วารสารเมธีวิจัย Savant Journal of Social Sciences
ปีที่ 1 ฉบับที่ 5 กันยายน – ตุลาคม 2567
Volume 1 Number 5 September - October 2024

ปัญหาความมั่นคงไซเบอร์และความร่วมมือในการแก้ปัญหา

Cyber security problems and cooperation in solving them

ชนลดา อินบุตร
Chonlada Inbut
คณะสังคมศาสตร์, มหาวิทยาลัยมหามกุฏราชวิทยาลัย วิทยาเขตอีสาน
Faculty of Social Sciences, Mahamakut Buddhist University Isan Campus.
Corresponding Author, E-mail: giftchonlada29@gmail.com

Received 02/03/2024 | Revised 26/06/2024 | Accepted 26/06/2024

บทความวิชาการ (Academic Article)

บทคัดย่อ

บทความวิชาการนี้มีวัตถุประสงค์เพื่อศึกษาปัญหาความมั่นคงไซเบอร์และความร่วมมือในการแก้ปัญหา ไม่ว่าจะในภาครัฐและภาคเอกชน เพราะในปัจจุบันนี้บุคลากรของภาครัฐนั้นส่วนมากจะเป็นคนรุ่นเก่าที่ยังขาดความเข้าใจและความรู้ในการเข้าถึงปัญหาไซเบอร์ จึงทำให้เกิดปัญหาในการที่จะทำให้ข้อมูลทางด้านเทคโนโลยีมีความปลอดภัยทางการใช้งาน แต่ในทางกลับกันยังมีความเสี่ยงสูงจากการขาดความรู้และความเข้าใจ ในการใช้ที่เทคโนโลยีระบบสารสนเทศนี้ ซึ่งจะปฏิเสธไม่ได้ว่าระบบใหม่ ๆ เข้ามามีบทบาทในการทำงานจัดเก็บข้อมูลหรือที่เรียกว่าฐานข้อมูลสารสนเทศ อีกทั้งยังเป็นช่องทางให้เกิดทั้งข้อดีและข้อเสียในการทำงานในปัจจุบันนี้อย่างมาก

คำสำคัญ: ปัญหาความมั่นคง; ไซเบอร์; ความร่วมมือ; การแก้ปัญหา

Abstract

This academic article aims to study cyber security problems and cooperation in solving problems. Whether in the public sector or the private sector, because nowadays most government personnel are the older generation who still lack understanding and knowledge in accessing cyber problems. Therefore causing problems in making technological information safe for use. But on the other hand, there is still a high risk from a lack of knowledge and understanding. In using this information system technology It cannot be denied that new systems play a role in data storage, also known as information databases. It is also a channel for both advantages. and many disadvantages in working today.

Keywords: Security problems; Cyber; cooperation; problem solving

บทนำ

การปกครองระบอบประชาธิปไตยนั้น รัฐบาลมีหน้าที่จะต้องบำบัดทุกข์บำรุงสุขให้แก่ประชาชน สร้างความอยู่ดีกินดีของประชาชน ตลอดจนการยกระดับการครองชีพ ของบุคคลที่ไม่ได้รับความผาสุกเท่าที่ควรให้ดีขึ้น ให้มาตรฐานความเป็นอยู่ของประชาชนอยู่ในระดับที่เหมาะสมเช่นเดียวกับคนอื่น ๆ ทั้งนี้ รัฐจะต้องมีบทบาทที่ สำคัญในการบริหารจัดการโดยจะต้องตระหนักถึงความต้องการพื้นฐาน (basic needs) ประชาชนทุกคนควรจะ ได้รับบริการขั้นพื้นฐานเพื่อไม่ให้ฐานะความเป็นอยู่ของประชาชนแตกต่างกันมากนัก รัฐจะต้องมีบทบาทที่สำคัญ และจะต้องให้ความเป็นธรรมทางสังคม (social justice) และตั้งอยู่บนพื้นฐานความถูกต้องของกฎหมาย ความยุติธรรมทางสังคม ไม่เลือกปฏิบัติ เน้นความโปร่งใสด้วยการเปิดโอกาสให้ประชาชนมีส่วนร่วมในการตรวจสอบแนวคิดเกี่ยวกับการจัดการภัยคุกคามอาชญากรรมไซเบอร์ ประเทศไทยมีภัยคุกคามทางด้านไซเบอร์เป็นจำนวนมาก ระบบคอมพิวเตอร์ของไทยถูกใช้เป็นฐานในการโจมตีไปยังประเทศอื่นด้วย ทำให้เกิดความเสียหายเป็นวงกว้าง หรือเสียหายต่อทรัพยากรภาพลักษณ์และ ความเชื่อมั่นต่อประเทศการโจมตีเป็นการเข้าไปเปลี่ยนแปลงหน้าเว็บเพจของหน่วยงานภาครัฐ ซึ่งเกิดเหตุขึ้น บ่อยครั้ง ฝ่ายความมั่นคงโดยเฉพาะกองทัพบกจึงต้องมีการดำเนินการจัดตั้งศูนย์ไซเบอร์กองทัพบก เนื่องจากมีกลุ่มผู้ไม่หวังดีใช้เครือข่ายมุ่งโจมตีหน่วยงานของรัฐ หรือการเผยแพร่ข่าวสารอันเป็นเท็จที่ส่งผลกระทบต่อความมั่นคงของชาติ การรักษาความปลอดภัยทางไซเบอร์ของกองทัพบกจะเน้นความร่วมมือกับหน่วยงานภาครัฐ และองค์กรภาคเอกชน โดยร่วมมือทั้งเรื่ององค์ความรู้ และการเฝ้าระวังภัยคุกคามทางด้านไซเบอร์ที่เป็นภัยคุกคาม ร้ายแรงต่อระบบเครือข่ายคอมพิวเตอร์โดยฝึกผู้เชี่ยวชาญด้านไซเบอร์มุ่งเน้นในเรื่องการรักษาความปลอดภัย ทางไซเบอร์ 3 ประการ ดังนี้ (อริย์ธัช แก้วเกาะสะน้า, 2560: 6-8)

