Today. “South Korea blames North for cyberattack”. (Online). Available: http: // www.usatoday.com/story/news/world/2013/07/16/korea-cyberattacks /2520017/, 2012.

US-CERT. “The National Strategy to Secure Cyberspace”. (Online). Available : https://www.us-cert. gov/sites/default /files/publications/cyberspace_strategy.pdf, 2003.

ประวัติย่อผู้วิจัย

ชื่อ พลเรือตรี วิโรจน์ ธันวรักษ์กิจ

วัน เดือน ปีเกิด ๒๐ ธันวาคม ๒๕๐๑

การศึกษา
โรงเรียนเตรียมทหาร
โรงเรียนนายเรือ Flensburg-Murwik สหพันธ์สาธารณรัฐเยอรมนี
หลักสูตรเสนาธิการทหารเรือ
หลักสูตรวิทยาลัยการทัพเรือ

ประวัติการทำงาน โดยย่อ
ผู้บังคับการเรือหลวงท่าดินแดง กองเรือทุ่นระเบิด กองเรือยุทธการ
ผู้อำนวยการกองนโยบายและแผน กรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ
ผู้อำนวยการกองนโยบายและแผน กรมส่งบำรุงทหารเรือ
ผู้อำนวยการกองนโยบายและแผน กรมกำลังพลทหารเรือ
ผู้อำนวยการกองการกำลังพล กรมกำลังพลทหารเรือ
เสนาธิการกองเรือทุ่นระเบิด กองเรือยุทธการ
รองผู้บัญชาการกองเรือทุ่นระเบิด กองเรือยุทธการ
รองเจ้ากรมยุทธการทหาร กองบัญชาการกองทัพไทย

ตำแหน่งปัจจุบัน เจ้ากรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ

สรุปย่อ

ลักษณะวิชา วิทยาศาสตร์และเทคโนโลยี

เรื่อง แนวทางการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศไทยในอนาคต

ผู้วิจัย พลเรือตรี วิโรจน์ ธันวรักษ์กิจ **หลักสูตร** วปอ. **รุ่นที่** ๕๖

ตำแหน่ง เจ้ากรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ

ความเป็นมาและความสำคัญของปัญหา

ความก้าวหน้าทางด้านเทคโนโลยีสารสนเทศได้ทำให้เกิดความเปลี่ยนแปลงของมนุษยชาติในหลายๆ ด้าน จนนักอนาคตศาสตร์อย่าง Alvin Toffler ตั้งทฤษฎี "คลื่นลูกที่สาม" โดย Toffler มองว่าเทคโนโลยีสารสนเทศคือคลื่นลูกที่สามของคลื่นปฏิวัติสังคมมนุษย์ต่อจากการทำการเกษตรและการปฏิวัติอุตสาหกรรม ซึ่งทฤษฎีดังกล่าวสอดคล้องกับตัวเลขทางเศรษฐกิจในปัจจุบัน ตามการจัดลำดับมูลค่าทางการตลาดของบริษัททั่วโลกในปี ๒๕๕๕ นอกจากความเปลี่ยนแปลงทางด้านเศรษฐกิจแล้ว เทคโนโลยีสารสนเทศยังทำให้เกิดความเปลี่ยนแปลงทางด้านสังคมและวัฒนธรรมอย่างลึกซึ้ง การติดต่อสื่อสาร การรับและเผยแพร่ข้อมูลข่าวสาร ทัศนคติและวิธีคิด โดยเฉพาะอย่างยิ่งเมื่อ Social Network ได้รับความนิยมและถูกใช้งานอย่างกว้างขวาง จนได้ชื่อว่า “สื่อใหม่” ซึ่งสามารถเข้ามาแทนที่ และมีอิทธิพลเหนือสื่อในรูปแบบเดิมที่ถือว่าเป็น “ฐานันดรที่สี่” ได้ส่งผลให้สื่อเดิมต้องมีการปรับตัว และนำสื่อใหม่มาปรับใช้ให้เท่าทันความเปลี่ยนแปลงทางวัฒนธรรมที่เกิดขึ้น

