บทความวิจัย

บทบาทภาครัฐในการป้องกันอาชญากรรมไซเบอร์เพื่อความมั่นคงทางเศรษฐกิจและสังคม

ชฎาภรณ์ สิงห์แก้ว
นักศึกษาหลักสูตรปรัชญาดุษฎีบัณฑิต สาขาการเมือง คณะรัฐศาสตร์ มหาวิทยาลัยรามคำแหง
email: thanggass@hotmail.com, โทร. 08-1890-5897
ผู้ช่วยศาสตราจารย์ ดร. นิพนธ์ โซะเฮง, คณะรัฐศาสตร์ มหาวิทยาลัยรามคำแหง
ผู้ช่วยศาสตราจารย์ ดร. พัด ลวางกูร, คณะรัฐศาสตร์ มหาวิทยาลัยรามคำแหง
อาจารย์ ดร. ศราวุฒิ อารีย์, คณะรัฐศาสตร์ มหาวิทยาลัยรามคำแหง

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์เพื่อศึกษา (1) บทบาทภาครัฐในการป้องกันอาชญากรรมไซเบอร์เพื่อความมั่นคงทางเศรษฐกิจและสังคม (2) ปัญหาและอุปสรรคของภาครัฐในการป้องกันอาชญากรรมไซเบอร์ เพื่อความมั่นคงทางเศรษฐกิจและสังคม และ (3) ข้อเสนอแนะและแนวทางแก้ไขการป้องกันอาชญากรรมไซเบอร์ เพื่อความมั่นคงทางเศรษฐกิจและสังคม โดยใช้วิธีการวิจัยเชิงคุณภาพ (Qualitative Research) เก็บข้อมูลจากการวิจัยเอกสาร และการสัมภาษณ์เจาะลึกจากผู้ให้ข้อมูลสาคัญ ได้แก่ บุคลากรในภาครัฐที่มีส่วนเกี่ยวข้องกับการป้องกันอาชญากรรมไซเบอร์เพื่อความมั่นคงทางเศรษฐกิจและสังคม การศึกษาวิจัยได้กระทาในช่วงปี 2557-2562 โดยนาเอาแนวคิดเกี่ยวกับบทบาทภาครัฐ แนวคิดเกี่ยวกับการจัดการภัยคุกคามอาชญากรรมไซเบอร์ แนวคิดเกี่ยวกับอาชญากรรมและการป้องกันอาชญากรรม แนวคิดเกี่ยวกับภัยคุกคามอาชญากรรมไซเบอร์ และแนวคิดเกี่ยวกับความมั่นคงแห่งชาติเป็นกรอบในการวิจัย การวิจัยในครั้งนี้

ผลการวิจัยพบว่า ประเทศไทยมีการพัฒนาด้านธุรกรรมทางอิเล็กทรอนิกส์ อาชญากรรมไซเบอร์จึงเป็นภัยที่ไทยต้องเผชิญอย่างหลีกเลี่ยงไม่ได้ การโจมตีระบบ การขโมยข้อมูล การปลอมบัญชีโซเชียลมีเดีย และภัยคุกคามไซเบอร์อื่น ๆ มีปรากฏอย่างต่อเนื่อง อาชญากรรมทางไซเบอร์จึงถือเป็นภัยคุกคามใหญ่หลวงต่อผลประโยชน์ทางเศรษฐกิจ ตลอดจนความมั่นคงของประเทศ ซึ่งภาครัฐเล็งเห็นความสาคัญในการรักษาความมั่นคงปลอดภัยไซเบอร์ ภาครัฐจึงได้ผลักดันร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และร่างพระราชบัญญัติข้อมูลส่วนบุคคล ในสมัยรัฐบาลคณะรักษาความสงบแห่งชาติ (คสช.) โดยมีผลบังคับใช้เมื่อวันที่ 28 พฤษภาคม 2562 เพื่อรองรับการเติบโตทางเศรษฐกิจดิจิทัลอย่างมั่นคงและปลอดภัย ซึ่งกาหนดให้มีสานักงานคณะกรรมการรักษา -ความมั่นคงปลอดภัยไซเบอร์แห่งชาติทาหน้าที่เป็นหน่วยงานกลางในการประสานและขับเคลื่อนนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ

คำสำคัญ: *บทบาทของภาครัฐ, อาชญากรรมไซเบอร์, อาชญากรรมไซเบอร์ทางเศรษฐกิจและสังคม*
Received: October 25, 2020, **Revised** Febuary 2, 2021, **Accepted** May 23, 2021

The Government's role in Cyber Crime Prevention for Economic and Social Security

Chadaporn Singkaew
Ph.d. (Politics) Student, Faculty of Political Science, Ramkhamhaeng University
email: thanggass@hotmail.com, โทร. 08-1890-5897
ASST. PROF. Dr. Nipon Sohheng, , Faculty of Political Science, Ramkhamhaeng University
ASST. PROF. Dr. Pad Lavankura, Faculty of Political Science, Ramkhamhaeng University
Dr. Sarawut Aree, Faculty of Political Science, Ramkhamhaeng University

Abstract

In this research, the researcher has objective to study: (1) Government's role in preventing cybercrime for economic and social security (2) Government sector's problems and obstacles in preventing cybercrime For economic and social security and (3) Recommendations and solutions to prevent cybercrime For economic and social stability Using qualitative research methods, collecting data from research papers. And in-depth interviews From key informants are government personnel involved in cybercrime prevention for economic and social security. Research studies were conducted during the years 2014 - 2019 with the idea of government role. Concept of cyber crime threat management Concept of crime and crime prevention Concept of cyber crime and the concept of national security as a framework for research.

The findings revealed that the study of Thailand is developing electronic transactions. Cyber crime is therefore a threat that Thailand has to face inevitably. Fake social media accounts And other cyber threats are constantly emerging, cybercrime poses a huge threat to economic interests. As well as the security of the country The government sector sees the importance of maintaining cybersecurity. Therefore pushed for a draft act on cybersecurity And draft the Personal Information Act During the government of the National Council for Peace and Order (NCPO), it came into effect on May 28, 2019 in order to support stable and secure digital economic growth. Which requires the National Cybersecurity Commission to act as the central agency for coordinating and driving the country's cybersecurity policy.

Keywords: *Government's role, Cyber crime, Cyber crime prevention for economic and social security*

คำขอบคุณ : งานวิจัยนี้ได้เป็นส่วนหนึ่งของการศึกษาหลักสูตรปรัชญาดุษฎีบัณฑิต สาขาการเมือง คณะรัฐศาสตร์ มหาวิทยาลัยรามคำแหง

บทนำ

จากรายงานอาชญากรรมด้านความปลอดภัยบนอินเทอร์เน็ต (Internet Security Threat Report--ISTR) ฉบับที่ 22 ของไซแมนเทค ปรากฏว่ามีการตรวจพบภัยคุกคามใหม่ ๆ เพิ่มขึ้นบนอุปกรณ์พกพา และแนวโน้มดังกล่าวยังคงเพิ่มขึ้นอย่างต่อเนื่อง

