บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบันเทคโนโลยีสารสนเทศและการติดต่อสื่อสารได้ถูกพัฒนาอย่างรวดเร็ว โดยเฉพาะเทคโนโลยีทางด้านคอมพิวเตอร์และระบบเครือข่ายอินเทอร์เน็ต (ระบบเครือข่ายอินเทอร์เน็ต เป็นระบบเครือข่ายคอมพิวเตอร์ขนาดใหญ่ที่เกิดจากการเชื่อมต่อเครือข่ายต่างๆไม่ว่าจะเป็นระบบ LAN หรือระบบ WAN เข้าด้วยกัน ทำให้เครื่องคอมพิวเตอร์นับล้านๆเครื่องทั่วโลกสามารถติดต่อสื่อสารกันได้โดยใช้มาตรฐานเดียวกันที่เรียกว่า หรือ Transmission Control Protocol : TCP หรือ Internet Protocol : IP และเครื่องคอมพิวเตอร์ที่อยู่ในเครือข่ายอินเทอร์เน็ตจะต้องมีหมายเลข IP Address)[1] การเชื่อมโยงของสังคมข้อมูลข่าวสารจึงกลายเป็นสังคมที่มีการติดต่อที่สะดวกรวดเร็ว เครือข่ายการส่งผ่านข้อมูลสารสนเทศต่างๆได้ถูกส่งผ่านทางคอมพิวเตอร์และระบบเครือข่ายอินเทอร์เน็ต ซึ่งเป็นเครือข่ายการติดต่อสื่อสารที่ไร้พรมแดนทางภูมิศาสตร์สามารถเชื่อมโยงกันได้ทั่วโลก เทคโนโลยีทางด้านคอมพิวเตอร์และระบบเครือข่ายอินเทอร์เน็ตได้ถูกพัฒนาให้มีความทันสมัยและกลายมาเป็นส่วนหนึ่งของชีวิตมนุษย์ที่บุคคลทั่วไปสามารถเข้าถึงได้โดยง่าย ด้วยเหตุนี้จึงทำให้จำนวนของผู้ใช้คอมพิวเตอร์และระบบเครือข่ายอินเทอร์เน็ตมีจำนวนเพิ่มสูงขึ้นอย่างต่อเนื่อง

จากความก้าวหน้าของเทคโนโลยีอินเทอร์เน็ตความเร็วสูง (Broadband Internet) ในปัจจุบันนั่นเอง ทำให้การใช้งานอินเทอร์เน็ตมีความหลากหลายมากขึ้นกว่าการใช้อินเทอร์เน็ตผ่านเบราเซอร์แต่เพียงอย่างเดียว อีกทั้งการรับ-ส่งจดหมายอิเล็กทรอนิกส์ (Electronic Mail) ไม่ได้ถูกจำกัดเฉพาะผู้ที่มีเครื่องคอมพิวเตอร์ดังเช่นในอดีตที่ผ่านมา ผนวกกับความต้องการเข้าถึงอินเทอร์เน็ตได้ทุกที่ทุกเวลา ทำให้มีการพัฒนาเทคโนโลยีโทรศัพท์เคลื่อนที่และอุปกรณ์เคลื่อนที่ต่างๆที่ทำงานผ่านเครือข่ายไร้สาย* (Wireless Device) ให้สามารถรองรับการเชื่อมต่อ

---

[1] ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ, รายงานผลการสำรวจกลุ่มผู้ใช้อินเทอร์เน็ตในประเทศไทย ปี 2550 : Internet User Profile of Thailand 2007, (กรุงเทพมหานคร: ด่านสุทธาการพิมพ์, 2550), หน้า 7-8.

* การสื่อสารแบบไร้สาย (Wireless Communication) หมายถึง การสื่อสารที่ใช้สื่อชนิดที่ทำหน้าที่เป็นตัวกลางให้คลื่นแม่เหล็กไฟฟ้าสามารถผ่านไปได้โดยไม่ต้องอาศัยสายส่งข้อมูล ซึ่งปกติแล้วจะอาศัยอากาศที่อยู่รอบๆ ทำหน้าที่เสมือนกับสายส่งข้อมูล ส่วนการส่งคลื่นผ่านอากาศนั้น โดยส่วนใหญ่แล้วจะเป็นการกระจายไปรอบทิศทาง โดยสื่อแบบไร้สาย แบ่งตามวิธีการแพร่สัญญาณได้ 3 วิธี

อินเทอร์เน็ตความเร็วสูงได้อย่างมีประสิทธิภาพ ความต้องการติดต่อสื่อสารที่มีมากขึ้นประกอบกับความต้องการเข้าถึงสื่อบันเทิงรูปแบบต่างๆอย่างสะดวกรวดเร็ว ก่อให้เกิดการพัฒนาเนื้อหาดิจิทัลบนโทรศัพท์เคลื่อนที่ (Mobile Content) ซึ่งเป็นรูปแบบการให้บริการเนื้อหาจากการหลอมรวมสื่อและการให้บริการใหม่ๆหลากหลายรูปแบบ เพื่อให้สอดคล้องกับความต้องการของผู้ใช้ ไม่ว่าจะเป็นการดาวน์โหลดเพลง ภาพยนต์ โล้โก้ ริงโทน และเกม ซึ่งล้วนแล้วแต่เป็นช่องทางใหม่ๆที่เกิดขึ้นจากนวัตกรรมทางเทคโนโลยีที่มีความทันสมัยมากขึ้น ทำให้การสื่อสารในรูปแบบเดิมได้เปลี่ยนไปจนไม่สามารถแบ่งแยกความแตกต่างและขอบเขตการให้บริการติดต่อสื่อสารทางโทรคมนาคม อินเทอร์เน็ต และวิทยุ โทรทัศน์ ได้อย่างชัดเจนอีกต่อไป ทั้งนี้เป็นผลเนื่องจากการหลอมรวมทางด้านเทคโนโลยี (Technological Convergence) และการหลอมรวมทางด้านการให้บริการ (Service Convergence) เป็นที่เชื่อกันว่าอินเทอร์เน็ตเป็นตัวกลางสำคัญของการหลอมรวม (Convergence) ของสื่อโทรคมนาคมสารสนเทศและวิทยุโทรทัศน์เข้าด้วยกัน การเข้าถึงข้อมูลข่าวสาร ตลอดจนแหล่งบันเทิงต่างๆ นำมาซึ่งการบริการอันหลากหลายที่สามารถทำได้หรือทำได้ยากในปัจจุบัน เช่น การให้บริการทางโทรศัพท์ อินเทอร์เน็ต และวิทยุ โทรทัศน์ในรูปแบบหลอมรวมเครือข่ายเดียวกัน[2]

