ยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย

หยาดพิรุณ นาชัยสินธุ์

ดุษฎีนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรรัฐศาสตรดุษฎีบัณฑิต
สาขาวิชายุทธศาสตร์และความมั่นคง
คณะรัฐศาสตร์และนิติศาสตร์ มหาวิทยาลัยบูรพา
มิถุนายน2558

อาจารย์ผู้ควบคุมดุษฎีนิพนธ์และคณะกรรมการสอบดุษฎีนิพนธ์ ได้พิจารณาดุษฎีนิพนธ์ของ หยาดพิรุณ นาชัยสินธุ์ ฉบับนี้แล้ว เห็นสมควรรับเป็นส่วนหนึ่งของการศึกษาตามหลักสูตรรัฐศาสตรดุษฎีบัณฑิต สาขาวิชายุทธศาสตร์และความมั่นคง ของมหาวิทยาลัยบูรพาได้

อาจารย์ผู้ควบคุมดุษฎีนิพนธ์

..... อาจารย์ที่ปรึกษา

(รองศาสตราจารย์ ดร.ดำรงค์ วัฒนา)

คณะกรรมการสอบปากเปล่า

..... ประธาน

(ศาสตราจารย์ พันตำรวจเอก หญิง ดร.พัชรา สินลอยมา)

..... กรรมการ

(รองศาสตราจารย์ ดร.ดำรงค์ วัฒนา)

..... กรรมการ

(พันเอก ดร.ธีรนันท์ นันทขว้าง)

..... กรรมการ

(ผู้ช่วยศาสตราจารย์ ว่าที่เรือตรี ดร.เอกวิทย์ มณีธร)

คณะรัฐศาสตร์และนิติศาสตร์ อนุมัติให้รับดุษฎีนิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรรัฐศาสตรดุษฎีบัณฑิต สาขาวิชายุทธศาสตร์และความมั่นคง ของมหาวิทยาลัยบูรพา

..... คณบดีคณะรัฐศาสตร์และนิติศาสตร์

(ผู้ช่วยศาสตราจารย์ ว่าที่เรือตรี ดร.เอกวิทย์ มณีธร)

วันที่ 22 เดือน สิงหาคม พ.ศ. 2559

ประกาศคุณูประการ

ดุษฎีนิพนธ์สำเร็จลงได้ด้วยความกรุณาจาก รองศาสตราจารย์ ดร.ดำรงค์ วัฒนา อาจารย์ที่ปรึกษาหลักและพันเอก ดร.ธีรนันท์ นันทขว้าง อาจารย์ที่ปรึกษาร่วมที่กรุณาให้คำปรึกษาแนะนำแนวทางที่ถูกต้องด้วยความเอาใจใส่ตลอดจนช่วยเหลือผู้วิจัยด้วยดีเสมอมา ผู้วิจัยรู้สึกซาบซึ้งและขอกราบขอบพระคุณเป็นอย่างสูงไว้ ณ. โอกาสนี้

ขอขอบพระคุณ ศาสตราจารย์ พันตำรวจเอกหญิง ดร.พัชรา สินลอยมา ที่กรุณาเป็นประธานสอบดุษฎีนิพนธ์และให้คำแนะนำกับผู้วิจัย ขอบพระคุณ ผู้ช่วยศาสตราจารย์ว่าที่เรือตรี ดร.เอกวิทย์ มณีธร ที่กรุณามาเป็นกรรมการสอบและให้คำแนะนำในการเรียน

ขอขอบพระคุณมหาวิทยาลัยสวนดุสิตที่มอบทุนการศึกษาให้กับผู้วิจัยและขอขอบพระคุณ ดร.สฤษดิ์ ธัญกิจจานุกิจ ผู้อำนวยการศูนย์การศึกษานอกที่ตั้ง ตรังที่คอยส่งเสริมและให้คำแนะนำแนวทางการเรียนควบคู่ไปกับการทำงานจนจบการศึกษา ขอกราบขอบพระคุณผู้ทรงคุณวุฒิทุกท่านที่กรุณาให้ผู้วิจัยได้เข้าสัมภาษณ์และให้ข้อแนะนำจนนำไปสู่ข้อสรุปของผลการวิจัย ขอบคุณผู้ตอบแบบสอบถามที่ให้ความกรุณาตอบแบบสอบถามการในการศึกษาวิจัยซึ่งให้ความร่วมมือเป็นอย่างดีคุณค่าและประโยชน์ของดุษฎีนิพนธ์ฉบับนี้ ผู้วิจัยขอมอบเป็นกตัญญูกตเวทิตาแก่บิดา มารดา บูรพาจารย์และผู้มีพระคุณทุกท่านทั้งในอดีตและปัจจุบันที่ทำให้ผู้วิจัยมีความเพียรพยายามจนจบการศึกษาในปัจจุบัน

หยาดพิรุณ นาชัยสินธุ์

53820020:สาขาวิชา: ยุทธศาสตร์และความมั่นคง; ร.ด. (ยุทธศาสตร์และความมั่นคง)
คำสำคัญ: ยุทธศาสตร์/ก่อการร้าย/ ต่อต้านการก่อการร้าย/ไซเบอร์

หยาดพิรุณ นาชัยสินธุ์: ยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย (STRATEGIES TO COUNTER CYBER TERRORISM IN THAILAND) คณะกรรมการควบคุมดุษฎีนิพนธ์: ดำรงค์ วัฒนา, ปร.ด., ธีรนันท์ นันทขว้าง, ปร.ด. 264หน้าปีพ.ศ.2559.

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อศึกษาความก้าวหน้าทางไซเบอร์ที่มีการนำมาใช้เป็นเครื่องมือทางยุทธศาสตร์ในการก่อการร้ายศึกษาลักษณะการก่อการร้ายโดยใช้ไซเบอร์มาเป็นเครื่องมือทางยุทธศาสตร์ในการก่อการร้ายในประเทศไทยและวิเคราะห์ประเมินการก่อการร้ายทางไซเบอร์ในประเทศไทยโดยใช้การวิเคราะห์จุดแข็ง จุดอ่อน โอกาสและอุปสรรควิธีการวิเคราะห์สถานการณ์และองค์กรแห่งการเรียนรู้ เพื่อพัฒนายุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทยดำเนินการวิจัยด้วยการใช้เทคนิคเดลฟาย สัมภาษณ์เชิงลึกและนำข้อมูลที่ได้มาจัดทำเป็นแบบสอบถามเชิงปริมาณสอบถามกับกลุ่มตัวอย่างจำนวน 690 คน นำข้อมูลที่ได้มาวิเคราะห์ทางสถิติและปรับปรุงเป็นยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ของประเทศไทย ผลการวิจัยปรากฏว่าความก้าวหน้าทางไซเบอร์คือการพัฒนาทางเทคโนโลยีที่สามารถเชื่อมต่อกันได้อย่างรวดเร็วสะดวกขึ้น ทำให้ทุกคนติดต่อกันได้ไม่ว่าจะอยู่ที่ใดในโลกการก่อการร้ายทางไซเบอร์ใช้เครื่องมือทางเทคโนโลยี เช่น โทรศัพท์มือถือ คอมพิวเตอร์ หรือเครื่องมือประเภทอื่น ๆ ที่เชื่อมต่อทางอินเทอร์เน็ตและอินเทอร์เน็ตเป็นช่องทางที่สำคัญที่ใช้ในการก่อการร้าย

การพัฒนายุทธศาสตร์การต่อต้านการก่อการร้ายในประเทศไทย นำเสนอยุทธศาสตร์ในการต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย ดังนี้ ยุทธศาสตร์ READ: CLIP ประกอบด้วย ยุทธศาสตร์ที่ 1 Research ยุทธศาสตร์การเสริมสร้างการวิจัยเพื่อการพัฒนาทางไซเบอร์ ยุทธศาสตร์ที่ 2 Education ยุทธศาสตร์การจัดการศึกษาในการสร้างพื้นฐานของประชาชนในประเทศไทย ยุทธศาสตร์ที่ 3 Awareness ยุทธศาสตร์การสร้างการตระหนักรู้ทางไซเบอร์ให้กับประชาชน ยุทธศาสตร์ที่ 4 Development ยุทธศาสตร์การพัฒนาความก้าวหน้าทางไซเบอร์ ยุทธศาสตร์ที่ 5 Coordinate ยุทธศาสตร์การส่งเสริมความร่วมมือระหว่างภาครัฐ ภาคเอกชน และภาคประชาชนยุทธศาสตร์ที่ 6 Law ยุทธศาสตร์การกำหนดใช้กฎหมายทางไซเบอร์และการบังคับใช้กับประชาชน ยุทธศาสตร์ที่ 7 Integration ยุทธศาสตร์การใช้บูรณาการร่วมกันเพื่อแบ่งปันข้อมูล และยุทธศาสตร์ที่ 8 Perception Prepares and Protect ยุทธศาสตร์การรับรู้ทางไซเบอร์ร่วมกันตระเตรียมและปกป้องทางไซเบอร์

53820020:MAJOR: STRATEGY AND SECURITY; D.POL.SC
(STRATEGY AND SECURITY)
KEYWORDS: STRATEGY/ TERRORISM /COUNTER TERRORISM / CYBER
YARDPIRUN NACHAISIN: STRATEGIES TOCOUNTER CYBERTERRORISM IN THAILAND.ADVISORY COMMITTEE: DAMRONG WATTANA, Ph.D., TEERANAN NANDHANKWANG, Ph.D., 264P. 2016

This research aimed to 1. To study the cyber development that is applied as a strategy tool of cyber terrorism in Thailand. 2.To examine terrorism characteristics that uses cyber as a strategy tool of cyber terrorism in Thailand and assess cyber terrorism in Thailand using strength, weakness, opportunity and How to analyze the situation and the organization of learning. 3. To develop strategies to counter terrorism in Thailand. Research conducted using the Delphi technique Depth interviews and survey data were prepared in quantitative. The questionnaire was applied to the sample of 690 persons. The collected data was analyzed statistically and developed into the strategies to counter cyber terrorism in Thailand. The results are as follows. The cyber development is the technology development that can be connected faster and more convenience than before. This made people can communicate with each other no matter where they are in the world. The cyber terrorism is the implementation of technology tools, such as mobile phone, computer or other tools that connected through internet. READ: CLIP Strategy comprises of 8 strategies as follows. 1.Research is the strategy that promotes the cyber development research. 2. Education is the strategy to arrange basic education of 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. Coordinate is the strategy that promotes the cooperation of government, private and public sectors. 6. Law is the strategy that specifies cyber law and enforces with people.7. Integration is the strategy of integration to share data. Lastly,8. Perception Prepares and Protect is the strategy to perceive, prepare and protect the cyber together.

สารบัญ

สารบัญ(ต่อ)

สารบัญ (ต่อ)

สารบัญตาราง

ตารางที่ หน้า

สารบัญภาพ

ภาพที่ หน้า

บทที่ 1
บทนำ

ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันโลกก้าวเข้าสู่ยุคโลกาภิวัตน์ในศตวรรษที่ 21 อินเทอร์เน็ตนับได้ว่ามีบทบาทสำคัญต่อการดำรงชีวิตของประชาชน อินเทอร์เน็ตเป็นปัจจัยสำคัญที่ทำให้เกิดการเชื่อมต่อกันทั่วโลกและเป็นปรากฏการณ์ในการเชื่อมโยงข้อมูลข่าวสารของคนทั้งประเทศเข้าด้วยกันโดยได้รับข่าวสารเนื้อหาเดียวกันรวมถึงการนำมาเพิ่มประสิทธิภาพในการทำงาน การสื่อสารแลกเปลี่ยนข้อมูลสามารถทำได้สะดวก รวดเร็ว ค่าใช้จ่ายน้อยและไม่มีข้อจำกัดในเรื่องของปัจจัยทางกายภาพ กล่าวได้ว่า อินเทอร์เน็ตส่งผลให้เกิดการเปลี่ยนแปลงทาง สังคม เศรษฐกิจและทางการเมือง อย่างมาก สิ่งสำคัญที่สุดในศตวรรษนี้คือ โลกของสารสนเทศ จนกลายเป็นปรากฏการณ์ในมิติของการสร้างระบบเครือข่ายทางสังคมหรือที่เรียกกันว่า สังคมออนไลน์ ประเทศไทยมีปรากฏการณ์ที่เกิดขึ้นจากสังคมออนไลน์ซึ่งก่อประโยชน์ในหลายๆด้าน ทำให้การเติบโตของอินเทอร์เน็ตขยายตัวไปและการใช้เทคโนโลยีสารสนเทศในประเทศไทยที่ได้รับความนิยมในปัจจุบันคือเฟซบุ๊ก (Facebook statistics Thailand as ASEAN's top three, 2015) จากสถิติล่าสุดวันที่ 17เมษายน 2015 ผลสำรวจพบว่า ประเทศไทยมีประชากรที่ใช้เฟซบุ๊กมากเป็นอันดับ 3 ของอาเซียนอยู่ที่ 35 ล้านบัญชี การใช้เฟซบุ๊กเติบโตขึ้น 34.62 เปอร์เซ็นต์ ทั้งนี้ไทยมียอดเติบโตของผู้ใช้เฟซบุ๊กมากเป็นอันดับที่ 5 ของอาเซียนจากกระแสความตื่นตัวทางเทคโนโลยีสารสนเทศและความนิยมในการใช้ไซเบอร์ส่งผลให้เกิดการเปลี่ยนแปลงทางสังคม เศรษฐกิจและการเมืองอย่างรวดเร็ว ถึงแม้ว่าไซเบอร์จะทำให้เกิดประโยชน์อย่างมหาศาลแก่มนุษย์ แต่หากมนุษย์ใช้ไซเบอร์ไปในทางที่ไม่ถูกต้องนำไปเป็นเครื่องมือเพื่อวัตถุประสงค์บางประเภท เช่น การนำไปปลุกระดมมวลชน การชักจูงหรือเผยแพร่ข่าวสารทั้งในทางที่ถูกและที่ผิด นำไปก่อการร้าย เป็นต้น อาจก่อให้เกิดความเสียหายอย่างมากได้เช่นกัน

ความเป็นมาของการก่อการร้ายได้เริ่มเกิดขึ้นนับจากศตวรรษแรกและดำเนินมาจนถึงปัจจุบันซึ่งการก่อการร้ายได้พัฒนาความรุนแรงและขยายวงกว้างมากอย่างเห็นได้ชัดโดยส่วนใหญ่แล้วมีความเกี่ยวเนื่องกับประเด็นทางการเมือง ในปัจจุบันเมื่อก้าวเข้าสู่ศตวรรษที่ 21 จากการเกิดเหตุการณ์วินาศกรรมในประเทศสหรัฐอเมริกา การก่อการร้ายยิ่งทวีความรุนแรง น่าสะพรึงกลัวและซับซ้อน มีลักษณะกระจายตัวเป็นเครือข่ายปฏิบัติงานเชื่อมโยงตามพื้นที่ในภูมิภาคต่าง ๆ ทั่ว

โลกจนยากแก่การป้องกันและปราบปรามมากขึ้น เช่นการปฏิบัติการก่อการร้ายของกลุ่มอัลกออิดะห์ (Al – Qaida) (ดลยา เทียนทอง, 2549)

ประเทศสหรัฐอเมริกา ซึ่งเป็นมหาอำนาจของโลก มีเหตุการณ์ที่สำคัญให้คนทั้งโลกได้ตะลึงและจดจำเรื่องราวแม้จะผ่านมา 13ปี แล้วก็ตาม จากผู้ก่อการร้าย 19 คนจากกลุ่มอิสลามหัวรุนแรงอัลกออิดะจี้อากาศยานโดยสารสี่ลำ โจรจี้เครื่องบินนำเครื่องบินทั้งสองพุ่งชนกับตึกแฝดเวิลด์เทรดเซ็นเตอร์ในนครนิวยอร์กโดยเจตนาและอาคารทั้งสองถล่มลงภายในสองชั่วโมงโจรจี้เครื่องบินชนเครื่องบินลำที่สามกับอาคารเพนตากอนในอาร์ลิงตัน รัฐเวอร์จิเนียส่วนเครื่องบินยูไนเต็ดแอร์ไลน์เที่ยวบินที่ 93 ตกในทุ่งใกล้กับแชงค์วิลล์รัฐเพนซิลเวเนียก่อนจะถึงเป้าหมายที่โจรจี้เครื่องบินต้องการพุ่งชนอาคารรัฐสภาสหรัฐ มีผู้เสียชีวิตเกือบ 3,000 คนในเหตุโจมตีดังกล่าวและไม่มีผู้รอดชีวิตจากเครื่องบินทั้งสี่ลำ (วินาศกรรม 11 กันยายน 2544, 2554)การเกิดเหตุการณ์สะเทือนขวัญในครั้งนี้ได้เกิดขึ้นและมีการขยายผลไปทั่วโลกอีกทั้งประเทศต่าง ๆ ทั่วโลกได้มีการพัฒนาทางเทคโนโลยีในทุกด้านไม่ว่าจะเป็นด้านการขนส่งเช่น การขนส่งทางอากาศ ทางทะเลและเทคโนโลยีสารสนเทศและการสื่อสาร เช่น อินเทอร์เน็ต เป็นต้น ส่งผลให้โลกเชื่อมต่อกันอย่างสมบูรณ์ข้อมูลข่าวสารสามารถกระจายส่งต่อกันได้อย่างรวดเร็วจนทำให้โลกวิ่งเข้าสู่ยุคโลกาภิวัตน์ (Globalization) จึงทำให้ภัยคุกคามของโลกได้เปลี่ยนไปโดยมิใช่ภัยคุกคามที่สามารถแก้ปัญหาได้ด้วยการใช้กำลังทางทหารเพียงอย่างเดียวได้อีกต่อไป แต่กลับกลายเป็นภัยคุกคามที่เราเรียกว่าภัยคุกคามรูปแบบใหม่ (Non-traditional threat) ซึ่งต้องใช้การบูรณาการทรัพยากรมนุษย์และเทคโนโลยีอย่างชาญฉลาดอีกทั้งต้องมีความร่วมมือระดับนานาชาติกับมิตรประเทศจึงจะสามารถแก้ปัญหาได้

ตารางที่ 1 ข้อมูลแรงจูงใจหลักที่อยู่เบื้องหลังการโจมตีทางไซเบอร์(The Major Motivation behind Cyber Attacks, 2014)

The Major Motivation behindCyber Attacks	
Hacktivism*	50%
Cyber Crime	40%
Cyber Espionage	7%
Cyber Warfare	3%

หมายเหตุ *Hacktivism is the use of computers and computer networks to promote political ends, chiefly free speech, human rights, and information ethics

แสดงให้เห็นจากข้อมูลแรงจูงใจหลักที่อยู่เบื้องหลังการโจมตีทางไซเบอร์พบว่า การบุกรุกเข้าไปในระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต ร้อยละ 50 อาชญากรรมทางไซเบอร์ ร้อยละ 40 จารกรรมทางไซเบอร์ ร้อยละ 7และสงครามทางไซเบอร์ ร้อยละ 3

ปัญหาการก่อการร้ายในยุคโลกาภิวัตน์(Globalization) เป็นปัญหาที่คุกคามประชาชนทั่วโลกและประเทศที่พัฒนาแล้วประเทศต่าง ๆ ตื่นตัวต่อภัยคุกคามในรูปแบบใหม่ที่เรียกได้ว่าเป็นการก่อการร้ายที่เป็นภัยต่อประชาคมระหว่างประเทศ แม้ประเทศไทยจะยังคงมีความห่างไกลในการก่อการร้ายระหว่างประเทศแต่สิ่งที่พึงระวังไว้เนื่องจากสถานการณ์หลาย ๆ อย่างที่เกิดขึ้นในประเทศปัจจุบันนำมาซึ่งความเสียหายและทำลายระบบความมั่นคงของประเทศ การก่อการร้ายระหว่างประเทศ เป็นภัยคุกคามที่ร้ายแรงต่อประชาคมระหว่างประเทศ โดยมีแนวโน้มจะขยายขอบเขตและระดับความรุนแรงยิ่งขึ้นจากเดิม ซึ่งเป็นการต่อสู้ด้วยการใช้กำลัง เนื่องจากความขัดแย้งทางความคิด อุดมการณ์ เชื้อชาติ ศาสนา ผลประโยชน์ ทั้งภายในและภายนอกประเทศ มาเป็นการแย่งชิงข้อมูลข่าวสาร การรับจ้างก่อการร้ายสากลโดยอาศัยเครือข่ายอินเทอร์เน็ต การเสริมสร้างอานุภาพทางการทหารเพื่อข่มขวัญและการต่อสู้แย่งชิง แสวงผลประโยชน์ทางเศรษฐกิจ กลุ่มเชื้อชาติ หรือกลุ่มศาสนา ทั้งนี้ประเทศที่เป็นกลุ่มมุสลิมหัวรุนแรงปฏิบัติการก่อการร้ายในลักษณะข้ามชาติมากขึ้น โดยมิได้จำกัดเฉพาะเป้าหมายที่เป็นประเทศตะวันตก โดยเฉพาะอย่างยิ่งสหรัฐอเมริกาและประเทศกลุ่มพันธมิตร รวมทั้งอิสราเอลและชนชาติยิวทั่วโลก แต่ขยายการโจมตีทุกเป้าหมาย นอกจากนี้ยังมีความพยายามนำอาวุธที่มีอำนาจทำลายล้างสูง (Mass – destructive weapons –MDW) อาทิ อาวุธเคมีชีวภาพ และอาวุธนิวเคลียร์ เข้ามาใช้ในการก่อการร้ายระหว่างประเทศเพิ่มขึ้น ประกอบกับการใช้คอมพิวเตอร์เป็นอาวุธในการทำลายระบบสื่อสารคมนาคม และบริการทางธุรกิจด้านอิเล็กทรอนิกส์อื่น ๆ

ตารางที่ 2 ข้อมูลทางสถิติการฝ่าฝืนกฎหมายทางเครือข่ายคอมพิวเตอร์ในอุตสาหกรรม(The Major Motivation behind Cyber Attacks, 2014)

Data Breach Statistics by Industry

Industry	%
Medical/Healthcare	38.9
Business	35.1
Educational	10.7
Government/Military	9.9
Banking/Credit/Financial	5.3

จากข้อมูลในเว็บไซต์(Data Breach Statisics by Industry, 2013) พบว่า ข้อมูลทางสถิติการฝ่าฝืนกฎหมายทางเครือข่ายคอมพิวเตอร์ในอุตสาหกรรม ประกอบด้วย ทางการแพทย์/สุขภาพ ร้อยละ 38.9 ทางธุรกิจ ร้อยละ 35.1 ทางการศึกษา ร้อยละ 10.7 ทางการปกครอง/ทหาร ร้อยละ 9.9 และทางธนาคาร/ บัตรเครดิต/การเงินร้อยละ 5.3

จากสถานการณ์บ้านเมืองของประเทศไทย ตั้งแต่ปี 2548 ถึงปัจจุบัน จะเห็นได้อย่างชัดเจนว่าบทบาทของไซเบอร์มีผลต่อระบบสถาบันทางการเมือง มีปัญหาอันเกิดจากความไม่เชื่อมั่นและความแตกแยกจากคนในชาติสูง ผ่านตัวแทนของกลุ่มต่างๆ ซึ่งส่งผลให้สถาบันการเมืองไร้เสถียรภาพทางด้านความมั่นคง โดยกลุ่มต่างๆ ได้ใช้ช่องทางของสื่อสังคมออนไลน์ ปลุกเร้ามวลชนเพื่อการตอบโต้และบ่อนทำลายฝ่ายตรงกันข้ามหรือบั่นทอนความเชื่อมั่นทางสถาบันความมั่นคงของประเทศ โดยลักษณะของสื่อสังคมออนไลน์ที่ใช้เป็นช่องทางโจมตีหรือชักจูงเพื่อสร้างแรงจูงใจให้ประชาชน เช่น การแสดความคิดเห็นใน ยูทูบเฟซบุ๊ก ทวิสเตอร์ ไลน์และสื่อดั้งเดิม เช่น หนังสือพิมพ์ วิทยุชุมชน โทรทัศน์ เป็นต้น

ในช่วงที่อินเทอร์เน็ตเกิดการแพร่หลายในประเทศไทย ความน่าสนใจเกิดจากการเริ่มมีการเคลื่อนไหวเพื่อต่อต้านนายกรัฐมนตรี พ.ต.ท.ทักษิณ ชินวัตร โดยกลุ่มพันธมิตรเพื่อประชาธิปไตยเป็นแกนหรือเรียกอีกอยางว่ากลุ่มคนเสื้อเหลืองทำให้เกิดการวิพากษ์วิจารณ์และการสนทนาในประเด็นทางการเมืองมากขึ้น การต่อต้านมีความชัดเจนมากขึ้นเมื่อเว็บไซต์ผู้จัดการออนไลน์กลายมาเป็นเว็บไซต์ที่มีการรณรงค์ทางการเมืองและเป็นช่องทางการสื่อสารหลักของกลุ่มพันธมิตรเพื่อประชาชน ควบคู่ไปกับสถานีโทรทัศน์ผ่านดาวเทียมและยังมีฝ่ายที่สนับสนุน พ.ต.ท.ทักษิณ ด้วยการเปิดเว็บไซต์มากมาย ภายหลังจากมีการปฏิวัติรัฐประหาร รัฐบาลทหารของพล.อ.สุรยุทธ์ จุลานนท์ ได้ตอบโต้ด้วยมาตรการปิดกั้นสื่อออนไลน์ ทั้งการใช้การประกาศผ่านคณะรัฐประหารได้มีการตอบโต้ด้วยมาตรการปิดกั้นสื่อออนไลน์ ในปี 2553 รัฐบาลที่มีนายอภิสิทธิ์ เวชชาชีวะ เป็นนายกรัฐมนตรี ยังได้บังคับใช้พระราชกำหนดบริหารราชการในสถานการณ์ฉุกเฉินเพื่อปิดเว็บไซต์วิทยุชุมชน เคเบิลทีวี ในระหว่างการชุมชุมของคนเสื้อแดงเพื่อเรียกร้องให้นายกรัฐมนตรียุบสภา จากสถานการณ์ทางการเมืองที่มีความขัดแย้งทางการเมืองนี้ บริการเครือข่ายสังคมออนไลน์ โดยบริการที่ได้รับความนิยมในประเทศไทย ได้แก่ ทวิตเตอร์และเฟซบุ๊ก การนำทวิตเตอร์มาเป็นเครื่องมือที่สำคัญในการรายงานข่าวจากพื้นที่การชุมนุมที่นักข่าวหรือผู้ที่อยู่ในเหตุการณ์ใช้อุปกรณ์การถ่ายทอดสดเข้าไปไม่ถึง โดยมีนักข่าวภาคสนามได้ใช้โทรศัพท์มือถือถ่ายภาพและรายงานสถานการณ์ชุมนุมจากพื้นที่ชั้นในของกรุงเทพฯผ่านทางอินเทอร์เน็ตรวมถึงการแสดงวิดีโอสั้นผ่านยูทูบและเฟซบุ๊กเป็นหลักฐานแสดงความชอบธรรมของฝ่ายต่างๆ ส่วนเฟซบุ๊กเริ่มได้รับความนิยมสำหรับการใช้งานทางการเมืองเช่น การประกาศเพื่อแจ้งข่าวการรวมมวลชน หรือในช่วงของการ

ชุมนุมมีปรากฏการณ์ของการรวมกลุ่มกันของผู้ใช้เฟซบุ๊กเพื่อสนับสนุนหรือต่อต้านรัฐบาลโดยกลุ่มผู้สนับสนุนรัฐบาลได้นำข้อความของผู้ต่อต้านรัฐบาลมาประจานหรือเป็นหลักฐานส่งให้เจ้าหน้าที่ตำรวจในข้อหาหมิ่นพระบรมเดชานุภาพจากเหตุการณ์ที่เป็นส่วนหนึ่งของสถานการณ์ทางการเมืองจะเห็นได้ว่า ประเทศไทยเปิดโอกาสให้ไซเบอร์เข้ามามีบทบาทต่อการดำรงชีวิตและเป็นส่วนหนึ่งของการเป็นเครื่องมือในการก่อให้เกิดความคิด ความเข้าใจที่สามารถเป็นได้ทั้งในทางที่ถูกและผิด เมื่อไซเบอร์เป็นเครื่องมือที่สำคัญของการทำความเข้าใจทางการเมืองโดยไม่ได้ผ่านกระบวนการกลั่นกรองหรือสืบหาข้อเท็จจริง ก็นำมาซึ่งความขัดแย้งของคนในประเทศและเป็นช่องทางของการก่อการร้ายของผู้ก่อการร้ายทั้งภายในประเทศและการก่อการร้ายข้ามชาติ

สำหรับประเทศไทยแม้ไม่ได้เกี่ยวข้องโดยตรงกับปัญหาและความขัดแย้งต่าง ๆ ที่เป็นสาเหตุของการก่อการร้ายแต่ก็ได้รับผลจากความขัดแย้งเนื่องจากมีความสัมพันธ์ทางการทูตกับประเทศที่เป็นเป้าหมายการก่อการร้าย เช่น สหรัฐฯ อิสราเอล ประเทศอาหรับสายกลาง อินเดีย ปากีสถาน รวมทั้งเป็นที่ตั้งของชุมชนและผลประโยชน์ของประเทศเหล่านั้น เช่น สถานเอกอัครราชทูต สถานกงสุล สำนักงานการค้า สำนักงานสายการบิน เครื่องบินโดยสารบริษัทและห้างร้านต่าง ๆ ซึ่งเป็นสิ่งจูงใจสำคัญที่เชื่อมโยงให้กลุ่มก่อการร้ายระหว่างประเทศเข้ามาปฏิบัติการในประเทศ ปัจจุบันไทยเป็นแหล่งหลบซ่อน ที่ติดต่อ จุดพักเพื่อเตรียมการ แหล่งสนับสนุน และจุดฝังตัวและต่อต้านของผู้ก่อการร้าย เพื่อปฏิบัติการในประเทศที่สาม นอกจากนี้ ยังเป็นตลาดซื้อขายอาวุธสงครามให้แก่กลุ่มก่อการร้ายในภูมิภาคเอเชียแปซิฟิก จึงทำให้โอกาสที่จะมีการก่อการร้ายเกิดขึ้นในไทยได้ทุกเมื่อ

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งมีหน้าที่ในการรับผิดชอบการจัดทำแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร (ฉบับที่ 3) ของประเทศไทย พ.ศ.2557 – 2561 โดยมีความต่อเนื่องจากแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารแห่งประเทศไทย (ฉบับที่ 2) ของประเทศไทย พ.ศ.2552 – 2556กำหนดให้มียุทธศาสตร์ 4 ด้าน คือ การพัฒนาทุนมนุษย์ให้เป็นกำลังในการพัฒนาเทคโนโลยีสารสนเทศของประเทศไทยและมีความพร้อมในการมีส่วนร่วมในการพัฒนา การพัฒนาโครงสร้างพื้นฐานที่คุ้มค่าและพอเพียง การพัฒนาระบบบริการของภาครัฐอย่างชาญฉลาดและการพัฒนาภาคธุรกิจและอุตสาหกรรมเทคโนโลยีสารสนเทศให้เติบโต จะเห็นได้ว่าความพร้อมของประเทศไทยต่อการพัฒนาทางเทคโนโลยีสารสนเทศให้มีความทันสมัยและก้าวทันต่อการเปลี่ยนแปลงของโลกอย่างต่อเนื่องแต่ขณะเดียวกันก็อาจเป็นภัยคุกคามอันเกิดจากการใช้เทคโนโลยีที่ไม่เหมาะสมเพิ่มขึ้นด้วย เช่น การเกิดปัญหาอาชญากรรมรูปแบบใหม่ การละเมิดทรัพย์สินทางปัญญา เทคโนโลยีทำให้คนมีพฤติกรรมเบี่ยงเบนทางสังคม การละเมิดข้อมูล

ส่วนบุคคล การนำข้อมูลส่วนบุคคลของผู้อื่นไปหาประโยชน์ การเข้าถึงสื่อลามกของเยาวชน การก่อการร้ายและการก่อการร้ายข้ามชาติ เป็นต้น

ปัจจุบันเครือข่ายอินเทอร์เน็ตหรือที่เรียกทั่วไปว่า ไซเบอร์สเปซ (Cyberspace) ที่ใช้กันอยู่แพร่หลายถูกนำมาประยุกต์ใช้งานอย่างกว้างขวาง ผู้ก่อการร้ายหรืออาชญากรก็พยายามแสวงประโยชน์จากเครือข่ายอินเตอร์เน็ตด้วย ภัยคุกคามที่อาจเกิดขึ้นจากการใช้อินเตอร์เน็ต เช่น การขัดจังหวะ การสกัดและคัดลอก การแก้ไขและเปลี่ยนแปลง และการปลอมแปลง เป็นต้น ส่วนการคุกคามทางอินเทอร์เน็ต มีหลายวิธี เช่น แฮกเกอร์คือผู้ที่บุกรุกเข้าไปในเครือข่ายคอมพิวเตอร์ของผู้อื่น โดยที่ตนเองไม่มีสิทธิ์ เพื่อลักลอบดูข้อมูล ดัดแปลงแก้ไขข้อมูล ประกอบอาชญากรรมฉ้อโกงทางการเงิน ทำจารกรรมล้วงความลับทางการค้า อุตสาหกรรม และข้อมูลทางการวิจัย ทำให้มีการส่งข่าวสารผิดไปยังผู้ปลอมแปลงการโจมตีอีเมล์เป็นการส่งข่าวสารจำนวนมหาศาลเข้าไป ทำให้อีเมล์ใช้ไม่ได้ รวมถึงการปลอมอีเมล์ของผู้อื่นและปลอมแปลงข่าวสารอีกทั้งการส่งไวรัสโจมตีและก่อกวนเครือข่ายคอมพิวเตอร์ของผู้อื่น ทำให้ข้อมูลของผู้อื่นเสียหาย เป็นต้น การก่อการร้ายยุคใหม่ได้เปลี่ยนแปลงเป้าหมายการโจมตีจากเป้าหมายเดิมที่เรียกว่า เป้าหมายแข็ง (Hard targets)เช่น ค่ายทหาร หรือสถานที่ทำการของรัฐบาลของแต่ละประเทศยังได้ขยายการโจมตีไปยัง เป้าหมายอ่อน (Soft targets) เช่น ภัตตาคาร สถานบันเทิง โรงละคร ทั้งนี้เนื่องจากเป้าหมายเหล่านี้จะไม่มีการป้องกันหรือมีการป้องกันเพียงเล็กน้อย จึงมีการลงมือปฏิบัติการได้ง่ายและมีผู้คนจำนวนมากส่งผลให้เกิดการบาดเจ็บหรือเสียชีวิต

ประเทศไทยมีสถานการณ์ที่สำคัญที่เกิดจากใช้การก่อการร้าย เช่น กรณีระเบิดบริษัท เอ.อี. นานา การปล้นยึดเครื่องบินจากไทยไปแอลจีเรีย กรณีลอบสังหารนักการทูตซาอุดีอาระเบีย กรณีนักศึกษาพม่าปล้นยึดเครื่องบินมาลงในไทย กรณีพยายามลอบวางระเบิดซีโฟร์ในไทย เป็นต้น จะเห็นได้ว่าการก่อการร้ายระหว่างประเทศโดยมีการก่อการร้ายทางคอมพิวเตอร์สนับสนุนเป็นปฏิบัติการที่เป็นภัยคุกคามต่อความมั่นคงปลอดภัย และความสงบสุขของประชาคมระหว่างประเทศ อีกทั้งหากกลุ่มก่อการร้ายระหว่างประเทศเข้ามาปฏิบัติการภายในประเทศไทย ก็ย่อมจะส่งผลเสียกระทบโดยตรงต่อผลประโยชน์ของชาติ พันธกรณีระหว่างประเทศ นโยบายของชาติ ทั้งด้านการเมืองและการป้องกันประเทศ เศรษฐกิจ และสังคมจิตวิทยา รวมทั้งชื่อเสียงและเกียรติภูมิของชาติ นอกจากนี้ การก่อการร้ายระหว่างประเทศโดยมีการก่อการร้ายสนับสนุนยังเกิดขึ้นอย่างต่อเนื่อง กลุ่มก่อการร้ายก็ยังคงเคลื่อนไหวตลอดมาโดยมีศักยภาพที่จะปฏิบัติการได้ทุกขณะ ขึ้นอยู่กับสถานการณ์ เงื่อนไขและโอกาส ตลอดจนความบกพร่องของระบบการรักษาความปลอดภัยในแต่ละสถานที่จะเอื้ออำนวยให้ปฏิบัติการ ในปี 2556 ไทยเซิร์ตได้รับแจ้งเหตุภัยคุกคามผ่านระบบอัตโนมัติเพิ่มเติมจากปี 2555 ข้อมูลภัยคุกคามบอตเน็ตและรายงานระบบเว็บไซต์ที่ถูกเจาะระบบ

สำเร็จ ทำให้ไทยเซิร์ตสามารถวิเคราะห์ข้อมูลเกี่ยวกับสถานการณ์ภัยคุกคามของเครือข่ายระบบอินเทอร์เน็ตภายในประเทศได้ครอบคลุมและแม่นยำมากขึ้น รายงานภัยคุกคามที่ได้รับมากที่สุดผ่านระบบอัตโนมัติ เป็นภัยคุกคามประเภทบอตเน็ตโดยมีจำนวนถึง 41,046,337 รายการคิดเป็นหมายเลขไอพีที่ไม่ซ้ำกันถึง 2,829,348 หมายเลข รองลงมาคือ Open DNS Resolver และสแปม มีจำนวนหมายเลขไอพีที่ไม่ซ้ำกัน 1,695,783 และ 848,976 หมายเลขตามลำดับ(ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย, 2556) นอกจากนั้นประเทศไทยยังมีภัยคุกคามในกรณีอื่น ๆ เช่น การโจมตีเว็บไซต์ของหน่วยงานสำคัญ การโจมตีของผู้ใช้งานระบบอัตโนมัติของธนาคารไทย และการตรวจพบช่องโหว่ของแอพลิเคชั่นการสนทนาระหว่างกันซึ่งมีผู้ใช้งานในประเทศไทยเป็นจำนวนมาก

จากแนวคิดดังกล่าวนำมาสู่การพัฒนายุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ ซึ่งเป็นการก่อการร้ายที่นำไซเบอร์มาทำลายหรือสร้างความเสียหายต่อประเทศและส่งผลต่อความมั่นคงแห่งชาติ ประเทศไทยมีการพัฒนาและใช้เทคโนโลยีสารสนเทศในการขับเคลื่อนประเทศให้ก้าวหน้าเข้าสู่การเป็นประชาคมอาเซียนและการพัฒนาทางไซเบอร์ที่มีมากขึ้นเป็นเป้าหมายที่สำคัญของการก่อการร้ายทั้งในประเทศและการก่อการร้ายข้ามชาติ ด้วยเหตุนี้ผู้วิจัยตระหนักว่าประเทศไทยต้องให้ความสำคัญและเข้าใจถึงปัญหาจากการใช้ไซเบอร์และการนำไซเบอร์เป็นเครื่องมือในการก่อการร้าย อีกทั้งสถานการณ์ความมั่นคงทางไซเบอร์และความเสี่ยงอันอาจจะเกิดขึ้นได้ทุกเมื่อจึงมีความจำเป็นที่ต้องกำหนดยุทธศาสตร์การต่อต้านการก่อการร้ายโดยใช้ไซเบอร์ของประเทศไทย

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาความก้าวหน้าทางไซเบอร์ที่มีการนำมาใช้เป็นเครื่องมือทางยุทธศาสตร์ในการก่อการร้ายในประเทศไทย

2. เพื่อศึกษาลักษณะการก่อการร้ายโดยใช้ไซเบอร์มาเป็นเครื่องมือทางยุทธศาสตร์ในการก่อการร้ายของประเทศไทยและวิเคราะห์ประเมินการก่อการร้ายทางไซเบอร์ในประเทศไทยโดยใช้การวิเคราะห์จุดแข็ง จุดอ่อน โอกาสและอุปสรรควิธีการวิเคราะห์สถานการณ์และองค์กรแห่งการเรียนรู้

3. เพื่อพัฒนายุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย

สมมติฐานของการวิจัย

1. การก่อการร้ายที่มีการใช้เทคโนโลยีความก้าวหน้าสูงเทียบเท่ากับความก้าวหน้าทางไซเบอร์จะฉวยโอกาสนำความก้าวหน้าทางไซเบอร์เพื่อมาใช้ประโยชน์ในการก่อการร้ายอย่างมีนัยสำคัญ

2. ประเทศไทยมีความล้าหลังกว่าผู้ใช้ยุทธศาสตร์การก่อการร้ายแนวทางการพัฒนาหรือการต่อต้านการก่อการร้ายเป็นการแก้ไขมากกว่าการป้องกัน การจัดการปัญหาการก่อการร้ายควรแตกต่าง เพื่อจัดทำยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย

3. การวิเคราะห์หรือประเมินการก่อการร้ายเครื่องมือที่ใช้ต้องมีวิธีการเรียนรู้ที่สะท้อนในรูปแบบเชิงความคิดที่ต่อต้านหรือป้องกันการก่อการร้ายได้

ขอบเขตของการวิจัย

1. ผู้วิจัยได้ศึกษาความก้าวหน้าทางไซเบอร์ลักษณะการก่อการร้าย การก่อการร้ายทางไซเบอร์ ยุทธศาสตร์ นโยบายและการดำเนินการตามนโยบาย การดำเนินการต่อต้านการก่อการร้ายทางไซเบอร์ การกำหนดยุทธศาสตร์ที่เหมาะสมต่อความมั่นคงทางไซเบอร์ทั้งในประเทศและต่างประเทศ

2. ผู้วิจัยกำหนดกลุ่มของผู้เชี่ยวชาญโดยคัดเลือกจากผู้ที่ปฏิบัติงานในหน่วยงานที่เกี่ยวข้องกับการดำเนินการกำหนดยุทธศาสตร์ การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย โดยมีหลักของการคัดเลือกจาก(Lincoln &Guba1985)กล่าวว่าการเลือกตัวอย่างที่ครอบคลุมความหลากหลายในประชากรให้ได้มากที่สุดนั้น เป็นวิธีการเลือกตัวอย่างที่ดีที่สุด เนื่องจากลักษณะที่เกิดร่วมกันจากความหลากหลายของกลุ่มตัวอย่างเป็นสิ่งที่น่าสนใจและมีคุณค่าต่อการวิจัยเป็นอย่างยิ่ง ซึ่งสามารถบ่งชี้รูปแบบที่สามารถเกิดขึ้นได้เหมือนกันจากตัวอย่างซึ่งมีลักษณะต่างกันในกลุ่มที่ศึกษาได้ (วรรณี แกมเกตุ,2551)มีจำนวนทั้งสิ้น 10 คนโดยแบ่งออกเป็น 2 กลุ่ม กลุ่มแรกได้แก่ ผู้ที่มีบทบาทหรือส่วนเกี่ยวข้องกับการดำเนินการหรือการพัฒนาทางไซเบอร์และใช้การพัฒนาทาง

ไซเบอร์มาเป็นเครื่องมือในการดำเนินการพัฒนาในประเทศไทยจำนวน 4 คน กลุ่มที่สองได้แก่ ผู้ที่มีความรู้ความเชี่ยวชาญในส่วนของการกำหนดยุทธศาสตร์ทางเทคโนโลยีสารสนเทศในส่วนของภาครัฐ จำนวน 6 คน ประกอบด้วยกระทรวงเทคโนโลยีและสารสนเทศจำนวน 2 ท่าน หน่วยงานความมั่นคงแห่งชาติ 1 ท่าน สำนักงานตำรวจแห่งชาติ 2ท่าน และกองทัพไทย 1 ท่าน

3.ขอบเขตด้านเวลา

การวิจัยเรื่อง เรื่องยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย ใช้เวลา 1 ปี

คำจำกัดความที่ใช้ในการวิจัย

ยุทธศาสตร์ หมายถึง การใช้เครื่องมือที่เป็นพลังอำนาจแห่งชาติทุกๆด้าน เพื่อให้บรรลุวัตถุประสงค์หลักของชาติหรือผลประโยชน์ของชาติในแนวทางที่เหมาะสม

ก่อการร้าย หมายถึง การใช้กำลังหรือความรุนแรงกระทำต่อบุคคล ทรัพย์สิน โดยละเมิดต่อกฎหมายของประเทศที่ตกเป็นเป้าหมาย ด้วยวัตถุประสงค์เพื่อการข่มขู่ การใช้อำนาจบังคับ เป็นการข่มขวัญ สร้างความหวาดกลัวให้กับประชาชนผู้บริสุทธิ์ให้บรรลุวัตถุประสงค์ทางการเมืองตามที่ต้องการ

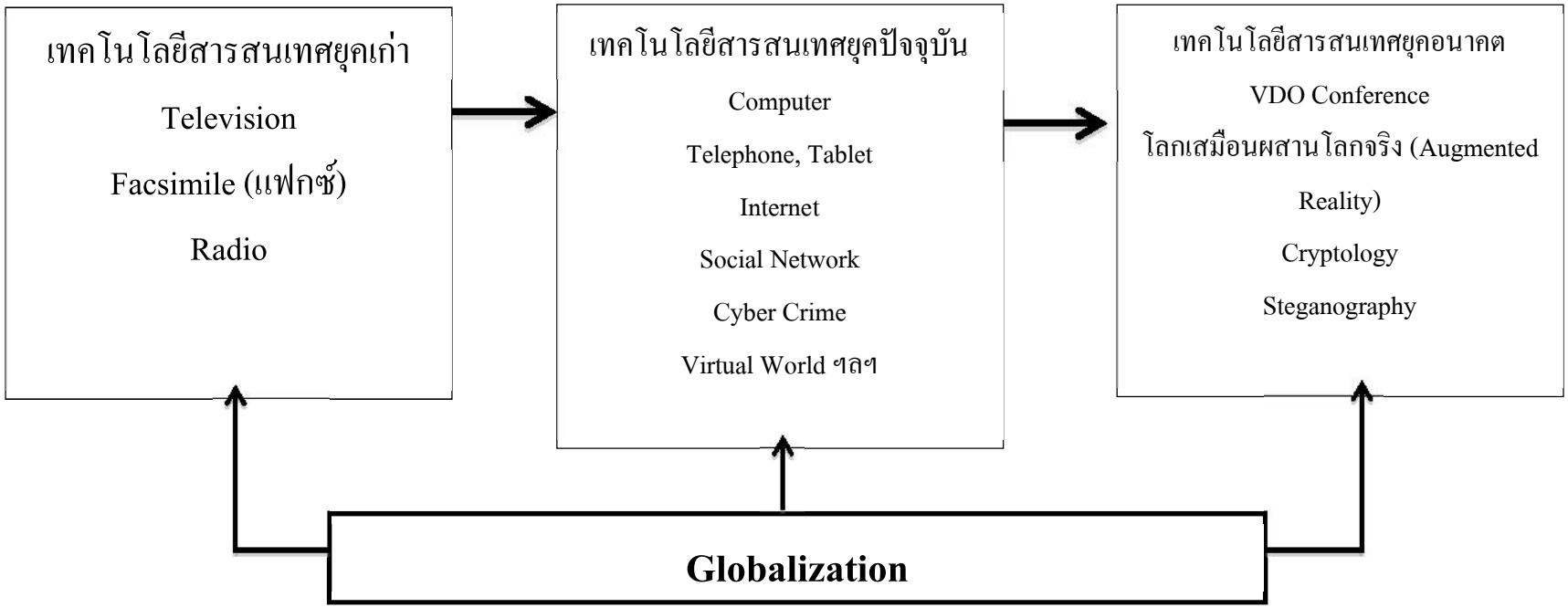
การต่อต้านการก่อการร้าย หมายถึงการใช้กลยุทธ์ เทคนิค ยุทธศาสตร์เพื่อแก้ปัญหาป้องกันและต่อต้านการกระทำที่มีเจตนาก่อให้เกิดความกลัว ข่มขู่ โดยมีวัตถุประสงค์ทางการเมือง ศาสนา หรืออุดมการณ์อย่างใดอย่างหนึ่ง

การก่อการร้ายทางไซเบอร์ หมายถึง ความรุนแรงและความน่ากลัวจากการใช้คอมพิวเตอร์ในการกระทำความผิด โดยใช้เป็นเครื่องมือในการกระทำความผิด เป็นเป้าหมายต่อการกระทำความผิด ใช้ในการเก็บข้อมูลที่เกี่ยวข้องกับการกระทำความผิด เป็นอาวุธหรือเป็นนโยบายต่อสู้ขู่ขวัญเพื่อหวังจะเอาชนะก่อให้เกิดความเสียหายทั้งทางตรงและทางอ้อม

ประโยชน์ที่คาดว่าจะได้รับ

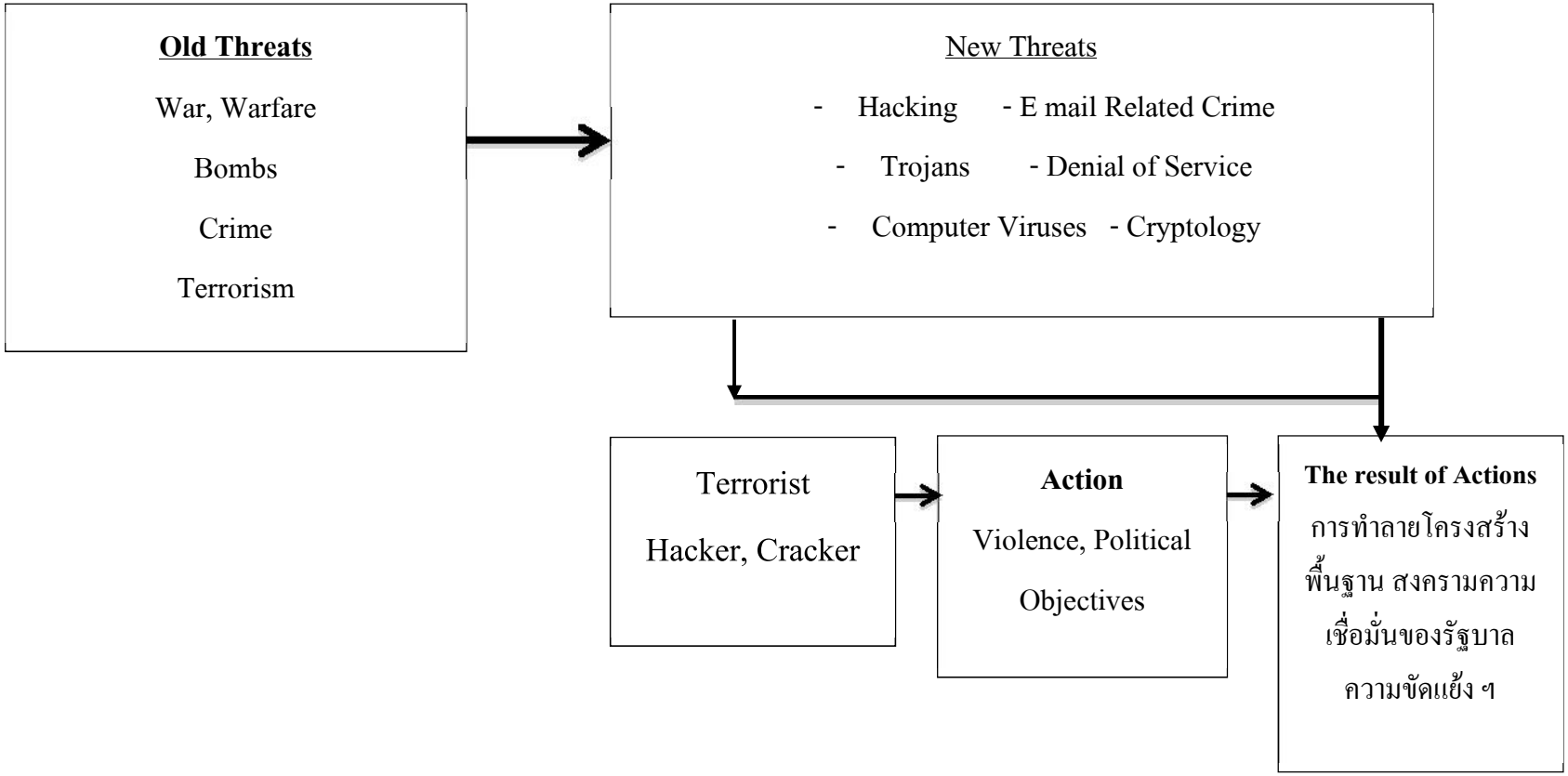
1. ทราบถึงความก้าวหน้าของไซเบอร์และลักษณะของการนำไซเบอร์มาเป็นเครื่องมือทางยุทธศาสตร์การก่อการร้ายและการต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย

2. นำเสนอยุทธศาสตร์ในการต่อต้านก่อการร้ายโดยใช้ไซเบอร์เป็นเครื่องมือในการก่อการร้ายในประเทศไทย