1. การป้องกัน (Identify & Protect) โดยการตรวจสอบช่องโหว่ที่มีในระบบการทดสอบการเจาะการเข้าสู่ระบบ หากตรวจพบช่องโหว่ในระบบจะได้ดำเนินการแก้ไขให้มีความปลอดภัยเพิ่มขึ้น

2. การเฝ้าระวังแบบเรียลไทม์ (Detect) ต้องทำการตรวจสอบวิเคราะห์ภัยคุกคาม ทางด้านไซเบอร์ ขั้นสูง การรวบรวมและศึกษาข่าวกรอง และการเฝ้าระวังภัยคุกคาม ทางด้านไซเบอร์ที่จะเกิดขึ้น

3. การสนองตอบภัยคุกคามแบบเรียลไทม์ (Re pond) โดยจัดทำแผนตอบสนองต่อภัยคุกคามตามขั้นตอน ที่ได้กำหนดไว้ คือการสืบสวนสอบสวนทางดิจิทัลและนิติวิทยาศาสตร์ การวิเคราะห์หาสาเหตุของภัยคุกคามที่เกิดขึ้น รวมถึงการประสานงานไปยังหน่วยงานที่เกี่ยวข้องเพื่อดำเนินงานตามขั้นตอนของกฎหมาย

กฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

ตัวอย่างกฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

- พ.ร.บ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
- พ.ร.บ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560
- พ.ร.บ คุ้มครองข้อมูลส่วนบุคคล
- มาตรฐานด้านความปลอดภัย ISO 27001 (ระบบบริหารจัดการความปลอดภัยของข้อมูล)

ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. ควรมีการแยก User ใช้งานกันของแต่ละบุคคล

2. ควร Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์
3. ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ
4. มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ
5. มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ
6. ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ
7. มีการใช้ Password ที่ดี และ ไม่ควรบอก Password แก่ผู้อื่น (อริย์ธัช แก้วเกาะสะบ้า, 2560)

