แนวทางการศึกษาถึงผลกระทบที่มีนัยสำคัญของอาชญกรรมคอมพิวเตอร์ (Cybercrime) ที่ส่งผลต่อความมั่นคงปลอดภัยของประเทศ (National Security) ความปลอดภัยสาธารณะ (Public Safety) ความมั่นคงในทางเศรษฐกิจของประเทศ (National Economic Security) โครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ (Infrastructure Serving Public Interest)

The study's framework for the significant impacts of cybercrime towards national security, public safety, national economic security, and infrastructure serving public interest

ชินะวัฒน์ อำนวยพล[1], ผู้ช่วยศาสตราจารย์ (พิเศษ) พลตำรวจโท ดร. ณรงค์ กุลนิเททศ[2],
ดร. ณิช วงศ์ส่องจ้า[3]
[1]นักศึกษาปริญญาเอก สาขานิติวิทยาศาสตร์ บัณฑิตวิทยาลัย มหาวิทายลัยราชภัฏสวนสุนันทา
E-mail: casper@fastmail.com
[2]ประธานหลักสูตรวิทยาศาสตร์ดุษฎีบัณฑิต สาขานิติวิทยาศาสตร์ คณะวิทยาศาสตร์และเทคโนโลยี
มหาวิทยาลัยราชภัฏสวนสุนันทา
E-mail: Narong.kulnides@gmail.com
[3]อาจารย์ที่ปรึกษาวิจัยหัวหน้าสาขานิติวิทยาศาสตร์ คณะวิทยาศาสตร์และเทคโนโลยี
มหาวิทยาลัยราชภัฏสวนสุนันทา
E-mail: Nich.wongsongja@gmail.com

บทคัดย่อ

ผลกระทบของอาชญากรรมคอมพิวเตอร์ (Cybercrime) มีผลกระทบในหลากหลายมิติ งานวิจัยนี้ประกอบด้วยตัวแปรอิสระหนึ่งตัว คือ อาชญากรรมคอมพิวเตอร์ (CYBE) และตัวแปรตามสี่ตัวแปร ซึ่งประกอบไปด้วย ความมั่นคงปลอดภัยของประเทศ (NATS) ความปลอดภัยสาธารณะ (PUBS) ความมั่นคงในทางเศรษฐกิจของประเทศ (NAEC) และ โครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ (INPU) งานวิจัยนี้ต้องการศึกษาผลกระตอบที่มีนัยสำคัญของ CYBE ที่มีผลต่อ NATS, PUBS, NAEC, และ INPU งานวิจัยนี้ประกอบไปด้วยสมมุติฐาน 4 สมการ ดังนี้ (1) CYBE = f(NATS, PUBS, NAEC, INPU); (2) NATS = f(PUBS, NAEC, INPU); (3) PUBS = f(NATS, NAEC, INPU); and (4) NAEC = f(NATS, PUBS) เพื่อให้ได้ข้อมูลที่สมบูรณ์และนำไปใช้ในการวิเคราะห์เชิงลึกได้ งานวิจัยนี้ได้ใช้ structural equation modelling (SEM) เพื่อนำมาตรวจสอบสมมุติฐาน

คำสำคัญ: อาชญากรรมคอมพิวเตอร์, ความมั่นคงปลอดภัยของประเทศ, ความปลอดภัยสาธารณะ, ความมั่นคงในทางเศรษฐกิจของประเทศ และโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ

Abstract

The significant impacts of cybercrime are multidimensional. This research comprises of one independent variable which is the cybercrime (CYBE) and of four dependent variables, which are national security (NATS), public safety (PUBS), national economic security (NAEC), and infrastructure serving public interest (INPU). This research attempts to

find the possible significant impact(s) of the CYBE towards NATS, PUBS, NAEC, and INPU. The research establishes four hypotheses which are (1) CYBE = f(NATS, PUBS, NAEC, INPU); (2) NATS = f(PUBS, NAEC, INPU); (3) PUBS = f(NATS, NAEC, INPU); and (4) NAEC = f(NATS, PUBS). To attain the most potential information and analysis, this research includes both qualitative and quantitative procedures. The research employs the structural equation modelling (SEM) to test the hypotheses and find the significant relations among the variables.