ซึ่งจะส่งผลให้ข้อมูลธุรกิจและข้อมูลลูกค้าอยู่ในสภาวะเสี่ยงเพิ่มมากขึ้น หากฐานข้อมูลไม่ได้รับการรักษาความปลอดภัย ความเป็นส่วนตัวและความปลอดภัยของลูกค้าอาจตกอยู่ในสภาวะเสี่ยงเช่นกัน (ThaiPR.NET, 2560) เช่นเดียวกับ Gareth Pereira ผู้อำนวยการด้านการสื่อสารมีเดียและเทคโนโลยีของ A.T. Kearny กล่าวว่า ประเทศในภูมิภาคอาเซียนให้ความสำคัญกับเศรษฐกิจดิจิทัล (Digital Economy) มากขึ้น ซึ่งประเทศไทยได้เข้าสู่ยุคการเปลี่ยนแปลงรูปแบบองค์กรอย่างมีกลยุทธ์ที่ใช้เทคโนโลยีเข้าช่วยเพื่อเพิ่มประสิทธิภาพและช่วยให้ทันตามโลกเศรษฐกิจอย่างเต็มตัว มีการใช้และทดลองเทคโนโลยีใหม่ ๆ เช่น AI (Artificial Intelligence หรือปัญญาประดิษฐ์ คือเทคโนโลยีสมองกลคอมพิวเตอร์ที่สามารถคิดได้เหมือนมนุษย์), AR (Augmented reality คือการเทคโนโลยีมาผสานระหว่างโลกแห่งความเป็นจริงและความเสมือนจริงเข้าด้วยกัน), IOT (Internet of Things คือสิ่งของทุกอย่างบนโลกใบนี้ที่สามารถเชื่อมต่อกับเครือข่ายเพื่อแลกเปลี่ยนและแบ่งปันข้อมูลได้)เป็นต้น นอกจากนี้ประเทศไทยถูกจัดเป็นประเทศที่มีการป้องกันภัยคุกคามไซเบอร์ต่ำกว่ามาตรฐาน และติดอันดับ 15 ของโลกในเรื่องประเทศที่มีความเสี่ยงด้านไซเบอร์ (Marketing Oops!, 2018) ขณะที่ประเทศไทยมีการพัฒนาด้านธุรกรรมทางอิเล็กทรอนิกส์มากเท่าใด ภัยคุกคามไซเบอร์ก็เป็นภัยที่ประชาชนต้องเผชิญอย่างหลีกเลี่ยงไม่ได้ ทั้งการโจมตีระบบ การขโมยข้อมูล การปลอมบัญชีโซเชียลมีเดีย และภัยคุกคามไซเบอร์อื่น ๆ ซึ่งปัจจุบันภัยคุกคามทางไซเบอร์ในประเทศไทยมีจำนวนที่เพิ่มสูงขึ้นและทวีความรุนแรงขึ้นตามลำดับ การเติบโตและความสามารถในการเข้าถึงโครงข่ายไซเบอร์ของประชากรในประเทศไทยได้เพิ่มขึ้นอย่างก้าวกระโดด จึงทำให้ความเสี่ยงด้านอาชญากรรมไซเบอร์มีสูงขึ้นหลายเท่าตัวและเป็นภัยคุกคามที่จะถูกยกระดับในเชิงยุทธศาสตร์ของประเทศ และการที่สิ่งต่าง ๆ ถูกเชื่อมโยงทุกสิ่งทุกอย่างเข้าสู่โลกอินเทอร์เน็ตทำให้ปัจจุบันมีการสั่งการควบคุมใช้งานอุปกรณ์ต่าง ๆ ผ่านทางเครือข่ายอินเทอร์เน็ตได้อย่างง่ายดาย จึงทำให้ความสามารถของอาชญากรทางไซเบอร์ที่มีจำนวนเพิ่มมากขึ้น ผู้โจมตีจะมีความสามารถในการเข้าถึงข้อมูลขององค์กรที่สำคัญ การโจมตีมีความซับซ้อนมากกว่าเดิมและผู้โจมตีจะมองหาช่องโหว่ในสภาพแวดล้อมการทำงานในองค์กรได้อย่างง่ายดาย จึงจำเป็นต้องกำหนดหลักเกณฑ์เพื่อกำหนดแนวทางและมาตรการต่างๆที่เกี่ยวข้องอย่างเป็นรูปธรรมโดยรัฐบาล คณะรักษาความสงบแห่งชาติ (คสช.) ได้มีการพิจารณาร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นกฎหมาย โดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นผู้เสนอโดยมีการปรับแก้หลายจุดให้สอดคล้องกับเทคโนโลยีสารสนเทศ เพื่อสามารถดำเนินการป้องกันหรือรับมือภัยไซเบอร์ได้อย่างทันท่วงที ซึ่งมีการแบ่งภัยคุกคามทางไซเบอร์เป็น 3 ระดับ คือ ไม่ร้ายแรง ร้ายแรง และวิกฤต ขณะที่มีการปรับแก้ร่างกฎหมายฉบับนี้หลายครั้งแต่ก็ยังคงมีปัญหาที่เสี่ยงจะถูกนำมาใช้ละเมิดสิทธิความเป็นส่วนตัวของประชาชนเป็นจำนวนมาก ซึ่งทำได้โดยง่ายและรวดเร็ว รวมทั้งสร้างความเดือดร้อนและความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล อันส่งผลให้ประชาชนยังมีข้อกังวลในร่างกฎหมาย ดังกล่าวแต่สุดท้ายร่างกฎหมายพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ และร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลได้ผ่านความเห็นชอบจากสภานิติบัญญัติแห่งชาติและบังคับใช้กฎหมายดังกล่าวเมื่อปี พ.ศ. 2562 โดยมิได้มีการแก้ไขข้อกังวลของภาคประชาชนแต่อย่างใดทั้งนี้ การป้องกันอาชญากรรมไซเบอร์เป็นความร่วมมือระหว่างภาครัฐ ภาคเอกชน และภาคประชาสังคมในการต่อต้านภัยคุกคามความร่วมมือระหว่างประเทศ ความร่วมมือจากผู้มีส่วนเกี่ยวข้อง ทั้งภาครัฐ ภาคเอกชน ภาคประชาสังคม และระดับประเทศ ซึ่งเป็นการมีส่วนร่วมของทุกภาคส่วน จะนำไปสู่การกำหนดนโยบายความมั่นคง ทางไซเบอร์อย่างรอบคอบและมีประสิทธิภาพจากแนวคิดของ Myriam and Florian (2019) มีความใกล้เคียงและสอดคล้องกับตัวแปรที่ศึกษาของผู้วิจัยเป็นอย่างมาก ผู้วิจัยจึงได้นำมาปรับและบูรณาการเป็นกรอบแนวคิดในการศึกษาผ่านกฎหมายที่เกี่ยวข้องกับการป้องกันอาชญากรรมไซเบอร์เพื่อความมั่นคงทางเศรษฐกิจและสังคม อาทิ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ตลอดจนโครงการหรือกิจกรรมที่สอดคล้องกับการส่งเสริมการป้องกันอาชญากรรมไซเบอร์เพื่อความมั่นคงทางเศรษฐกิจและสังคม ดังนั้นผู้วิจัยจึงสนใจบทบาทภาครัฐในการป้องกันอาชญากรรมไซเบอร์เพื่อความมั่นคงทางเศรษฐกิจ และสังคม โดยการจัดการความรู้จากเอกสารงานวิจัยที่เกี่ยวข้องทั้งภายในประเทศและต่างประเทศ

ทั้งนี้ เพื่อให้ความสำคัญและการป้องกันระบบข้อมูลของประเทศไม่ให้เกิดความเสียหายหรือได้รับผลกระทบจากอาชญากรรมไซเบอร์หรือการโจมตีจากภายนอกประเทศซึ่งจะส่งผลกระทบต่อระบบเศรษฐกิจและสังคมรวมถึงผลประโยชน์ของประเทศและประชาชนในภาพรวม

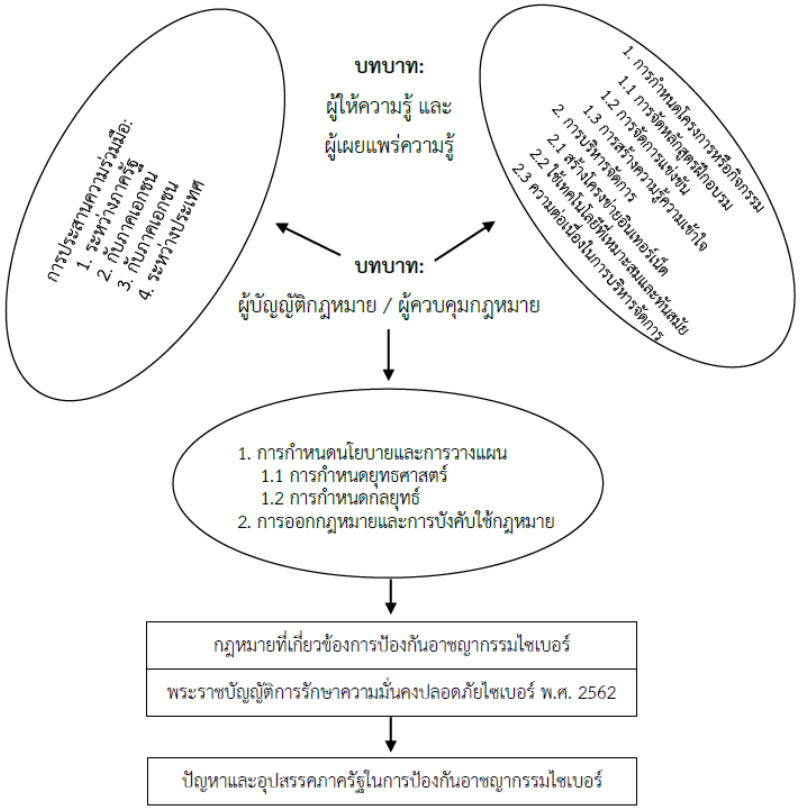
วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาบทบาทภาครัฐในการป้องกันอาชญากรรมไซเบอร์เพื่อความมั่นคงทางเศรษฐกิจและสังคม
2. เพื่อศึกษาปัญหาและอุปสรรคของภาครัฐในการป้องกันอาชญากรรมไซเบอร์ เพื่อความมั่นคงทางเศรษฐกิจและสังคม
3. เพื่อศึกษาข้อเสนอแนะและแนวทางแก้ไขการป้องกันอาชญากรรมไซเบอร์ เพื่อความมั่นคงทาง เศรษฐกิจและสังคม

คำถามการวิจัย

ตั้งแต่อดีตจนปัจจุบันภาครัฐป้องกันอาชญากรรมไซเบอร์เพื่อความมั่นคงทางเศรษฐกิจและสังคมอย่างไรมีหน่วยงานใดที่เกี่ยวข้องกับการป้องกันอาชญากรรมไซเบอร์เพื่อความมั่นคงทางเศรษฐกิจและสังคมและมีวิธีการป้องกันอย่างไร ตลอดจนปัญหาและอุปสรรคมีอะไรบ้าง และมีกฎหมายใดบ้างที่เกี่ยวข้องกับการป้องกันอาชญากรรม ไซเบอร์เพื่อความมั่นคงทางเศรษฐกิจและสังคม ซึ่งภาครัฐมีโครงการหรือกิจกรรมใดที่สอดคล้องกับการส่งเสริมการป้องกันอาชญากรรมไซเบอร์เพื่อความมั่นคงทางเศรษฐกิจและสังคม และภาครัฐควรด าเนินการป้องกันอาชญากรรมไซเบอร์เพื่อความมั่นคงทางเศรษฐกิจและสังคมอย่างไร