เมื่อเทคโนโลยีสารสนเทศเข้ามาเกี่ยวข้องกับคนจำนวนมาก โดยตามสถิติล่าสุดประชากรในประเทศไทยเกินกว่าครึ่งสามารถเข้าถึงอินเตอร์เน็ตได้ ภัยคุกคามด้านต่างๆ ที่เกี่ยวข้องกับการใช้ประโยชน์เทคโนโลยีสารสนเทศ จึงเป็นเรื่องที่หลีกเลี่ยงไม่ได้ ลักษณะของภัยคุกคามด้านสารสนเทศมีหลากหลายรูปแบบ รูปแบบที่มีมักพบเห็นมากที่สุดคือ การก่ออาชญากรรมคอมพิวเตอร์ที่เกี่ยวข้องกับระบบพาณิชย์อิเล็กทรอนิกส์ (E-Commerce) การทำธุรกรรมอิเล็กทรอนิกส์ (E-Transaction) รวมถึงการละเมิดสิทธิทรัพย์สินทางปัญญา มีการคาดการณ์ว่าความเสียหายอันเกิดจากการก่ออาชญากรรมคอมพิวเตอร์ในรูปแบบต่างๆมีมูลค่ารวมกันสูงถึงห้าแสนล้านเหรียญสหรัฐต่อปี ทำให้ส่งผลกระทบต่อเศรษฐกิจในวงกว้าง

ตัวอย่างภัยคุกคามไซเบอร์ที่ได้รับความสนใจไปทั่วโลกอีกกรณีหนึ่งคือ การโจมตีโรงงานผลิตอาวุธนิวเคลียร์ และโรงงานไฟฟ้านิวเคลียร์ด้วยไวรัสคอมพิวเตอร์ Stuxnet โดยไวรัสคอมพิวเตอร์มีขีดความสามารถในการโจมตีเฉพาะเจาะจงหน่วยงานและสามารถโจมตีเป้าหมายได้ในระดับอุปกรณ์ฮาร์ดแวร์ ซึ่งถือเป็นภัยคุกคามทางไซเบอร์ ที่ควรให้ความสนใจและให้ความระมัดระวังเป็นพิเศษ

จากความสำคัญของเทคโนโลยีสารสนเทศและผลกระทบวงกว้างของภัยคุกคามดังกล่าว ประเทศไทยจึงมีการจัดตั้ง “คณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ” ขึ้น (National Cyber Security Committee : NCSC) ซึ่งมีนายกรัฐมนตรีเป็นประธาน และมีหน่วยงานที่เกี่ยวข้องด้านความมั่นคง กระบวนการยุติธรรม และด้านเศรษฐกิจ ร่วมเป็นกรรมการฯ มีหน้าที่หลักในการจัดทำนโยบายความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อให้ประเทศไทยมีขีดความสามารถในการปกป้อง ป้องกัน รับมือ และลดความเสี่ยงจากสถานการณ์ด้านภัยคุกคามในไซเบอร์ ที่กระทบต่อความมั่นคงของชาติ ทั้งจากภายในและภายนอกประเทศ ครอบคลุมถึงความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ และความมั่นคงทางเศรษฐกิจ นอกจากนี้ยังได้กำหนดยุทธศาสตร์หลัก ๓ ด้าน ยุทธศาสตร์รอง ๕ ด้าน เพื่อเป็นกรอบในการพัฒนาการรักษาความมั่นคงปลอดภัยทางสารสนเทศสำหรับประเทศไทยในอีก ๕ ปี

เนื่องจากความมั่นคงปลอดภัยทางสารสนเทศเกี่ยวข้องกับองค์ความรู้หลายด้าน และองค์ความรู้เหล่านั้น เป็นเครื่องมือที่สำคัญที่สุดในการรักษาความมั่นคงปลอดภัย การกำหนดแนวทางในการรวบรวมความรู้ สนับสนุนการสร้างความรู้ เผยแพร่ความรู้ และสนับสนุนให้มีการนำความรู้ไปใช้งาน ถือเป็นองค์ประกอบหนึ่งที่ทำให้การรักษาความมั่นคงปลอดภัยเกิดประสิทธิภาพและประสิทธิผลสูงสุด ผู้วิจัยจึงเห็นว่าควรที่จะมีการศึกษาและวิจัย เพื่อให้ได้แนวความคิดในการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศไทยต่อไป