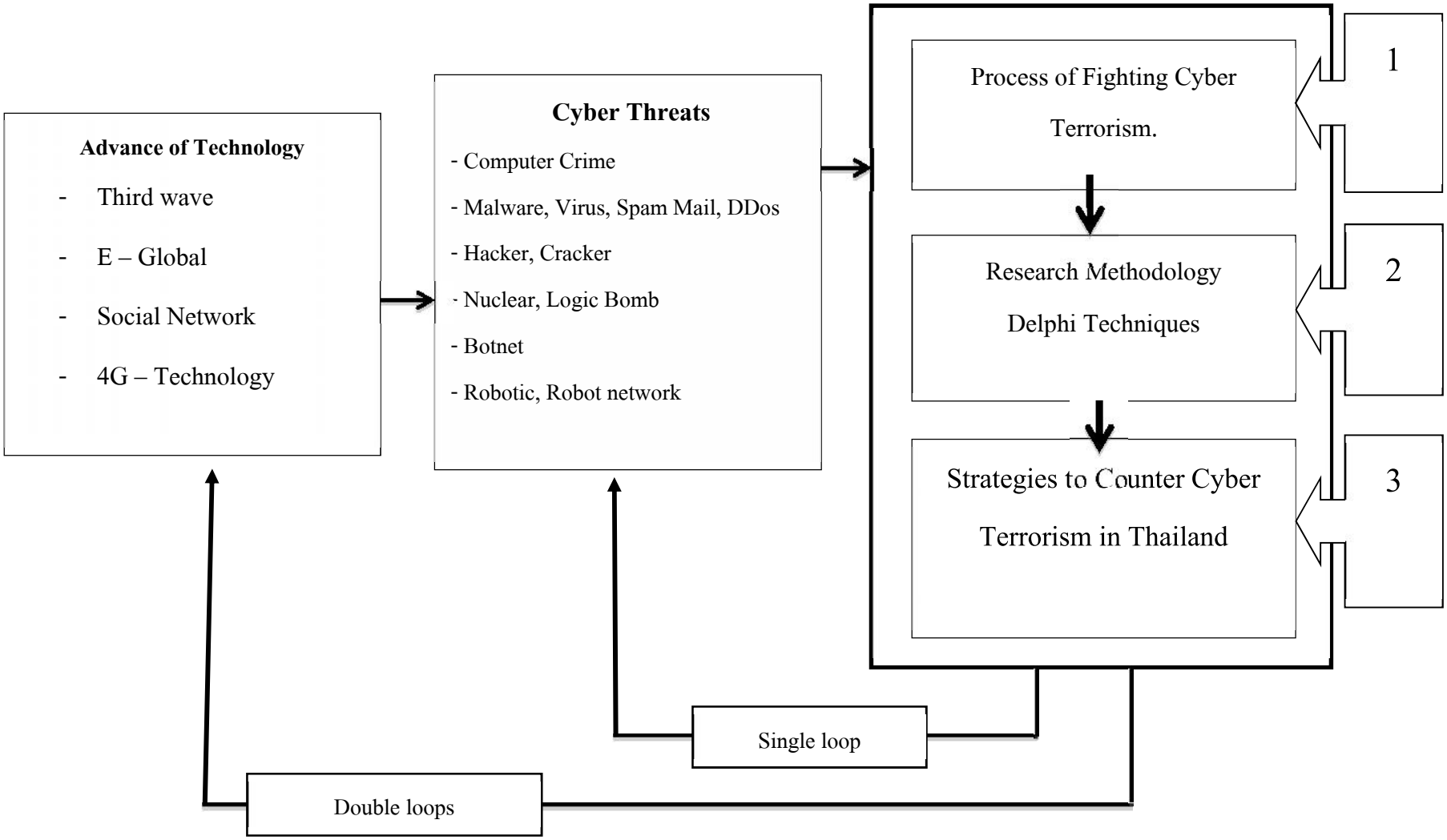
ภาพที่ 1 กรอบแนวคิดการวิจัยจากวัตถุประสงค์ ข้อที่ 1 ความก้าวหน้าทางไซเบอร์ที่มีการนำมาใช้เป็นเครื่องมือทางยุทธศาสตร์ในการก่อการร้ายในประเทศไทย

การพัฒนาของเทคโนโลยีมีการขยายตัวอย่างรวดเร็วเทคโนโลยีสารสนเทศยุคเก่ามีการคิดค้นและพัฒนาสิ่งประดิษฐ์เพื่อนำมาเป็นช่องทางในการสื่อสาร เช่น โทรทัศน์ แฟกซ์ วิทยุต่อมาเมื่อยุคที่เทคโนโลยีสารสนเทศได้มีการพัฒนามากขึ้นในยุคศตวรรษที่ 21 เทคโนโลยีเป็นสิ่งทีมีความจำเป็นต่อการดำรงชีวิตมนุษย์และเสมือนหนึ่งเป็นปัจจัยที่ห้าของการดำรงชีวิต เช่น คอมพิวเตอร์ โทรศัพท์มือถือ แท็บเล็ต สังคมเครือข่าย การอาชญากรรมทางไซเบอร์ โลกเสมือนจริงที่ติดต่อกันได้ทั่วโลก เป็นต้น ในอนาคต ปี 2020 คาดการณ์ว่า การพัฒนาเทคโนโลยีสารสนเทศจะพัฒนาอย่างต่อเนื่องและมีความสำคัญต่อการดำรงชีวิตของประชากรโลก ความเป็นโลกาภิวัตน์ทำให้มีอิทธิพลต่อการพัฒนาเทคโนโลยีแสดงให้เห็นถึงการเจริญเติบโตของโลก

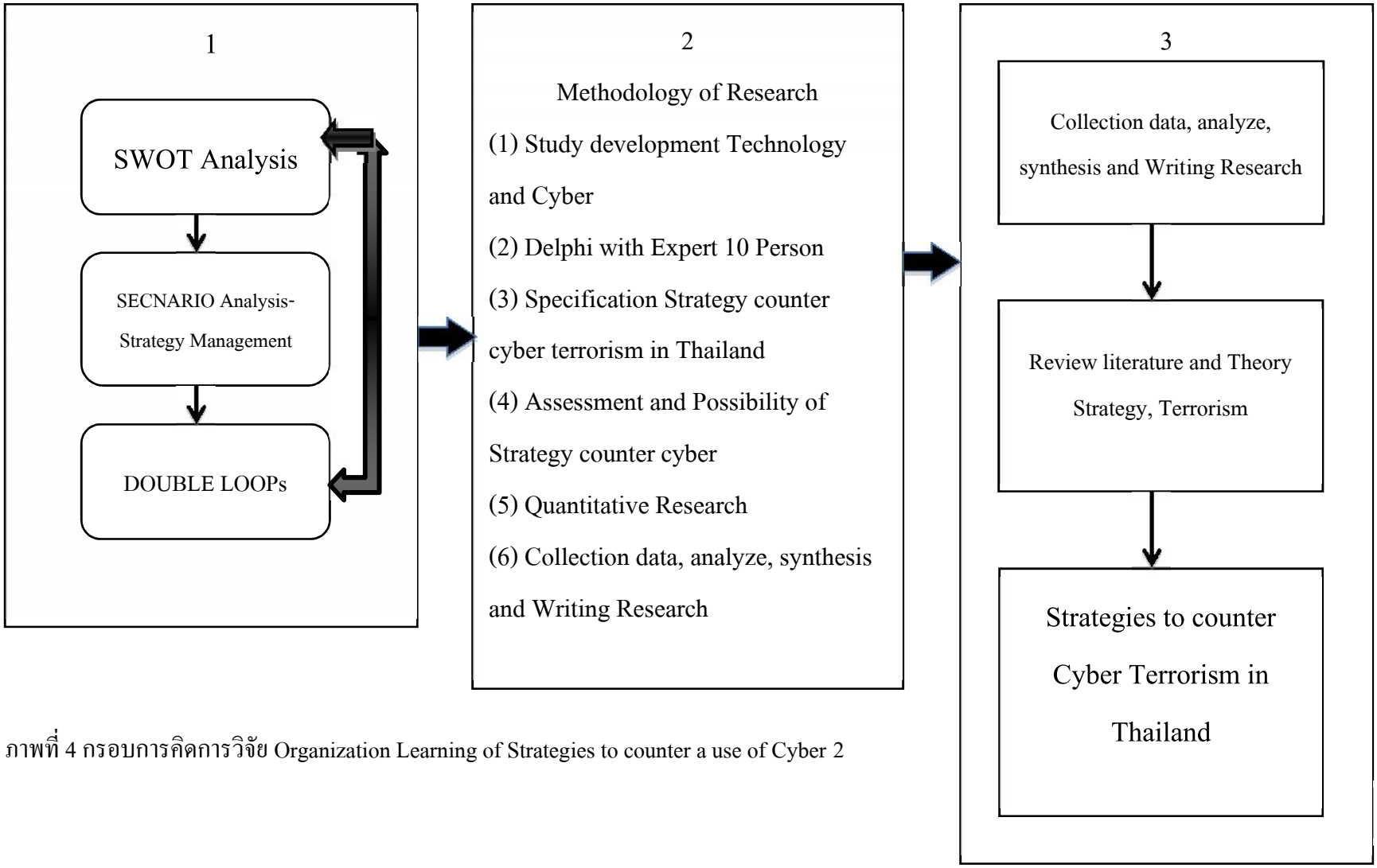


ภาพที่ 2 กรอบแนวคิดการวิจัยจากวัตถุประสงค์ข้อที่ 2 ลักษณะการก่อการร้ายโดยใช้ไซเบอร์มาเป็นเครื่องมือทางยุทธศาสตร์ในการก่อการร้ายในประเทศไทย

โลกตระหนักถึงภัยคุกคามที่เกิดขึ้นนอกจากภัยที่มาจากภัยธรรมชาติที่ไม่อาจหลีกเลี่ยงได้ ภัยคุกคามที่เกิดขึ้นอันนำมาซึ่งความเสียหายมีหลายรูปแบบ ภัยคุกคามในรูปแบบเดิม เช่น จากสงคราม การสู้รบ การวางระเบิด อาชญากรรม การก่อการร้าย เป็นต้น ในศตวรรษที่ 21 ภัยคุกคามจะเปลี่ยนรูปแบบนำไซเบอร์มาเป็นเครื่องมือในการก่อการร้าย เช่น การแฮกข้อมูล การปล่อยไวรัสทำลาย การสร้างรหัสเพื่อสร้างข้อมูล เป็นต้น ภัยคุกคามจะกระทำโดยผู้ก่อการร้ายที่มีความสามารถเข้าถึงหรือรู้ในด้านไซเบอร์มากกว่าผู้อื่น กระทำการที่แตกต่างจากรูปแบบของการก่อการร้ายแบบเดิม โดยมีวัตถุประสงค์ทางการเมืองเป็นสำคัญ ผลลัพธ์ที่เกิดจากการกระทำคือการทำลายโครงสร้างพื้นฐานของประเทศเป้าหมาย ทำลายความเชื่อมั่น ความน่าเชื่อถือของรัฐบาล สร้างความขัดแย้ง ความหวาดกลัวต่อประเทศคู่ขัดแย้งนำไปสู่การเกิดสงครามในที่สุด



ภาพที่ 3 กรอบแนวคิดการวิจัย Organization Learning of Strategies to counter a use of Cyber 1



ภาพที่ 4 กรอบการคิดการวิจัย Organization Learning of Strategies to counter a use of Cyber 2

บทที่ 2
เอกสารและงานวิจัยที่เกี่ยวข้อง

บทนี้เป็นการศึกษาเอกสารและงานวิจัยที่เกี่ยวข้องเพื่อเป็นกรอบความคิด ผู้ศึกษาได้ศึกษาค้นคว้าเอกสารและงานวิจัยที่เกี่ยวข้อง แบ่งออกเป็น 7 หัวข้อดังนี้

แนวคิดเรื่องโลกาภิวัตน์
แนวคิดเกี่ยวกับเทคโนโลยีสารสนเทศและการพัฒนาของเทคโนโลยีสารสนเทศ
แนวคิดเกี่ยวกับยุทธศาสตร์และกระบวนการจัดทำยุทธศาสตร์
แนวคิดเกี่ยวกับการก่อการร้ายและทฤษฎีการก่อการร้าย
แนวคิดเกี่ยวกับความมั่นคงแห่งชาติและความมั่นคงทางสารสนเทศ
แนวคิดเกี่ยวกับการก่อการร้ายทางไซเบอร์
งานวิจัยที่เกี่ยวข้อง

แนวคิดเรื่องโลกาภิวัตน์

ปัจจุบันนี้สังคมไทยกำลังเผชิญกับการเปลี่ยนแปลงครั้งใหญ่คือกระแสโลกาภิวัตน์ ซึ่งมีการพัฒนาจากอารยธรรมคลื่นลูกที่หนึ่งคือสังคมเกษตร มาสู่คลื่นลูกที่สองคือสังคมอุตสาหกรรม และก้าวย่างเข้าสู่คลื่นลูกที่สามคือสังคมข้อมูลข่าวสารปรากฏการณ์ที่เกิดขึ้นเพื่อเตรียมตัวและปรับตัวเข้ากับสังคมโลกยุคใหม่ สอดคล้องกับยุคโลกาภิวัตน์(Globalization) เป็นยุคที่เกิดการเปลี่ยนแปลงของเศรษฐกิจและสังคมอย่างรวดเร็ว ด้วยพลังแห่งเทคโนโลยี

ราชบัณฑิตยสถาน (2546) นิยามโลกาภิวัตน์ หมายถึง การแพร่กระจายไปทั่วโลก การที่ประชาคมโลกไม่ว่าจะอยู่ ณ จุดใดสามารถรับรู้ สัมพันธ์หรือรับผลกระทบจากสิ่งที่เกิดขึ้นได้อย่างรวดเร็วกว้างขวาง ซึ่งเนื่องมาจากพัฒนาระบบสารสนเทศเป็นต้น

แจน อาร์ต โชลเต (Scholte, 2007) เสนอแนวคิดโลกาภิวัตน์ในแง่ของการเปลี่ยนแปลงเชิงพื้นที่ของการติดต่อสัมพันธ์กัน (Spatial transformation of social connections) ของผู้คนซึ่งเชื่อมโยงกันทั่วโลกหรือข้ามเขตแดนต่างๆ โดยที่ความเชื่อมโยงทั่วโลกที่มีคนเป็นศูนย์กลางนี้ปรากฏเป็นการตัดข้ามพื้นที่อันหลากหลายของชีวิตทางสังคมซึ่งมีทั้งการสื่อสาร การท่องเที่ยว การผลิต ตลาด เงินทุน องค์การ กองทัพ นิเวศวิทยา สุขภาพ กฎหมาย และจิตสำนึก เขาเห็นว่าการเปลี่ยนรูปใหม่ของพื้นที่ทางสังคมนั้นเชื่อมโยงอย่างใกล้ชิดกับแบบแผนของความรู้ การผลิต การบริหารจัดการ อัตลักษณ์และวิธีการที่ผู้คนสัมพันธ์กับธรรมชาติ

หนังสือ Globalization ของ (Waters, 2001)กล่าวว่า การอธิบายปรากฏการณ์ที่เชื่อมโยงสังคมและรัฐชาติเข้าไว้ด้วยกันทั่วโลก ความเป็นสากลนิยมการติดต่อสื่อสารที่เชื่อมต่อถึงกันโดยทั่วและการกระทำเหตุการณ์ที่ส่งผลกระทบหรือการร่วมมือของคนทั้งโลก ในความเป็นโลกาภิวัตน์ในศตวรรษที่ 21 นี้การนำเทคโนโลยีที่มีประสิทธิภาพและการสร้างเครือข่ายทางสังคม ทำให้โลกเปรียบเป็นโลกเสมือน สามารถเจอกันได้ รับรู้ความเคลื่อนไหวและสามารถเข้าถึงทุกมุมทั่วโลก โลกาภิวัตน์เป็นระบบวัฒนธรรมโลกที่พัฒนาขึ้นเพื่อตอบสนองและเอื้ออำนวยต่อการเกิดขึ้นของระบบผูกขาดไร้พรมแดนเพื่อให้คนทั้งโลกขึ้นต่อวัฒนธรรมที่เรียกว่า Neo – westernization ที่เป็นการสร้างกระแสบริโภคนิยมทุกอย่างเป็นอเมริกา หรือญี่ปุ่น การเกิดกระแสบริโภคนิยมและการตามกระแสนั้นเป็นการรุกรานความเป็นท้องถิ่นและประเพณีดั้งเดิมของคนในพื้นที่ต่างๆ ของโลกและส่งผลกระทบในกลุ่มชาตินิยม ประเพณีนิยมและศาสนานิยม ส่งผลให้เกิดความไม่พอใจในกลุ่มมุสลิมหัวรุนแรงได้เนื่องจากกระแสโลกาภิวัตน์

แอนโธนีกิดเด็นส์ (Giddens,1990)ได้นิยามโลกาภิวัตน์ไว้ว่าเป็นกระบวนการที่ทำให้ความสัมพันธ์ทางสังคมมีความเข้มข้นขึ้นโดยเชื่อมท้องถิ่นที่อยู่ห่างไกลออกไป กระบวนการนี้เรียกว่า เป็นการยืดความสัมพันธ์ทางสังคมข้ามเวลาและพื้นที่ (Time – Space distanciation) มองว่าโลกาภิวัตน์เป็นความสมัยใหม่ที่ขยายตัวออกไป โดยชี้ให้เห็นพลังขับเคลื่อนความเป็นสมัยใหม่ที่สำคัญ 4 มิติคือ 1. กระบวนการพัฒนาอุตสาหกรรมที่ก่อให้เกิดการแบ่งงานกันทำระหว่างประเทศ 2. ลัทธิทุนนิยมที่ขับเคลื่อนให้เกิดระบบเศรษฐกิจทุนนิยมระดับโลก 3.ลัทธิทหารนิยมที่ก่อให้เกิดโครงสร้างพื้นฐานที่เป็นระเบียบทางการทหารระดับโลกและ 4. ลัทธิรัฐนิยมที่ได้รับการขับเคลื่อนซึ่งก่อให้เกิดระบบของรัฐชาติขึ้นมา โดยที่ระบบต่าง ๆ และโครงสร้างพื้นฐานต่าง ๆ ที่เกิดจากการขับเคลื่อนของมิติทั้ง 4 นั้นได้ก่อให้เกิดการเชื่อมโยงของผู้คน ครอบครัวและชุมชนทั่วโลกซึ่งอยู่ห่างไกลเข้าด้วยกัน

Holton (2000) pp.140 – 152 ศึกษาเรื่องผลกระทบทางสังคมวัฒนธรรมจากกระแสโลกาภิวัตน์โดยจำแนกพิจารณาได้ 3 ทฤษฎี คือ

1.ทฤษฎีการกลายเป็นเนื้อเดียวกัน โลกาภิวัตน์ทำให้เกิดความเหมือนกันและความคล้ายคลึงกันทางด้านวัฒนธรรมจนกล่าวได้ว่าสังคมต่าง ๆ จะมีการโคจรมาบรรจบกันทางวัฒนธรรม

2. ทฤษฎีการแยกขั้ว ชี้ต่อไปว่าจะเกิดความขัดแย้งและสงครามวัฒนธรรม เช่น ระหว่างตะวันตกกับฝ่ายปฏิปักษ์ หรืออาจเรียกว่า แนวคิดการปะทะทางอารยธรรม

3.ทฤษฎีการผสมผสาน โดยปฏิบัติทางวัฒนธรรมที่เป็นรูปธรรมนั้นมักเป็นผลมาจากการแลกเปลี่ยนและหยิบยืมองค์ประกอบทางวัฒนธรรมที่มาจากวัฒนธรรมต่าง ๆ ทั้งหลายกระแสของการพัฒนาวัฒนธรรม ข่าวสาร ผู้คน ฯ ข้ามแดน ปรากฏแนวนี้จะมีมากขึ้น

ระวิวรรณ ธรณี, ปราณี ประวิชพราหมณ์และภาวิณี อุ่นวัฒนา (2551, หน้า 28– 29) กล่าวถึงสังคมไทยกับโลกาภิวัตน์สภาพแวดล้อมที่เปลี่ยนแปลงไป โลกาภิวัตน์ทำให้เกิดประโยชน์และโทษแก่สังคมไทยดังนี้

1.ประโยชน์ที่ได้รับจากโลกาภิวัตน์

1.1 สังคมไทยมีเครื่องมือเครื่องใช้ที่ทันสมัยเหมาะกับการดำรงชีวิตแบบสมัยใหม่ เกิดความสะดวกสบาย และสามารถติดต่อกันได้รวดเร็วขึ้น

1.2ด้านการศึกษานำไปสู่การศึกษาตลอดชีวิต เพราะความเจริญและความรู้ใหม่ ๆ ที่มีมากขึ้นทำให้ต้องอ่าน ศึกษาหาความรู้ ตลอดเวลา เพื่อทราบข่าวสารใหม่ ทฤษฎีใหม่ ซึ่งสามารถค้นคว้าด้วยการสื่อสารเทคโนโลยีใหม่ ๆ เพื่อทราบข่าวสารใหม่ ทฤษฎีใหม่ ซึ่งสามารถค้นคว้าด้วยการสื่อสารเทคโนโลยีใหม่ ๆ ทำให้รับรู้เหตุการณ์ที่เกิดขึ้นอย่างรวดเร็ว

1.3 ด้านเศรษฐกิจ เศรษฐกิจไทยมีการพัฒนาอย่างรวดเร็ว ทัดเทียมประเทศที่เจริญแล้ว สามารถซื้อขายผ่านออนไลน์ คอมพิวเตอร์ ทำให้ประหยัดพลังงาน ค่าใช้จ่าย เวลาและสามารถจ่ายด้วยบัตรเครดิต การโอนเงินทั้งในประเทศ และต่างประเทศทำได้รวดเร็ว

1.4 นักลงทุน นักธุรกิจ ผู้ประกอบการสามารถรับข้อมูลมาประมวลการตัดสินใจในการลงทุนและเข้าสู่ตลาดการลงทุน

2.ผลเสียที่สังคมไทยได้รับจากโลกาภิวัตน์

2.1 รูปแบบครอบครัวเปลี่ยนจากครอบครัวขยายเป็นครอบครัวเดี่ยวมากยิ่งขึ้น สมาชิกในครอบครัวห่างเหินกันมากขึ้นนำไปสู่การหย่าร้าง ไม่มีเวลาดูแลบุตร บุตรเกิดความว้าเหว่ ขาดความอบอุ่น จนนำไปสู่การติดสิ่งเสพติด การมีพฤติกรรมเบี่ยงเบน

2.2 ค่านิยมของคนเปลี่ยนไปให้ความสำคัญกับเงินและวัตถุนิยม บริโภคนิยม เกิดการเอารัดเอาเปรียบและความโลภไม่ให้ความสนใจและความสำคัญทางจิตใจ

2.3 เกิดปัญหาสังคมไทยเพราะคนมั่งคั่ง กับคนจนมีรายได้ต่างกันมาก คนจนมีหนี้สินจนไม่สามารถหาเงินมาจ่ายคืนได้ นำไปสู่ปัญหาต่าง ๆ เช่น ปัญหาอาชญากรรม ปัญหาเพศพานิชย์ ตกงาน ปัญหาสิ่งแวดล้อมเป็นพิษ ฯลฯ

จากมุมมองของนักวิชาการข้างต้น ผู้วิจัยเห็นว่าแนวคิดโลกาภิวัตน์ เป็นกระบวนการที่สร้างให้สังคมมีความสัมพันธ์ที่แคบลง สามารถเชื่อมต่อและเกี่ยวโยงความสัมพันธ์ของคนทั่วโลกไว้ด้วยเทคโนโลยีสมัยใหม่ สร้างวัฒนธรรมใหม่ที่ทำให้คนมีแนวคิดและมีการกระทำที่คล้ายหรือ

เหมือนกันทั่วโลกแต่โลกาภิวัตน์ก็ส่งผลให้สังคมมีการเปลี่ยนแปลงไปในทางที่ไม่ดี หากคนในสังคมไม่ได้ปรับตัวตามการเปลี่ยนแปลงกระแสโลกาภิวัตน์จะส่งผลต่อพฤตกรรมกรดำรงชีวิตที่เปลี่ยนแปลงไปและเป็นช่องโหว่ของผู้ที่ไม่ประสงค์ดีนำมาเป็นช่องทางของการก่อการร้ายได้

แนวคิดเกี่ยวกับเทคโนโลยีสารสนเทศและการพัฒนาของเทคโนโลยีสารสนเทศ

เทคโนโลยีมีบทบาทกับการดำรงชีวิต การดำเนินธุรกิจและการศึกษา และแม้กระทั่งในระบบการเมือง เทคโนโลยีมีส่วนช่วยให้สังคมเกิดการพัฒนาในหลายด้านแต่ในทางกลับกันเทคโนโลยีก็มีผลเสียต่อความเป็นส่วนตัว หรือเป็นช่องโหว่ต่อการก่อการร้ายได้ง่ายมากขึ้น

ราชบัณฑิตสถาน (2546, หน้า 538) ได้ให้ความหมายของเทคโนโลยีว่า วิทยาการที่เกี่ยวข้องกับศิลปะในการนำเอาศิลปะในการนำวิทยาศาสตร์ประยุกต์มาใช้ให้เกิดประโยชน์ในทางปฏิบัติและอุตสาหกรรม

สุขุม เฉลยทรัพย์และคณะ (2551, หน้า 6) เทคโนโลยีสารสนเทศ และเทคโนโลยีสารสนเทศและการสื่อสาร เป็นคำที่ใช้แทนกันได้ หมายถึง เทคโนโลยีสองสาขาหลักที่ประกอบด้วยเทคโนโลยีคอมพิวเตอร์ และเทคโนโลยีสื่อสารโทรคมนาคมที่ผนวกเข้าด้วยกันเพื่อใช้ในการสร้างสรรค์ จัดหา จัดเก็บ ค้นคืน จัดการถ่ายทอดและเผยแพร่ข้อมูลในรูปดิจิทัล(Digital Data) ไม่ว่าจะเป็นเสียง ภาพ ภาพเคลื่อนไหว ข้อความหรือตัวอักษรและตัวเลขเพื่อเพิ่มประสิทธิภาพ ความถูกต้องความแม่นยำและความรวดเร็วต่อการนำไปใช้ประโยชน์

เบอเกลแมน, คริสเต็นเซ่นและวีลไรน์ (Burgelman, Christensen, Wheelwright, 2008, p.1) ได้กล่าวว่า เทคโนโลยี ทฤษฎี ความรู้และทักษะ สิ่งประดิษฐ์ที่ใช้สำหรับการพัฒนาผลิตภัณฑ์ บริการ หรือกระบวนการทำงานต่าง ๆ ขององค์กร เทคโนโลยีอาจอยู่ในตัวบุคคล วัตถุดิบ กระบวนการคิด การรับรู้ กระบวนการทางกายภาพ เครื่องมือ หรืออุปกรณ์ต่าง ๆ เทคโนโลยีอาจเป็นกิจกรรมการพัฒนารูปแบบการใช้งานของสิ่งประดิษฐ์ต่าง ๆ ก็ได้ ซึ่งกล่าวได้ว่า เทคโนโลยีเป็นทรัพยากรที่สำคัญขององค์กร ที่ต้องการบริหารจัดการที่ดีเพื่อสร้างความได้เปรียบทางการแข่งขันให้กับองค์กรด้วยการบูรณาการเข้ากับกลยุทธ์ขององค์กร

ดารณี พิมพ์ช่างทอง (2552, หน้า 23) อินเทอร์เน็ต มาจากคำว่า Inter connection network หมายถึง เครือข่ายของเครือข่ายคอมพิวเตอร์ เป็นเครือข่ายขนาดใหญ่ที่เชื่อมต่อระบบเครือข่ายจากทุกมุมโลกเข้าด้วยกัน อินเทอร์เน็ตเป็นสื่อกลางในการสื่อสารที่สำคัญที่เปลี่ยนแปลงการดำเนินธุรกิจขององค์กรหลายชนิด อินเทอร์เน็ตเปลี่ยนแปลงโครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศทั่วโลกและสนับสนุนการสื่อสารระหว่างโปรแกรมประยุกต์บนระบบเครือข่าย

สรุปได้ว่า เทคโนโลยีเป็นประดิฐกรรมที่มีกระบวนการผลิต การประมวลผลและการจำแนกแจกจ่ายสารสนเทศไปยังผู้ใช้งาน กระบวนการของเทคโนโลยีมีความทันสมัย ประกอบด้วยสองส่วนคือเทคโนโลยีคอมพิวเตอร์และเทคโนโลยีสารสนเทศ มีทั้งข้อมูลในรูปแบบของเสียง ภาพ ภาพเคลื่อนไหว ข้อความ ตัวอักษร ตัวเลข เพื่อให้ผู้ใช้ได้รับอย่างถูกต้องและการใช้เทคโนโลยีในยุคโลกาภิวัตน์ต้องมีการเชื่อมโยงระบบอินเทอร์เน็ตหรือเครือข่ายคอมพิวเตอร์ที่สามารถติดต่อกันได้ ไม่ว่าจะอยู่ที่ใดบนโลก

การพัฒนาของเทคโนโลยีสารสนเทศ

เทคโนโลยีสารสนเทศเป็นเทคโนโลยีที่มีการขยายตัวอย่างรวดเร็วมีความสามารถในการใช้งานเพิ่มขึ้นขณะเดียวกันก็มีราคาถูกลงผลของการพัฒนานี้ทำให้มีการประยุกต์ใช้งานกันอย่างกว้างขวางจนกล่าวได้ว่าปัจจุบันเทคโนโลยีสารสนเทศได้เข้ามามีส่วนเกี่ยวข้องกับมนุษย์ทุกคนไม่ทางตรงก็ทางอ้อมประเทศไทยได้เริ่มใช้ระบบคอมพิวเตอร์มาเป็นเวลานานกว่า 30 ปีแล้วเมื่อปีพ.ศ.2506 เครื่องคอมพิวเตอร์เครื่องแรกเป็นเครื่อง IBM 1401 ติดตั้งที่สานักงานสถิติแห่งชาติเพื่อจัดทำสถิติและสำมะโนประชากรต่อมาพ.ศ.2527 รัฐบาลได้แต่งตั้งคณะกรรมการคอมพิวเตอร์แห่งชาติเพื่อทำหน้าที่ในการพิจารณาอนุมัติการจัดหาคอมพิวเตอร์ของส่วนราชการพ.ศ.2534 รัฐบาลได้ยุบคณะกรรมการคอมพิวเตอร์แห่งชาติเพื่อให้หน่วยราชการต่างๆมีความคล่องตัวในการจัดหาคอมพิวเตอร์เพราะคอมพิวเตอร์มีราคาถูกลงและนิยมใช้แพร่หลายขึ้นพ.ศ. 2535 มีการจัดตั้งศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติซึ่งเป็นหน่วยงานในสังกัดสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติกระทรวงวิทยาศาสตร์เทคโนโลยีและสิ่งแวดล้อมมีการแต่งตั้งคณะกรรมการส่งเสริมการพัฒนาเทคโนโลยีสารสนเทศแห่งชาติจากนั้นคณะกรรมการส่งเสริมการพัฒนาเทคโนโลยีสารสนเทศแห่งชาติได้แต่งตั้งอนุกรรมการด้านต่างๆ7 ด้านได้แก่การแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์การค้าระหว่างประเทศการวางแผนพัฒนาเทคโนโลยีสารสนเทศการวางแผนพัฒนาบุคลากรด้านเทคโนโลยีสารสนเทศการส่งเสริมการใช้เทคโนโลยีสารสนเทศในหน่วยงานของรัฐการพัฒนากฎหมายเทคโนโลยีสารสนเทศและการส่งเสริมการค้นคว้าวิจัยด้านเทคโนโลยีสารสนเทศ

ประเทศสหรัฐอเมริกาเป็นประเทศหนึ่งที่มีการเปลี่ยนแปลงอย่างชัดเจนในอดีตประเทศสหรัฐอเมริกาเป็นประเทศเกษตรกรรมมีผลผลิตทางด้านการเกษตรเป็นสินค้าหลักต่อมามีการเปลี่ยนโครงสร้างการผลิตเป็นประเทศอุตสาหกรรมปริมาณสัดส่วนของสินค้าอุตสาหกรรมได้เพิ่มขึ้นอย่างรวดเร็วปัจจุบันเป็นยุคของเทคโนโลยีสารสนเทศโครงสร้างการผลิตของประเทศสหรัฐอเมริกาเน้นไปที่ธุรกิจบริการและการใช้สารสนเทศกันมากหากพิจารณาการใช้งานคอมพิวเตอร์และระบบสื่อสารทั่วไปของโลกปัจจุบันมูลค่าของสินค้าทางด้านเทคโนโลยี

สารสนเทศได้ขยายตัวอย่างรวดเร็วสิ่งที่น่าสนใจคือประเทศที่พัฒนาแล้ว 10ประเทศได้แก่1. สหรัฐอเมริกา2. สิงคโปร์3. ฟินแลนด์4. ลักเซมเบิร์ก5. เนเธอร์แลนด์6. ฮ่องกง7. ไอซแลนด์8. สวีเดน9. แคนาดาและ10. สวิตเซอร์แลนด์มีสัดส่วนการใช้คอมพิวเตอร์มากกว่า 90 เปอร์เซ็นต์ของปริมาณการใช้คอมพิวเตอร์ทั่วโลกนอกจากนี้ประเทศในแถบเอเชียที่เป็นประเทศอุตสาหกรรมใหม่ก็มีแนวโน้มการใช้เทคโนโลยีสารสนเทศมากขึ้น

ระบบเครือข่ายอินเทอร์เน็ตทำให้โลกของการสื่อสารเปลี่ยนไปอย่างรวดเร็ว การติดต่อสื่อสารระหว่างบุคคล หน่วยงาน หรือการเผยแพร่ข่าวสารข้อมูลสู่สาธารณะเป็นสิ่งที่ง่ายและรวดเร็ว สื่อใหม่จึงส่งผลกระทบต่อสื่อสิ่งพิมพ์ที่เป็นสื่อเดิม โดยเฉพาะอย่างยิ่งโทรศัพท์มือถือที่มีศักยภาพเพียงพอที่จะกลายเป็นสื่อใหม่ ที่ทรงพลังอันประกอบด้วย 1. ความต้องการที่จะสื่อสารของมนุษย์ทุกคน 2. โทรศัพท์มือถือถูกออกแบบให้มีขนาดเล็ก สามารถพกพาไปใช้งานได้ทุกที่ 3. โทรศัพท์มือถือเป็นเสมือนจุดหมายปลายทางของการผสมผสานกันของอุปกรณ์อิเล็กทรอนิกส์ สื่อใหม่ ผ่านช่องทางใหม่ ๆ ย่อมกระตุ้นการรับรู้ของผู้รับสารได้เป็นอย่างดี 4. สามารถทำการซื้อขายสินค้าหรือกระทำการใด ๆ ผ่านโทรศัพท์มือถือ จึงทำให้สื่อใหม่ผ่านโทรศัพท์มือถือได้รับความนิยม (วรพจน์ วงศ์กิจรุ่งเรือง และอธิป จิตตฤกษ์, 2554 หน้า 177)

นับตั้งแต่เทคโนโลยีสารสนเทศเข้ามามีบทบาทมากในชีวิตประจำวันการใช้เทคโนโลยีเป็นไปอย่างกว้างขวางหมายถึงการใช้เทคโนโลยีด้านต่างๆแน่นอนที่ทุกสิ่งย่อมมีทั้งคุณและโทษภาพยนตร์หลายเรื่องได้สะท้อนความคิดของการนาเอาเทคโนโลยีสารสนเทศมาใช้ในทางลบผลกระทบในทางลบเหล่านี้บางอย่างเป็นเพียงการคาดคะเนเท่านั้นอาจไม่ได้เกิดขึ้นจริงแต่อย่างไรก็ตามย่อมมีโอกาสเกิดขึ้น ได้แก่

1.ทำให้เกิดอาชญากรรมเทคโนโลยีสารสนเทศเป็นหนทางในการก่ออาชญากรรมได้โจรผู้ร้ายอาจใช้เทคโนโลยีสารสนเทศในการวางแผนปล้นวางแผนโจรกรรมมีการลักลอบใช้ข้อมูลข่าวสารมีการโจรกรรมหรือแก้ไขตัวเลขบัญชีด้วยคอมพิวเตอร์การลอบเข้าไปแก้ไขข้อมูลอาจทาให้เกิดปัญหาหลายอย่างเช่นการแก้ไขระดับคะแนนของนักศึกษาการแก้ไขข้อมูลในโรงพยาบาลเพื่อให้การรักษาพยาบาลคนไข้ผิดซึ่งเป็นการทำร้ายหรือฆาตกรรมดังที่เห็นในภาพยนตร์

2. ทำให้ความสัมพันธ์ของมนุษย์เสื่อมถอยการใช้คอมพิวเตอร์และอุปกรณ์สื่อสารทำให้สามารถติดต่อสื่อสารกันได้โดยไม่ต้องเห็นตัวการใช้งานคอมพิวเตอร์หรือแม้แต่การเล่นเกมมีลักษณะการใช้งานเพียงคนเดียวทำให้ความสัมพันธ์กับผู้อื่นลดลงผลกระทบนี้ทำให้มีความเชื่อว่ามนุษยสัมพันธ์ของบุคคลจะน้อยลงสังคมใหม่จะเป็นสังคมที่ไม่ต้องพึ่งพากันมากอย่างไรก็ดีได้มีงานวิจัยคัดค้านและแสดงความคิดเห็นที่ว่าเทคโนโลยีได้ช่วยให้มนุษย์มีการติดต่อสื่อสารถึงกันมากขึ้นและความสัมพันธ์ดีขึ้น

3. ทำให้เกิดความวิตกกังวลผลกระทบนี้เป็นผลกระทบทางด้านจิตใจของกลุ่มบุคคลบางกลุ่มที่มีความวิตกกังวลว่าคอมพิวเตอร์อาจทำให้เกิดการว่าจ้างงานน้อยลงมีการนำเอาหุ่นยนต์มาใช้ในงานมากขึ้นมีระบบการผลิตที่อัตโนมัติมากขึ้นทำให้ผู้ใช้แรงงานอาจตกงานหรือหน่วยงานอาจเลิกว่าจ้างได้โดยความจริงแล้วความคิดเหล่านี้จะเกิดขึ้นกับบุคลากรบางกลุ่มเท่านั้นแต่ถ้าบุคคลนั้นมีการปรับตัวให้เข้ากับเทคโนโลยีหรือมีการพัฒนาให้มีความรู้ความสามารถสูงขึ้นแล้วปัญหานี้จะไม่เกิดขึ้นอย่างไรก็ดีได้มีงานวิจัยคัดค้านและแสดงความคิดเห็นที่ว่าเทคโนโลยีได้ช่วยให้มนุษย์มีการติดต่อสื่อสารถึงกันมากขึ้นและความสัมพันธ์ดีขึ้น

4. ทำให้เกิดการเสี่ยงภัยทางด้านธุรกิจธุรกิจในปัจจุบันจำเป็นต้องพึ่งพาอาศัยเทคโนโลยีสารสนเทศมากขึ้นข้อมูลข่าวสารทั้งหมดของธุรกิจฝากไว้ในศูนย์ข้อมูลเช่นข้อมูลลูกหนี้การค้าข้อมูลสินค้าและบริการต่างๆหากเกิดการสูญหายของข้อมูลอันเนื่องมาจากเหตุอุบัติภัยเช่นไฟไหม้น้ำท่วมหรือด้วยสาเหตุใดก็ตามที่ทำให้ข้อมูลหายหมดย่อมทำให้เกิดผลกระทบต่อธุรกิจโดยตรง

5. ทำให้มีการพัฒนาอาวุธที่มีอำนาจทำลายสูงประเทศที่เป็นเจ้าของเทคโนโลยีสามารถนำเทคโนโลยีมาช่วยในการสร้างอาวุธที่มีอานุภาพการทำลายสูงทำให้เสี่ยงต่อการเกิดสงครามและมีการสูญเสียมากขึ้น

6. ทำให้เกิดการแพร่วัฒนธรรมและกระจายข่าวสารที่ไม่เหมาะสมอย่างรวดเร็วคอมพิวเตอร์เป็นอุปกรณ์ที่ทำงานตามคำสั่งอย่างเคร่งครัดการนำมาใช้ในทางใดจึงขึ้นอยู่กับผู้ใช้จริยธรรมการใช้คอมพิวเตอร์เป็นเรื่องสำคัญดังเช่นการใช้งานอินเทอร์เน็ตมีผู้สร้างโฮมเพจหรือสร้างข้อมูลข่าวสารในเรื่องภาพที่ไม่เหมาะสมเช่นภาพอนาจารหรือภาพที่ทาให้ผู้อื่นเสียหายการดำเนินการเช่นนี้ย่อมขึ้นอยู่กับจริยธรรมของผู้ดาเนินการนอกจากนี้ยังมีการปลอมแปลงระบบจดหมายเพื่อส่งจดหมายถึงผู้อื่นโดยมีเจตนากระจายข่าวที่เป็นเท็จจริยธรรมการใช้งานเครือข่ายเป็นเรื่องสำคัญที่ต้องปลูกฝังอย่างมาก

7. ทำให้ข้อมูลหรือโปรแกรมถูกทำลายได้ง่ายด้วยเทคโนโลยีสารสนเทศมีการพัฒนามากข้อมูลก็มีความสำคัญมากขึ้นตามไปด้วยเทคโนโลยีทำให้ข้อมูลถูกทำลายได้ง่ายอาจจะถูกทำลายด้วยไวรัสคอมพิวเตอร์ซึ่งเป็นโปรแกรมคอมพิวเตอร์ประเภทหนึ่งที่สามารถทำสำเนาตัวเองเข้าไปอยู่ในระบบคอมพิวเตอร์ได้สามารถแพร่ไปยังระบบคอมพิวเตอร์อื่นๆได้โดยผ่านเครือข่ายคอมพิวเตอร์ไวรัสคอมพิวเตอร์บางชนิดทำลายโปรแกรมหรือข้อมูลต่างๆบางชนิดทำให้เครื่องคอมพิวเตอร์ทำงานช้าลงส่งผลกระทบต่อการทำงานของคอมพิวเตอร์นั้น

สรุปได้ว่า เทคโนโลยีสารสนเทศและอินเทอร์เน็ตมีความสำคัญมาก มีการพัฒนาอย่างรวดเร็วมีความสามารถจากการพัฒนาของมนุษย์อย่างมากมาย แต่ในทางเดียวกัน เทคโนโลยีที่มี

ความสามารถมากมายก็สามารถส่งผลในทางลบหรือนำไปเชื่อมโยงกับการกระทำความผิดได้เช่นเดียวกัน

แนวคิดเกี่ยวกับยุทธศาสตร์และกระบวนการจัดทำยุทธศาสตร์

1. ความหมายของยุทธศาสตร์

ราชบัณฑิตยสถาน (2546) ได้ให้ความหมายของคำว่า ยุทธศาสตร์ ไว้ว่า “วิชาว่าด้วยการพัฒนาและการใช้อำนาจทางการเมือง เศรษฐกิจ จิตวิทยาและกำลังรบทางทหารตามความจำเป็นทั้งในยามสงบและยามสงคราม” จากความหมาย จะเห็นได้ว่า คำว่า ยุทธศาสตร์ (Strategy) มีความหมายที่มีความแตกต่างจากในอดีต ด้วยเหตุจากการวิวัฒนาการแนวความคิดจากการรบของทหาร และมักนำไปใช้ในการดำเนินกิจกรรมในยามสงคราม อาจกล่าวได้ว่า เป็นศิลปะของผู้นำทัพและเป็นยุทธวิธีในการนำทหารเข้าสู่สนามรบ แต่ในความเปลี่ยนแปลงของโลก การตีความในความหมายของยุทธศาสตร์ ได้มีความหมายที่แตกต่างกันไป กล่าวได้ว่า ยุทธศาสตร์มิได้มีความหมายเฉพาะเพียงพลังอำนาจทางทหารเท่านั้น แต่ยุทธศาสตร์ยังครอบคลุมในความหมายหลายด้านทั้งด้านธุรกิจ ด้านการแพทย์ ด้านการกีฬา ความหมายของคำว่า ยุทธศาสตร์ แตกต่างกับคำว่า กลยุทธ์ ในภาษาไทยมีความหมายใกล้เคียงกัน ควรมีการทำความเข้าใจกับสองความหมายนี้ พจนานุกรมฉบับราชบัณฑิตยสถาน พ.ศ. 2525 ได้ให้ความหมายของคำสองคำนี้ ได้แก่

ยุทธศาสตร์ หมายถึง วิชาการรบ ที่มีความสำคัญในการรบ

กลยุทธ์ หมายถึง การรบที่มีเล่ห์เหลี่ยม วิธีการต่อสู้ที่ต้องใช้กลอุบายต่าง ๆ

กระทรวงกลาโหมของสหรัฐอเมริกา ได้ให้ความหมายในพจนานุกรมทางการทหารของสหรัฐฯ (DOD Dictionary of military and associated terms) และกองบัญชาการทหารสูงสุดของประเทศไทยได้ถอดความใช้ในพจนานุกรมศัพท์ทหารอังกฤษ – ไทย ฉบับใช้สามเหล่าทัพ พ.ศ. 2544ไว้ว่า ยุทธศาสตร์ หมายถึง ศิลป์และศาสตร์ในการพัฒนาและการใช้กำลัง อำนาจทางการเมือง ทางเศรษฐกิจ ทางจิตวิทยาและกำลังรบทางทหาร ตามความจำเป็นทั้งในยามสงบและยามสงคราม เพื่อทำให้บังเกิดการสนับสนุนอย่างสูงสุดต่อนโยบายด้านต่าง ๆ เพื่อมุ่งที่จะเพิ่มพูนโอกาสและผลของชัยชนะในทางที่เกื้อกูลและลดโอกาสพ่ายแพ้ให้น้อยลง (ชรัติอุ่มสัมฤทธิ์, 2550, หน้า 100)

จุลชีพ ชินวรรณโณ (2546,หน้า 6) ได้กล่าวว่า ยุทธศาสตร์ในความหมายที่แคบคือ ยุทธศาสตร์ เป็นแนวทางในการใช้กำลัง หรือขู่ว่าจะใช้กำลังทหารในการดำเนินความสัมพันธ์ระหว่างประเทศ ด้วยการวางแผนการใช้กำลังอย่างแยบยล เพื่อให้บรรลุเป้าประสงค์ทางการเมือง อีกทั้งเป็นศิลปะการใช้กำลังเพื่อประสบชัยชนะในสมรภูมิ เป็นการใช้กำลังอย่างไร เมื่อไหร่ ที่ไหน เพื่อจัดการข้าศึกแต่ในปัจจุบัน คำว่า “ยุทธศาสตร์” ได้ถูกขยายความและนำไปใช้ในวงการต่าง ๆ

นอกเหนือจากวงการทหาร โดยเฉพาะอย่างยิ่ง ในภาคเอกชน ความหมายของยุทธศาสตร์ จึงขยายความไปถึง การวางแผน การปฏิบัติการอย่างเป็นระบบเพื่อให้บรรลุวัตถุประสงค์ที่กำหนดไว้ สอดคล้องกับแนวคิดของ Carroll, 2008 (cited in Liotta and Lloyd, 2004: 1) ได้กล่าวว่า ทั้งหลายทั้งมวลแล้ว ยุทธศาสตร์ไม่ใช่เรื่องที่จะแก้ปัญหาการเมืองได้อย่างรวดเร็ว ยุทธศาสตร์เป็นเครื่องมือที่มุ่งเน้นผลระยะยาว ซึ่งจะช่วยให้เกิดความผกผันต่อสภาวะแวดล้อมในอนาคต

ยุทธศาสตร์ของการก่อการร้าย

ยุทธศาสตร์ของการก่อการร้าย อาจจำแนกเป็นยุทธศาสตร์ทางการเมือง ยุทธศาสตร์ทางเศรษฐกิจ ยุทธศาสตร์ทางทหาร ยุทธศาสตร์ด้านจิตวิทยา และยุทธศาสตร์ทางสังคม

ยุทธศาสตร์ทางการเมือง มีจุดประสงค์จะทำให้การบริหารงานของรับเกิดความสับสน ชะงักงันไม่ต่อเนื่อง ทำให้เกิดความไม่แน่ใจ ความสามารถของรัฐที่จะบริหารประเทศ ยุทธศาสตร์เศรษฐกิจ มุ่งทำให้ระบบธุรกิจเกิดปัญหาการชะงักงันของภาคส่วนต่าง ๆ ในการบริหารแรงงาน อุตสาหกรรม การลงทุน การเงินการธนาคาร และอื่น ๆ ยุทธศาสตร์ทางทหารจะมุ่งให้แตกแยกภายในหมู่ทหาร ความขัดแย้งภายในกองทัพ และระหว่างกองทัพ ยุยงให้ทหารขัดแย้งกับประชาชน ทำให้ประชาชนไม่พอใจทหาร รวมถึงการก่อวินาศกรรมที่ตั้งทางทหารและอาวุธยุทโธปกรณ์ ยุทธศาสตร์ด้านจิตวิทยา โฆษณาชวนเชื่อให้เห็นจุดอ่อนข้อบกพร่องของรัฐที่กระทำต่อประชาชน และแสวงหาผู้ร่วมอุดมการณ์ และยุทธศาสตร์ทางสังคม ต้องการให้มีการเปลี่ยนแปลงจัดระบบสังคมเสียใหม่ ทำลายภาคประชาสังคม และบีบบังคับให้ประชาชน เกิดความกลัวและหันมาสนับสนุน (กองข่าวกองทัพภาคที่ 2, ม.ป.ป., หน้า 11 – 12)

จากความหมายดังกล่าวข้างต้น ผู้วิจัยสรุปได้ว่า ยุทธศาสตร์ เป็นศาสตร์และศิลป์ที่มีองค์ประกอบหลัก 3 ประการคือ1.วัตถุประสงค์ (Ends) 2. วิธีการไปสู่เป้าหมาย (Ways)และ 3. เครื่องมือ (Means) ที่จะบรรลุเป็นยุทธศาสตร์ที่สำเร็จได้ ในความหมายของยุทธศาสตร์ เป็นคำที่เริ่มมาจากคำศัพท์ทางทหาร เพื่อใช้ในการรบ แต่ปัจจุบันได้มาการนำมาใช้แพร่หลายในหลาย ๆ ด้าน ยุทธศาสตร์เป็นแนวทาง วิธีการ เทคนิคที่ดำเนินการเพื่อให้บรรลุวัตถุที่กำหนดไว้ โดยเป้าหมายยุทธศาสตร์ต้องมีการกำหนดห้วงเวลาที่เป็นไปได้ในทางปฏิบัติ โดยยุทธศาสตร์มุ่งเน้นในการกำหนดเป้าหมายในระยะยาว พร้อมทั้งวิธีการและทรัพยากรให้บรรลุเป้าหมาย ส่วนยุทธวิธีเป็นการมุ่งวิธีการปฏิบัติเพื่อให้ได้ผลสัมฤทธิ์ตามความต้องการของผู้กำหนด

2. กระบวนการจัดทำยุทธศาสตร์

ยุทธศาสตร์เริ่มจากแนวคิดที่จะใช้ทรัพยากรขององค์การอย่างมีประสิทธิภาพ ภายใต้สภาพแวดล้อมที่เปลี่ยนแปลง ยุทธศาสตร์มีขอบเขตของการทำงานในระยะยาว จึงแตกต่างจากการวางแผนในการแข่งขันเพียงครั้งเดียว สนามเดียว จึงสรุปได้ว่า ยุทธศาสตร์ (Strategy) เป็นวิธีการ

(Mean) มีทิศทาง (Way) ที่จะบรรลุวัตถุประสงค์ (End)สำหรับกระบวนการทางยุทธศาสตร์ที่ใช้แตกต่างกันออกไป 2 ลักษณะ คือ กระบวนการทางยุทธศาสตร์ที่ใช้ทางด้านพลเรือน โดยเฉพาะด้านธุรกิจเรียกว่า กระบวนการจัดการเชิงกลยุทธ์ (Strategic management process) ส่วนทางด้านความมั่นคงและการทหารเรียกว่า กระบวนการทางยุทธศาสตร์ (The strategic process) ดังนี้

การจัดการเชิงกลยุทธ์ เป็นการกำหนดวิสัยทัศน์ ทิศทาง ภารกิจและวัตถุประสงค์ขององค์กรอย่างเป็นระบบ เพื่อให้องค์กรมีทิศทางและเป้าหมายที่ชัดเจน รวมทั้งเป็นการกำหนดวิธีการหรือแนวทางในการดำเนินงาน โดยในการกำหนดแนวทางในการดำเนินงานนี้องค์กรธุรกิจจะต้องทำการวิเคราะห์ และประเมินปัจจัยต่าง ๆ ทั้งภายในและภายนอกองค์การ เพื่อคิดค้นแนวทางการดำเนินงานที่เหมาะสมที่สุด ท่ามกลางการเปลี่ยนแปลงของปัจจัยต่าง ๆ การวางแผน และประยุกต์สำหรับธุรกิจเป็นหน้าที่หลักของผู้บริหารองค์กร การจัดทำและปฏิบัติตามแผนกลยุทธ์ จัดเป็นหน้าที่ซึ่งมีความสำคัญเป็นอันดับต้น รวมทั้งเป็นหน้าที่ซึ่งมีอิทธิพลต่อการดำเนินการในระยะยาวขององค์กร (พักตร์ผจง วัฒนสินธุ์ อ้างถึงใน เฉลิม คูหาวิชานันท์, เรือรบ เมืองมั่น, 2545: 45 – 46)

(Porter, 2005) ให้คำนิยามยุทธศาสตร์ว่าการกำหนดฐานะขององค์กรโดยการสร้างสมดุลและความเหมาะสมในการดำเนินกิจกรรมทั้งปวง

ระดับของยุทธศาสตร์ 3 ระดับ คือ

1. ยุทธศาสตร์ระดับบรรษัท (Corporate) หรือยุทธศาสตร์ในภาพรวมทางธุรกิจ (Multi business strategy) หมายถึง นิยามคุณค่า เป้าหมายที่เกี่ยวกับเงินและเป้าหมายที่ไม่เกี่ยวกับการเงิน ซึ่งมีศูนย์กลางอยู่ที่การกำหนด การสร้างหรือการได้มาซึ่งทรัพยากรและสมรรถนะในการตัดสินใจว่า องค์การจะดำเนินอย่างไรในการเป็นพันธมิตร หรือการแข่งขันในเชิงธุรกิจ ยุทธศาสตร์บรรษัทจะกำหนดว่าการแบ่งทรัพยากรควรดำเนินการอย่างไรและมีข้อจำกัดอย่างไร

2. ยุทธศาสตร์ระดับการแข่งขัน (Competitive strategy) หรือยุทธศาสตร์ระดับหน่วยงานทางธุรกิจ (Business unit strategy) อธิบายวิธีที่องค์กรจะเข้าสู่การแข่งขัน เช่น วิธีการสร้างคุณค่าขององค์กรซึ่งเกี่ยวข้องกับวิสัยทัศน์ (ความคลุมเครือ หรือความชัดเจนในสิ่งที่ลูกค้าพึงจะได้รับ นอกจากนั้นยุทธศาสตร์การแข่งขันยังเป็นมากกว่าวิสัยทัศน์ คือ เป็นกิจกรรมเฉพาะและกระบวนการในการปฏิบัติการขององค์กร ซึ่งสามารถสร้างอัตลักษณ์แห่งคุณค่าให้แก่ลูกค้า สร้างความเหมาะสมในการดำเนินกิจกรรมทั้งปวง เพื่อสร้างความแข็งแกร่งในด้านศักยภาพ ความได้เปรียบให้แก่ฐานะขององค์กรในเชิงการแข่งขัน

