

มาตรการทางกฎหมายของอาเซียนเพื่อการคุ้มครองและป้องกันอาชญากรรมทางคอมพิวเตอร์

ASEAN LEGAL MEASURES FOR THE PROTECTION OF COMPUTER CRIME

วรณัฐ บุญเจริญ

นิติศาสตรมหาบัณฑิต

สำนักวิชานิติศาสตร์
มหาวิทยาลัยแม่ฟ้าหลวง

2557

©ลิขสิทธิ์ของมหาวิทยาลัยแม่ฟ้าหลวง

มาตรการทางกฎหมายของอาเซียนเพื่อการคุ้มครอง และป้องกันอาชญากรรมทางคอมพิวเตอร์

ASEAN LEGAL MEASURES FOR THE PROTECTION OF COMPUTER CRIME

วรณัฐ บุญเจริญ

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษา
ตามหลักสูตรปริญญานิติศาสตรมหาบัณฑิต

สำนักวิชานิติศาสตร์
มหาวิทยาลัยแม่ฟ้าหลวง
2557

©ลิขสิทธิ์ของมหาวิทยาลัยแม่ฟ้าหลวง

มาตรการทางกฎหมายของอาเซียนเพื่อการคุ้มครอง และป้องกันอาชญากรรมทางคอมพิวเตอร์

ASEAN LEGAL MEASURES FOR THE PROTECTION OF COMPUTER CRIME

วรณัฐ บุญเจริญ

วิทยานิพนธ์นี้ได้รับการพิจารณาอนุมัติให้นับเป็นส่วนหนึ่งของการศึกษา
ตามหลักสูตรปริญญานิติศาสตรมหาบัณฑิต
2557

คณะกรรมการสอบวิทยานิพนธ์

.....ประธานกรรมการ
(รองศาสตราจารย์ ดร. อภิรัตน์ เพ็ชรศิริ)

.....อาจารย์ที่ปรึกษา
(ดร. ชูเกียรติ น้อยฉิม)

.....กรรมการ
(ดร. ณัฐกร วิทิตานนท์)

.....กรรมการภายนอกมหาวิทยาลัย
(ศาสตราจารย์ วีรพงษ์ บุญโญภาส)

©ลิขสิทธิ์ของมหาวิทยาลัยแม่ฟ้าหลวง

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงไปด้วยดีด้วยความช่วยเหลือจาก ดร. ชูเกียรติ น้อยฉิม อาจารย์ที่ปรึกษาวิทยานิพนธ์ ท่านได้ให้คำแนะนำและข้อคิดเห็นอันเป็นประโยชน์อย่างยิ่งในการเขียนวิทยานิพนธ์ฉบับนี้ และยังได้ช่วยแก้ปัญหาและอุปสรรคต่าง ๆ ระหว่างดำเนินการทั้งในด้านวิชาการและด้านอื่น ๆ ขอขอบคุณ รองศาสตราจารย์ ดร. อภิรัตน์ เพ็ชรศิริ ประธานกรรมการ ดร. ณัฐกร วิทิตานนท์ กรรมการ และ ศาสตราจารย์ วีรพงษ์ บุญโญภาส กรรมการภายนอกมหาวิทยาลัยที่ได้ให้คำแนะนำในการแก้ไขเพิ่มเติมให้วิทยานิพนธ์ฉบับนี้มีความสมบูรณ์ อาจารย์สุวิจักขณ์ จันดาพันธ์ ที่ช่วยเหลือด้านปัจจัยต่าง ๆ ในขณะเร่งทำรูปเล่มวิทยานิพนธ์ ว่าที่ร้อยตรี สมพร รุจิกิตติอังศุธร ที่ช่วยแก้ไขปรับปรุงรูปเล่ม รวมไปถึงเพื่อนสนิทมิตรสหายให้กำลังใจจนวิทยานิพนธ์ฉบับนี้สำเร็จออกมาเป็นรูปเล่มได้

สุดท้ายนี้ ขอขอบคุณบิดามารดาและครอบครัวที่ให้ความช่วยเหลือ ทั้งในด้านกำลังกายและกำลังทรัพย์ในการศึกษาเล่าเรียน ตลอดจนให้กำลังใจผู้วิจัยเสมอมาจนสำเร็จการศึกษา

วรณัฐ บุญเจริญ

ชื่อเรื่องวิทยานิพนธ์ มาตรการทางกฎหมายของอาเซียนเพื่อการคุ้มครองและป้องกันอาชญากรรมทางคอมพิวเตอร์

ชื่อผู้เขียน วรณัฐ บุญเจริญ

หลักสูตร นิติศาสตรมหาบัณฑิต

อาจารย์ที่ปรึกษา ดร. ชูเกียรติ น้อยฉิม

บทคัดย่อ

วิทยานิพนธ์ฉบับนี้ได้ศึกษาหลักเกณฑ์ว่าด้วยเรื่องอาชญากรรมทางคอมพิวเตอร์ทั้งในระดับระหว่างประเทศและระดับภูมิภาค รวมถึงมาตรการทางกฎหมายขององค์การความร่วมมือระหว่างประเทศของสมาคมประชาชาติเอเชียตะวันออกเฉียงใต้ หรืออาเซียน (Association of Southeast Asian Nation: ASEAN) และประเทศสมาชิกอาเซียน ในการรับมืออาชญากรรมทางคอมพิวเตอร์ข้ามชาติ และจากการศึกษาวิจัยพบว่าปัญหาและอุปสรรคที่เกิดขึ้นนั้น เกิดจากความแตกต่างทางโครงสร้างพื้นฐานในด้านข้อมูลข่าวสาร และการขาดแคลนบทบัญญัติทางกฎหมายในประเทศสมาชิกอาเซียนบางประเทศ ซึ่งจะต้องแก้ไขอย่างเร่งด่วน รวมไปถึงพิจารณาความเป็นไปได้ในการสร้างมาตรฐานกลางในด้านการคุ้มครองและป้องกันอาชญากรรมทางคอมพิวเตอร์ โดยอาศัยข้อเสนอแนะต่าง ๆ เพื่อการพัฒนาและนำไปปฏิบัติจริง และเป็นแนวทางในการสร้างหลักเกณฑ์กลางซึ่งมีข้อกำหนดที่ยืดหยุ่น สอดคล้อง และทันสมัย ในเรื่องอาชญากรรมทางคอมพิวเตอร์ของภูมิภาคอาเซียน

คำสำคัญ: กฎหมายว่าด้วยอาชญากรรมทางคอมพิวเตอร์/กฎหมายว่าด้วยอาชญากรรมไซเบอร์/การสร้างความสอดคล้องทางกฎหมายของอาเซียน

Thesis Title	ASEAN Legal Measures for the Protection of Computer Crime
Author	Vorranat Booncharoen
Degree	Master of Law
Advisor	Dr. Chukeat Noichim

ABSTRACT

This thesis outlines the International regulations of computer crime law and the attempts of Association of Southeast Asian Nation (ASEAN) including its member's state in fighting Transnational Computer Crime threats. The study indicates the challenge to be originated from the difference in ICT infrastructures including inconsistence of cybercrime law or lack thereof among ASEAN member's state. These significant issues called for immediate response in the form of harmonization of ASEAN member's state cybercrime legal standard through recommendations and pragmatic approach in order to push ASEAN towards resilient and harmonized regional computer crime regulation.

Keywords: Computer Crime Law/Cybercrime Law/ASEAN Legal Harmonization

สารบัญ

	หน้า
กิตติกรรมประกาศ	**(3)**
บทคัดย่อภาษาไทย	**(4)**
บทคัดย่อภาษาอังกฤษ	**(5)**
สารบัญตาราง	**(8)**
สารบัญภาพ	**(9)**
บทที่	
1 บทนำ	**1**
1.1 ความเป็นมาและความสำคัญของปัญหา	1
1.2 วัตถุประสงค์ของการวิจัย	4
1.3 สมมติฐานของการวิจัย	4
1.4 ขอบเขตของการวิจัย	5
1.5 วิธีดำเนินการวิจัย	5
1.6 ประโยชน์ที่คาดว่าจะได้รับจากการวิจัย	5
2 แนวคิด และทฤษฎีที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์	**6**
2.1 นิยามของอาชญากรรมทางคอมพิวเตอร์	10
2.2 แนวคิดเกี่ยวกับกฎหมายบนอินเตอร์เน็ต	22
3 หลักเกณฑ์ระหว่างประเทศที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์	**45**
3.1 องค์กรระหว่างประเทศที่ดูแลเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์	47
3.2 หลักเกณฑ์ระหว่างประเทศที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์	57
4 หลักการและกฎเกณฑ์ทางกฎหมายในเรื่องอาชญากรรมคอมพิวเตอร์ของอาเซียน	**65**
4.1 วิวัฒนาการเกี่ยวกับความร่วมมือในเรื่องอาชญากรรมทางคอมพิวเตอร์ของอาเซียน	66

สารบัญ (ต่อ)

หน้า

บทที่

4.2 กลไกในการรับมืออาชญากรรมทางคอมพิวเตอร์ของอาเซียน 71

4.3 แผนการเพื่อรับมืออาชญากรรมทางคอมพิวเตอร์ของอาเซียน 76

4.4 กฎหมายที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ของประเทศสมาชิกอาเซียน 82

5 วิเคราะห์สภาพปัญหาในปัจจุบัน และมาตรการทางกฎหมาย ในการควบคุมอาชญากรรมทางคอมพิวเตอร์ในอาเซียน 109

5.1 การสร้างคู่มือ (Guidelines) เพื่อนำมาใช้ในระดับภูมิภาค 111

5.2 สภาพปัญหาอาชญากรรมทางคอมพิวเตอร์ของอาเซียน 118

6 บทสรุป และข้อเสนอแนะ 142

6.1 บทสรุป 142

6.2 ข้อเสนอแนะ 143

6.3 ข้อเสนอแนะเพื่อการศึกษาเพิ่มเติมในอนาคต 150

รายการอ้างอิง 152

ภาคผนวก 165

ภาคผนวก ก อนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ 166

ภาคผนวก ข ASEAN ICT MASTER PLAN 2015 172

ภาคผนวก ค ASEAN POLITICAL SECURITY BLUEPRINT 173

ภาคผนวก ง MASTER PLAN ON ASEAN CONECTIVITY 175

ประวัติผู้เขียน 176

สารบัญตาราง

ตาราง **หน้า**

4.1 แผนการเพื่อรับมืออาชญากรรมทางคอมพิวเตอร์ของอาเซียน 81
4.2 กฎหมายที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ของประเทศมาเลเซีย 85
4.3 กฎหมายที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ของประเทศสิงคโปร์ 87
4.4 กฎหมายที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ของประเทศอินโดนีเซีย 90
4.5 กฎหมายที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ของประเทศฟิลิปปินส์ 93
4.6 กฎหมายที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ของประเทศบรูไน 95
4.7 กฎหมายที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ของประเทศกัมพูชา 96
4.8 กฎหมายที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ของประเทศลาว 98
4.9 กฎหมายที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ของประเทศเวียดนาม 100
4.10 กฎหมายที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ของประเทศพม่า 102
4.11 กฎหมายที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ของประเทศไทย 105
4.12 สรุปสภาพกฎหมายอาชญากรรมทางคอมพิวเตอร์ของประเทศสมาชิกอาเซียน 106
5.1 รวมของเหตุการณ์สำคัญที่เกิดขึ้นบนไซเบอร์สเปซในอาเซียน
ตั้งแต่ปี พ.ศ. 2555-2556 ที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ 135
5.2 สรุปปัญหาในการรับมืออาชญากรรมทางคอมพิวเตอร์ในอาเซียน 138

สารบัญภาพ

ตาราง **หน้า**

4.1 กลไกของอาเซียนในเรื่องอาชญากรรมทางคอมพิวเตอร์ 76

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญปัญหา

ความก้าวหน้าของเทคโนโลยีในปัจจุบันทำให้คอมพิวเตอร์และอุปกรณ์ที่เกี่ยวข้องถูกบูรณาการเข้าไปยังกิจกรรมในทุกภาคส่วนของสังคมไม่ว่าจะเป็นการดำเนินชีวิตประจำวันของประชาชน กิจกรรมธุรกิจการค้า หรือแม้แต่งานบริหารประเทศและความมั่นคงของรัฐ ซึ่งวิทยาการคอมพิวเตอร์โดยเฉพาะอย่างยิ่งอินเตอร์เน็ตในปัจจุบันมีศักยภาพสูงสามารถเสริมศักยภาพในการดำเนินกิจการต่าง ๆ ได้เป็นอย่างดี แต่อย่างไรก็ตาม เมื่อพัฒนาการทางคอมพิวเตอร์นั้นเปลี่ยนแปลงอย่างรวดเร็ว การขยายตัวอย่างต่อเนื่องของวิทยาการได้สร้างช่องว่างทางกฎหมายในการก่ออาชญากรรมซึ่งมีลักษณะพิเศษเฉพาะด้านขึ้น ซึ่งผู้กระทำเป็นผู้มีความรู้ความเชี่ยวชาญยากต่อการจับกุมเอาผิด ซึ่งเรียกว่า อาชญากรรมทางคอมพิวเตอร์ (Computer crime) โดยในการควบคุมและปราบปรามอาชญากรรมทางคอมพิวเตอร์นั้น การออกแบบให้กฎหมายรองรับกับเทคโนโลยีและกระบวนการทางคอมพิวเตอร์ รวมถึงการปรับปรุงแก้ไขนิยามขององค์ประกอบต่าง ๆ ที่กฎหมายให้การรับรอง เพื่อการกำกับดูแลที่เหมาะสมจึงเป็นสิ่งจำเป็น ซึ่งหากกระบวนการยุติธรรมเข้าใจเรื่องดังกล่าวล่าช้า ที่ก่อให้เกิดช่องว่างในการประกอบอาชญากรรมทางคอมพิวเตอร์และเป็นสาเหตุหนึ่งให้เกิดความเสียหายต่อทั้งทางเศรษฐกิจและสังคม กฎหมายอาชญากรรมทางคอมพิวเตอร์จึงจำเป็นต้องได้รับความเอาใจใส่อย่างต่อเนื่องจากภาครัฐทั้งในระดับประเทศและในระดับระหว่างประเทศ

นับแต่อาชญากรรมทางคอมพิวเตอร์ได้เกิดขึ้นมาตั้งแต่ช่วงต้นทศวรรษที่ 60 จนถึงปัจจุบันระบบคอมพิวเตอร์และอินเตอร์เน็ตถูกพัฒนาให้มีความก้าวหน้าซับซ้อนยิ่งขึ้น จึงเป็นเหตุหนึ่งให้อาชญากรรมทางคอมพิวเตอร์มีความหลากหลายและซับซ้อนตามไปด้วย และด้วยลักษณะของอินเตอร์เน็ตที่เป็นระบบโครงข่ายการสื่อสารที่เชื่อมโยงเข้าด้วยกันในระดับระหว่างประเทศจึงก่อให้เกิดปัญหาการบังคับใช้มาตรการทางกฎหมาย การจับกุม หรือการดำเนินคดีเป็นอย่างมาก สำหรับการเตรียมความพร้อมในการรับมือกับสงครามข้อมูลข่าวสารหรือที่เรียกว่า “สงครามไซเบอร์

(Cyber warfare)[1]" ซึ่งเป็นอาชญากรรมทางคอมพิวเตอร์ที่เป็นภัยอย่างยิ่งต่อความมั่นคงของโลกในปัจจุบันนับเป็นเรื่องสำคัญเช่นกัน เนื่องด้วยวิทยาการและเทคโนโลยีสมัยใหม่นั้นง่ายต่อการเข้าถึงในทุกระดับของสังคม ทำให้การสู้รบในสงครามข้อมูลข่าวสารมีศักยภาพในการก่อให้เกิดความเสียหายเป็นวงกว้างมากขึ้น จากการโจมตีระบบเครือข่ายส่วนบุคคลขยายขอบเขตเป็นสงครามระดับโลกที่สร้างความเสียหายและเป็นภัยต่อความมั่นคงในระดับนานาชาติ เนื่องจากสงครามไซเบอร์มีศักยภาพสูงในการเข้าแทรกซึมด้านข้อมูลข่าวสารเพื่อก่อกวนก่อความไม่สงบหรือสร้างความแตกแยกในสังคม จนส่งผลผลักดันให้เกิดความเปลี่ยนแปลงในระดับประเทศ รวมไปถึงการจารกรรมข้อมูลลับทางทหาร ซึ่งในระดับระหว่างประเทศได้เกิดความตื่นตัวเพื่อการรับมือสงครามไซเบอร์และจัดตั้งหน่วยงานในการรับมืออาชญากรรมทางคอมพิวเตอร์ประเภทนี้ขึ้นมา เช่น Center of Excellence on Cybercrime ขององค์กรสนธิสัญญาป้องกันแอตแลนติกเหนือ (North Atlantic Treaty Organization: NATO) ณ กรุงทาลินน์ ประเทศเอสโตเนีย

จากการที่การกระทำผิดทางคอมพิวเตอร์ในปัจจุบันกลายเป็นอาชญากรรมข้ามชาติ (Transnational Crime) ด้วยเหตุนี้จึงมีแรงผลักดันให้เกิดความร่วมมือในระดับระหว่างประเทศขึ้นเพื่อจัดการเกี่ยวกับปัญหาอาชญากรรมคอมพิวเตอร์ โดยองค์การสหประชาชาติเป็นหน่วยงานหลักในการวางแนวทางให้แก่ภูมิภาคและประเทศต่าง ๆ โดยจัดทำคู่มือป้องกันและควบคุมอาชญากรรมคอมพิวเตอร์ของสหประชาชาติ[2] และกฎเกณฑ์ว่าด้วยโทรคมนาคมระหว่างประเทศ (International Telecommunication Regulation: ITR) เป็นต้น

สำหรับความร่วมมือระหว่างประเทศระดับภูมิภาคในการป้องกันและจัดการปัญหาอาชญากรรมคอมพิวเตอร์ก็ได้มีการดำเนินการโดยสหภาพยุโรปได้มีการจัดทำคำแนะนำขององค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนาของยุโรป (Recommendation No. R(89)9 Analysis of Legal Policy in 1986) อนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ (Convention on Cybercrime) สำหรับภูมิภาคเอเชียตะวันออกเฉียงใต้ ซึ่งมีความร่วมมือในรูปแบบของสมาคมประชาชาติแห่งเอเชียตะวันออกเฉียงใต้ (Association of Southeast Asia Nations:

---

[1] สงครามไซเบอร์ (Cyber warfare) เป็นคำที่นิยามขึ้นมาโดยผู้เชี่ยวชาญด้านระบบความปลอดภัยของรัฐบาลสหรัฐอเมริกา ริชาร์ด เอ. คลาร์ก ว่า "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).

[2] United Nations, *International review of criminal policy-United Nations manual on the prevention and control of computer-related crime,* Retrieved 2013, November 10, from www.uncjin.org/Documents/irpc4344.pdf

ASEAN)[3] โดยมีจุดมุ่งหมายหลักในการรวมกลุ่มคือความร่วมมือทั้งในด้านเศรษฐกิจ การเมืองและวัฒนธรรม และแม้อาเซียนจะก่อตั้งมากว่า 40 ปี แต่ความร่วมมือภายในอาเซียนยังไม่มีความชัดเจนแน่นอนเป็นรูปธรรมเท่าที่ควรจะเป็นในด้านการป้องกันอาชญากรรมทางคอมพิวเตอร์ ซึ่งอาจก่อให้ความเสียหายอย่างร้ายแรงต่อเสถียรภาพของความมั่นคงในระดับภูมิภาคได้ แม้ว่าในปัจจุบันอาเซียนจะมีแนวทางการรับมือการกระทำผิดทางคอมพิวเตอร์ของอาเซียนได้ถูกกำหนดไว้ในแผนแม่บทไอซีทีอาเซียน 2015 (ASEAN ICT MASTERPLAN 2015)[4] และได้รับการระบุไว้ในแผนงานจัดตั้งประชาคมการเมืองและความมั่นคงอาเซียน (ASEAN Political and Social Community blueprint: APSC blueprint) ก็ตาม

ดังนั้น เพื่อสร้างความตระหนักให้แก่ประเทศสมาชิกอาเซียน ในยุคที่อาชญากรรมทางคอมพิวเตอร์ทำให้โลกก้าวเข้าสู่วิวัฒนาการอีกขั้นหนึ่งของความร่วมมือเพื่อสร้างกฎเกณฑ์ระหว่างประเทศที่ออกแบบกฎหมายมาปกป้องขอบเขตทางยุทธศาสตร์ในพรหมแดนที่ 4[5] หรือไซเบอร์สเปซที่มีการเปลี่ยนแปลงอยู่ตลอดเวลา ซึ่งเป็นความท้าทายที่ต้องเผชิญอย่างหลีกเลี่ยงไม่ได้ ดังนั้น เพื่อรับมือทั้งอาชญากรรมและสงครามยุคใหม่ในโลกดิจิตอลที่มีการขยายตัวอย่างรวดเร็ว ปัญหานี้จึงเป็นหนึ่งในประเด็นความมั่นคงที่ต้องการจัดการอย่างเร่งด่วน สำหรับองค์การอาเซียนนั้นมีความจำเป็นอย่างยิ่งที่จะต้องเร่งปรับตัว และปรับปรุงการดำเนินงานให้ก้าวทันกระแสของการเปลี่ยนแปลงดังกล่าว โดยเฉพาะภัยทางด้านอาชญากรรมและความมั่นคงที่นับวันจะทวีความรุนแรงมากขึ้น เนื่องจากการรวมกลุ่มประชาคมอาเซียนจะเป็นปัจจัยสำคัญที่ช่วยสร้างเสริมความแข็งแกร่งทางทั้งเศรษฐกิจ สังคม และความมั่นคง และเพิ่มศักยภาพในการรับมือกับภัยคุกคามทั้งจากอาชญากรรมและความมั่นคงกับชาติอื่น ๆ นอกอาเซียนทั้งนี้ การส่งเสริมความร่วมมือด้านความมั่นคงระหว่างประเทศสมาชิกที่ลึกซึ้งและกว้างขวางมากขึ้น โดยไม่จำกัดเฉพาะในทางด้านกฎหมาย แต่อาจรวมไปถึงด้านการอำนวยความสะดวกเพื่อลดอุปสรรคในการดำเนินการ ซึ่งจะนำไปสู่การพัฒนา และสวัสดิภาพ ความมั่นคงของประชาชนในประเทศสมาชิก ในปัจจุบันองค์การอาเซียนและประเทศสมาชิกได้เล็งเห็นถึงปัญหาภัยคุกคาม ซึ่งเกิดขึ้นบนอินเตอร์เน็ตที่เป็นหนึ่งในปัจจัยด้านความมั่นคงและความปลอดภัยในการคุ้มครองสวัสดิภาพของประชาชน โดย

---

[3] อาเซียนก่อตั้งขึ้นเมื่อวันที่ 8 สิงหาคม พ.ศ. 2510 โดยเริ่มแรกมีสมาชิกทั้งหมด 5 ประเทศ คือ อินโดนีเซีย มาเลเซีย สิงคโปร์ ไทย และบรูไน ในปัจจุบันมีสมาชิกทั้งหมด 10 ประเทศ โดย พม่า ลาว เวียดนาม และกัมพูชาได้เข้ามาสมทบ

[4] ASEAN ICT MASTERPLAN 2015, มาตรการ 4.2 “ส่งเสริมให้เครือข่ายมีความมั่นคง และปลอดภัย มีการปกป้องข้อมูล รวมทั้งมีความร่วมมือระหว่างหน่วยงานรักษาความปลอดภัยคอมพิวเตอร์ (Computer Emergency Response Team: CERT)”.

[5] จากเดิมพรหมแดนทั้ง 3 ได้แก่ ภาคพื้นดิน ทางอากาศ และทางทะเล.

อาเซียนยังต้องกำหนดยุทธศาสตร์และมาตรการทางกฎหมายเพื่อรับมือกับอาชญากรรมทางคอมพิวเตอร์ ดังนั้น วิทยานิพนธ์ฉบับนี้จึงมุ่งศึกษาวิจัยเพื่อหาแนวทางและมาตรการทางกฎหมายในการป้องกันและควบคุมอาชญากรรมทางคอมพิวเตอร์ของประชาคมอาเซียน รวมทั้งศึกษาหาแนวทางในการพัฒนาและปรับปรุงกฎเกณฑ์ทางกฎหมายที่ใช้ในการป้องกันและควบคุมและป้องกันอาชญากรรมทางคอมพิวเตอร์ให้ได้มาตรฐานเป็นไปในทิศทางเดียวกัน ซึ่งนำไปสู่เป้าหมายการจัดตั้งประชาคมอาเซียนที่มีความมั่นคงและยั่งยืนต่อไป

1.2 วัตถุประสงค์ของการวิจัย

1.2.1 เพื่อศึกษาแนวคิดและทฤษฎีทางกฎหมายที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์

1.2.2 เพื่อศึกษาหลักเกณฑ์ทางกฎหมายที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ในระดับสากลและระดับภูมิภาค

1.2.3 เพื่อศึกษาหลักเกณฑ์ทางกฎหมายขององค์การอาเซียนและกฎหมายภายในของประเทศสมาชิกอาเซียนที่เกี่ยวกับ

1.2.4 เพื่อศึกษาสภาพปัญหาในปัจจุบันที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ของประชาคมอาเซียน

1.2.5 ศึกษาวิเคราะห์เพื่อหาแนวทางหรือมาตรการกลางทางกฎหมายเพื่อนำมาปรับใช้ในการป้องกันปัญหาที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ของอาเซียนให้กลมกลืนกัน

1.3 สมมติฐานของการวิจัย

อาชญากรรมทางคอมพิวเตอร์กลายเป็นปัญหาสำคัญระดับโลกโดยนานาชาติต่างพยายามสร้างหลักเกณฑ์ร่วมกันเพื่อรับมือกับปัญหาดังกล่าวแต่ไม่สามารถแก้ไขปัญหาได้อย่างมีประสิทธิภาพ ปัจจุบันองค์การอาเซียนยังไม่มีกฎหมายแม่แบบที่จะนำมาปรับใช้กับปัญหานี้ ดังนั้นควรทำการศึกษาวิจัยเพื่อหาความเป็นไปได้ในการสร้างแนวทางหรือมาตรการทางกฎหมายที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ที่เป็นมาตรฐานกลางของอาเซียนที่จะใช้คุ้มครองและป้องกันปัญหาอาชญากรรมทางคอมพิวเตอร์ในอาเซียน รวมทั้งเพื่อที่จะนำมาตรการทางกฎหมายที่ได้รับนี้ไปปรับใช้เพื่อให้กฎหมายภายในของประเทศสมาชิกมีความกลมกลืนกัน

1.4 ขอบเขตของการวิจัย

งานวิจัยฉบับนี้ มุ่งศึกษากฎหมายอาชญากรรมทางคอมพิวเตอร์ของประเทศสมาชิกอาเซียนทั้ง 10 ประเทศ เพื่อปรับปรุงให้กลมกลืนเป็นไปในแนวทางเดียวกันทั้งภูมิภาคอาเซียน โดยงานวิจัยฉบับนี้จะทำการศึกษากฎเกณฑ์ระหว่างประเทศโดยมีอนุสัญญาอาชญากรรมทางคอมพิวเตอร์ของสหภาพยุโรป กฎเกณฑ์ขององค์การสหประชาชาติและสหภาพโทรคมนาคมระหว่างประเทศ รวมไปถึงกฎเกณฑ์ของอาเซียน รวมทั้งกฎหมายภายในของประเทศสมาชิกอาเซียนที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์เป็นแม่แบบ

1.5 วิธีดำเนินการวิจัย

การวิจัยนี้ใช้การวิจัยเอกสาร (Documentary research) โดยศึกษาค้นคว้าและรวบรวมข้อมูลจากเอกสารทั้งภาษาไทยและภาษาอังกฤษ ทั้งที่เป็นหนังสือ บทความ วารสาร หัวข้อข่าว ตำรากฎหมายต่าง ๆ ข้อมูลอิเล็กทรอนิกส์ สารนิพนธ์ วิทยานิพนธ์ ตัวบทอนุสัญญาระหว่างประเทศ และกฎเกณฑ์ระหว่างประเทศ รวมถึงข้อมูลทางเว็บไซต์ (Website) ต่าง ๆ ที่เกี่ยวข้องในการศึกษาวิจัยวิทยานิพนธ์ฉบับนี้

1.6 ประโยชน์ที่คาดว่าจะได้รับจากการวิจัย

1.6.1 ทราบถึงหลักเกณฑ์แนวคิดและทฤษฎีในเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์

1.6.2 ทราบถึงหลักเกณฑ์ความร่วมมือเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ในระดับสากลและระดับภูมิภาค

1.6.3 ทราบถึงหลักเกณฑ์ของประชาคมอาเซียน และกฎหมายภายในของประเทศสมาชิกในเรื่องอาชญากรรมทางคอมพิวเตอร์ เปรียบเทียบกับสหภาพยุโรป

1.6.4 ทราบถึงสภาพปัญหาในเรื่องอาชญากรรมทางคอมพิวเตอร์ของประชาคมอาเซียน

1.6.5 ได้แนวทางและมาตรการทางกฎหมายในการแก้ไขปัญหาอาชญากรรมทางคอมพิวเตอร์ของภูมิภาคอาเซียนให้เป็นไปในทิศทางเดียวกัน (Legal harmonization)

บทที่ 2

แนวคิด และทฤษฎีที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์

อาชญากรรมทางคอมพิวเตอร์ ในปัจจุบันยังไม่มีนิยามความหมายที่ชัดเจนและเป็นที่ยอมรับกันโดยทั่วไป หากแต่สามารถกล่าวได้อย่างกว้าง ๆ ว่าเป็นอาชญากรรมที่ถูกกระทำโดยมีคอมพิวเตอร์เป็นเครื่องมือหรือมีข้อมูลทางคอมพิวเตอร์เป็นเป้าหมาย[6] โดย อาชญากรรมทางคอมพิวเตอร์ตามกฎหมายระหว่างประเทศ เช่น อนุสัญญาอาชญากรรมคอมพิวเตอร์ ปี ค.ศ. 2001 (Convention on Cybercrime 2001) จัดให้เป็นการละเมิดซึ่งทำต่อปัจเจกหรือกลุ่มคนด้วยเจตนาร้ายในการทำให้เสื่อมเสียชื่อเสียงหรือก่อให้เกิดความเสียหายทางร่างกายหรือจิตใจ ไม่ว่าโดยทางตรงหรือทางอ้อม โดยการกระทำดังกล่าวอาจเป็นอันตรายต่อความมั่นคงและเศรษฐกิจระดับชาติ โดยใช้คอมพิวเตอร์หรืออุปกรณ์ที่เกี่ยวข้องเป็นเครื่องมือ

อาชญากรรมคอมพิวเตอร์ในระดับระหว่างประเทศมักท้าทายประสิทธิภาพของกฎหมายภายในและกฎหมายระหว่างประเทศรวมไปถึงการบังคับใช้กฎหมายเหล่านั้น เนื่องจากกฎหมายดั้งเดิมในหลายประเทศไม่ได้ถูกวางรูปแบบไว้เพื่อต่อกรกับอาชญากรรมคอมพิวเตอร์ ปัจจุบันอาชญากรประกอบอาชญากรรมมากขึ้นบนอินเตอร์เน็ตโดยอาศัยโทษที่เบาและความยากในการติดตาม ไม่ว่าจะเป็นประเทศพัฒนาแล้วหรือประเทศกำลังพัฒนา รัฐบาลต่างรับรู้ถึงภัยคุกคามใหญ่หลวงจากอาชญากรรมคอมพิวเตอร์ต่อเศรษฐกิจ ความมั่นคงทางการเมือง และประโยชน์สาธารณะ อย่างไรก็ดี ความซับซ้อนทั้งในด้านของชนิดและรูปแบบของอาชญากรรมคอมพิวเตอร์สร้างความยากลำบากในการรับมือ ฉะนั้นการต่อสู้กับอาชญากรรมทางคอมพิวเตอร์จำเป็นต้องได้รับความร่วมมือในระดับนานาชาติควรที่รัฐบาลหลายชาติรวมทั้งองค์กรต่าง ๆ ได้รวมตัวกันเพื่อสร้างมาตรฐานกลางของมาตรการและการออกกฎหมายทั้งในระดับภูมิภาคและระดับโลก โดยความร่วมมือระหว่างจีนและสหรัฐอเมริกาเป็นตัวอย่างสำคัญในฐานะที่ทั้งสองประเทศจัดเป็นแหล่งที่มาของอาชญากรรมคอมพิวเตอร์ที่ใหญ่ที่สุดในโลกในปัจจุบัน

---

[6] Chang, W., Chung, W., Chen, H., & Chou, S., *An international perspective on fighting cybercrime*, ISI'03 Proceedings of the 1st NSF/NIJ Symposium on Intelligence and security informatics (ISI 2003), (Arizona: Springer, 2003), 379-384.

เทคโนโลยีด้านข้อมูลข่าวสาร (Information and Communication technology: ICT) มีบทบาทสำคัญในการช่วยให้เกิดความร่วมมือด้านความปลอดภัยในระดับมาตรฐานโลก สำหรับมาตรการตอบโต้ทั่วไปที่ได้ถูกนำมาใช้ในการจำแนกอาชญากรรมทางคอมพิวเตอร์ เช่นมาตรการในการสร้างความสมบูรณ์แบบให้กับแนวทาง ในการออกกฎหมายและประเด็นทางเทคนิคในการติดตามจับกุมอาชญากรรมคอมพิวเตอร์ผ่านระบบเครือข่าย การควบคุมเนื้อหาบนอินเตอร์เน็ตโดยใช้ พร็อกซี่ (proxy)[7] ส่วนบุคคลหรือสาธารณะ การค้นหาและพิสูจน์หลักฐานดิจิตอล (Computer Forensics)[8] การเข้ารหัสข้อมูล (Encryption)[9] เป็นต้น

อินเตอร์เน็ตจัดเป็นหนึ่งในสาขาที่มีพัฒนาการรวดเร็วที่สุดในสาขาของพัฒนาการทางวิทยาการ[10] ปัจจุบันเทคโนโลยีสารสนเทศนั้น มีอยู่ในอุปกรณ์หรือผลิตภัณฑ์แทบทุกอย่าง แนวโน้มของการสร้างสรรค์สิ่งต่าง ๆ หรือแปลงสิ่งที่มีอยู่ให้เป็นรูปแบบดิจิตอล (Digitalization) เติบโตอย่างรวดเร็ว ความต้องการเทคโนโลยีในการเชื่อมต่ออินเตอร์เน็ตทำให้เกิดการบูรณาการเทคโนโลยีดังกล่าวเข้าไปเป็นส่วนหนึ่งของผลิตภัณฑ์ต่าง ๆ ซึ่งแต่เดิมสามารถใช้งานได้โดยไม่จำเป็นต้องมีการเชื่อมต่ออินเตอร์เน็ต เช่น รถยนต์และอสังหาริมทรัพย์ หรือ สาธารณูปโภคต่าง ๆ (ประปา ไฟฟ้า หรือโครงสร้างพื้นฐานทางโทรคมนาคม) รวมทั้งปฏิบัติการทางทหารและการขนส่ง โดยบริการต่าง ๆ ในปัจจุบันล้วนพึ่งพาการใช้งานเทคโนโลยีสารสนเทศแทบทั้งสิ้น

แม้ว่าการพัฒนาวิทยาการใหม่ ๆ นั้นมุ่งเน้นไปที่การสนองตอบต่อความต้องการของผู้บริโภคในกลุ่มประเทศตะวันตกเป็นหลัก แต่ประเทศกำลังพัฒนาต่างสามารถได้รับประโยชน์จากวิทยาการใหม่ ๆ ได้เช่นกัน ด้วยการมีขึ้นของการสื่อสารไร้สายระยะไกลผ่านเทคโนโลยี เช่น

---

[7] proxy คือตัวกลางในการติดต่อสื่อสาร เช่น เมื่อเปิด website ผ่าน proxy ระบบจะส่งข้อมูลไปยัง proxy ก่อน และ proxy ก็จะส่งต่อไปยัง website ที่ระบบต้องการจะเปิด แทนที่ระบบจะติดต่อกับ website นั้นโดยตรง.

[8] Computer Forensic คือ การเก็บหลักฐาน, การค้นหา, วิเคราะห์ และการนำเสนอหลักฐานทางดิจิตอลที่อยู่ในอุปกรณ์คอมพิวเตอร์และอิเล็กทรอนิกส์ รวมถึงหลักฐานดิจิตอลที่ถูกสร้างจากระบบคอมพิวเตอร์ ซึ่งตรวจสอบข้อมูลอีเล็กทรอนิกส์ และนำข้อมูลที่คัดลอกนั้นมาวิเคราะห์ เช่น การค้นหาไฟล์ที่น่าสงสัย ตรวจสอบการใช้อีเมลและเว็บไซต์ และกู้ไฟล์ที่ถูกลบ รวมถึงการสร้างรายงานให้นำไปวิเคราะห์ต่อได้.

[9] การเข้ารหัสข้อมูล (Encryption) หมายถึง วิธีการเปลี่ยนแปลงข้อมูลเพื่อไม่ให้สามารถถูกอ่านได้จากบุคคลอื่น โดยข้อมูลที่ทำการเข้ารหัสต้องมีการถอดรหัสข้อมูล (Decryption) โดยเปลี่ยนแปลงข้อมูลที่ได้จากการเข้ารหัสข้อมูล เป็นข้อมูลก่อนที่จะถูกทำการเข้ารหัส.

[10] 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/

WiMAX[11] และค่าใช้จ่ายในการซื้อหาอุปกรณ์คอมพิวเตอร์ที่ในปัจจุบันมีราคาถูกลงเป็นอย่างมาก ผู้คนในประเทศกำลังพัฒนาจึงสามารถเข้าถึงบริการและผลิตภัณฑ์ที่มีอยู่บนอินเตอร์เน็ตได้อย่างกว้างขวาง

อิทธิพลของ ICT ที่มี ต่อสังคมได้พัฒนาไปไกลกว่าการเป็นเพียงโครงสร้างพื้นฐานการสื่อสาร การมีอยู่ของ ICT นับเป็นรากฐานของพัฒนาการทางความคิด การสร้างสรรค์ และการใช้งานบริการบนพื้นฐานของระบบเครือข่าย (Network-based Services) เมื่อ E-mail และบริการสังคมออนไลน์ (Social network) ได้เข้ามาแทนที่การส่งจดหมาย การนำเสนอองค์กรผ่านเว็บไซต์กลายเป็นมาตรฐานของโลกธุรกิจมากกว่าการนำเสนอผ่านเอกสาร แผ่นพับ ใบปลิว การสื่อสารผ่านอินเตอร์เน็ตและโทรศัพท์มือถือเติบโตไวกว่าการสื่อสารผ่านสายภาคพื้นดิน (Landline communication) ดังนั้น ICT และบริการบนพื้นฐานของระบบเครือข่ายได้สร้างประโยชน์ให้สังคมในภาพรวม โดยเฉพาะอย่างยิ่งประเทศกำลังพัฒนา การประยุกต์ใช้เทคโนโลยี ICT กับบริการต่าง ๆ เช่น e-government[12], e-commerce, e-educatiom, e-health และ e-environment นับเป็นปัจจัยในการพัฒนาประเทศที่มีความสำคัญอย่างยิ่งยวด เนื่องจากบริการเหล่านี้สามารถเพิ่มวิธีการที่มีประสิทธิภาพในการกระจายบริการขั้นพื้นฐานต่าง ๆ ไปยังพื้นที่ห่างไกล โดยมีค่าใช้จ่ายน้อย การลงทุนในเทคโนโลยี ICT หากได้รับการจัดการอย่างเหมาะสมแล้วสามารถส่งผลให้เกิดการพัฒนาที่มีประสิทธิภาพและประสิทธิผล ช่วยในการลดช่องว่างทางสังคมและเพิ่มคุณภาพชีวิตให้ประชาชนได้เป็นอย่างมาก

สำหรับค่าใช้จ่ายในการเข้าถึงบริการบนอินเตอร์เน็ตในปัจจุบันมักจะมีราคาถูกกว่าบริการประเภทเดียวกันภายนอกระบบเครือข่ายเป็นอย่างมาก เช่น การเข้าถึงบริการ Wikipedia[13] หรือส่งข้อความออนไลน์ที่ปราศจากค่าใช้บริการ ด้วยต้นทุนที่ต่ำมากนี่เองทำให้ผู้ใช้จำนวนมากสามารถ

---

[11] Worldwide Interoperability for Microwave Access หรือ WiMAX ซึ่งเป็นเทคโนโลยีบรอดแบนด์ไร้สายความเร็วสูง ส่งข้อมูลได้ระยะไกลส่งข้อมูลได้ระยะห่าง 30 ไมล์ (ประมาณ 50 กิโลเมตร) ด้วยจุดเด่นนี้ทำให้เป็นประโยชน์ในการเชื่อมต่ออินเตอร์เน็ตของพื้นที่ห่างไกล.

[12] รัฐบาลอิเล็กทรอนิกส์ หรือที่เรียกว่า e-Government คือ วิธีการบริหารจัดการภาครัฐสมัยใหม่ โดยการใช้เทคโนโลยีคอมพิวเตอร์และเครือข่ายสื่อสารเพื่อเพิ่มประสิทธิภาพการดำเนินงานภาครัฐ ปรับปรุงการบริการแก่ประชาชน การบริการด้านข้อมูลและสารสนเทศเพื่อส่งเสริมการพัฒนาเศรษฐกิจและสังคม ประชาชนมีความใกล้ชิดกับภาครัฐมากขึ้น สื่ออิเล็กทรอนิกส์จะเป็นเครื่องมือที่สำคัญในการเข้าถึงบริการของรัฐ ประการสำคัญจะต้องมีความร่วมมืออย่างใกล้ชิดและเต็มใจจากทั้ง 3 ฝ่าย ได้แก่ ภาครัฐ ภาคธุรกิจและประชาชน, สืบค้นเมื่อ 10 พฤศจิกายน 2557, จาก http://www.dld.go.th/ict/article/egov/e-gev02.html.

[13] วิกิพีเดีย (Wikipedia) เป็นสารานุกรมเนื้อหาเสรีหลายภาษาบนเว็บไซต์ ซึ่งได้รับการสนับสนุนจากมูลนิธิวิกิมีเดีย องค์กรไม่แสวงผลกำไร ทุกคนที่สามารถเข้าถึงวิกิพีเดียสามารถร่วมแก้ไขได้แทบทุกบทความได้อย่างเสรี.

เข้าถึงบริการได้ แม้ว่าจะเป็นประชากรของประเทศที่มีรายได้ต่อหัวต่ำ อินเตอร์เน็ตทำให้คนเหล่านี้สามารถใช้บริการที่พวกเขาไม่อาจเข้าถึงได้ภายนอกระบบเครือข่าย

ดังนั้นการนำเทคโนโลยีสารสนเทศเข้ามาบูรณาการในทุกภาคส่วนจึงนำไปสู่พัฒนาการของกรอบความคิดสมัยใหม่ในสังคมข้อมูลข่าวสาร โดยพัฒนาการของสังคมข้อมูลข่าวสารนี้ได้มอบโอกาสแก่ผู้คนทุกระดับในการเข้าถึงข้อมูลโดยปราศจากอุปสรรคซึ่งเป็นตัวสนับสนุนระบอบการปกครองแบบประชาธิปไตยเป็นอย่างดี เมื่อการไหลเวียนของข้อมูลข่าวสารถูกนำออกไปจากความควบคุมชองเจ้าหน้าที่รัฐ ดังตัวอย่างเหตุการณ์ที่เกิดขึ้นในยุโรปตะวันออก นวัตกรรมเหล่านี้ได้มอบโอกาสเพื่อคุณภาพชีวิตที่ดีกว่าให้แก่ประชาชน เช่น การจับจ่ายใช้สอยหรือทำธุรกรรมออนไลน์ การใช้งานระบบการสื่อสารไร้สายและบริการ VoIP (Voice Over Internet Protocol)[14] ซึ่งสิ่งเหล่านี้เป็นเพียงตัวอย่างของ นวัตกรรมมากมายที่แสดงให้เห็นความก้าวหน้าของการบูรณาการเทคโนโลยีสารสนเทศ มาใช้ในชีวิตประจำวัน

อย่างไรก็ดี การเติบโตของสังคมข้อมูลข่าวสารได้มาพร้อมกับภัยอันตรายร้ายแรงรูปแบบใหม่ สาธารณูปโภคที่สำคัญเช่น ประปา หรือไฟฟ้า ในปัจจุบันที่ต้องพึ่งพา ICT เพื่อดำเนินการ ทั้งยานพาหนะ ระบบควบคุมการจราจร หรือระบบโทรคมนาคม ต่างต้องพึ่งการดำเนินการของเทคโนโลยีสารสนเทศ ที่มีเสถียรภาพ ดังนั้นหากมีการจู่โจมโครงสร้างพื้นฐานทางข้อมูลข่าวสารและบริการอินเตอร์เน็ต จึงเป็นการสั่นคลอนความมั่นคงของสังคมและถือว่าอาชญากรรมประเภทนี้มีศักยภาพสูง โดยอาชญากรรมดังกล่าวมีมาในหลายรูปแบบด้วยกัน ทั้งการฉ้อโกงออนไลน์ การเผยแพร่ภาพอนาจารเด็กและการเจาะระบบต่างเป็นเพียงตัวอย่างบางประการของอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ที่แผ่ขยายเป็นวงกว้างมากขึ้นในทุก ๆ วัน ความเสียหายทางเศรษฐกิจที่เกิดจากอาชญากรรมคอมพิวเตอร์นั้นมหาศาล เพียงแค่ในปี พ.ศ. 2546 เกิดความเสียหายจากโปรแกรมประสงค์ร้าย (Malicious software: Malware) ต่อเศรษฐกิจเกินหมื่นเจ็ดพันล้านเหรียญสหรัฐ[15] จากการประมาณ ผลประโยชน์จากการก่ออาชญากรรมคอมพิวเตอร์มีมากกว่าแสนด้านเหรียญสหรัฐในปี พ.ศ. 2550 ล้ำหน้าธุรกิจการค้ายาเสพย์ติดเป็นครั้งแรก[16] โดยกว่า 60% ของภาคธุรกิจในสหรัฐอเมริกา

---

[14] วีโอไอพี (VoIP) ย่อมาจาก Voice over Internet Protocol เป็นการสื่อสารทางเสียงผ่านโครงข่ายอินเทอร์เน็ต หรือโครงข่ายอื่น ๆ ที่ใช้อินเทอร์เน็ต สัญญาณเสียงจะถูกส่งไปบนโครงข่ายข้อมูล แทนการใช้วงจรเฉพาะตามวิธีการสื่อสารในระบบโทรศัพท์.

[15] Congressional Research Service, *The Economic Impact of Cyber-Attacks*, (Washington D.C.: CRS, 2004), 10,

[16] 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.

เชื่อว่าอาชญากรรมทางคอมพิวเตอร์สร้างความเสียหายแก่พวกเขามากกว่าอาชญากรรมประเภทอื่น[17] สิ่งเหล่านี้แสดงให้เห็นถึงความสำคัญในการปกป้องโครงสร้างขั้นพื้นฐานทางข้อมูลข่าวสาร และอันตรายจากภัยของอาชญากรรมคอมพิวเตอร์ต่อสังคมโลกในปัจจุบัน

2.1 นิยามของอาชญากรรมทางคอมพิวเตอร์

2.1.1 ความหมายของอาชญากรรมคอมพิวเตอร์

ความหมายของอาชญากรรมทางคอมพิวเตอร์เปลี่ยนแปลงไปพร้อมกับพัฒนาการทางเทคโนโลยี จากประวัติศาสตร์ทำให้เกิดข้อโต้แย้งว่าเมื่ออาชญากรรมคอมพิวเตอร์นั้นเข้าไปเกี่ยวข้องกับอาชญากรรมทุกหมวดหมู่ การนิยามความหมายของอาชญากรรมคอมพิวเตอร์ให้เกิดความครอบคลุมจึงจำเป็นต้องเน้นย้ำไปยังความรู้หรือการใช้งานเทคโนโลยีทางคอมพิวเตอร์เป็นหลัก

ผู้ริเริ่ม และได้รับการยอมรับว่าเป็นบิดาแห่งความรู้ในเรื่องอาชญากรรมคอมพิวเตอร์คือ Donn B. Parker ชาวสหรัฐอเมริกา เขาได้เป็นส่วนหนึ่งของการวิจัยในช่วงต้นทศวรรษที่ 70 โดยดำรงตำแหน่ง Senior Computer Security Consultant ณ Stanford Research Institute International (SRI International) และเป็นผู้ประพันธ์หลักในคู่มือการออกกฎหมายอาชญากรรมคอมพิวเตอร์ในสหรัฐอเมริกา (Computer Crime–Criminal Justice Resource Manual) ในปี ค.ศ. 1979 โดยคู่มือดังกล่าวเปรียบเสมือนสารานุกรมสำหรับแนวทางการออกกฎหมายอาชญากรรมคอมพิวเตอร์ทั้งของประเทศสหรัฐอมริกาและสากล

จากคู่มือดังกล่าวได้ให้ความหมายอาชญากรรมคอมพิวเตอร์ในแบบกว้าง ๆ ไว้ว่า เป็น “การกระทำทีผิดกฎหมายใด ๆ ซึ่งความรู้ทางวิทยาการคอมพิวเตอร์นั้นมีความสำคัญต่อการปฏิบัติการให้สำเร็จลุล่วง[18]”

นับแต่นั้นเป็นต้นมา อาชญากรรมทางคอมพิวเตอร์ได้ถูกให้นิยามโดยรายงานการศึกษาวิจัยและกฎหมายระหว่างประเทศอีกหลายฉบับ โดยให้ความหมายในเชิงกว้างและแคบแตกต่างกัน เช่น การศึกษาอาชญากรรมคอมพิวเตอร์ระดับสากลในปี ค.ศ. 1983 อาชญากรรม

---

[17] IBM survey published 14.05.2006, Retrieved 2013, October 17, from http://www.03.ibm.com/industries/consumerproducts/doc/content/news/pressrelease/1540939123.html.

[18] “any illegal act for which knowledge of computer technology is essential for its successful prosecution” SRI international, *The criminal justice resource manual on computer crime*, (Menlo Park, CA: SRI international, 1979).

คอมพิวเตอร์ถูกให้ความหมายว่า "หมายรวมถึงการกระทำที่ผิดกฎหมาย ซึ่งความรู้ทางวิทยาการคอมพิวเตอร์นั้นสำคัญต่อการกระทำผิด[19]"

OECD Recommendations of 1986 ได้รวมเอานิยามเพื่อเป็นฐานในการศึกษาไว้ว่า "อาชญากรรมที่เกี่ยวกับคอมพิวเตอร์นั้นถูกพิจารณาว่าเป็นพฤติกรรมอันผิดกฎหมาย ผิดศีลธรรมจรรยา หรือไม่ได้รับอนุญาต ที่เกี่ยวข้องกับการประมวลผลอัตโนมัติหรือการส่งข้อมูล[20]"

The Council of Europe Recommendation of 1989 ได้แนะแนวทางที่สามารถนำไปใช้ได้จริง โดยอาชญากรรมทางคอมพิวเตอร์ถูกอธิบายอย่างง่าย ๆ ว่าเป็น "การกระทำผิดที่ชี้วัดและนิยามโดยแนวทางที่ถูกเสนอหรือคำแนะนำสำหรับผู้ร่างกฎหมายในแต่ละประเทศ"[21]

The Council of Europe Recommendation of 1995[22] ในเรื่องกฎหมายวิธีพิจารณาความอาญา ความหมายไว้ว่า "การกระทำผิดที่เกี่ยวโยงกับเทคโนโลยีข้อมูลข่าวสาร[23]" (ความผิดเกี่ยวกับ IT หรือ อาชญากรรม IT) ได้ถูกนำมาใช้ โดยความผิดเกี่ยวกับ IT ได้ถูกอธิบายว่า "รวมไปถึงความผิดทางอาชญากรรม ในการสืบสวนที่เจ้าพนักงานสืบสวนต้องได้รับการเข้าถึงข้อมูลที่ถูกประมวลหรือส่งออกในระบบคอมพิวเตอร์ หรือระบบประมวลผลข้อมูลทางอิเลคทรอนิกส์[24]"

คณะกรรมาธิการสหภาพยุโรป (Commission of the European Union) ในปี ค.ศ. 2001 ได้ให้ความหมายอาชญากรรมทางคอมพิวเตอร์ว่า "อาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ที่ถูกระบุในความหมายที่กว้างที่สุดเป็นอาชญากรรมใด ๆ ซึ่งเกี่ยวข้องกับการใช้เทคโนโลยีข้อมูลข่าวสาร

---

[19] "Encompasses any illegal act for which knowledge of computer technology is essential for its perpetration" Schjolberg, S., *Computers and penal legislation–A study of legal politics of a new technology*, (Germany: Universitetsforlaget, 1986). 3/86.

[20] "Computer-related crime is considered as the offences enumerated and defined in the proposed guidelines or recommendation for national legislators", Organization for Co-operation Development, *Computer related criminality: Analysis of Legal Politics in the OECD Area*, (Paris: OECD, 1986).

[21] "…the offences enumerated and defined in the proposed guidelines or recommendation for national legislators…", Recommendation No. R (89) 9, adopted by the Committee of Ministers of the Council of Europe on September 13 1989 and Report by the European Committee on Crime Problems: Computer-related crime.

[22] Recommendation No. R (95) 13, approved by the European Committee on Crime Problems (CDPC) at its 44th plenary session May 29–June 2, 1995: Concerning problems of criminal procedural law connected with information technology.

[23] "…offences connected with Information Technology". Ibid.

[24] encompassing any criminal offence, in the investigation of which investigating authorities must obtain access to information being processed or transmitted in computer systems, or electronic data processing systems.

(IT) ไม่ทางใดก็ทางหนึ่ง[25]"และยังให้ความแตกต่างระหว่างอาชญากรรมคอมพิวเตอร์และอาชญากรรมทั่วไปที่ใช้คอมพิวเตอร์ในการช่วยกระทำการอีกด้วย

สำหรับอนุสัญญาอาชญากรรมคอมพิวเตอร์และการก่อการร้ายโดยมหาวิทยาลัยแสตนฟอร์ต (Stanford University) ในปี ค.ศ. 2000[26] ให้ความหมายอาชญากรรมคอมพิวเตอร์ไว้ว่า "การกระทำที่เกี่ยวข้องกับระบบคอมพิวเตอร์ที่ถูกจัดหมวดหมู่ให้สามารถได้รับการลงโทษโดยอนุสัญญานี้ได้[27]" โดยความหมายของระบบคอมพิวเตอร์ (Cyber system) ในข้อเสนอนี้หมายความถึง "คอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ใด ๆ ที่ถูกใช้ในถ่ายทอด ส่ง ประสานงาน หรือควบคุมการสื่อสารของข้อมูลหรือโปรแกรม[28]"

ข้อเสนอของสำหรับขอบข่ายการตัดสินใจในการโจมตีระบบข้อมูลข่าวสารของสภาสหภาพยุโรปในวันที่ 19 เมษายน ค.ศ. 2002 ทางคณะกรรมการได้ให้ความหมายของอาชญากรรมคอมพิวเตอร์ไว้ด้วยได้แก่ "อาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ควรได้รับความเข้าใจว่ารวมไปถึงการโจมตีระบบข้อมูลข่าวสารซึ่งให้นิยามไว้ในข้อกำหนดในขอบข่ายนี้[29]"

อนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของสหภาพยุโรป ค.ศ. 2001 (Convention on Cybercrime 2001) ให้คำนิยามของอาชญากรรมคอมพิวเตอร์ไว้ใน มาตรา 2-10 กฎหมายลักษณะอาญา ใน 4 หมวดหมู่ได้แก่ (1) ความผิดต่อความลับ ความสมบูรณ์ และการมีอยู่ของข้อมูลและระบบ (2) ความผิดเกี่ยวกับคอมพิวเตอร์ (3) ความผิดเกี่ยวกับเนื้อหา (4) ความผิดเกี่ยวกับการ

---

[25] The Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions, "Computer-related crime is addressed in the broadest sense as: any crime that in some way or other involves the use of information technology", The Communication from the Commission to the Council, the European Parliament, *The economic and social committee and the committee of the regions,* (2001, January 26), Retrieved 2013, October 17, from http://eur-lex.europa.eu/legal-content/.EN/ALL/;ELX_SESSIONID=GwZLJy5TV3NhBcLyRM882MNrT022QNfGD15kddlNskcvqkPkC7PJ!-7040371?uri=CELEX:52000DC0890

[26] Center for International Security and Cooperation (CISAC) Stanford University, *A proposal for an international convention on cyber crime and terrorism*, (2000, August), Retrieved 2013, October 17, from http://cisac.stanford.edu/publications/11912

[27] conduct with respect to cyber systems that is classified as an offense punishable by this Convention, Ibid.

[28] Any computer or network of computers used to relay, transmit, coordinate, or control communications of data or programs, Ibid.

[29] McGonagle, T., *European commission adoption of proposal to combat cybercrime*, (Netherland: Institute for Information Law (IViR), University of Amsterdam, n.d.), Retrieved 2013, October 17, from http://merlin.obs.coe.int/iris/2002/6/article7.en.html

ละเมิดลิขสิทธิ์และสิทธิ์ที่เกี่ยวข้อง[30] โดยได้กำหนดมาตรฐานขั้นต่ำของมาตรการทางกฎหมายทั้งภายในประเทศรวมไปถึงในระดับระหว่างประเทศ

การกระทำผิดเกี่ยวกับเนื้อหา เช่น การละเมิดลิขสิทธิ์ การหมิ่นเชื้อชาติ และสื่อลามกอนาจารเด็ก โดยปกติอาจไม่ถูกจัดอยู่ในอาชญากรรมคอมพิวเตอร์ การละเมิดลิขสิทธิ์มีพื้นฐานบนข้อตกลงทางแพ่งและสัญญาอีกทั้งยังไม่จัดเป็นความผิดอาญาในหลายประเทศ ความผิดฐานละเมิดลิขสิทธิ์มักได้รับการเยียวยาทางแพ่งเนื่องจากปัญหาความยุ่งยากซับซ้อน สื่อลามกอนาจารเด็กนั้นเป็นความผิดอาญาอยู่แล้วแม้จะไม่ได้อยู่ในรูปแบบดิจิตอล

ปัจจุบันได้รวมเอาการโจรกรรมเอกลักษณ์บุคคล (Identity theft)[31] สแปม[32] phishing[33] และการตระเตรียมก่อนการพยายามกระทำความผิดเข้าไปด้วย อาชญากรรมคอมพิวเตอร์อาจรวมไปถึงการโจมตีร่วมกันจำนวนมากต่อโครงสร้างพื้นฐานทางข้อมูลข่าวสารของประเทศ แม้กระทั่งการแยกแยะการก่อการร้ายซึ่งยังไม่มีความชัดเจน โดยเฉพาะการใช้งานอินเตอร์เน็ตโดยมิชอบของผู้ก่อการร้ายเพื่อให้ข้อมูลบิดเบือนสร้างความตื่นตระหนกทางสังคม การเรียกรับสมาชิกหรือฝึกฝนเพื่อการก่อการร้าย เป็นต้น

โดยสรุปแล้ว ผู้วิจัยเห็นว่า อาชญากรรมคอมพิวเตอร์ในปัจจุบันนั้น ได้เปลี่ยนแปลงไปจากอดีตเป็นอย่างมาก จากเดิมที่เป้าหมายเป็นเพียงข้อมูลทางคอมพิวเตอร์มาเป็นตัวผู้ใช้คอมพิวเตอร์ แม้กระทั่งใช้เป็นอาวุธในการทำสงครามหรือจู่โจมระบบโครงสร้างพื้นฐาน ดังนั้นอาชญากรรมทาง

---

[30] Convention on Cybercrime, Chapter 1-4, (1) Offences against the confidentiality, integrity and availability of computer data and systems; (2) computer-related offences, (3) content-related offences; (4) offences related to infringements of copyright and related rights.

[31] การโจรกรรมเอกลักษณ์บุคคล (Identity Theft) คือ การที่ข้อมูลส่วนตัวของเหยื่อถูกขโมยและนำไปใช้อย่างผิดกฎหมาย เช่น เพื่อเปิดบัญชีและซื้อสินค้าในชื่อของเหยื่อ บ่อยครั้งการโจรกรรมข้อมูลของบุคคลหรือของธุรกิจถูกนำไปใช้เพื่อก่ออาชญากรรมอื่น ๆ ต่อ เช่น การโกงบัตรเครดิต เป็นต้น นี่คือข้อเท็จจริงบางประการเกี่ยวกับการโจรกรรมเอกลักษณ์บุคคล.

[32] สแปม (spam) คือชื่อเรียกของการส่งข้อความที่ผู้รับไม่ได้ร้องขอ ผ่านทางระบบอิเล็กทรอนิกส์ สแปมที่พบเห็นได้บ่อยได้แก่ การส่งสแปมผ่านทางอีเมล เพื่อโฆษณาชวนเชื่อ โฆษณาขายของ โดยการส่ง อีเมลประเภทหนึ่งที่เราไม่ต้องการ โดยปัจจุบันสแปมไม่ได้จำกัดเฉพาะอีเมล์เท่านั้น แต่อาจอยู่ในรูปของข้อความ SMS ข้อความผ่านห้องสนทนาต่าง ๆ อีกด้วย.

[33] ฟิชชิง (phishing) คือการหลอกลวงทางอินเทอร์เน็ต เพื่อขอข้อมูลที่สำคัญเช่น รหัสผ่าน หรือหมายเลขบัตรเครดิต โดยการส่งข้อความผ่านทางอีเมลหรือเมสเซนเจอร์ เช่น การบอกแก่ผู้รับปลายทางว่าเป็นธนาคารหรือบริษัทที่น่าเชื่อถือ และแจ้งว่ามีสาเหตุทำให้คุณต้องเข้าสู่ระบบและใส่ข้อมูลที่สำคัญใหม่ โดยเว็บไซต์ที่ลิงก์ไปนั้น มักจะมีหน้าตาคล้ายคลึงกับเว็บที่กล่าวถึง.

คอมพิวเตอร์ควรมีความหมายรวมไปถึงความผิดใด ๆ ที่ใช้คอมพิวเตอร์เป็นเครื่องมือไม่ว่าเป้าหมายจะเป็นอะไรก็ตาม

2.1.2 รูปแบบของอาชญากรรมทางคอมพิวเตอร์

ด้วยความไม่เป็นเอกภาพของมาตรการบังคับใช้ทางกฎหมายรวมไปถึงมาตรการทางเทคนิคในการรับมืออาชญากรรมคอมพิวเตอร์ในแต่ละประเทศ จึงเกิดความพยายามในการสร้างมาตรการทางกฎหมายที่เป็นมาตรฐานกลางและวางหลักการร่วมกันในระดับนานาชาติขึ้น ทั้งนี้ได้มีการจำแนกรูปแบบของอาชญากรรมทางคอมพิวเตอร์ในปัจจุบันดังนี้

2.1.2.1 ความผิดประเภทบุกรุก

1. การเข้าถึงยังระบบคอมพิวเตอร์อย่างผิดกฎหมาย (llegal access)
2. การลักลอบขโมยข้อมูล (Data espionage)
3. การรบกวนข้อมูล (Data interference)

2.1.2.2 ความผิดด้านเนื้อหา

1. เนื้อหาประเภทสื่อลามกเด็ก (Child pornography)
2. เนื้อหาประเภทที่ก่อให้เกิดความเกลียดชัง เหยียดเชื้อชาติ เหยียดศาสนา (Hate speech, Racism, Blasphemy)

2.1.2.3 เนื้อหาประเภทสแปม (Spam)

1. การกระทำผิดประเภทการละเมิดลิขสิทธิ์และเครื่องหมายการค้า
2. การละเมิดลิขสิทธิ์ทั่วไป (Copyright Infringement)
3. การละเมิดเครื่องหมายการค้า (Trademark violations)

2.1.2.4 อาชญากรรมทางคอมพิวเตอร์ที่มีเป้าหมายเป็นผู้ใช้คอมพิวเตอร์ (Social Engineering Scam)

1. การฉ้อโกง (Fraud)
2. การปลอมแปลง (Forgery)
3. การโจรกรรมเอกลักษณ์บุคคล (Identity theft)

2.1.2.5 การกระทำผิดแบบผสมผสาน (Combination offences)

1. การก่อการร้ายไซเบอร์ (Cyber terrorism)
2. สงครามไซเบอร์ (Cyber warfare)
3. การทุจริตฟอกเงินไซเบอร์ (Cyber laundering)

2.1.3 แนวโน้มของอาชญากรรมคอมพิวเตอร์

เนื่องจากอาชญากรคอมพิวเตอร์รู้ถึงศักยภาพในด้านผลประโยชน์ทางเศรษฐกิจจากการก่ออาชญากรรมคอมพิวเตอร์ จึงมีแนวโน้มที่อาชญากรรมประเภทนี้จะเปลี่ยนจากการทดลอง และการทำลายทรัพย์สินสาธารณะอย่างไร้เหตุผลเป็นอาชญากรรมที่มุ่งเป้าหลากหลายมากขึ้น โดยเฉพาะบนอุปกรณ์หรือระบบซึ่งข้อมูลที่มีมูลค่าสูงสะสมอยู่จำนวนมาก เช่น คอมพิวเตอร์ อุปกรณ์เคลื่อนที่ และ กลุ่มเมฆข้อมูล (The cloud)

2.1.3.1 การเปลี่ยนข้ามแพลตฟอร์ม (Platform changes)

อาชญากรรมคอมพิวเตอร์เปลี่ยนสนามรบจากคอมพิวเตอร์ที่ใช้ระบบปฏิบัติการวินโดว์ของไมโครซอฟท์มาเป็นแพลตฟอร์มอื่นที่หลากหลายมากขึ้น รวมไปถึงโทรศัพท์มือถือประเภทสมาร์ทโฟน (Smartphone)[34] คอมพิวเตอร์แทบเล็ต (Tablet)[35] และบริการ VoIP เนื่องจากมาตรฐานความปลอดภัยได้มาถึงจุดอิ่มตัว เมื่อผู้จัดจำหน่ายซอฟท์แวร์ได้มีการพัฒนาระบบรักษาความปลอดภัยที่รัดกุมและปรับปรุงผลิตภัณฑ์ของตนเองอย่างรวดเร็วและสม่ำเสมอ กอปรกับความแพร่หลายของอุปกรณ์สื่อสารเคลื่อนที่อย่างโทรศัพท์มือถือสมาร์ทโฟนและแทบเล็ตทำให้อาชญากรเปลี่ยนเป้าหมายไปยังอุปกรณ์เหล่านี้มากขึ้น

2.1.3.2 การโจมตีโดยใช้วิธีการทางจิตวิทยา (Social engineering scams)

หมายถึงการล่วงละเมิดที่ไม่ได้กระทำด้วยวิธีการทางเทคนิค แต่พึ่งพาอีเมล์หรือการสนทนาบนระบบเครือข่ายเพื่อหลอกลวงเหยื่อให้ดาวโหลดซอฟท์แวร์ที่เป็นอันตราย (Malware) หรือให้ข้อมูลส่วนตัวแก่อาชญากรไป โดยการโจมตีทางจิตวิทยานี้ได้ผลเป็นอย่างยิ่งต่อระบบคอมพิวเตอร์ที่ได้รับการคุ้มครองเป็นอย่างดีแต่มีช่องโหว่ที่ตัวผู้ใช้ (User vulnerability) เครือข่ายสังคมออนไลน์ (Social network) เป็นเครื่องมือสำคัญที่อาชญากรใช้ในการโจมตีประเภทนี้โดยอาชญากรจะจ้างวาน Money mules เพื่อให้ความช่วยเหลือในการฟอกเงินรอบโลก โดย Spammer ไม่เพียงแต่กระจายการล่อลวง (Spoof) ด้วยข้อความทางสังคมออนไลน์เพื่อหลอกล่อเหยื่อให้เปิด

---

[34] สมาร์ทโฟน (Smartphone) เป็นโทรศัพท์เคลื่อนที่ที่มีความสามารถที่เพิ่มเติมนอกเหนือจากโทรศัพท์มือถือทั่วไปสมาร์ทโฟนได้ถูกมองว่าเป็นคอมพิวเตอร์พกพาที่ทำงานในลักษณะของโทรศัพท์เคลื่อนที่ โดยที่สามารถเชื่อมต่อความสามารถหลักของโทรศัพท์มือถือ เข้าร่วมกับแอปพลิเคชันของโทรศัพท์เอง สมาร์ทโฟนสามารถให้ผู้ใช้งานติดตั้งโปรแกรมเสริมสำหรับเพิ่มความสามารถของโทรศัพท์ตัวเอง โดยรูปแบบนั้นขึ้นอยู่กับแพลตฟอร์มของโทรศัพท์และระบบปฏิบัติการ.

[35] แทบเล็ตคอมพิวเตอร์ (Tablet computer) เรียกสั้น ๆ ว่า แทบเล็ต เป็นคอมพิวเตอร์ที่รวมการทำงานทุกอย่างไว้ในจอสัมผัสโดยใช้ปากกาสไตลัส ปากกาดิจิตอล หรือปลายนิ้ว เป็นอุปกรณ์อินพุตพื้นฐาน แทนการใช้คีย์บอร์ดและเมาส์ แต่มีอยู่หรือไม่มีก็ได้.

เข้าไปเพื่อขโมยข้อมูลส่วนบุคคลเท่านั้น แต่ยังใช้ความเชื่อใจกันของเหล่าผู้ใช้ในเครือข่ายสังคมออนไลน์เพื่อดึงดูดเหยื่อรายใหม่ให้เข้ามาเป็นลูกโซ่อีกด้วย

2.1.3.3 การโจมตีแบบเจาะจงเป้าหมาย (Hypertargeting)

เป็นการโจมตีโดยอาชญากรจะสร้างไวรัสหรือมัลแวร์เพื่อจู่โจมเฉพาะเป้าหมายที่ตนต้องการ เช่น อุปกรณ์ของบริษัทใดบริษัทหนึ่ง มีเป้าหมายเพื่อขัดขวางระบบทางอุตสาหกรรม เช่น stuxnet worm ที่มีเป้าหมายโจมตีอุปกรณ์ของบริษัท Siemens ที่เชื่อมต่อบนระบบปฏิบัติการวินโดว์ของไมโครซอฟท์ เป็นต้น

2.1.3.4 การแพร่มัลแวร์ (Malware dissemination)

มัลแวร์มักอยู่ในรูปของไวรัส หนอนไวรัส โทรจัน[36] หรือสปายแวร์[37] คอมพิวเตอร์ ซึ่งเป็นโปรแกรมที่ถูกสร้างขึ้นเพื่อก่อกวนหรือสร้างความเสียหายให้กับระบบคอมพิวเตอร์ หรือเพื่อการจารกรรมข้อมูล

2.1.3.5 การขโมยทรัพย์สินทางปัญญา (Intellectual property theft)

กว่า 90% ของซอฟแวร์ ภาพยนตร์ ในรูปของ Bluray, CD, DVD ที่ถูกวางจำหน่ายบนโลกเป็นของละเมิดลิขสิทธิ์ ด้วยธรรมชาติของอินเตอร์เน็ตที่กลายแพร่กระจายของข้อมูลเกิดขึ้นอย่างรวดเร็ว การละเมิดลิขสิทธิ์จึงเกิดขึ้นได้ง่ายและสร้างความเสียหายเป็นวงกว้าง จากเดิมที่มีการส่งต่อข้อมูลผ่านระบบ IRC จนมาถึงการกระจายข้อมูลละเมิดลิขสิทธิ์ผ่านการให้บริการ Peer to peer file sharing หรือที่เรียกว่า Bit torrent[38] รวมไปถึงเว็บไซต์ที่ให้บริการรับฝากไฟล์ซึ่งผู้เข้าใช้

---

[36] ม้าโทรจัน (Trojan horse) หมายถึง โปรแกรมคอมพิวเตอร์ที่ถูกบรรจุเข้าไปในคอมพิวเตอร์ เพื่อลอบเก็บข้อมูลของคอมพิวเตอร์เครื่องนั้น เช่น ข้อมูลชื่อผู้ใช้ รหัสผ่าน เลขที่บัญชีธนาคาร หมายเลขบัตรเครดิต และข้อมูลส่วนบุคคลอื่น ๆ โดยส่วนใหญ่แฮกเกอร์จะส่งโปรแกรมเข้าไปในคอมพิวเตอร์เพื่อดักจับข้อมูลดังกล่าว แล้วนำไปใช้ในการเจาะระบบ และเพื่อโจมตีคอมพิวเตอร์, เซิร์ฟเวอร์, หรือระบบเครือข่ายอีกที ซึ่งเป็นที่รู้จักกันในชื่อการโจมตีเพื่อ “ปฏิเสธการให้บริการ” (Denial of Services) โปรแกรมม้าโทรจัน ถือเป็นโปรแกรมที่สอดคล้องกับการทำงานของคอมพิวเตอร์ ไม่มีคำสั่งหรือการปฏิบัติการที่เป็นอันตรายต่อตัวคอมพิวเตอร์ จึงไม่ถือว่าเป็นไวรัสคอมพิวเตอร์.

[37] สปายแวร์ คือ ประเภทโปรแกรมคอมพิวเตอร์ที่บันทึกการกระทำของผู้ใช้บนเครื่องคอมพิวเตอร์ และส่งผ่านอินเทอร์เน็ตโดยที่ผู้ใช้ไม่ได้รับทราบ โปรแกรมแอบดักข้อมูลนั้นสามารถรวบรวมข้อมูล สถิติการใช้งานจากผู้ใช้ได้หลายอย่างขึ้นอยู่กับการออกแบบของโปรแกรม ซึ่งส่วนใหญ่แล้วบันทึกเว็บไซต์ที่ผู้ใช้เข้าถึง และส่งไปยังบริษัทโฆษณาต่าง ๆ บางโปรแกรมอาจบันทึกว่าผู้ใช้พิมพ์อะไรบ้าง เพื่อพยายามค้นหารหัสผ่าน หรือเลขหมายบัตรเครดิต.

[38] Peer-to-peer คือ ระบบการเชื่อมต่อที่ยอมให้ผู้ใช้สามารถแลกเปลี่ยนข้อมูลหรือใช้ทรัพยากรร่วมกันผ่านระบบเครือข่าย ซึ่งผู้ใช้สามารถรับหรือส่งข้อมูลกันได้โดยไม่จำต้องผ่าน server ซึ่ง server ทำหน้าที่เพียงจับคู่ระหว่างผู้ใช้หนึ่งกับผู้ใช้อื่น ๆ เท่านั้น โดยเรียกโปรแกรมที่ใช้ในการแลกเปลี่ยนไฟล์ระหว่างกันโดยไม่ได้ร้องขอไฟล์จากแม่ข่ายว่า โปรแกรมประเภท “P2P File Sharing” เช่น โปรแกรมประเภท bittorrent อย่าง Utorrent หรือ bitcomet เป็นต้น.

บริการใด ๆ สามารถเข้าไปดาว์นโหลดข้อมูลที่มีผู้อัพโหลดไว้ได้อย่างอิสระ เช่น เว็บไซต์ www.4shared.com เป็นต้น

2.1.4 สงครามไซเบอร์ (Cyber warfare)

จากที่ได้กล่าวมาในหัวข้อประวิติศาสตร์อาชญากรรมคอมพิวเตอร์ในเรื่องของการที่เทคโนโลยี ICT เข้ามาเป็นส่วนหนึ่งของแทบทุกภาคส่วนของสังคมไม่เว้นแต่กิจการด้านความมั่นคงเช่นปฏิบัติการทางทหาร เมื่ออินเตอร์เน็ตกลายเป็นพื้นที่เสมือนผ่านการเชื่อมต่อกันของระบบเครือข่าย พรหมแดนใหม่แห่งที่ 4 หรือพรหมแดนไซเบอร์ (Cyber frontier) จึงถือกำเนิดขึ้น รัฐบาลนานาชาติต่างเกิดความตระหนักในการปกป้องพรหมแดนดังกล่าวจากภัยทางความมั่นคงภายนอกจากรัฐอื่น ที่เรียกว่า “สงครามไซเบอร์”

สงครามไซเบอร์ หมายความถึงการเจาะระบบโดยมีเป้าหมายทางการเมืองเพื่อทำลายหรือลักลอบจารกรรมข้อมูล เรียกได้ว่าเป็นรูปแบบหนึ่งของสงครามข้อมูลข่าวสาร การโจมตีทางอินเตอร์เน็ตและเทคโนโลยีสารสนเทศสามารถทำได้จากทุกแห่งบนโลก ทำให้มีทางเลือกในการก่ออาชญากรรมที่ซับซ้อนและยากแก่การตรวจสอบ เนื่องจากโลกทางไซเบอร์นั้นไม่อาจระบุขอบเขตได้อย่างชัดเจนในหลายเรื่อง เช่น ขอบเขตระหว่างโลกจริงและโลกเสมือน หรือขอบเขตระหว่างพลเรือนกับทหาร โดยสงครามไซเบอร์อาจเกิดจากองค์กรที่ไม่มีการจัดตั้งอย่างเป็นทางการ (Non-state actors), องค์กรรัฐที่จัดตั้งขึ้นอย่างเป็นทางการ (State actors) และอาจเป็นรูปแบบของตัวแทน (proxy) ก็ได้ และแม้ว่าสงครามไซเบอร์ไม่ได้ก่อให้เกิดการสูญเสียเลือดเนื้อของทหารหรือประชาชนโดยตรง แต่ก็อาจทำให้เกิดความขัดแย้งที่รุนแรงในระดับถอนรากถอนโคนได้

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

ในเดือนสิงหาคม ปีพ.ศ. 2553 บริษัทญี่ปุ่น Mitsubishi Heavy Industries ตกเป็นเป้าหมายการโจมตีจากประเทศจีน[39] หนึ่งในนักวิจารณ์จาก Financial Times ให้ความเห็นว่าภัยทางอินเตอร์เน็ตอาจนำไปสู่การสร้างมาตรฐานกลางในการสร้างพันธมิตรด้านความปลอดภัยทางการทหารระหว่าง

---

[39] Buerk, R., *Japan defence firm Mitsubishi heavy in cyber attack*, BBC News, (2011, September 20), Retrieved 2013, October 17, from http://www.bbc.co.uk/news/world-asia-pacific-14982906.