แนวคิดเกี่ยวกับอาชญากรรมไซเบอร์และความสัมพันธ์กับอาชญากรรมเศรษฐกิจ

"อาชญากรรมไซเบอร์" เป็นปรากฏการณ์ทางสังคมที่ถือกำเนิดขึ้นจากการพัฒนาเทคโนโลยีคอมพิวเตอร์ ปฏิเสธไม่ได้ว่าในปัจจุบันเทคโนโลยีคอมพิวเตอร์ ได้เข้ามาเป็นส่วนหนึ่งในชีวิตประจำวัน ของกลุ่มคนส่วนใหญ่ในสังคม ไม่ว่าจะเป็นในระดับปัจเจกบุคคลที่ใช้เทคโนโลยีคอมพิวเตอร์ผ่าน อุปกรณ์สมาร์ท ดีไว (Smart Devices) ที่เป็นตัวเชื่อมต่อกับระบบอินเทอร์เน็ต เข้ามาช่วยเหลือ กิจกรรมส่วนตัวต่าง ๆ และในระดับกลุ่มที่ใหญ่ขึ้นจากสังคมรอบตัวที่นำเอาเทคโนโลยีคอมพิวเตอร์ เข้ามาเป็นตัวช่วยเสริมกิจกรรมทางสังคมในหลากหลายด้าน จะเห็นได้ว่าเทคโนโลยีคอมพิวเตอร์นั้น ไม่ได้เป็นสิ่งที่อยู่ไกลตัว แต่กลับเข้ามาอยู่รอบตัวของเราโดยที่เราไม่ทันรู้ตัว การพัฒนาเทคโนโลยี คอมพิวเตอร์ในยุคปัจจุบัน ถูกพัฒนาอยู่บนพื้นฐานของระบบอินเทอร์เน็ต ซึ่งในรอบปีที่ผ่านมาได้มี กระแสสังคมกล่าวถึงแนวคิดในการใช้เทคโนโลยีคอมพิวเตอร์เชื่อมต่อทุกสิ่งรอบตัวเข้าสู่ ระบบ อินเทอร์เน็ต ซึ่งมีชื่อที่เรียกกันโดยทั่วไปในสังคมว่า "แนวคิดอินเทอร์เน็ตแห่งสรรพสิ่ง" (The Internet of Things) แนวคิดดังกล่าวเป็นการนำเสนอแนวทางสร้างสังคมที่สามารถเชื่อมโยงทุกสิ่ง เอาไว้ด้วยกัน การเชื่อมต่ออินเทอร์เน็ตเข้าสู่วัตถุรอบตัวเราจะทำให้เรามองเห็นความสัมพันธ์ระหว่าง คน เครื่องจักรกล และสิ่งของด้วยมุมมองที่ลุ่มลึกกว่าเดิม อีกทั้งยังก่อให้เกิดชุดของฐานข้อมูลขนาด ใหญ่ (Big Data) ที่แสดงให้เห็นถึงความสัมพันธ์กันของทุกสรรพสิ่งในระดับที่สูงขึ้นจากเดิม หาก ย้อนกลับไปพิจารณาถึงเทคโนโลยีคอมพิวเตอร์ในช่วง 10 ปี ที่ผ่านมาเปรียบเทียบกับในปัจจุบัน จะเห็นถึงพัฒนาการของเทคโนโลยีคอมพิวเตอร์ที่ก้าวล้ำเกินกว่าที่ได้คาดการณ์เอาไว้ กรอบแนวคิด ดังกล่าวจึงดูเหมือนจะไม่ใช่เรื่องที่ดูเพ้อฝันเกินจริงเหมือนกับนิยายวิทยาศาสตร์ แต่เป็นสิ่งที่กำลัง เกิดขึ้นจริงแล้วในสังคม (จุฑารัตน์ เอื้ออำนวย, 2560) แนวคิดดังกล่าวข้างต้นสอดคล้องกับสิ่งที่ Samuel Greengard ได้หยิบยกมานำเสนอใน มุมมองต่าง ๆ ไว้ได้อย่างน่าสนใจภายในหนังสือ "อินเทอร์เน็ตแห่งสรรพสิ่ง" ซึ่งเนื้อหาภายในหนังสือ มีการกล่าวถึง ความพยายามของกลุ่มคนในยุคสมัยปัจจุบันที่ต้องการนำเอาแนวคิดอินเทอร์เน็ตแห่ง สรรพสิ่งเข้ามาเปลี่ยนแปลงสังคม โดยถูกคาดการณ์ว่าจะเข้ามาทำหน้าที่เป็นโครงสร้างพื้นฐานสำหรับ การใช้ชีวิตประจำวันและการงานของผู้คนในสังคมทั้งหมดในอนาคตอันใกล้ การพัฒนาเทคโนโลยีคอมพิวเตอร์นั้นก็ไม่ได้มีแต่ด้านดีเพียงอย่างเดียว ผลเสีย และผลกระทบที่ตามมาจากการพัฒนาเทคโนโลยีคอมพิวเตอร์ ก่อให้เกิดปัญหาอาชญากรรมไซเบอร์ ตามขึ้นมาอย่างหลีกเลี่ยงไม่ได้ โดย Samuel Greengard ยังได้กล่าวต่อไปถึงสาเหตุของปัญหา ดังกล่าว โดยให้เหตุผลว่าปัญหามาจากช่องโหว่ของระบบอินเทอร์เน็ต ที่ขาดการออกแบบระบบความ มั่นคงปลอดภัยทางไซเบอร์ที่เหมาะสมมาตั้งแต่เริ่มต้น ซึ่งสถานการณ์ในปัจจุบันผู้เชี่ยวชาญด้านความ มั่นคงปลอดภัยทางไซเบอร์เสมือนกำลังเล่นไล่จับกับอาชญากรไซเบอร์ เมื่อมีภัยคุกคามหรือ จุดบกพร่องในรูปแบบใหม่ ๆ ทีมจัดการความมั่นคงปลอดภัยทางไซเบอร์ก็จะสืบเสาะหารอยรั่วและรีบอุดรูรั่วนั้นทันที สถานการณ์นี้ทำให้

เกิดเครื่องมือ วิธีการ และเทคนิคที่ผสมผสานกัน ซึ่งเป็นที่ทราบกันดีว่าไม่มีวิธีการใดวิธีการหนึ่งที่จะสามารถแก้ไขปัญหาได้อย่างเบ็ดเสร็จ โดยในทุกวันนี้การจัดการ ความมั่นคงปลอดภัยทางไซเบอร์ต้องใช้การผสมผสานเครื่องมือทั้งไฟร์วอลล์ ระบบตรวจจับมัลแวร์ การรักษาความปลอดภัยที่อุปกรณ์ปลายทาง การเข้ารหัส ระบบจัดการพาสเวิร์ด รวมทั้งการเฝ้าระวัง เครือข่ายและวิธีการ อื่น ๆ ร่วมไปด้วยกัน (ซา มูเอล กรีนการ์ด, 2560: 12)

สถานการณ์ในปัจจุบันปัญหาอาชญากรรมไซเบอร์ได้เพิ่มพูนจำนวนและความรุนแรงมากขึ้นเรื่อย ๆ ซึ่งจะเห็นได้จากจำนวนตัวเลขสถิติการก่ออาชญากรรมทางไซเบอร์ทั่วโลก ที่ยังคงเดินหน้า สร้างสถิติเพิ่มจำนวนสูงขึ้นเรื่อย ๆ ในทุกวินาทีที่หมุนไปจะมีการโจมตีทางไซเบอร์บนพื้นที่โลกไซเบอร์ อยู่ตลอดเวลา โดยสามารถติดตามได้จากแหล่งข้อมูลสาธารณะที่น่าเชื่อถือ ในที่นี้ผู้วิจัยจะขอ ยกตัวอย่างรายงานสถานการณ์สถิติการโจมตีทางไซเบอร์บนเว็บไซต์ของบริษัทแคสเปอร์สกี้ 4 บริษัทผู้ผลิตซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์จากประเทศรัสเซีย โดยในรายงานสถิติบนเว็บไซต์จะ แสดงการรายงานข้อมูลการตรวจจับการโจมตีทางไซเบอร์จากโปรแกรมแอนตี้ไวรัส ที่ติดตั้งอยู่บน ระบบเครื่องคอมพิวเตอร์ของผู้ใช้บริการทั่วโลก ซึ่งจะมีการรายงานผลข้อมูลตัวเลขด้วยระบบ เรียลไทม์ (Real-Time System) เพื่อแสดงให้เห็นถึงรายละเอียดการเคลื่อนไหวของข้อมูลตัวเลข การถูกโจมตีในระดับวินาที