วัตถุประสงค์การวิจัย

๑. เพื่อศึกษาวิเคราะห์ปัญหา สาเหตุและผลกระทบที่เกิดจากภัยคุกคามต่อความมั่นคงของชาติในด้านต่าง ๆ เช่น เศรษฐกิจ สังคม วัฒนธรรม การเมือง และการทหาร เป็นต้น

๒. เพื่อศึกษา วิเคราะห์ เปรียบเทียบ แนวทางต่าง ๆ ในการรักษาความมั่นคงปลอดภัยทางสารสนเทศ

๓. เพื่อเสนอแนะแนวทางที่เหมาะสมในการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศไทยในอนาคต

ขอบเขตของการวิจัย

ศึกษา วิเคราะห์บทบาท และผลกระทบของเทคโนโลยีสารสนเทศต่อความมั่นคงด้านเศรษฐกิจ สังคม วัฒนธรรม การเมืองและอื่นๆ ที่สำคัญของประเทศไทย ประเทศที่มีความก้าวหน้าทางเทคโนโลยีสารสนเทศ และประเทศที่มีอิทธิพลทางการทหาร รวมถึงศึกษาแนวทาง ขั้นตอนการดำเนินการ และอุปสรรคข้อขัดข้อง ในการรักษาความมั่นคงปลอดภัยทางสารสนเทศ สังเคราะห์ให้ได้แนวทางในการป้องกัน ต่อต้าน และบรรเทาผลกระทบที่เกิดจากภัยคุกคามทางไซเบอร์ของประเทศไทยในอนาคต

วิธีดำเนินการวิจัย

๑. ดำเนินการวิจัยเชิงคุณภาพ โดยรวบรวม ศึกษาและวิเคราะห์ข้อมูลที่ได้จากการศึกษาค้นคว้า จากแหล่งต่าง ๆ ทั้งในประเทศและต่างประเทศ

๒. ศึกษาแนวทาง ขั้นตอนการดำเนินการ อุปสรรค ข้อขัดข้องการรักษาความมั่นคงปลอดภัยทางสารสนเทศของหน่วยงานต่าง ๆ ในประเทศไทยในปัจจุบัน

๓. ศึกษาแนวทาง และวิเคราะห์เปรียบเทียบ แนวทางการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศต่าง ๆ

๔. วิเคราะห์เพื่อหาข้อสรุป แนวทางการรักษาความมั่นคงปลอดภัยทางสารสนเทศในระยะสั้น ระยะกลาง และระยะยาว เพื่อป้องกัน ต่อต้าน และบรรเทาผลกระทบที่เกิดจากภัยคุกคามทางไซเบอร์ให้เกิดประสิทธิภาพ และประสิทธิผลสูงสุด

ผลการวิจัย

จากผลการศึกษาวิเคราะห์ ปัญหา สาเหตุและผลกระทบที่เกิดจากภัยคุกคามทางไซเบอร์ต่อความมั่นคงปลอดภัยในด้านต่างๆ ทำให้สามารถจำแนกประเภทของภัยคุกคามที่มีผลกระทบต่อความมั่นคงของประเทศ ได้เป็น ๔ ประเภทใหญ่ๆ ได้แก่

๑. ภัยคุกคามต่อความมั่นคงทางเศรษฐกิจ

๒. ภัยคุกคามต่อสังคมและจิตวิทยา

๓. ภัยคุกคามต่อความมั่นคงทางทหาร

๔. ภัยคุกคามในรูปแบบการก่อการร้าย

จากการวิเคราะห์และและหาสาเหตุของปัญหารวมทั้งผลกระทบที่เกิดขึ้น เพื่อหาแนวทางในการแก้ไขปัญหาให้ได้ผลเป็นรูปธรรม สรุปได้ดังนี้

