ยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย
Strategies to Counter Cyber Terrorism in Thailand

หยาดพิรุณ นาชัยสินธุ์*
คณะรัฐศาสตร์และนิติศาสตร์ มหาวิทยาลัยบูรพา

Yardpirun Nachaisin*
Faculty of Political Science and Law, Burapha University

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อ 1) ศึกษาความก้าวหน้าทางไซเบอร์ที่มีการนำมาใช้เป็นเครื่องมือทางยุทธศาสตร์การก่อการร้ายในประเทศไทย 2) พัฒนายุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย การวิจัยครั้งนี้เป็นการวิจัยโดยใช้วิธีการศึกษาเชิงคุณภาพจากเทคนิคเดลฟายและการสัมภาษณ์เจาะลึก ประกอบด้วยผู้เชี่ยวชาญ 2 กลุ่ม คือ ผู้ที่มีบทบาทเกี่ยวข้องกับการดำเนินการหรือพัฒนาทางไซเบอร์ และผู้เชี่ยวชาญการกำหนดยุทธศาสตร์ทางเทคโนโลยีสารสนเทศ ทำการวิเคราะห์เนื้อหาและประเมินลักษณะการก่อการร้ายทางไซเบอร์ในประเทศไทย ผลการศึกษาพบว่า ความก้าวหน้าทางไซเบอร์คือ การพัฒนาทางเทคโนโลยีที่สามารถเชื่อมต่อกันได้อย่างรวดเร็วสะดวกขึ้น การก่อการร้ายทางไซเบอร์เป็นการใช้เครื่องมือทางเทคโนโลยี เช่น โทรศัพท์มือถือ คอมพิวเตอร์ แท็บเล็ตหรือเครื่องมือประเภทอื่นๆ ที่เชื่อมต่อทางอินเทอร์เน็ตเพื่อการก่อการร้าย และอินเทอร์เน็ตเป็นช่องทางที่สำคัญที่ใช้ในการก่อการร้าย ยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย คือ READ: CLIP ประกอบด้วย 1. Research ยุทธศาสตร์การเสริมสร้างการวิจัยเพื่อการพัฒนาทางไซเบอร์ 2. Education ยุทธศาสตร์การจัดการศึกษาในการสร้างพื้นฐานของประชาชนในประเทศไทย 3. Awareness ยุทธศาสตร์การสร้างการตระหนักรู้ทางไซเบอร์ให้กับประชาชน 4. Development ยุทธศาสตร์การพัฒนาความก้าวหน้าทางไซเบอร์ 5. Coordinate ยุทธศาสตร์การส่งเสริมความร่วมมือระหว่างภาครัฐ ภาคเอกชน และภาคประชาชน 6. Law ยุทธศาสตร์การกำหนดใช้กฎหมายทางไซเบอร์และการบังคับใช้กับประชาชน 7. Integration ยุทธศาสตร์การใช้บูรณาการร่วมกันเพื่อแบ่งปันข้อมูล 8. Perception Prepares and Protect ยุทธศาสตร์การรับรู้ทางไซเบอร์ร่วมกัน ตระเตรียมและปกป้องทางไซเบอร์

คำสำคัญ: ยุทธศาสตร์ การก่อการร้าย ต่อต้านการก่อการร้าย ไซเบอร์

* ผู้ประสานงานหลัก (Corresponding Author)
e-mail: Yard_pirun@hotmail.com

Abstract

This research aims to 1) Study the cyber development that is applied as a strategic tool of cyber terrorism in Thailand. 2) Examine terrorism characteristics that use the cyber environment as a strategic tool of cyber terrorism in Thailand. This research mainly applied qualitative analysis and in-depth interviews. The research targets were 2 groups of expert, which were persons who have had roles in usage or cyber development and experts who have specified the information technology strategies. The information was analyzed and the cyber terrorism characteristics in Thailand were assessed. The results observed are as follows. The cyber development is the technological development that can be connected faster and more conveniently than before. Cyber terrorism is the implementation of technological tools, such as mobile phones, computers or other tools that can be connected through the internet for terrorism purposes. In addition, the internet is an important channel for terrorism. The strategies to counter cyber terrorism in Thailand are summarized by the acronym READ: CLIP, which comprises 8 strategies as follows. 1. Research is the strategy that promotes the cyber development research. 2. Education is the strategy to arrange basic education for people in Thailand. 3. Awareness is the strategy that creates cyber awareness of people. 4. Development is the strategy that improves the cyber development. 5. Coordination is the strategy that promotes the cooperation of government, private and public sectors. 6. Law is the strategy that specifies cyber law and enforcement. 7. Integration is the strategy of integration to share data. 8. Perception Preparation and Protection is the strategy to perceive, prepare and protect the cyber environment together.

Keywords: Strategy, Terrorism, Counter Terrorism, Cyber

บทนำ

การก้าวเข้าสู่ยุคความเป็นโลกาภิวัตน์ศตวรรษที่ 21 การพัฒนาทางไซเบอร์มีบทบาทสำคัญต่อการดำรงชีวิตของประชาชนเป็นอย่างมาก อินเทอร์เน็ตกลายเป็นปัจจัยสำคัญในการดำรงชีวิตและการเชื่อมโยงข้อมูลข่าวสารของคนทั้งประเทศ การพัฒนาของระบบอินเทอร์เน็ตส่งผลให้เกิดการเปลี่ยนแปลงทางสังคม เศรษฐกิจ และการเมือง ซึ่งกล่าวได้ว่าสิ่งสำคัญที่สุดในศตวรรษนี้ คือ โลกของสารสนเทศกลายเป็นปรากฏการณ์ใหม่ในมิติของการสร้างระบบเครือข่ายทางสังคมหรือที่เรียกว่า สังคมออนไลน์ ซึ่งเป็นการติดต่อสื่อสารโดยการใช้ไซเบอร์ส่งผลให้ประเทศไทยมีความนิยมของการใช้เฟซบุ๊กได้รับความนิยมสูงสุด (Facebook statistics Thailand as ASEAN's top three, 2015) จากสถิติล่าสุดวันที่ 17 เมษายน 2015 ผลสำรวจพบว่า ประเทศไทยมีประชากรที่เล่นเฟซบุ๊กมากเป็นอันดับ 3 ของอาเซียนอยู่ที่ 35 ล้านบัญชี การใช้เฟซบุ๊กในประเทศไทยเติบโตขึ้น 34.62 เปอร์เซ็นต์ ทั้งนี้ประเทศไทยมียอดเติบโตของผู้ใช้เฟซบุ๊กมากเป็นอันดับที่ 5 ของอาเซียน