สหรัฐและญี่ปุ่นขึ้นมาใหม่ ความเห็นนี้ยิ่งดูน่าเชื่อถือมากขึ้นเมื่อสองเดือนต่อมาสภาล่างของรัฐสภาญี่ปุ่นถูกโจมตีอีกครั้ง โดยการโจมตีดังกล่าวนั้นมาจากประเทศจีนเช่นกัน[40]

แนวคิดแบบสงครามเย็นนี้เริ่มชี้นำรัฐบาลชาติต่าง ๆ ให้เพ่งความสนใจไปที่ “สงครามไซเบอร์” และ “อธิปไตยไซเบอร์ (Cyber sovereignty)” ยกตัวอย่างในเดือนเมษายนปี พ.ศ. 2553 ศูนย์บัญชาการไซเบอร์ของสหรัฐถูกก่อตั้งขึ้น และเมื่อทำเนียบขาวเผยแผนยุทธศาสตร์ไซเบอร์สเปซระหว่างประเทศเป็นครั้งแรก ตามหลังแผนยุทธศาสตร์ของกระทรวงความมั่นคงในเรื่องพรหมแดนไซเบอร์อย่างกระชั้นชิด โดย Leon panetta เลขานุการความมั่นคงแห่งชาติสหรัฐอเมริกาเปรียบเทียบผลลัพธ์ที่อาจเกิดขึ้นได้ของการโจมตีที่อาจเป็น “เหตุการณ์เพิร์ลฮาเบอร์หนต่อไป”[41] ในขณะนั้นเอง ประเทศจีนยืนยันการมีอยู่ของ “Cyber blue team” หน่วยรบในสังกัดกองทัพสาธารณรัฐประชาชนจีนในปี พ.ศ. 2554 และไม่นานมานี้เองนักคิดทางการทหารของจีนต่างเรียกหาการจัดการแบบ “สังคมรวม (All-society approach)” ต่อการเคลื่อนพลรบไซเบอร์โดยอาศัยภาคพลเรือน อุตสาหกรรม และเครือข่ายทางทหาร

การจารกรรมข้อมูลทางอินเตอร์เน็ตมักมีแรงผลักดันทางเศรษฐกิจอยู่เบื้องหลัง เช่นการจารกรรมข้อมูลของจีนที่คาดว่าเป็นส่วนหนึ่งของความพยายามลดการพึ่งพาทางวิทยาการจากตะวันตกจาก “สร้างในจีน (Made in china)” เป็น “คิดค้นในจีน (Innovated in china)” แทน บางครั้งการโจมตีทางอินเตอร์เน็ตอาจมีสาเหตุจากภาคการเมือง เช่น รัสเซียโจมตีเว็บไซต์ของรัฐบาลจอร์เจียในปี พ.ศ. 2551 ซึ่งเกิดขึ้นในเวลาใกล้เคียงกันกับการแยกตัวเป็นอิสระของ Ossetia ใต้ ในปีเดียวกันกลุ่มนักเจาะระบบรักชาติ (Patriotic hacker) จีนประกาศโจมตี CNN หลังสำนักข่าวออกอากาศรายงานการกดขี่ธิเบตของจีน การเผชิญหน้าระหว่างจีนและเวียดนามในเดือนมิถุนายน พ.ศ. 2554[42] สร้างเส้นขนานระหว่างทั้งสองชาติบนอินเตอร์เน็ตเมื่อนักเจาะระบบจากทั้งสองประเทศต่างฝ่ายต่างเจาะเข้ามาเปลี่ยนสัญลักษณ์บนเว็บไซต์ของรัฐบาลฝ่ายตรงข้าม

เหตุการณ์หนึ่งซึ่งทำให้เกิดการตื่นตัวในเรื่องการจู่โจมไซเบอร์ที่มีรัฐอยู่เบื้องหลัง และอาจเรียกได้ว่าเป็นสงครามไซเบอร์ครั้งแรกของโลก คือเหตุการณ์ความขัดแย้งทางไซเบอร์ (Cyber

---

[40] Cyber-attack from server in China targets Lower House, *Asahi Shimbun*, (2011, October 25), Retrieved 2013, 17 October, from http://ajw.asahi.com/article/behind_news/social_affairs/AJ2011102515710.

[41] Lee, A., CIA Chief Leon Panetta: Cyber attack could be next pearl harbor, *The Huffington Post*, (2013, June 13), Retrieved 2013, October 17, from http://www.huffingtonpost.com/2011/06/13/panetta-cyberattack-next-pearl-harbor_n_875889.html

[42] Vietnam and China hackers escalate Spratly Islands row, *BBC News*, (2011, June 9), Retrieved 17 October 2013, from http://www.bbc.co.uk/news/world-asia-pacific-13707921

conflict) ระหว่างรัสเซียและเอสโตเนีย ในปี พ.ศ. 2553[43] หลังประเทศเอสโตเนีย หนึ่งในอดีตสาธารณรัฐของสหภาพโซเวียต ซึ่งปัจจุบันเป็นทั้งสมาชิกกลุ่มสหภาพยุโรป และนาโต้ ทำการย้ายรูปปั้นทหารโซเวียตซึ่งรัสเซียสร้างเพื่ออุทิศให้กับทหารซึ่งสู้รบกับนาซีเยอรมันในสงครามโลกครั้งที่ 2 จากเขตใจกลางเมืองหลวง ไปไว้ในอีกที่หนึ่งเมื่อปลายเดือนมิถุนายน พ.ศ. 2553 เอสโตเนียจึงถูกฝ่ายรัสเซีย จู่โจมทางอินเตอร์เน็ต ในช่วงแรกพบว่ามีการโจมตีจากเครื่องคอมพิวเตอร์จากสถาบันของรัฐในรัสเซีย แต่โดยหลักแล้วการโจมตีนั้นมาจากทั่วทุกมุมโลก เนื่องจากเป็นการโจมตีประเภท DDoS (Denial of service attack) ซึ่งอาศัยการจู่โจมเข้ามาพร้อม ๆ กันจากคอมพิวเตอร์จำนวนมาก เอสโตเนียเป็นประเทศเล็ก ๆ มีประชากรเพียง 1.4 ล้านคน และเคยตกเป็นของรัสเซียหลายครั้ง รวมเป็นเวลากว่าหลายร้อยปี เป็นเหตุบ่มเพาะความเกลียดชังต่อคนรัสเซียอย่างมาก โดยประเทศตะวันตกต่างอาศัยประโยชน์จากความเกลียดชังนี้รุกเข้ามาประชิดพรมแดนรัสเซียอยู่ในปัจจุบัน เพื่อหาทางบั่นทอนอิทธิพลของรัสเซีย เอสโตเนียเป็นสังคมที่มีการออนไลน์กันมากที่สุดแห่งหนึ่งในยุโรป และเป็นผู้บุกเบิกรัฐบาลอิเล็กทรอนิกส์ (e-government) แต่สิ่งที่เป็นจุดแข็งของประเทศกลับสร้างความเสียหายให้กับประเทศทันทีเมื่อเกิดสงครามไซเบอร์ ซึ่งเป้าหมายที่ถูกโจมตีนั้นได้แก่เว็บไซต์ประธานาธิบดีและรัฐสภา กระทรวงต่าง ๆ พรรคการเมือง องค์กรสื่อยักษ์ใหญ่ 3 แห่งจาก 6 แห่ง ธนาคารใหญ่ที่สุด 2 แห่ง บริษัทด้านการสื่อสาร โดยปัจจุบันไม่มีการเปิดเผยว่าความเสียหายเหล่านี้มีมูลค่ามากน้อยเพียงใด

พัฒนาการของเครื่องมือและอุปกรณ์ที่มีอยู่ในปัจจุบันแสดงให้เห็นถึงศักยภาพมหาศาลในการเปลี่ยนนิยามของการโจมตีมุ่งร้าย และเพื่อเป็นการสนองตอบต่อปัญหาดังกล่าว นานาชาติต่างปรับเปลี่ยนรูปแบบปฏิบัติการเพื่อปฏิวัติกิจการทหาร กลุ่มธุรกิจต่าง ๆ ทั้ง การคมนาคม พลังงาน การค้นคว้าวิจัย สาธารณสุข วิชาการ และบริการทางสังคม ต่างมุ่งหวังให้ผู้นำประเทศจัดแจงแผนการเพื่อคุ้มครองกิจการของพวกเขาบนพรหมแดนไซเบอร์ เนื่องจากสงครามไซเบอร์นั้นเป้าหมายสามารถเป็นได้ทั้งเครือข่ายของกองทัพหรือพลเรือน สงครามไซเบอร์อาจแบ่งรูปแบบการโจมตีได้ดังนี้

2.1.4.1 การลักลอบจารกรรมข้อมูลและการเจาะระบบรักษาความปลอดภัยของชาติ (Espionage and national security breaches)

คือการจู่โจมที่มุ่งหวังขโมยข้อมูลที่เป็นความลับ ที่อาจเป็นข้อมูลอันมีความละเอียดอ่อนหรือเป็นข้อมูลที่อยู่ในลำดับความสำคัญสูง (Classified) จากบุคคล คู่แข่งทางการค้าหรือรัฐบาล เพื่อความได้เปรียบทางการทหาร การเมือง หรือเศรษฐกิจ โดยใช้วิธีการที่ผิดกฎหมาย

---

[43] Estonia hit by “Moscow cyber war”, *BBC News*, (2007, May 17), Retrieved 2013, October 17, from http://news.bbc.co.uk/2/hi/europe/6665145.stm

(illegal exploitation) บนอินเตอร์เน็ต เครือข่ายต่าง ๆ ซอฟท์แวร์หรือคอมพิวเตอร์ ข้อมูลในลำดับความสำคัญที่ไม่ได้รับการดูแลที่เหมาะสมอาจถูกดักจับหรือแม้แต่เปลี่ยนแปลงแก้ไข ทำให้การจารกรรมข้อมูลสามารถกระทำได้แม้อยู่ห่างกันคนละซีกโลก

2.1.4.2 การก่อวินาศกรรม (Sabotage)

กิจกรรมทางทหารที่ใช้คอมพิวเตอร์และดาวเทียมเพื่อระบุเป้าหมายมีความเสี่ยงที่อุปกรณ์จะถูกขัดขวางการทำงาน คำสั่งและการสื่อสารอาจถูกดักจับหรือแทนที่ด้วยคำสั่งที่มุ่งร้าย โครงสร้างพื้นฐานเช่น ไฟฟ้า ประปา เชื้อเพลิง การสื่อสาร และการคมนาคม มีความเสี่ยงที่ต้องหยุดชะงักจากการโจมตีประเภทนี้ ยกตัวอย่างกรณีหนอนคอมพิวเตอร์ Stuxnet ซึ่งเข้าจู่โจมคอมพิวเตอร์ของโรงงานไฟฟ้าที่ใช้อุปกรณ์ของบริษัท Siemens และกระจายไปยังโรงไฟฟ้าที่ใช้อุปกรณ์อย่างเดียวกันทั่วโลก ซึ่งเหตุการณ์ดังกล่าวนับเป็นการโจมตีโครงสร้างพื้นฐานครั้งแรกของโลก[44]

2.1.4.3 การจู่โจมระบบการไฟฟ้า (Electronic power grid)

รัฐบาลกลางสหรัฐยอมรับว่าการส่งกระแสไฟฟ้านั้นมีความเสี่ยงต่อภัยทางสงครามไซเบอร์[45] โดยกระทรวงความปลอดภัยแห่งชาติสหรัฐอเมริกาได้ทำงานร่วมกับภาคอุตสาหกรรมในการระบุจุดอ่อนและช่วยเพิ่มความปลอดภัยให้กับระบบควบคุม พลังงานไฟฟ้าจัดเป็นสาธารณูปโภคพื้นฐานทางพลังงานที่สำคัญที่สุดของประเทศชาติ เนื่องจากในทุกภาคส่วนมีความต้องการใช้ไฟฟ้าทั้งสิ้น กิจการทั้งการคมนาคม โทรคมนาคม สาธารณสุข และกิจการทหาร ต่างพึ่งพาพลังงานไฟฟ้าในการปฏิบัติงาน เมื่อถูกทำให้หยุดชะงักจะทำให้เกิดความเสียหายอย่างประเมินค่ามิได้ และทำให้ประเทศตกอยู่ในภาวะเสี่ยงต่อการถูกโจมตีได้ง่าย

2.1.5 ผลกระทบจากภัยคุกคามทางอาชญากรรมทางคอมพิวเตอร์

อาชญากรรมทางคอมพิวเตอร์มีลักษณะเป็นเช่นเดียวกันกับอาชญากรรมรูปแบบอื่น ๆ ที่มีแรงผลักดันในการก่ออาชญากรรมอาจเป็นเรื่องผลประโยชน์ทางเศรษฐกิจ อำนาจ เพื่อแก้แค้น การแสวงหาความรู้ เพื่อทดลอง อุดมคติหรือความโลภ โดยภัยคุกคามจากปัจจัยที่กล่าวมาสามารถจัดหมวดหมู่ได้ ดังนี้

---

[44] Malware Hits Computerized Industrial Equipment, *New York Times*, (2010, September 24), Retrieved 2013, October 17, from http://bits.blogs.nytimes.com/2010/09/24/malware-hits-computerized-industrial-equipment/

[45] Maggie, S., Spies “infiltrate US power grid”, *BBC News*, (2009, September 4), Retrieved 2013, October 17, from http://news.bbc.co.uk/2/hi/technology/7990997.stm.

2.1.5.1 ความมั่นคงทางเศรษฐกิจ

ชื่อเสียงและความน่าเชื่อถือทางสังคมต่างพบปัญหาอย่างหนักจากการหลอกลวงทางอินเตอร์เน็ต การปลอมแปลง การปลอมตัวเป็นผู้อื่น และการปิดบังตัวตน การขู่กรรโชก การฟอกเงินอิเล็กทรอนิกส์ การละเมิดลิขสิทธิ์ และการเลี่ยงภาษี

2.1.5.2 ประโยชน์สาธารณะ และความมั่นคงของชาติ

อาจถูกคุกคามจากการแพร่สิ่งไม่พึงปรารถนา เช่น สื่อลามกอนาจาร การหมิ่นประมาท การดูหมิ่นเชื่อชาติ ศาสนา ถ้อยคำที่ทำให้เกิดความเกลียดชัง การตามตื๊อ ก่อกวนทางอินเตอร์เน็ต (Cyber Stalking/harassment) สื่อลามกอนาจารเด็ก การก่อการร้ายไซเบอร์ เป็นต้น

2.1.5.3 ความปลอดภัยของข้อมูลส่วนบุคคล

ข้อมูลภายในประเทศ หรือแม้แต่ข้อมูลทางการทูต ถูกคุกคามโดยการเข้าถึงโดยไม่ได้รับอนุญาตและการใช้งาน ICT โดยมิชอบ ผ่านการโจมตีแบบ DDoS (Denial of service) หรือการลักลอบตรวจจับการสื่อสาร

2.1.5.4 ความมั่นคงภายในหรือระดับภูมิภาค

ต่างถูกคุกคามโดยอาชญากรรมทางคอมพิวเตอร์ เนื่องจากลักษณะของอาชญากรรมทางคอมพิวเตอร์ ดำเนินการในระดับข้ามชาติ (Transnational) นานาประเทศจึงไม่สามารถจัดการปัญหานี้ได้ด้วยตนเอง แต่ต้องอาศัยความร่วมมือ ในระดับระหว่างประเทศเพื่อป้องกันภัยจากอาชญากรรมคอมพิวเตอร์ในระดับโลก

อาชญากรรมทางคอมพิวเตอร์มีแนวโน้มที่จะขยายตัวเข้าไปทำความเสียหายให้แก่ทุกภาคส่วนของสังคมเนื่องมาจากการบูรณาการเทคโนโลยีเข้าไปเป็นส่วนหนึ่งของชีวิตประจำวันและโครงสร้างขั้นพื้นฐานต่าง ๆ ยิ่งวิทยาการก้าวหน้าไปมากเท่าไร ความซับซ้อน หลากหลายของอาชญากรรมทางคอมพิวเตอร์ยิ่งมีมากขึ้นเป็นเงาตามตัว ดังนั้น กระบวนการยุติธรรม การแสวงหาหลักฐาน และการสืบสวนสอบสวน รวมทั้งข้อกฎหมายจึงต้องมีความเป็นพลวัตรเพียงพอให้เท่าทันกับอาชญากร เพื่อลดความเสียหายและผลกระทบที่อาจเกิดขึ้นจากการก่ออาชญากรรมให้มากที่สุด รวมทั้งสามารถตามจับผู้กระทำผิดมาลงโทษได้ตามกฎหมาย ทั้งนี้เนื่องจากอาชญากรรมคอมพิวเตอร์เป็นการกระทำผิดที่มีลักษณะเป็นอาชญากรรมระหว่างประเทศ จึงจำเป็นต้องสร้างความร่วมมือในระดับนานาชาติผ่านองค์กรระหว่างประเทศเพื่อสร้างมาตรฐานการที่จะมากำหนดแนวทางในการออกกฎเกณฑ์รวมถึง วิธีปฏิบัติของเจ้าหน้าที่และความช่วยเหลือซึ่งกันและกันระหว่างประเทศในการสืบสวนสอบสวนและจับกุมผู้กระทำผิดที่ชัดเจนและมีความเท่าทันต่อการกระทำความผิดของอาชญากร เพื่อคุ้มครองผลประโยชน์ของทุกภาคส่วนในสังคมไม่ว่าจะเป็นภาครัฐหรือเอกชน

2.2 แนวคิดเกี่ยวกับกฎหมายบนอินเตอร์เน็ต

การสื่อสารด้วยคอมพิวเตอร์ผ่านระบบเครือข่ายในระดับโลกก้าวข้ามเขตแดนระหว่างประเทศได้ สร้างอาณาเขตใหม่ที่มนุษย์เข้ามาใช้ทำกิจกรรมร่วมกัน แล้วดังนั้น สังคมที่เกิดขึ้นใหม่นี้จึงต้องการกฎเกณฑ์เพื่อใช้ในการกำกับดูแลให้เป็นระเบียบเรียบร้อย แม้ว่าเขตแดนใหม่นี้จะสร้างความสับสนระหว่างเขตแดนทางกายภาพและพรหมแดนที่ประกอบขึ้นจากเครือข่ายอิเล็กตรอนและโปรแกรมคอมพิวเตอร์ซึ่งแยกตัวเองออกจากโลกที่ประกอบไปด้วยอะตอมและวัตถุที่จับต้องได้ เขตแดนใหม่นี้ได้ให้นิยามความหมายใหม่ของดินแดนที่ต้องการสถาบันทางกฎหมายและการออกแบบข้อบังคับของตนเอง ซึ่งแนวคิดนี้จะเปลี่ยนแปลงนิยามต่าง ๆ ในกฎหมายรูปแบบเดิมที่อาศัยเขตแดนที่จับต้องได้เป็นหลัก (Territorial based law) และขัดแย้งกับนักกฎหมายที่เชื่อในแนวคิดทางกฎหมายแบบเดิมที่ผูกติดกับวัตถุหรือพื้นที่ทางกายภาพ แต่ด้วยธรรมชาติของไซเบอร์สเปซซึ่งประกอบไปด้วยเทคโนโลยีต่าง ๆ ที่เปลี่ยนแปลงอย่างรวดเร็วทำให้ยากต่อการนำนิยามซึ่งกำหนดขอบเขตทางกายภาพของกฎหมายรูปแบบเดิมมาปรับใช้ทำให้เกิดความตระหนักถึงความสำคัญของถึงแนวคิดในการสร้างหลักเกณฑ์เฉพาะเพื่อ นิยามความเป็นบุคคลและทรัพย์สิน การแก้ไขข้อขัดแย้ง และการชี้วัดถึงแก่นแท้ของคุณค่า (Core values) ของสิ่งต่าง ๆ บนไซเบอร์สเปซ

2.2.1 ที่มาและประวัติศาสตร์ของกฎหมายอาชญากรรมคอมพิวเตอร์

ตั้งแต่อินเตอร์เน็ตถูกนำมาเผยแพร่แก่สาธารณะชนเป็นครั้งแรกช่วงปลายทศวรรษที่ 60 (ค.ศ. 1969-1970)[46] คอมพิวเตอร์ในฐานะของอุปกรณ์จัดเก็บข้อมูลที่เชื่อมต่อกับระบบเครือข่ายซึ่งประกอบไปด้วยข้อมูลมหาศาล กลายเป็นเป้าหมายของภัยคุกคามทางอาชญากรรมรูปแบบใหม่ที่โลกไม่เคยพบเจอมาก่อน นั่นคือ “อาชญากรรมคอมพิวเตอร์”

2.2.1.1 อาชญากรรมทางคอมพิวเตอร์ยุคแรก

ในสมัยนั้นคอมพิวเตอร์ทำหน้าที่เป็นเพียงพื้นที่เก็บและประมวลผลข้อมูลขนาดใหญ่ซึ่งเชื่อมต่อฐานข้อมูลต่าง ๆ ของประชาชนแต่ละพื้นที่เข้าด้วยกัน โดยเฉพาะในสหรัฐอเมริกาที่หน่วยงานต่าง ๆ นำคอมพิวเตอร์เข้ามาเพื่อใช้จัดเก็บข้อมูลอย่างแพร่หลาย อย่างไรก็ดีการที่ข้อมูลต่าง ๆ ถูกรวมเข้าด้วยกันภายใต้การดูแลของรัฐทำให้เกิดข้อวิตกขึ้นว่ารัฐจะสามารถควบคุม ตรวจสอบ และจับตาดูประชาชนได้ตลอดเวลา และด้วยอิทธิพลของนิยายวิทยาศาสตร์เรื่อง 1984

---

[46] Ward, M., Celebrating 40 years of the net: Technology correspondent, *BBC News*, (2009, October 29), Retrieved 2013, October 8, from http://news.bbc.co.uk/2/hi/technology/8331253.stm

(Nineteen eighty four)[47] ซึ่งชี้ให้เห็นถึงอนาคตที่วิทยาการในการจัดการบริหารข้อมูลที่ทำให้เกิดประโยชน์ต่อการทำงานของมนุษย์แต่ก็ส่งผลให้รัฐใช้อำนาจเกินขอบเขตและล่วงล้ำสิทธิของประชาชน และเนื่องจากการที่คอมพิวเตอร์เป็นเพียงพื้นที่เก็บรวบรวมข้อมูลนี้เองทำให้การกระทำผิดเกี่ยวกับคอมพิวเตอร์ในยุคแรกหมายถึงการกระทำผิดใด ๆ ที่เป็นอันตรายต่อข้อมูล ที่อยู่ในระดับความลับของรัฐหรือความเป็นส่วนตัวของประชาชนเท่านั้น ดังนั้นข้อมูลจึงเป็นสิ่งที่กฎหมายมุ่งคุ้มครองเป็นหลัก โดยเฉพาะอย่างยิ่ง “ข้อมูลส่วนบุคคล” เช่น ความลับในวิชาชีพ ข้อมูลทางการแพทย์ ความลับของราชการ ข้อมูลทางการเงินการธนาคาร หรือข้อมูลด้านคดีความเป็นต้น ซึ่งความร้ายแรงของอาชญากรรมจะขึ้นอยู่กับชนิดของข้อมูลที่ถูกละเมิด ว่าเป็นของรัฐหรือเป็นเพียงข้อมูลส่วนบุคคล การจารกรรมข้อมูลข่าวสารที่เกี่ยวกับความมั่นคงของรัฐนั้นก่อให้เกิดอันตรายในวงกว้างกว่าการขโมยข้อมูลส่วนบุคคล เพื่อนำไปข่มขู่หรือรีดไถจากเจ้าของข้อมูล ยกตัวอย่าง เช่น คดีการขโมยข้อมูลการรักษา ผู้ป่วยโรคเอดส์ในประเทศแอฟริกาใต้ ซึ่งต่อมาข้อมูลนั้น ถูกส่งต่อไปยังผู้จ้างงานของผู้ป่วยจนเขาได้รับเสียหาย หรือคดีที่บริษัท IBM ถูกฟ้องร้องเมื่อปี ค.ศ. 1986 ว่าระบบความปลอดภัย (Resource Access Control Facility: RACF) อาจโดนพนักงานของบริษัทตรวจสอบโดยเจ้าของไม่อนุญาต[48] ดังนั้น อาชญากรรมคอมพิวเตอร์ในยุคแรกมีรูปแบบที่ไม่หลากหลายเช่นในปัจจุบันเนื่องจากข้อจำกัดของเทคโนโลยี โดยอาชญากรรมทางคอมพิวเตอร์ในยุคแรกจะมุ่งเป้าไปที่ข้อมูลคอมพิวเตอร์เป็นหลัก

ทั้งนี้เมื่อเวลาผ่านไปคอมพิวเตอร์ถูกนำไปใช้ในวงกว้างมากขึ้น ก่อให้เกิดช่องทางการก่ออาชญากรรมทางคอมพิวเตอร์โดยมุ่งหวังผลทางด้านเศรษฐกิจ เกิดเป็นอาชญากรรมทางเศรษฐกิจขึ้น โดยได้มีการเพิ่มศักยภาพอุปกรณ์ทางคอมพิวเตอร์ ที่ใช้เป็นอุปกรณ์ทางคอมพิวเตอร์เป็นอุปกรณ์เพื่อกระทำความผิดขึ้น

2.2.1.2 อาชญากรรมทางคอมพิวเตอร์ในฐานะอาชญากรรมทางเศรษฐกิจ

ทศวรรษที่ 70 (ช่วงปี ค.ศ. 1970-1980) ปัญหาการกระทำความผิดทางคอมพิวเตอร์ไม่ได้จำกัดขอบเขตให้อยู่ที่ประเด็นการกระทำความผิดต่อข้อมูลข่าวสารส่วนบุคคลอีกต่อไป รัฐทั้งหลายเริ่มหันมาให้ความสนใจในประเด็นปัญหา “อาชญากรรมทางเศรษฐกิจ” มากขึ้น โดยอาชญากรรมทางเศรษฐกิจนี้ถือว่ายังคงเป็นภัยทางอาชญากรรมคอมพิวเตอร์ที่โลกให้ความสำคัญเป็นอันดับต้น ๆ เนื่องจากรัฐทั้งหลายพบว่าสถิติการกระทำความผิดทางคอมพิวเตอร์ที่ส่งผลกระทบต่อเศรษฐกิจโดยรวมของประเทศโดยเฉพาะอย่างยิ่งในกลุ่มธุรกิจการเงิน เพิ่มจำนวนสูงขึ้นจนน่าวิตก

---

[47] Orwell, G., *Nineteen eighty-four, A novel*, (London: Secker & Warburg, 1949).

[48] Sieber, U., *The international handbook on computer crime*, (New York: Wiley, 1986), 23.

อาชญากรรมคอมพิวเตอร์ในยุคแรกนั้นอาจไม่ได้ก่อให้เกิดปัญหาในชีวิตหรือความปลอดภัยของประชาชน หรือก่อให้เกิดผลกระทบทางเศรษฐกิจโดยตรง แต่ในยุคสมัยต่อมาอาชญากรรมทางคอมพิวเตอร์ได้เคยถูกนำไปรวมอยู่ในกลุ่มของ “อาชญากรรมทางเศรษฐกิจ“ หรือ “อาชญากรรมคอเชิ้ตขาว (White collar crimes)” ซึ่งผู้กระทำความผิดเป็นกลุ่มผู้มีความรู้ความสามารถ ความหมายของอาชญากรรมทางเศรษฐกิจนั้นกว้างและครอบคลุมความผิดหลายประเภทเป็นการกระทำที่สร้างความเสียหายทั้งแก่ปัจเจกชนและสังคมส่วนรวม มีเป็นลักษณะเป็นการทำลายความเชื่อถือและความมั่นคงทางเศรษฐกิจ เช่น ความผิดเกี่ยวกับการปลอมแปลงเงินตรา, การปั่นหุ้น, ความผิดเกี่ยวกับภาษีอากร, ธุรกิจต่าง ๆ, สถาบันการเงิน เกี่ยวกับการค้า หรือธุรกิจเงินนอกระบบ เป็นต้น

หลังจากที่เทคโนโลยีอินเตอร์เน็ตเกิดขึ้นและได้รับการพัฒนาเรื่อยมา จนอินเตอร์เน็ตได้กลายเป็นส่วนสำคัญในการทำงานในหน่วยงานของรัฐ รวมทั้งผู้ดำเนินธุรกิจรายใหญ่ ทำให้เกิดช่องว่างให้อาชญากรสามารถใช้ความรู้และเครื่องมือทางคอมพิวเตอร์จารกรรมข้อมูลไปใช้ประโยชน์ทางธุรกิจของตน หรือสร้างความเสียหายต่อธุรกิจอื่น จากเดิมที่ การประกอบอาชญากรรมเศรษฐกิจโดยมักเป็นแค่เพียงการปลอมแปลงแก้ไขเอกสารบัญชีการเงินการธนาคารและเอกสารประเภทอื่น เท่านั้น ไม่มีเครื่องมือพิเศษช่วยเพิ่มศักยภาพในการกระทำความผิด ดังนั้นเทคโนโลยีคอมพิวเตอร์และเครือข่ายอินเตอร์เน็ตจึงทำให้อาชญากรรมทางเศรษฐกิจสามารถขยายขอบเขตไปสู่ความเสียหายต่อเศรษฐกิจในด้านอื่น ๆ จึงได้มีการจำแนกอาชญากรรมคอมพิวเตอร์ออกเป็นสองกลุ่มใหญ่ ได้แก่ กลุ่มที่ผู้กระทำอาศัยคอมพิวเตอร์เป็น “เครื่องมือ” และ กลุ่มที่ระบบคอมพิวเตอร์ และข้อมูลที่อยู่ในคอมพิวเตอร์เป็น “เป้าหมาย” ของผู้กระทำความผิด

โดยความผิดที่เป็นที่รู้จัก ได้แก่ การเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ การก่อวินาศกรรมคอมพิวเตอร์ หรือการกรรโชกรีดไถทางคอมพิวเตอร์, การเข้าไปในระบบโดยปราศจากอำนาจ รวมทั้งการละเมิดลิขสิทธิ์ต่าง ๆ เช่น เพลง หรือภาพยนตร์ ซอฟท์แวร์คอมพิวเตอร์ เป็นต้น

หลังจากเทคโนโลยีทางคอมพิวเตอร์ได้พัฒนาขึ้นจนสามารถเข้าถึงประชาชนและกลายเป็นส่วนหนึ่งของกิจวัตรประจำวัน เกิดบริการรูปแบบต่าง ๆ ขึ้นมากมายเพื่อรองรับความต้องการของผู้ใช้งานอินเตอร์เน็ต ซึ่งไม่จำกัดอยู่เพียงแต่รัฐหรือบริษัทใหญ่อีกต่อไป อินเตอร์เน็ตกลายเป็นแหล่งรวมของผู้คนที่เข้ามาเผยแพร่ผลงานสร้างสรรค์และแลกเปลี่ยนความคิดเห็นกันอย่างเสรีภายใต้ “บริการเครือข่ายสังคม (Social network service)[49]” ขึ้น และด้วยความใหญ่โตของ

---

[49] บริการเครือข่ายสังคม (social network service) เป็นรูปแบบของเว็บไซต์ ในการสร้างเครือข่ายสังคมสำหรับผู้ใช้งานในอินเทอร์เน็ต เขียนและอธิบายความสนใจ และกิจการที่ได้ทำ และเชื่อมโยงกับความสนใจและกิจกรรมของผู้อื่น.

เครือข่ายสังคมไร้เขตแดนที่ผู้คนจากทั่วโลกสามารถติดต่อสื่อสารกันได้อย่างอิสระ พื้นที่สาธารณะบนอินเตอร์เน็ตจึงกลายเป็นเป้าหมายของอาชญากรรมคอมพิวเตอร์ที่อาชญากรจะใช้คอมพิวเตอร์ในการกระทำความผิดโดยมีเป้าหมายไปที่ตัวผู้ใช้งานคอมพิวเตอร์และอุปกรณ์ที่เกี่ยวข้อง

2.2.1.3 การเผยแพร่เนื้อหาข้อมูลที่ไม่ชอบด้วยกฎหมายและอาชญากรรมไซเบอร์

ตั้งแต่ทศวรรษที่ 90 จนถึงปัจจุบัน อาชญากรรมคอมพิวเตอร์นั้นไม่ได้จำกัดอยู่เพียงแค่เฉพาะการละเมิดข้อมูลส่วนบุคคล หรือ อาชญากรรมที่ก่อให้ความเสียหายต่อเศรษฐกิจเท่านั้น แต่ยังรวมความไปถึงการกระทำความผิดต่อสิ่งที่กฎหมายประสงค์จะคุ้มครองในด้านอื่น ๆ ผ่านบริการทั้งหลายบนอินเทอร์เน็ตด้วย

หลังจากการใช้งานอินเตอร์เน็ตแพร่หลายในประชาชนทั่วไป การเผยแพร่ข้อมูลที่ไม่ชอบด้วยกฎหมายหลายประเภท เช่น ภาพลามกอนาจารเด็ก (Child pornography), การพนัน (Online gambling) หรือเผยแพร่ข้อมูลที่มีเนื้อหาแอบแฝงแนวคิดก้าวร้าว รุนแรง (Hate speech) หรือ แนวคิดในการดูหมิ่นชนชาติอื่น (Racism) การเลือกปฏิบัติ รวมทั้งการหมิ่นประมาท ผ่านบริการบนเครือข่ายอินเตอร์เน็ต โดยเฉพาะอย่างยิ่งบนเว็บไซท์ และบริการเครือข่ายสังคม (Social network service) ต่าง ๆ จึงเกิดเป็น “อาชญากรรมไซเบอร์” (Cybercrime) หรืออาชญากรรมคอมพิวเตอร์ซึ่งขยายขอบเขตไปสู่อินเตอร์เน็ตขึ้น

จากการสำรวจพบว่า เว็บไซท์ที่มีเนื้อหาเกี่ยวกับการดูหมิ่นชนชาติ เกิดขึ้นเป็นจำนวนมาก แม้เว็บไซท์ที่มีเนื้อหาลักษณะดังกล่าวจะถูกปิดไปแล้วจำนวนหนึ่ง แต่ก็ยังคงมีการลักลอบเผยแพร่แนวคิดทำนองดังกล่าวอยู่เป็นจำนวนไม่น้อย ทำให้ในปัจจุบันอาชญากรรมคอมพิวเตอร์ ได้ขยายขอบเขตผลกระทบไปสู่การสร้างความเสียหายแก่ประโยชน์สาธารณะ และส่งผลกระทบต่อค่านิยม แนวคิด สังคม รวมทั้งพัฒนาการของมนุษย์

2.2.1.4 ความผิดรูปแบบอื่น ๆ

นอกจากความผิดรูปแบบที่ดังกล่าวมาข้างต้น การกระทำความผิดที่มีคอมพิวเตอร์เข้ามาเกี่ยวข้องก็เริ่มมีจำนวนมากขึ้น จากสถิติพบว่าการเปลี่ยนแปลงข้อมูลทางคอมพิวเตอร์ (Computer manipulation)[50] หลายคดีผู้กระทำไม่ได้มุ่งหมายเพื่อผลประโยชน์ในทางทรัพย์สิน หรือสร้างความเสียหายด้านเศรษฐกิจเท่านั้น แต่มีเป้าหมายในการทำร้าย หรือละเมิด ชีวิต ร่างกายของเหยื่อผู้เสียหาย

---

[50] เปลี่ยนแปลงข้อมูลทางคอมพิวเตอร์ (Computer manipulation) แต่เดิมเป้าหมายหลัก ๆ ของผู้กระทำความผิดยังคงอยู่ที่บัญชีด้านการเงินการธนาคารของบริษัทและผู้ประกอบธุรกิจต่าง ๆ อาทิ การกระทำความผิดด้วยการเปลี่ยนแปลง หรือบิดเบือนข้อมูลการชำระเงิน, การเปลี่ยนแปลงรายรับ-รายจ่ายของบริษัท, การเปลี่ยนแปลงงบดุลบัญชีบริษัท, การเปลี่ยนแปลงรายการหรือสถานภาพการเงินของธนาคาร รวมทั้งการเปลี่ยนแปลงระบบ “บัญชีเงินสะสม” ของบริษัทต่าง ๆ ก็เกิดขึ้นเป็นจำนวนมากในระยะหลัง ๆ, สาวิตรี สุขศรี, *ประวัติศาสตร์ อาชญากรรมคอมพิวเตอร์*, สืบค้นเมื่อ 17 ตุลาคม 2555, จาก http://facthai.wordpress.com/2009/11/09/ประวัติศาสตร์-อาชญากรรม/

เช่น การเปลี่ยนแปลงข้อมูลการรักษาพยาบาลในฐานข้อมูลของโรงพยาบาล การทำลายระบบรักษาความปลอดภัย หรือข้อมูลการบินของอากาศยาน เป็นต้น อีกทั้งในปัจจุบันเทคโนโลยีคอมพิวเตอร์ยังถูกนำมาใช้เพื่อสร้างเสริมประสิทธิภาพการทำงาน หรือเพื่อความสะดวกในการติดต่อสื่อสารระหว่างอาชญากรในองค์กรอาชญากรรม และในขบวนการผู้ก่อการร้ายอีกด้วย

ตัวอย่างคดี ความผิดคอมพิวเตอร์ที่มีผลต่อชีวิตเคยเกิดขึ้นในประเทศอังกฤษราวปี ค.ศ. 1994 เมื่อนักเจาะระบบชาวอังกฤษคนหนึ่ง ทำการเจาะระบบฐานข้อมูลของโรงพยาบาลลิเวอร์พูล เพื่อสร้างความเสียหายแก่เครื่องบันทึกข้อมูล อย่างไรก็ตามเขาได้ทำการเปลี่ยนข้อมูลการให้ยารักษาคนไข้เด็กอายุ 9 ขวบรายหนึ่ง โชคดีที่นางพยาบาลผู้ดูแลตรวจสอบข้อมูลก่อน คนไข้เด็กจึงไม่ได้ตกเป็นเหยื่อการกระทำครั้งนั้น[51]

การเปลี่ยนแปลงข้อมูลในคอมพิวเตอร์ หรือการก่อวินาศกรรมคอมพิวเตอร์ (Computer sabotage)[52] จนทำให้การประมวลผลข้อมูลผิดพลาด ก็เคยสร้างปัญหาให้กับระบบการทำงานในกองทัพหลายต่อหลายครั้งเช่นกัน ซึ่งหากกองทัพไม่เร่งหาทางป้องกันระบบฐานข้อมูลเหล่านี้ให้แน่นหนา ในอนาคตความเสียหายที่เกิดขึ้นอาจไม่เพียงแต่ตัวระบบความปลอดภัยของกองทัพเท่านั้น แต่อาจร้ายแรงถึงขนาดก่อให้เกิดสงครามกับประเทศอื่นโดยไม่ตั้งใจ โดยเฉพาะอย่างยิ่งประเทศที่ฝากระบบการจัดการด้านกองกำลัง และอาวุธส่วนใหญ่ไว้กับเทคโนโลยีชนิดนี้[53] ดังตัวอย่างหนึ่งที่เคยเกิดขึ้นกับกองทัพสหรัฐในปี ค.ศ. 1995 ครั้งนั้น ผลจากการถูกเจาะระบบเปลี่ยนแปลงข้อมูลผ่านอินเทอร์เน็ต เป็นผลให้กองทัพเรือสหรัฐ ส่งเรือรบไปยังสถานที่หนึ่งซึ่งผิดไปจากเป้าหมายถึง 7 ลำ เป็นต้น

ปัญหาการปรับใช้กฎหมายกับอาชญากรรมทางคอมพิวเตอร์ในปัจจุบันนั้น เกิดขึ้น โดยเมื่อเริ่มเมื่อมีการให้ความสำคัญกับข้อมูลข่าวสารส่วนบุคคล จนเกิดกฎหมายเพื่อ คุ้มครองข้อมูลส่วนบุคคล และคุ้มครองสิทธิความเป็นส่วนตัวขึ้นในหลายประเทศ ต่อมาฐานข้อมูลทางเศรษฐกิจ โปรแกรมคอมพิวเตอร์ ระบบความปลอดภัยทางคอมพิวเตอร์ เนื้อหาดิจิตอล ไปจนถึงความมีเสถียรภาพของเศรษฐกิจโดยรวมได้กลายเป็นประเด็นสำคัญที่ต้องคุ้มครองเป็นพิเศษ มาจนถึง

---

[51] สาวิตรี สุขศรี, *ประวัติศาสตร์ อาชญากรรมคอมพิวเตอร์*.

[52] การก่อวินาศกรรมคอมพิวเตอร์ (Computer sabotage) ความผิดส่วนใหญ่ที่เกิดขึ้นมักเป็นการกระทำต่อคอมพิวเตอร์ส่วนบุคคล ด้วยวิธีปล่อยโปรแกรมไวรัสหรือวอร์มทำลายระบบหรือข้อมูลคอมพิวเตอร์เท่านั้น ส่วนการก่อวินาศกรรมที่สร้างความเสียหายกับบริษัทใหญ่ ๆ มีจำนวนไม่มากนัก การกระทำความผิดในลักษณะนี้ เริ่มขยายตัวมากขึ้นภายหลังจากระบบเครือข่ายคอมพิวเตอร์ได้รับการพัฒนา ทั้งนี้เพราะผู้กระทำความผิดเขียนโปรแกรมทำลายแค่เพียงครั้งเดียวแต่สามารถส่งต่อ เผยแพร่ สร้างความเสียหายให้เหยื่อได้จำนวนมาก ไวรัสที่มีเป้าหมายในการทำลายล้างหรือเพื่อก่อวินาศกรรม (Sabotage), เรื่องเดียวกัน.

[53] เรื่องเดียวกัน.

ปัจจุบันที่รูปแบบและนวัตกรรมใหม่ที่เกิดขึ้นด้วยเครื่องมือทางเทคโนโลยีสำหรับ ปัญหาประเภทความแตกต่างระหว่างคำนิยามของ เอกสาร กับ ฐานข้อมูล, การบุกรุกทางกายภาพ กับ การเจาะระบบคอมพิวเตอร์ ไปจนถึง การลักทรัพย์ที่มีรูปร่าง กับการจารกรรม ทำซ้ำข้อมูลคอมพิวเตอร์ ทำให้แต่ละประเทศต้องดำเนินการแก้ไขปรับปรุงกฎหมายภายในให้มีความทันสมัยอยู่ตลอดเวลา และเมื่ออินเตอร์เน็ตกลายเป็นส่วนหนึ่งของชีวิตประจำวันของมนุษย์ การเผยแพร่สิ่งผิดกฎหมาย หมิ่นประมาท และปลูกฝังความเกลียดชัง ก่อให้เกิดผลกระทบต่อสังคม ทั้งในด้านของค่านิยม และแนวคิด และอาจทำให้เกิดความเสียหายต่อร่างกายและชีวิตได้ และเนื่องจากการกระทำทั้งหมดมีลักษณะไร้พรหมแดนตามธรรมชาติของอินเตอร์เน็ตที่เป็นระบบเครือข่ายสากลยากแก่การหาตัวผู้กระทำผิด ทำให้การกำหนดความผิดไม่สำคัญเท่ากับ การออกแบบกฎหมายเพื่อกำหนดวิธีการสืบสวนสอบสวน ค้นหาพยานหลักฐานอิเล็กทรอนิกส์ เพื่อติดตามตัวผู้กระทำความผิด ที่เป็นความร่วมมือระหว่างประเทศทั้งในระดับภูมิภาคและระดับโลกเช่น อนุสัญญาอาชญากรรมคอมพิวเตอร์ (Convention on cybercrime) ที่ออกโดยคณะมนตรียุโรป (Council of Europe) ฯลฯ

อย่างไรก็ดี ความรวดเร็วของพัฒนาการด้านนวัตกรรมของเทคโนโลยีคอมพิวเตอร์และอินเตอร์เน็ต ก่อให้เกิดปัญหาในการปรับปรุงกฎหมายให้เท่าทันต่อความเปลี่ยนแปลงที่เกิดขึ้นทำให้เกิดช่องทางการกระทำผิดที่มีความซับซ้อนมากขึ้นเรื่อย ๆ อีกทั้งปัจจุบันแนวโน้มที่ภาคส่วนต่าง ๆ ของสังคม จะนำเทคโนโลยีคอมพิวเตอร์ไปใช้เป็นส่วนประกอบ หรือเป็นส่วนหนึ่งของระบบควบคุม จัดการ เพื่อพัฒนาศักยภาพการทำงานให้ดียิ่งขึ้นนั้น มีสูงขึ้นอย่างต่อเนื่อง ไม่ว่าจะเป็นด้านสาธารณูปโภค เช่น ประปา ไฟฟ้า การขนส่ง คมนาคม การศึกษา การทหาร และการสื่อสาร ทั้งนั้นเมื่อหลายสิ่งมีแนวโน้มที่จะถูกควบคุมโดยคอมพิวเตอร์ ความหลากหลายซับซ้อนของอาชญากรรมทางคอมพิวเตอร์ซึ่งแปรผันตรงกับความก้าวหน้าทางวิทยาการจึงสามารถพัฒนาต่อไปได้อีกเรื่อย ๆ

2.2.2 ขอบเขตและแนวคิดในการกำกับดูแลอินเตอร์เน็ต

การเกิดขึ้นของไซเบอร์สเปซได้ก่อให้เกิดผลกระทบทางด้านกฎหมายเพราะในกรอบความคิดแบบดั้งเดิมนั้นการใช้อำนาจทางกฎหมายในการกำกับดูแลสังคมจะผูกติดกับตำแหน่งทางกายภาพระหว่างทำเลที่ตั้งทางภูมิศาสตร์ แต่ไซเบอร์สเปซเป็นเขตแดนเสมือนที่ไม่สามารถจับต้องได้ ดังนั้น การแผ่ขยายและความซับซ้อนที่เพิ่มมากขึ้นของระบบเครือข่ายคอมพิวเตอร์ได้ทำให้จุดเกาะเกี่ยวในทางกฎหมายระหว่างทำเลที่ตั้งทางภูมิศาสตร์และอำนาจในการบังคับใช้กฎหมายของผู้ปกครองในการเข้ามาควบคุมพฤติกรรมของผู้ใช้ระบบเครือข่ายคอมพิวเตอร์เปลี่ยนไป ซึ่งส่งผลกระทบต่อความชอบธรรมของการใช้อำนาจอธิปไตยในการบังคับใช้กฎเกณฑ์ที่มีอยู่เดิมกับพฤติกรรมบนอินเตอร์เน็ตของบุคคลในปัจจุบัน

ธรรมชาติของอินเตอร์เน็ตนั้นขัดแย้งกับระบบการสร้างกฎหมายเดิมที่อาศัยหลักที่มีพื้นฐานว่าด้วยดินแดนอาณาเขตระหว่างพื้นที่ทางกายภาพ อย่างน้อยก็ขัดกับหลักการที่เกี่ยวข้องกับแนวคิดที่ว่าไซเบอร์สเปซต้องการการกำกับดูแลโดยกฎที่มีพื้นฐานการให้คำนิยามบนเขตแดนทางกายภาพ เพราะคอนเซปท์ของการเคลื่อนไหวของข้อมูลบนระบบเครือข่ายเป็นอิสระจากตำแหน่งพื้นที่ทางกายภาพ ข้อมูลสามารถถูกส่งจากจุดหนึ่งไปยังจุดหนึ่งอย่างรวดเร็วจนไม่สามารถชี้วัดแนวความคิดว่าด้วย "ระยะทาง" บนพรหมแดนไซเบอร์ได้ ซึ่งต่างจากพื้นที่ทางภูมิศาสตร์ที่มีระยะทางที่แน่นอนและสามารถเป็นตัวชี้วัดขนาดของพื้นที่และคนที่อยู่บนพื้นที่นั้นได้ อินเตอร์เน็ตทำให้เกิดการสื่อสารกันระหว่างบุคคลที่ต่างฝ่ายไม่อาจระบุตำแหน่งของแต่ละฝ่ายได้อย่างชัดเจนแน่นอน ดังนั้นจึงก่อให้เกิดปัญหาขึ้นมากมาย

เนื่องจากพัฒนาการทางเทคโนโลยีที่แผ่ขยายเข้าไปยังทุกภาคส่วนของสังคมและถูกนำไปใช้อย่างแพร่หลายในระดับโลกจึงมีแนวคิดในการที่จะจัดระเบียบสังคมอินเตอร์เน็ตขึ้นเป็นแนวคิดในเรื่องการกำกับดูแลอินเตอร์เน็ต (Internet governance) ซึ่งได้ถูกนำมาอภิปรายกันอย่างกว้างขวางในการประชุมนานาชาติหลายเวที เช่น การประชุมสุดยอดของโลกว่าด้วยการสื่อสาร (World Summit on Information Society: WSIS) ซึ่งจัดขึ้น ณ กรุงเจนีวา ประเทศสวิสเซอร์แลนด์ในเดือนธันวาคม พ.ศ. 2546 ฯลฯ

อย่างไรก็ดี เนื่องจากไม่ได้มีการให้คำนิยามคำว่า "การกำกับดูแลอินเตอร์เน็ต" และขอบเขตที่ชัดเจน ตลอดจนมุมมองที่แตกต่างกันของรัฐบาลประเทศต่าง ๆ ต่อกติกาที่เหมาะสมในการกำกับดูแลอินเตอร์เน็ต ที่ประชุมสุดยอดของโลกว่าด้วยสังคมข้อมูลข่าวสาร ครั้งที่ 1 จึงไม่สามารถหาข้อยุติสำหรับประเด็นดังกล่าวได้ และมีมติให้จัดตั้งคณะทำงานเรื่องการกำกับดูแลอินเตอร์เน็ต (The working group on internet governance: WGIG) ขึ้น เพื่อศึกษาประเด็นเชิงนโยบายที่เกี่ยวข้อง ตลอดจนท่าทีของผู้มีส่วนเกี่ยวข้องรวมทั้งประเทศต่าง ๆ ในประเด็นเรื่องการกำกับดูแลอินเตอร์เน็ต เพื่อนำมาพิจารณาต่อไปเป็นการประชุมใหญ่ครั้งที่ 2 ณ กรุงตูนิส ประเทศตูนีเซียในเดือนมิถุนายน พ.ศ. 2548[54] โดยการประชุมครั้งที่ 2ของการประชุมสุดยอดของโลกว่าด้วยสังคมข้อมูลข่าวสาร คณะทำงานด้านการกำกับดูและอินเตอร์เน็ต ได้ให้คำนิยาม "การกำกับดูแลอินเตอร์เน็ต" ไว้ในรายงานฉบับเดือนมิถุนายน พ.ศ. 2548 มีใจความดังนี้

"การกำกับดูแลอินเตอร์เน็ตนั้นเป็นการที่ภาครัฐและเอกชน รวมทั้งภาคประชาสังคมได้คำนึงถึงกฎเกณฑ์ต่าง ๆ ที่เกี่ยวกับหลักเกณฑ์ต่าง ๆ ที่ใช้ร่วมกัน ประเพณีปฏิบัติ กฎเกณฑ์

---

[54] Regional Internet Governance Forum, *About APrIGF 2011*, (2011, July 13), Retrieved 2011, July 13, from http://2011.rigf.asia/

กระบวนการตัดสินใจ และโครงการเพื่อกำหนดทิศทางของวิวัฒนาการและการใช้ประโยชน์จากอินเตอร์เน็ต"[55]

สำหรับในเวทีระดับภูมิภาค ภาคประชาสังคมอาเซียนและเครือข่ายพลเมืองเน็ตได้ร่วมกันจัดการประชุมเรื่องการกำกับดูแลอินเตอร์เน็ตใน "เวทีภูมิภาคเอเชียแปซิฟิก" (Asia-pacific Regional Internet Governance Forum: APrIGF) ครั้งที่ 1 เมื่อวันที่ 15 และ 16 มิถุนายน พ.ศ. 2553 ณ เขตการปกครองพิเศษฮ่องกง (Hong Kong Special Administrative Region: SAR)[56] โดยภายหลังการประชุมดังกล่าว ภาคประชาสังคมอาเซียนและเครือข่ายพลเมืองเน็ต ได้ออก "แถลงการณ์ประชาสังคมเอเชียตะวันออกเฉียงใต้ ค.ศ. 2010 (พ.ศ. 2553) ว่าด้วยการกำกับดูแลอินเตอร์เน็ต" (2010 Southeast Asia Civil Society Statement on Internet Governance) เพื่อนำเสนอต่อต่อหน่วยงานต่าง ๆ ที่เกี่ยวข้องทั้งในประเทศของตน และในระดับนานาชาติ โดยเฉพาะอย่างยิ่งการนำเสนอต่อที่ประชุมว่าด้วยการกำกับดูแลอินเตอร์เน็ต (Internet Governance Forum: IGF) ซึ่งเป็นที่ประชุมพหุภาคีระดับโลก ณ กรุงเจนีวา เมื่อวันที่ 28-29 มิถุนายน พ.ศ. 2553 โดยแถลงการณ์ดังกล่าวนี้ได้ระบุถึงประเด็นเร่งด่วนของการกำกับดูแลอินเตอร์เน็ตในภูมิภาคนี้ทั้งสามประเด็น คือ ความเปิดเผย การเข้าถึง และสิทธิในความเป็นส่วนตัว

นอกจากนั้นยังมีข้อเสนอถึงที่ประชุมว่าด้วยการกำกับดูแลอินเตอร์เน็ต ที่จัดขึ้นระหว่างวันที่ 14-17 กันยายน พ.ศ. 2553 ณ กรุงวิลนีอุส ประเทศลิทัวเนีย โดยมีเนื้อหาสาระสำคัญ คือ ขอให้ที่ประชุมว่าด้วยการกำกับดูแลอินเทอร์เน็ตคำนึงถึงหลักการสำคัญของการประชุมสุดยอดโลกว่าด้วยสังคมข้อมูลข่าวสาร ดังนี้ "สังคมสารสนเทศนั้นจะต้องให้คนเป็นศูนย์กลาง ไม่เลือกปฏิบัติ คารพหลักสิทธิมนุษยชนสากล ทั้งตระหนักถึงกฎหมายที่จำกัดเสรีภาพในการแสดงออกในประเทศกำลังพัฒนา และให้สนับสนุนการมีส่วนร่วมจากคนทั่วไปผ่านเทคโนโลยี เช่น Webcast twitter หรือ การประชุมวีดีโอทางไกล นอกจากนี้ กระบวนการกำกับดูแลจะต้องเป็นไปอย่างโปร่งใส เป็นประชาธิปไตย และมาจากการมีส่วนร่วมของทุกภาคส่วน ตลอดจนที่ประชุมระดับโลกว่าด้วยการกำกับดูแลอินเตอร์เน็ต ZIGFX และเวทีการประชุมทั้งระดับโลก ระดับภูมิภาค และระดับประเทศควรมีรูปแบบ เวลา และกระบวนการที่เปิดกว้างให้ทุกภาคส่วนสามารถมีส่วนร่วมได้โดยสะดวก"[57] และต่อมาเมื่อวันที่ 16 และ 17 มิถุนายน พ.ศ. 2554 ภาคประชาสังคมอาเซียนและเครือข่าย

---

[55] Regional Internet Governance Forum, *About APrIGF 2011*.

[56] "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.", Ibid.

[57] สราวุธ ปิติยาศักดิ์, *กฎหมายเทคโนโลยีสารสนเทศ*, (กรุงเทพฯ: นิติธรรม, 2555), 12.

พลเมืองเน็ตได้ร่วมกันจัดประชุมเรื่องการกับดูแลอินเตอร์เน็ตในเวทีภูมิภาคเอเชียแปซิฟิก ครั้งที่ 2 ณ ประเทศสิงคโปร์ ต่อมาที่ประชุมระดับโลกว่าด้วยการกำกับดูแลอินเตอร์เน็ต จัดให้มีการประชุมที่ประเทศเคนยา ระหว่างวันที่ 27-30 กันยายน พ.ศ. 2554[58]

สำหรับประเทศไทย ฝ่ายพัฒนานโยบายและกฎหมาย ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (National Electronic and Computer Technology Center: NECTEC) ตระหนักถึงความจำเป็นในการศึกษาวิจัยในประเด็นเกี่ยวกับการกำกับดูแลอินเตอร์เน็ต จึงจัดให้มีโครงการศึกษาวิจัยการกำกับดูแลอินเตอร์เน็ต ขึ้น เพื่อติดตามความคืบหน้าของประเด็นดังกล่าวอันเป็นผลสืบเนื่องมาจากการประชุมสุดยอดโลกว่าด้วยสังคมข้อมูลข่าวสาร ครั้งที่ 1 และครั้งที่ 2 ตลอดจนจัดทำข้อมูลที่เกี่ยวข้องและจัดทำข้อเสนอแนะในการกำหนดท่าทีของประเทศไทยต่อเรื่องดังกล่าวในการประชุมสุดยอดโลกว่าด้วยสังคมข้อมูล และข้อเสนอแนะแนวทางการวางกรอบนโยบายสำหรับการกำกับดูแลอินเตอร์เน็ตในประเทศไทย[59]

อนึ่ง กระบวนการกำกับดูแลอินเตอร์เน็ตของคณะทำงานเรื่องการกำกับดูแลอินเตอร์เน็ตของ WGIG เป็นกระบวนการสหวิทยาการ (Multidisciplinary approach) จึงกล่าวถึงหลักการกำกับดูแลอินเตอร์เน็ตในหลายมิติ ทั้งทางเทคนิค นโยบาย เศรษฐศาสตร์ สถาบัน และกฎหมาย ถึงแม้ว่าประเด็นทางกฎหมายจะมิใช่ประเด็นแรกของการพิจารณาในการกำกับดูแลอินเตอร์เน็ตของคณะทำงานเรื่องการกำกับดูแลอินเตอร์เน็ต แต่ประเด็นทางกฎหมายก็ได้รับการยอมรับว่าเป็นส่วนหนึ่งของการกำกับดูแลอินเตอร์เน็ต คณะทำงานเรื่องการกำกับดูแลอินเตอร์เน็ต ได้อภิปรายในข้อกฎหมายเกี่ยวกับการกำกับดูแลอินเตอร์เน็ตและรายงานต่อที่ประชุมสุดยอดโลกว่าด้วยข้อมูลข่าวสาร ในสองเรื่องด้วยกัน ได้แก่ ประเด็นกฎหมายที่เกี่ยวกับอินเตอร์เน็ต ได้แก่ อาชญากรรมทางคอมพิวเตอร์ การละเมิดทรัพย์สินทางปัญญาบนเครือข่ายอินเตอร์เน็ต การคุ้มครองข้อมูลส่วนบุคคลบนเครือข่ายอินเตอร์เน็ต สิทธิส่วนบุคคลบนเครือข่ายอินเตอร์เน็ตรวมทั้งสิทธิของผู้บริโภคบนเครือข่ายอินเตอร์เน็ต และ กลไกทางกฎหมายสำหรับการกำกับดูแลอินเตอร์เน็ต ได้แก่ กฎเกณฑ์ควบคุมตนเองของกิจการบนเครือข่ายอินเตอร์เน็ต (Self-regulation) อนุสัญญาระหว่างประเทศ (International affairs)[60] และเขตอำนาจศาล

---

[58] 2011 IGF Nairobi, *Internet Governance Forum*, Retrieved 2013, December 26, from www.intgov forum.org/cms/2011-igf-nairobi.

[59] ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, *โครงการศึกษาวิจัยการอภิบาลกิจการเกี่ยวกับอินเตอร์เน็ต*, สืบค้นเมื่อ 13 กรกฎาคม 2555, จาก http://www.nectec.or.th/pld/igovernanace/index.htm.

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

ภายหลังที่ประชุมสุดยอดโลกว่าด้วยสังคมข้อมูลข่าวสาร ได้รับรายงานจากคณะทำงานเรื่องการกำกับดูแลอินเตอร์เน็ต จึงนำเสนอถึงกลไกทางกฎหมายที่เหมาะสมสำหรับการกำกับดูแลอินเตอร์เน็ต โดยเน้นประเด็นทางกฎหมายเกี่ยวกับกระบวนการและวิธีการสำหรับการกำกับดูแลอินเตอร์เน็ตภายใต้กรอบกฎหมายภายในประเทศและกฎหมายระหว่างประเทศ โดยประเด็นดังกล่าว ได้แก่ กระบวนการมีส่วนร่วมของผู้มีส่วนได้เสีย (Stakeholders) ในการกำกับดูแลอินเตอร์เน็ต เครื่องมือทางกฎหมายระหว่างประเทศที่เหมาะสมในการกำกับดูแลอินเตอร์เน็ต ตลอดจนความสัมพันธ์ระหว่างกฎหมายระหว่างประเทศแผนกคดีเมืองและแผนกคดีบุคคลภายใต้กรอบการกำกับดูแลอินเตอร์เน็ต[61] ปัจจุบันมุมมองเกี่ยวกับกลไกทางกฎหมายที่เหมาะสมในการกำกับดูแลอินเตอร์เน็ตแบ่งได้ 2 กระบวนทัศน์ (Paradigms) ได้แก่

2.2.2.1 กระบวนทัศน์ในทางบวก (Techno-optimism)

ผู้สนับสนุนกระบวนทัศน์นี้สนับสนุนพัฒนาการของกฎหมายไซเบอร์ (Cyber law) โดยเห็นว่าอินเตอร์เน็ตเป็นวิธีการสื่อสารสมัยใหม่ เป็นการสื่อสารไร้พรหมแดน ทำให้เกิดอุปสรรคต่อกฎหมายที่บังคับใช้อยู่ ฉะนั้นกฎหมายไซเบอร์จึงมีความจำเป็นอย่างยิ่งและต้องการการพัฒนาที่ต่อเนื่อง[62]

2.2.2.2 กระบวนทัศน์เทคโนตามความเป็นจริง (Techno-realist)

ผู้สนับสนุนกระบวนทัศน์นี้เห็นว่าอินเตอร์เน็ตไม่ได้แตกต่างจากเทคโนโลยีการสื่อสารที่มีมาก่อน เช่น โทรศัพท์ ฯลฯ เพียงแต่อินเตอร์เน็ตมีความสะดวกและรวดเร็วกว่าและครอบคลุมระยะทางได้กว้างขวางกว่าเท่านั้น ฉะนั้นกฎหมายที่บังคับอยู่ในปัจจุบันจึงนำมาใช้กับอินเตอร์เน็ตได้[63] อย่างไรก็ดีในบางประเด็นที่เป็นเรื่องเฉพาะ เช่น กรณีกฎหมายเครื่องหมายการค้าซึ่งจำเป็นต้องมีการปรับปรุงกฎหมายปัจจุบันเพื่อให้ปรับใช้กับอินเตอร์เน็ตได้อย่างเหมาะสม และกรณีปัญหาที่เป็นเรื่องที่เกิดขึ้นใหม่ ก็จำเป็นต้องมีการบัญญัติกฎหมายสำหรับปัญหาเฉพาะนั้น ๆ เช่น การส่งสแปมเมล์หรือจดหมายอิเล็กทรอนิกส์ขยะ (Spam mail or Junk mail) ซึ่งยังคงเป็นปัญหาที่สำคัญภายใต้กฎหมายของหลายประเทศรวมทั้งประเทศไทย

ลักษณะพิเศษประการสำคัญของอินเตอร์เน็ต คือ เป็นการติดต่อสื่อสารไร้พรหมแดน จึงมีการอภิปรายถึงความจำเป็นที่จะมีหลักเกณฑ์ระดับโลกหรือกฎหมายระหว่างประเทศบังคับใช้สำหรับอินเตอร์เน็ต ผู้สนับสนุนแนวคิดนี้เห็นว่าอินเตอร์เน็ตมีลักษณะพิเศษเฉพาะที่จะต้องมีหลักเกณฑ์ระดับโลกหรือกฎหมายระหว่างประเทศในการกำกับดูแล เพราะกฎหมายภายในของแต่

---

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

[62] เรื่องเดียวกัน, 13.

[63] เรื่องเดียวกัน, 14.

ละประเทศไม่อาจบังคับใช้ได้อย่างมีประสิทธิภาพ กรณีตัวอย่างที่สนับสนุนความเห็นนี้ คือ กรณีแฮกเกอร์ซึ่งอาศัยอยู่ประเทศฟิลิปปินส์ได้ส่งหนอนคอมพิวเตอร์ชื่อว่า “ILOVEYOU” ซ่อนไปกับจดหมายอิเล็กทรอนิกส์ เพื่อโจมตีเครื่องคอมพิวเตอร์นับล้านเครื่องทั่วโลกในปี ค.ศ. 2000[64] การกระทำดังกล่าวก่อให้เกิดความเสียหายแก่ผู้ใช้คอมพิวเตอร์จำนวนมากในหลายประเทศแต่ผู้เสียหายไม่สามารถฟ้องร้องแฮกเกอร์ผู้นั้นได้เพราขณะนั้นการกระทำดังกล่าวไม่เป็นความผิดตามกฎหมายอาญาฟิลิปปินส์[65]

อย่างไรก็ดี แม้หลักเกณฑ์ระดับโลกเป็นสิ่งสำคัญ แต่กฎเกณฑ์ระดับภูมิภาคและระดับประเทศน่าจะมีความสำคัญมากกว่า เพราะในปัจจุบันอินเตอร์เน็ตมีลักษณะที่ยึดโยงกับภูมิประเทศมากขึ้น อุปกรณ์สมัยใหม่สามารถสืบค้นและระบุตำแหน่งที่ตั้งทางภูมิศาสตร์ของผู้ใช้อินเตอร์เน็ตได้ ยิ่งไปกว่านั้น ยังมีการพัฒนาเครื่องมือที่สามารถจำกัดการใช้บริการอินเตอร์เน็ตเฉพาะผู้ใช้บริการที่อยู่ในประเทศหนึ่ง ๆ ได้ นอกเหนือจากเทคโนโลยีแล้ว การเพิ่มมาตรการทางกฎหมายก็มีส่วนกดดันให้ผู้ให้บริการทางอินเตอร์เน็ต (Internet Service Providers: ISP) ต้องเก็บข้อมูลส่วนตัวของผู้ใช้บริการทางอินเตอร์เน็ตและเปิดเผยข้อมูลให้แก่พนักงานเจ้าหน้าที่ผู้มีอำนาจ ด้วยพัฒนาการทางเทคโนโลยีและกฎหมายดังกล่าว ทำให้อินเตอร์เน็ตกลายเป็นสื่อที่เปิดเผยตัวผู้ใช้มากขึ้น รัฐบาลในหลายประเทศจึงเห็นด้วยกับการประสานกันระหว่างเทคโนโลยีและกฎหมาย ดังนั้นกลไกในการกำกับดูแลอินเตอร์เน็ตที่เป็นการเฉพาะ (Unique Governance) จึงมีความจำเป็นน้อยลง[66]

นอกจากนี้ วิธีการที่ทรงประสิทธิภาพที่สุดในการกำหนดหลักเกณฑ์ระดับโลกในการกำกับดูแลอินเตอร์เน็ตคือการทำให้กฎหมายแต่ละประเทศเป็นเอกภาพหรือเป็นอันหนึ่งอันเดียวกันที่มีลักษณะเป็นกฎหมายสากล (Universal Law) โดยควรมีการยกร่างกฎหมายแม่แบบ (Model Law) เพื่อให้แต่ละประเทศนำไปบัญญัติเป็นกฎหมายภายใน เมื่อกฎหมายภายในของแต่ละประเทศทั่วโลกเป็นเอกภาพแล้ว ผลทางกฎหมายในเรื่องเดียวกันที่ตัดสินในแต่ละประเทศก็จะไม่แตกต่างกัน การทำให้กฎหมายเป็นเอกภาพนี้จะประสบความสำเร็จหากเป็นที่ยอมรับของประชาคมโลก ตัวอย่างเช่นในประเด็นเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ คณะกรรมาธิการการค้าระหว่างประเทศแห่งสหประชาชาติ (United Nations Commission on International Trade Law: UNCITRAL) ได้จัดทำกฎหมายแม่แบบ มีชื่อว่า “UNCITRAL Model Law on Electronic Commerce 1996” เพื่อเป็น

---

[64] U.S. catches “Love” virus, *CNN Money*, Retrieved 2014, March 31, from http://money.cnn.com/2000/05/05/technology/loveyou/

[65] Kurbalijia, J., *Internet governance and international law*, Retrieved 2013, October 17, from http://www.wgig.org/docs/book/Jovan_Kurbalija%20.pdf

[66] Ibid.

แม่แบบสำหรับนานาประเทศทั่วโลกใช้เป็นตัวอย่างในการบัญญัติกฎหมายภายในของแต่ละประเทศ ซึ่ง UNCITRAL Model Law on Electronic Commerce 1996 ได้เป็นแม่แบบของกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ของประเทศชั้นนำต่าง ๆ ทั่วโลกเช่น ประเทศสหรัฐอเมริกา ประเทศสิงคโปร์ ประเทศออสเตรเลีย เขตปกครองพิเศษฮ่องกง รวมทั้งประเทศไทยด้วย

ในอนาคต ปัญหาจดหมายอิเล็กทรอนิกส์ขยะ (Spam mail) ปัญหาเว็บไซต์ลามก ปัญหาเว็บไซต์การพนัน ปัญหาการฉ้อโกงบนเครือข่ายอินเตอร์เน็ต และอื่น ๆ ก็อาจได้รับการยอมรับจากประชาคมโลกในความจำเป็นที่จะต้องมีกฎหมายเอกภาพเป็นแม่แบบในการกำกับดูแลในอนาคตเช่นกัน

2.2.3 เขตอำนาจศาลบนเครือข่ายอินเตอร์เน็ต (Internet Jurisdiction)

ลักษณะของระบบเครือข่ายอินเตอร์เน็ตกับกฎหมายมีความแตกต่างกันเป็นนัยสำคัญ กล่าวคือ ระบบอินเตอร์เน็ตถูกสร้างขึ้นเพื่อให้บุคคลจากสถานที่หนึ่งหรือประเทศหนึ่งสามารถติดต่อสื่อสารกับบุคคลที่อยู่อีกสถานที่หนึ่งหรืออีกประเทศหนึ่งที่อยู่ห่างออกไปแม้คนละซีกโลก ระบบอินเตอร์เน็ตจึงเป็นเรื่องของกิจกรรมที่ไร้พรหมแดน (Without national boundary) ในขณะที่กฎหมายถูกบัญญัติขึ้นเพื่อใช้กับบุคคลหรือกิจกรรมที่อยู่ภายในเขตพรหมแดนของประเทศใดประเทศหนึ่งเท่านั้น กฎหมายจึงเป็นเรื่องของกิจการภายในดินแดนอาณาเขตของของแต่ละประเทศ (Within national boundary) ความแตกต่างอันเป็นนัยสำคัญระหว่างระบบเครือข่ายอินเตอร์เน็ตกับกฎหมายนี้ก่อให้เกิดประเด็นปัญหาเรื่องเขตอำนาจศาล กล่าวคือ โดยปกติศาลของประเทศใดประเทศหนึ่งจะมีอำนาจเหนือจำเลยในกิจกรรมหรือการกระทำที่เกิดขึ้นภายในประเทศนั้นเท่านั้น แต่การกระทำอันขัดต่อกฎหมายผ่านทางระบบเครือข่ายอินเตอร์เน็ตส่วนใหญ่มักเกิดขึ้นจากผู้กระทำที่อยู่นอกเขตแดนของประเทศนั้น ตัวอย่างเช่นการที่บุคคลอยู่ในต่างประเทศเขียนข้อความหมิ่นประมาทแล้วโพสข้อความดังกล่าวบนเครือข่ายอินเตอร์เน็ต ทำให้ผู้เสียหายที่อยู่ในประเทศไทยได้รับความเสียหาย หรือการที่แฮกเกอร์ที่อยู่ต่างประเทศเจาะระบบของผู้เสียหายที่อยู่ในประเทศไทย เช่นนี้ ศาลไทยจะมีเขตอำนาจศาลในการพิจารณาพิพากษาคดีความดังกล่าวอย่างไร

เพราะแต่ละประเทศมีวิธีการแตกต่างกัน ยกตัวอย่างเช่น ศาลของประเทศสหรัฐอเมริกาจะถือว่าศาลมีเขตอำนาจเหนือจำเลย โดยใช้หลักเขตอำนาจเหนือบุคคล (Personal jurisdiction) มาพิจารณา[67]

กรณีเขตอำนาจศาลบนเครือข่ายอินเตอร์เน็ต ในระยะแรก ศาลของสหรัฐอเมริกามีแนวโน้มถือว่าจำเลยมีความสัมพันธ์ขั้นต่ำกับประเทศสหรัฐอเมริกา หากเว็บไซต์บนระบบเครือข่ายอินเตอร์เน็ตของจำเลยสามารถเข้าเยี่ยมชมได้จากประชาชนในประเทศสหรัฐอเมริกา[68]

---

[67] ตามหลักเขตอำนาจเหนือบุคคล โจทก์ไม่สามารถฟ้องจำเลยซึ่งเป็นบุคคลที่มิใช่ชนชาติของประเทศสหรัฐอเมริกา (Non–resident defendant) เป็นคดีต่อศาลไปประเทศสหรัฐได้ เว้นแต่จำเลยจะได้มีความสัมพันธ์ทางกายภาพต่อประเทศสหรัฐอเมริกา เช่น จำเลยมีภูมิลำเนา ที่อยู่อาศัย ทรัพย์สิน หรือตัวตนทางกายภาพปรากฏอยู่ในประเทศสหรัฐอเมริกาในเวลาที่ประกอบกิจกรรมหรือกระทำการใด ๆ อันละเมิดต่อกฎหมายประเทศสหรัฐอเมริกา แต่ต่อมาในยุคที่การติดต่อสื่อสารพัฒนามากยิ่งขึ้น ผู้ประกอบกิจกรรมหรือผู้กระทำการอันละเมิดต่อกฎหมายสหรัฐอเมริกาอาจกระทำการอยู่นอกประเทศสหรัฐอเมริกา แต่ผลของการกระทำหรือความเสียหายเกิดขึ้นในประเทศสหรัฐอเมริกาได้ ด้วยเหตุนี้ในปี พ.ศ. 2488 ศาลฎีกาแห่งประเทศสหรัฐอเมริกา (The United states supreme court) ในคดี International Shoe Corp. v State of Washington จึงได้นำเอาหลักเกณฑ์ “การใช้เขตอำนาจรัฐนอกดินแดน (Long Arm Jurisdiction) มาใช้ในการขยายเขตอำนาจศาลแห่งประเทศสหรัฐอเมริกาออกไปถึงจำเลยที่ไม่มีตัวตนอยู่ในเขตศาล โดยศาลฎีกาในคดีดังกล่าวได้วางหลักว่าการวินิจฉัยว่าศาลจะมีอำนาจเหนือจำเลยซึ่งไม่ได้มีตัวตนทางกายภาพอยู่ในเขตศาลหรือไม่ ต้องปรากฏข้อเท็จจริงเบื้องต้นว่า จำเลยมีความสำพันธ์ขั้นต่ำ (Minimum contact) กับประเทศสหรัฐอเมริกา และการดำเนินการดังกล่าวไม่ขัดกับประเพณีการดำเนินการอย่างเป็นธรรมและความยุติธรรมอันเป็นสาระสำคัญ (Traditional notions of fair play and substantial justice), สราวุธ ปิติยาศักดิ์, *กฎหมายเทคโนโลยีสารสนเทศ*, 401.

[68] ในคดี Maris Inc. v Cybergold Inc. ระหว่างบริษัท Marits โจทก์ซึ่งเป็นบริษัทในมลรัฐมิสซูรี่ และบริษัท Cybergold จำเลยซึ่งเป็นบริษัทในมลรัฐแคลิฟอเนีย ข้อเท็จจริงปรากฏว่าจำเลยได้ใช้เครื่องหมายการค้าจดทะเบียนของโจทย์ไปจดทะเบียนชื่อโดเมนแล้วนำชื่อโดเมนดังกล่าวไปใช้เป็นชื่อเว็บไซต์ของตน โจทก์จึงฟ้องจำเลยในข้อหาละเมิดเครื่องหมายการค้าตามมาตรา 43 ของกฎหมายเครื่องหมายการค้าของสหรัฐอเมริกา ค.ศ. 1946 และเป็นการแข่งขันไม่เป็นธรรมโดยอ้างว่าเว็บไซต์ของจำเลยกระทำการประชาสัมพันธ์โดยตรงกับประชาชนชาวมลรัฐมิสซูรี่ จำเลยให้การต่อสู้ว่าจำเลยไม่อยู่ในเขตอำนาจแห่งมลรัฐมิสซูรี่ เพราเว็บไซต์ของจำเลยเป็นเพียงเว็บไซต์ที่ให้ข้อมูลข่าวสารแก่ผู้ให้บริการอินเตอร์เน็ต จึงเป็นเว็บไซต์ที่ไม่มีปฏิสัมพันธ์ (Passive website) ใด ๆ กับมลรัฐมิสซูรี่ และแม้จะมีผู้ใช้บริการอินเตอร์เน็ตในมลรัฐมิสซูรี่เข้าเยี่ยมชมเว็บไซต์ของจำเลยไม่น้อยกว่า 311 ครั้ง แต่ในจำนวนดังกล่าว มีการเข้าชมประมาณ 180 ครั้ง เป็นการเข้าชมของโจทก์และลูกจ้างของโจทก์ศาลแห่งมลรัฐมิสซูรี่พิเคราะห์ว่า การที่เว็บไซต์ของจำเลยสามารถนำเสนอข้อมูลข่าวสารให้แก่ผู้ใช้อินเตอร์เน็ตได้อย่างรวดเร็วและสามารถเข้าถึงผู้ใช้บริการได้ทั่วโลก แสดงว่าจำเลยมีเจตนาเผยแพร่ข้อมูลข่าวสารไปยังผู้ใช้บริการอินเตอร์เน็ตผ่านทางเว็บไซต์ของตน โดยรู้ว่าข้อมูลเหล่านั้นจะได้เผยแพร่ไปทั่วโลก ฉะนั้น ศาลจึงไม่ยอมรับข้อต่อสู้ของจำเลยในประเด็นที่ว่าเว็บไซต์ของจำเลยเป็นเว็บไซต์ที่ไม่มีปฏิสัมพันธ์ แต่ศาลวินิจฉัยว่า การที่จำเลยได้ให้ผู้ใช้บริการของจำเลยแก่ชาวมลรัฐมิสซูรี่ ศาลจึงตัดสินยกคำร้องของจำเลยที่ว่าศาลแห่งมลรัฐมิสซูรี่ไม่มีเขตอำนาจศาลในการพิจารณาคดีดังกล่าว, เรื่องเดียวกัน, 402.