Keywords: cybercrime, national security, public safety, national economic security, infrastructure serving public interest

บทนำ

อาชญากรรมคอมพิวเตอร์ถือได้ว่าเป็นอาชญากรรมที่ได้รับความสนใจอย่างกว้างขวาง ไม่ว่าจะเป็นบุคคลทั่วไป นักกฎหมาย พนักงานของภาครัฐ องค์กรของรัฐและเอกชน เพราะอาชญากรรมคอมพิวเตอร์ ณ ปัจจุบันนี้เรียกได้ว่ามีผลกระทบกับชีวิตความเป็นอยู่และความปลอดภัยของทุกๆหน่วยในสังคมตั้งแต่ระดับประชาชนไปจนถึงระดับนาๆชาติ (Saini, Rao, and Panda, 2012) อีกทั้งความมั่นคงและเสถียรภาพของประเทศก็อาจถูกทำให้สั่นคลอนได้หากไม่สามารถรับมือกัอาชญากรรมคอมพิวเตอร์ได้อย่างจริงจัง (Broadhurst, 2006; Choo, 2011) Goodman (2016) มองว่าสาเหตุหนึ่งที่ทำให้อาชญากรรมคอมพิวเตอร์มีอิทธิพลต่อความปลอดภัยของประชาชนมากขึ้น ก็เพราะการที่มนุษย์ยอมรับให้เทคโนโลสารสนเทศ (Information Technology ย่อว่า IT) เข้ามาเป็นส่วนหนึ่งในการดำรงชีวิตมากขึ้น มีการใช้ระบบคอมพิวเตอร์เข้ามาควมคุมระบบต่างๆ เช่น การเงิน สาธารณูปโภค การทหาร การแพทย์ การศึกษา ฯลฯ เพื่อให้เขาใจง่ายในประเด็นที่ Goodman (2016) พยายามจะชี้ให้เห็น ก็สามารถนำไปเปรียบเทียบกับคำพูดในพุทธภาษิตที่ว่า "หากไม่มีภพก็ไม่มีชาติ" นักวิชาการหลายคนให้ความสำคัญกับอาชญากรรมประเภทนี้เพราะเป็นอาชญากรรมแห่งอนาคต (Future Crime) ซึ่งไม่สามารถหลีกเลี่ยงได้ (Broadhurst, 2006; Taylor, Fritsch, Liderbach, 2014) เพราะแนวโน้มของสังคมมนุษย์เดินไปในทิศทางของการพึ่งพิง IT มากกว่าเดินออกห่างจาก IT (Choo, 2011; Goodman 2016)