กระแสความตื่นตัวทางเทคโนโลยีสารสนเทศและความนิยมในการใช้ไซเบอร์อย่างมากมายส่งผลให้เกิดการเปลี่ยนแปลงทางสังคม เศรษฐกิจ และการเมืองอย่างรวดเร็ว ถึงแม้ว่าไซเบอร์จะทำให้เกิดประโยชน์อย่างมหาศาลแต่หากมนุษย์ใช้ไซเบอร์ในทางที่ไม่ถูกต้องนำไปเป็นเครื่องมือเพื่อวัตถุประสงค์บางประเภท เช่น การนำไปปลุกระดมมวลชน การชักจูงหรือเผยแพร่ข่าวสาร การแฮกข้อมูล การปล่อยไวรัส จะนำไปสู่ก่อการร้ายได้ ส่งผลให้เกิดความเสียหายอย่างมากแก่มนุษย์ อีกทั้งการใช้ไซเบอร์เพื่อเป็นเครื่องมือที่สำคัญต่อการก่อการร้ายและสร้างความเสียหายและสูญเสียเป็นจำนวนมาก หลังจากเหตุการณ์ก่อการร้ายในประเทศสหรัฐอเมริกาเมื่อวันที่ 11 กันยายน 2001 เกิดขึ้นและมีการขยายผลไปทั่วโลกทำให้มีผู้เสียชีวิตเป็นจำนวนมาก ประเทศสหรัฐอเมริกาจึงเป็นประเทศแกนนำในการต่อต้านการก่อการร้ายนานาประเทศทั่วโลก ได้มีการพัฒนาทางเทคโนโลยีในทุกด้านทั้งการขนส่ง การสื่อสาร ระบบอินเทอร์เน็ต เป็นต้น ส่งผลให้โลกมีการติดต่อสื่อสารเชื่อมต่อกันอย่างสมบูรณ์สามารถกระจายข่าวสารถึงกันได้อย่างรวดเร็วจากการเป็นยุคโลกาภิวัฒน์จึงทำให้ภัยคุกคามการก่อการร้ายของโลกได้เปลี่ยนแปลงรูปแบบอย่างรวดเร็ว ปัจจุบันปัญหาการก่อการร้ายในยุคโลกาภิวัตน์เป็นปัญหาที่คุกคามคนทั่วโลกหลายประเทศตื่นตัวต่อภัยคุกคามในรูปแบบใหม่ซึ่งเป็นการก่อการร้ายระหว่างประเทศที่เป็นภัยต่อคนทั่วโลก โดยมีแนวโน้มจะขยายขอบเขต และความรุนแรงยิ่งขึ้นจากเดิม จากการเปลี่ยนแปลงรูปแบบการต่อสู้โดยใช้กำลังการสู้รบแบบเผชิญหน้าเป็นการแย่งชิงข้อมูลข่าวสาร การรับจ้างก่อการร้ายสากลโดยอาศัยเครือข่ายอินเทอร์เน็ต การต่อสู้แย่งชิงแสวงหาผลประโยชน์ทางเศรษฐกิจของกลุ่มชน กลุ่มเชื้อชาติ และกลุ่มศาสนา

สำหรับประเทศไทยแม้ไม่ได้เกี่ยวข้องโดยตรงกับปัญหาความขัดแย้งต่างๆ ที่เป็นสาเหตุของการก่อการร้าย แต่ก็ได้รับผลจากการที่มีสมาชิกกลุ่มก่อการร้ายได้เดินทางเข้ามาปฏิบัติการต่อเป้าหมายในประเทศไทย เนื่องจากประเทศไทยมีการดำเนินความสัมพันธ์ทางการทูตกับประเทศที่เป็นเป้าหมายของการก่อการร้าย เช่น สหรัฐอเมริกา อิสราเอล กลุ่มประเทศอาหรับ เป็นต้น รวมทั้งเป็นที่ตั้งของชุมชนและ

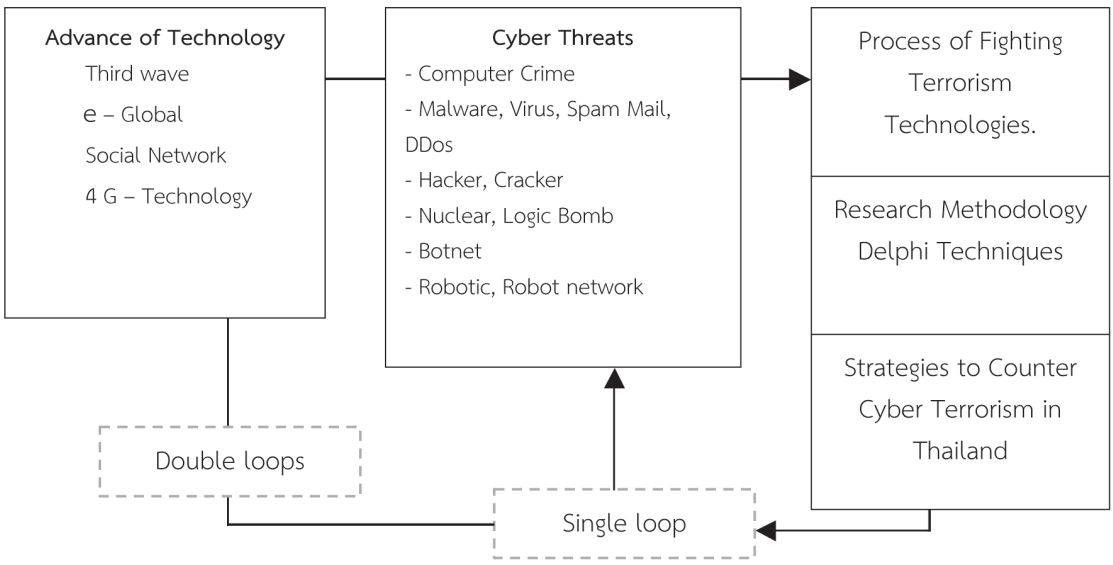
ผลประโยชน์ของประเทศเหล่านั้น อีกทั้งประเทศไทยยังเป็นแหล่งหลบซ่อน สถานที่ติดต่อ จุดพักเพื่อเตรียมการแหล่งสนับสนุน จุดฝังตัวและต่อต้านของผู้ก่อการร้ายเพื่อปฏิบัติการในประเทศที่สามจึงทำให้ประเทศไทยมีโอกาสเสี่ยงที่จะมีการก่อการร้ายได้ทุกเมื่อ การก่อการร้ายทางไซเบอร์เป็นการโจมตีระบบสารสนเทศข้อมูลของผู้ใช้หรือระบบคอมพิวเตอร์ที่มีแรงจูงใจทางการเมืองหรืออุดมการณ์โดยมุ่งหวังให้เกิดผลลัพธ์รุนแรง (มีความแตกต่างกันบางอย่างทางด้านวิธีการระหว่างการก่อการร้ายทางไซเบอร์กับการเจาะเข้าระบบของอาชญากร แต่โดยทั่วไปแรงจูงใจเป็นส่วนบ่งบอกความแตกต่าง) การโจมตีของผู้ก่อการร้ายทางไซเบอร์ไม่จำกัดอยู่แค่การรบกวนระบบ ผู้ก่อการร้ายที่ลักลอบขนยาเสพติด กลุ่มผู้ค้ายา และอาชญากรจะสามารถใช้เครื่องมือทางไซเบอร์ดำเนินการก่อการร้ายได้ เนื่องจากแนวโน้มของการพัฒนาทางเทคโนโลยีมีสูงขึ้น ผู้ก่อการร้ายสามารถทำทุกอย่างไม่ว่าจะเป็นการใช้สังคมออนไลน์ในการติดต่อสื่อสาร การปิดการจ่ายไฟฟ้า การควบคุมระบบโครงสร้างพื้นฐาน การปล่อยไวรัสคอมพิวเตอร์โจมตีระบบของอุตสาหกรรมทั่วประเทศ เป็นต้น

จากแนวคิดดังกล่าวนำมาสู่การพัฒนายุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย ซึ่งเป็นการก่อการร้ายที่ใช้เทคโนโลยีสารสนเทศสมัยใหม่มาทำลายหรือสร้างความเสียหายกับประเทศไทย และยังส่งผลต่อความมั่นคงแห่งชาติ ด้วยเหตุนี้ผู้วิจัยตระหนักว่าประเทศไทยต้องให้ความสำคัญและเข้าใจถึงปัญหาอันเกิดจากการใช้ไซเบอร์และนำมาเป็นเครื่องมือในการก่อการร้าย อีกทั้งสถานการณ์ความมั่นคงทางเทคโนโลยีและความเสี่ยงอันอาจจะเกิดขึ้นได้ทุกเมื่อจึงมีความจำเป็นต้องกำหนดยุทธศาสตร์การต่อต้านการก่อการร้ายโดยใช้ไซเบอร์มาเป็นเครื่องมือในการก่อการร้ายซึ่งการกระทำดังกล่าวมีผลต่อความมั่นคงแห่งชาติและเพื่อป้องกันการก่อการร้ายให้ประเทศไทยเข้าสู่การเป็นประเทศที่พัฒนาและการเป็นประชาคมอาเซียนอย่างมีประสิทธิภาพ

วัตถุประสงค์

1. เพื่อศึกษาความก้าวหน้าทางไซเบอร์ที่มีการนำมาใช้เป็นเครื่องมือทางยุทธศาสตร์ในการก่อการร้ายในประเทศไทย
2. เพื่อพัฒนายุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย

กรอบแนวคิด



ภาพที่ 1 กรอบแนวคิดในการวิจัย

ระเบียบวิธีการวิจัย

1. ประชากรและกลุ่มตัวอย่าง

ประชากรที่ใช้ในการวิจัยครั้งนี้ คือ ข้าราชการที่ปฏิบัติงานเกี่ยวกับเทคโนโลยีสารสนเทศและผู้ที่มีบทบาทหรือส่วนเกี่ยวข้องกับการดำเนินการหรือการพัฒนาทางไซเบอร์และใช้การพัฒนาทางไซเบอร์มาเป็นเครื่องมือ ในการดำเนินการพัฒนาในประเทศไทย กลุ่มตัวอย่างที่ใช้ในการวิจัยครั้งนี้ คือ ผู้เชี่ยวชาญที่ถูกเลือกมาให้ข้อมูลสำหรับการศึกษาในเรื่องยุทธศาสตร์นโยบายและการดำเนินการตามนโยบาย รวมทั้งบทบาทของประเทศไทยต่อการดำเนินการต่อต้านการก่อการร้ายทางไซเบอร์ รวมทั้งปัญหาอันเกิดจากการก่อการร้ายในปัจจุบัน การเลือกตัวอย่างที่ครอบคลุมความหลากหลายในประชากรให้ได้มากที่สุดนั้นเป็นวิธีการเลือกตัวอย่างที่ดีที่สุด เนื่องจากลักษณะที่เกิดร่วมกันจากความหลากหลายของกลุ่มตัวอย่างเป็นสิ่งที่น่าสนใจและมีคุณค่าต่อการวิจัยเป็นอย่างยิ่ง ซึ่งสามารถบ่งชี้รูปแบบที่สามารถเกิดขึ้นได้เหมือนกันจากตัวอย่างซึ่งมีลักษณะต่างกันในกลุ่มที่ศึกษาได้ Lincoln & Guba, 1985 อ้างถึงใน Kaemkate (2008) มีจำนวนทั้งสิ้น 10 คน โดยแบ่งออกเป็น 2 กลุ่ม

กลุ่มแรก ได้แก่ ผู้ที่มีบทบาทหรือส่วนเกี่ยวข้องกับการดำเนินการหรือการพัฒนาทางไซเบอร์และใช้การพัฒนาทางไซเบอร์มาเป็นเครื่องมือในการดำเนินการพัฒนาในประเทศไทย จำนวน 4 คน กลุ่มที่สอง ได้แก่ ผู้ที่มีความรู้ความเชี่ยวชาญในส่วนของการกำหนดยุทธศาสตร์ทางเทคโนโลยีในส่วนของภาครัฐ จำนวน 6 คน ประกอบด้วย กระทรวงเทคโนโลยีและสารสนเทศ จำนวน 2 คน หน่วยงานความมั่นคงแห่งชาติ จำนวน 1 คน สำนักงานตำรวจแห่งชาติ จำนวน 2 คน และกองทัพไทย จำนวน 1 คน

2. การสร้างและพัฒนาคุณภาพเครื่องมือ

การดำเนินการวิจัยด้วยการสัมภาษณ์ผู้เชี่ยวชาญเพื่อทำการรวบรวมข้อมูลและความคิดเห็นที่เป็นประโยชน์ต่อการศึกษาในครั้งนี้จะมีลักษณะเฉพาะคือ การสัมภาษณ์เชิงลึกแบบรายบุคคลเพื่อหลีกเลี่ยงการเผชิญหน้ากันระหว่างผู้เชี่ยวชาญแต่ละท่าน ทำให้ผู้เชี่ยวชาญแต่ละท่านปราศจากการชี้นำจากกลุ่มและไม่อยู่ในอิทธิพลทางความคิดเห็นของผู้เชี่ยวชาญท่านอื่น เครื่องมือเป็นแบบสัมภาษณ์เกี่ยวกับความก้าวหน้าทางไซเบอร์ ลักษณะการก่อการร้ายทางไซเบอร์ และการนำไซเบอร์มาเป็นเครื่องมือทางยุทธศาสตร์ในการก่อการร้าย พัฒนาเครื่องมือโดยวิธีการยกร่างแบบสัมภาษณ์ นำแบบสัมภาษณ์ให้อาจารย์ที่ปรึกษาให้ข้อเสนอแนะ ปรับปรุงแบบสัมภาษณ์ตามข้อเสนอแนะของอาจารย์ที่ปรึกษา ทดลองสัมภาษณ์บุคคลผู้ที่ไม่ใช่ผู้ทรงคุณวุฒิในครั้งนี้และปรับปรุงอีกครั้ง

3. การเก็บและรวบรวมข้อมูล

ผู้วิจัยดำเนินการส่งหนังสือจากคณะรัฐศาสตร์และนิติศาสตร์ มหาวิทยาลัยบูรพา ไปยังผู้เชี่ยวชาญ จำนวน 10 คน เพื่อขออนุญาตให้ดำเนินการเก็บรวบรวมข้อมูล และผู้วิจัยนัดหมายผู้ให้สัมภาษณ์ นัดหมายเกี่ยวกับวัน เวลา และสถานที่ในการสัมภาษณ์ และผู้วิจัยส่งแบบสอบถามการสัมภาษณ์ให้ผู้สัมภาษณ์ด้วยตนเอง เพื่อให้ผู้รับสัมภาษณ์มีการเตรียมตัวพร้อมทราบแนวคำถามล่วงหน้าและทำการบันทึกการสัมภาษณ์ในระหว่างการสัมภาษณ์ ตั้งแต่วันที่ 30 พฤษภาคม 2015 ถึง วันที่ 20 ตุลาคม 2015 หลังจากนั้นรวบรวมข้อมูลจากผู้ให้สัมภาษณ์เพื่อนำมาวิเคราะห์ข้อมูล

4. การวิเคราะห์ข้อมูล

ผู้วิจัยใช้การวิเคราะห์แบบอุปนัย โดยผู้วิจัยจะนำข้อมูลที่ได้มาจดบันทึกเป็นระบบโดยจำแนกว่าใครพูดอะไร และนำมาหาความหมาย แยกแยะองค์ประกอบที่เชื่อมโยง หาความสัมพันธ์ของข้อมูลเพื่ออธิบายความสัมพันธ์ของข้อมูลที่รวบรวมจากการสัมภาษณ์ โดยผู้วิจัยจะเก็บรวบรวมข้อมูลไปพร้อมกับการวิเคราะห์ทุกครั้ง เพื่อให้ได้ข้อมูลที่ถูกต้องครบถ้วน สมบูรณ์ ตามประเด็นที่ต้องการ หลังจากนั้นผู้วิจัยใช้การวิเคราะห์ข้อมูลโดยการจำแนกชนิดของข้อมูลซึ่งการจำแนกชนิดของข้อมูล กรอบในการจำแนกตามประเด็นที่เกี่ยวข้องกับความก้าวหน้าทางไซเบอร์ ลักษณะของการก่อการร้าย การก่อการร้ายทางไซเบอร์ การนำไซเบอร์มาเป็นเครื่องมือทางยุทธศาสตร์ในการก่อการร้าย การต่อต้านการก่อการร้ายทางไซเบอร์ของประเทศไทย

การวิเคราะห์จุดแข็ง จุดอ่อน โอกาส และอุปสรรค

ผู้วิจัยนำข้อมูลจากการสัมภาษณ์ผู้เชี่ยวชาญเกี่ยวกับสภาพแวดล้อมภายในและสภาพแวดล้อมภายนอกมาจัดทำตารางวิเคราะห์เมทริกซ์เพื่อนำมาวิเคราะห์ประกอบการจัดทำยุทธศาสตร์

1. จัดทำตาราง SWOT Matrix

2. จับคู่จุดแข็งหลัก – โอกาสหลัก (SO) กำหนดยุทธศาสตร์ที่เหมาะสม โดยยุทธศาสตร์ คือ การใช้จุดแข็งเพื่อให้ได้โอกาสมากที่สุด

