นิติปรัชญากับการศึกษาวิเคราะห์ร่างพระราชบัญญัติความมั่นคงไซเบอร์

ชูเกียรติ น้อยฉิม[1] และ วรณัฐ บุญเจริญ[2]

บทคัดย่อ

ไซเบอร์สเปซเป็นเขตแดนเสมือนและเมื่อมีผู้ใช้ระบบเครือข่ายคอมพิวเตอร์และอินเตอร์เน็ตมากยิ่งขึ้น ก็ยิ่งทำให้ความซับซ้อนของไซเบอร์สเปซมีเพิ่มมากขึ้น เนื่องจากพัฒนาการทางเทคโนโลยีที่แผ่ขยายเข้าไปยังทุกภาคส่วนของสังคมโลก ซึ่งอาจจะก่อให้เกิดอาชญากรรมทางคอมพิวเตอร์ประเภทหนึ่งที่เรียกว่า “สงครามไซเบอร์ (Cyber warfare)” ที่เป็นภัยอย่างยิ่งต่อความมั่นคงของโลก ดังนั้น ในปัจจุบันประชาคมโลกจึงมีแนวคิดในการที่จะจัดระเบียบสังคมอินเตอร์เน็ตขึ้นเพื่อเตรียมการรับมือกับอาชญากรรมทางคอมพิวเตอร์ โดยการจัดตั้งหน่วยงานที่ดูแลเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ขึ้นและมีการสร้างกฎเกณฑ์มาปกป้องไซเบอร์สเปซ สำหรับประเทศไทยก็เช่นเดียวกันที่ได้มีการตราร่างพระราชบัญญัติความมั่นคงไซเบอร์ขึ้นมาเพื่อใช้รับมืออาชญากรรมทางคอมพิวเตอร์ (ไซเบอร์) แต่อย่างไรก็ตาม ร่างพระราชบัญญัตินี้ได้รับการวิพากย์วิจารณ์ถึงความเป็นมาตรฐานสากลในการที่จะนำมาใช้ และจากการศึกษาวิเคราะห์โดยใช้หลักทางนิติปรัชญาพบว่า ประเทศไทยควรที่จะปรับปรุงร่างกฎหมายฉบับนี้ให้อยู่บนพื้นฐานของเหตุผล โดยเคารพซึ่งสิทธิเสรีภาพของประชาชน รวมทั้งควรมีการระบบการคานอำนาจและตรวจสอบอำนาจรัฐในกรณีที่เจ้าพนักงานและคณะกรรมการฯตามร่างพระราชบัญญัตินี้อาจใช้อำนาจทางกฎหมายเกินกว่าขอบอำนาจ

---

[1] อาจารย์ประจำสำนักวิชานิติศาสตร์ มหาวิทยาลัยแม่ฟ้าหลวง จังหวัดเชียงราย

[2] ผู้เชี่ยวชาญด้านกฎหมายคอมพิวเตอร์, นิติศาสตรบัณฑิตและนิติศาสตรมหาบัณฑิต, สำนักวิชานิติศาสตร์ มหาวิทยาลัยแม่ฟ้าหลวง จังหวัดเชียงราย

คำสำคัญ: ไซเบอร์สเปซ / นิติปรัชญา / อาชญากรรมทางคอมพิวเตอร์ / สงครามไซเบอร์ / ความมั่นคงไซเบอร์

Abstract

Cyberspace is the virtual frontier. The more its user's increases, the more complicate it becomes. The information and communication technology which was implemented in every segments of the world society made the computer crime threat called "Cyber Warfare" much more imminent. Therefore, the global society has been attempted to govern the internet by establishing monitoring organizations and enacted the law to protect cyber space. Thailand, as one of the countries in concern, has also drafted cybercrime legislation called Cyber Security Act 2015. However, the draft Act was criticized and forced to retreat because of legal standard issue. By reviewing legal philosophy, the findings point out that Thailand should amend the Cyber Security Act draft base on people's consent and rationality with respect of its citizen's rights, including the check and balance of government power in case the authorities was abused by the committee or officers appointed by this Act.

Keywords: Cyberspace / Legal Philosophy / Computer Crime / Cyber warfare / Cyber Security

1. บทนำ

ปัจจุบัน ระบบคอมพิวเตอร์และอินเตอร์เน็ตได้ถูกพัฒนาให้มีความก้าวหน้าและมีความซับซ้อนมากยิ่งขึ้นในการนำไปใช้ประโยชน์ในด้านต่างๆ เนื่องด้วยวิทยาการและเทคโนโลยีสมัยใหม่นี้ง่ายต่อการเข้าถึงในทุกระดับของสังคม ดังนั้นจึง

เป็นสาเหตุหนึ่งที่ทำให้อาชญากรรมทางคอมพิวเตอร์มีความหลากหลายและซับซ้อนตามไปด้วย และด้วยลักษณะของอินเตอร์เน็ตที่เป็นระบบโครงข่ายการสื่อสารที่เชื่อมโยงเข้าด้วยกันในระดับระหว่างประเทศ จึงได้ก่อให้เกิดอาชญากรรมทางคอมพิวเตอร์ประเภทหนึ่งที่เรียกว่า “สงครามไซเบอร์ (Cyber warfare)[3]” หรือ สงครามข้อมูลข่าวสาร โดยใช้วิธีการโจมตีระบบเครือข่ายส่วนบุคคลและขยายขอบเขตเป็นสงครามระดับประเทศและระดับโลกที่เป็นภัยอย่างยิ่งต่อความมั่นคงของประชาคมโลก เพราะสามารถก่อให้เกิดความเสียหายได้เป็นวงกว้างมากขึ้น เนื่องจากสงครามไซเบอร์[4] มีศักยภาพสูงในการเข้าแทรกซึมด้านข้อมูลข่าวสาร เพื่อก่อกวน ก่อความไม่สงบ หรือสร้างความแตกแยกในสังคม ที่อาจก่อให้เกิดความเปลี่ยนแปลงทั้งในระดับประเทศและระดับระหว่างประเทศได้ รวมถึงการจารกรรมข้อมูลลับทางการทหารด้วย ปัจจุบันนี้ประเทศต่างๆ ได้เกิดความตื่นตัวและเตรียมความพร้อมในการรับมือกับสงครามไซเบอร์ โดยทำการ (1) จัดตั้งหน่วยงานในการรับมืออาชญากรรมทางคอมพิวเตอร์ประเภทนี้ขึ้นมา และ (2) สร้างกฎเกณฑ์มาปกป้องขอบเขตทาง ไซเบอร์สเปซ (ยุทธศาสตร์ในพรหมแดนที่ 3) ที่มีการเปลี่ยนแปลงอยู่ตลอดเวลา ซึ่งเป็นความ ท้าทาย

[3] สงครามไซเบอร์ (Cyber warfare) เป็นคำที่นิยามขึ้นมาโดยผู้เชี่ยวชาญด้านระบบความปลอดภัยของรัฐบาลสหรัฐอเมริกา โดย ริชาร์ด เอ. คลาร์ก กล่าวว่า “เป็นการกระทำของรัฐ-ชาติ เพื่อแทรกซึมไปยังระบบคอมพิวเตอร์หรือเครือข่าย มีจุดประสงค์เพื่อทำลายหรือสร้างความแตกแยก”, Clarke, R. A., & Knake, R., *Cyber war: The next threat to national security and what to do about it*, (New York: HarperCollins, 2012).

[4] ลักษณะเด่นของสงครามไซเบอร์ คือ (1) ไม่สามารถระบุตัวตนและที่ตั้งของผู้โจมตี (Attacker) ได้โดยง่าย ผู้โจมตีสามารถปฏิบัติการที่ใดก็ได้ในโลก (2) สภาพลมฟ้าอากาศไม่เป็นปัจจัยในการโจมตี (3) เป้าหมายของผู้โจมตีมีหลากหลายและจำนวนมากขึ้นทุกขณะ (4) การโจมตีใช้ทรัพยากรน้อย (งบประมาณต่ำ) และสามารถหาได้ทั่วไป (5) จำนวนผู้โจมตีไม่ใช่ปัจจัยแห่งความสำเร็จแห่งชัยชนะ (6) ปัจจัยแห่งความสำเร็จคือการรักษาความลับและความรู้ ความเชี่ยวชาญของผู้โจมตี

และเป็นสิ่งที่ต้องเผชิญอย่างหลีกเลี่ยงไม่ได้ ดังนั้น เพื่อรับมือกับอาชญากรรมและสงครามยุคใหม่ในโลกดิจิตอลอย่างเร่งด่วน องค์การสหประชาชาติจึงได้มีการจัดทำคู่มือป้องกันและควบคุมอาชญากรรมคอมพิวเตอร์ขึ้น สำหรับประเทศไทยนั้นก็ได้เร่งปรับตัว และปรับปรุงการดำเนินงานให้ก้าวทันกระแสของการเปลี่ยนแปลงดังกล่าว โดยเฉพาะภัยทางด้านอาชญากรรมคอมพิวเตอร์ที่นับวันจะทวีความรุนแรงมากขึ้น โดยประเทศไทยได้กำหนดยุทธศาสตร์และออกมาตรการทางกฎหมาย เพื่อรับมือกับอาชญากรรมทางคอมพิวเตอร์ขึ้น โดยได้มีการร่างพระราชบัญญัติความมั่นคงไซเบอร์ออกมา แต่อย่างไรก็ตามร่างพระราชบัญญัตินี้ได้รับการวิพากษ์วิจารณ์เป็นอย่างมากในสังคมไทยขณะนี้ ถึงความเป็นมาตรฐานที่ควรจะอยู่บนพื้นฐานของแนวคิดและหลักกฎหมายที่ถูกต้องเหมาะสม โดยบทความนี้มุ่งที่จะศึกษาวิเคราะห์ร่างพระราชบัญญัติความมั่นคงไซเบอร์ของประเทศไทยว่าเป็นไปตามมาตรฐานสากลหรือไม่ โดยจะใช้หลักทฤษฎีทางด้านนิติปรัชญามาใช้ในการศึกษาวิเคราะห์ เช่น แนวคิดทฤษฎีของสำนักกฎหมายธรรมชาติและสำนักกฎหมายบ้านเมือง ฯลฯ

2. สภาพปัญหาในปัจจุบันที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์

ปัจจุบันเทคโนโลยีสารสนเทศ (Information and Communication Technology: ICT) นั้น มีอยู่ในอุปกรณ์หรือผลิตภัณฑ์เครื่องมือเครื่องใช้แทบทุกอย่าง และแนวโน้มของการสร้างสรรค์สิ่งต่างๆ ได้ถูกแปลงให้อยู่ในรูปแบบดิจิตอล (Digitalization) ที่มีความต้องการเชื่อมต่อทางอินเตอร์เน็ต (*อินเตอร์เน็ตจัดเป็นหนึ่งในสาขาที่มีพัฒนาการรวดเร็วที่สุดในสาขาของพัฒนาการทางวิทยาการ*[5]) มากขึ้น เพื่อที่จะทำให้เกิดการบูรณาการเทคโนโลยีสารสนเทศดังกล่าวเข้าไปเป็นส่วนหนึ่งของ

[5] International Telecommunication Union, The world information society report 2007, (2007, June), Retrieved 2013, November, 10, from http://www.itu.int/osg/spu/publications/worldinformationsociety/2007/