ต่อมาศาลของสหรัฐอเมริกาในคดี Zippo[69] ได้พัฒนา “แบบทดสอบการมีปฏิสัมพันธ์และไม่ปฏิสัมพันธ์” ขึ้นเพื่อวิเคราะห์เขตอำนาจศาลตามแบบทดสอบดังกล่าว หากจำเลยที่มิใช่คนชาติของประเทศสหรัฐอเมริกาสามารถเข้าทำสัญญาผ่านระบบเครือข่ายอินเตอร์เน็ตกับเว็บไซต์ที่มีปฏิสัมพันธ์ (Active website) ในประเทศสหรัฐอเมริกา ถือว่าศาลแห่งสหรัฐอเมริกาสามารถมีอำนาจในการดำเนินคดีดังกล่าว สำหรับกรณีที่มีการโพสข้อความผ่านระบบเครือข่ายอินเตอร์เน็ตกับเว็บไซต์ที่ไม่มีปฏิสัมพันธ์ (Passive website) ถือว่าศาลแห่งสหรัฐอเมริกาไม่มีเขตอำนาจเหนือจำเลยคนนั้น หลังจากคดี zippo หลายต่อหลายคดีเกี่ยวกับการละเมิดสิทธิบัตรและเครื่องหมายการค้าบนเครือข่ายอินเตอร์เน็ตถูกพิจารณาด้วยแบบทดสอบการมีปฏิสัมพันธ์และไม่มีปฏิสัมพันธ์และคดีจำนวนมากได้ถูกยกฟ้องเพราะคดีอยู่นอกเขตอำนาจศาล ต่อมาในปลายปี ค.ศ. 1999 ศาลแห่งสหรัฐอเมริกาจำนวนมากได้เปลี่ยนจากการวิเคราะห์เขตอำนาจศาลด้วยแบบทดสอบการมีปฏิสัมพันธ์และไม่ปฏิสัมพันธ์เป็นแบบทดสอบผลกระทบ (The effects test) ซึ่งถูกสร้างขึ้นครั้งแรกโดยศาลฎีกาแห่งสหรัฐอเมริกาในคดี Calder v Jones ในปี ค.ศ. 1989[70] ตามหลักเกณฑ์ของแบบทดสอบผลกระทบ ศาลแห่งสหรัฐอเมริกาจะมีเขตอำนาจเหนือบุคคลที่ไม่ใช่คนชาติของประเทศสหรัฐอเมริกาต่อเมื่อครบหลักเกณฑ์สามประการคือ ประการแรก จำเลยได้กระทำละเมิดโดยเจตนา ประการที่สอง จำเลยเจตนาโดยแจ้งชัดกระทำต่อประเทศสหรัฐอเมริกา และประการสุดท้าย จำเลยทราบว่าความเสียหายจะเกิดขึ้นในประเทศสหรัฐอเมริกา

ในประเทศฝรั่งเศส คดียาฮู (Yahoo case)[71] มีข้อสังเกตที่สำคัญสองประการในเรื่องของเขตอำนาจศาลฝรั่งเศส ประการแรก ตามหลักกฎหมายของฝรั่งเศส ข้อเท็จจริงเพียงประชาชนชาว

---

[69] Zippo Mfg. Co. v Zippo Dot Com., 1997 US Dist. LEXIS 1701 (W.D. Pa. 1997), อ้างถึงใน สราวุธ ปิติยาศักดิ์, *กฎหมายเทคโนโลยีสารสนเทศ*, 402.

[70] Calder v Jones, 1984 US LEXIS 41 (Supreme Court 1984), อ้างถึงใน เรื่องเดียวกัน, 402.

[71] เป็นคดีระหว่างสมาคมฝรั่งเศสแห่งหนึ่งที่มีชื่อว่า “ไลกล้า (La Ligue Contre Racisme Et L’Antisemitisme: LICRA)” กับบริษัทยาฮูจำกัด (Yahoo! Incoporation) แห่งเมืองเดลาแวร์ ประเทศสหรัฐอเมริกา ซึ่งเป็นคดีที่มีความสำคัญยิ่งเกี่ยวกับเขตอำนาจศาลเหนือกิจกรรมบนเครือข่ายอินเตอร์เน็ตในประเทศฝรั่งเศส ในคดีดังกล่าวไลกล้าได้มีคำร้องขอให้ศาลฝรั่งเศสมีคำสั่งห้ามเว็บไซต์ของบริษัทยาฮูให้บริการแก่ผู้ใช้บริการอินเตอร์เน็ตในประเทศฝรั่งเศสในการเข้าถึงเว็บเพจที่เกี่ยวกับการประมูลขายเครื่องสวัสดิกะหรือเครื่องหมายนาซีเยอรมัน (Nazi memorabilia) ของเว็บไซต์ยาฮู ศาลฝรั่งเศสมีคำสั่งห้ามบริษัทยาฮูในประเทศสหรัฐอเมริกามิให้ชนชาติฝรั่งเศสเข้าถึงเว็บเพจการประมูลเครื่องหมายสวัสดิกะของเว็บไซต์ยาฮู บริษัทยาฮูไม่ได้อุทธรณ์คำสั่งศาลฝรั่งเศสต่อศาลอุทธรณ์ในประเทศฝรั่งเศส แต่บริษัทยาฮูได้ยื่นคำร้องต่อศาลของสหรัฐอเมริกาว่าคำพิพากษาของศาลฝรั่งเศสไม่สมบูรณ์และไม่อาจบังคับได้ในสหรัฐอเมริกา เพราะการประมูลเครื่องหมายสวัสดิกะของบริษัทยาฮูในประเทศสหรัฐอเมริกาได้รับความคุ้มครองตามหลักเสรีภาพในการแสดงความคิดเห็น (Freedom of expression) ภายใต้หลัก First Amendment ของรัฐธรรมนูญแห่งประเทศสหรัฐอเมริกา, เรื่องเดียวกัน, 403.

ฝรั่งเศสในประเทศฝรั่งเศสสามารถเข้าเยี่ยมชมเว็บไซต์ของต่างประเทศ ถือว่าทำให้ศาลฝรั่งเศสมีเขตอำนาจเหนือเว็บไซต์ดังกล่าว ประการที่สอง คำพิพากษาของศาลประเทศหนึ่งไม่อาจบังคับได้ในอีกประเทศหนึ่ง เว้นแต่จะมีข้อตกลงระหว่างประเทศยินยอมให้บังคับกันได้ เช่น ในอนุสัญญากรุงบรัสเซลส์และอนุสัญญาลูกาโน (The brussels convention and lugano convention) ซึ่งเป็นอนุสัญญาที่ใช้บังคับกันในแถบยุโรป กำหนดให้คำพิพากษาในคดีแพ่งและพาณิชย์ของประเทศสมาชิกซึ่งบังคับได้โดยชอบด้วยกฎหมายของประเทศดังกล่าวสามารถบังคับได้ในประเทศสมาชิกอื่น หากผู้มีส่วนได้เสียในคำพิพากษานั้นได้ยื่นคำร้องขอให้ประเทศที่ตนประสงค์ให้บังคับคำพิพากษาดังกล่าวประกาศยืนยันการบังคับตามคำพิพากษานั้น

ในประเทศอังกฤษ คดีระหว่าง Menashe business mercantile Ltd. โจทก์ กับ William Hill Organization จำเลย โดยคดีนี้เป็นคดีแรกเกี่ยวกับการละเมิดสิทธิบัตรบนเครือข่ายอินเตอร์เน็ต[72] ศาลตัดสินให้โจทก์เป็นฝ่ายชนะคดี โดยวินิจฉัยว่าระบบเกมคอมพิวเตอร์มีผลกระทบเกิดขึ้นในประเทศอังกฤษ เพราะไม่มีนักธุรกิจผู้ใดคิดว่าระบบนั้นไม่มีผลในประเทศอังกฤษในเมื่อระบบของจำเลยประสงค์จะให้ผู้เล่นม้าในประเทศอังกฤษเล่นม้าผ่านระบบดังกล่าว แบบทดสอบที่ศาลอังกฤษใช้ในการวินิจฉัยเขตอำนาจศาลในคดี Menashe Business Mercantile Ltd. V William Hill Organization มีลักษณะคล้ายแบบทดสอบผลกระทบ (The effects test) ของศาลฎีกาแห่งสหรัฐอเมริกาในคดี Calder v Jones อย่างไรก็ตาม ความแตกต่างคือ แบบทดสอบผลกระทบของศาลแห่งสหรัฐอเมริกานั้นเข้มงวดกว่า เพราะโจทก์ต้องพิสูจน์ต่อศาลให้ได้ครบเงื่อนไข 3 ประการ คือ จำเลยได้กระทำละเมิดโดยเจตนา ประการที่สอง จำเลยเจตนาโดยชัดแจ้งกระทำต่อประเทศสหรัฐอเมริกา และประการสุดท้าย จำเลยทราบว่าความเสียหายจะเกิดขึ้นในประเทศสหรัฐอเมริกา ในขณะที่ศาลอังกฤษเพียงได้ข้อเท็จจริงว่านักธุรกิจทั่วไปหรือวิญญูชนมีความเชื่อว่าผลกระทบจะเกิดขึ้นใน

---

[72] ในคดีดังกล่าว โจทก์เป็นเจ้าของสิทธิบัตรระบบเกมคอมพิวเตอร์ในประเทศอังกฤษ (Computer based gaming system) จำเลยดำเนินธุรกิจเกมคอมพิวเตอร์ให้กับนักเล่นม้าในประเทศอังกฤษ คอมพิวเตอร์แม่ข่ายที่เป็นฐานข้อมูลหรือเซิฟเวอร์ที่ใช้ดำเนินการอยู่นอกประเทศอังกฤษ และได้บันทึกจัดเก็บระบบคอมพิวเตอร์ที่โจทก์เป็นเจ้าของสิทธิบัตรนอกประเทศอังกฤษ แต่ผู้เล่นหรือผู้บริโภคระบบเกมคอมพิวเตอร์ดังกล่าวอยู่ในประเทศอังกฤษโดยการสื่อสารผ่านเครือข่ายอินเตอร์เน็ต โจทก์อ้างว่าจำเลยกระทำการละเมิดมาตรา 60(2) ของพระราชบัญญัติสิทธิบัตรอังกฤษ ค.ศ. 1977 เนื่องจากเมื่อนักเล่นม้าในประเทศอังกฤษได้เข้าถึงระบบเกมคอมพิวเตอร์ของจำเลยที่อยู่นอกประเทศอังกฤษ ถือว่าระบบเกมคอมพิวเตอร์ดังกล่าวตกอยู่ภายใต้กฎหมายสิทธิบัตรอังกฤษและเป็นการละเมิดบทกฎหมายนั้นฝ่ายจำเลยโต้แย้งว่าระบบเกมคอมพิวเตอร์ไม่ได้ละเมิดสิทธิบัตรอังกฤษเพราะเกมคอมพิวเตอร์แม่ข่ายตั้งอยู่นอกประเทศอังกฤษ จึงไม่ควรตกอยู่ภายใต้กฎหมายสิทธิบัตรอังกฤษและไม่เป็นการละเมิดมาตรา 60 (2), สราวุธ ปิติยาศักดิ์, *กฎหมายเทคโนโลยีสารสนเทศ*, 405.

ประเทศอังกฤษเท่านั้น ก็เพียงพอที่ศาลอังกฤษจะมีเขตอำนาจศาลเหนือคดีนั้น[73] ส่วนกรณีการพิจารณาเขตอำนาจศาลไทยบนเครือข่ายอินเตอร์เน็ต อาจแบ่งเป็น 2 กรณี คือ

2.2.3.1 เขตอำนาจศาลไทยเหนือการละเมิดทางแพ่งบนเครือข่ายอินเตอร์เน็ต

การละเมิดทางแพ่งบนเครือข่ายอินเตอร์เน็ตที่พบในประเทศไทยส่วนใหญ่เป็นกรณีของการหมิ่นประมาท และอาจพบได้ในกรณีอื่น ๆ เช่น การละเมิดสิทธิ์ การละเมิดเครื่องหมายการค้า ฯลฯ ซึ่งตามประมวลกฎหมายวิธีพิจารณาความแพ่ง (แก้ไขเพิ่มเติม พ.ศ. 2534) ศาลไทยจะมีเขตอำนาจเหนือจำเลยซึ่งมิใช่คนสัญชาติไทยเหนือการกระทำละเมิดทางแพ่งบนเครือข่ายอินเตอร์เน็ตเมื่อเข้าเงื่อนไขใดเงื่อนไขหนึ่งดังนี้

1. ในกรณีที่จำเลยมีภูมิลำเนาอยู่ในประเทศไทย ศาลไทยที่มีเขตอำนาจพิจารณาพิพากษาคดีได้แก่ ศาลที่จำเลยมีภูมิเลาเนาอยู่ในเขต[74]

2. ในกรณีที่มีมูลคดีเกิดขึ้นในประเทศไทย ศาลไทยที่มีเขตอำนาจพิจารณาพิพากษาคดีได้แก่ ศาลที่จำเลยมีภูมิเลาเนาอยู่ในเขต[75]

3. ในกรณีที่มูลคดีเกิดขึ้นในเรือไทยหรืออากาศยานไทยที่อยู่นอกราชอาณาจักร ศาลที่มีเขตอำนาจพิจาณาพิพากษาคดีได้แก่ ศาลแพ่ง[76]

4. ในกรณีที่จำเลยมิได้อยู่ในประเทศไทยและมูลคดีเกิดขึ้นในประเทศไทย แต่โจทก์มีสัญชาติไทยหรือมีภูมิลำเนาอยู่ในประเทศไทย ศาลที่มีเขตอำนาจพิจารณาพิพากษาคดี ได้แก่ ศาลแพ่งและศาลที่โจทก์มีภูมิลำเนาอยู่ในเขตศาล[77]

ตามบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความแพ่งข้างต้น เห็นได้ชัดว่ากฎหมายได้กำหนดขอบเขตอำนาจศาลไทยไว้อย่างกว้าง ๆ แม้แต่คดีที่มีมูลคดีที่ไม่ได้เกิดขึ้นในประเทศไทยหรือจำเลยไม่มีภูมิลำเนาอยู่ในประเทศไทย เพียงแต่โจทก์เป็นคนสัญชาติไทยหรือมีภูมิลำเนาอยู่ในประเทศไทย ศาลไทยก็มีเขตอำนาจเหนือคดีดังกล่าว[78] ฉะนั้น ปัญหาเรื่องเขตอำนาจศาลจึงไม่ใช่ประเด็นปัญหาที่สำคัญในการนำคดีละเมิดทางแพ่งบนเครือข่ายอินเตอร์เน็ตที่จำเลยมีภูมิลำเนาอยู่ต่างประเทศมาสู่ศาลไทยแต่อย่างใด แต่อย่างไรก็ตาม ปัญหาสำคัญที่แท้จริงก็คือ ปัญหา

---

[73] สราวุธ ปิติยาศักดิ์, *กฎหมายเทคโนโลยีสารสนเทศ*, 405.

[74] ประมวลกฎหมายวิธีพิจารณาความแพ่ง, มาตรา 4(1).

[75] เรื่องเดียวกัน.

[76] เรื่องเดียวกัน, มาตรา 3 (1)

[77] เรื่องเดียวกัน, มาตรา 4 ตรี

[78] ธีรศักดิ์ กองสมบัติ, *เขตอำนาจศาลเหนือการกระทำละเมิดทางแพ่งในไซเบอร์สเปซ*, วิทยานิพนธ์นิติศาสตรมหาบัณฑิต สาขาวิชานิติศาสตร์, (กรุงเทพฯ: มหาวิทยาลัยธรรมศาสตร์, 2552), 193-203.

การพิจารณาว่าจะนำกฎหมายของประเทศใดมาบังคับใช้แก่คดี ที่เรียกว่า “การขัดกันแห่งกฎหมาย” เพราะคดีดังกล่าวเป็นคดีที่มีองค์ประกอบหรือจุดเกาะเกี่ยวในทางระหว่างประเทศกล่าวคือ จำเลยมีภูมิลำเนาอยู่ต่างประเทศ ดังนั้น เมื่อมีข้อต่อสู้ดังกล่าวขึ้นสู่ศาล ศาลจำต้องพิเคราะห์ว่ากฎหมายที่จะนำมาปรับใช้แก่คดีดังกล่าวได้แก่กฎหมายของประเทศใด ซึ่งโดยหลักกฎหมายระหว่างประเทศแผนกคดีบุคคลหรือหลักกฎหมายขัดกัน กฎหมายที่นำมาบังคับใช้แก่คดีได้แก่กฎหมายของประเทศที่มีการกระทำละเมิดเกิดขึ้น

ตามหลักการคุ้มครองทรัพย์สินทางปัญญาในกรณีที่มีความผิดที่เกี่ยวข้องกับทรัพย์สินทางปัญญาได้กระทำบนอินเตอร์เน็ต กฎหมายทรัพย์สินทางปัญญาจะให้ความคุ้มครองเฉพาะในประเทศที่ทรัพย์สินทางปัญญานั้นได้จดทะเบียนไว้เท่านั้น เช่น สิทธิบัตรหรือเครื่องหมายการค้าที่จดทะเบียนในประเทศไทย ด้วยเหตุนี้ การใช้สิทธิบัตรไทยหรือเครื่องหมายการค้าไทยในประเทศที่มิได้มีการจดทะเบียนไว้ แม้จะไม่ได้รับอนุญาตจากผู้ทรงสิทธิในประเทศไทย ก็ไม่เป็นการละเมิดเครื่องหมายการค้าไทยหรือสิทธิบัตรไทยนั้น

นอกจากนี้ ในกรณีการบังคับคดีตามคำพิพากษาของประเทศใดย่อมบังคับได้ภายในประเทศนั้นเท่านั้น จะนำไปบังคับในต่างประเทศมิได้ เว้นแต่มีข้อตกลงว่าด้วยการบังคับตามคำพิพากษาระหว่างประเทศไทยกับประเทศใดประเทศหนึ่ง ดังนั้น แม้ศาลไทยจะมีเขตอำนาจเหนือคดีก็ตาม โจทก์ก็ต้องคำนึงถึงหลักการขัดกันแห่งกฎหมายและการบังคับตามคำพิพากษาก่อนที่จะตัดสินใจนำคดีที่ผู้กระทำละเมิดเป็นผู้มีภูมิลำเนาอยู่ต่างประเทศมาสู่ศาลไทย

2.2.3.2 เขตอำนาจศาลไทยในคดีการกระทำผิดเกี่ยวกับคอมพิวเตอร์

ลักษณะของการกระทำผิดเกี่ยวกับคอมพิวเตอร์ส่วนหนึ่งเป็นเรื่องของการกระทำความผิดอาญาที่ไร้พรหมแดนผู้กระทำความผิดอาจอยู่ต่างประเทศแล้วกระทำความผิดเกี่ยวกับคอมพิวเตอร์กับเหยื่อที่อยู่ในประเทศไทย แต่เนื่องจากการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เป็นความผิดอาญา จึงต้องนำหลักกฎหมายความรับผิดในเรื่องหลักดินแดนตามที่บัญญัติไว้ในมาตรา 5 และมาตรา 6 แห่งประมวลกฎหมายอาญามาปรับใช้กับการกระทำความผิดอาญาที่เกี่ยวกับคอมพิวเตอร์ด้วย

กรณีที่เกี่ยวกับ “ความพยายามกระทำการใด ๆ” ตามที่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กำหนดไว้ให้เป็นความผิด แม้ความพยายามนั้นจะได้กระทำขึ้นนอกประเทศไทย แต่ถ้าหากมีกระทำไปตลอดจนถึงขั้นความผิดสำเร็จแล้ว ผลของการกระทำนั้นจะเกิดขึ้นในประเทศไทย ก็ให้ถือว่าความพยายามกระทำความผิดนั้น กระทำในประเทศไทยตามมาตรา 5 วรรคสองแห่งประมวลกฎหมายอาญา

กรณีการกระทำความผิดอาญาที่เกี่ยวกับคอมพิวเตอร์ไม่ได้เกิดขึ้นในประเทศไทย และยังไม่เป็นความผิดสำเร็จ แต่หากว่าการกระทำนั้นหากได้กระทำต่อไปจนถึงขั้นความเป็นความผิดสำเร็จ ซึ่งผลของการกระทำความผิดจะเกิดขึ้นในประเทศไทย จึงถือว่าการพยายามกระทำความผิดดังกล่าว ได้กระทำในประเทศไทย ตามประมวลกฎหมายอาญา มาตรา 5 วรรคสอง

นอกจากนี้ ตัวการ ผู้สนับสนุน หรือผู้ใช้ให้กระทำความผิดตามพระราชบัญญัตินี้ หากได้มีการกระทำ การสนับสนุน หรือใช้ให้กระทำความผิด นอกประเทศไทย ก็ถือว่าตัวการ ผู้สนับสนุน หรือผู้ใช้ให้กระทำความผิดได้กระทำการในประเทศไทย ซึ่งการกระทำผิดที่กล่าวมาทั้งหมดศาลไทยมีเขตอำนาจตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 22

อย่างไรก็ตาม บางกรณี ทั้งการกระทำ ผลแห่งการกระทำ และผู้มีส่วนร่วมในการกระทำในความผิดเกี่ยวกับคอมพิวเตอร์อาจเกิดขึ้นหรืออยู่นอกประเทศไทยทั้งสิ้น แต่ผู้กระทำเป็นคนไทย หรือผู้เสียหายเป็นคนไทยหรือรัฐบาลไทย เช่นคนไทยเจาะระบบของกองทัพอังกฤษ รัฐบาลอังกฤษจึงร้องขอให้ลงโทษ กรณีนี้ถือว่าผู้กระทำความผิดเป็นคนไทยและรัฐบาลแห่งประเทศที่ความผิดได้เกิดขึ้นร้องขอให้ลงโทษ แต่เนื่องจากการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ไม่อยู่ในฐานความผิดต่าง ๆ ที่กำหนดให้การกระทำความผิดนอกราชอาณาจักรที่ต้องรับโทษในราชอาณาจักรตามมาตรา 8 ของประมวลกฎหมายอาญา[79] การกระทำความผิดเกี่ยวกับคอมพิวเตอร์นอกประเทศไทยจึงไม่ต้องรับโทษในประเทศไทยตามประมวลกฎหมายอาญา ดังนั้น เพื่อขจัดปัญหาดังกล่าว มาตรา 17 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550[80] จึงบัญญัติเพิ่มเติมให้การกระทำความผิดเกี่ยวกับคอมพิวเตอร์นอกประเทศไทยต้องรับโทษในประเทศไทยไว้โดยมีศาลอาญาและศาลซึ่งการสอบสวนนั้นได้กระทำลงตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 22(2) เป็นศาลที่มีขอบเขตอำนาจในการตัดสินคดี

---

[79] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550, มาตรา 8 บัญญัติว่า “ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ”.

[80] พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550, มาตรา 17 บัญญัติว่า “ผู้ใดกระทำความผิดตามพระราชบัญญัตินี้นอกราชอาณาจักรและ

(1) ผู้กระทำความผิดนั้นเป็นคนไทย และรัฐบาลแห่งประเทศที่ความผิดเกิดขึ้นหรือผู้เสียหายได้ร้องขอให้ลงโทษ หรือ

(2) ผู้กระทำความผิดนั้นเป็นคนต่างด้าว และรัฐบาลไทยหรือคนไทยเป็นผู้เสียหาย และผู้เสียหายได้ร้องขอให้ลงโทษ ผู้กระทำความผิดนั้นต้องรับโทษในราชอาณาจักร”.

2.2.4 หลักการบังคับใช้คำพิพากษาตามศาลต่างประเทศ (Enforcement of foreign judgments)

การกระทำผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์เป็นการกระทำความผิดที่มีลักษณะไร้พรหมแดน ดังนั้น ความเสียหายที่เกิดจากอาชญากรรมทางคอมพิวเตอร์จึงมีลักษณะเป็นวงกว้าง ก่อให้เกิดผลกระทบต่อคนจำนวนมากและทำได้รวดเร็วกว่าการกระทำผิดประเภทอื่น ๆ ด้วยเหตุนี้ การส่งเสริมความร่วมมือทางกฎหมายระหว่างประเทศจึงมีความสำคัญในการรับมือกับอาชญากรรมทางคอมพิวเตอร์เป็นอย่างยิ่ง เพื่อให้การดำเนินการสืบสวนคดีรวดเร็วและมีประสิทธิภาพและเท่าทันต่อเล่ห์เหลี่ยมของอาชญากร ซึ่งแนวคิดในการบังคับตามคำพิพากษาศาลต่างประเทศจึงมีความเหมาะสมที่จะนำมาใช้เพื่อเป็นประโยชน์ในการดำเนินการและลดอุปสรรคต่าง ๆ รวมถึงความล่าช้าในกระบวนการยุติธรรมในปัจจุบัน

สำหรับ “การบังคับตามคำพิพากษาศาลต่างประเทศ” นั้น หมายถึง การที่ศาลของประเทศที่ได้รับคำร้องขอ ต้องดำเนินการในการบังคับตามคำพิพากษาของศาลต่างประเทศโดยอาศัยหลักเกณฑ์และวิธีการของศาลที่ได้รับคำร้องขอให้มีการบังคับ เพื่อให้คำพิพากษาของศาลต่างประเทศบังเกิดผล หรือกล่าวอีกนัยหนึ่ง คือการนำผลของคำพิพากษาของศาลต่างประเทศหนึ่งไปขอให้ศาลอีกประเทศหนึ่งบังคับตามให้ ทั้งนี้ บุคคลที่ร้องขอให้นำผลของคำพิพากษาของศาลประเทศหนึ่งไปขอให้ศาลอีกประเทศหนึ่งบังคับตามให้นั้น จะต้องเป็นผู้ที่มีส่วนเกี่ยวข้องและต้องการให้มีการบังคับตามคำพิพากษานั้น เช่น โจทก์ ฯลฯ มิใช่เป็นบุคคลอื่น เช่น ศาลที่มีคำพิพากษาหรือองค์กรอื่นบังคับคดีแทนให้[81]

ซึ่งแนวคิดดังกล่าวเริ่มมาจากความพยายามในการลดความยุ่งยากในทางกฎหมายระหว่างประเทศ ที่ต้องมีการอนุวัติโดยกฎหมายภายในของประเทศนั้นๆ ก่อนจึงจะสามารถดำเนินการตามสนธิสัญญาระหว่างประเทศได้ แต่อย่างไรก็ตาม หลักการนี้มิได้ประสงค์จะลบล้างอำนาจอธิปไตยของรัฐที่มีอยู่เหนือดินแดนของตนเองเพื่อปกป้องผลประโยชน์ของปัจเจกชนในการให้ความคุ้มครองตามกฎหมายของประเทศนั้นๆ แต่เป็นเพียงการให้ยับยั้งการใช้อำนาจในระดับหนึ่งเท่านั้น โดยแนวความคิดที่สนับสนุนการบังคับตามคำพิพากษาศาลระหว่างประเทศ ได้แก่ หลักอัธยาศัยไมตรีระหว่างประเทศ และหลักถ้อยทีถ้อยอาศัยระหว่างกัน (Comity and reciprocity) หลักแห่งพันธกรณี (Doctrine of obligation) หลักความเป็นที่สุดและเสร็จเด็ดขาดของคำพิพากษา (Final and conclusive judgment)

---

[81] กนก อินทรัมพรรย์, ความเห็นและข้อสังเกตในเรื่องความร่วมมือทางศาลเกี่ยวกับการยอมรับบังคับตามคำพิพากษาศาลต่างประเทศ, *ดุลพาห*, *2*(31), (มีนาคม–เมษายน 2527), 56-69.

2.2.4.1 หลักอัธยาศัยไมตรีระหว่างประเทศ และหลักถ้อยทีถ้อยอาศัยระหว่างกัน

ปกติโดยทั่วไปแล้ว รัฐจะมีอำนาจอธิปไตยเป็นของตนเอง กล่าวคือ รัฐจะไม่ยอมให้มีการก้าวก่ายอำนาจข้ามรัฐกัน ซึ่งการไม่ยอมหรือไม่อนุญาตเช่นนี้เป็นการล่วงการพัฒนาเจริญเติบโตทางด้านการค้าเป็นอย่างมาก ดังนั้น หลักอัธยาศัยไมตรีระหว่างประเทศ และหลักถ้อยทีถ้อยปฏิบัติตอบแทนระหว่างกันนี้เป็นหลักพื้นฐานสำคัญที่จะทำให้เกิดการบังคับตามพิพากษาศาลต่างประเทศ กล่าวคือ หากรัฐหนึ่งยอมลดอำนาจอธิปไตยของตนลงมา เพื่อที่จะแสดงให้เห็นว่า ตนยอมรับอำนาจอธิปไตยของอีกรัฐหนึ่ง โดยการยอมบังคับตามคำพิพากษาของศาลต่างประเทศให้ และในขณะเดียวกันรัฐที่ยอมรับก็หวังที่จะให้รัฐที่มีคำพิพากษานั้นยอมรับบังคับตามคำพิพากษาของรัฐตนด้วย ซึ่งทั้งหมดอาศัยพื้นฐานจากหลักการในเรื่องอัธยาศัยไมตรีโดยพิจารณาจากความช่วยเหลือในการปฏิบัติตอบแทนซึ่งกันและกัน จากความสัมพันธ์ฉันท์มิตร

ดังนั้น กล่าวโดยสรุปคือ ประเทศทั้งสองหรือหลายประเทศต่างต้องยอมรับบังคับตามคำพิพากษาของกันและกัน ในลักษณะที่เหมือนกันและเท่าเทียมกัน[82]

แนวความคิดนี้ เป็นแนวความคิดดั้งเดิมของประเทศอังกฤษ โดยศาลอังกฤษเชื่อว่าศาลของประเทศหนึ่งมีพันธะหรือข้อผูกพันตามกฎหมายระหว่างประเทศที่จะต้องให้ความช่วยเหลือยังศาลของอีกประเทศหนึ่ง และยังเกรงว่าหากคำพิพากษาต่างประเทศไม่ได้รับการยอมรับบังคับให้ในประเทศอังกฤษแล้ว คำพิพากษาของอังกฤษเองก็จะไม่ได้รับการบังคับตามในต่างประเทศด้วยเช่นกัน โดยอาศัยหลักอัธยาศัยไมตรี และหลักปฏิบัติตอบแทนระหว่างกัน[83]

แต่การที่จะยึดถือตามหลักนี้อย่างเคร่งครัดแล้ว ก็เท่ากับว่า ศาลอังกฤษยอมรับบังคับตามคำพิพากษาศาลต่างประเทศอย่างเต็มที่ โดยไม่มีเงื่อนไขอย่างอื่นใด (Full faith and credit)[84] ด้วยเหตุนี้จึงก่อให้เกิดปัญหาขึ้นได้ เช่น หากคำพิพากษานั้นขัดต่อความสงบเรียบร้อย หรือขัดต่อหลักแห่งความยุติธรรม ซึ่งตามกฎหมายอังกฤษถือเป็นเหตุสำคัญที่จะทำให้ศาลอังกฤษไม่ยอมบังคับตามคำพิพากษานั้นให้ปัญหาดังกล่าวจึงนำไปสู่แนวทางตามหลักแห่งพันธะกรณี ซึ่งจะกล่าวต่อไป

ประเทศใดจะยอมรับและบังคับคดีตามคำพิพากษาศาลต่างประเทศนั้น ย่อมอาศัยหลักอัธยาศัยไมตรีระหว่างประเทศ (Comity) โดยเป็นการยอมรับตามหลักกฎหมายระหว่างประเทศโดยสมัครใจของประเทศนั้น มิใช่ยอมรับเพราะหน้าที่หรือพันธกรณีระหว่างประเทศแต่อย่างใด

---

[82] ประสิทธิ ปิวาวัฒนพานิช, *คำอธิบายกฎหมายระหว่างประเทศแผนกคดีบุคคล*, (กรุงเทพฯ: มหาวิทยาลัยธรรมศาสตร์, 2551), 294-295.

[83] Collins, L. A., Dicey, A. V., Carlile Morris, J. H., *Dicey and Morris on the conflict of laws Vol. 1*, 13th ed., (London: Sweet & Maxwell, 2000), 469.

[84] Scoles, E. F., & Hay, P., *Conflict of Laws*, 3rd ed., (St. Paul, MN: West Group, 2000), 1188-1190.

2.2.4.2 หลักแห่งพันธกรณี (Doctrine of obligation)

หลักแห่งพันธกรณีนี้ก็มีแหล่งกำเนิดในประเทศอังกฤษ ในปี ค.ศ. 1842 โดยผู้พิพากษา Baron park ได้กล่าวไว้ในคดี Russell v. Smyth มีหลักการที่สำคัญ คือ ศาลต่างประเทศซึ่งมีเขตอำนาจศาลเหนือจำเลย ย่อมวินิจฉัยตัดสินคดีโดยกำหนดจำนวนเงินเพื่อให้จำเลยชำระหนี้ให้แก่โจทก์หรือเป็นการกำหนดหน้าที่หรือความรับผิดในการที่จำเลยจะต้องชำระหนี้ไว้ ซึ่งหน้าที่ที่จะต้องชำระหนี้ตามจำนวนดังกล่าวย่อมกลายเป็นพันธะทางกฎหมายอันอาจจะถูกบังคับชำระหนี้โดยประเทศอื่นได้

กล่าวคือ คำพิพากษาของศาลซึ่งมีเขตอำนาจในการพิจารณาคดีย่อมที่จะกำหนดหน้าที่หรือภาระหนี้ให้แก่ตัวจำเลยได้ เพื่อให้จำเลยปฏิบัติตามคำพิพากษานั้น ซึ่งศาลในประเทศอื่น ๆ ก็ย่อมมีความผูกพันที่จะต้องบังคับตามหนี้แห่งคำพิพากษานั้นด้วย นอกจากนั้นยังได้รับการยืนยันซึ่งปรากฏอยู่ในคดี Williams v Jones และคดี Schibsby v Westenholz[85]

จากหลักดังกล่าวจะเห็นได้ว่า เมื่อศาลทุกศาลตัดสินคดีแล้ว ก็จะเกิดหน้าที่หรือความผูกพันที่จะต้องปฏิบัติตามคำพิพากษานั้น (Obligation) เป็นหน้าที่หรือความผูกพัน ที่ยอมรับกันทั่วไป โดยถือว่าคำพิพากษามีความศักดิ์สิทธิ์ต้องปฏิบัติตาม จึงเกิดหลักการเป็นรูปเดียวกันและเข้ากันได้หมดในทุกประเทศ ทั้งนี้ การนำคำพิพากษาของศาลต่างประเทศมาใช้บังคับในประเทศอื่นนั้นจะต้องนำคำพิพากษาของศาลต่างประเทศมาฟ้องขอให้ศาลในอีกประเทศหนึ่งยอมรับและบังคับให้ (Action on judgment) โดยถือว่าคำพิพากษาของศาลต่างประเทศเป็นมูลคดี (Cause of action) เพื่อเรียกร้องหนี้แห่งคำพิพากษาของศาลต่างประเทศนั่นเอง

2.2.4.3 หลักความเป็นที่สุดและเสร็จเด็ดขาดของคำพิพากษา (Final and conclusive judgment; Res Judicata)

เมื่อเกิดข้อพิพาทขึ้นคู่กรณีมักจะนำเรื่องขึ้นสู่ศาล เพื่อให้มีการดำเนินกระบวนพิจารณาคดี และในที่สุดก็นำไปสู่การมีคำพิพากษาตัดสินคดี ซึ่งถือว่าคำพิพากษาในข้อพิพาทนั้นเป็นที่ยุติได้ เพราะศาลได้ทำหน้าที่ในการวินิจฉัยชี้ขาดตัดสินคดีโดยผ่านขั้นตอนการกลั่นกรองและไตร่ตรองในการพิพากษาคดีด้วยความบริสุทธิ์ ยุติธรรม โดยปราศจากอคติ

ด้วยเหตุนี้คำพิพากษาของศาลจึงมีความศักดิ์สิทธิ์ เป็นสิ่งที่คู่ความในคดีหรือผู้ที่เกี่ยวข้องในคดีจะต้องยอมรับและปฏิบัติตาม โดยคู่ความจะถูกห้ามมิให้โต้แย้งในคำพิพากษานั้น แต่ทั้งนี้ หากคำพิพากษานั้นเป็นคำพิพากษาของศาลล่าง คู่ความก็อาจโต้แย้งคำพิพากษาของศาลล่าง

---

[85] อานนท์ ศรีบุญโรจน์, *การรับรองและการบังคับตามคำพิพากษาศาลต่างประเทศในกลุ่มประเทศอาเซียน*, วิทยานิพนธ์นิติศาสตรมหาบัณฑิต สาขาวิชานิติศาสตร์, (กรุงเทพฯ: มหาวิทยาลัยธรรมศาสตร์, 2554), 20.

ต่อศาลสูงได้ ถ้าไม่เข้ากรณีที่กฎหมายห้ามไว้ และเมื่อศาลสูงตัดสินคดีเป็นอย่างไรแล้ว คู่ความก็ต้องยอมรับและปฏิบัติไปตามนั้น จะโต้แย้งอีกไม่ได้[86]

หลักความเป็นที่สุดแห่งคำพิพากษานี้ (Res Judicata) มีลักษณะทำนองเดียวกับหลักเกณฑ์ในเรื่องฟ้องซ้ำตามประมวลกฎหมายวิธีพิจารณาความแพ่ง มาตรา 148 ของประเทศไทย ซึ่งเป็นหลักกฎหมายปิดปาก (Estoppel) กล่าวคือ ห้ามมิให้คู่ความนำคดีมาฟ้องร้องอีก หากเข้าหลักเกณฑ์ 3 ประการ คือ (1) คดีที่ได้มีคำพิพากษาหรือคำสั่งชี้ขาดในคดีก่อนถึงที่สุดแล้ว (2) คู่ความหรือผู้มีส่วนได้เสียเกี่ยวข้องในคดีก่อนกับคู่ความหรือผู้มีส่วนได้เสียเกี่ยวข้องในคดีหลังต้องเป็นคู่ความเดียวกัน (3) ประเด็นในคดีหลังต้องเป็นประเด็นเดียวกันกับประเด็นในคดีก่อน ซึ่งได้มีการวินิจฉัยชี้ขาดแล้ว

ในส่วนที่เกี่ยวข้องกับการบังคับตามคำพิพากษาของศาลต่างประเทศ ก็ได้มีการนำหลักความเป็นที่สุดและเสร็จเด็ดขาดของคำพิพากษา (Final and conclusive judgment) นี้มาใช้เป็นแนวทางเดียวกัน คือ หากโจทก์นำคดีมาฟ้องจำเลยในประเทศหนึ่งโดยอาศัยมูลคดีเดิมจำเลยสามารถที่จะยกคำพิพากษาศาลต่างประเทศเป็นข้อต่อสู้ได้ เช่น คำพิพากษาศาลต่างประเทศได้ให้โจทก์ได้รับชำระหนี้บางส่วนตามที่เรียกร้อง และจำเลยได้ปฏิบัติตามคำพิพากษาต่างประเทศแล้ว แต่โจทก์ก็ยังไม่พอใจจึงได้นำคดีโดยอาศัยมูลคดีเดิมมาฟ้องร้องในอีกประเทศหนึ่งซึ่งจำเลยมีทรัพย์สินอยู่ และเป็นภูมิลำเนาของจำเลย ในกรณีนี้จำเลยก็สามารถที่จะอ้างคำพิพากษาต่างประเทศเป็นข้อต่อสู้ได้[87]

ในทางตรงกันข้าม โจทก์ก็สามารถที่จะฟ้องจำเลยในอีกประเทศหนึ่งได้โดยอาศัยมูลหนี้ที่เกิดขึ้นตามคำพิพากษาของศาลต่างประเทศนั้นได้ เพื่อให้มีการบังคับคดีตามคำพิพากษาของศาลต่างประเทศ ทั้งนี้ ศาลในประเทศที่โจทก์นำคดีไปฟ้องถือว่า คำพิพากษาของศาลต่างประเทศเป็นคำพิพากษาของศาลที่มีอำนาจเหนือคู่ความในคดีนั้นแล้ว โดยศาลในประเทศที่โจทก์นำคดีไปฟ้องจะไม่ก้าวล่วงเข้าไปตรวจสอบความถูกต้องของคำพิพากษานั้นอีก เพราะถือว่าคดีนั้นได้มีการต่อสู้และวินิจฉัยในด้านสาระหรือเนื้อหา (Merits) ของคดีมาแล้ว หากคู่ความฝ่ายใดไม่เห็นด้วยกับคำพิพากษา คู่ความฝ่ายนั้นก็สามารถที่จะใช้สิทธิอุทธรณ์คำพิพากษานั้นในประเทศที่มีคำพิพากษาเอง คำพิพากษานั้นจึงถือว่ามีความเสร็จเด็ดขาด (Conclusive)[88]

ในอีกประเทศหนึ่ง ระหว่างคู่ความเดียวกันในคดีที่ได้มีคำพิพากษาในต่างประเทศนั้นแล้วฉะนั้น จำเลยจึงไม่อาจโต้แย้งหรือคัดค้านคำพิพากษาของศาลต่างประเทศ ในส่วนที่เกี่ยวกับความ

---

[86] ประสิทธิ ปิวาวัฒนพานิช, *คำอธิบายกฎหมายระหว่างประเทศแผนกคดีบุคคล*, 310-311.

[87] เรื่องเดียวกัน.

[88] เรื่องเดียวกัน.

ถูกต้องของคำพิพากษา ถึงแม้จำเลยจะพิสูจน์ให้ศาลในประเทศที่โจทก์นำคดีมาฟ้องเห็นว่า ศาลต่างประเทศที่ได้วินิจฉัยและมีคำพิพากษานั้น วินิจฉัยข้อเท็จจริงหรือข้อกฎหมายผิดพลาดไปก็ตาม แต่อย่างไรก็ตาม ศาลในประเทศที่โจทก์นำคดีมาฟ้องจะยอมรับบังคับตามคำพิพากษาของศาลต่างประเทศหรือไม่ ก็ต้องพิจารณาตามหลักเกณฑ์ในการยอมรับบังคับคดีของประเทศนั้น[89]

[89] ประสิทธิ ปิวาวัฒนพานิช, *คำอธิบายกฎหมายระหว่างประเทศแผนกคดีบุคคล*, 310.

บทที่ 3

หลักเกณฑ์ระหว่างประเทศที่เกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์

ธรรมชาติของอาชญากรรมทางคอมพิวเตอร์และปัญหาทางกฎหมายที่เกี่ยวข้องนั้นเป็นเรื่องระหว่างประเทศ จึงมีความพยายามในการสร้างความสอดคล้องของกฎหมายในแต่ละประเทศผ่านองค์กรระหว่างประเทศต่าง ๆ เช่น UN, ITU, Interpol, APEC, OECD และ EU ฯลฯ

องค์กรแรกที่ชี้ให้เห็นปัญหาระดับระหว่างประเทศในการออกกฎหมายอาชญากรรมทางคอมพิวเตอร์คือองค์การตำรวจสากล (Interpol) ในการประชุม ณ กรุงปารีส พ.ศ. 2522[90] โดย Interpol ได้อภิปรายในเรื่องการฉ้อโกงทางคอมพิวเตอร์ (Computer fraud) และช่วงปี พ.ศ. 2523-2524 Interpol ได้ออกแบบสอบถามเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์และถูกส่งเวียนไปยังประเทศสมาชิก ต่อมา ได้จัด Interpol training seminar for investigators of Computer crime ขึ้นครั้งแรก ณ กรุงปารีส ในวันที่ 7-11 ธันวาคม พ.ศ. 2524[91] นับแต่นั้นเป็นต้นมา ความร่วมมือระหว่างประเทศในการต่อสู้กับอาชญากรรมทางคอมพิวเตอร์ได้เพิ่มมากขึ้นทั้งในระดับภูมิภาคและระดับโลก เมื่อประเทศต่าง ๆ ได้ตระหนักว่าอาชญากรรมทางคอมพิวเตอร์ได้พัฒนาศักยภาพมากขึ้นตามนวัตกรรมและเทคโนโลยี โดยอาศัยอินเตอร์เน็ตซึ่งเชื่อมแต่ละชาติเข้าด้วยกันอย่างไร้พรหมแดนและมีผู้ใช้งานเป็นจำนวนมาก[92] ซึ่งทำให้การกระทำผิดทางคอมพิวเตอร์กลายเป็นอาชญากรรมข้ามชาติ (Transnational Crime) ที่อาชญากรสามารถใช้ประโยชน์จากช่องโหว่ทางกฎหมายที่เกิดจาก

---

[90] The Third Interpol Symposium on International Fraud, Saint-Cloud, Paris. France, December 11-13, 1979.

[91] การประชุมจัดโดยองค์กรตำรวจสากลร่วมกับผู้พิพากษา Stein Schjoberg ชาวนอร์เวย์ มีผู้เข้าร่วม 66 คนจาก 26 ประเทศ โดยผู้ปราศรัยหลักในงานคือ Donn B.Parker จาก SRI International แคลิฟอเนีย ประเทศสหรัฐอเมริกา ผู้ก่อตั้ง “combat against computer crime”, Schjolberg, S., *Crossing jurisdictional boundaries*, (Hague, Netherland: Europol Headquarter, 2013), Retrieved 23 February, 2014, from http://www.cybercrimelaw.net/documents/Europol-INTERPOL.pdf

[92] นับตั้งแต่ปี พ.ศ. 2543-2554 การใช้งานอินเตอร์เน็ตของโลกขยายตัวขึ้นกว่า 528.1% โดยมีผู้ใช้อินเตอร์เน็ตกว่า 2,267,233,742 คน คิดเป็นกว่า 32.7% ของประชากรโลกทั้งหมด โดยทวีปเอเชียมีอัตราขยายตัวของผู้ใช้งานอินเตอร์เน็ตกว่า 789.6%, *World Internet Users and Population Stats*, Retrieved 2014, February 23, from http://www.internetworldstats.com/ stats.htm

ความแตกต่างกันในข้อกฎหมายของแต่ละประเทศเป็นช่องทางในการกระทำผิด ดังนั้นความร่วมมือในการสร้างมาตรฐานกลางเพื่อเป็นแนวทางในการออกกฎหมายภายในของแต่ละประเทศ รวมไปถึงการกำหนดมาตรการความร่วมมือที่ชัดเจนเพื่อนำไปสู่การกระบวนการสืบสวนสอบสวนและส่งตัวผู้กระทำผิดที่มีประสิทธิภาพจึงเป็นจุดมุ่งหมายที่สำคัญของความร่วมมือเพื่อรับมืออาชญากรรมทางคอมพิวเตอร์

การสร้างฐานความผิดทางอาญาเพื่อคุ้มครองข้อมูลและการสื่อสารในระบบเครือข่ายนั้น กฎหมายต้องปัจจุบันถูกตราออกมาอย่างชัดเจนและเฉพาะเจาะจงที่สุดเท่าที่จะทำได้ โดยลดการตีความอย่างคลุมเครือจากกฎหมายที่มีอยู่เดิม เมื่อกฎหมายอาชญากรรมคอมพิวเตอร์ถูกนำมาปรับใช้ ผู้กระทำผิดจะถูกพิสูจน์ว่ากระทำผิดอย่างชัดแจ้งและไม่ใช่ด้วยการตีความฐานความผิดของกฎหมายที่มีอยู่เดิมให้กว้างขึ้น หรือโดยกฎหมายที่ถูกตราเพื่อวัตถุประสงค์อื่นที่ครอบคลุมในเรื่องอาชญากรรมทางคอมพิวเตอร์เพียงเล็กน้อยเท่านั้น

หนึ่งในวัตถุประสงค์สำคัญของการบัญญัติกฎหมายอาญาคือเพื่อป้องกันการกระทำผิด ผู้ที่มีความเสี่ยงจะกระทำผิดต้องได้รับการเตือนอย่างชัดเจนว่าการกระทำเช่นนั้นจะไม่ได้รับการให้อภัย บนระบบเครือข่ายด้วย และเมื่อการกระทำผิดเกิดขึ้น ผู้กระทำผิดต้องถูกตัดสินโทษจากการกระทำผิดที่ถูกกระทำโดยชัดแจ้ง และเพียงพอต่อการขัดขวางไม่ให้เกิดการกระทำผิดซ้ำอีก หลักการพื้นฐานเหล่านี้สามารถนำมาใช้กับอาชญากรรมทางคอมพิวเตอร์ได้เช่นกัน

อาชญากรรมทางคอมพิวเตอร์ รวมถึงการโจมตีร่วมกันขนานใหญ่ต่อโครงสร้างพื้นฐานทางข้อมูลข่าวสารสำคัญของประเทศ และการกระทำผิดของผู้ก่อการร้ายโดยใช้อินเตอร์เน็ตเป็นเครื่องมือเป็นอาชญากรรมระดับโลก พื้นที่ระบบเครือข่ายกลายเป็นสภาวะแวดล้อมใหม่ของการกระทำผิดทางอาญา ความพยายามในการสร้างความสอดคล้องของกฎหมายภายในประเทศแต่ละประเทศควรถูกกระทำผ่านองค์กรระหว่างประเทศ ในรูปของอนุสัญญา (Convention) ข้อเสนอแนะ (Recommendations) และการสร้างคู่มือนโยบาย (Guideline)

เป้าหมายหลักในการการสร้างความมั่นคงบนอินเตอร์เน็ตในระดับสากล คือ การเสริมยุทธศาสตร์เพื่อการพัฒนาต้นแบบกฎหมายอาชญากรรมทางคอมพิวเตอร์ซึ่งสามารถประยุกต์ใช้ได้ในระดับโลกและทำงานร่วมกันได้กับกฎหมายภายในประเทศและมาตรการทางกฎหมายที่มีอยู่เดิมของภูมิภาคต่าง ๆ

เพื่อที่จะสามารถปรับปรุงกฎหมายให้มีความสอดคล้องกันในระดับโลกในเรื่องอาชญากรรมทางคอมพิวเตอร์ รวมไปถึงการสร้างความเข้าใจร่วมกันในเรื่องความมั่นคงไซเบอร์และอาชญากรรมไซเบอร์ระหว่างประเทศ ในทุกระดับการพัฒนา การสร้างข้อตกลงระดับโลกของ

องค์การสหประชาชาติควรถูกจัดตั้งขึ้นโดยมีเป้าหมายเพื่อชี้ให้เห็นถึงอุปสรรคและปัญหาอย่างครอบคลุมและทั่วถึง

3.1 องค์กรระหว่างประเทศที่ดูแลเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์

3.1.1 องค์กรเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (Organization for Economic and Co-operation Development: OECD)

ในปี พ.ศ. 2525 OECD เป็นองค์กรแรกที่ออกข้อเสนอแนะเกี่ยวกับอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ตามออกมา โดยการประชุม OECD ณ กรุงปารีสได้ตัดสินใจจัดตั้งคณะกรรมการผู้เชี่ยวชาญและเพื่ออภิปรายในเรื่องอาชญากรรมที่เกี่ยวกับคอมพิวเตอร์ และความต้องการในการแก้ไขกฎหมายอาญา จากผลของข้อเสนอของกรรมการผู้เชี่ยวชาญและของคณะกรรมการ ICCP ของ OECD ในปี พ.ศ. 2529 ได้มีข้อแนะนำซึ่งมีใจความดังนี้

“ด้วยประเด็นที่เกี่ยวข้องกับอาชญากรรมข้ามชาติของกิจกรรมการกระทำผิดในส่วนของอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ ซึ่งปัญหาสำคัญได้ชี้ไปยังความประสงค์เพื่อสร้างความร่วมมือระหว่างประเทศในการปราบปรามและควบคุมกิจกรรมดังกล่าว และการที่ประเทศสมาชิกจะพิจารณาว่าการกระทำใด ซึ่งทราบได้ว่ากระทำภายในขอบเขตดังกล่าวนี้ควรอยู่ภายใต้บังคับของกฎหมายอาญาของชาติ โดยการกระทำเหล่านี้อาจถูกแสดงออกอย่างกว้างที่สุดเท่าที่จะทำได้ในทางปฏิบัติมากกว่าเทคโนโลยี”[93]

โดยรายการของการกระทำที่อาจเข้าข่ายการกระทำผิดที่กฎหมายของประเทศสมาชิกที่สามารถสร้างให้ครอบคลุมร่วมกันได้ถูกเสนอแนะขึ้นมา ซึ่งรายการดังกล่าวประกอบไปด้วย การฉ้อโกงทางคอมพิวเตอร์ การปลอมแปลงทางคอมพิวเตอร์ การทำความเสียหายต่อข้อมูลคอมพิวเตอร์หรือโปรแกรม และการละเมิดต่อโปรแกรมคอมพิวเตอร์ถูกป้องกันไว้โดยไม่ได้รับอนุญาต[94] เป็นต้น

---

[93] “With respect to the transnational aspects of computer-related criminal activity, important issues have been noted which point to the desirability for international cooperation in repressing and controlling such activity. And that all member countries consider the extent to which acts committed knowingly in this field should be covered by national penal legislation. These acts may be expressed as far as possible in terms of functions rather than technology.”, Organization for Co-operation Development, *Computer related criminality: Analysis of legal politics in the OECD area*.

[94] Ibid.

โดยในปี พ.ศ. 2545 OECD ได้ออก Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security[95] เพื่อเป็นแนวทางในด้านความปลอดภัยของระบบเครือข่ายข้อมูลข่าวสาร

OECD เป็นองค์กรระหว่างประเทศองค์กรแรก ๆ ที่ริเริ่มวางแนวทางสำหรับอาชญากรรมทางคอมพิวเตอร์ ปัจจุบันนี้ OECD ไม่ได้มุ่งเน้นไปที่อาชญากรรมทางคอมพิวเตอร์โดยตรง แต่องค์กรได้มุ่งเน้นในด้านความมั่นคงทางโครงข่าย (Cyber security) มากกว่า และสนับสนุนความร่วมมือในด้านนโยบายระดับนานาชาติ เพื่อสร้างความน่าเชื่อถือและความมั่นใจ โดย OECD Working Party on Information and Privacy (WPISP) ทำหน้าที่ในการพัฒนาแนวทางระหว่างประเทศ

3.1.2 องค์การสหประชาชาติ (United Nations: UN)

องค์การสหประชาชาติได้เริ่มพัฒนากรอบนโยบายด้านอาชญากรรมทางคอมพิวเตอร์ขึ้นในปี พ.ศ. 2533 ในการประชุมสหประชาชาติครั้งที่ 8 ว่าด้วยการป้องกันอาชญากรรมและการปฏิบัติต่อผู้กระทำผิด (8th United nations congress on the prevention of crime and treatment of offenders) ซึ่งกำหนดมาตรการเกี่ยวกับอาชญากรรมคอมพิวเตอร์ในข้อมติที่ 45/121

ต่อมาในปี พ.ศ. 2537 สหประชาชาติได้จัดทำคู่มือการป้องกันและควบคุมอาชญากรรมทางคอมพิวเตอร์ (UN manual on the prevention and control of computer-related crime)[96] ออกเผยแพร่ ซึ่งมีเนื้อหาเกี่ยวกับแนวทางการบัญญัติฐานความผิดและกฎหมายวิธีพิจารณาความที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์ รวมไปถึงกลไกความร่วมมือระหว่างประเทศ

การประชุมทั่วไปขององค์การสหประชาชาติได้มีมติเกี่ยวกับอาญากรรมทางคอมพิวเตอร์หลายประการ โดยข้อมติการประชุมทั่วไปที่ 55/63 ของวันที่ 4 ธันวาคม พ.ศ. 2543 และ 56/121 ของ 19 ธันวาคม พ.ศ. 2544 หัวข้อ “การรับมือกับการใช้งานเทคโนโลยีข้อมูลข่าวสารในทางที่ผิดของอาชญากร[97]” นั้นมีความสำคัญที่สุด โดยข้อมติที่ 55/63 มีเนื้อหาดังนี้

(a) รัฐควรทำให้แน่ใจว่ามีกฎหมายและการดำเนินการเพื่อทำลายแหล่งหลบภัยของผู้ซึ่งกระทำผิดโดยอาศัยเทคโนโลยีข้อมูลข่าวสารเป็นเครื่องมือ

---

[95] Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, *OECD*, Retrieved 2014, February 23, from http://www.oecd.org/internet/interneteconomy/15582260.pdf

[96] United Nations, International review of criminal policy, *The United Nations Manual on computer-related crime*, *43-44*(1994). Retrieved 2014, February 23, from http://www.uncjin.org/Documents/EighthCongress.html.

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

(b) ระบบยุติธรรมควรคุ้มครองความลับ ความสมบูรณ์ และสภาพพร้อมใช้งาน ของข้อมูลและระบบคอมพิวเตอร์ จากการเข้ามาสร้างความเสียหายโดยไม่ได้รับอนุญาต และรับรองว่าการกระทำผิดของอาชญากรต้องได้รับการลงโทษ

ข้อมติที่ 56/121 ของสมัชชาใหญ่แห่งองค์การสหประชาชาติ ชักชวนให้ประเทศสมาชิกนำเอางานและผลสัมฤทธิ์ของคณะกรรมการป้องกันอาชญากรรมและกระบวนการทางอาญามาเพื่อพิจารณานอกเหนือจากปัจจัยอื่น ๆ ด้วยเมื่อออกกฎหมาย นโยบาย หรือแนวทางปฏิบัติระดับชาติในการรับการใช้ข้อมูลข่าวสารเพื่อกระทำผิดของอาชญากร[98]

การประชุมสหประชาชาติว่าด้วยอาชญากรรม (United nations crime congresses) ได้พิจารณาถึงปัญหาทางเทคนิค และการบังคับใช้กฎหมายอาชญากรรมที่เกี่ยวข้องกับการใช้คอมพิวเตอร์โดยมิชอบ และโดยการประชุมสหประชาชาติครั้งที่ 8 ว่าด้วยการป้องกันอาชญากรรมและการปฏิบัติต่อผู้กระทำผิด (8th United nations congress on the prevention of crime and the treatment of offenders) ที่เมืองฮาวานา ประเทศคิวบา ในปี พ.ศ. 2533 ที่ประชุมได้มีมติได้มีการออกกฎหมายอาชญากรรมทางคอมพิวเตอร์มาใช้

ต่อมาการประชุมสหประชาชาติว่าด้วยอาชญากรรมในกรุงเทพมหานคร ซึ่งที่ประชุมได้มีการออกปฏิญญากรุงเทพ เพื่อมุ่งเน้นไปที่ปัญหาเกี่ยวกับอาชญากรรมคอมพิวเตอร์ โดยข้อที่ 16 ของปฏิญญากรุงเทพ สำนักงานป้องกันยาเสพติดและปราบปรามอาชญากรรมแห่งสหประชาชาติ (UN office on drugs and crime) ได้กำหนดว่า

“เรารับทราบว่าในยุคโลกาภิวัตน์ เทคโนโลยีสารสนเทศและการพัฒนาอย่างรวดเร็วของระบบโทรคมนาคมและเครือข่ายคอมพิวเตอร์แบบใหม่ได้มีการใช้เทคโนโลยีดังกล่าวในทางที่ผิดเพื่อวัตถุประสงค์ในทางอาชญากรรมรวมอยู่ด้วย เพราะฉะนั้นเราจึงยินดีในความพยายามที่จะขยายและเพิ่มความร่วมมือที่มีอยู่เพื่อป้องกัน สืบสวนสอบสวน และฟ้องคดีการกระทำความผิดที่เกี่ยวข้องกับเทคโนโลยีระดับสูงและคอมพิวเตอร์ รวมถึงการพัฒนาความร่วมมือภาคเอกชน เราขอยอมรับการมีส่วนร่วมอย่างสำคัญของสหประชาชาติ และเวทีระดับภูมิภาคและระดับระหว่างประเทศอื่น ๆ ในการต่อต้านอาชญากรรมเกี่ยวกับคอมพิวเตอร์ และขอเชิญชวนคณะกรรมาธิการว่าด้วยการป้องกันอาชญากรรมและความยุติธรรมทางอาญาตรวจสอบความเป็นไปได้ในการให้ความ

---

[98] “…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.

ช่วยเหลือเพิ่มเติมในเรื่องดังกล่าวภายใต้การสนับสนุนของสหประชาชาติ โดยร่วมกับองค์กรอื่นที่มีวัตถุประสงค์คล้ายกันโดยพิจารณาจากประสบการณ์ที่มี[99]"

3.1.3 สหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunications Union: ITU)

สหภาพโทรคมนาคมระหว่างประเทศ เป็นหน่วยงานที่มีบทบาทมากที่สุดในการสร้างมาตรฐานกลางของระบบการรักษาความปลอดภัยไซเบอร์ของโลก และ การออกกฎหมายอาชญากรรมทางอินเตอร์เน็ต

การประชุมทั่วไปสหประชาชาติในปี พ.ศ. 2543 ทำให้เกิดความต้องการในการทำการประชุมแบบเป็นหลายลำดับขั้นตอน (Multi-phase) ของการประชุมสุดยอดระดับโลกว่าด้วยสังคมสารสนเทศ (World Summit on Information Society: WSIS) และขอให้ ITU รับบทบาทเป็นผู้นำในการประสานความร่วมมือของผู้มีส่วนเกี่ยวข้อง โดย ลำดับขั้นที่ 1 จัดขึ้นในเจนีวา ในเดือนธันวาคม พ.ศ. 2546 และลำดับที่ 2 ปี พ.ศ. 2548 ในตูนีเซีย ตามมาด้วยการประชุม WSIS และ ITU Plenipotentiary conference ในปี พ.ศ. 2549 ITU มีบทบาทสำคัญในการผสานความร่วมมือและสร้างความมั่นใจในการรักษาความปลดภัยในการใช้งาน ICT ของโลก

ในการประชุม WSIS ปี พ.ศ. 2548 ณ กรุงตูนิส ประเทศตูนีเซีย ITU ได้รับมอบหมายให้เป็นวิทยากรกระบวนการ (Facilitator) สำหรับ Action line 5 "สร้างคามมั่นใจและความปลอดภัยในการใช้งานเทคโนโลยีข้อมูลข่าวสาร[100]"

เลขาธิการใหญ่ของสหภาพโทรคมนาคมระหว่างประเทศ ได้ริเริ่มโครงการ Global Cybersecurity Agenda: GCA ซึ่งโครงการนี้ได้เริ่มดำเนินการเมื่อเดือนพฤษภาคม พ.ศ. 2550 และโครงการนี้มีวัตถุประสงค์เพื่อ เป็นกรอบเค้าโครงของการอภิปรายและความร่วมมือระหว่างประเทศซึ่งมุ่งหมายเพื่อเสนอยุทธศาสตร์สำหรับวิธีการในการเสริมประสิทธิภาพการรักษาความปลอดภัยในสังคมข้อมูลข่าวสาร ทั้งนี้ GCA มีเป้าหมายทางยุทธศาสตร์ สำหรับมาตรการทางการออกกฎหมาย รายละเอียดเพิ่มเติมของยุทธศาสตร์สำหรับการพัฒนาต้นแบบการออกกฎหมายอาชญากรรมไซเบอร์ซึ่งสามารถนำมาประยุกต์ใช้ได้กับกฎหมายทั้งในระดับโลก ระดับภูมิภาคและระดับชาติ (Interoperable) ที่มีอยู่เดิม

---

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

[100] WSIS Action line 5 Building confidence and security in the use of information and communication technologies (ICTs), Retrieved 2014, February 23, from http://www.itu.int/wsis/stocktaking/help-action-lines.html

นอกจากนี้ ITU ได้ก่อตั้ง High Level Express Group: HLEG ขึ้นเมื่อเดือนตุลาคมปี พ.ศ. 2550 โดยประกอบไปด้วยกลุ่มของผู้เชี่ยวทั่วโลกกว่า 100 คน โดยมีวัตถุประสงค์เพื่อพัฒนาข้อเสนอทางยุทธศาสตร์ด้านอาชญากรรมทางคอมพิวเตอร์ให้แก่รัฐสมาชิกของ ITU และในปี พ.ศ. 2551 HLEG ได้ให้คำแนะนำเรื่องยุทธศาสตร์ใน 5 หมวดหมู่ด้วยกัน ได้แก่ มาตรการทางกฎหมาย มาตรการทางเทคนิคและกระบวนการ โครงสร้างอย่างเป็นระบบ การสร้างสมรรถภาพ และ ความร่วมมือระหว่างประเทศ

โดยสรุปแล้ว เป้าหมายหลักของ ITU คือการหาข้อสรุปในการสร้างมาตรฐานกลางของกรอบความร่วมมือระหว่างประเทศในการรักษาความปลอดภัยไซเบอร์ และเพื่อที่จะบรรลุถึงความเข้าใจร่วมกันในปัญหาภัยคุกคามทางอินเตอร์เน็ตของนานาประเทศในทุกระดับของการพัฒนาเศรษฐกิจ ซึ่งรวมไปถึงการพัฒนาและนำไปปฏิบัติซึ่งแนวทางการแก้ไขปัญหาที่มุ่งเป้าไปยังการระบุปัญหาอาชญากรรมทางคอมพิวเตอร์และความปลอดภัยไซเบอร์ในฐานะของภัยคุกคามในระดับโลก โดย ITU ได้ใช้ GCA เป็นกรอบเค้าโครงในการเสนอยุทธศาสตร์เพื่อเสริมความมั่นใจและการรักษาความปลอดภัยในสังคมข้อมูลข่าวสาร ภายใต้การรักษาความปลอดภัยไซเบอร์ โดยหลักการนี้ถูกนำมาใช้ใน Tunis Agenda 2005 ของ WSIS[101]

3.1.4 กลุ่มประเทศ G-8 (G8 group of states)

กลุ่ม G8 หรือ Group of eight ประกอบไปด้วยหัวหอกประเทศอุตสาหกรรมใหญ่ 8 ประเทศด้วยกัน ได้แก่ สหรัฐอเมริกา อังกฤษ รัสเซีย ฝรั่งเศส อิตาลี ญี่ปุ่น และแคนาดา ได้ออก Ministers' Communiqué ที่ประกอบไปด้วยแผนปฏิบัติการและหลักในการรับมืออาชญากรรมคอมพิวเตอร์และคุ้มครองข้อมูลและระบบคอมพิวเตอร์ G8 ยังประกาศว่าเจ้าหน้าที่ผู้บังคับใช้กฎหมายต้องได้รับการฝึกฝนและอุปกรณ์เพียบพร้อมในการต่อกรกับอาชญากรรมคอมพิวเตอร์และมอบหมายให้ประเทศสมาชิกมีการติดต่อสื่อสารกันตลอด 24 ชม.

---

[101] "Paragraph 40 Tunis Agenda 2005, We call upon governments in cooperation with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, UNGA Resolutions 55/63 and 56/121 on "Combating the criminal misuse of information technologies" and regional initiatives including, but not limited to, the Council of Europe's Convention on Cybercrime.

Paragraph 42 Tunis Agenda 2005, We affirm that measures undertaken to ensure Internet stability and security, to fight cybercrime and to counter spam, must protect and respect the provisions for privacy and freedom of expression as contained in the relevant parts of the Universal Declaration of Human Rights and the Geneva Declaration of Principles., Retrieved 2014, February 23, from http://www.itu.int/wsis/docs2/tunis/off/6rev1.html

กลุ่มประเทศ G8 ได้ก่อตั้งคณะอนุกรรมการด้านอาชญากรรมที่ใช้เทคโนโลยีขั้นสูง (G8 Subgroup on High-tech Crime) ขึ้นในปี พ.ศ. 2540 โดยคณะอนุกรรมการชุดนี้ได้จัดทำหลักการด้านอาชญากรรมทางคอมพิวเตอร์ซึ่งควรที่ประเทศต่าง ๆ จะนำไปปฏิบัติ[102] เช่น ควรมีระบบกฎหมายเอื้อให้สามารถเก็บรักษาข้อมูลและเข้าถึงข้อมูลเพื่อกระทำการสืบสวนสอบสวน ควรประสานความร่วมมือระหว่างประเทศในการแลกเปลี่ยนข้อมูลข่าวสารเพื่อให้สามารถรวบรวมพยานหลักฐานได้อย่างทันท่วงที ควรสร้างมาตรฐานในการสืบค้นพยานหลักฐานที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ ฯลฯ

และในการประชุม G8 ณ กรุงวอชิงตันดีซี ประเทศสหรัฐอเมริกา เมื่อปี พ.ศ. 2547 โดยกลุ่ม G8 ได้นำเอาหลักปฏิบัติในการรับมืออาชญากรรมทางคอมพิวเตอร์ดังกล่าวมาใช้ โดยมีเป้าหมายเพื่อทำให้แน่ใจว่าอาชญากรจะไม่มีแหล่งหลบภัยไม่ว่าที่ใดในโลก

นอกจากนี้ ในการประชุมระดับรัฐมนตรียุติธรรมและกิจการภายในของกลุ่มประเทศ G8 ได้ออกแถลงการณ์ร่วม ว่าด้วยการเริ่มมีผลบังคับใช้ของอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของสหภาพยุโรป โดยกระตุ้นให้รัฐต้องเริ่มดำเนินการนำเอามาตรฐานทางกฎหมายทั่วไปที่อนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์มีอยู่มาใช้อย่างกว้าง ๆ (ณ กรุงวอชิงตัน ดีซี ประเทศสหรัฐอเมริกา ระหว่างวันที่ 10-11 พฤษภาคม พ.ศ. 2547)

ในปี พ.ศ. 2548 แถลงการณ์ของการประชุม G8 มีเป้าหมายในเรื่องกฎหมายอาชญากรรมทางคอมพิวเตอร์ซึ่งถูกเน้นหนักคือ

“เพื่อให้แน่ใจว่าหน่วยงานบังคับใช้กฎหมายสามารถตอบสนองต่อภัยไซเบอร์และอุบัติภัยได้อย่างทันท่วงที”

ในปี พ.ศ. 2549ในการประชุมรัฐมนตรียุติธรรมและกิจการภายในกลุ่มประเทศ G8 ณ กรุงมอสโคว ได้มีการอภิปรายเกี่ยวกับอาชญากรรมคอมพิวเตอร์และปัญหาในไซเบอร์สเปซ โดยคำแถลงได้ถูกเน้นหนักดังนี้

“เราได้อภิปรายปัญหาเกี่ยวข้องกับการแบ่งปันประสบการณ์สั่งสมร่วมกันในระดับนานาชาติเพื่อรับมือการก่อการร้ายเช่นเดียวกับการวิเคราะห์เชิงเปรียบเทียบของกฎหมายที่เกี่ยวข้อง เราได้อภิปรายถึงความจำเป็นในการพัฒนามาตรการตอบโต้ที่มีประสิทธิภาพซึ่งจะป้องกันการก่อการร้าย IT และการกระทำอันมีลักษณะเป็นการก่อการร้ายในขอบเขตของวิทยาการขั้นสูง เพื่อการนั้นจึงจำเป็นต้องสร้างชุดของมาตรการป้องกันการกระทำผิดเช่นนั้น รวมไปถึงในขอบเขตของการ

---

[102] Meeting of G8 Justice and Interior Ministers, *Principles and action plan to combat high-tech crime*, (Washington, D.C.: n.p., 1997), Retrieved 2014, February 24, from http://www.coe.int/T/e/legal_affairs/Legal_cooperation/Fight_against_terrorism/Texts_&_documents/Principles%20and%20Action.pdf

โทรคมนาคม โดยประกอบด้วยงานต่อต้านการขายข้อมูลส่วนบุคคล ข้อมูลเท็จและโปรแกรมประยุกต์ประเภทไวรัสและโปรแกรมคอมพิวเตอร์ที่เป็นอันตรายอื่น ๆ เราจะอบรมผู้เชี่ยวชาญของเราเพื่อให้กำเนิดวิธีการเข้าถึงที่เป็นหนึ่งเดียวในการต่อสู้กับอาชญากรรมไซเบอร์ และเราจำเป็นต้องมีฐานทางกฎหมายระหว่างประเทศเพื่อใช้ในงานนี้ และเราจะประยุกต์ใช้ทุกสิ่งที่กล่าวมาข้างต้นเพื่อป้องกันผู้ก่อการร้ายจากการใช้คอมพิวเตอร์และเว็บไซต์อินเตอร์เน็ตในการว่าจ้างผู้ก่อการร้ายหน้าใหม่และชักชวนให้เข้าร่วมเป็นผู้กระทำผิดกฎหมายอื่น ๆ"[103]

ต่อมาในการประชุมสุดยอดผู้นำ G8 ณ กรุงเซนต์ ปีเตอร์สเบิร์ก ในปี พ.ศ. 2549 แถลงการณ์การประชุมตอบโต้การก่อการร้ายมีประกอบไปด้วยข้อความดังต่อไปนี้

"เรายืนยันพันธสัญญาในการทำงานร่วมกันกับพันธมิตรนานาประเทศเพื่อต่อสู้กับภัยก่อการร้าย รวมทั้ง

การนำไปปฏิบัติและพัฒนากรอบเค้าโครงกฎหมายระหว่างประเทศเพื่อตอบโต้การก่อการร้าย

การตอบโต้อย่างมีประสิทธิภาพต่อความพยายามใช้ไซเบอร์สเปซเพื่อวัตถุประสงค์ในการก่อการร้าย รวมถึงการปลุกปั่นให้กระทำการ สื่อสารเพื่อวางแผนก่อการร้าย เช่นเดียวกับการชักชวนให้เข้าร่วมและฝึกฝนผู้ก่อการร้าย"

สำหรับการประชุมรัฐมนตรียุติธรรมและกิจการภายในกลุ่มประเทศ G8 ณ กรุงมิวนิก ประเทศเยอรมณีในระหว่างวันที่ 23-25 พฤษภาคม พ.ศ. 2550 ตัวแทนต่างตกลงที่จะ "มุ่งทำให้การใช้อินเตอร์เน็ตอย่างผิดกฎหมายที่มีรูปแบบเฉพาะเป็นความผิดอาญาภายใต้กรอบเค้าโครงของกฎหมายระดับชาติ"

3.1.5 สหภาพยุโรป (European Union: EU)

สหภาพยุโรปได้ดำเนินการเกี่ยวกับอาชญากรรมคอมพิวเตอร์หลายประการ โดยได้ริเริ่มอย่างจริงจังในปี พ.ศ. 2541 เมื่อคณะกรรมาธิการยุโรป (European Commission) ได้นำเสนอผล

---

[103] "We also discussed issues related to sharing accumulated international experience in combating terrorism, as well as comparative analysis of relevant pieces of legislation on that score. We discussed the necessity of improving effective countermeasures that will prevent IT terrorism and terrorist acts in this sphere of high technologies. For that it is necessary to device a set of measures to prevent such possible criminal acts, including in the sphere of telecommunication. That includes work against the selling of private data, counterfeit information and application of viruses and other harmful computer programs. We will instruct our experts to generate unified approaches to fighting cyber criminality, and we will need an international legal base for this particular work, and we will apply all of that to prevent terrorists from using computer and Internet sites for hiring new terrorists and the recruitment of other illegal actors.", *Press Conference on the Results of the G8 Justice and Home Affairs Ministerial*, (16 June 2006), Retrieved 2014, February 24, from http://www.g8.utoronto.ca/justice/justice2006.htm

การศึกษาเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ (Legal Aspects of Computer-Related Crime in the Information Society: COMCRIME study) ต่อสภายุโรป (Europe on Council) โดยมีเนื้อหาเกี่ยวกับภาพรวมของการก่ออาชญากรรมและแนวทางการแก้ไขด้านต่าง ๆ และต่อมาในปี พ.ศ. 2543 สภายุโรปและ คณะกรรมาธิการยุโรปได้จัดทำแผน eEurope Action ขึ้นซึ่งเป็นส่วนหนึ่งของแผนดังกล่าว โดยได้ระบุวิธีการดำเนินการเพื่อส่งเสริมให้เครือข่ายคมนาคมมีความปลอดภัย และส่งเสริมความร่วมมือในการแก้ไขปัญหาอาชญากรรมทางคอมพิวเตอร์ให้บรรลุผลสำเร็จภายในปี พ.ศ. 2545

นอกจากนี้คณะกรรมาธิการยุโรปได้เผยแพร่เอกสารที่มีชื่อว่า Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime[104] โดยมีวัตถุประสงค์เพื่อสร้างความตื่นตัวเกี่ยวกับการก่อการอาชญากรรมบนอินเตอร์เน็ตและวิธีการจัดการกับปัญหาอาชญากรรมทางคอมพิวเตอร์ทั้งที่อยู่ในรูปของกฎหมายและไม่เป็นกฎหมายโดยการร่วมมือระหว่างหน่วยงานด้านการบังคับใช้กฎหมายกับฝ่ายต่าง ๆ ที่เกี่ยวข้องอาทิ ผู้ให้บริการ ผู้บริโภค รวมไปถึงองค์กรด้านการคุ้มครองข้อมูลส่วนบุคคลต่าง ๆ ด้วยเหตุนี้เองจึงได้มีการจัดตั้ง EU Forum on Cybercrime เพื่อให้เป็นเวทีแลกเปลี่ยนความรู้และก่อให้เกิดความร่วมมือกันระหว่างหน่วยงานด้านการบังคับใช้กฎหมายกับฝ่ายที่เกี่ยวข้องข้างต้นในเวลาต่อมา

ต่อมาในปี พ.ศ. 2544 คณะกรรมาธิการยุโรปได้เสนอ ข้อเสนอ “Network and Information Security: Proposal for a European Policy Approach[105]” โดยมีวัตถุประสงค์เพื่อชี้ให้เห็นถึงการคุกคามความมั่นคงหรือความปลอดภัยของระบบคอมพิวเตอร์ด้วยวิธีการต่าง ๆ และข้อเสนอแนะในการกำหนดนโยบายด้านการรักษาความมั่นคง อาทิมาตรการทางสังคม กฎหมาย และมาตรการทางเทคนิคอันรวมถึงมาตรฐานในการรักษาความมั่นคงต่าง ๆ

ในด้านมาตรการทางกฎหมายโดยเฉพาะนั้น คณะกรรมาธิการยุโรปได้นำเสนอโครงร่างที่ว่าด้วย Council Framework Decision on attacks against information systems[106] ต่อคณะกรรมาธิการ

---

[104] *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

[105] *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

[106] *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

ยุโรปในปี พ.ศ. 2545 โดยมีวัตถุประสงค์เพื่อนำเสนอรูปแบบการก่ออาชญากรรมทางคอมพิวเตอร์รูปแบบใหม่ ๆ และข้อเสนอในการบัญญัติกฎหมายอาชญากรรมทางคอมพิวเตอร์ภายในกลุ่มประเทศสมาชิกเพื่อให้มีความสอดคล้องกันทั้งกฎหมายสารบัญญัติและวิธีสบัญญัติ โดยเนื้อหาในส่วนของโครงร่างดังกล่าวได้มาจากการศึกษาเปรียบเทียบ Convention on Cybercrime ของสภายุโรป เช่น การกำหนดความผิดฐานการเข้าถึงระบบสารสนเทศโดยมิชอบ (Illegal access to Information Systems) ความผิดฐานรบกวนระบบสารสนเทศโดยมิชอบ (Illegal interference with Information Systems) ฯลฯ ทั้งนี้ ประเทศสมาชิกจะต้องปฏิบัติให้เป็นไปตามข้อเสนอภายในวันที่ 31 ธันวาคม พ.ศ. 2546[107]

3.1.6 องค์การสนธิสัญญาป้องกันแอตแลนติกเหนือ (North Atlantic Treaty Organization: NATO)

ได้จัด Science for Peace and Security Advanced Research Workshop ณ กรุงโซเฟีย ประเทศบัลแกเรีย เมื่อเดือนตุลาคม พ.ศ. 2549[108] โดยมุ่งความสนใจไปยังประเด็นการก่อการร้ายไซเบอร์ (Cyber Terrorism) และในปี พ.ศ. 2551 NATO ได้เปิด Center of excellence on cybercrime ณ กรุงทาลินน์ ประเทศเอสโตเนีย[109] เพื่อกระทำการวิจัยและฝึกฝนในเรื่องการรับมือสงครามไซเบอร์

3.1.7 ความร่วมมือทางเศรษฐกิจเอเชียแปซิฟิก (Asia-Pacific Economic Cooperation: APEC)

กลุ่มความร่วมมือทางเศรษฐกิจในเอเชียแปซิฟิกหรือ APEC ได้เริ่มให้ความสำคัญกับปัญหาอาชญากรรมคอมพิวเตอร์อย่างจริงจังตั้งแต่ปี พ.ศ. 2544 อันเป็นผลสืบเนื่องจากการผลักดันของสหรัฐอเมริกาที่ต้องการให้ประเทศต่าง ๆ ให้ความสำคัญกับปัญหาการก่อการร้ายมากยิ่งขึ้นภายหลังเหตุการณ์ก่อการร้ายเมื่อวันที่ 11 กันยายน พ.ศ. 2544

โดยในการประชุมระดับผู้นำ APEC ได้มีการออกแถลงการณ์เพื่อต่อต้านการก่อการร้าย (Statement on Counter-Terrorism) เพื่อประณามการก่อการร้ายและเพื่อเสริมสร้างความร่วมมือใน

---

[107] 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.