3. จับคู่จุดแข็งหลัก – อุปสรรคหลัก (ST) กำหนดยุทธศาสตร์ที่เหมาะสม โดยยุทธศาสตร์ คือ การใช้จุดแข็งเพื่อหลีกเลี่ยงภาวะที่เป็นอุปสรรค

4. จับคู่จุดอ่อนหลัก – จุดแข็งหลัก (WO) กำหนดยุทธศาสตร์ที่เหมาะสม โดยยุทธศาสตร์ที่เหมาะสม คือ การลดจุดอ่อนเพื่อเพิ่มโอกาส

5. จับคู่จุดอ่อนหลัก – ภาวะอุปสรรคหลัก (WT) กำหนดยุทธศาสตร์ที่เหมาะสม โดยยุทธศาสตร์ที่เหมาะสม คือ การลดจุดอ่อนและหลีกเลี่ยงภาวะที่เป็นอุปสรรค

นำข้อมูลทั้งหมดเข้าสู่การดำเนินการในตารางวิเคราะห์เมทริกซ์จากยุทธศาสตร์ทั้งหมดผู้วิจัยนำไปพัฒนาเป็นยุทธศาสตร์ที่สำคัญและกำหนดเป็นยุทธศาสตร์หลักของการวิจัย

ผลการวิจัย

สรุปผลการวิจัยตามวัตถุประสงค์ข้อที่ 1. เพื่อศึกษาความก้าวหน้าทางไซเบอร์ที่มีการนำมาใช้เป็นเครื่องมือทางยุทธศาสตร์ในการก่อการร้ายในประเทศไทย

1. ความก้าวหน้าทางไซเบอร์ คือ เทคโนโลยีที่มีอินเทอร์เน็ตเพื่อเชื่อมต่อการสื่อสารได้ทุกที่ทุกเวลา ไม่ว่าจะอยู่ที่ใดบนโลก สะดวก รวดเร็ว และไซเบอร์มีความสำคัญอย่างมากต่อการดำรงชีวิตในปัจจุบัน โดยมีเครื่องมือที่ใช้ในการติดต่อสื่อสาร ประกอบด้วย คอมพิวเตอร์ โทรศัพท์มือถือ หรือแท็บเล็ต เครื่องมืออื่นๆ ที่เชื่อมต่ออินเทอร์เน็ตได้และความก้าวหน้าทางไซเบอร์ต้องมีความเร็วสูง มีระบบปฏิบัติการที่ดีและมีประสิทธิภาพสามารถเข้าถึงได้ง่าย

2. ประเทศไทยมีโอกาสในการพัฒนาความก้าวหน้าทางไซเบอร์ได้อีกมาก ด้วยบริบทของประเทศไทยยังคงเป็นประเทศที่ไม่ได้มีการใช้ไซเบอร์ทั้งระบบในโครงสร้างพื้นฐานและมีโอกาสในการพัฒนาทางไซเบอร์ด้วยปัจจัยหลายด้าน เช่น ความสามารถของคนรุ่นใหม่ที่มีความสนใจทางไซเบอร์ ความตื่นตัวต่อการเรียนรู้ทางไซเบอร์ การพัฒนาโครงสร้างพื้นฐานให้มีความพร้อม สามารถพัฒนาควบคู่ไปกับการใช้ไซเบอร์และมีวิธีการป้องกันที่ดีต่อการก่อการร้าย เป็นต้น

3. ประเทศไทยกล่าวได้ว่าแม้ไม่ใช่เป้าหมายโดยตรงของกลุ่มผู้ก่อการร้ายแต่อาจตกเป็นเป้าหมายสำหรับการปฏิบัติการของกลุ่มผู้ก่อการร้าย เนื่องจากประเทศไทยมีผลประโยชน์เกี่ยวข้องกับประเทศต่างๆ โดยเฉพาะประเทศตะวันตกซึ่งเป็นเป้าหมายของกลุ่มผู้ก่อการร้ายจำนวนมาก โดยกลุ่มผู้ก่อการร้ายส่วนใหญ่ที่เข้ามาเคลื่อนไหวและปฏิบัติการในประเทศไทยจะใช้ประเทศไทยเป็นแหล่งที่หลบภัยและผลิตยุทโธปกรณ์

ของกลุ่มผู้ก่อการร้าย อีกทั้งยังแสวงหาผลประโยชน์จากทางการเงิน การธนาคาร ประเทศไทยมีมาตรการที่ไม่รัดกุมเป็นช่องทางสนับสนุนทางการเงินของกลุ่มผู้ก่อการร้าย นอกจากนี้การก่อการร้ายเชื่อมโยงกับการก่ออาชญากรรมประเภทอื่นด้วย เช่น การลักลอบค้ายาเสพติด การค้าอาวุธ การฟอกเงิน การปลอมแปลงเอกสารเดินทาง บัตรประจำตัวประชาชนหรือเอกสารราชการ เป็นต้น ผู้ก่อการร้ายผลิตและลักลอบค้ายาเสพติดสามารถสร้างเงินและรายได้จำนวนมหาศาลให้กับผู้ก่อการร้าย และนำเงินที่ได้มาซื้ออาวุธหรือสร้างฐานกำลังเพื่อดำเนินการก่อการร้ายกับประเทศที่เป็นเป้าหมาย โดยมีวัตถุประสงค์ในการใช้ประเทศไทยเป็นฐาน หรือศูนย์กลางในการจัดส่งอาวุธ หรือเป็นทางผ่านไปยังประเทศเป้าหมาย

4. การก่อการร้ายจะต้องมีเป้าหมาย วัตถุประสงค์ และรูปแบบในการกระทำที่ชัดเจน ซึ่งกระทำได้จากบุคคล องค์กร หรือรัฐ แต่การก่อการร้ายทางไซเบอร์มีหลากหลายรูปแบบทั้งประเภทที่กระทำโดยไม่ได้มุ่งหวังทำลายล้างหรือการกระทำที่สร้างความเสียหายต่อประเทศ โดยมีรูปแบบที่หลากหลายและซับซ้อน แม้ประเทศไทยจะไม่ใช่เป้าหมายของการก่อการร้ายโดยตรง แต่คนไทยก็ไม่มีการตระหนักต่อภัยของการก่อการร้ายในสถานการณ์การก่อการร้ายปกติและการก่อการร้ายทางไซเบอร์ ประเทศไทยมีความพร้อมของการรับมือต่อการเกิดสถานการณ์จากหน่วยงานซึ่งมีหน้าที่ดูแลรับผิดชอบ แต่ก็ยังคงมีช่องโหว่ เช่น ทางด้านกฎหมาย ทางด้านของหน้าที่ในการดูแลและความรับผิดชอบต่อการป้องกันการก่อการร้าย เป็นต้น ผู้ก่อการร้ายสามารถใช้ช่องโหว่นี้ก่อการร้ายได้ทุกเมื่อ

5. ในศตวรรษที่ 21 มีรูปแบบของการก่อการร้ายที่สังคมมีความตื่นตัวกับการป้องกันภัยของการก่อการร้าย การก่อการร้ายทางไซเบอร์เป็นรูปแบบของการก่อการร้ายโดยมีการนำเทคโนโลยีสารสนเทศที่ทันสมัยนำมาเป็นเครื่องมือช่วยให้กลุ่มก่อการร้ายสามารถดำเนินกิจกรรมต่างๆ ได้อย่างมีประสิทธิภาพ โดยใช้พลังอำนาจของเทคโนโลยีสารสนเทศเป็นแนวทางปฏิบัติหรือปรับองค์กรไปสู่รูปแบบใหม่ของการก่อการร้ายทางไซเบอร์อาศัยช่องว่างการขยายตัวของโลกสมัยใหม่ที่มีการเชื่อมโยงของข้อมูลข่าวสารผ่านระบบคอมพิวเตอร์ในระบบเครือข่าย จึงทำให้ผู้ก่อการร้ายสามารถใช้ช่องทางไซเบอร์และผู้ใช้ไซเบอร์ตกเป็นเป้าของการโจมตีเพื่อทำลายหรือขัดขวางการทำงานระบบเครือข่ายคอมพิวเตอร์ทั้งระบบเครือข่ายการสื่อสารหรือระบบคอมพิวเตอร์ที่เกี่ยวข้องกับการทำงานขององค์กรขนาดใหญ่ การควบคุมโครงสร้างพื้นฐาน หรือระบบโครงสร้างความมั่นคงทางทหาร หรือการล้วงข้อมูลความมั่นคงของประเทศ เป็นต้น โดยใช้วิธีการสร้างความเสียหายก่อให้เกิดความตื่นตระหนกต่อประชาชนและดึงดูดความสนใจของสื่อมวลชนหรือบุคคลต่างๆ ซึ่งคาดหมายว่าอนาคตจะมีการก่อการร้ายทางไซเบอร์และเป็นยุทธวิธีหนึ่งในการก่อการร้ายทางไซเบอร์

6. วิธีการก่อการร้ายทางไซเบอร์ มีวิธีการดังนี้ 1) ผู้ก่อการร้ายซึ่งต้องมีความรู้ทางไซเบอร์หรือเทคโนโลยี ศึกษาข้อมูลที่เกี่ยวกับเป้าหมายที่ต้องการจะกระทำ 2) สร้างหรือพัฒนาเครื่องมือให้ตรงกับความต้องการต่อเป้าหมาย เครื่องมือที่สำคัญของการก่อการร้ายทางไซเบอร์คือ อินเทอร์เน็ต 3) ระดมคนหรือหาสมาชิกที่มีแนวความคิดแนวทางเดียวกัน 4) ระดมเงินทุนในการสนับสนุน 5) ปฏิบัติการตามวัตถุประสงค์ที่วางไว้เพื่อมุ่งเป้าหมายทางการเมือง

7. ปัจจัยที่เกี่ยวข้องกับแรงจูงใจในการก่อการร้ายทางไซเบอร์ด้วยประเทศไทยเป็นประเทศเปิดเสรีรับนักท่องเที่ยวและมีนโยบายส่งเสริมให้เกิดการท่องเที่ยวในทุกที่โดยไม่มีข้อจำกัด ดังนั้นจึงเป็นเหมือนสวรรค์ของผู้ก่อการร้าย อีกทั้งการส่งเสริมการเปิดใช้อินเทอร์เน็ตในทุกที่ทำให้ประชาชนขาดการตระหนักรู้ในเรื่องของการใช้ไซเบอร์ การก่อการร้ายทางไซเบอร์นั้นผู้ก่อการร้ายจะใช้เครื่องมือทางไซเบอร์ที่หาง่ายและใช้เครื่องมือได้ทุกที่ เช่น โทรศัพท์มือถือ แท็บเล็ต คอมพิวเตอร์ ที่สามารถเชื่อมต่ออินเทอร์เน็ตได้ทำให้คนเข้าถึงได้ง่ายและเชื่อง่ายขึ้น แรงจูงใจที่นำไซเบอร์มาก่อการร้าย ผู้เชี่ยวชาญมองว่าเป็นเรื่องเงินเป็นสำคัญ รองมาเป็นเรื่องของแนวคิด อุดมการณ์ทางการเมืองหรือทางศาสนาหรือแม้แต่ความไม่พอใจต่อหน่วยงานหรือองค์กร แต่ปัจจัยที่สำคัญที่ผู้เชี่ยวชาญมองต่างกันคือ แรงจูงใจที่สำคัญต่อการกระทำที่เป็นการก่อการร้ายจะต้องเป็นการกระทำที่มาจากแรงจูงใจทางเมืองเป็นสำคัญ จึงเห็นได้ว่าความเข้าใจในความหมายของการก่อการร้ายที่แตกต่างกัน นำไปสู่การอธิบายแรงจูงใจของการก่อการร้ายที่ต่างกันด้วย การอธิบายแรงจูงใจต่อการก่อการร้ายทางไซเบอร์จึงไม่ได้มีการให้คำจำกัดความที่ชัดเจนเช่นเดียวกัน

8. ผู้ก่อการร้ายแสวงหาโอกาสจากประเทศไทยในหลายด้านเพื่อก่อการร้าย ประเด็นสำคัญที่พบได้คือ ประเทศไทยเป็นประเทศที่เปิดเสรี และประชาชนมีการต้อนรับชาวต่างประเทศ มีการยิ้มแย้มแจ่มใสและต้อนรับผู้อื่นอย่างเป็นมิตรจึงเหมือนกับเป็นสวรรค์ของผู้ก่อการร้าย ส่วนใหญ่ผู้ก่อการร้ายจะใช้ประเทศไทยเป็นฐานในการเตรียมการก่อการร้ายไปยังประเทศที่สาม หรือประเทศที่เป็นเป้าหมายมากกว่าและประเทศไทยไม่มีมาตรการในการป้องกันความปลอดภัยทางไซเบอร์ ประชาชนยังไม่มีการตระหนักรู้ต่อภัยคุกคามทางไซเบอร์จึงทำให้มีการใช้อย่างไม่ระวัง

สรุปผลการวิจัยตามวัตถุประสงค์ข้อที่ 2 เพื่อพัฒนายุทธศาสตร์การต่อต้านการก่อการร้ายในประเทศไทย

ยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทยมาจากการใช้ประโยชน์จากจุดแข็งเพื่อหาแนวทางลดจุดอ่อน หาแนวทางเพื่อค้นหาหรือใช้ประโยชน์จากโอกาสและหาแนวทางเพื่อบรรเทาหรือเอาชนะต่อภาวะคุกคาม โดยการจับคู่จุดแข็งหลัก – โอกาสหลัก (SO) การจับคู่จุดแข็งหลัก – ภาวะคุกคามหลัก (ST) การจับคู่จุดอ่อนหลัก – โอกาสหลัก (WO) และการจับคู่จุดอ่อนหลัก – ภาวะคุกคามหลัก (WT) หลังจากนั้นดำเนินการวิเคราะห์ข้อมูลโดยใช้ Scenario Analysis และวิธีการ Double Loops เพื่อพัฒนายุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย ได้ยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ (Cyber) ในประเทศไทยดังนี้

วิสัยทัศน์

ประเทศไทยมีศักยภาพในการสร้างภูมิคุ้มกันป้องกัน และร่วมกันต่อต้านการก่อการร้ายทางไซเบอร์

พันธกิจ

สร้างฐานความรู้ทางไซเบอร์ให้กับประชาชนทุกระดับพร้อมทั้งมุ่งพัฒนาความเข็มแข็งทางไซเบอร์เพื่อความมั่นคงของประเทศไทย

เป้าประสงค์

เพื่อพัฒนาและเสริมสร้างความมั่นคงทางไซเบอร์ให้กับประเทศไทย

ยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย ประกอบด้วย READ: CLIP คือ 1. Research ยุทธศาสตร์การเสริมสร้างการวิจัยเพื่อการพัฒนาทางไซเบอร์ 2. Education ยุทธศาสตร์การจัดการศึกษาในการสร้างพื้นฐานของประชาชนในประเทศไทย 3. Awareness ยุทธศาสตร์การสร้างการตระหนักรู้ทางไซเบอร์ให้กับประชาชน 4. Development ยุทธศาสตร์การพัฒนาความก้าวหน้าทางไซเบอร์ 5. Coordinate ยุทธศาสตร์การส่งเสริมความร่วมมือระหว่างภาครัฐ ภาคเอกชน และภาคประชาชน 6. Law ยุทธศาสตร์การกำหนดใช้กฎหมายทางไซเบอร์และการบังคับใช้กับประชาชน 7. Integration ยุทธศาสตร์การใช้การบูรณาการร่วมกันเพื่อแบ่งปันข้อมูล 8. Perception Prepares and Protect ยุทธศาสตร์การรับรู้ทางไซเบอร์ร่วมกัน ตระเตรียมและปกป้องทางไซเบอร์ ดังนี้

ยุทธศาสตร์ที่ 1 Research ยุทธศาสตร์การเสริมสร้างงานวิจัยเพื่อการพัฒนาทางไซเบอร์

แนวทางหรือมาตรการ มีดังต่อไปนี้

1. มีการส่งเสริมให้ประชาชน นักวิชาการ หรือภาคเอกชนมีความสนใจในประเด็นทางไซเบอร์และการก่อการร้ายทางไซเบอร์มากขึ้น ให้ครอบคลุมทุกด้าน