กรอบแนวคิดการวิจัย



ภาพที่ 1 กรอบแนวคิดในการวิจัย

การทบทวนวรรณกรรม

การศึกษานี้เป็นการศึกษาถึงวิธีการป้องกันอาชญากรรมไซเบอร์เพื่อความมั่นคงทางเศรษฐกิจและสังคม ตั้งแต่อดีตถึงปัจจุบันรวมทั้งศึกษากฎหมายที่เกี่ยวข้องกับการป้องกันอาชญากรรมไซเบอร์เพื่อความมั่นคงทาง เศรษฐกิจและสังคม และศึกษาโครงการหรือกิจกรรมที่สอดคล้องกับการส่งเสริมการป้องกันอาชญากรรมไซเบอร์ เพื่อความมั่นคงทางเศรษฐกิจและสังคม ตลอดจนทำการศึกษาปัญหาและอุปสรรคของภาครัฐในการป้องกัน อาชญากรรมไซเบอร์เพื่อความมั่นคงทางเศรษฐกิจและสังคมโดยภาครัฐ โดยมุ่งศึกษาแนวคิดเกี่ยวกับบทบาท ภาครัฐ แนวคิดเกี่ยวกับการจัดการภัยคุกคามอาชญากรรมไซเบอร์ แนวคิดเกี่ยวกับอาชญากรรมและการป้องกันอาชญากรรม แนวคิดเกี่ยวกับภัยคุกคามอาชญากรรมไซเบอร์ แนวคิดเกี่ยวกับความมั่นคงแห่งชาติ และ งานวิจัยที่เกี่ยวข้อง แนวคิดเกี่ยวกับบทบาทภาครัฐ

ทฤษฎีเกี่ยวกับบทบาทเป็นแนวคิดทางสังคมวิทยาและจิตวิทยาสังคมที่มองตัวบุคคลในฐานะเป็นสมาชิกของสังคม การปฏิสัมพันธ์หรือการเกี่ยวข้องกันในสังคมเป็นลักษณะสำคัญของบทบาทที่แสดงอยู่และไม่มี ทางหลีกเลี่ยงที่จะไม่ไปเกี่ยวข้องสัมพันธ์กับบุคคลอื่นๆเพื่อให้สังคมก้าวไปสู่สังคมที่บุคคลส่วนใหญ่ปรารถนาและต้องการที่จะให้เป็นไป ดังนั้นการเข้าใจทฤษฎีบทบาทจะทำให้สามารถวิเคราะห์พฤติกรรมของมนุษย์ได้ซึ่งในเรื่องของบทบาทนี้ได้มีนักวิชาการแบ่งประเภทของบทบาทไว้ดังนี้

Cohen (1978, p. 35) ได้อธิบายเรื่องลักษณะของบทบาทไว้ ดังนี้

1. บทบาทที่ถูกกำหนด (prescribed role) คือ การที่สังคมได้กำหนดเฉพาะเจาะจงให้เราปฏิบัติหน้าที่ตามบทบาทใดบทบาทหนึ่งนั้น ถึงแม้ว่าบุคคลบางคนจะไม่ได้ ประพฤติปฏิบัติตามบทบาทที่คาดหวังโดยผู้อื่น เราก็ยังยอมรับว่าจะต้องปฏิบัติไปตามบทบาทที่สังคมกำหนดให้

2. บทบาทที่ปฏิบัติจริง (enacted role) เป็นวิธีที่บุคคลได้แสดงหรือปฏิบัติออกมาจริงตามตำแหน่งของเขา ความไม่ตรงกันของบทบาทหน้าที่ถูกกำหนดกับบทบาทที่ปฏิบัติจริงอาจมีสาเหตุมาจากบุคคลขาด ความเข้าใจในส่วนของบทบาทที่ต้องการ (lack of understanding) ความไม่เห็นด้วย (not to conform) หรือไม่ลงรอยกับบทบาทที่ถูกกำหนดและบุคคลไม่มีความสามารถ (inability) ที่จะแสดงบทบาทนั้นได้อย่างมีประสิทธิภาพจากทฤษฎีสัญญาประชาคม ที่มีความเกี่ยวพันกับสมมติฐานในเรื่องของภาวะธรรมชาติ และสิทธิโดย ธรรมชาติ กล่าวคือ เมื่อสมัยโบราณยังไม่มีการรวมตัวเป็น บ้านเมืองหรือไม่มีการรวมตัวเป็นรัฐนับได้ว่าเป็นภาวะ ธรรมชาติ โดยขาดความสัมพันธ์เชิงการเมือง ภาวะธรรมชาติเป็นเพียงสภาพแห่งความเป็นองค์รวมของสังคม (society) ยังไม่มีสภาพเป็นสังคมการเมือง (political society or polity) ดังนั้น ในภาวะธรรมชาติ เมื่อยังไม่มี การเกิดขึ้นของสังคมการเมือง มนุษย์ย่อมมีสิทธิตามธรรมชาติ อันได้แก่ สิทธิที่มีมาแต่กำเนิด โดยเฉพาะในการ ปกครองตนเอง และเมื่อมีอยู่ในตัวคนย่อมสามารถ มอบให้บุคคลอื่นได้ ซึ่งการมอบหมายสิทธิที่มีติดตัวเองมา (คือสิทธิธรรมชาติ) ให้ผู้อื่นนี้ อาจทำได้ในรูปของการให้ทำหน้าที่อย่างหนึ่งหรือประกอบกิจหลายอย่างก็ได้ การ มอบหมาย (delegate) มีลักษณะแห่งการให้เป็น “ตัวแทน” (representation) ในข้อ สมมติฐานว่ามีการมอบหมาย สิทธินี้ให้ถือว่าเป็นการกระทำพร้อม ๆ กันหลายคน เรียกว่ามีการทำ “สัญญาประชาคม” คือ ข้อสมมติฐานว่ามี การทำสัญญาโดยที่มีการมอบอำนาจหรือมอบสิทธิให้บุคคลใดบุคคลหนึ่งให้เป็นผู้นำหรือผู้ปกครองของชุมชนนั้น มีนักคิดหลายคนที่ได้สร้างทฤษฎีเกี่ยวกับสัญญาประชาคม เช่น ฮอบส์ และจอห์น ล็อค เป็นต้น ซึ่งผู้ปกครองที่ได้ มอบหมายอำนาจนี้บางทฤษฎีสัญญาประชาคมอ้างว่าเป็นการมอบหมายอย่างเต็มที่และเด็ดขาด บางทฤษฎีอ้าง ว่าเป็นการมอบหมายโดยมีเงื่อนไข (จิรโชค วีระสย, สุรพล ราชภัณฑารักษ์ และสุรพันธ์ ทับสุวรรณ์, 2551, หน้า 156-158)

การบริหารภาครัฐ มีขอบข่ายกว้างขวางและมีผลกระทบต่อคนจำนวนมากทั่วประเทศ เป็นการบริหารที่อยู่ภายใต้การควบคุมของประชาชน ประชาชนอาจจะควบคุม เองหรืออาจให้สมาชิกสภานิติบัญญัติควบคุมก็ได้ประชาชนมีสิทธิที่จะทราบผลของการ ปฏิบัติงานของภาครัฐ ประชาชนมีสิทธิที่จะทราบขั้นตอนการปฏิบัติ ประชาชนหรือสื่อมวลชนมีสิทธิที่จะวิพากษ์วิจารณ์

เจ้าหน้าที่ภาครัฐในประเทศที่มีการปกครองระบอบประชาธิปไตย จะโกรธหรือประณามประชาชนไม่ได้ การบริหารภาครัฐเป็นกิจกรรมส่วนรวมซึ่งประชาชนพุกคนเป็นเจ้าของและ มีส่วนได้ส่วนเสีย เพราะประชาชนเสียภาษีอากรให้รัฐนำไปบริหารประเทศ เป็นกิจกรรมที่เกี่ยวข้องกับการเมือง

การปกครองระบอบประชาธิปไตยนั้น รัฐบาลมีหน้าที่จะต้องบำบัดทุกข์บำรุงสุขให้แก่ประชาชน สร้าง ความอยู่ดีกินดีของประชาชน ตลอดจนการยกระดับการครองชีพ ของบุคคลที่ไม่ได้รับความผาสุกเท่าที่ควรให้ดีขึ้น ให้มาตรฐานความเป็นอยู่ของประชาชนอยู่ในระดับที่เหมาะสมเช่นเดียวกับคนอื่น ๆ ทั้งนี้ รัฐจะต้องมีบทบาทที่ สำคัญในการบริหารจัดการโดยจะต้องตระหนักถึงความต้องการพื้นฐาน (basic needs) ประชาชนทุกคนควรจะ ได้รับบริการขั้นพื้นฐานเพื่อไม่ให้ฐานะความเป็นอยู่ของประชาชนแตกต่างกันมากนัก รัฐจะต้องมีบทบาทที่สำคัญ และจะต้องให้ความเป็นธรรมทางสังคม (social justice) และตั้งอยู่บนพื้นฐานความถูกต้องของกฎหมาย ความ ยุติธรรมทางสังคม ไม่เลือกปฏิบัติ เน้นความโปร่งใสด้วยการเปิดโอกาสให้ประชาชนมีส่วนร่วมในการตรวจสอบแนวคิดเกี่ยวกับการจัดการภัยคุกคามอาชญากรรมไซเบอร์

ประเทศไทยมีภัยคุกคามทางด้านไซเบอร์เป็นจำนวนมาก ระบบคอมพิวเตอร์ของไทยถูกใช้เป็นฐานใน การโจมตีไปยังประเทศอื่นด้วย ทำให้เกิดความเสียหายเป็นวงกว้าง หรือเสียหายต่อทรัพยากรภาพลักษณ์ และ ความเชื่อมั่นต่อประเทศการโจมตีเป็นการเข้าไปเปลี่ยนแปลงหน้าเว็บเพจของหน่วยงานภาครัฐ ซึ่งเกิดเหตุขึ้น บ่อยครั้ง ฝ่ายความมั่นคงโดยเฉพาะกองทัพบกจึงต้องมีการดำเนินการจัดตั้งศูนย์ไซเบอร์กองทัพบก เนื่องจากมี กลุ่มผู้ไม่หวังดีใช้เครือข่ายมุ่งโจมตีหน่วยงานของรัฐ หรือการเผยแพร่ข่าวสารอันเป็น เท็จที่ส่งผลกระทบต่อ ความมั่นคงของชาติ การรักษาความปลอดภัยทางไซเบอร์ของ กองทัพบกจะเน้นความร่วมมือกับหน่วยงานภาครัฐ และองค์กรภาคเอกชน โดยร่วมมือทั้งเรื่ององค์ความรู้ และการเฝ้าระวังภัยคุกคามทางด้านไซเบอร์ที่เป็นภัยคุกคาม ร้ายแรงต่อระบบเครือข่ายคอมพิวเตอร์โดยฝึกผู้เชี่ยวชาญด้านไซเบอร์มุ่งเน้นในเรื่องการรักษา ความปลอดภัย ทางไซเบอร์ 3 ประการ ดังนี้ (อริย์ธัช แก้วเกาะสะน้า, 2560, หน้า 6-8)