๑. การบริหารจัดการการรักษาความมั่นคงปลอดภัย

การดำเนินการตามยุทธศาสตร์ของคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติมีนายกรัฐมนตรีเป็นประธาน ได้กำหนดยุทธศาสตร์หลัก ๓ ด้าน ยุทธศาสตร์รอง ๕ ด้าน ยังไม่ได้กำหนดหน่วยงานใดเป็นหน่วยงานหลักมารองรับการดำเนินการของคณะกรรมการดังกล่าวให้เห็นผลเป็นรูปธรรม เพื่อดำเนินการบูรณาการงานด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศให้สามารถแปลงนโยบายและยุทธศาสตร์ของคณะกรรมการฯ มาสู่การปฏิบัติได้อย่างต่อเนื่องและมีประสิทธิผล ทั้งนี้หน่วยงานต่างๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางสารสนเทศ ได้แก่ กห. กระทรวง ICT (สพธอ.และสำนักป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศ) สตช.(กลุ่มงาน

ตรวจสอบและวิเคราะห์การกระทำความผิดทางเทคโนโลยี กองบังคับการสนับสนุนทางเทคโนโลยี (บก.สสท.) และกองบังคับการปราบปรามการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.)) และหน่วยงานด้านการวิจัย ได้แก่ กห.(สำนักงานเทคโนโลยีป้องกันประเทศ (สทป.)) วท. (NECTEC) รวมทั้งหน่วยงานที่เกี่ยวข้องกับไซเบอร์เกตเวย์ของประเทศ ได้แก่ กระทรวง ICT (TOT และ กสท) ก็ยังขาดการบูรณาการงานในภาพรวมของการดำเนินการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางสารสนเทศ โดยยังเป็นการดำเนินการแบบเอกเทศทั้งในระดับนโยบายและระดับปฏิบัติการเพื่อรองรับภารกิจของแต่ละกระทรวงหรือหน่วยงานตนเองเท่านั้น ทำให้ขาดศักยภาพในการดำเนินการรับมือกับภัยคุกคามรูปแบบต่างๆ

๒. บุคลากร

ศักยภาพด้านสงครามไซเบอร์ในประเทศไทย ในมุมมองจากผู้ที่เกี่ยวข้องและนักวิชาการมีความเห็นตรงกันว่าขีดความสามารถด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศไทยยังอยู่ในระดับต่ำในภาครัฐ (ฝ่ายพลเรือน และฝ่ายความมั่นคง) ซึ่งดูได้จากตัวชี้วัดเช่น จำนวนบุคลากรที่มีความเชี่ยวชาญด้านไซเบอร์ จึงจำเป็นต้องมีการบูรณาการทั้งด้านการบริหารจัดการ บุคลากรที่มีจำนวนจำกัด รวมทั้งการส่งเสริมสร้างนักวิจัย

๓. กฎหมายและ พ.ร.บ.ที่เกี่ยวข้อง

พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ และ พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๔๔ ยังไม่สามารถรองรับภัยคุกคามด้านสังคมและจิตวิทยา รวมทั้งภัยคุกคามอื่นๆ ไม่ว่าจะเป็นทางด้านการทหาร การรับมือกับการก่อการร้าย การกระทำความผิดผ่านทางเครือข่ายสารสนเทศ พบว่ามีปัญหาการตรวจจับและควบคุมไม่ให้กระทำความผิดเพิ่มมากขึ้น ทำได้ยากและใช้เวลานาน การค้นหาเว็บไซต์ที่เผยแพร่ข้อมูลที่ผิดกฎหมาย เช่นการหมิ่นสถาบันพระมหากษัตริย์ฯ การปลุกระดมทางการเมืองให้เกิดความขัดแย้งแล้วทำการปิดกั้นเว็บไซต์ดังกล่าว ซึ่งใช้ระยะเวลานานเมื่อดำเนินการตามกฎหมาย พบว่าไม่ได้ช่วยลดความเสียหายที่เกิดขึ้น รวมทั้งการจับกุมผู้กระทำความผิดเป็นไปได้ยากเนื่องจากมีการซ่อนพลางแหล่งที่มาของผู้กระทำผิด