2. สนับสนุนด้านงบประมาณด้านการวิจัยทางไซเบอร์เพื่อสร้างแรงจูงใจให้กับนักวิจัยทางไซเบอร์อย่างมีประสิทธิภาพ

ยุทธศาสตร์ที่ 2 Education ยุทธศาสตร์การจัดการศึกษาในการสร้างพื้นฐานของประชาชนในประเทศไทย

แนวทางหรือมาตรการ มีดังต่อไปนี้

1. กำหนดหลักสูตรที่เกี่ยวกับไซเบอร์ในทุกระดับเพื่อให้เยาวชนได้มีรากฐานของการศึกษาและเข้าใจต่อการใช้ไซเบอร์อย่างถูกต้อง

2. พัฒนาหลักสูตรในระดับอุดมศึกษาเพื่อพัฒนาองค์ความรู้ทางไซเบอร์ให้สามารถนำความรู้ไปใช้อย่างครอบคลุมและมีประสิทธิภาพในทุกๆ ด้าน

ยุทธศาสตร์ที่ 3 Awareness ยุทธศาสตร์การสร้างการตระหนักรู้ทางไซเบอร์ให้กับประชาชน

แนวทางหรือมาตรการ มีดังต่อไปนี้

1. สนับสนุนให้ประชาชนมีการสร้างความรู้ ความเข้าใจที่ดีต่อการใช้ไซเบอร์ และมีการถ่ายทอดความรู้ความเข้าใจที่ดีต่อการใช้ไซเบอร์ รวมทั้งมีการถ่ายทอดความรู้ความเข้าใจจากรุ่นไปสู่รุ่น

2. เผยแพร่ความรู้และประชาสัมพันธ์ให้ประชาชนมีการใช้ไซเบอร์ รวมทั้งตระหนักถึงการใช้ไซเบอร์อย่างถูกต้องเพื่อป้องกันการนำมาเป็นเครื่องมือในการก่อการร้าย

ยุทธศาสตร์ที่ 4 Development ยุทธศาสตร์การพัฒนาความก้าวหน้าทางไซเบอร์

แนวทางหรือมาตรการ มีดังต่อไปนี้

1. มีการจัดตั้งหน่วยงานการพัฒนาทางไซเบอร์เพื่อพัฒนาระบบสารสนเทศและการรักษาความปลอดภัยทางไซเบอร์ข้อมูลข่าวสาร

2. จัดฝึกอบรมให้ความรู้ สนับสนุนการจัดสอบเพื่อให้บุคลากรผ่านเกณฑ์มาตรฐานสากล สนับสนุนการวิจัยสร้างองค์ความรู้ใหม่ทางไซเบอร์

3. พัฒนาบุคลากรให้มีความเชี่ยวชาญในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ รวมทั้งสร้างแรงจูงใจในการจงรักภักดีและทำงานเพื่อประเทศชาติเพื่อป้องกันสมองไหลไปยังต่างประเทศ

ยุทธศาสตร์ที่ 5 Coordinate ยุทธศาสตร์การส่งเสริมความร่วมมือระหว่างภาครัฐ ภาคเอกชน และภาคประชาชน

แนวทางหรือมาตรการ มีดังต่อไปนี้

1. มีการเสริมสร้างความเข้าใจร่วมกันในการกำหนด นิยาม ความหมายของไซเบอร์ การก่อการร้ายและการก่อการร้ายทางไซเบอร์

2. มีการกำหนดนโยบาย แนวทาง และแผนปฏิบัติการที่ชัดเจนเพื่อให้เกิดการแปลงแผนไปสู่กลยุทธ์และไปสู่การปฏิบัติตามวิสัยทัศน์ พันธกิจ และเป้าประสงค์ที่กำหนดไว้อย่างมีประสิทธิภาพ

3. กำหนดกลไกในการทบทวน ติดตาม และประเมินความเสี่ยงต่อการนำแผนไปปรับใช้เพื่อปรับแนวทางให้มีความเหมาะสมตามสถานการณ์ใหม่หรือสถานการณ์ที่แตกต่าง

ยุทธศาสตร์ที่ 6 Law ยุทธศาสตร์การกำหนดใช้กฎหมายทางไซเบอร์และการบังคับใช้กับประชาชน

แนวทางหรือมาตรการ มีดังต่อไปนี้

1. กำหนดกฎหมาย กฎระเบียบ ขั้นตอน ที่เกี่ยวข้องกับการใช้ไซเบอร์ ความมั่นคงทางไซเบอร์และการต่อต้านการก่อการร้ายทางไซเบอร์อย่างครอบคลุม

2. กำหนดแนวทางที่ชัดเจนต่อการบังคับใช้กฎหมาย พร้อมทั้งมาตรการ บทลงโทษต่อการกระทำอันเกี่ยวข้องกับก่อการร้าย

ยุทธศาสตร์ที่ 7 Integration ยุทธศาสตร์การใช้การบูรณาการร่วมกันเพื่อแบ่งปันข้อมูล

แนวทางหรือมาตรการ มีดังต่อไปนี้

1. จัดตั้งหน่วยงานกลางมีหน้าที่ในการดูแล ดำเนินการทางด้านไซเบอร์ มีการแบ่งปันข้อมูลร่วมกันเพื่อประโยชน์ของประชาชน รวมทั้งมีการบูรณาการการทำงานร่วมกัน อีกทั้งระบุโอกาส และความท้าทายในการเพิ่มขีดความสามารถของกลไกการตอบสนองต่อการร้าย

2. สร้างฐานข้อมูลกลางเพื่อรวบรวมข้อมูลสำคัญจากทุกภาคส่วน รวมทั้งมีการควบคุมดูแลเพื่อไม่ให้ข้อมูลถูกเผยแพร่ เปิดโอกาสให้ทุกหน่วยงานที่เกี่ยวข้องกับไซเบอร์สามารถดึงข้อมูลไปใช้ในทางที่ถูกต้อง

3. จัดตั้งศูนย์ข่าวกรองทางไซเบอร์ เพื่อทำงานด้านการข่าวทางไซเบอร์ แบ่งปันข้อมูลข่าวสารและประสานงานความร่วมมือระหว่างหน่วยงาน

ยุทธศาสตร์ที่ 8 Perception Prepares and Protect ยุทธศาสตร์การรับรู้ทางไซเบอร์ร่วมกัน ตระเตรียม และปกป้องทางไซเบอร์

แนวทางหรือมาตรการ มีดังต่อไปนี้

1. ปลูกฝังทัศนคติและแนวทางการใช้ไซเบอร์ที่เป็นรูปธรรมเพื่อให้ประชาชนมีการรับรู้ต่อการใช้ไซเบอร์ในทางที่ถูกต้อง

2. สร้างการมีส่วนร่วมของประชาชน รวมทั้งวิธีการในการตระเตรียมตนเองเพื่อให้เกิดการปฏิบัติอย่างรู้เท่าทัน

อภิปรายผล

การวิจัยเรื่องยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ ผลการศึกษามีดังนี้ การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย ยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย คือ READ: CLIP ประกอบด้วย ยุทธศาสตร์ที่ 1 Research ยุทธศาสตร์การเสริมสร้างการวิจัยเพื่อการพัฒนาทางไซเบอร์ ยุทธศาสตร์ที่ 2 Education ยุทธศาสตร์การจัดการศึกษาในการสร้างพื้นฐานของประชาชนในประเทศไทย ยุทธศาสตร์ที่ 3 Awareness ยุทธศาสตร์การสร้างการตระหนักรู้ทางไซเบอร์ให้กับประชาชน ยุทธศาสตร์ที่ 4 Development ยุทธศาสตร์การพัฒนาความก้าวหน้าทางไซเบอร์ ยุทธศาสตร์ที่ 5 Coordinate ยุทธศาสตร์การส่งเสริมความร่วมมือระหว่างภาครัฐ ภาคเอกชน และภาคประชาชน ยุทธศาสตร์ที่ 6 Law ยุทธศาสตร์การกำหนดใช้กฎหมายทางไซเบอร์และการบังคับใช้กับประชาชน ยุทธศาสตร์ที่ 7 Integration ยุทธศาสตร์การใช้บูรณาการร่วมกันเพื่อแบ่งปันข้อมูล และยุทธศาสตร์ที่ 8 Perception Prepares and Protect ยุทธศาสตร์การรับรู้ทางไซเบอร์ร่วมกัน ตระเตรียมและปกป้องทางไซเบอร์การศึกษาวิจัยการต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทยโดยใช้วิธีการศึกษาเชิงคุณภาพจากเทคนิคเดลฟายและการสัมภาษณ์เจาะลึกเกิดข้อค้นพบที่นำมาอภิปรายดังนี้