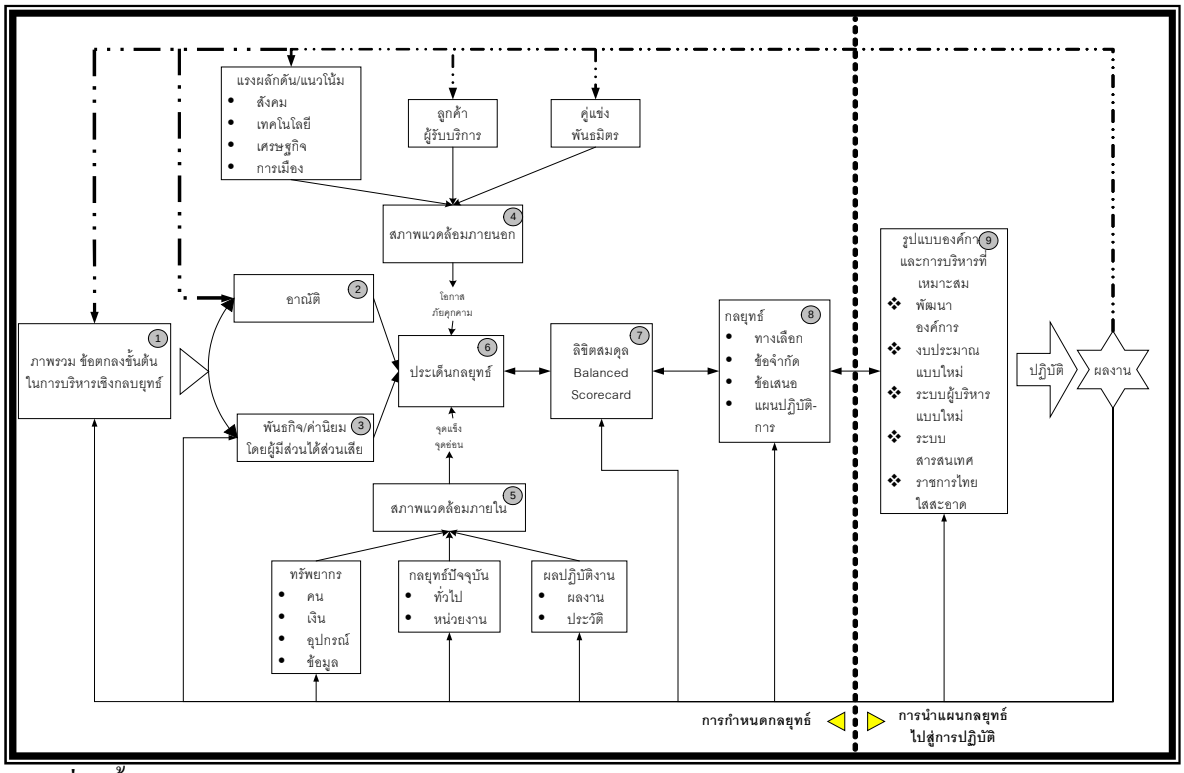
3. ยุทธศาสตร์ระดับปฏิบัติการ (Functional strategies) เช่นยุทธศาสตร์การตลาด ยุทธศาสตร์การเงิน ยุทธศาสตร์การวิจัย และยุทธศาสตร์การปฏิบัติงาน สร้างความแข็งแกร่งให้ยุทธศาสตร์การแข่งขันขององค์กร อธิบายถึงกิจกรรมและกระบวนการที่ทำให้องค์กรได้รับ

ผลประโยชน์ในฐานะของการแข่งขัน การอธิบายและวิเคราะห์ยุทธศาสตร์ ลักษณะการปฏิบัติงานจะแสดงให้เห็นชัดเจนว่าแต่ละหน่วยงานมีความเหมาะสมกับยุทธศาสตร์หรือไม่และชี้ให้เห็นว่าความคลุมเครือในด้านความร่วมมือระหว่างหน่วยงาน

ขั้นตอนการจัดทำแผนยุทธศาสตร์ (ดำรงค์ วัฒนา, 2548, หน้า 18-23)

1. ขั้นตอนการทำข้อตกลงเบื้องต้น

การเริ่มต้นการจัดทำแผนยุทธศาสตร์เป็นขั้นตอนที่สำคัญอย่างยิ่ง มีผู้กล่าวว่าหากเริ่มต้นดีงานก็จะสำเร็จไปครึ่งหนึ่งดังนั้นองค์การจะต้องแสดงความจำเป็นในการพัฒนาแผนยุทธศาสตร์ให้แก่สมาชิกขององค์การโดยเฉพาะอย่างยิ่งผู้บริหารระดับสูงไม่เพียงแต่การยอมรับความสำคัญของแผนยุทธศาสตร์เท่านั้นแต่จะต้องแสดงออกให้เป็นรูปธรรมได้แก่การดำเนินการเป็นลายลักษณ์อักษรให้มีการจัดทำแผนและผู้บริหารจะเป็นเจ้าของงานเป็นผู้ผลักดันงานและสนับสนุนให้ดำเนินไปให้สำเร็จทั้งนี้จะต้องแสดงให้เป็นรูปธรรม ผู้บริหารทุกระดับจะตกลงในหลักการซึ่งจะใช้เป็นรากฐานของการจัดทำแผนยุทธศาสตร์โดยเชื่อมโยงกับแผนในระดับสูงขึ้นไปเช่นแผนในระดับชาติรวมทั้งสร้างความสัมพันธ์กับนโยบายของรัฐบาลให้ชัดเจนรวมทั้งการใช้เครือข่ายภายนอกที่มีความเชี่ยวชาญด้านการวางแผนยุทธศาสตร์และด้านต่างๆที่เกี่ยวข้องมาช่วยเหลือโดยมีการกำหนดเจ้าของงาน (Project owner) เป็นผู้บริหารงานในภาพรวมโดยอาศัยแผนยุทธศาสตร์เป็นเครื่องมือเพื่อให้องค์การสามารถนำกลยุทธ์ไปสู่การปฏิบัติได้สำเร็จกลยุทธ์ในการจัดทำแผนยุทธศาสตร์มีหลายกลยุทธ์ซึ่งพอสรุปได้ดังนี้



ภาพที่ 5 ขั้นตอนการจัดทำแผนยุทธศาสตร์(ดำรง วัฒนา, 2548)

1.1 การปรับเปลี่ยนโดยการสั่งการ

การปรับเปลี่ยนองค์การด้วยวิธีนี้เป็นการที่ผู้บริหารใช้อำนาจสั่งการอย่างเป็นทางการให้มีการผู้เกี่ยวข้องปรับเปลี่ยนในส่วนต่างๆที่จำเป็นซึ่งโดยผู้ที่ปฏิบัติงานมีหน้าที่เพียงปฏิบัติตามคำสั่งเท่านั้นซึ่งเป็นวิธีที่เหมาะสมเฉพาะในสถานการณ์ที่วิกฤติที่ทุกส่วนมีความสับสนวุ่นวายและในสถานการณ์ที่ทุกอย่างสงบเรียบร้อยราบรื่นอย่างมากโดยที่ทุกคนในองค์การพร้อมจะปฏิบัติตามทุกอย่างที่ผู้นำต้องการ

1.2 การปรับเปลี่ยนโดยการให้มีส่วนร่วมในวงจำกัด

การปรับเปลี่ยนองค์การด้วยวิธีนี้ใช้การเปิดโอกาสให้บุคลากรที่มีสำคัญโดยตำแหน่งหน้าที่หรือโดยการยอมรับอย่างไม่เป็นทางการเข้ามามีส่วนร่วมในการเป็นผู้นำในการจัดทำแผนยุทธศาสตร์สำหรับการปรับเปลี่ยนองค์การซึ่งอาจมีคณะกรรมการทำงานซึ่งอาจจะเป็นการลดกระแสการต่อต้านได้บ้างและเป็นการระดมความคิดความร่วมมือจากหลายฝ่ายแต่อาจจะมีปัญหาเรื่องความล่าช้าความเบี่ยงเบนจากเป้าหมายเดิมได้

1.3 การปรับเปลี่ยนองค์การโดยการสร้างกระแสวัฒนธรรมใหม่

วิธีนี้ใช้การเปิดโอกาสให้ทุกๆคนในองค์การสามารถริเริ่มให้มีการเปลี่ยนแปลงต่างๆในองค์การได้อย่างกว้างขวางที่สุดโดยให้ทุกคนเปลี่ยนจากการทำงานที่ยึดกฎหมายหรือความเคยชินตามสามัญสำนึกผิดๆมาเป็นการใช้แผนยุทธศาสตร์เป็นเครื่องมือโดยอาจจัดให้มีระบบข้อเสนอแนะการจัดให้มีการจัดระบบงานกันเองในทีม (Autonomous work team) หรือการจัดให้มีระบบการจัดการคุณภาพโดยรวม (Total quality management) ฯลฯวิธีการเหล่านี้อาจช่วยให้มีการเปลี่ยนแปลงองค์การตามแผนหลักในจุดต่างๆอยู่เสมอซึ่งเป็นการทำให้องค์การเรียนรู้และปรับตัวอยู่ตลอดเวลาแต่การเปลี่ยนแปลงนั้นอาจเป็นไปเพียงในวงจำกัดหากองค์การไม่มีระบบการสื่อสารประชาสัมพันธ์ภายในที่ดีพอและที่สำคัญก็คือการเปลี่ยนแปลงที่เกิดขึ้นอาจไม่สอดคล้องกับกลยุทธ์ที่วางไว้และเมื่อผู้ปฏิบัติงานได้มีส่วนร่วมปรับสร้างสิ่งใดขึ้นมาแล้วความรู้สึกหวงแหนเป็นเจ้าของอาจเป็นอุปสรรคต่อการเปลี่ยนแปลงสิ่งที่เขาคิดริเริ่มขึ้นมาได้

1.4 กลยุทธ์แบบผสม

การนำกลยุทธ์การเปลี่ยนแปลงองค์การหลายๆแบบมาใช้ร่วมกันเช่นธนาคารพาณิชย์แห่งหนึ่งใช้กลยุทธ์การสั่งโดยผู้บริหารระดับสูงลงมาเป็นวิทยากรในการบรรยายเรื่องการวางแผนยุทธศาสตร์และปรับกลยุทธ์การดำเนินงานขององค์การด้วยตัวเองการประกอบกับการสร้างทีมงานการรื้อปรับระบบงานของสาขาและการส่งเสริมกระบวนการเรียนรู้ขององค์การอย่างต่อเนื่องซึ่งเป็นการพัฒนาส่วนต่างๆขององค์การด้วยกลยุทธ์การเปลี่ยนแปลงองค์การที่ต่างกันในสภาพการณ์ที่เปลี่ยนแปลงไปอย่างรวดเร็วและรุนแรงนอกจากองค์การจะต้องมีการวางกลยุทธ์ให้ดีแล้วการพัฒนาขีดความสามารถขององค์การในการปรับตัวเองขององค์การก็เป็นสิ่งสำคัญซึ่งเป็นตัวบ่งชี้ถึงความสามารถในการเรียนรู้ขององค์การองค์การที่เรียนรู้ปรับตัวได้อย่างรวดเร็วและมีประสิทธิภาพก็จะสามารถอยู่รอดและเจริญก้าวหน้าได้ดีกว่าส่วนองค์การที่ไม่สามารถที่จะเรียนรู้ได้ดีก็จะมีโอกาสที่จะประสบความล้มเหลวได้ง่าย

1.5 กลยุทธ์ในองค์การที่เรียนรู้จะต้องมีการเรียนรู้ร่วมกันเป็นทีม (Team learning)

การแบ่งปันแลกเปลี่ยนถ่ายทอดข้อมูลระหว่างกันและกันมีความสำคัญอย่างยิ่งทั้งในเรื่องของความรู้ใหม่ๆที่ได้มาจากการค้นคิดหรือจากภายนอกและในด้านของประสบการณ์การเรียนรู้ซึ่งอาจจะมีทั้งความสำเร็จและความล้มเหลวข้อสำคัญคือการนำความรู้เหล่านี้มาแลกเปลี่ยนกันย่อมทำให้เกิดการแพร่กระจาย (Diffusion) ของวิทยาการใหม่ๆส่วนในด้านการนำความล้มเหลวมาแลกเปลี่ยนกันนั้นก็จะช่วยไม่ให้ต้องมีคนอื่นมาทำผิดซ้ำในเรื่องที่เคยมีคนพลาดมาแล้วนั่นเองและนอกจากนี้การเรียนรู้เป็นทีมยังควรครอบคลุมไปถึงการเรียนรู้เกี่ยวกับการทำงานร่วมกันเป็นทีมด้วยซึ่งการเรียนรู้และพัฒนาในเรื่องนี้ก็จะช่วยให้การทำงานร่วมกันในองค์การมีความเป็นทีมที่ดีขึ้นซึ่งจะช่วยให้สมาชิกแต่ละคนสามารถแสดงศักยภาพที่มีอยู่ออกมาได้อย่างเต็มที่ด้วย

1.6 การศึกษาอาณัติ (Mandate)

องค์การได้รับการจัดตั้งมาจากความจำเป็นตามอาณัติที่มาจากแหล่งต่างๆองค์การภาครัฐต้องดำเนินตามข้อกำหนดของกฎหมายและนโยบายของรัฐบาลองค์การจึงต้องให้ความสำคัญต่ออาณัติขององค์การ

SWOT Analysis Framework

กีรติ ยศยิ่งยง (2549,หน้า 129 – 131) กล่าวว่า SWOT Analysis Framework เป็นการวิเคราะห์สภาพแวดล้อมทั้งภายในและภายนอกองค์กรอย่างละเอียด เพื่อให้ได้มาซึ่งข้อมูล เกี่ยวกับแหล่งที่มาและขีดความสามารถขององค์กรกับสภาพแวดล้อมทางการแข่งขัน อันเป็นส่วนสำคัญในการออกแบบการพัฒนาองค์การ ซึ่งสามารถสรุปได้ดังนี้

1.จุดแข็งของขององค์การเป็นแหล่งที่มา และขีดความสามารถที่จะใช้เป็นพื้นฐานในการพัฒนาขีดความสามารถทางการแข่งขัน

2. จุดอ่อนขององค์การเป็นสิ่งที่ขาดแคลนของจุดแข็ง

3.โอกาสเป็นการวิเคราะห์สภาพแวดล้อมภายนอกซึ่งอาจเป็นการประเมินโอกาสใหม่สำหรับการเติบโตหรือกการทำกำไรขององค์การ

4. ภัยคุกคามเป็นการเปลี่ยนแปลงสภาพแวดล้อมภายนอกซึ่งอาจเป็นภัยคุกคามในปัจจุบันขององค์การ

The SWOT/TOWS Matrix เป็นการพัฒนากลยุทธ์ จับคู่พิจารณามีลักษณะดังนี้

S – O Strategies เป็นการไล่ตามโอกาสซึ่งเหมาะกับจุดแข็งขององค์การ

S – T Strategies เป็นการกำหนดวิธีโดยการใช้จุดแข็งขององค์การลดจุดที่อาจถูกโจมตีได้ง่ายขององค์การจากภัยคุกคามภายนอก

W – O Strategies เป็นการพิชิตจุดอ่อนเพื่อไล่ตามให้ทันโอกาส

W –T Strategies เป็นการสร้างแผนการต่อต้านเพื่อป้องกันจุดอ่อนขององค์การจากการทำให้เกิดผลกระทบจากภัยคุกคามภายนอก

การสรุปจุดแข็ง จุดอ่อน โอกาสและภัยคุกคามหรือข้อจำกัดหลังจากการดำเนินการวิเคราะห์สภาพแวดล้อมภายนอกและภายในองค์การ หรือสถานการณ์ภายนอกและสถานการณ์ภายใน จนสามารถสังเคราะห์โอกาสและภัยคุกคามกับจุดแข็งและจุดอ่อน ประมวลข้อมูลสองด้านเข้าด้วยกัน เพื่อสรุปและอาจสร้างตารางความสัมพันธ์แบบเมทริกซ์ Matrix ของปัจจัยเชิงกลยุทธ์ทั้งสองด้าน (ปกรณ์ ปรียากร, 2547, หน้า 130)

The 7’ Mckinsey Model

The 7’ Mckinsey Model ในช่วงปลายศตวรรษที่ 1970Tom Peter และ Robert Waterman ที่ปรึกษาของบริษัท แมคคินซี (Mckinsey & Co. Co., Ltd) อธิบายความสำคัญของประสิทธิภาพของทีมงานในองค์การ เพราะองค์การจะประสบความสำเร็จได้ จำเป็นต้องอาศัยปัจจัยองค์ประกอบขององค์การที่สำคัญ 7 ประการ คือ กลยุทธ์ โครงสร้าง ระบบ วิถีปฏิบัติ บุคลากร ทักษะและค่านิยมร่วม ความสัมพันธ์ระหว่างปัจจัยต่าง ๆ เชื่อมโยงระหว่างกัน ดังนั้นในการกำหนดยุทธศาสตร์จำเป็นต้องคำนึงถึงปัจจัยต่าง ๆ อีก 6 ประการ อย่างระมัดระวังการให้น้ำหนักสำคัญแต่เพียงปัจจัยเดียวย่อมเป็นอันตรายจะเป็นผลให้ความล้มเหลวมีโอกาสเกิดขึ้นและแต่ละปัจจัยจะมีความสัมพันธ์และมีลักษณะเป็นไปในแนวทางหรือทิศทางเดียวกันกับปัจจัยอื่น ๆ คือ

1.กลยุทธ์เป็นการปฏิบัติตามแผนขององค์การในการเตรียมการตอบโต้หรือรับมือกับการเปลี่ยนแปลงที่จะเกิดขึ้นจากสภาพแวดล้อมภายนอก

2. โครงสร้างพื้นฐานสำหรับความเชี่ยวชาญและความร่วมมือที่มีอิทธิพลสำคัญต่อกลยุทธ์ ขนาดและความหลากหลายขององค์การ

3. ระบบเป็นกระบวนการที่เป็นทางการและไม่เป็นทางการที่สนับสนุนกลยุทธ์และโครงสร้าง

4. วิถีปฏิบัติหรือวัฒนธรรม ประกอบด้วยองค์ประกอบ 2 องค์ประกอบคือ วัฒนธรรมองค์การเป็นสิ่งที่มีอิทธิพลหรือครอบงำคุณค่า ความเชื่อ และรูปแบบหรือบรรทัดฐานขององค์การซึ่งจะมีการพัฒนาอยู่ตลอดเวลาและมีความสัมพันธ์กับรูปแบบที่ยาวนาน ทนทานกับวิถีวิติขององค์การและอีกองค์ประกอบหนึ่ง คือรูปแบบการจัดการเป็นรูปแบบและวิถีการดำเนินการบริหารจัดการของผู้บริหารทั้งในด้านการปฏิบัติงาน ความมุ่งมั่น ฯลฯ อันเป็นพื้นฐานความรับผิดชอบของผู้บริหาร

5. บุคลากรเป็นกระบวนการทางจัดการทรัพยากรมนุษย์ขององค์การ ทั้งในการพัฒนาบุคลากร การสร้างบรรยากาศการทำงาน การสร้างคุณค่าพื้นฐาน การจ้างงานและการพัฒนาสายอาชีพ

6. ทักษะเป็นขีดความสามารถพิเศษของบุคลากรองค์การ ซึ่งจะต้องพิจารณาว่าองค์การได้ทำสิ่งที่ดีเพื่อเพิ่มขีดความสามารถหรือไม่ อะไรบ้าง และมีการเปลี่ยนแปลง พัฒนาเพื่อเพิ่มขีดความสามารถอย่างไร

7. ค่านิยมร่วมหรือเป้าหมายที่สำคัญขององค์การ เป็นรูปแบบการแนะนำแนวคิดหรือความคิดพื้นฐานขององค์การซึ่งเป็นเป้าหมายหรือเป็นสิ่งที่องค์การต้องการ

การมองอนาคตด้วยวิธีการวิเคราะห์สถานการณ์(Scenario analysis)

(Gray, 2003)กล่าวถึง การวิเคราะห์สถานการณ์ (Scenario analysis) เป็นเทคนิคที่ง่ายที่สุดและธรรมดาที่สุดในการวิเคราะห์ความเสี่ยง การเข้าถึงความเสี่ยงในเรื่องเหตุการณ์ที่ไม่พึงปรารถนาจะให้เกิดขึ้น ผลรวมของเหตุการณ์และผู้ที่เกี่ยวข้องขนาดหรือความสูญเสียขอเหตุการณ์ที่ส่งผลกระทบ โอกาสที่จะเกิดเหตุการณ์ เมื่อใดที่เหตุการณ์จะส่งผลต่อโครงการ และความสัมพันธ์กับส่วนอื่น ๆ โดยการใช้ตารางความเสี่ยง

การวิเคราะห์สถานการณ์ (Scenario analysis)ถือเป็นการผสมผสานระหว่างศาสตร์และศิลป์ เนื่องจากถ้าทำได้ดี จะทำให้ผู้บริหารและทุกคนในองค์กรได้เกิดภาพความเข้าใจร่วมกันเกี่ยวกับภาพและความเป็นไปได้ที่จะเกิดขึ้นในอนาคต รวมทั้งจะทำให้สามารถเตรียมตัวต่อการเปลี่ยนแปลงที่อาจเกิดขึ้นในอนาคต ประโยชน์ที่สำคัญประการหนึ่งของการพัฒนาสถานการณ์ (Scenario) ไม่ได้อยู่ที่การศึกษาและวิเคราะห์ต่อการเปลี่ยนแปลงของปัจจัยภายนอกเท่านั้น แต่ยังทำให้ผู้บริหารได้กลับมาทบทวนต่อทิศทางและการดำเนินงานขององค์กร กระบวนการในการพัฒนาสถานการณ์ (Scenario) ที่มีการทำอย่างต่อเนื่องถือเป็นกระบวนการในการพัฒนาผู้บริหารอย่างต่อเนื่อง เนื่องจากต้องมีการทำวิจัยและทำให้ผู้บริหารได้ร่วมกันคิดว่าอะไรคือปัจจัยภายนอกเหล่านั้น และการวางแผนสถานการณ์(Scenario planning)เป็นเครื่องมือทางการบริหารที่ถือว่ามีประโยชน์อย่างมาก ถ้าองค์กรได้มีการนำมาใช้อย่างจริงจัง เนื่องจากประโยชน์ของการวางแผนสถานการณ์ (Scenario planning)ไม่ได้อยู่ที่ผลอย่างเดียว แต่ยังเป็นกระบวนการในการพัฒนาบุคลกรและสร้างบรรยากาศของความเข้าใจร่วมกันในองค์กรโดยมีวิธีการดังนี้

หาสิ่งที่จะพิจารณา (Where to look) โดยถามว่าอะไรคือปัจจัยที่สำคัญทางกลยุทธ์ขององค์กร รวมทั้งประเด็นที่ผู้บริหารคิดว่าอะไรเป็นปัจจัยที่มีความสำคัญต่อความสำเร็จขององค์กร

เริ่มต้นจากการหาปัจจัยชี้นำ (Drivers) ที่นำไปสู่ความสำเร็จขององค์กรโดยการวิเคราะห์ SWOT ภายหลังจาการวิเคราะห์ SWOT ให้นำผลที่ได้จากการวิเคราะห์ SWOT มาเพื่อกำหนดวาระของสถานการณ์(Scenario agenda)หรือการประกันของสถานการณ์ (Scenario) ซึ่งเป็นประเด็นสำคัญทางด้านภาวะแวดล้อมที่องค์กรจะต้องพิจารณาถึงซึ่งส่วนใหญ่ต้องเป็นประเด็นหลักกว้าง ๆ ไม่เกิน 4 ประเด็นโดยเฉพาะประเด็นเหล่านี้ ต้องเป็นประเด็นที่มีความไม่แน่นอนที่อาจเกิดขึ้นในอนาคต โดยบริษัทมีความกังวลและประเด็นแต่ละประเด็นที่ควรจะมีความเป็นอิสระจากกัน นั่นคือไม่ควรเป็นประเด็นที่มีความสัมพันธ์กัน หลังจากกำหนดวาระของสถานการณ์ที่สำคัญได้แล้ว ก็ให้จัดเรียงตามลำดับความสำคัญของประเด็นในแต่ละด้าน หลังจากนั้นก็ให้กำหนดระยะเวลาแต่ละประการ โดยมองไปในอนาคตว่ากำหนดการของสถานการณ์ในแต่ละประการจะส่งผลกระทบต่อกลยุทธ์และการตัดสินใจในปัจจุบันอย่างไรจำนวนของสถานการณ์ที่เหมาะสมนั้นไม่ควรต่ำกว่า

สองและไม่ควรที่จะเกินสี่ โดยเมื่อกำหนดวาระของสถานการณ์ (Scenario agenda) เสร็จสิ้นแล้วก็นำวาระของสถานการณ์(Scenario agenda) แต่ละประเด็นมาเปรียบเทียบกันเพื่อกำหนดขึ้นมาเป็นสถานการณ์หรือความเป็นไปได้ในอนาคตตามวาระของสถานการณ์(Scenario agenda)ที่กำหนดขึ้น

สรุปได้ว่ายุทธศาสตร์เป็นศาสตร์และศิลป์ในการดำเนินการเพื่อให้บรรลุวัตถุประสงค์โดยใช้พลังอำนาจในชาติ ในทางทหาร หมายถึงการใช้ศิลปะในการนำทัพหรืออำนวยการทั้งปวงเกี่ยวกับการนำทัพเพื่อให้ได้ชัยชนะ แต่ในปัจจุบัน การจัดทำยุทธศาสตร์ได้นำมาใช้ทั้งในภาครัฐและเอกชน เพื่อให้บรรลุวัตถุประสงค์ (Objective) หรือจุดมุ่งหมาย (Ends) เข้ากับวิถีหรือหนทาง (Ways) และวิธีการหรือเครื่องมือ (Means)

องค์การแห่งการเรียนรู้ (Learning organization)

องค์การแห่งการเรียนรู้ เป็นการทำให้คนในองค์การเรียนรู้ปัจจัยต่าง ๆ ทั้งจากภายในและภายนอก โดยนำความรู้มาพัฒนาตนเองและพัฒนาองค์การเพื่อองค์การเรียนรู้ปัจจัยต่าง ๆ ทั้งจากภายในและภายนอก หรือกล่าวได้ว่า องค์การแห่งการเรียนรู้เป็นองค์การที่มีการปรับเปลี่ยนและค้นหาวิธีการใหม่ ๆ ในการพัฒนาผลิตภัณฑ์หรือบริการอันนำมาซึ่งการเพิ่มประสิทธิภาพและประสิทธิผลในการดำเนินงานขององค์การ

องค์การแห่งการเรียนรู้ หมายถึง องค์การที่ส่งเสริมให้มีการสื่อสารและการให้ความร่วมมือจากบุคลากรทุกคนในองค์การ ทั้งในด้านการวิเคราะห์และการแก้ปัญหาร่วมกัน การดำเนินการเพื่อให้องค์การเกิดการเรียนรู้ในประสบการณ์ใหม่ ๆ อีกทั้งให้ดำเนินการปรับปรุงและเพิ่มขีดความสามารถขององค์การอย่างต่อเนื่อง (Daft, 2001)

องค์การแห่งการเรียนรู้ หมายถึง องค์การที่มุ่งเน้นและจูงใจให้สมาชิกทุกคนมีความกระตือรือร้นที่จะพัฒนาตนเองอยู่ตลอดเวลาเพื่อเพิ่มศักยภาพของตนเองและขององค์การ ทั้งนี้เนื่องจากการเปลี่ยนแปลงที่เกิดขึ้นอย่างรวดเร็วทั้งในด้านเศรษฐกิจ สังคม การเมือง วัฒนธรรม ภายใต้สภาวะที่เกิดการเปลี่ยนแปลงอย่างรวดเร็วและยากแก่การพยากรณ์ว่าจะเกิดอะไรขึ้น แต่ละคนจึงต้องพัฒนาตนเองให้เป็นบุคคลที่เรียนรู้อยู่ตลอดเวลา เพราะความรู้ที่เคยมีมาในอดีตถูกท้าทายโดยความรู้ใหม่ที่เกิดขึ้นตลอดเวลา (ธเนศ ขำเกิด, 2541)

Garvin (1993)กล่าวว่า องค์การแห่งการเรียนรู้เป็นทักษะในการสร้าง จัดหาและถ่ายทอดความรู้ รวมทั้งการปรับเปลี่ยนพฤติกรรมของบุคลากรที่จะมีผลต่อความรู้ใหม่ ๆ ขณะที่การจัดการความรู้ก็เป็นเรื่องสำคัญที่ทำให้เกิดการเรียนรู้และประยุกต์ใช้ความรู้ รวมทั้งแปลงความรู้ของคนไปเป็นความรู้ขององค์การ ซึ่งการที่จะเป็นองค์การแห่งการเรียนรู้ได้นั้นจะต้องมีทักษะ 5 ด้านคือ

1. การแก้ปัญหาอย่างเป็นระบบ

2. การทดลองปฏิบัติกับแนวทางใหม่

3. การเรียนรู้จากประสบการณ์ในอดีต

4. การเรียนรู้จากวิธีปฏิบัติที่เป็นเลิศของผู้อื่น

5. การถ่ายทอดความรู้ทั่วทั้งองค์การ

เปี่ยมพงศ์ นุ้ยบ้านด่าน (2543) การพัฒนาองค์การอาจเกิดไม่ได้ในชั่วข้ามคืน การเปลี่ยนแปลงด้วยความเร่งรีบมักนำมาซึ่งปัญหา ข้อขัดแย้งและความล้มเหลว การพัฒนาองค์การแห่งการเรียนรู้ ควรจะประกอบด้วย 3 ขั้นตอนดังนี้

1. ขั้นเตรียมความพร้อมที่จะเปลี่ยนแปลง (Unfreeze) สิ่งจำเป็นในขั้นตอนนี้คือ การสร้างกระแสของความต้องการการเปลี่ยนแปลง ระดมความคิดว่าต้องการการเปลี่ยนแปลงอย่างไร องค์การต้องการอะไร ในขณะเดียวกันก็ต้องคำนึงว่าผู้ใดมีอำนาจที่จะผลักดันในเกิดการเปลี่ยนแปลงในองค์การ

2. ขั้นตอนการเปลี่ยนแปลง(Change) การที่จะเปลี่ยนแปลงอย่างไรนั้น เราควรจะศึกษาองค์การของเราให้เข้าใจปัญหาที่แท้จริงเพื่อที่จะแก้ปัญหาได้ตรงจุด ซึ่งจะนำไปสู่ความสำเร็จในการเปลี่ยนแปลงองค์การ

3. ขั้นตอนหลังการเปลี่ยนแปลง (Refreeze) เมื่อองค์การเกิดการเปลี่ยนแปลงไปในทางที่ดีแล้วควรหยุดการเปลี่ยนแปลง แล้วกลับเข้าสู่ภาวะงานตามปกติ ถ้าองค์การมีการเปลี่ยนแปลงอยู่ตลอดเวลาคงไม่เป็นผลดีต่องานขององค์การเป็นแน่

จากแนวความคิดดังกล่าว สรุปได้ว่า การพัฒนาองค์การให้ประสบความสำเร็จ องค์การต้องพยายามแสวงหาแนวคิด วิธีการ และกระบวนการต่าง ๆ มาพัฒนา ปรับปรุงองค์การ ให้สามารถอยู่รอดมีการจัดการอย่างเป็นระบบผ่านกระบวนการแลกเปลี่ยนความรู้ซึ่งกันและกัน ทั้งในการพัฒนาบุคลากรและการพัฒนาองค์การ นำไปสู่การเป็นองค์การแห่งการเรียนรู้

แนวคิดเกี่ยวกับการก่อการร้ายและทฤษฎีการก่อการร้าย

แนวคิดเกี่ยวกับการก่อการร้ายความหมายของการก่อการร้ายมีการให้คำนิยามและความหมายที่แตกต่างกันออกไป ขึ้นอยู่กับแต่ละประเทศว่ามีมุมมองและประสบการณ์และความสัมพันธ์กับการก่อการร้าย รวมถึงองค์การระหว่างประเทศที่เกี่ยวข้อง Central Intelligence Agency (CIA) นิยามว่า “การก่อการร้ายหมายถึง ปฏิบัติการรุนแรงที่มีการคิดและการเตรียมการไว้ล่วงหน้าโดยที่มีเหตุจูงใจทางการเมือง กระทำต่อเป้าหมาย ซึ่งไม่ได้มีส่วนเกี่ยวข้องกับสงครามและ

ไม่มีศักยภาพในการทำการรบโดยกลุ่มขบวนการที่มิได้เป็นตัวแทนของรัฐในทางการเมืองระหว่างประเทศ หรือโดยกลุ่มสายลับของรัฐที่กระทำการในทางลับ" (ธันยวัต ชูส่งแสง, 2547, หน้า 1) คำนิยามของกระทรวงกลาโหมสหรัฐอเมริกา "การก่อการร้ายคือการใช้ความรุนแรงหรือการข่มขู่ว่าจะใช้ความรุนแรงที่ได้คิดการไว้ที่จะทำให้เกิดความรู้สึกหวาดกลัวโดยเจตนาที่จะบีบบังคับ หรือคุกคามรัฐบาลหรือสังคมกลุ่มใด เพื่อให้บรรลุจุดมุ่งหมาย ซึ่งโดยทั่วไปเป็นทางการเมือง ศาสนา และลัทธิ" (พงศธร สัตย์เจริญ, 2549, หน้า 4)อีกความหมายหนึ่ง คือยุทธศาสตร์ของความรุนแรงซึ่งมุ่งผลต่อทางจิตใจ เฉพาะอย่างยิ่งความหวาดกลัวต่อกลุ่มเป้าหมาย เพื่อบรรลุวัตถุประสงค์ทางการเมืองอย่างใดอย่างหนึ่งหรือหลายอย่างหรือเป็นแนวทางปฏิบัติหรือทฤษฎีที่อยู่เบื้องหลังแนวทางปฏิบัติซึ่งกลุ่มใดหรือพรรคใด ๆ นำไปใช้ปฏิบัติเพื่อบรรลุเป้าหมายของตนที่ตั้งใจไว้โดยการใช้ความรุนแรงอย่างเป็นระบบ (ศูนย์การศึกษาการก่อการร้าย, 2549)การกระทำที่เป็นลักษณะที่เรียกว่า การก่อการร้ายตามทฤษฎีสงคราม การก่อการร้ายถือเป็นการทำสงครามในลักษณะหนึ่ง ซึ่งเป็นสงครามที่มีต้นทุนต่ำที่สุดโดยการเปิดศึกได้ง่าย ความเสี่ยงต่ำ ความอยู่รอดสูง การสูญเสียชีวิตและทรัพย์สินก่อการก่อสงครามต่ำ (Geocities, 2004) ในขณะเดียวกันคู่กรณีมีความเสียหายสูงในลักษณะเชิงเปรียบเทียบ ตามประวัติศาสตร์ทางสงคราม พบว่า สงครามก่อการร้าย สงครามกบฏศึกหรือสงครามกองโจร และสงครามกลางเมืองมีความสัมพันธ์กันตรงที่ว่าเป็นการสร้างความศรัทธาหรือการสร้างความหวาดกลัวให้กับผู้ที่ไม่เกี่ยวข้องกับการสงครามต้องเลือกฝ่ายเข้าเป็นแนวร่วมเพื่อให้การสนับสนุนทั้งรูปธรรม เช่น การสนับสนุนเสบียง เสื้อผ้า อาวุธยุทโธปกรณ์และรูปธรรม เช่น การหาข่าว เป็นฐานเสียงแสดงพลังฐานความนิยม ซึ่งเป็นองค์ประกอบสำคัญในการสถาปนาอำนาจรัฐ เมื่อบรรลุเป้าหมายสงครามเรียบร้อยบริบูรณ์ ดังนั้น ประชาชนผู้ที่ไม่รู้เรื่องของแก่นสารความขัดแย้งหรือสาเหตุสำคัญของวิถีสงครามนั้น มักจะเป็นผู้รับกรรม แต่สิ่งที่ร้ายที่สุด คือ การนำเอาคนกลุ่มนี้มาเป็นเครื่องสังเวย เพื่อความสำเร็จในการต่อรองและการชักนำหรือใช้เป็นเครื่องเรียกร้องความสนใจจากมวลชน การก่อการร้ายเป็นส่วนหนึ่งของกลยุทธ์หรือยุทธวิธีในสงครามกองโจร (guerrilla warfare)(โกวิท วงศ์สุรวัฒน์, 2550)

สรุปได้ว่า การก่อการร้าย หมายถึง การกระทำความผิดโดยใช้กำลังประทุษร้ายหรือการกระทำการอันใดอันก่อให้เกิดอันตรายต่อชีวิต ร่างกายหรือเสรีภาพของผู้อื่นทำให้เกิดความเสียหายอย่างร้ายแรงต่อโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะทำให้เกิดการเสียหายต่อทรัพย์สินไม่ว่าของรัฐใด บุคคลใด หรือแก่สิ่งแวดล้อมโดยเป็นการกระทำ เพื่อขู่เข็ญหรือบังคับรัฐบาล ไม่ว่าเป็นประเทศใดหรือองค์กรใดระหว่างประเทศหรือสร้างความหวาดกลัวในหมู่ประชาชน

การก่อการร้าย (Terrorism) มีต้นกำเนิดมาจากเหตุการณ์ความรุนแรงทางการเมืองในประเทศฝรั่งเศสหลังการปฏิวัติเปลี่ยนแปลงการปกครองจากระบอบสมบูรณาญาสิทธิราชย์มาเป็น

ระบบสาธารณรัฐ เมื่อปี ค.ศ. 1789 เนื่องจากได้มีประชาชนกลุ่มหนึ่งพยายามก่อความไม่สงบขึ้น โดยใช้วัตถุระเบิดเป็นอาวุธ ยังผลให้มีผู้บาดเจ็บและเสียชีวิตจำนวนมากตลอดจนทรัพย์สินของประชาชนได้รับความเสียหายอยู่เสมอ ประกอบกับรัฐบาลฝรั่งเศสได้ดำเนินการปราบปรามและลงโทษผู้กระทำผิดอย่างรุนแรง ดังนั้น ชาวฝรั่งเศสจึงเรียกการกระทำอันรุนแรงนั้นว่าการก่อการร้ายและเรียกการปกครองของฝรั่งเศสในห้วงเวลาระหว่างปี ค.ศ. 1793 – 1794 ว่า ยุคแห่งความหวาดกลัว ตั้งแต่นั้นมาคำว่า ก่อการร้ายได้ถูกใช้อย่างกกว้างขวางในการอธิบายถึงพฤติกรรมที่รุนแรง แต่ถึงแม้คำว่าก่อการร้ายจะเพิ่งเกิดขึ้นในเร็ว ๆ นี้ แต่ยุทธวิธีของการก่อการร้ายก็ได้เกิดขึ้นมานานแล้ว โดยขบวนการปาเลสไตน์โบราณชาวยิว และกลุ่มหัวรุนแรงได้นำมาใช้เป็นครั้งแรกในการต่อต้านผู้ปกครองชาวเยอรมัน (Geocities, 2004)งานเขียนเกี่ยวกับก่อการร้ายในทศวรรษ 1960 ของ เท็ด โรเบิร์ตกูร์(Gurr, 1988) ได้นำเสนอเนื้อหาบางส่วนที่สรุปได้ว่า การก่อการร้ายประกอบด้วย องค์ประกอบ 3 ส่วนกล่าวคือ

1. มีรูปแบบและวิธีการที่เด่นชัด เช่น การลอบวางระเบิด การลอบวางเพลิงเป็นเครื่องมือรวมถึงยุทธศาสตร์และวิธีการที่เด่นชัดอื่น ๆ เพื่อบรรลุเป้าหมายตามที่ต้องการ

2. มีการพุ่งเป้าประสงค์ไปที่สาธารณะชนหรือเป้าหมายทางการเมือง รวมถึงตึกอาคาร สัญลักษณ์ทางการเมือง กองกำลังทหารและตำรวจ อีกทั้งเป้าหมายเอกชนที่อาจตกเป็นตัวเลือกสำหรับผู้ก่อการร้ายอันเนื่องมาจาก มีความเกี่ยวพันกับกลุ่มทางการเมืองหรือเนื่องจากเหตุผลส่วนบุคคล เป็นต้น

3. ลักษณะของการกระทำการก่อการร้าย จะมีการแสดงออกถึงการใช้ความรุนแรง (Violence) โดยกลุ่มหรือบุคคลหรือกลุ่มบุคคลอย่างลับ

เป็นแนวทางเดียวกับ ธอมัส พี. ทอร์นตัน (Thornton, 2005)ได้นำเสนอคำนิยามของการก่อการร้ายที่สำคัญ โดยอาศัยการใช้สัญลักษณ์ในการกระทำการก่อการร้าย ซึ่งกล่าวว่า การก่อการร้ายเป็นการกระทำเชิงสัญลักษณ์ มีจุดมุ่งหมายเพื่อสร้างอิทธิพลเหนือพฤติกรรมทางการเมืองของประเทศ โดยวิถีทางที่ไม่ปกติ อย่างการใช้ความรุนแรงเป็นเครื่องมือบรรลุเป้าหมาย ในมุมมองของทอร์นตัน การก่อการร้ายจึงเป็นเสมือนสัญลักษณ์การตอบโต้ทางการเมืองและเป็นอาวุธของผู้ที่อ่อนแอกว่าในการใช้ต่อต้านผู้ที่มีอำนาจเหนือกว่าทางการเมือง นอกจากนี้ทอร์นตัน เชื่อว่า การกระทำที่สร้างความหวาดกลัวคล้ายกับการจงใจเพื่อการโฆษณาการกระทำของตน โดยการส่งผ่านข้อความ สัญลักษณ์หรือการเตือนไปยังฝ่ายตรงกันข้าม ประชาชนที่เป็นกลาง และประชาชนที่เป็นพวกเดียวกันกับพวกเขาหรือเข้าข้างหรือเห็นอกเห็นใจกับขบวนการก่อการร้าย

จากการให้คำนิยามข้างต้น เห็นได้ชัดว่า การให้ความหมายของคำว่า การก่อการร้าย ของแต่ละประเทศมีความแตกต่างกัน ทำให้เกิดความไม่ชัดเจน จากความไม่ชัดเจนของลักษณะของตัว

บุคคลหรือกลุ่มการก่อการร้าย รูปแบบ วิธีการและวัตถุประสงค์ รวมทั้งการเปลี่ยนแปลงในทางสังคมและการเมือง ความเชื่อทางศาสนา อาจทำให้ปัญหาการนิยามคำว่าการก่อการร้ายซึ่งไม่อาจที่จะแก้ไขในอนาคตอันใกล้นี้ อย่างไรก็ตามมีนักวิชาการหลายท่านได้ให้ความหมายของการก่อการร้ายไว้แตกต่างกัน

ประเภทของการก่อการร้าย

ประเภทของการก่อการร้ายแบ่งได้ออกเป็นหลายประเภทมีรูปแบบแตกต่างกันออกไป ไม่ได้มีการกำหนดตายตัว มีเพียงแนวทางกว้าง ๆ ในการทำความเข้าใจในลักษณะของการกระทำหรือเกณฑ์อื่น ๆ ดังนี้

ดลยา เทียนทอง(2549)กล่าวว่าการแบ่งประเภทการก่อการร้ายตามขอบเขตของการปฏิบัติการ (Rage of operations) ซึ่งสามารถแยกออกได้เป็น 8 ประเภทดังนี้

1. การก่อการร้ายโดยรัฐ (State terrorism)

2. การก่อการร้ายที่เกิดจากความคิดเห็นที่ไม่ลงรอย (Dissident terrorism)

3. การก่อการร้ายโดยกลุ่มฝ่ายซ้าย (Leftist terrorism)

4. การก่อการร้ายโดยกลุ่มฝ่ายขวา (Rightist terrorism or Neo – fascism)

5. การก่อการร้ายในทางอาชญากรรม (Criminal dissident terrorism)

6. การก่อการร้ายโดยกลุ่มเคร่งศาสนา (Religious terrorism)

7.การก่อการร้ายโดยกลุ่มอนาธิปไตย (Anarchist Terrorism)

8. การก่อการร้ายสากล/ระหว่างประเทศ (International terrorism)

อีกแนวทางหนึ่ง Wilkinson ได้จัดแบ่งประเภทลัทธิของการก่อการร้ายตามวัตถุประสงค์ทั่วไปของการก่อการร้ายได้เป็น 4 ประเภทดังนี้

1. กระทำความผิดกฎหมาย (Criminal) ลัทธิก่อการร้ายที่กระทำผิดกฎหมาย ถูกจำกัดความว่าเป็นการวางแผนใช้ความสยดสยอง/หวาดกลัว เพื่อผลประโยชน์เกี่ยวกับเงินและวัตถุ

2. ทางจิตวิญญาณ (Psychic) ลัทธิก่อการร้ายทางด้านจิตวิญญาณ จะเกี่ยวข้องกับความเชื่อเรื่องเวทย์มนต์คาถา เทพนิยาย และลัทธิไสยศาสตร์ ซึ่งถูกโน้มน้าวจากการคลั่งศาสนา

3. ด้านสงคราม (War) ลัทธิก่อการร้ายที่เกี่ยวกับการสงครามเป็นการทำลายล้างศัตรูในทุกวิถีทางที่จะทำได้

4. ด้านการเมือง (Political) ลัทธิก่อการร้ายที่เกี่ยวกับการเมือง ถูกจำกัดความว่า เป็นการใช้ความรุนแรงและความกลัวอย่างเป็นระบบ เพื่อให้บรรลุวัตถุประสงค์ทางการเมือง

นอกจากนี้ Wilkinson ยังได้แบ่งการก่อการร้ายทางด้านการเมือง ออกไปอีก 3 ประเภท คือ

1.การปฏิวัติ (Revolution) แบบที่มีลักษณะใกล้เคียงการปฏิวัติ (Sub – revolution) และใช้การบีบบังคับ (Repressive) ลัทธิการก่อการร้ายที่มีลักษณะปฏิวัติเป็นการแสดงออกถึงการใช้กลยุทธ์การก่อการร้ายด้วยความรุนแรงอย่างเป็นธรรมเพื่อจุดมุ่งหมายที่จะนำมาซึ่งการปฏิวัติทางการเมือง การก่อการร้ายประเภทนี้มีจุดเด่นพิเศษหลัก 4 อย่างคือ

1.1 มักจะเป็นการปฏิบัติการรุนแรงของกลุ่มมากกว่าบุคคล

1.2 การพิจารณาด้านศีลธรรม สำหรับการใช้ความสยดสยองหรือหวาดกลัวมักจะพบในอุดมการณ์องการปฏิวัติ

1.3 พวกผู้นำก่อการร้ายมักจะเป็นหลักสำคัญในการรับสมาชิกใหม่ เพื่อเสริมสร้างกำลังก่อการร้าย

1.4 ขบวนการเคลื่อนไหวด้วยการปฏิวัติจะต้องพัฒนาและวางแผนนโยบายเอง รวมทั้งโครงสร้างพื้นฐานและมาตรการในการปฏิบัติ

2. การก่อการร้ายที่มีลักษณะใกล้เคียงกับการปฏิวัติ เป็นการใช้ความสยดสยองหรือหวาดกลัวเพื่อจุดหมายปลายทางการเมืองมากกว่าการปฏิวัติเป็นการกดขี่รัฐบาล ซึ่งการก่อการร้ายประเภทนี้จะบีบบังคับโดยตรง ให้เปลี่ยนแปลงนโยบายเกี่ยวกับความขัดแย้งทางการเมือง การประกาศเตือนเจ้าหน้าที่ของรัฐ หรือโต้กลับรัฐในการกระทำบางอย่างที่กลุ่มก่อการร้ายเห็นว่าพึงได้รับการประณาม

3. การก่อการร้ายโดยการบีบบังคับ (Repressive) หมายถึง การปฏิบัติการรุนแรงของการก่อการร้ายอย่างเป็นระบบ เพื่อจุดมุ่งหมายในการบีบบังคับ การปราบปราม การสังหาร หรือการกักขังหน่วงเหนี่ยว กลุ่มบางกลุ่ม บุคคลบางพวกหรือรูปแบบพฤติกรรมที่ถือว่าไม่เป็นที่ต้องการของผู้กดขี่

วงษ์พิทักษ์ เจียนเกาะ (2550 หน้า 15)กล่าวว่า ในการก่อการร้ายก็มีระดับความรุนแรงและความมุ่งหมายที่อาจแตกต่างกันออกไปซึ่งหาจุดเริ่มต้นและสิ้นสุดที่ตรงกันไม่ได้ สาเหตุหรือมูลเหตุชักจูงใจของการก่อการร้ายเมื่อแบ่งออกเป็นกว้าง ๆ น่าจะเกิดจาก

1. ลัทธิความเชื่อ เช่น ศาสนาหรือการเมือง

2. ความแตกต่าง เช่นเชื้อชาติหรือวัฒนธรรม

3. ฝักใฝ่อำนาจและความมั่งคั่งทางเศรษฐกิจ เช่น แย่งชิงดินแดนหรือรับจ้างก่อการร้ายหรือสอนการก่อการร้าย

อีกหนึ่งประเภทของการก่อการร้าย ทางไซเบอร์ (Cyber terrorism) เป็นการก่อการร้ายที่มีความเกี่ยวพันกับความทันสมัยของเทคโนโลยีที่ช่วยให้กลุ่มก่อการร้ายดำเนินกิจกรรมต่าง ๆ ได้อย่างมีประสิทธิภาพ โดยใช้พลังอำนาจของเทคโนโลยีสารสนเทศเป็นแนวทางปฏิบัติหรือปรับ

องค์กรไปสู่รูปแบบใหม่มีการคาดการณ์ว่า การก่อการร้ายทางไซเบอร์ จะเป็นรูปแบบการก่อการร้ายที่เป็นอีกหนึ่งยุทธวิธีในการต่อสู้มากขึ้น โดยสามารถสร้างความเสียหายให้เกิดผลกระทบทั้งทางด้านจิตวิทยาและดึงดูดความสนใจจากสื่อมวลชนหรือบุคคลต่าง ๆ การก่อการร้ายรูปแบบนี้จะอาศัยช่องว่างจากการขยายตัวของโลกสมัยใหม่ที่มีลักษณะของการเชื่อมโยงข้อมูลผ่านคอมพิวเตอร์ในระบบเครือข่าย จึงตกเป็นเป้าหมายของการโจมตีไซเบอร์เพื่อทำลายหรือขัดขวางการทำงานระบบเครือข่ายคอมพิวเตอร์แบบต่าง ๆ ไม่ว่าจะเป็นเครือข่ายการสื่อสาร หรือเครือข่ายคอมพิวเตอร์ที่ควบคุมการทำงานระบบสาธารณูปโภค โครงสร้างพื้นฐาน หรือไปจนถึงระบบทางด้านความมั่นคงทางทหาร หรือการล้วงข้อมูลสำคัญต่าง ๆ เป็นต้น

การก่อการร้ายมีการบ่งชี้ความแตกต่างของการกระทำที่ต่างไปจากอาชญากรรม ข้อสังเกตที่เป็นความแตกต่างการก่อการร้ายคือการก่อการร้ายไม่ใช่องค์กรอาชญากรรม แม้จะมีความคล้ายคลึงกัน เช่น รูปแบบการกระทำ วิธีการสมคบคิดและการแบ่งหน้าที่กันทำ แต่ผู้ก่อการร้ายไม่ได้กระทำผิดเพื่อเป็นอาชีพอย่างต่อเนื่อง แต่มีวัตถุประสงค์กระทำเพื่อเปลี่ยนแปลงบางอย่าง ในสังคม ซึ่งเป็นอุดมการณ์ความเชื่อ และเมื่อเกิดผลตามการกระทำแล้วก็จะหยุดการกระทำนั้น ซึ่งแตกต่างจากอาชญากรรมทั่วไปที่มักแสวงหาผลประโยชน์ในทรัพย์สินเป็นหลัก

แรงจูงใจ เป้าหมายวิธีการก่อการร้าย

ดลยา เทียนทอง (2549, หน้า 9) กล่าวถึงมูลเหตุหรือแรงจูงใจของการก่อการร้ายนั้น พบว่า เกิดสภาพแวดล้อมภายในหรือภายนอกประเทศแบบไม่ปกติ ประกอบกับมีปฏิกิริยาแบบโต้ตอบจากบุคคลหรือกลุ่มบุคคลซึ่งถูกกีดกัน ถูกบีบบังคับ รวมทั้งคับข้องใจอันเนื่องมากจากสภาพแวดล้อมที่ไม่ปกติและที่สำคัญเกิดจากแรงจูงใจภายใน (Motivation) ที่ผลักดันให้เกิดพฤติกรรมการก่อการร้าย ซึ่งมี 4 ประการคือ 1. ความมั่นใจทางศีลธรรม 2. การนิยามอย่างง่าย ๆ ระหว่างความดีและความชั่วร้าย 3. การแสวงหาสังคมในอุดมคติ 4. การอุทิศตน สอดคล้องกับ สุรินทร์ หิรัญบูรณะ (2547, หน้า 16 – 17) การก่อการร้ายในสังคมโลกปัจจุบันได้ทวีความรุนแรงและมีวิธีการกระทำที่ซับซ้อนมากขึ้น สร้างความเสียหายต่อชีวิตผู้คนและทรัพย์สินเป็นจำนวนมาก ซึ่งมีเหตุจูงใจมาจากเป้าหมายหลายอย่าง ทั้งทางการเมือง เศรษฐกิจและสังคมเพื่อที่จะกดดันหรือผลักดันความคิดอุดมการณ์ หรือให้ฝ่ายตรงกันข้ามกระทำหรือละเว้นการกระทำตามเจตจำนงของกลุ่มก่อการร้าย โดยจำแนกวัตถุประสงค์ดังนี้

1. การข่มขู่ เป็นวัตถุประสงค์ที่ให้เกิดความกลัว โดยรูปแบบของการข่มขู่นั้นจะแตกต่างกันไป เช่น การลอบสังหารผู้นำที่เอาใจออกห่างหรือมีนโยบายที่เข้าข้างศัตรูของกลุ่มก่อการร้าย การข่มขู่ให้กลัวเพื่อปกป้องผลประโยชน์

2. การแก้แค้น เป็นการกระทำที่เกี่ยวข้องกับศักดิ์ศรีและยังเป็นการปิดกันการล้างแค้นตอบโต้