ข้อสังเกตที่เห็นได้ชัดคือ การเพิ่มขึ้นของอาชญกรรมคอมพิวเตอร์ในแต่ละปี (Crawford & Evan, 2017; Goodman 2016) ในประเทศไทย จากข้อมูลสำนักงานพัฒนาธุรกิจทางอิเล็กทรอนิกส์ (องค์กรมหาชน) (สพธอ.) ได้ทำการเก็บข้อมูลพบว่า ในปี 2554 ถึง 2559 ผู้ใช้ IT มีมากขึ้นจาก 16.6 ล้านคน เป็น 29.8 ล้านคน และผู้ร้องเรียนที่ได้รับภัยคุมคามทางคอมพิวเตอร์เพิ่มจาก 846 รายในปี พ.ศ. 2554 เป็น 3,797 ในปี พ.ศ. 2559 ซึ่งให้ข้อสังเกตุว่าจำนวนผู้ใช้ IT มากขึ้นและจำนวนอาชญากรรมคอมพิวเตอร์ก็มากขึ้นเช่นกัน นอกจากจะสร้างความเสียหายในระดับบุคคลแล้ว รัฐก็ได้รับผลกระทบต่ออาชญากรรมคอมพิวเตอร์ที่เกิดขึ้นเช่นกัน โดยจากรายงาน Cyber Attack Trends: Mid-Year Report ของบริษัท Check Point พบว่า ในครึ่งแรกของปี 2560 การก่ออาชญากรรมทางไซเบอร์เพิ่มขึ้นอย่างมากเมื่อเปรียบเทียบกับปีก่อนหน้า โดยเฉพาะอย่างยิ่งเมื่อเครื่องมือเจาะระบบที่รัฐบาลเป็นผู้พัฒนาได้หลุดรั่วออกมาสู่กลุ่มผู้ก่ออาชญากรรมก็ทำให้เกิดความเสียหายในวงกว้าง (ตัวอย่างเช่น เหตุการณ์มัลแวร์เรียกค่าไถ่ WannaCry) มัลแวร์เรียกค่าไถ่, botnet, และมัลแวร์ที่มีจุดประสงค์เพื่อขโมยบัญชีธนาคารออนไลน์ เริ่มมุ่งเป้าโจมตีผู้ใช้งานโทรศัพท์มือถือ ในขณะที่ช่องทางการแพร่กระจายมัลแวร์โดยอาศัย Macro ของ Microsoft Office ยังคงใช้ได้ผลอยู่

จากรายงาน 2017 Cloud Security Report ของบริษัท Alert Logic ที่สำรวจข้อมูลตั้งแต่เดือนสิงหาคม 2558 ถึงมกราคม 2560 พบว่า สัดส่วนการโจมตี web application ของหน่วยงานมีมากกว่าการพยายามแพร่กระจายมัลแวร์เรียกค่าไถ่ โดยประเภทช่องโหว่ web application ที่พบมากที่สุดคือ SQL Injection (55%) รองลงมาคือ Remote Code Execution (22%) ส่วนซอฟต์แวร์ CMS ที่ตกเป็นเป้าการโจมตีมากที่สุดคือ Joomla! ในขณะที่ซอฟต์แวร์ e-Commerce ที่ตกเป็นเป้าการโจมตีมากที่สุดคือ Magento

จากรายงาน 2017 Threat Monitoring, Detection & Response Report ของบริษัท Dtex Systems ที่เป็นการสำรวจผู้ปฏิบัติงานด้านไอที 400 คน พบว่า ภัยคุกคามทางไซเบอร์ที่น่ากังวลและตรวจจับได้ยากที่สุดคือการโจมตีจากคนในองค์กร (insider threats) สาเหตุหนึ่งที่ทำให้การป้องกันทำได้ยากเกิดจากนโยบายการอนุญาตให้พนักงานนำอุปกรณ์ส่วนตัวเข้ามาเชื่อมต่อและใช้เครือข่ายของที่ทำงานได้ (BYOD)

เนื่องจากในประเทศไทย แม้นักวิชาการต่างๆจะกล่าวถึงความรุนแรงและความเสียหายที่เกิดจากอาชญากรรมคอมพิวเตอร์ แต่ก็เป็นเพียงความคิดเห็นส่วนบุคคล ยังไม่ปรากฏในรูปแบบของงานวิจัยที่สามารถนำมาใช้ได้จริงและเป็นรูปธรรม จากปัญหาและความสำคัญที่กล่าวมาข้าต้น ผู้วิจัยจึงสนใจที่จะศึกษาการศึกษาถึง อาชญากรรมคอมพิวเตอร์ (Cybercrime) ที่ส่งผลต่อ ความมั่นคงปลอดภัยของประเทศ (National Security), ความปลอดภัยสาธารณะ (Public Safety), ความมั่งคงในทางเศรษฐกิจของประเทศ (National Economic Security), โครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ (Infrastructure Serving Public Interest) เพื่อเป็นแนวทางในการแก้ไขปัญหาทางด้านอาชญากรรมคอมพิวเตอร์ในเชิงนโยบาย และเป็นความรู้พื้นฐานที่จะใช้ในงานวิจัยอื่นๆต่อไป