1. ความก้าวหน้าทางไซเบอร์เป็นเทคโนโลยีที่มีอินเทอร์เน็ตเพื่อเชื่อมต่อการสื่อสารได้ทุกที่ทุกเวลาไม่ว่าจะอยู่ที่ใดบนโลก สะดวก รวดเร็ว และไซเบอร์มีความสำคัญต่อการดำรงชีวิตของมนุษย์ โดยมีเครื่องมือที่ใช้ในการติดต่อสื่อสาร เช่น คอมพิวเตอร์ โทรศัพท์มือถือหรือแท็บเล็ต เป็นต้น สอดคล้องกับแนวความคิดของ Waters (2001) กล่าวว่า การอธิบายปรากฏการณ์ที่เชื่อมโยงสังคมและรัฐชาติเข้าไว้ด้วยกันทั่วโลก ความเป็นสากลนิยมการติดต่อสื่อสารที่เชื่อมต่อถึงกันโดยทั่วและการกระทำเหตุการณ์ที่ส่งผลกระทบหรือการร่วมมือของคนทั้งโลกในความเป็นโลกาภิวัตน์ในศตวรรษที่ 21 การนำเทคโนโลยีที่มีประสิทธิภาพและการสร้างเครือข่ายทางสังคม ทำให้โลกเปรียบเป็นโลกเสมือนสามารถเจอกันได้ รับรู้ความเคลื่อนไหว

และสามารถเข้าถึงทุกมุมทั่วโลก จึงสามารถสรุปได้ว่า ความก้าวหน้าทางไซเบอร์ เป็นเทคโนโลยีที่เชื่อมต่อการสื่อสารได้ทุกที่ทุกเวลาไม่ว่าจะอยู่ที่ใดบนโลกสะดวก รวดเร็ว โดยมีเครื่องมือเพื่อการติดต่อสื่อสาร เช่น คอมพิวเตอร์ โทรศัพท์มือถือหรือแท็บเล็ต เป็นต้น ความก้าวหน้าทางไซเบอร์ส่งผลให้เกิดกระแสวัฒนธรรมบริโภคนิยมนำมาซึ่งความไม่พอใจของกลุ่มชาตินิยม เคร่งศาสนาและกลุ่มมุสลิมหัวรุนแรง กระทำการก่อการร้ายเพื่อวัตถุประสงค์ให้เกิดความรุนแรงและการก่อการร้ายในรูปแบบใหม่ในอนาคต

2. การก่อการร้ายทางไซเบอร์เป็นรูปแบบของการก่อการร้ายโดยมีการนำเทคโนโลยีสารสนเทศที่ทันสมัยนำมาเป็นเครื่องมือที่ช่วยให้กลุ่มก่อการร้ายสามารถดำเนินกิจกรรมต่างๆ ผู้ก่อการร้ายสามารถใช้ช่องทางไซเบอร์และผู้ใช้เทคโนโลยีสารสนเทศตกเป็นเป้าของการโจมตี (Cyber Attack) เพื่อทำลายหรือขัดขวางการทำงานระบบเครือข่ายคอมพิวเตอร์แบบต่างๆ ไม่ว่าจะเป็นเครือข่ายการสื่อสารหรือเครือข่ายระบบคอมพิวเตอร์ที่เกี่ยวข้องกับการทำงานขององค์กรขนาดใหญ่ การควบคุมโครงสร้างพื้นฐาน หรือระบบโครงสร้างความมั่นคงทางทหาร หรือการล้วงข้อมูล ความมั่นคงของประเทศ เป็นต้น โดยใช้วิธีการสร้างความเสียหาย ก่อให้เกิดความตื่นตระหนกต่อประชาชนและดึงดูดความสนใจของสื่อมวลชนหรือบุคคลต่างๆ ซึ่งคาดหมายว่าอนาคตจะมีการก่อการร้ายทางไซเบอร์และเป็นยุทธวิธีในการก่อการร้ายที่มีอานุภาพร้ายแรงมาก การก่อการร้ายทางไซเบอร์ มีวิธีการดังนี้ 1. ผู้ก่อการร้ายต้องมีความรู้ทางไซเบอร์หรือเทคโนโลยี ศึกษาข้อมูลที่เกี่ยวกับเป้าหมายที่ต้องการจะกระทำ 2. สร้างหรือพัฒนาเครื่องมือให้ตรงกับความต้องการต่อเป้าหมายเครื่องมือที่สำคัญของการก่อการร้ายทางไซเบอร์คือ อินเทอร์เน็ต 3. ระดมคนหรือหาสมาชิกที่มีแนวความคิดแนวทางเดียวกัน 4. ระดมเงินทุนในการสนับสนุน 5. ปฏิบัติการตามวัตถุประสงค์ที่วางไว้เพื่อมุ่งเป้าหมายทางการเมือง สอดคล้องกับ Gobran (2015) ที่วิจัยเรื่อง ภัยคุกคามของผู้ก่อการร้ายทางไซเบอร์ พบว่า กลุ่มผู้ก่อการร้ายเริ่มต้นการปรับให้เข้ากันและยึดเอาความได้เปรียบของเครื่องมือทางไซเบอร์และความสามารถของเครื่องมือทางไซเบอร์ การคุกคามผู้ก่อการร้ายจะกระทำเพื่อการเติบโตของกลุ่มร่วมกัน ถึงแม้ว่าผู้ก่อการร้ายจะไม่มีฝีมือต่อการฆ่าคนอย่างรวดเร็วโดยตรงกับการใช้เครื่องมือทางไซเบอร์การประทุษร้ายหรือการขัดขวางทางสังคม การโจมตีสามารถเป็นเหตุพอดีกับวัตถุประสงค์การดำเนินการ

ปัญหาที่สำคัญของการต่อต้านการก่อการร้ายเกิดจากแนวคิดของการก่อการร้าย และความไม่รู้ถึงความรุนแรงอันเกิดจากการก่อการร้ายของคนในประเทศใครคือ ผู้ก่อการร้าย และอะไรคือการก่อการร้าย เนื่องจากภัยการก่อการร้ายเป็นเรื่องไกลตัวและยังไม่มีการสร้างความตระหนักอย่างชัดเจน ดังนั้นมุมมองต่อการก่อการร้ายของแต่ละประเทศ มีการให้ความหมายและแนวคิดไปตามทิศทางของตนเอง สอดคล้องกับ Silapun (2013) ที่วิจัยเรื่อง ความชัดเจนและความเหมาะสมในการกำหนดนิยามของการก่อการร้ายในประมวลกฎหมายอาญาของไทย พบว่า การบัญญัติความผิดฐานก่อการร้ายขึ้นใหม่ควรบัญญัติให้เป็นการกระทำความผิดอาญาที่โหดร้ายรุนแรง อันมีผลต่อ การดำเนินชีวิตปกติสุขของประชาชนโดยทั่วไป จึงทำให้เกิดความรู้สึกหวาดกลัวและไม่ปลอดภัยของประชาชน อันเป็นวัตถุประสงค์หลักของผู้ก่อการร้าย การนิยามความหมายของการก่อการร้ายให้เป็นกลางเป็นที่ยอมรับทั่วไปอย่างเป็นสากลยังไม่สามารถทำได้ เพราะแต่ละประเทศยังยอมรับไม่ตรงกัน อีกทั้งคำนิยามของการก่อการร้ายระหว่างประเทศ