ผลิตภัณฑ์ต่างๆ ซึ่งแต่เดิมในอดีตสามารถใช้งานได้โดยไม่จำเป็นต้องมีการเชื่อมต่ออินเตอร์เน็ต เช่น สาธารณูปโภคต่างๆ รวมทั้งปฏิบัติการทางทหารและการขนส่ง ฯลฯ การเติบโตของสังคมข้อมูลข่าวสารในปัจจุบันทำให้ด้านสาธารณูปโภคที่สำคัญเช่น ประปา ไฟฟ้า ระบบควบคุมการจราจร หรือระบบโทรคมนาคมต้องพึ่งพาการเชื่อมต่อหรือดำเนินการของเทคโนโลยีสารสนเทศเพื่อความมีเสถียรภาพ แต่อย่างไรก็ดีเทคโนโลยีสารสนเทศดังกล่าวนี้ก็มาพร้อมกับภัยอันตรายที่ร้ายแรงรูปแบบใหม่ ดังนั้นหากมีการจู่โจมโครงสร้างพื้นฐานทางข้อมูลข่าวสารและบริการอินเตอร์เน็ต จึงเป็นการสั่นคลอนความมั่นคงของสังคมและถือว่าอาชญากรรมทางคอมพิวเตอร์ประเภทนี้มีศักยภาพสูง โดยอาชญากรรมดังกล่าวมีมาในหลายรูปแบบด้วยกัน ทั้งการฉ้อโกงออนไลน์ การเผยแพร่ภาพลามกอนาจารเด็กและการเจาะระบบต่างเป็นเพียงตัวอย่างบางประการของอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ที่แผ่ขยายเป็นวงกว้างมากขึ้นในทุกๆ วัน ความเสียหายทางเศรษฐกิจที่เกิดจากอาชญากรรมคอมพิวเตอร์ที่เรียกว่าสงครามไซเบอร์นั้นมหาศาล เพียงแค่ในปี พ.ศ. 2546 เกิดความเสียหายจากโปรแกรมประสงค์ร้าย (Malicious software: Malware) ต่อเศรษฐกิจเกินหมื่นเจ็ดพันล้านเหรียญสหรัฐ[6] จากการประมาณ ผลประโยชน์จากการก่ออาชญากรรมคอมพิวเตอร์มีมากกว่าแสนล้านเหรียญสหรัฐในปี พ.ศ. 2550 ล้ำหน้าธุรกิจการค้ายาเสพย์ติดเป็นครั้งแรก[7] โดยกว่า 60% ของภาคธุรกิจในสหรัฐอเมริกาเชื่อว่าอาชญากรรมทางคอมพิวเตอร์สร้างความเสียหายแก่พวกเขามากกว่าอาชญากรรมประเภทอื่น สิ่งเหล่านี้แสดงให้เห็นถึงความสำคัญในการปกป้องโครงสร้างขั้นพื้นฐานทางข้อมูลข่าวสาร (ความมั่นคงไซเบอร์) และอันตรายจากภัยของอาชญากรรมคอมพิวเตอร์ต่อสังคมโลกในปัจจุบัน แต่

---

[6] Congressional Research Service, The economic impact of cyber-attacks, (Washington, DC: CRS, 2004), 10.

[7] O'Connell, K., Cyber-crime hits $100 billion in 2007, (2007, October 17). Retrieved 2013, October 17, from http://www.ibls.com/internet_law_news_portal_view_prn.aspx?s= latestnews&id=1882

อย่างไรก็ตามในปัจจุบันอาชญากรรมทางคอมพิวเตอร์ ยังไม่มีคำนิยามที่ชัดเจนและเป็นที่ยอมรับกันโดยทั่วไป หากแต่สามารถกล่าวได้อย่างกว้างๆ ว่าเป็นอาชญากรรมที่ถูกกระทำโดยมีคอมพิวเตอร์เป็นเครื่องมือหรือมีข้อมูลทางคอมพิวเตอร์เป็นเป้าหมาย โดยอาชญากรรมทางคอมพิวเตอร์ตามกฎหมายระหว่างประเทศ เช่น อนุสัญญาอาชญากรรมคอมพิวเตอร์ ค.ศ. 2001 (Convention on Cybercrime) ถือว่าเป็นการทำละเมิดที่กระทำต่อปัจเจกชนหรือกลุ่มบุคคลด้วยเจตนาร้ายในการทำให้เสื่อมเสียชื่อเสียงหรือก่อให้เกิดความเสียหายทางร่างกายหรือจิตใจ ไม่ว่าโดยทางตรงหรือทางอ้อม โดยการกระทำดังกล่าวอาจเป็นอันตรายต่อความมั่นคงและเศรษฐกิจระดับชาติ โดยการใช้คอมพิวเตอร์หรืออุปกรณ์ที่เกี่ยวข้องเป็นเครื่องมือกระทำความผิด ทั้งนี้ผู้เขียนเห็นว่าอาชญากรรมคอมพิวเตอร์ในปัจจุบันนี้ ได้เปลี่ยนแปลงไปจากอดีตเป็นอย่างมาก จากเดิมที่มีเป้าหมายเพียงข้อมูลทางคอมพิวเตอร์เท่านั้น มาเป็นตัวผู้ใช้คอมพิวเตอร์แม้กระทั่งใช้เป็นอาวุธในการทำสงครามหรือจู่โจมระบบโครงสร้างพื้นฐาน ดังนั้นอาชญากรรมทางคอมพิวเตอร์จึงควรมีความหมายรวมไปถึงความผิดใดๆ ที่ใช้คอมพิวเตอร์เป็นเครื่องมือไม่ว่าเป้าหมายจะเป็นอะไรก็ตาม

2.1 แนวคิดและทฤษฎีเกี่ยวกับความมั่นคงไซเบอร์

ไซเบอร์สเปซเป็นเขตแดนเสมือนที่ไม่สามารถจับต้องได้และยิ่งมีผู้ใช้ระบบเครือข่ายคอมพิวเตอร์มากขึ้น ก็ยิ่งทำให้การแผ่ขยายและความซับซ้อนของไซเบอร์สเปซมีเพิ่มมากขึ้นตามไปด้วยเพราะว่าธรรมชาติของอินเตอร์เน็ตทำให้เกิดการสื่อสารกันระหว่างบุคคลที่ต่างฝ่ายไม่อาจระบุตำแหน่งของแต่ละฝ่ายได้อย่างชัดเจนแน่นอน เพราะการเคลื่อนไหวของข้อมูลบนระบบเครือข่ายเป็นอิสระจากตำแหน่งพื้นที่ทางกายภาพ ข้อมูลสามารถถูกส่งจากจุดหนึ่งไปยังจุดหนึ่งอย่างรวดเร็วจนไม่สามารถชี้วัดแนวความคิดว่าด้วย “ระยะทาง” บนพรหมแดนไซเบอร์ได้ ดังนั้น สังคมโลกจึงมีแนวคิดในเรื่องการกำกับดูแลอินเตอร์เน็ต (Internet governance) ขึ้น สำหรับแนวคิดในการที่จะจัดระเบียบสังคมอินเตอร์เน็ตนี้ได้ถูกนำมาอภิปรายกันอย่างกว้างขวางในการประชุมนานาชาติหลายเวที เช่น การประชุมสุดยอดของโลกว่าสังคมข้อมูลข่าวสาร ครั้ง

ที่ 1 (World Summit on Information Society: WSIS) ซึ่งจัดขึ้น ณ กรุงเจนีวา ประเทศสวิสเซอร์แลนด์ ในเดือนธันวาคม พ.ศ. 2546 และ ครั้งที่ 2 ณ กรุงตูนิส ประเทศตูนีเซีย ในเดือนมิถุนายน พ.ศ. 2548 โดยทางคณะทำงานด้านการกำกับดูและอินเตอร์เน็ต ได้ให้คำนิยามการกำกับดูแลอินเตอร์เน็ตไว้ว่า “การกำกับดูแลอินเตอร์เน็ต คือ การที่ภาครัฐและเอกชน รวมทั้งภาคประชาสังคมได้คำนึงถึงกฎเกณฑ์และหลักเกณฑ์ต่างๆ ที่ใช้ร่วมกัน ประเพณีปฏิบัติ กระบวนการตัดสินใจ และโครงการเพื่อกำหนดทิศทางของวิวัฒนาการและการใช้ประโยชน์จากอินเตอร์เน็ต”[8] ภายหลังจากที่ประชุมสุดยอดโลกว่าด้วยสังคมข้อมูลข่าวสารนี้ คณะทำงานเรื่องการกำกับดูแลอินเตอร์เน็ต (The Working Group on Internet Governance: WGIG) ได้นำเสนอรูปแบบกลไกทางกฎหมายที่เหมาะสมสำหรับการกำกับดูแลอินเตอร์เน็ต โดยมุ่งเน้นประเด็นทางกฎหมายเกี่ยวกับกระบวนการและวิธีการสำหรับการกำกับดูแลอินเตอร์เน็ตภายใต้กรอบกฎหมายภายในประเทศและกฎหมายระหว่างประเทศ ซึ่งประเด็นที่นำเสนอดังกล่าว ได้แก่ กระบวนการมีส่วนร่วมของผู้มีส่วนได้เสีย (Stakeholders) ในการกำกับดูแลอินเตอร์เน็ต เครื่องมือทางกฎหมายระหว่างประเทศที่เหมาะสมในการกำกับดูแลอินเตอร์เน็ต ตลอดจนความสัมพันธ์ระหว่างกฎหมายระหว่างประเทศแผนกคดีเมืองและแผนกคดีบุคคลภายใต้กรอบการกำกับดูแลอินเตอร์เน็ต[9] ปัจจุบันนี้มุมมองเกี่ยวกับกลไกทางกฎหมายที่เหมาะสมในการกำกับดูแลอินเตอร์เน็ตแบ่งออกเป็น 2 กระบวนทัศน์ (Paradigms) ได้แก่

---

[8] “Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision making procedures, and programmes that shape the evolution and use of the internet.”, Regional Internet Governance Forum, *About APrIGF 2011*.

[9] สราวุธ ปิติยาศักดิ์, *กฎหมายเทคโนโลยีสารสนเทศ*, 13.

1. กระบวนทัศน์ในทางบวก (Techno-optimism)

ผู้สนับสนุนกระบวนทัศน์นี้สนับสนุนพัฒนาการของกฎหมายไซเบอร์ (Cyber law) โดยเห็นว่าอินเตอร์เน็ตเป็นวิธีการสื่อสารสมัยใหม่ เป็นการสื่อสารไร้พรหมแดน ทำให้เกิดอุปสรรคต่อกฎหมายที่บังคับใช้อยู่ ฉะนั้นกฎหมายไซเบอร์จึงมีความจำเป็นอย่างยิ่งและต้องการการพัฒนาที่ต่อเนื่อง[10]

2. กระบวนทัศน์เทคโนตามความเป็นจริง (Techno-realist)

ผู้สนับสนุนกระบวนทัศน์นี้เห็นว่าอินเตอร์เน็ตไม่ได้แตกต่างจากเทคโนโลยีการสื่อสารที่มีมาก่อน เช่น โทรศัพท์ ฯลฯ เพียงแต่อินเตอร์เน็ตมีความสะดวกและรวดเร็วกว่าและครอบคลุมระยะทางได้กว้างขวางกว่าเท่านั้น ฉะนั้นกฎหมายที่บังคับอยู่ในปัจจุบันจึงนำมาใช้กับอินเตอร์เน็ตได้[11]

2.2 มาตรการทางกฎหมายที่เกี่ยวกับความมั่นคงไซเบอร์ในปัจจุบัน

เป้าหมายหลักในการสร้างความมั่นคงไซเบอร์ (อินเตอร์เน็ต) คือ การเสริมยุทธศาสตร์เพื่อการพัฒนาต้นแบบกฎหมายอาชญากรรมทางคอมพิวเตอร์ ซึ่งสามารถประยุกต์ใช้ได้ทั้งในระดับโลกและภายในประเทศ รวมทั้งมาตรการทางกฎหมายที่มีอยู่เดิมของภูมิภาคต่างๆ เพื่อที่จะสามารถพัฒนาปรับปรุงกฎหมายให้มีความสอดคล้องกันทั้งโลกในเรื่องอาชญากรรมทางคอมพิวเตอร์ รวมไปถึงการสร้างความเข้าใจร่วมกันในเรื่องความมั่นคงไซเบอร์และอาชญากรรมไซเบอร์ระหว่างประเทศ

2.2.1 มาตรการด้านความมั่นคงไซเบอร์ในระดับระหว่างประเทศ

องค์การสหประชาชาติ (United Nations: UN) ได้เริ่มพัฒนากรอบนโยบายด้านอาชญากรรมทางคอมพิวเตอร์ขึ้นในปี พ.ศ. 2533 และในการประชุมสภาว่าด้วยการป้องกันอาชญากรรมและการปฏิบัติต่อผู้กระทำผิดขององค์การสหประชาชาติ ครั้งที่ 8 ได้มีกำหนดมาตรการเกี่ยวกับอาชญากรรมคอมพิวเตอร์ขึ้น

[10] เรื่องเดียวกัน, 13.