นอกจากนี้ช่องทางการเชื่อมต่อเครือข่ายอินเทอร์เน็ตภายในประเทศกับเครือข่ายอินเทอร์เน็ตต่างประเทศผ่านหน่วยงานรัฐ ผู้ให้บริการอินเทอร์เน็ตทั้งภาครัฐและเอกชน มีเป็นจำนวนมาก ดังนั้นการตรวจสอบและสกัดกั้นข้อมูลการจราจรทางอินเทอร์เน็ตตามกฎหมาย การควบคุมข้อมูลที่ผิดกฎหมายหรือมีผลกระทบต่อความมั่นคง รวมทั้งการป้องกันการโจมตีทางไซเบอร์ จึงทำได้ค่อนข้างยาก

๔. โครงสร้างพื้นฐานของประเทศ

คณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ได้กำหนดไว้ในยุทธศาสตร์ข้อ ๓ “การป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ ปกป้องโครงสร้างพื้นฐานสำคัญของ

ประเทศและระบบสารสนเทศที่เกี่ยวข้อง" อย่างไรก็ตามยังไม่มีการดำเนินการกำหนดอุตสาหกรรมและระบบสาธารณูปโภคสำคัญที่เกี่ยวกับโครงสร้างพื้นฐานสำคัญของประเทศที่ชัดเจน

จากการวิเคราะห์ภัยคุกคามและสาเหตุของปัญหารวมทั้งผลกระทบที่เกิดขึ้น เพื่อหาแนวทางการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศไทย จึงจำเป็นต้องมีการบูรณาการงานด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศของหน่วยต่างๆ เพื่อให้สามารถแปลงนโยบายและยุทธศาสตร์ของคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติมาสู่การปฏิบัติได้อย่างเป็นรูปธรรม โดยสามารถจัดแบ่งการดำเนินการออกเป็นระยะสั้น ระยะกลาง และระยะยาว สรุปได้ดังนี้

การบูรณาการงานรักษาความมั่นคงปลอดภัยทางสารสนเทศแห่งชาติ มีเป้าหมายได้แก่ จัดตั้งหน่วยงานรักษาความมั่นคงปลอดภัยทางสารสนเทศแห่งชาติ เป็นหน่วยงานหลักระดับชาติ รับผิดชอบงานด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศ โดยมีโครงสร้างการบริหาร การรักษาความมั่นคงปลอดภัยระดับชาติ พร้อมบทบาทหน้าที่ในการประสานความร่วมมือ มีอำนาจสั่งการ ลงโทษ (ตามกลไกการดำเนินงานของรัฐ) รองรับ กำกับ ตรวจสอบ ประเมิน มีความสามารถในการพัฒนา วิจัย และเตรียมความพร้อมด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศ รวมทั้งมีศักยภาพในการตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยทางสารสนเทศ สามารถรับมือภัยคุกคามได้ทุกรูปแบบ

๑. การดำเนินการในระยะสั้น เห็นควรให้กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เป็นเจ้าภาพหลักในการดำเนินการในระยะสั้นดังนี้

๑.๑ ศึกษาผลกระทบของการปรับโครงสร้างหน่วยงานต่างๆที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางสารสนเทศ

๑.๒ ศึกษาผลกระทบด้านกฎหมายที่เกี่ยวข้องกับการปฏิบัติการทางไซเบอร์ในเชิงรุก รวมทั้งกฎหมายเกี่ยวข้องกับการตรวจสอบการกระทำความผิดทางอินเตอร์เน็ต การเข้าถึงข้อมูลทางอินเตอร์เน็ต (Lawful Interception)

๑.๓ สำรวจและกำหนดอุตสาหกรรมและระบบสาธารณูปโภคสำคัญที่เกี่ยวกับโครงสร้างพื้นฐานสำคัญของประเทศ (Critical Infrastructure Security) ครอบคลุมกลุ่มสำคัญ ประกอบด้วย กลุ่มอุตสาหกรรมเคมี เชื่อนและโรงงานไฟฟ้า อุตสาหกรรมป้องกันประเทศ กลุ่มพลังงาน หน่วยงานรัฐบาล กลุ่มคมนาคมและการขนส่ง กลุ่มอาหาร กลุ่มงานด้านเทคโนโลยีสารสนเทศ กลุ่มงานด้านอาหาร กลุ่มการเงินและธนาคาร