คำถามวิจัย

ระดับของผลกระทบที่เกิดขึ้นจาก การกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ (รวมเรียกว่าอาชญากรรมคอมพิวเตอร์และใช้ภาษาอักฤษว่า Cybercrime) ที่มีต่อ ความมั่นคงของประเทศ (National Security) ความปลอดภัยสาธารณะ (Public Safety) ความมั่นคงในทางเศรษฐกิจของประเทศ (National Economic Security) โครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ (Infrastructure Serving Public Interest)

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาระดับของปัจจัยและอิทธิผลของ อาชญากรรมคอมพิวเตอร์ (Cybercrime) ที่ผลต่อความมั่นคงของประเทศ (National Security) ความปลอดภัยสาธารณะ (Public Safety) ความมั่นคงในทางเศรษฐกิจของประเทศ (National Economic Security) และ โครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ (Infrastructure Public Interest)

2. เพื่อต้องการวิเคราะห์ปัจจัยความสัมพันธ์ของตัวแปร ความมั่นคงของประเทศ (National Security) ความปลอดภัยสาธารณะ (Public Safety) ความมั่นคงในทางเศรษฐกิจของประเทศ (National Economic Security) และ โครงสร้างอันพื้นฐานอันเป็นประโยชน์สาธารณะ (Infrastructure Public Interest)

สมมติฐานของการวิจัย

จากกรอบแนวความคิดที่ได้จากการทบทวนวรรณกรรมและทฤษฎีที่เกี่ยวข้องต่างๆ และเพื่อสามารถหาผลลัพธ์ที่ได้ให้เห็นเป็นรูปธรรมงานวิจัยนี้จึงได้เลือกใช้ แบบจำลองสมการโครงสร้าง (Structural Equation

Modelling, SEM) มาใช้ในการวิเคราะห์ เพราะวิธีนี้เป็นการวิเคราะห์แบบบูรณาการ ซึ่งสามารถทำการประมาณค่าพารามิเตอร์ในการวิเคราะห์ความถดถอย (Regression Analysis) ที่อยู่ภายใน SEM ที่สร้างขึ้นมา

ในงานวิจัยนี้ รูปแบบของสมการโครงสร้าง และสมการมาตรวัด เพื่อใช้ในการวิเคราะห์ข้อมูล มีรายละเอียด ดังนี้

สมมติฐานข้อที่ 1

อาชญากรรมคอมพิวเตอร์ (Cybercrime: CYBE) มีผลต่อ ความมั่นคงของประเทศ (National Security: NATS) ความปลอดภัยสาธารณะ (Public Safety: PUBS) ความมั่นคงในทางเศรษฐกิจของประเทศ (National Economic Security: NAEC) และ โครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ (Infrastructure Public Interest: INPU)

CYBE = □ (NATS, PUBS, NAEC, INPU) ..... (1)

สมมติฐานข้อที่ 2

ความมั่นคงของประเทศ (National Security: NATS) มีผลต่อ ความปลอดภัยสาธารณะ (Public Safety: PUBS) ความมั่นคงในทางเศรษฐกิจของประเทศ (National Economic Security: NAEC) และโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ (Infrastructure Public Interest: INPU)

NATS = □ (PUBS, NAEC, INPU) ..... (2)

สมมติฐานข้อที่ 3

ความปลอดภัยสาธารณะ (Public Safety: PUBS) มีผลต่อ ความมั่นคงของประเทศ (National Security: NATS) ความมั่นคงในทางเศรษฐกิจของประเทศ (National Economic Security: NAEC) และโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ (Infrastructure Public Interest: INPU)