[11] เรื่องเดียวกัน, 14.

ต่อมาในปี พ.ศ. 2537 สหประชาชาติได้จัดทำคู่มือการป้องกันและควบคุมอาชญากรรมทางคอมพิวเตอร์ (UN manual on the prevention and control of computer-related crime) ออกเผยแพร่ ซึ่งมีเนื้อหาเกี่ยวกับแนวทางการบัญญัติฐานความผิดและกฎหมายวิธีพิจารณาความที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์ รวมไปถึงกลไกความร่วมมือระหว่างประเทศ และที่ประชุมของสมัชชาใหญ่แห่งองค์การสหประชาชาติ เมื่อวันที่ 4 ธันวาคม พ.ศ. 2543 ได้มีออกข้อมติที่ 55/63 เกี่ยวกับอาญากรรมทางคอมพิวเตอร์ เพื่อ“การรับมือกับการใช้งานเทคโนโลยีข้อมูลข่าวสารในทางที่ผิดของอาชญากร”[12] โดยมีเนื้อหาดังนี้ (ก) รัฐควรทำให้แน่ใจว่ามีกฎหมายและการดำเนินการเพื่อทำลายแหล่งหลบภัยของผู้ซึ่งกระทำผิดโดยอาศัยเทคโนโลยีข้อมูลข่าวสารเป็นเครื่องมือ และ (ข) ระบบยุติธรรมควรคุ้มครองความลับ ความสมบูรณ์ และสภาพพร้อมใช้งานของข้อมูลและระบบคอมพิวเตอร์ จากการเข้ามาสร้างความเสียหายโดยไม่ได้รับอนุญาต และรับรองว่าการกระทำผิดของอาชญากรต้องได้รับการลงโทษ นอกจากนี้ ข้อมติที่ 56/121 ของที่ประชุมของสมัชชาใหญ่แห่งองค์การสหประชาชาติก็ได้เชิญชวนให้ประเทศสมาชิกนำเอางานและผลสัมฤทธิ์ของคณะกรรมการป้องกันอาชญากรรมและกระบวนการทางอาญาขององค์การสหประชาชาติ มาใช้เพื่อประกอบการพิจารณาด้วยเมื่อประเทศสมาชิกจะมีออกกฎหมาย นโยบาย หรือแนวทางปฏิบัติระดับชาติในการรับมือกับการใช้ข้อมูลข่าวสารเพื่อกระทำผิดของอาชญากร[13]

---

[12] “Combating the criminal misuse of information technology”, UN General Assembly (4 December 2000) Resolution 55/63.

[13] “…invites Member States, when developing national laws, policy and practices, to combat the criminal misuse of information technologies, to take into account, *inter alia*, the work and achievements of the Commission on Crime Prevention and Criminal Justice.”, UN General Assembly (19 December 2001) Resolution 56/121.

2.2.2 มาตรการด้านความมั่นคงไซเบอร์ในระดับภูมิภาค

ก. สหภาพยุโรป (European Union: EU) สหภาพยุโรปได้ดำเนินการรับมือเกี่ยวกับอาชญากรรมคอมพิวเตอร์จริงจังในปี พ.ศ. 2541 เมื่อคณะกรรมาธิการยุโรป (European Commission) ได้นำเสนอผลการศึกษาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ (Legal Aspects of Computer-Related Crime in the Information Society: COMCRIME study) ต่อสภายุโรป (European Council) โดยมีเนื้อหาเกี่ยวกับภาพรวมของการก่ออาชญากรรมและแนวทางการแก้ไขปัญหาด้านต่างๆ ต่อมาในปี พ.ศ. 2543 สภายุโรป และคณะกรรมาธิการยุโรปได้จัดทำแผน *eEurope Action* ขึ้น ซึ่งเป็นส่วนหนึ่งของแผนการรับมือเกี่ยวกับอาชญากรรมคอมพิวเตอร์ดังกล่าว โดยแผนนี้ได้ระบุวิธีการดำเนินการเพื่อส่งเสริมให้เครือข่ายคมนาคมมีความปลอดภัย และส่งเสริมความร่วมมือในการแก้ไขปัญหาอาชญากรรมทางคอมพิวเตอร์ให้บรรลุผลสำเร็จภายในปี พ.ศ. 2545 นอกจากนี้ สหภาพยุโรปได้เผยแพร่เอกสารที่มีชื่อว่า Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime[14] โดยมีวัตถุประสงค์เพื่อสร้างความตื่นตัวเกี่ยวกับการก่อการอาชญากรรมบนอินเตอร์เน็ต และวิธีการจัดการกับปัญหาอาชญากรรมทางคอมพิวเตอร์ทั้งที่อยู่ในรูปของกฎหมายและไม่เป็นกฎหมาย โดยการร่วมมือระหว่างหน่วยงานต่างๆ ที่เกี่ยวข้อง อาทิ ผู้ให้บริการ ผู้บริโภค รวมไปถึงองค์กรด้านการคุ้มครองข้อมูลส่วนบุคคล ด้วยเหตุนี้ สหภาพยุโรปจึงได้มีการจัดตั้ง EU Forum on Cybercrime เพื่อให้เป็นเวทีแลกเปลี่ยนความรู้และก่อให้เกิดความร่วมมือกันระหว่างหน่วยงานด้านการบังคับใช้กฎหมายกับฝ่ายที่เกี่ยวข้องข้างต้นในเวลาต่อมา และในปี พ.ศ. 2544

[14] Communication of the European Commission: Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime of 26.1.2001: COM (2000) 890 final, Retrieved 2013, March 19, from http://europa.eu.int/ISPO/eif/ InternetPoliciesSite/Crime/CrimeCommEN.htm

คณะกรรมาธิการยุโรปได้นำเสนอ “Network and Information Security: Proposal for a European Policy Approach”[15] โดยมีวัตถุประสงค์เพื่อชี้ให้เห็นถึงการคุกคามความมั่นคงหรือความปลอดภัยของระบบคอมพิวเตอร์ด้วยวิธีการต่างๆ และข้อเสนอแนะในการกำหนดนโยบายด้านการรักษาความมั่นคง เช่น มาตรการทางสังคม กฎหมาย และมาตรการทางเทคนิคต่างๆ ฯลฯ สำหรับมาตรการทางกฎหมายนั้น คณะกรรมาธิการยุโรปได้นำเสนอโครงร่างที่ว่าด้วย Council Framework Decision on attacks against information systems[16] ในปี พ.ศ. 2545 โดยมีวัตถุประสงค์เพื่อนำเสนอการก่ออาชญากรรมทางคอมพิวเตอร์รูปแบบใหม่ๆ และข้อเสนอในการบัญญัติกฎหมายอาชญากรรมทางคอมพิวเตอร์ภายในกลุ่มประเทศสมาชิกเพื่อให้มีความสอดคล้องกันทั้งกฎหมายสารบัญญัติและวิธีสบัญญัติ โดยเนื้อหาในส่วนของโครงร่างดังกล่าวนี้มาจากการศึกษาเปรียบเทียบ Convention on Cybercrime ของสภายุโรป เช่น การกำหนดความผิดฐานการเข้าถึงระบบสารสนเทศโดยมิชอบ (Illegal access to Information Systems) ความผิดฐานรบกวนระบบสารสนเทศโดยมิชอบ (Illegal interference with Information Systems) ฯลฯ ที่ประเทศสมาชิกจะต้องปฏิบัติให้เป็นไปตามข้อเสนอภายในวันที่ 31 ธันวาคม พ.ศ. 2546[17]

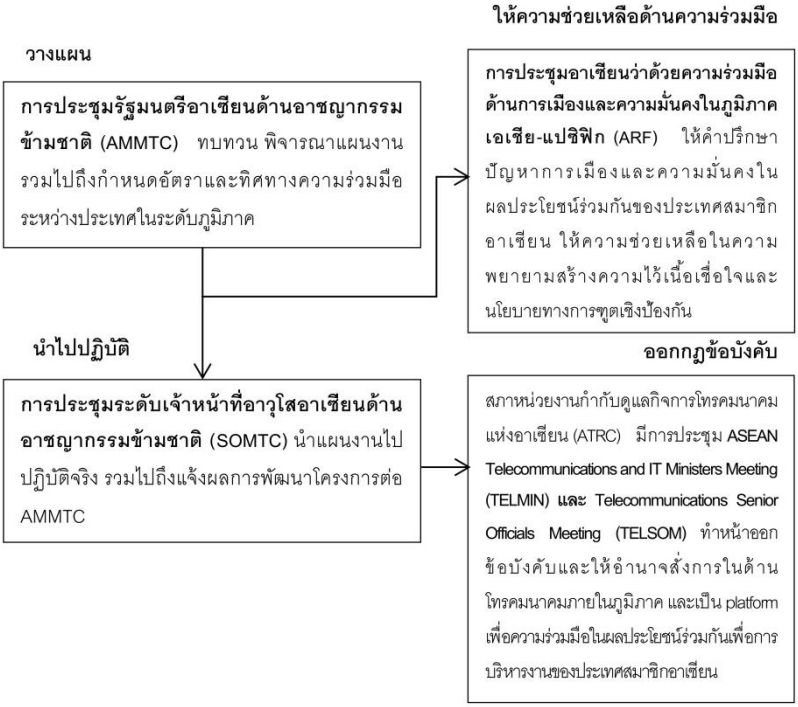
---

[15] Communication from the commission to the council the European parliament the European Economic and Social Committee and the Committee of the Regions Network and Information Security: Proposal for A European Policy Approach of 6.6.2001 COM (2001) 298 final, Retrieved 2014, April 6, from http://www.etsi.org/public-interest/Documents/PoliticalInitiatives/ Com2001_0298.pdf

[16] Proposal for a Council Framework Decision on attacks against information systems of 19.04.2002 COM (2002) 173 final., Retrieved 6 April 2014, from http://europa.eu.int/eur-lex/en/com/pdf/2002/com2002_0173en01.pdf

[17] Article 13 concerns the implementation and follow-up of this Framework Decision. Member States are required to take the necessary measures to comply with this Framework Decision not later than 31 December 2003, Proposal for a Council Framework Decision on attacks against information systems of 19.04.2002 COM(2002) 173 final.