1. การป้องกัน (Identify & Protect) โดยการตรวจสอบช่องโหว่ที่มีในระบบการทดสอบการเจาะการ เข้าสู่ระบบ หากตรวจพบช่องโหวในระบบจะได้ดำเนินการแก้ไขให้มีความปลอดภัยเพิ่มขึ้น

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

3. การสนองตอบภัยคุกคามแบบเรียลไทม์ (Repond) โดยจัดทำแผนตอบสนอง ต่อภัยคุกคามตามขั้นตอน ที่ได้กำหนดไว้ คือการสืบสวนสอบสวนทางดิจิทัลและนิติวิทยาศาสตร์ การวิเคราะห์หาสาเหตุของภัยคุกคามที่ เกิดขึ้น รวมถึงการประสานงานไปยังหน่วยงานที่เกี่ยวข้องเพื่อดำเนินงานตามขั้นตอนของกฎหมาย

สถานภาพด้านความปลอดภัยไซเบอร์ของโลกและประเทศไทย

สหภาพโทรคมนาคมระหว่างประเทศ (ITU) ได้จัดทำดัชนีความมั่นคงปลอดภัยทางไซเบอร์โลก (Global Cybersecurity Index -- GCI) ซึ่งเป็นดัชนีชี้วัดระดับของการ พัฒนาการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ของแต่ละประเทศ โดยมีวัตถุประสงค์ เพื่อสร้างแรงจูงใจให้แต่ละประเทศตระหนักถึงการรักษาความมั่นคง ปลอดภัยทางไซเบอร์ โดยการใช้จัดอันดับ (ranking) มาเป็นเครื่องมือสำคัญในการสร้างความตระหนักเรื่องการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งมีเป้าหมายสูงสุดที่ต้องการทำให้การรักษาความมั่นคงปลอดภัยทาง ไซเบอร์เป็นวัฒนธรรมของโลกและหลอมรวมให้อยู่ในแก่นของเทคโนโลยีสารสนเทศและการสื่อสาร การประเมิน ความมั่นคงปลอดภัยทางไซเบอร์ จึงพิจารณาจากปัจจัยหลักทั้งหมด 5 ด้าน ได้แก่ มาตรการทางกฎหมาย (Legal Measures) มาตรการทางเทคนิค (Technical Measures) มาตรการการจัดโครงสร้างองค์กร (Organization Measures) การพัฒนา ศักยภาพบุคลากร (Capacity Building) และการสร้างความร่วมมือ (Cooperation)

แนวคิดเกี่ยวกับเกี่ยวกับอาชญากรรมและการป้องกันอาชญากรรม

ความหมายของอาชญากรรมพจนานุกรมฉบับราชบัณฑิตยสถาน พ.ศ. 2525 (ราชบัณฑิตยสถาน, 2531, หน้า 105) อธิบายว่า อาชญากรรมเป็นการกระทำผิดทางอาญา

Quinney (1970, pp. 15-16) กล่าวว่า อาชญากรรม คือ พฤติกรรมของคนที่องค์กร ซึ่งมีอำนาจหน้าที่ ในสังคมที่ดำรงอยู่แบบการเมืองได้กำหนดขึ้น หมายความว่า พฤติกรรมใดจะเป็นอาชญากรรมก็ต่อเมื่อองค์กรเป็น ผู้กำหนดขึ้น ซึ่งการกำหนดนั้นกำหนดไว้ในกฎหมาย องค์กรที่ว่านี้เป็นองค์กรที่มีอำนาจหน้าที่ในเรื่องอาชญากรรม ด้วย และเป็นองค์กรซึ่งเกิดขึ้นในสังคมที่ดำรงอยู่แบบการเมือง คือ เป็นสังคมที่มีผู้ปกครอง และผู้ใต้ปกครอง แนวความคิดนี้มีองค์ประกอบที่สำคัญ 3 ประการ คือ มีกฎหมายมีผู้ออกและผู้ใช้กฎหมาย และมีผู้ละเมิดกฎหมาย

โสพส พินิจศักดิ์ (2526, หน้า 11-12) กล่าวว่า อาชญากรรม หมายถึง ปรากฏการณ์หนึ่งทางสังคมที่เกิดขึ้น โดยการกระทำของบุคคล ซึ่งการกระทำนั้น กฎหมายได้บัญญัติเป็นข้อห้ามและถือว่าเป็นความผิด ซึ่งผู้กระทำ จะต้องได้รับการลงโทษ

อัณณพ ชูบำรุง (2532, หน้า 4) กล่าวว่า อาชญากรรม หมายถึง พฤติกรรมซึ่งมีผล ให้บุคคลและสังคม ได้รับอันตรายทั้งต่อชีวิต ร่างกายและทรัพย์สิน จึงจำเป็นต้องมีการ ลงโทษผู้ประพฤติเช่นนั้น โดยฝ่ายที่มีอำนาจ ทางกฎหมาย

นวลจันทร์ ทัศนชัยกุล (2541, หน้า 32) กล่าวว่า อาชญากรรม หมายถึง พฤติกรรมที่ไม่ถูกต้องตามกฎหมาย หรือผิดแปลกไปจากประเพณีและวัฒนธรรมที่สังคมวางไว้

ดังนั้น อาชญากรรม หมายถึง พฤติกรรมของบุคคลที่มีความเกี่ยวข้องสัมพันธ์ หรือเชื่อมโยงกับสิ่งอื่น ๆ อีกหลายสิ่งเป็นพฤติกรรมที่เบี่ยงเบนไปจากบรรทัดฐานของ สังคมซึ่งเป็นกฎเกณฑ์ที่สังคมกำหนดขึ้น เพื่อให้ บุคคลส่วนใหญ่ในสังคมอยู่ในบรรทัดฐานที่สังคมเห็นว่าเป็นสิ่งที่ดีงาม หากบุคคลใดประพฤติเบี่ยงเบนออกไป จากบรรทัด ฐานดังกล่าว สังคมย่อมมอง เห็นและแสดงปฏิกิริยาตอบโต้ออกไป อาชญากรรมจึง เกี่ยวข้องกับ ปัจจัยหลัก 2 ประการ คือ ปัจจัยทางกฎหมายและปัจจัยทางสังคมวิทยา โดยปัจจัยทางกฎหมายควรมีการกำหนด บทลงโทษที่ชัดเจน ส่วนปัจจัยทางสังคมวิทยา เป็น การควบคุมพฤติกรรมของบุคคลไม่ให้กระทำความผิด

แนวความคิดเกี่ยวกับการป้องกันอาชญากรรม

มีนักวิชาการได้ให้ทัศนะเกี่ยวกับความหมายของการป้องกันอาชญากรรม (crime prevention) ไว้ ดังต่อไปนี้

Sutherland and Cressey (1966, p. 142) ได้ให้ความหมายของการป้องกันอาชญากรรมว่าหมายถึง ความพยายามที่จะสกัดกั้นล่วงหน้ามิให้อาชญากรรมเกิดขึ้น

Reckless (1967, p. 124) ได้ให้ความหมายของการป้องกันอาชญากรรมว่าเป็นความพยายามที่จะ สกัดกั้นล่วงหน้ามิให้อาชญากรรมเกิดขึ้นในขณะที่การแก้ไข หมายถึงการลดการกระทำความผิดซ้ำสอง

Beccaria (1963, pp. 91-95) ได้เสนอทัศนะในการป้องกันอาชญากรรมไว้อย่าง กว้าง ๆ สรุปได้ดังนี้

1. การป้องกันอาชญากรรมต้องมีการวางรากฐานโดยนักปรัชญาที่เฉลียวฉลาด พร้อมด้วยคุณธรรมรวมทั้งมีการบัญญัติกฎหมายที่เที่ยงธรรม

2. การป้องกันอาชญากรรม ต้องอาศัยผู้รักษาและตีความกฎหมายที่เที่ยงตรง

3. การป้องกันอาชญากรรม ต้องครอบคลุมถึงการสนับสนุนคุณงามความดีในสังคมโดยยกย่องสรรเสริญและให้รางวัลแก่ผู้ประพฤติปฏิบัติชอบ

4. การป้องกันอาชญากรรม ต้องเน้นความสำคัญที่ส่งเสริมปรับปรุงระบบการศึกษาให้สมบูรณ์ ดังนั้น การป้องกันอาชญากรรม หมายถึง การสกัดกั้นไม่ให้เกิดอาชญากรรมในเบื้องต้น ซึ่งสามารถทำการวางแผนเตรียมการ และลดการกระทำผิดซ้ำได้ในขั้นตอนเดียวกัน ถือว่าการป้องกันอาชญากรรมเป็นมาตรการ ที่จะหยุดยั้งการเกิดอาชญากรรมอย่างได้ผลดีที่สุด