๑.๔ สำรวจบุคลากรที่มีศักยภาพด้านสงครามไซเบอร์ในระดับประเทศ

๒. การดำเนินการในระยะกลาง เห็นควรให้กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เป็นเจ้าภาพหลักในการดำเนินการในระยะกลางดังนี้

๒.๑ ผลักดันให้มีการตรวจสอบการกระทำความผิดทางอินเตอร์เน็ต โดยมีการออกกฎหมายในการเข้าถึงข้อมูลทางอินเตอร์เน็ต (Lawful Interception)

๒.๒ ปรับปรุงกฎหมายระหว่างประเทศเพื่อรองรับการปฏิบัติการทางไซเบอร์ในเชิงรุก

๒.๓ ผลักดันให้มีการทำไซเบอร์เกตเวย์แห่งชาติ (National Cyber Gateway)

๒.๔ ประสานความร่วมมือ ทั้งระหว่างภาครัฐ เอกชน รวมทั้งความร่วมมือระหว่างประเทศในการสร้างเครือข่ายการรักษาความมั่นคงปลอดภัยทางสารสนเทศ

๒.๕ ส่งเสริมและสร้างบุคลากร นักวิจัย ในทุกระดับชั้นให้มีองค์ความรู้ด้านการรักษาความมั่นคงปลอดภัยทางสารสนเทศ จนถึงระดับแฮกเกอร์

๓. การดำเนินการในระยะยาว

๓.๑ จัดตั้งหน่วยงานรักษาความมั่นคงปลอดภัยทางสารสนเทศแห่งชาติ ทำหน้าที่ดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางสารสนเทศของประเทศ และบูรณาการงานด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศกับหน่วยงานทุกภาคส่วน ทั้งฝ่ายความมั่นคง ทหาร ภาครัฐและเอกชน กำหนดให้เป็นหน่วยขึ้นตรงกับนายกรัฐมนตรี ภายใต้การกำกับดูแลของคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติที่มีนายกรัฐมนตรีเป็นประธาน

๓.๒ ปรับโครงสร้างของศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ ให้เป็นหน่วยงานระดับชาติและขึ้นตรงต่อหน่วยงานรักษาความมั่นคงปลอดภัยทางสารสนเทศแห่งชาติ ทำหน้าที่ตอบสนองและจัดการกับสถานการณ์ด้านความมั่นคงปลอดภัยทางสารสนเทศ และให้การสนับสนุนและคำแนะนำในการแก้ไขภัยคุกคามทางสารสนเทศที่เกิดขึ้น โดยโครงสร้างของศูนย์ฯ ต้องมีขีดความสามารถรองรับงานไซเบอร์เกตเวย์แห่งชาติ เพื่อทำหน้าที่แก้ปัญหาการกระทำความผิดผ่านทางระบบสารสนเทศ รวมถึงดำเนินการปิดกั้นข้อมูลที่ก่อให้เกิดผลกระทบต่อความมั่นคงของชาติขึ้น โดยใช้บุคลากรบางส่วนจาก กสท. และ TOT รวมทั้งการ Outsource จากภาครัฐ เอกชน โดยรวมการเครื่องมือที่เกี่ยวข้องกับเกตเวย์ของทั้ง กสท. และ TOT

๓.๓ จัดตั้งศูนย์รวมความเป็นเลิศด้านไซเบอร์ ขึ้นตรงกับหน่วยงานรักษาความมั่นคงปลอดภัยทางสารสนเทศแห่งชาติ ทำหน้าที่วิจัยและพัฒนาเพื่อความมั่นคงปลอดภัยทางสารสนเทศ และศึกษาติดตามภัยคุกคามรูปแบบใหม่ๆ ที่จะเป็นภัยคุกคามกับประเทศในอนาคต โดยกำลังพลหลักมาจากหน่วยงานวิจัยพัฒนาของหน่วยต่างๆ ที่มีศักยภาพในด้านไซเบอร์ ได้แก่ กห.(สทป.) วท.(NECTEC) รวมทั้งหน่วยงานภาครัฐและเอกชน

ข้อเสนอแนะ

การกำหนดให้การรักษาความมั่นคงปลอดภัยทางสารสนเทศ เป็นวาระแห่งชาติเร่งด่วน