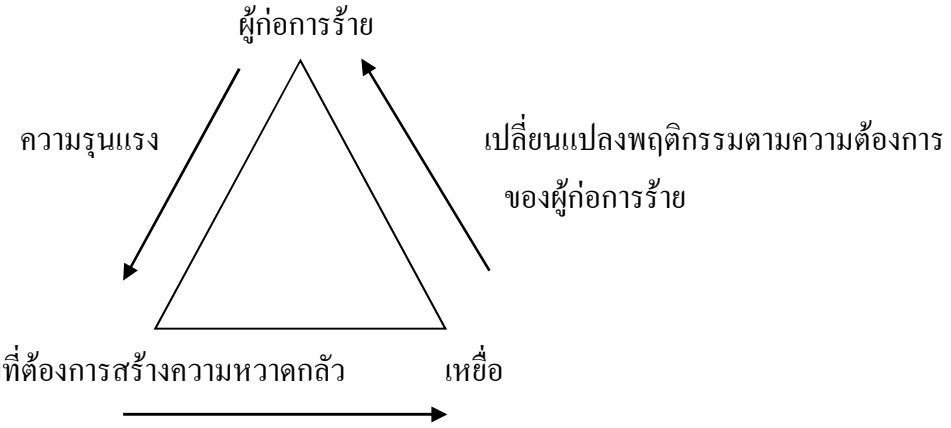
3. การสร้างประชามติ มีเป้าหมายมากกว่าการข่มขู่ให้กลัว แต่จะกระตุ้นให้เกิดประชามติให้หันมาให้การสนับสนุนและเพื่อเป็นการสร้างแนวร่วมเพื่อปฏิบัติงานได้บรรลุวัตถุประสงค์ บุญรอดศรีสมบัติ (2548, หน้า 35– 37) กล่าวว่า การก่อการร้ายในปัจจุบันถือเป็นภัยคุกคามที่สำคัญยิ่ง เพราะหลายประเทศได้ถูกคุกคามด้วยการถูกใช้เป็นสถานที่ในการดำเนินการก่อการร้าย สำหรับเป้าหมายของการก่อการร้ายสามารถแบ่งออกเป็น 2 ลักษณะ คือ เป้าหมายทางทหารและเป้าหมายทางพลเรือน โดยการก่อการร้ายนั้นจะกระทำต่อเป้าหมายที่ทำการคัดเลือกและอาศัยการวางแผนที่รัดกุมด้วยการรักษาไว้เป็นความลับจนกว่าการปฏิบัติการจะสำเร็จทำให้ยากต่อการป้องกัน ส่วนรูปแบบการก่อการร้ายจากในอดีตที่ผ่านมาจะมีลักษณะดังต่อไปนี้ ลอบวางระเบิด (Bombing) ยึดพาหนะในการโดยสาร (Hijacking) ลักพาตัว (Kidnapping) ข่มขู่ (Threat) ลอบสังหาร (Assassination) บุกโจมตีด้วยอาวุธ (Raid) จับกุมตัวประกัน (Hostage) ซุ่มยิง (Sipping) ก่อวินาศกรรม (Sabotage) และใช้อาวุธชีวเคมีในที่ชุมชน (Biological & Chemical weapon attacking) สายฝน แสงสวัสดิ์ (2557) กล่าวถึงปัจจัยที่เกี่ยวข้องในการก่อการร้าย เอาไว้ 3 ประการคือ

1. ปัจจัยทางด้านคมนาคม – ขนส่ง ในปัจจุบันการก่อการร้ายได้แพร่ขยายเข้าไปในพื้นที่แทบทุกส่วนของโลก เนื่องจากการคมนาคมขนส่งที่รวดเร็วและหลากหลาย ผู้ก่อการร้ายจึงสามารถเคลื่อนไหวกิจกรรมต่าง ๆ ได้ง่าย ประกอบกับการใช้อุปกรณ์ที่ทันสมัย เครือข่ายการสื่อสารในการรับส่งข้อมูล สั่งการและการติดตามผลจึงทำให้การติดตามผู้ก่อการร้ายจึงเป็นเรื่องยาก หรืออาจต้องใช้การรวบรวมข่าวสารต่าง ๆ

2. ปัจจัยทางด้านการสนับสนุนจากรัฐบาล ผู้ก่อการร้ายบางกลุ่มในปัจจุบันเป็นผู้ก่อการร้ายภายใต้การจัดตั้งหรือได้รับการสนับสนุนจากรัฐบาลหรือประเทศต่าง ๆ เพื่อจะใช้ประโยชน์ในการดำเนินการนโยบายทางการเมือง โดยลักษณะของชาติต่าง ๆ มักจะเป็นกำลังทหารอ่อนแอหรือพลังอำนาจแห่งชาติไม่เข้มแข็งและกำลังเผชิญหน้ากับประเทศมหาอำนาจ หรือชาติที่ไม่ต้องการดำเนินนโยบายทางการเมือง การทหารที่รุนแรงโดยเปิดเผย ประเทศเหล่านี้จะเลือกใช้กองกำลังของผู้ก่อการร้ายปฏิบัติภารกิจแทน

3. ปัจจัยด้านเงินทุนหมุนเวียน การก่อการร้ายไม่ใช่สงครามตามแบบแต่เป็นรูปแบบของสงครามหลบซ่อน ชาติที่ถูกกระทำจะป้องกันและตอบโต้และการก่อการร้ายส่วนใหญ่ไม่ได้ต้องการเงินทุนสนับสนุนมากมาย การก่อการร้ายใช้เงินน้อยกว่ากิจกรรมข้ามชาติที่ผิดกฎหมายเช่น การค้ายาเสพติด หรือการค้าอาวุธ การแกะรอยเส้นทางการเงินที่หมุนเวียนในระบบจึงเป็นเรื่องยาก

วรนุช พุ่มเรือง (2554, หน้า 77)ได้อธิบายรูปแบบของการก่อการร้ายทั้งหมดได้ทำให้เกิดวงจรความสัมพันธ์ระหว่างผู้ก่อการร้าย เหยื่อ และเป้าหมายที่ผู้ก่อการร้ายต้องการคุกคามหรือส่งสารไปถึงและเป็นวงจรดังนี้



ภาพที่ 6 รูปแผนภูมิการก่อการร้าย (วรนุช พุ่มเรือง, 2554)

จากแผนภาพสามารถอธิบายได้ว่า ผู้ก่อการร้ายจะอาศัยรูปแบบต่าง ๆ โดยจะเน้นให้เกิดความรุนแรงที่ส่งผลไปกระทำกับเหยื่อหรือเป้าหมายเพื่อให้เกิดบรรยากาศแห่งความหวาดกลัวขึ้นในสังคมและเป็นการส่งสารไปยังเป้าหมายที่แท้จริง ผู้ก่อการร้ายต้องการจะสื่อสารด้วย เช่น รัฐหรือผู้ปกครองหรือผู้มีอำนาจในขณะนั้นให้เกิดการยอมรับและเปลี่ยนแปลงพฤติกรรมตามความต้องการของผู้ก่อการร้าย

กลุ่มก่อการร้ายสากล

การก่อการร้ายสากล จะประกอบด้วยกลุ่มก่อการร้ายประมาณ 33 กลุ่ม ที่ปฏิบัติการอยู่ในพื้นที่ของเอเชีย ยุโรป แอฟริกาและอเมริกา โดยเฉพาะในพื้นที่ตามภูมิภาคต่าง ๆ ของเอเชียดังนี้

1.เอเชีย

1.1 เอเชียตะวันออกเฉียงใต้

1.1.1 กลุ่มอาบูซายัฟAbu Sayyaf Group (ASG)

1.1.2 กลุ่มเจมาห์อิสลามิยา หรือ เจไอJemaah Islamiya (JI)

1.2 เอเชียตะวันออก

1.2.1 กลุ่มAum Supreme Truth (AUM)

1.2.2 กลุ่ม Japanese Red Army (JRA)

1.3เอเชียใต้

1.3.1 กลุ่มHarakatul – Mujahidin (HUM)

1.3.2 กลุ่มJaish – e – Mohammed (JEM)

1.3.3 กลุ่ม Liberation Tiger of Tamil Eelam (LTTE)

1.3.4 กลุ่มLashkar – e - Tayyiba (LT)

1.4 เอเชียตะวันตก (ตะวันออกกลาง)

1.4.1กลุ่ม Abu Nidal organization (ANO)

1.4.2 กลุ่ม Al – Aqsa Martyrs Brigada

1.4.3 กลุ่ม Al – Gama' a aj – Islamiya (Islamic Group – IG)

1.4.4 กลุ่ม Al – Jihad

1.4.5 กลุ่ม Al – Qaida

1.4.6 กลุ่มAsbat al – Ansar

1.4.7 กลุ่ม Hamas (Islamic Resistance Movement)

1.4.8 กลุ่มHizballah (Party of God)

1.4.9 กลุ่มKahane Chai (Kach)

1.4.10 กลุ่ม Kurdistan Workers' Party (PKK)

1.4.11 กลุ่มMalahedin – e Khalq Organization (MEK or MKO)

1.4.12 กลุ่ม Palestine Liberation Front (PLF)

1.4.13 กลุ่ม Population Front for the Liberation of Palestine (PFLP)

1.4.14 กลุ่ม Popular Front for the Liberation of Palestine Gencral Command (PFLP – GC)

1.4.15 กลุ่ม The Palestine Islamic Jihad (PIJ)

1.5 เอเชียกลาง

1.5.1 กลุ่ม Islamic Movement of Uzbekistan (IMU)

2. ยุโรป

2.1ยุโรปตะวันตก

2.1.1 กลุ่ม Basque Fatherland and Liberty (ETA)

2.1.2 กลุ่ม Real IRA (RIRA)

3. แอฟริกา

3.1 กลุ่ม Armed Islamic Group (GIA)

3.2 กลุ่มThaSalafist Group for Call and Combat (GSPC)

4. อเมริกาใต้

4.1 กลุ่มRevolutionary Armed Forces of Columbia (FARC)

4.2 กลุ่มSenderoLuminoso (Shining Path, or SL)

4.3 กลุ่มUnited Self – Defense Force / Group of Columbia (AUC – AutodefensasUnidas de Columbia) (ดลยา เทียนทอง, ม.ป.ป., หน้า 4 – 5)

กลุ่มรัฐอิสลามหรือ กลุ่มไอเอส(Islamic state) เป็นการรวมตัวของกลุ่มนักรบหลายเครือข่าย ถือกำเนิดขึ้นตั้งแต่ลงครามอิรัก เมื่อ พ.ศ. 2546 เดิมเป็นเครือข่ายกลุ่มอัลกออิดะห์เดิม ซึ่งกลุ่มไอเอสมีความสามารถพิเศษในการปลุกระดมนักรบจากทั่วโลกทั้งจากสหรัฐอเมริกา ยุโรป ตะวันออกกลาง หรือแม้แต่ประเทศออสเตรเลีย ผู้หลงเชื่อเป็นเด็กวัยรุ่น ที่เปลี่ยนมานับถือศาสนาอิสลาม โดยส่วนใหญ่ถูกล่อลวงผ่านสื่อสังคมออนไลน์ ผู้นำคนปัจจุบันคือ นายอาบู บาการ์ แบกดาดี (Abu Bakral Baghddi) กลุ่มไอเอสมีจุดมุ่งหมายในการสถาปนารัฐอิสลาม ที่ปกครองโดยผู้นำการเมืองและผู้นำศาสนาเพียงคนเดียวตามหลักกฎหมายอิสลาม หรือ ซารีอะฮ์ (ยอดชาย วิถีพานิช, 2558)

สถานการณ์การก่อการร้าย

การก่อการร้ายยังคงเป็นภัยคุกคามของนานาประเทศโดยเฉพาะประเทศในภูมิภาคเอเชียใต้ ตะวันออกกลาง และเอเชียตะวันออกเฉียงใต้ โดยกลุ่มที่เคลื่อนไหวอย่างต่อเนื่องคือกลุ่มหัวรุนแรงอิสลามนิยม เช่น อัลกออิดะห์ ซึ่งมีเครือข่ายอยู่ในหลายทวีปนอกจากนั้น ยังมีกลุ่มหัวรุนแรงต่าง ๆ ทั่วโลก อาทิ กลุ่มขวาจัด กลุ่มแบ่งแยกดินแดนและกลุ่มก่อการร้ายที่เกิดขึ้นใหม่ เช่น กลุ่มไอซิส การก่อเหตุจะมีแรงจูงใจทางการเมือง เพื่อสร้างความหวาดกลัวและความเสียหายให้แประเทศที่เป็นกลุ่มเป้าหมายทั่วโลก การเกิดเหตุการณ์การก่อการร้าย (จิ๊กซอ, 2558) ที่ผ่านมามีดังนี้

1. ผู้ก่อการร้ายยิงประชาชนสำนักพิมพ์ ชาร์ลี เอ็บโด

การก่อการร้ายที่น่าตกใจมากที่เมื่อมีคนร้ายถือปืนไรเฟิลเข้าไปกราดยิงในสำนักพิมพ์ของประเทศฝรั่งเศส ซึ่งคาดว่าที่เข้าไปยิง เพราะไม่พอใจสำนักพิมพ์ดังกล่าวที่วาดการ์ตูนล้อเลียนเสียดสีศาสนาอิสลาม เพราะก่อนที่จะยิงนั้นได้ตะโกนขึ้นมาว่า “เราจะแก้แค้นให้แก่ท่านมูฮัมหมัด” ซึ่งจากเหตุการณ์นี้ทำให้มีผู้เสียชีวิตกว่า 12 คน โดยทั้งนักเขียนและบรรณาธิการของสำนักพิมพ์ชาร์ลี เอ็บโด ก็ถูกยิงเสียชีวิตด้วย

2. 15 ธันวา 57 ก่อการร้ายใน3 ประเทศ

การก่อการร้ายที่น่าตกใจอย่างมากที่ในวันเดียวกันจะมีการก่อการร้ายเกิดขึ้นถึง 3 ประเทศ ที่แรกคือที่ซิดนีย์ ออสเตรเลีย ที่มีชายชาวอิหร่านได้บุกเข้าไปในลินด์ คาเฟ่ และจับตัว

ประกันหลายคนที่อยู่ภายในร้าน จนทำให้มีผู้เสียชีวิต 3 คน รวมผู้ก่อการร้าย ต่อมาที่สหรัฐอเมริกา มือปืนรายหนึ่งได้เปิดฉากยิงผู้คนตามบ้านเรือนที่อยู่อาศัยต่าง ๆ ตลอดทางที่เขาเดินไป ส่งผลให้มีผู้เสียชีวิตแล้ว 6 ราย และมีผู้บาดเจ็บ 3 ราย และที่สุดท้ายคือที่เบลเยียมมีผู้แจ้งว่าคนร้ายติดอาวุธ 3-4 ราย ได้บุกเข้าไปในอพาร์ทเม้นท์ ก่อนจะจับชายคนหนึ่งเป็นตัวประกัน ทำให้เจ้าหน้าที่ตำรวจต้องนำกำลังปิดล้อมอพาร์ทเม้นท์และเข้าไปช่วยตัวประกันได้ก่อนจะมีใครเสียชีวิต แต่ที่น่าสงสัยคือผู้ต้องสงสัยไม่มีอาวุธเลยสักคน

3. การก่อวินาศกรรม 9/11

การก่อการร้ายที่ร้ายแรงที่สุดในประวัติศาสตร์ เมื่อวันที่ 11 กันยายน พ.ศ. 2544 ผู้ก่อการร้าย 19 คนจากกลุ่มอิสลามหัวรุนแรงอัลกออิดะฮ์ จี้อากาศยานโดยสารสี่ลำ โดยนำเครื่องบินสองลำพุ่งชนกับ ตึกแฝด เวิลด์เทรดเซ็นเตอร์ในนครนิวยอร์กโดยเจตนา ทำให้อาคารทั้งสองถล่มลงภายในสองชั่วโมง ส่วนเครื่องบินลำที่สามก็ชนเข้ากับอาคารเพนตากอนในอาร์ลิงตัน รัฐเวอร์จิเนีย ส่วนเครื่องบินลำที่สี่ ยูไนเต็ดแอร์ไลน์ เที่ยวบินที่ 93 ตกในทุ่งใกล้กับแชงค์วิลล์ รัฐเพนซิลเวเนีย ก่อนจะถึงเป้าหมายที่โจรจี้เครื่องบินต้องการพุ่งชนอาคารรัฐสภาสหรัฐ ในวอชิงตัน ดี.ซี. จนทำให้มีผู้เสียชีวิตมากถึง 3,000 คน ซึ่ง 10 ปีต่อมาอุซามะฮ์ บิน ลาดิน ผู้นำกลุ่มก็ถูกสังหารในที่สุด

4. ระเบิด 14 ลูกที่สเปน

การเกิดเหตุการณ์ระเบิดครั้งใหญ่ของสเปน หรือที่เรียกกันว่า 11-M เกิดขึ้นเมื่อวันที่ 11 มีนาคม ค.ศ. 2004 เมื่อรถไฟสายชานเมืองเข้าเทียบสถานี Atochaสถานีรถไฟที่ใหญ่ที่สุดในเมืองมาดริดระเบิดตามกันมาถึง 14 ลูก ทำให้มีผู้เสียชีวิต 200 คนและบาดเจ็บอีกประมาณ 1500 คน นับเป็นโศกนาฏกรรมครั้งใหญ่ที่สุดในประวัติศาสตร์ยุคใหม่ของสเปนเลยทีเดียว

5. การบุกสนามบินจินนาห์

เกิดเหตุการณ์ที่เกิดขึ้นในอากาศยานนานาชาติจินนาห์ ในการาจี ประเทศปากีสถาน เมื่อวันที่ 8 มิถุนายน 2557 ที่กองกำลังติดอาวุธอย่างน้อย 10 คนได้ฝ่าด่านรักษาความปลอดภัยของสนามบิน และโจมตีสถานีขนส่งสินค้าด้วยปืนกล ระเบิด และจรวดอาร์พีจี ทั้งยังพยายามจี้เครื่องบินแต่ไม่สำเร็จ โดยหลังจากการโจมตี 90 นาที หน่วยรบพิเศษคอมมานโดจำนวนหลายร้อยนายก็มาถึงและเริ่มต่อสู้กับผู้ก่อการร้าย ทำให้ผู้ร้าย 8 คนเสียชีวิต ส่วนอีก 2 คนก็ได้ระเบิดตัวเองเมื่อจนมุม ซึ่งเหตุการณ์นี้ทำให้มีผู้เสียชีวิต 29 คน

6. เกิดการโจมตีในนอร์เวย์

การเกิดเหตุโจมตีเพื่อก่อการร้ายถึงสองครั้งด้วยกัน ในวันที่ 22 กรกฎาคม พ.ศ. 2554 ซึ่งครั้งแรกเป็นเหตุระเบิดในกรุงออสโล นอกสำนักงานนายกรัฐมนตรี ทำให้มีผู้เสียชีวิต 8 คน และ

ได้รับบาดเจ็บอีกมาก ส่วนเหตุโจมตีครั้งที่สองนั้นเกิดขึ้นในราวสองชั่วโมงให้หลัง ที่ค่ายเยาวชน โดยมีมือปืนอย่างน้อยหนึ่งคนปลอมตัวเป็นตำรวจกราดยิงใส่ผู้เข้าค่าย โดยไม่ได้สนใจว่าจะเป็นผู้ใหญ่ เด็ก ผู้หญิง หรือผู้ชาย ทำให้มีผู้เสียชีวิตกว่า 68 คน ซึ่งถือเป็นเหตุที่มือปืนเดี่ยวสังหารผู้อื่นไปมากที่สุดในประวัติศาสตร์ก็ว่าได้

7. การเกิดระเบิดรถไฟใต้ดิน ลอนดอน

เกิดเหตุการณ์ในช่วงเช้าของวันที่ 7 กรกฎาคม พ.ศ. 2548 เกิดการระเบิดขึ้นสี่ครั้งต่อเนื่อง ที่กรุงลอนดอน ในอังกฤษ โดยรถไฟใต้ดินสามขบวนถูกวางระเบิดภายในช่วงเวลาครึ่งชั่วโมง จากนั้นอีกครึ่งชั่วโมงรถเมล์สองชั้นอีกหนึ่งคันก็ถูกระเบิด ได้รับการยืนยันว่ามีผู้เสียชีวิต 56 ศพ และผู้ได้รับบาดเจ็บมากกว่า 700 คน จนทำให้มีการสั่งปิดระบบรถไฟใต้ดินของลอนดอนและระบบรถประจำทาง รวมไปถึงถนนสายใกล้กับกับสถานีที่เกิดเหตุเลยทีเดียว ทางรัฐบาลอังกฤษได้มุ่งความสนใจไปที่กลุ่มก่อการร้ายอัลเคดาว่าเป็นผู้เกี่ยวข้อง เพราะในเว็บไซต์ของอัลเคด้ามีข้อความเกี่ยวกับเหตุการณ์ระเบิดด้วย

8. เกิดเหตุการณ์ระเบิดกลางงานวิ่งมาราธอน

เหตุการณ์ระเบิดเกิดขึ้นที่เมืองเวลิเวริยา รอบนอกของกรุงโคลอมโบ ประเทศศรีลังกา ที่สาเหตุมาจากความขัดแย้งทางเชื้อชาติระหว่างชาวสิงหลและชาวทมิฬ โดยชาวทมิฬต้องการที่จะแบ่งแยกดินแดนทางภาคเหนือและภาคตะวันออกของประเทศ จึงได้ก่อตั้งกลุ่มแอลทีทีอีเพื่อเป็นกองกำลังในการก่อต่อสู้กับรัฐบาล โดยครั้งนี้ทำให้มีผู้เสียชีวิต 11 คน บาดเจ็บกว่า 50 คน และ 1 ในผู้เสียชีวิตก็คือรัฐมนตรีทางหลวง จียะราช เฟนันโดปุลเล

9. ตัวประกัน ณ โรงละครมอสโก

การยึดโรงละครซึ่งเต็มไปด้วยตัวประกันกว่า 850 ชีวิต เมื่อวันที่ 23 ตุลาคม พ.ศ. 2545 โดยกลุ่มติดอาวุธเชเชนราว 50 คน โดยการนำของ มอฟซาร์ บาราเยฟ ที่อ้างความภักดีต่อขบวนการแบ่งแยกดินแดนอิสลามในเชชเนีย โดยเรียกร้องให้ถอนกำลังรัสเซียออกจากเชชเนีย และยุติสงครามเชชเนียครั้งที่สอง หลังการล้อมนานสองวันครึ่ง กองกำลังสเปซนาซของรัสเซียได้สูบสารเคมีไม่ทราบชื่อ เข้าไปในระบบระบายอากาศของอาคารและลงมือโจมตี ทำให้คนร้าย 39 คน ถูกสังหารโดยกองทัพรัสเซีย แต่ที่น่าสลดคือตัวประกันกว่า 129 คน ก็ได้เสียชีวิตเพราะแก๊สนี้ ทำเอาคนทั่วโลกต่างพากันประณาม การใช้วิธีนี้ของรัสเซีย

10. ระเบิดย่านท่องเที่ยวในบาหลี

เหตุสะเทือนขวัญนี้เกิดขึ้นเมื่อวันที่ 12 ตุลาคม พ.ศ. 2545 บนเกาะบาหลี ซึ่งเกิดจากการระเบิดนั่นเอง ลูกหนึ่งเป็นอุปกรณ์ติดกับเป้สะพายหลังซึ่งมือระเบิดพลีชีพนำติดตัวไปด้วย อีกลูก

หนึ่งเป็นคาร์บอมบ์ขนาดใหญ่ ซึ่งทั้งสองลูกนั้นถูกจุดใกล้กับไนท์คลับที่ได้รับความนิยมในคูตา ส่วนระเบิดลูกสุดท้าย เป็นอุปกรณ์ขนาดเล็กกว่ามาก ซึ่งจุดระเบิดนอกสถานกงสุลสหรัฐอเมริกาในเดนปาซาร์ โดยทำให้มีประชาชนเสียชีวิตกว่า 200 คน และบาดเจ็บอีก 240 คน ซึ่งว่ากันว่าเป็นฝีมือของกลุ่มญะมาอะห์ อิสลามียะห์ กลุ่มอิสลามหัวรุนแรง ที่ถูกตัดสินประหารในที่สุด

มาตรการต่อต้านการก่อการร้าย

เครื่องมือในการต่อต้านการก่อการร้าย ในขณะที่ผู้ก่อการร้ายไม่ยึดหลักกฎหมายและความถูกต้องใด ๆ และปฏิบัติการด้วยความโหดเหี้ยมทารุณ แม้ทรัพยากรมีจำกัด แต่สามารถนำจุดอ่อนของฝ่ายเจ้าหน้าที่ของรัฐมาใช้ประโยชน์ได้ทั้งยังสามารถสร้างเครือข่ายและรักษาการริเริ่มทำให้เครื่องมือในการต่อสู้การก่อการร้ายต้องใช้ทรัพยากรมหาศาล เครื่องมือในการต่อต้านการก่อการร้ายได้แก่ นโยบายทางการทูตเพื่อสร้างพันธมิตร และเสียงสนับสนุนในเวทีการเมืองระหว่างประเทศเพื่อความชอบธรรมในการดำเนินการต่อต้านการก่อการร้าย กฎหมายที่ดำเนินคดีกับผู้ก่อการร้ายในศาลยุติธรรม การควบคุมแหล่งเงินด้วยการตัดวงจรของเงินสนับสนุน การใช้กำลังทหาร การข่าวกรอง และการนำยุทธศาสตร์ผสมเครื่องมือทุกชนิดมารวมกันใช้ให้เกิดศักยภาพสูงสุด (กองข่าวกองทัพภาคที่ 2, ม.ป.ป., หน้า 17 – 21)

มาตรการต่อต้านการก่อการร้ายเป็นมาตรการในการลดความสามารถและลดความเป็นไปได้ของการเกิดการก่อการร้าย รวมทั้งเทคนิคป้องกันการเกิดอาชญากรรมและวิธีการตรวจสอบก่อนเกิดเหตุการณ์ มาตรการตอบโต้เป็นมาตรการต่อเหตุการณ์ที่เกิดขึ้น ขึ้นอยู่กับการวางแผนการปฏิบัติการทางยุทธวิธีภายหลังเกิดเหตุการณ์ และเป็นการทำให้โอกาสที่ผู้ก่อการร้ายปฏิบัติการสำเร็จลดลง (กองข่าวกองทัพภาคที่ 2, ม.ป.ป., หน้า 17) ประเทศสหรัฐอเมริกา กำหนดแนวคิดยุทธศาสตร์ 4 มิติ คือ การเอาชนะองค์การก่อการร้าย (Defeat) การไม่เป็นแหล่งเงินทุน/ การให้ที่หลบภัย (Deny) ลดสภาวะแอบแฝงของการก่อการร้าย (Diminish) และการปกป้องประชาชนและผลประโยชน์ (Defend) และในการปฏิบัติการ ได้กำหนดยุทธศาสตร์ 3 ระยะ คือ ยุทธศาสตร์เฉพาะหน้า ยุทธศาสตร์ระยะกลาง และยุทธศาสตร์ระยะยาว

ยุทธศาสตร์เฉพาะหน้าเป็นการปฏิบัติการโดยตรง ด้วยการตั้งเป้าหมายต่อบุคคลที่ทราบว่าเป็นผู้ก่อการร้าย ยุทธศาสตร์ระยะกลาง เป็นการรวบรวมข่าวกรองเป็นฐานสนับสนุนขั้นต้นในการก่อการร้ายสากลให้กับสังคมโลก ปฏิบัติการร่วมกับพันธมิตรและเสริมสร้างความร่วมมือ ยุทธศาสตร์ระยะยาว เป็นเรื่องของสงครามทางความคิด มุ่งเน้นการสนับสนุนด้านศาสนา และอุดมการณ์ ปฏิบัติการต่ออิทธิพลที่ครอบงำระดับโลก ทำลายความน่าเชื่อถือของการอ้างความชอบธรรมด้วยกฎหมายของการก่อการร้าย และรักษาความสนใจและให้ความสำคัญในการต่อต้านการก่อการร้ายสากลจากทั่วโลกไว้ให้ได้ (ศูนย์พลเรือนและทหารสัมพันธ์, 2548, หน้า 18 – 19)

สรุปได้ว่า การปฏิบัติการก่อการร้าย มีเพิ่มมากขึ้นอย่างต่อเนื่อง ขีดความสามารถของผู้ก่อการร้ายมีการพัฒนาจากเทคโนโลยีและความทันสมัยของอาวุธ ผู้ก่อการร้ายจึงมีวิธีการในการแสวงหาเป้าหมายและนำอาวุธทางเทคโนโลยีมาใช้ ทำให้สามารถเลือกเวลาและสถานที่ในการดำเนินการ หากรัฐมีพฤติกรรมที่สนับสนุนหรือเป็นแนวร่วมในการที่หลบซ่อนหรือให้ความช่วยเหลือในการจัดหาอาวุธที่มีอานุภาพทำลายล้างสูง ยิ่งมีผลให้การก่อการร้ายเป็นภัยคุกคามและเป็นอันตรายที่ใกล้ตัวประชาชนบนโลกมากยิ่งขึ้น

แนวคิดเกี่ยวกับความมั่นคงแห่งชาติและความมั่นคงทางสารสนเทศ

ความมั่นคงแห่งชาติ(National Security) แนวคิดเรื่องความมั่นคงแห่งชาตินับว่าเป็นเรื่องที่มีความสำคัญยิ่ง Nye (1995: 90 – 102) ได้กล่าวว่า ความมั่นคงมีความสำคัญเหมือนกับออกซิเจน ซึ่งเป็นสิ่งที่มนุษย์ขาดไม่ได้ แต่ในภาวะปกติเรามักจะนึกไม่ถึงและบางทีเรายังเป็นตัวการในการทำลายออกซิเจนด้วย โดยทั่วไป ความมั่นคง (Security) หมายถึงสภาวะความอิสระจากภัยคุกคามต่อคุณค่าที่ถือว่าสำคัญ หรืออีกนัยหนึ่ง ความมั่นคงเป็นความปลอดภัยจากภัยคุกคาม ปลอดจากความวิตกกังวล หรือภัยอันตรายต่าง ๆ ความมั่นคง หมายถึง ภาวะทางจิตของบุคคล อาจเป็นของประชาชน หรือของผู้นำที่มีต่อสภาวะแวดล้อมมากกว่าสภาพที่แท้จริง (จุลชีพ ชินวรรณโณ, 2546, หน้า 6 – 7)

วีรพล วรานนท์ (2547, หน้า 12) ได้กล่าวว่าการดำเนินการให้เกิดความมั่นคงแห่งชาติคือการทำให้ประเทศมีความปลอดภัยจากการรุกราน โจมตีและยึดครองดินแดน การทำให้เศรษฐกิจรุ่งเรือง และการทำให้ประเทศเป็นที่ยอมรับนับถือ จากต่างประเทศในสังคมโลก ซึ่งจะส่งผลให้ภายในประเทศเกิดความสงบสุข ร่มเย็น ประชาชนมีความกินดีอยู่ดี ไม่มีความหวาดระแวงในชีวิต สามารถเผชิญหน้ากับชาวต่างชาติได้อย่างมีศักดิ์ศรีโดยเฉพาะอย่างยิ่งในสภาวะปัจจุบันที่สังคมโลกเป็นสังคมเปิด การแข่งขันระหว่างประเทศมีมากขึ้นและยุ่งยากกว่าเดิม มิติความมั่นคงแห่งชาติเปลี่ยนไปจากเดิมที่เน้นจากการทหารไปเป็นด้านการเมืองและเศรษฐกิจ

วิชัย ชูเชิด (2547, หน้า 15) ได้ให้ความหมายของความมั่นคงแห่งชาติ หมายถึง สภาวการณ์หรือสภาพที่รัฐชาติ ภายใต้การนำของรัฐบาลที่มีอำนาจอธิปไตยในการปกครองดินแดนดังกล่าวด้วยตนเอง ที่สามารถดำรงอยู่ด้วยความปลอดภัยจากอันตรายทั้งปวงไม่ว่าจะเป็นเกณฑ์การเสี่ยง ความเกรงกลัว ความกังกล และความสงสัย มีความเจริญก้าวหน้า มีเสรีต่อแรงกดดันต่าง ๆ ที่มากระทบในทุก ๆ ด้าน ทั้งในด้านเอกราช อธิปไตย ในด้านบูรณาภาพแห่งดินแดน ในด้านสวัสดิภาพ ความปลอดภัยและผาสุกของประชาชน ในด้านการปกครองของประเทศ และวิถีของการดำเนินชีวิตของตนเอง อีกทั้งต้องมีขีดความสามารถที่พร้อมจะเผชิญต่อสถานการณ์ต่าง ๆ ที่เกิดขึ้น

ชาคริต บุญฑีย์กุล (2549, หน้า 5) ได้กล่าวถึงมิติความมั่นคงว่า ประกอบด้วย การเมือง การป้องกันประเทศ การทหาร เศรษฐกิจ สังคมจิตวิทยา ความมั่นคงของมนุษย์ วิทยาศาสตร์ เทคโนโลยี พลังงานและสิ่งแวดล้อม

จากความหมายของความมั่นคงแห่งชาติ ผู้วิจัยจึงสรุปได้ว่า ความมั่นคงแห่งชาติ เป็นการดำเนินการของประเทศเพื่อให้ประชาชนในชาติอยู่ดีมีความสุข ปลอดภัยจากภัยคุกคาม มีการดำเนินชีวิตของตนเอง และประเทศปลอดภัยจากการรุกรานของชาติอื่น ๆ มีเศรษฐกิจรุ่งเรืองและเป็นที่ยอมรับของนานาประเทศ

ผลประโยชน์แห่งชาติ จากสถานการณ์ความมั่นคง ทั้งในระดับสังคมโลก และภูมิภาค ส่งผลให้ประเทศต่าง ๆ รวมทั้งประเทศไทย ต้องเผชิญกับปัญหาความมั่นคงในรูปแบบใหม่มากมาย นอกจากนี้ยังมีปัญหาที่เกิดจากปัจจัยภายในประเทศและเกิดจากปัจจัยเชื่อมโยงกับประเทศเพื่อบ้านด้วย การกำหนดผลประโยชน์แห่งชาติจึงเป็นความสำคัญและความปรารถนาของประชาชนส่วนรวมในชาติไว้ ผลประโยชน์แห่งชาติของประเทศไทย พ.ศ. 2558 – พ.ศ. 2564 ได้แก่

1. การมีเอกราช อธิปไตย และบูรณภาพแห่งเขตอำนาจรัฐ

2. การดำรงอยู่อย่างมั่นคง ยั่งยืนของสถาบันหลักของชาติ

3. การดำรงอยู่อย่างมั่นคงของชาติและประชาชนจากภัยคุกคามทุกรูปแบบ

4. การอยู่ร่วมกันอย่างสันติสุข เป็นปึกแผ่น มั่นคงทางสังคม ท่ามกลางพหุสังคมและการมีเกียรติและศักดิ์ศรีของความเป็นมนุษย์

5. ความเจริญเติบโตของชาติ ความเป็นธรรม และความอยู่ดีมีสุขของประชาชน

6. ความยั่งยืนของฐานทรัพยากรธรรมชาติ สิ่งแวดล้อม ความมั่นคงทางพลังงาน อาหาร

7. ความสามารถในการรักษาผลประโยชน์ของชาติภายใต้การเปลี่ยนแปลงของสภาวะแวดล้อมระหว่างประเทศ

8. การอยู่ร่วมกันอย่างสันติ ประสานสอดคล้องกันด้านความมั่นคงในประชาคมอาเซียนและประชาคมโลกอย่างมีเกียรติและศักดิ์

เจมส์ เอน โรสนาว (Rosenau, 1969) ได้อธิบายว่า ผลประโยชน์แห่งชาติใช้วิเคราะห์การเมืองและวิเคราะห์การกระทำทางการเมือง เพื่ออธิบายและประเมินแหล่งที่มาของนโยบายต่างประเทศ ส่วนในการวิเคราะห์การกระทำทางการเมือง แนวคิดผลประโยชน์แห่งชาติ เป็นวิถีทางในการตัดสินใจประกาศ หรือกำหนดนโยบายต่างประเทศ แต่อย่างไรก็ดี Rosenau ก็ไม่ได้กำหนดความหมายที่ชัดเจนของแนวคิดผลประโยชน์แห่งชาติ แต่ก็ได้ให้ความหมายของผลประโยชน์แห่งชาติอย่างกว้าง ๆ เอาไว้ว่า หมายถึง สิ่งที่ดีที่สุดสำหรับรัฐชาติในการดำเนินความสัมพันธ์ระหว่างประเทศ

ฮันส์ เจ มอร์เกนทอ (Morgenthau, 2005) ได้ให้ความหมายของผลประโยชน์แห่งชาติในทางปฏิบัติว่า การที่รัฐหนึ่งดำเนินนโยบายใด ๆ ก็โดยวัตถุประสงค์ที่ต้องการปกป้องอธิปไตย ระบอบการเมือง เศรษฐกิจ ศาสนา ภาษาและเชื้อชาติของตนไว้ จากการรุกรานของชาติอื่น รัฐต่าง ๆ อาจดำเนินนโยบายร่วมมือกันถ่วงดุลอำนาจหรือเป็นพันธมิตรกันโดยการช่วยเหลือซึ่งกันและกัน เพื่อให้บรรลุจุดมุ่งหมายนี้ นอกจากนี้ มอร์เกนทอ ได้จำแนกนโยบายที่ใช้ปกป้องและแสวงหาผลประโยชน์แห่งชาติไว้ 3 รูปแบบคือ นโยบายรักษาอำนาจ (Policy designed to preserve the status quo) นโยบายขยายอำนาจ (Policy designed to achieve imperialistic expansion) ซึ่งเป็นการขยายอำนาจทั้งทางการทหาร เศรษฐกิจและสังคม วัฒนธรรม และ นโยบายแสดงอำนาจเพื่อศักดิ์ศรี (Policy designed toprestige) นโยบายนี้ไม่ใช่อำนาจปฏิบัติโดยตรงแต่จะเป็นการใช้ศิลปะในการแสดงแสนยานุภาพของชาติตนให้ชาติอื่นยำเกรง

ขณะที่ชาร์ล โอ เลอร์เช่กับอับดุล เอ สะอีด(Lerche& Said, 1995) ได้แสดงความคิดเห็นว่า ผลประโยชน์ของชาติพื้นฐานของทุกรัฐควรประกอบด้วยปัจจัยสำคัญ 6 ประการดังนี้

1.การดำรงอยู่ของชาติ (Self – preservation) หมายถึง การดำรงรักษาปัจจัยความเป็นชาติ อันได้แก่ รัฐบาล ดินแดน ประชาชน และอำนาจอธิปไตย ปัจจัยนี้ถือว่าเป็นวัตถุประสงค์พื้นฐานของนโยบายต่างประเทศ เป็นวัตถุประสงค์ที่ทุกรัฐมีเหมือนกันและถือว่าเป็นผลประโยชน์ที่ทุกรัฐมีร่วมกันในการปกป้องประชาชนและดินแดนของตน

2. ความมั่นคงปลอดภัย (Security) หมายถึง การที่รัฐจะดำเนินความสัมพันธ์กับรัฐอื่น ๆ เพื่อให้รัฐของตนดำรงอยู่ได้ต่อไป โดยแต่ละรัฐมีเป้าหมายของความมั่นคงปลอดภัย ด้วยการป้องกันและลดภัยคุกคามที่มีต่อรัฐของตน ซึ่งถือว่าเป็นวัตถุประสงค์พื้นฐานแรกของนโยบายต่างประเทศเช่นกัน เป็นเป้าหมายที่สำคัญอีกประการหนึ่งที่ทุกรัฐมี โดยการป้องกันตนเองเนื่องจากในระบบการเมืองระหว่างประเทศนั้น การคงอยู่ของแต่ละรัฐไม่มีอะไรที่แน่นอน

3. การแสวงหาการกินดีอยู่ดี (Well – being) หมายถึง การที่รัฐจะดำเนินการเพื่อการพัฒนาความเป็นอยู่ของประชาชนในรัฐให้มีความเป็นอยู่ที่ดี โดยสามารถวัดได้จากเศรษฐกิจของประเทศ คือ ผลผลิตมวลรวมของประชาชาติ (Gross national product) อัตราการเติบโตทางเศรษฐกิจ (Rate of economic gross) ดังนั้นเพื่อให้แต่ละรัฐมีความพึงพอใจต่อเป้าหมายเบื้องต้นแต่ละรัฐก็จะพยายามปรับปรุงความเป็นอยู่ของประชากรของตนเองต่อไป โดยในทางปฏิบัติและทางแนวคิดนั้น การกินดีอยู่ดี (Well – being) หมายถึง สวัสดิการส่วนรวม ไม่ใช่ของปัจเจกชน \

4. การเสริมสร้างเกียรติภูมิของชาติ (Prestige) หมายถึง การที่รัฐหนึ่งจะแสดงออกด้วยการกระทำต่าง ๆ เพื่อให้รัฐอื่นเกิดความชื่นชม ประทับใจ และแสดงออกถึงการยอมรับและเคารพต่อรัฐตน

5. อุดมการณ์ของชาติ (Ideology) หมายถึง การที่รัฐหนึ่ง ๆ ซึ่งมีความเชื่อถือในอุดมการณ์ ก็พยายามเผยแพร่อุดมการณ์ของตนให้เป็นที่ยอมรับของรัฐอื่น โดยเป้าหมายมีความสำคัญยิ่งสำหรับบางรัฐไม่ว่าจะเป็นรับใหญ่หรือรัฐเล็ก เพื่อส่งเสริมหรือปกป้องอุดมการณ์ของชาติตนเองไว้ ให้เป็นส่วนประกอบที่สำคัญของนโยบายต่างประเทศของพวกเขาด้วย

6. การแสวงหาอำนาจ (Power) ได้แก่ การที่ทุกรัฐจะต้องมีอำนาจ คือขีดความสามารถที่รัฐชาติหนึ่ง ๆ จะกระทำตามเจตนารมณ์ของตนเองได้ ซึ่งอำนาจที่ทุกรัฐต้องมีอย่างน้อยที่สุดคือการอยู่รอดของชาติและการคงอำนาจอธิปไตยของตนเองไว้ได้ โดยอำนาจเป็นผลประโยชน์แห่งชาติที่สำคัญ

สรุปได้ว่า ผลประโยชน์ของชาติเพื่อดำรงไว้ซึ่งความมั่นคงของชาติ ได้แก่ ประชาชน ดินแดน รัฐบาลและอำนาจอธิปไตย เพื่อให้ประชาชนอยู่ดีกินดี มีความสุข ป้องกันและลดภัยคุกคามที่มาจากภายนอกประเทศ สร้างความภูมิใจให้แก่ประชาชนในรัฐ และการอยู่รอดของชาติและการดำรงอธิปไตยของตนเองไว้ได้

ความมั่นคงปลอดภัยทางสารสนเทศ

ความมั่นคงปลอดภัย (Security) คือสถานะที่มีความปลอดภัยไร้กังวล กล่าวคือ อยู่ในสถานะที่ไม่มีอันตรายและได้รับการป้องกันอันตรายทั้งที่เกิดขึ้นโดยตั้งใจหรือโดยบังเอิญ (Whitman &Mattord, 2005)เช่น ความมั่นคงปลอดภัยของประเทศ ย่อมเกิดขึ้นโดยมีระบบป้องกันหลายระดับ เพื่อปกป้องผู้นำประเทศ ทรัพย์สิน ทรัพยากร และประชากร ของประเทศ เป็นต้น องค์กรต่างๆหากต้องการให้เกิดความมั่นคงปลอดภัยย่อมต้องมีระบบป้องกันสิ่งต่างๆหลายระดับเช่นกันโดยทั่วไป องค์กรควรมีความมั่นคงปลอดภัยในส่วนต่างๆดังนี้

ความมั่นคงปลอดภัยทางกายภาพ (Physical security) เป็นการป้องกันสิ่งใดๆ ทางกายภาพ ไม่ว่าจะเป็นสิ่งของ สถานที่ หรือพื้นที่ใดๆขององค์กร จากการเข้าถึงที่ไม่ได้รับอนุญาตหรือการนำไปใช้ในทางที่ผิด

ความมั่นคงปลอดภัยส่วนบุคคล (Personal security) เป็นการป้องกันที่เกี่ยวข้องกับบุคคลหรือกลุ่มบุคคล

ความมั่นคงปลอดภัยในการปฏิบัติงาน (Operations security)เป็นการป้องกันรายละเอียดต่างๆ ของกิจกรรมหรือกลุ่มกิจกรรมใดๆ

ความมั่นคงปลอดภัยในการติดต่อสื่อสาร (Communications security) เป็นการป้องกันสื่อที่ใช้ในการติดต่อสื่อสาร รวมถึงเทคโนโลยีที่ใช้และเนื้อหาหรือข้อมูลที่ถูกส่งไปตามสื่อสัญญาณดังกล่าวแล้ว

ความมั่นคงปลอดภัยของเครือข่าย (Network security) เป็นการป้องกันองค์ประกอบ การเชื่อมต่อ และข้อมูลในเครือข่ายคอมพิวเตอร์

ความมั่นคงปลอดภัยของสารสนเทศ (Information security) เป็นการป้องกันภัยสารสนเทศในระบบคอมพิวเตอร์

ความมั่นคงปลอดภัยของสารสนเทศ(Information security) คือ การป้องกันสารสนเทศและองค์ประกอบอื่นๆ ที่เกี่ยวข้องกัน ซึ่งรวมถึงระบบและฮาร์ดแวร์ที่ใช้ในการจัดเก็บและถ่ายโอนสารสนเทศนั้นด้วย

แนวคิดหลักของความมั่นคงปลอดภัยของสารสนเทศ

ความลับ (Confidentiality)

ความลับเป็นการรับประกันว่าผู้มีสิทธิ์และได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลได้ เมื่อสารสนเทศถูกเข้าถึงได้โดยบุคคลที่ไม่มีสิทธิ์หรือไม่ได้รับอนุญาต จะถือว่าสารสนเทศที่เป็นความลับถูกเปิดเผย ซึ่งองค์กรต้องมีมาตรการป้องกันการเข้าถึงสารสนเทศที่เป็นความลับ เช่น

การจัดประเภทของสารสนเทศ

การรักษาความปลอดภัยให้กับแหล่งการจัดเก็บข้อมูล

กำหนดนโยบายการรักษาความมั่นคงปลอดภัยและการนำไปใช้

ให้การศึกษาแก่ทีมงานความมั่นคงปลอดภัยและการนำไปใช้

ในองค์กรโดยทั่วไป สารสนเทศที่ต้องการเก็บเป็นความลับ คือ สารสนเทศส่วนบุคคลของลูกค้าและพนักงาน ตลอดจนบุคคลที่ติดต่อกับองค์กร และต้องมีการให้ข้อมูล/สารสนเทศส่วนตัวแก่องค์กร บุคคลเหล่านี้ย่อมมีความหวังว่าสารสนเทศส่วนบุคคลของตนจะถูกเก็บเป็นความลับ แต่เป็นปัญหาที่เป็นภัยคุกคามต่อความลับของสารสนเทศย่อมเกิดขึ้นเมื่อมีการเผยแพร่สารสนเทศดังกล่าว จะด้วยความบังเอิญหรือไม่ก็ตาม เช่น อาจมีการส่งไปรษณีย์อิเล็กทรอนิกส์ (E – Mail)สารสนเทศส่วนบุคคลของลูกค้าไปให้พนักงานในแผนกเดียวกันที่อยู่สาขาอื่น แต่พิมพ์ไปรษณีย์อิเล็กทรอนิกส์ (E – Mail address)ผิดกลายเป็นไปรษณีย์อิเล็กทรอนิกส์ (E – Mail address) ของผู้รับฝ่ายบริษัทคู่ค้า กรณีเช่นนี้ก็ถือว่าเป็นการเปิดเผยความลับโดยไม่ตั้งใจ ซึ่งหากผู้รับคนดังกล่าวไปใช้ประโยชน์ต่อก็อาจทำให้เกิดความเสียหายแก่ลูกค้าได้ เป็นต้น

นอกจากนี้ในบางกรณีที่พนักงานทิ้งเอกสารจากการดำเนินงานในแต่ละวันโดยไม่ทันสังเกตว่า ภายในเอกสารดังกล่าวอาจมีสารสนเทศที่เป็นความลับปะปนอยู่ด้วย หากมีผู้ไม่หวังดีมาพบเข้า สารสนเทศที่เป็นความลับก็ถูกเปิดเผยได้เช่นกัน หรืออาจเป็นภัยคุกคามจากแฮคเกอร์ที่เจาะเข้าสู่ระบบงานบนเว็บไซต์ขององค์กร เพื่อเข้าถึงฐานข้อมูลเว็บ แล้วขโมยสารสนเทศที่เป็นความลับต่อไปขายต่อ เช่น ชื่อ – ที่อยู่ลูกค้า หมายเลขโทรศัพท์ หมายเลขบัตรเครดิต เป็นต้น ภัย

คุกคามที่มีเพิ่มมากขึ้นในปัจจุบันมีสาเหตุมาจากความก้าวหน้าทางเทคโนโลยี ประกอบกับความต้องการความสะดวกสบายในการสั่งซื้อสินค้าของลูกค้า โดยการยอมให้สารสนเทศส่วนบุคคลแก่เว็บไซต์เพื่อสิทธิ์ในการทำธุรกรรมต่างๆ บนเว็บไซต์ได้ โดยลืมไปว่าเว็บไซต์เป็นแหล่งข้อมูลที่สามารถขโมยสารสนเทศดังกล่าวได้ไม่ยากนัก

ความสมบูรณ์ (Integrity)

ความสมบูรณ์ คือ ความครบถ้วน ถูกต้อง และไม่มีสิ่งปลอมปน ดังนั้น สารสนเทศที่มีความสมบูรณ์จึงเป็นสารสนเทศที่สามารถนำไปใช้ประโยชน์ได้อย่างถูกต้องและครบถ้วน สารสนเทศจะขาดความสมบูรณ์ก็ต่อเมื่อสารสนเทศนั้นถูกนำไปเปลี่ยนแปลงปลอมปนด้วยสารสนเทศอื่น ถูกทำให้เสียหาย ถูกทำลาย หรือถูกกระทำในรูปแบบอื่น ๆ เพื่อขัดขวางการพิสูจน์การเป็นสารสนเทศจริง (ไม่ใช่สารสนเทศที่ถูกปลอมปนเข้ามา) ภัยคุกคามสำคัญที่มีต่อความสมบูรณ์ของสารสนเทศคือ ไวรัส(Virus) และ เวิร์ม (Worm) เนื่องจากทั้งไวรัสและเวิร์ม ถูกพัฒนาขึ้นมาเพื่อปลอมปนข้อมูลที่กำลังถูกเคลื่อนย้ายไปมาในเครือข่าย หรือแม้กระทั่งข้อมูลที่ถูกจัดเก็บอยู่ในเครื่องคอมพิวเตอร์ก็ตาม นอกจากนี้ แฮคเกอร์ก็สามารถปลอมปนหรือสร้างความเสียหายให้กับข้อมูลในองค์กรได้และสัญญาณรบกวนในขณะขนส่งข้อมูลตามสายสัญญาณ ก็เป็นอีกหนึ่งสาเหตุที่ทำให้ข้อมูลเกิดความเสียหายหรือถูกเปลี่ยนแปลงได้เช่นกัน จึงกล่าวได้ว่า ภัยคุกคามต่อความสมบูรณ์ของข้อมูลหรือสารสนเทศนั้น สามารถเกิดขึ้นได้ทั้งจากภายในและภายนอกองค์กร

ความพร้อมใช้ (Availability)

ความพร้อมใช้หมายถึง สารสนเทศจะถูกเข้าถึงหรือเรียกใช้งานได้อย่างราบรื่น โดยผู้ใช้หรือระบบอื่นที่ได้รับอนุญาตเท่านั้น หากเป็นผู้ใช้หรือระบบที่ไม่ได้รับอนุญาต การเข้าถึงหรือเรียกใช้งานจะถูกขัดขวางและล้มเหลวในที่สุด เช่น การป้องกันเนื้อหางานวิจัยที่อยู่ในห้องสมุด เนื้อหางานวิจัยจะพร้อมใช้ต่อผู้ใช้ที่ได้รับอนุญาต ซึ่งก็คือสมาชิกของห้องสมุดนั่นเอง ดังนั้นจึงต้องมีการระบุตัวตน (Identification) ว่าเป็นสมาชิกของห้องสมุดและพิสูจน์ว่าได้รับอนุญาตจริง (Authorization) สมาชิกจึงจะสามารถเข้าถึงและเรียกใช้ข้อมูลงานวิจัยได้อย่างอิสระ ตามลักษณะรูปแบบที่ต้องการ เป็นต้น

ความถูกต้องแม่นยำ (Accuracy)

ความถูกต้องแม่นยำ หมายถึง สารสนเทศจะต้องไม่มีความผิดพลาด และต้องมีค่าตรงกับความคาดหวังของผู้ใช้เสมอ ดังนั้น เมื่อใดก็ตามที่สารสนเทศมีค่าผิดเพี้ยนไปจากความคาดหวังของ

ผู้ใช้ ไม่ว่าจะเกิดจากการแก้ไขด้วยความตั้งใจหรือไม่ก็ตาม เมื่อนั้นจะถือว่าสารสนเทศ ไม่มีความถูกต้องแม่นยำเช่น เมื่อผู้ใช้ต้องการตรวจสอบยอดคงเหลือในบัญชีเงินฝากหลักจากที่ได้มีการถอนเงินไปแล้วจำนวนหนึ่ง ผลลัพธ์ที่ผู้ใช้คาดหวังคือยอดคงเหลือที่ถูกต้องตามจำนวนเงินที่ถอนไปหักออกจากยอดคงเหลือก่อนหน้า แต่เมื่อผลลัพธ์ออกมาผิดพลาดย่อมหมายถึงสารสนเทศนั้นไม่มีความถูกต้องแม่นยำ โดยหากเป็นการถอนเงินจากเจ้าหน้าที่ที่เคาน์เตอร์ของธนาคาร ความผิดพลาดดังกล่าวอาจเกิดจาก 2 กรณี 1.ขณะป้อนข้อมูลเข้าสู่ระบบเจ้าหน้าที่พิมพ์จำนวนถอนผิด2. ผู้ใช้กรอกจำนวนเงินถอนผิดพลาด เป็นต้น

เป็นของแท้ (Authenticity)

สารสนเทศที่เป็นของแท้ คือ สารสนเทศที่ถูกจัดทำขึ้นจากแหล่งที่ถูกต้อง ไม่ถูกทำซ้ำโดยแหล่งอื่นที่ไม่ได้รับอนุญาตหรือแหล่งที่ไม่คุ้นเคยหรือไม่ทราบมาก่อน เช่น การได้รับไปรษณีย์อิเล็กทรอนิกส์(E – Mail)จากผู้ส่งซึ่งผู้รับทราบแน่นอนว่าเป็นใคร (ไม่รวมกรณี Forward Mail)ไม่ทราบแหล่งกำเนิดสารสนเทศไปรษณีย์อิทรอนิกส์ (E – Mail)ที่แท้จริงเป็นต้น

ความเป็นส่วนตัว (Privacy)

ความเป็นส่วนตัว คือ สารสนเทศที่ถูกรวบรวมเรียกใช้และจัดเก็บโดยองค์กร จะต้องถูกใช้ในวัตถุประสงค์ที่ผู้เป็นเจ้าของสารสนเทศรับทราบขณะที่มีการรวบรวมสารสนเทศนั้น มิฉะนั้นจะถือว่าเป็นการละเมิดสิทธิส่วนบุคคลด้านสารสนเทศ