แนวคิดเกี่ยวกับภัยคุกคามอาชญากรรมไซเบอร์

ภัยคุกคาม หมายถึง การแสดงอำนาจด้วยกิริยาหรือวาจาให้หวาดกลัว และทำให้หวาดกลัว โดยพฤติการณ์ ที่คาดคะเนได้ว่าจะก่อให้เกิดความเสียหาย มีผลให้ ฝ่ายที่ถูกคุกคาม ต้องกระทำหรือละเว้นการกระทำอย่างใด อย่างหนึ่ง รวมไปถึงการกระทำอันจะเป็นอันตรายหรือสั่นคลอนต่อความมั่นคงของชาติในทุก ๆ ด้าน

ความหมายของคำว่า “ภัยคุกคามรูปแบบใหม่” ภาษาอังกฤษจะใช้คำว่า “Non- Traditional Threat” นั้น สามารถกล่าวได้ว่าเป็นภัยคุกคามในทุก ๆ มิติ ที่ไม่ใช่ภัยคุกคามเฉพาะมิติด้านทางการทหารเท่านั้น ดังตัวอย่างเช่น ปัญหาโลกร้อนที่ก่อให้เกิดการ เปลี่ยนแปลงทางสิ่งแวดล้อมที่มีผลกระทบต่อความเป็นอยู่ของมวลมนุษยชาติ และระบบนิเวศน์ หรือการเคลื่อนย้ายทุนจากบรรษัทข้ามชาติที่ส่งผลให้ประเทศบางประเทศล้มละลายได้ภายใน ชั่วข้ามคืน หรือการก่อการร้ายและการก่อความไม่สงบที่กระทำต่อผู้บริสุทธิ์ด้วยความรุนแรงและความหวาดกลัว หรือการค้ามนุษย์ข้ามชาติ เป็นต้น

การควบคุมการก่อการร้ายทางไซเบอร์สามารถกระทำได้โดย

1. การควบคุมอาวุธไซเบอร์นั้น ไม่สามารถลดศักยภาพในการทำสงครามไซเบอร์ได้ แตกต่างจากการลดหรือควบคุมอาวุธในรูปแบบอื่น ๆ ทำได้เพียงแค่ห้ามการกระทำต่าง ๆ เท่านั้น ดังนั้น ชาติใดชาติหนึ่งอาจสามารถ เปลี่ยนสถานะของตนจากความเป็นชาติที่ปฏิบัติตามพันธะทุกประการ กลายเป็นชาติที่ล่วงละเมิดได้ภายใน ระยะเวลาเพียงไม่กี่วินาที และโดยปราศจากการเตือนล่วงหน้า

2. นิยามของสงครามไซเบอร์แบบครอบคลุม อาทิ นิยามที่ครอบคลุมถึงการจารกรรมไม่สามารถตรวจสอบ ได้ และไม่จัดว่าเป็นผลประโยชน์ของสหรัฐอเมริกาในฐานะชาติหนึ่ง ถึงกระนั้นก็ตามหน่วยงานด้านข่าวกรองของ ชาติต่าง ๆ รวมถึงรัฐบาลของแต่ละประเทศ ควรริเริ่มให้มีช่องทางเพื่อการหารือกันโดยตรง เพื่อให้กิจกรรมด้าน การข่าวต่าง ๆ จะไม่เป็นกรณีบานปลายออกนอกเหนือการควบคุมหรือกลายเป็นเหตุแห่งความเข้าใจผิดว่าเป็น การแสดงถึงเจตนารมณ์การเป็นปฏิปักษ์

3. ความตกลงระหว่างประเทศซึ่งมีบทบัญญัติห้ามการกระทำที่แน่นอนบางอย่างไว้ อาทิ การโจมตีทาง ไซเบอร์ต่อโครงข่ายสาธารณูปโภคของพลเรือน ถือว่าเป็นประโยชน์สำหรับสหรัฐอเมริกา แต่ด้วยเหตุที่ว่าการ โจมตีดังกล่าวยังคงสามารถเกิดขึ้นได้ต่อไป ความตกลงดังกล่าวจึงไม่ใช่หนทางที่จะทำลายความจำเป็นในการ ดำเนินขั้นตอนต่าง ๆ เพื่อป้องกันในอันที่จะคุ้มครองสาธารณูปโภคเหล่านั้น

4. การตรวจสอบการปฏิบัติตามพันธะในความตกลงเพื่อจำกัดสงครามไซเบอร์ที่สามารถไว้วางใจได้ใน ระดับสูงนั้นไม่สามารถเกิดขึ้นได้ สามารถตรวจสอบพบการล่วงละเมิดได้ แต่การชี้ตัวผู้ลงมืออาจเป็นเรื่องยาก และอาจเป็นการกระทำที่ก่อให้เกิดความคลาดเคลื่อนในเจตนารมณ์ได้ อย่างไรก็ตาม ยังคงมีมาตรการหลายอย่าง ที่ยังผลให้เกิดธรรมเนียมปฏิบัติระหว่างประเทศเพื่อต่อต้านการโจมตีทางไซเบอร์ต่อพลเรือนได้ เช่น การจัดตั้ง คณะผู้เชี่ยวชาญระหว่างประเทศ การกำหนดให้รัฐบาลของแต่ละชาติต้องรับผิดชอบในการป้องกันไม่ให้เกิด การล่วงละเมิดที่มีต้นกำเนิดอยู่ในอาณาเขตของชาตินั้นขึ้น และพันธะในอันที่จะให้ความช่วยเหลือเพื่อยับยั้ง และสอบสวนการโจมตีทางไซเบอร์ขึ้น

5. การจำกัดการโจมตีด้วยสงครามไซเบอร์ต่อโครงข่ายสาธารณูปโภคพลเรือน อาจหมายความว่า สหรัฐอเมริกาและชาติรัฐอื่น ๆ อาจต้องยุติการกระทำใดซึ่งอาจดำเนินการไปแล้วโดยการติดตั้งลอจิกบอมน์ และอาจรวมแทรปดอร์ในโครงข่าย

สาธารณูปโภคของประเทศอื่น ๆ การลักลอบวางลอจิกบอมน์และแทรปดอร์ เอาไว้ทั่วโครงข่ายสาธารณูปโภคดังกล่าวนี้ ถึงแม้จะไม่เป็นที่สังเกตหรือพูดถึงกันมากมายในสื่อมวลชนและ ประชาชนทั่วไปก็ถือเป็นการยั่วยุที่อันตรายอย่างยิ่ง

สรุปได้ว่า ภัยคุกคามทางไซเบอร์ได้มีความรุนแรงมากขึ้นทุกวัน ผู้ก่อการร้ายอาจใช้ประโยชน์จาก ความก้าวหน้าทางไซเบอร์ เพื่อดำเนินการด้วยวิธีต่าง ๆ เช่น ก่อวินาศกรรม โดยมุ่งเป้าไปที่การทำลายที่มี ผลกระทบในวงกว้าง เช่น การทำให้ระบบโครงสร้างกระแสไฟฟ้าขัดข้อง การโจมตีระบบโครงข่ายการสื่อสาร หรือแม้กระทั่งการโจมตีระบบต่าง ๆ ที่ใช้ในการทหารก็อาจสามารถเกิดขึ้นได้เช่นกัน และบางประเทศสามารถ พัฒนาศักยภาพในการทำสงครามไซเบอร์ เพื่อเป็นปฏิบัติการที่ควบคู่ไปกับการทำสงครามแบบปกติ

แนวคิดเกี่ยวกับความมั่นคงแห่งชาติ

ความมั่นคงมีปัจจัยที่เกี่ยวข้องและมีหลักที่นำมาอภิปราย 4 ประการ คือ (ดนัยวัฒนา รุ่งอุทัย, 2558, หน้า 9-10)

1. จุดอ้างของความมั่นคง (Referent Object) หมายถึง การทำความมั่นคงนั้นทำเพื่อใครหรือเพื่ออะไร กล่าวคือเพื่อประชาชนหรือเพื่อรัฐ

2. ค่านิยมหลักหรือค่านิยมแกนกลางของความมั่นคงอยู่ที่ระดับใด เป็นความมั่นคงภายในประเทศ หรือ เป็นความมั่นคงระหว่างประเทศ

3. ลักษณะของภัยคุกคามเป็นการมองความมั่นคงว่าในลักษณะเดิมที่ยึดถือกันมา คือ เป็นเรื่องเกี่ยวกับ ด้านการทหารเพื่อความอยู่รอดของประเทศชาติ หรือรัฐ หรือเป็นการมองในมิติใหม่ คือ ขอบเขตของความมั่นคง ขยายออกไปเป็นความมั่นคงทางด้านเศรษฐกิจ สังคม วัฒนธรรม สิ่งแวดล้อม ประชากร และเรื่องอื่น ๆ

4. แนวคิดหรือวิธีการที่ใช้ในการสร้างความมั่นคง ดังนั้น จึงมีนักวิเคราะห์ด้านความมั่นคงอาจให้ ความสำคัญกับบางปัจจัย และไม่ให้ความสำคัญในบางปัจจัยที่กล่าวมาความหมายของความมั่นคง จึงมีได้ทั้ง แบบที่จำกัดหรือในแบบที่กว้างขวางก็ด้วยปัจจัยเหล่านี้