[108] SPS NATO, *Cyber terrorist-a serious threat to peace and security in the 21st century*, Retrieved 2014, April 6, from http://www.nato.int/science/news/2007/n070702b.htm

[109] NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia, Retrieved , 2014, April 6, from http://www.ccdcoe.org/

การป้องกันการก่อการร้าย ซึ่งส่วนหนึ่งของแถลงการณ์ดังกล่าวได้เรียกร้องให้ทุกเขตเศรษฐกิจใน APEC ให้ความสำคัญกับการป้องกันโครงสร้างพื้นฐานที่สำคัญของประเทศ และรวมถึงโครงสร้างพื้นฐานด้านโทรคมนาคมด้วย

เมื่อเดือนพฤษภาคม พ.ศ. 2545 ได้มีการประกาศปฏิญญาเซี่ยงไฮ้ (Shanghai Declaration) ซึ่งประกอบด้วยแถลงการณ์ด้านการรักษาความมั่นคงของโครงสร้างพื้นฐานสารสนเทศและการสื่อสาร (Statement on the Security of Information and Communications Infrastructures) ที่ได้รับความเห็นชอบจากเขตเศรษฐกิจที่เป็นสมาชิก APEC ในการดำเนินการกับการก่ออาชญากรรมทางคอมพิวเตอร์เข้าไว้ด้วย ซึ่งในแถลงการณ์ดังกล่าวนี้ยังได้มอบหมายให้คณะทำงานด้านโทรคมนาคมและสารสนเทศ (Telecommunications and Information Working Group: TEL Working Group) ให้ความสำคัญกับการป้องกันโครงสร้างพื้นฐานด้านสารสนเทศและการสื่อสารเป็นลำดับต้นๆ และในการประชุมครั้งที่ 26 ของ TEL Working Group ได้มีการจัดทำยุทธศาสตร์ด้านความมั่นคงของเครือข่าย (APEC Cyber Security Strategy) ซึ่งยุทธศาสตร์ดังกล่าวได้ผ่านการพิจารณาเห็นชอบจากรัฐมนตรี APEC (APEC Ministers) เมื่อเดือนตุลาคม พ.ศ. 2545 โดยยุทธศาสตร์ดังกล่าวประกอบไปด้วยประเด็นสำคัญดังนี้

การพัฒนากฎหมาย (Legal developments) โดยสมาชิก APEC ควรบัญญัติกฎหมายอาชญากรรมทางคอมพิวเตอร์หรือให้ความช่วยเหลือแก่สมาชิกอื่นในการบัญญัติกฎหมายภายที่มีเนื้อหาสอดคล้องกับอนุสัญญาอาชญากรรมทางคอมพิวเตอร์ (Convention on Cybercrime)

การให้ข้อมูลและประสานความร่วมมือ (Information sharing and cooperation) APEC จะให้ความช่วยเหลือสมาชิกในการพัฒนาและจัดตั้งสถาบันด้านการรักษาความมั่นคงทางเครือข่ายในลักษณะ Computer Emergency Response team: CERTs โดยมีความร่วมมือจากทั้งภาครัฐและเอกชน รวมทั้งส่งเสริมให้สมาชิก APEC เข้าร่วมเป็นสมาชิกของเครือข่าย High-tech Crime 24/7 point of Contact Network ซึ่งริเริ่มโดยกลุ่มประเทศ G8

การจัดทำแนวปฏิบัติด้านเทคนิคและความมั่นคง (Security and technical guidelines) เสนอให้มีการพัฒนามาตรฐานและแนวปฏิบัติด้านการรักษาความมั่นคง รวมทั้งเสนอให้มีการสำรวจกฎหมายภายในที่เกี่ยวข้องอาทิ การเข้ารหัส การใช้เทคโนโลยี PKI เป็นต้น

การสร้างความตื่นตัวให้กับประชาชน (Public awareness) สนับสนุนให้ประเทศสมาชิกสร้างความตื่นตัวด้านความมั่นคงแก่ประชาชนและภาคอุตสาหกรรม โดยอาศัยแนวทางขององค์การระหว่างประเทศอื่น ๆ ที่ได้จัดทำไว้แล้ว อาทิ แนวปฏิบัติด้านการรักษาความมั่นคงของระบบสารสนเทศและเครือข่ายของ OECD (Guidelines for the security of information systems and networks: towards a culture of security)

การฝึกอบรมและให้ความรู้ (Training and education) เสนอให้มีการจัดฝึกอบรมเพื่อให้ความรู้ทางเทคนิคการรักษาความมั่นคงและเทคนิคการสืบหาร่องรอยการกระทำผิด (Forensic) ตลอดจนประเด็นกฎหมายที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์ และส่งเสริมให้มีการเรียนการสอนด้านเทคโนโลยีความมั่นคง รวมถึงการสอบวัดมาตรฐานบุคคลที่ทำงานในด้านการรักษาความมันคงตลอดจนการสนับสนุนการพัฒนาวิชาการด้านการรักษาความปลอดภัย และ

การรักษาความมั่นคงในการสื่อสารแบบไร้สาย (Wireless security) เนื่องจากปัจจุบันมีการเชื่อมต่อกับระบบเครือข่ายผ่านอุปกรณ์สื่อสารแบบไร้สายเพิ่มมากขึ้น จึงจำเป็นที่จะต้องให้ความสนใจต่อการรักษาความปลอดภัยต่อการติดต่อสื่อสารแบบไร้สายนี้ด้วย โดยได้มีการเสนอให้มีการศึกษาถึงประเด็นต่าง ๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงในการติดต่อสื่อสารแบบไร้สายนี้เพิ่มมากขึ้น

นอกจากนี้ ในการประชุมดังกล่าวรัฐมนตรี APEC ยังมีความเห็นร่วมกันว่า ประเทศสมาชิก APEC ควรดำเนินการด้านอาชญากรรมทางคอมพิวเตอร์โดยเร่งด่วนใน 3 ประการดังนี้ด้วย คือ

3.1.7.1 บัญญัติกฎหมายที่เกี่ยวข้องกับความมั่นคงบนเครือข่าย (Cyber security) และอาชญากรรมคอมพิวเตอร์ (Cybercrime) ที่สอดคล้องกับแนวทางระหว่างประเทศอื่นที่สำคัญ อาทิ ข้อมติประชุมใหญ่สหประชาชาติที่ 55/63 และ อนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของสหภาพยุโรปให้แล้วเสร็จในเดือนตุลาคม พ.ศ.2546

3.1.7.2 จัดตั้งหน่วยงานด้านอาชญากรรมคอมพิวเตอร์ และหน่วยงานที่จะสามารถให้ความช่วยเหลือด้านอาชญากรรมทางคอมพิวเตอร์แก่ต่างประเทศภายในเดือนตุลาคม พ.ศ. 2546

3.1.7.3 จัดตั้งสถาบันเพื่อทำหน้าที่แลกเปลี่ยนข้อมูลเกี่ยวกับการรักษาความมั่นคงทางคอมพิวเตอร์ในทำนองเดียวกับ Computer Emergency Response Teams: CERTs ภายในเดือนตุลาคม พ.ศ. 2546

3.2 หลักเกณฑ์ระหว่างประเทศที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์

การมีหลักเกณฑ์กลางเพื่อให้แต่ละประเทศนำไปปฏิบัติบนบรรทัดฐานเดียวกันนั้นเป็นสิ่งสำคัญเพื่อเป็นการสร้างความสอดคล้องของกฎหมายภายในประเทศแต่ละประเทศ ดังเช่นที่ได้ระบุไว้ในคู่มือการป้องกันและควบคุมอาชญากรรมทางคอมพิวเตอร์ขององค์การสหประชาชาติ (UN Manual on the Prevention and Control of Computer-related Crime) ว่า “กฎหมาย ระบบยุติธรรมทางอาญา และความร่วมมือระหว่างประเทศไม่อาจก้าวทันความเปลี่ยนแปลงทางเทคโนโลยี มีเพียงบางประเทศเท่านั้นที่มีกฎหมายเพียงพอที่จะระบุต้นตอของปัญหา และเนื่องจากปัญหาที่กล่าวมานี้

จึงไม่มีประเทศใดสามารถแก้ปัญหาทางกฎหมาย การบังคับใช้ รวมไปถึงการป้องกันปัญหาต่าง ๆ ได้อย่างเด็ดขาด

เมื่อเรื่องนี้ได้ทวีความรุนแรงขึ้นไปสู่ระดับระหว่างประเทศ ปัญหาความขาดแคลนต่าง ๆ ได้ถูกขยายให้เด่นชัดมากขึ้น เพราะอาชญากรรมทางคอมพิวเตอร์เป็นอาชญากรรมข้ามชาติรูปแบบใหม่และการจะระบุถึงต้นตอของปัญหาได้อย่างมีประสิทธิภาพนั้นจำเป็นต้องมีความร่วมมืออย่างเห็นพ้องต้องกันของนานาชาติ โดยความร่วมมือดังกล่าวนี้จะเกิดขึ้นได้หากมีกรอบเค้าโครงร่วมกันเพื่อสร้างความเข้าใจว่าปัญหาคืออะไรและจะมีทางแก้ปัญหาอะไรบ้าง"[110] ในปัจจุบัน ความร่วมมือในรูปแบบนี้ได้เกิดขึ้นหลายประเภท เช่น ในรูปของสนธิสัญญา อนุสัญญา การทำสัญญาทวิภาคี บันทึกความเข้าใจ[111] ฯลฯ เพื่อเป็นแนวทางในการรับมือกับอาชญากรรมทางคอมพิวเตอร์ โดยความร่วมมือที่สำคัญและเป็นที่ยอมรับกันในระดับสากลในปัจจุบันนี้ได้แก่

3.2.1 คู่มือการป้องกันและควบคุมอาชญากรรมทางคอมพิวเตอร์ขององค์การสหประชาชาติ (UN Manual on the Prevention and Control of Computer-related Crime)

สมัชชาใหญ่แห่งองค์การสหประชาชาติ (United Nations General Assembly) ได้รับเอาข้อมติในเรื่องแนวทางการออกกฎหมายเพื่อรับมืออาชญากรรมทางคอมพิวเตอร์บนพื้นฐานของมติการประชุมที่ 45/121 (1990) หนึ่งในหลายๆ เรื่องที่ข้อมติได้กล่าวถึง มีการระบุถึงข้อเสนอแนะของการประชุมสหประชาชาติครั้งที่ 8 ว่าด้วยการป้องกันอาชญากรรมและการปฏิบัติต่อผู้กระทำผิด (8th Congress on the Prevention of Crime and the treatment of Offenders) ซึ่งจัดขึ้น ณ กรุงฮาวานา ประเทศคิวบา ระหว่างวันที่ 27 สิงหาคมถึง 7 กันยายน พ.ศ. 2533 ซึ่งในมติของที่ประชุมนี้เรียกร้อง

---

[110] "5. Laws, criminal justice systems and international cooperation have not kept pace with technological change. Only a few countries have adequate laws to address the problem, and of these, not one has resolved all of the legal, enforcement and prevention problems.

6. When the issue is elevated to the international scene, the problems and inadequacies are magnified. Computer crime is a new form of transnational crime and effectively addressing it requires concerted international cooperation. This can only happen, however, if there is a common framework for understanding what the problem is and what solutions there may be.", International Review of Criminal Policy, *UN Manual on the prevention and control of computer-related crime*, Retrieved 2014, April 6, from http://www.uncjin.org/Documents/EighthCongress.html

[111] เอ็มโอยู (Memorandum Of Understanding: MOU) หรือบันทึกความเข้าใจ เป็นหนังสือซึ่งฝ่ายหนึ่งแสดงความสมัครใจจะปฏิบัติอย่างหนึ่งอย่างใด และตามเงื่อนไขที่ปรากฏในหนังสือนั้นกับอีกฝ่ายหนึ่ง โดยที่หนังสือนี้ไม่ถือว่าเป็นสัญญาผูกมัด แต่แสดงความต้องการอันแน่วแน่ของผู้ลงนามว่าจะปฏิบัติดังที่ได้ระบุไว้ เช่น สถาบันการศึกษาแห่งหนึ่งในประเทศไทยทำบันทึกความเข้าใจกับสถาบันการศึกษาในต่างประเทศ เพื่อความร่วมมือทางวิชาการ การแลกเปลี่ยนอาจารย์และนักศึกษา.

ให้นานาประเทศเพิ่มความพยายามในการต่อสู้กับอาชญากรรมทางคอมพิวเตอร์ให้มีประสิทธิภาพมากขึ้น นับเป็นการกล่าวถึงเรื่องอาชญากรรมทางคอมพิวเตอร์เป็นครั้งแรกในมติของสมัชชาใหญ่แห่งองค์การสหประชาชาติ ก่อนอินเตอร์เน็ตจะเปิดให้เอกชนได้ใช้งานเสียอีก[112] องค์การสหประชาชาติได้นำแนวคิดดังกล่าวมาจัดทำ “คู่มือการป้องกันและควบคุมอาชญากรรมทางคอมพิวเตอร์ของขององค์การสหประชาชาติ” ซึ่งได้รับการตีพิมพ์เผยแพร่ในปี พ.ศ. 2537 โดยคู่มือได้ระบุถึงความจำเป็นในการปฏิรูปกฎหมายสบัญญัติและกฎหมายวิธีสารบัญญัติ ในการป้องกันอาชญากรรมผ่านการรักษาความปลอดภัยข้อมูลและความสำคัญของการสร้างความร่วมมือระหว่างประเทศ รวมไปถึงการนิยามรูปแบบของอาชญากรรมทางคอมพิวเตอร์รูปแบบต่าง ๆ เช่น การฉ้อโกง การปลอมแปลง วินาศกรรมคอมพิวเตอร์ การเข้าถึงโดยไม่ได้รับอนุญาต และการสำเนาโปรแกรมคอมพิวเตอร์

3.2.2 สนธิสัญญาว่าด้วยโทรคมนาคมระหว่างประเทศ (International Telecommunication Regulations: ITRs)

สนธิสัญญาว่าด้วยโทรคมนาคมระหว่างประเทศนี้ เกิดขึ้น ณ การประชุมผู้บริหารระดับโลกว่าด้วยการโทรเลขและโทรศัพท์ พ.ศ. 2531 (The 1988 World Administrative Telegraph and Telephone Conference: WATTC-88) ณ กรุงเมลเบิร์น ประเทศออสเตรเลีย โดยโดยสนธิสัญญานี้มีวัตถุประสงค์เพื่อกำหนดมาตรฐานในการให้บริการโทรคมนาคมระหว่างประเทศ และได้ออกข้อกำหนดต่าง ๆ ขึ้นมาบังคับใช้ เช่น

1. กำหนดการไหลเวียนของสัญญาณระหว่างผู้ให้บริการเครือข่ายโทรคมนาคม
2. กำหนดมาตรฐานของคุณภาพในบริการในระดับสากล ความเพียงพอของการให้บริการ
3. จัดสรรเส้นทางของสัญญาณระหว่างประเทศ และกำหนดมาตรฐานการบัญชีและการจ่ายค่าบริการระหว่างผู้ให้บริการ
4. กำหนดมาตรฐานในการลำดับความสำคัญในด้านความปลอดภัยและสุขภาพ
5. กำหนดแนวทางในการหลีกเลี่ยงอันตรายต่อระบบเครือข่ายและบริการต่าง ๆ

สนธิสัญญาว่าด้วยโทรคมนาคมระหว่างประเทศนี้อยู่ภายใต้การกำกับดูแลของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) โดยได้นำเอา ITRs กลับมาทบทวนอีกครั้งเพื่อทำการปรับปรุงแก้ไขให้ครอบคลุมไปถึงการจัดการดูแลอินเตอร์เน็ต ในการประชุมสากลว่าด้วยการโทรคมนาคม

---

[112] Lennon, L. Y.-c., *Cybercrime in the Greater China Region: Regulatory Responses and Crime Prevention Across the Taiwan Strait*, (United Kingdom: Edward Elgar publishing, 2012), 90.

ระหว่างประเทศ พ.ศ. 2555 (The 2012 World Conference on International Telecommunications) ณ กรุงดูไบ ประเทศสหรัฐอาหรับเอมิเรตส์ ระหว่างวันที่ 13-14 ธันวาคม พ.ศ. 2555 ทั้งนี้ ได้เปิดโอกาสให้ประเทศสมาชิกเข้าร่วมแสดงความคิดเห็นในร่างสนธิสัญญาว่าด้วยโทรคมนาคมระหว่างประเทศฉบับใหม่(Draft of the Future ITR)ที่ได้เพิ่มเติมประเด็นสำคัญที่เกี่ยวข้องกับอินเตอร์เน็ตไว้ เช่น

1. การจ่ายค่าใช้บริการแบบ Pay-Per-Click

2. กำหนดให้ผู้ผลิตเนื้อหาต้องจ่ายค่าตอบแทนให้แก่ผู้ให้บริการอินเตอร์เน็ต ด้วยแนวคิดที่ว่า “ฝ่ายส่งข้อมูลเป็นผู้จ่าย (Sending Party Network Pays)”

3. กำหนดให้มีการเปิดเผยประวัติการใช้งานของผู้ใช้อินเตอร์เน็ต

4. กำหนดนิยามของ Spam และขยายขอบเขตของ Cyber Security ให้ครอบคลุมไปถึงในส่วนของเนื้อหา

5. กำหนดนิยามศัพท์ที่เกี่ยวข้องกับอินเตอร์เน็ตเข้าไปในข้อบังคับด้วย

6. กำหนดให้สนธิสัญญาว่าด้วยโทรคมนาคมระหว่างประเทศมีสภาพเชิงบังคับ (Mandatory) ประเทศสมาชิกทุกประเทศจะต้องทำตามโดยไม่อาจตั้งข้อสงวนในข้อที่ไม่ต้องการผูกพันได้[113]

สำหรับ ส่วนที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์นั้น ได้มีข้อเสนอให้เพิ่มเติมมาตรา 5A และ 5B ลงไปใน ITRs เพื่อเพิ่มเสริมสร้างความมั่นคงในด้านโทรคมนาคมและเทคโนโลยีสารสนเทศ โดยได้รวมเอาเรื่องที่เกี่ยวข้องกับ Spam, อาชญากรรมทางคอมพิวเตอร์ (Cybercrime), ความมั่นคงไซเบอร์ (Cyber security), การสงวนรักษาข้อมูล (Data Preservation), การกักเก็บข้อมูล (Data Retention), การคุ้มครองข้อมูล (Data Protection), การคุ้มครองข้อมูลส่วนบุคคล (Protection of Personal Information), ความเป็นส่วนตัวและข้อมูล (Privacy and Data), ข้อมูลและการรักษาความปลอดภัยระบบเครือข่าย (Information and Network security) และการฉ้อโกง (Fraud) เอาไว้ด้วย[114] ซึ่งจากข้อเสนอแนะทั้งหมด ที่ประชุมได้มีข้อสรุป ดังนี้

“มาตรา 5A การรักษาความปลอดภัยและความแข็งแกร่งของระบบเครือข่าย

ประเทศสมาชิกต้องมีความอุตสาหะทั้งโดยส่วนตนและส่วนรวม ในการคงการรักษาความปลอดภัยและความแข็งแกร่งของเครือข่ายโทรคมนาคมระหว่างประเทศเพื่อบรรลุถึงการใช้งาน

---

[113] ณกฤช เศวตนันท์, กฎใหม่ ITU, *วิเคราะห์ตลาดโทรคมนาคม*, *11*(2), (พฤศจิกายน 2555).

[114] International Telecommunication Union, *Draft of the Future ITRs*, 2012, Article 5A and 5B, Retrieved 2014, April 19, from http://www.itu.int/en/wcit-12/Documents/draft-future-itrs-public.pdf

อย่างมีประสิทธิภาพ และ หลีกเลี่ยงอันตรายทางเทคนิค เช่นเดียวกับการพัฒนาบริการทางโทรคมนาคมระหว่างประเทศที่นำเสนอแก่สาธารณะอย่างสอดคล้องกัน[115]

"มาตรา 5B กลุ่มก้อนการสื่อสารทางอิเล็กทรอนิกส์ที่ไม่ได้ถูกร้องขอ

ประเทศสมาชิกต้องมีความอุตสาหะที่จะใช้มาตรการที่จำเป็นในป้องกันการการถ่ายทอดของกลุ่มก้อนการสื่อสารทางอิเล็กทรอนิกส์ที่ไม่ได้ถูกเรียกมา และลดผลกระทบของมันบนบริการโทรคมนาคมระหว่างประเทศให้เหลือน้อยที่สุด ประเทศสมาชิกได้รับการสนับสนุนให้ร่วมมือกันเช่นนั้น"[116]

โดยกลุ่มก้อนการสื่อสารทางอิเล็กทรอนิกส์ที่ไม่ได้ถูกร้องขอ (Unsolicited bulk electronic communication) คือ ข้อมูลจำพวก Spam ซึ่งจะเห็นได้ว่าข้อบังคับใหม่ในด้านการรักษาความปลอดภัยทางอินเตอร์เน็ตของ ITRs ที่ได้รับการเพิ่มเติมเข้าไปนั้นถูกเขียนไว้อย่างกว้าง ๆ เพื่อเปิดให้ประเทศสมาชิกสามารถตีความได้

3.2.3 อนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ (Convention on Cybercrime 2001)

อนุสัญญาอาชญากรรมคอมพิวเตอร์ได้เปิดให้ลงนามในการประชุม ณ กรุงบูดาเปส ประเทศฮังการี ในวันที่ 23 พฤศจิกายน พ.ศ. 2544 อนุสัญญามีผลบังคับใช้ในวันที่ 1 กรกฎาคม พ.ศ. 2547 โดยมีประเทศที่ลงนามแต่ยังไม่ได้ให้สัตยาบันจำนวน 23 ประเทศ และประเทศที่ให้สัตยาบันแล้วอีก 23 ประเทศ โดยประเทศในกลุ่มสหภาพยุโรปได้ตระหนักถึงความเสี่ยงที่ระบบคอมพิวเตอร์และข้อมูลอิเล็กทรอนิกส์ทั้งหลายจะถูกใช้เป็นเครื่องมือในการก่ออาชญากรรมทางคอมพิวเตอร์โดยการริเริ่มของสภายุโรป โดยจัดให้มีการประชุมในเรื่องอาชญากรรมทางคอมพิวเตอร์เกิดขึ้น (Conference

---

[115] International Telecommunication Union, *Draft of the Future ITRs*, 2012, Article 5A Security and robustness of networks.

Article 41B Member States shall individually and collectively endeavour to ensure the security and robustness of international telecommunication networks in order to achieve effective use thereof and avoidance of technical harm thereto, as well as the harmonious development of international telecommunication services offered to the public.

[116] Article 5B Unsolicited bulk electronic communications

Article 41C Member States should endeavour to take necessary measures to prevent the propagation of unsolicited bulk electronic communications and minimize its impact on international telecommunication services.

Member States are encouraged to cooperate in that sense.

International Telecommunication Union, *Final ACTS of the World Conference on International Telecommunications*, (Dubai, ITU, 2012), Retrieved 2014, April 19, from http://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf

of Criminological Aspects of Economic crime) ณ เมืองสตราส์บูร์กส์ ประเทศฝรั่งเศส เมื่อปี พ.ศ. 2519[117] หลังจากนั้นก็มีการเสนอข้อแนะนำ (Recommendations) หลายครั้งเช่น The Council of Europe Recommendations of 1989[118] และ The Council of Europe Recommendations of 1995[119]

โดยที่ประเทศในสมาชิกของ สหภาพยุโรปรวมถึงประเทศอื่น ๆ ที่ลงนามในอนุสัญญาฉบับนี้นั้นได้ตระหนักถึงความเป็นเร่ง ด่วนในการป้องกันสังคมจากอาชญากรรมทางคอมพิวเตอร์ ซึ่งตัวอนุสัญญานี้นับเป็นเหตุการณ์สำคัญในประวัติศาสตร์ของการต่อสู้อาชญากรรมทางคอมพิวเตอร์ และอาจเรียกได้ว่าเป็นแม่แบบในการออกกฎหมายภายในสำหรับประเทศต่าง ๆ ทั่วโลก อีกทั้งยังเป็นแนวปฏิบัติและเป็นการประสานความร่วมมือกับกลุ่มประเทศอื่น ๆ ที่ ได้ร่วมลงนามในอนุสัญญาฉบับนี้ด้วย นอกจากนี้ ข้อกำหนดเกี่ยวกับการกำหนดความผิดด้านการเหยียดเชื้อชาติและเหยียดชาวต่างชาติ (Xenophobia) ที่ถูกกระทำผ่านระบบคอมพิวเตอร์ในปี พ.ศ. 2546 ได้ถูกนำมาปรับใช้ในอนุสัญญาด้วย

อนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ใช้ภาษาที่เป็นกลางทางเทคโนโลยีเพื่อให้บทบัญญัติสามารถนำมาประยุกต์ใช้ได้ทั้งกับเทคโนโลยีที่มีอยู่ในปัจจุบันและต่อไปในอนาคต

อนุสัญญาประกอบไปด้วยบทบัญญัติทั้งหมด 4 บท ได้แก่

บทที่ 1 เป็นการให้คำจำกัดความของระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ผู้ให้บริการ และ ข้อมูลจราจรทางคอมพิวเตอร์

บทที่ 2 ประกอบไปด้วยการกำหนดมาตรการที่จัดให้พึงมีในระดับประเทศ กฎหมายสารบัญญัติ สบัญญัติ และเขตอำนาจศาล โดยกฎหมายสารบัญญัติได้แก่ การเข้าถึงโดยมิชอบด้วยกฎหมาย การดักข้อมูลโดยมิชอบด้วยกฎหมาย การแทรกแซงข้อมูล การแทรกแซงต่อระบบ การใช้อุปกรณ์โดยมิชอบ การปลอมแปลงเกี่ยวกับคอมพิวเตอร์ การฉ้อโกงที่เกี่ยวกับคอมพิวเตอร์ และความผิดประเภทเนื้อหา เช่น ความผิดเกี่ยวกับสื่อลามกอนาจารเด็ก ความผิดเกี่ยวกับการละเมิดสิทธิ์ต่าง ๆ เช่นการละเมิดลิขสิทธิ์ รวมไปถึงการกำหนดมาตรการลงโทษ ในส่วนของกฎหมายสบัญญัติได้กำหนดกฎหมายพิจารณาความเพื่อประยุกต์ใช้กับความผิดอาญาในเรื่องอาชญากรรมทางคอมพิวเตอร์ เพื่อวัตถุประสงค์ในการสอบสวนหรือดำเนินคดีอาญาในความผิดเกี่ยวกับ

---

[117] A Paper for the 12th Conference of Directors of Criminological Research Institutes, *Criminological Aspects of Economic Crime*, (Strasbourg: 15-18 November 1976), 225-229.

[118] Computer-related crime: Recommendation No. R (89) 9 (1990) adopted by the Committee of Ministers of the Council of Europe on 13 September 1989 and Report by the European Committee on Crime Problems, Strasbourg.

[119] Council of Europe: Recommendation No. R (95) 13 Concerning Problems of Criminal Procedural Law connected with Information Technology adopted by the Committee of Ministers on 11 September 1995.

คอมพิวเตอร์โดยเฉพาะ รวมไปถึงวิธีการเข้าเก็บรักษาข้อมูลคอมพิวเตอร์อย่างรวดเร็ว การสั่งให้ส่งข้อมูล การค้นและยึดข้อมูลคอมพิวเตอร์ที่ถูกเก็บไว้ การรวบรวมข้อมูลจราจรคอมพิวเตอร์ และการดักข้อมูลที่เป็นเนื้อหา

บทที่ 3 เป็นส่วนของความร่วมมือระหว่างประเทศ ที่ประกอบไปด้วยหลักการในการส่งผู้ร้ายข้ามแดน หลักการทั่วไปในการช่วยเหลือซึ่งกันและกัน กระบวนการที่เกี่ยวกับการร้องขอความช่วยเหลือในกรณีที่ไม่มีข้อตกลงระหว่างประเทศที่ใช้บังคับอยู่ การให้ความช่วยเหลือซึ่งกันและกันในเรื่องของมาตรการชั่วคราว การให้ความช่วยเหลือซึ่งกันในเรื่องอำนาจสอบสวนและระบบเครือข่าย 24 ชั่วโมง

บทที่ 4 บทบัญญัติภาคสุดท้าย ประกอบไปด้วยข้อกำหนดสุดท้ายซึ่งส่วนใหญ่เกี่ยวโยงกับบทบัญญัติทั่วไปในสนธิสัญญาต่าง ๆ ของสภายุโป เช่น มาตรา 40 วางหลักให้ในเวลาที่มีการลงนามหรือยื่นเอกสารหลักฐานของการให้สัตยาบัน การยอมรับ การเห็นชอบ หรือการภาคยานุวัติประเทศนั้นอาจแสดงเจตจำนงโดยยื่นเป็นหนังสือแจ้งต่อเลขาธิการสภายุโรป ภายตั้งหลักเกณฑ์ที่กำหนดไว้[120] หรือ มาตรา 42 ที่ให้ประเทศแสดงเจตจำนงไปยังเลขาธิการสภายุโรป ภายใต้หลักเกณฑ์ที่กำหนดไว้เช่นกัน[121]

อนุสัญญาว่าด้วยอาชญากรรมคอมพิวเตอร์ (Cybercrime Convention) ของสภายุโรป นับเป็นอนุสัญญาระหว่างประเทศที่มีผลผูกพันฉบับเดียวที่มีอยู่เกี่ยวกับการกระทำผิดทางคอมพิวเตอร์ และเป็นแนวทางในการสร้างมาตรการ รวมทั้งประสานความร่วมมือระหว่างประเทศเพื่อรับมืออาชญากรรมทางคอมพิวเตอร์ โดยคำนึงถึงปัจจัยด้านเสรีภาพและสิทธิมนุษยชน ซึ่งในกระบวนการกำหนดนโยบาย บางครั้งรัฐได้ละเลย หรือจงใจละทิ้งหรือจำกัดทางเลือกของนโยบายที่เสริมสร้างให้อินเตอร์เน็ตพัฒนาขึ้นเป็นพื้นที่สำคัญสำหรับกิจกรรมทางเศรษฐกิจ การมีส่วนร่วมในระบอบประชาธิปไตยและการพัฒนาของมวลมนุษยชาติ

---

[120] Convention on Cybercrime, Article 40 By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibility of requiring additional elements as provided for under Articles 2, 3, 6 paragraph 1.b, 7, 9 paragraph 3, and 27, paragraph 9.e.

[121] Convention on Cybercrime, Article 42 By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2 , Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

โดยสรุปในปัจจุบัน นานาประเทศกำลังแสวงหาข้อกำหนดใหม่ ๆ สำหรับการให้บริการอินเตอร์เน็ตและสื่อที่เกี่ยวข้อง เพื่อคัดกรองและสกัดกั้นเนื้อหาที่ไม่พึงประสงค์ ด้วยมาตรการควบคุมเครือข่ายและการเฝ้าระวังเพื่อบังคับใช้กฎระเบียบกับผู้ใช้งาน ซึ่งผลที่ได้ทำให้เกิดความยุ่งยากและขัดขวางการไหลเวียนของข้อมูลทั่วโลกจากการแข่งขันเรื่องอำนาจการควบคุมและการขัดกันของกฎหมายซึ่งคุกคามเสรีภาพอันเป็นคุณสมบัติเด่นที่ทำให้อินเตอร์เน็ตเป็นอย่างที่เป็นอยู่อย่างในทุกวันนี้ ดังนั้นการพัฒนากฎหมายและมาตรการความร่วมมือต่าง ๆ ร่วมกันในระดับระหว่างประเทศจึงเป็นสิ่งสำคัญที่จะทำให้กฎหมายทันสมัย ก่อให้เกิดความชอบธรรมและเป็นประโยชน์มากกว่าเป็นอุปสรรค และที่สำคัญคือสามารถใช้ปราบปรามอาชญากรรมทางคอมพิวเตอร์ได้อย่างมีประสิทธิภาพสูงสุด

อย่างไรก็ดี อนุสัญญาหรือสนธิสัญญาที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์นั้นเป็นข้อตกลงที่มีผลผูกมัดชัดเจนซึ่งผู้ลงนามเป็นสมาชิกอาจต้องรับผิดภายใต้กฎหมายระหว่างประเทศในกรณีผิดข้อตกลง ดังนั้นในบางกรณีการทำบันทึกความเข้าใจ จะเป็นข้อตกลงที่ยืดหยุ่นมากกว่าซึ่งบันทึกความเข้าใจมักชี้วัดแนวทางการกระทำระหว่างระดับพหุภาคี และมักถูกใช้ในกรณีที่แต่ละฝ่ายไม่ต้องการมีข้อผูกมัดทางกฎหมายหรืออยู่ในสถานการณ์ที่ไม่สามารถออกข้อตกลงที่บังคับใช้ตามกฎหมายได้ แม้ว่าบันทึกความเข้าใจจะไม่ผูกพันตามกฎหมายระหว่างประเทศแต่ก็จะถูกบันทึกไว้ในฐานข้อมูลของสหประชาชาติ

สำหรับอาเซียนในฐานะขององค์การระหว่างประเทศที่เกิดจากการรวมกลุ่มของประเทศในทวีปเอเชียตะวันออกเฉียงใต้ก็ได้ตระหนักถึงปัญหาอาชญากรรมคอมพิวเตอร์ที่ลุกลามไปทั่วโลกไม่เว้นแม้แต่ภูมิภาคเอเชียเองเช่นกัน ในขณะที่หลายประเทศในอาเซียนยังขาดมาตรการในการรับมือเกี่ยวกับการกระทำผิดประเภทนี้ จึงได้มีความพยายามในการที่จะแสดงให้เห็นถึงการต่อสู้กับปัญหาดังกล่าว โดยผ่านการประชุมหลายครั้งของอาเซียน จนเกิดเป็นแผนการต่าง ๆ เช่น ASEAN ICT Master plan 2015, APSC blueprint และ Master plan on ASEAN connectivity ทั้งนี้ประเทศสมาชิกอาเซียนต่างยึดเอาอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของสหภาพยุโรปเป็นแม่แบบในการร่างกฎหมาย ดังนั้นเห็นควรที่จะมีการศึกษาอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์และกฎหมายที่เกี่ยวข้องเป็นแนวทางในการสร้างมาตรฐานกลางในการรับมืออาชญากรรมทางคอมพิวเตอร์ในภูมิภาคเอเชียตะวันออกเฉียงใต้ เพื่อกำหนดให้มีความร่วมมือช่วยเหลือซึ่งกันและกันระหว่างประเทศสมาชิกที่ชัดเจนและมีประสิทธิภาพในการหยุดยั้งอาชญากรรมทางคอมพิวเตอร์ที่นับวันยิ่งทวีความรุนแรงมากขึ้นตามความก้าวหน้าของเทคโนโลยีสารสนเทศ

บทที่ 4

หลักการและกฎเกณฑ์ทางกฎหมายในเรื่องอาชญากรรมคอมพิวเตอร์ของอาเซียน

สมาคมประชาชาติเอเชียตะวันออกเฉียงใต้ (Association of Southeast Asian Nations: ASEAN) เป็นองค์กรระดับภูมิภาคองค์กรแรกที่รับเอากรอบเค้าโครงทางกฎหมายไซเบอร์ เพื่อที่ให้มีความสอดคล้องกันจากหลากหลายเขตอำนาจศาลมาใช้ ในช่วงกลางปี พ.ศ. 2552 ประเทศสมาชิกอาเซียนจะออกกฎหมายพาณิชย์อิเล็กทรอนิกส์ ในระดับชาติที่มีความสอดคล้องกันผ่านโครงการ e-ASEAN[122] ซึ่งเป็นตลาดร่วมในภูมิภาคอาเซียนที่เกิดจากการเปิดเสรีด้านการค้า บริการ และ การลงทุนด้านเทคโนโลยีและอิเล็กทรอนิกส์ระหว่างประเทศสมาชิก โครงการ e-ASEAN นับเป็นโครงการแรกที่ผลักดันให้มีการสร้างความสอดคล้องกันของกรอบโครงสร้างทางกฎหมาย

---

[122] e-ASEAN เกิดขึ้นที่ประชุมสุดยอดอาเซียนอย่างไม่เป็นทางการครั้งที่ 3 เมื่อเดือนพฤศจิกายน พ.ศ. 2542 ณ ประเทศฟิลิปปินส์ ได้เห็นชอบให้มีการดำเนินการความร่วมมือด้านอิเล็กทรอนิกส์ของอาเซียน โดยเสนอให้มีการจัดตั้งเขตการค้าเสรีด้านสินค้าบริการและการลงทุนที่เกี่ยวกับเทคโนโลยีสารสนเทศและการสื่อสารภายใต้ความตกลงด้านอิเล็กทรอนิกส์ของอาเซียน (e-ASEAN Agreement) โดยมีคณะทำงานเฉพาะด้านเทคโนโลยีสารสนเทศและอิเล็กทรอนิกส์ในอาเซียน ซึ่งคณะทำงานเฉพาะกิจดังกล่าวได้ทำหน้าที่ศึกษานโยบายและดำเนินการสาระของโครงการอาเซียนอิเล็กทรอนิกส์ไว้ 5 ด้าน คือ

1. การวางพื้นฐานด้านสารสนเทศของอาเซียนซึ่งจะต้องมีการวางผังโครงข่ายเคเบิลใยแก้วนำแสง (ASEAN backbone) รวมถึงการสนับสนุนให้เกิดศูนย์กลางแลกเปลี่ยนข้อมูลของอาเซียน

2. การส่งเสริมและอำนวยความสะดวกในการใช้สื่ออิเล็กทรอนิกส์ โดยภาครัฐจำเป็นต้องดำเนินการผลักดันให้เกิดความมั่นใจในการใช้สื่ออิเล็กทรอนิกส์ อาทิเช่น การมีกฎหมายรองรับ การมีระบบรักษาความปลอดภัยที่เป็นมาตรฐานสากล เป็นต้น

3. การเปิดเสรีด้านการค้า การบริการ และการลงทุนในส่วนที่เกี่ยวข้องกับด้านอิเล็กทรอนิกส์ทั้งหมด โดยในด้านการค้าจะต้องลดภาษีศุลกากรสำหรับสินค้าที่เกี่ยวข้องให้เหลือร้อยละ 0 ทางด้านบริการจะเน้นเปิดเสรีทางด้านบริการโทรคมนาคมและบริการวิชาชีพทางด้านการลงทุนจะเปิดให้ประเทศในอาเซียน สามารถลงทุนในด้านการสื่อสารอิเล็กทรอนิกส์ได้โดยเสรีมากขึ้น

4. ด้านสังคม จะเน้นให้เกิดสังคมอิเล็กทรอนิกส์ กล่าวคือสังคมอาเซียน จะสามารถใช้สื่ออิเล็กทรอนิกส์ได้อย่างมีประสิทธิภาพและทั่วถึง

5. การสร้างรัฐบาลอิเล็กทรอนิกส์ โดยจะเน้นการให้บริการประชาชนโดยใช้สื่ออิเล็กทรอนิกส์มากขึ้น เช่น การเสียภาษี ผ่านสื่ออิเล็กทรอนิกส์ การจดทะเบียนการค้า พิธีการ ศุลกากร เป็นต้น.

(Legal framework harmonization) เพื่อให้กฎหมายภายในของประเทศสมาชิกอาเซียนเป็นไปในทิศทางเดียวกัน

จุดมุ่งหมายของโครงการ e-ASEAN คือการสร้างความเท่าเทียมกันของประเทศสมาชิกในด้านโครงสร้างพื้นฐานทาง ICT เพื่อเสริมสร้างขีดความสามารถในการรองรับหลักเกณฑ์กลางของกฎหมายที่เกี่ยวข้อง รวมไปถึงกฎหมายที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ด้วย

โดยประเทศสมาชิกอาเซียนที่เป็นผู้นำในเรื่องความพยายามต่อสู้อาชญากรรมทางคอมพิวเตอร์ได้แก่สิงคโปร์และมาเลเซีย โดยมาเลเซียถือเป็นผู้ริเริ่มในเรื่องนี้ด้วยการออกกฎหมายอาชญากรรมทางคอมพิวเตอร์ก่อนประเทศสมาชิกอื่นในอาเซียนในปี พ.ศ. 2540 ตามมาด้วย Digital signature regulation ในปี พ.ศ. 2541 ตามด้วย electronic transaction act ของสิงคโปร์โดยกฎหมายอาชญากรรมทางคอมพิวเตอร์ในมาเลเซียและสิงคโปร์ออกตามแนวทางของอนุสัญญาระหว่างประเทศและกฎหมายของประเทศในภูมิภาคยุโรป

4.1 วิวัฒนาการเกี่ยวกับความร่วมมือในเรื่องอาชญากรรมทางคอมพิวเตอร์ของอาเซียน

สำหรับการจัดการเกี่ยวกับปัญหาอาชญากรรมทางคอมพิวเตอร์ของอาเซียนนั้น ประเทศสมาชิกอาเซียนได้ร่วมมือกันโดยผ่านทางองค์การอาเซียน ที่ได้พยายามผลักดันให้ประเทศสมาชิกอาเซียได้มีการออกกฎหมายว่าด้วยการป้องกันอาชญากรรมทางคอมพิวเตอร์ นอกจากนี้ องค์การอาเซียนยังได้จัดตั้ง ASEAN high level Ministerial Meeting on Transnational Crime: AMMTC และได้มีการประชุมครั้งแรก ที่กรุงเทพมหานคร ประเทศไทย ในวันที่ 8 มกราคม พ.ศ. 2547 ซึ่ง AMMTC ประกอบไปด้วยตัวแทนจากประเทศสมาชิกอาเซียนได้แก่ อินโดนีเซีย มาเลเซีย ฟิลิปปินส์ สิงคโปร์ ไทย กัมพูชา ลาว พม่า และเวียดนาม โดยในการประชุมครั้งนี้ได้มีการแถลงการณ์และได้รวมเอาเรื่องอาชญากรรมทางคอมพิวเตอร์ รวมทั้ง ความต้องการความร่วมมือระหว่างประเทศในการรับมืออาชญากรรมทางคอมพิวเตอร์เข้าไว้ด้วยกัน โดยได้ระบุถึงความต้องการความร่วมมือในทางด้านกฎหมายที่มีประสิทธิภาพ เพื่อเพิ่มขีดความสามารถในการต่อสู้กับอาชญากรรมข้ามชาติ ซึ่งผลลัพธ์ที่ได้ออกมาก็คือ แผนปฏิบัติการ (plan of action) เพื่อดำเนินการแผนยุทธศาสตร์ความร่วมมือของอาเซียน อาเซียนได้ริเริ่มแผนการรับมืออาชญากรรมทางคอมพิวเตอร์โดยอาศัยโครงสร้างพื้นฐานทางกฎหมาย e-commerce เป็นจุดเริ่มต้นในการสร้างหลักเกณฑ์ทางกฎหมายอาชญากรรมทางคอมพิวเตอร์ แต่อย่างไรก็ตาม กรอบโครงสร้าง e-ASEAN นั้นจำกัดอยู่เพียงกฎหมายระดับพื้นฐาน ซึ่งตัวกฎหมายเองไม่ได้ให้แนวทางเพื่อรับเอาข้อกฎหมายหรือวิธีปฏิบัติที่ระบุเรื่องการคุ้มครองข้อมูลหรือความเป็นส่วนตัว การคุ้มครองผู้บริโภค

อาชญากรรมทางคอมพิวเตอร์ ทรัพย์สินทางปัญญา การยอมรับข้อมูลที่ได้จากคอมพิวเตอร์เพื่อใช้เป็นหลักฐานในศาล หรือการควบคุมเนื้อหาบนอินเตอร์เน็ต เอาไว้ด้วย ดังนั้น ในปี พ.ศ. 2547 เกิดการขยายตัวของอาชญากรรมทางคอมพิวเตอร์อย่างมากและก่อให้เกิดความตระหนักในการส่งเสริมความร่วมมือระหว่างประเทศในการป้องกันอาชญากรรมทางคอมพิวเตอร์ขึ้น และมีการยอมรับว่าความร่วมมือระหว่างประเทศในการป้องกันอาชญากรรมทางคอมพิวเตอร์นั้นเป็นกิจกรรมที่สำคัญสำหรับประเทศสมาชิกอาเซียน ทั้งนี้ในปี พ.ศ. 2549 ASEAN regional forum: ARF ได้ออกแถลงการณ์เพื่อเน้นย้ำว่าการรับมือกับอาชญากรรมทางคอมพิวเตอร์และกิจกรรมของผู้ก่อการร้ายบนอินเตอร์เน็ตนั้นจำเป็นต้องมีความร่วมมือทางด้านกฎหมาย (ที่เพิ่มมากขึ้น รวดเร็วขึ้น และทำงานได้ดี) และ ความร่วมมือในด้านอื่น ๆ ด้วย โดยประเทศสมาชิกต่างให้คำปฏิญาณว่าจะดำเนินการพัฒนา ออกกฎหมาย และนำเอากฎหมายอาชญากรรมทางคอมพิวเตอร์และความปลอดภัยไซเบอร์ที่เหมาะสมกับสภาพสังคมของประเทศตนเอง โดยอาศัยแนวทางของกฎหมายระหว่างประเทศ (International guidelines) เพื่อการตรวจสอบ ป้องกัน ต่อสู้ และลดความรุนแรงของการโจมตีทางอินเตอร์เน็ต (Cyber-attack) ทั้งนี้ อาเซียนเองได้ตระหนักถึงคุณค่าของกรอบโครงสร้างระดับชาติเพื่อความร่วมมือและพันธมิตรในการรับมือกับอาชญากรรมที่เกิดขึ้นบนอินเตอร์เน็ต จึงได้มีการพัฒนาโครงสร้างเช่นนี้ต่อไปอีก[123]

นอกจากนี้ ประเทศสมาชิกอาเซียนได้ตระหนักถึงความสำคัญของการสร้างความร่วมมือระดับระหว่างประเทศในการรับมือกับอาชญากรรมที่เกิดขึ้นบนอินเตอร์เน็ตในวงที่กว้างมากขึ้น

---

[123] แถลงการณ์ของ ASEAN Regional Forum (ARF) เมื่อเดือนกรกฎาคม พ.ศ. 2549 ได้ระบุไว้ดังนี้

"เชื่อว่า การรับมือการโจมตีทางอินเตอร์เน็ตและการใช้อินเตอร์เน็ตโดยมิชอบของผู้ก่อการร้ายอย่างมีประสิทธิภาพนั้นต้องการกฎหมายที่ทำงานได้ดีรวมไปถึงความร่วมมือในรูปแบบอื่น ๆ ซึ่งต้องเพิ่มมากขึ้นอย่างต่อเนื่องด้วย

1. รัฐที่เข้าร่วม ARF และองค์กรที่มีความพยายามจะออกกฎหมาย และรวมเอากฎหมายอาชญากรรมไซเบอร์และความมั่นคงไซเบอร์เป็นกฎหมายภายในของชาติและโดยอ้างถึงเครื่องมือ คำแนะนำ หรือแนวทางเพื่อป้องกัน ตรวจหา ทำให้ลดลง หรือลดความรุนแรงของการโจมตี รวมไปถึงข้อแนะนำ 10 ประการที่ระบุใน UN General Assembly Resolution 55/63 on Combating the Criminal Misuse of Information technologies.

2. รัฐและองค์กรที่เข้าร่วม ARF ได้ทราบถึงความสำคัญของกรอบโครงสร้างระดับชาติสำหรับความร่วมมือและการทำงานร่วมกันในการจัดการปัญหาอาชญากรรมไซเบอร์ รวมไปถึงการก่อการร้าย และการใช้งานอินเตอร์เน็ตโดยมิชอบ อีกทั้งกระตุ้นให้มีการวางกฎเกณฑ์ของกรอบโครงสร้างนั้นโดยอาจรวมไปถึง...".

โดยในเดือนพฤศจิกายน พ.ศ. 2550 ได้มีการประชุมหารือกับประเทศจีน[124] และประเทศเกาหลีใต้ ณ ประเทศบรูไน โดยเป็นการประชุมระหว่างรัฐมนตรีประเทศสมาชิกอาเซียนและประเทศจีนในเรื่องความร่วมมือในการต่อสู้กับอาชญากรรมข้ามชาติ โดยที่ประชุมได้ยอมรับว่า เนื่องจากมีอุปสรรคและขอบข่ายที่เพิ่มมากขึ้นของความร่วมมืออาชญากรรมข้ามชาติ บันทึกความเข้าใจระหว่างอาเซียนและจีน (ASEAN-China Memorandum of understanding) จำเป็นต้องได้รับการแก้ไขทบทวนใหม่ตามปัญหาที่เกิดขึ้น

นอกจากนี้ใน Joint communique ซึ่งประกอบไปด้วย จีน ญี่ปุ่น และเกาหลีใต้[125] โดย Joint communique จาก ASEAN Chiefs of police Conference ในบรูไนเมื่อเดือนพฤษภาคม พ.ศ. 2551 ได้รวมข้อมติในเรื่องอาชญากรรมไซเบอร์เข้าไปด้วย

ต่อมาในปี พ.ศ. 2552 ได้มีการประชุมเชิงปฏิบัติการร่วมกันระหว่าง APEC (Asia Pacific Economic Cooperation)[126] และ ASEAN (APEC-ASEAN) ณ ประเทศฟิลิปปินส์ ในเรื่องความปลอดภัยของระบบเครือข่าย เพื่อแบ่งปันความรู้และประสบการณ์ รวมทั้งเสริมสร้างความสามารถในเรื่องความมั่นคงทางอินเตอร์เน็ตและอาชญากรรมทางคอมพิวเตอร์ ทั้งนี้ อนุสัญญาอาชญากรรมคอมพิวเตอร์ ซึ่งเป็นหลักเกณฑ์ที่ถูกพัฒนาขึ้นโดยสหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union: ITU) ได้ถูกนำมาใช้เป็นต้นแบบหลักเกณฑ์ทางกฎหมายเพื่อใช้อ้างอิงสำหรับกลุ่มประเทศสมาชิก APEC และประเทศสมาชิกอาเซียน โดยได้อภิปรายถึงการ

---

[124] เพื่อดำเนินการแผนยุทธศาสตร์ความร่วมมือของอาเซียน และจีนเพื่อสันติภาพและความเจริญรุ่งเรือง (ASEAN-China Strategic Partnership for peace and prosperity) ซึ่งได้รับการลงนามในวันที่ 8 ตุลาคม พ.ศ. 2546 ณ จังหวัดบาหลี ประเทศอินโดนีเซีย โดยอาเซียนและจีนจะร่วมกันทำให้สำเร็จลุล่วงซึ่งปฏิบัติการร่วมและมาตรการที่ได้กำหนดไว้ในแผนการ ทั้งนี้ ASEAN-China Strategic Partnership for peace and prosperity มาตรการ 2.5.7 กำหนดวิธีการดำเนินการร่วมกันและกระบวนการตอบสนองกรณีและฉุกเฉินรวมไปถึงการดูแลรักษาและเพิ่มประสิทธิภาพของการรักษาความปลอดภัยบนอินเตอร์เน็ต และป้องกันและรับมืออาชญากรรมไซเบอร์.

[125] “เราจัดการประชุมเพื่อและเปลี่ยนมุมมองเพื่อเสริมสร้างความแข็งแกร่งให้กับความร่วมมือ ASEAN+3 ในการรับมืออาชญากรรมข้ามชาติโดยมุ่งเน้นไปที่อุปสรรคของอาชญากรรมไซเบอร์และความเชื่อมโยงอันแข็งแกร่งของมันต่ออาชญากรรมข้ามชาติอื่น ๆ ยกตัวอย่างเช่นการก่อการร้ายและการค้ามนุษย์”.

[126] ความร่วมมือทางเศรษฐกิจเอเชีย-แปซิฟิก (Asia Pacific Economic Cooperation: APEC)” เป็นกรอบความร่วมมือทางเศรษฐกิจระหว่างเขตเศรษฐกิจในภูมิภาคเอเชีย-แปซิฟิกก่อตั้งขึ้นเมื่อปี พ.ศ. 2532 โดยประเทศไทยอยู่ ในสมาชิกแรกเริ่มของ APEC ตั้งแต่ต้น ซึ่งมี 12 เขตเศรษฐกิจคือ ออสเตรเลีย บรูไน แคนาดา อินโดนีเซีย ญี่ปุ่น เกาหลีใต้ มาเลเซีย นิวซีแลนด์ ฟิลิปปินส์ สิงคโปร์ ไทย และสหรัฐอเมริกา ต่อมาเอเปคได้รับสมาชิกเพิ่มในปีต่าง ๆ รวมเป็น 21 เขตเศรษฐกิจ ดังนี้ สาธารณรัฐประชาชนจีน (2534) เขตบริหารพิเศษฮ่องกง (2534) จีนไทเป (2534) เม็กซิโก (2536) ปาปัวนิวกินี (2536) ชิลี (2537) เปรู (2540) เวียดนาม (2540) และรัสเซีย (2540), ศูนย์บริการข้อมูลเศรษฐกิจระหว่างประเทศ, *ภูมิหลัง APEC*, สืบค้นเมื่อ 8 ตุลาคม 2557, จาก http://www.mfa.go.th/business/th/customize/16530-ภูมิหลัง-APEC.html

ร่างกฎหมายและการฝึกฝนผู้เชี่ยวชาญเฉพาะทางในการพิสูจน์หลักฐานดิจิตอล (Digital forensics) ใน เดือนพฤษภาคม พ.ศ. 2551 ประเทศสมาชิกรับเอามติในเรื่องอาชญากรรมคอมพิวเตอร์มาใช้ โดยในขณะนั้นอาเซียนมีประเทศที่ออกกฎหมายอาชญากรรมทางคอมพิวเตอร์เรียบร้อยแล้ว 7 ประเทศ ซึ่งประเทศอินโดนีเซียมีร่างกฎหมายว่าด้วยอาชญากรรมทางคอมพิวเตอร์ โดยกฎหมายนี้ประกอบไปด้วยความผิดที่ใกล้เคียงกัน แต่แตกต่างกันเล็กน้อย การกำหนดความผิดมุ่งเน้นในเรื่องการครอบคลุมการเข้าถึงโดยไม่ได้รับอนุญาต การเข้าถึงโดยไม่ได้รับอนุญาตโดยมีเจตนากระทำความผิด การเปลี่ยนแปลงข้อมูลคอมพิวเตอร์โดยไม่ได้รับอนุญาต เป็นต้น ทั้งนี้ กฎหมายฉบับนี้ยังประกอบไปด้วยข้อบังคับในการเปิดเผยรหัสเชื่อมต่อคอมพิวเตอร์โดยไม่ได้รับอนุญาตอีกด้วย

ในเดือนพฤษภาคม พ.ศ. 2552[127] ได้มีการประชุมอธิบดีกรมตำรวจอาเซียนขึ้น ณ กรุงฮานอย ประเทศเวียดนาม และมีการประชุมรัฐมนตรีทางด้านโทรคมนาคมและสารสนเทศของประเทศสมาชิกอาเซียน ณ นครหลวงเวียงจันทน์ ประเทศสาธารณรัฐประชาธิปไตยประชาชนลาว ในเดือนตุลาคมปีเดียวกัน รวมทั้งการประชุม AMMTC ณ นครเสียมเรียบ ประเทศกัมพูชา ก็ได้มีการกล่าวถึงความสำคัญในการรับมืออาชญากรรมข้ามชาติ และเมื่อวันที่ 18 พฤศจิกายน พ.ศ. 2552 รัฐมนตรีอาเซียนได้ลงนามในบันทึกความเข้าใจ Asean+1 (China) ว่าด้วยความร่วมมือในการแก้ไขปัญหาอาชญากรรมพิเศษ (Nontraditional crime) ระหว่างปี พ.ศ. 2552-2557[128]

นอกจากนี้ ระหว่างวันที่ 10-11 ตุลาคม พ.ศ. 2554 ได้มีการประชุม AMMTC ครั้งที่ 8 ที่บาหลี ประเทศอินโดนีเซีย เพื่อรวมเป็นหนึ่งและสร้างความแข็งแกร่งยิ่งขึ้นซึ่งความร่วมมือระดับภูมิภาคในการต่อสู้กับอาชญากรรมข้ามชาติ และระหว่างวันที่ 30 พฤษภาคม–3 มิถุนายน พ.ศ. 2554 ได้มีการประชุมสำนักงานตำรวจอาเซียน (ASEAN Chiefs of Police conference: ASEANAPOL) ขึ้น ณ นครหลวงเวียงจันทน์ ประเทศลาว โดยมีความร่วมมือเพื่อเป็นพันธมิตรกับองค์การตำรวจสากล (INTERPOL) เพื่อทำให้ ASEANAPOL มีศักยภาพเพียงพอในการตอบสนองต่ออุปสรรคที่เกิดขึ้นจากอาชญากรรมไซเบอร์

ต่อมาประเทศสมาชิกอาเซียนได้เข้าร่วมทำพันธะสัญญาในการจัดตั้ง ASEAN Economic Community: AEC ขึ้นในปี พ.ศ. 2558 โดยมีเป้าหมายสำคัญของพันธะสัญญานี้คือ การพัฒนาความสอดคล้องของโครงสร้างทางกฎหมาย ดังเช่นที่ได้กำหนดไว้ใน Roadmap for Integration of

---

[127] ในที่ประชุมได้มีมติเกี่ยวกับอาชญากรรมคอมพิวเตอร์ เช่น “8.7.1 เพื่อที่จะกระตุ้นให้ประเทศสมาชิกทบทวนถึงการสร้างชุดของกฎหมายที่จะเป็นมาตรฐานในเรื่องอาชญากรรมทางคอมพิวเตอร์ต่อไปและเพื่อจัดให้มีการตรากฎหมายดังกล่าวเมื่อจำเป็น”.

[128] โดยบันทึกความเข้าใจฉบับนี้เป็นการยืดระยะเวลาจากบันทึกความเข้าใจ ฉบับเดิมที่มีระยะเวลาจากปี พ.ศ. 2547-2552 ซึ่งได้ดำเนินการสำเร็จไปแล้ว ซึ่งแผนดังกล่าวครอบคลุมถึงการแบ่งปันประสบการและความร่วมมือการปฏิบัติการสืบสวนอาชญากรรมไซเบอร์และยาเสพย์ติด รวมถึงการอบรมภาษาสำหรับกลุ่มประเทศ CLMV.

e-ASEAN Sector โดยแผน Roadmap ได้เรียกร้องให้ประเทศสมาชิกอาเซียนรับเอาข้อปฏิบัติและแนวทางในการรับมือปัญหาอาชญากรรมทางคอมพิวเตอร์ เช่น การคุ้มครองข้อมูล การคุ้มครองผู้บริโภค การคุ้มครองทรัพย์สินทางปัญญา ความรับผิดของผู้ให้บริการอินเตอร์เน็ต เป็นต้น โดยมีข้อกำหนดระยะเวลาอยู่ระหว่าง พ.ศ. 2553 ถึง พ.ศ. 2556

สำหรับการประชุมเจ้าหน้าที่อาวุโสอาเซียนด้านอาชญากรรมข้ามชาติ (ASEAN Senior Officials Meeting on Transnational Crime: SOMTC ครั้งที่ 13 ซึ่งจัดขึ้น ณ จังหวัดดานัง ประเทศเวียดนาม ระหว่างวันที่ 19-20 มิถุนายน พ.ศ. 2556 โดยการประชุมครั้งนี้นับเป็นการให้การรับรองอย่างเป็นทางการของโครงการซึ่งจะดำเนินงานในช่วงปี พ.ศ. 2556-2558 ของการประชุมเจ้าหน้าที่อาวุโสอาเซียนด้านอาชญากรรมข้ามชาติ ซึ่งประกอบไปด้วยแนวทางปฏิบัติ (guidelines) และกิจกรรม (activities) ใน 8 สาขาของอาชญากรรมข้ามชาติ ได้แก่ การก่อการร้าย การค้ายาเสพย์ติด การค้ามนุษย์ การลักลอบค้าอาวุธ โจรสลัด การฟอกเงิน อาชญากรรมทางเศรษฐกิจข้ามชาติและอาชญากรรมทางคอมพิวเตอร์ โดยการประชุมเพื่อวางแผนงานเพื่อรับมือปัญหาดังกล่าวจะมีขึ้น ณ การประชุมรัฐมนตรีอาเซียนด้านอาชญากรรมข้ามชาติ ครั้งที่ 9 ที่นครหลวงเวียงจันทน์ ประเทศสาธารณรัฐประชาธิปไตยประชาชนลาว ระหว่างวันที่ 15-19 กันยายน พ.ศ. 2556 เพื่อให้รัฐมนตรีแต่ละประเทศนำไปปรับใช้กับนโยบายภายในประเทศ และการประชุม SOMTC ยังได้รับรองการจัดตั้งคณะทำงานด้านอาชญากรรมทางคอมพิวเตอร์ขึ้น โดยได้ขอคำปรึกษาจาก ออสเตรเลีย แคนาดา จีน อินเดีย ญี่ปุ่น เกาหลีใต้ และสหรัฐอเมริกา เพื่อเพิ่มประสิทธิภาพด้านความร่วมมือของคู่เจรจาอาเซียน (ASEAN Dialogue Partners)[129] โดยทั้งเจ้าหน้าที่อาวุโสอาเซียนด้านอาชญากรรมข้ามชาติ และ คู่เจรจาอาเซียนต่างมีความเห็นไปในทางเดียวกันให้มีการบูรณาการความร่วมมือเชิงปฏิบัติการ เพื่อสนับสนุนความพยายามในการรับมืออาชญากรรมข้ามชาติ ซึ่งรวมถึงอาชญากรรมทางคอมพิวเตอร์ของอาเซียน ทั้งนี้ โครงการในอนาคตจะประกอบไปด้วยการบูรณาการแผนงานร่วมในการรับมืออาชญากรรมข้ามชาติรวมไปถึงกิจกรรมอื่น ๆ ที่เกี่ยวข้องอีกด้วย

นอกเหนือจากการประชุมระหว่างประเทศแล้ว อาเซียนยังได้มีการจัดประชุมเชิงปฏิบัติการ (workshop) ขึ้นอีกหลายครั้งเพื่อให้ความรู้และพัฒนาการร่างกฎหมายเพื่อรับมือกับอาชญากรรมคอมพิวเตอร์ เช่น การประชุมเชิงปฏิบัติการร่วมสหภาพยุโรปและอาเซียนในการร่างกฎหมายอาชญากรรมทางคอมพิวเตอร์ในประเทศสมาชิกอาเซียน (EU-ASEAN Workshop on Cybercrime

---

[129] คู่เจรจาอาเซียน (ASEAN Dialogue Partners) ประกอบด้วย 9 ประเทศ 1 กลุ่มประเทศ และ 1 องค์การระหว่างประเทศ คือ ออสเตรเลีย แคนาดา จีน อินเดีย ญี่ปุ่น สาธารณรัฐเกาหลี นิวซีแลนด์ รัสเซีย สหรัฐอเมริกา ประชาคมยุโรป และโครงการพัฒนาแห่งสหประชาชาติ โดยคู่เจรจาเหล่านี้ (ยกเว้นโครงการพัฒนาแห่งสหประชาชาติ) จะเข้าร่วมการประชุม PMC ด้วย.

Legislation in ASEAN Member States)[130] จัดขึ้น ณ กรุงกัวลาลัมเปอร์ ประเทศมาเลเซียระหว่างวันที่ 27-28 พฤศจิกายน พ.ศ. 2552 ซึ่งการประชุมเชิงปฏิบัติการนี้มีวัตถุประสงค์เพื่อสนับสนุนการพัฒนากฎหมายอาชญากรรมทางคอมพิวเตอร์ในประเทศสมาชิกอาเซียนบนพื้นฐานของอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของสหภาพยุโรป (Cybercrime convention) เพื่อส่งเสริมให้ประเทศสมาชิกอาเซียนเข้าภาคยานุวัติ เป็นสมาชิกของอนุสัญญาในอนาคต และเพื่อชี้ให้เห็นว่าประเทศสมาชิกแต่ละประเทศยังมีความต้องการในการเพิ่มขีดความสามารถ เพื่อออกกฎหมายอย่างมีประสิทธิภาพ และส่งเสริมความร่วมมือทั้งภายในและภายนอกภูมิภาคคู่เจรจา ที่รวมถึงความร่วมมือเชิงปฏิบัติการและการแลกเปลี่ยนข้อมูลระหว่างกันอีกด้วย

สำหรับการประชุมเชิงปฏิบัติการร่วมสหภาพยุโรปและอาเซียนในการร่างกฎหมายอาชญากรรมทางคอมพิวเตอร์ในประเทศสมาชิกอาเซียน มีประเทศสมาชิกที่ได้ส่งเจ้าหน้าที่กระทรวงยุติธรรมประเทศเข้าร่วมได้แก่ บรูไน กัมพูชา อินโดนีเซีย ลาว มาเลเซีย ฟิลิปปินส์ สิงคโปร์ และเวียดนาม อีกทั้งยังมี สมาชิกของสภาหน่วยงานกำกับดูแลกิจการโทรคมนาคมแห่งอาเซียน (ASEAN Telecommunications Regulators Council: ATRC) เข้าร่วมประชุมด้วย โดยการประชุมได้ถูกจัดขึ้นบนแผนความร่วมมือระหว่างอาเซียนและสหภาพยุโรปเพื่อการช่วยเหลือในการบูรณาการ–ระยะที่สอง (ASEAN EU-Programme for Regional Integration Support–Phase II [APRIS II]) ระหว่าง สหภาพยุโรป เลขานุการอาเซียน สภาหน่วยงานกำกับดูแลกิจการโทรคมนาคมแห่งอาเซียน และ คณะกรรมาธิการการสื่อสารและมัลติมีเดียมาเลเซีย (Malaysian Communications And Multimedia Commission: MCMC) โดยเป็นส่วนหนึ่งของ Regional EU-ASEAN Dialogue Instrument programme ซึ่งตรงกับเป้าหมายของ ASEAN-EU Strategic Partnership ซึ่งเริ่มดำเนินการ ณ การประชุมสุดยอดเพื่อฉลองการครบรอบความสัมพันธ์ 30 ปี (ASEAN-EU Commemorative Summit) ที่สิงคโปร์ในปี พ.ศ. 2551

4.2 กลไกในการรับมืออาชญากรรมทางคอมพิวเตอร์ของอาเซียน

อาเซียนมีความพยายามในการสร้าง นโยบาย แผนยุทธศาสตร์และหลักเกณฑ์ที่เป็นมาตรฐานกลาง เพื่อใช้เป็นมาตรการที่สำคัญในการรับมือกับอาชญากรรมทางคอมพิวเตอร์ของภูมิภาค โดยสามารถแบ่งกลไกในการรับมืออาชญากรรมทางคอมพิวเตอร์ของอาเซียนได้ดังนี้

---

[130] EU-ASEAN Workshop on Cybercrime Legislation in the ASEAN Member States, Retrieved 2013, June 18, from http://www.asean.org/archive/apris2/file_pdf/Press%20Releases/EU-ASEAN%20Workshop%20on%20Cybercrime%20 Legislation%20in%20the%20ASEAN%20Member%20States.pdf

4.2.1 การประชุมรัฐมนตรีอาเซียนด้านอาชญากรรมข้ามชาติ (ASEAN Ministerial Meeting on Transnational Crime: AMMTC)

การประชุมรัฐมนตรีอาเซียนด้านอาชญากรรมข้ามชาติ[131] นี้ได้ทำหน้าที่ในการ พิจารณาและทบทวนแผนงานจากหน่วยงานต่าง ๆ ของอาเซียนในด้านอาชญากรรมข้ามชาติ โดยในการประชุม AMMTC ครั้งที่ 3 ซึ่งจัดขึ้นในวันที่ 11 ตุลาคม พ.ศ. 2544 อาชญากรรมทางคอมพิวเตอร์ได้ถูกรวมเข้ามาในแผนงานรับมืออาชญากรรมข้ามชาติของอาเซียน (ASEAN plan of action to combat transnational crime) รวมทั้งได้จัดตั้งคณะทำงานในเรื่องอาชญากรรมทางคอมพิวเตอร์ขึ้นในการประชุมครั้งที่ 9 เมื่อวันที่ 17 กันยายน พ.ศ. 2556 ณ นครหลวงเวียนจันทร์ ประเทศลาว

4.2.2 การประชุมระดับเจ้าหน้าที่อาวุโสอาเซียนด้านอาชญากรรมข้ามชาติ (ASEAN Senior Officials Meeting on Transnational Crime: SOMTC)

การประชุมระดับเจ้าหน้าที่อาวุโสอาเซียนด้านอาชญากรรมข้ามชาติ[132] นี้ได้จัดทำแผนงาน ASEAN Plan of Action to Combat Transnational Crime ที่ได้ถูกนำไปปฏิบัติในอาเซียน ซึ่งแผนงานนี้ได้นำเสนอองค์ประกอบของอาชญากรรมทางคอมพิวเตอร์[133] และได้รับการลงมติยอมรับในการประชุม SOMTC ครั้งที่ 2 เมื่อเดือนพฤษภาคม พ.ศ. 2545 ณ กรุงกัวลาลัมเปอร์ ประเทศมาเลเซีย และเมื่อวันที่ 26-27 มิถุนายน พ.ศ. 2550 ในการประชุม SOMTC ครั้งที่ 7 ณ นครหลวงเวียงจันทน์ ประเทศลาว ที่ประชุมได้ลงมติรับรองกรอบเค้าโครงสามัญ (Common framework) ในการสร้างศักยภาพการบังคับใช้กฎหมายอาชญากรรมทางคอมพิวเตอร์ของอาเซียน เพื่อสนับสนุนการรับมือกับอาชญากรรมทางคอมพิวเตอร์ในระดับสากล นอกจากนี้ ในการประชุม SOMTC ครั้งที่ 13 ระหว่างวันที่ 19-20 มิถุนายน พ.ศ. 2556 ณ นครหลวงเวียงจันทน์ ประเทศลาว ที่ประชุมได้ให้การรับรองการจัดตั้งคณะทำงานในเรื่องอาชญากรรมทางคอมพิวเตอร์อย่างเป็นทางการ

---

[131] AMMTC มีเป้าหมายเพื่อทบทวนและพิจารณาผลงานจากหน่วยงานต่าง ๆ ของอาเซียนในเรื่องอาชญากรรมข้ามชาติรวมไปถึงกำหนดอัตราและทิศทางความร่วมมือระหว่างประเทศในระดับภูมิภาคเพื่อรับมืออาชญากรรมเหล่านั้น.

[132] ASEAN Senior Officials Meeting on Transnational Crime-SOMTC มีเป้าหมายเพื่อทบทวนและพิจารณานโยบายและแผนยุทธศาสตร์และการนำแผนงานไปปฏิบัติจริง รวมไปถึงแจ้งผลการพัฒนาโครงการต่อ AMMTC โดย SOMTC ครอบคลุมอาชญากรรมข้ามชาติ 8 รูปแบบด้วยกัน ได้แก่ การก่อการร้าย ค้ามนุษย์ ค้ายาเสพย์ติด ฟอกเงิน ค้าอาวุธ โจรสลัด อาชญากรรมทางธุรกิจ และ อาชญากรรมทางคอมพิวเตอร์.

[133] ASEAN Plan of Action to Combat Transnational Crime องค์ประกอบของอาชญากรรมทางคอมพิวเตอร์ที่ได้รับการลงมติประกอบไปด้วยเขตความร่วมมือ 5 หมวดหมู่ด้วยกัน ได้แก่ การแลกเปลี่ยนข้อมูลข่าวสาร, กฎหมาย, การบังคับใช้กฎหมาย, การฝึกฝนและสร้างศักยภาพ และความร่วมมือนอกภูมิภาค.

4.2.3 การประชุมอาเซียนว่าด้วยความร่วมมือด้านการเมืองและความมั่นคงในภูมิภาคเอเชีย-แปซิฟิก (ASEAN Regional Forum: ARF)

การประชุมอาเซียนว่าด้วยความร่วมมือด้านการเมืองและความมั่นคงในภูมิภาคเอเชีย-แปซิฟิก[134] ได้ออกแถลงการณ์ในเรื่องความร่วมมือในการรับมือการโจมตีไซเบอร์และการใช้ไซเบอร์สเปซในทางที่ผิดของผู้ก่อการร้าย เมื่อวันที่ 28 กรกฎาคม พ.ศ. 2549 ณ กรุงกัวลาลัมเปอร์ ประเทศ มาเลเซีย โดยได้มีการประกาศข้อตกลงด้านความร่วมมือในเรื่องอาชญากรรมทางคอมพิวเตอร์ไว้ด้วย[135]

นอกจากนี้ การประชุมอาเซียนว่าด้วยความร่วมมือด้านการเมืองและความมั่นคงในภูมิภาคเอเชีย-แปซิฟิก ยังมีแถลงการณ์ในเรื่องการรับรองความมั่นคงไซเบอร์ (ARF Statement on Cooperation in Ensuring Cyber Security) เมื่อวันที่ 12 กรกฎาคม พ.ศ. 2555 ณ กรุงพนมเปญ

---

[134] ASEAN Regional Forum ทำหน้าที่นำเอาผลจากการอภิปรายในการประชุมไปปฏิบัติและให้คำปรึกษาปัญหาการเมืองและความมั่นคงในผลประโยชน์ร่วมกันของประเทศสมาชิกอาเซียน รวมไปถึงให้ความช่วยเหลือในความพยายามสร้างความไว้เนื้อเชื่อใจและนโยบายทางการฑูตเชิงป้องกันในภูมิภาคเอเชียแปซิฟิก.

[135] ARF Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyber Space, Kuala Lumpur, 28 July 2006.

1. Endeavor to enact and implement cyber crime and cyber security laws in accordance with their national conditions and by referring to relevant international instruments and recommendations/guidelines for the prevention, detection, reduction, and mitigation of attacks to which they are party.

2. Acknowledge the importance of a national framework for cooperation and collaboration in addressing criminal, including terrorist, misuse of cyber space and encourage the formulation of such a framework.

3. Agree to work together to improve their capabilities to adequately address cyber crime, including the terrorist misuse of cyber space

4. Commit to continue working together in the fight against cyber crime, including terrorist misuse of cyber space, through activities aimed at enhancing confidence among different national Computer Security Incident Response Teams (CSIRTs), as well as formulating advocacy and public awareness programs.

ประเทศกัมพูชา ที่ประกอบไปด้วยมาตรการเพื่อเพิ่มความร่วมมือระดับภูมิภาคในเรื่องความปลอดภัยในการใช้งานข้อมูลข่าวสารและวิทยาการการสื่อสาร[136]

4.2.4 สภาหน่วยงานกำกับดูแลกิจการโทรคมนาคมแห่งอาเซียน (ASEAN Telecommunications Regulators Council: ATRC)

สภาหน่วยงานกำกับดูแลกิจการโทรคมนาคมแห่งอาเซียนประกอบไปด้วย ASEAN Telecommunications and IT Ministers Meeting (TELMIN) และ Telecommunications Senior Officials Meeting (TELSOM) ทำหน้าออกข้อบังคับและให้อำนาจสั่งการในด้านโทรคมนาคมภายในภูมิภาค และเป็น platform เพื่อความร่วมมือในผลประโยชน์ร่วมกันเพื่อการบริหารงานของประเทศสมาชิกอาเซียน ระบุและส่งเสริมในด้านโทรคมนาคมในพื้นที่ที่มีศักยภาพระหว่างประเทศสมาชิกอาเซียน และอำนวยความสะดวกในการแลกเปลี่ยนข้อมูลข่าวสารผ่านแผนงานต่าง ๆ

ในการประชุม TELMIN ครั้งที่ 3 ในปี พ.ศ. 2546 ที่สิงคโปร์ได้มีการออกแถลงการณ์สิงคโปร์ (Singapore Declaration) ที่มุ่งเน้นไปที่ความพยายามในการจัดตั้งโครงสร้างพื้นฐานทางข้อมูลข่าวสารของอาเซียนโดยมีทรรศนะในการส่งเสริมการทำงานร่วมกัน (Interoperability) การเชื่อมต่อซึ่งกันและกัน (Interconnectivity) ความมั่นคง (Security) และ ความเป็นอันหนึ่งอันเดียวกัน (Integrity) เหล่ารัฐมนตรีการสื่อสารและสารสนเทศต่างเห็นร่วมกันว่าประเทศสมาชิกอาเซียนควรพัฒนาและดำเนินการเชิงปฏิบัติซึ่งหน่วยงาน Computer Emergency Response Teams: CERTs ในระดับชาติ ภายในปี พ.ศ. 2548 ไปในทางเดียวกันกับการตกลงร่วมกันในเงื่อนไขการปฏิบัติงานขั้นต่ำ โดยเวทีประชุมจำลองในเรื่องความมั่นคงไซเบอร์กำลังถูกทำให้เป็นรูปเป็นร่างเพื่อสร้างกรอบเค้าโครงในการแลกเปลี่ยนข้อมูลข่าวสารให้เป็นไปในทิศทางเดียวกัน การจัดตั้งมาตรฐานและความร่วมมือระหว่างหน่วยงานบังคับใช้กฎหมาย และกรอบเค้าโครงสำหรับการดำเนินงานร่วมกันในด้านความปลอดภัยระบบเครือข่ายร่วมไปกับแผนปฏิบัติการได้รับการลงมติ

---

[136] ARF Statement on Cooperation in Ensuring Cyber Security, Phnom Penh, 12 July 2012.