การปฏิบัติการข่าวสารหรือ IO(Information Operations)

(จตุชัย แพงจันทร์, 2558)การปฏิบัติการข่าวสารหรือ IO(Information Operations) หมายถึง การปฏิบัติการที่มีการบูรณาการสารสนเทศในทุก ๆ ด้าน เพื่อปกป้อง สนับสนุน และเพื่อการทวีกำลังรบ โดยมีเป้าหมายเพื่อให้มีอำนาจในการควบคุมสนามรบในเวลาและสถานที่ที่ต้องการ โดยใช้อาวุธยุทโธปกรณ์รวมทั้งทรัพยากรที่เหมาะสม ด้วยการปฏิบัติการอย่างต่อเนื่องในการรวบรวม นำเข้ากระบวนการแยกแยะและวิเคราะห์และนำสู่การปฏิบัติข้อมูลข่าวสาร เพื่อนำไปสู่การได้เปรียบในการปฏิบัติทางทหาร การปฏิบัติการข่าวสาร เป็นหลักการที่ออกเป็นเอกสารอย่างเป็นทางการครั้งแรกโดยกระทรวงกลาโหมสหรัฐอเมริกา ในปี ค.ศ. 2003 อนุมัติหลักการโดยนายโดนัลรัมเฟล รัฐมนตรีว่าการกระทรวงกลาโหมสหรัฐอเมริกาและเป็นเอกสารที่เปิดเผยในปี 2006เป็นการขยายผลหลักการที่เกี่ยวข้องกับสงครามข้อมูลข่าวสาร (Information Warfare: IW) ในมุมมองของกองทัพสหรัฐอเมริกา อย่างไรก็ตาม การนำหลักการการปฏิบัติการข่าวสารของกองทัพสหรัฐอเมริกาซึ่งเป็นผู้คิดค้นต้นแบบมาใช้มาใช้กับกองทัพในประเทศต่าง ๆ โดยตรงนั้นอาจไม่เหมาะสม ทั้งนี้เนื่องจากโครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศและการสื่อสาร

วัฒนธรรมองค์กร ความพร้อมของบุคลากรและกระบวนการปฏิบัติงานมีความแตกต่างกันอย่างมาก การนำมาใช้โดยไม่มีการเตรียมการอาจทำให้ไม่เกิดประสิทธิผลได้

(สุรชาติ บำรุงสุข, 2553) ปัจจุบันปฏิบัติการข่าวสารถือว่าเป็นเครื่องมือสำคัญในระดับแนวหน้าของการปฏิบัติการทางทหาร ทั้งนี้เพราะการนำเอาเทคโนโลยีมาใช้ในสนามรบสามารถทำให้การเผยแพร่ข้อมูลข่าวสารและการควบคุมพื้นที่ในสนามรบมีประสิทธิภาพอย่างมากและถือเป็นข้อมูลสำคัญที่ผู้นำทางการทหารจะนำไปใช้ประกอบในการตัดสินใจในการทำการรบ เพราะในการทำสงครามนั้น ฝ่ายทหารจำเป็นต้องเข้าใจถึงอิทธิพลที่มีอิทธิพลต่อการตัดสินใจของฝ่ายตรงกันข้ามและต้องมีการปฏิบัติการพิสูจน์ทราบเกี่ยวกับฝ่ายตรงกันข้าม 3 ประการดังนี้

1.ศักยภาพของฝ่ายตรงกันข้ามในการปฏิบัติการ โดยเฉพาะการได้รับการสนับสนุนจากประชาชน เพราะการสนับสนุนจากประชาชนเป็นแหล่งที่มาสำคัญที่สุดของพลังอำนาจแห่งชาติ ความแข็งแกร่งของกองกำลัง การเคลื่อนไหวอย่างเสรี และกำลังใจในการต่อสู้ของฝ่ายตรงกันข้าม

2. เจตนาในการต่อสู้เป็นปัจจัยที่บ่งชี้ว่า ฝ่ายตรงกันข้ามคิดจะต่อสู้ต่อไปหรือยอมแพ้ ทั้งนี้เพราะหากฝ่ายตรงกันข้ามเห็นว่าสงครามข้างหน้าฝ่ายของตนมีโอกาสจะชนะย่อมมีการระดมสรรพกำลังเข้าต่อสู้อย่างเต็มที่ ในทางกลับกันหากฝ่ายตรงกันข้ามตระหนักว่า ไม่มีโอกาสจะชนะสงคราม ก็อาจยอมเจรจา ยอมถอนกำลังทหารหรือยอมวางอาวุธ เป็นต้น

3. กระบวนการทางความคิดของฝ่ายตรงกันข้าม หมายถึง ข้อมูลข่าวสารที่เชื่อถือได้ ความสมบูรณ์และความน่าเชื่อถือของข้อมูลข่าวสารและห้วงเวลาที่เหมาะสมของสถานการณ์เป็นปัจจัยสำคัญที่ฝ่ายตรงกันข้ามใช้ในการตัดสินใจปฏิบัติการ

สรุปได้ว่า การปฏิบัติการข่าวสารมีความสำคัญอย่างมากต่อสถานการณ์ที่มีความขัดแย้งจากภายในประเทศ โดยการนำการบูรณาการข้อมูลข่าวสารสารสนเทศมาเพื่อปกป้อง สนับสนุนและพัฒนากำลังรบทางการทหารให้มีความเข้มแข็ง อีกทั้งการนำปฏิบัติการทางทหารมาจะช่วยให้การเผยแพร่ข้อมูลข่าวสารและการควบคุมพื้นที่ในสนามรบสามารถทำได้อย่างมีประสิทธิภาพมาก จะเห็นได้ว่า เทคโนโลยีสารสนเทศมีความสำคัญต่อยุคปัจจุบันเป็นอย่างมาก การนำเทคโนโลยีสารสนเทศมาใช้ในการปฏิบัติการข่าวสารจะทำให้กลุ่มเป้าหมายได้ข้อมูลข่าวสารครบถ้วน ทั่วถึง ครอบคลุม รวดเร็ว ทำให้เกิดการรับรู้รับทราบ และเข้าใจถึงความต้องงการในการขับเคลื่อนไปสู่เป้าหมายได้

แนวคิดเกี่ยวกับการก่อการร้ายทางไซเบอร์

สงครามไซเบอร์เกิดขึ้นครั้งแรกเมื่อปี ค.ศ.2007 ระหว่างประเทศรัสเซียและประเทศเอสโตเนีย โดยเหตุเกิดเนื่องจากประเทศเอสโตเนียย้ายอนุสารวรีย์รูปปั้นทหารที่เมืองทาลลินน์ ประเทศเอสโตเนีย ซึ่งรัสเซียสร้างขึ้นมาเพื่อเป็นอนุสรณ์แก่ทหารรัสเซียที่เสียชีวิตจาการต่อสู้ในสงครามโลกครั้งที่สอง การเคลื่อนย้ายดังกล่าวไม่พอใจอย่างยิ่งต่อประเทศรัสเซีย และเป็นสาเหตุให้รัสเซียต้องโจมตีทางไซเบอร์ต่อระบบต่าง ๆ ในประเทศเอสโตเนีย (จตุชัย แพงจันทร์,2558) สิ่งที่เอสโทเนียเจอเข้าไปคือ ดีดีโอเอส (Distribute Denial of Service – DDOS) หรือการโจมตีด้วยการระดมคำสั่งเข้าใส่จนเซิร์ฟเวอร์ไม่สามารถให้บริการได้ตามปกติ โดยทั่วไปดีดีโอเอส เป็นโปรแกรมที่ถูกจัดเตรียมไว้ล่วงหน้าให้ทำหน้าที่ส่งคำสั่งจำนวนมาก ๆ พร้อมกันโดยถูกออกแบบมาเพื่อให้การจราจรในอินเทอร์เน็ตติดขัดหรือทำให้เครือข่ายล่มลง คำสั่งที่ส่งออกไปมาจากคอมพิวเตอร์นับหมื่นเครื่อง คอมพิวเตอร์ที่ทำหน้าที่โจมตีดังกล่าวรวมกันเรียกว่า บอตเน็ตหรือโรโบติกเน็ตเวิร์ก – เครือข่ายหุ่นยนต์ ของคอมพิวเตอร์ในสภาพซอมบี้ ที่ถูกควบคุมอยู่ระยะไกล ในกรณีของเอสโตเนีย การโจมตีด้วยดีดีโอเอสนับเป็นการโจมตีครั้งใหญ่ที่สุด เสมือนว่ามีบอตเน็ตที่แตกต่างกันหลายบอตเน็ต ซึ่งแต่ละเครือข่ายมีคอมพิวเตอร์ลูกข่ายติดเชื้อไวรัสอยู่หลายหมื่นเครื่อง การพุ่งเป้าโจมตีของบอตเน็ตพุ่งเป้าไปยังที่อยู่อินเทอร์เน็ต ไม่ใช่หน้าเว็บซึ่งเปิดเผยต่อสาธารณะแต่เป็นที่อยู่ของเซิร์ฟเวอร์ที่ใช้รองรับการทำงานของเครือข่ายโทรศัพท์ และเซิร์ฟเวอร์ที่เป็นทำเนียบรายชื่อเว็บไซต์ที่เรียกกันว่าอินเตอร์เน็ตไดเร็กทอรี่ ผลลัพธ์ คือระบบการสื่อสารและพาณิชยกรรมทั่วประเทศกระทบกระเทือนทันทีและการโจมตียังคงมีอย่างต่อเนื่อง (คลาร์ก, ริชาร์ด เอ,2555)

เมื่อปี ค.ศ.2009 ได้เกิดการแพร่ระบาดของโกสต์เน็ต (GhostNet) ซึ่งเป็นไวรัสประเภทบอตเน็ต(Botnet)ที่เชื่อกันว่าพัฒนาและใช้งานโดยรัฐบาลประเทศจีน เพื่อการจารกรรมข้อมูลของรัฐบาลประเทศอื่น โดยเหตุผลที่สรุปว่า รัฐบาลจีนอยู่เบื้องหลังเนื่องจากว่าระบบบัญชาการและควบคุมของบอตเน็ต (Botnet) มีฐานปฏิบัติการอยู่ในประเทศจีน และเป้าหมายเพื่อจารกรรมข้อมูลขององค์ดาไลลามะ โดยคอมพิวเตอร์ที่ถูกโจมตีส่วนใหญ่เป็นของสถานทูต กระทรวงการต่างประเทศและหน่วยงานของรัฐอื่น ๆ เพื่อจารกรรมข้อมูลเกี่ยวกับการเคลื่อนไหวทางการเมือง เศรษฐกิจและข้อมูลที่สำคัญของประเทศนั้น

ต่อมาเมื่อปี ค.ศ.2010 อิสราเอลได้ร่วมมือกับสหรัฐอเมริกาในการโจมตีโรงงานผลิตอาวุธนิวเคลียร์ของอิหร่านโดยทั้งสองประเทศได้สร้างอาวุธไซเบอร์ที่มีชื่อว่า สตักซ์เน็ต (Stuxnet) ซึ่งถือว่าเป็นอาวุธสงครามชิ้นแรกที่ใช้บนสมรภูมิไซเบอร์สเปซ โดยใช้เพื่อทำลายเป้าหมายทางทหาร อาวุธนี้ได้พิสูจน์ให้เห็นว่ามีอานุภาพการทำล้างสูงและที่สำคัญส่งผลกระทบทางกายภาพได้จริง จนทำให้โครงการผลิตอาวุธนิวเคลียร์ของประเทศอิหร่านต้องหยุดชะงักหรือล่าช้าออกไปโดย

ไม่มีกำหนด สตักซ์เน็ตยังสามารถใช้ทำลายโรงงานอุตสาหกรรมอื่น ๆ ที่ใช้ระบบควบคุมเหมือนโรงงานนิวเคลียร์ของอิหร่าน เช่น โรงไฟฟ้าพลังงานนิวเคลียร์ โรงกลั่นน้ำมัน ระบบควบคุมท่อส่งก๊าซธรรมชาติ ระบบควบคุมโครงข่ายกระแสไฟฟ้า เป็นต้น

การก่อการร้ายทางไซเบอร์ (Cyber - terrorism) เป็นวิธีการก่อการร้ายโดยโจมตีเป้าหมายเพื่อสร้างความเสียหายให้กับระบบแฟ้มข้อมูลหรือทำให้ระบบคอมพิวเตอร์เสียหาย เช่น การเข้าถึงข้อมูลเพื่อลักลอบแก้ไขทำลาย คัดลอก ทำให้คอมพิวเตอร์ทำงานผิดพลาด ซึ่งล้วนก่อให้เกิดความเสียหายมหาศาลอาทิ บิดเบือนข้อมูลหรือลบข้อมูลทางเศรษฐกิจในคอมพิวเตอร์ของประเทศเป้าหมายโอนเงินจากบัญชีธนาคารหนึ่งไปเข้าอีกบัญชีหนึ่งทำให้โปรแกรมควบคุมและสั่งการทางทหารใช้การไม่ได้เมื่อเกิดวิกฤตการณ์ระหว่างประเทศทำให้ไม่สามารถควบคุมดาวเทียมจากระยะไกลได้ด้วยคอมพิวเตอร์ ฯลฯ มีรายงานว่า ในปี 2538 นักฝ่าด่าน (Hacker/Cracker) หรือนักก่อกวนระบบเครือข่ายคอมพิวเตอร์เคยโจมตีระบบคอมพิวเตอร์ของกระทรวงกลาโหมสหรัฐฯ ถึง 250,000 ครั้งและสามารถเจาะผ่านระบบรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ได้ประมาณร้อยละ70 นอกจากนี้กลุ่มผู้ก่อการร้ายยังใช้อินเทอร์เน็ตเป็นเครื่องมือในการแลกเปลี่ยนข้อมูลส่งแผนปฏิบัติการและสั่งการให้ลงมือปฏิบัติงานโดยไม่ต้องมาพบกันและยังติดต่อกันข้ามทวีปได้ระบบอินเทอร์เน็ตมีความปลอดภัยจากการถูกจับได้กว่าเครื่องมือหรือวิธีสื่อสารอื่นเนื่องจากสามารถใช้รหัสลับ ใช้เวลาสั้น และตรวจจับได้ยากยิ่ง

อาวุธไซเบอร์ (Cyber weapon) เป็นซอฟต์แวร์ที่นักรบไซเบอร์ใช้ในการโจมตีระบบของฝ่ายตรงกันข้าม ซึ่งโดยส่วนใหญ่เป็นเครื่องมือหรือซอฟต์แวร์ที่เหล่าแฮกเกอร์ทั่วไปใช้ในการจะระบบต่าง ๆ เครื่องมือที่แฮกเกอร์ใช้ทั่วไป ยังมีเครื่องมือที่เรียกได้ว่าเป็นอาวุธสงครามไซเบอร์ที่ถูกพัฒนาขึ้นมาเพื่อใช้ปฏิบัติภารกิจเฉพาะอย่าง เช่น สตักซ์เน็ต (Stuxnet) ซึ่งเป็นไวรัสแบบก้าวหน้าที่ใช้ประโยชน์จากช่องโหว่แบบซีโร่เดย์ (Zero – day) และมีขีดความสามารถในการทำลายโรงงานผลิตอาวุธนิวเคลียร์ ถึงแม้ว่าโรงงานจะไม่ได้ถูกทำลายในทางกายภาพก็ตาม แต่เครื่องจักรที่ใช้ผลิตอาวุธนั้นต้องหยุดชะงักไม่สามารถทำงานช่วงระยะเวลาหนึ่งซึ่งนั่นถือว่าบรรลุเป้าหมาย เครื่องมือหรืออาวุธไซเบอร์ สามารถแบ่งออกเป็นประเภทต่าง ๆ ขึ้นอยู่กับฟังก์ชั่นที่ใช้ เครื่องมือหรือโปรแกรมที่เหล่าแฮกเกอร์ใช้นั่นมีมากมายและหลากหลายและสามารถดาวน์โหลดจากอินเทอร์เน็ตมาใช้งานได้โดยง่าย เครื่องมือทางไซเบอร์เหล่านี้เปรียบเสมือนดาบสองคม ขึ้นอยู่กับผู้ใช้งานถ้านำไปใช้ในทางที่ดีก็จะมีประโยชน์อย่างมาก แต่หากนำมาใช้เพื่อประสงค์ร้าย ก็ยิ่งเป็นอันตรายต่อผู้อื่น(ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย, 2556) ยกตัวอย่างเช่น

1.บอตเน็ต (Botnet)ภัยคุกคามสารสนเทศที่เกิดกับกลุ่มของเครื่องคอมพิวเตอร์ที่มีโปรแกรมไม่พึงประสงค์ติดตั้งอยู่ ซึ่งโปรกรมที่ไม่พึงประสงค์นี้จะทำการรับคำสั่งจากผู้ควบคุมผ่านเครือข่ายอินเทอร์เน็ต โดยอาจเป็นคำสั่งที่ให้ทำการโจมตีผ่านระบบเครือข่าย เช่น ส่งสแปม หรือโจรกรรมข้อมูลในเครื่องคอมพิวเตอร์นั้น

2. ตั้งค่าเครือข่ายของเครื่องให้บริการ (Open DNS Resolver)ภัยคุกคามสารสนเทศที่เกิดจากการตั้งค่าเครือข่ายของเครื่องให้บริการ DNS อาจถูกใช้เป็นส่วนหนึ่งในการโจมตีระบบต่าง ๆ ในลักษณะของ DDosได้

3.การเจาะระบบ (Web defacement)ภัยคุกคามด้านสารสนเทศที่เกิดจากการเจาะระบบได้สำเร็จ และทำการเปลี่ยนแปลงข้อมูลบนหน้าเว็บไซต์โดยมีจุดประสงค์เพื่อสร้างความอับอายทำให้หน่วยงานเจ้าของเว็บไซต์หรือผู้ที่เกี่ยวข้องเสียหาย

4. การฉ้อฉล ฉ้อโกง หรือหลอกลวง (Phishing)ภัยคุกคามด้านสารสนเทศในลักษณะการฉ้อฉล ฉ้อโกง หรือหลอกลวงเพื่อประโยชน์ ส่วนใหญ่มีวัตถุประสงค์เพื่อขโมยข้อมูลสำคัญของผู้ใช้งาน เช่น บัญชีผู้ใช้งาน รหัสผ่าน หรือข้อมูลสำคัญทางธุรกรรมทางอิเล็กทรอนิกส์ เป็นต้น ผู้โจมตีใช้วิธีการล่อลวงให้ผู้ใช้งานเข้าถึงบริการที่ทำปลอมขึ้น

5.การโจมตีสภาพความพร้อมใช้งานของระบบ(DDos) ภัยคุมคามสารสนเทศในลักษณะการโจมตีสภาพความพร้อมใช้งานของระบบ โดยมีลักษณะการโจมตีมาจากหลายที่มีการโจมตีเป้าหมายเดียวกันภายในช่วงเวลาเดียวกัน เพื่อทำให้บริการต่าง ๆ ของระบบไม่สามารถให้บริการได้ตามปกติ มีผลกระทบตั้งแต่เกิดความล่าช้าในการตอบสนองของบริการจนกระทั่งระบบไม่สามารถให้บริการต่อไปได้

6. เนื้อหาที่เป็นภัยภัยคุกคามสารสนเทศ ที่เกิดจากการใช้หรือเผยแพร่ข้อมูลที่เป็นจริงหรือไม่เหมาะสม (Abusive Content) เพื่อทำลายความน่าเชื่อถือ เพื่อก่อให้เกิดความไม่สงบหรือข้อมูลที่ไม่ถูกต้องตามกฎหมาย เช่น ลามก อนาจาร หมิ่นประมาท และรวมถึงการโฆษณาขายสินค้าต่าง ๆ ทางอีเมล์ที่ผู้รับไม่ได้มีความประสงค์จะรับข้อมูลโฆษณานั้น

7.โปรแกรมที่ไม่พึงประสงค์ ที่เกิดจากโปรแกรมชุดคำสั่งที่พัฒนาขึ้นด้วยความประสงค์ร้าย (Malicious code) เพื่อทำให้เกิดความขัดข้องหรือเกิดความเสียหายกับระบบหรือโปรแกรมหรือซอฟต์แวร์ไม่พึงประสงค์นี้ติดตั้งอยู่ โดยปกติโปรแกรมหรือซอฟต์แวร์ไม่พึงประสงค์ประเภทนี้ต้องอาศัยผู้ใช้งานเป็นผู้เปิดก่อน จึงจะสามารถติดตั้งตัวเองหรือทำงานได้ เช่น ไวรัสเวิมส์ โทรจัน หรือสปายแวร์ต่าง ๆ

8.ความพยายามรวบรวมข้อมูลของระบบ ภัยคุกคามด้านสารสนเทศที่เกิดจากความพยายามของผู้ไม่หวังดีในการรวบรวมข้อมูลจุดอ่อนของระบบ (Scanning) ด้วยการเรียกใช้บริการ

ต่าง ๆ ที่อาจเปิดในระบบ เช่น ข้อมูลเกี่ยวกับระบบปฏิบัติการ ระบบซอฟต์แวร์ที่ติดตั้งหรือใช้งาน ข้อมูลบัญชีผู้ใช้งาน (User account) ที่มีอยู่ในระบบ เป็นต้น

9.การบุกรุกหรือเจาะระบบได้สำเร็จ ภัยคุกคามสารสนเทศที่เกิดกับระบบที่ถูกบุกรุก/เจาะเข้าระบบได้สำเร็จ (Intrusions) และระบบถูกครอบครองด้วยผู้ที่ไม่ได้รับอนุญาต

10.ฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ (Fraud) สามารถเกิดได้ในหลายลักษณะ เช่น การลักลอบใช้งานระบบหรือทรัพยากรทางสารสนเทศที่ไม่ได้รับอนุญาตเพื่อแสวงหาผลประโยชน์ของตนเอง หรือขายสินค้าหรือซอฟต์แวร์ที่ละเมิดลิขสิทธิ์

Resource Material Series (1990, p 208)อาชญากรรมคอมพิวเตอร์เป็นสิ่งที่ยากแก่การแก้ไข ทางออกที่ดีที่สุดก็คือ ต้องทำให้ยากต่อการก่อความผิด โดยนัยนี้สิ่งที่สำคัญมาก คือ จะต้องกวดขันในเรื่องระบบความปลอดภัยทางคอมพิวเตอร์ การก่อการร้ายทางคอมพิวเตอร์ เป็นการดำเนินการโดยรัฐชาติแห่งหนึ่งเพื่อแทรกซึมคอมพิวเตอร์หรือเครือข่ายของอีกรัฐชาติหนึ่ง เพื่อวัตถุประสงค์ในการก่อการให้เกิดความเสียหายหรือการรบกวนขัดขวางกระบวนการดำเนินการตามปกติให้หยุดชะงักปลายทศวรรษที่ 1990 จีนได้ดำเนินการทุกประการอย่างเป็นระบบเท่าที่ประเทศหนึ่งควรได้ทำ หากประเทศนั้นคิดที่จะมีศักยภาพเชิงรุกในการทำสงครามไซเบอร์และยังคิดว่าตนเองก็อาจตกเป็นเป้าการโจมตีจากสงครามไซเบอร์พร้อมกันไปด้วย การดำเนินการดังกล่าวประกอบด้วย

1. จัดตั้งกลุ่มแฮกเกอร์พลเรือนดำเนินการจารกรรมไซเบอร์อย่างกว้างขวาง รวมทั้งการจารกรรมทั้งซอฟแวร์และฮาร์ดแวร์คอมพิวเตอร์ของสหรัฐอเมริกาดำเนินการขั้นตอนหลายประการเพื่อป้องกันไซเบอร์สเปซของตนเอง

2. จัดตั้งหน่วยทหารเพื่อการรบในสงครามไซเบอร์ขึ้นและติดตั้งระเบิด “ลอจิกบอมบ์” ไว้ทั่วทั้งโครงข่ายสาธารณูปการของสหรัฐอเมริกานอกจากการพัฒนายุทธศาสตร์ไซเบอร์แล้ว จีนยังใช้ประโยชน์จากกลุ่มแฮกเกอร์เอกชนพร้อมกันไปด้วย ด้วยการทำให้กลุ่มนี้ดำเนินการอยู่ในแนวเดียวกับผลประโยชน์ของชาติอย่างใกล้ชิด คณะกรรมาธิการทบทวนความสัมพันธ์ด้านความมั่นคงระหว่างจีนกับสหรัฐอเมริกาประเมินเอาไว้ว่า มีกลุ่มแฮกเกอร์ในจีนมากถึง 250 กลุ่ม ซึ่งมีขีดความสามารถสูงเพียงพอต่อการเป็นภัยคุกคามต่อผลประโยชน์ของสหรัฐอเมริกาในไซเบอร์สเปซได้

ปี 2003 จีนประกาศจัดตั้งหน่วยงานทหารเพื่อการทำสงครามไซเบอร์ขึ้นมา ประกอบด้วยเทคนิคที่สาม (Third Technical Department)แห่งกองทัพปลดปล่อยประชาชนจีนและสำนักงานการสื่อสารด้านข่าวกรองหลิงสวี่ ตั้งอยู่ที่ฐานทัพเรือบนเกาะไหหนาน ตามข้อมูลของเพนตากอนหน่วยงานเหล่านี้รับผิดชอบทั้งปฏิบัติการเชิงรุกและป้องกันในไซเบอร์สเปซและยังทำหน้าที่เพื่อ

การออกแบบอาวุธไซเบอร์ซึ่งไม่เคยพบเห็นกันมาก่อนและไม่มีระบบป้องกันใดถูกออกแบบมาเพื่อให้ยับยั้งมันได้ ในเอกสารที่ตีพิมพ์ออกมาฉบับหนึ่ง ทางการจีนจัดทำรายงานตัวอย่างของอาวุธและเทคนิคเหล่านี้เอาไว้ดังนี้ติดตั้งกับระเบิดข้อมูลดำเนินการสอดแนมข้อมูลเปลี่ยนแปลงข้อมูลเน็ตเวิร์ก ปล่อยระเบิดข้อมูลข่าวสาร ดัมพ์ข้อมูลขยะ แพร่ข้อมูลโฆษณาชวนเชื่อ เผยแพร่ข้อมูลโคลนนิ่งจัดตั้งการป้องกันข้อมูลข่าวสารและ จัดตั้งสถานีจารกรรมเครือข่าย

ปี 2007 รัฐบาลจีนเข้าไปเกี่ยวข้องในการแทรกซึมเจาะเข้าสู่เน็ตเวิร์กของยุโรปและสหรัฐอเมริกาต่อเนื่องในวงกว้างเป็นชุดๆ ประสบความสำเร็จในการทำสำเนาและส่งข้อมูลจำนวนมหึมากลับออกมาได้ โจนาธาน อีแวนส์ ผู้อำนวยการสำนักงานข่าวกรองภายในประเทศเอ็มไอ 5 ของอังกฤษทำหนังสือถึงบริษัทชั้นนำ 300 บริษัทในสหราชอาณาจักร แนะนำว่าเครือข่ายคอมพิวเตอร์ของพวกเขาอาจถูกแทรกซึมโดยรัฐบาลจีน ฮันเรมเบิร์ก ซึ่งดำรงดำแหน่งเดียวกันสำหรับเยอรมนีก็กล่าวหารัฐบาลปักกิ่งด้วยเช่นกัน คราวนี้เป็นเรื่องของการเจาะทะลวงเข้าไปในคอมพิวเตอร์ของแองเกลา แมร์เคิล นายกรัฐมนตรีเยอรมนี

การจารกรรมคอมพิวเตอร์ครั้งนี้ยังพุ่งเป้าไปที่เจ้าหน้าที่อเมริกันระดับสูงหลายคน เช่น มีการแฮกคอมพิวเตอร์ของ โรเบิร์ตเกตส์ รัฐมนตรีว่าการกระทรวงกลาโหม ถัดมาเจ้าหน้าที่ของจีนลอกก๊อปปี้ข้อมูลออกจากคอมพิวเตอร์โน๊ตบุ๊กของคาร์ลอส กูเทียเรส รัฐมนตรีกระทรวงพาณิชย์เมื่อท่านรัฐมนตรีอยู่ระหว่างการเดินทางเยือนจีน จากนั้นก็พยายามใช้ข้อมูลดังกล่าวนั้นเพื่อเข้าถึงระบบคอมพิวเตอร์ของกระทรวงพาณิชย์สหรัฐอเมริกา เมื่อถูกขอความเห็นเกี่ยวกับฝ่ายจีน โรเบิร์ตลอร์เลสส์ รองปลัดกระทรวงพาณิชย์ยอมรับว่าเจ้าหน้าที่เหล่านั้นมีศักยภาพสูงอย่างยิ่งในการโจมตีและลดระดับการป้องกันของระบบคอมพิวเตอร์ของเรา เพื่อปิดระบบสำคัญของเรา พวกเขาเห็นว่าเป็นองค์ประกอบสำคัญของขีดความสามารถในการทำสงครามนอกระบบของตัวเอง

ปี 2009 ทีมวิจัยแคนาดาค้นพบโปรแกรมคอมพิวเตอร์ที่มีสมรรถนะสูงและขนานนามว่าโกสต์เน็ตที่สามารถยึดครองคอมพิวเตอร์รวมแล้วกว่า 1,300 เครื่องในสถานเอกอัครราชทูตต่างๆในหลายประเทศทั่วโลก โปรแกรมโกสต์เน็ตยังมีความสามารถในการส่งคำสั่งจากระยะไกลเพื่อเปิดงานใช้กล้องและไมโครโฟนที่ติดตั้งไว้กับคอมพิวเตอร์โดยไม่ทำให้ผู้ใช้งานคอมพิวเตอร์ดังกล่าวอยู่รู้ตัวหรือระแคะระคาย เพื่อใช้เป็นช่องทางในการส่งภาพและเสียงออกไปอย่างเงียบกลับไปยังเซิร์ฟเวอร์ที่ตั้งอยู่ในประเทศจีน เป้าหมายลำดับแรกสุดของโปรแกรมดังกล่าวคือบรรดาสำนักงานขององค์กรเอกชนต่างๆ ที่ทำงานเกี่ยวกับประเด็นเรื่องทิเบต ปฏิบัติการดังกล่าวดำเนินการไปอย่างต่อเนื่อง 22 เดือนจึงถูกตรวจสอบพบ ในปีเดียวกันนั้นหน่วยข่าวกรองของสหรัฐอเมริกาปล่อยข่าวไปยังสื่อว่าแฮกเกอร์จากจีนได้แทรกซึมเข้าสู่ระบบการจ่ายกระแสไฟฟ้าหรือพาวเวอร์กริดของสหรัฐอเมริกา และทิ้งเครื่องมือที่สามารถใช้ในการปิดการทำงานของระบบ

เอาไว้ขอบเขตและปริมาณที่รัฐบาลของจีนเจาะเข้าไปในระบบเครือข่ายของอุตสาหกรรมและสถาบันเพื่อการวิจัยและพัฒนาต่างๆ ของอุตสาหกรรม ในสหรัฐอเมริกา ยุโรปและญี่ปุ่น มหาศาลชนิดไม่เคยปรากฏมาก่อนในประวัติศาสตร์ของการจารกรรมข้อมูลมหาศาล ถูกก๊อปปี้จากห้องทดลองของมหาวิทยาลัย อุตสาหกรรมและสำนักงานของรัฐบาลต่างๆ ความลับที่อยู่เบื้องหลังทุกสิ่งทุกอย่างตั้งแต่สูตรเวชภัณฑ์ ไปจนถึงการออกแบบวิศวชีวกรรม (ไบโอเอ็นจิเนียริ่ง) นาโนเทคโนโลยี ระบบอาวุธต่างๆ ตลอดจนผลิตภัณฑ์อุตสาหกรรมประจำวันทั่วไป ถูกลอบดึงเอาไปโดยกองทัพปลดปล่อยประชาชนจีนและกลุ่มแฮกเกอร์ต่างๆ หลังจากนั้นก็ส่งมอบต่อให้กับบริษัทผู้ผลิตทั้งหลายของจีนต่อไป

ไซเบอร์สเปซ (Cyberspace)หมายถึง เครือข่ายคอมพิวเตอร์ทั้งหลายที่มีอยู่ในโลกนี้และทุกๆอย่างที่มันเชื่อมต่อและควบคุมอยู่ ไม่ได้หมายถึงเพียงอินเทอร์เน็ตเท่านั้น อินเตอร์เน็ตเป็นเครือข่ายคอมพิวเตอร์เปิดที่เชื่อมโยงเครือข่ายคอมพิวเตอร์หลายๆเครือข่ายเข้าด้วยกัน จากเครือข่ายใดๆบนอินเตอร์เน็ตผู้ใช้สามารถติดต่อสื่อสารกับคอมพิวเตอร์ที่เชื่อมต่ออยู่บนเน็ตเวิร์คทั้งหลายของอินเตอร์เน็ตนั้น ไซเบอร์สเปซรวมทั้งอินเตอร์เน็ตบวกกับเครือข่ายคอมพิวเตอร์ทั้งหลายที่ไม่ควรจะเข้าถึงได้ผ่านทางอินเตอร์เน็ต เครือข่ายคอมพิวเตอร์ที่เป็นเอกเทศเหล่านี้มีลักษณะคล้ายอินเทอร์เน็ต แต่แยกเป็นอิสระอยู่อย่างน้อยก็ในทางทฤษฎี ส่วนอื่นๆที่เหลืออยู่ของไซเบอร์สเปซคือเครือข่ายหรือเน็ตเวิร์กเพื่อการทำธุรกรรมซึ่งทำหน้าที่เป็นเหมือนผู้รับ–ส่งข้อมูลเกี่ยวกับการถ่ายโอนเงิน การซื้อขายหุ้นในตลาดหรือธุรกรรมเกี่ยวกับบัตรเครดิตต่างๆ บางเครือข่ายเป็นระบบเพื่อใช้ในการควบคุม เพื่อให้เครื่องจักรสามารถพูดคุยซึ่งกันและกันได้เช่น แผงควบคุมที่ทำหน้าที่ออกคำสั่งต่อปั๊ม ลิฟท์ และเครื่องกำเนิดไฟฟ้า เป็นต้น อาชญากรไซเบอร์การเข้าถึงระบบเน็ตเวิร์กเพื่อเจาะเข้าถึงเครือข่ายเหล่านี้เพื่อควบคุมหรือหยุดการทำงานของมันได้ หากควบคุมเน็ตเวิร์กหนึ่งได้ อาชญากรไซเบอร์ก็สามารถขโมยข้อมูลเกี่ยวกับเน็ตเวิร์กนั้นๆได้หรือสามารถส่งคำสั่งที่จะโอนเงิน ปล่อยน้ำมันรั่วไหลทิ้ง เปิดวาล์วปล่อยก๊าซ หรือระเบิดเครื่องกำเนิดไฟฟ้าทิ้งทำให้รถไฟตกราง ทำให้เครื่องบินตก ส่งกำลังทหารไปดักซุ่มโจมตีหรือจุดระเบิดขีปนาวุธให้ยิงเข้าใส่เป้าหมายที่ไม่ควรตกเป็นเป้าหมายได้ หากอาชญากรไซเบอร์ทำให้เน็ตเวิร์กล่ม ข้อมูลจะสูญหาย เปลี่ยนคอมพิวเตอร์ให้กลายเป็นท่อนไม้จากนั้นระบบการเงินทั้งหมดอาจล่ม ระบบห่วงโซ่อุปทานต้องยุติลง ดาวเทียมอาจหลุดจากวงโคจรหายไปในอวกาศ และสายการบินอาจต้องจอดนิ่งสนิทอยู่กับพื้นซึ่งไม่ใช่เรื่องสมมุติที่ไม่มีเหตุผล หลายสิ่งหลายอย่างในทำนองเดียวกันนี้เคยเกิดขึ้นมาแล้ว บางครั้งเกิดขึ้นในระหว่างการทดลอง บางครั้งเกิดเพราะความผิดพลาดพลั้งเผลอและบางครั้งเกิดขึ้นในสถานะที่เป็นผลของสงครามไซเบอร์หรืออาชญากรรมไซเบอร์ อย่างที่พลเรือเอกแม๊กคอร์เนลล์ตั้งข้อสังเกตไว้ ระบบสารสนเทศบริหารจัดการโดยคอมพิวเตอร์เน็ตเวิร์ก ซึ่งดำเนินการด้านสาธารณูปโภค การ

ขนส่ง การธนาคาร และการสื่อสาร สามารถใช้เป็นประโยชน์หรือเพื่อการโจมตีได้ภายในไม่กี่วินาทีจากสถานที่ห่างไกลในต่างแดน ไม่มีกองเรือรบหรือขีปนาวุธข้ามทวีป หรือกองทัพใดๆ สามารถปกป้องเราจากการโจมตีจากที่ตั้งห่างไกลดังกล่าว ซึ่งไม่เพียงอยู่นอกอาณาเขตของเราแต่ยังอยู่นอกเหนือปริมณฑลทางการภาพ ไปอยู่ในปริมณฑลทางดิจิตอลของไซเบอร์สเปซ

ไซเบอร์สเปซเหมือนกับระบบอินเทอร์เน็ตที่เต็มไปด้วยปัญหาของซอฟแวร์และฮาร์ดแวร์และความไม่สมบูรณ์ของโครงร่าง (Configuration) ต่างๆดังนั้น คอมพิวเตอร์เน็ตเวิร์กที่บริษัทสำคัญใช้ในการดำเนินงาน ไม่ว่าจะเป็นบริษัทสาธารณูปโภค หรือเพื่อการขนส่งเรื่อยไปจนถึงบริษัทผู้ผลิตจึงเต็มไปด้วยข้อบกพร่องเช่นเดียวกัน คอมพิวเตอร์เน็ตเวิร์กเป็นสิ่งจำเป็นในการปฏิบัติงานของบริษัทหรือสำนักงานของรัฐต่างๆ ตัวอย่างที่ชัดเจนที่สุดของการพึ่งพาและความเปราะบางที่เกิดขึ้นจากการใช้คอมพิวเตอร์ในการควบคุมสิ่งต่างๆ ยังเกิดขึ้นในระบบที่ทุกอย่างต้องพึ่งพาและเชื่อมโยงอยู่ นั่นคือระบบโครงข่ายเพื่อการจ่ายกระแสไฟฟ้าหรือพาวเวอร์กริด การควบคุมโดยคอมพิวเตอร์สามารถทำให้หลายสิ่งหลายอย่างทำลายตัวมันเองได้คือเครื่องกำเนิดไฟฟ้า เครื่องกำเนิดไฟฟ้าสร้างกระแสไฟฟ้าจากการหมุนและจำนวนรอบของการหมุนต่อนาทีในการสร้างกระแสไฟฟ้าแสดงออกมาเป็นหน่วยวัดเรียกว่าเฮิร์ตซ์ ในสหรัฐอเมริกาและแคนาดา เครื่องกำเนิดไฟฟ้าในสถานีย่อยในโครงข่ายส่วนใหญ่หมุนอยู่ที่ 60 เมกะเฮิร์ตซ์ เมื่อเครื่องปั่นไฟฟ้าเริ่มทำงาน มันจะถูกเชื่อมต่อเข้ากับโครงข่ายที่ความเร็วอื่น หรือถ้าหากความเร็วในการปั่นเกิดการเปลี่ยนแปลงไปมากเกินไปในขณะที่มันกำลังเชื่อมต่ออยู่กับโครงข่ายกระแสไฟฟ้าจากเครื่องกำเนิดไฟฟ้าอื่นๆ ทั้งหมดที่อยู่ในโครงข่ายและกำลังปั่นอยู่ที่ 60 เมกะเฮิร์ตซ์ จะไหลลงมายังเครื่องกำเนิดตัวที่หมุนช้านั่น ก่อให้เกิดอาการผิดปกติ

เหตุผลสำคัญของสหรัฐอเมริกาต่อการใช้ยุทธศาสตร์การป้องกันทางไซเบอร์

1. สหรัฐอเมริกาต้องพึ่งพาระบบควบคุมผ่านไซเบอร์มากกว่าชาติที่อาจเป็นปฏิปักษ์ผู้บริโภคในประเทศอื่นๆ อย่างเช่นเกาหลีใต้หรือเอสโทเนียอาจเข้าถึงบอร์ดแบนด์ได้มากกว่าเรา อีกบางประเทศอย่างเช่นสหรัฐอาหรับเอมิเรตส์อาจมีสัดส่วนของจำนวนอุปกรณ์เชื่อมต่ออินเตอร์เน็ตเคลื่อนที่ต่อหัวประชากรมากกว่าเรา แต่มีน้อยประเทศมากที่ใช้เครือข่ายคอมพิวเตอร์มากมายและกว้างขวางไปจนถึงเรื่องของการควบคุมโครงข่ายสำหรับจ่ายกระแสไฟฟ้า ท่อลำเลียงน้ำมัน สายการบิน การเดินรถไฟ การกระจายสินค้าอุปโภคบริโภค, การธนาคารและการดำเนินการของบริษัทที่เป็นคู่สัญญากับกองทัพ

2. มีเพียงสองสามประเทศและแน่นอนว่าประเทศที่มีโอกาสจะเป็นปฏิปักษ์กับสหรัฐอเมริกาไม่ได้รวมอยู่ในกลุ่มนี้ที่มีระบบที่จำเป็นในระดับชาติ ซึ่งมีวิสาหกิจเอกชนเป็นเจ้าของและเป็นผู้ดำเนินกิจการเหมือนอย่างในสหรัฐอเมริกา

3. ไม่มีชาติอุตสาหกรรมสำคัญอื่นใดและชาติที่มีพัฒนาการด้านเทคโนโลยีสูงชาติใดที่มีเจ้าของและผู้ดำเนินการด้านสาธารณูปการซึ่งทรงอิทธิพลทางการเมืองมากเสียจนสามารถป้องกันไม่ให้รัฐบาลออกฎมาควบคุมการดำเนินงานของพวกเขาได้หรือทำให้กฎเกณฑ์ต่างๆ เหล่านั้นอ่อนแอเบาบางลงได้เท่ากับสหรัฐอเมริกา ระบบการเมืองอเมริกันที่เปิดโอกาสให้มีการล๊อบบี้ยิสต์ที่มีการสนับสนุนทางการเงินเป็นอย่างดีและเปิดให้มีการบริจาคเงินเพื่อการรณรงค์หาเสียงได้แทบจะเรียกได้ว่าไร้ขีดจำกัดนั้นได้ให้อำนาจใหญ่หลวงต่อกลุ่มอุตสาหกรรมเอกชน โดยเฉพาะอย่างยิ่งเมื่อพูดถึงเรื่องที่ต้องหาทางหลีกเลี่ยงการควบคุมที่มีความหมายจากรัฐบาลกลาง

4. กองทัพสหรัฐอเมริกาเปราะบางอย่างยิ่งต่อการโจมตีทางไซเบอร์ กองทัพสหรัฐอเมริการวมศูนย์อยู่ได้ด้วยเครือข่ายอินเตอร์เน็ตที่เรียกว่า เน็ตเซนทริกซึ่งจะเป็นเครื่องมือนำพาเข้าถึงฐานข้อมูลและข้อมูลข่าวสารไปยังหน่วยปฏิบัติการย่อยต่างๆแทบทุกชนิดขององค์กรปฏิบัติการทางทหารเท่าที่สามารถจะจินตนาการออกมาได้ความสามารถในการเข้าถึงระบบข้อมูลข่าวสารนำมาซึ่งการพึ่งพาระบบดังกล่าวด้วย ยกตัวอย่างเช่น เมื่อปลายปี 2009 ผู้ก่อการร้ายในอิรักใช้ซอฟแวร์ราคาแค่ 26ดอลล่าร์ในการลักลอบติดตามสัญญาณวิดีโอที่ถูกป้อนผ่านระบบเชื่อมต่อเพื่อการสื่อสารที่ไม่มีการเข้ารหัสให้กับพรีเดเตอร์ อากาศยานไร้นักบิน ในขณะที่เหตุการณ์ดังกล่าวไม่เป็นภัยคุมคามโดยตรงต่อทหารอเมริกันแต่การค้นพบดังกล่าวสร้างข้อกังขามากมายต่ออาวุธใหม่ที่เพนตากอน จะเกิดอะไรขึ้นถ้าสัญญาณที่ไม่ได้เข้ารหัสถูกรบกวนหรือแทรกแซง และทำให้อากาศยานไร้นักบินดังกล่าวบินกลับฐาน ปฏิบัติการของกองกำลังอเมริกันคงถูกล้มล้างด้วยเครื่องมือทรงคุณค่าราคาถูกที่หาซื้อได้ทั่วไป แต่สามารถเอาชนะผลผลิตที่ผ่านการวิจัยและพัฒนาคิดเป็นมูลค่าหลายล้านดอลล่าร์อย่างง่ายได้ กองกำลังสหรัฐอเมริกานอกจากจะพึ่งพาเครือข่ายคอมพิวเตอร์มากกว่าแล้วยังต้องพึ่งพาการสนับสนุนจากคู่สัญญาที่เป็นบริษัทเอกชนมากกว่ากองกำลังของชาติที่อาจเป็นศัตรูในสงครามไซเบอร์ใด แม้ว่าเครือข่ายกองทัพของสหรัฐอเมริกาอาจจะปลอดภัยและเชื่อถือได้แต่เครือข่ายของบริษัทคู่สัญญาเหล่านั้นซึ่งมักอาศัยเครือข่ายอินเตอร์เน็ตสาธารณะทั่วไป อาจไม่ปลอดภัยและเชื่อถือได้เหมือนของกองทัพ

การควบคุมการก่อการร้ายทางไซเบอร์สามารถกระทำได้โดย

1.การควบคุมอาวุธไซเบอร์นั้นไม่สามารถลดศักยภาพในการทำสงครามไซเบอร์ได้แตกต่างจากการลดหรือควบคุมอาวุธในรูปแบบอื่นๆ ทำได้เพียงแค่ห้ามการกระทำต่างๆ เท่านั้น ดังนั้น ชาติใดชาติหนึ่งอาจสามารถเปลี่ยนสถานะของตนจากความเป็นชาติที่ปฏิบัติตามพันธะทุกประการกลายเป็นชาติที่ล่วงละเมิดได้ภายในระยะเวลาเพียงไม่กี่วินาทีและโดยปราศจากการเตือนล่วงหน้า

2. นิยามของสงครามไซเบอร์แบบครอบคลุม อาทินิยามที่ครอบคลุมถึงการจารกรรมไม่สามารถตรวจสอบได้ และไม่จัดว่าเป็นผลประโยชน์ของสหรัฐอเมริกาในฐานะชาติชาติหนึ่ง ถึงกระนั้นก็ตามหน่วยงานด้านข่าวกรองของชาติต่างๆ รวมถึงรัฐบาลของแต่ละประเทศควรริเริ่มให้มีช่องทางเพื่อการหารือกันโดยตรง เพื่อให้กิจกรรมด้านการข่าวต่างๆ จะไม่เป็นกรณีบานปลายออกนอกเหนือการควบคุมหรือกลายเป็นเหตุแห่งความเข้าใจผิดว่าเป็นการแสดงถึงเจตนารมณ์การเป็นปฏิปักษ์

3.ความตกลงระหว่างประเทศซึ่งมีบทบัญญัติห้ามการกระทำที่แน่นอนบางอย่างไว้ อาทิ การโจมตีทางไซเบอร์ต่อโครงข่ายสาธารณูปโภคของพลเรือน ถือว่าเป็นประโยชน์สำหรับสหรัฐอเมริกา แต่ด้วยเหตุที่ว่าการโจมตีดังกล่าวยังคงสามารถเกิดขึ้นได้ต่อไป ความตกลงดังกล่าวจึงไม่ใช่หนทางที่จะทำลายความจำเป็นในการดำเนินขั้นตอนต่างๆ เพื่อป้องกันในอันที่จะคุ้มครองสาธารณูปโภคเหล่านั้น

4.การตรวจสอบการปฏิบัติตามพันธะในความตกลงเพื่อจำกัดสงครามไซเบอร์ที่สามารถไว้วางใจได้ในระดับสูงนั้นไม่สามารถเกิดขึ้นได้ สามารถตรวจสอบพบการล่วงละเมิดได้ แต่การชี้ตัวผู้ลงมืออาจเป็นเรื่องยากและอาจเป็นการกระทำที่ก่อให้เกิดความคลาดเคลื่อนในเจตนารมณ์ได้ อย่างไรก็ตาม ยังคงมีมาตรการหลายอย่างที่ยังผลให้เกิดธรรมเนียมปฏิบัติระหว่างประเทศเพื่อต่อต้านการโจมตีทางไซเบอร์ต่อพลเรือนได้ เช่น การจัดตั้งคณะผู้เชี่ยวชาญระหว่างประเทศ การกำหนดให้รัฐบาลของแต่ละชาติต้องรับผิดชอบในการป้องกันไม่ให้เกิดการล่วงละเมิดที่มีต้นกำเนิดอยู่ในอาณาเขตของชาตินั้นขึ้นและพันธะในอันที่จะให้ความช่วยเหลือเพื่อยับยั้งและสอบสวนการโจมตีทางไซเบอร์ขึ้น

5. การจำกัดการโจมตีด้วยสงครามไซเบอร์ต่อโครงข่ายสาธารณูปโภคพลเรือน อาจหมายความว่าสหรัฐอเมริกาและชาติรัฐอื่นๆ อาจต้องยุติการกระทำใดซึ่งอาจดำเนินการไปแล้วโดยการติดตั้งลอจิกบอมบ์และอาจรวมแทรปดอร์ ในโครงข่ายสาธารณูปโภคของประเทศอื่นๆ การลักลอบวางลอจิกบอมบ์และแทรปดอร์เอาไว้ทั่วโครงข่ายสาธารณูปโภคดังกล่าวนี้ ถึงแม้จะไม่เป็นที่สังเกตหรือพูดถึงกันมากมายในสื่อมวลชนและประชาชนทั่วไปก็ถือเป็นการยั่วยุที่อันตรายอย่างยิ่ง

สรุปได้ว่า ภัยคุกคามทางไซเบอร์ได้มีความรุนแรงมากขึ้นทุกวัน ผู้ก่อการร้ายอาจใช้ประโยชน์จากความก้าวหน้าทางไซเบอร์ เพื่อดำเนินการด้วยวิธีต่าง ๆ เช่น ก่อวินาศกรรม โดยมุ่งเป้าไปที่การทำลายที่มีผลกระทบในวงกว้าง เช่น การทำให้ระบบโครงสร้างกระแสไฟฟ้าขัดข้อง การโจมตีระบบโครงข่ายการสื่อสารหรือแม้กระทั่งการโจมตีระบบต่าง ๆ ที่ใช้ในการทหารก็อาจ

สามารถเกิดขึ้นได้เช่นกัน และบางประเทศสามารถพัฒนาศักยภาพในการทำสงครามไซเบอร์ เพื่อเป็นปฏิบัติการที่ควบคู่ไปกับการทำสงครามแบบปกติ

EU Cybersecurity Dashboard - BSA(n.d., p 11 – 16)วิวัฒนาการของไซเบอร์กลยุทธ์การรักษาความปลอดภัยของประเทศสมาชิกสหภาพยุโรป

ประเทศเอสโตเนีย (2008) ให้ความสำคัญต่อความจำเป็นของความมั่นคงทางโลกเทคโนโลยีสารสนเทศในทั่วไปและเน้นไปยังระบบการสื่อสารแนะนำมาตรการทั้งหมดของคุณลักษณะของพลเมืองและให้ความสนใจบนกฎข้อบังคับ การศึกษาและการทำงานร่วมกัน

ประเทศฟินแลนด์ (2008) รากฐานของยุทธศาสตร์คือ การมองไปยังความมั่นคงของไซเบอร์ขณะที่ประเด็นความมั่นคงของข้อมูลและขณะที่สิ่งที่ต้องทำความสำคัญที่เกี่ยวกับเศรษฐกิจนั่นคือการปิดสิ่งที่เกี่ยวข้องกันต่อการพัฒนาความสำเร็จของสังคมข่าวสาร

ประเทศสโลวาเกีย (2008) การสร้างความมั่นใจในความมั่นคงทางข่าวสารคือจุดองค์ประกอบสำคัญของโครงสร้างและการพัฒนาสังคม เพราะฉะนั้นวัตถุประสงค์ของยุทธศาสตร์คือการพัฒนาที่ครอบคลุมกรอบความคิดและวัตถุประสงค์เชิงกลยุทธ์ของยุทธศาสตร์การมุ่งเน้นการป้องกันปัญหาเช่นเดียวกันการเตรียมความพร้อมและการพัฒนาอย่างยั่งยืน

สาธารณรัฐเช็ก (2011) วัตถุประสงค์ที่สำคัญยุทธศาสตร์ความมั่นคงทางไซเบอร์ประกอบด้วย การปกป้อง ที่เกี่ยวกับการคุกคามต่อข้อมูลข่าวสารและระบบการสื่อสารและเทคโนโลยีเป็นการเปิดเผยและการบรรเทาผลกระทบที่อาจเกิดขึ้นในกรณีของการโจมตีกับไอซีทียุทธศาสตร์จุดเน้นส่วนใหญ่เน้นการเข้าถึงโดยปราศจากการขัดขวางการให้บริการความสมบูรณ์ของข้อมูลและความลับของโลกเทคโนโลยีสารสนเทศของสาธารณรัฐเช็กและมีการประสานงานกับกลยุทธ์อื่นๆ ที่เกี่ยวข้องและแนวความคิด

ประเทศฝรั่งเศส (2011) มุ่งเน้นไปที่ความเป็นไปได้ของระบบสารสนเทศเพื่อต่อต้านเหตุการณ์ในโลกไซเบอร์ที่อาจทำให้ขาดความพร้อม ความสมบูรณ์หรือความลับของข้อมูล ประเทศฝรั่งเศสเน้นวิธีการทางเทคนิคที่เกี่ยวข้องกับการรักษาความปลอดภัยของระบบสารสนเทศและการต่อสู้กับอาชญากรรมและการป้องกัน

ประเทศเยอรมนี (2011) ประเทศเยอรมนีมุ่งเน้นไปที่การป้องกันและการฟ้องร้องโจมตีไซเบอร์และเกี่ยวกับการป้องกันความล้มเหลวของไอที โดยเฉพาะอย่างยิ่งที่เกี่ยวกับวิกฤตโครงสร้างพื้นฐาน ยุทธศาสตร์พื้นฐานสำหรับการป้องกันของโครงสร้างข้อมูล มีการสำรวจระเบียบที่มีอยู่เพื่อชี้แจงและเรียกร้องอำนาจเพิ่มเติมที่จะต้องรักษาความปลอดภัยของระบบไอทีในประเทศเยอรมนี โดยหมายถึงการให้หน้าที่การรักษาความปลอดภัยขั้นพื้นฐานที่ได้รับการรับรองโดยรัฐและ SMEs ยังสนับสนุนโดยการตั้งค่าการทำงานใหม่