การพัฒนาเทคโนโลยีไร้สายความเร็วสูงสำหรับการเชื่อมต่อเครือข่ายอินเทอร์เน็ตและการพัฒนาเทคโนโลยีสำหรับการให้บริการโทรคมนาคมมีการปรับปรุงพัฒนาและเพิ่มขีดความสามารถของช่องสัญญาณ (Bandwidth) บนเครือข่ายโทรคมนาคมและสารสนเทศได้มากเท่าใด โอกาสการเข้าถึงเทคโนโลยีไร้สายสำหรับการเชื่อมต่อเครือข่ายอินเทอร์เน็ตก็มากขึ้นเป็นเงาตามตัว ความต้องการใช้บริการอินเทอร์เน็ตบนโทรศัพท์เคลื่อนที่ของผู้ใช้บริการอินเทอร์เน็ตขยายตัวเพิ่มสูงขึ้น เนื่องจากความสะดวกในการเข้าถึงเครือข่ายอินเทอร์เน็ตที่สะดวกมากขึ้น ปัจจุบันเทคโนโลยีการเชื่อมต่ออินเทอร์เน็ตสำหรับโทรศัพท์เคลื่อนที่ที่นิยมใช้ได้แก่ EDGE GPRS WAP

---

1. Ground Propagation เป็นวิธีการแพร่คลื่นวิทยุ ออกไปในระดับล่าสุดของชั้นบรรยากาศ สัญญาณที่ส่งออกไปเป็นสัญญาณคลื่นความถี่ต่ำ และจะเคลื่อนที่ไปตามความโค้งของโลกส่วนระยะทางที่สามารถเดินทางไปได้นั้น ขึ้นอยู่กับกำลังส่งว่ามีมากน้อยเพียงใด เช่นหากตัวส่งมีกำลังส่งสูง ก็จะสามารถส่งสัญญาณออกไปได้เป็นระยะทางไกลๆ

2. Sky Propagation เป็นการส่งคลื่นวิทยุขึ้นไปในชั้นบรรยากาศชั้นไอโอโนสเฟียร์ (Ionosphere) ซึ่งเป็นชั้นบรรยากาศที่มีอิออนอยู่มาก และบรรยากาศในชั้นนี้จะทำหน้าที่สะท้อนคลื่นนั้นกลับมายังพื้นโลกอีกครั้ง ความถี่ของสัญญาณในการส่งแบบนี้จะสูงกว่าแบบแรก และถ้าใช้กำลังส่งเท่ากันแล้วจะสามารถส่งไปได้ในระยะทางที่ไกลกว่า

3. Line of Sight Propagation เป็นการส่งคลื่นวิทยุความถี่สูง โดยลักษณะของการส่งจะเป็นแบบเส้นตรงระหว่างตัวส่งและตัวรับ ดังนั้นเสาอากาศที่จะใช้ในการรับส่งสัญญาณจะต้องมีความสูงเพียงพอที่จะสามารถทำการรับส่งกันได้ เนื่องจากการส่งแบบนี้สัญญาณจะเคลื่อนที่ไปตามแนวความโค้งของโลก

[2] ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ. รายงานผลการสำรวจกลุ่มผู้ใช้อินเทอร์เน็ตในประเทศไทย ปี 2550 : Internet User Profile of Thailand 2007. หน้า 7-8.

และ Wi-Fi เมื่อรูปแบบความต้องการใช้อินเทอร์เน็ตเปลี่ยนแปลงไป ทำให้ผู้ให้บริการอินเทอร์เน็ตจำเป็นต้องมีการปรับเปลี่ยนทิศทางการให้บริการด้วย เมื่อพิจารณาทิศทางของเทคโนโลยีสื่อสารในปี พ.ศ. 2550 พบว่าตลาดให้บริการอินเทอร์เน็ตความเร็วสูง (Broadband) ยังคงเป็นตลาดที่มีการเจริญเติบโตมาก โดยเฉพาะการให้บริการที่เกิดจากการหลอมรวมทางเทคโนโลยี เช่น เทคโนโลยีสัญญาณเสียงผ่านโครงข่ายข้อมูลอินเทอร์เน็ต หรือ Voice Over Internet Protocol : VoIP และการให้บริการโทรทัศน์เคลื่อนที่บนโทรศัพท์เคลื่อนที่ ปัจจัยอย่างหนึ่งที่ทำให้การใช้อินเทอร์เน็ตเติบโตขึ้นอย่างมีนัยสำคัญในประเทศไทยคือ ปริมาณการใช้คอมพิวเตอร์แบบพกพาและโทรศัพท์เคลื่อนที่ประเภทสมาร์ทโฟน เช่น I-phone และ Blackberry ที่มีคุณสมบัติและการปฏิบัติงานคล้ายคลึงกับคอมพิวเตอร์ ทำให้อัตราการขยายตัวเพิ่มขึ้นอย่างต่อเนื่อง จากวิถีชีวิตที่เปลี่ยนแปลงไปทำให้โทรศัพท์เคลื่อนที่กลายมาเป็นปัจจัยที่ 5 ของการใช้ชีวิตในสังคมเมือง

จากรายงานการศึกษาของ OECD เกี่ยวกับอัตราการเจริญเติบโตของเนื้อหาดิจิทัลบนโทรศัพท์เคลื่อนที่ปี ค.ศ. 2003 พบว่าตลาดในภูมิภาคเอเชียแปซิฟิกมีการเติบโตมากกว่าตลาดในภูมิภาคอเมริกาเหนือและยุโรป และจากรายงานการศึกษาของ European Commission ระบุว่าตลาดในประเทศยุโรปจะสามารถเจริญเติบโตได้ถึง 25 พันล้านเหรียญสหรัฐ ในปี ค.ศ. 2008 จากข้อมูลดังกล่าวจะเห็นได้อย่างชัดเจนว่าภูมิภาคเอเชียมีการเจริญเติบโตของเนื้อหาดิจิทัลบนโทรศัพท์เคลื่อนที่ที่ค่อนข้างสูงทั้งในด้านของบริการสื่อสารประเภทข้อมูลรูปแบบต่างๆ และทางด้านของเกมบนโทรศัพท์เคลื่อนที่ ทั้งนี้ ปัจจัยหนึ่งที่ทำให้เกิดการเจริญเติบโตในระดับที่สูงสำหรับประเทศในภูมิภาคเอเชีย คืออัตราการใช้อินเทอร์เน็ตที่ยังไม่ถึงจุดอิ่มตัวดังเช่นในประเทศสหรัฐอเมริกา และกลุ่มประเทศยุโรป