แนวคิดเรื่องความมั่นคงแห่งชาตินับว่าเป็น เรื่องที่มีความสำคัญยิ่ง ซึ่ง Nye (1995, pp. 90-102 อ้างถึงใน จุลชีพ ชินวรรณโณ, 2546, หน้า 6-7) ได้กล่าวว่า ความมั่นคงมีความสำคัญเหมือนกับออกซิเจนซึ่งเป็นสิ่งที่มนุษย์ ขาดไม่ได้ แต่ในภาวะปกติเรามักจะนึกไม่ถึงและบางทีเรายังเป็นตัวการในการทำลายออกซิเจนด้วย โดยทั่วไป ความมั่นคง (Security) หมายถึง สภาวะความอิสระจากภัยคุกคามต่อคุณค่าที่ถือว่าสำคัญ หรืออีกนัยหนึ่ง ความมั่นคงเป็นความปลอดภัยจากภัยคุกคาม ปลอดจากความวิตกกังวล หรือภัยอันตรายต่าง ๆ ความมั่นคง หมายถึง ภาวะทางจิตของบุคคล อาจเป็นของประชาชน หรือของผู้นำที่มีต่อสภาวะแวดล้อมมากกว่าสภาพที่แท้จริง

ความมั่นคงแห่งชาติ จึงเป็นการดำเนินการของประเทศเพื่อให้ประชาชน ในชาติอยู่ดีมีความสุข ปลอดภัย จากภัยคุกคามมีการดำเนินชีวิตของตนเองและประเทศ ปลอดภัยจากการรุกรานของชาติอื่น ๆ มีเศรษฐกิจ รุ่งเรืองและเป็นที่ยอมรับของนานาประเทศ

ความมั่นคงปลอดภัยทางไซเบอร์

ความมั่นคงปลอดภัย (Security) คือ สถานะที่มีความปลอดภัยไร้กังวล กล่าวคือ อยู่ในสถานะที่ไม่มี อันตรายและได้รับการป้องกันอันตรายทั้งที่เกิดขึ้นโดยตั้งใจหรือโดย บังเอิญ (Whitman & Mattord, 2005) เช่น ความมั่นคงปลอดภัยของประเทศย่อมเกิดขึ้น โดยมีระบบป้องกันหลายระดับเพื่อปกป้องผู้นำประเทศ ทรัพย์สินทรัพยากรและประชากรของประเทศเป็นต้นองค์กรต่าง ๆ หากต้องการให้เกิดความมั่นคงปลอดภัย ย่อมต้องมีระบบป้องกันสิ่งต่าง ๆ หลายระดับเช่นกันโดยทั่วไป องค์กรควรมีความมั่นคงปลอดภัยในส่วนต่าง ๆ ดังนี้

1. ความมั่นคงปลอดภัยทางกายภาพ (Physical security) เป็นการป้องกันสิ่งใด ๆ ทางกายภาพ ไม่ว่าจะเป็นสิ่งของสถานที่หรือพื้นที่ใด ๆ ขององค์กร จากการเข้าถึงที่ไม่ได้รับอนุญาตหรือการนำไปใช้ในทางที่ผิด

2. ความมั่นคงปลอดภัยส่วนบุคคล (Personal security) เป็นการป้องกันที่เกี่ยวข้องกับบุคคลหรือ กลุ่มบุคคล

3. ความมั่นคงปลอดภัยในการปฏิบัติงาน (Operations security) เป็นการป้องกันรายละเอียดต่าง ๆ ของกิจกรรมหรือกลุ่มกิจกรรมใด ๆ

4. ความมั่นคงปลอดภัยในการติดต่อสื่อสาร (Communications security) เป็นการป้องกันสื่อที่ใช้ใน การติดต่อสื่อสาร รวมถึงเทคโนโลยีที่ใช้และเนื้อหาหรือข้อมูลที่ถูกส่งไปตามสื่อสัญญาณดังกล่าวแล้ว

5. ความมั่นคงปลอดภัยของเครือข่าย (Network security) เป็นการป้องกันองค์ประกอบการเชื่อมต่อ และข้อมูลในเครือข่ายคอมพิวเตอร์

6. ความมั่นคงปลอดภัยของสารสนเทศ (Information security) เป็นการป้องกันภัยสารสนเทศในระบบ คอมพิวเตอร์

7. ความมั่นคงปลอดภัยของสารสนเทศ (Information security) คือ การป้องกันสารสนเทศและองค์ประกอบอื่น ๆ ที่เกี่ยวข้องกัน ซึ่งรวมถึงระบบและฮาร์ดแวร์ที่ใช้ในการจัดเก็บและถ่ายโอนสารสนเทศนั้นด้วย

วิธีดำเนินการวิจัย

การวิจัยครั้งนี้ เป็นการวิจัยเชิงคุณภาพ (qualitative research) อันประกอบไปด้วยกระบวนการศึกษา และวิเคราะห์ข้อมูลจากเอกสารหรือการวิจัยเชิงเอกสาร (documentary research) และกระบวนการสัมภาษณ์ เจาะลึก (in-depth interview) มาใช้ในการดำเนินกระบวนการวิจัย

การเก็บรวบรวมข้อมูลที่นำมาใช้ในการวิจัยครั้งนี้ได้กำหนดกระบวนการหรือแนวทางในการเก็บรวบรวม ข้อมูลไว้ 2 รูปแบบ ดังนี้ (1) การเก็บรวบรวมข้อมูลโดยการศึกษาค้นคว้าข้อมูลจากเอกสารทางวิชาการ และ ข้อมูลจากเทคโนโลยีสารสนเทศ (2) การเก็บรวบรวมข้อมูลโดยการสัมภาษณ์แบบเจาะลึก

การวิเคราะห์ข้อมูล ผู้วิจัยได้นำข้อมูลที่ได้จากการสัมภาษณ์เจาะลึก (in-depth interview) มาใช้ใน กระบวนการวิเคราะห์และประมวลผลข้อมูล โดยดำเนินการร่วมกับกระบวนการรวบรวมข้อมูล จากการ ศึกษา ค้นคว้าข้อมูลจากเอกสาร โดยกระบวนการและวิธีการวิเคราะห์อันจะได้ดำเนินกระบวนการตามแนวทางของ การวิจัยเชิงคุณภาพ ได้แก่ การวิเคราะห์ข้อมูลโดยพิจารณาประเด็นหลัก ที่พบในข้อมูลที่ได้รับจากการสัมภาษณ์ ทั้งหมด จากนั้นจึงนำประเด็นหลักมาพิจารณาแบ่งแยกออกเป็นประเด็นย่อยและหัวข้อย่อย อันเป็นกระบวนการ วิเคราะห์ โดยการเริ่มต้นจากการวิเคราะห์ภาพรวมไปสู่การวิเคราะห์ประเด็นย่อยของกระบวนการวิเคราะห์ตามแนว ทางการวิจัยเชิงคุณภาพ ซึ่งทำให้การวิจัยในครั้งนี้มีความเที่ยงตรงและแม่นยำมากยิ่งขึ้น รวมทั้งผู้วิจัยจะดำเนิน กระบวนการในการวิเคราะห์ข้อมูลที่ได้จากการสัมภาษณ์เจาะลึก (in-depth interview) โดยการพรรณาข้อมูลตามปรากฏการณ์ร่วมด้วย เพื่อให้ได้มาซึ่งข้อค้นพบจากกระบวนการวิจัยเชิงคุณภาพ อันประกอบไปด้วย (1) พันตำรวจโท วิชัย สุวรรณประเสริฐ ผู้อำนวยการกองคดีเทคโนโลยีและสารสนเทศ สังกัดกองคดีเทคโนโลยีและ สารสนเทศ กรมสอบสวนคดีพิเศษ (D.S.I.) กระทรวงยุติธรรม (2) นายณัฐวัฒน์ วรสิทธิ์ตระกูล ผู้เชี่ยวชาญพัฒนา ระบบดิจิทัล สังกัดฝ่ายปฏิบัติการ ส่วนสนับสนุนบริการ สำนักงานพัฒนา -รัฐบาลดิจิทัล (สพร.) (3) นายอารยะ - สวัสดิชัย รักษาการผู้จัดการศูนย์ประสานงานความมั่นคงปลอดภัยไซเบอร์ สำนักงานพัฒนาธุรกรรมอิเล็กทรอนิคส์ (สพธอ.) (4) นางสาวอัจฉรินทร์ พัฒนาพันธ์ชัย ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และ (5) พลตรี อภิศักดิ์ - สมบัติเจริญนนท์ ผู้อำนวยการศูนย์ศึกษายุทธศาสตร์ สถาบัน -วิชาการป้องกันประเทศ

กองทัพบก ซึ่งผู้ให้ข้อมูล สำคัญกลุ่มนี้ มีตำแหน่งเป็นผู้บริหารระดับสูงขององค์กร และเป็นหน่วยงานขนาดใหญ่ที่มีข้อมูลครบถ้วน และมี ประสบการณ์ด้านการป้องกันอาชญากรรมไซเบอร์เพื่อความมั่นคงทางเศรษฐกิจและสังคม

ผลการวิจัย

การวิจัยเรื่อง บทบาทภาครัฐในการป้องกันอาชญากรรมไซเบอร์เพื่อความมั่นคง ทางเศรษฐกิจและสังคม ผลการวิจัยพบว่า การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ รัฐบาลจำเป็น ต้องใช้มาตรการทางกฎหมาย รวมถึงการกำกับดูแลตนเอง และการกำกับดูแลร่วมกันของทุกภาคส่วน ได้แก่ ภาครัฐ ภาคเอกชน และภาคประชาสังคม อย่างไรก็ดี แม้มาตรการทางกฎหมายจะเข้มงวดมากเท่าใด แต่ก็ อาจมีความจำเป็นในการรักษาความมั่นคงปลอดภัยไซเบอร์ อันอาจกระทบถึงความมั่นคงของชาติ แต่ความเข้มข้น ของมาตรการดังกล่าว รัฐบาลก็ต้องคำนึงถึงสิทธิเสรีภาพของประชาชน ให้ประชาชนยังคงดำรงซึ่งสิทธิเสรีภาพ ในโลกไซเบอร์เสมอกับที่มีในโลกแห่งความเป็นจริงด้วยปัญหาและอุปสรรคบทบาทภาครัฐในการป้องกันอาชญากรรมไซเบอร์เพื่อความมั่นคงทางเศรษฐกิจ และสังคม มีดังนี้ (1) ความซ้ำซ้อนของข้อมูล (2) การบูรณาการ (3) ความทันสมัยของเทคโนโลยี (4) การประสาน ความร่วมมือ (5) การจัดสรรงบประมาณ และ (6) ศักยภาพของบุคลากร