PUBS = □ (NATS, NAEC, INPU) ..... (3)

สมมติฐานข้อที่ 4

ความมั่นคงในทางเศรษฐกิจของประเทศ (National Economic Security: NAEC) มีผลต่อ ความมั่นคงของประเทศ (National Security: NATS) ความปลอดภัยสาธารณะ (Public Safety: PUBS) และโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ (Infrastructure Public Interest: INPU)

NAEC = □ (NATS, PUBS) ..... (4)

ขอบเขตของการวิจัย

งานวิจัยนี้มีขอบเขตของงานวิจัย ดังนี้

1. ขอบเขตด้านประชากร

1.1 วิธีการวิจัยเชิงคุณภาพ (Qualitative Research)

เนื่องจากงานวิจัยนี้เกี่ยวข้องกับ อาชญากรรมคอมพิวเตอร์ (Cybercrime) ความมั่นคงของประเทศ (National Security) ความปลอดภัยสาธารณะ (Public Safety) ความมั่นคงในทางเศรษฐกิจของประเทศ (National Economic Security) โครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ (Infrastructure Serving Public Interest) ดังนั้น ผู้เชี่ยวชาญที่เกี่ยวข้องและมีความเข้าใจควรจะเป็นผู้เชี่ยวชาญที่มีความเป็นพหุศาสตร์ (Multidisciplinary) ดังนั้น การสุ่มตัวอย่างจึงเป็นแบบเจาะจง (Purposive Sampling) โดยเลือกจากผู้ที่มีความรู้ ความเข้าใจ และประสบการณ์ที่เกี่ยวข้องกับการบริหารจัดการประเทศทั้งด้านเศรษฐกิจ สังคม และความมั่นคงของชาติ บวกกับมีความเข้าใจในอาชญากรรมคอมพิวเตอร์ (Cybercrime) ในระดับหนึ่ง โดยกลุ่มตัวอย่างที่กล่าวมาสามารถแบ่งได้เป็น 5 ประเภท ดังนี้

1) ข้าราชการทหาร ประกอบด้วย
   1.1) ข้าราชการทหารที่เกี่ยวกับการออกนโยบาย
   1.2) ข้าราชการทหารฝ่ายตุลาการ หรือทหารรัฐธรรมนูญ
   1.3) ข้าราชการทหารฝ่าย IT
2) เจ้าหน้าที่จากกระทรวงเทคโนโลยีสารสนเทศ และการสื่อสาร
3) นักวิชาการทางด้านเทคโนโลยีสารสนเทศจากมหาวิทยาลัย
4) ข้าราชการตำรวจ ประกอบด้วย
   4.1) เจ้าหน้าที่ตำรวจฝ่ายสืบสวน และสอบสวนจากหน่วยงานในพื้นที่
   4.2) เจ้าหน้าที่ตำรวจพิสูจน์หลักฐานเกี่ยวกับอาชญากรรมไซเบอร์
   4.3) เจ้าหน้าที่ตำรวจ กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญกรรมทางเทคโนโลยี
   4.4) เจ้าหน้าที่ตำรวจจากกระทรวงเทคโนโลยีสารสนเทศ และการสื่อสาร
5) นักวิชาการด้านการเมืองและความมั่นคง

1.2 วิธีการวิจัยเชิงปริมาณ (Qualitative Research)

เลือกทำการศึกษาและเก็บรวมรวมข้อมูลเฉพาะพนักงานที่ยินยอมให้ความร่วมมือและอยู่ในเขตพื้นที่กองบังคับการตำรวจนครบาล 1-9 และหน่วยทหารที่เกี่ยวข้อง

2. ขอบเขตของตัวแปรที่ใช้ในการวิจัย

งานวิจัยนี้ได้กำหนดขอบเขตในการศึกษาตัวแปรแต่ละตัวตามการนิยามศัพท์เฉพาะ ดังต่อไปนี้

2.1 ตัวแปรอิสระ ได้แก่

1) อาชญากรรมคอมพิวเตอร์ (Cybercrime: CYBE)

2.2 ตัวแปรตาม ได้แก่

1) ความมั่นคงของประเทศ (National Security: NATS)
2) ความปลอดภัยสาธารณะ (Public Safety: PUBS)
3) ความมั่นคงในทางเศรษฐกิจของประเทศ (National Economic Security: NAEC)
4) โครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ (Infrastructure Serving Public Interest: INPU)

ข้อตกลงเบื้องต้น

เนื่องจากอาชญากรรมคอมพิวเตอร์ (Cybercrime) เป็นอาชญากรรมที่เกิดขึ้นใหม่ งานวิจัยนี้มุ่งเน้นไปที่ความเข้าใจในความเป็นไปและสถานการณ์ของอาชญากรรมคอมพิวเตอร์ที่เกินขึ้นในปัจจุบันและแนวโน้มของอาชญากรรมประเภทนี้ในอนาคตที่พอคาดเดาได้เท่านั้น เพื่อเป็นประโยชน์ในการนำงานวิจัยไปใช้ได้จริงในยุคปัจจุบัน งานวิจัยนี้ไม่ได้อยู่ในกรอบของแนวการศึกษาอาชญากรรมคอมพิวเตอร์ในมุมมองของอาชญวิทยา หรือสังคมศาสตร์เป็นที่ตั้ง แต่อาจนำหลักและทฤษฎีของอาชญวิทยาและสังคมศาสตร์มาอธิบายอาชญากรรมคอมพิวเตอร์เพื่อความเข้าใจพื้นฐานเท่านั้น

ข้อจำกัดของการวิจัย

ผลลัพท์ของงานวิจัยนี้หากทำให้สมบูรณ์ที่สุด จำเป็นต้องได้รับความร่วมมือจากองค์กรหลายฝ่าย และคำตอบที่ได้ส่วนมากก็เป็นคำตอบในที่อยู่ในมิติของ ความคิดเห็นของผู้เชี่ยวชาญเป็นส่วนมาก ดังนั้นความเข้าใจในอาชญากรรมคอมพิวเตอร์ในงานวิจัยนี้ สามารถอธิบายความเป็นไปได้ในยุคสมัยปัจจุบันเท่านั้น

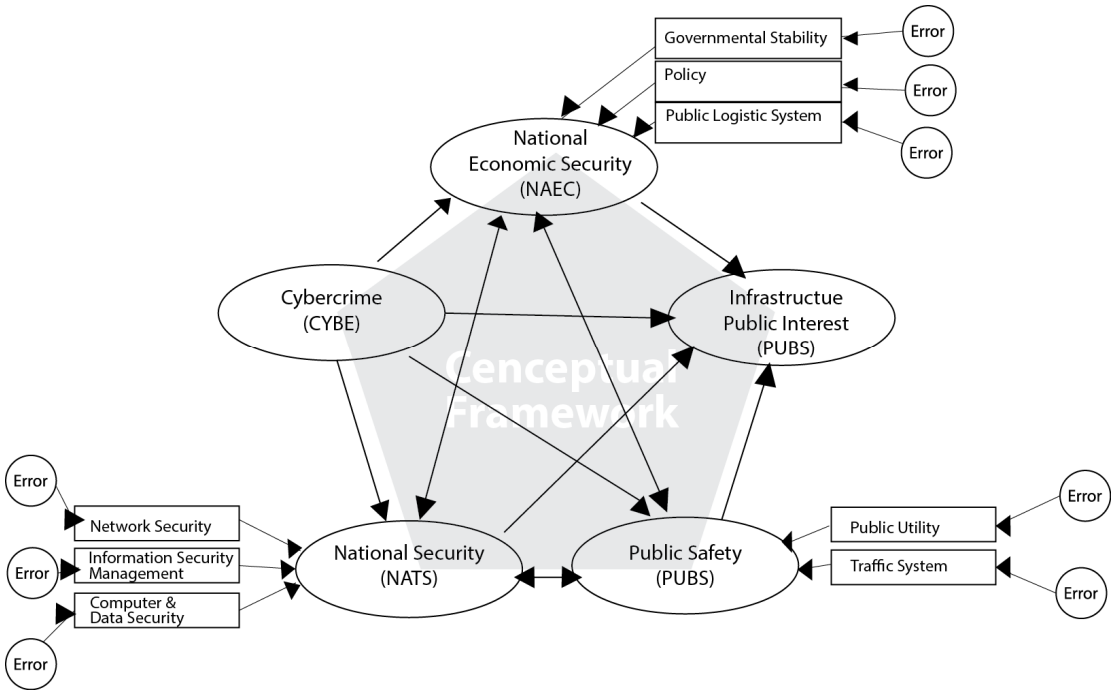
เพราะในอนาคตเมื่อความสลับซับซ้อนของระบบ IT ที่มีผลต่อมนุษย์มีมากขึ้น ผลงานวิจัยที่ได้มาก็เป็นอันต้องตกยุคไป