ภายหลังจากนั้นเป็นต้นมาก็ได้มีการให้คำนิยามการกระทำความผิดทางคอมพิวเตอร์ตามมา อีกมากมายตามยุคสมัยที่เปลี่ยนแปลงไป โดยเฉพาะในช่วงเวลาหลังปีพุทธศักราช 2543 เป็นปีที่ สังคมกระแสหลักได้เริ่มสัมผัสกับเทคโนโลยีคอมพิวเตอร์ที่มีชื่อเรียกว่า ระบบอินเทอร์เน็ต หรือ ระบบ เครือข่ายคอมพิวเตอร์ ส่งผลให้คำนิยามที่ถูกนำมาอธิบายในยุคสมัยดังกล่าวได้มีการเริ่มกล่าวถึงระบบ อินเทอร์เน็ตในนิยามจำกัดความของการกระทำความผิดทางคอมพิวเตอร์มากขึ้น พร้อมทั้งมีการ ปรับเปลี่ยนชื่อเรียกการกระทำความผิดทางคอมพิวเตอร์เหล่านี้ว่าเป็น “อาชญากรรมไซเบอร์ (Cybercrime)”

คำนิยามอาชญากรรมไซเบอร์ที่มีการกล่าวถึงระบบอินเทอร์เน็ต หรือ ระบบเครือข่ายคอมพิวเตอร์ ได้ปรากฏให้เห็นในหนังสือ Introduction to Cybercrime ที่แต่งโดย Joshua B. Hill และ Nancy E. Marion ที่ได้ให้คำนิยามอาชญากรรมไซเบอร์เอาไว้ว่า “อาชญากรรมไซเบอร์เป็นอาชญากรรมที่มีความเกี่ยวข้องกับคอมพิวเตอร์และเครือข่าย ระบบคอมพิวเตอร์ โดยทั่วไปแล้วหมายถึงการกระทำที่อาชญากรใช้ระบบอินเทอร์เน็ต หรือ ระบบ คอมพิวเตอร์อื่น ๆ กระทำอันตราย หรือ สร้างความรบกวนให้กับระบบคอมพิวเตอร์

โดยคำนิยามจำกัดความข้างต้นสอดคล้องกับความคิดเห็นของ Brian K. Payne ที่ได้กล่าวถึง ในหนังสือ White - Collar Crime เอาไว้ว่า

“อาชญากรรมคอมพิวเตอร์และอาชญากรรมไซเบอร์ หมายถึง ประเภทของอาชญากรรมที่มีความเกี่ยวข้องกับการใช้คอมพิวเตอร์ ในการกระทำความผิดตามกฎหมาย หรือ กระทำอันตรายอื่น ๆ ต่อระบบคอมพิวเตอร์ ซึ่งในกรณีนี้รวมถึงการที่ระบบคอมพิวเตอร์ตกเป็นเป้าหมายในการถูกโจมตี หรือ ระบบคอมพิวเตอร์ถูกนำมาใช้เป็นเครื่องมือในการประกอบอาชญากรรม หรือ การกระทำที่ ส่งผลกระทบจนก่อให้เกิดอาชญากรรม – The terms computer crime and cybercrime refer to a range of computer – related behaviors that are criminally illegal or otherwise harmful. In case of computer crime, the computer is either a target of the offense or a tool for the crime or is incidental to the crime. (ปรมัตถ์ ไวรักษ์, 2562)

อาชญากรรมเศรษฐกิจเป็นรูปแบบของอาชญากรรมจำพวกหนึ่งที่ได้รับผลกระทบจากการ เข้ามาของอาชญากรรมไซเบอร์ ความเป็นมาของปัญหาอาชญากรรมเศรษฐกิจนั้นเริ่มถูกกล่าวถึงใน สังคมราวตอนต้นศตวรรษที่ 19 โดยเริ่มต้นจากการเกิดขึ้นของอาชญากรรมรูปแบบใหม่ ๆ ที่เริ่ม ปรากฏให้เห็นในวงการธุรกิจการเงินการธนาคาร อาทิ ความผิดเกี่ยวกับเช็ค การฉ้อโกง การปลอม แปลงเอกสาร และการปลอมแปลงเงินตรา ซึ่งได้ส่งผลกระทบต่อระบบเศรษฐกิจในขณะนั้นเป็นอย่าง มาก ประกอบกับในยุคสมัยดังกล่าวยังไม่มีการร่างกฎหมายที่สามารถนำมาบังคับใช้ควบคุมปัญหา อาชญากรรมเศรษฐกิจได้อย่างเหมาะสม ส่งผลให้นักวิชาการจากหลากหลายสาขา อาทิ นักอาชญา วิทยา นักสังคมวิทยา และนักกฎหมาย ได้เริ่มทำการศึกษาถึงต้นตอสาเหตุของปัญหาอาชญากรรม เศรษฐกิจที่เกิดขึ้น โดยนักอาชญาวิทยาที่มีชื่อเสียงที่สุดในยุคอย่าง Edwin Sutherland ได้ศึกษาและ ให้คำนิยามอาชญากรรมเศรษฐกิจเอาไว้ว่า “เป็นการกระทำความผิดทางอาญาหรือกฎหมายอื่น ๆ จากบุคคลที่มีสถานภาพทางเศรษฐกิจโดยอาศัยความสัมพันธ์ทางอาชีพของเขาเหล่านั้นและความผิด ดังกล่าวก่อให้เกิดความเสียหายต่อวงการธุรกิจตลอดจนระบบเศรษฐกิจของประเทศ” จากคำนิยาม ข้างต้นชี้ให้เห็นว่า อาชญากรรมเศรษฐกิจมีการให้คำนิยามไว้แบบกว้าง ๆ ครอบคลุมการกระทำ ความผิดในทุกลักษณะที่มีส่วนเกี่ยวข้องและสร้างความเสียหายต่อระบบเศรษฐกิจ อาชญากรรมเศรษฐกิจนั้น จัดว่าเป็นอาชญากรรมที่มีความเฉพาะตัว ผู้กระทำผิดจะเป็นผู้ที่มี ความรู้ความสามารถเฉพาะทางในระดับสูง ซึ่งจะมีความแตกต่างจากอาชญากรรมในประเภทอื่น ๆ การกระทำความผิดทางเศรษฐกิจถูกเรียกในชื่อที่แตกต่างกัน ตามแต่ลักษณะรูปแบบการประกอบ อาชญากรรม อาทิ อาชญากรรมคอปกขาว (White Collar Crime) อาชญากรรมทางธุรกิจ (Business Crime) อาชญากรรมทางการพาณิชย์ (Commercial Crime) และอาชญากรรมทางการเงิน (Financial Crime) ซึ่งการกระทำความผิดทั้งหมดข้างต้นล้วนมีความหมายอยู่ในลักษณะเดียวกัน คือ เป็นการประกอบความผิดโดยมีวัตถุประสงค์เพื่อให้ได้มาซึ่งผลกำไรหรือผลประโยชน์ทางเศรษฐกิจ โดยเป็นการกระทำผิดต่อกฎหมายเกี่ยวกับการพาณิชย์อันจะมีผลกระทบต่อระบบเศรษฐกิจและความ มั่นคงของประเทศ เพื่อให้ครอบคลุมถึงการกระทำความผิดทางเศรษฐกิจทั้งหมด (ชญานิศ ภาชีรัตน์, 2543)

ในส่วนของกฎหมายที่น่าสนใจของกฎหมายชุดนี้อยู่ในส่วนของ “พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560” โดยมีการปรับปรุงบทบัญญัติจากพระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่มีประเด็นปัญหาในการบังคับใช้ กฎหมายให้มีความเหมาะสมต่อการป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ในปัจจุบันที่มีรูปแบบซับซ้อนมากขึ้นตามพัฒนาการทางเทคโนโลยีคอมพิวเตอร์ที่เปลี่ยนแปลงอย่าง รวดเร็ว มีการกำหนดฐานความผิดขึ้นใหม่และแก้ไขเพิ่มเติมฐานความผิดเดิม รวมทั้งบทกำหนดโทษ ของความผิด อาทิ การกำหนดให้บุคคลใดก็ตามที่กระทำการอย่างหนึ่งอย่างใดกับระบบคอมพิวเตอร์ ไม่ว่าจะเป็นการส่งคำสั่งเข้าไปฝังตัวเพื่อลักลอบนำข้อมูล หรือขัดขวางการทำงาน หรือสั่งทำลาย ระบบคอมพิวเตอร์ของผู้อื่น เป็นการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ความร้ายแรงของการ กระทำผิดในลักษณะนี้จะทวีความรุนแรงมากขึ้น เมื่อกระทำต่อองค์กรหรือหน่วยงานที่เป็นโครงสร้าง พื้นฐานสำคัญของประเทศ เช่น ระบบของธนาคาร ระบบสาธารณูปโภค ระบบพลังงาน ระบบควบคุม การบิน ระบบของโรงพยาบาล เป็นต้น การปรับปรุงพระราชบัญญัติยังรวมไปถึงการปรับหลัก กฎหมายให้เอื้อต่อการประสานความร่วมมือระหว่างประเทศ มีการปรับปรุงกระบวนการและ หลักเกณฑ์ในการระงับ การเผยแพร่หรือลบข้อมูลคอมพิวเตอร์ตลอดจนกำหนดให้มีการแก้ไข เพิ่มเติมอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ให้เหมาะสมยิ่งขึ้น กฎหมายที่มีความน่าสนใจในอีกประเด็นเป็น “พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล” ซึ่งเป็นการให้ความคุ้มครอง