ยังไม่ยุติ บางประเทศเห็นว่าการต่อสู้เพื่ออิสรภาพไม่เป็นการก่อการร้ายระหว่างประเทศ ในขณะที่บางประเทศกลับเห็นว่า การกระทำดังกล่าวเป็นการก่อการร้ายระหว่างประเทศ สรุปได้ว่าการสร้างความเข้าใจต่อความหมาย การนิยามและการสร้างการตระหนักรู้ต่อการก่อการร้ายจึงเป็นสิ่งสำคัญที่ประชาชนไทยควรได้รับการส่งเสริม อีกทั้งในปัจจุบันประชาชนใช้ไซเบอร์เป็นเสมือนส่วนหนึ่งของชีวิตประจำวัน ซึ่งเป็นช่องทางหนึ่งที่เป็นช่องโหว่ของการนำมาซึ่งก่อการร้าย จึงต้องมีการส่งเสริมให้มีการสร้างความเข้าใจที่ถูกต้อง

การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย พบว่า ประเทศไทยมีการตื่นตัวและตระหนักในเรื่องของการต่อต้านการก่อการร้ายทางไซเบอร์แต่มีการดำเนินการแบบแยกส่วน มีการจัดตั้งหน่วยงานที่ตระหนักในความปลอดภัยทางไซเบอร์ สอดคล้องกับ Numfon (2006) ที่วิจัยเรื่อง การจัดตั้งองค์การชำนาญพิเศษเพื่อดำเนินการยุทธศาสตร์ต่อต้านการก่อการร้าย พบว่า เมื่อเกิดเหตุการณ์การก่อการร้ายในประเทศไทยในลักษณะที่มีความรุนแรงรวมถึงการก่อการร้ายรูปแบบใหม่ในอนาคต องค์การต่อต้านการก่อการร้ายจะไม่สามารถจัดการและปัญหาของโครงสร้างขององค์กรคือ องค์การมีสายการบังคับบัญชาและปฏิบัติตามคำสั่งองค์การสูงสุดเหนือขึ้นไป ต้องได้รับการอนุมัติในการเข้าจัดการกับปัญหาทุกครั้งและองค์การมีโครงสร้างหลวม บริหารงานยากขาดเอกภาพในการแก้ปัญหา อำนาจในการตัดสินใจและสั่งการด้านนโยบายไม่มีอิสระ สรุปได้ว่าประเทศไทยให้ความสำคัญต่อการก่อการร้ายในศตวรรษที่ 21 ที่มีความรุนแรงของการก่อการร้ายมากขึ้น โดยแนวทางหรือนโยบายของผู้บริหารที่มีทิศทางของการสร้างการตระหนักรู้ต่อภัยในการโจมตีของไซเบอร์ ประเด็นสำคัญคือ การสร้างความชัดเจนหรือมีนโยบายต่อการดำเนินงานขององค์กรให้มีการดำเนินการไปในทิศทางเดียวกัน ลดปัญหาเรื่องระบบการทำงานที่มีระบบอุปถัมภ์การคอร์รัปชั่น สายการบังคับบัญชาที่มีมากจนเกิดความยุ่งยาก หากลดปัญหาเหล่านี้ได้จะทำให้การทำงานในการป้องกันหรือต่อต้านการก่อการร้ายมีประสิทธิภาพมากที่สุด

ข้อเสนอแนะ

1. รัฐบาลควรให้ความสำคัญกับการสร้างการตระหนักรู้ทางไซเบอร์ให้กับประชาชน เพื่อปลูกฝังให้คนไทยมีความเข้าใจและดำรงชีวิตอย่างปลอดภัยต่อภัยคุกคามทางไซเบอร์ที่จะเกิดขึ้นในอนาคต

2. การกำหนดนโยบายทางการศึกษาการสร้างหรือพัฒนาหลักสูตรทางไซเบอร์ให้กับเยาวชนเพื่อให้เยาวชนสามารถใช้ไซเบอร์ได้อย่างระมัดระวังและไม่ตกเป็นเหยื่อผู้ไม่หวังดีที่จะนำไซเบอร์มาใช้ในการเป็นเครื่องมือในการสร้างอุดมคติที่รุนแรงอันนำไปสู่การก่อการร้ายได้

3. รัฐบาลควรกำหนดนโยบายการวิจัยทางไซเบอร์ในระดับประเทศเพื่อส่งเสริมให้นักวิชาการหรือบุคคลที่มีความสนใจก่อให้เกิดการค้นคว้า การศึกษาการวิจัยทางไซเบอร์ในแง่มุมทางด้านสังคมศาสตร์ พฤติกรรมศาสตร์ และมนุษยศาสตร์ เป็นต้น

4. รัฐบาลมอบหมายให้มีเจ้าภาพรับผิดชอบหลักที่มีการดูแล ป้องกันและต่อต้านภัยคุกคามทางไซเบอร์ที่สามารถดำเนินการในภาพรวมและประสานงานเชื่อมต่อระหว่างหน่วยงานทั้งภาครัฐ ภาคเอกชนและภาคประชาชน เพื่อให้การดำเนินงานในทางไซเบอร์ของประเทศไทยมีประสิทธิภาพ

5. ควรกำหนดกฎหมาย ระเบียบที่เกี่ยวข้องกับการต่อต้านอาชญากรรมและการก่อการร้ายทางไซเบอร์และมีผลบังคับใช้ได้ในทางปฏิบัติ โดยให้ประชาชนเข้ามามีส่วนร่วมในการคิดและตัดสินใจร่วมกันกับภาครัฐ ตลอดจนเพิ่มอำนาจของภาคประชาชนในการร่วมกันป้องกันภัยคุกคามทางไซเบอร์

6. สร้างความร่วมมือระหว่างประเทศทั้งในรูปแบบของทวิภาคีและพหุภาคีของการต่อต้านการก่อการร้ายทางไซเบอร์เพื่อเป็นภูมิคุ้มกันในการป้องกันการก่อการร้ายทางไซเบอร์ที่อาจเกิดขึ้นในประเทศไทยได้อย่างมีประสิทธิภาพ

References

ดุสิต น้ำฝน. (2549). *การจัดตั้งองค์การขำนาญพิเศษเพื่อดำเนินงานยุทธศาสตร์ต่อต้านการก่อการร้าย* (วิทยานิพนธ์ปริญญามหาบัณฑิต). ชลบุรี: มหาวิทยาลัยบูรพา.

กมลนวล ศิลาพันธ์. (2556). *ความชัดเจนและความเหมาะสมในการกำหนดนิยามของการก่อการร้ายในประมวลกฎหมายอาญาของไทย* (วิทยานิพนธ์ปริญญามหาบัณฑิต). กรุงเทพ: มหาวิทยาลัยธุรกิจบัณฑิต.

Facebook statistics Thailand as ASEAN's top three. *BIBLIOGRAPHY \l 1033 (2015).* Retrieved March 15, 2015, from www.it24hrs.com/2015/facebook-population-aec-2o15/.

Gobran, A. (2015). *Cyber Terrorism Threats* (Master's thesis). New York, NY: Utica College.

Kaemkate, W. (2008). *Research Methodology in Behavioral Sciences* (2nd ed.) Bangkok: Chulalongkorn University.

Waters, M. (2001). *Globalization.* London: Routledge.

Transtated Thai References

Numfon, D. (2004). *The Establishment of Specialized Organization for Counter Terrorism in Thailand* (Master's thesis). Chonburi: Burapha University. (in Thai)

Silapun, K. (2013). *The Clarity and Appropriation in the Definition of Terrorism in the Thai Criminal Code* (Master's thesis). Bangkok: Dhurakij Pundit Univerisy. (in Thai)

ผู้เขียน

นางสาวหยาดพิรุณ นาชัยสินธุ์

คณะรัฐศาสตร์และนิติศาสตร์ มหาวิทยาลัยบูรพา

169 ถนนลงหาดบางแสน ตำบลแสนสุข อำเภอเมือง จังหวัดชลบุรี 20131

e-mail: Yard_pirun@hotmail.com