ข้อเสนอแนะและแนวทางแก้ไขการป้องกันอาชญากรรมไซเบอร์ เพื่อความมั่นคงทางเศรษฐกิจและสังคม พบว่า แนวทางแก้ไขบทบาทภาครัฐในการป้องกันอาชญากรรมไซเบอร์เพื่อความมั่นคงทางเศรษฐกิจและสังคม ได้แก่ การปกป้อง ป้องกันอาชญากรรมไซเบอร์ เสริมสร้างความปลอดภัยระบบเทคโนโลยีสารสนเทศ พัฒนาการ บังคับใช้กฎหมาย พัฒนาศักยภาพทางด้านเทคโนโลยีสารสนเทศ การบูรณาการด้านข้อมูลและกฎหมาย รวมทั้ง ความร่วมมือระหว่างภาครัฐ ภาคเอกชน ภาคประชาชน และระหว่างประเทศ ขณะเดียวกันยังต้องมีการจัดสรร งบประมาณให้เพียงพอต่อการพัฒนาศักยภาพ ทั้งด้านบุคลากรและเทคโนโลยีที่ทันสมัย

อภิปรายผล

จากกระแสโลกาภิวัตน์มีการเปลี่ยนแปลงอย่างรวดเร็วทำให้เกิดการกระทำอาชญากรรมทางคอมพิวเตอร์ หรือไซเบอร์อย่างกว้างขวาง ภาครัฐมีภารกิจเกี่ยวข้องโดยตรงเกี่ยวกับการป้องกันและปราบปรามอาชญากรรม คอมพิวเตอร์ ตระหนักถึงปัญหาเรื่องภัยคุกคามทางคอมพิวเตอร์ที่มีผลกระทบต่อความมั่นคงของประเทศ ประกอบกับการปฏิบัติงานด้านป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ และพระราชบัญญัติการรักษา ความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ให้เป็นไปอย่างมีประสิทธิภาพ เพื่อแลกเปลี่ยนความคิดเห็นในเรื่อง แนวทางการปฏิบัติงานร่วมกันในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ที่มีผลกระทบต่อความ มั่นคงของประเทศ เพื่อบูรณาการหน่วยงานที่เกี่ยวข้องในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ โดยหน่วยงานหลักด้านการป้องกันอาชญากรรมไซเบอร์ ได้แก่ กองทัพบก กรมสอบสวนคดีพิเศษ สำนักงานพัฒนา -ธุรกรรมอิเล็กทรอนิกส์ (สพธอ.) สำนักงานพัฒนารัฐบาลดิจิทัล และกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ได้มี การพัฒนาบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์มาอย่างต่อเนื่อง ทั้งนี้มีการบูรณาการร่วมกันระหว่าง หน่วยงานภาครัฐ ภาคเอกชน ภาคประชาชน และสถาบันการศึกษาต่าง ๆ เพื่อเป็นการป้องกันอาชญากรรมไซเบอร์ ให้ครอบคลุมงานแต่ละสาขา รวมทั้งระบบโครงสร้างพื้นฐานของประเทศ ซึ่งสอดคล้องกับงานวิจัยของ ธำรงค์ -เมฆเฉลิม (2549) ศึกษาเรื่อง บทบาทของกองอำนวยการรักษาความมั่นคงภายในกับภัยคุกคามในยุคโลกาภิวัตน์ ผลการศึกษาพบว่า โครงสร้างในภาพรวมต้องมีการปรับปรุงโครงสร้างให้เป็นหน่วยที่มีอัตราการจัดหน่วยที่ถาวร รับผิดชอบงานเรื่องความมั่นคงภายในทั้งหมด โดยบูรณาการหน่วยงานที่เกี่ยวข้องมาปฏิบัติงาน และให้ประชาชน มีส่วนร่วมในการแก้ปัญหาอย่างจริงจัง เพื่อเพิ่มขีดความสามารถในการปฏิบัติงานด้านการสืบสวนสอบสวนและ ป้องกัน

ปราบปรามอาชญากรรม และเพื่อร่วมกันกำหนดแนวทางการปฏิบัติงานด้านการป้องกัน และปราบปราม อาชญากรรมคอมพิวเตอร์ที่มีผลกระทบต่อความมั่นคงของประเทศ

ปัญหาและอุปสรรคของภาครัฐในการป้องกันอาชญากรรมไซเบอร์เพื่อความมั่นคงทางเศรษฐกิจและสังคม ได้แก่ ความซ้ำซ้อนของข้อมูล การบูรณาการ ความทันสมัยของเทคโนโลยี การประสานความร่วมมือ การจัดสรร งบประมาณ และศักยภาพของบุคลากร ซึ่งสอดคล้องกับผลงานวิจัยของ อุบลวรรณ ภีระเป็ง (2558) ผลการศึกษา พบว่า แม้ว่าการโจมตีทางไซเบอร์จะเป็นวิธีการและปัจจัยในการสู้รบใหม่และไม่ปรากฏข้อบทที่เกี่ยวข้องกับการใช้เทคโนโลยีตามกฎหมายมนุษยธรรมระหว่างประเทศแต่กฎหมายมนุษยธรรมระหว่างประเทศสามารถ ยืดหยุ่น ครอบคลุมกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ อันเป็นการนำเอาเทคโนโลยี สารสนเทศและคอมพิวเตอร์หรือไซเบอร์มาใช้ในปฏิบัติการทางทหารและการสู้รบได้ อีกทั้งการโจมตีทางไซเบอร์ยังเป็นการกระทำภายในห้วงไซเบอร์ที่ไม่มีลักษณะทางกายภาพ ก่อให้เกิดข้อท้าทายในบังคับใช้หลักการสำคัญ ตามกฎหมายมนุษยธรรมระหว่างประเทศ ไม่ว่าจะเป็นหลักการแยกแยะเป้าหมาย หลักความได้สัดส่วนในการ โจมตี หลักการใช้ความระมัดระวังในการโจมตีอย่างมีนัยสำคัญ จำเป็นจะต้องอาศัยความร่วมมือจากผู้ที่มีส่วน เกี่ยวข้องทั้งภาคประชาสังคม ภาครัฐ และความร่วมมือระหว่างประเทศในการพัฒนาแนวทางการรับมือการโจมตี ทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่จะนำไปสู่แนวทางปฏิบัติของรัฐที่ชัดเจนต่อไป และยังสอดคล้องกับ งานวิจัยของ ธนะศักดิ์ ปฏิมาประกร (2557) ผลการวิจัยพบว่า นโยบายความมั่นคงในระดับชาติ กองทัพไทย รับผิดชอบจัดระเบียบความมั่นคงชายแดนนับเป็นโอกาสดีที่ทุกภาคส่วนได้ให้ความสำคัญกับการเข้าสู่ประชาคม -อาเซียน เกิดการบูรณาการร่วมได้ดียิ่งขึ้น แต่ยังมีอุปสรรคจากภัยคุกคามทั้งตามแบบและไม่ตามแบบ ซึ่งจุดแข็ง ของกองทัพไทยเป็นกองทัพชั้นนำกองทัพหนึ่งของอาเซียน ทั้งกำลังพลและยุทโธปกรณ์ และมีกลไกความร่วมมือ ด้านความมั่นคงกับประเทศเพื่อนบ้านจุดอ่อนยังขาดกฎหมายรองรับ และขาดแคลนยุทโธปกรณ์ที่เหมาะสม รวมถึงการเมืองที่ไม่มีเสถียรภาพส่งผล ต่อความต่อเนื่องในการบริหารจัดการความมั่นคง ตลอดจนการประสาน ความร่วมมือ ไม่สามารถดำเนินได้เพียงลำพัง จำเป็นต้องประสานความร่วมมือกันภายในหน่วยงาน ระหว่าง หน่วยงาน และระหว่างประเทศ เพื่อป้องกันปราบปรามให้เกิดประสิทธิภาพยิ่งขึ้น สอดคล้องกับผลงานวิจัยของ ณรงค์ กุลนิเทศ (2558) ผลการศึกษาพบว่า การสร้างเครือข่ายพันธมิตร (alliance) ของหน่วยงานต่าง ๆ ทั้ง ภาครัฐและภาคเอกชน โดยเฉพาะในการให้ความช่วยเหลือด้านการรวบรวมพยานหลักฐาน การรวบรวมข้อเท็จจริง ต่าง ๆ ที่ยุ่งยากซับซ้อน จะทำให้ปรากฏได้ง่ายขึ้น

ข้อเสนอแนะ

ข้อเสนอแนะจากผลที่ได้ในการศึกษา

1. ภาครัฐควรมีการกำหนดโครงสร้างพื้นฐานวิกฤตของชาติให้ชัดเจน และกำหนดนโยบายที่คุ้มครองโครงสร้างพื้นฐานวิกฤตของชาติ การดำเนินการดังกล่าวเป็นเรื่องระดับชาติที่ต้องใช้เวลาและทรัพยากรจำนวนมาก จะต้องมีการกำหนดมาตรการและแนวทางดำเนินการที่มีกรอบเวลาที่ชัดเจน