1. Promote further consideration of strategies to address threats emerging in this field consistent with international law and its basic principles;

2. Promote dialogue on confidence-building, stability, and risk reduction measures to address the implications of ARF participants' use of ICTs, including exchange of views on the potential use of ICTs in conflict;

3. Encourage and enhance cooperation in bringing about culture of cyber security;

4. Develop an ARF work plan on security in the use of ICTs, focused on practical cooperation on confidence building measures, which could set out corresponding goals and a timeframe for their implementation;

5. Review a possibility to elaborate common terms and definitions relevant to the sphere of the use of ICTs.

รับรองในการประชุม ATRC ครั้งที่ 11 ณ กรุงปีนัง ประเทศมาเลเซีย ในระหว่างวันที่ 16-18 สิงหาคม พ.ศ. 2548 และฉบับทบทวนของกรอบเค้าโครงได้รับการลงมติรับรอง ณ การประชุม ATRC ครั้งที่ 19 ในกรุงมานาโด ประเทศอินโดนีเซีย ในเดือนสิงหาคม พ.ศ. 2556 โดยได้เปลี่ยนแปลงเนื้อหาเพื่อขยายของเขตของปัญหาด้านความปลอดภัยและรวมเอาการดำเนินการร่วมกันกับหน่วยงานอื่นที่ทำหน้าที่บังคับใช้กฎหมายด้านความปลอดภัยเครือข่ายเข้าไปด้วย ซึ่ง Mactan Cebu Declaration เมื่อการประชุม TELMIN ครั้งที่ 12 ณ กรุงเซบู ประเทศฟิลิปปินส์ ระหว่างวันที่ 15-16 พฤศจิกายน พ.ศ. 2555 ได้ระบุถึงการสร้างความร่วมมือระหว่างหน่วยงาน CERTs เพื่อรับมืออาชญากรรมทางคอมพิวเตอร์ไว้ด้วย[137]

4.2.5 การประชุมเจ้าหน้าที่อาวุโสอาเซียนด้านสวัสดิการสังคมและการพัฒนา (ASEAN Senior Officials Meeting on Social Welfare and Development: SOMSWD)

SOMSWD ได้จัดการประชุมย่อยภายใต้ชื่อว่า ASEAN Conference on Working toward a cyber pornography and cyber prostitution free southeast asia จัดขึ้น ณ กรุงมนิลา ประเทศมาเลเซีย ระหว่างวันที่ 18-22 พฤษภาคม พ.ศ. 2555 และครั้งที่ 2 ซึ่งจัดขึ้นที่ Tagbilaran, Bohol ประเทศฟิลิปปินส์ ระหว่างวันที่ 22-26 เมษายน พ.ศ. 2556 โดยข้อเสนอแนะหลายประการจากการประชุมที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์เกี่ยวข้องกับความผิดประเภทเนื้อหาของอาชญากรรมทางคอมพิวเตอร์เช่นการค้าประเวณีและการเผยแพร่สื่อลามกอนาจารเด็กบนอินเตอร์เน็ต[138]

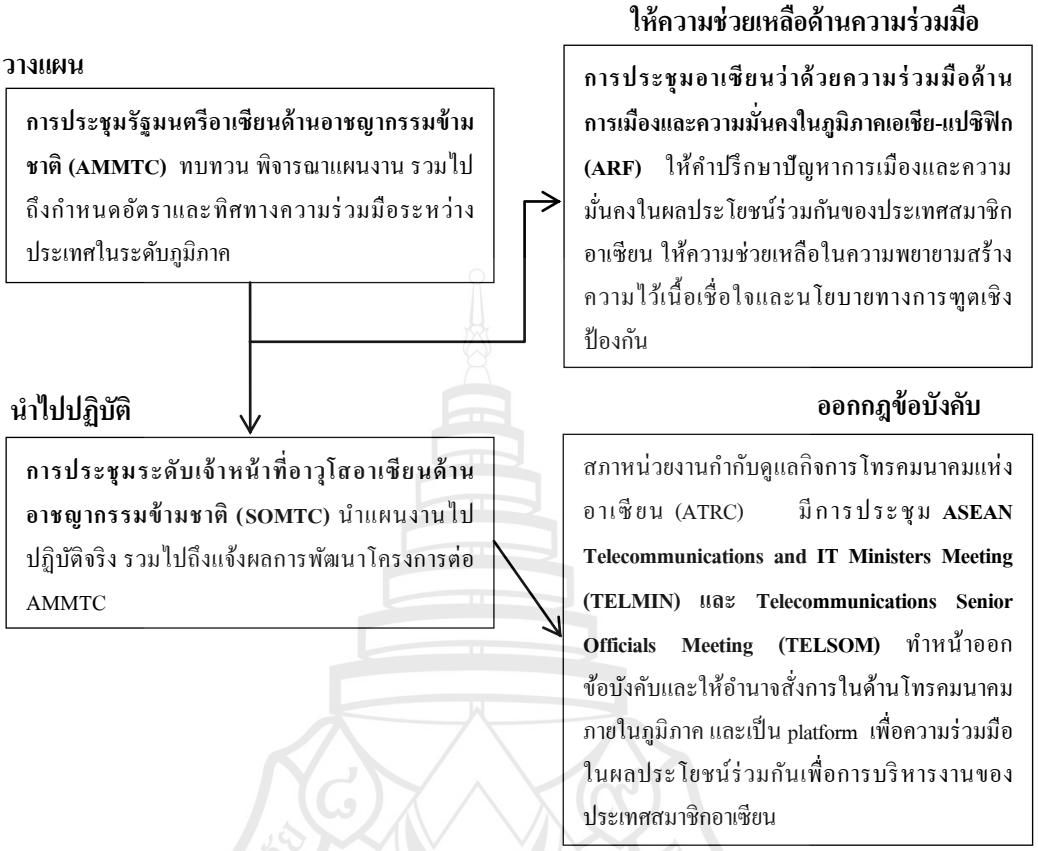
---

[137] การประชุม TELMIN ครั้งที่ 12 ณ กรุงเซบู ประเทศฟิลิปปินส์ ได้ระบุถึงเรื่องการรับมืออาชญากรรมทางคอมพิวเตอร์ไว้ว่า “Continue the collaborative activities among ASEAN Computer Emergency Response Teams (CERTs) such as the ASEAN CERTS Incident Drills (ACID), so as to enhance incident investigation and coordination amongst CERTs in support of the ASEAN Network Security Action Council (ANSAC) activities”.

[138] SOMSWD ได้มีมติให้เสริมความแข็งแกร่งของกฎหมายระดับชาติว่าให้ นิยาม ห้าม และกำหนดโทษบนพื้นฐานของหลักมาตรฐานสิทธิมนุษยชน การกระทำอันเป็นการแสวงหาประโยชน์โดยมิชอบทางเพศในเด็กและผู้เยาว์ เช่น สื่อลามกอนาจารและการค้าประเวณีบนอินเตอร์เน็ต

ส่งเสริมความร่วมมือของอาเซียนเกี่ยวกับเขตอำนาจศาลนอกอาณาเขตและการให้ความช่วยเหลือทางกฎหมายซึ่งกันและกันเพื่อช่วยให้การดำเนินคดีผู้กระทำผิดเป็นไปอย่างมีประสิทธิภาพ ในทุกคดีการแสวงหาประโยชน์ทางเพศโดยมิชอบในเด็กและผู้เยาว์ และบทลงโทษที่เหมาะสมต่อการกระทำผิดดังกล่าว

เสริมความแข็งแกร่งของหลักเกณฑ์ด้านโทรคมนาคมเพื่อครอบคลุมทั้งภาคส่วนที่เกี่ยวข้องกับการพาณิชย์และไม่ใช่เพื่อการพาณิชย์และเพื่อทำให้นโยบายการให้เก็บรักษาข้อมูล (Data retention policy) เป็นมาตรฐานสำหรับผู้ให้บริการ และ พัฒนามาตรฐานทางจริยธรรมและระบบส่งต่อ หรือ กลไกการดำเนินการร่วมกันระหว่างหน่วยงานในการดูแล รายงาน และดำเนินคดีความ และดูแลเหยื่อของสื่อลามกอนาจารและการค้าประเวณีบนอินเตอร์เน็ตที่ชัดเจน ในประเทศสมาชิกอาเซียน.



ภาพที่ 4.1 กลไกของอาเซียนในเรื่องอาชญากรรมทางคอมพิวเตอร์

4.3 แผนการเพื่อรับมืออาชญากรรมทางคอมพิวเตอร์ของอาเซียน

อาเซียนมีความพยายามการสร้างมาตรฐานด้านความปลอดภัยเพื่อรับมือกับปัญหาอาชญากรรมทางคอมพิวเตอร์ทั้งภายในและภายนอกภูมิภาค โดยอาศัยแม่แบบจากหลักเกณฑ์สากลต่าง ๆ และนำมาปรับใช้ให้เหมาะสมกับภูมิภาคที่ผ่านการประชุมต่าง ๆ หลายครั้ง ซึ่งได้กำหนดเป้าหมายการพัฒนาโครงสร้างพื้นฐานทางเทคโนโลยีการสื่อสารและสารสนเทศและความปลอดภัยไซเบอร์ลงไปในแผนงานอย่างมากมาย เช่น

4.3.1 แผนแม่บทไอซีทีอาเซียน 2015 (ASEAN ICT MASTERPLAN 2015: AIM 2015)

เรื่องความมั่นคงทางไซเบอร์ (Cyber security) นั้น แผนแม่บทไอซีทีอาเซียน[139] (AIM 2015) ได้กำหนดมาตรการ 2.4 การสร้างความเชื่อมั่น โดยส่งเสริมให้การทำธุรกรรมทางอิเล็กทรอนิกส์ที่มีความมั่นคงและปลอดภัยในภูมิภาคอาเซียน ด้วยการพัฒนาข้อตกลงยอมรับร่วมสาขาวิชาชีพ (Mutual Recognition Arrangement: MRA) เพื่อใช้ใบรับรองอิเล็กทรอนิกส์ (Electronics Certificate) ข้ามประเทศภายในภูมิภาคอาเซียนและส่งเสริมระบบความปลอดภัย 2 ชั้น เพื่อการระบุตัวตน (Two-factor authentication) รวมทั้ง การรณรงค์สร้างความตระหนักในเรื่องความมั่นคงและปลอดภัยโดยการให้ความรู้แก่สาธารณชน เพื่อสร้างความตระหนักเรื่องความมั่นคงและปลอดภัยของระบบออนไลน์ โดยการเชื่อมโยงและสร้างความร่วมมือกับภาคอุตสาหกรรม รวมทั้งผู้มีส่วนได้เสีย เพื่อให้ความมั่นใจว่ามีมาตรการป้องกันความปลอดภัยของข้อมูลส่วนบุคคล

AIM 2015 ได้กำหนดเรื่องความปลอดภัยไว้ในมาตรการ 4.2 โดยส่งเสริมให้เครือข่ายมีความมั่นคง และปลอดภัย มีการปกป้องข้อมูล รวมทั้ง มีความร่วมมือระหว่างหน่วยงานรักษาความปลอดภัยคอมพิวเตอร์ (Computer Emergency Response Team: CERT) โดยมีการร่วมสร้างกรอบว่าด้วยความมั่นคงปลอดภัยของเครือข่าย ด้วยการจัดทำมาตรฐานขั้นต่ำว่าด้วยมาตรการปกป้องเครือข่ายให้มีระดับการเตรียมพร้อมและการปกป้องเครือข่ายทั่วทั้งอาเซียน และสร้างโปรแกรมเพื่อกลั่นกรองข้อมูล (Health screening) สำหรับอาเซียน ที่สามารถทำหน้าที่กลั่นกรองเป็นช่วง ๆ อย่างต่อเนื่อง นอกจากนี้ ยังพัฒนาแนวทางปฏิบัติเพื่อให้ธุรกิจดำเนินไปได้อย่างต่อเนื่องและสามารถกู้คืนความเสียหายจากภัยพิบัติได้ รวมไปถึงการจัดทำให้มีหน่วยงานที่ทำหน้าที่เป็น ASEAN Network Security Action Council (ANSAC) เพื่อส่งเสริมให้เกิดความร่วมมือระหว่าง CERT ในการแลกเปลี่ยนประสบการณ์ ฯลฯ อีกทั้งยังร่วมมือในการสร้างกรอบเพื่อความมั่นคงและความปลอดภัยของข้อมูลเพื่อแลกเปลี่ยนวิธีปฏิบัติเกี่ยวกับการปกป้องข้อมูลและโครงสร้างพื้นฐานด้านสารสนเทศทั่วทั้งอาเซียนด้วย

ANSAC ซึ่งเป็นองค์กรความร่วมมือในเชิงพหุภาคี (Multi-stakeholder) จะเข้ามามีบทบาทประสานความร่วมมือระหว่าง Computer Emergency Response team ของประเทศสมาชิกอาเซียน

---

[139] แผนแม่บทไอซีทีของอาเซียน 2015 ได้กำหนดวิสัยทัศน์ จุดประสงค์ และการบรรลุผล โดยเป็นแผนแม่แบบในการดำเนินการปฏิรูปและเสริมศักยภาพทางเทคโนโลยีของอาเซียนด้วย ICT ซึ่งมีวัตถุประสงค์เพื่อเปลี่ยนแปลงโครงสร้างพื้นฐานในการดำรงชีวิตของประชาชนในภูมิภาคในทุกด้าน ทั้งด้านการศึกษา บันเทิง การทำงาน และชีวิตประจำวัน โดยทุกภาคส่วนของสังคม ไม่ว่าจะเป็นภาครัฐหรือเอกชน เพื่อสร้างสภาวะแวดล้อมที่เอื้อต่อการสร้างนวัตกรรม และธุรกิจรูปแบบใหม่ รวมถึงการทำให้เทคโนโลยี ICT ประสบความสำเร็จในภูมิภาคและเชื่อมต่อทุกภาคส่วนในอาเซียนเข้าด้วยกันไม่ว่าจะเป็นภาคเอกชนหรือรัฐ.

โดยมีประเทศมาเลเซียเป็นผู้รับผิดชอบภายใต้เงินทุนจาก ASEAN ICT FUND ทั้งนี้ การประชุม ANSAC ครั้งแรกได้จัดขึ้นเมื่อวันที่ 5 มิถุนายน พ.ศ. 2556 ณ กรุงมานาโด ประเทศอินโดนีเซีย

4.3.2 แผนงานจัดตั้งประชาคมการเมืองและความมั่นคงอาเซียน (ASEAN Political and Social Community blueprint: APSC blueprint)

APSC blueprint[140] ได้วางแนวทางในเรื่องของอาชญากรรมทางคอมพิวเตอร์ไว้ในข้อ B 4.1 เสริมสร้างความร่วมมือในการรับมือกับประเด็นปัญหาความมั่นคงรูปแบบใหม่ (Non-traditional Security Issues) โดยเฉพาะอย่างยิ่ง เรื่องการต่อต้านอาชญากรรมข้ามชาติและความท้าทายข้ามแดนอื่น ๆ[141] สำหรับ ข้อที่ 16-17 นั้นก็ “เสริมสร้างความร่วมมือและให้ความช่วยเหลือในการต่อต้านและควบคุมการแพร่ขยายของอาชญากรรมทางคอมพิวเตอร์ ซึ่งรวมถึงความร่วมมือระหว่างหน่วยงานผู้บังคับใช้กฎหมาย โดยคำนึงถึงความจำเป็นของแต่ละประเทศในการพัฒนากฎหมายเพื่อรับมือปัญหาอาชญากรรมทางคอมพิวเตอร์”[142]

4.3.3 แผนแม่บทว่าด้วยความเชื่อมโยงระหว่างกันในภูมิภาคอาเซียน (Master Plan on ASEAN Connectivity)[143]

ภายใต้แผนยุทธศาสตร์ที่ 6 ที่เร่งพัฒนาการของโครงสร้างพื้นฐานสารสนเทศและบริการในทุกประเทศสมาชิกอาเซียน ได้มีปฏิบัติการสำคัญ (Key action) ที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์ คือ “ส่งเสริมบูรณาภาพของระบบเครือข่ายและความปลอดภัยข้อมูล การคุ้มครอง

---

[140] APSC blueprint เป็นแผนการความร่วมมือด้านการเมืองและความมั่นคงของอาเซียน ซึ่งจะเป็นหลักประกันสำหรับประชาชนและประเทศสมาชิกอาเซียนในการอยู่ร่วมกันอย่างสันติในบรรยากาศของความเป็นประชาธิปไตย ความยุติธรรมและการปรองดอง ส่งเสริมพัฒนาการด้านการเมืองโดยยึดหลักประชาธิปไตยและคุ้มครองสิทธิมนุษยชน ภายใต้กฎบัตรอาเซียน ส่งเสริมความร่วมมือระหว่างประเทศ อีกทั้งยังสนับสนุนแนวทางด้านความมั่นคงที่ครอบคลุมทุกมิติและพึ่งพาการแก้ปัญหาอย่างสันติวิธี.

[141] ปัญหาในรูปแบบ Non-traditional Security (NTS) ได้แก่ อาชญากรรมข้ามชาติ และผลกระทบทางด้านลบต่าง ๆ เช่น ผลกระทบต่อสิ่งแวดล้อมและปัญหาสาธารณสุข เป็นต้น.

[142] APSC blueprint B 4.2 XVI. Manner, Illicit Small Arms and Light Weapons (International Tracing Instrument); Strengthen cooperation and assistance in combating and suppressing cybercrimes including cooperation among law enforcement agencies, taking into account the need.

XVII.of each country to develop laws to address cybercrimes.

[143] Master Plan on ASEAN Connectivity ทำหน้าที่เป็นแผนแม่บทในโครงการใหญ่และแผนยุทธศาสตร์ระยะยาวเพื่อพัฒนาภูมิภาคในด้านการเชื่อมต่อทางกายภาพ สถาบัน และผู้คน ในขณะที่ยอมรับประโยชน์ที่จับต้องได้ของการเชื่อมต่อที่ใกล้มากยิ่งขึ้น แผนแม่บทได้ยอมรับว่าปัญหาที่เกิดจากอาชญากรรมข้ามชาติ การหลบหนีเข้าเมืองโดยผิดกฎหมายการทำลายสภาวะแวดล้อมและมลพิษ และอุปสรรคข้ามเขตแดนนั้นต้องได้รับการจัดการอย่างเหมาะสม.

ข้อมูล และความร่วมมือระหว่าง CERTs โดยการพัฒนากรอบเค้าโครงสามัญและจัดตั้งมาตรฐานกลางร่วมกันในกรณีที่จำเป็น เพื่อเป็นหลักประกันของระดับความพร้อมและบูรณาภาพของระบบเครือข่ายทั่วอาเซียนภายในปี พ.ศ. 2558 (2015)"[144]

4.3.4 โครงการของ ATRC ร่วมกับคู่เจรจาอาเซียน (ATRC Projects with ASEAN Dialogue Partners)

โครงการของ ATRC ร่วมกับคู่เจรจาอาเซียนนั้น ได้มีการประชุมเชิงปฏิบัติการร่วมในรูปแบบต่าง ๆ เช่น

READI Workshop on cybercrime legislation in ASEAN member states จัดขึ้นระหว่างวันที่ 27-28 พฤศจิกายน พ.ศ. 2551 ณ กรุงกัวลา ลัมเปอร์ ประเทศมาเลเซีย และระหว่างวันที่ 26-28 มกราคม พ.ศ. 2553 ณ กรุงมนิลา ประเทศฟิลิปปินส์

ASEAN–EU Training for law enforcement, judges and prosecutors on cybercrime จัดขึ้นระหว่างวันที่ 4-8 กรกฎาคม พ.ศ. 2554 ประเทศมาเลเซีย

ASEAN-Japan information security policy meeting ที่จัดขึ้นทุกปีตั้งแต่ พ.ศ. 2551 และ ASEAN-Japan network security workshop ที่จัดขึ้นทุกปีตั้งแต่ พ.ศ. 2552 โดยมีประเทศญี่ปุ่นและประเทศสมาชิกอาเซียนผลัดกันเป็นเจ้าภาพ ASEAN-China network security ที่จัดขึ้นทุกปีตั้งแต่ พ.ศ. 2552 โดยมีประเทศจีนเป็นเจ้าภาพ

โดยสรุปแล้วถึงแม้อาเซียนยังไม่สามารถหาวิธีการจัดการอาชญากรรมทางคอมพิวเตอร์แบบเบ็ดเสร็จเด็ดขาด และยังคงเป็นปัญหาที่ต้องมีการศึกษาทำความเข้าใจต่อไปในภายภาคหน้า แต่ความพยายามในการร่วมมือกัน เพื่อสร้างมาตรฐานกลางในกรอบเค้าโครงด้านความมั่นคงไซเบอร์ในระดับภูมิภาคจะไม่เพียงเป็นประโยชน์ร่วมกันของประเทศสมาชิกอาเซียนเท่านั้น แต่จะเป็นประโยชน์ต่อภูมิภาคและประชาคมโลกโดยรวมอีกด้วย ในแผนแม่บทว่าด้วยความเชื่อมโยงระหว่างกันในภูมิภาคอาเซียน ได้กำหนดเป้าหมายเพื่อสร้างทางออกแบบสมประโยชน์สำหรับทุกฝ่ายแก่ประเทศสมาชิกอาเซียน โดยการเชื่อมโยงอาเซียนเข้าด้วยกันเพื่อสร้างตลาดร่วมตลาดเดียวและฐานการผลิตรวมทั้งการช่วยเหลือประเทศคู่เจรจาในเอเชียแปซิฟิกในด้านการขนส่งหรือขนถ่ายพลังงาน อย่างระบบรางรถไฟหรือการสร้างท่อส่งกาซธรรมชาติข้ามประเทศ มาตรการเหล่านี้จะช่วยยกตำแหน่งอาเซียนในเวทีการประชุมนานาชาติ และช่วยส่งเสริมความพยายามในการปรับปรุง

---

[144] Master Plan on ASEAN Connectivity (iv) Promote network integrity and information security, data protection and Computer Emergency Response Team (CERT) cooperation by developing common frameworks and establishing common minimum standards where appropriate, to ensure a level of preparedness and integrity of networks across ASEAN by 2015.

โครงสร้างของการจัดการภายในภูมิภาคที่พัฒนาขึ้นเรื่อย ๆ และสนับสนุนความร่วมมือระหว่างประเทศในขณะนั้นและในอนาคตเช่นเดียวกับความพยายามในด้านการรักษาความปลอดภัยไซเบอร์ที่มีความจำเป็นในการรับมือกับอาชญากรรมทางคอมพิวเตอร์ ที่มีลักษณะข้ามชาติอย่างมีประสิทธิภาพ รัฐบาลและสถาบันต่าง ๆ จำเป็นต้องปรับตัวอย่างรวดเร็วและให้เท่าทันต่อเหตุการณ์เพื่อคาดการณ์ถึงแนวโน้มที่จะเกิดขึ้น ดังนั้น เพื่อหลีกเลี่ยงการเพลี่ยงพล้ำต่อการเปลี่ยนแปลงของสังคมโลก การรับเอาโครงสร้างและวิธีการคิดใหม่ ๆ มาปรับใช้จึงเป็นสิ่งที่อาเซียนและประเทศสมาชิกต้องทำและทบทวนอยู่เสมอ

4.3.5 สรุปแผนงาน แผนปฏิบัติการ และกรอบเค้าโครงของอาเซียนที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์

ASEAN Secretariat, Master Plan on ASEAN Connectivity, January 2011

ASEAN Secretariat, ASEAN ICT Master plan 2015 (AIM), 2011

ASEAN Secretariat, ASEAN Political-Security Community Blueprint, June 2009

ASEAN Secretariat, ASEAN Socio-Cultural Community Blueprint, June 2009

ASEAN Secretariat, ASEAN Economic Community Blueprint, January 2008

ASEAN, Initiative for ASEAN Integration (IAI) Strategic Framework and IAI Work Plan 2 (2009 -2015)

The Framework for Cooperation on Network Security and Action Plan adopted at the 11th ATRC Meeting, 16-18 August 2005

ปฏิญญา

ASEAN, Mactan Cebu Declaration Connected ASEAN: Enabling Aspirations, 19 November 2012

ASEAN, Bali Declaration on ASEAN Community in a Global Community of Nations “Bali Concord III”, 19th ASEAN Summit, 17 November 2011

Singapore Declaration, 3rd TELMIN 2003

ตารางที่ 4.1 แผนการเพื่อรับมืออาชญากรรมทางคอมพิวเตอร์ของอาเซียน

แผนการ	รายละเอียด
APSC blueprint	เสริมสร้างความร่วมมือและให้ความช่วยเหลือในการต่อต้าน และควบคุมการแพร่ขยายของอาชญากรรมทางคอมพิวเตอร์ ซึ่งรวมถึงความร่วมมือระหว่างหน่วยงานผู้บังคับใช้กฎหมาย โดยคำนึงถึงความจำเป็นของแต่ละประเทศในการพัฒนากฎหมายเพื่อรับมือปัญหาอาชญากรรมทางคอมพิวเตอร์
ASEAN ICT Master plan 2015	1. มีความร่วมมือระหว่างหน่วยงานรักษาความปลอดภัยคอมพิวเตอร์ CERT 2. จัดทำมาตรฐานขั้นต่ำว่าด้วยมาตรการปกป้องเครือข่ายให้มีระดับการเตรียมพร้อมและการปกป้องเครือข่ายทั่วทั้งอาเซียน 3. สร้างโปรแกรมเพื่อกลั่นกรองข้อมูล (Health screening) สำหรับอาเซียน 4. ส่งเสริมระบบความปลอดภัย 2 ชั้นเพื่อการระบุตัวตน (Two-factor authentication) 5. การสร้างพัฒนาข้อตกลงยอมรับร่วมสาขาวิชาชีพ (Mutual Recognition Arrangement, MRA) เพื่อใช้ใบรับรองอิเล็กทรอนิกส์ข้ามประเทศภายในอาเซียน 6. จัดทำให้มีหน่วยงานที่ทำหน้าที่เป็น ASEAN Network Security Action Council 7. สร้างความเชื่อมั่นโดยส่งเสริมให้ทำธุรกรรมทางอิเล็กทรอนิกส์ที่มีความมั่นคงและปลอดภัยในภูมิภาคอาเซียน 8. รณรงค์สร้างความตระหนักในเรื่องความมั่นคงและปลอดภัยโดยการให้ความรู้แก่สาธารณชนในเรื่องความปลอดภัยออนไลน์ เพื่อสร้างความตระหนักเรื่องความมั่นคงและปลอดภัยของระบบออนไลน์ และ เชื่อมโยง สร้างความร่วมมือกับภาคอุตสาหกรรมและผู้มีส่วนได้เสีย และให้มั่นใจว่ามีมาตรการป้องกันความปลอดภัยของข้อมูลส่วนบุคคล
Master Plan on ASEAN Connectivity	ส่งเสริมบูรณาภาพของระบบเครือข่ายและความปลอดภัยข้อมูล การคุ้มครองข้อมูล และ ความร่วมมือระหว่าง CERT โดยการพัฒนากรอบเค้าโครงสามัญและจัดตั้งมาตรฐานกลางร่วมกันในกรณีที่จำเป็น เพื่อประกันระดับของความพร้อมและบูรณาภาพของระบบเครือข่ายทั่วอาเซียนภายในปี พ.ศ. 2558
ASEAN SOMSWD	เสริมสร้างกฎหมายระดับชาติและความร่วมมือระหว่างประเทศ นิยาม ห้าม และกำหนดโทษบนพื้นฐานของหลักมาตรฐานสิทธิมนุษยชน การกระทำอันเป็นการแสวงหาประโยชน์โดยมิชอบทางเพศในเด็กและผู้เยาว์ เช่น สื่อลามกอนาจาร และการค้าประเวณีบนอินเตอร์เน็ต

4.4 กฎหมายที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ของประเทศสมาชิกอาเซียน

ประเทศสมาชิกอาเซียนได้ตระหนักถึงความสำคัญของปัญหาอาชญากรรมคอมพิวเตอร์ โดยได้ให้ความสำคัญกับการบัญญัติกฎหมายเพื่อรับมือกับอาชญากรรมทางคอมพิวเตอร์ประเภทต่าง ๆ ที่อาศัยแนวทางจากทั้งคำแนะนำขององค์กรระหว่างประเทศต่าง ๆ[145] เช่น องค์การสหประชาชาติ และสภาพยุโรป ฯลฯ เพื่อสร้างความสอดประสานกันไม่เพียงในระดับภูมิภาคแต่ยังรวมถึงระดับโลกอีกด้วย จากรายงานของ UNCTAD เมื่อเดือนกันยายน พ.ศ. 2556 แสดงให้เห็นว่า 8 ใน 10 ของประเทศสมาชิกอาเซียน มีกฎหมายอาชญากรรมทางคอมพิวเตอร์อยู่ในระดับสูงกว่ามาตรฐานโลก[146] ดังนี้

4.4.1 ประเทศมาเลเซีย

ประเทศมาเลเซียถือว่าเป็นผู้นำด้านความมั่นคงไซเบอร์และอาชญากรรมทางคอมพิวเตอร์ในภูมิภาคอาเซียน เนื่องเป็นประเทศที่ออกกฎหมายอาชญากรรมทางคอมพิวเตอร์มาใช้เป็นประเทศแรก ๆ ในอาเซียน ตั้งแต่ปี พ.ศ. 2540 (Computer Crime Act of 1997, The Digital Act 1997) รวมทั้ง Digital signature regulation และ Communication and Multimedia Act of 1998 ในปี พ.ศ. 2541 ซึ่งครอบคลุมทั้งในส่วนของกฎหมายวิธีสบัญญัติและวิธีสารบัญญัติตามมาตรฐานอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของสหภาพยุโรป โดยประเทศมาเลเซียได้จัดตั้ง Malaysia's Communications and Multimedia (MCMC or SKMM) ขึ้นเพื่อดูแลความมั่นคงทางอินเตอร์เน็ตทั่วไป และการให้คำแนะนำแก่เว็บไซต์ในเรื่องความปลอดภัย รวมทั้งยังมีความร่วมมือระหว่างภาครัฐและเอกชน โดยเฉพาะในพื้นที่ชนบท เพื่อให้ประชาชนสามารถเข้าถึงบริการของรัฐได้อย่างทั่วถึง

นอกจากนี้ ประเทศมาเลเซียยังมีหน่วยงานของรัฐอีกหลายองค์กรที่ดูแลในเรื่องความปลอดภัยไซเบอร์ ได้แก่

Cyber Security Malaysia เป็นองค์กรที่อยู่ใต้การดูแลของ MOSTI กระทรวงวิทยาศาสตร์เทคโนโลยีและนวัตกรรม หน้าที่หนึ่งขององค์กรนี้ คือ เป็นศูนย์การดำเนินการช่วยเหลือ Cyber999 ที่ก่อตั้งมาเพื่อให้ผู้ใช้งานอินเตอร์เน็ตชาวมาเลเซียสามารถแจ้งเหตุภัยคุกคามต่าง ๆ เช่น ความพยายามเจาะระบบ การข่มขู่ การฉ้อโกง และแสปม ฯลฯ

---

[145] Council of Europe, *Project on Cybercrime final report (September 2006-February 2009)*, (Strasburg: Council of Europe, 2009), 17-19.

[146] UNCTAD, *UNCTAD review of ASEAN e-commerce laws published*, 20 September 2013, Retrieved 2014, April 24, from http://unctad.org/en/pages/newsdetails.aspx?OriginalVersionID=613&Sitemap_x0020_Taxonomy=UNCTAD%20Home;

Malaysian Communications & Multimedia Commission (MCMC or SKMM) MCMC เป็นหน่วยงานที่ให้บริการข้อมูลแก่ผู้ปกครองในด้านปัญหาความปลอดภัยทางอินเตอร์เน็ตแก่เด็กทั้งในเรื่อง การกลั่นแกล้งทางสื่ออิเล็กทรอนิกส์ (Cyber bullying) ไปจนถึงปัญหาการเสพย์ติดเกมคอมพิวเตอร์

Cyber Security Awareness For Everyone (CyberSAFE Malaysia) ซึ่งดำเนินการภายใต้การอุปถัมภ์ของ Cyber Security Malaysia โดยองค์กรมุ่งเป้าไปที่การสร้างความปลอดภัยบนอินเตอร์เน็ตและให้ข้อมูลด้านความปลอดภัยไซเบอร์แก่ประชาชนในทุกพื้นที่

Multimedia Development Corporation (MDec) เป็นองค์กรที่ดำเนินการโดยอาศัยทุนจากรัฐบาล แต่องค์กรนี้มุ่งจะดำเนินการในรูปขององค์กรเอกชนมากกว่าหน่วยงานของรัฐ โดย MDec ร่วมงานกับภาครัฐด้วยการให้คำปรึกษาแก่รัฐบาลในการออกนโยบายเกี่ยวกับกฎหมายอินเตอร์เน็ต (Cyber laws)[147]

ในส่วนของตัวบทกฎหมาย รัฐบาลมาเลเซียได้ออกกฎหมายเพื่อรับมือกับปัญหาอาชญากรรมทางคอมพิวเตอร์มาตั้งแต่ปี พ.ศ. 2540 เพื่อลดความเสี่ยงในการทำธุรกรรมออนไลน์ รวมไปถึงลดปัญหาการฉ้อโกงทางอินเตอร์เน็ต โดยอาจแบ่งกฎหมายที่บัญญัติออกมาตั้งแต่อดีตถึงปัจจุบันได้ดังนี้

The Digital Act 1997 มีวัตถุประสงค์เพื่อควบคุมวิธีการสื่อสารหรือทำธุรกรรมออนไลน์ของประชาชนเพื่อป้องกันการใช้งานโดยมิชอบ โดยลายเซ็นอิเล็กทรอนิกส์ (Digital signature) ถือเป็นเครื่องระบุตัวตนของผู้ใช้ โดยวิธีการเข้ารหัสเพื่อป้องกันการปลอมแปลง ซึ่งช่วยปกป้องข้อมูลที่ถูกส่งออกไปจากการถูกรบกวนหรือดักจับ โดยลายเซ็นอิเล็กทรอนิกส์จะถูกต้องตามกฎหมายเมื่อได้รับ Certificate authority license โดยผู้มีอำนาจในสิทธิ์นั้น และธุรกรรมใด ๆ ที่กระทำโดยถูกต้องตามกฎหมายฉบับนี้ถือว่าเป็นธุรกรรมที่ชอบด้วยกฎหมาย

The Computer Crime Act 1997 เป็นกฎหมายโดยเฉพาะเพื่อรับมือกับอาชญากรรมทางคอมพิวเตอร์ ฉบับแรกของประเทศสมาชิกอาเซียน โดยเนื้อหาของกฎหมายฉบับนี้จะครอบคลุมการใช้งานคอมพิวเตอร์โดยมิชอบทางกฎหมาย เช่น การเจาะระบบและทำลายระบบเครือข่ายคอมพิวเตอร์และการแพร่ไวรัสคอมพิวเตอร์ คุ้มครองสิทธิ์และความเป็นส่วนตัวของผู้ใช้คอมพิวเตอร์ ซึ่งความผิดตามกฎหมายฉบับนี้ได้แก่ การเข้าถึงข้อมูลคอมพิวเตอร์ของผู้อื่นโดยไม่ได้รับอนุญาต (Unauthorized access) การแก้ไขข้อมูลโดยไม่ได้รับอนุญาต (Unauthorized modification) โดยกฎหมายนี้มีความคล้ายคลึงกับ Computer Fraud and Abuse Act 1986 ของ

---

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

ประเทศสหรัฐอเมริกา Computer Misuse Act 1990 ของประเทศสหราชอาณาจักร และ Computer Misuse Act 1993 ของประเทศสิงคโปร์

Communication and Multimedia Act 1998 กฎหมายฉบับนี้มีวัตถุประสงค์เพื่อส่งเสริมนโยบายของชาติในภาคการสื่อสารและมัลติมีเดีย และรับรองความปลอดภัยและความน่าเชื่อถือของข้อมูล รวมทั้งราคาค่าบริการต่าง ๆ ที่เกี่ยวข้องอยู่ในระดับที่สาธารณชนสามารถใช้บริการได้อย่างเหมาะสม กฎหมายฉบับนี้ได้ออกข้อกำหนดต่าง ๆ ที่หลากหลาย เช่น การกำหนดสัญญาอนุญาต (License agreement) ของผู้ให้บริการเครือข่าย ผู้ให้บริการโปรแกรม และผู้ให้บริการเนื้อหาออนไลน์ รวมไปถึงการดำเนินคดีกับผู้ที่ส่ง Email หรือ Sms ลามกอานาจาร หรือโพสท์ข้อความมุ่งร้ายหรือดูหมิ่นผู้อื่น เป็นต้น

Copyright Act ฉบับแก้ไขเพิ่มเติม ปี ค.ศ. 1997 กฎหมายลิขสิทธิ์ของประเทศมาเลเซียได้รับการแก้ไขเพื่อรองรับการเปลี่ยนแปลงทางวิทยาการในอนาคต ซึ่งอาจจะกลายเป็นปัญหาต่องานอันมีลิขสิทธิ์บนอินเตอร์เน็ตได้ โดยมีการเพิ่มการคุ้มครองลิขสิทธิ์ซอฟท์แวร์และให้การแก้ไขระบบป้องกันที่มากับซอฟท์แวร์เป็นความผิด รวมไปถึงควบคุมการส่งข้อมูลเพลง หนังสือ หรือภาพยนตร์ในรูปแบบดิจิตอลบนอินเตอร์เน็ต[148] คล้ายคลึงกับ U.S. Digital Millennium Act ของประเทศสหรัฐอเมริกา

Personal Data Protection Act 2010 เป็นกฎหมายที่ให้การคุ้มครองข้อมูลส่วนบุคคลของมาเลเซีย โดยคุ้มครองข้อมูลส่วนบุคคลในด้านการทำธุรกรรมและปกป้องประโยชน์ของผู้ใช้ข้อมูลนั้น ซึ่งมุ่งหมายเพื่อสร้างความเชื่อมั่นและส่งเสริมให้มีการใช้งานธุรกรรมอิเล็กทรอนิกส์ ทั้งนี้กฎหมายฉบับนี้ได้กำหนดหลักเกณฑ์ในการจัดการข้อมูลส่วนบุคคลในบริษัทและองค์กรต่าง ๆ ในการทำธุรกรรมระหว่างกัน

โดยสรุป จะเห็นได้ว่าประเทศมาเลเซียมีความพยายามเป็นอย่างมากในการสร้างความปลอดภัยและน่าเชื่อถือให้กับไซเบอร์สเปซเพื่อส่งเสริมธุรกิจอิเล็กทรอนิกส์และเพิ่มจำนวนผู้ใช้อินเตอร์เน็ตให้มากขึ้น

---

[148] Malaysia Copyright (Amendment) Act 1997 (Act A994).

ตารางที่ 4.2 กฎหมายที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ของประเทศมาเลเซีย

ประเภท	กฎหมาย
Privacy	มี (Personal Data Protection Act 2010)
Cyber crime	มี (The Computer Crime Act 1997)
Spam	มี (Communication and Multimedia Act1998)
Online Content filtering	มี (Communication and Multimedia Act1998)
Copyright (Digital)	มี (Copyright Act ฉบับแก้ไขเพิ่มเติม ปี 1997)

4.4.2 ประเทศสิงคโปร์

ประเทศสิงคโปร์มีความตั้งใจในการปรับปรุงกฎหมายให้ได้มาตรฐานโลกอยู่เสมอตั้งแต่การพัฒนานโยบายและยุทธศาสตร์เพื่อตอบสนองต่อการเติบโตของ Cloud computing ไปจนถึงการออกกฎหมายคุ้มครองข้อมูลส่วนบุคคล Personal Data Protection Act 2012 ประเทศสิงคโปร์ถือว่าเป็นประเทศที่มีอัตราการใช้งานเทคโนโลยีสารสนเทศ อินเตอร์เน็ตและโทรศัพท์มือถือต่อจำนวนประชากรสูงที่สุดในอาเซียน[149]

สำหรับกฎหมายว่าด้วยอาชญากรรมคอมพิวเตอร์ของประเทศสิงคโปร์คือ Computer Misuse Act 1993 นั้นได้รับอิทธิพลจากกฎหมาย Computer Misuse Act ของสหราชอาณาจักร ในกฎหมายสารบัญญัติ และในด้านเนื้อหาของตัวบทกฎหมายที่รับมาจากกฎหมายอาญาดั้งเดิมซึ่งมีพื้นฐานอยู่บนหลักการและแนวทางในการตัดสินของผู้พิพากษา (Case law) กฎหมาย Computer Misuse Act 1993 ฉบับนี้ได้ให้นิยามคำว่าคอมพิวเตอร์ไว้อย่างกว้าง ๆ และไม่เจาะจงเฉพาะเทคโนโลยีใดเทคโนโลยีหนึ่งเท่านั้น หากแต่สามารถประยุกต์ใช้กับใครก็ได้ ไม่ว่าที่อยู่ทางกายภาพจะอยู่ที่ใด ได้กระทำการใดที่เกี่ยวข้องกับคอมพิวเตอร์ โปรแกรม และข้อมูลที่อยู่ในประเทศสิงคโปร์ ณ เวลานั้น ทั้งนี้ บทบัญญัติที่ว่าด้วยความผิดในกฎหมาย Computer Misuse Act 1993 ของสิงคโปร์นั้นได้สอดคล้องกับอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ โดยเฉพาะอย่างยิ่งในส่วนที่เกี่ยวข้องกับกฎหมายวิธีพิจารณาความอาญานั้นได้ครอบคลุมไปถึงการค้นหาและยึดข้อมูลทางคอมพิวเตอร์เช่นเดียวกับการสั่งให้มีการจัดทำข้อมูล แต่อย่างไรก็ตาม กฎหมายภายในประเทศสิงคโปร์ไม่ได้ให้

[149] อัตราการลงชื่อใช้บริการโทรศัพท์มือถือ 149.5 ต่อประชากร 100 คน จำนวนหลังคาเรือนที่เชื่อมต่ออินเตอร์เน็ต 85% และร้อยละ 75 ของประชากรทั้งหมดใช้อินเตอร์เน็ต, UNCTAD, *Review of e-commerce legislation harmonization in the Association of Southeast Asian Nations (ASEAN) [UNCTAD/DTL/STICT/2013/1]*, (Geneva: UNCTAD, 2013), 37-39.

อำนาจในการดักจับข้อมูลหรือเนื้อหาจากการสื่อสารผ่านโทรศัพท์หรืออินเตอร์เน็ตเหมือนกับอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์[150] ซึ่งอาจทำให้เกิดข้อจำกัดในด้านความร่วมมือระหว่างประเทศตามที่ได้กำหนดไว้ในอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์[151]

นอกจากนี้ ประเทศสิงคโปร์ได้แบ่งการควบคุมเนื้อหาทางออนไลน์ออกเป็นสามส่วนด้วยกัน ได้แก่ การควบคุมโดยรัฐด้วยการออกใบอนุญาต (Class license) การควบคุมด้วยตนเองในภาคธุรกิจ (Self-regulation) และโครงการให้การศึกษาสาธารณะ

สำนักงานพัฒนาสื่อ (Media Development Authority: MDA) ของสิงคโปร์ทำหน้าที่ออกใบอนุญาตและเงื่อนไขการลงทะเบียนซึ่งกำหนดโทษให้กับเนื้อหาบนอินเตอร์เน็ตและผู้ให้บริการหากดำเนินการไม่สอดคล้องกับข้อห้ามของ MDA และ สำนักงานนี้ยังทำหน้าที่รับรองว่าจะไม่มีสิ่งใดที่ประกอบไปด้วยเนื้อหาของสื่อใด ๆ ก็ตามที่รบกวนความสงบเรียบร้อยของสังคมหรือขัดต่อศีลธรรมอันดีของประชาชน หัวใจของกรอบเค้าโครงนี้คือแผนการออกใบอนุญาต ซึ่ง MDA เป็นผู้กำหนดเงื่อนไข ภายใต้กฎหมายการกระจายภาพและเสียง (Broadcasting Act) และ นโยบายทางธุรกิจ และข้อบังคับต่าง ๆ ที่ออกโดย MDAสำหรับแผนการออกใบอนุญาต ผู้ให้บริการอินเตอร์เน็ต (ISPs) และผู้ให้บริการเนื้อหาบนอินเตอร์เน็ต (ICPs) ทั้งหมดไม่ว่าจะเป็นพรรคการเมืองหรือปัจเจกชนใดที่ประสงค์จะทำการเผยแพร่ ส่งเสริม หรือ อภิปราย ในเรื่องทางการเมืองหรือศาสนา ต้องทำการลงทะเบียนกับ MDA ในฐานะผู้รับใบอนุญาต ISPs และ ICPs จะผูกพันภายใต้ระเบียบปฏิบัติ (Code of practice) ของ MDA ซึ่งได้ให้คำนิยาม เนื้อหาต้องห้าม (Prohibited material) อย่างกว้าง ๆ โดยระบุชี้ชัดเฉพาะมาตรฐานสำหรับเนื้อหาที่เกี่ยวกับเพศ ความรุนแรง และไม่เป็นที่ยอมรับในสังคมเท่านั้น ในขณะที่การกลั่นกรองเนื้อหาไม่ได้อยู่ในของเขตอำนาจของ ISPs หน้าที่ในการปฏิเสธการเข้าถึงเนื้อหาเหล่านั้นจะเป็นของ ICPs หากได้รับคำสั่งจาก MDA ในกรณีที่ผู้รับใบอนุญาตไม่กระทำตามจะได้รับบทลงโทษ เช่น ปรับ และ พักหรือยกเลิกใบอนุญาต นอกจากนี้ประเทศสิงคโปร์ยังมีกฎหมายเกี่ยวกับการห้ามเผยแพร่เนื้อหาอันเป็นการดูหมิ่นเชื้อชาติ (Racism) ใน Sedition Act ซึ่งปรับใช้กับเนื้อหาบนอินเตอร์เน็ตได้อีกด้วย

สำหรับกฎหมายคุ้มครองข้อมูลส่วนบุคคล Personal Data Protection Act 2012 ของประเทศสิงคโปร์นั้นได้บัญญัติตามคู่มือด้านสิทธิส่วนบุคคลของ OECD และสอดคล้องกับแนวทางของสหภาพยุโรปว่าด้วยการคุ้มครองข้อมูล ประเทศสิงคโปร์เป็นสมาชิกของ APEC ด้วย ดังนั้นจึง

---

[150] Cybercrime Convention, Article 16 Expedited preservation of stored computer data. รายละเอียดปรากฏในภาคผนวก ก หน้า 166.

[151] Cybercrime Convention, Article 29 Expedited preservation of stored computer data., Article 30 Expedited disclosure of preserved traffic data., รายละเอียดปรากฏในภาคผนวก ก หน้า 166.

ได้รับอิทธิพลจากกรอบเค้าโครงด้านสิทธิส่วนบุคคลของ APEC มาด้วย โดยกฎหมายได้กำหนดให้มีการจัดตั้งคณะกรรมาธิการคุ้มครองข้อมูล (Data protection commission) ขึ้นเป็นองค์กรอิสระ[152]

โดยสรุปแล้วประเทศสิงคโปร์นอกจากจะมีบทบัญญัติทางกฎหมายที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์แล้วก็ยังให้ความสำคัญในด้านความร่วมมือระหว่างประเทศโดยประเทศสิงคโปร์มี SingCERT และใช้วิธีทำข้อตกลงทวิภาคี อีกทั้งยังมีการนำเอาหลักถ้อยทีถ้อยอาศัย (Reciprocity) มาปรับใช้

ตารางที่ 4.3 กฎหมายที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ของประเทศสิงคโปร์

ประเภท	กฎหมาย
Privacy	มี (Personal Data Protection Act 2012)
Cyber crime	มี (Computer Misuse Act 1993)
Spam	มี
Online Content filtering	มี (Sedition Act)
Copyright (Digital)	มี

4.4.3 ประเทศอินโดนีเซีย

สำหรับประเทศอินโดนีเซียนั้นได้บัญญัติกฎหมาย Electronic Information and Transaction law 2008 ซึ่งประกอบไปด้วยข้อบังคับในด้านการพาณิชย์อิเล็กทรอนิกส์ ความเป็นส่วนตัว อาชญากรรมทางคอมพิวเตอร์ และการควบคุมเนื้อหาออนไลน์ไว้ด้วยกัน โดยนำเอาข้อเสนอแนะ (Recommendation) ของสภายุโรปมาปรับใช้ครอบคลุมในกฎหมายสารบัญญัติ เช่นเดียวกับกฎหมายวิธีพิจารณาความอาญา และมีการออกกฎหมายอาชญากรรมคอมพิวเตอร์เพื่อให้ครอบคลุมปัญหาเฉพาะบางประการในเรื่องกฎหมายวิธีสารบัญญัติ บทบัญญัติทางกฎหมายอาชญากรรมทางคอมพิวเตอร์ในกฎหมายฉบับนี้ครอบคลุมตามแบบในมาตรา 29-37 ของอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ที่ครอบคลุมเรื่อง การเข้าถึงอย่างผิดกฎหมาย (Illegal Access) การดักจับข้อมูลอย่างผิดกฎหมาย (Illegal interception) การรบกวนข้อมูล (Data interference) การใช้งานอุปกรณ์ในทางที่ผิด (Misuse of devices) การฉ้อโกงทางคอมพิวเตอร์ (Computer related fraud) และการปลอมแปลง (Forgery) นอกจากนี้กำลังอยู่ในระหว่างการร่างกฎหมายสบัญญัติซึ่งจะเป็นไปตามมาตรฐานของ

[152] Personal Data Protection Commission Singapore, *Personal Data Protection Act: Overview*, (28 January 2014), Retrieved 2014, March 8, from http://www.pdpc.gov.sg/personal-data-protection-act

อนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์[153] ซึ่งประเทศอินโดนีเซียจะมีการเพิ่มเติมในส่วนของกฎหมายสารบัญญัติในเรื่องความรับผิดร่วม บทลงโทษและมาตรการในส่วนของกฎหมายสารบัญญัติที่มีเงื่อนไขและการป้องกัน การเร่งเข้าสงวนข้อมูลคอมพิวเตอร์ (Expedited preservation of stored computer data) การเร่งเข้าสงวนและเปิดเผยข้อมูลการจราจรอิเล็กทรอนิกส์ (Expedited preservation and partial disclosure of traffic data) คำสั่งผลิต (Production order) การสืบค้นและยึดข้อมูลคอมพิวเตอร์ (Search and seizure of stored computer data) การเก็บข้อมูลจราจรอิเล็กทรอนิกส์แบบ Real-time (Real time collection of traffic data) รวมไปถึงหลักทั่วไปในเรื่องความร่วมมือระหว่างประเทศ การส่งผู้ร้ายข้ามแดน และการให้ความช่วยเหลือซึ่งกันและกันในด้านการเข้าถึงข้อมูล เก็บข้อมูล และการตรวจจับข้อมูลข้ามเขตแดน และมีการจัดตั้ง Indonesia-Security Incident Response Team on Internet Infrastructure: ID SIRTII อย่างไรก็ดี ในปัจจุบัน ประเทศอินโดนีเซียสามารถให้ความร่วมมือในระดับระหว่างประเทศในรูปแบบของการทำสัญญาทวิภาคีเท่านั้น

ประเทศอินโดนีเซียได้บัญญัติความคุ้มครองข้อมูลและความเป็นส่วนตัวไว้อย่างกระชับในมาตรา 26 ของ Electronic Information and Transaction law[154] อย่างไรก็ดีในอนาคตเป็นที่คาดว่ามาตรา 26 นี้จะถูกแทนที่ด้วยข้อบังคับที่ละเอียดมากยิ่งขึ้น วิธีการของอินโดนีเซียนั้นไม่มีพื้นฐานบนต้นแบบจากกฎหมายระหว่างประเทศใด ๆ แม้ว่าในอนาคตจะมีแนวโน้มว่ากฎหมายเหล่านี้จะได้รับอิทธิพลจาก Guidelines on the protection of privacy and transborder flows of personal data ของ OECD หรือ APEC privacy framework ซึ่งประเทศอินโดนีเซียได้เป็นสมาชิกของ APEC data privacy subgroup อยู่ก็ตาม

สำหรับ Regulation of the government of the republic of Indonesia Number 82 of 2012; Concerning electronic system and transaction operation ได้ให้ความคุ้มครองข้อมูลส่วนบุคคลไว้อย่างละเอียด โดยให้ผู้ให้บริการระบบอิเล็กทรอนิกส์ต้องรับรองความคุ้มครองข้อมูลส่วนบุคคลใด ๆ ที่มี

---

[153] Noor, M., *Cyber Legislation of Indonesia*, Paper presented at the Octopus Interface Conference-Cooperation against Cybercrime (2010), Retrieved 2013, July 11, from http://unpan1.un.org/intradoc/groups/public/documents/ UNGC/UNPAN040467.pdf

[154] Electronic Information and Transaction law 2008, Article 26 (1) Unless provided otherwise by Laws and Regulations, use of any information through electronic media that involves personal data of a person must be made with the consent of the person concerned.

อยู่ในครอบครอง โดยได้ให้ความหมายของการคุ้มครองไว้อย่างกว้าง ๆ ซึ่งครอบคลุมถึงการได้รับการยินยอมและรับรองว่าข้อมูลจะถูกใช้เพื่อจุดประสงค์ในการสื่อสารกับเป้าหมายของข้อมูลนั้นเท่านั้น[155] โดยข้อบังคับใหม่ได้รวมเอาเงื่อนไขที่ผู้ให้บริการจะต้องแจ้งเป็นลายลักษณ์อักษรให้ผู้ส่งข้อมูลนั้นทราบเมื่อพบว่ามีการเปิดเผยข้อมูลหรือประมวลผลข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต โดยข้อมูลส่วนบุคคลไม่จำกัดอยู่เพียงข้อมูลที่เปิดเผยตัวตนของบุคคลโดยตัวมันเอง แต่มีความหมายอย่างกว้าง ๆ ให้รวมถึงว่าเป็นข้อมูลใด ๆ ของบุคคลที่ถูกเก็บหรือปกป้องไว้ในฐานะข้อมูลลับด้วย[156]

ด้วยความที่ประเทศอินโดนีเซียประชากรส่วนใหญ่นับถือศาสนาอิสลาม ดังนั้น กฎหมายควบคุมเนื้อหาบนอินเตอร์เน็ทของอินโดนีเซียจึงค่อนข้างเข้มงวดตามหลักศาสนาอิสลาม โดยบัญญัติไว้ในมาตรา 27 และมาตรา 28 ของ Electronic Information and Transaction law 2008 ที่ห้ามการทำออกเผยแพร่หรือแจกจ่ายซึ่งเนื้อหาในหมวดหมู่ที่จัดว่า “ผิดศีลธรรม (Immoral)” และเนื้อหาที่ส่งเสริมการพนัน[157] อย่างไรก็ดี เนื้อหาข้อบังคับที่จำเป็นในการนำเอาเงื่อนไขดังกล่าวไป

---

[155] Regulation of the government of the republic of Indonesia Number 82 of 2012, Concerning Electronic System and Transaction Operation Article 15 (1) Electronic System Operator shall:

a. keep on secrecy, integrity, and availability of Personal Data are managed;

b. ensure that the acquisition, use, and utilization of Personal Data based on approval from the owner of Personal Data, unless otherwise provided by regulations: and

c. ensure the use or disclosure of the data based on approval from owner of such Personal Data, and in accordance with the purpose of being delivered to the owner of Personal Data on the data acquisition.

[156] Ibid., Article 15 (2) If there is a failure in the protection of confidential Personal Data that are managed, Electronic System Operator shall notify in writing to the owner of those Personal Data. Ibid

[157] Electronic Information and Transaction law 2008, Article 27

(1) Any Person who knowingly and without authority distributes and/or transmits and/or causes to be accessible Electronic Information and/or Electronic Records with contents against propriety.

(2) Any Person who knowingly and without authority distributes and/or transmits and/or causes to be accessible Electronic Information and/or Electronic Records with contents of gambling.

(3) Any Person who knowingly and without authority distributes and/or transmits and/or causes to be accessible Electronic Information and/or Electronic Records with contents of affronts and/or defamation.

(4) Any Person who knowingly and without authority distributes and/or transmits and/or causes to be accessible Electronic Information and/or Electronic Records with contents of extortion and/or threats.

Article 28. (1) Any Person who knowingly and without authority disseminates false and misleading information resulting in consumer loss in Electronic Transactions.

(2) Any Person who knowingly and without authority disseminates information aimed at inflicting hatred or dissension on individuals and/or certain groups of community based on ethnic groups, religions, races, and intergroups (SARA).

ปฏิบัติยังไม่มีอย่างชัดแจ้ง ด้วยเหตุนี้จึงยังไม่มีการนำไปใช้กลั่นกรองอย่างจริงจังนัก อีกทั้งยังมีความพยายามนำเอากฎหมาย The Pornography Law No. 44/2008 (Undang-undang No. 44/2008 ttg Pornografi) มาใช้ในการออกข้อบังคับในเนื้อหาออนไลน์ด้วย[158]

ตารางที่ 4.4 กฎหมายที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ของประเทศอินโดนีเซีย

ประเภท	กฎหมาย
Privacy	อยู่ในระหว่างการร่างกฎหมาย
Cyber crime	มี (Regulation of the government of the republic of Indonesia Number 82 of 2012 Concerning Electronic System and Transaction Operation)
Spam	มี
Online Content filtering	มี (The Pornography Law No. 44/2008, Electronic Information and Transaction law 2008)
Copyright (Digital)	มี

4.4.4 ประเทศฟิลิปปินส์

ประเทศฟิลิปปินส์ได้ออกกฎหมาย Cybercrime Prevention Act 2012 โดยมีวัตถุประสงค์เพื่อเพิ่มการคุ้มครองสิทธิส่วนบุคคลและยับยั้งการหลอกลวงและการขโมยเอกลักษณ์ของบุคคลบนอินเตอร์เน็ต[159] แต่ได้รับการวิพากษ์วิจารณ์เป็นอย่างมากว่าเป็นการละเมิดต่อหลักเสรีภาพในการแสดงออก และจากการที่ได้กำหนดคำนิยามของการหมิ่นประมาทและบทลงโทษที่รุนแรง ต่อมาหลังจากที่กฎหมายฉบับนี้ได้ผ่านการพิจารณาก็เกิดการต่อต้านจากภาคประชาชนอย่างมากจนในที่สุดศาลสูงสุดประเทศฟิลิปปินส์ได้ออกคำสั่งยับยั้งชั่วคราว (Temporary Restraining Order: TRO)[160] ต่อการบังคับใช้กฎหมายหลังจากที่กลุ่มทนายความและองค์กรสื่อยื่นคำฟ้อง 15 ฉบับเพื่อ

[158] Nugraha, Y., *Social Media Ecosystem in Indonesia*, ITU-ASEAN Forum on Promoting Effective and Secure Social Media 18-19 July 2012, Kuala Lumpur, Malaysia., (July 2012), Retrieved 2013, December 4, from http://www.itu.int/ITU-D/asp/CMS/Events/2012/socialmedia/S6.3_Indonesia.pdf

[159] South East Asia Cyberwatch, *Citizen Lab*, (June 2012), Retrieved 2014, March 7, from https://citizenlab.org/2012/06/southeast-asia-cyber-watch-june-2012-2/#ph

[160] Pedrasa, I., SC issues 120-day TRO vs cybercrime law, *ABS CBN News*, (9 September 2012), Retrieved 2014, February 3, from http://www.abs-cbnnews.com/nation/10/09/12/sc-issues-tro-vs-cybercrime-law-source/

ชี้ให้เห็นว่าตัวกฎหมายทั้งหมดหรือบางส่วนนั้นขัดต่อรัฐธรรมนูญ ในช่วงต้นเดือนธันวาคม พ.ศ. 2555 รัฐบาลได้ร้องขอให้ศาลยกคำสั่งยับยั้งชั่วคราวโดยอ้างว่าตัวกฎหมายมีความชอบธรรมและปฏิเสธข้อกล่าวหาที่ว่าตัวกฎหมายฉบับนี้พยายามที่จะควบคุมหรือลงโทษต่อเสรีภาพในการพูด[161] อย่างไรก็ดีในเดือนเมษายน พ.ศ. 2556 กระทรวงยุติธรรมประเทศฟิลิปปินส์ได้แถลงการณ์ยกเลิกหลายมาตราที่ได้รับการคัดค้านจากประชาชนในเรื่องการหมิ่นประมาท อย่างเช่น การกด Like บน Facebook หรือ Retweet บน twitter รวมไปถึงเนื้อหาเกี่ยวกับสื่อลามกเด็กซึ่งให้ความเห็นว่าได้มีการบัญญัติบทลงโทษไว้ในกฎหมายอื่นแล้ว และตัวกฎหมายฉบับที่ได้รับการแก้ไขจะถูกนำขึ้นพิจารณาในการประชุมสภาประเทศฟิลิปปินส์ครั้งที่ 16[162] ซึ่งกฎหมายเดิมที่ให้ครอบคลุม

[161] Phneah, E., Philippine govt asks court to lift injunction on Cybercrime Law, *ZDNET*, (11 December 2012), Retrieved 2014, April 27, from http://www.zdnet.com/ph/philippine-govt-asks-court-to-lift-injunction-on-cyber crime-law-7000008597/

[162] Acosta, R., DOJ deletes libel from new anti-cybercrime, *Businessmirror*, Retrieved 2014, April 27, from http://www.businessmirror.com.ph/index.php/en/news/nation/13927-doj-deletes-libel-from-new-anti-cybercrime-bill

อาชญากรรมทางคอมพิวเตอร์บางส่วนอยู่ใน Electronic Commerce Act 2000[163] ที่ระบุถึงการเข้าถึงข้อมูลโดยชอบด้วยกฎหมาย และการเปิดเผยรหัสเพื่อเข้าถึงข้อมูล และความผิดพื้นฐานอย่างการเจาะระบบ ทำลายระบบ และการเข้าถึงโดยไม่ได้รับอนุญาตโดยใช้คอมพิวเตอร์เพื่อทำให้เสียเปลี่ยนแปลง ขโมย หรือทำลาย ข้อมูลอิเล็กทรอนิกส์และการละเมิดทรัพย์สินทางปัญญาบนอินเตอร์เน็ต เป็นต้น

ประเทศฟิลิปปินส์มีกฎหมายเฉพาะในเรื่องการคุ้มครองข้อมูลและความเป็นส่วนตัว คือ Data Privacy Act 2012[164] ซึ่งนับเป็นหนึ่งในกฎหมายคุ้มครองความเป็นส่วนตัวที่ทันสมัยที่สุดในภูมิภาค โดยได้รวมเอาแนวทางจากสหภาพยุโรป APEC และ OECD เข้าไว้ด้วยกัน จุดเด่นของกฎหมายฉบับนี้อยู่ที่การกำหนดความผิดอาญาขึ้นมาเป็นจำนวนมาก โดยบทบัญญัติเกี่ยวกับสิทธิส่วนบุคคลและส่วนมากมีพื้นฐานจากกฎหมายละเมิดและการไกล่เกลี่ยข้อพิพาทมากกว่ากฎหมายอาญา

---

[163] Republic Act No. 8792 of Philippines Electronic Commerce Act of 2000 SEC. 31 Lawful Access. - Access to an electronic file, or an electronic signature of an electronic data message or electronic document shall only be authorized and enforced in favor of the individual or entity having a legal right to the possession or the use of the plaintext, electronic signature or file and solely for the authorized purposes. The electronic key for identity or integrity shall not be made available to any person or party without the consent of the individual or entity in lawful possession of that electronic key.

SEC. 32 Obligation of Confidentiality. - Except for the purposes authorized under this Act, any person who obtained access to any electronic key, electronic data message, or electronic document, book, register, correspondence, information, or other material pursuant to any powers conferred under this Act, shall not convey to or share the same with any other person.

SEC. 33 Penalties. - The following Acts shall be penalized by fine and/or imprisonment, as follows:

(a) Hacking or cracking which refers to unauthorized access into or interference in a computer system/server or information and communication system; or any access in order to corrupt, alter, steal, or destroy using a computer or other similar information and communication devices, without the knowledge and consent of the owner of the computer or information and communications system, including the introduction of computer viruses and the like, resulting in the corruption, destruction, alteration, theft or loss of electronic data messages or electronic document shall be punished by a minimum fine of one hundred thousand pesos (P100,000.00) and a maximum commensurate to the damage incurred and a mandatory imprisonment of six (6) months to three (3) years;

(b) Piracy or the unauthorized copying, reproduction, dissemination, distribution, importation, use, removal, alteration, substitution, modification, storage, uploading, downloading, communication, making available to the public, or broadcasting of protected material, electronic signature or copyrighted works including legally protected sound recordings or phonograms or information material on protected works, through the use of telecommunication.

[164] Republic Act No. 10173.

ตารางที่ 4.5 กฎหมายที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ของประเทศฟิลิปปินส์

ประเภท	กฎหมาย
Privacy	มี (Data Privacy Act 2012)
Cyber crime	มี (Cybercrime Prevention Act2012)
Spam	มี
Online Content filtering	มี
Copyright (Digital)	มี

4.4.5 ประเทศบรูไน

กฎหมายอาชญากรรมคอมพิวเตอร์ของประเทศบรูไนคือ Computer Misuse Order 2000 (แก้ไขเพิ่มเติมปี ค.ศ. 2007) ได้รับอิทธิพลอย่างมากจากกฎหมายอาชญากรรมคอมพิวเตอร์ของสิงคโปร์ ซึ่งมีต้นแบบจาก Computer Misuse Act 1993 ของสหราชอาณาจักร โดยตัวกฎหมายได้ครอบคลุมกฎหมายวิธีสบัญญัติทั้งตัวบทและนำเอากฎหมายอาญาดั้งเดิมที่มีพื้นฐานบนระบบกฎหมายที่ถือเอาคำพิพากษาเป็นบรรทัดฐาน (Case law) มาปรับใช้ร่วมด้วย โดยกฎหมายอาชญากรรมทางคอมพิวเตอร์ของประเทศบรูไน มุ่งเน้นไปที่การดำเนินคดีความผิดประเภทบุกรุก เช่น การเข้าถึง หรือแก้ไขข้อมูลของผู้อื่นและการเปิดเผยรหัสผ่านโดยไม่ได้รับอนุญาต การขัดขวางรบกวนการใช้งานระบบคอมพิวเตอร์[165] ในส่วนของกฎหมายวิธีพิจารณาความอาญานั้นจะมีการแก้ไขต่อไปในอนาคตในเรื่องของอำนาจในการสืบสวนสอบสวนคดีความทางอาชญากรรมคอมพิวเตอร์ กฎหมายอาชญากรรมทางคอมพิวเตอร์ของบรูไนสอดคล้องกับอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์อย่างกว้าง ๆ แม้ว่าบรูไนเองจะไม่ได้เป็นภาคีในอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ปี ค.ศ. 2000 นอกจากนี้ในส่วนของการจัดการปัญหาในเรื่องของ

[165] กำหนดไว้ในมาตรา 3-7 และมาตรา 10 ของ Computer Misuse Order 2000

Part II OFFENCES

Article 3 Unauthorised access to computer material.

Article 4 Access with intent to commit or facilitate commission of offence

Article 5 Unauthorised modification of computer material

Article 6 Unauthorised use or interception of computer service.

Article 7 Unauthorised obstruction of use of computer.

Article 8 Unauthorised disclosure of access code.

Article 10 Abetments and attempts punishable as offences.

อุปกรณ์ที่ใช้ในการกระทำผิดตามที่ระบุไว้ในมาตรา 6(1)(i) ของอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์นี้ประเทศบรูไนไม่ได้นำมาปรับใช้ หากแต่ได้มีการนำเอาหลักเกณฑ์ตามที่กำหนดไว้ในมาตรา 6(1)(ii) ของอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์นี้มาบัญญัติไว้ในส่วนของการเปิดเผยข้อมูลรหัสผ่านโดยมิชอบด้วย[166]

สำหรับส่วนของการคุ้มครองความเป็นส่วนตัวและข้อมูลนั้น นโยบายคุ้มครองข้อมูลของชาติ (National data protection policy) กำลังอยู่ในระหว่างการยกร่างและคาดหวังว่าจะกลายเป็นพื้นฐานของกฎหมายว่าด้วยการคุ้มครองข้อมูลและความเป็นส่วนตัวในอนาคต โดยใช้การศึกษาจากต้นแบบของประเทศสิงคโปร์และประเทศมาเลย์เซียเป็นหลัก

การควบคุมเนื้อหาบนอินเตอร์เน็ตนั้น ประเทศบรูไนใช้การออกสัญญาอนุญาตแบบ ให้แก่ผู้ให้บริการในทุกระดับและ Internet code of practice โดยมีข้อกำหนดของประเทศสิงคโปร์เป็นต้นแบบ Internet Code of Practice มีผลบังคับใช้ในปี พ.ศ. 2548 ซึ่งบังคับให้ผู้ให้บริการอินเตอร์เน็ต (Internet Service Providers: ISPs) และผู้ให้บริการเนื้อหาบนอินเตอร์เน็ต (Internet Content Providers: ICPs) ต้องได้รับสัญญาอนุญาตผ่าน Broadcasting Notification 2001 เพื่อรับรองว่าจะไม่มีเนื้อหาที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีบนการให้บริการอย่างเด็ดขาด โดย ผู้ให้บริการเชื่อมต่ออินเตอร์เน็ต (Internet Access Service Providers: IASP) และ ICPs จะได้รับอนุญาตผ่าน Broadcasting notification โดยอัตโนมัติ โดยเงื่อนไขในการเผยแพร่เนื้อหาสู่อินเตอร์เน็ต คือ หาก ISP หรือ ICP ได้รับการแจ้งให้ทราบโดยเจ้าหน้าที่ผู้มีอำนาจดูแลการกระจายเสียงว่ามีเนื้อหาที่ขัดต่อ Internet code of practice หรือผิดต่อความสงบเรียบร้อยและศีลธรรมอันดีของประชาชน ผู้ให้บริการต้องนำเอาเนื้อหาดังกล่าวหรือปิดกั้นการเข้าถึงเนื้อหาดังกล่าว กฎหมายเซ็นเซอร์ฉบับอื่น ๆ เช่น the Censorship of Films and Public Entertainments Act 1963, the Undesirable Publications Act 1982, the Penal Code 1952 และ the Sedition Act 1983 ถูกนำมาใช้ในการเซ็นเซอร์เนื้อหาออนไลน์ด้วยเช่นกัน ประเทศบรูไนเป็นประเทศหนึ่งที่มีกฎหมายควบคุมเนื้อหาบนอินเตอร์เน็ตที่ ครอบคลุมเนื้อหาต้องห้ามมากกว่ากฎหมายประเทศอื่น ๆ ในอาเซียน อย่างไรก็ดีในทางปฏิบัตินั้นไม่เข้มงวดมากนัก นอกจากนี้ประเทศบรูไนมี BruCERT เพื่อประสานความร่วมมือระหว่างประเทศด้วย[167]

---

[166] Council of Europe, *Cybercrime legislation–Brunei country profile (2008)*, Retrieved 2013, December 19, from http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documentscountryprofiles/cyber_cp_Brunei_%202008_November.pdf.

[167] UNCTAD, *Review of e-commerce legislation harmonization in the Association of Southeast Asian Nations (ASEAN) [UNCTAD/DTL/STICT/2013/1*, 17-20.

ตารางที่ 4.6 กฎหมายที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ของประเทศบรูไน

ประเภท	กฎหมาย
Privacy	ไม่มี
Cyber crime	มี (Computer Misuse Order 2000 (แก้ไขเพิ่มเติมปี 2007)
Spam	มี
Online Content filtering	มี (the Censorship of Films and Public Entertainments Act 1963, the Undesirable Publications Act 1982, the Penal Code 1952 และ the Sedition Act 1983)
Copyright (Digital)	มี

4.4.6 ประเทศกัมพูชา

ประเทศกัมพูชายังไม่ได้ออกบัญญัติทางกฎหมายว่าด้วยอาชญากรรมทางคอมพิวเตอร์เข้าไปในกฎหมายภายในประเทศ แต่อย่างไรก็ตาม ในการประชุมเจ้าหน้าที่อาวุโสอาเซียนด้านอาชญากรรมข้ามชาติ ครั้งที่ 7 ซึ่งจัดขึ้น ณ กรุงเวียงจันทน์ ประเทศลาว ในช่วงวันที่ 25-28 มิถุนายน พ.ศ. 2551 ได้เผยให้เห็นว่ามีรายงานเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ในประเทศกัมพูชาเช่นกัน แม้ว่าจนถึงปัจจุบันยังไม่มีกฎหมายเฉพาะสำหรับรับมืออาชญากรรมทางคอมพิวเตอร์ และยังไม่เป็นที่แน่ชัดว่ากฎหมายอาญาและกฎหมายวิธีพิจารณาความอาญาที่มีอยู่ของประเทศกัมพูชานั้นจะสามารถรับมือกับอาชญากรรมคอมพิวเตอร์ตามแบบที่อนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ได้กำหนดไว้เพียงใด อย่างไรก็ดี ประเทศกัมพูชาได้มีการจัดตั้งหน่วยงานเพื่อทำหน้าที่ประสานงานระหว่างศูนย์ปฏิบัติการรับมืออาชญากรรมทางคอมพิวเตอร์ในภูมิภาคอาเซียนขึ้นแล้ว คือ Cambodia Computer Emergency Response team: camCERT โดยเป็นหน่วยงานที่ประกอบไปด้วยผู้เชี่ยวชาญและเจ้าหน้าที่ด้านการรักษาความปลอดภัยคอมพิวเตอร์ซึ่งขึ้นตรงกับ National Information Communications Technology Development Authority: NiDA ซึ่งเป็นหน่วยงานของรัฐที่รับผิดชอบในการวางแผนและพัฒนา รวมไปถึงส่งเสริมนโยบายทางเทคโนโลยีสารสนเทศของประเทศกัมพูชา นอกจากนั้น NiDA ยังทำหน้าที่บูรณาการนโยบายสารสนเทศเพื่อเพิ่มศักยภาพในการเติบโตของเศรษฐกิจ รวมไปถึงตรวจสอบและควบคุมดูแลการใช้นโยบายดังกล่าวทั่วราชอาณาจักรด้วย ปัจจุบันจากรายงานของ UNCTAD พบว่า ประเทศกัมพูชากำลังอยู่ในระหว่างการยกร่างกฎหมายว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ทั้งนี้เนื่องจากประเทศกัมพูชาไม่มีกฎหมายคุ้มครองข้อมูลหรือความเป็นส่วนตัว ซึ่งอาจบัญญัติเพิ่มเติมเข้ามาในภายหลัง

เป็นส่วนหนึ่งของกฎหมายธุรกรรมอิเล็กทรอนิกส์ (E-Transaction law) ที่มีอยู่แล้วได้ ประเทศกัมพูชามีข้อกำหนดด้านการควบคุมเนื้อหาบนอินเตอร์เน็ตในมาตรา 12 กฎหมายว่าด้วยสิ่งพิมพ์ของประเทศกัมพูชา (Cambodia law on the regime of the press)[168] ซึ่งห้ามการเผยแพร่ข้อมูลใด ๆ ที่กระทบต่อความมั่นคงและเสถียรภาพทางการเมือง แม้ไม่ได้เป็นกฎหมายที่ออกมาเพื่อควบคุมเนื้อหาออนไลน์โดยตรงแต่สามารถนำมาปรับใช้ได้โดยอนุโลม

ตารางที่ 4.7 กฎหมายที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ของประเทศกัมพูชา

ประเภท	กฎหมาย
Privacy	ไม่มี
Cyber crime	อยู่ในระหว่างการร่างกฎหมาย
Spam	ไม่มี
Online Content filtering	มี (E-Transaction law)
Copyright (Digital)	มี

4.4.7 ประเทศลาว

ประเทศลาวยังไม่มีกฎหมายว่าด้วยอาชญากรรมทางคอมพิวเตอร์ทั้งในกฎหมายวิธีสบัญญัติและวิธีสารบัญญัติ แต่อย่างไรก็ตาม ประเทศลาวก็มีกฎหมายการพาณิชย์อิเล็กทรอนิกส์ (E-commerce act) ซึ่งเปิดโอกาสให้มีการบัญญัติกฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์เข้าไปได้ หน่วยงานที่กำกับดูแลด้านอาชญากรรมทางคอมพิวเตอร์ของลาวได้แก่ National Authority of Post & Telecommunications: NAPT ซึ่งรับผิดชอบในด้านนโยบายและข้อบังคับการสื่อสารโทรคมนาคมและอินเตอร์เน็ตของประเทศ และยังมี National Authority of Science & Technology: NAST ซึ่งรับผิดชอบในการออกนโยบายและยุทธศาสตร์ด้านสารสนเทศภายในประเทศลาว และยัง

[168] Law on the Regime of the Press 1995, Article 12: The press shall not publish or reproduce any information that may cause harm to the National Security and Political Stability.

Employer, editor and journalists shall be penalized to pay fine from 5,000,000 Riels to 15,000,000 Riels, without yet taking into account of due punishment according to Criminal Law.

The Ministries of Information and of Interior shall have rights to confiscate immediately the offending issue of the press.