ข. อาเซียน (Association of Southeast Asian Nations: ASEAN) การจัดการเกี่ยวกับปัญหาอาชญากรรมทางคอมพิวเตอร์ของอาเซียนนั้น ทางองค์การอาเซียน ที่ได้พยายามผลักดันให้ประเทศสมาชิกอาเซียนได้มีการออกกฎหมายว่าด้วยการป้องกันอาชญากรรมทางคอมพิวเตอร์ นอกจากนี้ องค์การอาเซียนยังได้จัดตั้ง ASEAN high level Ministerial Meeting on Transnational Crime: AMMTC และได้มีการประชุมครั้งแรก ที่กรุงเทพมหานคร ประเทศไทย เมื่อวันที่ 8 มกราคม พ.ศ. 2547 โดยในการประชุมครั้งนี้ได้รวมเอาเรื่องอาชญากรรมทางคอมพิวเตอร์ และการส่งเสริมความร่วมมือระหว่างประเทศในการรับมือกับอาชญากรรมทางคอมพิวเตอร์เข้าไว้ด้วยกัน เพื่อเพิ่มขีดความสามารถในการต่อสู้กับอาชญากรรมข้ามชาติ โดยอาเซียนได้ริเริ่มแผนการรับมืออาชญากรรมทางคอมพิวเตอร์โดยอาศัยโครงสร้างพื้นฐานทางกฎหมาย e-commerce เป็นจุดเริ่มต้นในการสร้างหลักเกณฑ์ทางกฎหมายอาชญากรรมทางคอมพิวเตอร์ อย่างไรก็ตาม กรอบโครงสร้าง e-ASEAN นั้นจำกัดอยู่เพียงกฎหมายระดับพื้นฐานเท่านั้น เมื่อปี พ.ศ. 2547 ได้เกิดการขยายตัวของอาชญากรรมทางคอมพิวเตอร์อย่างมากจึงก่อให้เกิดความตระหนักและยอมรับว่าความร่วมมือระหว่างประเทศในการป้องกันอาชญากรรมทางคอมพิวเตอร์นั้นเป็นเรื่องที่สำคัญ นอกจากนี้ อาเซียนได้มีความพยายามในการสร้างนโยบาย แผนยุทธศาสตร์และหลักเกณฑ์ที่เป็นมาตรฐานกลาง เพื่อใช้เป็นมาตรการที่สำคัญในการรับมือกับอาชญากรรมทางคอมพิวเตอร์ของภูมิภาคนี้ โดยสามารถแบ่งกลไกในการรับมืออาชญากรรมทางคอมพิวเตอร์ของอาเซียนได้ดังที่จะปรากฏตามโครงสร้างข้างล่างนี้



รูปที่ 1 กรอบแนวคิดเกี่ยวกับกลไกในการรับมืออาชญากรรมทางคอมพิวเตอร์ของอาเซียน

2.2.3 **มาตรการด้านความมั่นคงไซเบอร์ในระดับประเทศ**

ประเทศสมาชิกอาเซียนที่เป็นผู้นำในความพยายามต่อสู้อาชญากรรมทางคอมพิวเตอร์ได้แก่ ประเทศสิงคโปร์และประทศมาเลเซีย โดยกฎหมายที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ของประเทศมาเลเซียและประเทศสิงคโปร์นี้ออกตามแนวทางของอนุสัญญาระหว่างประเทศและกฎหมายของประเทศในภูมิภาคยุโรป

ก. ประเทศมาเลเซีย ถือว่าเป็นผู้นำด้านความมั่นคงไซเบอร์และอาชญากรรมทางคอมพิวเตอร์ในภูมิภาคอาเซียนโดยประเทศมาเลเซียได้จัดตั้ง

Malaysia's Communications and Multimedia (MCMC or SKMM) ขึ้นเพื่อดูแลความมั่นคงทางไซเบอร์ทั่วไป และการให้คำแนะนำแก่เว็บไซต์ในเรื่องความปลอดภัย รวมทั้งยังมีความร่วมมือระหว่างภาครัฐและเอกชน นอกจากนี้ ประเทศมาเลเซียยังมีหน่วยงานของรัฐอีกหลายองค์กรที่ดูแลในเรื่องความปลอดภัยไซเบอร์ ได้แก่ (1) Cyber Security Malaysia หน้าที่ขององค์กรนี้ คือ เป็นศูนย์การดำเนินการช่วยเหลือ Cyber999 ที่ก่อตั้งมาเพื่อให้ผู้ใช้งานอินเตอร์เน็ตชาวมาเลเซียสามารถแจ้งเหตุภัยคุกคามต่างๆ เช่น ความพยายามเจาะระบบ การข่มขู่ การฉ้อโกง และแสปม ฯลฯ (2) Malaysian Communications & Multimedia Commission (MCMC or SKMM) MCMC เป็นหน่วยงานที่ให้บริการข้อมูลแก่ผู้ปกครองในด้านปัญหาความปลอดภัยทางอินเตอร์เน็ตแก่เด็กทั้งในเรื่องการกลั่นแกล้งทางสื่ออิเล็กทรอนิกส์ (Cyber bullying) ไปจนถึงปัญหาการเสพย์ติดเกมคอมพิวเตอร์ (3) Cyber Security Awareness For Everyone (CyberSAFE Malaysia) ซึ่งดำเนินการภายใต้การอุปถัมภ์ของ Cyber Security Malaysia โดยองค์กรมุ่งเป้าไปที่การสร้างความปลอดภัยบนอินเตอร์เน็ตและให้ข้อมูลด้านความปลอดภัยไซเบอร์แก่ประชาชนในทุกพื้นที่ และ (4) Multimedia Development Corporation (MDec) เป็นองค์กรที่ดำเนินการโดยอาศัยทุนจากรัฐบาล แต่องค์กรนี้มุ่งจะดำเนินการในรูปขององค์กรเอกชนมากกว่าหน่วยงานของรัฐ โดย MDec ร่วมงานกับภาครัฐด้วยการให้คำปรึกษาแก่รัฐบาลในการออกนโยบายเกี่ยวกับกฎหมายอินเตอร์เน็ต (Cyber laws)[18]

นอกจากนี้ ประเทศมาเลเซียยังเป็นเป็นประเทศแรกๆ ในอาเซียนที่ออกกฎหมายอาชญากรรมทางคอมพิวเตอร์มาใช้ตั้งแต่ปี พ.ศ. 2540 ในชื่อว่า Computer Crime Act of 1997 โดยเนื้อหาของกฎหมายฉบับนี้จะครอบคลุมการใช้งานคอมพิวเตอร์โดยมิชอบทางกฎหมาย เช่น การเจาะระบบและทำลายระบบเครือข่าย

[18] Malaysia, *Global Resource and Information Directory*, Retrieved 2014, March 21, from http://www.fosigrid.org/asia/Malaysia

คอมพิวเตอร์และการแพร่ไวรัสคอมพิวเตอร์ คุ้มครองสิทธิ์และความเป็นส่วนตัวของผู้ใช้คอมพิวเตอร์ ซึ่งความผิดตามกฎหมายฉบับนี้ได้แก่ การเข้าถึงข้อมูลคอมพิวเตอร์ของผู้อื่นโดยไม่ได้รับอนุญาต (Unauthorized access) การแก้ไขข้อมูลโดยไม่ได้รับอนุญาต (Unauthorized modification), The Digital Act 1997 มีวัตถุประสงค์เพื่อควบคุมวิธีการสื่อสารหรือทำธุรกรรมออนไลน์ของประชาชนเพื่อป้องกันการใช้งานโดยมิชอบ โดยลายเซ็นอิเล็กทรอนิกส์ (Digital signature) ถือเป็นเครื่องระบุตัวตนของผู้ใช้โดยวิธีการเข้ารหัสเพื่อป้องกันการปลอมแปลง ซึ่งช่วยปกป้องข้อมูลที่ถูกส่งออกไปจากการถูกรบกวนหรือดักจับ โดยลายเซ็นอิเล็กทรอนิกส์จะถูกต้องตามกฎหมายเมื่อได้รับ Certificate authority license โดยผู้มีอำนาจในสิทธิ์นั้น และธุรกรรมใดๆ ที่กระทำโดยถูกต้องตามกฎหมายฉบับนี้ถือว่าเป็นธุรกรรมที่ชอบด้วยกฎหมาย, และ Communication and Multimedia Act of 1998 กฎหมายฉบับนี้มีวัตถุประสงค์เพื่อส่งเสริมนโยบายของชาติในภาคการสื่อสารและมัลติมีเดีย และรับรองความปลอดภัยและความน่าเชื่อถือของข้อมูล รวมทั้งราคาค่าบริการต่างๆ ที่เกี่ยวข้องอยู่ในระดับที่สาธารณชนสามารถใช้บริการได้อย่างเหมาะสม กฎหมายฉบับนี้ได้ออกข้อกำหนดต่างๆ ที่หลากหลาย เช่น การกำหนดสัญญาอนุญาต (License agreement) ของผู้ให้บริการเครือข่าย ผู้ให้บริการโปรแกรม และผู้ให้บริการเนื้อหาออนไลน์ รวมไปถึงการดำเนินคดีกับผู้ที่ส่ง Email หรือ SMS ลามกอนาจาร หรือโพสต์ข้อความมุ่งร้ายหรือดูหมิ่นผู้อื่น เป็นต้น

ข. ประเทศสิงคโปร์ ได้แบ่งการควบคุมเนื้อหาทางออนไลน์ออกเป็นสามส่วนด้วยกัน ได้แก่ การควบคุมโดยรัฐด้วยการออกใบอนุญาต (Class license) การควบคุมด้วยตนเองในภาคธุรกิจ (Self-regulation) และโครงการให้การศึกษาสาธารณะ โดยสำนักงานพัฒนาสื่อ (Media Development Authority: MDA) ของสิงคโปร์ทำหน้าที่ออกใบอนุญาตและเงื่อนไขการลงทะเบียนซึ่งกำหนดโทษให้กับเนื้อหาบนอินเตอร์เน็ตและผู้ให้บริการหากดำเนินการไม่สอดคล้องกับข้อห้ามของ MDA และสำนักงานนี้ยังทำหน้าที่รับรองว่าจะไม่มีสิ่งใดที่ประกอบไปด้วยเนื้อหาของ

สื่อใดๆ ก็ตามที่รบกวนความสงบเรียบร้อยของสังคมหรือขัดต่อศีลธรรมอันดีของประชาชน หัวใจของกรอบเค้าโครงนี้คือแผนการออกใบอนุญาต ซึ่ง MDA เป็นผู้กำหนดเงื่อนไข ภายใต้กฎหมายการกระจายภาพและเสียง (Broadcasting Act) และนโยบายทางธุรกิจ และข้อบังคับต่างๆ ที่ออกโดย MDA สำหรับแผนการออกใบอนุญาตผู้ให้บริการอินเตอร์เน็ต (Internet Service Providers: ISPs) และผู้ให้บริการเนื้อหาบนอินเตอร์เน็ต (Internet Content Providers: ICPs) ทั้งหมดไม่ว่าจะเป็นพรรคการเมืองหรือปัจเจกชนใดที่ประสงค์จะทำการเผยแพร่ ส่งเสริม หรืออภิปราย ในเรื่องทางการเมืองหรือศาสนา ต้องทำการลงทะเบียนกับ MDA ในฐานะผู้รับใบอนุญาต ISPs และ ICPs จะผูกพันภายใต้ระเบียบปฏิบัติ (Code of practice) ของ MDA ซึ่งได้ให้คำนิยามเนื้อหาต้องห้าม (Prohibited material) อย่างกว้างๆ โดยระบุชี้ชัดเฉพาะมาตรฐานสำหรับเนื้อหาที่เกี่ยวกับเพศ ความรุนแรง และไม่เป็นที่ยอมรับในสังคมเท่านั้น ในขณะที่การกลั่นกรองเนื้อหาไม่ได้อยู่ในของเขตอำนาจของ ISPs หน้าที่ในการปฏิเสธการเข้าถึงเนื้อหาเหล่านั้นจะเป็นของ ICPs หากได้รับคำสั่งจาก MDA ในกรณีที่ผู้รับใบอนุญาตไม่กระทำตามจะได้รับบทลงโทษ เช่น ปรับ และพัก หรือยกเลิกใบอนุญาต นอกจากนี้ประเทศสิงคโปร์ยังมีกฎหมายเกี่ยวกับการห้ามเผยแพร่เนื้อหาอันเป็นการดูหมิ่นเชื้อชาติ (Racism) ใน Sedition Act ซึ่งปรับใช้กับเนื้อหาบนอินเตอร์เน็ตได้อีกด้วย