ประเทศลิทัวเนีย(2011) ประเทศลิทัวเนียมีวัตถุประสงค์เพื่อกำหนดเป้าหมายและการพยายามการพัฒนาของข้อมูลอิเล็กทรอนิกส์การบริการในไซเบอร์สเปซ การปกป้องเครือข่ายการสื่อสารอิเล็กทรอนิกส์ระบบข้อมูลและโครงสร้างพื้นฐานด้านข้อมูลที่สำคัญต่อเหตุการณ์ที่เกิดขึ้นและการโจมตีทางไซเบอร์การป้องกันข้อมูลส่วนบุคคลและความเป็นส่วนตัว ยุทธศาสตร์นั้นนอกจากจะกำหนดงานซึ่งเมื่อนำมาใช้จะช่วยในการรักษาความปลอดภัยรวมของไซเบอร์สเปซและหน่วยงานดำเนินการ

ประเทศลักเซมเบอร์ก (2011) การตระหนักถึงการแพร่หลายของไอซีที ยุทธศาสตร์นั่นคือสิ่งที่สำคัญเพื่อป้องกันไม่ให้เกิดผลกระทบต่อสุขภาพ ความปลอดภัยของประชาชนหรือเศรษฐกิจ นอกจากนี้ยังกล่าวถึงความสำคัญของไอซีทีสำหรับประชาชน สังคม และสำหรับการเติบโตทางเศรษฐกิจ ยุทธศาสตร์นี้คือพื้นฐานบน 5 เส้นทางการกระทำ สิ่งเหล่านี้สามารถสรุปสั้นๆ เป็น CIIP และการตอบสนองเหตุการณ์ที่เกิดขึ้น คือความทันสมัยของกรอบกฎหมาย ชาติและความร่วมมือระหว่างประเทศ การศึกษาการรับรู้และการส่งเสริมมาตรฐาน

ประเทศอังกฤษ (2011) วิธีการในอังกฤษมุ่งเน้นที่วัตถุประสงค์แห่งชาติที่เชื่อมโยงกับการพัฒนาความปลอดภัยทางไซเบอร์ การกระทำของอังกฤษส่วนหนึ่งของเศรษฐกิจที่สำคัญคือนวัตกรรมการลงทุนและคุณภาพในด้านไอซีทีและโดยสิ่งนี้จะสามารถใช้ประโยชน์อย่างเต็มที่ตามศักยภาพและผลประโยชน์ของไซเบอร์สเปซ โดยมีวัตถุประสงค์เพื่อแก้ไขปัญหาความเสี่ยงจากโลกไซเบอร์ เช่น การโจมตีจากอาชญากร ผู้ก่อการร้ายและรัฐต้องทำให้เป็นพื้นที่ปลอดภัยสำหรับประชาชนและธุรกิจ

ประเทศเนเธอร์แลนด์ (2011) มีจุดมุ่งหมายทางเทคโนโลยีสารสนเทศที่ปลอดภัยและเชื่อถือได้หวาดกลัวการข่มเหงและการโจมตีขนาดใหญ่ในเวลาเดียวกันรับรู้ความต้องการที่จะปกป้อง การเปิดกว้างและเสรีภาพทางอินเทอร์เน็ต รวมทั้งคำนิยามของการรักษาความปลอดภัยในโลกไซเบอร์ ความมั่นคงทางไซเบอร์คือการเป็นอิสระจากอันตรายสาเหตุของความเสียหายที่เกิดจากการทำลาย หรือทะเลาะกันของไอซีที และการรุกรานของไอซีทีอันตรายหรือความเสียหายจากการผิดกฎ รุกราน ทำลาย หรือการทะเลาะกันสามารถประกอบด้วยข้อจำกัดการใช้ประโยชน์และความน่าเชื่อถือของไอซีที การละเมิดของการรักษาความลับของข้อมูลที่เก็บไว้ในไอซีทีหรือความเสียหายต่อความสมบูรณ์นั้น

สรุปได้ว่า ภัยคุกคามทางไซเบอร์เป็นสถานการณ์ที่แต่ละประเทศมีการกำหนดยุทธศาสตร์หรือแนวทางในการป้องกันภัยจากการโจมตีทางไซเบอร์เพื่อไม่ให้เกิดผลกระทบหรือก่อให้เกิดความเสียหาย ซึ่งการโจมตีจากไซเบอร์ทางด้านโครงสร้างพื้นฐาน สาธารณูปโภค ข้อมูล

ส่วนบุคคล ระบบสารสนเทศของประเทศ สิ่งเหล่านี้จะส่งผลต่อความเสียหายต่อประเทศทั้งในด้านเศรษฐกิจและการมุ่งเป้าทางการเมืองด้วย

งานวิจัยที่เกี่ยวข้อง

1. การศึกษาวิจัยต่างประเทศ

งานวิจัยของ ดวล (Daud, 2011) ได้วิจัยเรื่อง “ไซเบอร์- ความขัดแย้ง” ในตะวันกลาง : เครื่องมือในการต้านทานการเมือง พบว่า การกำหนดในการศึกษาครั้งนี้ถึงการใช้อินเทอร์เน็ตต่อการแสดงความไม่พอใจทางการเมือง การวิพากษ์วิจารณ์การปกครอง องค์กรทางการปกครองขัดแย้งกับการกระทำ (เช่น การประท้วงและการชุมนุม) การเปิดเผยพฤติกรรมรัฐบาลและทางเลือกอุดมการณ์ทางการเมืองที่เหมาะสม BlogsheresYoutube Facebookและเว็บไซด์ความขัดแย้งทางการเมือง เป็นหลักพื้นฐานของ Cyberspaceเป็นเครื่องมือที่ใช้สำหรับคัดค้านทางการเมืองในตะวันออกกลาง ในการวิจัยครั้งนี้ 3 คำถามจะมีคำตอบ คำถามที่ 1 สิ่งที่ต้องการคือ โครงสร้าง และบริบทของไซเบอร์ – ความขัดแย้ง โดยการใช้วิธีการเชิงคุณภาพ สมมุติฐานที่สำคัญคือโครงสร้างและบริบทของไซเบอร์ – ความขัดแย้ง มีอิทธิพลอย่างมากโดยคุณภาพภายในประเทศในส่วนที่สองในการวิจัยโดยวิธีการเชิงปริมาณ คำถามคือ อะไรคือสาเหตุของคนตะวันออกกลางต่อการนัดหมายของไซเบอร์ – ความขัดแย้ง คณะผู้อภิปรายทางการเมือง – การวิเคราะห์การถดถอยของข้อมูลของ 39 ของรัฐในตะวันออกกลางและแอฟริกา (MENA) และตะวันออกกลางและแอฟริกาส่วนภูมิภาค (MENA) คือการทดสอบจาก 2002 – 2007 โดยผู้วิจัยแสดงให้เห็นขั้นตอนตลอดการวิจัยในระดับสูงของการเซ็นเซอร์ที่สำคัญเป็นกุญแจ ของสาเหตุปัจจัยของไซเบอร์ – ความขัดแย้งสุดท้ายการกดเซ็นเซอร์และอินเทอร์เน็ตเซ็นเซอร์ คือการเห็นความแตกต่างผู้วิจัยวิเคราะห์ผลกระทบของอินเทอร์เน็ตเซนเซอร์บนไซเบอร์ – ความขัดแย้ง

การค้นพบที่สำคัญครั้งแรกคือ ระดับของการเรียกร้องในประเทศการกำหนดเซ็นเซอร์ผลกระทบ ไซเบอร์ – ความขัดแย้ง อื่นๆ มุมมองของโครงสร้างกฎหมายของประเทศ นอกจากนี้ยังสามารถยับยั้งความขัดแย้งทางการเมือง

การค้นพบครั้งที่สอง คือ การค้นพบอัตราร้อยละของเยาวชนประเทศ ให้ความนิยมสร้างสรรค์ในระดับสูงของการทำข้อตกลงระดับสูงใน ไซเบอร์ – ความขัดแย้ง

การค้นพบครั้งที่สาม คือ การค้นพบของมหานครมีโอกาสในการเข้าใช้เทคโนโลยีไม่ใช่เพียงแค่การปลอมแปลงในการทำข้อตกลงระดับสูงในไซเบอร์ – ความขัดแย้งคือแรงบันดาลใจที่จะเป็นประชาธิปไตยในภูมิภาค

การค้นพบครั้งที่สี่ คือ การค้นพบการตระหนักของโครงสร้างและบริบทของตะวันออกกลางและแอฟริกา สังคมออนไลน์มีความสำคัญต่อการทำความเข้าใจของความคับข้องใจของผู้คน ในท้ายที่สุดจะนำไปสู่การปฏิวัติความสำคัญของความคับข้องใจของคนโดยขณะที่แสดงเนื้อหาออนไลน์คือ ละเมิดของอำนาจ การทรมานและ การคอร์รัปชั่น

งานวิจัยของคิม (Kim, 2010)ได้วิจัยเรื่อง ไซเบอร์ – เฝ้าระวัง: กรณีศึกษาในการปกครองและการพัฒนา พบว่า เป็นการพิจารณาทางประวัติศาสตร์ของการควบคุมดูแล การควบคุมดูแลอิเล็กทรอนิกส์และ ไซเบอร์ – เฝ้าระวังดูแลจากอาณานิคม เวลาในสหรัฐอเมริกาที่เกิดขึ้นในปัจจุบันการนำเสนอการควบคุมดูแลกฎหมาย เทคโนโลยีและนโยบายที่สมดุลระหว่างความมั่นคงของชาติและความเป็นส่วนตัว การพิจารณาเมื่อไม่นานมานี้การพัฒนา งานวิจัยประกอบด้วยกรณีศึกษาของ 3 เครื่องมือในการควบคุมดูแลไซเบอร์ :Carnivore, Lantern และNarus เรียกว่าเป็นหน้าที่ในการปฏิบัติการ การคำนวณและการค้นหาหน้าที่และการทำให้มีค่าน้อยลงของความสามารถทางร่างกายหรือจิตใจของเครื่องมือในส่วนท้าย เป็นการประเมินการเคลื่อนไหวความสมดุลระหว่างการบรรลุผลสำเร็จของความมั่นคงของชาติและสิ่งจำเป็นสาธารณะและความต้องการต่อการทำให้คงอยู่อย่างถูกต้องและสิ่งที่คาดหวังว่าจะเกิดขึ้นในอนาคตของความเป็นส่วนตัวของบุคคล

งานวิจัยของ กอร์เบรน (Gobran, 2015) ได้วิจัยเรื่องภัยคุกคามของผู้ก่อการร้ายทางไซเบอร์ พบว่า กลุ่มผู้ก่อการร้ายเริ่มต้นการปรับให้เข้ากันและยึดเอาความได้เปรียบของเครื่องมือทางไซเบอร์และความสามารถของเครื่องมือทางไซเบอร์ การคุกคามผู้ก่อการร้ายจะกระทำเพื่อการเติบโตของกลุ่มร่วมกัน ถึงแม้ว่าผู้ก่อการร้ายจะไม่มีฝีมือต่อการฆ่าคนอย่างรวดเร็วโดยตรงกับการใช้เครื่องมือทางไซเบอร์ การประทุษร้ายหรือการขัดขวางทางสังคม การโจมตีสามารถเป็นเหตุพอดีกับวัตถุประสงค์การดำเนินการ

งานวิจัยของ โอซีเรน (Ozeren, 2005) ได้วิจัยเรื่อง การตอบสนองของโลกต่อการก่อการร้ายทางไซเบอร์และอาชญากรรมทางไซเบอร์ พบว่า การก่อการร้ายทางไซเบอร์อาชญากรรมไซเบอร์นำเสนอทางเลือกใหม่สำหรับการบังคับใช้กฎหมายและการใช้นโยบายเพราะธรรมชาติของบริษัทข้ามชาติ ความจริงและการตอบสนองต่อภัยคุกคามเรียกร้อง การทำงานร่วมกันในระดับชาติเกี่ยวพันกับการมีส่วนร่วมของทั้งหมดที่เกี่ยวข้องในสังคมชุมชนระดับชาติ ไม่ว่าจะความอ่อนแอปรากฏออกมาจากจำนวนที่เพิ่มขึ้น ความมั่นใจบนเทคโนโลยีขาดมาตรการทางกฎหมายและขาดความร่วมมือที่ประเทศและระหว่างประเทศระดับอธิบายความจริงอุปสรรคที่มีประสิทธิภาพตอบสนองต่อภัยคุกคามในผลรวมการขาดความคิดเห็นของคนส่วนใหญ่ทั้งโลกในช่วงของการตอบสนองต่อการก่อการร้ายทางไซเบอร์และอาชญากรรมไซเบอร์คือปัญหาทั่วไป

งานวิจัยของ สโนเดน (Snowden, 2015) ได้วิจัยเรื่อง การรับรู้ของภัยคุกคามทางไซเบอร์และความร่วมมือภาคีต่อทฤษฎีการป้องกัน แรงจูงใจและกลุ่มคนรุ่นใหม่ พบว่า ภัยคุกคามทางไซเบอร์การกระทำที่พัฒนาขึ้นความเสียหายที่เกี่ยวกับส่วนบุคคล ธุรกิจและระดับชาติ ครั้งหนึ่งภัยคุกคามไซเบอร์ทำให้เป็นจริง มันกลับมาโจมตีไซเบอร์ ซึ่งคือการกระทำของการก่อการร้ายทางไซเบอร์ ชนิดของการรุกราน การขู่ต่อโลกเศรษฐกิจ ความมั่นคงแห่งชาติของรัฐบาลทั่วโลกและบุคคล เศรษฐกิจ ความเป็นอยู่ที่ดีของบุคคล ดังนั้น องค์การมีความต้องการพนักงานที่มีความตระหนักต่อการโจมตีทางไซเบอร์ที่สำคัญกว่านั้น องค์การต้องการบุคคลที่เข้าใจป้องกันตนเองจากการเกี่ยวข้องกับการโจมตี การวิจัยครั้งนี้อธิบายถึงความร่วมมือภาคีระหว่าง ทฤษฎีการป้องกันแรงจูงใจหลักฐานโดยความรุนแรงและความอ่อนแอที่ยาวนานกับกลุ่มคนรุ่นใหม่และความร่วมมือภาคีต่อการรับรู้ของพนักงานของพื้นฐานกับภัยคุกคามทางไซเบอร์ ดังนี้ 1.ทัศนคติของพนักงานไปทางที่มีต่อการดำเนินการรักษาความปลอดภัยที่ได้รับการยอมรับลงมติโดยองค์กร 2. ความรู้ของการดำเนินการของพนักงานเอาใจใส่ต่อความมั่นคงออนไลน์และความเต็มใจที่จะปรับตัวต่อการเปลี่ยนแปลงในเทคโนโลยีที่จำเป็น 3. การบังคับใช้ทางกฎหมายของพนักงานต่อไวรัสระเบียบการและการตระหนักรู้ของพวกเขาหรือไม่ใช่แฮกเกอร์ต่อการเข้าถึงไฟล์ข้อมูลของพวกเขา

จากการศึกษาจะเห็นได้ว่า การให้ความสำคัญต่อการใช้อินเทอร์เน็ตและเครื่องมือทางไซเบอร์มีความจำเป็นอย่างมาก อินเทอร์เน็ตเป็นเครื่องมือต่อการแสดงความไม่พอใจและการแสดงออกทางการเมืองได้ ไซเบอร์มีผลต่อการดำรงชีวิตของมนุษย์และเป็นช่องโหว่ให้เกิดอาชญากรรมและการก่อการร้ายได้หากประชาชนไม่มีการรับรู้และประเทศไม่มีการป้องกันที่ดีและมีประสิทธิภาพ

2. การศึกษาวิจัยในประเทศ

งานวิจัยของ กมลนวล ศิลาพันธ์ (2556) เรื่อง ความชัดเจนและความเหมาะสมในการกำหนดนิยามของการก่อการร้ายในประมวลกฎหมายอาญาของไทย พบว่า การบัญญัติความผิดฐานการก่อการร้ายขึ้นใหม่ควรบัญญัติให้เป็นการกระทำความผิดอาญาที่โหดรุนแรงอันมีผลกระทบต่อการดำเนินชีวิตอย่างปกติสุขของประชาชนโดยทั่วไป ซึ่งทำให้เกิดความรู้สึกหวาดกลัวและไม่ปลอดภัยของประชาชนอันเป็นวัตถุประสงค์หลักของผู้ก่อการร้าย การนิยามความหมายของการก่อการร้ายให้เป็นกลางเป็นที่ยอมรับทั่วไปอย่างเป็นสากลยังไม่สามารถทำได้ เพราะแต่ละประเทศยังยอมรับไม่ตรงกันอีกทั้งคำนิยามของการก่อการร้าย ระหว่างประเทศยังไม่ยุติบางประเทศเห็นว่าการต่อสู้เพื่ออิสรภาพไม่เป็นการก่อการร้ายระหว่างประเทศ ในขณะที่บางประเทศกลับเห็นว่าการกระทำดังกล่าวเป็นการก่อการร้ายระหว่างประเทศ ลักษณะของการก่อการร้ายอาจพิจารณาได้จากปัจจัยเหล่านี้คือ 1. เป้าหมายในการกระทำจะมุ่งต่อประชาชนผู้บริสุทธิ์ มิได้พุ่งเป้าไปยังประชาชน

พลเมือง 2. วัตถุประสงค์เพื่อทำให้เกิดความกลัวอันเป็นลักษณะของการขู่เข็ญต่อประชาชน 3. มูลเหตุจูงใจของการก่อการร้าย โดยมากมักมีเหตุจูงใจมาจากความต้องการบรรลุผลทางการเมือง อุดมการณ์หรือศาสนาไม่ใช่ลักษณะต้องการผลในทางส่วนตัว โดยต้องการให้สาธารณะชนเกิดความหวาดกลัวหรืออาจเป็นการขู่รัฐบาลให้กระทำการอย่างใดอย่างหนึ่ง การก่อการร้ายมักมีการรวมกลุ่มกันลักษณะคล้ายองค์กรอาชญากรรมแต่ต่างกันตรงที่ผู้ก่อการร้ายไม่ได้มีวัตถุประสงค์ที่จะกระทำความผิดเป็นอาชีพอย่างต่อเนื่อง

วิจัยของดุสิต น้ำฝน (2549) เรื่องการจัดตั้งองค์การชำนาญพิเศษเพื่อดำเนินการยุทธศาสตร์ต่อต้านการก่อการร้าย ผลการศึกษาพบว่า 1.เมื่อเกิดเหตุการณ์ก่อการร้ายภายในประเทศในลักษณะที่มีความรุนแรงรวมถึงการก่อการร้ายรูปแบบใหม่ในอนาคต องค์การต่อต้านการก่อการร้ายจะไม่สามารถจัดการปัญหาได้อย่างมีประสิทธิภาพ 2. ปัญหาของโครงสร้างขององค์กรคือ องค์การมีสายการบังคับบัญชาและปฏิบัติตามคำสั่งองค์การสูงสุดที่เหนือขึ้นไป ต้องได้รับการอนุมัติในการเข้าจัดการกับปัญหาทุกครั้ง และองค์กรมีโครงสร้างหลวม บริหารงานยาก ขาดเอกภาพในการแก้ปัญหา อำนาจในการตัดสินใจและสั่งการด้านนโยบายขึ้นกับรัฐบาลไม่อิสระ

นอกจากนี้ การปฏิบัติการขององค์การมีความเสี่ยงสูงในการตัดสินใจแก้ไขปัญหาเพราะเกี่ยวข้องกับความรุนแรง หากตัดสินใจพลาด สั่งการโจมตีหรือปะทะด้วยกำลังอันตรายต่อตัวประกัน ประชาชน เป็นสิ่งที่องค์กรต้องรับผิดชอบ และไม่มีการประกันความเสี่ยงเหมือนกันกิจกรรมขององค์การอื่นๆ ทั้งนี้เครื่องมือเครื่องใช้ในการต่อต้านการก่อการร้ายที่มีประสิทธิภาพสูงเป็นทรัพยากรภายนอกองค์การทั้งหมด

ปัญหาประการต่อมาคือ องค์การยังไม่มีกฎหมายเฉพาะรองรับการใช้อำนาจหน้าที่ในการจัดการความรุนแรงเฉพาะทาง (ด้านการก่อการร้าย) ในกรณีเกิดสถานการณ์เลวร้ายที่สุด (Worst case) คือ เกิดการก่อการร้ายที่มีความรุนแรง และเกิดพร้อมกันหลายจุดหรือหลายเป้าหมาย องค์การจะไม่สามารถจัดการที่เกิดขึ้นพร้อมกันได้เพราะข้อจำกัดขององค์การหลายด้าน โครงสร้าง แนวทางควรจัดหน่วยให้เป็นองค์การเบ็ดเสร็จระดับกระทรวงหรือทบวง ปกป้องมาตุภูมิที่มีการจัดการหน่วยขึ้นตรงต่อผู้บริหารสูงสุดมีกองกำลังต่อทหารในบังคับของตนเองในระดับที่สามารถจัดการปัญหากับความรุนแรงได้เบื้องต้น และปานกลาง มีทรัพยากร เครื่องมือ เครื่องใช้ งบประมาณ บุคลากร หน่วยวิจัย หน่วยการข่าวและหน่วยชำนาญเฉพาะด้าน

งานวิจัยของ จันทิมา เภาเจริญ (2550) เรื่องการก่อการร้ายสากลในเอเชียตะวันออกเฉียงใต้ พบว่า แม้ประเทศไทยจะไม่ได้เกี่ยวข้องโดยตรงกับปัญหาและความขัดแย้งซึ่งเป็นสาเหตุของการก่อการร้ายสากล แต่กระนั้นการได้รับผลกระทบเป็นสิ่งที่ไม่อาจหลีกเลี่ยงได้ เพราะประเทศไทยมีความสัมพันธ์อันดีกับประเทศที่เป็นเป้าหมายของการก่อการร้าย เช่น สหรัฐอเมริกา อิสราเอล

ฯลฯ เนื่องจากว่าสถานทูต สถานกงสุล บริษัทการค้าและบริบทสายการบินต่างๆ ตั้งอยู่ในประเทศไทย ดังนั้นสถานที่เหล่านี้จึงเป็นเขตปริมณฑลในการปฏิบัติการก่อการร้ายแต่ยังไม่ใช่เป้าหมายของตัวของมันเอง ประเทศไทยจึงต้องร่วมมือกันไม่ว่าจะด้วยวิธีการกับประเทศต่างๆ ในการต่อต้านการก่อการร้าย เพราะการก่อการร้ายเป็นภัยคุกคามของชุมชนระหว่างประเทศ

วิจัยของ วรนุช พุ่มเรือง (2554) เรื่องบทบาทของปากีสถานในการต่อต้านการก่อการร้ายในสมัยประธานาธิบดีเปอร์เวซมุชัวร์ฟ (ค.ศ. 1999 – 2008) พบว่า การแสดงบทบาทการต่อต้านการก่อการร้าย เป็นการเน้นเข้าหาความร่วมมือกับประเทศภายนอกต่างๆ ทั้งในรูปแบบพหุภาคีและทวีภาคี กับมหาอำนาจและประเทศเพื่อนบ้านอย่างเป็นรูปธรรม คือมาตรการทางการทูต มาตรการทางกฎหมาย และมาตรการทางทหาร เช่นการยุติความสัมพันธ์กับกลุ่มตอลีบาน การร่วมมือกับนานาประเทศภายใต้มติสหประชาชาติการแก้ไขพระราชบัญญัติการต่อต้านการก่อการร้ายถึง 4 ฉบับ การใช้ปฏิบัติการทหารภายในประเทศ เพื่อกำจัดกลุ่มก่อการร้ายที่แทรกซึมเข้าตามแนวชายแดนปากีสถาน – อัฟกานิสถาน และพบว่า การแสดงบทบาทดังกล่าวเป็นผลมาจากอิทธิพลของปัจจัยภายนอกอย่าง มหาอำนาจสหรัฐอเมริกา เป็นสำคัญ ที่นำประชาคมโลกเข้าสู่ยุคที่เรียกว่าสงครามต่อต้านการก่อการร้าย การใช้มาตรการกดดันและเสนอแรงจูงใจต่อปากีสถานอย่างมีอาจปฏิเสธได้ เนื่องจากไม่สามารถต่อกรกับสหรัฐอเมริกาได้ในทุกด้าน โดยเฉพาะทางทหาร อีกทั้งผลประโยชน์ที่ได้รับจะช่วยสร้างความกินดีอยู่ดีให้กับประชากรของประเทศและเสริมสร้างเกียรติภูมิให้กับประเทศ จึงนำมาสู่การร่วมมือการต่อต้านการก่อการร้ายกับสหรัฐอเมริกาและนานาประเทศในที่สุด

วิจัยของอัศวิน ศุกระศร (2549) เรื่องความผิดฐานการก่อการร้ายในประเทศไทย: มาตรการป้องกันและปราบปราม พบว่า จากการศึกษาถึงแนวคิดและลักษณะการกระทำความผิดเกี่ยวกับการก่อการร้าย มีความแตกต่างจากลักษณะการกระทำความผิดประเภทอื่น ๆ แม้ว่าจะมีการใช้รูปแบบในการกระทำความผิดเหมือนกันก็ตาม แต่เมื่อพิจารณาจากองค์ประกอบอื่นแล้ว ก็ทำให้พิจารณาได้ว่าเป็นการกระทำความผิดในประเภทใด ความผิดอาญาสามัญ (Common crimes) เช่น การฆ่าผู้อื่น การวางเพลิงเผาทรัพย์ เป็นการกระทำความผิดที่ผู้กระทำมีมูลเหตุจูงใจหรือวัตถุประสงค์เป็นการส่วนตัวหรือเป็นประโยชน์ส่วนตัว เป็นการกระทำอันมีลักษณะเฉพาะเจาะจง ซึ่งเกิดจากเหตุใด ๆ ก็ได้ เช่น ความโกรธแค้น การอาฆาตพยาบาท ในขณะที่ผู้กระทำความผิดเกี่ยวกับการก่อการร้ายจะมีมูลเหตุจูงใจทางการเมืองหรือศาสนา อุดมการณ์ความเชื่อของตน ความผิดอาญา (Political crimes) เช่นการฆ่าผู้อื่น (ผู้นำทางการเมือง) แม้ว่าจะมีมูลเหตุจูงใจทางการเมืองหรืออุดมการณ์ทางการเมือง แต่เป็นความมุ่งหมายเพื่อต้องการยึดอำนาจรัฐ การเปลี่ยนแปลงรัฐบาลเพื่อให้การกระทำใด ๆ หรือเพื่อให้ประชาชนเกิดความหวาดกลัว ความตื่น

ตกใจ ความสับสนอลหม่าน ดังนั้นจึงมุ่งเป้าไปยังประชาชนผู้บริสุทธิ์ (มิใช่ผู้นำทางการเมืองหรือรัฐบาล) ความผิดองค์กรอาชญากรรมแม้จะมีการฆ่าผู้อื่นแต่เป็นการกระทำเพื่อแสวงหารายได้จากการกระทำความผิดหรือมีความมุ่งหมายเพื่อกระทำการอันมิชอบด้วยกฎหมาย โดยไม่มีเหตุจูงใจจากทางการเมืองซึ่งมูลเหตุจูงใจในการกระทำความผิดนี้เป็นสาระสำคัญของการพิจารณา เพราะความผิดบางประเภทนั้น มูลเหตุจูงใจอาจเป็นองค์ประกอบของความรับผิด (เป็นเจตนาพิเศษ) และทำให้พิจารณาได้ว่าเป็นความผิดประเภทใด

จากการทบทวนวรรณกรรมที่เกี่ยวข้องจะเห็นได้ว่า การก่อการร้ายเป็นการกระทำที่นำมาซึ่งความเสียหายและความรุนแรง ส่งผลต่อความมั่นคงของโลก สาเหตุของการก่อการร้ายมาจากเหตุจูงใจทางการเมือง ทางศาสนาหรืออุดมการณ์ แตกต่างการกระทำในทางอาชญากรรมที่มุ่งผลประโยชน์ทางส่วนตัว การแสดงบทบาทการต่อต้านการก่อการร้ายมาจากอิทธิพลของประเทศมหาอำนาจสหรัฐอเมริกา ที่นำประชาคมโลกเข้าสู่ยุคที่เป็นสงครามต่อต้านการก่อการร้าย ภัยคุกคามของผู้ก่อการร้ายทางไซเบอร์จะยึดเอาความได้เปรียบของเครื่องมือทางไซเบอร์และความสามารถของเครื่องมือทางไซเบอร์นำมาวางแผนและโจมตีทางไซเบอร์ และใช้เครื่องมือในการติดต่อสื่อสารของยูทูบ เฟสบุ๊กและเว็บไซต์ทางการเมืองนำมาสู่การสร้างหรือชักจูงการก่อการร้ายทางไซเบอร์ได้ ประเทศไทยแม้ไม่ได้เกี่ยวข้องกับการก่อการร้ายโดยตรงแต่ก็มีความมีความสัมพันธ์กับนานาประเทศ ทำให้ไม่สามารถหลีกเลี่ยงภัยของการคุกคามทางไซเบอร์ได้

บทที่3
วิธีดำเนินการวิจัย

การวิจัยในครั้งนี้เป็นการศึกษายุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย โดยมีวัตถุประสงค์การวิจัย 1. เพื่อศึกษาความก้าวหน้าทางไซเบอร์ที่มีการนำมาใช้เป็นเครื่องมือทางยุทธศาสตร์ในการก่อการร้ายในประเทศไทย2.เพื่อศึกษาลักษณะการก่อการร้ายโดยใช้ไซเบอร์มาเป็นเครื่องมือทางยุทธศาสตร์ในการก่อการร้ายของประเทศไทยและวิเคราะห์ประเมินการก่อการร้ายทางไซเบอร์ในประเทศไทยโดยใช้การวิเคราะห์จุดแข็ง จุดอ่อน โอกาสและอุปสรรค วิธีการวิเคราะห์สถานการณ์และองค์กรแห่งการเรียนรู้ 3. เพื่อพัฒนายุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทยมีขั้นตอนและรายละเอียดที่ดำเนินการตามวัตถุประสงค์การวิจัย 5 ขั้นตอนดังนี้

รูปแบบการวิจัย

การวิจัยเรื่อง ยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทยใช้รูปแบบการวิจัยแบบผสมผสาน (Mixed methods) (Creswell, 2007) โดยใช้การวิจัยแบบรับรองภายใน (Embedded Design) (Creswell, 2013) โดยการวิจัยเชิงคุณภาพเป็นหลักและวิจัยเชิงปริมาณมาสนับสนุนการวิจัยให้มีข้อมูลที่น่าเชื่อถือ เพื่อให้ได้รายละเอียดของข้อมูลต่าง ๆ อย่างลึกซึ้งและสามารถตอบคำถามการวิจัยได้

ขั้นตอนที่ 1 การศึกษาข้อมูลจากเอกสาร

ศึกษาความก้าวหน้าทางไซเบอร์ การก่อการร้าย การก่อการร้ายทางไซเบอร์และรวบรวมข้อมูลในเรื่องยุทธศาสตร์ นโยบายและการดำเนินการตามนโยบาย บทบาทของประเทศไทยต่อการดำเนินการต่อต้านการก่อการร้ายทางไซเบอร์ รวมทั้งปัญหาอันเกิดจากการก่อการร้ายในปัจจุบันและการกำหนดยุทธศาสตร์ที่เหมาะสมต่อความมั่นคงทางไซเบอร์และงานวิจัยที่เกี่ยวข้อง

ขั้นตอนที่ 2 ดำเนินการวิจัย (การวิจัยเชิงคุณภาพ)

การวิจัยเชิงคุณภาพด้วยการใช้เทคนิคเดลฟาย5 ขั้นตอนดังนี้

1.กำหนดและเตรียมตัวกลุ่มผู้เชี่ยวชาญ

การกำหนดกลุ่มผู้เชี่ยวชาญโดยใช้วิธีเลือกแบบเจาะจง (Purposive sampling) คัดเลือกผู้ให้ข้อมูลโดยใช้การสุ่มตัวอย่างแบบลูกโซ่ หรือการบอกต่อหรือสโนว์บอล (Snoeball Technique Sampling) ซึ่งเป็นผู้ที่มีความรู้ความเข้าใจและสามารถให้ข้อมูลได้ลึกซึ่งที่สุด กลุ่มของผู้เชี่ยวชาญที่ถูกเลือกมาให้ข้อมูลสำหรับการศึกษาในเรื่องยุทธศาสตร์ นโยบายและการดำเนินการตามนโยบาย รวมทั้งบทบาทของประเทศไทยต่อการดำเนินการต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศและระดับอาเซียน รวมทั้งปัญหาอันเกิดจากการก่อการร้ายในปัจจุบัน Lincoln and Guba (1985) กล่าวว่าการเลือกตัวอย่างที่ครอบคลุมความหลากหลายในประชากรให้ได้มากที่สุดนั้น เป็นวิธีการเลือกตัวอย่างที่ดีที่สุด เนื่องจากลักษณะที่เกิดร่วมกันจากความหลากหลายของกลุ่มตัวอย่างเป็นสิ่งที่น่าสนใจและมีคุณค่าต่อการวิจัยเป็นอย่างยิ่ง ซึ่งสามารถบ่งชี้รูปแบบที่สามารถเกิดขึ้นได้เหมือนกันจากตัวอย่างซึ่งมีลักษณะต่างกันในกลุ่มที่ศึกษาได้ (วรรณี แกมเกตุ, 2551) มีจำนวนทั้งสิ้น 10 คน โดยแบ่งออกเป็น2 กลุ่มดังนี้

กลุ่มที่หนึ่ง ได้แก่ ผู้ที่มีบทบาทหรือส่วนเกี่ยวข้องกับการดำเนินการหรือการพัฒนาทางไซเบอร์และใช้การพัฒนาทางไซเบอร์มาเป็นเครื่องมือในการดำเนินการพัฒนาในประเทศไทย จำนวน 4 คน

กลุ่มที่สองได้แก่ผู้ที่มีความรู้ความเชี่ยวชาญในส่วนของการกำหนดยุทธศาสตร์ทางเทคโนโลยีในส่วนของภาครัฐ จำนวน 6 คน ประกอบด้วยกระทรวงเทคโนโลยีและสารสนเทศ จำนวน 2 ท่าน หน่วยงานความมั่นคงแห่งชาติ 1 ท่าน สำนักงานตำรวจแห่งชาติ 2ท่าน และกองทัพไทย 1 ท่าน

2. สัมภาษณ์กลุ่มผู้เชี่ยวชาญ

ผู้วิจัยได้ดำเนินการเลือกผู้ให้ข้อมูลในการสัมภาษณ์เชิงลึก (In – depth interview) เพื่อทำการรวบรวมข้อมูลที่เป็นประโยชน์ต่อการวิจัย การสัมภาษณ์จะมีลักษณะเฉพาะคือเป็นการสัมภาษณ์แบบรายบุคคล เพื่อหลีกเลี่ยงการเผชิญหน้ากันระหว่างผู้เชี่ยวชาญแต่ละท่าน ทำให้ผู้เชี่ยวชาญแต่ละท่านปราศจากการชี้นำจากกลุ่มและไม่ตกอยู่ในอิทธิพลทางความคิดเห็นของผู้เชี่ยวชาญท่านอื่นผู้วิจัยดำเนินการการสัมภาษณ์แบบกึ่งมีโครงสร้างคือ มีการเตรียมประเด็นในการสัมภาษณ์ไว้ล่วงหน้า เพื่อป้องกันไม่ให้หลงลืมประเด็นสำคัญต่างๆ ในระหว่างการสัมภาษณ์ เนื้อหาของการสัมภาษณ์จะครอบคลุมถึงประเด็นที่เกี่ยวข้องกับยุทธศาสตร์ นโยบาย และการดำเนินงานตามนโยบายของประเทศไทยและเป็นการสัมภาษณ์แบบเปิดไม่ชี้นำ เพื่อเปิดโอกาสให้ผู้เชี่ยวชาญได้แสดงความคิดเห็นในประเด็นต่างๆ ได้อย่างอิสระและเป็นการสัมภาษณ์เชิงลึกเพื่อช่วยให้ได้รายละเอียดแบบเจาะลึกในประเด็นสำคัญและสามารถดัดแปลงแก้ไขคำถามที่ใช้ในการสัมภาษณ์ได้ถ้าหากพบว่าผู้เชี่ยวชาญยังไม่เข้าใจคำถามอย่างถูกต้อง

กลุ่มของผู้เชี่ยวชาญประกอบด้วย

2.1 คุณกำพล ศรธนะรัตน์ ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์แห่งประเทศไทย (ก.ล.ต.)

2.2 คุณสันต์ทศน์ สุริยันต์ ผู้อำนวยการสำนักความมั่นคงปลอดภัย สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์กรมหาชน) สพธอ.

2.3 ดร.กิตติ โฆษะวิสุทธ์ ผู้จัดการฝ่ายความปลอดภัยเทคโนโลยี ธนาคารกรุงเทพจำกัด (มหาชน)

2.4 คุณปริญญา หอมอเนก ประธานบริษัท ACIS Professional Center Co., Ltd.(ACIS)

2.5 คุณณัฐ พยงค์ศรี นักวิชาการคอมพิวเตอร์ชำนาญการ พนักงานเจ้าหน้าที่ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ.2550 กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (ไอซีที)

2.6 ดร.พันธ์ศักดิ์ ศิริรัชตพงษ์ ผู้อำนวยการสำนักเลขานุการคณะกรรมการเตรียมการด้านดิจิทัลเพื่อเศรษฐกิจและสังคมกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (ไอซีที)

2.7 คุณลือจิต ถิ่นพังงา นักวิเคราะห์นโยบายและแผน ระดับชำนาญการ สภาความมั่นคงแห่งชาติ

2.8 พ.ต.อ. ญาณพล ยั่งยืน อดีตรองอธิบดีกรมสอบสวนคดีพิเศษ

2.9 ศ.พ.ต.อ.หญิง ดร. พัชรา สินลอยมา คณบดีคณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ

2.10 พันเอกชาติชาย ชัยเกษม ผู้อำนวยการกองสงครามเครือข่าย สำนักปฏิบัติการ กรมยุทธการ กองบัญชาการกองทัพไทย

3.การเก็บรวบรวมข้อมูล

ผู้วิจัยดำเนินการเก็บรวบรวมข้อมูลตามลำดับดังนี้

1. ผู้วิจัยส่งหนังสือจากคณะรัฐศาสตร์และนิติศาสตร์ มหาวิทยาลัยบูรพาถึงกลุ่มผู้เชี่ยวชาญจำนวน 10 คน เพื่อขออนุญาตให้ดำเนินการเก็บรวบรวมข้อมูลและผู้วิจัยนัดหมายผู้ให้สัมภาษณ์เกี่ยวกับ วัน เวลาและสถานที่ในการสัมภาษณ์

2. ผู้วิจัยส่งแบบสอบถามการสัมภาษณ์ให้ผู้สัมภาษณ์ด้วยตนเอง เพื่อให้ผู้ให้ข้อมูลการสัมภาษณ์ทราบแนวคำถามและเตรียมการตอบ

3. ผู้วิจัยดำเนินการสัมภาษณ์กลุ่มผู้เชี่ยวชาญ ตั้งแต่วันที่30 พฤษภาคม 2558ถึง วันที่ 20 ตุลาคม 2558

4. รวบรวมข้อมูลจากผู้ให้สัมภาษณ์ครบทั้ง 10คน

เครื่องมือที่ใช้ในการวิจัย

การสัมภาษณ์เชิงลึก (In – depth interview) มีเครื่องมือ 2 ลักษณะดังนี้

1. เครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูลเพื่อให้มีประสิทธิภาพและสมบูรณ์ยิ่งขึ้นคือ สมุดบันทึกการสัมภาษณ์ เครื่องบันทึกเสียง การเสวนาและประเด็นสัมภาษณ์

2. แบบสัมภาษณ์เชิงลึก (In – depth interview) โดยผู้วิจัยใช้แนวคำถามในการสัมภาษณ์ โดยมีวิธีการสร้างเครื่องมือ ดังต่อไปนี้

2.1 การเขียนร่างแนวคำถามในการสัมภาษณ์เชิงลึก เกี่ยวกับ ความก้าวหน้าทางไซเบอร์ ลักษณะการก่อการร้ายทางไซเบอร์ และการนำไซเบอร์มาเป็นเครื่องมือทางยุทธศาสตร์ในการก่อการร้าย

2.2 พัฒนาเครื่องมือโดยวิธีการยกร่างแบบสัมภาษณ์ และนำแบบสัมภาษณ์เสนอต่ออาจารย์ที่ปรึกษางานวิจัยเพื่อพิจารณาความเหมาะสมและปรับปรุงแก้ไขตามข้อเสนอแนะจากอาจารย์ที่ปรึกษาวิทยานิพนธ์

2.3 นำแนวคำถามในการสัมภาษณ์ไปให้ผู้เชี่ยวชาญตรวจสอบความเข้าใจ ความถูกต้องและความเหมาะสมของเครื่องมือก่อนนำไปใช้สัมภาษณ์ผู้ให้ข้อมูลที่สำคัญในการวิจัย ทั้งนี้เพื่อให้มั่นใจได้ว่าการวิจัยได้ดำเนินการด้วยวิธีที่ถูกต้องและเหมาะสม

2.4 ผู้วิจัยได้ข้อมูลจากการสัมภาษณ์ ในการวิเคราะห์ข้อมูลผู้วิจัยใช้การทำรหัสหรือดัชนีข้อมูล (data coding/indexing) เป็นการกำหนดถ้อยคำ วลี ข้อความสั้น ๆ เพื่อใช้จำแนกแยกแยะข้อมูลออกเป็นส่วนหรือหมวดหมู่ ภายหลังจากการเก็บข้อมูลเสร็จเรียบร้อยแล้ว (Coffey & Atkinson, 1996; Neuman, 2000) และตรวจสอบความถูกต้องและแก้ไขอีกครั้งหนึ่งก่อนที่จะได้มีการนำข้อมูลและความเห็นดังกล่าวไปใช้ในการสร้างไปใช้ในการสร้างเครื่องมือสำหรับทำเทคนิคเดลฟาย

3.แบบสอบถามปลายปิดให้กลุ่มผู้เชี่ยวชาญ (ทำเทคนิคเดลฟาย)

ผู้วิจัยได้ข้อมูลจากการสัมภาษณ์ครบทั้ง10 คน ได้นำข้อมูลทั้งหมดมาวิเคราะห์และสังเคราะห์เพื่อพัฒนาเครื่องมือสำหรับทำเทคนิคเดลฟายคือการสร้างแบบสอบถามปลายปิดที่เป็นแบบสอบถามแบบมาตราส่วนประเมินค่า (Rating scale) เพื่อให้ผู้เชี่ยวชาญแต่ละท่านแสดงความคิดเห็นในลักษณะของการจัดระดับความสำคัญในคำถามแต่ละข้อ พร้อมทั้งระบุเหตุผลที่เห็นด้วย

หรือไม่เห็นด้วยและคำแนะนำเพิ่มเติมในคำถามแต่ละข้อ ผู้วิจัยได้ดำเนินการขออีเมล์และส่งแบบสอบถามทางอีเมล์ของผู้เชี่ยวชาญทั้ง 10 ท่าน และได้ผลตอบกลับมาทั้งหมด 8 ท่าน

4.การเขียนสรุปผลจากเทคนิคเดลฟาย

การเขียนการสรุปผลที่ได้จากการศึกษานั้น จะแบ่งเนื้อหาออกเป็นประเด็นทั้งหมด 7 ประเด็นประกอบด้วย

4.1การก่อการร้าย (Terrorism) การก่อการร้ายทางไซเบอร์และปัจจัยที่เกี่ยวข้องกับการก่อการร้ายทางไซเบอร์

4.2 แรงจูงใจในการก่อการร้ายและการแสวงหาโอกาสในการก่อการร้ายทางไซเบอร์

4.3 ปัญหาในการจัดการกับการก่อการร้าย

4.4 ความก้าวหน้าทางไซเบอร์ (Cyber)

4.5 การแสวงหาโอกาสในการก่อการร้ายทางไซเบอร์

4.6 การนำไซเบอร์มาเป็นเครื่องมือในการก่อการร้าย

4.7 การก่อการร้ายทางไซเบอร์ (Cyber) และการต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย

5. การวิเคราะห์ข้อมูล

ดำเนินการวิเคราะห์ข้อมูลโดยการวิเคราะห์เนื้อหา (Content analysis) ดังนี้

1. ให้การวิเคราะห์แบบอุปนัย โดยผู้วิจัยจะนำข้อมูลที่ได้มาจดบันทึกเป็นระบบโดยจำแนกว่าใคร พูดอะไร และนำมาหาความหมาย แยกแยะองค์ประกอบที่เชื่อมโยง หาความสัมพันธ์ของข้อมูลเพื่ออธิบายความสัมพันธ์ของข้อมูลต่างๆ ที่รวบรวมจากการสัมภาษณ์ โดยผู้วิจัยจะเก็บรวบรวมข้อมูลไปพร้อม ๆ กับการวิเคราะห์ทุกครั้ง เพื่อให้ได้ข้อมูลที่ถูกต้องครบถ้วน สมบูรณ์ ตามประเด็นที่ต้องการ

2. ใช้การวิเคราะห์ข้อมูลโดยการจำแนกชนิดของข้อมูล (Typological analysis) ซึ่งการจำแนกชนิดของข้อมูล จะยึดกรอบในการจำแนกตามประเด็นที่เกี่ยวข้องกับ ความก้าวหน้าทางไซเบอร์ ลักษณะของการก่อการร้าย การก่อการร้ายทางไซเบอร์ การนำไซเบอร์มาเป็นเครื่องมือทางยุทธศาสตร์ในการก่อการร้าย การต่อต้านการก่อการร้ายทางไซเบอร์ของประเทศไทย

การวิเคราะห์ข้อมูลเพื่อให้ได้ยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย ใช้การวิเคราะห์จุดแข็ง จุดอ่อน โอกาส และภาวะคุกคาม (SWOT Analysis) จากการ

สัมภาษณ์เชิงลึกผู้เชี่ยวชาญเพื่อประกอบในการตัดสินใจกำหนดยุทธศาสตร์และสังเคราะห์ออกมาเป็นยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย

ขั้นตอนนี้ใช้เทคนิคการวิเคราะห์จุดแข็ง จุดอ่อน โอกาสและอุปสรรค นำข้อมูลที่ได้จากการวิเคราะห์ SWOT มาใส่ตาราง SWOT Matrix มีดังนี้

SWOT Matrix	จุดแข็ง (S) 1…… 2…… 3……	จุดอ่อน (W) 1…… 2…… 3……
โอกาส (O) 1…… 2…… 3……	(SO) 1…… 2…… 3……	(WO) 1…… 2…… 3……
อุปสรรค (T) 1…… 2…… 3……	(ST) 1…… 2…… 3……	(WT) 1…… 2…… 3……

ภาพที่ 7 ตารางSWOT Matrix

เพื่อให้ได้ตารางยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย จึงใช้เทคนิคการวิเคราะห์ตารางSWOT Matrixโดย

1. จับคู่จุดแข็งหลัก – โอกาสหลัก (SO) กำหนดยุทธศาสตร์ที่เหมาะสม โดยยุทธศาสตร์คือการใช้จุดแข็งเพื่อให้ได้โอกาสมากที่สุด

2. จับคู่จุดแข็งหลัก – อุปสรรคหลัก (ST) กำหนดยุทธศาสตร์ที่เหมาะสม โดยยุทธศาสตร์คือการใช้จุดแข็งเพื่อหลีกเลี่ยงภาวะที่เป็นอุปสรรค

3. จับคู่จุดอ่อนหลัก – จุดแข็งหลัก (WO) กำหนดยุทธศาสตร์ที่เหมาะสม โดยยุทธศาสตร์ที่เหมาะสมคือการลดจุดอ่อนเพื่อเพิ่มโอกาส

4. จับคู่จุดอ่อนหลัก – ภาวะอุปสรรคหลัก (WT) กำหนดยุทธศาสตร์ที่เหมาะสม โดยยุทธศาสตร์ที่เหมาะสมคือการลดจุดอ่อนและหลีกเลี่ยงภาวะที่เป็นอุปสรรค
นำข้อมูลทั้งหมดเข้าสู่การดำเนินการในตาราง SWOT Matrix จากยุทธศาสตร์ทั้งหมดผู้วิจัยนำไปพัฒนาเป็นยุทธศาสตร์ที่สำคัญและกำหนดเป็นยุทธศาสตร์หลักของการวิจัยผลของการวิเคราะห์ความสัมพันธ์ในข้อมูลแต่ละคู่ดังกล่าว ทำให้เกิดยุทธศาสตร์ สามารถแบ่งออกได้เป็น 4 ประเภท ดังนี้

ยุทธศาสตร์เชิงรุก(SO Strategy)

ยุทธศาสตร์เชิงป้องกัน (ST Strategy)

ยุทธศาสตร์เชิงแก้ไข (WO Strategy)

ยุทธศาสตร์เชิงรับ (WT Strategy)

ขั้นตอนที่ 3 การกำหนดยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์

กำหนดยุทธศาสตร์เพื่อต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย ด้วยการนำข้อมูล ผลจากการสัมภาษณ์และสรุปผลความเห็นจากผู้เชี่ยวชาญทั้งหมดจากเทคนิคเดลฟาย มาวิเคราะห์และสังเคราะห์ในขั้นตอนที่ 1 และขั้นตอนที่ 2 มากำหนดเป็นยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย

ขั้นตอนที่ 4 ดำเนินการวิจัย (การวิจัยเชิงปริมาณ)

1. ผู้วิจัยนำข้อมูลที่ได้จากการสัมภาษณ์เชิงลึกและยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทยนำมากำหนดเป็นแบบสอบถามเชิงปริมาณ โดยกำหนดเป็นแบบสอบถามปลายปิดและแบบสอบถามปลายเปิดเพื่อให้ผู้ตอบแบบสอบถามได้แสดงความคิดเห็นเกี่ยวกับยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย

2.ประชากรและกลุ่มตัวอย่างที่ใช้ในการสอบถาม

2.1 ประชากรที่ศึกษา ได้แก่ ข้าราชการ (ข้าราชการพลเรือนสามัญ จำนวน 362,534 คน ข้อมูลจาก เอกสารเผยแพร่กำลังคนภาครัฐ พ.ศ.2555 สำนักงานคณะกรรมการข้าราชการพลเรือน) นักธุรกิจ นักเรียน/นักศึกษาและบุคคลทั่วไป

2.2 กลุ่มตัวอย่างแบ่งออกเป็น 4 กลุ่ม ได้แก่ข้าราชการ นักธุรกิจนักเรียน/นักศึกษาและบุคคลทั่วไปซึ่งมีส่วนเกี่ยวข้องกับการใช้ไซเบอร์โดยแบ่งกลุ่มตัวอย่างจากการกำหนดกลุ่มตัวอย่างของ Yamane ที่ระดับความเชื่อมั่นร้อยละ95 (วรรณี แกมเกตุ, 2555, หน้า 285) ดังนี้

ตารางที่ 3 ตารางกลุ่มตัวอย่าง

ประเภทของกลุ่มตัวอย่าง*	จำนวนประชากร	จำนวนกลุ่มตัวอย่าง	จำนวนกลุ่มตัวอย่างที่ต้องการ
กลุ่มข้าราชการพลเรือน	358,735 คน	400 คน	150 คน
กลุ่มนักธุรกิจ	5000 คน	400 คน	150 คน
กลุ่มนักเรียน/นักศึกษา	573 คน	222 คน	150 คน
กลุ่มบุคคลทั่วไป	7,980,000 คน	400 คน	150 คน
รวมตัวอย่างทั้งสิ้น		1222 คน	600 คน

*กลุ่มตัวอย่างกำหนดในเขตจังหวัดกรุงเทพมหานครเท่านั้น

ผู้วิจัยกำหนดกลุ่มตัวอย่างโดยการสุ่มตัวอย่างไม่อาศัยหลักความน่าจะเป็น (Nonprobability sampling) เป็นการเลือกตัวอย่างแบบบังเอิญ (Accidental sampling) โดยเลือกจากประชาชนเป้าหมายโดยไม่มีหลักเกณฑ์ใด ๆ เพียงแต่ให้ได้จำนวนครบตามที่ต้องการ (สิทธิ์ ธีรสรณ์, 2552, หน้า 101)

เครื่องมือที่ใช้ในการวิจัย

เครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูล ได้แก่ แบบสอบถามที่ผู้วิจัยได้สร้างขึ้นสำหรับสอบถามกลุ่มตัวอย่างซึ่งมีส่วนเกี่ยวข้องกับการใช้ไซเบอร์ โดยแบ่งออกเป็น 3 ตอนดังนี้

ตอนที่ 1 ข้อมูลทั่วไป

ตอนที่ 2 ประเด็นความก้าวหน้าทางไซเบอร์และลักษณะการก่อการร้ายทางไซเบอร์และนำมาเป็นเครื่องมือทางยุทธศาสตร์ในการก่อการร้าย

ตอนที่ 3 ประเด็นยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์

การทดสอบความเที่ยงของแบบสอบถาม

การตรวจสอบคุณภาพของแบบสอบถาม ผู้วิจัยกำหนดประเด็นหลักให้ตรงตามวัตถุประสงค์และพัฒนาจากข้อมูลการสัมภาษณ์ กำหนดข้อคำถามแต่ละประเด็น จากนั้นผู้วิจัย

ตรวจสอบคุณภาพของเครื่องมือ โดยเสนออาจารย์ที่ปรึกษาและผู้ทรงคุณวุฒิ จำนวน 3 ท่าน เพื่อตรวจสอบความเที่ยงตรง ตามเนื้อหา หลังจากนั้นผู้วิจัยปรับปรุงแก้ไข เครื่องมือตามข้อเสนอแนะก่อนนำไปใช้ข้อมูลต่อไป

ผู้ทรงคุณวุฒิประกอบด้วย

1.ดร.สฤษดิ์ ธัญกิจจานุกิจ ผู้อำนวยการกองกฎหมาย มหาวิทยาลัยสวนดุสิต

2.ผศ.ดร.ยุทธพงษ์ ลีลากิจไพศาล ผู้อำนวยการหลักสูตรรัฐประศาสนศาสตรมหาบัณฑิต มหาวิทยาลัยสวนดุสิต

3. พันเอกชาติชาย ชัยเกษม ผู้อำนวยการกองสงครามเครือข่าย สำนักปฏิบัติการ กรมยุทธการกองบัญชาการกองทัพไทย

นำแบบสอบถามที่ได้ปรับปรุงแก้ไขเรียบร้อยแล้ว ตรวจสอบความตรงเชิงเนื้อหา หาค่า IOC (Index of Item – Objective Congruence) ได้ผลการประมวลผลค่า IOC อยู่ระหว่าง0.6 – 1.00 จำนวน 33 ข้อและไปทดลองใช้ (Try out) กับผู้ที่ใช้หรือเกี่ยวข้องกับไซเบอร์ จำนวน 30 ฉบับ ในเดือนพฤศจิกายน 2558

4. นำแบบสอบถามที่ได้รับกลับมาคำนวณหาค่าความเชื่อมั่น โดยวิธีการหาสัมประสิทธิ์ความเชื่อมั่นด้วยสูตรสัมประสิทธิ์แอลฟา (Coefficient Alpha) ของครอนบาค (Cronbach, 1974, p.161) ได้ค่าความเชื่อมั่นเท่ากับ .94

การวิเคราะห์ข้อมูลแบบสอบถาม

ผู้วิจัยใช้การวิเคราะห์ข้อมูลทางสถิติ โดยนำข้อมูลที่ได้จากการเก็บรวบรวมจากแบบสอบถามทำการวิเคราะห์ โดยมีขั้นตอนดังต่อไปนี้ 1. ตรวจสอบความสมบูรณ์ของแบบสอบถามแล้วนำมาวิเคราะห์ 2. ดำเนินการวิเคราะห์ข้อมูลด้วยโปรแกรมสำเร็จรูป SPSS (Statistical Package for the Social Science) โดยข้อมูลเชิงปริมาณทำการประมวลผลด้วยการวิเคราะห์สถิติเชิงพรรณนา (Descriptive statistics) ได้แก่การแจกแจงความถี่ (Frequency) ร้อยละ (Percentage) ค่าเฉลี่ย (Mean) ส่วนเบี่ยงเบนมาตรฐาน (Standard deviation) ทดสอบสมมุติฐานโดยใช้สถิติเชิงอนุมาน คือ t – Test และ One – way ANONA

การวิเคราะห์ข้อมูล

ผู้วิจัยประมวลผลและวิเคราะห์ข้อมูลระดับความคิดเห็นของกลุ่มตัวอย่างตามประเด็นในแบบสอบถาม ด้วยการหาค่าเฉลี่ยและค่าส่วนเบี่ยงเบนมาตรฐาน (SD) โดยกำหนดค่าคะแนนของคำตอบดังนี้

ระดับคำตอบ 5 หมายถึง มากที่สุด กำหนดให้ค่าคะแนนเท่ากับ 5

ระดับคำตอบ 4 หมายถึง มาก กำหนดให้ค่าคะแนนเท่ากับ 4

ระดับคำตอบ 3 หมายถึงปานกลาง กำหนดให้ค่าคะแนนเท่ากับ 3

ระดับคำตอบ 2 หมายถึงน้อย กำหนดให้ค่าคะแนนเท่ากับ 2

ระดับคำตอบ 1หมายถึง น้อยที่สุด กำหนดให้ค่าคะแนนเท่ากับ 1

การแปลความหมายของค่าเฉลี่ยแบ่งเป็น 5 ระดับดังนี้

ค่าเฉลี่ยระหว่าง 4.21 – 5.00 หมายถึง เป็นค่าระดับที่เหมาะสม/เป็นไปได้มากที่สุด

ค่าเฉลี่ยระหว่าง 3.41 – 4.20 หมายถึง เป็นค่าระดับที่เหมาะสม/เป็นไปได้มาก

ค่าเฉลี่ยระหว่าง 2.61 – 3.40 หมายถึง เป็นค่าระดับที่เหมาะสม/เป็นไปได้ปานกลาง

ค่าเฉลี่ยระหว่าง 1.81 – 2.60 หมายถึง เป็นค่าระดับที่เหมาะสม/เป็นไปได้น้อย

ค่าเฉลี่ยระหว่าง 1.00 – 1.80 หมายถึง เป็นค่าระดับที่เหมาะสม/เป็นไปได้น้อยที่สุด

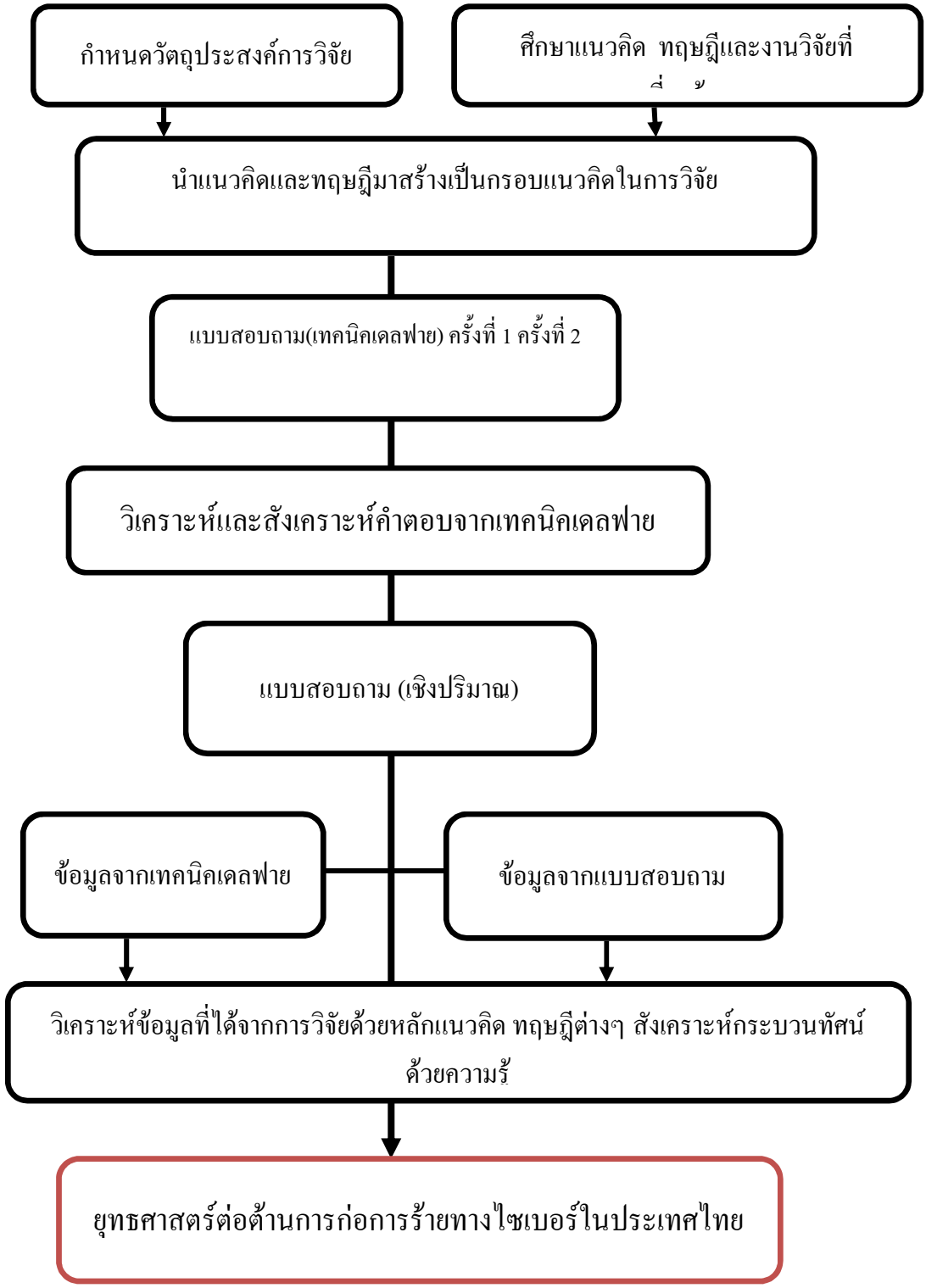
ผู้วิจัยดำเนินการวิเคราะห์ข้อมูลจากแบบสอบถามด้วยการแจกแจงความถี่ ร้อยละ ส่วนเบี่ยงเบนมาตรฐาน เพื่อนำข้อมูลมาประกอบการวิเคราะห์ประกอบยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ต่อไป

ขั้นตอนที่ 5 ยกร่างยุทธศาสตร์

การยกร่างยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทยเครื่องมือในขั้นตอนนี้เป็นตัวนักวิจัย เนื่องจากในขั้นตอนนี้เป็นการวิจัยเชิงคุณภาพ ผู้วิจัยถือเป็นเครื่องมือที่สำคัญที่สุดในกระบวนการวิจัยเชิงคุณภาพ ผู้วิจัยเป็นผู้ที่มีปฏิสัมพันธ์โดยตรงต่อเหตุการณ์หรือสถานการณ์ใดสถานการณ์หนึ่ง ในการเก็บรวมรวบข้อมูลและการวิเคราะห์ข้อมูลและนำข้อมูลการวิจัยเชิงปริมาณมาสนับสนุนการยกร่างยุทธศาสตร์

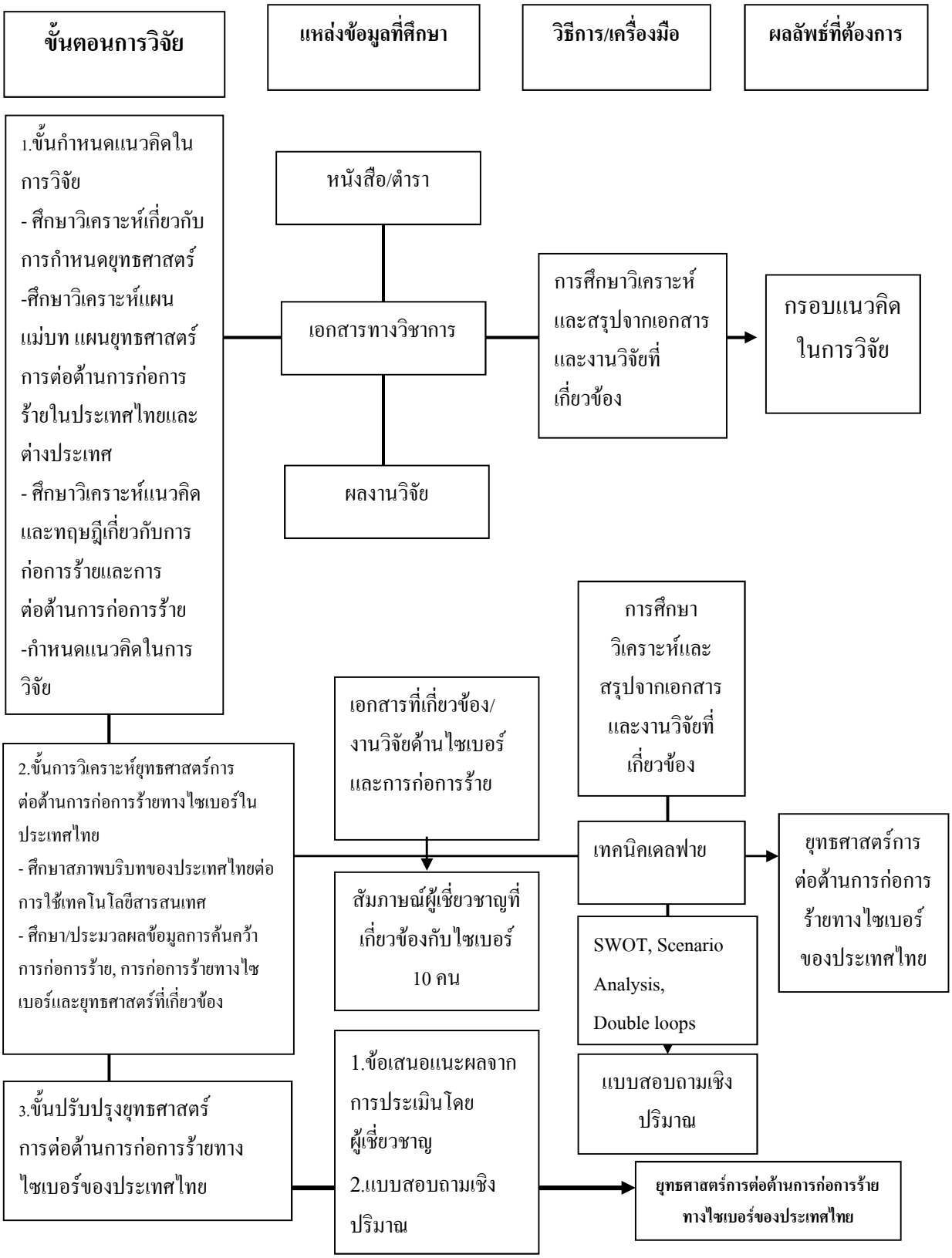
สรุปการวิจัยเรื่อง ยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย มีวัตถุประสงค์เพื่อ 1.เพื่อศึกษาความก้าวหน้าทางไซเบอร์ที่มีการนำมาใช้เป็นเครื่องมือทางยุทธศาสตร์ในการก่อการร้ายในประเทศไทย 2.เพื่อศึกษาลักษณะการก่อการร้ายโดยใช้ไซเบอร์มาเป็นเครื่องมือทางยุทธศาสตร์ในการก่อการร้ายของประเทศไทยและวิเคราะห์ประเมินการก่อการร้ายทางไซเบอร์ในประเทศไทยโดยใช้การวิเคราะห์จุดแข็ง จุดอ่อน โอกาสและอุปสรรควิธีการวิเคราะห์สถานการณ์และองค์กรแห่งการเรียนรู้ 3.เพื่อพัฒนายุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทยกลุ่มตัวอย่างในการวิจัยในครั้งนี้ประกอบด้วย เชิงคุณภาพคือ ผู้ที่มีบทบาทหรือส่วนเกี่ยวข้องกับการดำเนินการหรือการพัฒนาทางไซเบอร์และใช้การพัฒนาทางไซเบอร์มาเป็นเครื่องมือในการดำเนินการพัฒนาในประเทศไทยและผู้ที่มีความรู้ความเชี่ยวชาญในส่วนของการกำหนดยุทธศาสตร์ทางเทคโนโลยีในส่วนของภาครัฐ จำนวน 10 คน เชิงปริมาณคือ

ข้าราชการ นักธุรกิจ นักเรียน/นักศึกษาและบุคคลทั่วไป จำนวน 690 คน เก็บข้อมูลระหว่าง 30 พฤษภาคม 2558 ถึง วันที่ 20 พฤศจิกายน 2558 ได้นำมาวิเคราะห์เนื้อหา (Content analysis) และวิเคราะห์ โดยใช้ การแจกแจงความถี่ (Frequency) ร้อยละ (Percentage) ค่าเฉลี่ย (Mean) ส่วนเบี่ยงเบนมาตรฐาน (Standard deviation) ทดสอบสมมุติฐานโดยใช้สถิติเชิงอนุมาน คือ t – Test และ One – way ANONA การวิเคราะห์ความเชื่อมั่นด้วยตามวิธีการของครอนบาค ได้ค่าความเชื่อมั่นเท่ากับ .94



ภาพที่ 8 ขั้นตอนการวิจัยและการนำเสนอข้อมูล

ขั้นตอนการวิจัย



บทที่4
ความก้าวหน้าทางไซเบอร์และการก่อการร้ายทางไซเบอร์

การวิจัยเรื่องยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย โดยมีวัตถุประสงค์การวิจัยดังนี้1. เพื่อศึกษาความก้าวหน้าทางไซเบอร์ที่มีการนำมาใช้เป็นเครื่องมือทางยุทธศาสตร์ในการก่อการร้ายในประเทศไทย 2. เพื่อศึกษาลักษณะการก่อการร้ายโดยใช้ไซเบอร์มาเป็นเครื่องมือทางยุทธศาสตร์ในการก่อการร้ายของประเทศไทยและวิเคราะห์ประเมินการก่อการร้ายทางไซเบอร์ในประเทศไทยโดยใช้การวิเคราะห์จุดแข็ง จุดอ่อน โอกาสและอุปสรรควิธีการวิเคราะห์สถานการณ์และองค์กรแห่งการเรียนรู้ 3. เพื่อพัฒนายุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย ผู้วิจัยแบ่งผลการวิเคราะห์ข้อมูลของการศึกษาออกเป็น 2 ตอน โดยใช้กรอบแนวความคิดที่จะนำไปสู่การวิเคราะห์ยุทธศาสตร์การก่อต้านการก่อการร้ายดังนี้

บริบทของประเทศไทยและสถานการณ์การความมั่นคงปลอดภัยทางไซเบอร์

การเปลี่ยนแปลงจากภายในประเทศและการเปลี่ยนแปลงจากปัจจัยภายนอกประเทศจากกระแสโลกาภิวัตน์ทำให้ประเทศไทยมีการเปลี่ยนแปลงที่สำคัญเป็นปัจจัยผลักดันให้เกิดการตื่นตัวอย่างต่อเนื่องในศตวรรษที่ 21 นี้ ในระยะที่ผ่านมาประเทศไทยมีความเสี่ยงในหลายด้านทั้งเหตุการณ์ทางการเศรษฐกิจ เหตุการณ์ทางสังคม และเหตุการณ์ทางการเมืองที่ก่อให้เกิดปัญหาความรุนแรงในหลายด้านมากระทบส่งผลต่อการพัฒนาประเทศ

1. การเปลี่ยนแปลงทางเศรษฐกิจ

ประเทศไทยในด้านเศรษฐกิจมีการส่งเสริมให้ภาคอุตสาหกรรมส่วนของภาคการผลิตมีบทบาทสูงขึ้นและภาคเกษตรยังเป็นแหล่งรายได้หลักของประชาชนส่วนใหญ่ในประเทศ ภาคบริการและการท่องเที่ยวเป็นแหล่งสร้างมูลค่าเพิ่มที่สำคัญของประเทศ การเชื่อมโยงทั้งในประเทศและต่างประเทศก่อให้เกิดกิจกรรมการค้าระหว่างประเทศ ระบบเศรษฐกิจประเทศไทยยังคงต้องพัฒนาหรือส่งเสริมในด้านการพัฒนาทางเทคโนโลยีให้ทันสมัย คุณภาพการให้บริการของโครงสร้างพื้นฐาน กฎหมาย นโยบายของรัฐที่เอื้อต่อระบบเศรษฐกิจทำให้เกิดการแข่งขันและการเติบโตในทิศทางที่ดีและมีคุณภาพ

2. การเปลี่ยนแปลงทางสังคม

ประเทศไทยปี 2560 จะก้าวเข้าสู่สังคมผู้สูงอายุที่เพิ่มขึ้น วัยเด็กและวัยแรงงานลดลง ประชาชนได้รับการดูแลในด้านสวัสดิการทางสังคมในหลายรูปแบบ การเกิดปัญหาในเรื่องของการ

ได้รับบริการทางสังคมอย่างไม่เท่าเทียมกันความเหลื่อมล้ำทางรายได้ของประชาชนและโอกาสในการเข้าถึงทรัพยากรของประเทศยังคงเป็นปัญหาหลักและสำคัญของประเทศ อีกทั้งการแพร่หลายของยาเสพติด การพนัน การใช้สื่อสังคมออนไลน์ในชีวิตประจำวัน การเสพติดการสื่อสารออนไลน์โดยเฉพาะในกลุ่มเด็กและเยาวชน การเปลี่ยนแปลงแบบก้าวกระโดดของเทคโนโลยีสารสนเทศ ทำให้ผู้คนต้องปรับเปลี่ยนตัวเองเพื่อให้ทันสมัยกับเทคโนโลยี เรียกได้ว่าเป็นสังคมแห่งไซเบอร์สเปซ (Cyberspace)ในด้านหนึ่งก็ได้ประโยชน์อย่างมหาศาลแต่อีกด้านหนึ่งก็ก่อให้เกิดปัญหาต่าง ๆ ตามมาได้อย่างมากมาย

3.การเปลี่ยนแปลงทางการเมือง

ประเทศไทยผ่านวิกฤตการณ์ทางการเมืองหลายสถานการณ์ส่งผลให้ประชาชนมีความสนใจและตื่นตัวทางการเมืองสูงขึ้นแต่ความขัดแย้งทางการเมืองยังคงเป็นปัญหาที่ต้องแก้ไขในระยะยาว อีกทั้งปัญหาความไม่สงบในจังหวัดชายแดนภาคใต้ การบริหารงานของรัฐบาลยังคงต้องให้ความสำคัญในหลายด้านเช่น การแก้ปัญหาในเรื่องของทุจริตทั้งภายในองค์กรและในระดับประเทศ การกระจายอำนาจในยังท้องถิ่นยังคงมีความทับซ้อนและการถ่ายโอนภารกิจที่ไม่ชัดเจน รวมทั้งการคอร์รัปชั่นทั้งภายในองค์กรและระดับประเทศ สุดท้ายสิ่งสำคัญที่ประเทศไทยยังคงมีปัญหาและเป็นอุปสรรคในการพัฒนาประเทศคือปัญหาคอร์รัปชั่น ประเทศไทยยังมีปัญหาด้านอื่นๆ ทั้งยังคงต้องระวังความเสี่ยง ทั้งปัญหาที่มาจากการก่อความไม่สงบภายในประเทศ ปัญหาการก่อการร้ายการพัฒนาทางเทคโนโลยีและโครงสร้างพื้นฐานให้มีการพัฒนาอย่างพอเพียงกับความต้องการของประชาชน ภัยพิบัติต่าง ๆทั้งที่เกิดจากฝีมือมนุษย์และจากภัยธรรมชาติที่มีความรุนแรง รวมทั้งการที่ประเทศไทยจะต้องสร้างศักยภาพในทุก ๆ ด้านเพื่อการเข้าสู่ประชาคมอาเซียนได้อย่างมีประสิทธิภาพ

จากบริบทของประเทศไทยจะพบว่าในช่วงทศวรรษที่ผ่านมา ความก้าวหน้าของเทคโนโลยีสารสนเทศและการสื่อสารมีอย่างมากมายและในอนาคตแนวโน้มของเทคโนโลยีสารสนเทศก็มีการพัฒนามากขึ้น นักวิเคราะห์จากหลาย ๆ สำนักรวมไปถึงผู้เชี่ยวชาญและนักวิเคราะห์ นักคิดระดับโลกต่างลงความเห็นกันว่า เทคโนโลยีสารสนเทศและการสื่อสารในอนาคตที่จะส่งผลต่อการเปลี่ยนแปลงของโลกในปัจจุบันและในอีก 5 – 10 ปี ข้างหน้า ซึ่งจะมีบทบาทสำคัญในการเปลี่ยนแปลงวิถีชีวิตจะประกอบด้วย 1.เทคโนโลยีพกพา (Mobile) 2. เครือข่ายสังคมออนไลน์ (Social network) 3.การประมวลผลแบบก้อนเมฆ(Cloud computing) 4. เทคโนโลยีการจัดการข้อมูลจำนวนมหาศาล (Big data) เทคโนโลยีทั้งสี่ประเด็นนี้หากประเทศไทยมีการศึกษาและหลอมรวมเรื่องดังกล่าวเพื่อให้สามารถเรียนรู้ได้อย่างเท่าทัน จะส่งผลต่อการพัฒนาประเทศได้อย่างมหาศาล

จากข้อมูลของผู้ให้สัมภาษณ์ พบว่าประเทศไทยมีโอกาสในการพัฒนาความก้าวหน้าทางไซเบอร์ได้อีกมาก ด้านบริบทของประเทศไทยยังคงเป็นประเทศที่ไม่ได้มีการใช้ไซเบอร์ทุกระบบทั้งประเทศ และมีโอกาสในการพัฒนาทางไซเบอร์ด้วยปัจจัยหลายด้าน เช่น ความสามารถของคนรุ่นใหม่ที่มีความสนใจทางไซเบอร์ ความตื่นตัวต่อการเรียนรู้ทางไซเบอร์ การพัฒนาโครงสร้างพื้นฐานให้มีความพร้อมสามารถพัฒนาควบคู่ไปกับการใช้ไซเบอร์ และมีวิธีการป้องกันที่ดีต่อการก่อการร้าย

จากแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร (ฉบับที่ 3) ของประเทศไทย ผู้เชี่ยวชาญในวงการด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารในระดับนานาชาติมีความเห็นไปในทิศทางเดียวกันว่า ปัญหาความมั่นคงปลอดภัยในระบบสารสนเทศและการสื่อสารในปัจจุบัน มีแนวโน้มที่จะเผชิญการโจมตีในลักษณะแนวร่วมที่เป็นระบบมากขึ้น (Coordinate attacks) มีแรงจูงใจและเป้าหมายที่ชัดเจนมากขึ้น มีความพยายามในการซ่อนตัวมากขึ้น เพื่อให้สามารถโจมตีระบบได้เป็นระยะเวลานาน ก่อนที่ผู้ดูแลระบบจะรู้ตัว เช่น ในลักษณะของการจารกรรมทางอุตสาหกรรม (Industrial espionage) การก่อการร้ายต่อรัฐ การสอดแนมเพื่อล้วงความลับที่มีความสำคัญต่อความมั่นคงของประเทศ การโจมตีเครือข่ายของสถาบันทางการเงิน และการโจมตีระบบสารสนเทศและการสื่อสารของธุรกิจขนาดกลางและขนาดย่อม หรือ SME เป็นต้น

ปัจจุบันรัฐบาลและหน่วยงานทั้งภาครัฐและเอกชนในประเทศไทย ได้ให้ความสำคัญต่อความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสาร โดยการจัดตั้งองค์กรกรรมการและรูปแบบที่คล้ายกันระดับชาติที่มีหน้าที่รับผิดชอบโดยตรง อาทิ เช่น คณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (Thai CERT) และเครือข่ายความร่วมมือด้านความปลอดภัยในระบบคลาวด์คอมพิวติ้ง (Cloud security alliance Thailand chapte) เป็นต้น ตลอดจนมีการประกาศใช้กฎหมายต่าง ๆ ที่เกี่ยวข้อง เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 พระราชบัญญัติสุขภาพแห่งชาติ พ.ศ.2550 มาตรา 71 ซึ่งวางหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลที่เป็นข้อมูลประวัติสุขภาพ เป็นต้น ซึ่งสิ่งเหล่านี้เป็นส่วนหนึ่งของจุดเริ่มต้นที่จะนำไปสู่ความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศที่ดีขึ้นในประเทศไทย

ภาพรวมสถานภาพการพัฒนาด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการสื่อสารของประเทศไทยยังขาดการประสานกันระหว่างหน่วยงานต่าง ๆ และการนำมาตรฐานที่ได้รับการยอมรับในระดับสากลมาบังคับใช้และถือปฏิบัติ เพื่อให้เกิดการปฏิบัติตามข้อกำหนดใน

มาตรฐานต่างๆ (Compliance) เช่นมาตรฐาน ITIL และ COBIT และมาตรฐานในชุด SP800 ที่กำหนดโดย National Institute of Standards and Technology (NIST) นอกจากนี้หน่วยงานต่างๆ โดยเฉพาะภาครัฐยังขาดบุคลากรที่มีความรู้ความสามารถในการนำแนวทางปฏิบัติที่กำหนดไว้ในมาตรฐาน มาดำเนินการอย่างเป็นรูปธรรม ในการพัฒนาด้านนี้จึงจำเป็นต้องมีการพัฒนาอย่างเป็นระบบตามมาตรฐานสากล

การก่อการร้ายการก่อการร้ายทางไซเบอร์และแรงจูงใจที่เกี่ยวข้องต่อความก้าวหน้าทางไซเบอร์นำมาก่อการร้าย

ประเทศไทย กล่าวได้ว่าแม้ไม่ใช่เป้าหมายโดยตรงของกลุ่มผู้ก่อการร้าย แต่ตกเป็นเป้าหมายสำหรับการปฏิบัติการของกลุ่มผู้ก่อการร้าย เนื่องจากประเทศไทยมีผลประโยชน์เกี่ยวข้องกับประเทศต่างๆ โดยเฉพาะประเทศตะวันตก ซึ่งเป็นเป้าหมายของกลุ่มผู้ก่อการร้ายจำนวนมากโดยกลุ่มผู้ก่อการร้ายส่วนใหญ่ที่เข้ามาเคลื่อนไหวและปฏิบัติการในประเทศไทย จะใช้ประเทศไทยเป็นแหล่งที่หลบภัยและผลิตยุทโธปกรณ์ของกลุ่มผู้ก่อการร้าย อีกทั้งยังแสวงหาผลประโยชน์จากทางการเงิน การธนาคาร ประเทศไทยมีมาตรการที่ไม่รัดกุม เป็นช่องทางสนับสนุนทางการเงินของกลุ่มผู้ก่อการร้าย นอกจากนี้ การก่อการร้ายเชื่อมโยงกับการก่ออาชญากรรมประเภทอื่นๆ ด้วย เช่น การลักลอบค้ายาเสพติด การค้าอาวุธ การฟอกเงินการปลอมแปลงเอกสารเดินทาง บัตรประจำตัวประชาชนหรือเอกสารราชการอื่น ๆ ผู้ก่อการร้ายผลิตและลักลอบค้ายาเสพติดสามารถสร้างเงินและรายได้จำนวนมหาศาลให้กับผู้ก่อการร้าย และนำเงินที่ได้มาซื้ออาวุธหรือสร้างฐานกำลังเพื่อดำเนินการก่อการร้ายกับประเทศที่เป็นเป้าหมาย โดยมีวัตถุประสงค์ในการใช้ประเทศไทยเป็นฐานหรือศูนย์กลางในการจัดส่งอาวุธ หรือเป็นทางผ่านไปยังประเทศเป้าหมาย

จากการศึกษาในการก่อการร้ายจะพบว่าปัจจัยที่ทำให้กลุ่มก่อการร้ายแทรกซึมเข้ามาปฏิบัติการในประเทศไทย ประกอบด้วย6 ประการด้วยกัน คือ

1. ประเทศไทยเป็นศูนย์กลางการคมนาคมและการสื่อสารในภูมิภาคเอเชียตะวันออกเฉียงใต้

2. ประเทศไทยมีความเป็นอิสระในหลาย ๆ ด้านนโยบายที่สำคัญคือการเปิดประเทศเพื่อส่งเสริมการท่องเที่ยวและเพิ่มรายได้ให้กับประชาชนในภูมิภาคที่นักท่องเที่ยวนิยมไปเที่ยวหรือไปพักพิงเป็นเวลานาน

3. ประเทศไทยมีช่องโหว่ของกฎหมายในหลาย ๆ ฉบับ ที่ยังไม่ครอบคลุมประเด็นในเรื่องของการก่อการร้าย

4. ประเทศไทยยังขาดความเป็นหนึ่งเดียวกันทั้งในระบบการบริหารงานและการดำเนินการในทุกภาคส่วน ไม่มีกลไกที่มีประสิทธิภาพและขาดความร่วมมือกันอย่างเชื่อมโยงระหว่างหน่วยงานทั้งภาครัฐ ภาคเอกชน และภาคประชาชนต่อการต่อต้านการก่อการร้าย

5. มีปัญหาในเรื่องของคอร์รัปชั่นขององค์กร ขาดความโปร่งใส การบริหารงานภายในองค์กรที่ยังคงเป็นระบบอุปถัมภ์

6. บุคคลากรที่มีความเชี่ยวชาญทางด้านเทคโนโลยียังไม่เพียงพอ ขาดงบประมาณในการสนับสนุนเพื่อพัฒนาทางด้านเทคโนโลยีและการดำเนินการเพื่อการต่อต้านการก่อการร้าย อีกทั้งเมื่อพัฒนาบุคลากรไปศึกษาต่อเมื่อเกิดความชำนาญก็จะมีปัญหาสมองไหล ทำงานยังต่างประเทศด้วยเหตุจากการสนับสนุนหรือสร้างแรงจูงใจ เช่น ในเรื่องเงินเดือน การเลื่อนขั้นตามความสามารถยังมีน้อย เป็นต้น

จะเห็นได้ว่า การก่อการร้ายจะต้องมีเป้าหมาย วัตถุประสงค์และรูปแบบในการกระทำที่ชัดเจน ซึ่งกระทำได้จากบุคคล องค์กร หรือรัฐ แต่การก่อการร้ายทางไซเบอร์ มีหลากหลายรูปแบบทั้งประเภทที่กระทำโดยไม่ได้มุ่งหวังทำลายล้างหรือการกระทำที่สร้างความเสียหายต่อประเทศโดยมีรูปแบบที่หลากหลายและซับซ้อน แม้ประเทศไทยจะไม่ใช่เป้าหมายของการก่อการร้ายโดยตรง แต่คนไทยก็ไม่มีการตระหนักต่อภัยของการก่อการร้ายในสถานการณ์การก่อการร้ายปกติและการก่อการร้ายทางไซเบอร์ ประเทศไทยมีความพร้อมของการรับมือต่อการเกิดสถานการณ์จากหน่วยงานซึ่งมีหน้าที่ดูแลรับผิดชอบ แต่ก็ยังคงมีช่องโหว่ เช่น ทางด้านกฎหมาย ทางด้านของหน้าที่ในการดูแลและรับผิดชอบต่อการป้องกันการก่อการร้าย ผู้ก่อการร้ายสามารถใช้ช่องโหว่นี้ก่อการร้ายได้ทุกเมื่อ

ผลการวิเคราะห์ข้อมูลจากการสัมภาษณ์ประเภท: การก่อการร้าย สถานการณ์การก่อการร้ายในประเทศไทย ดังนี้

“การก่อการร้ายคือการทำให้ได้ในสิ่งที่เหนือคนอื่น การทำให้คนนั้นสูญเสียอำนาจ” (มนตรี, นามสมมติ, สัมภาษณ์, 11 พฤษภาคม 58)

“การทำอันตรายต่อสิ่งใดก็ตามไม่ว่าจะเป็นระบบหรือคน ที่มุ่งเป้าไปสู่ความเสียหายอย่างรุนแรง ความเสียหายต่อประเทศหรือระดับประเทศ” (วิเชียร, นามสมมติ, สัมภาษณ์, 26 พฤษภาคม 58)

“การก่อการร้ายเป็นการกระทำที่ก่อให้เกิดผลเสียอย่างใดอย่างหนึ่งต่อบุคคล บุคคลหนึ่งหรือแม้แต่ภาพรวมหรือมีผู้เสียหายเพราะไม่สามารถตอบได้ว่าการโจมตีจะเป็นบุคคลหนึ่งหรือเป็นภาพรวม แต่การโจมตีบุคคลหนึ่งก็มีผลกระทบต่อบุคคลอื่นตามไปด้วย” (มงคล, นามสมมติ, สัมภาษณ์, 27 พฤษภาคม 58)

“การก่อการร้ายคือการใช้เครื่องมือหรือยุทธวิธีทั้งหลายโดยที่ไม่ใช้วิธีแบบดั้งเดิม ไม่ได้รบประชันหน้า การไปให้ถึงเป้าหมาย ให้บรรลุเป้าหมายส่วนใหญ่เป็นทางการเมือง แต่ก็มีเหมือนกันให้บรรลุเป้าหมายทางเศรษฐกิจ สังคม ส่วนใหญ่เป็นวิธีการรุนแรง เนื่องจากว่าต้องการให้ได้รับความสนใจ เพราะฉะนั้นการก่อการร้ายก็มักจะมีที่มาจากกลุ่มคนที่ไม่ได้รับความเป็นธรรมจากสังคม ไม่ว่าจะแง่ไหนก็ตาม เศรษฐกิจ สังคม การเมือง หรือเป็นพวกที่มีความคิดเป็นอุดมคติจนเกินไป โดยมีเหตุจากแรงจูงใจหรือความเชื่อหรืออะไรก็ตาม” (สัญญา, นามสมมติ, สัมภาษณ์, 10 กรกฎาคม 58)

“การก่อการร้ายเป็นลัทธิเป็นความเชื่อ เป็นการปลุกระดมความแตกแยก ความระส่ำระส่าย ก่อให้เกิดการขยายตัว ทำให้ไซเบอร์ขยายตัวตามไปด้วย เนื่องจากไซเบอร์มีการเข้ามาอย่างรวดเร็ว ไซเบอร์จึงเป็นพลังอำนาจที่สำคัญ ที่ทำให้เกิดความเสียหายทางการเงินและการธนาคาร มันไม่ใช่ความรุนแรงถึงขั้นชีวิต แต่ทำให้เกิดการขยายผลได้” (อวยพร, นามสมมติ, สัมภาษณ์, 20 ตุลาคม 58)

สรุปได้ว่า การก่อการร้ายหมายถึง กระทำการใด ๆ เพื่อให้เกิดความเสียหาย ส่งผลกระทบต่อส่วนรวม ก่อให้เกิดความหวาดกลัว การใช้ความรุนแรงหรือขู่ว่าจะใช้ความรุนแรงเพื่อให้เกิดความตื่นตระหนก โดยมีแรงจูงใจและเหตุจูงใจทางการเมือง ทั้งนี้เพื่อนำไปสู่การเปลี่ยนแปลงในทางสังคมทางการเมืองและทางเศรษฐกิจ

การก่อการร้ายทางไซเบอร์

ประเภทของการก่อการร้ายสามารถแบ่งได้เป็นหลายประเภทโดยใช้เกณฑ์แบ่งประเภทที่แตกต่างกันออกไป และมิได้กำหนดแน่นอนแต่เป็นเพียงแนวทางกว้างๆ เพื่อให้ทำความเข้าใจในลักษณะและรูปแบบของการก่อการร้าย มีการแบ่งออกเป็น 3 ประเภทดังนี้

1.การก่อการร้ายที่ไม่ได้รับการสนับสนุนจากประเทศอื่น ๆ การก่อการร้ายประเภทนี้จะเป็นเพียงองค์กรกลุ่มเล็กๆ ที่มีความคิดเป็นของตนเอง ไม่มีความสัมพันธ์กับรัฐบาลหรือรัฐประเทศอื่นใดมีการสร้างฐานเงินทุนด้วยตนเองหรือหาแหล่งเงินทุนสนับสนุนด้วยกลุ่มของตนเอง หรือใช้วิธีการระดมทุนด้วยรูปแบบต่าง ๆ เช่น การลักพาตัว การข่มขู่ การปล้น โดยส่วนใหญ่ลักษณะประเภทนี้จะเป็นจุดเริ่มต้นขององค์กรก่อการร้ายต่อไป

2.การก่อการร้ายที่ได้รับการสนับสนุนจากรัฐหรือประเทศอื่น ๆการก่อการร้ายประเภทนี้จะได้รับการสนับสนุนหรือการติดต่อกับรัฐหรือประเทศที่ให้การสนับสนุนด้านอาวุธ เงินทุน ที่ลี้ภัยทางการเมือง รวมทั้งการสนับสนุนในด้านอื่นๆ แม้จะได้รับการสนับสนุนจากประเทศอื่นๆ ก็ไม่มีอำนาจในการควบคุมองค์กรก่อการร้าย ในส่วนของรัฐที่เกี่ยวข้องกับการก่อการร้ายจะจำกัดอยู่ใน

ลักษณะของการสนับสนุนด้านการเงิน การช่วยเหลือทางทหาร การฝึกและอุดมการณ์ การให้ความคิดริเริ่ม

3.การก่อการร้ายในการควบคุมของรัฐบาลหรือประเทศใดๆในศตวรรษที่ 21 นี้มีรูปแบบของการก่อการร้ายที่สังคมมีความตื่นตัวกับการป้องกันภัยของการก่อการร้ายนี้ การก่อการร้ายทางไซเบอร์ (Cyber terrorism) เป็นรูปแบบของการก่อการร้ายโดยมีการนำเทคโนโลยีสารสนเทศที่ทันสมัยนำมาเป็นเครื่องมือที่ช่วยให้กลุ่มก่อการร้ายสามารถดำเนินกิจกรรมต่าง ๆ ได้อย่างกระจายตัวอย่างมีประสิทธิภาพ โดยใช้พลังอำนาจของเทคโนโลยีสารสนเทศเป็นแนวทางปฏิบัติหรือปรับองค์กรไปสู่รูปแบบใหม่

การก่อการร้ายรูปแบบนี้อาศัยช่องว่างการขยายตัวของโลกสมัยใหม่ที่มีการเชื่อมโยงของข้อมูลข่าวสารผ่านระบบคอมพิวเตอร์ในระบบเครือข่าย จึงทำให้ผู้ก่อการร้ายสามารถใช้ช่องทางนี้และผู้ใช้เทคโนโลยีสารสนเทศตกเป็นเป้าของการโจมตี (Cyber attack) เพื่อทำลายหรือขัดขวางการทำงานระบบเครือข่ายคอมพิวเตอร์แบบต่างๆ ไม่ว่าจะเป็นเครือข่ายการสื่อสารหรือเครือข่ายระบบคอมพิวเตอร์ที่เกี่ยวข้องกับการทำงานขององค์กรขนาดใหญ่ การควบคุมโครงสร้างพื้นฐาน หรือระบบโครงสร้างความมั่นคงทางทหาร หรือการล้วงข้อมูลความมั่นคงของประเทศ เป็นต้น โดยใช้วิธีการสร้างความเสียหาย ก่อให้เกิดความตื่นตระหนกต่อประชาชน และดึงดูดความสนใจของสื่อมวลชนหรือบุคคลต่าง ๆ ซึ่งคาดหมายว่า อนาคตจะมีการก่อการร้ายทางไซเบอร์ (Cyber Terrorism) และเป็นยุทธวิธีหนึ่งในการก่อการร้ายการก่อการร้ายทางไซเบอร์

ผลการวิเคราะห์ข้อมูลจากการสัมภาษณ์: การก่อการร้ายทางไซเบอร์ดังนี้

“การก่อการร้ายหากเป็นวิธีการทางเทคนิคก็สามารถป้องกันได้ วิธีการที่ดีที่สุดของผู้ก่อการร้ายคือสร้างความเชื่อ(Trust) เป็นการล่อลวงความโลภจากคน สังคมไทยเป็นสังคมการพนันที่สะท้อนความโลภ ความหวัง สังคมทุนนิยม วัตถุนิยม เป็นเรื่องของรสนิยมที่สร้างความสำเร็จในทางที่ผิด เป็นการสร้างช่องทางที่ทำให้ผู้ก่อการร้ายทางไซเบอร์ใช้เป็นช่องทางในการหาประโยชน์จากตัวเรา หาประโยชน์จากความโลภของมนุษย์ เราอาจยังไม่ได้กล่าวถึงสงครามไซเบอร์ หากถามว่าประเทศไทยมีไหม ตอบว่ามี เช่นมีการทำลายระบบโครงสร้างพื้นฐาน ทำลายระบบน้ำ ระบบไฟฟ้า ทำจริงก็ทำได้ แต่แรงจูงใจไม่ขนาดนั้น” (มนตรี, นามสมมติ, สัมภาษณ์, 11 พฤษภาคม 58)

“ผู้ก่อการร้ายนำไซเบอร์มาเป็นเครื่องมือในการก่อการร้าย 1.ติดต่อพรรคพวก 2.ชักชวนเพื่อร่วมอุดมการณ์ 3.โฆษณาชวนเชื่อ เพื่อสร้างผลงาน ตบทรัพย์ เรียกเงินจากนายทุน มหาเศรษฐี ผลประโยชน์เงิน และอุดมการณ์เพื่อให้บรรลุเป้าหมายเฉพาะกลุ่ม” (วิเชียร, นามสมมติ, สัมภาษณ์, 26 พฤษภาคม 58)

“วิธีการปฏิบัติการหลักของการก่อการร้ายทางไซเบอร์คือ ต้องศึกษาเป้าหมายที่ต้องการใช้เป็นเป้าหมาย ลักษณะของหน่วยงานเรื่องของระบบหรืออาจจะเป็นการจัดอันดับหรือเรื่องอื่น ๆ ประเทศนั้นเป็นอย่างไร เป็นขั้นตอนแรกของแฮกเกอร์ และหลังจากนั้นเริ่มเห็นว่าโอกาสว่ามีความยากง่ายเพียงใด หลังจากนั้นพัฒนาเครื่องมือต่างๆ พัฒนาให้ตรงเป้าหมายที่ต้องการ แต่ถ้าเป็นเรื่องระหว่างประเทศ อาจลัดขั้นตอนเป็นการกำหนดไว้เลยว่า ตรงนี้ ด้วยเหตุผลอะไรก็แล้วแต่ อาจจะเป็นเรื่องของการเมืองหรือเหตุผลอื่นก็ตามก็คงต้องมีการศึกษาหรือมีกลยุทธ์ที่ซับซ้อนกว่า” (มงคล, นามสมมติ, สัมภาษณ์, 27 พฤษภาคม 58)

“การก่อการร้ายทางไซเบอร์ ประการแรกการใช้อินเทอร์เน็ต เป็นเครื่องมือหลักในการติดต่อสื่อสารหรือช่องทางในการก่อการร้าย เพราะอินเทอร์เน็ตสามารถไปถึงทุกคนได้ทั่วโลก สองต้องมีเงินทุน ต้องมีผู้ให้การสนับสนุน เพราะต้องใช้เวลาต้องหาวิธีการที่ต้องมีทุนในการสนับสนุน เช่นต้องไปโจมตีเพื่อหาทุน อาจจะใช้ช่องทางที่ถูกกฎหมายและไม่ถูกกฎหมายเพื่อให้ได้เงินทุน สาม กลุ่มสมาชิกก็เป็นสิ่งสำคัญ ถึงแม้จะมีการทำเพียงคนเดียว เพราะการโจมตีมากกว่าหนึ่งก็ต้องมีผลตอบแทนได้ดีกว่าโจมตีเพียงคนเดียว มีเป้าหมายหรือวัตถุประสงค์ที่ชัดเจนว่าทำไปเพื่ออะไร อย่างน้อยต้องรู้ว่าทำไปเพื่ออะไร” (สัญญา, นามสมมติ, สัมภาษณ์, 10 กรกฎาคม 58)

“การก่อการร้ายทางไซเบอร์ มีวิธีปฏิบัติการหลักคือ หนึ่งต้องมีแฮกเกอร์ สองต้องเจาะระบบ การปล่อยไวรัสหรือมัลแวร์เข้าไปในระบบและก็ใช้การเจาะระบบคอมพิวเตอร์ เช่น การเข้าไปหยุดระบบโรงงานนิวเคลียร์ อาวุธ มีการปล่อยอาวุธทั้งหลายเข้าไป อีกส่วนหนึ่งคือการระดมคนเข้ามาร่วมกลุ่มของตนเอง โดยใช้ไซเบอร์เข้ามารวมพล สองคือ เผยแพร่แนวคิดของตนเองให้คนได้รู้ สามคือให้ความรู้สอนวิธีการทำระเบิด ข้อความที่เป็นคู่มือ สี่ใช้วิธีการสื่อสาร” (วรรณี, นามสมมติ, สัมภาษณ์, 13 กรกฎาคม 58)

“การก่อการร้ายทางไซเบอร์ วิธีการปฏิบัติการคือ 1.เก็บข้อมูลเกี่ยวกับเป้าหมาย ว่าเป้าหมายมีระบบอะไร ทำอะไรบ้าง มีช่องโหว่ตรงไหน พยายามหาให้ได้ 2.เจาะช่องโหว่ตรงนั้น ช่องโหว่เกิดขึ้นได้ตลอด จากการสำรวจพบว่า 1 ครั้งใช้การสำรวจ 205 วัน กว่าจะรู้ว่าเป็นช่องโหว่ก็จะทำให้คนที่รู้ช่องโหว่ก่อนไปโจมตีซึ่งเป็นใครก็ได้ที่สนใจ 3.หาเครื่องมือในการยึดระบบนี้เป็นฐานจะยึดเลยหรือจะยึดเพื่อไปหาที่อื่นต่อ 4. ทำลายหลักฐาน เช่น ransomware คือการเรียกค่าไถ่ เป็นการเอามัลแวร์ไปฝังกับเครื่องคอมพิวเตอร์ของเหยื่อ เช่นอาจส่งผ่านอีเมล์หรือส่งผ่านเว็บที่มีมัลแวร์ตัวนี้ฝังอยู่และเมื่อติดก็จะสแกนไฟล์ที่มีเอกสาร (Document) ที่มีอยู่ทั้งหมด โดยจะสร้างกุญแจขึ้นมาก่อนและสร้างรหัสข้อมูลที่สำคัญและจะโยนกุญแจที่สร้างขึ้นไปไว้ที่เครื่องให้บริการแม่ข่าย (Sever) เสร็จแล้วจะส่งอีเมล์กลับมายังเจ้าของไฟล์ที่เข้ารหัสไว้ ถ้าอยากถอดรหัสให้จ่ายเงิน

เช่น Bit coin และสามารถไปถึงรัฐชาติและราคาไม่สูงมาก" (สมชัย, นามสมมติ, สัมภาษณ์, 16 กรกฎาคม 58)

สรุปวิธีการก่อการร้ายทางไซเบอร์ มีวิธีการดังนี้ 1.ผู้ก่อการร้ายซึ่งต้องมีความรู้ทางไซเบอร์หรือเทคโนโลยี ศึกษาข้อมูลที่เกี่ยวกับเป้าหมายที่ต้องการจะกระทำ 2.สร้างหรือพัฒนาเครื่องมือให้ตรงกับความต้องการต่อเป้าหมาย เครื่องมือที่สำคัญของการก่อการร้ายทางไซเบอร์คืออินเทอร์เน็ต 3.ระดมคนหรือหาสมาชิกที่มีแนวความคิดแนวทางเดียวกัน 4.ระดมเงินทุนในการสนับสนุน 5.ปฏิบัติการตามวัตถุประสงค์ที่วางไว้เพื่อมุ่งเป้าหมายทางการเมือง

แรงจูงใจที่เกี่ยวข้องต่อความก้าวหน้าทางไซเบอร์นำมาก่อการร้าย

การก่อการร้ายเป็นการกระทำที่นำมาซึ่งความเสียหาย นำมาซึ่งความสูญเสีย เป็นการกระทำที่มุ่งกระทำต่อเป้าหมายที่เป็นสัญลักษณ์ รวมถึงประชาชนทั่วไปโดยมีเจตจำนงเฉพาะในการกระทำ ปัจจุบันการก่อการร้ายขยายขอบเขตของการดำเนินการไปด้วยปัจจัยหลายประการไม่ว่าจะเป็นเรื่องของศาสนา อิสรภาพ สิทธิมนุษยชน แต่ในปัจจุบันการก่อการร้ายมักมุ่งเป้าไปในเรื่องของการเงิน ด้วยการทำสงครามในการปฏิบัติการที่เต็มรูปแบบจำเป็นต้องใช้กำลังเงินและยุทโธปกรณ์จำนวนมาก มุ่งเป้าไปยังสถานที่ที่มีการวางกำลัง หรือระบบป้องกันหนาแน่น ซึ่งอาจเป็นการยากต่อการปฏิบัติการในปัจจุบันจึงพบว่า การก่อการร้ายเปลี่ยนมาเป็นการปฏิบัติการต่อเป้าหมายที่เด่นชัด มีระบบการป้องกันไม่แน่นหนา หรือเข้าปฏิบัติการในช่วงเวลาที่ไม่ได้ถูกคาดหมาย ระบบการรักษาความปลอดภัยยังมีน้อย และเป้าหมายนั้นต้องเป็นเป้าหมายที่ได้รับความสนใจต่อคนส่วนใหญ่ ปัจจัยที่มีส่วนเกี่ยวข้องในการก่อการร้ายมีดังนี้

1. การก่อการร้ายได้แพร่ขยายในทุกพื้นที่แทบทุกส่วนของโลก ด้วยเทคโนโลยีสารสนเทศที่มีความรวดเร็วและหลายช่องทางในยุคปัจจุบัน ผู้ก่อการร้ายสามารถเคลื่อนไหวดำเนินกิจกรรมต่างๆ ได้สะดวก รวดเร็ว และการพัฒนาของอุปกรณ์ที่มีความทันสมัยในการรับส่งข้อมูลข่าวสาร การสั่งการ การติดตามผล อันเป็นการยากต่อการติดตามร่องรอยของผู้ก่อการร้าย การดำเนินการปราบปรามจึงต้องใช้เวลานานและต้องใช้การรวบรวมข้อมูลข่าวกรองจากหลายๆ แห่ง และเป็นเวลานานกว่าจะสืบทราบข้อเท็จจริง

2. ส่วนหนึ่งของผู้ก่อการร้ายได้รับการสนับสนุนจากรัฐบาลหรือประเทศต่างๆ เพื่อใช้ประโยชน์ในการดำเนินการนโยบายทางการเมือง โดยประเทศที่เป็นผู้สนับสนุนส่วนใหญ่เป็นประเทศที่มีกำลังทหารที่อ่อนแอ หรือพลังอำนาจแห่งชาติไม่เข้มแข็ง และมีประเทศส่วนหนึ่งที่กำลังเผชิญหน้ากับประเทศมหาอำนาจ หรือเข้มแข็งกว่า รวมไปถึงประเทศที่ไม่ต้องการเปิดเผยนโยบายทางการเมืองที่รุนแรง หลีกเลี่ยงการปะทะโดยใช้กำลังแบบโดยตรง

3. ส่วนหนึ่งของการก่อการร้ายเป็นทางเลือกที่ถูกนำมาใช้เพราะการก่อการร้ายในยุคสมัยใหม่เป็นสงครามแบบกองโจรหรือสงครามแบบหลบซ่อน ยากที่จะป้องกันหรือตอบโต้การกระทำนั้น การก่อการร้ายส่วนใหญ่ไม่ต้องการเงินสนับสนุนจำนวนมาก การก่อการร้ายแบบนี้ใช้เงินทุนจำนวนไม่มาก จึงเป็นเรื่องง่ายต่อการระดมทุนในแต่ละครั้ง การติดตามเส้นทางการเงินที่หมุนเวียนจึงเป็นเรื่องยาก เพราะผู้ก่อการร้ายมักใช้บัญชีปลอมในการทำธุรกรรมต่างๆ ทางการเงินกับธนาคารและสถาบันทางการเงิน เงินหมุนเวียนส่วนใหญ่จะเป็นการนำเงินมาจากกิจกรรมที่ถูกต้องตามกฎหมายรวมเงินเข้ากับกิจกรรมที่ผิดกฎหมาย ความสนใจในการติดตามเงินที่ถูกโยกย้ายออกนอกระบบธนาคารจึงไม่เป็นที่น่าสนใจเท่าที่ควร

ผลการวิเคราะห์ข้อมูลจากการสัมภาษณ์ประเภท: แรงจูงใจที่เกี่ยวข้องต่อความก้าวหน้าทางไซเบอร์นำมาก่อการร้ายดังนี้