Moreover, the Ministry of Interior may also have rights to suspend the publication for a period which shall not exceed thirty (30) days and to forward all dossiers to the court.

ทำหน้าที่บูรณาการระบบ E-government เข้ากับระบบราชการอีกด้วย ปัจจุบันวิศวกรด้านสารสนเทศจำนวนหนึ่งได้เข้าร่วมโครงการฝึกสอนเพื่อเป็นหน่วยงาน Lao Computer Emergency Response Team: LaoCERT หน่วยงานแรกของประเทศสาธารณรัฐประชาชนลาวที่กำลังจะก่อตั้งขึ้นเพื่อรับมือกับอาชญากรรมทางคอมพิวเตอร์[169] โดยการฝึกสอนจะดำเนินการจนถึงวันที่ 11 ตุลาคม พ.ศ. 2556

ตารางที่ 4.8 กฎหมายที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ของประเทศลาว

ประเภท	กฎหมาย
Privacy	ไม่มี
Cyber crime	กำลังอยู่ในขั้นตอนการร่างกฎหมาย
Spam	ไม่มี
Online Content filtering	ไม่มี
Copyright (Digital)	กำลังอยู่ในขั้นตอนการร่างกฎหมาย

4.4.8 ประเทศเวียดนาม

ประเทศเวียดนามมีบางมาตราในกฎหมายอาญาและกฎหมายวิธีพิจารณาความทั่วไปที่สามารถนำมาปรับใช้โดยอนุโลมกับอาชญากรรมทางคอมพิวเตอร์ได้ในระดับหนึ่ง เช่น มาตรา 121 และมาตรา 122 ของกฎหมายอาญาเวียดนามในเรื่องที่ว่าด้วยการหมิ่นประมาท (Slander) และการ

[169] ASEAN Business Forum, *Laos officials train to fight cybercrime*, (2013, August 1), Retrieved 2013, December 10, from http://www.aseanbusinessforum.com/news/allDetail.php?sec=1&id=48763

ทำให้ผู้อื่นได้รับความอับอาย (Humiliating other persons)[170] ประเทศเวียดนามได้ออกพระราชกฤษฎีกาว่าด้วยการบริหารจัดการและการใช้บริการอินเตอร์เน็ต (Management and Use of Internet Services Decree 2001) ในปี พ.ศ. 2544 ซึ่งกำหนดความผิดเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ เช่น การใช้งานเครื่องมือในรูปซอฟท์แวร์ รหัสเชื่อมต่อ การเข้ารหัสข้อมูลหรือข้อมูลส่วนบุคคลเพื่อเชื่อมต่ออินเตอร์เน็ตอย่างผิดกฎหมาย การขโมยรหัสผ่าน รหัสเชื่อมต่อ หรือข้อมูลส่วนบุคคลขององค์กรและเผยแพร่ ใช้อินเตอร์เน็ตด้วยเจตนาเพื่อข่มเหงรังแก ข่มขู่ หรือทำให้ผู้อื่นเสื่อมเสียชื่อเสียง สร้างและกระจายไวรัสคอมพิวเตอร์ลงบนระบบอินเตอร์เน็ต[171]

กฎหมายสารสนเทศของประเทศเวียดนามมีการบังคับใช้ตั้งแต่ปี พ.ศ. 2549 และได้มีการบัญญัติกฎหมายเพิ่มเติมเกี่ยวกับอาชญากรทางคอมพิวเตอร์เข้ามาในปี พ.ศ. 2553 อย่างไรก็ดี กฎหมายอาชญากรรมทางคอมพิวเตอร์ในประเทศเวียดนามนั้นครอบคลุมความผิดในวงที่จำกัดและไม่กว้างขวางเท่ากับอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์[172]

---

[170] Penal Code, Article 121, Humiliating Other Persons. This Article imposes a penalty of a warning, non-custodial reform for up to two years or a prison term of between three months and two years for anyone who seriously infringes upon the dignity or honor of other persons. The following aggravating circumstances will increase the penalty to between one and three years' imprisonment: the crime was committed against more than one person or more than once; the offender abused his/her position and/or power; the offender is responsible for the victim's education, care or medical treatment; the offense is committed against persons who are performing their professional duties. In addition, the offender may also be banned from holding certain posts, practicing certain occupations or doing certain jobs for between one and five years.

Penal Code, Article 122, Slander. States that anyone who creates or spreads stories knowing them to be fabricated in order to infringe upon the honor or damage the legitimate rights and interests of other persons will be subject to warning, non-custodial reform for up to two years or a prison term of between three months and two years. The same sentence applies to anyone who makes up a story that other persons commit crimes and denounces them before the competent agencies. The following aggravating circumstances will increase the penalty to between one and seven years' imprisonment: the crime was committed in an organized manner; the offender abused their position or powers to commit the crime; the crime was committed against more than one person, against persons who are performing their official duties, against the offender's own grandfathers, grandmothers, fathers, mothers or persons who teach, nurture, look after, educate and/or medically treat them; the slander accused the victim or committing a very serious or particularly serious crime. In addition, the offender may be subject to a fine of between VND 1,000,000 and VND 10,000,000, a ban from holding certain posts, practicing certain occupations or doing certain jobs for between one and five years.

[171] Decree No. 55/2001/ND-CP of August 23, 2001 on the management, provision and use of internet services.

[172] UNCTAD, *Review of e-commerce legislation harmonization in the Association of Southeast Asian Nations (ASEAN) [UNCTAD/DTL/STICT/2013/1*, 43-45.

สำหรับกรอบโครงสร้างทางกฎหมาย (Legal framework) ของประเทศเวียดนามนั้นอยู่ภายใต้ความรับผิดชอบของกระทรวงวัฒนธรรมและข้อมูลข่าวสาร (Ministry of culture and information) ซึ่งมุ่งเน้นไปที่ความผิดประเภทเนื้อหาอย่างสื่อลามกอนาจาร การเผยแพร่ความความเชื่อ หรือความรุนแรง ในขณะที่กระทรวงความมั่นคง (Ministry of public security) ดูแลด้านเนื้อหาที่เกี่ยวข้องกับการเมือง โดยข้อมูลซึ่งถูกจัดเก็บ หรือรับส่งจากอินเตอร์เน็ตต้องเป็นไปตามข้อบังคับของกฎหมายสื่อสิ่งพิมพ์ และกฎหมายอื่น ๆ ที่เกี่ยวข้องของประเทศเวียดนาม องค์กรใด ๆ ทั้งภายในประเทศและต่างประเทศ ที่เกี่ยวข้องกับกิจกรรมทางอินเตอร์เน็ตในประเทศประเทศเวียดนามจะต้องมีความรับผิดทางกฎหมายต่อเนื้อหาที่ตนเองสร้าง เผยแพร่ หรือจัดเก็บเอาไว้ ในกรณีที่มีการใช้ทรัพยากรบนอินเตอร์เน็ตหรือจัดเก็บข้อมูลอันเป็นปฏิปักษ์ต่อรัฐ หรือสั่นคลอนความมั่นคง เศรษฐกิจ หรือ ความเป็นระเบียบเรียบร้อยของสังคม กระตุ้นการต่อต้านรัฐ เปิดเผยความลับของรัฐ ละเมิดต่อองค์กรหรือสิทธิส่วนบุคคลหรือกระทำทำการรบกวนเซิฟเวอร์ DNS ของรัฐ[173] นอกจากนี้ รัฐบาลของประเทศเวียดนามยังคงควบคุมการเชื่อมต่อทั้งโครงสร้างพื้นฐานของอินเตอร์เน็ตและเนื้อหาทั้งหมด โดยผู้ใช้งานอินเตอร์เน็ตในประเทศเวียดนามต้องเชื่อมต่ออินเตอร์เน็ตผ่าน ISPs ที่ได้รับอนุญาตเท่านั้น ห้ามเชื่อมต่อโดยตรงกับ ISPs ต่างประเทศโดยการโทรศัพท์ตรงไปยังเลขหมายต่างประเทศ[174] ปัจจุบันประเทศเวียดนามได้มีการตั้งสาขาของสำนักงานตำรวจสากลและจัดตั้ง VNCERT เพื่อประสานความร่วมมือระหว่างประเทศ

[173] Binlot, A., Vietnam Bloggers Face Government Crackdown, *TIME*, (30 December 2008), Retrieved 2014, March 19, from http://www.time.com/time/world/article/0.8599.1869130.00.html

[174] Paragraph 3.2(c), section II of circular 04.

โดยสรุปแล้วประเทศเวียดนามได้มีบทบัญญัติที่ครอบคลุมการคุ้มครองข้อมูลส่วนบุคคลอยู่บางส่วนในกฎหมายคุ้มครองสิทธิผู้บริโภค (The Law on Protection of Consumers' Rights 2010) ซึ่งกำหนดเงื่อนไขขององค์กรในการเก็บข้อมูลจากลูกค้าบนอินเตอร์เน็ต[175]

ตารางที่ 4.9 กฎหมายที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ของประเทศเวียดนาม

ประเภท	กฎหมาย
Privacy	ไม่มี
Cyber crime	มี (เพิ่มเติมเข้าไปใน Penal code)
Spam	ไม่มี
Online Content filtering	มี (เพิ่มเติมเข้าไปใน Penal code)
Copyright (Digital)	ไม่มี (ปรับใช้กฎหมายลิขสิทธิ์)

4.4.9 ประเทศพม่า

ประเทศพม่ามีข้อกฎหมายที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์อยู่ในกฎหมายสองฉบับด้วยกันได้แก่ Computer Science Development Law 1996 และกฎหมายการพาณิชย์อิเล็กทรอนิกส์ (E-transaction law 2004)[176] ภายใต้กระทรวงการสื่อสาร ไปรษณีย์และโทรเลข โดยในการดำเนินคดีผู้กระทำความผิดซึ่งใช้คอมพิวเตอร์และอินเตอร์เน็ตเป็นเครื่องมือในการก่ออาชญากรรม

---

[175] Law on Protection of Consumers' Right, Article 6 Protection of consumer information

1. Consumers' information shall be kept safe and confidential when they participate in transactions, use of goods or services, except where competent state agencies required the information.

2. Where the collection, use and transfer of consumer information, the organizations or individuals trading goods and/or services shall:

a) Notify clearly and openly the consumer of the purpose of the collection and use of consumer information before such activities being done;

b) Use information in conformity with the purpose informed to consumers, and with the consent by the consumers;

c) Ensure safety, accuracy, completeness during collection, use and transfer of consumer information.

d) Update or adjust by themselves or help consumers to update and adjust as the information is found to be incorrect.

[176] The state of peace and Development Council Law No. 5/2004 The 12th Waxing Day of Kason, 1366 M.E. 30th April 2004.

นั้นจะนำกฎหมายอาญาที่มีอยู่มาปรับใช้ประกอบกับ E-transaction law 2004 ซึ่งมีอัตราโทษจำคุกระหว่างเจ็ดถึงสิบห้าปีแก่ผู้เจาะระบบของรัฐบาลหรือเผยแพร่สื่อลามกอนาจารบนอินเตอร์เน็ต[177] และกำหนดความผิดประเภทบุกรุก รวมทั้งทำลายข้อมูลอิเล็กทรอนิกส์การดักจับหรือเชื่อมต่อการสื่อสาร การใช้ลายเซ็นอิเล็กทรอนิกส์โดยไม่ได้รับอนุญาตจากเจ้าของ รวมไปถึงการสร้างหรือแก้ไขหรือรบกวน ซึ่งทำให้ผู้อื่นเสียประโยชน์หรือทำให้บุคคลหรือองค์กรเสื่อมเสียชื่อเสียงไว้ในมาตรา 34 ของ E-transaction law 2004[178] รวมไปถึงการรับหรือส่งข้อมูลที่บ่อนทำลายความมั่นคงของรัฐ[179] นอกจากนี้ ประเทศพม่ายังกำหนดให้การนำเข้าหรือครอบครองคอมพิวเตอร์และการเชื่อมต่อเข้ากับระบบเครือข่ายโดยไม่ผ่านการรับรองจากรัฐมนตรีกระทรวงการสื่อสาร ไปรษณีย์และโทรเลขเป็นความผิดตามกฎหมาย Computer Science Development Law 1996 อีกด้วย[180] ปัจจุบันประเทศพม่ามีหน่วยงาน mmCERT ทำหน้าที่ในการประสานความร่วมมือระหว่างประเทศ

---

[177] Myanmar E-transaction law 2004, Article 33 Whoever commits any of the following acts by using electronic transactions technology shall, on conviction be punished with imprisonment for a term which may extend from a minimum of 7 years to a maximum of 15 years and may also be liable to a fine.

[178] Myanmar E-transaction law 2004, Article 34

(a) Hacking or the dishonest modification or destruction of electronic records.

(b) Intercepting a communication or giving access to a communication without the permission of the originator.

(c) Communicating with another person using the electronic signature of that person without their consent.

(d) Creating or modifying information or distributing this information such that it causes detriment to the interest or lowers the dignity of an organization or person.

[179] Computer Science Development Law 1996 Article 34 Obtaining or sending information that undermines state security, the prevalence of law and order and community peace and tranquility, national unity, state economy or national culture.

[180] Computer Science Development Law 1996, Article 31 Importing or possessing a computer without the approval of the Myanmar Computer Science Development Council, subject to some conditions.

Article 32 Setting up a network or access to a network without the approval of the Ministry of Communications, Posts and Telegraphs.

ตารางที่ 4.10 กฎหมายที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ของประเทศพม่า

ประเภท	กฎหมาย
Privacy	ไม่มี
Cyber crime	มี (Computer Science Development Law 1996, E-transaction law 2004)
Spam	ไม่มี
Online Content filtering	มี (Computer Science Development Law 1996, E-transaction law 2004)
Copyright (Digital)	กำลังอยู่ในขั้นตอนการร่างกฎหมาย

4.4.10 ประเทศไทย

ประเทศไทยได้ออกพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เพื่อใช้เป็นเครื่องมือในการจัดการกับปัญหาอาชญากรรมทางคอมพิวเตอร์ เนื่องจากอาชญากรรมทางคอมพิวเตอร์มีลักษณะพิเศษ จึงจำเป็นต้องมีกฎหมายใหม่ที่ไม่กระทบต่อโครงสร้างของประมวลกฎหมายอาญาเดิม เพื่อเข้ามาทำหน้าที่อุดช่องโหว่ทางกฎหมายของประมวลกฎหมายอาญาที่ไม่สามารถ นำตัวผู้กระทำความผิดมาลงโทษได้ นอกจากนี้ในการบังคับใช้กฎหมายอาชญากรรมทางคอมพิวเตอร์ จำเป็นต้องมีอำนาจพิเศษของเจ้าพนักงานบางประการ เช่น การถอดรหัสลับข้อมูล การเรียกข้อมูลจราจรทางคอมพิวเตอร์ ฯลฯ อีกทั้งการแก้ไขประมวลกฎหมายอาญานั้นใช้เวลานาน ประเทศไทยจึงออกกฎหมายในลักษณะพระราชบัญญัติแทนที่จะแก้ไขเข้าไปในกฎหมายที่มีอยู่เดิม โดยการจัดทำพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ขึ้นมาโดยได้นำเอามาตรฐานและข้อตกลงในเรื่องการรับมือกับอาชญากรรมทางคอมพิวเตอร์ของโลก เช่น อนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์(Convention on Cybercrime) ของสหภาพยุโรป นอกจากนี้ ยังได้พิจารณานำเอากฎหมายของหลาย ๆ ประเทศ อาทิ เยอรมนี อังกฤษ สิงคโปร์ สหรัฐอเมริกา อินเดีย ฯลฯ มาปรับใช้เป็นต้นแบบในการพิจารณากำหนดข้อบังคับต่าง ๆ อีกด้วย[181]

พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แบ่งออกเป็นสองหมวดหลัก ได้แก่ หมวดความผิดเกี่ยวกับคอมพิวเตอร์ ซึ่งเป็นส่วนของกฎหมายสารบัญญัติในการ

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

กำหนดฐานความผิดและบทลงโทษสำหรับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และหมวดพนักงานเจ้าหน้าที่ซึ่งเป็นส่วนของกฎหมายวิธีสบัญญัติในการกำหนดอำนาจหน้าที่ของพนักงานเจ้าหน้าที่เกี่ยวกับการดำเนินคดีอาญาตามฐานความผิดเกี่ยวกับคอมพิวเตอร์

เมื่อวันที่ 28 มีนาคม พ.ศ. 2554 กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ได้จัดให้มีประชุมรับฟังและให้ความคิดเห็นเกี่ยวกับการปรับปรุงแก้ไขพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และได้ทำการแจกร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฉบับใหม่ซึ่งได้แก้ไขเพิ่มเติมในส่วนของการให้คำนิยามผู้ดูแลระบบ เพิ่มความผิดเกี่ยวกับการคัดลอกไฟล์ การมีสื่อลามกอนาจารเด็กไว้ในครอบครอง การเผยแพร่สิ่งที่เป็นการดูหมิ่นบุคคลอื่นผ่านระบบคอมพิวเตอร์ มีโปรแกรมหรืออุปกรณ์เจาะระบบไว้ในครอบครอง และเพิ่มโทษผู้เจาะระบบ รวมไปถึงการจัดตั้งหน่วยงาน สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ. และให้ใช้ชื่อเป็นภาษาอังกฤษว่า Electronic Transactions Development Agency (Public Organization) หรือ ETDA ขึ้นมาเป็นองค์การมหาชนภายใต้การกำกับดูแลของกระทรวงไอซีที อีกทั้งยังจัดตั้งคณะกรรมการป้องกันและปราบปรามการกระทำความผิดทางคอมพิวเตอร์ขึ้นเพื่อเพิ่มประสิทธิภาพการดำเนินการสืบสวนสอบสวนและรับมืออาชญากรรมทางคอมพิวเตอร์[182]

นอกเหนือจากพระราชบัญญัติการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ปัจจุบันมีกฎหมายอีกหลายฉบับทั้งที่ตราขึ้นใช้บังคับแล้ว และที่อยู่ระหว่างดำเนินการทางนิติบัญญัติ ที่มีเนื้อหาเกี่ยวข้องกับการป้องกันหรือปราบปรามอาชญากรรมทางคอมพิวเตอร์ เช่น พระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544 มาตรา 74 ซึ่งกำหนดฐานความผิดเกี่ยวกับการดักรับไว้ หรือใช้ประโยชน์ หรือเปิดเผยข้อความข่าวสาร หรือข้อมูลอื่นใดที่มีการสื่อสารโทรคมนาคมโดยไม่ชอบด้วยกฎหมาย

สำหรับประมวลกฎหมายอาญา ลักษณะ 7 ว่าด้วยความผิดเกี่ยวกับการปลอมแปลง หมวด 4[183] ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ โดยเป็นการกำหนดฐานความผิดเกี่ยวกับการปลอมหรือแปลงบัตรอิเล็กทรอนิกส์ ตลอดจนกำหนดฐานความผิดเกี่ยวกับการใช้ การมีไว้เพื่อใช้ นำเข้า หรือ

---

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

[183] 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.

ส่งออก การจำหน่ายซึ่งบัตรอิเล็กทรอนิกส์ปลอมหรือแปลง และลงโทษบุคคลที่ทำการผลิต หรือมีเครื่องมือในการผลิตบัตรดังกล่าว

ทั้งนี้ มาตรา 59 ของประมวลกฎหมายวิธีพิจารณาความอาญา[184] ได้บัญญัติในส่วนที่เกี่ยวกับการส่งสำเนาหมายอาญาทางสื่ออิเล็กทรอนิกส์ โดยเป็นการแก้ไขเพิ่มเติมบทบัญญัติเกี่ยวกับการส่งสำเนาหมายอาญาผ่านทางสื่ออิเล็คทรอนิคส์และสื่อสารสนเทศอื่น ๆ

สำหรับมาตรการด้านความร่วมมือระหว่างหน่วยงานต่าง ๆ ที่เกี่ยวข้อง ทั้งภาครัฐและเอกชน ทั้งหน่วยงานที่มีหน้าที่ตามกฎหมาย รวมถึงหน่วยงานอื่น ๆ ที่อาจเกี่ยวข้องไม่ว่าจะเป็นในด้านของผู้พัฒนาระบบหรือผู้กำหนดนโยบายและหน่วยงานด้านความปลอดภัยของเครือข่ายเพื่อรับมือกับปัญหาฉุกเฉินด้านความปลอดภัยคอมพิวเตอร์ขึ้นโดยเฉพาะ และเป็นศูนย์กลางคอยให้ความช่วยเหลือในด้านต่าง ๆ รวมทั้งให้คำปรึกษาถึงวิธีการหรือแนวทางแก้ไข ซึ่งปัจจุบันศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ หรือเนคเทค ได้จัดตั้งศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย Thai Computer Emergency Response Team: ThaiCERT เพื่อเป็นหน่วยงานให้ความช่วยเหลือและให้ข้อมูลทางวิชาการเกี่ยวกับการ ตรวจสอบและการรักษาความปลอดภัยคอมพิวเตอร์แก่ผู้ที่สนใจทั้ง ภาครัฐและเอกชน รวมทั้งเป็นหน่วยงานรับแจ้งเหตุกรณีที่มีการละเมิดต่อความปลอดภัยทางคอมพิวเตอร์อีกด้วย

ในด้านการคุ้มครองข้อมูลส่วนบุคคล ประเทศไทยกำลังยกร่างพระราชบัญญัติว่าด้วยคุ้มครองข้อมูลส่วนบุคคล ที่หากมีการเสนอร่างและผ่านการพิจารณาเรียบร้อยแล้วกฎหมายนี้จะ

---

[184] ประมวลกฎหมายวิธีพิจารณาความอาญา, มาตรา 59 บัญญัติว่า “ศาลจะออกคำสั่งหรือหมายจับ หมายค้น หรือหมายขัง ตามที่ศาลเห็นสมควรหรือโดยมีผู้ร้องขอก็ได้ในกรณีที่ผู้ร้องขอเป็นพนักงานฝ่ายปกครองหรือตำรวจต้องเป็นพนักงานฝ่ายปกครองตั้งแต่ระดับสามหรือตำรวจซึ่งมียศตั้งแต่ชั้นร้อยตำรวจตรีหรือเทียบเท่าขึ้นไป

ในกรณีจำเป็นเร่งด่วนซึ่งมีเหตุอันควรโดยผู้ร้องขอไม่อาจไปพบศาลได้ ผู้ร้องขออาจร้องขอต่อศาลทางโทรศัพท์ โทรสาร สื่ออิเล็กทรอนิกส์ หรือสื่อเทคโนโลยีสารสนเทศประเภทอื่นที่เหมาะสมเพื่อขอให้ศาลออกหมายจับหรือหมายค้นก็ได้ ในกรณีเช่นว่านี้เมื่อศาลสอบถามจนปรากฏว่ามีเหตุที่จะออกหมายจับหรือหมายค้นได้ตามมาตรา 59/1 และมีคำสั่งให้ออกหมายนั้นแล้ว ให้จัดส่งสำเนาหมายเช่นว่านี้ไปยังผู้ร้องขอโดยทางโทรสาร สื่ออิเล็กทรอนิกส์ หรือสื่อเทคโนโลยีสารสนเทศประเภทอื่น ทั้งนี้ ตามหลักเกณฑ์และวิธีการที่กำหนดในข้อบังคับของประธานศาลฎีกา

เมื่อได้มีการออกหมายตามวรรคสามแล้ว ให้ศาลดำเนินการให้ผู้ที่เกี่ยวข้องกับการขอหมายมาพบศาลเพื่อสาบานตัวโดยไม่ชักช้า โดยจดบันทึกถ้อยคำของบุคคลดังกล่าวและลงลายมือชื่อของศาลผู้ออกหมายไว้ หรือจะใช้เครื่องบันทึกเสียงก็ได้โดยจัดให้มีการถอดเสียงเป็นหนังสือและลงลายมือชื่อของศาลผู้ออกหมาย บันทึกที่มีการลงลายมือชื่อรับรองดังกล่าวแล้ว ให้เก็บไว้ในสาระบบของศาล หากความปรากฏต่อศาลในภายหลังว่าได้มีการออกหมายไปโดยฝ่าฝืนต่อบทบัญญัติแห่งกฎหมาย ศาลอาจมีคำสั่งให้เพิกถอนหรือแก้ไขเปลี่ยนแปลงหมายเช่นว่านั้นได้ ทั้งนี้ ศาลจะมีคำสั่งให้ผู้ร้องขอจัดการแก้ไขเพื่อเยียวยาความเสียหายที่เกิดขึ้นแก่บุคคลที่เกี่ยวข้องตามที่เห็นสมควรก็ได้”.

กลายเป็นหลักปฏิบัติในเรื่องการคุ้มครองข้อมูลส่วนบุคคลของทั้งภาครัฐและเอกชน ในปัจจุบัน แม้ว่าประเทศไทยจะยังไม่มีกฎหมายคุ้มครองข้อมูลหรือสิทธิส่วนบุคคลโดยตรง แต่ได้มีกำหนดไว้ในกฎหมายอื่น ๆ ซึ่งอาจนำมาปรับใช้แล้วแต่กรณี เช่น มาตรา 34 และมาตรา 35 แห่งกฎหมายรัฐธรรมนูญแห่งประเทศไทย พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 กฎหมายอาญา มาตรา 323-324 พระราชบัญญัติการประกอบธุรกิจข้อมูลบัตรเครดิต พ.ศ. 2545 เป็นต้น

ตารางที่ 4.11 กฎหมายที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ของประเทศไทย

ประเภท	กฎหมาย
Privacy	อยู่ในระหว่างการร่างกฎหมาย
Cyber crime	มี (พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550)
Spam	มี (พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550)
Online Content filtering	มี (พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550)
Copyright (Digital)	มี (ร่างพระราชบัญญัติลิขสิทธิ์ฉบับใหม่เพิ่มเติมในเรื่อง Digital Right Management)

ตารางที่ 4.12 สรุปสภาพกฎหมายอาชญากรรมทางคอมพิวเตอร์ของประเทศสมาชิกอาเซียน

ประเทศ	ลักษณะกฎหมายภายในประเทศ	ความร่วมมือระหว่างประเทศ	อื่น ๆ
มาเลเซีย	ครอบคลุมทั้งในส่วนของกฎหมายวิธีสบัญญัติและวิธีสารบัญญัติตามมาตรฐานของอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์	MyCERT	มาเลเซียประเทศที่มีกฎหมายอาชญากรรมทางคอมพิวเตอร์ก้าวหน้าเป็นอันดับต้นๆ ของอาเซียน
สิงคโปร์	กฎหมายสารบัญญัติ ไม่ว่าในด้านตัวบทกฎหมายหรือตามกฎหมายอาญาดั้งเดิมที่มีพื้นฐานบนระบบกฎหมายที่ใช้แนวทางการตัดสินของผู้พิพากษา (Case law) ในส่วนที่เกี่ยวข้องกับกฎหมายวิธีพิจารณาความอาญาได้ครอบคลุมไปถึงการค้นหาและยึดข้อมูลทางคอมพิวเตอร์เช่นเดียวกับการสั่งให้มีการจัดทำข้อมูล	ทำข้อตกลงทวิภาคี นำเอาหลักถ้อยทีถ้อยอาศัย (Reciprocity) มาปรับใช้ SingCERT, BP Digital Security Incident Response Team, National University of Singapore Computer Emergency Response Team	กฎหมายอาชญากรรมคอมพิวเตอร์ของประเทศสิงคโปร์นั้นได้รับอิทธิพลจากกฎหมาย Computer misuse act ของสหราชอาณาจักร และมีการปรับปรุงแก้ไขอยู่เสมอ (ล่าสุดปี 2007)
อินโดนีเซีย	Electronic Information and Transaction law ได้นำเอาคำแนะนำของสภายุโรปมาปรับใช้ครอบคลุมในกฎหมายสารบัญญัติ เช่นเดียวกับกฎหมายวิธีพิจารณาความอาญา	อินโดนีเซียสามารถให้ความช่วยเหลือระหว่างประเทศในรูปแบบของการทำสัญญาทวิภาคีเท่านั้น / ID-CERT	-
ฟิลิปปินส์	ได้ออกกฎหมาย Cybercrime Prevention Act 2012 เพื่อเพิ่มการคุ้มครองสิทธิส่วนบุคคลและยับยั้งการหลอกลวงและการขโมยเอกลักษณ์บุคคลบนอินเตอร์เน็ต	PhCERT	ศาลสูงสุดฟิลิปปินส์ได้ออกคำสั่งยับยั้งชั่วคราว (Temporary Restraining Order: TRO) แต่ขณะนี้ได้ประกาศใช้แล้วตั้งแต่เดือนกุมภาพันธ์ พ.ศ. 2557 โดยได้ปรับปรุงแก้ไขบางส่วน

ตารางที่ 4.12 (ต่อ)

ประเทศ	ลักษณะกฎหมายภายในประเทศ	ความร่วมมือระหว่างประเทศ	อื่น ๆ
บรูไน	ได้รับอิทธิพลอย่างมากจากกฎหมายอาชญากรรมคอมพิวเตอร์ของสิงคโปร์ ครอบคลุมกฎหมายวิธีสบัญญัติทั้งตัวบทและกฎหมายอาญาดั้งเดิมที่มีพื้นฐานบนระบบกฎหมายที่ใช้แนวทางการตัดสินของผู้พิพากษา	BruCERT	-
กัมพูชา	ยังไม่ได้บัญญัติกฎหมายอาชญากรรมทางคอมพิวเตอร์เข้าไปในกฎหมายภายในประเทศ แต่อยู่ในระหว่างร่างกฎหมาย	CamCERT	มาตรา 12 กฎหมายสิ่งพิมพ์กัมพูชา (Cambodia Law on the regime of the press) ซึ่งห้ามการเผยแพร่ข้อมูลใด ๆ ที่กระทบต่อความมั่นคงและเสถียรภาพทางการเมือง มักถูกนำมาปรับใช้กับการควบคุมเนื้อหาออนไลน์
ลาว	ยังไม่มีกฎหมายอาชญากรรมคอมพิวเตอร์ทั้งในกฎหมายวิธีสบัญญัติและวิธีสารบัญญัติ แต่อยู่ในระหว่างร่างกฎหมาย	LaoCERT	-
เวียดนาม	กฎหมายบางมาตราในกฎหมายอาญาและกฎหมายวิธีพิจารณาความทั่วไปที่สามารถนำมาปรับใช้กับอาชญากรรมทางคอมพิวเตอร์ได้ในระดับหนึ่ง และได้มีการบัญญัติกฎหมายเพิ่มเติมเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์เข้ามาในปี พ.ศ. 2553	VNCERT/ Bach Khoa Internetwork Security Center	-

ตารางที่ 4.12 (ต่อ)

ประเทศ	ลักษณะกฎหมายภายในประเทศ	ความร่วมมือระหว่างประเทศ	อื่น ๆ
พม่า	นำเอากฎหมายอาญาที่มีอยู่มาปรับใช้ประกอบกับกฎหมายการพาณิชย์อิเล็กทรอนิกส์ (E-transaction law 2004) กำหนดโทษจำคุกระหว่างเจ็ดถึงสิบห้าปีแก่ผู้เจาะระบบของรัฐบาลหรือเผยแพร่สื่อลามกอนาจารบนอินเตอร์เน็ต	mmCERT	-
ไทย	พระราชบัญญัติการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544 ประมวลกฎหมายอาญา ประมวลกฎหมายวิธีพิจารณาความอาญา	ThaiCERT	ร่างพระราชบัญญัติการกระทำผิดเกี่ยวกับคอมพิวเตอร์เพิ่มความผิดเกี่ยวกับ child pornography และการครอบครองโปรแกรมเพื่อการเจาะระบบ รวมไปถึงเพิ่มนิยามของสแปมให้ครอบคลุมมากขึ้น

บทที่ 5

วิเคราะห์สภาพปัญหาในปัจจุบัน และมาตรการทางกฎหมายในการควบคุมอาชญากรรมทางคอมพิวเตอร์ในอาเซียน

ประเทศสมาชิกอาเซียนได้มีพัฒนาบทบัญญัติทางกฎหมายของตนให้สอดคล้องกับหลักเกณฑ์สากลในเรื่องการติดต่อสื่อสารผ่านระบบเครือข่ายอินเตอร์เน็ตเพิ่มมากขึ้น เพื่อสลายกำแพงที่ปิดกั้นระหว่างบริการออนไลน์และความมั่นคงในการทำธุรกรรมผ่านระบบเครือข่ายอินเตอร์เน็ต และเพื่อสร้างความปลอดภัยให้แก่สังคมโดยทั่วไป ทั้งนี้การนำเอากฎหมายไซเบอร์มาปรับใช้นับเป็นขั้นตอนที่สำคัญเพื่อเปิดโอกาสให้มีการพัฒนาทางด้านเศรษฐกิจในทุกภาคส่วนของสังคมทั้งในระดับภูมิภาคและระดับโลก เพื่อแก้ไขปัญหาต่าง ๆ ที่เกิดขึ้น เช่น ความปลอดภัย ความเป็นส่วนตัว กฎหมายคุ้มครองผู้บริโภค สิทธิในทรัพย์สินทางปัญญา และจำเป็นต้องได้รับความเอาใจใส่ในสังคมที่นำเอาระบบคอมพิวเตอร์เข้ามาบูรณาการในทุกภาคส่วน

จากการบัญญัติกฎหมายที่เกี่ยวข้องกับการกำกับดูแลทางอินเตอร์เน็ตทำให้เกิดความตื่นตัวของประเทศต่าง ๆ ในการพัฒนาระบบสารสนเทศของตนด้วย เพื่อตอบสนองต่อการลงทุนจากต่างชาติ และจากผลสำรวจของการประชุมสหประชาชาติว่าด้วยการค้าและการพัฒนา (United Nations Conferences on Trade and Development: UNCTAD) พบว่า กว่า 93% ของ 32 ประเทศที่ได้ทำการสำรวจได้มีการเตรียมตัวหรืออยู่ในกระบวนการปรับใช้เทคโนโลยีสารสนเทศเพื่อให้ได้ประโยชน์สูงสุดจากตลาด ICT และการเติบโตทางเศรษฐกิจ รวมถึงโอกาสในการพัฒนาประเทศซึ่งมาพร้อมกัน โดยประเทศในกลุ่มที่ทำการสำรวจส่วนใหญ่เลือกที่จะใช้ กฎหมายแม่แบบของคณะกรรมาธิการองค์การสหประชาชาติว่าด้วยกฎหมายการค้าระหว่างประเทศ (UNCITRAL Model Law on International Commercial Arbitration) มาพิจารณา[185] แสดงให้เห็นถึงความสำคัญของการปรับปรุงกฎเกณฑ์ให้สอดคล้องกันในระดับนานาชาติ (International harmonization) ในมุมมองของความต้องการในการสร้างความเป็นหนึ่งเดียวของการปรับใช้กฎหมายในสังคมข้อมูลข่าวสารของโลกและพัฒนาการของการประสานกันของความสัมพันธ์ทางเศรษฐกิจระหว่างประเทศในระดับภูมิภาคและระดับโลก

---

[185] UNCTAD, *Information Economy Report 2007-2008*, (Geneva: United Nations. 2007).

ประเทศกำลังพัฒนาในภูมิภาคต่าง ๆ ได้เล็งเห็นถึงความสำคัญในการสร้างความสอดคล้องของแนวทางในการดำเนินการตามกรอบของกฎหมาย เพื่อสร้างอำนาจการแข่งขันในภูมิภาคของตนเองที่เกี่ยวกับตลาดสารสนเทศและเพิ่มศักยภาพของตนในการเติบโตทางเศรษฐกิจ โครงการริเริ่มในระดับภูมิภาคของการปรับปรุงกฎหมายว่าด้วยอาชญากรรมทางคอมพิวเตอร์ให้มีความสอดคล้องกันกำลังพัฒนาไปข้างหน้าและต้องเผชิญกับอุปสรรคซึ่งประกอบไปด้วย ความแตกต่างทางระบบกฎหมาย สภาพสังคมและเศรษฐกิจของแต่ละประเทศในภูมิภาค ปัจจัยอื่น ๆ ที่อาจเป็นอุปสรรคซึ่งได้แก่ การขาดแคลนทรัพยากรบุคคล สาธารณะชนขาดความเข้าใจในขอบข่ายและประโยชน์ที่ได้รับจากกฎหมาย ความปลอดภัยบนอินเตอร์เน็ตทั้งในด้านความเป็นส่วนตัวและการทำธุรกรรม หรือจะกล่าวให้กว้างกว่านั้นก็คือ ผู้บริโภคไม่ไว้วางใจในความปลอดภัยของการทำธุรกรรมอิเล็กทรอนิกส์ และการคุ้มครองข้อมูลส่วนบุคคลบนอินเตอร์เน็ต อีกทั้งยังมีปัญหาในด้านการวางระบบโครงสร้างพื้นฐานทางเทคนิค และการปฏิรูปกฎหมายในระดับชาติ

ดังนั้น เพื่อที่จะสร้างความสอดคล้องกันของกฎหมายระหว่างประเทศในด้านอาชญากรรมทางคอมพิวเตอร์ซึ่งเป็นส่วนหนึ่งในยุทธศาสตร์ของอาเซียนในด้านกฎหมายเทคโนโลยีสารสนเทศจึงสามารถกระทำได้ตามวิธีการดังนี้ คือ

5.1 การสร้างคู่มือ (Guidelines) เพื่อนำมาใช้ในระดับภูมิภาค

อาเซียนเป็นองค์กรระดับภูมิภาค องค์กรแรกในกลุ่มประเทศกำลังพัฒนาที่นำเอากรอบโครงร่างทางกฎหมายที่สอดคล้องกันที่ข้ามเขตอำนาจศาล (Harmonized legal framework across jurisdiction) มาใช้โดยเริ่มจากกฎหมายการค้าอิเล็กทรอนิกส์ ผ่านโครงการต่าง ๆ ของอาเซียน ซึ่งช่วยให้ประเทศสมาชิกสามารถพัฒนาและบรรลุผลในการสร้างโครงสร้างพื้นฐานทางกฎหมายที่สอดคล้องกันขึ้นมาได้ โดยแนวทางปฏิบัติดังกล่าวสามารถนำมาปรับใช้กับการสร้างความสอดคล้องทางกฎหมายอื่น ๆ ระหว่างประเทศภายในภูมิภาคอาเซียนได้ โดยเฉพาะกฎหมายอาชญากรรมทางคอมพิวเตอร์ที่มีความเกี่ยวข้องโดยตรงกับพัฒนาการทางกฎหมายและพัฒนาทางด้านการตลาดสารสนเทศ

เมื่อเทคโนโลยี ICT ได้มีแพร่หลายเพิ่มมากขึ้นในภูมิภาคอาเซียน ประเทศสมาชิกอาเซียนให้การรับรองโครงการ e-ASEAN อย่างเป็นทางการในปี พ.ศ. 2542 ซึ่งเป็นผลมาจากโครงการ

ASEAN vision 2020[186] ที่ได้เริ่มดำเนินการไปแล้ว 2 ปีก่อนหน้านั้น และเพื่อทำให้เกิดอิสรภาพในการไหลเวียนของสินค้า บริการและการลงทุน สร้างระบบเศรษฐกิจที่เท่าเทียมกัน รวมทั้ง ลดช่องว่างทางสังคม เป้าหมายของโครงการ e-ASEAN คือ การบรรลุซึ่งเป้าหมายในทางยุทธศาสตร์สารสนเทศ และส่งเสริมการเจริญเติบโตทางเศรษฐกิจ และการแข่งขันเพื่อเพิ่มการบูรณาการระบบสารสนเทศของประเทศสมาชิกอาเซียนไปสู่สังคมเศรษฐกิจระดับโลก โดยโครงการ e-ASEAN ได้สร้างแผนปฏิบัติการที่มุ่งเน้นในด้านรูปธรรม กฎหมาย ตรรกะ สังคม และโครงสร้างพื้นฐานทางเศรษฐกิจ เพื่อรองรับพัฒนาการของเทคโนโลยีสารสนเทศในอนาคต

โดยในปี พ.ศ. 2543 ประเทศสมาชิกอาเซียนได้เข้าร่วมในข้อตกลงว่าด้วยกรอบโครงสร้าง e-ASEAN ซึ่งดำเนินการตามแผน e-ASEAN roadmap[187] โดยโครงการนี้ได้ช่วยสนับสนุนให้ ASEAN บรรลุถึง เป้าหมายหลักในแผน Roadmap สองประการได้แก่

1. ออกกฎหมายภายในประเทศเพื่อรองรับการทำธุรกรรมอิเล็กทรอนิกส์ (เช่น กฎหมายไซเบอร์) บนพื้นฐานของกรอบโครงสร้างอ้างอิง (กำหนดเส้นตาย 31 ธันวาคม พ.ศ. 2551) ตามมาตรการที่ 78 ของอาเซียน

2. ส่งเสริมธุรกรรมอิเล็กทรอนิกส์ข้ามแดนและการใช้งานลายเซ็นอิเล็กทรอนิกส์ (กำหนดเส้นตาย 31 ธันวาคม 2009) มาตรการที่ 79 ของอาเซียน[188]

โดยเป้าหมายและเส้นตายเหล่านี้ได้รับการรับรองจาก ที่ประชุมระดับรัฐมนตรีเศรษฐกิจอาเซียน ณ กรุงเซบู ประเทศฟิลิปปินส์ ในเดือนธันวาคม พ.ศ. 2549

สำหรับโครงการ e-ASEAN ได้จัดให้มีคณะทำงานขึ้น คือ ASEAN e-commerce and ICT Trade facilitating working group ซึ่งทำหน้าที่เป็น Coordinating body และรายงานการดำเนินการผ่าน ASEAN TELSOM (Telecommunications and ICT senior Officials meeting) ซึ่งจะทำการรายงานแก่ Ministers of Telecommunications and ICT ต่อไป โดยวาระของคณะทำงานดังกล่าวประกอบไปด้วยการสร้างโครงสร้างพื้นฐานทางสารสนเทศ e-government และ การสร้างประสิทธิภาพทางเทคโนโลยีสารสนเทศ เป็นต้น

---

[186] ASEAN Vision 2020 คือชื่อเดิมของแผนการจัดตั้งประชาคมอาเซียน 2015 (ASEAN Community 2015).

[187] ASEAN Secretariat, *Roadmap for Integration of e-ASEAN Sector*, (2004, November 29), Retrieved 2013, September 7, from http://aseansec.org/16689.htm

[188] e-ASEAN Roadmap, Measure 78: Enact domestic legislation to provide legal recognition of electronic transactions (i.e. cyber laws) based on common reference frameworks (deadline: 31 December 2008).

Measure 79: Facilitate cross-border electronic transactions and the use of digital signatures (deadline: 31 December 2009).

โดยแผน e-ASEAN roadmap มีอยู่ 3 ขั้นตอน (phases) ด้วยกัน ได้แก่

ขั้นตอนที่ 1 การสร้างความสอดคล้องของกรอบแนวทางในการดำเนินการทางกฎหมาย ประกอบไปด้วย การจัดทำโครงสร้างทางกฎหมายระดับสูง ข้อบังคับ และสถาบัน อย่างกว้าง ๆ

ขั้นตอนที่ 2 การทดสอบศักยภาพที่สามารถจะพัฒนาได้ ซึ่งการจัดทำโครงสร้างตามขั้นตอนที่ 1 รวมไปถึงวิธีการระงับข้อพิพาทออนไลน์ (Online Dispute Resolution: ODR) และ

ขั้นตอนที่ 3 เป็นการทดสอบความเป็นไปได้ในการจัดตั้งโครงสร้างตามข้อ 1 เพื่อความเข้าใจร่วมกันในเรื่องของลายเซ็นอิเล็กทรอนิกส์เพื่อส่งเสริมการค้าข้ามแดน

โดยในแต่ละขั้นตอนของโครงการจะดำเนินการตามผลสัมฤทธิ์จากขั้นตอนก่อนหน้า และผลลัพธ์ที่ได้จากแต่ละขั้นตอนจะมีรายละเอียดที่มากขึ้น ในขณะที่โครงการโดยรวมก็คืบหน้าไปเรื่อย ๆ

โดยจะเห็นได้ว่าการจัดการแผนการดำเนินงานที่เป็นขั้นตอนนั้นสามารถลำดับพัฒนาการบูรณาการผลสัมฤทธิ์ในแต่ละขั้นตอนก่อนหน้าและนำผลที่ได้มาประเมินความเป็นไปได้ในการดำเนินการจัดตั้งโครงสร้างในขั้นตอนต่อไปได้

5.1.1 โครงสร้างของการสร้างความสอดคล้อง (Harmonization Structure)

โครงการสร้างความสอดคล้อง (Harmonization project) นั้นถูกออกแบบมาเพื่อแก้ปัญหาช่องโหว่ทางกฎหมาย ความทับซ้อนและซ้ำซ้อนของกฎหมายในประเทศสมาชิกของ ASEAN[189] โดยมีวัตถุประสงค์เพื่อเพิ่มความแน่นอนทางกฎหมายสำหรับประเทศที่เกี่ยวข้องมากกว่าหนึ่งประเทศขึ้นไป กระบวนการสร้างความสอดคล้องมักถูกจัดเป็นสองรูปแบบด้วยกันได้แก่ Hard harmonization และ Soft harmonization ในการสร้างความสอดคล้องทางกฎหมายด้านธุรกิจมักดำเนินการด้วยวิธี Soft harmonization ซึ่งมิได้มุ่งเน้นให้ประเทศสมาชิกต้องรับเอากฎหมายแม่แบบหรือกฎเกณฑ์เดียวกันกันมาใช้ แต่มุ่งเป้าไปยังการฝึกฝนและการสร้างประสิทธิภาพเพื่อให้ประเทศสมาชิกมีความเข้าใจร่วมกัน (หรือสอดคล้องกัน) ในเรื่องบทบัญญัติทางกฎหมาย

ทั้งนี้ วิธีการแบบ Soft harmonization นี้มีศักยภาพอย่างมากในการบูรณาการและการประสานงานกันกับกิจกรรมการเสริมสร้างขีดความสามารถ (Capacity building) อื่น ๆ ของภูมิภาคนี้ ซึ่งทำให้สิ้นเปลืองค่าใช้จ่ายน้อยและสามารถร่วมมือกันกับภูมิภาคเพื่อนบ้านได้เป็นอย่างดี นอกจากนี้ ความช่วยเหลืออื่น ๆ ของสังคมโลกยังอาจจะมีอยู่แล้วในรูปแบบของคู่มือและเครื่องมือ

---

[189] ASEAN secretariat and Galexia, *Harmonization structure are from ASEAN E-Commerce Project*, (2004, November), Documented Analysis of International Developments–Discussion Paper 2 (DP2), (internal project materials).

ทางกฎหมาย เช่น UNCITRAL ได้พัฒนาสื่อการฝึกอบรมเกี่ยวกับ United Nations Convention on the Use of Electronic communication in International Contracts 2005 และองค์กรสหประชาชาติได้ออก UN Manual on the Prevention and Control of Computer และ Convention on Cybercrime ของสหภาพยุโรป เพื่อเป็นแนวทางในการปรับปรุงกฎหมายให้มีประสิทธิภาพและมีความสอดคล้องเป็นอันหนึ่งอันเดียวกัน การฝึกอบรมอย่างสอดคล้องกับสื่อเหล่านี้ในทางทฤษฎีย่อมก่อให้เกิดผลลัพธ์ที่มีประสิทธิภาพ แต่อย่างไรก็ดีการปฏิบัติตามแนวทางดังกล่าวก็ไม่ได้ก่อให้เกิดผลลัพธ์ที่สอดคล้องกันเสมอไป เช่น กฎหมายแม่แบบ UNCITRAL ได้ถูกนำไปปรับใช้แตกต่างกันมากในนานาประเทศ แม้ว่าจะมีความช่วยเหลือในการฝึกอบรมและเสริมสร้างขีดความสามารถในรูปแบบเดียวกันก็ตาม

ดังนั้น ความกังวลใจหนึ่งของอาเซียน และประเทศสมาชิก คือ การที่ภูมิภาคนี้จะไม่สามารถควบคุมการพัฒนาและการฝึกอบรมรวมทั้งสื่อต่าง ๆ ได้ เพราะเหตุปัจจัยเหล่านั้นล้วนมาจากภายนอกภูมิภาค โดยเฉพาะอย่างยิ่งแนวทางเพื่อบรรลุผลสำเร็จที่สามารถช่วยในเรื่องความสอดคล้องกันของกฎหมาย รวมทั้ง สื่อในการฝึกอบรมประเภทเดียวที่องค์กรมีขณะเริ่มโครงการ คือ สื่อทั่วไปที่ไม่ได้รับการปรับแต่งให้เข้ากับผู้รับสาสน์ในภูมิภาคที่มีความแตกต่างกันทั้งสภาวะทางสังคม การเมือง และระบบกฎหมายในประเทศสมาชิก

สำหรับ วิธีการแบบ Hard harmonization คือการออกข้อบังคับต่าง ๆ เพื่อให้ประเทศสมาชิกในภูมิภาคต้องปฏิบัติตาม เช่น การที่สหภาพยุโรปและประเทศสมาชิกได้สร้างมาตรฐานกฎหมายพาณิชย์อิเล็คทรอนิคส์ภายในประเทศที่ตั้งอยู่บนพื้นฐานของ EU Directive on Electronic Commerce ปี ค.ศ. 2000

ซึ่งในที่สุดแล้ว ASEAN ต้องการที่จะใช้วิธีแบบ Hard harmonization เพื่อให้ประเทศสมาชิกออกกฎหมายบนพื้นฐานของแนวทางปฏิบัติ (Guidelines) มากกว่าเป็นเพียงแค่การเสริมสร้างขีดความสามารถ (Capacity-building) เท่านั้น โดยวิธีการแบบ Hard Harmonization ซึ่งมีพื้นฐานบนการสร้างคู่มือแนวทางปฏิบัติ ซึ่งเป็นเครื่องมือที่ครอบคลุมและสามารถทำให้แน่ใจได้ว่าประเทศสมาชิกอาเซียนที่มีศักยภาพในการพัฒนาน้อยกว่าจะเข้าร่วม อีกทั้งแนวทางปฏิบัติยังให้ขั้นตอนการดำเนินงานที่รับรองความสอดคล้องในทางกฎหมายมากกว่าวิธีแบบ Soft Harmonization นอกจากนั้น ตัวแนวทางปฏิบัติเองยังได้กำหนดตารางเวลาการดำเนินการในแต่ละขั้นตอนเอาไว้ทำให้การพัฒนาเป็นไปอย่างมีระบบระเบียบ เป็นการพัฒนากรอบโครงสร้างทางกฎหมายแบบมีขั้นมีตอน (Phased development) อีกทั้งยังเปิดโอกาสให้มีการตีความที่แคบลงเพื่อที่จะลดความไม่สอดคล้องต้องกันอีกด้วย จึงทำให้แนวทางปฏิบัติยังคงเป็นเครื่องมือที่ยืดหยุ่นและสามารถทบทวนหรือเพิ่มเติมได้ (เช่น ทุก ๆ สามปีเป็นต้น)

ภายใต้ทางเลือกแบบ Hard harmonization คู่มือแนวปฏิบัติสำหรับโครงการ Harmonization project จะถูกจัดทำขึ้น โดยคู่มือจะถูกออกแบบบนพื้นฐานของเป้าหมายร่วมกัน โดยหลักการต่าง ๆ สำหรับกรอบโครงสร้างทางกฎหมาย คู่มือจะประกอบไปด้วยข้อมูลซึ่งกำหนดมาให้สำหรับลำดับการนำไปปฏิบัติและขอบเขตระยะเวลา โดยอาจจัดทำโดยอาศัยความช่วยเหลือจากองค์กรภายนอกภูมิภาคพร้อมด้วยผู้เชี่ยวชาญเฉพาะด้านจากประเทศสมาชิกอาเซียน เป็นต้น

โดยหากยกเอาแนวทางการสร้างคู่มือสำหรับโครงการ e-ASEAN มาเป็นตัวอย่างการออกแบบแนวทางปฏิบัติมีองค์ประกอบดังนี้

5.1.1.1 หลักการที่จะนำไปปฏิบัติจริงในระดับภูมิภาค (Regional implementation)

โครงการ e-ASEAN นี้ประกอบไปด้วยกิจกรรมและผลการดำเนินการมากมายตลอดระยะเวลาดำเนินการ ทั้งการประชุมเชิงปฏิบัติการระหว่างประเทศสมาชิกอาเซียนและผู้เข้าร่วมจากภูมิภาคอื่น เช่น ออสเตรเลีย ญี่ปุ่น และสหรัฐอเมริกา และยังมีการติดต่อกับองค์กรระหว่างประเทศอื่น ๆ เช่น APEC, UNCITRAL, UNCTAD และ UNESCAP สำหรับ แนวทางการปฏิบัติและการตรวจสอบรายการ (Checklist) หลาย ๆ อย่างได้ถูกจัดทำขึ้นระหว่างการดำเนินโครงการ ทั้งคู่มือทั่วไป (ในระดับภูมิภาค) และคู่มือเฉพาะ (ในระดับประเทศ)

โดยได้มีการออกแบบสำรวจหลายครั้งในช่วงการดำเนินโครงการเพื่อศึกษาพัฒนาการและปัญหาต่าง ๆ ของภูมิภาค และเพื่อให้โอกาสกับประเทศสมาชิกในการให้ข้อมูลอย่างละเอียดในขั้นตอนสำคัญ ๆ (Key stages) ของโครงการ ซึ่งแบบสอบถามนี้ได้ถูกส่งไปยังตัวแทนรัฐบาลของประเทศสมาชิกอาเซียนทุกประเทศ และได้ถูกนำมาตีพิมพ์ในช่วงของการดำเนินโครงการ

5.1.1.2 หลักการเพื่อนำไปปฏิบัติภายในประเทศสมาชิก (Domestic implementation)

หากเปรียบเทียบกับการรวมกลุ่มของกลุ่มประเทศอื่น ๆ แล้ว สมาชิกอาเซียนทั้ง 10 ประเทศมีความแตกต่างกันเป็นอย่างมากทั้ง วัฒนธรรม ศาสนาประจำชาติ ระบบกฎหมาย รูปแบบของการปกครองและระดับการพัฒนาทางเศรษฐกิจ ซึ่งเมื่อองค์การอาเซียนต้องการนำกฎหมายใดก็ตามมาปรับใช้ในภูมิภาคนี้ ปัญหาและอุปสรรคที่จะต้องพบก็คือ การจะทำอย่างไรที่ทำให้หลักเกณฑ์ดังกล่าวถูกนำไปใช้กับกฎหมายภายในของแต่ละประเทศได้อย่างสอดคล้องกันเพราะมีความแตกต่างกันอยู่ ซึ่งความเหลื่อมล้ำที่เห็นได้ชัดที่สุดในเรื่องของโครงสร้างทางกฎหมายที่เกี่ยวกับวิทยาการสารสนเทศและอาชญากรรมทางคอมพิวเตอร์นั้น คือ ระดับความแตกต่างของการพัฒนาประเทศสมาชิกแต่ละประเทศมีไม่เท่าเทียมกัน เนื่องจากอาเซียนประกอบไปด้วยประเทศพัฒนาแล้ว เช่น สิงคโปร์ ซึ่งมีโครงสร้างทางกฎหมายสารสนเทศและคอมพิวเตอร์ที่สมบูรณ์ และประเทศกำลังพัฒนา เช่น ประเทศลาว และประเทศกัมพูชา ที่ส่วนใหญ่มีเพียงโครงสร้างพื้นฐานทางกฎหมายสารสนเทศ

อย่างไรก็ดี ด้วยพัฒนาการของวิทยาการและเศรษฐกิจที่มีเทคโนโลยีสารสนเทศเป็นตัวผลักดันให้พัฒนาไปอย่างรวดเร็วทำให้หลายประเทศในอาเซียนไม่เว้นแต่กลุ่ม CLMV ได้ออกกฎหมายเพื่อรองรับสภาพความเปลี่ยนแปลงของเศรษฐกิจและสังคมในระยะเวลาอันสั้น ขณะนี้เกือบทุกประเทศสมาชิกของอาเซียนได้มีกฎหมายที่เกี่ยวข้องกับ ICT และ อาชญากรรมทางคอมพิวเตอร์ทั้งที่บังคับใช้แล้วและยังอยู่ในขั้นตอนการยกร่างกฎหมาย แต่อย่างไรก็ตาม อุปสรรคสำคัญในการสร้างหลักเกณฑ์กลางยังคงอยู่ที่การทำให้ประเทศสมาชิกอาเซียนทั้ง 10 ประเทศต้องมีการอนุวัติกฎหมายภายในประเทศให้สอดคล้องกัน เพราะบางประเทศยังไม่สามารถรับรองผู้ให้บริการลายเซ็นอิเล็คทรอนิคส์ซึ่งนับเป็นเงื่อนไขพื้นฐานของธุรกรรมออนไลน์เลยทีเดียว

นอกจากนี้ ประเทศสมาชิกที่มีกฎหมายว่าด้วยอาชญากรรมทางคอมพิวเตอร์อยู่แล้วอาจต้องพิจารณาทบทวนกฎหมายเหล่านั้นใหม่เพื่อให้เป็นไปในแนวทางเดียวกันกับคู่มือเกี่ยวกับการออกกฎหมายอาชญากรรมทางคอมพิวเตอร์ เช่น คู่มือของโครงการ e-ASEAN แนะนำให้ประเทศสมาชิกแก้ไขกฎหมายของตนให้สอดคล้องกับ United Nations Convention on the Use of Electronic Communication in International Contracts 2005 เป็นต้น โดยคู่มือกฎหมายว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของอาเซียนอาจแนะนำให้ประเทศสมาชิกแก้ไขกฎหมายให้สอดคล้องกับอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์

การนำเอาหลักเกณฑ์ตามคู่มือนี้มาปรับใช้กับกฎหมายภายในประเทศสมาชิกอาเซียนทุกประเทศนั้นจากการสำรวจพบว่าอุปสรรคสำคัญที่แท้จริงอยู่ที่ ขีดจำกัดของนโยบายและการสนับสนุนจากภาครัฐ การให้ทุนที่จำกัด รวมไปถึงการขาดแคลนทักษะและการฝึกอบรมทรัพยากรบุคคล โดยความร่วมมือกันของทั้งภาครัฐและเอกชนเป็นปัจจัยสำคัญต่อการนำเอาหลักเกณฑ์ตามคู่มือนี้มาปรับใช้กับกฎหมายภายในประเทศ เนื่องจากอาชญากรรมทางคอมพิวเตอร์นั้นเป็นปัญหาใหญ่ซึ่งหากพึ่งพาแต่เพียงภาครัฐอาจไม่สามารถดำเนินการเพื่อรองรับกับปัญหาดังกล่าวได้อย่างมีประสิทธิภาพเพียงพอ

ส่วนอุปสรรคสำคัญอีกอันหนึ่งในนำเอาหลักเกณฑ์ตามคู่มือมาปรับใช้กับกฎหมายของประเทศในกลุ่ม CLMV[190] ซึ่งเป็นกลุ่มประเทศที่มีระดับการพัฒนาด้อยกว่าประเทศสมาชิกอีก 6 ประเทศในอาเซียนนั้นคือ มีความแตกต่างจากประเทศสมาชิกอื่นในเรื่องของนโยบายและการสนับสนุนจากภาครัฐ การขาดตลาดรองรับที่แข็งแรงพอสำหรับบริการทางด้านสารสนเทศ การให้ทุนที่จำกัด รวมไปถึงการขาดแคลนทักษะและการฝึกอบรมทรัพยากรบุคคล โดยข้อจำกัดในด้าน

---

[190] ASEAN secretariat and Galexia, *Survey of Implementation Issues and Constraints for a Harmonized E-Commerce Legal Infrastructure in ASEAN*, ASEAN E-Commerce Project, (2005, February), (S2), (internal project materials).

นโยบายของภาครัฐเป็นปัญหาสำคัญต่อการปรับใช้หลักเกณฑ์ตามคู่มือกับกฎหมายภายในประเทศ เนื่องจากรัฐอาจให้ความสำคัญกับเรื่องอื่นมาก่อนการพัฒนาโครงสร้างทางกฎหมายว่าด้วยอาชญากรรมทางคอมพิวเตอร์ หรือรัฐบาลอาจเห็นว่าในขณะนี้ตลาดที่รองรับยังมีไม่มากนักจนสามารถที่จะก่อให้เกิดปัญหาร้ายแรงมากกว่าอาชญากรรมรูปแบบดั้งเดิมแต่อย่างใด

หากปราศจากการสนับสนุนจากรัฐบาลแล้วการนำเอาหลักเกณฑ์ระหว่างประเทศมาปรับใช้เป็นกฎหมายภายในก็ไม่อาจบรรลุผลสำเร็จได้ อย่างไรก็ตาม กิจกรรมที่เกี่ยวข้องกับการเตรียมความพร้อมเพื่อรับมือกับอาชญากรรมทางคอมพิวเตอร์ได้ถูกจัดขึ้นมาอยู่เรื่อย ๆ ระหว่างประเทศสมาชิก ซึ่งเป็นตัวผลักดันให้เกิดพัฒนาการของโครงสร้างทางกฎหมายสารสนเทศและอาชญากรรมทางคอมพิวเตอร์ ซึ่งกิจกรรมเหล่านี้ต่างต้องอาศัยทุนจากภาครัฐและมักต้องใช้งบประมาณจากกิจกรรมในสาขาอื่น ๆ ซึ่งหากมีการสนับสนุนเงินทุนเพื่อสร้างโครงสร้างพื้นฐานทางกฎหมายว่าด้วยอาชญากรรมทางคอมพิวเตอร์จากรัฐอย่างเพียงพอแล้ว กิจกรรมอื่น ๆ ก็จะสามารถดำเนินการต่อยอดไปได้อย่างต่อเนื่อง แต่หากเงินทุนจากภาครัฐขาดแคลนอาจกลายเป็นอุปสรรคสำคัญในการเสริมสร้างขีดความสามารถ (Capacity building) ในการรับมืออาชญากรรมทางคอมพิวเตอร์ในอนาคต

ด้านเงินทุนนั้นมีความสำคัญในระยะเริ่มต้นของการกำหนดขอบเขตและสร้างนโยบายผ่านการนำไปปฏิบัติและติดตามผล ซึ่งหากการสนับสนุนจากรัฐบาลไม่เพียงพออาจทำให้เกิดความจำเป็นต้องพึ่งพาความช่วยเหลือจากหน่วยงานภายนอก เช่น อาเซียน สหประชาชาติ หรือองค์กรภูมิภาคอื่น ๆ

สำหรับโครงการเพื่อสร้างความสามารถในการรับมือกับอาชญากรรมทางคอมพิวเตอร์ ถือว่ามีบทบาทสำคัญในการให้ความรู้แก่เจ้าหน้าที่ของรัฐบาลในประเทศสมาชิกอาเซียน และทำให้เกิดความเข้าใจไปในทิศทางเดียวกันในหมู่ประเทศสมาชิกในเรื่องหลักเกณฑ์ตามคู่มือฯ การสร้างความสามารถในการรองรับนั้นไม่เพียงแต่เพิ่มทักษะและความรู้ของผู้เชี่ยวชาญแต่ยังช่วยให้เกิดความสอดคล้องในเรื่องความเข้าใจในกรอบโครงสร้างทางกฎหมายหากต้องดำเนินโครงการในระดับภูมิภาค

อย่างไรก็ดี โครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศในประเทศกลุ่ม CLMV นั้นยังอยู่ในระยะเริ่มพัฒนาทำให้ไม่มีตลาดที่เติบโตเพียงพอถึงขนาดทำให้รัฐบาลเล็งเห็นความสำคัญเป็นลำดับต้น ๆ ในการดำเนินนโยบายเพื่อเร่งพัฒนาโครงสร้างพื้นฐานทางกฎหมายสารสนเทศอย่างจริงจัง แต่ด้วยอัตราการเติบโตของผู้ใช้อินเตอร์เน็ตในกลุ่มประเทศเหล่านี้ที่เพิ่มขึ้นอย่างต่อเนื่อง เช่น เวียดนามที่ในปี พ.ศ. 2543 มีผู้ใช้อินเตอร์เน็ตเพียง 0.3% ในระยะเวลา 10 ปีมีผู้ใช้อินเตอร์เน็ต

เพิ่มขึ้นจนถึง 30% แซงหน้าประเทศไทยซึ่งมีประชากรผู้ใช้อินเตอร์เน็ต 22.4% (ปี พ.ศ. 2553)[191] ทำให้รัฐบาลต้องเร่งพัฒนากฎหมายเพื่อรองรับการเติบโตดังกล่าว

องค์การอาเซียนได้เข้าร่วมโครงการหลายโครงการเพื่อลดช่องว่างทางการพัฒนาเทคโนโลยีสารสนเทศของประเทศสมาชิกในภูมิภาค เช่น การริเริ่มเพื่อการรวมตัวของอาเซียน (The Initiative for ASEAN Integration: IAI) ที่เป็นโครงการที่จัดหากรอบโครงสร้างในด้านความร่วมมือของภูมิภาค โดยให้ประเทศสมาชิกอาเซียนที่มีพัฒนาการมากกว่าให้ความช่วยเหลือแก่ประเทศสมาชิกอื่น ๆ โดยมุ่งเน้นไปที่การศึกษา การพัฒนาทักษะ และการฝึกแรงงาน

แผนงานของ IAI สำหรับประเทศในกลุ่ม CLMV นั้นมุ่งเน้นไปที่การให้ความสำคัญต่อการพัฒนาโครงสร้างพื้นฐาน (การคมนาคมและพลังงาน) การพัฒนาทรัพยากรมนุษย์ (การเสริมสร้างขีดความสามารถในภาครัฐ แรงงาน การจ้างงาน และการศึกษา) ข้อมูลข่าวสารและวิทยาการการสื่อสาร และส่งเสริมการบูรณาการทางด้านเศรษฐกิจในระดับภูมิภาค (การค้าขายสินค้าและบริการ ภาษีศุลกากรและการลงทุน)[192]

โครงการ IAI และแผนปฏิบัติการเชิงรุกเพื่อการพัฒนาอื่น ๆ ในระดับภูมิภาค และระดับภายในประเทศต่างมีเป้าหมายในการปรับปรุงโครงสร้างทางด้านสารสนเทศและการสื่อสารในประเทศสมาชิกอาเซียน เพราะโครงสร้างดังกล่าวจะกลายเป็นฐานสำคัญในการพัฒนาโครงสร้างทางกฎหมายที่ก้าวหน้าเพิ่มมากขึ้น รวมไปถึงการพัฒนากฎหมายอาชญากรรมทางคอมพิวเตอร์ที่เป็นเอกภาพอีกด้วย กล่าวได้ว่าการจะบรรลุผลสำเร็จในการสร้างความสอดคล้องในทางกฎหมายระดับภูมิภาคได้นั้นยังต้องให้ความสำคัญกับประเทศในกลุ่ม CLMV เช่นกัน

การขาดการฝึกอบรมทักษะและความรู้ถือว่าเป็นอุปสรรคที่สำคัญในการที่จะนำเอาข้อแนะนำจากคู่มือไปปรับใช้กับกฎหมายภายในประเทศของแต่ละประเทศ เพราะหากผู้เชี่ยวชาญภายในประเทศใดประเทศหนึ่งขาดประสบการณ์กับการทำงานบนข้อบังคับหรือกรอบโครงสร้างนโยบายทางสารสนเทศที่เป็นสากล ก็จะทำให้ผู้เชี่ยวชาญในประเทศนั้น ๆ ไม่สามารถขัดเกลาทักษะและความรู้ในสาขานั้นได้

จากการสำรวจพบว่า ทรัพยากรที่ประเทศสมาชิกต้องการเพื่อนำไปพัฒนากรอบโครงสร้างทางกฎหมายสารสนเทศมากที่สุด ได้แก่ เงินทุนในการจัดกิจกรรม โครงการบูรณาการของคณะกรรมการอาเซียนเพื่อเป็นช่องทางในการส่งความช่วยเหลือไปยังประเทศสมาชิกที่ยังไม่พัฒนา

---

[191] ข้อมูลจาก google.com ค้นหาด้วย keyword Vietnam internet users.

[192] *ความริเริ่มเพื่อการรวมตัวของอาเซียน*, สืบค้นเมื่อ 10 สิงหาคม 2555 จาก http://www.mfa.go.th/asean/contents/files/asean-media-center-20121218-095324-481007.pdf

การฝึกอบรมทางกฎหมายเพื่อเจ้าหน้าที่ดำเนินการ เช่น ผู้กำหนดนโยบายและผู้ร่างกฎหมาย รวมไปถึงการกระตุ้นความตระหนักให้แก่ทั้งภาครัฐและเอกชน

5.2 สภาพปัญหาอาชญากรรมทางคอมพิวเตอร์ของอาเซียน

เมื่อภัยจากอาชญากรรมทางคอมพิวเตอร์ไม่ว่าจะมาจากจากแรงจูงใจทั่วไป (การเมือง, ศาสนา ความท้าทาย ฯลฯ) หรือมาจากอาชญากรรมที่กระทำอย่างเป็นระบบ (Organized crime) ที่ได้แผ่ขยายมากขึ้นตามอัตราการเข้าถึงอินเตอร์เน็ตที่เพิ่มขึ้นอย่างมหาศาลในประเทศสมาชิกอาเซียนก็ตาม และด้วยการที่อาชญากรรมทางคอมพิวเตอร์เป็นอาชญากรรมข้ามชาติซึ่งต้องการความร่วมมือในระดับพหุภาคี (Multilateral cooperation) ในการรับมือ ดังนั้น ความสอดคล้องของกฎหมายในแต่ละประเทศจึงเป็นปัจจัยที่สำคัญในการดำเนินคดีกับอาชญากรทางคอมพิวเตอร์ โดยในปัจจุบันภูมิภาคเอเชียตะวันออกเฉียงใต้ถูกมองจากประชาคมโลกว่าเป็นแหล่งกบดาน (Safe haven) ของอาชญากรทางคอมพิวเตอร์เนื่องจากความด้อยพัฒนาในด้านโครงสร้างพื้นฐานทางกฎหมายว่าด้วยอาชญากรรมทางคอมพิวเตอร์และหลายประเทศในภูมิภาคเปิดช่องให้องค์กรอาชญากรรมได้แฝงตัวเพื่อใช้เป็นฐานการก่ออาชญากรรมได้ สาเหตุเพราะการที่กระบวนการยุติธรรมภายในประเทศเหล่านั้นมีความไม่สอดคล้องกับแนวทางปฏิบัติสากล ทำให้ไม่สามารถดำเนินการสืบสวนหาหลักฐาน จับกุม หรือส่งผู้ร้ายข้ามแดนในคดีที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์ได้อย่างมีประสิทธิภาพ ทำให้หลายประเทศในภูมิภาคกลายเป็นต้นตอของ Attack traffic จำนวนมาก ซึ่งก่อให้เกิดปัญหากับทั้งประเทศสมาชิกอาเซียนและนานาชาติ แต่อย่างไรก็ตาม ประเทศในกลุ่มอาเซียนต่างเล็งเห็นถึงความเร่งด่วนในการจัดการปัญหาดังกล่าว จึงได้ทำการออกกฎหมายว่าด้วยอาชญากรรมทางคอมพิวเตอร์โดยอาศัยแม่แบบของกฎหมายที่เป็นสากลต่าง ๆ เพื่อใช้เป็นแนวทางในการยกร่างกฎหมายให้ครอบคลุมในทุกรูปแบบของอาชญากรรมทางคอมพิวเตอร์

5.2.1 ความครอบคลุมในด้านเนื้อหาของกฎหมายที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์และความปลอดภัยบนอินเตอร์เน็ต (Cybercrime law and cyber security law coverage)

ปัจจุบัน ความครอบคลุมในด้านเนื้อหาของกฎหมายอาชญากรรมทางคอมพิวเตอร์นั้นมีความแตกต่างกันไปในแต่ละประเทศสมาชิกอาเซียน ซึ่งอาจแบ่งความครอบคลุมตามตามแต่ละประเภทของอาชญากรรมทางคอมพิวเตอร์ไว้ดังนี้

5.2.1.1 กฎหมายว่าด้วยการคุ้มครองความเป็นส่วนตัวและการคุ้มครองข้อมูล (Data Protection and Privacy law)

ปัจจุบันมีเพียงประเทศมาเลเซีย ฟิลิปปินส์และสิงคโปร์ที่มีกฎหมายว่าด้วยการคุ้มครองข้อมูลและความเป็นส่วนตัวบนอินเตอร์เน็ต นอกจากนั้น ยังมี ประเทศไทย[193] และอินโดนีเซียที่อยู่ในระหว่างการยกร่างกฎหมาย อย่างไรก็ดีประเทศสมาชิกอาเซียนส่วนใหญ่เป็นสมาชิกของกลุ่ม APEC ที่ได้พัฒนาและดำเนินการ APEC privacy framework[194] ตั้งแต่ปี พ.ศ. 2547 โดยกรอบโครงสร้างด้านความเป็นส่วนตัวดังกล่าวได้มีอิทธิพลต่อพัฒนาการของการคุ้มครองความเป็นส่วนตัวทั่วทั้งทวีปเอเชียด้วย เช่น สภาพนิรนามและการเข้ารหัสข้อมูล (Anonymity and encryption) โดยสภาวะนิรนามของบุคคลเมื่อใช้งานอินเตอร์เน็ตนั้น ถือว่ามีความเสี่ยงที่จะก่อให้เกิดการกระทำที่ผิดกฎหมาย การใช้งานเครื่องมือที่มีแจกจ่ายกันแพร่หลายบนอินเตอร์เน็ตเพื่อปิดบัง IP Address ตำแหน่งทางกายภาพหรืออัตลักษณ์ทำให้การทำงานของเจ้าหน้าที่มีความยากลำบากมากยิ่งขึ้น เช่นเดียวกับการเข้ารหัสข้อมูล (encryption) เพื่อป้องกันการเข้าถึงข้อมูลจากบุคคลที่สาม ในขณะที่การใช้งานอุปกรณ์เหล่านี้ก่อประโยชน์ต่อผู้ใช้ในแง่ของการคุ้มครองข้อมูล การที่อาชญากรไซเบอร์สามารถนำเอาเครื่องมือเหล่านี้มาใช้ได้ง่ายนั้นทำให้มีความจำเป็นต้องมีการระบุถึงแนวทางการควบคุมดูแลการใช้งานหรือการเผยแพร่เครื่องมือประเภทดังกล่าวนี้ในกฎหมายว่าด้วยอาชญากรรมทางคอมพิวเตอร์ด้วย[195]

5.2.1.2 อาชญากรรมทางคอมพิวเตอร์ ความผิดประเภทบุกรุก (Unauthorized access)

ปัจจุบันกฎหมายอาชญากรรมทางคอมพิวเตอร์ ของประเทศสมาชิกอาเซียนมีความแตกต่างกันเล็กน้อย อย่างไรก็ดี ความผิดที่มีอยู่ในกฎหมายของทุกประเทศสมาชิกที่มีกฎหมายอาชญากรรมทางคอมพิวเตอร์ คือ ความผิดประเภทบุกรุก เช่น ความผิดประเภทการการเข้าถึงยังระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต (Unauthorized access) การเข้าถึงยังระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตด้วยเจตนากระทำความผิด (Unauthorized access with the intent of committing a crime) และการเปลี่ยนแปลงแก้ไขข้อมูลทางคอมพิวเตอร์โดยไม่ได้รับอนุญาต (Unauthorized modification of computer material) โดยความผิดเหล่านี้มีอยู่ใน Computer Misuse Act 1990 ของ

---

[193] ร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล.

[194] APEC, *Fact sheets (APEC Data Privacy Pathfinder)*, Retrieved 2013, September 22, from http://www.apec.org/About-Us/About-APEC/Fact-Sheets/APEC-Privacy-Framework.aspx

[195] เป็นกฎหมายประเภท Key disclose law คือ กฎหมายที่บังคับให้ส่งกุญแจการเข้ารหัส (Cryptographic keys) แก่เจ้าพนักงานกฎหมายเมื่อมีการร้องขอ เพื่อให้สามารถเข้าถึงหลักฐานดิจิตอลที่มีการเข้ารหัส (Encryption) ไว้ได้ เพื่อใช้เป็นหลักฐานในศาลหรือเพื่อประโยชน์ด้านความมั่นคงของชาติ มีการบังคับใช้ในหลายประเทศด้วยกัน เช่น สหรัฐอเมริกา อินเดีย เบลเยียม แคนาดา ฟินแลนด์ ฝรั่งเศส โปแลนด์ สหราชอาณาจักร ออสเตรเลีย เป็นต้น.

สหราชอาณาจักรซึ่งเป็นต้นแบบของกฎหมายอาชญากรรมทางคอมพิวเตอร์ของประเทศสิงคโปร์และประเทศบรูไน ในปัจจุบันความผิดประเภทบุกรุกนี้เกือบทุกประเทศสมาชิกของอาเซียนถือว่าการเปิดเผยรหัสเชื่อมต่อคอมพิวเตอร์โดยไม่ได้รับอนุญาตเป็นความผิดอีกด้วย และ เนื่องจากการเมืองประเทศสมาชิกอาเซียนหลายประเทศมีความตึงเครียดเป็นอย่างมาก ส่งผลให้อาชญากรรมทางคอมพิวเตอร์ที่มีการเมืองเป็นแรงผลักดันจึงเกิดขึ้นบ่อยครั้ง โดยมากเป้าหมายจะเป็นเว็บไซต์ของรัฐบาล และเป็นการโจมตีประเภทเปลี่ยนแปลงแก้ไขหน้าเว็บ (Defacement) และ DDoS เช่น เหตุการณ์เปลี่ยนแปลงหน้าเว็บไซต์สำนักนายกรัฐมนตรีของประเทศไทย โดยนักเจาะระบบนำรูปนายกรัฐมนตรีพร้อมข้อความดูหมิ่นไปใส่ไว้แทนหน้าเว็บเดิม[196] เป็นต้น

ปัจจุบันมีเครื่องมือสำเร็จรูปจำนวนมากบนอินเตอร์เน็ตที่ผู้ใช้อินเตอร์เน็ตสามารถนำมาใช้ได้ง่าย โดยไม่จำเป็นต้องเป็นผู้เชี่ยวชาญ และสามารถฝึกฝนเพื่อใช้งานได้ในเวลาไม่นาน ดังนั้นเมื่อเกิดเหตุการณ์พิพาทต่าง ๆ ไม่ว่าจะเป็นภายในประเทศหรือระหว่างประเทศ ผู้ใช้อินเตอร์เน็ตจะปลดปล่อยความโกรธแค้นของพวกเขาบนอินเตอร์เน็ตผ่านการโจมตีเป้าหมายซึ่งอาจเป็นเว็บไซต์หรือบริการผ่านเครือข่ายอินเตอร์เน็ตของรัฐ ซึ่งในประเทศสมาชิกอาเซียนส่วนใหญ่เว็บไซต์เหล่านี้มีระดับการรักษาความปลอดภัยที่ค่อนข้างต่ำ เนื่องจากรัฐบาลมักไม่ใช้งบประมาณในการตั้งหน่วยรับมือการโจมตีซึ่งจำเป็นจะต้องทำงานตลอด 24 ชั่วโมง[197] หลายครั้งที่ข้อพิพาทระหว่างประเทศเป็นเหตุให้เกิดการโจมตีล้างแค้นกันไปมา เช่นกรณีแฮกเกอร์ประเทศไต้หวันและประเทศฟิลิปปินส์ผลัดกัน DDoS เว็บไซต์ของหน่วยงานรัฐทั้งสองประเทศ เนื่องมาจากการที่ประเทศฟิลิปปินส์ปฏิเสธที่จะขอโทษไต้หวันในเหตุการณ์เรือตรวจการของฟิลิปปินส์ยิงใส่เรือประมงของไต้หวันจนทำให้ชาวประมงชาวไต้หวันเสียชีวิต[198] จนเป็นเหตุให้บริการของรัฐต้องหยุดชะงัก นอกจากนี้ การนำเอาบอทเน็ท (Bot-net) [199] มาใช้ในการก่ออาชญากรรมทางคอมพิวเตอร์

---

[196] ASTVผู้จัดการออนไลน์, *มือดีแฮกเว็บสำนักนายกฯ ด่า "ยิ่งลักษณ์" เย้ย ICT*, (8 พฤษภาคม 2556), สืบค้นเมื่อ 7 ธันวาคม 2556, จาก http://www.manager.co.th/Politics/ViewNews.aspx?NewsID=956000005516

[197] Most government agencies and corporations do not have the resources to build and maintain a team of Internet security professionals that are on the watch 24/7., Nexusguard, *When it comes to defending against DDoS attacks, DDoS Alert: Taiwan and the Philippines Exchanging Digital Blows*, Retrieved 2013, December 7, from http:// www.prweb.com/releases/2013/5/ prweb10735330.htm

[198] Ibid.

[199] ในปัจจุบันการใช้งานบอทเน็ตนับว่าเป็นพัฒนาการมากที่สุดของอาชญากรรมทางคอมพิวเตอร์นับตั้งแต่การลงนามในอนุสัญญาอาชญากรรมทางคอมพิวเตอร์ของสภายุโรป ด้วยการใช้คอมพิวเตอร์ในระบบเครือข่ายจำนวนมากที่ถูกบอทเน็ตเข้าควบคุม อาชญากรสามารถกระทำการโจมตีซึ่งก่อให้เกิดความเสียหายอย่างหนัก มีการค้นพบเครือข่ายของบอทเน็ตที่ประกอบไปด้วยคอมพิวเตอร์นับแสนเครื่อง โดยมีเป้าประสงค์เพื่อใช้ในการก่อการร้ายไซเบอร์หรือสงครามไซเบอร์.

โดยเฉพาะอย่างยิ่งในความผิดประเภทบุกรุก เช่น อาชญากรรมร้ายแรงอย่างการโจมตีแบบ DDoS และยังสามารถใช้ส่งสแปมปริมาณมหาศาลรวมทั้งข้อความล่อลวง (Phishing message) จากบัญชีผู้ใช้ (Account) ที่ถูกขโมยโดยบอทเน็ตได้อีกด้วย กว่า 80% ของการกระทำผิดประเภท Phishing นั้นมาจากบอทเน็ททั้งสิ้น[200] โดยการใช้งานบอทเน็ตอาจลอกเลียนแบบบางวิธีการของอาชญากรรมทางคอมพิวเตอร์แบบเป็นระบบ (Cyber organized crime)[201] นอกจากนี้ การใช้งานคอมพิวเตอร์ซึ่งมีบอทเน็ตแฝงตัวอยู่เพื่อดำเนินการโจมตี อาชญากรสามารถหลีกเลี่ยงหรือแม้แต่ก่อกวนกระบวนการสืบสวนเนื่องจากคอมพิวเตอร์ซึ่งตกเป็นเหยื่อของบอทเน็ตนั้นมักกระจายตัวอยู่ทั่วโลก และในปัจจุบันยังไม่มีคู่มือเพื่อการดำเนินการสืบสวนในระดับระหว่างประเทศเป็นการเฉพาะ ซึ่งปัจจุบันผู้ที่ต้องการใช้งานบอทเน็ตสามารถทำการซื้อหรือแม้แต่เช่าตัวซอฟท์แวร์ผ่านอินเตอร์เน็ตในราคาไม่แพงนัก แม้แต่อาชญากรที่ไม่ได้มีความเชี่ยวชาญทางเทคนิคมากนักก็สามารถใช้เครื่องมือที่ถูกจัดไว้ให้โดยผู้สร้างบอทเน็ทได้อย่างง่ายดายหรือจะจ้างนักเจาะระบบดำเนินการให้ก็ได้ และเมื่อ ทั้งเครื่องคอมพิวเตอร์ที่บอทเน็ตแฝงตัวอยู่ รวมไปถึงตัวผู้ซื้อ และผู้ขายบอทเน็ตสามารถอยู่กันคนละประเทศ ดังนั้น ความร่วมมือระหว่างประเทศในแบบ Real-time ผ่านความร่วมมือกันระหว่างหน่วยงาน CERT ของแต่ละประเทศจึงมีความจำเป็นอย่างยิ่ง

โดยเมื่อต้นปี ค.ศ. 2010 บริษัทด้านความปลอดภัย Akamai ได้ออกมาเปิดเผยข้อมูลว่ากว่า 21% ของการโจมตีทางอินเตอร์เน็ตมีต้นตอมาจากเอเชียตะวันออกเฉียงใต้[202] ซึ่งได้มีการตรวจพบว่าการจู่โจมด้วยบอทเน็ตผ่านคอมพิวเตอร์ที่มีบอทเน็ตแฝงตัวอยู่จำนวนมากนั้นมาจากประเทศอินโดนีเซีย ทั้งนี้เดือนมกราคม พ.ศ. 2556 แฮกเกอร์ได้ทำการเปลี่ยนแปลงหน้าเว็บ (defacement) ของรัฐบาลอินโดนีเซียเพื่อเป็นการประท้วงรัฐบาลที่จับกุมตัวแฮกเกอร์ซึ่งได้กระทำการเจาะระบบเว็บไซต์ของรัฐบาลก่อนหน้า[203] นอกจากนี้ สำนักข่าวซิงหัวของประเทศจีนได้รายงานข่าวเกี่ยวกับ

---

[200] Schjolberg, S., & Ghernaouti-Helie, S., *A global treaty on cybersecurity and cybercrime (Second Edition)*, (2011), Retrieved 2013, December 4, from http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime_Second_edition_2011.pdf.

[201] Chan, Y. C., *Cybercrime across the Taiwan strait—Regulatory responses and crime prevention*, Unpublished Ph.D. thesis, (Canberra: Australian National University, 2010)

[202] *AKAMAI*, *The State of the Internet 2013 Full report*, (2013), Retrieved 2014, February 3, from http://www.akamai.com/dl/akamai/akamai_soti_q113.pdf.

[203] Muncaster, P., Indonesian hackers protest hacker's arrest by hacking, *The Register*, (2013, January 30), Retrieved, 2014, April 4, from http://www.theregister.co.uk/2013/01/30/hacker_indonesia_sby_arrest/

แผนการจัดตั้งกองทัพไซเบอร์ของรัฐบาลอินโดนีเซีย[204] เพื่อรับมือกับการก่อการร้ายไซเบอร์และสงคามไซเบอร์ ประเทศอินโดนีเซียถูกจัดให้อยู่ในอันดับที่สอง ของประเทศที่มีการโจมตีทางอินเตอร์เน็ตมากที่สุดในโลกรองจากประเทศจีน[205]

5.2.1.3 สงคราม การจารกรรม และการก่อการร้ายไซเบอร์ (Cyber warfare, cyber espionage and cyber terrorism)

อุปสรรคที่สำคัญในการจัดการภัยไซเบอร์ระหว่างประเทศ คือ ความไม่ชัดเจนของขอบเขตระหว่างอาชญากรรมทางคอมพิวเตอร์ (Cyber-crime) การจารกรรมไซเบอร์ (Cyber-espionage) และ การจู่โจมไซเบอร์ (Cybert-attack) เพราะสงครามไซเบอร์มักถูกมองว่าเป็นเรื่องที่ดูร้ายแรงน้อยกว่าความเป็นจริง ทั้งนี้ภัยจากการจารกรรมและการจู่โจมไซเบอร์ยิ่งจะมีความเสี่ยงในการถูกประเมินความร้ายแรงต่ำกว่าความเป็นจริงอีกด้วย โดยการจารกรรมและจู่โจมไซเบอร์ที่เกิดขึ้นมากในภูมิภาคอาเซียนแสดงให้เห็นถึงการขาดเสถียรภาพในการบริหารจัดการความปลอดภัยทางอินเตอร์เน็ต แม้ว่าความเสี่ยงภัยที่เห็นได้ชัดเจนและดูจะร้ายแรงที่สุดในปัจจุบันคือการจารกรรมทางเศรษฐกิจ ซึ่งมีเป้าหมายไปที่เทคโนโลยี งานวิจัย ข้อมูลลับทางธุรกิจ และทรัพย์สินทางปัญญา แต่กิจกรรมการทหารที่เปลี่ยนแปลงจากสงครามตามแบบแผน (Conventional warfare) มาเป็นสงครามนอกแบบ (Non-conventional Warfare) ที่มีต้นทุนในการดำเนินการที่ต่ำแต่สามารถสร้างความเสียหายได้มากมายและแผ่ขยายไปยังส่วนอื่น ๆ ของกองทัพด้วย แม้อาจไม่ทำให้เกิดความเสียหายอย่างทันทีทันใด แต่เป้าหมายของการจารกรรมไซเบอร์ คือ การไม่ถูกตรวจสอบพบได้นั่นเอง

จากมุมมองทางกฎหมายและการเมืองแล้ว การแยะแยะระหว่างกองกำลังติดอาวุธ การจารกรรม และอาชญากรรมนั้นสำคัญมากต่อการวินิจฉัยสั่งการ เพราะแม้การก่ออาชญากรรมที่มีรัฐเป็นผู้สนับสนุนอยู่เบื้องหลังนั้นไม่ได้ถือเป็นความชอบธรรมในการดำเนินการตอบโต้ทางการทหารภายใต้กฎหมายระหว่างประเทศ หรือการจารกรรมเองก็ไม่ได้สร้างความชอบธรรมในการตอบโต้ด้วยกำลังทหาร แม้ทั้งอาชญากรรมทางคอมพิวเตอร์และการจารกรรมนั้นอาจสร้างความเสียหายได้มากก็ตาม นานาประเทศจะไม่ตัดสินใจก่อสงครามเพราะสาเหตุนี้ หลายประเทศที่สนับสนุนอาชญากรรมประเภทนี้ต่างควบคุมการดำเนินการให้อยู่ภายใต้ระดับที่จะถูกพิจารณาเป็น

---

[204] Hanifah, A., Indonesia to create its own “cyber army”, *Xinhua*, (2013, July 29), Retrieved 2014, April 4, from http://news.xinhuanet.com/english/world/2013-05/29/c_132416837.htm

[205] Milian, M., Indonesia joins China as cyber-attack powerhouse, *Bloomberg*, (2013, July 23), Retrieved 2014, September 9, from http://www.bloomberg.com/news/2013-07-23/indonesia-joins-china-as-cyber-attack-powerhouse.html

การใช้กำลังทางทหารหรือการกระทำที่เป็นการก่อสงคราม (act of war) อย่างไรก็ดี การกระทำมุ่งร้ายผ่านระบบเครือข่ายนั้นสามารถมีลักษณะข้ามชาติได้ ด้วยการดำเนินการจากนักเจาะระบบในประเทศหนึ่งต่อประเทศอื่น ๆ ด้วยเหตุนี้เอง การตอบโต้เชิงป้องกันต่อการจารกรรมข้อมูลหรือการกระทำผิดจึงมีความสลับซ้ำซ้อนมากเนื่องจากอาจไม่มี “ตัวผู้กระทำผิด” ที่มีตัวตนจับต้องได้บ่อยครั้งที่ไม่อาจกักขัง หรือแม้แต่ระบุชี้ชัดได้

กฎหมายระหว่างประเทศได้วางหลักเกณฑ์ไว้กว้าง ๆ ในเรื่องอาชญากรรมทางคอมพิวเตอร์ และยังมีหลักเปรียบเทียบที่เกี่ยวข้องกับอาวุธนอกแบบแผน (Unconventional weapon) นิวเคลียร์ อาวุธชีวภาพ อาวุธเคมี และอาวุธแพร่กัมมันตรังสี ซึ่งอาจใช้เป็นข้ออ้างอิงในการประยุกต์ใช้หลักการทางกฎหมายระหว่างประเทศกับสงครามไซเบอร์ อย่างไรก็ดีปัญหาหลายประการ เช่น ข้อกำหนดในเรื่องสันติภาพและความมั่นคงของกฎบัตรสหประชาชาติจะสามารถประยุกต์ใช้กับ Non-state actor หรือการปฏิบัติต่อกรณีที่ประเทศล่มสลายทางเศรษฐกิจจากการโจมตีไซเบอร์แบบเดียวกับการกระทำด้วยอาวุธทางกายภาพ (Kinetic weapon) ได้หรือไม่

ประเทศสหรัฐอเมริกา จีน และรัสเซีย ได้สร้างระบบข่าวกรองที่กว้างขวางและแผ่ขยายไปทั่วโลกรวมทั้งภูมิภาคเอเชีย นอกจากนี้ยังส่งกองกำลังทางทหารไปประจำการตามภูมิภาคต่าง ๆ สำหรับศักยภาพทางด้านข่าวกรองและการรบบนไซเบอร์สเปซของประเทศสมาชิกอาเซียนนั้นมีความแตกต่างกันมากระหว่างมีแค่ในนามไปจนถึงระดับเชี่ยวชาญ โดยประเทศที่ริเริ่มโครงการเสริมศักยภาพทางการทหารและพัฒนาหลักการทางสงครามไซเบอร์ในอาเซียน ได้แก่ ประเทศมาเลเซีย พม่า บรูไน และ สิงคโปร์ ที่ถือว่าเป็นประเทศแรกๆ ที่ริเริ่มพัฒนาศักยภาพด้านการป้องกันทางไซเบอร์[206] และแม้ว่าในปัจจุบันที่ทุกประเทศในอาเซียนต่างมีหน่วยงานประเภท CERT เพื่อรับมืออาชญากรรมทางคอมพิวเตอร์แล้ว ก็ยังมีข้อกังขาในด้านศักยภาพในการรับมือจากการจู่โจมที่มีความซับซ้อนเป็นระบบที่อยู่ในรูปแบบปฏิบัติการทางทหารซึ่งต่างจากอาชญากรรมทางคอมพิวเตอร์แบบอื่น ๆ ที่รวมไปถึงมาตรการและกฎเกณฑ์ในการตอบโต้และบริหารจัดการในรูปแบบสงครามด้วย ซึ่งหากมีการละเลยต่อการพัฒนาศักยภาพในด้านนี้ อาเซียนจะไม่สามารถพ้นจากภาวะเสียเปรียบทางยุทธศาสตร์ต่อประเทศมหาอำนาจทั้งหลายที่มีศักยภาพทางการรบไซเบอร์ได้ในยุคสมัยที่ทุกภาคส่วนเชื่อมต่อกันด้วยระบบเครือข่ายอินเตอร์เน็ต

อย่างไรก็ตาม จำนวนประเทศที่เริ่มเสริมศักยภาพการรบไซเบอร์ที่เพิ่มมากขึ้นนั้นไม่น่าเป็นห่วงเท่าใดนัก เนื่องจากการจู่โจมไซเบอร์นั้นก็ไม่ได้ต่างจากการมียุทโธปกรณ์ในการรบอื่น

---

[206] Lewis, J. A., & Timlin, K., Cybersecurity and cyberwarfare: Preliminary assessment of national doctrine and organization, *UNIDIR*, Retrieved 2014, August, 17 from http://unidir.org/files/publications/pdfs/cyber security-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf

ๆ เช่น เครื่องบินหรือรถถังที่ในไม่ช้าก็จะกลายเป็นส่วนหนึ่งของกองทัพในทุกประเทศ เพียงแต่การจารกรรมไซเบอร์จะขยายกิจกรรมด้านข่าวกรองทางทหารออกไปสู่พรหมแดนใหม่ซึ่งก็คืออินเตอร์เน็ต และทุกประเทศต่างเฝ้าจับตาอยู่แล้ว ส่วนในกลุ่มประเทศที่มีโครงการแทรกซึมเพื่อสืบราชการลับในต่างประเทศอยู่แล้วก็จะนำเทคนิคทางไซเบอร์นี้ไปปรับใช้ ดังนั้นการเพิ่มเข้ามายุทโธปกรณ์ไซเบอร์จะไม่เปลี่ยนแปลงดุลยอำนาจระหว่างประเทศในอาเซียนมากนัก

5.2.1.4 อาชญากรรมทางคอมพิวเตอร์ประเภทความผิดเกี่ยวกับการหลอกลวง (Social Engineering Scams)

อาชญากรรมทางคอมพิวเตอร์ประเภทความผิดเกี่ยวกับการหลอกลวง มีเกิดขึ้นเป็นจำนวนมาก เช่น การรังควานทางอินเตอร์เน็ต (Online harassment) การตามตื๊อ (Stalking) หรือ การล่อลวงเด็ก (Child grooming) นั้นกระทำได้ง่ายมากขึ้นผ่านเว็บเครือข่ายสังคมออนไลน์ซึ่งเป็นที่แพร่หลายทั่วโลกในปัจจุบัน (เช่น Facebook เป็นต้น) บริการเหล่านี้เป็นประโยชน์ในการเข้าสังคมและสร้างโอกาสทางธุรกิจ แต่ด้วยระบบที่ด้อยประสิทธิภาพในการคุ้มครองผู้ใช้ที่อยู่ในกลุ่มเสี่ยงและรู้เท่าไม่ถึงการณ์อย่างเด็ก ๆ ทำให้การใช้งานสื่อสังคมออนไลน์นั้นสุ่มเสี่ยงต่อภัยอันตรายที่อาจเกิดกับเด็กหรือผู้ใช้ที่รู้เท่าไม่ถึงการณ์ ความใส่ใจและการออกกฎหมายเพื่อดูแลบริการประเภทนี้ด้วยความร่วมมือจากภาคเอกชนนั้นจำเป็นต่อความปลอดภัยสาธารณะ จากเหตุที่เกิดขึ้นเหล่านี้อาจกระตุ้นให้ทั้งภาครัฐและเอกชนได้เล็งเห็นถึงความสำคัญในการเชื่อมโยงฐานข้อมูลอาชญากรเข้าด้วยกันอย่างเป็นระบบ สำหรับประเด็นที่สำคัญและเป็นกังวลในเรื่องอาชญากรรมทางคอมพิวเตอร์ประเภทความผิดเกี่ยวกับการหลอกลวงนี้ คือ ข้อโต้แย้งในเรื่องความเป็นส่วนตัวนั้นมักจะละเลยความปลอดภัยของผู้ที่เป็นเหยื่ออาชญากรรม

ในปี พ.ศ. 2554 บริษัทด้านการรักษาความปลอดภัยระบบคอมพิวเตอร์ Symantec เปิดเผยข้อมูลว่า จากคอมพิวเตอร์ซึ่งใช้บริการของบริษัทกว่า 133 ล้านเครื่องมีรายงานการตรวจพบโปรแกรมมุ่งร้ายประเภท ไวรัสคอมพิวเตอร์ หนอนไวรัสคอมพิวเตอร์ และบอทเน็ท[207] ซึ่งโปรแกรมประเภทดังกล่าวถูกแพร่กระจายผ่านเทคนิคการหลอกลวง (Social engineering techniques) ซึ่งเป็นวิธีการตบตาโดยทำให้เหยื่อเกิดความเชื่อถือเพื่อขโมย ข้อมูลการเชื่อมต่อ เช่น การสร้างเว็บไซต์ซึ่งมีหน้าตาเหมือนกับเว็บไซต์บริการต่าง ๆ เพื่อหลอกให้ผู้ใช้กรอกข้อมูลเพื่อแพร่สแปมหรืออีเมล์หลอกลวงต่อไปเป็นทอด ๆ โดยกลุ่มอาชญากรจะทำการบุกรุกเข้าระบบ

---

[207] Symantec, *Symantec internet security threat report trends for 2010*, (2011, April), Retrieved 2014, August 17, from https://www4.symantec.com/mktginfo/downloads/ 21182883_GA_REPORT_ISTR_Main-Report_04-11_HI-RES.pdf

เครือข่ายเพื่อขโมยข้อมูลสำคัญ เช่น รหัสผ่านหรือข้อมูลระบุตัวตน ซึ่งกระบวนการดังกล่าวอาจใช้เพื่อก่ออาชญากรรมทางการเงินซึ่งก่อความเสียหายในวงกว้าง

ความผิดเกี่ยวกับการหลอกลวงนี้นับเป็นวิธีการที่ได้ผลเป็นอย่างมากสำหรับอาชญากรในการเข้าถึงข้อมูลบนอุปกรณ์พกพาหรือคอมพิวเตอร์ โดยการกระทำผิดประเภทนี้จะรวมเอาทั้งการกระทำผิดประเภทบุกรุกซึ่งใช้ความเชี่ยวชาญทางคอมพิวเตอร์รวมไปกับการใช้จิตวิทยาในการหลอกให้เหยื่อหลงเชื่อรับเอาโปรแกรมที่เป็นอันตราย (malware) เข้ามาในเครื่องของตนโดยไม่รู้ตัว โดยวิธีการของอาชญากรอาจแตกต่างกันไปตั้งแต่การใช้ Spyware, phishing rootkits หรือ botnet เพื่อแฝงเข้าไปยังเครื่องของเหยื่อ การแพร่โปรแกรมที่เป็นอันตรายเหล่านี้จะมีประสิทธิภาพยิ่งขึ้นเมื่อตัวอาชญากรเข้าถึงเหตุการณ์ที่เกิดขึ้นและลักษณะของวัฒนธรรมในประเทศนั้น ๆ และทำให้การหลอกลวงได้ผลยิ่งขึ้น เช่น การหลอกลวงประเภทนี้ในประเทศจีนจะเป็นการหลอกว่าเหยื่อถูกลอตเตอรี่ หรือโปรแกรมมุ่งร้ายบางตัวถูกออกแบบให้มุ่งเป้าไปยังเว็บไซต์ที่เป็นภาษาจีนและมักซ่อนเร้นไว้ด้วยเนื้อหาที่ทำให้เกิดความรู้สึกรักชาติ เป็นต้น

แนวโน้มของพัฒนาการด้านภัยคุกคามด้วยการใช้ปัญญาของมนุษย์แทนการใช้ปัญญาประดิษฐ์นั้นเป็นที่น่าสนใจเพราะความผิดเกี่ยวกับการหลอกลวง (Social engineering scam) ซึ่งอาศัยมนุษย์เป็นเสาหลักในการดำเนินการสามารถเข้าถึงข้อมูลได้หลากหลายในขณะที่การใช้งานโปรแกรมเพียงอย่างเดียวไม่สามารถกระทำได้

ปัจจุบันในประเทศสมาชิกอาเซียน อาชญากรรมทางคอมพิวเตอร์ประเภทความผิดเกี่ยวกับการหลอกลวง (Social engineering scam) ได้เริ่มทวีความรุนแรงมากยิ่งขึ้น จากการขโมยบัญชีผู้ใช้อีเมล์เพื่อส่งแสปมไปจนถึงการก่ออาชญากรรมทางการเงินที่ร้ายแรง เมื่อการทำธุรกรรมอิเล็กทรอนิกส์ประเภท Electronic banking เป็นที่นิยมมากยิ่งขึ้น เช่น ในประเทศไทยอาชญากรจะทำการส่งข้อความหรืออีเมล์ลวงให้ผู้ใช้เข้าไปเปลี่ยนรหัสผ่านในหน้าเว็บที่ทำไว้ Phishing และส่ง SMS OTP (One time password; รหัสผ่านครั้งเดียว)[208] ปลอมให้แก่ผู้ใช้เพื่อทำการ Verify รหัสผ่านเข้าใช้ครั้งเดียวของทางธนาคาร หรือ นำข้อมูลบัญชีผู้ใช้และรหัสผ่านของเหยื่อซึ่งได้จากการจารกรรมมาติดต่อกับธนาคารด้วยเอกสารปลอมเพื่อโอนเงินออกจากบัญชีของเหยื่อ[209] เป็นต้น ในปัจจุบันกฎหมายอาชญากรรมทางคอมพิวเตอร์ในประเทศสมาชิกอาเซียนซึ่งส่วนใหญ่อาศัย

---

[208] One Time Password (OTP) หรือ Secure ID Solutions คือ เครื่องมือที่ใช้ในการสร้างรหัสผ่าน หรือ Password ในการ Log-In เข้าสู่ระบบต่าง ๆ เช่น VPN , E-Mail Server , File Server , Active Directory , Radius ฯลฯ โดยรหัสผ่านที่สร้างนั้น จะสามารถใช้ได้ครั้งเดียวเท่านั้น และจะทำการสุ่มรหัสผ่านใหม่ในทุกนาที โดยระบบดังกล่าวจะสามารถเพิ่มระดับความปลอดภัยของระบบหากเปรียบเทียบกับการใช้รหัสผ่านแบบเดิมซึ่งเป็นแบบกำหนดตายตัว.

[209] Pantip, *เตือนภัย Internet Banking รูปแบบใหม่ ปลอมเป็นตัวคุณ (Clone) แล้วสวมรอยโอนเงินออกไปอย่างง่ายดาย*, สืบค้นเมื่อ 10 สิงหาคม 2557, จาก http://pantip.com/topic/30799070

อนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์เป็นแม่แบบ นั้นครอบคลุมในส่วนของกฎหมายสารบัญญัติ ความผิดประเภทฉ้อโกง (Computer-related Fraud) แต่มาตรการทางกฎหมายที่จำเป็นในการสืบสวนหาผู้กระทำผิดและดำเนินคดียังไม่สามารถจัดการกับอาชญากรรมที่มีลักษณะเป็นระบบเช่นนี้ได้อย่างมีประสิทธิภาพมากนัก ความร่วมมือระหว่างประเทศในด้านการสืบสวนและจับกุมผู้กระทำผิดที่ชัดเจนและเป็นมาตรฐานเดียวกันทั้งภูมิภาคจึงมีความจำเป็นอย่างมากในการรับมืออาชญากรรมทางคอมพิวเตอร์ประเภทนี้

5.2.1.5 การควบคุมเนื้อหา (Content regulation)

ประเทศสมาชิกอาเซียนส่วนใหญ่มีกฎหมายควบคุมเนื้อหาที่ได้รับการเผยแพร่บนอินเตอร์เน็ต โดยมีพื้นฐานอยู่บน สภาพสังคม การเมือง ศีลธรรม ความเชื่อทางศาสนา ของรัฐบาลแต่ละประเทศโดยเป็นการควบคุมที่มีลักษณะใกล้เคียงกับการควบคุมสื่อสิ่งพิมพ์ และยิ่งมีการใช้งานอินเตอร์เน็ตมากขึ้นเรื่อย ๆ การควบคุมเนื้อหาของรัฐบาลแต่ละประเทศต่างสะท้อนออกมาในเชิงการให้คุณค่าทางศีลธรรม และสถานะทางการเมืองของประเทศนั้นชัดเจนมากขึ้น ในประเทศสมาชิกอาเซียนที่มีระดับการพัฒนาสูงจะมีการควบคุมเนื้อหาที่รัดกุม เนื่องจากรัฐบาลมีความพยายามที่จะควบคุมการเข้าถึงเนื้อหาที่ผิดกฎหมายอย่างเช่น สื่อลามกอนาจารเด็ก สื่อที่มีเนื้อหาดูหมิ่นชาติพันธุ์ หรือสื่อที่เผยแพร่ข้อมูลอันขัดต่อความสงบเรียบร้อยของสาธารณะแก่ประชาชนซึ่งการควบคุมเนื้อหาที่ถูกเผยแพร่ออนไลน์นั้น นโยบายของรัฐมีบทบาทสำคัญในการสร้างกรอบข้อบังคับที่ชัดเจน สำหรับกลุ่มประเทศสมาชิกอาเซียนที่ระดับการพัฒนาน้อยอาจต้องใช้เวลาจนกว่าการสร้างโครงสร้างพื้นฐานทาง ICT จะมั่นคงและประชาชนเข้าถึงการใช้งานอินเตอร์เน็ตมากขึ้น

ความผิดประเภทเนื้อหานี้ก็เป็นเช่นเดียวกับอาชญากรรมทางคอมพิวเตอร์ประเภทบุกรุกเพราะในภูมิภาคเอเชียที่เกี่ยวข้องกับการเมืองนั้นพบได้ทั่วไปว่า การเซ็นเซอร์เนื้อหาทางอินเตอร์เน็ตและไมโครบลอกนั้นเกิดขึ้นอย่างต่อเนื่องในแทบทุกประเทศสมาชิกอาเซียน กฎหมายว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของแต่ละประเทศดูเหมือนจะมุ่งเน้นไปที่การกลั่นกรองเนื้อหาออนไลน์ กฎหมายบางประเทศถูกต่อต้านโดยภาคประชาชนเป็นอย่างมากเช่น Cybercrime prevention Act 2012 ของประเทศฟิลิปปินส์ซึ่งถูกศาลสั่งระงับชั่วคราว โดยแนวโน้มของการกลั่นกรองเนื้อหาทางการเมืองผ่านการใช้กฎหมายสารสนเทศหรืออาชญากรรมทางคอมพิวเตอร์นั้นสูงมาก โดยจะเห็นได้ว่า ร่างพระราชบัญญัติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ของประเทศไทย ที่ได้เพิ่มเหตุผลซึ่งรัฐจะสามารถทำการปิดกั้นการเข้าถึงเว็บไซต์ โดยขยายไปถึงความผิดในกฎหมายอื่น ๆ ที่ใช้คอมพิวเตอร์เป็นเครื่องมือได้ด้วย ประเทศเวียดนามเองก็กำหนดให้ผู้ให้บริการรับส่งข้อมูลทางอินเตอร์เน็ตต้องเป็นไปตามที่รัฐบาลกำหนด และตัวผู้ให้บริการจะต้องรับผิดทางกฎหมายในเนื้อหาที่ตนเองสร้างขึ้นโดยองค์กรของรัฐจะมีการตรวจตราเนื้อหาดังกล่าวอย่าง

ต่อเนื่อง รัฐบาลเวียดนามทำการปิดกั้นการเข้าถึงเว็บไซต์ที่ทำการวิพากษ์วิจารณ์รัฐบาล เว็บไซต์ของพรรคการเมือง พรรคการเมืองที่ถูกเนรเทศ และองค์กรสิทธิมนุษยชนระหว่างประเทศ

นอกจากนี้ บางประเทศสมาชิกของอาเซียนยังได้กำหนดให้เนื้อหาที่เป็นการดูหมิ่นชาติพันธุ์ (Racism) และดูหมิ่นศาสนา (Blasphemy) เป็นความผิดตามกฎหมายภายใน เช่น ประเทศมาเลเซีย อินโดนีเซียและสิงคโปร์ ซึ่งประกอบด้วยประชากรหลายเผ่าพันธุ์มักเกิดปัญหาเกี่ยวกับการเหยียดเชื้อชาตินี้ขึ้น แม้แต่พม่าซึ่งมีเหตุการณ์ความไม่สงบในรัฐยะไข่ซึ่งชาวพุทธไล่ทำร้ายชาวมุสลิม ระบบอินเตอร์เน็ตซึ่งมีสื่อสังคมที่ผู้คนมารวมตัวกันได้เป็นจำนวนมากจึงสุ่มเสี่ยงต่อการเผยแพร่เนื้อหาที่อาจก่อให้เกิดความขัดแย้งในเชื้อชาติ บางประเทศเช่นประเทศสิงคโปร์มีกฎหมาย Sedition Act ที่กำหนดให้เนื้อหาประเภทดูหมิ่นชาติพันธุ์หรือศาสนาเป็นความผิด ซึ่งมีบล็อกเกอร์หลายรายได้รับโทษในกรณีโพสท์ข้อความซึ่งขัดกับมาตรา 3.1(e) ของกฎหมายฉบับนี้ ที่กำหนดให้ผู้เผยแพร่เนื้อหาที่ส่งเสริมความรู้สึกมุ่งร้ายระหว่างชาติพันธุ์หรือชนชั้นของประชาชนสิงคโปร์[210] มีความผิดตามกฎหมาย อย่างไรก็ดี กฎหมายประเภทนี้ยังไม่เป็นที่แพร่หลายในอาเซียน แม้ในหลายประเทศ เช่นประเทศมาเลเซียซึ่งมีการแบ่งแยกด้านชนชั้นในสังคมชัดเจนระหว่างสิทธิประโยชน์ที่รัฐบาลให้แก่ชาวมาเลย์ดั้งเดิมและชาวมาเลย์เชื้อสายจีนก็ตาม

อย่างไรก็ตาม ประเทศสมาชิกอาเซียนไม่เพียงออกกฎหมายเพื่อควบคุมเนื้อหาที่เกี่ยวข้องกับการเมือง แต่เนื้อหาลามกอนาจารก็ยังถือเป็นความผิดอีกด้วย การเผยแพร่สื่อลามกอนาจารโดยเฉพาะสื่อลามกอนาจารเด็กได้ถูกระบุไว้ในกฎหมายอาชญากรรมทางคอมพิวเตอร์ของประเทศสมาชิกอาเซียนแทบทุกประเทศแล้วด้วยเช่นกัน ตัวอย่างเช่นในร่างกฎหมายพระราชบัญญัติความผิดเกี่ยวกับคอมพิวเตอร์ของประเทศไทยกำหนดให้เพียงแค่มีในครอบครองซึ่งสื่อลามกอนาจารเด็กก็เป็นความผิดแล้ว อย่างไรก็ดีข้อสรุปในเรื่องขอบเขตของสื่อลามกยังแตกต่างกันไปในแต่ละประเทศสมาชิกอาเซียน โดยประเทศมุสลิมนั้นมีข้อจำกัดที่เข้มงวดที่สุดในเรื่องนี้ โดยอาจถือว่าการเปลือยทุกรูปแบบจัดเป็นสื่อลามกอนาจารทั้งสิ้น

ทั้งนี้ ประเทศสมาชิกอาเซียนต่างพยายามปิดกั้นเนื้อหาผิดกฎหมายผ่านการปิดกั้นและขึ้นบัญชีดำ (Blacklisted) เว็บไซต์ ประเภทสื่อลามกอนาจารและเนื้อหาทางการเมือง อย่างไรก็ดี ความพยายามปิดกั้นใด ๆ โดยรัฐไม่อาจหยุดการเข้าถึงสื่อเหล่านี้ของประชาชนได้ เนื่องจากมี

---

[210] Sedition Act, Chapter 290--3.1 A seditious tendency is a tendency

(e) to promote feelings of ill-will and hostility between different races or classes of the population of Singapore.

เครื่องมือหลายประเภทที่สามารถใช้เพื่อ bypass การปิดกั้นของรัฐเช่นบริการพร็อกซี่ (Proxy) ฟรีบนอินเตอร์เน็ต หรือเบราเซอร์ (Browser) ที่ทำหน้าที่เป็นพร็อกซี่อย่าง Tor[211] เป็นต้น

5.2.1.6 เครือข่ายสังคมออนไลน์ (Social networks)

เครือข่ายสังคมออนไลน์เป็น platform เพื่อสร้างเครือข่ายความสัมพันธ์ระหว่างผู้คนซึ่งแลกเปลี่ยนความสนใจ พื้นเพ กิจกรรม หรือแม้แต่การดำเนินชีวิตจริงร่วมกัน การกระทำผิดส่วนใหญ่บนเครือข่ายสังคมออนไลน์อาจครอบคลุมโดยกฎหมายอาญาดั้งเดิม แต่ไม่เพียงพอเสมอไป พัฒนาการของพฤติกรรมที่ก่อให้เกิดความเสี่ยงภัยบนเครือข่ายสังคมออนไลน์ต้องถูกจับตาดูอย่างใกล้ชิด หากมีกรณีที่เป็นประเด็นทางกฎหมายที่ต้องดูแลเป็นพิเศษและต้องการความคุ้มครองโดยกฎหมายอาญา การออกมาตรการพิเศษเกี่ยวกับเรื่องนี้อาจมีความจำเป็น เพราะกรณีดังกล่าวอาจกลายเป็นเรื่องระดับโลก และถูกนำเข้าเป็นส่วนหนึ่งในสนธิสัญญาในอนาคตได้ นอกจากนี้ การบังคับใช้กฎหมายในปัจจุบัน หากทำการร้องขอข้ามเขตแดนอาจทำได้ช้าและมีกระบวนการที่ซับซ้อนวุ่นวายมาก โดยเฉพาะคำร้องเกี่ยวกับเครือข่ายสังคมออนไลน์บนอินเตอร์เน็ต ยกตัวอย่างคดีฆาตกรรมร้ายแรงที่สุดในปี พ.ศ. 2554 ซึ่งประชาชนกว่า 68 คนถูกสังหารอย่างเหี้ยมโหดในนอร์เวย์รวมไปถึงความเสียหายของสิ่งปลูกสร้างของรัฐสามแห่งและคนอีก 9 คนที่ต้องสังเวยชีวิต[212] ซึ่งกว่า Facebook จะตอบสนองต่อคำร้องขอหลักฐานก็เมื่อการพิจารณาคดีเริ่มขึ้นในกรุงออสโล เมื่อเดือนเมษายน พ.ศ. 2555 โดยคำร้องขอได้ถูกส่งไปหลายเดือนก่อนหน้านั้นแล้ว

5.2.1.7 ลิขสิทธิ์ในเนื้อหาดิจิตอล (Digital content copyright)

ประเทศสมาชิกอาเซียนทุกประเทศมีกฎหมายที่ทำการคุ้มครองลิขสิทธิ์ อย่างไรก็ดี การคุ้มครองลิขสิทธิ์ในรูปแบบดิจิตอลนั้นแตกต่างกันออกไปในแต่ละประเทศสมาชิก บางประเทศมีการกำหนดอย่างชัดเจนในเรื่องความครอบคลุมของการคุ้มครองลิขสิทธิ์บนอินเตอร์เน็ต แต่บาง

---

[211] Tor สร้างโดยกลุ่มอาสาสมัครผู้เชี่ยวชาญด้านเทคนิค มีจุดประสงค์ต้องการต่อต้านการวิเคราะห์เครือข่าย (Network Analysis) ที่คุกคามอิสระและความเป็นส่วนตัวของผู้ใช้ Internet ทั่วโลก ดังนั้น Tor จึงได้รับการออกแบบมาพิเศษ ไม่เหมือนกับโปรแกรม Proxy ทั่วไป มีการเข้ารหัส (Encrypt) ข้อมูลทุกอย่างที่เราจะส่งไปหาเว็บปลายทาง เพื่อป้องกันการดักอ่านและปลอมแปลงข้อมูลระหว่างทาง ระหว่างที่โปรแกรมทำงาน Tor จะเลือกสุ่ม Proxy Servers ประมาณ 3-4 เครื่องจาก Tor Servers ทั่วโลกมาให้เราใช้งาน โดยเชื่อมโยงเครื่องเหล่านี้เข้าด้วยกันเป็นวงจร (Circuit) ผลที่ได้ก็คือระหว่างที่โปรแกรมทำงาน Tor จะเลือกสุ่ม Proxy Servers ประมาณ 3-4 เครื่องจาก Tor Servers ทั่วโลกมาให้เราใช้งาน โดยเชื่อมโยงเครื่องเหล่านี้เข้าด้วยกันเป็นวงจร (Circuit) ผลที่ได้ก็คือ วงจรที่ว่านั้น Tor จะสุ่มเลือกวงจรใหม่ให้เรา เมื่อเราเปลี่ยนเว็บปลายทาง หรือสุ่มใหม่ตามช่วงเวลาประมาณ 10 นาที ทำให้ข้อมูลของเราวิ่งผ่านวงจรหลายวงจร ทำให้ยากต่อการติดตามเป็นอย่างยิ่ง, IZONE, *การท่องเว็บแบบปกปิดตัวตน ตอนที่ 7 (Tor)*, สืบค้นเมื่อ 11 สิงหาคม พ.ศ.2557, จาก http://izonex.wordpress.com/2008/10/26/anoymous-software-tor/

[212] Huffingtonpost, *Norway Attacks: Police Lower Youth Camp Death Toll To 68*, Retrieved 2014, August 17, from http://www.huffingtonpost.com/2011/07/25/norway-attacks-police_n_908647.html

ประเทศก็ไม่พัฒนากฎหมายมากไปกว่าการให้ความหมายว่าลิขสิทธิ์มีอยู่ในโปรแกรมคอมพิวเตอร์และการให้สิทธิที่เกี่ยวข้องเพียงเท่านั้น ดังนั้น ประเทศสมาชิกอาเซียนจึงมีกฎหมายลิขสิทธิ์เดิมที่สามารถนำมาปรับใช้กับเนื้อหาบนอินเตอร์เน็ตได้ในระดับหนึ่ง

5.2.1.8 สแปม (Spam)

ในปัจจุบันมีเพียงประเทศสิงคโปร์และเวียดนามที่ได้ออกกฎหมายต่อต้านสแปมมาบังคับใช้แล้ว มาเลเซียมีบทบัญญัติกฎหมายใกล้เคียงที่อาจใช้ดำเนินคดีกับผู้ปล่อยสแปมได้บ้างแต่อยู่ในขอบเขตที่จำกัด[213] สำหรับประเทศไทยมีมาตรา 11 ของพระราชบัญญัติการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ที่บัญญัติให้ผู้ส่งจดหมายอิเล็กทรอนิกส์โดยไม่เปิดเผยชื่อผู้ส่งมีความผิด ซึ่งยังไม่มีความครอบคลุมถึงลักษณะอันหลากหลายของสแปม ดังนั้น จึงมีการแก้ไขปรับปรุงร่างพระราชบัญญัติความผิดทางคอมพิวเตอร์ปี พ.ศ. 2556 ขึ้นใหม่ว่า ให้การส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เปิดโอกาสให้ผู้รับแจ้งบอกเลิกหรือปฏิเสธการรับ ถือว่ามีความผิด แต่ยังไม่ได้มีผลบังคับใช้เนื่องจากยังอยู่ในขั้นตอนการยกร่างกฎหมาย ส่วนประเทศฟิลิปปินส์ได้บัญญัติความผิดเกี่ยวกับสแปมไว้ใน Cybercrime prevention act 2012

5.2.1.9 เขตอำนาจศาล (Jurisdiction)

ประเด็นเรื่องเขตอำนาจศาลเป็นอุปสรรคที่สำคัญในการปรับใช้กฎหมายอาชญากรรมทางคอมพิวเตอร์ สำหรับองค์กรระหว่างประเทศที่พยายามสร้างความสอดคล้องของกรอบโครงสร้างทางกฎหมายที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ ประเด็นเรื่องเขตอำนาจศาลบนเครือข่ายอินเตอร์เน็ตถือว่ามีความสำคัญเป็นอย่างมาก อย่างไรก็ดี ปัญหาดังกล่าวยังไม่มีทางออกที่เหมาะสม ไม่เฉพาะแต่ในองค์การอาเซียนแต่รวมถึงองค์กรระหว่างประเทศอื่น ๆ ทั่วโลกอีกด้วย

การที่จะบรรลุถึงความสอดคล้องของเขตอำนาจศาลและกฎหมายว่าด้วยอาชญากรรมทางคอมพิวเตอร์นั้น การบูรณาการของหลักเกณฑ์กลางทางกฎหมายถือว่ามีความสำคัญต่ออาเซียนอย่างมากในโครงการหลายโครงการที่อาเซียนจัดขึ้นและได้ทำการศึกษาเกี่ยวกับพัฒนาการของความร่วมมือระหว่างประเทศนี้ รวมไปถึงการพัฒนาด้านการสร้างความสอดคล้องของเขตอำนาจศาลในสหภาพยุโรป และ OECD และที่ประชุมแห่งกรุงเฮกว่าด้วยกฎหมายระหว่างประเทศแผนกคดีบุคคล (Hague Conference on Private International law) อีกทั้งยังพิจารณากฎหมายประเภท case law และตัวอย่างในเรื่องแนวทางปฏิบัติต่อเขตอำนาจศาลบนอินเตอร์เน็ตจากประเทศออสเตรเลีย

---

[213] the Malaysia Communications and Multimedia Act 1998 (Act 588), Section 233 “provides that a person who initiates a communication using any applications service, whether continuously, repeatedly or otherwise, during which communication may or may not ensue, with or without disclosing his identity and with intent to annoy, abuse, threaten or harass any person at any number or electronic address commits an offence”.

และญี่ปุ่น[214] อีกด้วย อย่างไรก็ตาม ณ ขณะนี้ยังไม่มีข้อสรุปที่ชัดเจนในเรื่องเขตอำนาจศาล ดังนั้น การที่จะสร้างคู่มือเพื่อกำหนดแนวทางปฏิบัติในเรื่องเขตอำนาจศาลที่กระตุ้นให้ประเทศสมาชิกอาเซียนนำเอาไปปฏิบัติอย่างเป็นอันหนึ่งอันเดียวกันจึงมีความสำคัญเพื่อที่จะใช้เป็นทางออกในการสร้างความชัดเจนให้กับหลักเกณฑ์ปฏิบัติระหว่างประเทศในเรื่องนี้

นอกจากนี้ ประเด็นสำคัญอีกประเด็นหนึ่งที่เป็นอุปสรรคในด้านความร่วมมือข้ามเขตอำนาจศาลในด้านอาชญากรรมทางคอมพิวเตอร์ คือ การยอมให้มีการเข้าถึงข้อมูลข้ามเขตแดน (Trans-border access to stored computer data) ซึ่งรวมไปถึงการตรวจจับและเก็บข้อมูลการจราจรอิเล็กทรอนิกส์แบบ Real-time โดยไม่จำเป็นต้องผ่านการอนุญาตจากประเทศปลายทางก่อน ซึ่งเป็นองค์ประกอบสำคัญในการติดตามสืบสวนหาต้นตอของการก่ออาชญากรรม และมีความสำคัญต่อการสงวนรักษาข้อมูลคอมพิวเตอร์ที่เป็นพยานหลักฐานซึ่งมีการเปลี่ยนแปลงอย่างรวดเร็วได้อย่างทันท่วงที โดยมีความกังวลกันว่าการยินยอมตามหลักการดังกล่าวจะเป็นการยอมให้เกิดการล่วงล้ำอำนาจอธิปไตยจากชาติอื่นขึ้น แต่อย่างไรก็ตาม ด้วยปัญหาอาชญากรรมทางคอมพิวเตอร์ที่ทวีความรุนแรงขึ้นเรื่อย ๆ ประเทศอินโดนีเซียซึ่งนับเป็นประเทศซึ่งมีอัตราการส่ง Attack traffic มากที่สุดในประเทศสมาชิกอาเซียนได้เตรียมยกร่างกฎหมายในด้านความร่วมมือดังกล่าวแล้ว นอกจากนี้ ยังมีการประมวลผลแบบกลุ่มเมฆ (Cloud computing) เนื่องจากธรรมชาติของการประมวลผลแบบกลุ่มเมฆและอาชญากรรมที่อยู่ภายใต้หลายเขตอำนาจศาล (Multi-Jurisdictional crime) ได้กลายมาเป็นอุปสรรคที่สำคัญในกระบวนการสืบสวนสอบสวนและตัดสินคดีความ เนื่องจากข้อมูลใน Cloud นั้นจะถูกเคลื่อนย้ายจาก Server หนึ่งไปยังอีกเซิฟเวอร์หนึ่งอยู่เรื่อย ๆ เคลื่อนเข้าออกระหว่างประเทศต่าง ๆ อยู่ตลอดเวลา อีกทั้งข้อมูลใน cloud อาจถูกคัดลอกด้วยเหตุผลทางความปลอดภัยหรือความพร้อมให้บริการของข้อมูลนั้น ๆ ทำให้อาจพบข้อมูลหนึ่งในหลายสถานที่ภายในประเทศหนึ่งหรือในหลายประเทศก็ได้ ซึ่งแม้แต่ผู้ให้บริการเองก็ไม่อาจระบุได้แน่ชัดว่าข้อมูลที่ถูกเรียกมาอยู่ที่ใดบ้าง[215] ในอาเซียนนี้ประเทศสิงคโปร์ถือว่าเป็นประเทศที่เริ่มร่างยุทธศาสตร์และนโยบายใจการจัดการปัญหานี้เป็นประเทศแรก

---

[214] ASEAN E-Commerce Project, *Documented analysis of international activity in electronic contracting and Online Dispute Resolution (ODR)–Discussion paper 4 (DP4)*, ASEAN secretariat and Galexia, (internal project materials), May 2006.

[215] Schjolberg, *An international criminal tribunal for cyberspace*, A paper for the EastWest Institute (EWI) Cybercrime Legal Working Group, (2012, March), Retrieved 2014, August 13, from http://www.cybercrime law.net/documents/ICTC.pdf

5.2.2 ปัญหาการปรับใช้อนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ภายในภูมิภาคอาเซียน (Cybercrime Convention Application in ASEAN)

ปัจจุบันองค์ประกอบของการกระทำผิดที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์ทั้งหมดนั้นไม่ครอบคลุมในทุกขอบเขตอำนาจทางกฎหมาย ซึ่งถือว่าเป็นปัญหาที่สำคัญในกระบวนการยุติธรรมที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ เพราะบ่อยครั้งที่ตัวผู้กระทำผิด ผู้เสียหาย และหลักฐานกระจัดกระจายอยู่ในเขตอำนาจศาลที่ต่างกัน ดังนั้นความร่วมมือระหว่างประเทศทางกฎหมายจึงเป็นที่ต้องการอย่างมากเพื่อดำเนินการสืบสวนและดำเนินคดีที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์

อนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของสหภาพยุโรป ปี ค.ศ. 2001 หรือที่รู้จักกันในนาม อนุสัญญาบูดาเปสต์ นั้นเป็นเพียงอนุสัญญาฉบับเดียวในปัจจุบัน ซึ่งเป็นข้อตกลงในระดับนานาชาติ (Multi-national agreement) ที่ให้ช่องทางในการดำเนินคดีกับอาชญากรคอมพิวเตอร์และแสดงให้เห็นถึงความพยายามในการควบคุมไซเบอร์สเปซ โดยสภายุโรปได้ร่างอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์นี้ เพื่อที่จะประสานกฎหมายอาญาและกระบวนการยุติธรรมระหว่างประเทศในสหภาพยุโรปเพื่อดำเนินคดีกับอาชญากรคอมพิวเตอร์ ซึ่งจุดเริ่มต้นในเรื่องนี้อาจย้อนหลังไปในปี พ.ศ. 2532 เมื่อสภายุโรปตีพิมพ์ชุดข้อแนะนำ (Recommendations) ในเรื่องความจำเป็นในการมีกฎหมายอาญาที่กฎหมายสารบัญญัติ เพื่อกำหนดบทลงโทษทางอาญาให้แก่การกระทำที่เป็นอันตรายต่อกระทำที่ผ่านระบบเครือข่ายคอมพิวเตอร์ โดยในปี พ.ศ. 2540 สภายุโรปได้จัดให้มีคณะกรรมาธิการที่ประกอบไปด้วยผู้เชี่ยวชาญทางด้านอาชญากรรมบนไซเบอร์สเปซในการร่างอนุสัญญาเพื่ออำนวยความสะดวกในด้านความร่วมมือระหว่างประเทศในการสืบสวนและดำเนินคดีอาชญากรรมทางคอมพิวเตอร์ และให้ทางออกในปัญหาอาชญากรรมทางคอมพิวเตอร์ผ่านการรับเอาเครื่องมือทางกฎหมายระหว่างประเทศไปใช้ และเมื่อเดือนพฤศจิกายน ปี พ.ศ. 2544 อนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ได้ลงนามและมีผลบังคับใช้ในเดือนกรกฎาคม พ.ศ. 2547 หลังจากลงนามครบ 5 ประเทศซึ่งเป็นมาตรฐานขั้นต่ำ

นอกเหนือจากส่วนของกฎหมายสารบัญญัติซึ่งกำหนดองค์ประกอบและนิยามความผิดทั่วไปแล้ว ส่วนของกฎหมายวิธีสบัญญัติของอนุสัญญานี้ก็มุ่งไปที่การทำให้มีกระบวนวิธีสบัญญัติร่วมกันในเรื่องกฎหมายอาชญากรรมทางคอมพิวเตอร์ และปรับใช้มาตรการรับมือกับอาชญากรรมทั่วไป เช่น การสืบค้นและยึด รวมไปถึงมาตรการใหม่ ๆ เช่นการเก็บรักษาข้อมูล เนื่องจากข้อมูลในอินเตอร์เน็ตนั้นมีความเป็นพลวัตรเปลี่ยนแปลงอยู่ตลอดเวลา ดังนั้น การเก็บข้อมูลจราจรอิเล็กทรอนิกส์ หรือการดักจับเนื้อหาของข้อมูล ก็มีการปรับปรุงเพื่อให้มีการเก็บข้อมูลอิเล็กทรอนิกส์ในระหว่างกระบวนการสื่อสารระหว่างตำรวจหรือผู้ให้บริการ โดยการเก็บข้อมูล

แบบจราจรอิเล็กทรอนิกส์ แบบ real-time และการดับจับเนื้อหาข้อมูลนี้ นับเป็นอำนาจที่ล่วงล้ำที่สุดของอนุสัญญา[216]

หลายประเทศในเอเชียตะวันออกเฉียงใต้ได้รับเอาหลักการในอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์มาปรับใช้แม้ว่าจะไม่มีประเทศสมาชิกอาเซียนใดเลยได้ลงนามในอนุสัญญาฉบับนี้ อันเนื่องมาจากหลายสาเหตุด้วยกัน ซึ่งจะกล่าวถึงต่อไปในบทนี้ แต่อย่างไรก็ตาม แม้ว่าจะไม่มีการลงนามในอนุสัญญาฉบับนี้ แต่หลายประเทศได้ยอมรับว่าได้นำเอาหลักเกณฑ์ต่าง ๆ ในอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์มาปรับใช้กับกฎหมายภายในประเทศ เช่น ประเทศฟิลิปปินส์ ซึ่งได้กล่าวในการประชุม ARF Cybercrime capacity-building conference[217] ว่าได้ปฏิบัติตามหลักเกณฑ์ของอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ในการออกนโยบายและวางยุทธศาสตร์เพื่อรับมือกับอาชญากรรมทางคอมพิวเตอร์

แม้ว่าอนุสัญญาบูดาเปสต์นี้ได้รับการยอมรับว่าเป็นอนุสัญญาที่ครอบคลุมระดับโลกในเรื่องอาชญากรรมทางคอมพิวเตอร์โดยองค์การสหประชาชาติ[218] บางประเทศยังมองว่าอนุสัญญาบูดาเปสต์เป็นเพียงอนุสัญญาที่ครอบคลุมในระดับภูมิภาคเท่านั้น แม้ว่าตัวอนุสัญญาจะไม่บังคับให้ประเทศในภูมิภาคเท่านั้นลงนามเข้าร่วม แต่มีเพียงออสเตรเลีย ญี่ปุ่น และสหรัฐอเมริกาเท่านั้นซึ่งเป็นประเทศนอกยุโรปที่ลงนาม[219]

การปรับใช้หลักเกณฑ์ของอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์หรืออนุสัญญาบูดาเปสต์ของประเทศสมาชิกอาเซียนนั้นอยู่ในระดับที่จำกัด และยังคงมีบางประเทศที่ยังไม่มีโครงสร้างพื้นฐานทางกฎหมายอาชญากรรมทางคอมพิวเตอร์ที่อยู่ในระดับมาตรฐาน ดังนั้นความแตกต่างของรูปแบบกฎหมายภายในของแต่ละประเทศอาจเป็นปัจจัยหนึ่งที่ทำให้บางประเทศยังชั่ง

---

[216] Csonka, P., The draft Council of Europe Convention on Cybercrime: A response to the challenge of crime in the age of the Internet, *Computer Law & Security Report*, *16*(5), (2001, October 1), 329-330.

[217] อธิบดีศูนย์ความมั่นคงไซเบอร์แห่งชาติฟิลิปปินส์ Maria Lourdes กล่าวว่าฟิลิปปินส์ได้ดำเนินการตามอนุสัญญาปูดาเปสต์ (อนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์), ARF, *Co-Chairs summary report ARF Cybercrime Capacity Building Conference Bandar Seri Begawan Brunei Darussalam April 27-28 2010, 4*, Retrieved 2014, September 19, from http://aseanregionalforum.asean.org/files/library/ARF%20Chairman's%20Statements%20and%20Reports/The%20Seventeenth%20ASEAN%20Regional%20Forum,%202009-2010/Cybercrime%20Conference%20Summary%20Report.doc

[218] เนื่องจากอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์เป็นอนุสัญญาที่เปิดให้ประเทศอื่นซึ่งไม่ใช่ชาติสมาชิกสภายุโรปลงนามได้ จึงนับได้ว่าเป็นสนธิสัญญาระดับโลก (International treaty) แทนที่จะเป็นเพียงระดับภูมิภาค, Archick, K., *The Council of Europe Convention*, (Washington DC: The Library of Congress, 2006).

[219] Council of Europe, *Convention on Cybercrime CETS No.: 185*, Retrieved 2014, August 19, from http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG

ใจที่จะรับเอาหลักการของอนุสัญญามาปรับใช้หรือไม่ หรือแม้แต่การลงนามเป็นภาคี และปัจจัยหนึ่งอาจเป็นเพราะอาเซียนไม่ได้มีส่วนร่วมในขั้นตอนการจัดทำอนุสัญญา การไม่มีส่วนร่วมในการพัฒนาข้อบังคับนี้เองทำให้การผูกพันตนเข้ากับข้อตกลงในอนุสัญญาฉบับนี้นั้นจำเป็นต้องได้รับการทบทวนเป็นอย่างมาก โดยเฉพาะในส่วนของการสืบค้นและยึดข้อมูลทางคอมพิวเตอร์ ที่อาจจะเป็นการล่วงละเมิดต่ออธิปไตยของประเทศสมาชิกอาเซียนได้

ตั้งแต่ในช่วงปลายทศวรรษที่ 90 เมื่อสภายุโรปเริ่มกระบวนการสร้างอนุสัญญาอนุสัญญาบูดาเปสต์ผ่านกระบวนการทางการทูตและข้อเสนอแนะจากสภายุโรป แต่ขาดความร่วมมือในทางกฎหมายระหว่างภูมิภาคในทางอาญาที่มีประสิทธิภาพกับประเทศในภูมิภาคเอเชียและกลุ่มประเทศอาเซียน โดยเฉพาะอย่างยิ่งในส่วนของอาชญากรรมทางคอมพิวเตอร์ เช่น Commonwealth nations model law on computer related crime and international cooperation ที่หลายประเทศยอมรับว่าให้แนวทางที่มีประโยชน์โดยเฉพาะกับประเทศที่มีพื้นฐานด้านพัฒนาการทางกฎหมายที่เป็นแบบเดียวกัน แม้กระนั้นก็ตามสนธิสัญญาทวิภาคีนับวันยิ่งมีความจำเป็นในการสร้างความเข้าใจร่วมกันที่เพียงพอในการให้ความช่วยเหลือระหว่างประเทศในด้านกฎหมาย

ปัญหาสำคัญอีกข้อหนึ่งซึ่งทำให้การรับเอาอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์หรืออนุสัญญาบูดาเปสต์มาใช้อย่างเต็มรูปแบบในประเทศสมาชิกอาเซียนไม่ได้เต็มที่ คือ การให้อำนาจในการล่วงล้ำอธิปไตยของประเทศอื่นซึ่งมีอยู่ในมาตรา 32b ของอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์[220] การเข้าถึงข้อมูลคอมพิวเตอร์ที่เก็บไว้ข้ามเขตแดน ซึ่งทำให้ประเทศหนึ่งสามารถเข้าถึงหรือรับข้อมูลผ่านระบบคอมพิวเตอร์ในอาณาเขตของตนซึ่งข้อมูลคอมพิวเตอร์ที่อยู่ในอาณาเขตของอีกประเทศหนึ่งได้โดยไม่ต้องบอกกล่าวแก่เจ้าหน้าที่ของประเทศนั้น โดยมาตรานี้ให้อำนาจในการล่วงล้ำอธิปไตยของประเทศอื่นซึ่งสร้างความกังวลให้แก่หลายประเทศในการเข้าร่วมลงนามในอนุสัญญา ซึ่งข้อตกลงในด้านความปลอดภัยข้อมูลระหว่างประเทศ ซึ่งในการประชุม ARF ในปี พ.ศ. 2553 รัสเซียได้ให้ความเห็นว่า Shanghai cooperation organization (SCO) ได้รับเอาแนวทางซึ่งมีความสอดคล้องกับพื้นฐานในด้านความร่วมมือระหว่างประเทศทางกฎหมายของประเทศในกลุ่ม ASEAN ได้ดีกว่า[221]

---

[220] Convention on Cybercrime, Article 32–Trans-border access to stored computer data with consent or where publicly available

b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

[221] ARF Cybercrime capacity building Conference, *CO-CHAIRS SUMMARY REPORT*, Banda Seri Begawan Brunei Darussalam, April 27-28 2010.

ประเทศกำลังพัฒนาทั้งหลายอาจลังเลที่จะลงนามในอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของสหภาพยุโรปเพราะเงื่อนไขที่เข้มงวดในกฎหมายวิธีสบัญญัติและความร่วมมือระหว่างประเทศ ยกตัวอย่างประเทศบราซิลซึ่งปฏิเสธจะลงนามในอนุสัญญาฉบับนี้เนื่องมาจากข้อกังวลในเรื่องการทำให้การละเมิดลิขสิทธิ์เป็นความผิดทางอาญา ซึ่งแสดงให้เห็นว่าข้อตกลงนี้อาจไม่สามารถใช้บังคับร่วมกันได้ในทุกประเด็น ธรรมเนียมปฏิบัติในเรื่องหลักปทัสฐานทางอาญาตรงกัน (Dual criminality)[222] ในเรื่องการให้ความช่วยเหลือในทางกฎหมายระหว่างประเทศยังคงเป็นอุปสรรคที่สำคัญในเรื่องการยอมรับในตัวอนุสัญญาฉบับนี้ อย่างไรก็ดี Recommendation of the 12th United Nations Congress on Crime Prevention and Criminal Justice ได้แสดงให้เห็นว่านานาชาติต่างเห็นพ้องต้องกันในเรื่องความสำคัญของอาชญากรรมนอกรูปแบบ (Non-traditional crime) โดยแม่แบบจากอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ของสหภาพยุโรปจะเป็นแนวทางที่เป็นประโยชน์ในการสร้างสนธิสัญญาที่มีความเป็นสากลอย่างแท้จริง

แม้ว่าอนุสัญญาบูดาเปสต์ได้สร้างรากฐานในการสร้างความสอดคล้องระหว่างกฎหมายและข้อบังคับระหว่างประเทศ ในการรับมือกับอาชญากรรมทางคอมพิวเตอร์ แต่มีแนวโน้มว่าจะไม่มีประเทศในอาเซียนเข้าร่วมลงนามในอนุสัญญาอาชญากรรมทางคอมพิวเตอร์ในอนาคตอันใกล้ และอาจกลายเป็นอุปสรรคในด้านความร่วมมือระหว่างประเทศในการสืบสวนและดำเนินคดีอาชญากรรมทางคอมพิวเตอร์ ด้วยแนวโน้มของพัฒนาการทางเทคโนโลยีสารสนเทศ ระบบการประมวลผลแบบกลุ่มเมฆและอุปกรณ์คอมพิวเตอร์พกพาที่เข้ามาทดแทนการใช้งานคอมพิวเตอร์แบบดั้งเดิม รวมไปถึงพัฒนาการของ Botnet และการเข้ารหัสข้อมูล รวมไปถึงอาชญากรรมในรูปแบบของ Social engineering scams ที่นับวันยิ่งทวีความรุนแรงมากขึ้นจากการขยายตัวของจำนวนผู้ใช้อินเตอร์เน็ตในแต่ละประเทศ แสดงให้เห็นถึงความจำเป็นในการแก้ไขปรับปรุงอนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์เสียใหม่ ทั้งในด้านเนื้อหาและมาตรการ โดยให้ประเทศที่อยู่ภายนอกภูมิภาคยุโรปเข้ามามีส่วนร่วมด้วย

---

[222] หลักปทัสฐานตรงกัน (Dual criminality) คือ หลักการที่ประเทศซึ่งจะให้ความช่วยเหลือทางอาญา เช่น การร้องขอให้มีการส่งผู้ร้ายข้ามแดนได้นั้น การกระทำนั้นต้องเป็นความผิดอาญาตามกฎหมายทั้งของรัฐผู้ขอและของรัฐผู้ส่ง หลักนี้อาจขยายครอบคลุมไปถึงเงื่อนไขให้อำนาจดำเนินคดีและเงื่อนไขการลงโทษอื่น ๆ ด้วย

ตารางที่ 5.1 รวมของเหตุการณ์สำคัญที่เกิดขึ้นบนไซเบอร์สเปซในอาเซียน ตั้งแต่ปี พ.ศ. 2555-2556 ที่เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์

ประเทศ	เหตุการณ์	เดือนและปีที่เกิดเหตุ
บรูไน	ITPSS บันทึกเหตุโจมตีไซเบอร์กว่า 2,000 ครั้ง ตั้งแต่ปี พ.ศ. 2553-2555 (62% ไวรัส 26% สแปม 7% Defacement และ 4% SCAM	พฤศจิกายน พ.ศ. 2555
กัมพูชา	Nullcrew กลุ่มแฮกเกอร์โจมตีเว็บไซต์ประเทศกัมพูชาเพื่อประท้วงการปิดกั้นเนื้อหาทางอินเตอร์เน็ตและการจับกุมผู้ร่วมก่อตั้งเว็บไซต์ The Pirate Bay โดยประกาศว่าจะมุ่งเป้าไปยังภาคธุรกิจ ภาครัฐ และกองทัพ และนำเอาพาสเวิร์ดไปแจกจ่ายให้นักเคลื่อนไหวอื่น ๆ	กันยายน พ.ศ. 2555
	เว็บไซต์กรมตำรวจแห่งชาติและศาลฎีกาประเทศกัมพูชาถูกเจาะระบบโดยนักเจาะระบบชาวอินโดนีเซียนามแฝง Hmei7 อ้างว่าเป็นผู้เจาะระบบเว็บไซต์กรมตำรวจ แต่ไม่ทราบผู้เจาะระบบศาลฎีกา	มกราคม พ.ศ. 2556
	รัฐบาลกัมพูชาเป็นเป้าหมายการเจาะระบบหลายครั้งในอดีต ซึ่งรวมไปถึงการที่กลุ่ม Annonymous เจาะเข้าไปขโมยและเผยแพร่เอกสารราชการของกระทรวงการต่างประเทศกัมพูชากว่า 5,000 ฉบับ	มกราคม พ.ศ. 2556
อินโดนีเซีย	Anonymous Indonesia ทำการเจาะระบบเข้าไปเปลี่ยนหน้าเว็บไซต์ของรัฐบาลมากกว่า 12 เว็บไซต์หลังจากการจับกุม Wildan Yani Ashair ซึ่งถูกกล่าวหาว่าเจาะระบบของเว็บไซต์ประธานาธิบดี ในช่วง 3 ปี เว็บไซต์ของรัฐบาลถูกเจาะระบบไปกว่า 36.6 ล้านครั้ง	มกราคม พ.ศ. 2556
	คดีฉ้อโกงออนไลน์ร้ายแรงซึ่งมีมูลค่าความเสียหายกว่า ห้าแสนเหรียญสหรัฐ ซึ่งนับเป็น 40% ของคดีอาชญากรรมทางคอมพิวเตอร์ 176 คดีในช่วง 4 เดือนแรกของปี พ.ศ. 2556	
ลาว	ไม่พบการแจ้งเหตุ	

ตารางที่ 5.1 (ต่อ)

ประเทศ	เหตุการณ์	เดือนและปีที่เกิดเหตุ
มาเลย์เซีย	ตำรวจได้บันทึกคดีเจาะระบบกว่า 24 คดีในช่วงเดือนมกราคมถึงกันยายน พ.ศ. 2555 ซึ่งประเมินมูลค่าความเสียหายได้กว่า 1.1 ล้านเหรียญสหรัฐ	พฤศจิกายน พ.ศ. 2555
	แฮกเกอร์เจาะระบบเข้าไปโพสท์ข้อความในเว็บไซต์ของกระทรวงสารข้อมูลข่าวสาร ว่าประธานาธิบดี Datuk Seri Najib Tun Rasak ได้ลาออก	กุมภาพันธ์ พ.ศ. 2556
	สถานีวิทยุและเว็บไซต์ข่าวของฝ่ายค้าน ซาราวัก อ้างว่าถูก DDoS	
	FinSpy ส่วนหนึ่งของโปรแกรมบุกรุกและสอดแนม FinFisher แจกจ่ายโดย Gamma International มุ่งเป้าไปที่กลุ่มผู้ใช้ที่พูดภาษามาเลย์	มีนาคม พ.ศ. 2556
พม่า	ในช่วงเกิดเหตุการณ์สังหารหมู่ชาวมุสลิมโรฮิงยา เว็บไซต์ของกระทรวงข้อมูลข่าวสารถูก Deface ด้วยถ้อยคำเตือนให้รัฐบาลหยุดสังหารชาวมุสลิม	สิงหาคม พ.ศ. 2555
	กลุ่ม Annonymous ประกาศสนับสนุนชาวมุสลิมโรฮิงยา โดยมุ่งเป้าไปที่เว็บไซต์ของรัฐบาล องค์การสหประชาชาติ (จากการไม่แทรกแซงด้วยกำลังทหาร) และอองซานซูจีเพราะความนิ่งเฉยต่อเหตุการณ์ความรุนแรง	พฤษภาคม พ.ศ. 2556
	สื่อ 11 แห่งถูก Deface โดยกลุ่มนักเจาะระบบ Blink เพื่อตอบโต้บทความ Hate Speech และยังโจมตีเว็บไซต์กลุ่มผู้สนับสนุนมุสลิมโรฮิงยาจากเหตุขัดแย้งระหว่างชาวพุทธและมุสลิมในรัฐยะไข่	มิถุนายน พ.ศ. 2556
ฟิลิปปินส์	นักเจาะระบบชาวจีน Deface เว็บไซต์รัฐบาลฟิลิปปินส์ นักเจาะระบบชาวฟิลิปปินส์ตอบโต้ด้วยวิธีเดียวกันต่อเว็บไซต์รัฐบาลจีน	มิถุนายน พ.ศ. 2555
	กลุ่ม Annonymous Phillipines เจาะระบบเว็บไซต์ของประธานาธิบดีเพราะจัดการผิดพลาดในกรณีความขัดแย้งในกรุง Sabah กล่าวหารัฐบาลว่าปล่อยให้ทหารมาเลเซียสังหารประชาชน	มีนาคม พ.ศ. 2556

ตารางที่ 5.1 (ต่อ)

ประเทศ	เหตุการณ์	เดือนและปีที่เกิดเหตุ
ฟิลิปปินส์ (ต่อ)	กลุ่ม Annonymous Phillipines โจมตีธุรกิจที่มีชื่อเสียง องค์กรราชการ และ รัฐบาลเพื่อประท้วง Cyber crime Act 2012	กันยายน พ.ศ. 2555
	หลังจากเหตุยามชายฝั่งฟิลิปปินส์ยิงเรือประมงไต้หวัน นักเจาะระบบฟิลิปปินส์และไต้หวันทำการตอบโต้กันไปมาโดยการผลัดกันโจมตีเว็บไซต์ของประเทศตรงข้าม	พฤษภาคม พ.ศ. 2556
สิงคโปร์	Trend Micro บริษัทด้านการรักษาความปลอดภัยคอมพิวเตอร์ เปิดเผยว่าประชาชนสิงคโปร์กว่า 900 คนตกเป็นเหยื่อการฉ้อโกงออนไลน์แบงก์กิ้งในช่วงไตรมาสแรกของปี พ.ศ. 2556	พฤษภาคม พ.ศ. 2556
ไทย	กลุ่มนักเจาะระบบชาวตุรกีขโมยข้อมูลลูกค้าแมกโดนัลด์ประเทศไทยกว่า 2000 ราย กลุ่มเดียวกันนี้ยังอ้างว่าได้โจมตีเว็บไซต์สภากาชาดไทยเพื่อประท้วงการไม่เคารพศาสดามูฮัมหมัด	ตุลาคม พ.ศ. 2555
	ตั้งแต่เดือนมกราคมถึงพฤษภาคม พ.ศ. 2556 มีเหตุบุกรุกเว็บไซต์รัฐบาลกว่า 1,475 ครั้ง และการโจมตีด้วยโปรแกรมมุ่งร้ายหลายร้อยครั้ง รวมไปถึงการ phishing ด้วย	มิถุนายน พ.ศ. 2556
เวียดนาม	Baidu เว็บไซต์บริษัท Search engine ของจีนเวอร์ชันภาษาเวียดนาม แอบติดตั้งสปายแวร์และแอดแวร์ซึ่งเมื่อคอมพิวเตอร์ได้ดาว์นโหลดลงไปแล้วจะทำการติดตั้งโดยอัตโนมัติ และถูกควบคุม จารกรรมข้อมูล และถูกใช้เป็นเครื่องลูกข่ายในการโจมตีแบบ DDoS ได้จากระยะไกล	กรกฎาคม พ.ศ. 2555

ที่มา Heinl, C. H., Regional cybersecurity moving toward a resilient ASEAN cybersecurity regime, *ASIA Policy*, *18*(July 2014), 156-158.