แนวโน้มการบริโภคและการใช้งานเนื้อหาบนโทรศัพท์เคลื่อนที่ในปัจจุบันมีความต้องการเพิ่มขึ้นอย่างกว้างขวางทั้งในประเทศไทยและประเทศอื่นๆทั่วโลก โดยเฉพาะเมื่อผนวกกับความก้าวหน้าของโครงสร้างพื้นฐานทางเทคโนโลยีในด้านต่างๆ เช่น ระบบอินเทอร์เน็ตความเร็วสูง ระบบการสื่อสารไร้สาย และความสามารถในการประมวลผลของเครื่องคอมพิวเตอร์ทำให้ความต้องการเนื้อหาบนโทรศัพท์เคลื่อนที่ขยายตัวเพิ่มขึ้นในอัตราที่สูงมากในช่วงทศวรรษที่ผ่านมาส่งผลให้เกิดการพัฒนาเนื้อหาบนโทรศัพท์เคลื่อนที่อย่างกว้างขวางทั่วโลก

ในทางกลับกันความเจริญก้าวหน้าของคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตที่มีความทันสมัยและมีความรวดเร็วของเทคโนโลยีนั้นก็ได้ก่อให้เกิดอาชญากรรมรูปแบบใหม่ ที่เรียกว่า "อาชญากรรมทางคอมพิวเตอร์" วัตถุที่กลายมาเป็นเป้าหมายหลักได้เปลี่ยนไปเป็นฐานข้อมูลทาง

เศรษฐกิจ ผลิตภัณฑ์ทางดิจิทัล โปรแกรมคอมพิวเตอร์ ระบบรักษาความปลอดภัยทางคอมพิวเตอร์ เป็นต้น ซึ่งสิ่งเหล่านี้กลายมาเป็นสิ่งสำคัญที่รัฐต้องดูแลเป็นพิเศษด้วยรูปแบบและวิธีการใหม่ๆโดยอาศัยเครื่องมือทางเทคโนโลยีที่ทันต่ออาชญากรรม และจากการพัฒนาที่ก้าวไกลของเทคโนโลยีประเภทนี้อาจนำมาซึ่งอาชญากรรมข้ามชาติที่สามารถเกิดขึ้นได้โดยปราศจากเงื่อนไขของพรมแดนอีกต่อไป ซึ่งอาชญากรรมข้ามชาตินั้นอาจปรากฏออกมาในรูปแบบต่างๆ การก่อการร้ายโดยการบ่อนทำลาย โดยการใช้ไวรัสลบข้อมูล และเกิดความยากลำบากต่อการทำงานของระบบ หรือการใช้ระบบอินเทอร์เน็ตในกิจกรรมรูปแบบต่างๆ อาจเป็นเครื่องมือ หรือวิธีการของผู้ก่อการร้าย ซึ่งมีผลกระทบโดยตรงต่อความมั่นคงระหว่างประเทศ[3] จะเห็นได้ว่าเพราะความเจริญก้าวหน้าทางเทคโนโลยีของคอมพิวเตอร์และระบบเครือข่ายอินเทอร์เน็ตนี้เองที่ทำให้อาชญากรรมทางคอมพิวเตอร์สามารถเกิดขึ้นได้โดยง่าย กล่าวคือ สามารถเกิดขึ้นได้ ณ เวลา และสถานที่ใดๆ บนโลกก็ได้ โดยอาจเป็นการกระทำความผิดจากระยะไกลซึ่งผู้กระทำความผิดไม่ต้องอยู่ในสถานที่เกิดเหตุเหมือนอาชญากรรมรูปแบบเดิม หรืออาจเป็นการกระทำความผิดที่มีลักษณะข้ามประเทศ คือ มีการกระทำเกิดขึ้นในพรมแดนของรัฐมากกว่าหนึ่งรัฐ และผู้กระทำความผิดหรือเหยื่อของการกระทำความผิดเป็นพลเมืองของรัฐที่เข้ามาเกี่ยวข้องมากกว่าหนึ่งรัฐ การที่จะปราบปรามอาชญากรรมดังกล่าวให้ได้ผลอย่างจริงจังจึงอาจทำได้ยาก และปัญหาดังกล่าวข้างต้นเป็นปัญหาที่เกิดขึ้นทั่วโลกไม่เฉพาะในประเทศไทย เนื่องจากพื้นที่ในโลกอินเตอร์เน็ตนั้นไม่มีพรมแดนและไม่มีขอบเขตหรืออาณาเขต

ดังนั้น การบังคับใช้กฎหมายและใช้มาตรการทางเทคนิคของแต่ละประเทศอาจจะประสบปัญหาเขตอำนาจศาลในการพิจารณาคดีเมื่อเกิดข้อพิพาทศาลของประเทศใดจะมีอำนาจในการพิจารณาคดี หากมีหลายประเทศอ้างเขตอำนาจศาลเหนือการกระทำความผิดนั้น เพราะเว็บไซต์นั้นสามารถเข้าถึงเนื้อหาได้ทั่วโลก แต่กฎหมายของแต่ละประเทศนั้นจะสามารถบังคับใช้ได้เฉพาะในเขตอำนาจอธิปไตยหรือในดินแดนของตนเองเท่านั้น หรือหากศาลมีคำสั่งให้ปิดกั้นเนื้อหาเว็บไซต์ก็ไม่สามารถบังคับใช้กับเจ้าของเว็บไซต์ที่อยู่ในต่างประเทศได้

จากช่องโหว่ทางกฎหมายดังกล่าวทำให้ในทางปฏิบัติรัฐบาลในบางประเทศจึงมักนิยมใช้มาตรการทางเทคนิคในการปิดหรือบล็อกเว็บไซท์ที่มีเนื้อหาขัดต่อกฎหมายโดยออกคำสั่งไปยังผู้ให้บริการอินเตอร์เน็ต เจ้าของเว็บไซต์ ให้ทำการปิดหรือบล็อกเว็บไซต์ทั้งในและต่างประเทศ ซึ่ง

---

[3] สุจิต บุญบงการ และวีระพงษ์ บุญโญภาส, "รวมบทความและสาระหน้ารู้เกี่ยวกับมาตรการในการเข้าถึงข้อมูลข่าวสาร", ใน เอกสารประกอบการสัมมนาทางวิชาการเรื่องนโยบายความมั่นคงและปัญหาอาชญากรรมข้ามชาติ มุมมองไทย ยุโรปและนานาชาติ, (กรุงเทพฯ : ศูนย์ยุโรปศึกษาแห่งจุฬาลงกรณ์มหาวิทยาลัย, 2544,) หน้า 12-13.