สำหรับกฎหมายว่าด้วยอาชญากรรมคอมพิวเตอร์ของประเทศสิงคโปร์ในปัจจุบัน คือ Computer Misuse Act 1993 โดยกฎหมายฉบับนี้ได้ให้นิยามคำว่าคอมพิวเตอร์ไว้อย่างกว้างๆ และไม่เจาะจงเฉพาะเทคโนโลยีใดเทคโนโลยีหนึ่งเท่านั้น หากแต่สามารถประยุกต์ใช้กับใครก็ได้ ไม่ว่าที่อยู่ทางภูมิศาสตร์จะอยู่ ณ ที่ใดแต่ได้กระทำการใดที่เกี่ยวข้องกับคอมพิวเตอร์ โปรแกรม และข้อมูลที่อยู่ในประเทศสิงคโปร์ ณ เวลานั้น

2.3 มาตรการทางด้านความมั่นคงไซเบอร์ของประเทศไทย

ในปัจจุบันมาตรการทางด้านความมั่นคงของประเทศในด้านอาชญากรรมทางคอมพิวเตอร์และความมั่นคงไซเบอร์ของประเทศไทยนั้น มีกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (ไอซีที) เป็นหน่วยงานหลัก และมีสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ องค์การมหาชน ที่อยู่ภายใต้การกำกับดูแลของกระทรวงไอซีที รวมทั้ง คณะกรรมการป้องกันและปราบปรามการกระทำความผิดทางคอมพิวเตอร์เพื่อเพิ่มประสิทธิภาพการดำเนินการสืบสวนสอบสวนและรับมืออาชญากรรมทางคอมพิวเตอร์ด้วย[19]

2.3.1 มาตรการทางกฎหมายที่บังคับใช้อยู่ในปัจจุบันเกี่ยวกับความมั่นคงไซเบอร์

เนื่องจากอาชญากรรมทางคอมพิวเตอร์มีลักษณะพิเศษ จึงจำเป็นต้องมีการตรากฎหมายขึ้นมาใหม่ที่ไม่กระทบต่อโครงสร้างของประมวลกฎหมายอาญาเดิม เพื่อเข้ามาทำหน้าที่อุดช่องโหว่ทางกฎหมายของประมวลกฎหมายอาญาที่ไม่สามารถนำตัวผู้กระทำความผิดมาลงโทษได้ นอกจากนี้ ในการบังคับใช้กฎหมายอาชญากรรมทางคอมพิวเตอร์ จำเป็นต้องให้อำนาจพิเศษกับเจ้าพนักงานบางประการ เช่น การถอดรหัสลับข้อมูล การเรียกข้อมูลจราจรทางคอมพิวเตอร์ ฯลฯ ดังนั้น ประเทศไทยจึงได้จัดทำพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ขึ้นมาโดยได้นำเอามาตรฐานและข้อตกลงเกี่ยวกับการรับมือกับอาชญากรรมทางคอมพิวเตอร์ระหว่างประเทศ เช่น อนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ (Convention on Cybercrime) ของสหภาพยุโรปมาปรับใช้ รวมทั้งยังได้พิจารณานำเอาหลักกฎหมาย

---

[19] ILAW, *อัปเกรด พ.ร.บ.คอมฯ เพิ่มโทษผู้ดูแลระบบ ก๊อปไฟล์โหลดบิทเสี่ยงคุก*, (7 เมษายน 2554), สืบค้นเมื่อ 11 พฤศจิกายน 2556, จาก http://ilaw.or.th/node/857

ทางด้านอาชญากรรมทางคอมพิวเตอร์ของประเทศต่างๆ อาทิ เยอรมนี อังกฤษ สิงคโปร์ สหรัฐอเมริกา อินเดีย มาปรับใช้อีกด้วย[20]

นอกจากนี้ ประเทศไทยได้มีกฎหมายอีกหลายฉบับที่มีเนื้อหาเกี่ยวข้องกับการป้องกันหรือปราบปรามอาชญากรรมทางคอมพิวเตอร์ เช่น พระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544[21] ประมวลกฎหมายอาญา[22] และ ประมวลกฎหมายวิธีพิจารณาความอาญา[23] สำหรับการคุ้มครองข้อมูลส่วนบุคคลนั้น ปัจจุบันประเทศไทยยังไม่มีกฎหมายคุ้มครองข้อมูลหรือสิทธิส่วนบุคคลโดยตรง แต่ได้มีกำหนดไว้ในกฎหมายอื่นๆ ซึ่งอาจนำมาปรับใช้แล้วแต่กรณี เช่น รัฐธรรมนูญแห่งราชอาณาจักรไทย พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ประมวลกฎหมายอาญา และพระราชบัญญัติการประกอบธุรกิจข้อมูลบัตรเครดิต พ.ศ. 2545 ฯลฯ แต่อย่างไรก็ตาม ในปัจจุบันประเทศไทยได้มีการตรากฎหมายขึ้นมาอีกหลายฉบับและอยู่ระหว่างดำเนินการทางนิติบัญญัติ ที่มีเนื้อหาเกี่ยวข้องกับการป้องกันหรือปราบปรามอาชญากรรมทางคอมพิวเตอร์ เช่น ร่างพระราชบัญญัติความมั่นคงไซเบอร์ ฯลฯ

---

[20] NECTEC, *คำถามที่พบบ่อยเกี่ยวกับร่างพระราชบัญญัติการกระทำผิดเกี่ยวกับคอมพิวเตอร์*, สืบค้นเมื่อ 11 พฤศจิกายน 2556, จาก http://wiki.nectec.or.th/nectecpedia2/index.php/คำถามที่พบบ่อย_เกี่ยวกับร่างพรบ.การกระทำผิดเกี่ยวกับคอมพิวเตอร์

[21] มาตรา 74 ของ พระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544

[22] ประมวลกฎหมายอาญา ลักษณะ 7 ความผิดเกี่ยวกับการปลอมแปลง หมวด 4 ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ มาตรา 269/1 มาตรา 269/2 มาตรา 269/3 มาตรา 269/4 มาตรา 269/5 มาตรา 269/6 มาตรา 269/7 เพิ่มเติมพระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่ 17) พ.ศ. 2547.

[23] มาตรา 59 ของ ประมวลกฎหมายวิธีพิจารณาความอาญา

2.3.2 ร่างพระราชบัญญัติความมั่นคงไซเบอร์ พ.ศ.....

สำหรับหลักการและเหตุผลในการตรากฎหมายว่าด้วยความมั่นคงไซเบอร์แห่งชาติที่มีประสิทธิภาพและเกิดผลสัมฤทธิ์นั้นเนื่องมาจากความต้องการที่จะให้ประเทศไทยสามารถปกป้อง ป้องกัน หรือรับมือกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบหรืออาจก่อให้เกิดความเสี่ยงต่อการให้บริการหรือประยุกต์ใช้เครือข่ายคอมพิวเตอร์ อินเตอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการโดยปกติของดาวเทียม ซึ่งกระทบต่อความมั่นคงของชาติในมิติต่างๆ

โดยร่างพระราชบัญญัติความมั่นคงไซเบอร์ นี้ประกอบไปด้วย 43 มาตรา รวมทั้งหมด 6 หมวด ประกอบด้วย (1) การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (2) คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (3) สานักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (4) การปฏิบัติการและการรับมือภัยคุกคามทางไซเบอร์ (5) พนักงานเจ้าหน้าที่ และ (6) บทเฉพาะกาล ซึ่งได้มีการให้คำนิยามเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ไว้ในมาตรา 3[24] สำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาตินั้น ให้คำนึงถึงความสอดคล้องกับกรอบนโยบายและแผนแม่บทที่เกี่ยวกับการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมของคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคม และกรอบนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาความมั่นคงแห่งชาติ ซึ่งเห็นชอบโดยคณะรัฐมนตรี การดำเนินการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยจึงต้องครอบคลุมในเรื่องดังต่อไปนี้ (1)

---

[24] มาตรา 3 ของ ร่างพระราชบัญญัติความมั่นคงไซเบอร์ พ.ศ... บัญญัติว่า *"ความมั่นคงปลอดภัยไซเบอร์" หมายความว่า มาตรการและการดำเนินการที่กำหนดขึ้น เพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศให้สามารถปกป้อง ป้องกัน หรือรับมือกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบหรืออาจก่อให้เกิดความเสี่ยงต่อการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการโดยปกติของดาวเทียม อันกระทบต่อความมั่นคงของชาติซึ่งรวมถึงความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ และความมั่นคงทางเศรษฐกิจ...."*

การบูรณาการการจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศ (2) การสร้างศักยภาพในการตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์ (3) การปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (4) การประสานความร่วมมือระหว่างภาครัฐและเอกชนเพื่อความมั่นคงปลอดภัยไซเบอร์ (5) การสร้างความตระหนักและรอบรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (6) การพัฒนาระเบียบและกฎหมายเพื่อความมั่นคงปลอดภัยไซเบอร์ (7) การวิจัยและพัฒนาเพื่อความมั่นคงปลอดภัยไซเบอร์ และ (8) การประสานความร่วมมือระหว่างประเทศเพื่อความมั่นคงปลอดภัยไซเบอร์[25]

ร่างพระราชบัญญัตินี้กำหนดให้มีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติขึ้นเป็นหน่วยงานของรัฐที่มีฐานะเป็นนิติบุคคลไม่เป็นส่วนราชการและรัฐวิสาหกิจ[26] ที่จะเป็นผู้ดูแลเกี่ยวกับเรื่องนี้โดยมีอำนาจและหน้าที่ ดังต่อไปนี้ (1) ตอบสนองและรับมือกับภัยคุกคามไซเบอร์ เมื่อมีเหตุการณ์ด้านความมั่นคงปลอดภัย หรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ที่ส่งผลกระทบ หรืออาจก่อให้เกิดผลกระทบ ความสูญเสีย หรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรง โดยวางมาตรการเกี่ยวกับการดำเนินการที่คำนึงถึงชั้นความลับและการเข้าถึงข้อมูลที่มีชั้นความลับ (2) ประสานความร่วมมือทางปฏิบัติในการดำเนินการกับหน่วยงานของรัฐ หรือหน่วยงานภาคเอกชน เพื่อให้การยับยั้งปัญหาภัยคุกคามไซเบอร์ ได้รับการแก้ไขอย่างมีประสิทธิภาพและรวดเร็ว (3) ประสานงานกับหน่วยงานของรัฐและเอกชน เพื่อรวบรวมข้อมูลเกี่ยวกับภัยคุกคาม การป้องกัน การรับมือ ความเสี่ยงจากสถานการณ์ด้านภัยคุกคามทางไซเบอร์ และข้อมูลอื่นใดอันเกี่ยวกับ การรักษาความมั่นคงปลอดภัยไซเบอร์

[25] มาตรา 5 ของ ร่างพระราชบัญญัติความมั่นคงไซเบอร์ พ.ศ.....

[26] มาตรา 14 ของ ร่างพระราชบัญญัติความมั่นคงไซเบอร์ พ.ศ.....

เพื่อวิเคราะห์เสนอต่อ กปช.[27] (4) บริหารแผนงานรวม ประสานการบริหารและการปฏิบัติการตามแผนปฏิบัติการหรือตามคำสั่งการของ กปช. (5) ติดตามและเร่งรัดการปฏิบัติงานของหน่วยงานของรัฐที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์และรายงานต่อ กปช. (6) เป็นศูนย์กลางเครือข่ายข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ ทั้งภายในและภายนอกประเทศ (7) ติดตาม เฝ้าระวัง รวมทั้งสร้างความตระหนักเกี่ยวกับภัยคุกคามทางระบบสารสนเทศ รวมทั้งจัดตั้งและบริหารจัดการศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (National CERT) (8) ศึกษาและวิจัยข้อมูลที่จำเป็นสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อจัดทำข้อเสนอแนะเกี่ยวกับมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (9) ส่งเสริม สนับสนุน และดำเนินการเผยแพร่ความรู้ และการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ตลอดจนดำเนินการฝึกอบรมเพื่อยกระดับทักษะเกี่ยวกับมาตรฐานความมั่นคงปลอดภัย หรือกรณีอื่นใดเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ (10) รายงานความคืบหน้าและสถานการณ์เกี่ยวกับการปฏิบัติตามระเบียบนี้ รวมทั้งปัญหาและอุปสรรคต่อ กปช. (11) รับผิดชอบงานธุรการ งานวิชาการ งานการประชุม และงานเลขานุการของ กปช. (12) จัดทำรายงานสรุปผลการดำเนินงานรายงานประจำปีให้ กปช. ทราบ เว้นแต่เป็นกรณีฉุกเฉินให้รายงานให้ กปช. ทราบโดยเร็ว (13) ปฏิบัติงานอื่นใดอันเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศตามที่ กปช. หรือคณะรัฐมนตรีมอบหมาย[28]

โดยมีเลขาธิการเป็นหัวหน้าสำนักงานฯ รับผิดชอบการปฏิบัติงานของสำนักงาน ขึ้นตรงต่อประธานกรรมการ และเป็นผู้บังคับบัญชาพนักงานและลูกจ้างของสำนักงาน[29] ส่วนในกิจการของสำนักงานที่เกี่ยวกับบุคคลภายนอก ให้เลขาธิการเป็น

---

[27] คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรียกโดยย่อว่า กปช.

[28] มาตรา 17 ของ ร่างพระราชบัญญัติความมั่นคงไซเบอร์ พ.ศ.....

[29] มาตรา 21 ของ ร่างพระราชบัญญัติความมั่นคงไซเบอร์ พ.ศ.....

ผู้แทนของสำนักงาน เพื่อการนี้เลขาธิการอาจมอบอำนาจให้บุคคลใดปฏิบัติงานเฉพาะอย่างแทนก็ได้ นอกจากนี้ร่างพระราชบัญญัตินี้ให้มี คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรียกโดยย่อว่า กปช. และให้ใช้ชื่อภาษาอังกฤษว่า National Cyber security Committee เรียกโดยย่อว่า “NCSC” ประกอบด้วย รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นประธานกรรมการ, กรรมการโดยตำแหน่งจำนวน 4 คน (ได้แก่ เลขาธิการสภาความมั่นคงแห่งชาติ ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ปลัดกระทรวงกลาโหม ผู้บังคับการกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี สำนักงานตำรวจแห่งชาติ), กรรมการผู้ทรงคุณวุฒิจำนวนไม่เกินเจ็ดคน ซึ่งคณะรัฐมนตรีแต่งตั้งจากผู้มีความรู้ ความเชี่ยวชาญ และประสบการณ์เป็นที่ประจักษ์ในด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านนิติศาสตร์ หรือด้านอื่นที่เกี่ยวข้องและเป็นประโยชน์ต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ และให้เลขาธิการดำรงตำแหน่งเป็นกรรมการและเลขานุการโดยตำแหน่ง[30] โดยคณะกรรมชุดนี้มีอำนาจหน้าที่ดังต่อไปนี้ (1) กำหนดแนวทางและมาตรการตอบสนองและรับมือกับภัยคุกคามไซเบอร์ เมื่อมีเหตุการณ์ด้านความมั่นคงปลอดภัย หรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบ ความสูญเสีย หรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรง เพื่อให้เป็นศูนย์กลางการดำเนินการเมื่อมีเหตุการณ์หรือสถานการณ์ความมั่นคงปลอดภัยได้อย่างทันท่วงที มีความเป็นเอกภาพ เว้นแต่ภัยคุกคามทางไซเบอร์นั้นเป็นภัยที่กระทบต่อความมั่นคงทางทหารซึ่งเป็นอำนาจของสภากลาโหมหรือสภาความมั่นคงแห่งชาติ (2) กำหนดขั้นตอนการดำเนินการเพื่อให้มีการประสานความร่วมมือและอำนวยความสะดวกในการดำเนินการกับคณะกรรมการที่ตั้งขึ้นตามกฎหมายฉบับอื่น หน่วยงานของรัฐหรือ

[30] มาตรา 6 ของ ร่างพระราชบัญญัติความมั่นคงไซเบอร์ พ.ศ.....

หน่วยงานภาคเอกชน เพื่อให้การยับยั้งปัญหา ภัยคุกคามไซเบอร์ ได้รับการแก้ไขอย่างมีประสิทธิภาพและรวดเร็ว (3) กำหนดมาตรการและแนวทางในการยกระดับทักษะความเชี่ยวชาญระดับสูงของเจ้าพนักงานผู้ปฏิบัติหน้าที่ซึ่งได้รับการแต่งตั้งตามกฎหมายฉบับนี้ (4) จัดทำแผนปฏิบัติการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติที่สอดคล้องกับนโยบาย ยุทธศาสตร์ และแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม และกรอบนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาความมั่นคงแห่งชาติ (5) จัดทำรายงานสรุปผลการดำเนินงานที่มีผลกระทบอย่างมีนัยสำคัญ รายงานให้สภาความมั่นคงแห่งชาติและคณะรัฐมนตรีทราบตามลำดับ (6) เสนอแนะและให้ความเห็นต่อคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคม หรือคณะรัฐมนตรีในการพิจารณาอนุมัติแผนงาน โครงการ หรือการปฏิบัติงานของหน่วยงานของรัฐ และการพิจารณาแนวทางการแก้ไขปัญหาหรือข้อขัดข้องต่างๆ รวมถึงการจัดให้มีหรือปรับปรุงกฎหมายที่มีความเกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้การดำเนินการปกป้อง รับมือ ป้องกัน และลดความเสี่ยงจากสถานการณ์ภัยคุกคามทางไซเบอร์อันกระทบต่อความมั่นคงของชาติทั้งจากภายในและภายนอกประเทศมีความมั่นคงและยั่งยืน (7) แต่งตั้งคณะอนุกรรมการ หรือคณะทำงาน เพื่อพิจารณาหรือทาการใดๆ ตามที่คณะกรรมการมอบหมาย (8) สั่งการหรือประสานความร่วมมือกับหน่วยงานภาครัฐและภาคเอกชนเพื่อปฏิบัติให้เป็นไปตามนโยบายหรือแผนปฏิบัติการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือให้ดำเนินการอื่นใดที่จำเป็นต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งในประเทศและต่างประเทศ (9) ติดตามและประเมินผลการปฏิบัติตามพระราชบัญญัตินี้ (10) ดำเนินการอื่นใดในเรื่องที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ตามที่คณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมหรือคณะรัฐมนตรีมอบหมาย[31]

[31] มาตรา 7 ของ ร่างพระราชบัญญัติความมั่นคงไซเบอร์ พ.ศ.....

นอกจากนี้แล้ว ร่างพระราชบัญญัตินี้ยังคงให้อำนาจพนักงานเจ้าหน้าที่ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้ ที่ได้รับมอบหมายเป็นหนังสือจากเลขาธิการ มีอำนาจในการดำเนินงานเพื่อให้เป็นไปตามพระราชบัญญัติ ดังต่อไปนี้ (1) มีหนังสือสอบถามหรือเรียกให้หน่วยงานของรัฐ หรือบุคคลใดๆ มาให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งบัญชี เอกสาร หรือหลักฐานใดๆ มาเพื่อตรวจสอบหรือให้ข้อมูลเพื่อประโยชน์ในการปฏิบัติการตามพระราชบัญญัตินี้ (2) มีหนังสือขอให้หน่วยงานราชการ หรือหน่วยงานเอกชนดำเนินการเพื่อประโยชน์แห่งการปฏิบัติหน้าที่ของ กปช. (3) เข้าถึงข้อมูลการติดต่อสื่อสารทั้งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสารสื่ออิเล็กทรอนิกส์หรือ สื่อทางเทคโนโลยีสารสนเทศใด เพื่อประโยชน์ในการปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์และการดำเนินการตาม (3) ให้เป็นไปตามหลักเกณฑ์และเงื่อนไขที่คณะรัฐมนตรีกำหนด[32]

3. นิติปรัชญากับร่างพระราชบัญญัติความมั่นคงไซเบอร์ พ.ศ.....

จากการศึกษาถึงอาชญากรรมทางคอมพิวเตอร์ประเภทที่เรียกว่า “สงครามไซเบอร์” หรือ สงครามข้อมูลข่าวสาร ที่เป็นภัยอย่างยิ่งต่อความมั่นคงของประชาคมโลก เนื่องด้วยวิทยาการและเทคโนโลยีสมัยใหม่นี้ง่ายต่อการเข้าถึงในทุกระดับของสังคม ดังนั้น การที่ประเทศไทย โดยรัฐบาลได้พยายามที่จะตราพระราชบัญญัติความมั่นคงไซเบอร์ขึ้นมาเพื่อนำมาปรับใช้นั้นจึงเป็นเรื่องที่สำคัญและจำเป็นอย่างยิ่ง รวมทั้งเป็นที่เข้าใจได้ แต่อย่างไรก็ตาม จากที่ได้ทำการศึกษาวิเคราะห์ ปรากฏว่าร่างพระราชบัญญัติความมั่นคงไซเบอร์นี้ได้มีประเด็นปัญหาที่ต้องการถกเถียงเกิดขึ้นมาดังนี้

[32] มาตรา 35 ของ ร่างพระราชบัญญัติความมั่นคงไซเบอร์ พ.ศ.....

1. ร่างพระราชบัญญัติความมั่นคงไซเบอร์นี้ได้คุกคามเสรีภาพและความเป็นส่วนตัวของประชาชนในการการใช้ชีวิตปกติและสื่อสารที่ขัดต่อข้อตกลงระหว่างประเทศ ที่ประเทศไทยได้เข้าเป็นภาคีและขัดต่อรัฐธรรมนูญแห่งราชอาณาจักรไทยด้วย

2. ร่างพระราชบัญญัติความมั่นคงไซเบอร์นี้ ให้อำนาจคณะกรรมการรักษาความปลอดภัยไซเบอร์แห่งชาติอย่างกว้างขวางมากและคณะกรรมการฯ สามารถที่จะตีความว่าสิ่งใดเข้าข่ายอำนาจหน้าที่ของตนได้

3. ร่างพระราชบัญญัติความมั่นคงไซเบอร์นี้ให้อำนาจเจ้าหน้าที่ตรวจสอบการสื่อสารของประชาชนได้ทุกช่องทาง โดยไม่มีขอบเขตและไม่มีกระบวนการตรวจสอบใดๆ มาคานอำนาจ และพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้สามารถเข้าถึงข้อมูลการสื่อสารโดยไม่ต้องมีหมายศาล

4. ร่างพระราชบัญญัติความมั่นคงไซเบอร์นี้ เขียนคำนิยามศัพท์ไว้แบบกว้างๆ อ่านแล้วเข้าใจได้ยาก จึงอาจเปิดโอกาสให้เจ้าหน้าที่ใช้ดุลพินิจในการปฏิบัติงานได้อย่างกว้างขวาง

5. ร่างพระราชบัญญัติความมั่นคงไซเบอร์นี้จะก่อให้เกิดภาวะชะงักงันในการพัฒนาเศรษฐกิจของประเทศไทยเพราะว่าผู้ประกอบการภาคเอกชนที่จะมาลงทุนในประเทศจะเกิดความกังวลถึงความเป็นอิสระในการดำเนินธุรกิจภายใต้กฎหมายไทย เพราะพวกเขาไม่อาจมั่นใจในความปลอดภัยของข้อมูลในการดำเนินธุรกิจของตนได้เลย

นอกจากนี้ จากกรณีประเด็นปัญหาที่กล่าวมาข้างต้น เห็นควรที่จะทำการศึกษาวิเคราะห์โดยใช้แนวความคิดจากสำนักปรัชญาทางด้านกฎหมายทั้งหลายที่มีอิทธิพลต่อการแสวงหาคำตอบและแนวทางในการแก้ไขดังกล่าว เช่น สำนักกฎหมายธรรมชาติ (School of Natural Law) และสำนักกฎหมายบ้านเมือง (School of Positivism)

3.1 สำนักกฎหมายธรรมชาติ (School of Natural Law) โดยสำนักนี้ได้อธิบายว่า มนุษย์เป็นคนที่มีเหตุผล มีศักดิ์ศรีเท่าเทียมกัน และกฎหมาย คือ เหตุผลที่มี

อยู่แล้วตามธรรมชาติ ซึ่งทำให้ “กฎหมาย” ในสายตาของนักนิติศาสตร์ในสำนักนี้มีลักษณะสำคัญ 3 ประการ คือ (1) เป็นกฎหมายที่มีผลใช้บังคับโดยไม่จำกัดเวลา ทั้งในอดีต ปัจจุบัน และอนาคต (2) เป็นกฎหมายที่ใช้บังคับได้โดยไม่จำกัดสถานที่ ไม่ว่าจะเป็นภายในสังคมใดหรือภายในรัฐใดหรือในประชาคมของรัฐก็ตาม และ (3) อยู่เหนือกฎหมายของรัฐซึ่งเป็นกฎหมายที่มนุษย์สร้างขึ้น ดังนั้น กฎหมายของรัฐจะขัดกับกฎหมายธรรมชาติมิได้แนวความคิดที่ว่ายังปรากฏได้เห็นได้ชัดเจนในปัจจุบันนี้ โดยเฉพาะอย่างยิ่งในกรณีที่เกี่ยวกับเสรีภาพขั้นพื้นฐานของมนุษย์และสิทธิมนุษยชน

ดังนั้น เราจะเห็นได้ว่าในประเด็นปัญหาที่ร่างพระราชบัญญัติความมั่นคงไซเบอร์นี้ให้อำนาจของคณะกรรมการรักษาความปลอดภัยไซเบอร์แห่งชาติอย่างมาก และคณะกรรมการฯสามารถที่จะตีความว่าสิ่งใดเข้าข่ายอำนาจหน้าที่ของตนก็ได้ รวมทั้งประเด็นที่พนักงานเจ้าหน้าที่ตามพระราชบัญญัติความมั่นคงไซเบอร์นี้สามารถเข้าถึงข้อมูลการสื่อสาร โดยไม่ต้องมีหมายศาล และสามารถตรวจสอบการสื่อสารของประชาชนได้ทุกช่องทาง โดยไม่มีขอบเขตและไม่มีกระบวนการตรวจสอบใดๆ มาคานอำนาจ ในประเด็นนี้จะเห็นได้ว่าร่างพระราชบัญญัติความมั่นคงไซเบอร์นี้คุกคามเสรีภาพและความเป็นส่วนตัวของประชาชนในการสื่อสาร หากจะวิเคราะห์ตามหลักของสำนักกฎหมายธรรมชาติที่สอนให้มนุษย์รู้จักเคารพความเสมอภาคและความเป็นอิสระต่อกัน รู้ว่าแต่ละคนไม่ควรจะล่วงละเมิดชีวิต ร่างกาย เสรีภาพ และทรัพย์สินของกันและกัน เมื่อใดก็ตามที่รัฐละเมิดชีวิต ร่างกาย เสรีภาพ และทรัพย์สินของราษฎรแล้ว การกระทำของรัฐเช่นนั้นย่อมเป็นการฝ่าฝืนความไว้วางใจของราษฎร[33] ประชาชนย่อมมีสิทธิ์ที่จะเรียกร้องให้ยุติการกระทำเช่นนั้น ด้วยเหตุผลอันนี้ รัฐจึงมีหน้าที่รักษาความสงบและอำนวยความยุติธรรม รวมทั้งมีอำนาจที่จำกัด เพราะหลักประกันแห่งเสรีภาพไม่ได้อยู่ที่รูปแบบการปกครองแบบประชาธิปไตย แต่อยู่ที่รูปแบบรัฐบาลที่มีอำนาจ

[33] ปรีดี เกษมทรัพย์, *นิติปรัชญา*, (กรุงเทพฯ: โครงการตำราและเอกสารประกอบการสอน คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2539), 197.

จำกัด[34] เหตุผลก็เพราะว่าใครก็ตามที่มีอำนาจย่อมมีแนวโน้มจะใช้อำนาจไปในทางที่ไม่ชอบได้เสมอ[35] ดังนั้นเพื่อป้องกันการใช้อำนาจโดยมิชอบ จึงจำเป็นต้องมีระบบการควบคุมการใช้อำนาจโดยมิชอบ เพื่อถ่วงดุลอำนาจระหว่าง ผู้ถืออำนาจด้วยกันให้อยู่ในระดับที่เหมาะสม (ทั้งนี้ประสบการณ์ของมนุษย์ได้บอกเราเสมอว่า ผู้มีอำนาจมักใช้อำนาจเกินขอบเขต วิธีที่จะป้องกันเหตุเช่นนั้นได้ต้องใช้อำนาจมาคานอำนาจ)[36] ในกรณีของประเด็นเหล่านี้ผู้เขียนเห็นว่าพระราชบัญญัติความมั่นคงไซเบอร์นี้ควรที่จะมีการแก้ไขปรับปรุงอำนาจหน้าที่ของคณะกรรมการและพนักงานเจ้าหน้าที่ให้เป็นไปตามหลักสากลที่สามารถมีการคานอำนาจและตรวจสอบจากหน่วยงานอื่น (ศาล) ได้

3.2 สำนักกฎหมายบ้านเมือง (School of Positivism) สำนักนี้ได้รับอิทธิพลจากความคิดของ จัง โบแดง เกี่ยวกับอำนาจอธิปไตยของรัฐ โดยโทมัส ฮอบส์[37] ได้นำเอาทฤษฎีสัญญาสวามิภักดิ์มาอธิบายเพื่ออ้างความชอบธรรมในการปกครองมนุษย์และให้ประชาชนต้องเชื่อฟังกฎหมายของรัฐ เหตุเพราะว่ามนุษย์มีธรรมชาติเห็นแก่ตัว เลว และดื้อดึง[38] สำนักฯ นี้ถือว่า “กฎหมาย” คือกฎเกณฑ์ซึ่งเกิดจากเจตจำนง (will) ของรัฐ โดยจะให้ความสำคัญกับขั้นตอนหรือรูปแบบของการแสดงออกซึ่งเจตจำนงของรัฐมากกว่าเนื้อหาของกฎเกณฑ์ซึ่งเกิดจากเจตจำนงเช่นว่านั้น กล่าวอีกนัยหนึ่งก็คือ กฎเกณฑ์ที่จะเป็นกฎหมายในสายตาของสำนักความคิดกฎหมายบ้านเมืองก็คือ กระบวนการหรือขั้นตอนในการออกกฎหมายหรือการวางกฎเกณฑ์นั้นจะต้องสะท้อนถึงการแสดงออกซึ่งเจตจำนงที่แท้จริงของรัฐไม่ว่ารูปแบบในการแสดง

---

[34] เรื่องเดียวกัน, 199.

[35] เรื่องเดียวกัน

[36] ปรีดี เกษมทรัพย์, *นิติปรัชญา*, 200.

[37] การที่ ฮอบส์ได้อธิบายว่ารัฏฐาธิปัตย์มีอำนาจสมบูรณ์เด็จขาดและยืนยันว่ากฎหมายบ้านเมือง คือ คำสั่งของรัฏฐาธิปัตย์ก็เท่ากับเป็นการกรุยทางวางรากฐานทางความคิดให้แก่สำนักบ้านเมืองในเวลาต่อมา, ปรีดี เกษมทรัพย์, นิติปรัชญา, 2539 หน้า 190

[38] ปรีดี เกษมทรัพย์, *นิติปรัชญา*, 188-189.

เจตจำนงเช่นว่านั้นจะเรียกชื่ออย่างใดในทางการเมืองก็ตาม (เช่น ระบบประชาธิปไตย ระบอบสมบูรณาญาสิทธิราชย์ ระบอบสังคมนิยาม ฯลฯ) และไม่ว่าการจัดองค์กร ในการออกกฎเกณฑ์เช่นว่านั้นจะเป็นอย่างไรก็ตาม (เช่น โดยฝ่ายนิติบัญญัติหรือโดยประมุขของรัฐโดยความเห็นชอบและยินยอมของฝ่ายนิติบัญญัติ เป็นต้น) เมื่อกฎเกณฑ์ใดได้ออกโดยผ่านขั้นตอนตามรูปแบบซึ่งเป็นที่ยอมรับในแต่ละรัฐแล้ว กฎเกณฑ์เช่นว่านั้นก็ถือเป็นกฎหมายที่เป็นอยู่ ซึ่งใช้บังคับแก่บุคคลโดยทั่วไปและมีจะมีอำนาจบังคับควบคู่ไปด้วยเสมอ

จากการศึกษาร่างพระราชบัญญัติความมั่นคงไซเบอร์นี้พบว่ากฎหมายนี้ได้ดำเนินรอยตามแนวความคิดของสำนักกฎหมายบ้านเมืองที่เชื่อว่ารัฏฐาธิปัตย์มีอำนาจเด็ดขาด ประชาชนทุกคนย่อมต้องอยู่ภายใต้บังคับของรัฏฐาธิปัตย์โดยปราศจากเงื่อนไข รัฏฐาธิปัตย์มีอำนาจเต็มที่ในการรักษาความสงบเรียบร้อย ประชาชนไม่มีสิทธิกล่าวอ้างว่ารัฐเป็นผู้กระทำความผิดเหตุผลเพราะรัฏฐาธิปัตย์มิใช่คู่สัญญากับราษฎร และไม่มีหน้าที่ทำตามสัญญา ดังนั้นรัฏฐาธิปัตย์จึงมีอำนาจสมบูรณ์เด็ดขาดเหนือราษฎร เป็นนิรันดรและไม่ถูกจำกัดโดยสิ่งใดๆ[39] ด้วยเหตุนี้เราจะเห็นได้ว่า การที่ร่างพระราชบัญญัตินี้ได้ถูกตราออกมานั้นเป็นการยืนยันแนวความคิดที่ว่าอำนาจอธิปไตยย่อมสมบูรณ์เด็ดขาดเป็นนิรันดร และไม่อยู่ภายใต้บังคับของกฎหมายใดๆ เพราะเป็นความจงใจของรัฐ ดังจะเห็นได้ว่าอำนาจของคณะกรรมการรักษาความปลอดภัยไซเบอร์แห่งชาติที่มีอยู่อย่างกว้างขวาง และคณะกรรมการฯ สามารถที่จะตีความว่าสิ่งใดเข้าข่ายอำนาจหน้าที่ของตนก็ได้ นอกจากนี้ การที่พนักงานเจ้าหน้าที่ตามพระราชบัญญัติความมั่นคงไซเบอร์นี้สามารถเข้าถึงข้อมูลการสื่อสาร โดยไม่ต้องมีหมายศาล และสามารถตรวจสอบการสื่อสารของประชาชนได้ทุกช่องทาง โดยไม่มีขอบเขตและไม่มีกระบวนการตรวจสอบใดๆ มาคานอำนาจ ถึงแม้ว่ารัฐธรรมนูญแห่งราชอาณาจักรไทย (ฉบับชั่วคราว) พุทธศักราช 2557 มาตรา 4 ที่ยังคงยืนยัน ศักดิ์ศรี

[39] ปรีดี เกษมทรัพย์, *นิติปรัชญา*.

ความเป็นมนุษย์ สิทธิ เสรีภาพ และความเสมอภาค รวมถึงประเทศไทยต้องปฏิบัติตามพันธกรณีระหว่างประเทศที่ประเทศไทยมีอยู่แล้ว[40] เช่น กฎหมายระหว่างประเทศว่าด้วยการคุ้มครองสิทธิมนุษยชนก็ตาม จึงเท่ากับว่าผู้ร่างพระราชบัญญัติความมั่นคงไซเบอร์นี้เชื่อว่ากฎหมาย (พระราชบัญญัตินี้) ที่จะใช้บังคับอยู่ในบ้านเมืองเท่านั้นที่เป็นกฎหมายที่แท้จริง เป็นระบบที่สมบูรณ์อยู่ในตัวเอง ไม่มีความจำเป็นที่จะต้องไปอาศัยหลักการอะไรมาค้ำจุนด้วยประการใดๆ ทั้งสิ้น[41]

4. สรุปและข้อเสนอแนะ

โดยสรุปแล้วแนวความคิดของนักนิติศาสตร์ทั้งจากสำนักกฎหมายธรรมชาติและสำนักกฎหมายบ้านเมือง ต่างก็เห็นพ้องต้องกันว่ากฎหมายว่าด้วยความมั่นคงไซเบอร์นั้นมีความสำคัญต่อการคุ้มครองประชาชนและการพัฒนาทางเศรษฐกิจของประเทศไทย เพียงแต่ว่าแต่ละสำนักความคิดนั้น ไม่สามารถจะให้คำตอบที่ชัดเจนถึงลักษณะที่แท้จริงของกฎหมายว่าด้วยความมั่นคงไซเบอร์ที่ต่างๆ ยอมรับและถือปฏิบัติอยู่ ทั้งนี้เป็นเพราะว่าแต่ละสำนักความคิดนั้นต่างก็มองทางกฎหมายว่าด้วยความมั่นคงไซเบอร์เฉพาะในแง่มุมและทฤษฎีของตนเท่านั้น จึงทำให้มองข้ามลักษณะที่แท้จริงของกฎหมายว่าด้วยความมั่นคงไซเบอร์ไป ไม่ว่าจะเป็นในรูปของกฎหมายระหว่างประเทศหรือกฎหมายภายในของรัฐก็ตามย่อมมีทั้งที่อยู่บนพื้นฐานของเหตุผลและเจตจำนง และโดยเฉพาะอย่างยิ่งในส่วนของกฎหมายภายในประเทศนั้น กฎเกณฑ์ซึ่งเกิดจากเจตจำนงในรูปของการให้ความยินยอม ที่อยู่บนพื้นฐานของเหตุผลและความเชื่อว่ากฎเกณฑ์นั้นเป็นสิ่งถูกต้องควรได้รับความเคารพและปฏิบัติตาม โดยยึดถือมาตรฐานทางสังคมระหว่างประเทศ (สากล) เป็นหลัก และในที่สุดก็เพื่อทำให้ประโยชน์ที่ขัดแย้งกันนั้นมีความสมดุลในสังคม สามารถอยู่ด้วยกันได้โดยให้แต่ละฝ่าย

[40] มาตรา 4 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย (ฉบับชั่วคราว) พุทธศักราช 2557

[41] ปรีดี เกษมทรัพย์, นิติปรัชญา, 241.

ไม่เสียประโยชน์และต่างรักษาประโยชน์ไว้ให้ได้มากที่สุดเท่าที่จะมากได้โดยให้มีความขัดแย้งน้อยที่สุดเท่าที่จะทำได้

นอกจากนี้ อำนาจตามร่างพระราชบัญญัติความมั่นคงไซเบอร์นี้เข้าข่ายการสอดแนม (Surveillance) ที่หมายถึง การเฝ้าสังเกต หรือควบคุมดูแลซึ่งบุคคล โดยไม่จำกัดเฉพาะการสังเกตการณ์ทางกายภาพ แต่รวมไปถึงพฤติกรรมทุกประเภท ซึ่งรัฐมักอ้างว่าเป็นวิธีเพื่อรักษาความสงบเรียบร้อยของสังคม เพื่อรับมือกับอาชญากรรมก่อนที่มันจะเกิดขึ้น และหากผู้ใดไม่กระทำผิด ก็ไม่จำเป็นต้องกลัวหรือเป็นกังวลอันใด ซึ่งมองผิวเผินอาจดูเหมือนเป็นสิ่งที่ยอมรับได้โดยเฉพาะกับสังคมที่มีประชาชนที่เคารพกฎหมายเป็นส่วนมาก โดยพวกเขามักไม่คิดว่าตนเองจะเป็นเป้าหมายของการสอดแนมและไม่ส่งผลกระทบต่อการดำเนินชีวิตใดๆ ในขณะเดียวกันก็ทำให้ชีวิตปลอดภัยและสะดวกสบายขึ้นจากการลดจำนวนอาชญากร ด้วยเหตุนี้จึงทำให้ การดักฟังโทรศัพท์โดยปราศจากหมายศาลที่ดูเหมือนจะเป็นการก้าวล่วงความเป็นส่วนตัวของประชาชนอย่างน้อยที่สุดเท่านั้น อย่างไรก็ดี ในความเป็นจริงนโยบายการสอดแนมของรัฐเช่นนี้ย่อมไม่เป็นที่ยอมรับของประชาชนโดยทั่วไป ไม่ใช่ว่าเพราะพวกเขามีสิ่งที่ต้องปิดบังและเป็นอันตรายต่อสังคม แต่เป็นเพราะมันล่วงละเมิดความเป็นส่วนตัวและเสี่ยงต่อการถูกนำไปใช้ในทางมิชอบ โดยเฉพาะกับบุคลากรผู้รับผิดชอบในองค์กรของรัฐเองเมื่อคดีความหรือวัตถุประสงค์ในการใช้ข้อมูลเหล่านั้นจบสิ้นลง ข้อมูลเหล่านั้นจะยังถูกจัดเก็บหรือนำไปใช้ต่อไป ดังที่กล่าวไว้ว่า ใครก็ตามที่มีอำนาจย่อมมีแนวโน้มจะใช้อำนาจไปในทางที่ไม่ชอบได้เสมอ แต่อย่างไรก็ตามในทางปฏิบัติแล้ว การเรียกดูข้อมูลหรือการสอดแนมนั้นสามารถกระทำอย่างมีจริยธรรมได้หากกระทำโดยผ่านกระบวนการที่ชอบธรรมและเป็นเหตุเป็นผล เป็นที่ยอมรับของสังคมทั่วไป ดังนั้นการที่รัฐจะดำเนินการเรียกดูข้อมูลและทำการสอดแนมใดๆ นั้น วิธีการดังกล่าวควรได้รับการประเมินผลเสียก่อน

รายการอ้างอิง

ILAW. (2554, 7 เมษายน) *อัปเกรด พ.ร.บ. คอมฯ เพิ่มโทษผู้ดูแลระบบ ก๊อปไฟล์โหลด บิทเสี่ยงคุก*, จาก http://ilaw.or.th/node/857 [ค้นเมื่อ 11 พฤศจิกายน 2556]

NECTEC, *คำถามที่พบบ่อยเกี่ยวกับร่างพระราชบัญญัติการกระทำผิดเกี่ยวกับคอมพิวเตอร์*, จาก http://wiki.nectec.or.th/nectecpedia2/ index.php/คำถามที่พบบ่อย_เกี่ยวกับร่าง พรบ. การกระทำผิดเกี่ยวกับคอมพิวเตอร์ [ค้นเมื่อ 11 พฤศจิกายน 2556]

พระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544. (2544, 16 พฤศจิกายน) *ราชกิจจานุเบกษา*, เล่มที่ 118, ตอนที่ 106ก, หน้า 11-38.

ปรีดี เกษมทรัพย์. (2539) *นิติปรัชญา*, กรุงเทพฯ: โครงการตำราและเอกสารประกอบการสอน คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์.

สราวุธ ปิติยาศักดิ์. (2552) *กฎหมายเทคโนโลยีสารสนเทศ*, กรุงเทพฯ: นิติธรรม.

สมณ์ พรหมรส, *คำแปลปฏิญญากรุงเทพฯ*, สำนักงานกิจการยุติธรรม, จาก, http://www.oja.go.th/new2011/document/Lists/Download_1/Attachments/36/oja_symposium_5_G3_room6_6.pdf [ค้นเมื่อ 4 กันยายน 2555]

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). (ม.ป.ป.) *ร่างพระราชบัญญัติความมั่นคงไซเบอร์ พ.ศ. . . .*, จาก http://ictlawcenter.etda.or.th/files/de_law/file/7/32ce1e368d7f0f076c045fcab1b916c1.pdf [ค้นเมื่อ 4 กันยายน 2555]

รัฐธรรมนูญแห่งราชอาณาจักรไทย (ฉบับชั่วคราว) พุทธศักราช 2557. (2557, 22 กรกฎาคม) *ราชกิจจานุเบกษา*, เล่มที่ 131, ตอนที่ 55ก, หน้า 1-17.

Clarke, R. A., & Knake, R. (2012) *Cyber war: The next threat to national security and what to do about it*, New York: HarperCollins.

UN General Assembly. (2000, 4 December) *Combating the criminal misuse of information technology*, Resolution 55/63.

Communication of the European Commission: Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime of 26.1.2001: COM (2000) 890 final, [Online], Available: http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/CrimeCommEN.htm [19 March 2013]

Congressional Research Service. (2004) *The economic impact of cyber-attacks*, Washington, DC: CRS.

International Telecommunication Union. (2007, June) *The world information society report 2007*, [Online], Available: http://www.itu.int/osg/spu/publications/ worldinformationsociety/2007/ [10 November 2013]

Malaysia, Global Resource and Information Directory, [Online], Available: http://www.fosigrid.org/asia/Malaysia [21 March 2014]

O'Connell, K. (2007, October 17) *Cyber-crime hits $ 100 billion in 2007*, [Online], Available: http://www.ibls.com/internet_law_news_portal_ view_ prn.aspx?s=latestnews&id=1882 [17 October 2013]

Proposal for a Council Framework Decision on attacks against information systems of 19.04.2002 COM (2002) 173 final.

Regional Internet Governance Forum, About APrIGF 2011.