ตารางที่ 5.2 สรุปปัญหาในการรับมืออาชญากรรมทางคอมพิวเตอร์ในอาเซียน

ปัญหา	รายละเอียด
ความครอบคลุมด้านกฎหมายอาชญากรรมทางคอมพิวเตอร์ของประเทศสมาชิกอาเซียน	1. กฎหมายคุ้มครองความเป็นส่วนตัวและการคุ้มครองข้อมูล 1.1 ปัจจุบันมีเพียงมาเลเซีย ฟิลิปปินส์และสิงคโปร์ในอาเซียนที่มีกฎหมายคุ้มครองข้อมูล 1.2 ไทย อินโดนีเซียอยู่ในระหว่างการร่างกฎหมาย 1.3 มี APEC Privacy Framework เป็นกรอบการสร้างมาตรการ 1.4 ผู้ใช้มีเครื่องมือให้เลือกสรรมากมายในการปิดซ่อน IP address และตัวตนบนอินเตอร์เน็ต ในขณะที่ช่วยคุ้มครองความเป็นส่วนตัวก็ทำให้การค้นหาตัวผู้กระทำผิดของเจ้าหน้าที่ยากลำบากขึ้น 2. อาชญากรรมทางคอมพิวเตอร์ ความผิดประเภทบุกรุก 2.1 มีในทุกประเทศที่มีกฎหมายอาชญากรรมทางคอมพิวเตอร์ และถูกระบุไว้ในอนุสัญญาอาชญากรรมทางคอมพิวเตอร์ 2.2 Computer Misuse Act 1990 ของสหราชอาณาจักรเป็นต้นแบบของกฎหมายอาชญากรรมทางคอมพิวเตอร์ของสิงคโปร์และบรูไน ในแทบทุกประเทศสมาชิกอาเซียนยังให้ การเปิดเผยรหัสเชื่อมต่อคอมพิวเตอร์โดยไม่ได้รับอนุญาตเป็นความผิดอีกด้วย 2.3 รัฐบาลมักไม่ใช้งบประมาณในการตั้งหน่วยรับมือการโจมตีซึ่งจำเป็นจะต้องทำงานตลอด 24 ชั่วโมง 2.4 ปัญหาการแพร่กระจายของ Botnet ซึ่งทำได้ง่ายไม่จำเป็นต้องเป็นผู้เชี่ยวชาญทางคอมพิวเตอร์ ความรวดเร็วในการประสานงานและประสิทธิภาพของ CERT ในภูมิภาคจึงมีความสำคัญมากในการรับมืออาชญากรรมประเภทนี้ 3. สงคราม การจารกรรม และการก่อการร้ายไซเบอร์ 3.1 ขอบเขตที่ไม่ชัดเจนระหว่างอาชญากรรมทางคอมพิวเตอร์ทั่วไป และการโจมตีที่เข้าข่ายการประกาศสงคราม (ACT OF WAR) และปฏิบัติการทางการทหาร เป็นปัญหาสำคัญต่อการดำเนินการทางกฎหมายระหว่างประเทศ 3.2 การโจมตีด้วยซอฟท์แวร์คอมพิวเตอร์นับเป็นการใช้อาวุธตามกฎหมายระหว่างประเทศหรือไม่ 3.3 เมื่อผู้กระทำความผิดเป็นรัฐไม่ใช่ตัวบุคคล

ตารางที่ 5.2 (ต่อ)

ปัญหา	รายละเอียด
ความครอบคลุมด้านกฎหมายอาชญากรรมทางคอมพิวเตอร์ของประเทศสมาชิกอาเซียน (ต่อ)	3.4 ศักยภาพของ CERT ซึ่งอาจไม่พอรับมือการโจมตีประเภทนี้ 3.5 ข้อกำหนดในเรื่องสันติภาพและความมั่นคงของกฎบัตรสหประชาชาติจะสามารถประยุกต์ใช้กับ non-state actor หรือการปฏิบัติต่อกรณีที่ประเทศล่มสลายทางเศรษฐกิจจากการโจมตีไซเบอร์แบบเดียวกับการกระทำด้วยอาวุธทางกายภาพ (kinetic weapon) หรือไม่ 4. อาชญากรรมทางคอมพิวเตอร์ ความผิดประเภทการหลอกลวง 4.1 การรังควานทางอินเตอร์เน็ต (Online Harassment) การตามตื๊อ (Stalking) หรือ การล่อลวงเด็ก (Child grooming) นั้นกระทำได้ง่ายมากขึ้นผ่านเว็บเครือข่ายสังคมออนไลน์ซึ่งเป็นที่แพร่หลายทั่วโลกในปัจจุบัน 4.2 ระบบที่ด้อยประสิทธิภาพในการคุ้มครองผู้ใช้ที่อยู่ในกลุ่มเสี่ยงและรู้เท่าไม่ถึงการณ์ 4.3 ความร่วมมือจากภาคเอกชนมีความจำเป็น 4.4 การเชื่อมโยงฐานข้อมูลอาชญากรเข้าด้วยกันอย่างเป็นระบบ 4.5 ข้อกังวลในเรื่องความเป็นส่วนตัวนั้นมักไม่เล็งเห็นถึงความเป็นส่วนตัวและความปลอดภัยของผู้ที่เป็นเหยื่ออาชญากรรม 5. การควบคุมเนื้อหา 5.1 ประเทศสมาชิกอาเซียนส่วนใหญ่มีกฎหมายควบคุมเนื้อหาที่ได้รับการเผยแพร่บนอินเตอร์เน็ต โดยมีพื้นฐานอยู่บน สภาพสังคม การเมือง ศีลธรรม ความเชื่อทางศาสนา ของรัฐบาลแต่ละประเทศ 5.2 ใกล้เคียงกับการควบคุมสื่อสิ่งพิมพ์ 5.3 กฎหมายบางประเทศถูกต่อต้านโดยภาคประชาชนเป็นอย่างมากเช่น Cybercrime prevention Act 2012 ของฟิลิปปินส์ 5.4 ร่างพระราชบัญญัติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ที่ได้เพิ่มเหตุผลซึ่งรัฐจะสามารถทำการปิดกั้นการเข้าถึงเว็บไซต์โดยขยายไปถึงความผิดใน กฎหมายอื่น ๆ ที่ใช้คอมพิวเตอร์เป็นเครื่องมือได้ด้วย

ตารางที่ 5.2 (ต่อ)

ปัญหา	รายละเอียด
ความครอบคลุมด้านกฎหมายอาชญากรรมทางคอมพิวเตอร์ของประเทศสมาชิกอาเซียน (ต่อ)	5.5 เวียดนามกำหนดให้ผู้ให้บริการรับส่งข้อมูลทางอินเตอร์เน็ตต้องเป็นไปตามที่รัฐกำหนด และตัวผู้ให้บริการจะต้องรับผิดทางกฎหมายในเนื้อหาที่ตนเองสร้างขึ้น 5.6 บางประเทศกำหนดให้เนื้อหาที่เป็นการดูหมิ่นชาติพันธุ์ (Racism) และดูหมิ่นศาสนา (Blasphemy) เป็นความผิดในกฎหมาย เช่น มาเลเซีย อินโดนีเซียและสิงคโปร์ 5.7 สิงคโปร์มีกฎหมาย Sedition Act ผู้เผยแพร่เนื้อหาที่ส่งเสริมความรู้สึกมุ่งร้ายระหว่างชาติพันธุ์หรือชนชั้น มีความผิดทางกฎหมาย 6. สแปม (SPAM) 6.1 สิงคโปร์และเวียดนามที่ได้ออกกฎหมายต่อต้านสแปมมาบังคับใช้แล้ว 6.2 มาเลเซียมีบทบัญญัติกฎหมายใกล้เคียงที่อาจใช้ดำเนินคดีกับผู้ปล่อยแปมได้บ้างแต่อยู่ในขอบเขตที่จำกัด 6.3 พระราชบัญญัติการกระทำผิดเกี่ยวกับคอมพิวเตอร์ มาตรา 11ที่บัญญัติให้ผู้ส่งจดหมายอิเล็กทรอนิกส์โดยไม่เปิดเผยชื่อผู้ส่งมีความผิด แก้ไขในร่างพระราชบัญญัติใหม่ ให้การส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เปิดโอกาสให้ผู้รับแจ้งบอกเลิกหรือปฏิเสธการรับ ถือว่ามีความผิด 6.4 ฟิลิปปินส์ได้บัญญัติความผิดเกี่ยวกับสแปมไว้ใน Cybercrime prevention act 2012 แต่ถูกศาลสั่งระงับชั่วคราว (TRO) 7. ลิขสิทธิ์ในเนื้อหาดิจิตอล แทบทุกประเทศมีการคุ้มครองประเภทนี้ หากไม่มีบัญญัติไว้เฉพาะก็ปรับใช้จากกฎหมายลิขสิทธิ์เดิม ความแตกต่างอยู่ที่การบังคับใช้กฎหมายเท่านั้น

ตารางที่ 5.2 (ต่อ)

ปัญหา	รายละเอียด
เขตอำนาจศาล	1. ยังไม่มีทางออกที่เหมาะสม ไม่เฉพาะแต่ในอาเซียนแต่กับองค์กรรวมกลุ่มประเทศอื่น ๆ ทั่วโลก 2. การยอมให้มีการเข้าถึงข้อมูลข้ามเขตแดน (Trans-border access to stored computer data) ซึ่งรวมไปถึงการตรวจจับและเก็บข้อมูลการจราจรอิเล็กทรอนิกส์แบบ Real-time โดยไม่จำเป็นต้องผ่านการอนุญาตจากประเทศปลายทางก่อน เป็นอุปสรรคสำคัญ 3. อินโดนีเซียซึ่งนับเป็นประเทศซึ่งมีอัตราการส่ง Attack Traffic มากที่สุดในประเทศสมาชิกอาเซียนได้เตรียมร่างกฎหมายในเรื่องนี้แล้ว 4. การสร้างคู่มือเพื่อกำหนดแนวทางปฏิบัติในเรื่องเขตอำนาจศาลที่กระตุ้นให้ประเทศสมาชิกอาเซียนนำเอาไปปฏิบัติอย่างเป็นอันหนึ่งอันเดียวกันเป็นทางออก
ปัญหาการปรับใช้อนุสัญญาอาชญากรรมทางคอมพิวเตอร์ภายในภูมิภาคอาเซียน	1. ความแตกต่างของรูปแบบกฎหมายภายในแต่ละประเทศเป็นปัจจัยหนึ่งที่ทำให้บางประเทศชั่งใจที่จะรับเอาหลักการของอนุสัญญามาปรับใช้ หรือแม้แต่ลงนามเป็นภาคี และอาเซียนไม่ได้มีส่วนร่วมในขั้นตอนการจัดทำอนุสัญญา 3. การสืบค้นและยึดข้อมูลทางคอมพิวเตอร์ การเก็บข้อมูลแบบจราจรอิเล็กทรอนิกส์แบบ real-time และการดักจับเนื้อหาข้อมูลนับเป็นอำนาจที่ล่วงล้ำที่สุดของอนุสัญญา 4. การให้อำนาจในการล่วงล้ำอธิปไตยของประเทศอื่นซึ่งมีอยู่ในมาตรา 32b การเข้าถึงข้อมูลคอมพิวเตอร์ที่เก็บไว้ข้ามเขตแดน ซึ่งทำให้ประเทศหนึ่งสามารถเข้าถึงหรือรับข้อมูลผ่านระบบคอมพิวเตอร์ในอาณาเขตของตนซึ่งข้อมูลคอมพิวเตอร์ซึ่งอยู่ในอาณาเขตของอีกประเทศหนึ่งได้โดยไม่ต้องบอกกล่าวแก่เจ้าหน้าที่ของประเทศนั้น เป็นอุปสรรคสำคัญในการปรับใช้ 5. ธรรมเนียมปฏิบัติในเรื่องหลักปทัสฐานตรงกัน (dual criminality) ในเรื่องการให้ความช่วยเหลือในทางกฎหมายระหว่างประเทศยังคงเป็นอุปสรรคสำคัญ 6. ประเทศรัสเซียได้ให้ความเห็นว่า Shanghai Cooperation Organization (SCO) ได้รับเอาแนวทางซึ่งมีความสอดคล้องกับพื้นฐานในด้านความร่วมมือระหว่างประเทศทางกฎหมายของประเทศในกลุ่ม ASEAN ได้ดีกว่า

บทที่ 6

บทสรุป และข้อเสนอแนะ

6.1 บทสรุป

องค์การอาเซียนมีความพยายามที่จะสร้างกลไกเพื่อจัดการปัญหาอาชญากรรมทางคอมพิวเตอร์ทั้งภายในและภายนอกภูมิภาคโดยอาศัยแม่แบบจากหลักเกณฑ์สากลต่าง ๆ และนำมาปรับใช้ให้เหมาะสมกับภูมิภาคโดยผ่านการประชุมต่าง ๆ หลายครั้ง ซึ่งอาเซียนได้กำหนดเป้าหมายการพัฒนาโครงสร้างพื้นฐานทางเทคโนโลยีการสื่อสารและสารสนเทศและความปลอดภัยไซเบอร์ลงไปในแผนงานมากมาย เช่น ASEAN ICT Master plan 2015 และ Master plan on ASEAN connectivity ฯลฯ โดยอาเซียนได้มีการจัดตั้งหน่วยงานเพื่อต่อต้านการโจมตีไซเบอร์และประสานงานระหว่างประเทศสมาชิกด้วยกันตลอด 24 ชั่วโมง 7 วันต่อสัปดาห์ (CERTs) และมีการจัดตั้งคณะทำงานเพื่อศึกษาหาแนวทางการสร้างมาตรการร่วมกันของประเทศสมาชิกอาเซียน นอกจากนี้ ประเทศสมาชิกอาเซียนเองก็มีความตระหนักถึงภัยไซเบอร์ที่มีการขยายตัวอย่างรวดเร็วอันเนื่องมาจากพัฒนาการของเทคโนโลยีที่ก้าวหน้าขึ้นเรื่อย ๆ ในปัจจุบัน ประเทศสมาชิกของอาเซียนเกือบทุกประเทศได้พยายามออกกฎหมายเพื่อรับมือกับภัยจากอาชญากรรมทางคอมพิวเตอร์ โดยมีกฎเกณฑ์ที่ครอบคลุมความผิดทั้งในด้านบุกรุก การควบคุมเนื้อหาออนไลน์ และการคุ้มครองข้อมูลส่วนบุคคล เพื่อเสริมสร้างศักยภาพและความปลอดภัยไซเบอร์ของภูมิภาคให้ได้มาตรฐานสากลและเท่าทันอาชญากรรมทางคอมพิวเตอร์ที่หลากหลายและซับซ้อนมากยิ่งขึ้น

อย่างไรก็ตาม ประเทศสมาชิกอาเซียนยังคงประสบปัญหาและอุปสรรคในหลาย ๆ ด้าน เป็นต้นว่า ด้านการพัฒนาโครงสร้างพื้นฐานทางข้อมูลข่าวสารสารสนเทศและการสื่อสาร ความไม่สอดคล้องกันของกฎหมายในประเทศสมาชิกที่ความผิดในประเทศหนึ่งอาจไม่ถูกกำหนดเป็นความผิดในประเทศอื่น และ/หรือการกลั่นกรองเนื้อหาออนไลน์ที่มีมาตรฐานแตกต่างกันระหว่างประเทศในภูมิภาคนี้ โดยกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่ยังไม่มีความสมบูรณ์ในหลายประเทศ รวมทั้งหลักเกณฑ์ในการส่งเสริมความร่วมมือระหว่างประเทศยังไม่มีความชัดเจนในเรื่องการสืบสวนคดีอาชญากรรมทางคอมพิวเตอร์จึงก่อให้เกิดความล่าช้าในการสืบสวนดำเนินคดี เป็นต้น

สำหรับกลุ่มประเทศสมาชิกอาเซียนที่ต้องให้การช่วยเหลือเพื่อพัฒนาโครงสร้างพื้นฐานทาง ICT และร่างกฎหมายที่สอดคล้องกับประเทศสมาชิกอาเซียนอื่น ๆ มากที่สุดคือกลุ่มประเทศ CLMV โดยเฉพาะประเทศกัมพูชาและประเทศลาวที่ยังไม่มีการออกกฎหมายอาชญากรรมทางคอมพิวเตอร์โดยเฉพาะ สำหรับประเทศพม่านั้นในปี พ.ศ. 2554 ถือว่าเป็นประเทศที่มีการส่ง Attack traffic สูงที่สุดในภูมิภาค เพราะการขาดกฎหมายในการควบคุมอาชญากรรมทางคอมพิวเตอร์จึงทำให้ประเทศพม่ากลายเป็นแหล่งกบดาน (Safe haven) ของเหล่าอาชญากรและทางผ่านของกิจกรรมผิดกฎหมายไซเบอร์ ดังนั้นการพัฒนาโครงสร้างพื้นฐานและส่งเสริมการใช้งาน ICT ในประเทศสมาชิกอาเซียนจะช่วยให้รัฐมีความตระหนักถึงปัญหาและออกกฎเกณฑ์เพื่อดูแลได้อย่างมีประสิทธิภาพมากขึ้น รวมไปถึงการมีบุคลากรและผู้เชี่ยวชาญรวมไปถึงหน่วยงานที่สามารถรับมือกับเหตุการณ์ได้อย่างทันท่วงที

กรณีการปรับปรุงมาตรฐานในเรื่องการควบคุมเนื้อหาบนอินเตอร์เน็ต แม้จะกระทำได้ยาก เพราะมุมมองในด้านคุณค่า (Value) ของแต่ละชนชาติในอาเซียนมีความแตกต่างกัน แต่ในเรื่องที่มีความเป็นสากล เช่น การเหยียดเชื้อชาติ เนื้อหาซึ่งสร้างความเกลียดชัง การเหยียดผิว เหยียดเพศ เหยียดชนชั้น และการล่วงละเมิดเด็กและสตรี ควรกำหนดให้เป็นมาตรฐานกลางที่ประเทศสมาชิกอาเซียนต้องปฏิบัติตาม รวมไปถึงเสรีภาพในการแสดงออก (Right of expression) ในด้านต่าง ๆ ควรมีกรอบที่ชัดเจนและเป็นธรรมตามหลักสากล

ทั้งนี้ กฎหมายที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลควรจะมีความรัดกุมและมีขอบเขตชัดเจน ในส่วนของข้อมูลที่เปิดเผยได้และข้อมูลที่เป็นความลับ รวมไปถึงการกำหนดกรอบให้การตอบรับการส่งจดหมายอิเล็กทรอนิกส์รวมไปถึงข้อความอิเล็กทรอนิกส์ต่าง ๆ ที่ผู้รับไม่ยินยอมซึ่งถือว่าเป็นสิ่งผิดกฎหมาย (กำหนดขอบเขตที่ชัดเจนของ SPAM) โดยการสร้างเกราะป้องกันในด้านการกระจายข้อมูลนี้จะช่วยคุ้มครองเจ้าของข้อมูลจากการกระทำผิดในหลายรูปแบบทั้ง SPAM, การหลอกลวงบนอินเตอร์เน็ต, การเจาะระบบ เป็นต้น

6.2 ข้อเสนอแนะ

อาเซียนยังสามารถพัฒนากรอบโครงสร้างทางกฎหมายที่จะกลายมาเป็นหลักเกณฑ์กลางในการรับมือกับปัญหาอาชญากรรมทางคอมพิวเตอร์ในอนาคต ทั้งหมดภายในภูมิภาคนี้และส่งเสริมความร่วมมือในระดับโลกได้ด้วย โดยอาจสร้างหลักเกณฑ์กลางขึ้นโดยอ้างอิงจากเครื่องมือทางกฎหมายระหว่างประเทศที่มีอยู่ในปัจจุบันและกำลังจะมีขึ้นต่อไปในอนาคต สำหรับปัจจุบันนี้

เครื่องมือในการรับมืออาชญากรรมคอมพิวเตอร์ระหว่างประเทศที่มีผลผูกพันและเป็นที่ยอมรับกันอย่างสากล ได้แก่

อนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์ (The Convention on Cybercrime 2001)

อนุสัญญาเพื่อรับมือการกระทำความผิดทางเทคโนโลยีสารสนเทศของสันนิบาตอาหรับ (The League of Arab States Convention on Combating Information Technology Offences)

ข้อตกลงเครือจักรภพในการรับมือการกระทำผิดที่เกี่ยวข้องกับข้อมูลทางคอมพิวเตอร์ (The Commonwealth of Independent States Agreement on Cooperation in Combating Offences related to Computer Information)

ข้อตกลงขององค์การความร่วมมือเซี่ยงไฮ้ในด้านความปลอดภัยของข้อมูลนานาชาติ (The Shanghai Cooperation Organization Agreement in the Field of International Information Security)

โดยมีอย่างน้อย 82 ประเทศที่ได้ลงนามและให้สัตยาบันในข้อตกลงต่าง ๆ ที่กล่าวมาข้างต้น อย่างไรก็ดี ในปัจจุบันหลักเกณฑ์ทางกฎหมายว่าด้วยอาชญากรรมทางคอมพิวเตอร์และความร่วมมือระหว่างประเทศยังคงกระจัดกระจายแตกต่างกันไปในแต่ละประเทศ ดังนั้น อาเซียนเองควรพิจารณาหาวิธีการสร้างความสอดคล้องแบบ Soft harmonization เพื่อสร้างศักยภาพทาง ICT ในประเทศสมาชิกให้อยู่ในระดับใกล้เคียงกันและ Hard harmonization เพื่อสร้างคู่มือในการออกกฎหมายในระดับชาติให้สอดคล้องกันทั้งภูมิภาคต่อไป

6.2.1 ข้อเสนอแนะในเรื่องความร่วมมือระหว่างประเทศในเรื่องอาชญากรรมทางคอมพิวเตอร์

สำหรับปัญหาและอุปสรรคในปัจจุบันและที่จะมีต่อไปในอนาคตในการรับมืออาชญากรรมทางคอมพิวเตอร์ระหว่างประเทศนั้นมีแนวโน้มว่าจะมีการแผ่ขยายออกไปจากเดิม เนื่องจากปัญหาอาชญากรรมทางคอมพิวเตอร์ยุคใหม่ไม่ใช่เพียงปัญหาที่ว่าแต่ละชาติจะรักษาความปลอดภัยในชาติของตนได้อย่างไรเท่านั้น แต่จะกลายเป็นเรื่องการคุ้มครองความปลอดภัยของประชาคมโลกทั้งหมด[223] ซึ่งการขาดหลักเกณฑ์ในด้านการส่งเสริมความร่วมมือระหว่างประเทศในเรื่องอาชญากรรมคอมพิวเตอร์จะกลายมาเป็นอุปสรรคที่สำคัญอันหนึ่ง เช่น ระบบการสืบสวนสอบสวนแบบเดิมที่ล้าหลัง โดยแนวทางการสืบสวนสอบสวนแบบเก่านั้นอาจไม่เพียงพอในการจัดการเกี่ยวกับหลักฐานทางอิเล็กทรอนิกส์ เพราะการรวบรวมหลักฐานทางอิเล็กทรอนิกส์ข้ามแดน

[223] It is no longer a question of a nation protecting its own security, it is a question of the global community protecting itself" Kapil Sipal รัฐมนตรีกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารของอินเดีย กล่าวในการประชุมสุดยอดความมั่นคงไซเบอร์ (Cybersecurity Summit) ซึ่งจัดขึ้นในประเทศอินเดียในปี พ.ศ. 2555 สืบค้นเมื่อ 10 สิงหาคม 2557, จาก http://cybersummit2012.com/content/what-rules-cyberspace

นั้นสิ้นเปลืองเวลาเป็นอย่างมาก เนื่องจากหน่วยงานซึ่งบังคับใช้กฎหมายยังใช้หลักเกณฑ์แบบในยุคเก่า ในการรับมือกับอาชญากรรมบนเครือข่ายสังคมออนไลน์ ซึ่งปัจจุบันการสืบสวนคดีที่เกี่ยวข้องกับเครือข่ายสังคมออนไลน์ยิ่งมีบทบาทสำคัญเพิ่มมากขึ้นเรื่อย ๆ ในฐานะส่วนหนึ่งของการสืบสวนสอบสวนคดีอาญา ดังนั้นหลักเกณฑ์ใหม่ ๆ ที่ทันสมัย เหมาะสมและเป็นทางการในเรื่องความร่วมมือในการสืบสวนสอบสวนระหว่างประเทศจึงมีความจำเป็นที่จะต้องถูกจัดตั้งขึ้นเพื่อรับมืออาชญากรรมทางคอมพิวเตอร์

จากการศึกษาของสำนักงานยาเสพติดและอาชญากรรมแห่งสหประชาชาติ (United Nations Office of Drugs and Crime: UNODC) พบว่าปัญหาในการรับมืออาชญากรรมทางคอมพิวเตอร์หลักๆ นั้นมีอยู่สองประการ ได้แก่

การพึ่งพาระบบการสืบสวนเป็นทางการในทางระหว่างประเทศแบบเดิมไม่สามารถตอบสนองได้อย่างทันท่วงทีในการค้นหาหลักฐานทางอิเล็กทรอนิกส์ที่เปลี่ยนแปลงได้ง่ายซึ่งจะกลายเป็นปัญหาไม่เฉพาะต่ออาชญากรรมทางคอมพิวเตอร์ แต่กับอาชญาชากรรมโดยทั่วไปด้วย และอีกประการหนึ่งคือ ในปัจจุบันซึ่งระบบประมวลผลข้อมูลได้เปลี่ยนแปลงมาเป็นแบบกลุ่มเมฆ ซึ่งพึ่งพาศูนย์ข้อมูล (Data center) ในการประมวลผลข้อมูล ความหมายของคำว่า “ที่ตั้ง (Location)” จำเป็นต้องได้รับการกำหนดนิยามใหม่โดยพิจารณาถึงข้อสรุปในปัญหาที่เกี่ยวกับการเชื่อมต่อโดยตรงกับข้อมูลนอกดินแดนอาณาเขตของรัฐที่เป็นผู้บังคับใช้กฎหมาย

โดย แนวทางการแก้ปัญหาการสืบสวนคดีอาชญากรรมทางคอมพิวเตอร์ข้ามเขตแดนอาจทำได้โดยใช้วิธีการดังนี้

6.2.1.1 การสืบสวนโดยตำรวจ

ดำเนินกระบวนการสืบสวนโดยร่วมมือกับองค์การตำรวจสากล (INTERPOL) เป็นองค์กรที่เป็นผู้นำด้านความร่วมมือนานาชาติในการสืบสวนคดีอาชญากรรมทางคอมพิวเตอร์มาตั้งแต่ยุค 80s การร่วมมือกับ INTERPOL ซึ่งเป็นผู้เชี่ยวชาญในสาขาดังกล่าวจึงเป็นผลดีต่อประสิทธิภาพการสืบสวนคดีอาชญากรรมทางคอมพิวเตอร์ข้ามชาติของภูมิภาค โดยความร่วมมือระหว่างองค์กรตำรวจของภูมิภาคจะช่วยในการดำเนินการสืบสวนระหว่างประเทศได้เป็นอย่างดี

6.2.1.2 การสร้างคณะทำงานเฉพาะกิจระดับภูมิภาค (Regional virtual task force) สำหรับไซเบอร์สเปซ

การสร้างคณะทำงานที่สามารถประสานงานกันได้จากระยะไกลผ่านเทคโนโลยีต่าง ๆ ได้ควรถูกจัดตั้งขึ้นโดยประกอบไปด้วยผู้มีส่วนได้เสียในอุตสาหกรรมการสื่อสารและข้อมูลข่าวสาร ภาคการเงิน ภาคเอกชน NGOs สถานศึกษา และองค์กรบังคับใช้กฎหมายในระดับภูมิภาค

ซึ่งร่วมมือกับ INTERPOL โดยคณะทำงานจะช่วยในการประสานงานกับองค์กรใหญ่ระดับโลก เช่น Google, Facebook, Youtube, Apple, Microsoft และอื่น ๆ อีกมาก

คณะทำงานเฉพาะกิจนี้มีหน้าที่หลักเพื่อการสืบสวนและดำเนินคดีอาชญากรรมทางคอมพิวเตอร์ต้องทำงานร่วมกันภายใต้ความสัมพันธ์ที่เหนียวแน่นผ่านการทำบันทึกความเข้าใจ เพื่อประสานงาน บูรณาการ และแลกเปลี่ยนข้อมูลเพื่อป้องกันและรับมือกับอาชญากรรมทางคอมพิวเตอร์อย่างมีประสิทธิภาพ ทั้งนี้เพื่อการดำเนินการตอบสนองต่อการเกิดอาชญากรรมทางคอมพิวเตอร์ได้โดยทันที (Real-time) โดยดำเนินการผ่านห้องประชุมเสมือน (Virtual meeting rooms) หรือในสภาวะแวดล้อมแบบเสมือน

คณะทำงานเฉพาะกิจระดับภูมิภาคจะมีบทบาทสำคัญในการพิสูจน์และจัดการปัญหาอาชญากรไซเบอร์ข้ามชาติข้ามเขตอำนาจศาล

6.2.2 ข้อเสนอแนะในเรื่องแนวโน้มความเปลี่ยนแปลงและการรับมือกับอาชญากรรมทางคอมพิวเตอร์ที่พัฒนาขึ้นตามยุคสมัย

ปัจจุบันพัฒนาการทางเทคโนโลยีทั้งภาคประชาชนและภาคอุตสาหกรรมได้เปลี่ยนแปลงไปอย่างรวดเร็ว มีการเกิดของเทคโนโลยีใหม่ ๆ ซึ่งเปลี่ยนแปลงวิถีชีวิตของผู้คนอยู่ตลอดเวลา ทั้งการมาของเครือข่างสังคมออนไลน์ที่เชื่อมต่อผู้คนเข้าด้วยกันในระดับโลก และการเปลี่ยนแปลงการใช้งานอุปกรณ์คอมพิวเตอร์จากเดิมที่มีศูนย์กลางอยู่ที่เครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer: PC) เป็นหลักมาเป็นการใช้งานอุปกรณ์สื่อสารพกพาที่สามารถเชื่อมต่ออินเตอร์เน็ตได้ (Mobile Internet Device: MID) หลากหลายรูปแบบ ทั้งโทรศัพท์มือถือ แทบเล็ต หรือเครื่องเกมพกพา และอุปกรณ์แทบทุกอย่างซึ่งแต่เดิมถูกใช้งานแบบออฟไลน์ล้วนถูกเพิ่มความสามารถในการเชื่อมต่ออินเตอร์เน็ตเข้าไปแทบทิ้งสิ้น ไม่เว้นแม้กระทั่งตู้เย็นหรือหม้อหุงข้าว การเปลี่ยนแปลงอย่างฉับพลันเป็นอุปสรรคต่อการกำกับดูแลทางกฎหมายซึ่งต้องการเวลาในการศึกษาและปรับปรุงหลักเกณฑ์ ทั้งในระดับภูมิภาคและระดับสากล นอกจากนี้ วิธีการใช้งานอุปกรณ์คอมพิวเตอร์ก็เช่นเดียวกัน ในยุคก่อนระบบต่างถูกออกแบบมาเพื่อการประมวลผลแบบออฟไลน์บนอุปกรณ์ใดอุปกรณ์หนึ่ง ทั้งข้อมูลที่ประมวลผลและเอาท์พุตต่างอยู่บนอุปกรณ์ตัวนั้นและมักส่งผ่านข้อมูลกันแบบกายภาพเช่นการทำสำเนาบนแผ่นดิสก์ หรืออุปกรณ์ประเภทแฟลชไดรว์ แต่ปัจจุบันได้เปลี่ยนแปลงไปเป็นการประมวลผลแบบกลุ่มเมฆ (Cloud computing) แทน โดยระบบจะทำการประมวลผลบนกลุ่มของคอมพิวเตอร์เซิฟเวอร์ผ่านระบบเครือข่าย ซึ่งเปลี่ยนแปลงนิยามของการประมวลผลและการจัดเก็บข้อมูลทางคอมพิวเตอร์ในกฎหมายที่เกี่ยวกับข้อมูลสารสนเทศ เพราะกระบวนการและข้อมูลเกิดบนเซิฟเวอร์ของระบบคลาวด์ซึ่งไม่ได้มีเพียงเซิฟเวอร์เดียวแต่ร่วมกันประมวลผลและจัดเก็บข้อมูลกันเป็นจำนวนหลายเซิฟเวอร์ที่ตั้งอยู่ในพื้นที่ทางกายภาพที่แตกต่าง

กันคอมพิวเตอร์ อีกทั้งยังมีการโจมตีไซเบอร์ในระดับโลก (Global cyber attack) ต่อโครงสร้างพื้นฐานทางด้านข้อมูลข่าวสารซึ่งได้เริ่มกลายมาเป็นข้อกังวลของรัฐบาลหลายประเทศ องค์กรระหว่างประเทศ และสถาบันภาคเอกชนซึ่งมีความสำคัญในโครงสร้างพื้นฐานทางข้อมูลข่าวสารและการเงินของโลก ซึ่งองค์กรเหล่านี้ต่างมีความเสี่ยงที่จะตกเป็นเป้าของการโจมตีไซเบอร์ พัฒนาการของการโจมตีไซเบอร์ที่ร้ายแรงซึ่งกระทำต่อโครงสร้างพื้นฐานของภาคอุตสาหกรรมข้อมูลข่าวสารได้ทำให้เกิดความตระหนักถึงความสำคัญในการออกข้อกำหนดเฉพาะแยกต่างหากในการรับมือการโจมตีไซเบอร์ที่ร้ายแรงที่ส่งผลกระทบในระดับโลกเพื่อเป็นกลไกทางกฎหมายใหม่บนอินเตอร์เน็ต และควรถูกรวมเข้าไปในสนธิสัญญาระหว่างประเทศ เพื่อเป็นหลักเกณฑ์ทางกฎหมายในระดับสากลเนื่องจากในปัจจุบัน การโจมตีไซเบอร์ยังเป็นเรื่องที่ไม่ได้อยู่ภายใต้การควบคุมของกฎหมายระหว่างประเทศ

ในปัจจุบันที่ผู้คนนิยมติดต่อสื่อสารกันผ่านอินเตอร์เน็ตมากขึ้นจนกลายเป็นเป็นส่วนหนึ่งของวิถีชีวิตที่ได้เปลี่ยนแปลงรูปแบบของการปฏิสัมพันธ์ของผู้คนด้วยเช่นกัน ความเปลี่ยนแปลงนี้ทำให้สังคมแตกต่างไปจากเดิม หลักเกณฑ์ต่าง ๆ ที่ควบคุมดูแลสังคมจึงต้องการการปรับเปลี่ยนให้เหมาะสมกับรูปแบบของสังคมสมัยใหม่เพื่อความสงบสุขและมีเสถียรภาพของสังคม

6.2.3 ข้อเสนอแนะในเรื่องความเป็นส่วนตัวและสิทธิผู้บริโภคในสังคมดิจิตอล

ปัจจุบันอุปกรณ์ต่าง ๆ มีแนวโน้นจะนำเทคโนโลยีเพื่อการเชื่อมต่ออินเตอร์เน็ตเข้ามาเป็นส่วนหนึ่งของระบบการทำงาน ตั้งแต่อุปกรณ์พกพาไปจนถึงอุปกรณ์สวมใส่ต่าง ๆ โดยอุปกรณ์เหล่านี้มักมีการเก็บข้อมูลการใช้งานของผู้ใช้ เช่น เส้นทางการเดินทาง เว็บไซต์ที่เข้า ข้อมูลส่วนตัวต่าง ๆ ที่ผู้ใช้ได้บันทึกไว้ในระบบ เพื่อนำไปใช้ประโยชน์ในแง่ของข้อมูลสถิติเพื่อประโยชน์ทางการค้า[224] อย่างไรก็ดี การเก็บข้อมูลเหล่านี้โดยไม่ได้รับความยินยอมจากผู้ใช้นั้นนับเป็นการละเมิดสิทธิความเป็นส่วนตัว (Privacy) ของผู้ใช้ โดยหากปล่อยปละละเลยไม่มีการควบคุมดูแลที่เหมาะอาจทำให้ข้อมูลต่าง ๆ ที่มีความสำคัญในชีวิตประจำวันของประชาชนถูกนำไปใช้โดยมิชอบได้

นอกเหนือจากการลักลอบเก็บข้อมูลของภาคเอกชนแล้ว หลังจากมีการเปิดเผยการกระทำของ NSA (National Security Agency) ซึ่งเป็นหน่วยงานด้านความมั่นคงของสหรัฐอเมริกาโดยนายเอ็ดเวิร์ด สโนวเด็น อดีตเจ้าหน้าที่ CIA (Central Intelligent Agency) โดยจากข้อมูลดังกล่าวเปิดเผยว่า ผู้นำกว่า 35 ประเทศถูกสอดแนม ไม่เว้นแม้แต่ประชาชนในประเทศเองก็ถูกดักฟังข้อมูลทาง

---

[224] Arthur, C., iPhone keeps record of everywhere you go, *The guardian*, (2011, April 20), Retrieved 2014, October 9, from http://www.theguardian.com/technology/2011/apr/20/iphone-tracking-prompts-privacy-fears

โทรศัพท์และข้อมูลทางคอมพิวเตอร์[225] ซึ่งนอกจากปฏิบัติการของหน่วยงานของรัฐแล้วยังมีการขอความร่วมมืออย่างลับ ๆ ไปยังภาคเอกชนด้วย[226] การดักฟังประชาชนจำนวนมากและเจ้าหน้าที่ระดับสูงของรัฐบาลประเทศอื่น ๆ ไม่เว้นแม้แต่ประเทศพันธมิตรทำให้รัฐบาลหลายประเทศในยุโรปแสดงจุดยืนคัดค้านพฤติกรรมดังกล่าว[227] เหตุการณ์ที่เกิดขึ้นนี้อาจเป็นการละเมิดสิทธิมนุษยชนครั้งใหญ่ที่สุดของโลก ไม่ใช่เป็นเพียงเรื่องความไม่เหมาะสมทางการเมืองระหว่างประเทศเท่านั้น ซึ่งการออกมาเปิดเผยข้อมูลของอดีตเจ้าหน้าที่ CIA คนนี้ทำให้เกิดกระแสความตระหนักถึงการสอดแนมและละเมิดสิทธิส่วนบุคคลของประชาชนขึ้น เพราะไม่ใช่เพียง NSA เท่านั้นแต่ในประเทศอื่น ๆ ก็มีหน่วยงานแบบเดียวกันซึ่งมีนโยบายคล้ายคลึงกัน อย่างหน่วยงาน MI6 ของประเทศอังกฤษ หรือ มอสสาด (Mossad) ของอิสราเอล เป็นต้น โดยเหตุการณ์ดังกล่าวอาจทำให้เกิดความร่วมมือเพื่อสร้างข้อตกลงในระดับโลกขึ้นในรูปของสนธิสัญญาระหว่างประเทศเพื่อควบคุมการสอดแนมจากรัฐบาล

6.2.4 ข้อแนะนำในเรื่องแนวทางพัฒนาความร่วมมือในการพิจารณาคดี

การโจมตีไซเบอร์ที่เกิดขึ้นในรอบหลายปีมานี้เผยให้เห็นว่า แทบไม่มีผู้ถูกสืบสวนดำเนินคดีหรือตัดสินโทษเลย ซึ่งการกระทำเช่นนี้สมควรถูกกำหนดไว้ในสนธิสัญญาระดับโลกหรือข้อตกลงในระดับภูมิภาค เพื่อดำเนินการสืบสวนและดำเนินคดี โดยหากนับไซเบอร์สเปซเป็นพรหมแดนสามัญที่ 5 นอกเหนือจากพื้นดิน ทะเล อากาศ และ อวกาศแล้ว พื้นที่นี้ต้องการความร่วมมือทางกฎหมายระหว่างนานาประเทศเพื่อให้ชุมชนนานาชาติตระหนักถึงความสำคัญของการตอบสนองอย่างเร่งด่วนซึ่งภัยไซเบอร์ที่เพิ่มมากขึ้นเรื่อย ๆ ในอดีตศาลอาญาระหว่างประเทศถูกเรียกว่าเป็นส่วนสำคัญที่หายไปของระบบกฎหมายระหว่างประเทศ ในขณะนี้ซึ่งการขาดความร่วมมือในการพิจารณาคดีระหว่างประเทศ การมีศาลอาญาเฉพาะหรือศาลชำนัญพิเศษ (Tribunal)[228]

---

[225] Spying on allied leaders carries big risks: Our view, *USA Today*, (2013, October 24), Retrieved 2014, October 9, from http://www.usatoday.com/story/opinion/2013/10/24/nsa-eavesdropping-foreign-leaders-angela-merkel-editorials-debates/3183277/

[226] Hesseldahl, A., Apple denies working with NSA on iPhone backdoor, *AllthingsD*, (2013, December 31), Retrieved 2014, October 9, from http://allthingsd.com/20131231/apple-says-it-is-unaware-of-nsas-iphone-backdoor/

[227] EU leaders unite over US spying allegations, *Al Jazeera*, (2013, October 25), Retrieved 2014, March 4, from http://www.aljazeera.com/news/europe/2013/10/eu-leaders-unite-anger-over-us-spying-201310250312455233 3.html

[228] ศาลชำนัญพิเศษ เป็นศาลชั้นต้นที่ใช้วิธีพิจารณาพิเศษตามแตกต่างจากศาลชั้นต้นทั่วไป โดยผู้พิพากษาศาลชำนัญพิเศษจะเป็นผู้พิพากษาที่มีความรู้ความเข้าใจในเรื่องนั้น ๆ โดยเฉพาะ.

เพื่อตัดสินคดีอาชญากรรมทางคอมพิวเตอร์จึงมีความจำเป็นในการรับมืออาชญากรรมทางคอมพิวเตอร์ระดับสากล ซึ่งไซเบอร์สเปซเองควรได้รับความคุ้มครองด้วยกฎหมายระหว่างประเทศจากสนธิสัญญาและองค์กรระหว่างประเทศอย่างสหประชาชาติโดยการขยายขอบเขตอำนาจศาลอาญาระหว่างประเทศ แต่หากพิจารณาจากตำแหน่งของการให้สัตยาบันของศาลอาญาระหว่างประเทศแล้ว ทางออกที่ได้รับการยอมรับจากสหรัฐอเมริกา จีน และรัสเซีย ดูจะมีความเป็นไปได้มากกว่าซึ่งคงจำกัดอยู่ที่ศาลชำนัญพิเศษ

ศาลชำนัญพิเศษซึ่งโดยปกติแล้วจะเป็นการแก้ปัญหาขั้นต้นกลายเป็นทางเลือกเดียวในระดับโลก โดยอาจสมควรที่จะมีการพิจารณาเพื่อจัดตั้งศาลถาวรในอนาคตเพื่อจัดการปัญหาที่เกิดขึ้นในไซเบอร์สเปซ ซึ่งจะเป็นสัญญาณที่ดีจากองค์การสหประชาชาติและสังคมโลกว่าจะไม่อดกลั้นต่ออาชญากรรมทางคอมพิวเตอร์และการโจมตีไซเบอร์ซึ่งการจัดตั้งศาลชำนัญพิเศษระหว่างประเทศและการดำเนินคดีผู้กระทำผิดจะกลายเป็นการป้องปรามผู้คิดก่อเหตุอีกด้วย (Cyber attack deterrence)

การจัดตั้งศาลชำนัญพิเศษมีความจำเป็น การสำรวจจาก UNODC พบว่า 69 ประเทศมีเพียงประเทศในกลุ่มสหภาพยุโรปเท่านั้นที่เห็นว่ากรอบเค้าโครงกฎหมายที่มีอยู่เพียงพอต่อการจัดการปัญหาอาชญากรรมทางคอมพิวเตอร์ แต่กว่า 50% ของประเทศอื่น ๆ พบว่ามีกรอบเค้าโครงทางกฎหมายที่ไม่เพียงพอ โดยหลายประเทศจัดการปัญหากฎหมายขัดกันผ่านการเจรจาทั้งโดยทางการและไม่เป็นทางการระหว่างประเทศเท่านั้น โดยการใช้วิธีการดั้งเดิมของความร่วมมือในการพิจารณาคดีนั้นโดยพื้นฐานแล้วเพื่อการได้มาซึ่งหลักฐานนอกเขตอำนาจศาลในคดีอาชญากรรมทางคอมพิวเตอร์ กว่า 70% ใช้ความร่วมมือทางกฎหมายอย่างเป็นทางการ ซึ่ง 60% ของการร้องขอใช้วิธีการแบบทวิภาคี โดยวิธีการแบบพหุภาคีถูกใช้เพียง 20% จากกรณีดังกล่าวเท่านั้น โดยทั้งสองวิธีใช้เวลาดำเนินการหลายเดือน ซึ่งจะเป็นอุปสรรคอย่างยิ่งต่อการเก็บหลักฐานอิเล็กทรอนิกส์ที่เปลี่ยนแปลงได้ง่าย และแม้ว่าจะมีการใช้งานระบบตรวจสอบเครือข่ายตลอด 24 ชม 7 วันต่อสัปดาห์ที่ดูเหมือนจะช่วยเพิ่มศักยภาพในการรับมืออาชญากรรมทางคอมพิวเตอร์อย่างทันท่วงทีก็ตาม กลับมีเพียงแค่ 3% ของคดีอาชญากรรมทางคอมพิวเตอร์จากประเทศในรายงานผ่านระบบนี้เท่านั้น[229]

ในปัจจุบันเงื่อนไขที่เป็นทางการอย่าง การยินยอมของรัฐเมื่อเกิดการขัดกันของการบังคับใช้กฎหมายนับวันยิ่งกลายเป็นหลักที่ไม่ถูกปฏิบัติตามในคดีอาชญากรรมทางคอมพิวเตอร์ เนื่องจากการเข้าถึงข้อมูลโดยตรงโดยผู้สืบสวนมักถูกกระทำโดยไม่ได้รับความยินยอมจากประเทศที่ข้อมูล

---

[229] Expert Group to Conduct a Comprehensive Study on Cybercrime, *Comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector*, UNODC, (2013, January 23), Retrieved 2014, August 2, from http://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/ UNODC_CCPCJ_EG4_2013_2_E.pdf

นั้นอยู่ในทางกายภาพ ซึ่งหลักปฏิบัติในระดับภูมิภาคมุ่งไปที่การได้รับคำยินยอมจากบุคคลที่มีอำนาจเปิดเผยข้อมูลนั้นตามกฎหมายมากกว่า ซึ่งไม่อาจสนับสนุนการสืบสวนได้อย่างเพียงพอ การประมวลผลแบบกลุ่มเมฆและอาชญากรรมในระดับนานาชาติจะกลายเป็นอุปสรรคสำคัญและทำให้เกิดความต้องการกลไกทางกฎหมายเฉพาะเพื่อจัดการปัญหาดังกล่าว ซึ่งในปัจจุบันหลายภูมิภาคมีกลไกในการจัดการปัญหาการสืบสวนภายในกลุ่มของตนแต่กำหนดเงื่อนไขให้ทำการร้องขออย่างเป็นทางการแบบดั้งเดิมกับประเทศอื่น ๆ ภายนอกกลุ่ม การขาดกลไกที่เป็นสามัญในระดับโลกอาจทำให้เกิดปัญหาในเรื่องระยะเวลาการตอบรับการร้องขอได้

ซึ่งการขาดการตอบสนองที่รวดเร็ว การขาดข้อตกลงในการเข้าถึงข้อมูลนอกอาณาเขต รวมถึงระบบเครือข่ายการบังคับใช้กฎหมายอย่างไม่เป็นทางการและความร่วมมือที่หลากหลายเพื่ออุดช่องว่าง แสดงให้เห็นถึงอุปสรรคสำคัญในด้านการรับมืออาชญากรรมทางคอมพิวเตอร์

แม้จะไม่มีวิธีการที่จะสามารถจัดการครบทุกปัญหาได้ในคราวเดียวในการแก้ปัญหาอาชญากรรมทางคอมพิวเตอร์ซึ่งยังคงเป็นเรื่องที่ต้องมีการศึกษาทำความเข้าใจต่อไป แต่การสร้างมาตรฐานกลางในกรอบเค้าโครงด้านความมั่นคงไซเบอร์ในระดับภูมิภาคจะไม่เพียงเป็นประโยชน์ร่วมกันของประเทศสมาชิกอาเซียนเท่านั้น แต่จะเป็นประโยชน์ต่อภูมิภาคและประชาคมโลกโดยรวมอีกด้วย ในแผนแม่บทว่าด้วยความเชื่อมโยงระหว่างกันในภูมิภาคอาเซียน ได้กำหนดเป้าหมายหนึ่งเพื่อสร้างทางออกแบบสมประโยชน์ทุกฝ่ายแก่ประเทศสมาชิกอาเซียน โดยการเชื่อมโยงอาเซียนเข้าด้วยกันเพื่อสร้างตลาดร่วมตลาดเดียวและฐานการผลิตรวมทั้งการช่วยเหลือประเทศคู่เจรจาในเอเชียแปซิฟิกในด้านการขนส่งหรือขนถ่ายพลังงาน มาตรการเหล่านี้จะช่วยยกตำแหน่งอาเซียนในเวทีการประชุมนานาชาติ และช่วยส่งเสริมความพยายามในการปรับปรุงโครงสร้างของการจัดการภายในภูมิภาคที่พัฒนาขึ้นเรื่อย ๆ และสนับสนุนความร่วมมือระหว่างประเทศในขณะนั้นและในอนาคตเช่นเดียวกับความพยายามในด้านการรักษาความปลอดภัยไซเบอร์ที่มีความจำเป็นในการรับมือกับอาชญากรรมทางคอมพิวเตอร์ซึ่งมีลักษณะข้ามชาติอย่างมีประสิทธิภาพ รัฐบาลและสถาบันต่าง ๆ จำเป็นต้องปรับตัวอย่างรวดเร็วให้เท่าทันต่อเหตุการณ์และเพื่อคาดการณ์ถึงแนวโน้มที่จะเกิดขึ้น เพราะฉะนั้น เพื่อหลีกเลี่ยงการเพลี่ยงพล้ำต่อการเปลี่ยนแปลงการรับเอาโครงสร้างและวิธีการคิดใหม่ ๆ มาใช้เป็นสิ่งที่อาเซียนและประเทศสมาชิกต้องทำอยู่เสมอ

6.3 ข้อเสนอแนะเพื่อการศึกษาเพิ่มเติมในอนาคต

ปัจจุบันสมาชิกอาเซียนบางประเทศยังขาดกฎหมายเพื่อรับมืออาชญากรรมทางคอมพิวเตอร์ที่เป็นรูปธรรมอย่างประเทศลาวและกัมพูชา ซึ่งสามารถทำการศึกษาเพื่อพัฒนา

กฎหมายให้ออกมาสอดคล้องกับกรอบเค้าโครงทั้งในระดับสากลและของภูมิภาคที่กำลังมีความพยายามพัฒนาหลักเกณฑ์กลางทางกฎหมายอาชญากรรมทางคอมพิวเตอร์อยู่เช่นกัน อีกทั้งการศึกษาหาแนวทางเพื่อสร้างมาตรฐานในด้านความร่วมมือระหว่างประเทศในการสืบสวนคดีความและการใช้อำนาจนอกอาณาเขตเพื่อเข้าถึงข้อมูลซึ่งต้องการความรวดเร็วในการดำเนินการ ที่ในปัจจุบันมักใช้วิธีการอย่างไม่เป็นทางการมากกว่าการปฏิบัติตามหลักเกณฑ์ที่มีข้อจำกัดสูง การพัฒนากฎหมายอาชญากรรมทางคอมพิวเตอร์เพื่อรองรับการเปลี่ยนแปลงทางเทคโนโลยี เช่น การประมวลผลแบบกลุ่มเมฆ รวมไปถึงการศึกษากฎหมายคุ้มครองข้อมูลส่วนบุคคลเพื่อคุ้มครองข้อมูลของผู้ใช้ซึ่งนับวันยิ่งมีความจำเป็นต้องได้รับความคุ้มครองมากขึ้นเรื่อย ๆ จากการลักลอบเก็บข้อมูลของผู้ให้บริการ ผู้ผลิตอุปกรณ์หรือแม้แต่รัฐ อีกทั้งการศึกษาแนวโน้มและพัฒนาการของกฎเกณฑ์และมาตรการเพื่อควบคุมและกำกับการการทำสงครามไซเบอร์ซึ่งสามารถสร้างความเสียหายได้เช่นเดียวกับการทำสงครามรูปแบบดั้งเดิมอีกด้วย

รายการอ้างอิง

รายการอ้างอิง

กนก อินทรัมพรรย์. (2527, มีนาคม–เมษายน). ความเห็นและข้อสังเกตในเรื่องความร่วมมือทางศาลเกี่ยวกับการยอมรับบังคับตามคำพิพากษาศาลต่างประเทศ. *ดุลพาห*, *2*(31), 56-69.

ความริเริ่มเพื่อการรวมตัวของอาเซียน. (ม.ป.ป.). สืบค้นเมื่อ 10 สิงหาคม 2555 จาก http://www.mfa.go.th/asean/contents/files/asean-media-center-20121218-095324-481007.pdf

ณกฤช เศวตนันท์. (2555, พฤศจิกายน). กฎใหม่ ITU. *วิเคราะห์ตลาดโทรคมนาคม*, *11*(2).

ธีรศักดิ์ กองสมบัติ. (2552). *เขตอำนาจศาลเหนือการกระทำละเมิดทางแพ่งในไซเบอร์สเปซ*. วิทยานิพนธ์นิติศาสตรมหาบัณฑิต สาขาวิชานิติศาสตร์. มหาวิทยาลัยธรรมศาสตร์, กรุงเทพฯ.

ประสิทธิ ปิวาวัฒนพานิช. (2551). *คำอธิบายกฎหมายระหว่างประเทศแผนกคดีบุคคล*. กรุงเทพฯ: มหาวิทยาลัยธรรมศาสตร์.

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ. (ม.ป.ป.). *โครงการศึกษาวิจัยการอภิบาลกิจการเกี่ยวกับอินเตอร์เน็ต*. สืบค้นเมื่อ 13 กรกฎาคม 2555, จาก http://www.nectec.or.th/pld/igovernanace/index.htm

ศูนย์บริการข้อมูลเศรษฐกิจระหว่างประเทศ. (ม.ป.ป.). *ภูมิหลัง APEC*. สืบค้นเมื่อ 8 ตุลาคม 2557, จาก http://www.mfa.go.th/business/th/customize/16530-ภูมิหลัง-APEC.html

สมณ์ พรหมรส. (ม.ป.ป). *คำแปลปฏิญญากรุงเทพฯ*. สำนักงานกิจการยุติธรรม. สืบค้นเมื่อ 4 กันยายน 2555, จาก, http://www.oja.go.th/new2011/document/Lists/Download_1/Attachments/36/oja_symposium_5_G3_room6_6.pdf

สราวุธ ปิติยาศักดิ์. (2555). *กฎหมายเทคโนโลยีสารสนเทศ*, กรุงเทพฯ: นิติธรรม.

สาวิตรี สุขศรี. (ม.ป.ป.). *ประวัติศาสตร์ อาชญากรรมคอมพิวเตอร์*. สืบค้นเมื่อ 17 ตุลาคม 2555, จาก http://facthai.wordpress.com/2009/11/09/ประวัติศาสตร์-อาชญากรรม/

อานนท์ ศรีบุญโรจน์. (2554). *การรับรองและการบังคับตามคำพิพากษาศาลต่างประเทศในกลุ่มประเทศอาเซียน*. วิทยานิพนธ์นิติศาสตรมหาบัณฑิต สาขาวิชานิติศาสตร์. มหาวิทยาลัยธรรมศาสตร์, กรุงเทพฯ.

2011 IGF Nairobi. (2011). *Internet Governance Forum*. Retrieved 2013, December 26, from www.intgovforum.org/cms/2011-igf-nairobi

A Paper for the 12th Conference of Directors of Criminological Research Institutes. (1976, 15-18 November). *Criminological Aspects of Economic Crime*. (Strasbourg), pp. 225-229.

Acosta, R. (n.d.). DOJ deletes libel from new anti-cybercrime. *Businessmirror*. Retrieved 2014, April 27, from http://www.businessmirror.com.ph/index.php/en/news/nation/13927-doj-deletes-libel-from-new-anti-cybercrime-bill

AKAMAI. (2013). *The state of the internet 2013 full report*. Retrieved 2014, February 3, from http://www.akamai.com/dl/akamai/akamai_soti_q113.pdf

APEC. (n.d.). *Fact sheets (APEC data privacy pathfinder)*. Retrieved 2013, 22 September, from http://www.apec.org/About-Us/About-APEC/Fact-Sheets/APEC-Privacy-Framework.aspx

ARF Cybercrime capacity building Conference. (2010, April). *Co-chairs summary report.* Banda Seri Begawan Brunei Darussalam April 27-28 2010.

ARF. (2010, April). *Co-Chairs summary report ARF Cybercrime capacity building conference Bandar Seri Begawan Brunei Darussalam April 27-28 2010, 4*. Retrieved 2014, September 19, from http://aseanregionalforum.asean.org/files/library/ARF%20Chairman's%20Statements%20and%20Reports/The%20Seventeenth%20ASEAN%20Regional%20Forum,%202009-2010/Cybercrime%20Conference%20Summary%20Report.doc

Arthur, C. (2011, April 20). iPhone keeps record of everywhere you go. *The guardian*. Retrieved 2014, October 9, from http://www.theguardian.com/technology/2011/apr/20/iphone-tracking-prompts-privacy-fears

ASEAN Business Forum. (2013, August 1). *Laos officials train to fight cybercrime*. Retrieved 2013, December 10, from http://www.aseanbusinessforum.com/news/allDetail.php?sec=1&id=48763

ASEAN E-Commerce Project. (2006, May). *Documented analysis of international activity in electronic contracting and Online Dispute Resolution (ODR)–Discussion paper 4 (DP4)*. ASEAN secretariat and Galexia, (Internal project materials).

ASEAN secretariat and Galexia. (2004, November). *Harmonization structure are from ASEAN E-Commerce Project*. Documented Analysis of International Developments–Discussion Paper 2 (DP2), (internal project materials).

ASEAN secretariat and Galexia. (2005, February). *Survey of implementation issues and constraints for a harmonized e-commerce legal infrastructure in ASEAN*. ASEAN e-commerce Project, (S2), (internal project materials).

ASEAN Secretariat. (2004, November 29). *Roadmap for integration of e-ASEAN sector*. Retrieved 2013, September 7, from http://aseansec.org/16689.htm

ASTVผู้จัดการออนไลน์. (2556, พฤษภาคม 8). *มือดีแฮกเว็บสำนักนายกฯ ด่า "ยิ่งลักษณ์" เย้ย ICT*. สืบค้นเมื่อ 7 ธันวาคม 2556, จาก http://www.manager.co.th/Politics/ViewNews.aspx?NewsID=956000005516

Binlot, A. (2008, December 30). Vietnam bloggers face government crackdown. *TIME*. Retrieved 2014, March 19, from http://www.time.com/time/world/article/0.8599.1869130.00.html

Buerk, R. (2011, September 20). *Japan defence firm Mitsubishi heavy in cyber attack*. BBC News. Retrieved 2013, October 17, from http://www.bbc.co.uk/news/world-asia-pacific-14982906

Center for International Security and Cooperation (CISAC) Stanford University. (2000, August). *A proposal for an international convention on cybercrime and terrorism*. Retrieved 2013, October 17, from http://cisac.stanford.edu/publications/11912

Chan, Y. C. (2010). *Cybercrime across the Taiwan strait—Regulatory responses and crime prevention*. Unpublished Ph.D. thesis. Australian National University, Canberra.

Chang, W., Chung, W., Chen, H., & Chou, S. (2013). *An international perspective on fighting cybercrime*. ISI'03 Proceedings of the 1st NSF/NIJ Symposium on Intelligence and security informatics (ISI 2003). Arizona: Springer. pp. 379-384.

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

Collins, L. A., Dicey, A. V., & Carlile Morris, J. H. (2000). *Dicey and Morris on the conflict of laws Vol. 1* (13th ed.). London: Sweet & Maxwell.

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. (2001). Retrieved 2014, April 6, from http://www.etsi.org/public-interest/Documents/PoliticalInitiatives/Com2001_0298.pdf

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. (2001). Retrieved 2013, March 19, from http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/CrimeCommEN.htm

Congressional Research Service. (2004). *The Economic Impact of Cyber-Attacks*. Washington D.C.: CRS.

Council of Europe. *(2008). Cybercrime legislation–Brunei country profile*. Retrieved 2013, December 19, from http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documentscountryprofiles/cyber_cp_Brunei_%202008_November.pdf

Council of Europe. (2009). *Project on cybercrime final report (September 2006-February 2009)*. Strasburg: Council of Europe.

Council of Europe. (n.d.). *Convention on cybercrime CETS No.: 185*. Retrieved 2014, August 19, from http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG

Csonka, P. (2001, October 1). The draft council of Europe convention on Cybercrime: A response to the challenge of crime in the age of the Internet. *Computer Law & Security Report. 16*(5).

Cyber-attack from server in china targets lower house. (2011, October 25). *Asahi Shimbun*. Retrieved 2013, October 17, from http://ajw.asahi.com/article/behind_news/social_affairs/AJ2011102515710

Estonia hit by "Moscow cyber war". (2007, May 17). *BBC News*. Retrieved 2013, October 17, from http://news.bbc.co.uk/2/hi/europe/6665145.stm

EU leaders unite over US spying allegations. (2013, October 25). *Al Jazeera*. Retrieved 2014, March 4, from http://www.aljazeera.com/news/europe/2013/10/eu-leaders-unite-anger-over-us-spying-201310250312455233 3.html

EU-ASEAN Workshop on Cybercrime Legislation in the ASEAN Member States. (n.d.). Retrieved 2013, June 18, from http://www.asean.org/archive/apris2/file_pdf/Press %20Releases/EU-ASEAN%20Workshop%20on%20 Cybercrime%20 Legislation%20in%20the%20ASEAN%20Member%20States.pdf

Expert Group to Conduct a Comprehensive Study on Cybercrime. (2013, January 23). *Comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector*. UNODC. Retrieved 2014, August 2, from http://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_E.pdf

Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. (n.d.). *OECD*. Retrieved 2014, February 23, from http://www.oecd.org/internet/interneteconomy/15582260.pdf

Hanifah, A. (2013, July 29). Indonesia to create its own "cyber army". *Xinhua*. Retrieved 2014, April 4, from http://news.xinhuanet.com/english/world/2013-05/29/c_132416837.htm

Heinl, C. H. (July 2014). Regional cybersecurity moving toward a resilient ASEAN cybersecurity regime. *ASIA Policy*, *18*.

Hesseldahl, A. (2013, December 31). Apple denies working with NSA on iPhone backdoor. *AllthingsD*. Retrieved 2014, October 9, from http://allthingsd.com/20131231/apple-says-it-is-unaware-of-nsas-iphone-backdoor/

Huffingtonpost. (n.d.). *Norway attacks: police lower youth camp death toll to 68*. Retrieved 2014, August 17, from http://www.huffingtonpost.com/2011/07/25/norway-attacks-police_n_908647.html

IBM survey published 14.05.2006. Retrieved 2013, October 17. from http://www.03.ibm.com/industries/consumerproducts/doc/content/news/pressrelease/1540939123.html

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

International Review of Criminal Policy. *UN Manual on the prevention and control of computer-related crime*. Retrieved 6 April 2014, from http://www.uncjin.org/Documents/EighthCongress.html

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

International Telecommunication Union. (2012). *Draft of the Future ITRs*. Retrieved 2014, April 19, from http://www.itu.int/en/wcit-12/Documents/draft-future-itrs-public.pdf

International Telecommunication Union. *Final ACTS of the World Conference on International Telecommunications*. (2012). Dubai, ITU. Retrieved 2014, April 19, from http://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf

IZONE. (ม.ป.ป.). *การท่องเว็บแบบปกปิดตัวตน ตอนที่ 7 (Tor)*. สืบค้นเมื่อ 11 สิงหาคม 2557. จาก http://izonex.wordpress.com/2008/10/26/anoymous-software-tor/

Kurbalijia, J. (n.d.). *Internet governance and international law*. Retrieved 2013, October 17, from http://www.wgig.org/docs/book/Jovan_Kurbalija%20.pdf

Lee, A. (2013, June 13). CIA Chief Leon Panetta: Cyber attack could be next pearl harbor. *The Huffington Post*. Retrieved 2013, October 17, from http://www.huffingtonpost.com/ 2011/06/13/panetta-cyberattack-next-pearl-harbor_n_875889.html

Lennon, L. Y.-c. (2012). *Cybercrime in the Greater China Region: Regulatory Responses and Crime Prevention Across the Taiwan Strait*. United Kingdom: Edward Elgar publishing.

Maggie, S. (2009, September 4). Spies "infiltrate US power grid". *BBC News*. Retrieved 2013, October 17, from http://news.bbc.co.uk/2/hi/technology/7990997.stm

Malaysia. (n.d.). *Global Resource and Information Directory*. Retrieved 2014, March 21, from http://www.fosigrid.org/asia/Malaysia

Malware Hits Computerized Industrial Equipment. (2010, September 24). *New York Times*. Retrieved 2013, October 17, from http://bits.blogs.nytimes.com/2010/09/24/malware-hits-computerized-industrial-equipment/

McGonagle, T. (n.d.). *European commission adoption of proposal to combat cybercrime*. Netherland: Institute for Information Law (IViR), University of Amsterdam. Retrieved 2013, October 17, from http://merlin.obs.coe.int/iris/2002/6/article7.en.html

Meeting of G8 Justice and Interior Ministers. (1997). *Principles and action plan to combat high-tech crime*. Washington, D.C.: n.p. Retrieved 2014, February 24, from http://www.coe.int/T/e/legal_affairs/Legal_cooperation/Fight_against_terrorism/Texts_&_documents/Principles%20and%20Action.pdf

Milian, M. (2013, July 23). Indonesia joins China as cyber-attack powerhouse. *Bloomberg*. Retrieved 2014, September 9, from http://www.bloomberg.com/news/2013-07-23/indonesia-joins-china-as-cyber-attack-powerhouse.html

Muncaster, P. (2013, January 30). Indonesian hackers protest hacker's arrest by hacking. *The Register*. Retrieved, 2014, April 4, from http://www.theregister.co.uk/2013/01/30/hacker_indonesia_sby_arrest/

NATO Cooperative Cyber Defense Centre of Excellence Tallinn, Estonia. (n.d.). Retrieved , 2014, April 6, from http://www.ccdcoe.org/

NECTEC. (ม.ป.ป.). *คำถามที่พบบ่อยเกี่ยวกับร่างพระราชบัญญัติการกระทำผิดเกี่ยวกับคอมพิวเตอร์*. สืบค้นเมื่อ 11 พฤศจิกายน 2556. จาก http://wiki.nectec.or.th/nectecpedia2/index.php/คำถามที่พบบ่อย_เกี่ยวกับร่างพรบ.การกระทำผิดเกี่ยวกับคอมพิวเตอร์

Nexusguard. (n.d.). *When it comes to defending against DDoS attacks, DDoS alert: taiwan and the philippines exchanging digital Blows*. Retrieved 2013, December 7, from http://www.prweb.com/releases/2013/5/ prweb10735330.htm

Noor, M. (2010). *Cyber Legislation of Indonesia*. Paper presented at the Octopus Interface Conference-Cooperation against Cybercrime. Retrieved 2013, July 11, from http://unpan1.un.org/intradoc/groups/public/documents/ UNGC/UNPAN040467.pdf

Nugraha, Y. (2012, July). *Social Media Ecosystem in Indonesia*. ITU-ASEAN Forum on Promoting Effective and Secure Social Media 18-19 July 2012. Kuala Lumpur, Malaysia. Retrieved 2013, December 4, from http://www.itu.int/ITU-D/asp/CMS/Events/2012/socialmedia/S6.3_Indonesia.pdf

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

Organization for Co-operation Development. (1986). *Computer related criminality: Analysis of Legal Politics in the OECD Area*. Paris: OECD.

Organization for Co-operation Development. (n.d.). *Computer related criminality: Analysis of legal politics in the OECD area*.

Orwell, G. (1949). *Nineteen eighty-four, A novel*. London: Secker & Warburg.

Pantip. (n.d.). *เตือนภัย Internet Banking รูปแบบใหม่ ปลอมเป็นตัวคุณ(Clone) แล้วสวมรอยโอนเงินออกไป อย่างง่ายดาย*. สืบค้นเมื่อ 10 สิงหาคม 2557. จาก http://pantip.com/topic/30799070

Pedrasa, I. (2012, 9 September). SC issues 120-day TRO vs cybercrime law. *ABS CBN News*. Retrieved 2014, February 3, from http://www.abs-cbnnews.com/nation/10/09/12/sc-issues-tro-vs-cybercrime-law-source/

Personal Data Protection Commission Singapore. (2014, January 28). *Personal Data Protection Act: Overview*. Retrieved 2014, March 8, from http://www.pdpc.gov.sg/personal-data-protection-act

Phneah, E. (2012, 11 December). Philippine govt asks court to lift injunction on Cybercrime Law. *ZDNET*. Retrieved 2014, April 27, from http://www.zdnet.com/ph/philippine-govt-asks-court-to-lift-injunction-on-cybercrime-law-7000008597/

Press Conference on the Results of the G8 Justice and Home Affairs Ministerial. (2006, 16 June). Retrieved 2014, February 24, from http://www.g8.utoronto.ca/justice/justice2006.htm

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

Regional Internet Governance Forum. (2011, July 13). *About APrIGF 2011*. Retrieved 2011, July 13, from http://2011.rigf.asia/

Schjolberg, S. (1986). *Computers and penal legislation–A study of legal politics of a new technology*. Germany: Universitetsforlaget.

Schjolberg, S. (2013). *Crossing jurisdictional boundaries*. Hague, Netherland: Europol Headquarter. Retrieved 23 February, 2014, from http://www.cybercrimelaw.net/documents/Europol-INTERPOL.pdf

Schjolberg, S., & Ghernaouti-Helie, S. (2011*). A global treaty on cybersecurity and cybercrime (Second Edition)*. Retrieved 2013, December 4, from http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime_Second_edition_2011.pdf

Schjolberg. (2012, March). *An international criminal tribunal for cyberspace*. A paper for the EastWest Institute (EWI) Cybercrime Legal Working Group 10. Retrieved 2014, August 13, from http://www.cybercrimelaw.net/documents/ICTC.pdf

Scoles, E. F., & Hay, P. (2000). *Conflict of Laws* (3rd ed.). St. Paul, MN: West Group.

Sieber, U. (1986). *The international handbook on computer crime*. New York: Wiley.

South East Asia Cyberwatch. (2012, June). *Citizen Lab*. Retrieved 2014, March 7, from https://citizenlab.org/2012/06/southeast-asia-cyber-watch-june-2012-2/#ph

SPS NATO. (2007). *Cyber terrorist-a serious threat to peace and security in the 21st century.* Retrieved 2014, April 6, from http://www.nato.int/science/news/2007/n070702b.htm

Spying on allied leaders carries big risks: Our view. (2013, October 24). *USA Today*. Retrieved 2014, October 9, from http://www.usatoday.com/story/opinion/2013/10/24/nsa-eavesdropping-foreign-leaders-angela-merkel-editorials-debates/3183277/

SRI international. (1979). *The criminal justice resource manual on computer crime*. Menlo Park, CA: SRI international.

Symantec. (2011, April). *Symantec internet security threat report trends for 2010*. Retrieved 2014, August 17, from https://www4.symantec.com/mktginfo/downloads/21182883_GA_REPORT_ISTR_Main-Report_04-11_HI-RES.pdf

The European Parliament. (2001, January 26). *The economic and social committee and the committee of the regions*. Retrieved 2013, October 17, from http://eur-lex.europa.eu/legal-content/.EN/ALL/;ELX_SESSIONID=GwZLJy5TV3NhBcLyRM882MNrT022QNfGD15kddlNskcvqkPkC7PJ!-7040371?uri=CELEX:52000DC0890

U.S. catches "Love" virus. (n.d.). *CNN Money*. Retrieved 2014, March 31, from http://money.cnn.com/2000/05/05/technology/loveyou/

UNCTAD. (2007). *Information Economy Report 2007-2008*. Geneva: United Nations.

UNCTAD. (2013). *Review of e-commerce legislation harmonization in the Association of Southeast Asian Nations (ASEAN) [UNCTAD/DTL/STICT/2013/1]*. Geneva: UNCTAD.

UNCTAD. (2013, 20 September). *UNCTAD review of ASEAN e-commerce laws published*. Retrieved 2014, April 24, from http://unctad.org/en/pages/newsdetails.aspx?OriginalVersionID=613&Sitemap_x0020_Taxonomy=UNCTAD%20Home;

United Nations. (n.d.). *International review of criminal policy-United Nations manual on the prevention and control of computer-related crime.* Retrieved 2013, November 10, from www.uncjin.org/Documents/irpc4344.pdf

United Nations. International review of criminal policy. (1994). *The United Nations Manual on computer-related crime*, *43-44*. Retrieved 2014, February 23, from http://www.uncjin.org/Documents/EighthCongress.html

Vietnam and China hackers escalate Spratly Islands row. (2011, June 9). *BBC News*. Retrieved 2013, October 17, from http://www.bbc.co.uk/news/world-asia-pacific-13707921

Ward, M. (2009, October 29). Celebrating 40 years of the net: Technology correspondent. *BBC News*. Retrieved 2013, October 8, from http://news.bbc.co.uk/2/hi/technology/8331253.stm

World Internet Users and Population Stats. (n.d.). Retrieved 2014, February 23, from http://www.internetworldstats.com/ stats.htm



ภาคผนวก

ภาคผนวก ก

อนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์

Convention on Cybercrime

Budapest, 23.XI.2001

Preamble

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with the other States parties to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the

misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation;

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;

Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;

Considering the 1989 United Nations Convention on the Rights of the Child and the 1999 International Labour Organization Worst Forms of Child Labour Convention;

Taking into account the existing Council of Europe conventions on co-operation in the penal field, as well as similar treaties which exist between Council of Europe member States and other States, and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;

Welcoming recent developments which further advance international understanding and co-operation in combating cybercrime, including action taken by the United Nations, the OECD, the European Union and the G8;

Recalling Committee of Ministers Recommendations No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, No. R (88) 2 on piracy in the field of copyright and neighbouring rights, No. R (87) 15 regulating the use of personal data in the police sector, No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. R (95) 13 concerning problems of criminal procedural law connected with information technology;

Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, 10 and 11 June 1997), which recommended that the Committee of Ministers support the work on cybercrime carried out by the European Committee on Crime Problems (CDPC) in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation into such offences, as well as to Resolution No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, 8 and 9 June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cybercrime;

Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10 and 11 October 1997), to seek common responses to the development of the new information technologies based on the standards and values of the Council of Europe;

Have agreed as follows:

Chapter II – Measures to be taken at the national level

Section 2 – Procedural law

Title 2 – Expedited preservation of stored computer data

Article 16 – Expedited preservation of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of

specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Chapter III – International co-operation

Section 2 – Specific provisions

Title 1 – Mutual assistance regarding provisional measures

Article 29 – Expedited preservation of stored computer data

1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

2 A request for preservation made under paragraph 1 shall specify:

a the authority seeking the preservation;

b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

c the stored computer data to be preserved and its relationship to the offence;

d any available information identifying the custodian of the stored computer data or the location of the computer system;

e the necessity of the preservation; and

f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5 In addition, a request for preservation may only be refused if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.

6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

7 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

Article 30 – Expedited disclosure of preserved traffic data

1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the

requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

2 Disclosure of traffic data under paragraph 1 may only be withheld if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.

ภาคผนวก ข

ASEAN ICT MASTER PLAN 2015

4: Infrastructure Development

Infrastructure development is one of the three foundation thrusts recognized to be necessary for the successful implementation of the three thrusts mentioned above. In this context, the focus includes seeking to provide the infrastructure backbone to enable ICT services to all communities in ASEAN. Also, to put in place the required enabling policies and legislation to attract businesses and investments to the region.

Initiative 4.1: Improve broadband Connectivity

ACTION	DESCRIPTION
Establish an ASEAN Broadband Corridor	• Identify and develop locations in each ASEAN Member State which offer quality broadband connectivity • Enable seamless usage of broadband services and applications across ASEAN to further connect and enhance the development of ICT and other sectors • Promote the diversity of international connectivity among ASEAN Member States
Establish an ASEAN Internet Exchange Network	• Establish a regulator-operator forum to develop a platform to facilitate intra-ASEAN internet traffic • Facilitate peering amongst ASEAN internet access providers to improve latency and speeds as well as lower costs

Initiative 4.2: Promote network integrity and information security, data protection and CERT cooperation

ACTION	DESCRIPTION
Develop common framework for network security	• Establish common minimum standards for network security to ensure a level of preparedness and integrity of networks across ASEAN • Develop a network security "health screening" programme for ASEAN to be implemented at regular intervals • Develop best practice models for business continuity and disaster recovery for all sectors • Establish the ASEAN Network Security Action Council (multi-stakeholder) to promote CERT cooperation and sharing of expertise, amongst others
Develop common framework for information security	• Share best practices on the protection of data and information infrastructure across ASEAN

ภาคผนวก ค

ASEAN POLITICAL SECURITY BLUEPRINT

B.4. Non-Traditional Security Issues

25. A key purpose of ASEAN is to respond effectively and in a timely manner, in accordance with the principles of comprehensive security, to all forms of threats, transnational crimes and transboundary challenges.

B.4.1. Strengthen cooperation in addressing non-traditional security issues, particularly in combating transnational crimes and other transboundary challenges

Actions:

i. Implement effectively eight priority areas in the Work Programme to Implement the
ii. Plan of Action to Combat Transnational Crime;
Endeavour to ratify the Treaty on Mutual Legal Assistance in Criminal Matters among
iii. ASEAN Member States and work towards elevating it to an ASEAN treaty;
Continue the work of the working group, as mandated by the ASEAN Law Ministers'
iv. Meeting, to enhance cooperation on the issue of extradition;
Further strengthen criminal justice responses to trafficking in persons, bearing in mind the need to protect victims of trafficking in accordance with the ASEAN Declaration Against Trafficking in Persons Particularly Women and Children, and where applicable,
v. other relevant international conventions and protocols on trafficking in persons;
vi. Enhance cooperation to combat people-smuggling;
Work towards a drug-free ASEAN by 2015, in accordance with the ASEAN Work Plan for Combating Illicit Drug-Trafficking, by: strengthening measures to prevent the illicit production of drugs, import and export of controlled chemical precursors as well as regional cooperation in controlled delivery; and enhancing cross-border law enforcement cooperation through information sharing, best practices, and capacity building, in

vii. combating drug-trafficking;

viii. Develop multilateral or bilateral legal arrangements towards combating drug and precursor chemical trafficking starting in 2008;

ix. Provide assistance to ASEAN Member States in enhancing scientific laboratory capacity in precursor identification and drugs signature analysis for drug enforcement operation and intelligence;

x. Provide transfer of knowledge concerning the profile of drug crime syndicate groups as well as watch-list of their drug activities;

xi. Provide transfer of knowledge on best practices on the disposal of precursors and essential chemicals seized from clandestine laboratories;

xii. Strengthen the capacity of the criminal justice system including judges, prosecutors and law enforcement officials on drug control;

xiii. Enhance cooperation with relevant external parties in combating transnational crimes, including countering terrorism;

xiv. Enhance cooperation and coordination among existing ASEAN sectoral bodies in dealing with transnational crimes;

xv. Strengthen close cooperation among ASEAN Member States, to combat IUU fishing in the region and where applicable, through the implementation of the IPOA - IUU fishing and work towards the establishment of ASEAN Fisheries Consultative Forum (AFCF);

xvi. Promote full implementation by relevant sectoral bodies, to prevent, combat and eradicate the illicit trade in small arms and light weapons in all its aspects, in accordance with the UN Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All its Aspects (UN PoA) and the International Instrument to enable States to Identify and Trace, in Timely and Reliable Manner, Illicit Small Arms and Light Weapons (International Tracing Instrument);

xvii. Strengthen cooperation and assistance in combating and suppressing cyber crimes including cooperation among law enforcement agencies, taking into account the need of each country to develop laws to address cyber crimes;

xviii. Forge closer cooperation in fighting against sea piracy, armed robbery against ships, hijacking and smuggling, in accordance with international laws; and

Strengthen cooperation in the field of border management to jointly address matters of common concern, including forgeries of identification and travel documents, by enhancing the use of relevant technologies to effectively stem the flow of terrorists and criminals.

ภาคผนวก ง

MASTER PLAN ON ASEAN CONECTIVITY

Strategy 6: Accelerate the development of ICT infrastructure and services in each of the ASEAN Member States

11. A robust ICT infrastructure in tandem with better human resources and regulatory environment is critical for enabling ICT as an engine of trade, economic growth, innovation and better governance in the ASEAN region. A number of countries in the region are gaining global reputation in ICT infrastructure, ICT-based industries and services. However, the digital divide within ASEAN remains, especially between the lagging regions and the urban areas on the one hand and between countries on the other hand. The digital divide needs to be reduced in order to narrow the development gaps within the region.

Key actions:

(i) Establish an ASEAN Broadband Corridor by identifying and developing locations in each ASEAN Member State to offer quality broadband connectivity. This will enable seamless usage of broadband services and applications across ASEAN to further connect and enhance the development of ICT and other sectors by 2014.

(ii) Promote the diversity of international connectivity among ASEAN Member States by 2015.

(iii) Establish an ASEAN Internet Exchange Network to facilitate peering amongst ASEAN internet access providers to reduce latency and increase speed as well as lower costs by 2013.

(iv) Promote network integrity and information security, data protection and Computer Emergency Response Team (CERT) cooperation by developing common frameworks and establishing common minimum standards where appropriate, to ensure a level of preparedness and integrity of networks across ASEAN by 2015.

(v) Review Universal Service obligations and/or similar policies to ensure that infrastructure covered under these policies are broadband Internet capable by 2015.

(vi) Prioritise and expedite roll-out of broadband Internet capable infrastructure to schools by 2015.

(vii) Conduct feasibility study on developing after 2015 an ASEAN Single Telecommunications Market, in the context of free flow of products, services, investments and skilled human resources by 2015.



ประวัติผู้เขียน

ประวัติผู้เขียน

ชื่อ นายวรณัฐ บุญเจริญ

วัน เดือน ปีเกิด 2 กันยายน 2527

สถานที่อยู่ปัจจุบัน เลขที่ 128 หมู่ 10 ตำบลแม่เจดีย์
อำเภอเวียงป่าเป้า จังหวัดเชียงราย 57260

ประวัติการศึกษา

2550 ปริญญาตรี นิติศาสตรบัณฑิต
นิติศาสตร์ มหาวิทยาลัยแม่ฟ้าหลวง