เนื่องจากเป็นความคิดเห็นเป็นที่ตั้ง ดังนั้นความคิดเห็นของผู้เชี่ยวชาญอาจย้อนแย้งกันเอง หรือว่าให้ความคิดเห็นที่มาจากมุมมองและมิติที่ต่างกัน ทำให้การวิเคราะห์ผลดังกล่าวมีความผิดผลาดอยู่

ประโยชน์ที่คิดว่าจะได้รับจากการวิจัย

1. ทราบถึงสถาณการณ์และสภาพปัญหาปัจจุบันของอาชญากรรมคอมพิวเตอร์
2. เข้าใจผลกระทบของผลกระทบที่ อาชญากรรมคอมพิวเตอร์ (Cybercrime) มีต่อความมั่นคงของประเทศ (National Security) ความปลอดภัยสาธารณะ (Public Safety) ความมั่นคงในทางเศรษฐกิจของประเทศ (National Economic Security) โครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ (Infrastructure Serving Public Interest)
3. เป็นแนวทางในการประเมินและเป็นบรรทัดฐานในการสร้างนโยบายควมคุมอาชญากรรคอมพิวเตอร์

กรอบแนวคิด



รายการอ้างอิง

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. **American Journal of Police merged into Police Strategies & Management**, 29(3), 408-433.

Choo, K. K. R. (2011). The cyber threat landscape: challenges and future research directions. **Computer & Security**, 30, 719-731.

Crawford, A. & Evans, K. (2017). Crime Prevention and Community Safety. In: Leibling, A., Maruna, S., and McAra, L. (eds). **The Oxford handbook of criminology** (sixth edition). Oxford: Oxford University Press.

Goodman, M. (2016). **Future crimes: inside the digital underground and the battle for our connected world**. New York: Penguin Random House LLC.

Nissenbaum, H. (2005). Where computer security meets national security. **Ethics and Information Technology**, 7(2), 61-73.

Reith, M., Carr, C., and Gunsch, G. (2002). **An examination of digital forensic models. International Journal of Digital Evidence**, 1(3), 74-85.

Saini, H., Rao, Y. S., and Panda, T. C. (2012). Cyber-crimes and their impacts: a review. **International Journal of Engineering Research and Applications**, 2(2), 202-209.

Stevens, T. (2012). A cyberwar of ideas? deterrence and norms in cyberspace. **Contemporary Security Policy**, 33(1), 148-170.

Tabansky, L. (2012). Cybercrime: a national security issue? **Military and Strategic Affairs**, 4(3), 117-136.

Taylor, R. W., Fritsch, E. J., and Liderbach, J. (2014). **Digital Crime and Digital Terrorism** (3 rd ed.). NJ, USA: Prentice Hall Pass Upper Saddle River.