2. ภาครัฐควรกระตุ้นให้หน่วยงานต่าง ๆ ทั้งภาครัฐและภาคเอกชนนำมาตรฐาน ISO 27001 ซึ่งเป็น ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System -- ISMS) มาใช้ ในการป้องกันอาชญากรรมไซเบอร์ขั้นพื้นฐานให้แก่องค์กร

3. ประเทศไทยยังขาดแคลนบุคลากรทางด้านการป้องกันอาชญากรรมไซเบอร์ ภาครัฐควรเร่งพัฒนา ผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์ให้เพียงพอกับจำนวนของหน่วยงานภาครัฐและภาคเอกชน ซึ่งหลายองค์กร ยังขาดแคลนบุคลากรที่ได้รับการ

รับรองทางด้านความปลอดภัยไซเบอร์จากหน่วยงานสากล และมักจะให้ผู้ดูแล เครือข่าย ทำหน้าที่ในการดูแลอาชญากรรมไซเบอร์ไปด้วย

4. ภาครัฐควรให้การสนับสนุนและเพิ่มการสนับสนุนการดำเนินการวิจัยและพัฒนาเทคโนโลยีทั้งด้าน ฮาร์ดแวร์และซอฟต์แวร์ที่เกี่ยวข้องกับการรับมือกับอาชญากรรมไซเบอร์อย่างจริงจัง ซึ่งการวิจัยพัฒนาเป็น ส่วนสำคัญในการสร้างความแข็งแกร่งให้แก่บุคลากร และยังช่วยประหยัดงบประมาณในการที่ต้องนำเข้า เทคโนโลยีจากต่างประเทศ

5. หน่วยงานที่เกี่ยวข้องควรพัฒนาอาชญากรรมไซเบอร์ที่กำหนดโดย ITU มาเป็นแนวทางปฏิบัติ เพื่อ ยกระดับความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งประกอบด้วย การพัฒนาด้านกฎหมาย การพัฒนา ด้านเทคนิค การพัฒนาด้านองค์การ การพัฒนาด้านความสามารถ และการพัฒนาด้านการดำเนินงานร่วม

6. จากการที่อาชญากรรมไซเบอร์ส่งผลเสียหายเป็นวงกว้างและกระทบต่อความมั่นคงของชาติ หน่วยงาน ทั้งภาครัฐและภาคเอกชนควรให้ความสำคัญคับภัยคุกคามไซเบอร์ และควรดำเนินการจัดตั้งหน่วยงานหรือ ทีมงานซึ่งทำหน้าที่ในป้องกันอาชญากรรมไซเบอร์ให้แก่หน่วยงานของตนเอง

7. การป้องกันอาชญากรรมไซเบอร์ควรมีการปฏิบัติงานในลักษณะเป็นเครือข่าย การปฏิบัติงานเป็น การกระจายหน้าที่การแจ้งเตือนและการรับมือกับภัยคุกคามไซเบอร์ ให้แก่หน่วยงานอื่นที่ดำเนินงานด้าน เทคโนโลยีสารสนเทศและการสื่อสาร

8. การให้ความรู้ทั้งภาครัฐ ภาคเอกชน และภาคประชาชน ด้วยการจัดฝึกอบรม หรือจัดทำเอกสาร คู่มือโดยให้ความรู้ที่ทันเหตุการณ์ โดยความรู้ที่ควรเผยแพร่ ได้แก่ ความรู้เกี่ยวกับอาชญากรรมคอมพิวเตอร์ ความรู้เกี่ยวกับข้อกฎหมาย ความรู้เกี่ยวกับเทคโนโลยีในการป้องกัน และความรู้เกี่ยวกับการใช้งานคอมพิวเตอร์ และอินเตอร์เน็ตให้มีความปลอดภัย ซึ่งทุกภาคส่วนควรรู้เท่าทันและตระหนักถึงความเสี่ยงต่ออาชญากรรมไซเบอร์ เพื่อเป็นการป้องกันตนเอง โดยการให้ความรู้ต้องทำอย่างต่อเนื่องและสม่ำเสมอ

9. ในการพัฒนาข้อกฎหมายเกี่ยวกับอาชญากรรมไซเบอร์ควรจะรับฟังความคิดเห็นจากทุกภาคส่วนที่ เกี่ยวข้อง ได้แก่ ประชาชน ภาครัฐ องค์กรเอกชน ผู้ให้บริการอินเตอร์เน็ต เพื่อจัดทำข้อกฎหมายที่ชัดเจนเป็นธรรม โดยตั้งอยู่บนพื้นฐานสิทธิและเสรีภาพและความสมัครใจในการบังคับใช้กฎหมาย โดยคำนึงถึงความชัดเจนใน เกณฑ์การตัดสินคดีว่ากรณีใดผิด กรณีใดไม่ผิด เพื่อให้ทุกภาคส่วนมีทัศนคติที่ดีต่อกฎหมายที่นำมาบังคับใช้ โดยการสร้างทัศนคติที่ดีควรเริ่มจากการศึกษาปัญหาและร่างข้อกฎหมายร่วมกันจากทุกภาคส่วนที่มีความ เกี่ยวข้อง เพื่อหาจุดร่วมที่เป็นธรรมต่อทุกฝ่าย

ข้อเสนอแนะในการทำวิจัยต่อยอดในครั้งต่อไป

ควรมีการศึกษาแนวทางการเชื่อมโยงขององค์กรที่เกี่ยวข้องกับการพัฒนาทางไซเบอร์ เพื่อสร้างความ เข้มแข็งขององค์กรและสร้างเครือข่ายของหน่วยงานให้สามารถเชื่อมข้อมูลระหว่างกันได้ เนื่องจากไซเบอร์มี การเปลี่ยนแปลงอย่างต่อเนื่องและมีบทบาทต่อการดำรงชีวิตของประชาชน ซึ่งการป้องกันอาชญากรรมไซเบอร์ เพื่อความมั่นคงทางเศรษฐกิจและสังคมนี้เป็นองค์ความรู้ใหม่ เพื่อให้เข้าใจถึงอาชญากรรมแต่ละรูปแบบมี ผลกระทบต่อผู้ใช้งานอย่างไร เพื่อหาแนวทางการป้องกันอาชญากรรมไซเบอร์ในแต่ละรูปแบบได้อย่างเฉพาะ เจาะจง สามารถป้องกันและต่อต้านอาชญากรรมไซเบอร์ได้อย่างมีประสิทธิภาพมากยิ่งขึ้นต่อไป

เอกสารอ้างอิง

จิรโชค วีระสย, สุรพล ราชกัณฑารักษ์ และสุรพันธ์ ทับสุวรรณ. (2551). รัฐศาสตร์ทั่วไป. กรุงเทพฯ: สำนักพิมพ์- มหาวิทยาลัยรามคำแหง.

จุลชีพ ชินวรรณโณ. (2546). ความมั่นคงในภูมิภาคเอเชียตะวันออกเฉียงใต้ในศตวรรษที่ 21: ประเทศไทยกับ แนวคิดยุทธศาสตร์และความมั่นคงจากอดีตถึงปัจจุบัน. กรุงเทพฯ: วิทยาลัยป้องกันราชอาณาจักร- สถาบันวิชาการป้องกันประเทศ.

ดนัยวัฒนา รุ่งอุทัย. (2558). ความร่วมมือต้านความมั่นคงของประเทศในภูมิภาคเอเชียตะวันออกเฉียงใต้ ภายใต้อาเซียน. กรุงเทพฯ: จุฬาลงกรณ์มหาวิทยาลัย.

นวลจันทร์ ทัศนชัยกุล. (2541). อาชญากรรม. กรุงเทพฯ: พรทิพย์การพิมพ์.

ราชบัณฑิตยสถาน. (2531). พจนานุกรมฉบับราชบัณฑิตยสถาน พ.ศ. 2525. กรุงเทพฯ: ไทยวัฒนาพานิช.

โสพส พินิจศักดิ์. (2526). การยอมรับบทบาทของบุคลากรด้านอาชญาวิทยาในการบัญชาการตำรวจนครบาล. วิทยานิพนธ์รัฐศาสตรมหาบัณฑิต (สาขาอาชญาวิทยาและงานยุติธรรม), มหาวิทยาลัยมหิดล.

อริย์ธัช แก้วเกาะสะบ้า. (2560). ศูนย์ไซเบอร์กองทัพบก. กรุงเทพฯ: สำนักวิชาการ, สำนักงานเลขาธิการสภาผู้แทนราษฎร.

อัณณพ ชูบำรุง. (2532). ทฤษฎีอาชญาวิทยา. กรุงเทพฯ: มหาวิทยาลัยเกษตรศาสตร์.

Beccaria, c. (1963). On crime &punishment Indianapolis. New York: Bobbs- Merill.

Cohen, B. J. (1978). Introduction to sociology. New York: McGraw-Hill.

Marketing Oops. (2018). Cyber Security Archives. Retrieved April 12, 2019, from https://www.marketingoops.com/tag/cyber-security/

Mariam, D. C., & Florian, J. E. (2019). The Politics of Cybersecurity: Balancing Different Roles of the State. St Antony's International Review, 15(1): 37-57.

Quinney, R. (1970). The Social Reality Crime. Boston: Little Brown.

Reckless, W.C. (1967). The Crime Problem. New York: Apple-ton Century Crofts.

Sutherland, E. EL, & Cressey, F. G. (1966). Communication of Innovation: A Cross Culturach Approach. New York: The Free.

ThaiPR.NET. (2560). ภัยคุกคามรูปแบบใหม่บน ioT อีเมล์และคลาวด์. Retrieved 15 August 2018, from https://www.ryt9.eom/s/prg/2727778

Whitman, E. M., & Mattord, J. H. (2005). Principles of information security (2rd ed.). New York: