มาตรการป้องกันอาชญากรรมไซเบอร์ของกรมสอบสวนคดีพิเศษ

Cybercrime Prevention Measures of the Department of Special Investigation

ชฎาภรณ์ สิงห์แก้ว[1] ภานุเดช ปัญญา[2]

Chadaporn Singkaew and Panudet Panya

Received: October 27, 2021 Revised: October 27, 2021 Accepted: February 2, 2022

บทคัดย่อ (Abstract)

บทความนี้มีวัตถุประสงค์ เพื่อศึกษามาตรการป้องกันอาชญากรรมไซเบอร์ของกรมสอบสวนคดีพิเศษ โดยใช้วิธีการวิจัยเชิงคุณภาพ เก็บข้อมูลจากการวิจัยเอกสาร และการสัมภาษณ์เจาะลึกจากผู้ให้ข้อมูลสำคัญ โดยใช้วิธีการวิจัยเชิงคุณภาพ (Qualitative Research) เก็บข้อมูลจากการวิจัยเอกสาร และการสัมภาษณ์เจาะลึก จากผู้ให้ข้อมูลสำคัญ ได้แก่ บุคลากรที่มีส่วนเกี่ยวข้องกับมาตรการป้องกันอาชญากรรมไซเบอร์ของกรมสอบสวนคดีพิเศษ การศึกษาวิจัยได้กระทำในช่วงปี 2557 - 2562 โดยนำเอาแนวคิดการเมืองกับความปลอดภัยทางไซเบอร์ของ Myriam and Florian (2019) เป็นแนวคิดหลัก รวมทั้งแนวคิดเกี่ยวการจัดการภัยคุกคามอาชญากรรมไซเบอร์ และแนวคิดอาชญากรรมและการป้องกันอาชญากรรมเป็นกรอบในการวิจัย

ผลการวิจัยพบว่า กรมสอบสวนคดีพิเศษในฐานะหน่วยงานของรัฐที่มีภารกิจจะต้องดำเนินการเรื่องความมั่นคงปลอดภัยทางไซเบอร์อย่างเป็นรูปธรรม โดยมีมาตรการป้องกันอาชญากรรมไซเบอร์ที่สำคัญ 3 ด้าน ประกอบด้วย (1) บทบาทในด้านการรักษาความปลอดภัยโดยการสร้างความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ซึ่งหน่วยงานรัฐจำเป็นต้องใช้มาตรการทางกฎหมาย รวมถึงการกำกับดูแลตนเอง และการกำกับดูแลร่วมกันของทุกภาคส่วน ได้แก่ ภาครัฐ ภาคเอกชน และภาคประชาสังคม (2) บทบาทในด้าน

[1] คณะรัฐศาสตร์ มหาวิทยาลัยรามคำแหง

Faculty of Political Science, Ramkhamhaeng University, Email: thanggass@hotmail.com

[2] นักวิจัยอิสระ

Independent researchers, Email: panudet.p789@gmail.com

ผู้สนับสนุน โดยมีการบูรณาการร่วมกับหน่วยงานที่เกี่ยวข้องกับการปฏิบัติงานในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ที่มีผลกระทบต่อความมั่นคงของประเทศ และ (3) บทบาทในด้านตัวแทน โดยร่วมมือกับสถาบันการศึกษาเพื่อให้ความรู้เกี่ยวกับการป้องกันอาชญากรรมไซเบอร์ อย่างไรก็ดี แม้มาตรการทางกฎหมายจะเข้มงวดมากเท่าใด แต่ก็อาจมีความจำเป็นในการรักษาความมั่นคงปลอดภัยไซเบอร์ อันอาจกระทบถึงความมั่นคงของชาติ แต่ความเข้มข้นของมาตรการดังกล่าว รัฐบาลก็ต้องคำนึงถึงสิทธิเสรีภาพของประชาชน ให้ประชาชนยังคงดำรงซึ่งสิทธิเสรีภาพในโลกไซเบอร์เสมอกับที่มีในโลกแห่งความเป็นจริงด้วย

คำสำคัญ (Keywords): อาชญากรรมไซเบอร์ ภัยคุกคาม กรมสอบสวนคดีพิเศษ

Abstract

The article has objective to study the Cybercrime Prevention Measures of the Department of Special Investigation by using a qualitative research method. Collecting data from document and undertaking in-depth interviews with key informants, who are personnel working in the Cybercrime Prevention Measures, Department of Special Investigation The study, conducted from 2014 to 2019, taking the political and cybersecurity concepts of Myriam and Florian (2019) as the main idea. Moveoven the concept of cybercrime threat management and the concept of crime and crime prevention are a framework for research.

The findings revealed that the Department of Special Investigation, as a government agency, has a mission to take concrete action on cybersecurity. There are three important cybercrime prevention measures, consisting of: (1) role in security; by building the security of information technology systems and computer networks which government agencies need to take legal measures, including self-regulation and joint supervision of all sectors, namely the government, the private sector, and civil society, (2) the role in the advocacy, it is integrated with agencies involved in the prevention and suppression of computer crimes affecting national security, and (3) the role of agents by collaborating with educational institutions to educate about cybercrime prevention. But it may also be necessary to maintain

cybersecurity which may affect national security. Even then is the intensity of such measures, the government must take into account the rights and freedoms of the people. Encourage people to maintain their rights and freedoms in cyberspace as they do in the real world.

Keywords: Cyber crime, treat, Department of Special Investigation

บทนำ (Introduction)

การเปลี่ยนแปลงของโลกอย่างรวดเร็วส่งผลต่อพัฒนาการและการเปลี่ยนแปลงของระบบไอซีที ซึ่งมีผลกระทบต่อเศรษฐกิจ สังคม การดำเนินงานทางการเมือง การทหาร และสังคมจิตวิทยาของทุกประเทศในโลกเป็นอย่างมาก จนก่อให้เกิดพื้นที่มิติใหม่ที่เรียกว่า “โลกไซเบอร์” ด้วยเหตุนี้ความมั่นคงแห่งชาติ จึงได้รับผลกระทบจากการปฏิวัติและปรากฏการณ์ของโลกไซเบอร์โดยตรง จนมีการกล่าวถึงความมั่นคงด้านไซเบอร์ในบริบทของความมั่นคงแห่งชาติมากขึ้น ทั้งนี้อาชญากรรมไซเบอร์อาจไม่ได้เกิดจากการกระทำของกลุ่มบุคคล หรือผู้ก่อการร้ายด้านไซเบอร์ตามลำพัง เพราะการกระทำของบุคคลเหล่านี้อาจมีองค์การ หรือรัฐอยู่เบื้องหลังหรือให้การสนับสนุนก็ได้ เพื่อให้บรรลุเป้าหมายทางยุทธศาสตร์ในการสร้างความเสียหายต่อโครงสร้างและส่งผลกระทบต่อความมั่นคงแห่งชาติฝ่ายตรงข้าม นอกจากนี้อาชญากรรมไซเบอร์ยังคงเป็นภัยคุกคามต่อความมั่นคงตั้งแต่ระดับความมั่นคงแห่งชาติไปจนถึงระดับความมั่นคงของมนุษย์ ซึ่งโลกไซเบอร์ในอนาคตมีแนวโน้มขยายตัวเพิ่มขึ้นเป็นทวีคูณ เพราะได้กลายเป็นสิ่งอำนวยความสะดวกต่อวิถีชีวิตมนุษย์ทุกคน และการทำงานประจำวันในองค์กรต่าง ๆ ทุกประเภท อย่างไรก็ตาม โลกไซเบอร์ย่อมมีทั้งด้านที่เป็นบวกและเป็นลบ โดยขึ้นอยู่กับวัตถุประสงค์ของการใช้ ด้วยเหตุนี้การที่มนุษย์ได้ประโยชน์มากมายจากโลกไซเบอร์ก็นำมาซึ่งความท้าทายต่อการรับมือและป้องกันความเสียหายที่เกิดจากการใช้งานดังกล่าวด้วยเช่นกัน ทั้งนี้นักวิเคราะห์จากหลาย ๆ สำนักรวมไปถึงผู้เชี่ยวชาญและนักวิเคราะห์ นักคิดระดับโลกต่างลงความเห็นกันว่า เทคโนโลยีสารสนเทศและการสื่อสารในอนาคตที่จะส่งผลต่อการเปลี่ยนแปลงของโลกในปัจจุบันและในอีก 5-10 ปีข้างหน้า ซึ่งจะมีบทบาทสำคัญในการเปลี่ยนแปลงวิถีชีวิตจะประกอบด้วย (1) เทคโนโลยีพกพา (Mobile) (2) เครือข่ายสังคมออนไลน์ (Social network) (3) การประมวลผลแบบก้อนเมฆ (Cloud computing) (4) เทคโนโลยีการจัดการข้อมูลจำนวนมหาศาล (Big data) (วรุฒิ บุญประยงค์, 2558) เทคโนโลยีทั้งสี่ประเด็นนี้ หากประเทศไทยมีการศึกษาและหลอมรวมเรื่องดังกล่าวเพื่อให้สามารถเรียนรู้ได้อย่างเท่าทัน จะส่งผลต่อการพัฒนาประเทศได้อย่างมหาศาล

โลกเข้าสู่สังคมฐานความรู้ที่มีการเชื่อมโยงข้อมูลเป็นระบบเครือข่าย โดยเฉพาะอย่างยิ่งเครือข่ายอินเตอร์เน็ตเข้ามามีบทบาทในชีวิตของมนุษย์แทบทุกมิติ ไม่ว่าจะเป็นความบันเทิงและนันทนาการด้วยการอ่าน การดู และการฟังเนื้อหาสาระประเภทต่าง ๆ ในการทำงานที่มีการใช้สื่อสังคมออนไลน์ เพื่อการติดต่อสื่อสารกับผู้ร่วมงานมากขึ้น การติดตามความก้าวหน้าของงาน การรายงานปัญหาอุปสรรค การขอความคิดเห็น การสั่งและส่งงาน และในการรักษาความสัมพันธ์ส่วนบุคคลทั้งที่เป็นเพื่อนและครอบครัว (ไทยโพสต์, 2562) ผ่านการใช้เว็บไซต์ การรับส่งอีเมล์ การซื้อขายสินค้าไปจนถึงการทำธุรกรรมทางอิเล็กทรอนิกส์ เช่น ระบบ Internet Banking ระบบ GFMIS ของรัฐบาล และระบบการชำระภาษี เป็นต้น ซึ่งมีแนวโน้มเพิ่มมากขึ้นทุกวัน แนวโน้มในอนาคตของสังคมมนุษย์จึงย่อมหลีกเลี่ยงไม่ได้กับการใช้งานระบบเครือข่ายอินเทอร์เน็ตสากลที่เพิ่มมากขึ้น ตามการเปลี่ยนแปลงทั้งทางด้านวิทยาศาสตร์และเทคโนโลยี ตลอดจนการเชื่อมโยงกันระหว่างประเทศในยุคเศรษฐกิจดิจิทัล

การเปลี่ยนแปลงดังกล่าวได้ส่งผลให้ระบบเทคโนโลยีมีการพัฒนาอย่างรวดเร็ว ซึ่งอาชญากรรมไซเบอร์ (Cybercrime) ถือเป็นผลิตผลของเทคโนโลยีสารสนเทศที่สร้างพื้นที่ให้ผู้กระทำความผิดได้ใช้ในการก่ออาชญากรรมรูปแบบใหม่ที่เกี่ยวข้องกับการ ได้มา หรือการควบคุมบงการข้อมูล รวมถึงมูลค่าที่มีอยู่ในข้อมูลโดยกระทำผ่านระบบ เครือข่ายระดับโลก ทั้งนี้อาชญากรรมไซเบอร์ไม่ใช่ปรากฏการณ์ที่เพิ่งเกิดขึ้น แต่เป็นการวิวัฒนาการของพฤติกรรมที่ก่อให้เกิดความเสียหายที่เกี่ยวกับการใช้คอมพิวเตอร์ ซึ่งเกิดขึ้นมานานแล้ว และรูปแบบอย่างที่พบในปัจจุบันถือว่าเป็นอาชญากรรมไซเบอร์ในรุ่นที่สาม ซึ่งอาชญากรรมในรุ่นที่หนึ่ง เป็นการใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิดแบบดั้งเดิม และอาชญากรรมไซเบอร์รุ่นที่หนึ่ง หรืออาจเรียกว่า “อาชญากรรมคอมพิวเตอร์” เกิดขึ้นบนระบบคอมพิวเตอร์เดี่ยว ๆ ที่แยกต่างหากไม่ได้ เชื่อมต่อเป็นเครือข่ายคอมพิวเตอร์ ส่วนอาชญากรรมไซเบอร์รุ่นที่สองเป็นอาชญากรรม ที่เกิดขึ้นโดยอาศัยเครือข่ายคอมพิวเตอร์โดยเฉพาะอย่างยิ่งอินเตอร์เน็ต ทั้งนี้เนื่องจากอินเตอร์เน็ตได้เปิดพื้นที่ให้คอมพิวเตอร์มีการเชื่อมต่อกัน และมีการส่งข้อมูลระหว่างกันได้ไม่ว่าคอมพิวเตอร์นั้นจะอยู่ที่ใดของโลก ด้วยพื้นที่ไซเบอร์สเปซที่เกิดจากอินเตอร์เน็ตที่มีลักษณะไร้พรมแดนเป็นโลกาภิวัตน์ และข้ามเขตอำนาจศาลของแต่ละประเทศ ซึ่งเป็นการเปิดโอกาสให้การกระทำความผิดสามารถทำได้จากระยะไกลเป็นวงกว้าง และก่อให้เกิดปัญหาในการที่รัฐจะนำตัวผู้กระทำความผิดมาลงโทษได้ เพราะผู้ที่กระทำและการกระทำความผิดอยู่นอกพื้นที่ทางกายภาพของรัฐนั้น ๆ แต่ผลของการกระทำผิดเกิดขึ้นในอีกประเทศหนึ่ง ขณะที่อาชญากรรมไซเบอร์รุ่นที่สาม หรืออาชญากรรมไซเบอร์ในยุคปัจจุบันเป็นอาชญากรรมที่มีลักษณะกระจาย และมีความเป็นอัตโนมัติ นั่นคือการกระทำความผิดจะกระจาย

ไปในวงกว้าง และส่วนใหญ่เป็นการกระทำที่ถูกตั้งโปรแกรมไว้ให้ดำเนินการโดยอัตโนมัติ (นิติพัฒน์ วุฒิบุณยสิทธิ์, 2562)

อาชญากรรมไซเบอร์บางอย่างอาจก่อให้เกิดความเสียหายต่อชีวิต ทรัพย์สิน และ สังคมได้ แต่กฎหมายซึ่งมีบทลงโทษทางอาญาที่มีอยู่แต่เดิมนั้นครอบคลุมไปไม่ถึงการกระทำความผิดเกี่ยวกับคอมพิวเตอร์เหล่านั้น เช่น การเจาะข้อมูล การใช้โปรแกรม ประสงค์ที่มีลักษณะประสงค์ร้ายโจมตีทั้งหน่วยงานภาครัฐ ภาคเอกชน แม้กระทั่งส่วนบุคคล ซึ่งก่อให้เกิดความเสียหายต่อระบบคอมพิวเตอร์หรือข้อมูลที่เก็บอยู่ในนั้น ซึ่งในหลาย ๆ กรณีส่งผลกระทบร้ายแรงต่อทั้งตัวบุคคล สังคม หรือแม้กระทั่งความมั่นคงของชาติได้ อาทิ การเจาะระบบล้วง ทำลาย หรือเปลี่ยนแปลงข้อมูลสำคัญของหน่วยงานรัฐ การใช้โปรแกรมขัดขวางการทำงานของระบบเครือข่ายคอมพิวเตอร์ทำให้มีการแลกเปลี่ยนข้อมูลระหว่างกันช้าลง หรือบางครั้งอาจทำให้ระบบล่มได้

ปัจจุบันรัฐบาลและหน่วยงานทั้งภาครัฐและเอกชนในประเทศไทย ได้ให้ความสำคัญต่อความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสาร โดยการจัดตั้งองค์กรกรรมการและรูปแบบที่คล้ายกันระดับชาติที่มีหน้าที่รับผิดชอบโดยตรง ตลอดจนมีการประกาศใช้กฎหมายต่าง ๆ ที่เกี่ยวข้อง เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชบัญญัติสุขภาพแห่งชาติ พ.ศ. 2550 มาตรา 71 ซึ่งวางหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลที่เป็นข้อมูลประวัติสุขภาพ พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เป็นต้น ซึ่งสิ่งเหล่านี้เป็นส่วนหนึ่งของจุดเริ่มต้นที่จะนำไปสู่ความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศที่ดีขึ้นในประเทศไทย ซึ่งพิธุวรรณ กิติคุณ (2559) กล่าวว่า “*...ที่ผ่านมาภาครัฐไทยให้ความสำคัญกับการพัฒนาและการนำเทคโนโลยี สารสนเทศและการสื่อสารมาใช้เป็นเครื่องมือสนับสนุนการพัฒนาประเทศมาโดยตลอด และเมื่อโลกเริ่มก้าวเข้าสู่ยุคเทคโนโลยีดิจิทัล การเปลี่ยนแปลงกระบวนทัศน์ทางความคิดในทุกภาคส่วนจึงเกิดขึ้น โดยเฉพาะภาครัฐไทยได้เริ่มให้ความสำคัญกับการพัฒนาและการนำเทคโนโลยีดิจิทัลมาใช้เป็นเครื่องมือสำคัญในการขับเคลื่อนและพัฒนาประเทศ รวมถึงการปรับปรุงประสิทธิภาพการบริหารราชการแผ่นดิน หน่วยงานภาครัฐจึงจำเป็น ต้องร่วมมือกันพัฒนาและยกระดับภาครัฐในภาพรวมให้ก้าวสู่การเป็นรัฐบาลดิจิทัล เพื่อให้ประเทศไทยสามารถพัฒนาได้อย่างยั่งยืน และก้าวทันความเปลี่ยนแปลงในเวทีโลก...*”

นอกจากกฎหมายที่มีความสำคัญในฐานะเป็นเครื่องมือสนับสนุนในการป้องกันและรักษาความปลอดภัยอาชญากรรมไซเบอร์แล้ว หน่วยงานภาครัฐได้ตระหนักถึงความสำคัญในการมีทีมงานด้านความมั่นคงปลอดภัย เพื่อรับมือกับอาชญากรรมไซเบอร์ได้อย่างทันท่วงที รวมถึงการแลกเปลี่ยนข้อมูลกับทีมหรือหน่วยงานอื่น ๆ เพื่อควบคุม และระงับการแพร่ขยายของเหตุ

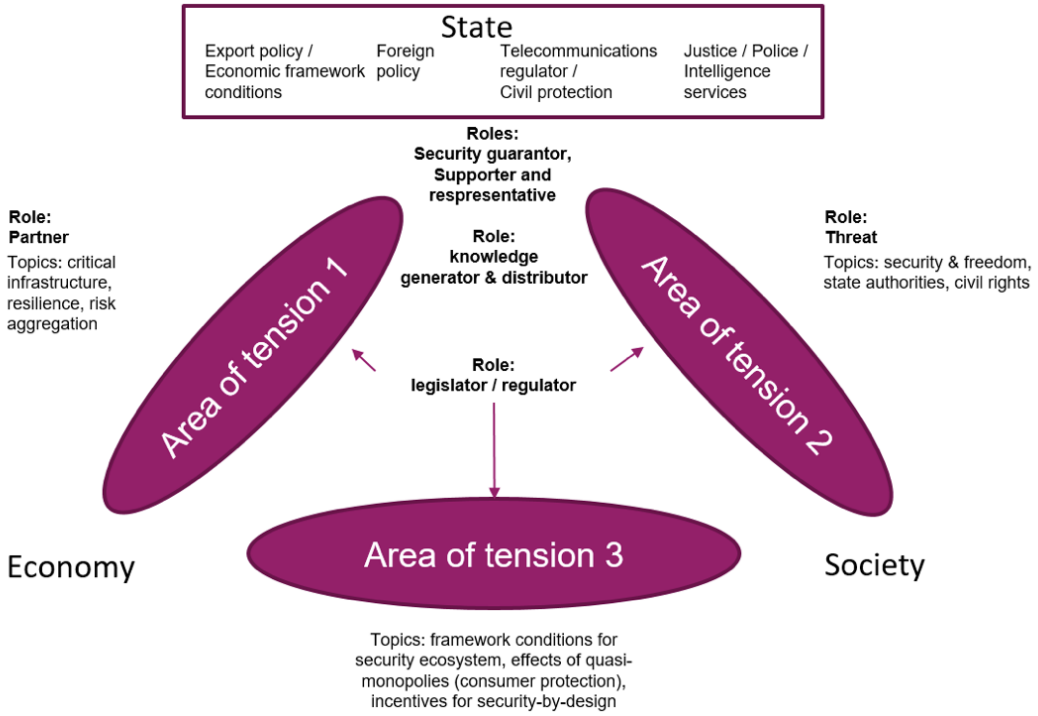
อาชญากรรมไซเบอร์ให้เร็วที่สุด จากปัญหาอาชญากรรมไซเบอร์ที่ทวีความรุนแรงมากขึ้นนี้เองทำให้กรมสอบสวนคดีพิเศษ จัดโครงการหรือกิจกรรมเพื่อส่งเสริมการป้องกันอาชญากรรมไซเบอร์เพื่อรับมือกับภัยคุกคามขนาดใหญ่ที่ส่งผลข้ามหน่วยงานหรือในระดับภาคธุรกิจ ซึ่งแต่ละหน่วยงานมีการประสานงาน แลกเปลี่ยนข้อมูล และช่วยเหลือกันเมื่อเกิดภัยอาชญากรรมไซเบอร์ รวมทั้งมีการทำบันทึกข้อตกลงความร่วมมือด้านการยกระดับความพร้อมรับมืออาชญากรรมไซเบอร์ ที่ส่งผลกระทบต่อภาคการเงิน การลงทุน การประกันภัย ภาคธุรกิจ การค้า อุตสาหกรรม และโครงสร้างพื้นฐานสำคัญของประเทศ

ดังนั้น ผู้วิจัยจึงมีความสนใจที่จะศึกษามาตรการป้องกันอาชญากรรมไซเบอร์ของกรมสอบสวนคดีพิเศษ โดยนำแนวคิดการเมืองกับความปลอดภัยทางไซเบอร์ของ Myriam and Florian (2019) เป็นแนวคิดหลักของการศึกษา โดยรัฐมีบทบาท 6 บทบาท ได้แก่ (1) ผู้ค้ำประกันความปลอดภัย (2) ผู้ออกกฎหมายและผู้บังคับใช้กฎหมาย (3) ตัวแทนของประชาชน (4) พันธมิตรด้านความปลอดภัย (5) ผู้สร้างและให้ความรู้แก่ประชาชน และ (6) ผู้คุกคามในการป้องกันอาชญากรรมไซเบอร์ จากการทบทวนวรรณกรรมมี 3 บทบาทที่มีความใกล้เคียงและสอดคล้องกับคำถามการวิจัยของผู้วิจัยเป็นอย่างมาก ผู้วิจัยจึงได้นำมาปรับและบูรณาการเป็นกรอบแนวคิดในการวิจัยครั้งนี้ โดยกรอบแนวคิดดังกล่าวได้แบ่งบทบาทที่สำคัญของรัฐออกเป็น 3 บทบาทหลัก ประกอบด้วย (1) บทบาทผู้รักษาความปลอดภัย ผู้สนับสนุน และตัวแทน (2) บทบาทผู้ให้ความรู้ และผู้เผยแพร่ความรู้ และ (3) บทบาทผู้บัญญัติกฎหมาย ผู้ควบคุมกฎหมาย เพื่อทำการศึกษาวิธีการป้องกันอาชญากรรมไซเบอร์เพื่อความมั่นคงทางเศรษฐกิจและสังคมตั้งแต่อดีตถึงปัจจุบัน ผ่านกฎหมายที่เกี่ยวข้องกับการป้องกันอาชญากรรมไซเบอร์เพื่อความมั่นคงทางเศรษฐกิจและสังคมโดยการจัดการความรู้จากเอกสาร งานวิจัยที่เกี่ยวข้องทั้งภายในประเทศและต่างประเทศ ทั้งนี้ เพื่อให้การป้องกันอาชญากรรมไซเบอร์ของประเทศ มีความพร้อม สามารถปกป้อง ป้องกัน และรับมือกับสถานการณ์ด้านอาชญากรรมไซเบอร์ในสถานการณ์ปกติ สถานการณ์ที่เป็นภัยต่อความมั่นคงอย่างร้ายแรง ตลอดจนเตรียมแผนปฏิบัติการและมาตรการตอบสนองด้านการป้องกันอาชญากรรมไซเบอร์ที่เป็นกลไกควบคุมการใช้อำนาจเป็นการเฉพาะตามระดับความรุนแรงของสถานการณ์ เพื่อให้สามารถแก้ไขสถานการณ์ที่เกิดขึ้นได้อย่างมีประสิทธิภาพและเป็นเอกภาพ รวมทั้งมีการป้องกันอาชญากรรมไซเบอร์อย่างต่อเนื่อง

วัตถุประสงค์ของการวิจัย (Research Objectives)

1. เพื่อศึกษาเพื่อศึกษามาตรการป้องกันอาชญากรรมไซเบอร์ของกรมสอบสวนคดีพิเศษ

กรอบแนวคิดการวิจัย (Conceptual Framwork)



ที่มา : The Politics of Cybersecurity: Balancing Different Roles of the State, by Mariam & Florian, 2019, St Antony's International Review, 15(1): **St Antony's International Review**, 15(1), pp. 50-52.

วิธีดำเนินการวิจัย (Research Method)

การวิจัยครั้งนี้ เป็นการวิจัยเชิงคุณภาพ (qualitative research) อันประกอบไปด้วยกระบวนการศึกษาและวิเคราะห์ข้อมูลจากเอกสารหรือการวิจัยเชิงเอกสาร (documentary research) และกระบวนการสัมภาษณ์เจาะลึก (in-depth interview) มาใช้ในการดำเนินกระบวนการวิจัย

การเก็บรวบรวมข้อมูลที่นำมาใช้ในการวิจัยครั้งนี้ได้กำหนดกระบวนการหรือแนวทางในการเก็บรวบรวมข้อมูลไว้ 2 รูปแบบ ดังนี้ (1) การเก็บรวบรวมข้อมูลโดยการศึกษาค้นคว้าข้อมูลจากเอกสารทางวิชาการ และข้อมูลจากเทคโนโลยีสารสนเทศ (2) การเก็บรวบรวมข้อมูลโดยการสัมภาษณ์แบบเจาะลึก

การวิเคราะห์ข้อมูล ผู้วิจัยได้นำข้อมูลที่ได้จากการสัมภาษณ์เจาะลึก (in-depth interview) มาใช้ในกระบวนการวิเคราะห์และประมวลผลข้อมูล โดยดำเนินการร่วมกับกระบวนการรวบรวมข้อมูลจากการศึกษาค้นคว้าข้อมูลจากเอกสาร โดยกระบวนการและวิธีการวิเคราะห์อันจะได้ดำเนินกระบวนการตามแนวทางของการวิจัยเชิงคุณภาพ ได้แก่ การวิเคราะห์ข้อมูลโดยพิจารณาประเด็นหลัก ที่พบในข้อมูลที่ได้รับจากการสัมภาษณ์ทั้งหมด จากนั้นจึงนำประเด็นหลักมาพิจารณาแบ่งแยกออกเป็นประเด็นย่อยและหัวข้อย่อย อันเป็นกระบวนการวิเคราะห์ โดยการเริ่มต้นจากการวิเคราะห์ภาพรวมไปสู่การวิเคราะห์ประเด็นย่อยของกระบวนการวิเคราะห์ตามแนวทางการวิจัยเชิงคุณภาพ ซึ่งทำให้การวิจัยในครั้งนี้มีความเที่ยงตรงและแม่นยำมากยิ่งขึ้น รวมทั้งผู้วิจัยจะดำเนินกระบวนการในการวิเคราะห์ข้อมูลที่ได้จากการสัมภาษณ์เจาะลึก (in-depth interview) จำนวน 1 ท่าน โดยการพรรณาข้อมูลตามปรากฏการณ์ร่วมด้วย เพื่อให้ได้มาซึ่งข้อค้นพบจากกระบวนการวิจัยเชิงคุณภาพ ได้แก่ พันตำรวจโท วิชัย สุวรรณประเสริฐ ผู้อำนวยการกองคดีเทคโนโลยีและสารสนเทศ สังกัดกองคดี-เทคโนโลยีและสารสนเทศ กรมสอบสวนคดีพิเศษ (D.S.I.) กระทรวงยุติธรรม ซึ่งผู้ให้ข้อมูลสำคัญรายดังกล่าว มีตำแหน่งเป็นผู้บริหารระดับสูงขององค์กร และเป็นหน่วยงานขนาดใหญ่ที่มีข้อมูลครบถ้วนและมีประสบการณ์ด้านการป้องกันอาชญากรรมไซเบอร์เพื่อความมั่นคงทางเศรษฐกิจและสังคม ซึ่งมีคุณสมบัติเหมาะสมกับวัตถุประสงค์และกรอบแนวคิดในการวิจัย สามารถให้ข้อมูลได้ครบถ้วน

ผลการวิจัย (Research Results)

การวิจัยเรื่อง มาตรการป้องกันอาชญากรรมไซเบอร์ของกรมสอบสวนคดีพิเศษ ผลการวิจัยพบว่า กรมสอบสวนคดีพิเศษมีมาตรการป้องกันอาชญากรรมไซเบอร์ที่สำคัญ 3 ด้านหลัก ได้แก่ (1) บทบาทในด้านการรักษาความปลอดภัย (2) บทบาทในด้านผู้สนับสนุน และ (3) บทบาทในด้านตัวแทน

บทบาทในด้านการรักษาความปลอดภัย พบว่า อาชญากรรมไซเบอร์ เช่น ปัญหาเด็ก ติดเกม นับวันจะยิ่งทวีความรุนแรงขึ้นเรื่อย ๆ ส่งผลกระทบทั้งทางด้านร่างกาย และจิตใจ ฟุ้มเฟือย เหม่อลอย การเรียน ตกต่ำ มีเพศสัมพันธ์ก่อนวัยอันควร หนักที่สุดก็แสดงความก้าวร้าวหรือมีพฤติกรรมเลียนแบบโดยใช้ความรุนแรง ที่สำคัญไม่เพียงแต่เกมเท่านั้นที่ส่งผลกระทบกับเด็กและเยาวชน แต่เว็บไซต์ที่เด็กและเยาวชนสามารถท่องไปในโลกที่พวกเขาอยากรู้อยากเห็นได้อย่างง่ายดาย โดยรู้เท่าไม่ถึงการณ์ยังเป็นอีกช่องทางหนึ่งที่เป็นปัจจัยเสริมให้เด็กเลียนแบบพฤติกรรมผิด ๆ จากปัญหาดังกล่าวทำให้กรมสอบสวนคดีพิเศษได้ตระหนักถึงการสร้างเกราะป้องกันจากเกมและเว็บไซต์ที่ไม่สร้างสรรค์เหล่านี้ โดยจัดทำ “โครงการอบรม เยาวชนในการสอดส่องและแจ้งเบาะแสการกระทำผิด

เกี่ยวกับคอมพิวเตอร์” หรือ “ DSI CYBER FORCE” ขึ้นมา ตั้งแต่ปี 2547 โดยมีเด็กและเยาวชนผ่านการอบรมในโครงการ กว่า 2,000 คน จาก 20 โรงเรียนทั่วประเทศ โครงการดังกล่าวเป็นโครงการที่เน้นให้ความรู้กับเยาวชนในเรื่องพิษภัยทางอินเทอร์เน็ต เพื่อไม่ให้เยาวชนตกเป็นเหยื่อ หรือเป็นผู้กระทำต่อเหยื่อเสียเอง โดยในการอบรมแต่ละครั้งจะมีทั้งนักเรียนและครูเข้าร่วมอบรม เพื่อเรียนรู้ถึงลักษณะของอาชญากรรมคอมพิวเตอร์ และตระหนักถึงพิษภัยบนอินเทอร์เน็ต รวมทั้งรู้วิธีการแก้ไขการป้องกันภัยทางอินเทอร์เน็ต การรักษาสภาพสถานที่ที่เกิดเหตุ แจ้งเบาะแสเว็บไซต์ที่ไม่เหมาะสมและอาชญากรรมอื่น ๆ ที่ใกล้ตัว ภัยด้านความมั่นคง ทั้งในการข่าวปกติ หรือที่ได้รับภารกิจเป็นพิเศษ โดยมีการรายงานข่าวหน้าเว็บไซต์ เพื่อความปลอดภัยของผู้แจ้ง รวมทั้งมีการกระจายความรู้ให้บุคคลรอบข้าง ซึ่งโครงการ “DSI CYBER FORCE” จะทำให้เยาวชนรู้เท่าทันภัยที่มาจากคอมพิวเตอร์ พร้อมให้คุณค่ากับเยาวชนว่าเขาเป็นผู้มีความสามารถทำความดีให้เพื่อนให้สังคมของเขาได้โดยการเป็นเครือข่ายยุติธรรมของกรมสอบสวนคดีพิเศษ ในการสอดส่องดูแล แจ้งเบาะแสการกระทำผิดทางคอมพิวเตอร์ และช่วยเหลือราชการประเทศชาติ

บทบาทในด้านผู้สนับสนุน พบว่า กรมสอบสวนคดีพิเศษ (DSI) โดยกองคดีเทคโนโลยีและสารสนเทศมีภารกิจเกี่ยวข้องโดยตรงเกี่ยวกับการป้องกัน และปราบปรามอาชญากรรมคอมพิวเตอร์และตระหนักต่อปัญหาเรื่องภัยคุกคามทางคอมพิวเตอร์ที่มีผลกระทบต่อความมั่นคงของประเทศประกอบกับการปฏิบัติงานด้านป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ให้เป็นไปอย่างมีประสิทธิภาพ และได้ร่วมกับหน่วยงานต่าง ๆ จัดสัมมนาเกี่ยวกับการระวังป้องกันภัยทางไซเบอร์ตามแนวทางร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และฉบับที่ 2 พ.ศ. 2560 เพื่อแลกเปลี่ยนความคิดเห็นในเรื่องแนวทางการปฏิบัติงานร่วมกันในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ที่มีผลกระทบต่อความมั่นคงของประเทศ เพื่อบูรณาการหน่วยงานที่เกี่ยวข้องในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ และเพิ่มขีดความสามารถในการปฏิบัติงานด้านการสืบสวนสอบสวนและป้องกันปราบปรามอาชญากรรม ตลอดจนร่วมกันกำหนดแนวทางการปฏิบัติงานด้านการป้องกัน และปราบปรามอาชญากรรมคอมพิวเตอร์ที่มีผลกระทบต่อความมั่นคงของประเทศ

บทบาทในด้านตัวแทน พบว่า กรมสอบสวนคดีพิเศษ ได้ร่วมมือกับสถาบันการศึกษาดำเนินโครงการเสริมสร้างภาพลักษณ์กรมสอบสวนคดีพิเศษในกิจกรรม DSI Campus tour season เพื่อให้ความรู้และถ่ายทอดประสบการณ์การดำเนินงานในคดีอาชญากรรมรูปแบบต่าง ๆ โดยเฉพาะอาชญากรรมในเทคโนโลยีสารสนเทศให้กับนักศึกษามหาวิทยาลัย โดยกิจกรรมภายในงานมีการ

บรรยายพิเศษเรื่องป้องกันอาชญากรรมไซเบอร์ การจัดนิทรรศการเรียนรู้กฎหมายเข้าใจคดีพิเศษ และการโชว์นวัตกรรมการยิงปืนจำลองสถานการณ์ และนวัตกรรมเทคโนโลยีสนับสนุนการสืบสวนคดีพิเศษ นอกจากนี้ กรมสอบสวนคดีพิเศษได้ประสานความร่วมมือระหว่างประเทศ เช่น โครงการเสริมสร้างเครือข่ายความมั่นคงไทย-ออสเตรเลีย ในการหารือเกี่ยวกับแนวทางการส่งเสริมความร่วมมือด้านไซเบอร์ระหว่างไทยกับออสเตรเลีย และแลกเปลี่ยนองค์ความรู้เกี่ยวกับแนวนโยบายและภาพรวมการดำเนินการเพื่อเสริมสร้างความมั่นคงทางไซเบอร์และรับทราบพัฒนาการในการเสริมสร้างความมั่นคงทางไซเบอร์ของไทยอันจะเป็นประโยชน์ต่อการสานต่อความร่วมมือระหว่างกันในอนาคต ทั้งนี้ กรมสอบสวนคดีพิเศษ มีภารกิจเกี่ยวข้องโดยตรงเกี่ยวกับป้องกัน ปราบปรามและควบคุมอาชญากรรมพิเศษ ได้แก่ อาชญากรรมทางเศรษฐกิจ อาชญากรรมทางคอมพิวเตอร์ อาชญากรรมที่มีอิทธิพลเข้ามาเกี่ยวข้อง อาชญากรรมข้ามชาติ องค์กรอาชญากรรมรวมทั้งอาชญากรรมอื่นที่สร้างความเสียหายและส่งผลกระทบอย่างร้ายแรงต่อระบบเศรษฐกิจสังคมและความมั่นคงของประเทศ การพัฒนาระบบรูปแบบวิธีการ และมาตรการในการป้องกันปราบปราม และควบคุมอาชญากรรมพิเศษ

อภิปรายผล (Research Discussion)

หน่วยงานรัฐที่รับผิดชอบจำเป็นต้องรักษาสมดุลระหว่างการรักษาความมั่นคงปลอดภัยทางไซเบอร์ การคุ้มครองความเป็นส่วนตัว และการอำนวยความสะดวกในการเข้าถึงระบบให้เหมาะสม เพราะเป็นกลไกสำคัญในการสร้างความไว้วางใจ และการส่งเสริมการใช้เทคโนโลยีดิจิทัลในการทำงานทุกภาคส่วน (สำนักงานรัฐบาลอิเล็กทรอนิกส์ (สรอ.), 2559) ซึ่งปัญหาภัยคุกคามทางไซเบอร์ (Cyber Security) ยังคงเติบโตอย่างต่อเนื่องตามเทคโนโลยีที่ทันสมัยมากขึ้น หน่วยงานภาครัฐจึงเป็นเป้าหมายสำคัญในการโจมตีทางไซเบอร์จากผู้ประสงค์ร้าย ทั้งจากการโจมตีเพื่ออาศัยความน่าเชื่อถือของหน่วยงานภาครัฐมาใช้หลอกลวงประชาชนอีกต่อหนึ่ง และการโจมตีเพื่อทำลายความน่าเชื่อถือของหน่วยงาน อันเกิดจากสาเหตุต่าง ๆ ไม่ว่าจะเป็นการมุ่งทำลายชื่อเสียง หรือแม้กระทั่งการโจมตีเพื่อทดสอบความสามารถของตนเองเพื่อแสดงให้กลุ่มแฮคเกอร์ด้วยกันเองได้รับรู้ ในอนาคตการโจมตีทางไซเบอร์จะมีการปรับเปลี่ยนวิธีการหรือมีความรุนแรงเพิ่มมากขึ้น จึงเป็นหน้าที่สำคัญของกรมสอบสวนคดีพิเศษในฐานะหน่วยงานของรัฐที่จะต้องดำเนินการเรื่องความมั่นคงปลอดภัยทางไซเบอร์อย่างเป็นรูปธรรม ซึ่งกรมสอบสวนคดีพิเศษได้เล็งเห็นพัฒนาการของเทคโนโลยีที่จะเปลี่ยนโลกในอนาคตหรือที่เรียกว่า Disruptive Technology (เทคโนโลยีสร้างความพลิกผัน) ที่มีอิทธิพลต่อการเปลี่ยนรูปแบบการดำเนินชีวิต การประกอบธุรกิจและทิศทางเศรษฐกิจ

ของโลก แต่สิ่งที่ตามมาคือภัยคุกคามทางไซเบอร์ใหม่ ๆ ที่ส่งผลกระทบต่อบุคคล องค์กร หรือความมั่นคงระดับชาติ ซึ่งอาชญากรเปลี่ยนรูปแบบการกระทำความผิดโดยใช้เทคโนโลยีเป็นเครื่องมือในการกระทำความผิดมากขึ้น ทำให้ยากต่อการติดตามค้นหาร่องรอยที่อาชญากรทิ้งไว้ กรมสอบสวนคดีพิเศษจึงมีบทบาทสำคัญในการรักษาความปลอดภัยทางไซเบอร์ ได้แก่ (1) การสร้างความตระหนักรู้ให้แก่ประชาชน โดยการจัดทำโครงการหรือกิจกรรมให้ความรู้การรู้เท่าทันภัยใกล้ตัวในชีวิตประจำ และ (2) การรักษาความมั่นคงของประเทศ ได้มีการร่วมมือและระดมความคิดเห็นเพื่อหาแนวทางการปฏิบัติงานร่วมกัน ในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ที่มีผลกระทบต่อความมั่นคงของประเทศ เพื่อบูรณาการหน่วยงานที่เกี่ยวข้องในการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ และเป็นการเพิ่มขีดความสามารถในการปฏิบัติงานด้านการสืบสวน สอบสวนและป้องกันปราบปรามอาชญากรรม โดยร่วมกันกำหนดแนวทางการปฏิบัติงานด้านการป้องกันและปราบปรามอาชญากรรมคอมพิวเตอร์ที่มีผลกระทบต่อความมั่นคงของประเทศ

ข้อเสนอแนะ (Research Suggestions)

ข้อเสนอแนะเชิงนโยบาย

ภาครัฐต้องดำเนินการปรับปรุงกฎหมายที่เกี่ยวข้องกับเศรษฐกิจและสังคมดิจิทัลให้มีความทันสมัย สอดคล้องต่อพลวัตของเทคโนโลยีดิจิทัลและบริบทของสังคม มีการออกพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งจะช่วยสร้างความพร้อมให้กับประเทศไทยในการรับมือความเสี่ยงและภัยคุกคามทางไซเบอร์ยุคใหม่ เช่น ไวรัส มัลแวร์ การโจมตีระบบจากอาชญากรรมที่อาจส่งผลกระทบต่อการให้บริการประชาชนหรือความสงบเรียบร้อยภายในประเทศ

ข้อเสนอแนะเชิงปฏิบัติ

1. ภาครัฐจะต้องสร้างความเข้าใจและความตระหนักในด้านความมั่นคงปลอดภัยของโลกไซเบอร์ ซึ่งจำเป็นจะต้องคำนึงถึงการคุ้มครองความเป็นส่วนตัวและความสะดวกสบายในการเข้าถึงระบบของแต่ละบุคคลด้วยเช่นกัน ทั้งนี้การมุ่งเน้นรักษาความมั่นคงของชาติอาจเป็นการรุกล้ำความเป็นส่วนตัวได้ ดังนั้น หน่วยงานรัฐที่รับผิดชอบจำเป็นต้องรักษาสมดุลระหว่างการรักษาความมั่นคงปลอดภัยทางไซเบอร์ การคุ้มครองความเป็นส่วนตัว และการอำนวยความสะดวกในการเข้าถึงระบบให้เหมาะสม เพราะเป็นกลไกสำคัญในการสร้างความไว้วางใจ และการส่งเสริมการใช้เทคโนโลยีดิจิทัลในการทำงานทุกภาคส่วน

2. ภาครัฐควรให้ประชาชนมีส่วนร่วมในการทำประชาพิจารณ์เพื่อรับฟังมุมมองที่เป็นประโยชน์และการได้รับการยอมรับจากภาคเอกชนและภาคประชาชน ทั้งนี้บุคลากรภาครัฐในทุก

ระดับจะต้องตระหนักถึงความสำคัญ การเฝ้าระวัง การปฏิบัติให้ถูกต้องตามมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงานเพื่อป้องกันตนเองและหน่วยงานให้ปลอดภัยจากการถูกโจมตี เพื่อรับมือกับภัยคุกคามใหม่ ๆ ที่เกิดขึ้นได้อย่างทันท่วงที

เอกสารอ้างอิง (References)

ไทยโพสต์. (2562). **สุขภาวะของคนไทยในโลกโซเชียล มนุษย์สองโลกแห่งศตวรรษที่ 21**. [Online]. Available : https://www.thaipost.net/main/detail/53548 Retrieved May, 18 2020.

พิธุวรรณ กิติคุณ. (2559). **ภาครัฐไทยกับการก้าวเข้าสู่รัฐบาลดิจิทัล**. กรุงเทพฯ: สำนักวิชาการ, สำนักงานเลขาธิการสภาผู้แทนราษฎร.

นิติพัฒน์ วุฒิบุณยสิทธิ์. (2563). **การสืบสวนสอบสวนคดีเทคโนโลยี**. [Online]. Available : https://training.cri.or.th/activity_train/downloads/2017_03_15_ict_law.pdf Retrieved May, 18 2020.

วรุฒิ บุญประยงค์. (2558). ความท้าทายในการใช้ข้อมูลขนาดใหญ่ทางด้านสุขภาพ. **วารสารการอาชีวะและเทคนิคศึกษา**, *5*(10) (กรกฎาคม-ธันวาคม): 68-75.

สำนักงานรัฐบาลอิเล็กทรอนิกส์ (สรอ.). (2559). **ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)**. [Online]. Available : https://www.dga.or.th/upload/download/file_769c60982e4c374dcd33b41c29227a31.pdf Retrieved November, 1 2020.

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.