ทันทีที่มีการปิดหรือบล็อกเว็บไซต์ดังกล่าว เจ้าของเว็บไซต์ก็จะย้ายไปเชื่อมต่อในประเทศอื่นทันที รวมถึงการแก้ไขเปลี่ยนแปลงชื่อเว็บไซท์ (Domain Name) และชื่อที่อยู่บนอินเตอร์เน็ต (IP Address) สามารถทำได้ภายในระยะเวลาเพียงไม่กี่วินาที

และเหตุนี้เองทำให้ทั่วโลกต้องการที่จะพัฒนาความร่วมมือระหว่างกันในทางอาญาโดยไม่ให้มีรัฐใดที่จะมีอำนาจอธิปไตยเหนือรัฐอื่นนอกเขตแดนของตน เพื่อป้องกันและปราบปรามอาชญากรรมดังกล่าว องค์การระหว่างประเทศต่างๆที่ตระหนักถึงสิ่งดังกล่าว เช่น

1. **องค์การสหประชาชาติ** (International Review of Criminal Policy - United Nations Manual on the Prevention and Control of Computer-related Crime)[4]

องค์การสหประชาชาติได้เริ่มพัฒนากรอบนโยบายด้านอาชญากรรมทางคอมพิวเตอร์ในปี 1990 ในการประชุม United Nations Congress on the Prevention of Crime and the Treatment of Offenders ครั้งที่ 8 ซึ่งได้กำหนดมาตรการเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ใน Resolution ที่ 45/121

ต่อมาในปี ค.ศ. 1994 ได้จัดทำคู่มือการป้องกันและควบคุมอาชญากรรมทางคอมพิวเตอร์ (United Nations Manual on the Prevention and Control of Computer related Crime) ออกเผยแพร่ ซึ่งมีเนื้อหาเกี่ยวกับแนวทางการบัญญัติฐานความผิดและกฎหมายวิธีพิจารณาความที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์ รวมไปถึงกลไกความร่วมมือระหว่างประเทศ และในปี ค.ศ. 2001 องค์การสหประชาชาติได้ออกข้อมติที่ประชุมใหญ่ (General Assembly Resolution 55/63)[5] ที่มีชื่อว่า Combating the Criminal Misuse of Information Technologies โดยกำหนดหลักการให้ประเทศสมาชิกนำไปใช้เป็นแนวทางในการต่อต้านอาชญากรรมทางคอมพิวเตอร์ 10 ประการ ได้แก่

1. ควรมีกฎหมายและวิธีปฏิบัติที่ทำให้มั่นใจได้ว่าจะสามารถลงโทษผู้ที่ใช้เทคโนโลยีสารสนเทศในการกระทำความผิดทางอาญาได้

2. ควรมีความร่วมมือกันในด้านการสอบสวนและการฟ้องร้องคดีอาชญากรรมทางคอมพิวเตอร์ในกลุ่มประเทศที่เกี่ยวข้องกับการกระทำความผิด

---

[4] สำนักงานเลขาธิการคณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ, แนวทางการจัดทำกฎหมายอาชญากรรมทางคอมพิวเตอร์, [ออนไลน์], 2553. แหล่งที่มา http://www.lawreform.go.th[2553, มกราคม 11] หน้า 54-56.

[5] เรื่องเดียวกัน, หน้า 21

3. ควรมีการแลกเปลี่ยนข้อมูลกันระหว่างประเทศที่ประสบปัญหาจากการใช้เทคโนโลยีสารสนเทศในทางมิชอบ

4. ควรมีการฝึกอบรมและจัดให้มีอุปกรณ์ที่เพียงพอแก่บุคลากรที่เกี่ยวข้องกับการใช้บังคับกฎหมายในการจัดการกับปัญหาการก่ออาชญากรรมโดยใช้เทคโนโลยีสารสนเทศ

5. ควรมีระบบกฎหมายที่สามารถให้ความคุ้มครองความลับ ความถูกต้องแท้จริง และความพร้อมใช้งานหรือความสามารถในการทำงานของข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์จากการทำให้เสียหายโดยมิชอบ และมั่นใจได้ว่าจะสามารถลงโทษผู้กระทำความผิดทางอาญาได้

6. ควรมีระบบกฎหมายที่อนุญาตให้มีการเก็บรักษา (Preservation) และสามารถเข้าถึงข้อมูลอิเล็กทรอนิกส์ (Data Massage หรือ Electronic Data) ที่เกี่ยวข้องในการสอบสวนคดีอาชญากรรมทางคอมพิวเตอร์ได้

7. ควรมีหลักเกณฑ์ด้านความร่วมมือระหว่างประเทศ เพื่อให้มั่นใจได้ว่าจะมีการสอบสวนการกระทำความผิดที่ใช้เทคโนโลยีสารสนเทศได้อย่างรวดเร็ว ตลอดจนสามารถรวบรวมและแลกเปลี่ยนพยานหลักฐานระหว่างกันได้อย่างทันท่วงที

8. ควรสร้างความตื่นตัว (Awareness) ถึงความจำเป็นในการป้องกันและการจัดการกับปัญหาการก่ออาชญากรรมโดยใช้เทคโนโลยีสารสนเทศให้แก่ประชาชนโดยทั่วไป

9. ควรมีการออกแบบเทคโนโลยีสารสนเทศที่ใช้สำหรับช่วยป้องกันและติดตามร่องรอยของผู้กระทำความผิด รวมไปถึงการรวบรวมพยานหลักฐานต่างๆ

10. ในการดำเนินการเพื่อต่อต้านการก่ออาชญากรรมโดยใช้เทคโนโลยีสารสนเทศนั้น จะต้องมีการพัฒนามาตรการที่จะสร้างความสมดุลระหว่างการปกป้องสิทธิเสรีภาพและความเป็นส่วนตัวของประชาชนควบคู่ไปกับการใช้อำนาจรัฐในการรับมือกับปัญหาอาชญากรรมทางคอมพิวเตอร์

ทั้งนี้ ในปี ค.ศ. 2003 องค์การสหประชาชาติ ได้ผ่านข้อมติที่ 239 ในการประชุมสามัญสมาชิกครั้งที่ 57 ซึ่งใช้ชื่อว่า Creation of a Global Culture of Cyber-security เพื่อให้ประเทศสมาชิกตระหนักถึงความสำคัญและจำเป็นในการร่วมมือกันรักษาความมั่นคงของเครือข่าย ทั้งนี้ หลักการทั้งหมดได้มาจากแนวปฏิบัติเพื่อการรักษาความมั่นคงของระบบสารสนเทศและเครือข่าย : มุ่งสู่วัฒนธรรมด้านความมั่นคง (Guidelines for the Security of

Information Systems and Networks : Towards a Culture of Security) ของ The Organization for Economic Cooperation and Development (OECD)

2. **องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา** (The Organization for Economic Cooperation and Development : OECD) Recommendation No. R (89) 9 Analysis of Legal Policy in 1986[6]

องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนานับได้ว่าเป็นองค์การระหว่างประเทศลำดับแรกที่ได้ริเริ่มพัฒนามาตรการที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์ ตั้งแต่ปี ค.ศ. 1983 ด้วยการจัดตั้งคณะกรรมาธิการผู้เชี่ยวชาญเพื่อหารือเกี่ยวกับปัญหาอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ (Computer Related-crime) ซึ่งต่อมาในปี ค.ศ. 1986 คณะกรรมาธิการดังกล่าวก็ได้จัดทำข้อเสนอแนะแก่ประเทศสมาชิกในการบัญญัติกฎหมายภายในให้มีความสอดคล้องกันในฐานความผิดที่สำคัญ เช่น การรบกวนข้อมูลหรือโปรแกรมคอมพิวเตอร์เพื่อให้ได้มาซึ่งประโยชน์ในทางทรัพย์สิน การปลอมแปลงทางคอมพิวเตอร์ การขัดขวางการทำงานของคอมพิวเตอร์และระบบโทรคมนาคม การเข้าถึงหรือการดักการสื่อสารของระบบคอมพิวเตอร์หรือระบบโทรคมนาคมโดยมิชอบ

นอกจากมาตรการด้านกฎหมายแล้ว OECD ยังได้พัฒนาแนวปฏิบัติเพื่อการรักษาความมั่นคงของระบบสารสนเทศ (Guidelines for the Security of Information Systems) ในปี ค.ศ. 1992 โดยมีวัตถุประสงค์เพื่อให้ภาครัฐและเอกชนได้ตระหนักถึงมาตรฐานขั้นต่ำในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ และได้มีการปรับปรุงแนวปฏิบัติดังกล่าวอีกครั้งในปี ค.ศ. 2002 โดยใช้ชื่อว่า แนวปฏิบัติเพื่อการรักษาความมั่นคงของระบบสารสนเทศและเครือข่าย : มุ่งสู่วัฒนธรรมด้านความมั่นคง (Guidelines for the Security of Information Systems and Network : Towards a Culture of Security) เพื่อให้สอดคล้องกับแนวโน้มการพัฒนาของเทคโนโลยีสารสนเทศที่มีความก้าวหน้าและมีความหลากหลายมากขึ้น ควบคู่ไปกับปัญหาการรักษาความมั่นคงของระบบสารสนเทศและเครือข่ายซึ่งทวีความรุนแรงและมีมูลค่าความเสียหายเพิ่มขึ้นทุกขณะ โดยแนวปฏิบัติฉบับใหม่นี้ได้กำหนดหลักเกณฑ์เพื่อการรักษาความมั่นคง 9 ประการ ได้แก่

1. การสร้างความตื่นตัว (Awareness) เนื่องจากระบบสารสนเทศหรือระบบเครือข่ายนั้นมีโอกาสที่จะตกอยู่ในภาวะเสี่ยงต่างๆอยู่ตลอดเวลาไม่ว่าจะมีสาเหตุจากภายในองค์กรหรือ

---

[6] เรื่องเดียวกัน, หน้า 56-60.

นอกองค์กร ซึ่งอาจส่งผลกระทบรุนแรงต่อบุคคลอื่นได้ ดังนั้น ทุกฝ่ายที่เกี่ยวข้องต้องตระหนักถึงความจำเป็นในการรักษาความมั่นคงในระบบสารสนเทศและเครือข่าย ตลอดจนมาตรการเท่าที่จะกระทำได้เพื่อปรับปรุงมาตรการรักษาความมั่นคง

2. การมีส่วนรับผิดชอบ (Responsibility) ทุกฝ่ายที่เกี่ยวข้องกับการเชื่อมต่อเข้าระบบเครือข่ายมีหน้าที่ในการรักษาความมั่นคงให้แก่ระบบสารสนเทศและเครือข่ายด้วยการพิจารณาทบทวนนโยบายหรือมาตรการในการรักษาความมั่นคงเพื่อความปลอดภัยของระบบคอมพิวเตอร์หรือระบบเครือข่ายที่มีอยู่เสมอและประเมินว่านโยบายหรือมาตรการเช่นว่านั้นมีความเหมาะสมกับสภาวการณ์ที่เป็นอยู่ในขณะนั้นหรือไม่ นอกจากนี้ ผู้พัฒนา ผู้ออกแบบตลอดจนผู้ขายสินค้าและบริการต่างๆที่เกี่ยวข้อง ควรมีส่วนร่วมในการรักษาความมั่นคงเช่นเดียวกัน โดยการให้ข้อมูลเกี่ยวกับการรักษาความมั่นคงในการใช้สินค้าหรือบริการดังกล่าวอยู่เสมอ

3. การตอบสนองต่อปัญหาอย่างทันท่วงที (Response) จากการที่มีการเชื่อมต่อระบบเครือข่ายโยงใยถึงกันทั่วโลกนี้เอง ทำให้เครือข่ายส่วนใดส่วนหนึ่งถูกโจมตีหรือประสบปัญหาไม่ว่าด้วยสาเหตุใด ก็ย่อมส่งผลกระทบและสร้างความเสียหายได้อย่างกว้างขวาง ดังนั้น ทุกฝ่ายที่เกี่ยวข้องกับการเชื่อมต่อเข้ากับระบบเครือข่ายจึงควรร่วมมือกันแก้ไขปัญหาที่เกิดขึ้นอย่างทันท่วงที ตลอดจนแบ่งปันข้อมูลให้กันเกี่ยวกับจุดอ่อนและวิธีการโจมตีระบบในเวลาที่เหมาะสม อีกทั้งวิธีปฏิบัติเพื่อการป้องกันที่ได้ผลอย่างรวดเร็ว

4. การมีจริยธรรม (Ethics) เนื่องจากในระบบสารสนเทศและเครือข่ายนั้น การกระทำหรือไม่กระทำอย่างใดอย่างหนึ่งของบุคคลหนึ่ง อาจก่อให้เกิดความเสียหายหรือมีผลกระทบต่อบุคคลอื่นอีกเป็นจำนวนมาก ดังนั้น จึงควรร่วมกันพัฒนาและหาแนวปฏิบัติที่ดีที่สุด ตลอดจนการประชาสัมพันธ์ให้ทุกส่วนในสังคมเคารพสิทธิของบุคคลอื่นด้วย

5. การเคารพหลักประชาธิปไตย (Democracy) การดำเนินการเพื่อรักษาความมั่นคงจะต้องดำเนินการให้มีความเหมาะสมและสอดคล้องหลักประชาธิปไตยหรือหลักเสรีภาพของประชาชนด้วย เช่น จะต้องคำนึงถึงสิทธิเสรีภาพในการติดต่อสื่อสาร สิทธิในความเป็นส่วนตัว และดำเนินการด้วยความโปร่งใส

6. การประเมินความเสี่ยง (Risk Assessment) ควรมีการประเมินความเสี่ยงเพื่อให้สามารถระบุถึงภัยและข้อบกพร่องต่างๆที่อาจเกิดขึ้นต่อระบบการรักษาความปลอดภัย ไม่ว่าจะเกิดขึ้นจากปัจจัยภายในหรือภายนอกองค์กร เช่น ปัจจัยทางกายภาพ เทคโนโลยี บุคลากร นโยบาย และการให้บริการด้านการรักษาความปลอดภัยจากบุคคลภายนอก ซึ่งมีผลจากการ