สิทธิความเป็นส่วนตัว ในสังคมปัจจุบันมีแนวโน้มเกิดการละเมิดสิทธิ ในข้อมูลส่วนบุคคลและสิทธิความเป็นส่วนตัวเพิ่มมากขึ้น โดยเฉพาะการนำข้อมูลส่วนบุคคลไป แสวงหาผลประโยชน์หรือนำไปเปิดเผยโดยมิชอบหรือโดยไม่ได้รับความยินยอมจากทางเจ้าของข้อมูล เพื่อประโยชน์ในทางการค้า หรือเพื่อประโยชน์ในการนำข้อมูลส่วนบุคคลไปใช้ในการกระทำความผิด อาทิการหลอกลวง การฉ้อโกง การหมิ่นประมาท เป็นต้น ซึ่งปัญหาเหล่านี้เมื่อได้กระทำความผิดบนโลกไซเบอร์ก็ถือได้ว่าเป็นปัญหาอาชญากรรมไซเบอร์เช่นเดียวกัน โดยปัญหานั้นย่อมส่งผลกระทบต่อ ความเชื่อมั่นในการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมตามนโยบายของรัฐบาล ดังนั้นจึงมีความ จำเป็นที่ประเทศไทยจะต้องตราบัญญัติกฎหมายว่า ด้วยการคุ้มครองข้อมูลส่วนบุคคลของประเทศ เพื่อสร้างกลไกการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นมาตรฐานเดียวกันและสอดคล้องกับ มาตรฐานที่เป็นสากล โดยต้องไม่สร้างภาระหน้าที่แก่ผู้เกี่ยวข้องจนกลายเป็นข้อจำกัด หรืออุปสรรคในการประกอบธุรกิจการค้าหรือการให้บริการของภาคส่วนต่าง ๆ จนเกินสมควร เพื่อแก้ไขปัญหาการ ละเมิดข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพ (พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)

ความมั่นคงไซเบอร์

มีนักวิชาการหลายท่านได้ให้ความหมายของความมั่นคงไซเบอร์ ไว้ดังนี้

ชนินทร เฉลิมทรัพย์ (2561) แนวทางการบูรณาการรักษา ความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติผู้วิจัยได้ศึกษาแนวคิดทฤษฎีเกี่ยวกับสมรรถนะองค์กร การบูรณาการการบริหารจัดการและการรักษาความมั่นคงปลอดภัยทางไซเบอร์มีการทำงานแบบเครือข่ายเชื่อมโยงตามประเด็นยุทธศาสตร์ร่วม (Common Agenda) ปฏิบัติงานตามมาตรฐานการปฏิบัติทางเทคโนโลยีและจัดตั้งศูนย์การศึกษาการวิจัยการพัฒนาด้าน ความมั่นคงปลอดภัยทางไซเบอร์ต่อไป

สุธาเทพ รุณเรศ (2561) กล่าวว่าหากจะทำการวิจัยเกี่ยวกับภัยคุกคามทางไซเบอร์ ดังนี้ ควรมีการศึกษาปัจจัยทางสังคมที่อาจมีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเตอร์เน็ต ควรจะใช้การวิจัยเชิงคุณภาพด้วยการสัมภาษณ์กลุ่มหรือการสัมภาษณ์เจาะลึกเพื่อศึกษาความตระหนัก ถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในเชิงลึกและข้อมูลที่รอบด้านครบมิติมากยิ่งขึ้น

สุรพงษ์ ทรัพยากร (2563) กล่าวว่า กรอบความมั่นคงความปลอดภัยทางไซเบอร์ที่จะสนับสนุนวัฒนธรรมความปลอดภัยทางไซเบอร์เพื่อป้องกันการโจมตีทางไซเบอร์ ให้คำนึงถึงการลดความเสี่ยงทางไซเบอร์และปรับปรุงการรักษาความปลอดภัยให้กับโครงสร้างพื้นฐานเป็นสำคัญ

อรรถพล ป้อมสถิตย์ (2563) กล่าวว่า ความปลอดภัยข้อมูลการรักษาความปลอดภัยทางไซเบอร์ด้านความปลอดภัยของข้อมูล ข้าราชการและหน่วยข่าวกรองอื่น ๆ ต้องพัฒนาเครื่องมือใหม่ที่ป้องกัน และปรับให้เข้ากับความเสี่ยงและภัยคุกคามที่อาจเกิดขึ้นในอนาคต

กริน ธัญญวิกรม และธีระ กุลสวัสดิ์ (2564) การจัดการความมั่นคงทาง เทคโนโลยีสารสนเทศ กรณีศึกษา การคุ้มครองข้อมูลส่วนบุคคลในการทำธุรกรรมทางอิเล็กทรอนิกส์ ของธนาคารพาณิชย์ไทย ผู้วิจัยเห็นว่าควรมีข้อเสนอแนะที่เป็นนัยยะในเชิงนโยบายที่สำคัญ คือ รัฐควรเร่งรัดการบังคับใช้ พ.ร.บ. ความมั่นคงปลอดภัยไซเบอร์และ พ.ร.บ.การคุ้มครองข้อมูล ส่วนบุคคล โดยการออกกฎหมายลูกและประกาศกฎเกณฑ์ต่าง ๆ เพื่อให้การดำเนินการมีความสอดคล้อง และเป็นไปในทิศทางเดียว

สรุปได้ว่า ความมั่นคงไซเบอร์ คือ ความปลอดภัยหรือมาตรการที่ดำเนินการป้องกันและรับมือความเสี่ยงจากภัยคุกคามทางคอมพิวเตอร์ทั้งภายในและภายนอกประเทศ เพื่อความสงบสุขของประชาชนและความสงบเรียบร้อยของประเทศ

ความร่วมมือ

มีนักวิชาการหลายท่านได้ให้ความหมายของความร่วมมือ ไว้ดังนี้

เสาวนีย์ จิตต์หมวด (2538) กล่าวว่า ความร่วมมือ คือวิถีการดำเนินชีวิต (Way of life) หรือรูปแบบแห่งพฤติกรรม (Behavior patterns) และบรรยายผลงานทั้งมวลที่มนุษย์ได้สร้างสรรค์ขึ้น อันได้แก่ ศาสนา ปรัชญา ภาษา กฎหมาย การปกครอง ศิลปะวิทยาการ เครื่องใช้ต่าง ๆ ซึ่งมีการส่งต่อและสืบทอดติดต่อกันมา

สุนทร (2540) กล่าวว่าพฤติกรรมที่ปฏิบัติกันอย่างสม่ำเสมอขณะที่บุคคล ติดต่อเกี่ยวข้องกับผู้อื่น ค่านิยมที่มีอยู่ร่วมกันภายในจิตใจของคนจำนวนหนึ่ง หรือคนส่วนใหญ่ในองค์การ คนกลุ่มใหญ่ดังกล่าวใช้ระบบความรู้ความคิดร่วมกันนี้เป็นแนวทางในการคิดตัดสินใจและ แก้ไขปัญหาที่เกิดขึ้นภายในองค์กร

ธิดารัตน์ รักประยูร (2545) กล่าวว่า ความร่วมมือ ฐานจากผลผลิตและพื้นฐาน การปรับตัวของมนุษย์และสิ่งแวดล้อมที่มีการสั่งสมประสบการณ์ของคนหลายชั่วอายุซึ่ง ในขณะเดียวกันก็ได้รับใช้ขั้นตอนการดำรงชีวิตของมนุษย์ด้วย เป็นสิ่งที่มนุษย์สร้างขึ้นและต้องเปลี่ยนแปลง

ธีรยุทธ์ บุญมี (2546) กล่าวว่า ความร่วมมือถึงความคิดแบบแผน ทุกอย่างที่จะทำให้ไม่เกิดปัญหาทางโลกออนไลน์ นั้นคือการไม่กระทำผิดกฎที่จะก่อให้เกิดความเสียหายของบุคคลในโลกไซเบอร์

สรุปได้ว่า ความร่วมมือ คือ แบบอย่างของการดำรงชีวิตของ ชนหมู่ใดหมู่หนึ่ง และก่อนที่จะเป็นแบบอย่างขึ้นมาได้ จะต้องมีการปฏิบัติในหมู่คนจำนวนมากจน ปฏิบัติตามกันไปทั้งกลุ่ม มีระยะเวลานานและเป็นแบบอย่างที่ชัดเจนแน่นอน

การแก้ปัญหา

มีนักวิชาการหลายท่านได้ให้ความหมายของการแก้ปัญหา ไว้ดังนี้

วิจารณ์ พานิช (2550) กล่าวว่าองค์กรที่จะสามารถแก้ไขปัญหาได้อาจเน้นความรู้เป็นสิ่งสำคัญแต่การเรียนรู้และการสร้างความรู้สำคัญที่สุด ดังนั้นเป้าหมายขององค์กรนี้คือ สามารถในการเผชิญกับ สภาพอนาคตที่ไม่แน่นอนได้

วีระชน ขาวผ่อง (2551) กล่าวว่าการแก้ไขปัญหาอาจมาจากจิตสำนึกของบุคคล คือ สภาวการณ์มีผลให้เกิด ความรู้สึก การรับรู้มุ่งสู่สภาวะจิตแห่งตน คือ ทัศนคติ ความคิด ความเชื่อ ความสนใจ อันจะก่อให้เกิด ความตระหนักและจิตสำนึก

พงษชัย เฉลิมกลิ่น (2551 กล่าวว่าความรับผิดชอบต่อสิ่งใดสิ่งหนึ่งหรือเหตุการณ์ใดเหตุการณ์หนึ่งซึ่งเป็นอารมณ์ความรู้สึกด้านทัศนคติ ค่านิยม ความชอบหรือไม่ชอบ ดีหรือไม่ดี ควรมีลำดับขั้นตอนการวางแผนในการแก้ไขปัญหาเพื่อให้มีความรัดกุมต่อเหตุที่เกิดขึ้น

นายสุธาเทพ รุณเรศ (2561) กล่าวว่าการแก้ไขปัญหาที่เกิดขึ้นหรือการป้องกันปัญหาที่อาจจะเกิดขึ้นนั้นควรมีการศึกษานโยบายของรัฐและองค์กรต่างๆเกี่ยวกับการป้องกันและการรับมือกับภัยคุกคามทาง ไซเบอร์ที่อาจเกิดขึ้นในอนาคต

สรุปได้ว่า การแก้ปัญหา คือ การทำงานหรือการป้องกันด้วยการพิจารณาใคร่ควรก่อนกระทำการเกี่ยวกับการเข้าถึงเทคโนโลยีทางโลกออนไลน์หรือเข้าสู่โลกไซเบอร์ และการตระหนักถึงการใช้สื่อออนไลน์อย่างเหมาะสม กำหนดนโยบายกลยุทธ์ที่มีประสิทธิภาพ เพื่อเสริมสร้างความแข็งแกร่งให้กับระบบและป้องกันการโจมตีที่อาจเกิดขึ้น ซึ่งอาจส่งผลกระทบต่อความก้าวหน้าทางเศรษฐกิจ

บทสรุป

ปัญหาความมั่นคงไซเบอร์เป็นภัยคุกคามร้ายแรงที่ทุกประเทศต้องเผชิญ การแก้ไขปัญหาจึงจำเป็นต้องอาศัยความร่วมมือจากทุกภาคส่วนทั้งภาครัฐ ภาคเอกชน และประชาชน ซึ่งในประเทศไทยปัญหานี่ยังไม่สามารถปราบปรามได้ให้หายไปจากประเทศนี้ โดยเฉพาะการหลอกลวงทางด้านธุรกรรมทางการเงิน หรือด้านฐานข้อมูลส่วนบุคคลที่เป็นปัญหาหลักในประเทศอยู่ขณะนี้ ซึ่งภัยคุกคามที่เริ่มมีมากขึ้นและมีความซับซ้อนทางด้านการโจรกรรมข้อมูลส่วนบุคคล การโจมตีทางไซเบอร์เพื่อขัดขวางการเลือกตั้ง ข่าวปลอมและการบิดเบือนข้อมูลที่เป็นจริง ซึ่งเหล่านี้ก็ล้วนเกิดจากซอฟต์แวร์และระบบที่เก่าหรือล้าสมัย การขาดแคลนบุคลากรที่มีทักษะด้านความปลอดภัยไซเบอร์ การขาดความตระหนักรู้ด้านความปลอดภัยไซเบอร์ กฎหมายและข้อบังคับที่ไม่เพียง จึงทำให้มีผลกระทบร้ายแรงไม่ว่าจะเป็นความเสียหายทางการเงิน การสูญเสียข้อมูลสำคัญ การหยุดชะงักของระบบและบริการ ความเสียหายต่อชื่อเสียง ความเสี่ยงต่อความมั่นคงของชาติ

ฉะนั้นการที่จะแก้ไขปัญหาเหล่านี้ได้จึงต้องมีการพัฒนายุทธศาสตร์และแผนปฏิบัติการด้านความมั่นคงไซเบอร์ โดยการจัดตั้งหน่วยงานที่รับผิดชอบด้านความมั่นคงไซเบอร์ให้มีการพัฒนากฎหมายและข้อบังคับที่เกี่ยวข้อง หรือรณรงค์สร้างความตระหนักรู้ด้านความปลอดภัยไซเบอร์ และที่สำคัญคือการพัฒนาบุคลากรที่มีทักษะด้านความปลอดภัยไซเบอร์ เพื่อพัฒนากลไกความร่วมมือในการรับมือกับภัยคุกคาม และความรู้ด้านความปลอดภัยไซเบอร์

เอกสารอ้างอิง

จุฑารัตน์ เอื้ออำนวย. 2560 *“การบริหารงานยุติธรรม: วิธีการศึกษา วิเคราะห์ และเปรียบเทียบการบริหารงานยุติธรรม,”* เอกสารประกอบการเรียน สาขาอาชญาวิทยาและงานยุติธรรม ภาควิชาสังคมวิทยาและมานุษยวิทยา คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย.

ชญานิศ ภาชีรัตน์. (2540). *“อาชญากรรมเศรษฐกิจที่เกี่ยวกับสถาบันการเงิน: ศึกษากรณีเปรียบเทียบมาตรการในการบังคับใช้กฎหมายของต่างประเทศและประเทศไทย,”* วิทยานิพนธ์ปริญญานิติศาสตรมหาบัณฑิต สาขาวิชา นิติศาสตร์ คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย.

ชฎาภรณ์ สิงห์แก้ว. (2564). *บทบาทภาครัฐในการป้องกันอาชญากรรมไซเบอร์เพื่อความมั่นคงทางเศรษฐกิจและสังคมวารสารวิชาการมหาวิทยาลัยการจัดการและเทคโนโลยีอีสเทิร์น ปีที่ 18 ฉบับที่ 1 มกราคม – มิถุนายน.*

ซามูเอล กรีนการ์ด. (2560). *The Internet of Things: อินเทอร์เน็ตแห่งสรรพสิ่ง* แปลโดยทีปกร วุฒิพิทยามงคล. กรุงเทพฯ: สำนักพิมพ์ โอเพ่นเวิลด์ส.

ฐิติมา ภู่ห้อย. (2564). *การสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์.* สืบค้นข้อมูลเมื่อ 2 กุมภาพันธ์ 2567, เข้าถึงได้จาก https://libdcms.nida.ac.th/thesis6/2563/b210818e.pdf.

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล. (2567). สืบค้นเมื่อวันที่ 20 กุมภาพันธ์ 2567, เข้าถึงได้จาก https://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0052.PDF.

วศิน ปั้นทอง. (2567).*ความมั่นคงไซเบอร์: แนวคิด ประสบการณ์ของต่างประเทศ และบทเรียนสำหรับประเทศไทย.* สืบค้นเมื่อวันที่ 2 มีนาคม 2567, เข้าถึงได้จาก https://www.nsc.go.th/wp-content/uploads/Journal/article-00102.pdf.

มหาวิทยาลัยศรีปทุม. (2567). *การสร้างกรอบวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กรสำหรับการเปลี่ยนผ่านทางความมั่นคงปลอดภัยไซเบอร์.* สืบค้นเมื่อวันที่ 2 มีนาคม 2567, เข้าถึงได้จาก http://www.dspace.spu.ac.th/bitstream/.pdf.