ประเมินความเสี่ยงดังกล่าวจะทำให้สามารถตัดสินใจได้ว่าระดับความเสี่ยงต่อระบบสารสนเทศและเครือข่ายนั้นอยู่ในระดับที่เหมาะสมเมื่อเปรียบเทียบกับลักษณะและความสำคัญของข้อมูลที่จะต้องปกป้องหรือไม่

7. การออกแบบด้านความปลอดภัยและการนำไปปฏิบัติ (Security Design and Implementation) องค์กรหรือหน่วยงานต่างๆควรจัดให้มีนโยบายด้านความปลอดภัยของระบบและเครือข่ายที่ชัดเจนและมีแนวทางเพื่อการนำไปปฏิบัติได้อย่างเหมาะสม เพื่อหลีกเลี่ยงหรือลดความรุนแรงที่อาจเกิดขึ้นจากจุดอ่อนของระบบโดยคำนึงถึงมูลค่าและความสำคัญของข้อมูลที่อยู่ในระบบขององค์กรนั้นๆ

8. การบริหารความปลอดภัย (Security Management) ควรตั้งอยู่บนพื้นฐานด้านการประเมินความเสี่ยงและมีการพัฒนาอยู่ตลอดเวลา ทั้งในเชิงป้องกันผลที่จะเกิดขึ้นและมาตรการที่จะใช้ในกรณีที่มีข้อบกพร่องเกิดขึ้นได้อย่างทันท่วงที

9. หลักการประเมินผลซ้ำ (Reassessment) ควรมีการทบทวนและประเมินการรักษาความปลอดภัยของระบบสารสนเทศและเครือข่ายอยู่เสมอ เพื่อให้สามารถปรับเปลี่ยนนโยบายหรือวิธีปฏิบัติเพื่อให้สอดรับกับการเปลี่ยนแปลงรูปแบบของการโจมตีและจุดอ่อนต่างๆ อยู่ตลอดเวลา

นอกจากนี้ ในปี ค.ศ. 2003 OECD ได้ออกแผนปฏิบัติการ (Implementation Plan) ให้สอดคล้องกับแนวปฏิบัติเพื่อการรักษาความมั่นคงดังกล่าวข้างต้น โดยเน้นขั้นตอนการดำเนินงานของหน่วยงานภาครัฐ เนื่องจากเห็นว่าภาครัฐควรเป็นผู้นำหลักในการพัฒนาวัฒนธรรมของความมั่นคงทั้งในฐานะที่เป็นผู้ให้บริการและเป็นผู้ใช้บริการโดยการกำหนดนโยบายที่จำเป็นต่างๆ เช่น การบัญญัติกฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ให้สอดคล้องกับอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 (Convention on Cyber Crime 2001) การจัดให้มีหน่วยงานและศูนย์รับแจ้งเหตุระดับชาติด้านอาชญากรรมทางคอมพิวเตอร์ การก่อตั้งสถาบันเพื่อแลกเปลี่ยนข้อมูลด้านการโจมตีและการประเมินจุดอ่อนต่างๆ ซึ่งอาจจัดให้อยู่ในรูปของหน่วยประสานงานการรักษาความปลอดภัยคอมพิวเตอร์แห่งชาติ (Nations CERTs : Computer Emergency Response Teams) การสร้างความตื่นตัวแก่ประชาชนด้านความมั่นคง ซึ่งรวมถึงการให้ความรู้ การพัฒนาแนวปฏิบัติที่ดีด้านความมั่นคง การจัดทำศูนย์ประสานงานและเว็บไซต์ให้ข้อมูลด้านความปลอดภัยที่ทันสมัยอยู่เสมอ

แม้ว่าแผนปฏิบัติการของ OECD ดังที่ได้กล่าวมาจะไม่มีสภาพบังคับในทางกฎหมายก็ตาม แต่ก็ถือได้ว่าแผนปฏิบัติการดังกล่าวเป็นส่วนหนึ่งในการส่งเสริมให้สังคมได้ตระหนักและให้ความสำคัญเกี่ยวกับการสร้างวัฒนธรรมของความมั่นคง (Culture of Security) อีกทั้งยังเป็นพื้นฐานสำคัญในการพัฒนาแนวปฏิบัติระดับสากลภายใต้กรอบการดำเนินงานของสหประชาชาติ นั่นคือ การจัดทำข้อมติที่ 239 ในการประชุมสามัญสมาชิกครั้งที่ 57 ซึ่งใช้ชื่อว่า Creation of a Global Culture Cyber Security

3. กลุ่มประเทศอุตสาหกรรมชั้นนำ[7] 8 ประเทศ[8] (Group of 8)

Group of 8 หรือที่รู้จักกันในนาม G8 ได้เริ่มให้ความสำคัญกับปัญหาอาชญากรรมทางคอมพิวเตอร์มาตั้งแต่ปี ค.ศ. 1995 โดยการจัดตั้งคณะทำงานผู้เชี่ยวชาญระดับสูงด้านองค์กรอาชญากรรม (Senior Expert Group on Organized Crime) ต่อมาคณะชุดทำงานดังกล่าวได้จัดทำข้อเสนอแนะในการสร้างความร่วมมือระหว่างประเทศต่อปัญหาอาชญากรรมที่ใช้เทคโนโลยีสมัยใหม่

ในปี ค.ศ. 1996 ได้จัดทำแถลงการณ์เกี่ยวกับความเสี่ยงอันเนื่องจากการที่ผู้ก่อการร้ายสามารถใช้เทคโนโลยีสารสนเทศเป็นเครื่องมือในการติดต่อสื่อสาร จึงได้มีความเห็นร่วมกันที่จะส่งเสริมให้มีข้อตกลงระหว่างประเทศเกี่ยวกับการเข้าถึงข้อมูลที่ได้ทีการเข้ารหัสลับ (Encryption) ในกรณีจำเป็นเพื่อประโยชน์ในการป้องกันและสืบสวนเกี่ยวกับการก่อการร้าย โดยคำนึงถึงความเป็นส่วนตัวของประชาชน อีกทั้งส่งเสริมให้มีการแลกเปลี่ยนข้อมูลด้านการใช้เทคโนโลยีสารสนเทศในการสื่อสารของกลุ่มผู้ก่อการร้าย

หลังจากนั้นก็ได้มีการจัดตั้งคณะอนุกรรมการที่ใช้เทคโนโลยีขั้นสูง (G8 Subgroup on High-tech Crime) ขึ้นในปี ค.ศ. 1997 ซึ่งต่อมาคณะกรรมการชุดดังกล่าวได้จัดทำหลักการ (Principle) ด้านอาชญากรรมทางคอมพิวเตอร์ที่ประเทศต่างๆควรนำไปปฏิบัติ เช่น การมีระบบกฎหมายที่ทำให้สามารถเก็บรักษาข้อมูลและเข้าถึงข้อมูลเพื่อทำการสอบสวนได้ ควรมีความร่วมมือระหว่างประเทศเพื่อการแลกเปลี่ยนข้อมูลข่าวสารและสามารถรวบรวมพยานหลักฐานได้

---

[7] เรื่องเดียวกัน, หน้า 60-62.

[8] สหรัฐอเมริกา อังกฤษ ฝรั่งเศส เยอรมัน อิตาลี ญี่ปุ่น แคนาดา และรัสเซีย อ้างถึงใน Privacy International Organization Cyber-Crime, [Online], Available from: http://www.privacyinternational.org/issues/cybercrime/index2.html[2009, May 23]

อย่างทันท่วงที ควรพัฒนาให้มีมาตรฐานในการสืบค้นพยานหลักฐานที่อยู่ในรูปข้อมูลอิเล็กทรอนิกส์

เพื่อให้ประเทศต่างๆสามารถดำเนินการให้บรรลุผลสำเร็จตามหลักการ 10 ข้อดังกล่าว คณะอนุกรรมการจึงได้จัดทำแผนปฏิบัติการ (Action Plan) เช่น การพัฒนาบุคลากรให้มีความรู้ความสามารถและมีเครื่องมือที่เพียงพอในการรับมือกับคดีอาชญากรรมทางคอมพิวเตอร์รวมทั้งสามารถให้ความช่วยเหลือกับหน่วยงานต่างประเทศได้ การร่วมมือกับภาคอุตสาหกรรมซอฟต์แวร์ในการพัฒนาเทคโนโลยีที่ใช้สำหรับรวบรวมและเก็บรักษาหลักฐานอิเล็กทรอนิกส์ และการจัดให้มีเครือข่ายความร่วมมือด้านอาชญากรรมทางคอมพิวเตอร์ที่มีเจ้าหน้าที่ตลอด 24 ชั่วโมง (24/7 Network) เพื่อทำหน้าที่ให้การช่วยเหลือในการสอบสวนคดีอาชญากรรมทางคอมพิวเตอร์ระหว่างประเทศ เป็นต้น[9]

ต่อมาได้มีการจัดตั้งเครือข่ายความร่วมมือด้านอาชญากรรมทางคอมพิวเตอร์ (High Tech Crime 24 Hour Points of Contact Network) ขึ้นภายในกลุ่มประเทศสมาชิก G8 ก่อน และได้ทำการเพิ่มจำนวนเป็นกว่า 30 ประเทศในปัจจุบัน ทั้งนี้ ประเทศที่จะเข้าร่วมเป็นสมาชิกในเครือข่ายดังกล่าวจะต้องมีคุณสมบัติ 2 ประการ คือ มีหน่วยงานที่มีเจ้าหน้าที่ซึ่งมีความรู้ความเชี่ยวชาญด้านการสอบสวนเกี่ยวกับคอมพิวเตอร์และพยานหลักฐานทางอิเล็กทรอนิกส์ และสามารถปฏิบัติหน้าที่ตลอดเวลา

ในส่วนของประเทศไทยเองก็ประสบปัญหาเกี่ยวกับการก่ออาชญากรรมรูปแบบใหม่นี้ ซึ่งสถานการณ์ความรุนแรงของการกระทำความผิดเกี่ยวกับคอมพิวเตอร์มีแนวโน้มเพิ่มสูงขึ้นมาก เนื่องจากจำนวนผู้ใช้คอมพิวเตอร์และเครือข่ายเพิ่มสูงขึ้นเรื่อยๆ บ่อยครั้งที่เนื้อหาที่เผยแพร่อยู่บนอินเทอร์เน็ตไม่เหมาะสมต่อการบริโภคของประชาชน โดยเฉพาะอย่างยิ่งแก่เด็กๆ และบ่อยครั้งที่คอมพิวเตอร์ อินเทอร์เน็ตและอุปกรณ์ไฮเทคต่างๆถูกนำมาใช้เป็นเครื่องมือในการก่ออาชญากรรมในรูปแบบใหม่ๆมากมาย

ถึงแม้ในปัจจุบันประเทศไทยจะได้มีการประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แต่ก็ยังพบว่าการดำเนินการส่วนใหญ่เกี่ยวกับปัญหาเหล่านี้ หากเป็นกรณีของผู้กระทำความผิดหรือเว็บไซต์นั้นมีที่ตั้งอยู่นอกประเทศก็จะประสานให้ผู้ให้บริการอินเทอร์เน็ต (ISP) ทำการปิดกั้น แต่เว็บไซต์ประเภทนี้ก็เกิดขึ้นใหม่อย่างต่อเนื่องจึง

---

[9] Ibid., p 1.

ยากที่จะทำการปิดกั้นได้อย่างทั่วถึง ในทางปฏิบัติจึงไม่สามารถเอาผิดกับผู้ก่ออาชญากรรมคอมพิวเตอร์ผ่านเครือข่ายข้ามประเทศได้ ซึ่งความร่วมมือระหว่างประเทศที่รวดเร็วเท่าทันกับสภาพของความเร่งด่วนในการสืบสวนสอบสวนอาชญากรรมเกี่ยวกับคอมพิวเตอร์ และการประสานงานกันทั้งทางเทคนิคและกฎหมาย จึงเป็นเรื่องจำเป็นในการป้องกันและปราบปราม รวมถึงการแก้ไขปัญหาอาชญากรรมดังกล่าว เนื่องจากต้องมีวิธีการจัดการที่รวดเร็วและเชื่อถือได้ การมองหาความร่วมมือระหว่างประเทศที่เอื้อต่อการต่อต้านอาชญากรรม จึงเป็นภารกิจหน้าที่ของประเทศที่จะรับมือกับภัยคุกคามชนิดใหม่ที่เกิดขึ้น และมั่นใจได้ว่าจะสามารถหยุดยั้งกิจกรรมเหล่านี้ไม่ให้คุกคามประชาชนของประเทศไทย ซึ่งสิ่งเหล่านี้สามารถแก้ไขได้ด้วยความร่วมมืออย่างใกล้ชิดในทุกมิติระหว่างรัฐบาลและทุกหน่วยงานทั้งในระดับประเทศและระดับระหว่างประเทศ โดยเฉพาะอย่างยิ่งด้วยการแลกเปลี่ยนข้อมูลข่าวสารและประสบการณ์ระหว่างกัน ถือเป็นสิ่งที่มีความสำคัญยิ่งที่ต้องตระหนักถึง

ดังนั้น จึงเป็นที่มาที่ผู้เขียนเห็นว่าควรทำการศึกษาอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 (Convention on Cyber Crime 2001) ซึ่งถือได้ว่าเป็นอนุสัญญาที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ฉบับแรก เพื่อให้ทราบถึงสาระสำคัญเกี่ยวกับมาตรการต่างๆที่ประเทศภาคีต้องปฏิบัติตามพันธกรณีของอนุสัญญา ทั้งนี้ อนุสัญญายังได้มีการบัญญัติถึงมาตรการโดยเฉพาะเจาะจงระหว่างประเทศภาคี ไม่ว่าจะเป็นการให้คำนิยามและคำจำกัดความเกี่ยวกับการกระทำความผิด การกำหนดฐานความผิดเกี่ยวกับคอมพิวเตอร์ที่มุ่งเน้นให้ประเทศภาคีต้องพิจารณาให้เป็นไปในทิศทางเดียวกัน วิธีการสืบสวนสอบสวนเฉพาะทางที่ต้องมีการเพิ่มเติมจากวิธีการสืบสวนสอบสวนความผิดทางกายภาพ เพื่อประโยชน์ในการสืบสวนสอบสวนและรวบรวมพยานหลักฐานที่อยู่ในรูปข้อมูลอิเล็กทรอนิกส์ เพื่อดำเนินคดีกับผู้กระทำความผิดในการป้องกันและปราบปรามอาชญากรรมรูปแบบใหม่นี้ รวมถึงความร่วมมือระหว่างประเทศที่จะช่วยส่งเสริมให้ประเทศภาคีสามารถป้องกันและปราบปรามผู้กระทำความผิดได้ พร้อมทั้งสามารถลดข้อขัดข้องต่างๆเกี่ยวกับความร่วมมือระหว่างประเทศในการดำเนินคดีกับผู้กระทำความผิด ไม่ว่าจะเป็นการส่งตัวผู้ร้ายข้ามแดน การให้ความช่วยเหลือซึ่งกันและกัน ซึ่งอนุสัญญานี้ได้เปิดกว้างให้ทุกประเทศสามารถเป็นสมาชิกได้ ทั้งนี้ จะต้องมีการไตร่ตรองอย่างรอบคอบถึงผลกระทบทางกฎหมายที่อนุสัญญานี้มีต่อประเทศไทย เพื่อรองรับการมีผลบังคับใช้อนุสัญญานี้หากประเทศไทยจะพิจารณาเพื่อเป็นภาคี โดยต้องทำการวิเคราะห์ถึงอนุสัญญาเพื่อเป็นข้อมูลว่าในอนาคตประเทศไทยควรพิจารณาเข้าร่วมเป็นภาคีของอนุสัญญานี้หรือไม่ เพื่อให้ได้ประโยชน์สูงสุดจากอนุสัญญา

1.2 วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาถึงแนวคิด ขอบเขตและวัตถุประสงค์ รวมถึงหลักกฎหมายและสาระสำคัญของอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 (Convention on Cyber Crime 2001) รวมถึงข้อดีและข้อเสียของอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์

2. เพื่อศึกษาถึงปัญหาและอุปสรรคในการปฏิบัติตามพันธกรณีของอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 (Convention on Cyber Crime 2001) ของประเทศที่เป็นภาคีบางประเทศ

3. เพื่อศึกษาถึงแนวทางและวิธีการในการแก้ไขปัญหาอาชญากรรมเกี่ยวกับคอมพิวเตอร์ที่เกิดขึ้นตามแนวทางของอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 (Convention on Cyber Crime 2001)

4. เพื่อศึกษาถึงความร่วมมือในกระบวนการยุติธรรมระหว่างประเทศเพื่อแก้ไขปัญหาอาชญากรรมเกี่ยวกับคอมพิวเตอร์ตามแนวทางของอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 (Convention on Cyber Crime 2001)

5. เพื่อศึกษาว่าหากประเทศไทยเข้าเป็นภาคีอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 (Convention on Cyber Crime 2001) จะมีผลกระทบทางด้านกฎหมายต่อประเทศไทยหรือไม่ และประเทศไทยจะได้รับประโยชน์ในการดำเนินการส่งตัวผู้ร้ายข้ามแดนหรือไม่

1.3 สมมุติฐานของการวิจัย

หากประเทศไทยเข้าเป็นภาคีอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 ซึ่งเป็นอนุสัญญาที่มีความสำคัญเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ในระดับสากล จะเป็นโอกาสที่ทำให้ประเทศไทยได้รับความร่วมมือกับสังคมระหว่างประเทศ ในการป้องกันและปราบปรามรวมถึงต่อต้านการก่อให้เกิดอาชญากรรมเกี่ยวกับคอมพิวเตอร์ได้อย่างมีประสิทธิภาพมากขึ้น

1.4 ขอบเขตของการวิจัย

ศึกษาอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 รวมถึงวิจัยปัญหาและอุปสรรคในการปฏิบัติตามพันธกรณีของประเทศภาคี พร้อมทั้งเสนอมาตรการทางกฎหมายและแนวทางแก้ไขปัญหาดังกล่าวหากประเทศไทยเข้าร่วมเป็นภาคีของอนุสัญญานี้

1.5 วิธีที่จะดำเนินการวิจัยโดยย่อ

การศึกษาวิจัยเกี่ยวกับอาชญากรรมคอมพิวเตอร์นี้ได้กำหนดวิธีวิจัยโดยการวิจัยจากเอกสาร (Document Research) ซึ่งจะศึกษาจากตัวบทกฎหมายโดยเน้นอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 เป็นหลัก ทั้งนี้รวมถึงการ ศึกษาจากข้อมูลทางเอกสารต่างๆ ไม่ว่าจะเป็นผลงาน รายงานวิจัย บทความ หรือคำพิพากษาของศาล แล้วนำข้อมูลดังกล่าวมาวิเคราะห์อย่างเป็นระบบ

1.6 ประโยชน์ที่จะได้รับจากการวิจัย

1. ทำให้ทราบถึงแนวคิด หลักกฎหมายและสาระสำคัญของอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 (Convention on Cyber Crime 2001)

2. ทำให้ทราบถึงความร่วมมือระหว่างประเทศที่นำมาใช้ในการป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ว่ามีข้อดีหรือข้อเสียอย่างไร

3. ทำให้ทราบถึงมาตรการในการแก้ไขปัญหาและอุปสรรคในการปฏิบัติตามพันธกรณีทั้งประเด็นของกฎหมายสารบัญญัติ กฎหมายสบัญญัติ

4. ทำให้ทราบถึงผลกระทบทางด้านกฎหมายและความพร้อมของประเทศไทยในการเข้าร่วมเป็นภาคีของอนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 (Convention on Cyber Crime 2001)