“แรงจูงใจเกิดจากความสนุก มีความพอใจ และการเปิดเสรีของประเทศไทย เมื่อเราเป็นฐานและถูกหลุดรอดจากการถูกจับกุม แม้ว่าประเทศไทยอาจไม่ได้ต้องการเป็นอิสระ แต่เราไม่รู้เท่าทัน เหมือนกับประเทศไทยเป็นดินแดนอิสระ บวกกับลักษณะทางกายภาพของประเทศไทยซึ่งเป็นมิตรกับทุกคน เราไม่ได้แยกแยะความน่าเชื่อถือระหว่างผู้ที่เข้ามาในประเทศว่าผู้ใดเป็นมิตร ผู้ใดที่เราควรจะปฏิเสธ เมื่อระบบเงินสามารถไปถึงจุดของข่าวกรองได้ ก็จะไม่สามารถแยกแยะได้ว่าคนไหนไม่ดี ฐานข้อมูลไม่ดีพอ เอกซเรย์คนไม่ได้ และก็จะยากถ้าคนไม่ช่วยกันสอดส่องดูแล ไม่มีใครบอกให้ตระหนักในเรื่องนี้ ผู้บริหารบางคนไม่ใช้สังคมออนไลน์ บางครั้งเมื่อไม่ใช้เทคโนโลยีก็ทำให้เป็นผู้รู้ได้ยาก เพราะประเทศไทยให้การศึกษาเฉพาะคนที่อยู่ในระบบ ช่องทางของการรับรู้ ช่องว่างระหว่างการรับรู้เป็นประเด็นสำคัญ ความรู้ความเข้าใจเป็นเรื่องของการรับรู้ ผิดกลุ่มเป้าหมาย” (มนตรี, นามสมมติ, สัมภาษณ์, 11 พฤษภาคม 58)

“การก่อการร้ายทางไซเบอร์ ประการแรก คือ เงิน หรือทางเศรษฐกิจเพราะอาจต้องการเงินหรือทรัพย์สิน ทำให้ระบบสาธารณูปโภค ธนาคารมีความเสียหายหรือเป็นช่องโหว่ของธนาคารให้ถูกโจมตีทำให้เกิดความผิดพลาด ประการที่สอง ต้องการที่จะมีชื่อเสียง อาจจะไม่ต้องการแค่ให้รู้จักชื่อกลุ่มหรือผู้กระทำ แต่ต้องการให้เกิดความเสียหาย อาจไม่ได้ต้องการประกาศแค่ชื่อ เพียงแค่ให้ฉายาของกลุ่มปรากฏไปทั่วโลก อีกประการเป็นความเกลียดชัง ความไม่ชอบนำมาสู่การโจมตี อาจมองได้หลายแง่มุม เช่น เชื้อชาติ หรือการแบ่งแยกดินแดนทางศาสนา ใช้สังคมออนไลน์โจมตีสาธารณูปโภคอีกประเทศหนึ่ง เพื่อให้หันมาใช้ของอีกประเทศหนึ่ง มีอำนาจในภูมิภาคหนึ่ง” (วิเชียร, นามสมมติ, สัมภาษณ์, 26 พฤษภาคม 58)

“การก่อการร้ายทางไซเบอร์มาจากสาเหตุ 1.ความภาคภูมิใจ 2.เพื่อเงิน 3. เพื่อชื่อเสียง 4.ต้องการให้เป็นที่รู้จักในระดับชาติ” (มงคล, นามสมมติ, สัมภาษณ์, 27 พฤษภาคม 58)

"แรงจูงใจต้องการเรียกร้องความสนใจ ให้คนหันมาสนใจให้รู้ว่าทำได้ สองคือความเข้าถึงง่ายของเทคโนโลยีจึงสามารถทำได้ง่าย และมีผลกระทบในวงกว้าง ส่งสารไปในวงกว้างมากขึ้นทำให้คนได้รับรู้ การก่อการร้ายเรื่องเงินไม่ใช่ปัจจัยหลัก แต่อาจเป็นปัจจัยสนับสนุน เช่นไปลักพาตัวมาหรือไปขโมยข้อมูลมาเพื่อให้โอนเงินให้เข้าบัญชี ส่วนใหญ่ผู้ก่อการร้ายมักต้องการให้เกิดการเปลี่ยนแปลง โดยเฉพาะทางการเมือง เปลี่ยนแปลงอย่างใหญ่มองเป้าหมายใหญ่มากกว่า" (สัญญา, นามสมมติ, สัมภาษณ์, 10 กรกฎาคม 58)

"การก่อการร้ายทางไซเบอร์เพื่อต้องการด้านการเงิน ด้านข้อมูลเอาข้อมูลไปใช้ อาจเป็นกลุ่มที่อาจใช้ข้อมูลไปใช้ทำประโยชน์ ด้วยธรรมชาติของประเทศไทยไม่ได้เป็นประเทศที่ต้องการชนกับประเทศอื่นๆ ธรรมชาติของคนไทยไม่ค่อยให้ความสำคัญเห็นว่าเป็นเรื่องไกลตัว คิดว่าน่าจะเป็นบทสรุปว่าคนไทยมีมุมมองในการก่อการร้าย และไม่มีความเข้าใจ ด้วยความที่เป็นแบบไทยๆ ประเทศไทยไม่ได้เป็นมหาอำนาจหรือไม่ได้มีทรัพยากรที่มีน้ำมัน หรือมีอาวุธ หรือมีเบื้องหลังทางการเมืองที่ไปขัดแย้งกับประเทศใดประเทศไทยเห็นชอบกับทุกสิ่ง" (วรรณี, นามสมมติ, สัมภาษณ์, 13 กรกฎาคม 58)

บทสรุป ปัจจัยที่เกี่ยวข้องกับแรงจูงใจในการก่อการร้ายทางไซเบอร์ด้วยประเทศไทยเป็นประเทศเปิดเสรี เปิดรับนักท่องเที่ยวและมีนโยบายส่งเสริมให้เกิดการท่องเที่ยวในทุกที่โดยไม่มีข้อจำกัด ดังนั้นจึงเป็นเหมือนสวรรค์ของผู้ก่อการร้าย อีกทั้งการส่งเสริมการเปิดใช้อินเทอร์เน็ตในทุกที่ ทำให้ประชาชนขาดการตระหนักรู้ในเรื่องของการใช้ไซเบอร์การก่อการร้ายทางไซเบอร์นั้น ผู้ก่อการร้ายจะใช้เครื่องมือทางไซเบอร์ที่หาง่ายและใช้เครื่องมือได้ทุกที่ไม่ว่าจะเป็นโทรศัพท์มือถือ แท็บเล็ต คอมพิวเตอร์ ที่สามารถเชื่อมต่ออินเทอร์เน็ตได้ทำให้คนเข้าถึงได้ง่ายและเชื่อง่ายขึ้น แรงจูงใจที่นำไซเบอร์มาก่อการร้าย ผู้เชี่ยวชาญมองว่าเป็นเรื่องเงินเป็นสำคัญ รองลองมาเป็นเรื่องของแนวคิด อุดมการณ์ทางการเมืองหรือทางศาสนา หรือแม้แต่ความไม่พอใจต่อหน่วยงานหรือองค์กร แต่ปัจจัยที่สำคัญที่ผู้เชี่ยวชาญมองต่างกันคือ แรงจูงใจที่สำคัญต่อการกระทำที่เป็นการก่อการร้ายจะต้องเป็นการกระทำที่มาจากแรงจูงใจทางเมืองเป็นสำคัญ จึงเห็นได้ว่า ความเข้าใจในความหมายของการก่อการร้ายที่แตกต่างกัน นำไปสู่การอธิบายแรงจูงใจของการก่อการร้ายที่ต่างกันด้วย เมื่ออธิบายความเข้าใจแรงจูงใจการก่อการร้ายทางไซเบอร์ จึงไม่ได้มีการให้คำจำกัดความที่ชัดเจน

ปัญหาในการจัดการกับการก่อการร้าย

สิ่งที่ค้นพบจากการวิจัยพบว่า ปัญหาที่สำคัญของการต่อต้านการก่อการร้ายเกิดจากแนวคิดของการก่อการร้าย และความหมายและความไม่รู้ถึงความรุนแรงอันเกิดจากการก่อการร้าย

ของคนในประเทศใครคือผู้ก่อการร้าย และอะไรคือการก่อการร้าย เนื่องจากภัยการก่อการร้ายเป็นเรื่องไกลตัวและยังไม่มีการสร้างความตระหนักอย่างชัดเจน ดังนั้น มุมมองต่อการก่อการร้ายของแต่ละประเทศ มีการให้ความหมายและแนวคิดไปตามทิศทางของตนเอง ผู้ก่อการร้ายในมุมมองของประเทศหนึ่ง มองแตกต่างกับอีกประเทศหนึ่ง ที่มองว่าเป็นนักต่อสู้เพื่ออิสรภาพก็เป็นได้ การกระทำของการก่อการร้ายก็จะมีการแสดงออกที่แตกต่างกัน การกระทำที่ชัดเจนระหว่างการกระทำที่โหดเหี้ยม ไม่คำนึงถึงกฎหมายโดยบุคคลใดหรือกลุ่มใด กับการกระทำที่เป็นการต่อสู้อันชอบธรรมของคนในประเทศที่ถูกกดขี่ข่มเหง จากอิทธิพลหรือการยึดครองของชาติมหาอำนาจ บางประเทศมีชนกลุ่มน้อยที่เขาคิดว่าไม่ได้รับความเป็นธรรม ภายในวิถีชีวิตและการปกครองภายใต้รัฐจึงดำเนินการชุมชุมประท้วงเรียกร้องและสร้างเงื่อนไขทางการเมืองขึ้น จนเป็นสาเหตุให้รัฐเข้าดำเนินการด้วยวิธีการต่าง ๆ เช่น การตอบโต้ หรือปราบปรามโดยใช้กำลังเข้าสลายการชุมชุมหรือการเรียกร้องดังกล่าว เมื่อความรุนแรงเพิ่มมากขึ้น แน่นอนว่าประชาชนไม่มีกำลังเพียงพอที่จะต่อสู้กับกำลังของทหารหรือตำรวจได้ จึงจัดตั้งเป็นองค์กรหรือกองกำลังของประชาชน ซึ่งกองกำลังเหล่านี้เองก็ถูกมองว่าเป็นผู้ก่อการร้ายในรัฐหรือประเทศนั้น ในความเข้าใจของกองกำลังหรือองค์กรที่จัดตั้งขึ้นก็มีความเข้าใจว่านี่เป็นการกระทำเพื่ออิสรภาพ สิ่งที่จะต้องพิจารณาคือ การศึกษารากเหง้าหรือปัญหาที่เกิดจากความต้องการของกลุ่มชน องค์กรหรือกองกำลังประชาชนที่ปฏิบัติการว่ามีวัตถุประสงค์ใด มีเหตุผลทางการเมืองประกอบในการกระทำหรือไม่และเป้าหมายสุดท้ายขององค์กรหรือกลุ่มเคลื่อนไหวคืออะไร เพื่อจะสามารถดำเนินการ ป้องกัน ต่อต้านหรือปราบปรามการกระทำได้ตรงจุดหรือตรงเป้าหมายในอีกประเด็นคือนโยบายการต่อต้านการก่อการร้ายของประเทศมีความแตกต่างกันในการปฏิบัติต่อการกระทำของผู้ก่อการร้าย หลายประเทศมีวิธีการตอบโต้ต่อการกระทำของผู้ก่อการร้ายในขั้นสูงสุดหรือต่อต้านการก่อการร้ายอย่างเปิดเผย แต่บางประเทศเลือกที่จะติดต่อหรือวางตัวเป็นกลางกับผู้ก่อการร้ายหรือองค์กรก่อการร้ายซึ่งอาจมีผลประโยชน์ร่วมกัน

ประเด็นต่อมา คือ ประเทศไทยปกครองแบบเสรีประชาธิปไตยการให้เสรีภาพไม่ว่าจะด้านใดๆ เป็นผลให้สิทธิเสรีภาพของประชาชนไม่มีขีดจำกัด โดยเฉพาะเสรีภาพทางสื่อและการใช้สังคมออนไลน์ สื่อสารมวลชนเป็นตัวกลางในการนำเสนอข่าวสารความเป็นจริงให้กับประชาชน หากสื่อมีอิสระสูงก็อาจเป็นเครื่องมือที่ชี้นำให้ประชาชนหรือการนำเสนอข่าวสารบางอย่าง หากเอนเอียงไปในทางใดทางหนึ่งก็อาจเป็นเครื่องมือต่อผู้ก่อการร้ายในการรู้ถึงความเคลื่อนไหวและตอบโต้รัฐได้ง่ายขึ้น ประเด็นที่ต้องพิจารณาคือ การกระจายสื่อและการควบคุมสื่อของรัฐบาล หากให้อิสระมากเกินไปก็เกินความเหมาะสม หรือหากควบคุมมากเกินไปก็ไม่สามารถเป็นตัวกลางในการนำเสนอข่าวสารได้อย่างแท้จริง

ประเด็นสุดท้ายคือ สิทธิเสรีภาพของประชาชน เป็นสิ่งที่ต้องพิจารณา ปัจจัยที่เกี่ยวข้องกับแรงจูงใจในการก่อการร้ายทางไซเบอร์ด้วยประเทศไทยเป็นประเทศเปิดเสรี เปิดรับนักท่องเที่ยวและมีนโยบายส่งเสริมให้เกิดการท่องเที่ยวในทุกที่โดยไม่มีข้อจำกัด ดังนั้นจึงเป็นเหมือนสวรรค์ของผู้ก่อการร้าย อีกทั้งการส่งเสริมการเปิดใช้อินเทอร์เน็ตในทุกที่ ทำให้ประชาชนขาดการตระหนักรู้ในเรื่องของการใช้ไซเบอร์ การก่อการร้ายทางไซเบอร์นั้นผู้ก่อการร้ายจะใช้เครื่องมือทางไซเบอร์ที่หาง่ายและใช้เครื่องมือได้ทุกที่ ไม่ว่าจะเป็นโทรศัพท์มือถือ แท็บเล็ต คอมพิวเตอร์ ที่สามารถเชื่อมต่ออินเทอร์เน็ตได้ทำให้คนเข้าถึงได้ง่ายและเชื่อง่ายขึ้น แรงจูงใจที่นำไซเบอร์มาก่อการร้าย ผู้เชี่ยวชาญมองว่าเป็นเรื่องเงินเป็นสำคัญ รองลองมาเป็นเรื่องของแนวคิด อุดมการณ์ทางการเมืองหรือทางศาสนา หรือแม้แต่ความไม่พอใจต่อหน่วยงานหรือองค์กร แต่ปัจจัยที่สำคัญที่ผู้เชี่ยวชาญมองต่างกันคือ แรงจูงใจที่สำคัญต่อการกระทำที่เป็นการก่อการร้ายจะต้องเป็นการกระทำที่มาจากแรงจูงใจทางเมืองเป็นสำคัญ จึงเห็นได้ว่า ความเข้าใจในความหมายของการก่อการร้ายที่แตกต่างกัน นำไปสู่การอธิบายแรงจูงใจของการก่อการร้ายที่ต่างกันด้วย เมื่ออธิบายความเข้าใจแรงจูงใจการก่อการร้ายทางไซเบอร์ จึงไม่ได้มีการให้คำจำกัดความที่ชัดเจน

ความก้าวหน้าทางไซเบอร์

โลกไซเบอร์ (Cyber world) เปรียบเหมือนสมองของร่างกายมนุษย์ที่มีความเชื่อมโยงของทุกส่วนของร่างกาย ขาดสิ่งใดสิ่งหนึ่งไม่ได้ในปัจจุบัน ไซเบอร์ก็เป็นส่วนหนึ่งที่มีเครือข่ายเชื่อมโยงตั้งแต่ในระดับประเทศจนถึงระดับนานาชาติ ความรู้ทางเทคโนโลยีและเครือข่ายรวมทั้งการปฏิบัติการ ด้านเครือข่ายคอมพิวเตอร์ เป็นสิ่งจำเป็นในปัจจุบัน มนุษย์เป็นสัตว์โลกประเภทหนึ่งที่มีพัฒนาการของความคิดได้อย่างก้าวกระโดด มีภูมิปัญญาเหนือกว่าสิ่งมีชีวิตอื่น ๆ ใดบนโลกใบนี้ มนุษย์สามารถนำเอาสติปัญญามาใช้เพื่อหาทางในการเอื้อประโยชน์ให้แก่ตนเอง ซึ่งจะมากน้อยขนาดไหนขึ้นอยู่กับจิตสำนึกและวิธีคิดของแต่ละบุคคล การที่มนุษย์เป็นนักประดิษฐ์มาตั้งแต่ยุคโบราณ นอกจากความทรงภูมิปัญญาของมนุษย์แล้ว ก็ยังมีความคิดที่ต้องการจะแสวงหาโอกาสที่ดีกว่าปกติ มนุษย์คิดสร้างเทคโนโลยี เพื่อให้มีชีวิตที่สะดวกสบาย รวดเร็ว ทำให้เกิดเทคโนโลยีต่างๆโลกไซเบอร์ (Cyber world) เป็นโลกไร้พรมแดนที่ผู้คนสามารถใช้เทคโนโลยีอย่างไรขีดจำกัด ปัจจุบันสถานการณ์ทางอาชญากรรมที่มีแนวโน้มของความรุนแรงเพิ่มมากขึ้น ซึ่งอาจนำไปสู่การก่อการร้ายได้ สถานการณ์ที่ต้องมีความระแวดระวังมากจากสถานการณ์ความมั่นคง มีความอ่อนไหวและซับซ้อนมากยิ่งขึ้นเมื่อโลกไซเบอร์มีขนาดใหญ่ขึ้น

ผลการวิเคราะห์ข้อมูลจากการสัมภาษณ์ประเภท: ความก้าวหน้าทางไซเบอร์ ดังนี้

“ความก้าวหน้าทางไซเบอร์เกิดจากจิตนาการ อะไรที่ไม่น่าเกิดก็สามารถเกิดขึ้นได้ ไม่ว่าจะเป็นในแง่ของนวัตกรรม ในแง่ของเทคโนโลยี จะเป็นด้านบวกหรือด้านลบ ไซเบอร์ถือว่าเป็นการใช้งานในด้านลบและหนักกว่านั้นถือว่าเป็นสิ่งไม่สามารถเห็นได้ของทุกหน่วยงานของทุกคน ถ้าหน่วยงานนั้นไม่รู้เท่าทัน ไม่เข้าใจภัยก็จะเกิดขึ้นได้ตลอดเวลา” (มนตรี, นามสมมติ, สัมภาษณ์, 11 พฤษภาคม 58)

“ไซเบอร์คือ อินเทอร์เน็ต เป็นการเชื่อมต่อสื่อสาร ความก้าวหน้าคือ เรามีเทคโนโลยีที่สามารถเชื่อมต่อกันได้อย่างสะดวกรวดเร็วขึ้น ทำให้ทุกคนติดต่อกันได้ไม่ว่าจะอยู่ที่ไหนในโลก ความก้าวหน้าทางไซเบอร์คือ เศรษฐกิจดิจิตอล (Digital economy) กำลังผลักดันของทุกภาคในประเทศไทย เป็นอีกปัจจัยหนึ่งที่ทำให้อินเทอร์เน็ตเข้าสู่คนทุกกลุ่มในประเทศได้” (วิเชียร, นามสมมติ, สัมภาษณ์, 26 พฤษภาคม 58)

“ความก้าวหน้าทางไซเบอร์คือโลกของอินเทอร์เน็ต ต้องย้อนกลับไปดูว่าเริ่มมีการใช้งานอินเทอร์เน็ต มีการติดต่อสื่อสารแลกเปลี่ยนข้อมูล ระหว่างคอมพิวเตอร์ไปสู่คอมพิวเตอร์ หรือระหว่างคนไปสู่คน โดยใช้อุปกรณ์ เริ่มที่จะเป็นจุดกำเนิดของโลกเทคโนโลยีโลกไซเบอร์ ไซเบอร์กับอินเทอร์เน็ตถือว่ามีความใกล้เคียงกัน ความก้าวหน้าทางไซเบอร์มีหลายปัจจัย ความเร็วของอินเทอร์เน็ตยิ่งมีความเร็วสูงยิ่งส่งผลต่อความก้าวหน้าทางไซเบอร์ แพลตฟอร์ม (Platform) หรือระบบปฏิบัติการที่ใช้ของเทคโนโลยีที่มีการพัฒนาจาก 3.0 ไปเป็น 4.0 และการเข้าถึงของอุปกรณ์ต่าง ๆ ที่สามารถเข้าถึงได้ทุกทีและมีความสามารถและมีประสิทธิภาพ” (มงคล, นามสมมติ, สัมภาษณ์, 27 พฤษภาคม 58)

“ความก้าวหน้าทางไซเบอร์เป็นสิ่งที่เราควรให้ความสำคัญอย่างมากเพราะในอนาคตต่อไปทุกอย่างจะเป็นดิจิตอลมากยิ่งขึ้น ในอนาคตทุกอย่างจะไม่ต้องมานั่งหน้าจอคอมพิวเตอร์ ทุกอย่างจะใช้ระบบคอมพิวเตอร์ใช้ปุ่มกดเยอะ เหมือนมันเป็นความนิยม ดูจากโทรศัพท์เข้าถึงได้เร็ว เพราะฉะนั้นคิดว่าความก้าวหน้าทางไซเบอร์จะมีมากขึ้นเรื่อยๆ แบบก้าวกระโดด ไซเบอร์เป็นสิ่งที่เราจะต้องตามให้ทัน ไซเบอร์คือทั้งหมดที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ระบบดิจิตอล ทุกอย่างมีส่วนในชีวิตประจำวันของเรา หรือแม้กระทั่งการเรียนการสอน เครือข่ายครอบคลุม อย่างระบบโทรศัพท์มือถือสามารถครอบคลุมใช้ได้หมด จากการลงทะเบียนหรือแม้กระทั่งภาคการเกษตรตอนนี้สามารถเข้าถึงและรู้ข่าวสารรู้การสื่อสารได้หมด (สัญญา, นามสมมติ, สัมภาษณ์, 10 กรกฎาคม 58)

“ความก้าวหน้าทางไซเบอร์ปัจจุบันค่อนข้างให้น้ำหนักในเรื่องของเทคโนโลยี ความก้าวหน้าทางเทคโนโลยีแทบไม่น่าเป็นห่วง เพราะว่าเป็นความก้าวหน้าที่เห็นเด่นชัดว่ามี

ความก้าวหน้าตลอดค่อนข้างจะเน้นไปทางด้านใดด้านหนึ่ง แต่ในมุมเรื่องของไซเบอร์เป็นมุมเรื่องของความเข้าใจของการบริหารจัดการอุปกรณ์ที่ไปทำเรื่องไซเบอร์" (วรรณี, นามสมมติ, สัมภาษณ์, 13 กรกฎาคม 58)

"ความก้าวหน้าทางไซเบอร์คือ เทคโนโลยี คนช่างคิดช่างแก้ปัญหาเพื่อให้เกิดสิ่งต่าง ๆ ไซเบอร์ก็คิดมาเพื่อจะแก้ปัญหาอะไรหลาย ๆ อย่าง เพื่อบันเทิงเริงรมย์แต่คนก็ไปใช้ในทางที่ผิดกันเดิมทีคนใช้วิธีการแลกเปลี่ยน จนพัฒนาไปเรื่อย ๆ เพื่อแก้ปัญหาในหลายประเด็น ความก้าวหน้าทางไซเบอร์เกิดจากการพัฒนาเทคโนโลยี พัฒนาเพื่อรองรับการเติบโต รองรับปัญหาของมนุษย์ทุกครั้งที่มีการพัฒนาก็จะเกิดปัญหาตามมา" (สุรศักดิ์, นามสมมติ, สัมภาษณ์, 22 กรกฎาคม 58)

"ความก้าวหน้าทางไซเบอร์คือ คนช่างคิดแก้ปัญหาเพื่อให้เกิดสิ่งต่าง ๆ ไซเบอร์ก็คิดมาเพื่อจะแก้ปัญหาอะไรหลาย ๆ อย่าง เพื่อติดต่อสื่อสาร เพื่อบันเทิงเริงรมย์ แต่คนใช้ไปในทางที่ผิดกัน ความก้าวหน้าทางไซเบอร์เกิดจากความก้าวหน้าทางเทคโนโลยี พัฒนาเพื่อรองรับการเติบโต รองรับปัญหาของมนุษย์แต่ขณะเดียวกันทุกครั้งที่มีการพัฒนาเกิดขึ้นปัญหาก็จะตามมาในทุกประการ ไซเบอร์จะเป็นเหรียญสองด้านเสมอ ความก้าวหน้าทางไซเบอร์คือการพัฒนาทางเทคโนโลยีเพื่อมาแก้ปัญหามนุษย์ ขณะเดียวกันก็สร้างปัญหาให้กับมนุษย์เช่นเดียวกัน" (จุติ, นามสมมติ, สัมภาษณ์, 7 กันยายน 58)

บทสรุปว่า ความก้าวหน้าทางไซเบอร์คือ เทคโนโลยีที่มีอินเทอร์เน็ต เพื่อเชื่อมต่อการสื่อสารได้ทุกที่ทุกเวลา ไม่ว่าจะอยู่ที่ใดบนโลก สะดวก รวดเร็ว และไซเบอร์มีความสำคัญอย่างมากต่อการดำรงชีวิตในปัจจุบัน โดยมีเครื่องมือที่ใช้ในการติดต่อสื่อสาร ไม่ว่าจะเป็น คอมพิวเตอร์ โทรศัพท์มือถือหรือแท็บเล็ต เป็นต้น ความก้าวหน้าทางไซเบอร์ต้องมีความเร็วสูง มีระบบปฏิบัติการที่ดีและมีประสิทธิภาพและสามารถเข้าถึงได้

การแสวงหาโอกาสในการก่อการร้ายทางไซเบอร์

การแสวงหาโอกาสในการก่อการร้ายทางไซเบอร์ เป็นการกระทำที่อาศัยช่องโหว่หรือจุดอ่อนที่ไม่มีการป้องกันของไฟร์วอลล์ ทำให้แฮกเกอร์มีช่องทางในการโจมตีระบบที่ได้กำหนดเป็นเป้าหมายไว้ การวิเคราะห์โอกาสหรือช่องทางในการกระทำความผิดจะเกิดหลังจากผู้ก่อการร้ายสร้างแรงจูงใจของตนเองในการก่อเหตุครั้งนั้น

ผลการวิเคราะห์ข้อมูลจากการสัมภาษณ์ประเภท: การแสวงหาโอกาสในการก่อการร้ายทางไซเบอร์ดังนี้

"ประเทศไทยมีทรัพยากรที่อุดมสมบูรณ์ ผู้ก่อการร้ายเข้ามาอยู่ในเมืองไทยได้ง่ายมาก คนไทยเป็นมิตรที่ดี เป็นสวรรค์ของผู้ก่อการร้ายและเป็นช่องทางที่เข้ามา ไม่ว่าจะเกิดอะไรขึ้นก็ตามคน

ไทยประนีประนอม เราไม่รู้เท่าทันและไม่มีใครบอกให้รู้เท่าทัน การคอร์รัปชั่นทำให้สังคมไทยผิดเพี้ยน มีแต่คอร์รัปชั่นตลอดเวลา ไม่เคารพสิทธิ์ ไม่มีวินัย ไม่สนใจโลกภายนอก เงินหรือไซฟ่อนเงิน เป็นสิ่งสำคัญ การหลอกให้โอนเงินหรือโกงเงินโดยมองเรื่องของเศรษฐกิจเป็นหลัก" (มนตรี, นามสมมติ, สัมภาษณ์, 11 พฤษภาคม 58)

"การแสวงหาโอกาสในการก่อการร้ายมีหลายปัจจัย 1.อยากลองอยากรู้ ว่าหากขโมยข้อมูลได้ก็จะภูมิใจ 2. การไม่พอใจต่อหน่วยงานนั้นคนนั้น เช่น ถูกไล่ออก หรือไม่ชอบหน้าคนนี้ เพราะมีการทะเลาะเบาะแว้งกันมาก่อน 3.ปัจจัยเรื่องเงิน" (วิเชียร, นามสมมติ, สัมภาษณ์, 26 พฤษภาคม 58)

"ประเทศไทยมีนโยบายส่งเสริมให้เข้าถึงอินเทอร์เน็ตได้มากขึ้น เหมือนเป็นสวรรค์ของผู้ไม่ประสงค์ดีทางไซเบอร์ คือมีการปล่อยให้มีการใช้และไม่มีการควบคุมก็จะทำได้ง่าย สอง ประชาชนยังขาดความตระหนักรู้ ไม่ใช้งานอย่างระแวดระวัง ยังประมาทในเรื่องไซเบอร์อยู่ สาม เรายอมให้ข้อมูลง่ายๆ คือการโชว์ข้อมูล เช่นการใช้สังคมออนไลน์เปิดเผยระบุตัวตน แสดงออก หรือให้ทุกคนเชื่อมต่ออุปกรณ์ของเราด้วยความยินยอม โดยการโพสต์ (แสดงความคิดเห็น) หรือเช็คอิน (ระบุตัวตน) ทำให้ผู้ไม่ประสงค์ดีเข้ามาติดตามเราได้ สี่ การใช้เทคโนโลยีอย่างขาดความระมัดระวัง ห้า การใช้แพลตฟอร์มในเมืองไทยการถูกโจมตีทางไซเบอร์ยังไม่รุนแรงมากนัก แต่ก็จะมีช่องโหว่มากส่วนในประเด็นของโครงสร้างพื้นฐาน ยังไม่ถึงขั้นนั้นเพราะเราไม่ได้ใช้การควบคุมโดยคอมพิวเตอร์ทั้งหมดยังมีระบบอนาล็อกอยู่" (มงคล, นามสมมติ, สัมภาษณ์, 27 พฤษภาคม 58)

" แรงจูงใจที่สำคัญเป็นเรื่องของอุดมการณ์เป็นหลัก เกี่ยวข้องกับศาสนา อุดมการณ์ความเท่าเทียมกันของมนุษย์ เรื่องที่สอง เงิน เพราะทำแล้วได้ประโยชน์" (สัญญา, นามสมมติ, สัมภาษณ์, 10 กรกฎาคม 58)

"ในสถานการณ์ปัจจุบัน คิดว่าด้านหนึ่งเป็นเรื่องของเงิน เพราะสังคมมีด้านนี้เป็นสังคมทุนนิยม เป็นปัจจัยหนึ่งที่ทำให้ทุกคนมองประเด็นนี้ ในบางส่วนเรื่องของการเมือง คงเป็นไปตามสถานการณ์ คงไม่ได้เกิดขึ้นตลอดเวลาขึ้นอยู่กับสถานการณ์ในช่วงนั้น เพื่อใช้เทคโนโลยีในปัจจุบันในแง่ของการเชื่อมต่ออินเทอร์เน็ต สร้างเหตุการณ์ขึ้นมาบางอย่างเป็นเรื่องของการก่อการร้าย" (วรรณี, นามสมมติ, สัมภาษณ์, 13 กรกฎาคม 58)

"ผู้ก่อการร้ายทั่วไป กลวิธีในการก่อการร้าย คือ การใช้ทุกอย่างที่ใช้ได้และใช้เทคโนโลยีล่าสุด จะนำมาใช้ประโยชน์ ไซเบอร์ก็เช่นเดียวกัน เหมือนเป็นอีกขั้นตอนหนึ่งของการก่อการร้าย แรงจูงใจอันหนึ่งจะใช้เครื่องมือทุกอย่างที่หาได้และแรงจูงใจที่ใช้ไซเบอร์คือโทรศัพท์มือถือ เพราะหาง่ายและตามหาได้ยากและประเทศไทยมีผู้ใช้อินเทอร์เน็ตมากขึ้น อีกอย่างคือเมื่อข้อมูลถูกโพสต์ในไซเบอร์ ทุกคนก็จะเชื่อ สามจังหวัดชายแดนภาคใต้หันมาใช้ไซเบอร์กันมากขึ้น ใช้ในการติดต่อ

ประสานงานหรือใช้เป็นเครื่องมือ เช่น จะโอนเงินหรือทำธุรกรรมต่าง ๆ แต่ก็ไม่ได้แสดงออกกว่าเชื่อมโยงกับกลุ่มก่อการร้ายอื่นๆ เช่น อัลเคด้า เจไอที่อินโดนีเซีย แต่โดยวิธีการก็สามารถเป็นไปได้ เช่นเว็บไซต์สอนทำระเบิด หรือวิธีการอย่างอื่นให้คนสามารถเข้าไปดูได้หรือสมาชิกในกลุ่มเข้าไปดูได้ วิธีการแนวคิดในประเด็นเรื่องของการถูกโจมตีโครงสร้างพื้นฐาน ประเทศไทยยังไม่ถึงขั้นนั้น ถ้าเทียบกับของสหรัฐอเมริกา เพราะสหรัฐอเมริกามีอาวุธนิวเคลียร์และมีโรงไฟฟ้านิวเคลียร์ ซึ่งถ้าโดนเจาะระบบก็เป็นเรื่องใหญ่ ประเทศไทยไม่มี ถึงแม้ประเทศไทยจะมีเตาปฏิกรณ์นิวเคลียร์ก็เป็นเพียงแค่การศึกษา แต่ถ้าถามว่าควรป้องกันไหมก็ควรป้องกันดีกว่า ประเทศไทย ผู้ก่อการร้ายหรืออาชญากรจะไม่ค่อยอยากทำอะไร เพราะไทยเป็นจุดศูนย์กลาง การขนส่งในภูมิภาค ไทยจะเป็นแหล่งส่งเสริมการท่องเที่ยวจะเข้าจะออกได้ง่าย เพราะฉะนั้นจะชอบใช้ไทยเป็นที่กบดานจึงไม่ค่อยอยากทำอะไรในไทย ถ้าไม่จำเป็นจริง ๆ แต่ถ้าถามว่าทำได้ไหมก็ทำได้" (สมชัย, นามสมมติ, สัมภาษณ์, 16 กรกฎาคม 58)

"การแสวงหาโอกาสผู้ก่อการร้ายใช้ทุกทาง คอยเฝ้าติดตามไม่ต้องทำไรมาก พัฒนาเฉย ๆ ว่าทำได้ไหม การก่อการร้ายที่ไหนก็ทำได้ เพียงแค่จะทำหรือเปล่า ทำได้เกิดได้ แต่ส่วนใหญ่ไม่ทำ" (สุรศักดิ์, นามสมมติ, สัมภาษณ์, 22 กรกฎาคม 58)

"การแสวงหาโอกาสในการก่อการร้าย ผู้ก่อการร้ายต่างกับโจรนิดเดียว ผู้ก่อการร้ายทำโดยมีจุดประสงค์ ทำอะไรก็ได้ที่ทำให้เกิดเป็นข่าวแก่ฝ่ายตรงกันข้าม โดยทำแล้วต้องให้บรรลุตามวัตถุประสงค์ที่วางไว้ ทำเพื่อความพอใจ การกระทำอะไรที่ทำให้เกิดผลทางการเมือง ตามอุดมการณ์ที่เค้าวางไว้ ทั้งหมดเป็นเรื่องจิตวิทยาที่กล่อมคนให้ไปทำ สร้างคอมพิวเตอร์เพื่อดึงดูดคน เพราะฉะนั้น การที่ก่อการร้ายทำไม่ได้มุ่งหวังประโยชน์ ได้เงินก็ดี แต่ก็ยังไม่ใช่หลักการวัตถุประสงค์ของการก่อการร้าย ไซเบอร์เป็นเครื่องมือหนึ่งของอีกหลายๆ วิธีการ การก่อการร้ายทางไซเบอร์เป็นการก่อการร้ายที่ใช้ทุนน้อยที่สุด ได้ผลดีที่สุด เป็นข่าวดังที่สุดและกว้างขวางที่สุด และใครก็ได้ทำได้ ใครหมายถึงคนรูปร่างไหนก็ทำได้ ต้องมีความรู้เรื่องนั้นด้วย ไซเบอร์เป็นสนามหนึ่งของการก่อการร้าย" (จุติ, นามสมมติ, สัมภาษณ์, 7 กันยายน 58)

"ประเทศไทยขาดคนที่มีความรู้ทางไซเบอร์หรือมีความรู้ทางไซเบอร์น้อยมาก เนื่องจากคนที่มีศักยภาพเมื่อส่งไปเรียนต่อต่างประเทศก็จะไม่กลับมา เนื่องจากต่างประเทศให้ค่าตอบแทนที่สูงกว่า เพราะประเทศไม่ได้สร้างเกียรติภูมิ ศักดิ์ศรี อีกทั้งไม่มีคนทำหน้าที่ดูแลระบบ" (อวยพร, นามสมมติ, สัมภาษณ์, 20 ตุลาคม58)

บทสรุป ผู้ก่อการร้ายแสวงหาโอกาสจากประเทศไทยในหลายด้านเพื่อก่อการร้าย ประเด็นสำคัญที่พบได้คือ ประเทศไทยเป็นประเทศที่เปิดเสรีและประชาชนมีการต้อนรับ

ชาวต่างประเทศ มีการยิ้มแย้มแจ่มใสและต้อนรับผู้อื่นจึงเหมือนกับเป็นสวรรค์ของผู้ก่อการร้าย ส่วนใหญ่ผู้ก่อการร้ายจะใช้ประเทศไทยเป็นฐานในการเตรียมการก่อการร้ายไปยังประเทศที่สาม หรือประเทศที่เป็นเป้าหมายมากกว่า และประเทศไทยไม่มีมาตรการในการป้องกันความปลอดภัยทางไซเบอร์ ประชาชนยังไม่ความตระหนักรู้ต่อภัยคุกคามทางไซเบอร์ จึงทำให้มีการใช้อย่างไม่ระแวดระวัง

การนำไซเบอร์มาเป็นเครื่องมือในการก่อการร้าย

ผลการวิเคราะห์ข้อมูลจากการสัมภาษณ์ประเภท: การนำไซเบอร์มาเป็นเครื่องมือในการก่อการร้ายดังนี้

“ภัยคุกคามทางไซเบอร์เหมือนกับภูเขาน้ำแข็ง ส่วนหนึ่งอยู่บนน้ำ อีกส่วนอยู่ใต้น้ำ ส่วนที่อยู่บนน้ำก็จะมีเทคโนโลยีเข้ามาช่วย ส่วนที่อยู่ใต้น้ำ มันก็จะใหญ่กว่าส่วนที่อยู่ด้านบน บางส่วนก็คาดเดาได้เอง แต่บางส่วนเทคโนโลยีอาจจะมาช่วยได้ เทคโนโลยีมาสนับสนุน ภัยทางไซเบอร์เป็นภัยที่เราสามารถสร้างเองได้ มันมีเครื่องมือช่วย เช่น Firewall IPE IBS แต่ละอย่างจำเป็นต้องซื้อเครื่องมือมาป้องกัน กลายเป็นคนที่สร้างภัยการก่อการร้าย ก็คือผู้ขายเครื่องมือป้องกัน กลายเป็นคนที่สร้างภัยการก่อการร้ายขึ้นมา ตอนนี้ทุกอย่างเข้ามาโดยไม่ได้กลั่นกรอง การให้การศึกษา เด็กที่ลืมตาขึ้นมาดูโลกจะให้เค้าตระหนักได้อย่างไร ประเทศไทยต้องมีคนกลางมาช่วย แบบไหนจำเป็นต้องควบคุม แบบไหนต้องทำให้สะดวกขึ้น เพราะมันเป็นไปไม่ได้ที่จะทำให้ประชากร 70 ล้านคนรู้เท่าทัน รัฐบาล หน่วยงานกลาง หน่วยงานที่จัดตั้งขึ้นเพื่อมีหน้าที่รับผิดชอบ ต้องเห็นแทนคน 70 ล้านคนอะไรที่ปลอดภัย อะไรที่ไม่ปลอดภัย เพราะฉะนั้น ต้องอาศัยความพร้อมของคนไทย รัฐบาลต้องอาศัยสิ่งอำนวยความสะดวกที่ควบคุมได้ อะไรที่ขัดขวางได้ ซึ่งจะต้องทำตั้งแต่ช่องทางซึ่งจะต้องมีคนปกป้องให้ปลอดภัย ซึ่งประเทศไทยต้องทำให้ได้แบบนี้ รัฐบาลจะกล่าวว่าเอกชนพร้อมให้ทำไปก่อนไม่ได้” (มนตรี, นามสมมติ, สัมภาษณ์, 11 พฤษภาคม 58)

“เครื่องมือทางไซเบอร์คือ เครื่องมือ (Tool) ของสังคมออนไลน์ที่ติดต่อสื่อสารกัน แอฟริเคชั่น (Application) บนโทรศัพท์มือถือ ผู้ก่อการร้ายใช้ช่องทางอื่นผ่านกล่องข้อความ ไลน์ ของอินเทอร์เน็ต สามารถติดต่อสื่อสารกันได้ทั่วโลก ทำให้ยากต่อการตรวจสอบ เป็นช่องทางการสื่อสารระหว่างบุคคลกับบุคคล และเทคโนโลยีต้องรักษาความปลอดภัยของข้อมูลรัฐ รัฐบาลไม่สามารถตรวจสอบได้ สังคมออนไลน์ก็เป็นช่องทางหนึ่งในการก่อการร้ายได้สำหรับโครงสร้างพื้นฐาน ในจำพวกฮาร์ดแวร์ยังไม่ค่อยมีปัญหาเท่าที่ควร มีการอัพเดทตลอดเวลา ส่วนใหญ่จะเจอในสังคมออนไลน์และไวรัสต่าง ๆ จะมาจากสังคมออนไลน์ส่วนเรื่องการหลอกลวงในเมืองไทย จะไม่ใช่การโจมตีทางไซเบอร์โดยตรง เช่นไวรัส หรือโจมตีผ่านเครือข่ายโดยตรง เป็นกลลวงทาง

สังคมหรือทางวิศวกรรม ส่วนใหญ่เป็นการชักจูงใจ ขาดความตระหนักว่าเป็นภัยอันตราย ปัจจุบันที่มีชื่อเสียงมากที่สุดคือ Ransomware ถือเป็นการโจมตีทางไซเบอร์อย่างหนึ่ง" (วิเชียร, นามสมมติ, สัมภาษณ์, 26 พฤษภาคม 58)

"เครื่องมือหมายถึงโทรศัพท์มือถือ สามารถติดต่ออินเทอร์เน็ตได้ คอมพิวเตอร์ได้ คอมพิวเตอร์ได้ ระบบคอมพิวเตอร์ทั้งหลายได้หมด ที่มีการติดต่อผ่านระบบ แต่การก่อการร้ายมองในแง่ของการก่อการร้ายทางไซเบอร์ (Cyber Terrorism) ก็สามารถเชื่อมอินเทอร์เน็ตช่วยในการก่อการร้าย โทรศัพท์หรือคอมพิวเตอร์ สามารถขโมยข้อมูลได้หมด ผู้ก่อการร้ายต้องมีความรู้ แต่ที่สำคัญคือการเข้าถึง ผู้ก่อการร้ายต้องเข้าถึงได้เพราะมีราคาถูก" (มงคล, นามสมมติ, สัมภาษณ์, 27 พฤษภาคม 58)

"เครื่องมือที่ใช้ในการก่อการร้ายสมัยนี้ค่อนข้างหาได้ง่าย ใครก็สามารถทำได้สมัยนี้เรามีช่องทางในการเข้าถึงอินเทอร์เน็ต ก็สามารถหาเจอได้ไม่ยาก ตอนนี้ยังมีกรณีเด็กนักเรียนประถมศึกษาใช้เครื่องมือนี้และไปทำอันตรายต่อระบบต่างๆ ซึ่งมีความเป็นไปได้" (สัญญา, นามสมมติ, สัมภาษณ์, 10 กรกฎาคม 58)

" โลกเจริญขึ้น เมืองไทยเจริญขึ้น การก่อการร้ายอุปกรณ์หรือเทคโนโลยีที่ไหนก็ทำเหมือนกันไปหมด ถามว่าอะไรเป็นเครื่องมือ ก็คือสิ่งที่ผู้ก่อการร้ายคิดมาทั้งหมด อุปกรณ์ทั้งหมด อะไรก็ได้ขอให้เป็นการนำมาใช้ในการก่อการร้ายใช้ได้ทั้งหมดถ้าคิดจะทำ" (สุรศักดิ์, นามสมมติ, สัมภาษณ์, 22 กรกฎาคม 58)

บทสรุปเครื่องมือทางไซเบอร์ที่นำมาใช้ในการก่อการร้ายในปัจจุบัน คือ โทรศัพท์มือถือ แท็บเล็ต คอมพิวเตอร์ หรืออุปกรณ์ที่สามารถเชื่อมต่ออินเทอร์เน็ตได้และสามารถใช้งานได้ทุกที่อย่างสะดวกและรวดเร็ว การเชื่อมต่ออินเทอร์เน็ตที่มีความเร็วสูงและมีระบบปฏิบัติการที่มีประสิทธิภาพจะช่วยการปฏิบัติการได้อย่างมีประสิทธิภาพ นอกจากนี้ ประเด็นสำคัญที่ค้นพบคือการใช้สังคมออนไลน์ทั้งกล่องข้อความ ไลน์ ทวิสเตอร์ เป็นต้น เพื่อใช้ในการติดต่อสื่อสารกันทั่วโลกและใช้เป็นช่องทางในการเผยแพร่แนวคิด วิดีโอ เพื่อให้เกิดความเชื่อ ต่อบุคคล ต่อสมาชิกในกลุ่ม เชื่อมโยงไปยังกลุ่มหรือปลุกระดมคนเพื่อนำมาสู่การก่อการร้ายได้

การก่อการร้ายทางไซเบอร์และการต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย

ผลการวิเคราะห์ข้อมูลจากการสัมภาษณ์ประเภท: การก่อการร้ายทางไซเบอร์ (Cyber) และการต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทยดังนี้

"การก่อการร้ายทางไซเบอร์ ในประเทศไทยเรื่องเงิน เรื่องเศรษฐกิจเป็นส่วนใหญ่ อีกส่วนเป็นเรื่องของการต่อสู้ด้วย การปฏิบัติการข้อมูลข่าวสาร (Information Operation IO)ใช้ข้อมูล

ต่อสู้กัน แต่ก็สามารถใช้การปฏิบัติการข้อมูลข่าวสาร ทำลายประเทศได้เช่น มีประเทศอื่นใช้ข้อมูลโจมตีประเทศไทย ประเทศไทยอาจไม่รู้ ไทยมีช่องทางในการเสพข้อมูลต่างๆ ได้ ประเทศไทยไม่ได้ปิดกั้นทุกอย่างด้วยเหตุผลของ พระราชบัญญัติการบังคับใช้กฎหมายไม่เข้มแข็ง กฎหมายเรื่องข้อมูลข่าวสารของไทยยังอ่อนแอ ส่วนใหญ่เป็นเรื่องของการโจมตีทางไซเบอร์ยังไม่มีประเด็นเรื่องสงครามข้อมูลข่าวสาร ควรจะมีหน่วยงานที่ดูแลเรื่องไซเบอร์โดยตรง ผู้ก่อการร้ายทางไซเบอร์เหมือนกับภูเขาน้ำแข็ง ลักษณะของผู้ก่อการร้ายเป็นส่วนที่อยู่ด้านล่างไม่มีและไม่รู้กำหนดที่ชัดเจน ไม่รู้ว่าสู้กับใครภัยของการโจมตีทางไซเบอร์ถือเป็นภัยอันดับ 1 ของโลก ผลที่เกิดขึ้นกับการก่อการร้ายภัยสูงสุดคือก่อความวุ่นวายในประเทศไทย ทำให้ระบบกายภาพเช่น ระบบโครงสร้างพื้นฐานถูกทำลาย ไม่สงบสุข ในเรื่องของสงครามข้อมูลข่าวสาร เช่น ทำให้ประเทศอื่นมองประเทศไทยไม่ดีถูกใส่ร้ายป้ายสี เพราะเราไม่มีกระบวนการรับรู้และโต้กลับ ในลักษณะที่เป็นรูปธรรมในปัจจุบันประเทศไทยก็มีสำนักข่าวกรองที่ดูแลเรื่องไซเบอร์เฉพาะ ประเทศไทยยังมีการสร้างการตระหนักรู้น้อยมาก เพราะคนที่มีหน้าที่ยังไม่ตระหนัก ยังไม่รู้บทบาทหน้าที่ของตนเอง ยังมองเรื่องภัยไซเบอร์ไม่ต่างจากภัยปัจจุบัน ประชาชนยังไม่มีความเข้าใจต่อปัญหาการก่อการร้าย คนยังไม่เข้าใจถึงภัยก่อการร้าย ต้องมีการจัดการกับขอบเขตบางอย่าง ซึ่งการจัดการกับขอบเขตนั้น เป็นเรื่องของกฎหมายกับการบังคับใช้ กฎหมายต้องมีการกำหนดว่า ใครมีหน้าที่ต้องทำอะไร ใครเป็นคนจัดการเรื่องอะไร มีหน้าที่ความรับผิดชอบเรื่องอะไรบ้าง" (มนตรี, นามสมมติ, สัมภาษณ์, 11 พฤษภาคม 58)

"ความก้าวหน้าทางไซเบอร์นำไปสู่การก่อการร้ายได้มาก ยิ่งโลกไซเบอร์ก้าวหน้ามากเท่าไหร่ประชาชนจะพบปะผู้คนได้มากขึ้น คนก็จะพบปะสิ่งที่ใหม่ได้ทั่วโลก การภูมิคุ้มกันในพื้นที่แต่เราก็ต้องเผชิญกับโลกทั้งโลก แต่ละคนก็จะมีภูมิคุ้มกันทางไซเบอร์ได้ไม่เหมือนกัน สรุปคือ เปิดประตูให้ทุกสิ่งทุกอย่างเข้ามา ทำให้เกิดการก่อการร้าย ผู้ก่อการร้ายมองเห็นทุกคนบนโลกได้เช่นเดียวกัน ผู้ก่อการร้ายทางไซเบอร์มองเรื่องผลประโยชน์ทางเศรษฐกิจที่เกี่ยวข้องกับประเทศไทย หรือดินแดนจะเป็นเป้าหมายหลักของผู้ก่อการร้ายได้มากกว่า อาจจะไม่มีเป้าหมายที่ชัดเจน ประเทศไทยยังมีน้อยที่เป็นเป้าหมาย คนไทยต้องยอมรับว่า ประเทศไทยใช้อินเทอร์เน็ตหลากหลายมาก ทำให้เกิดความสนใจ ยกเว้นว่าเรามีช่องโหว่ที่ชัดเจนมากทางการค้าหรือทางเศรษฐกิจ ทำให้เค้าเข้ามาโจมตีโดยตรง โดยอาจใช้ข้อมูลเป็นฐาน ผู้ก่อการร้ายไม่จำกัดด้วยอายุและเพศ ทุกคนสามารถเรียนรู้ช่องโหว่ก็สามารถทำได้ ผู้ก่อการร้ายต้องเป็นคนและเป็นผู้สร้างระบบขึ้นมา ไซเบอร์ไม่ได้ทำเพียงแค่ระบบหยุดชะงัก แต่ทำให้ระบบเศรษฐกิจสืบเนื่องนั้นใช้งานไม่ได้ทำให้เกิดความแตกแยกในสังคม อาจทำให้เกิดถึงขั้นเสียชีวิตก็เป็นได้ถ้าโจมตีไซเบอร์โดยตรง เช่น การ

เปลี่ยนแปลงโรงงานไฟฟ้านิวเคลียร์ เปลี่ยนแปลงเที่ยวบิน ถ้าหากสภาพสังคมมีความแตกแยกก็จะเปิดโอกาสให้ประเทศที่สามหรือเป็นการเปิดโอกาสให้ความแตกแยกดังกล่าวเข้ามาแทรกแซงก่อให้ผู้ก่อการร้ายทางไซเบอร์เข้ามากระทำ การเมืองก็มีผลในระดับหนึ่ง ถ้าการเมืองไม่นิ่ง นโยบายไม่มั่นคง การดำเนินการทางไซเบอร์ที่ทำอยู่ไม่ต้องเนื่อง การพัฒนามีค่อยข้างต่ำ ก็จะทำให้ประเทศถูกโจมตีได้" (วิเชียร, นามสมมติ, สัมภาษณ์, 26 พฤษภาคม 58)

"ระบบต่างๆ ของประเทศไทยยังมีช่องโหว่ด้านความมั่นคงค่อนข้างมาก อาจขาดการตระหนักในเรื่องนี้ หรือถ้าเกิดภัยคุกคามด้านไซเบอร์ขึ้นมาแล้วหน่วยงานอาจไม่รู้ว่ามีผลกระทบมากขนาดไหน รุนแรงแค่ไหน จากผลการสำรวจสถิติของประเทศไทยพบว่า ประเทศไทยมีช่องโหว่ค่อนข้างเยอะ และทำให้แฮกเกอร์จากที่อื่นขโมยข้อมูลได้ง่าย ประเด็นของการเปิดเผยข้อมูลซึ่งอยู่ในสังคมออนไลน์ซึ่งอาจเป็นการไม่รู้ตัวหรืออาจมีคนช่วยเปิดเผยข้อมูล ทำให้แฮกเกอร์หาข้อมูลคนหนึ่งสามารถหาข้อมูลได้ง่าย สามารถปลอมเป็นใครก็ได้ ในสถานการณ์นี้ประเทศไทยยังไม่รุนแรงมากแต่เกิดขึ้นได้" (มงคล, นามสมมติ, สัมภาษณ์, 27 พฤษภาคม 58)

" ความก้าวหน้าทางไซเบอร์นำไปสู่การก่อการร้ายได้จากการฉวยโอกาสและเป็นการใช้ความก้าวหน้าทางไวเบอร์ในทางที่ผิด แต่มันเป็นไปตามหลักการในการก่อการร้ายคือใช้ทุกอย่างที่ทำได้และหาได้ ส่วนใหญ่ประเทศไทยมองการก่อการร้ายเป็นเรื่องของศาสนา แต่ต่อไปสิ่งที่จะนำมาซึ่งการก่อการร้ายคือ การขาดแคลนทรัพยากร การเข้าถึงทรัพยากรต่อไปจะหนักมากขึ้นเรื่องทำให้คนต้องแย่งชิงกัน ผู้ก่อการร้ายทางไซเบอร์มักเป็นกลุ่มที่ตัดขาดจากสังคม คือไม่สามารถอยู่กับสังคมได้เลยต้องใช้ไซเบอร์เป็นตัวกำบัง เป็นเครื่องมือ หรือกลุ่มที่มีการมองสิ่งต่างๆ เป็นอุดมคติ ต้องแก้ปัญหามองโลกเป็นขาวกับดำ ต้องการเปลี่ยนแปลงขั้นรุนแรง ตอนนี้ไทยมีกลุ่มที่เรียกว่า SELF Radicalization คนที่มีความคิดรุนแรงโดยที่ไม่ได้สังกัดกลุ่มใดเลย ซึ่งกลุ่มนี้เป็นวัยรุ่นพยายามควบคุมอยู่ เพราะจะมีบางคนหรือบางกลุ่มเป็นแบบนี้ อาจเป็นคนเดียว ที่ใช้เวลาอยู่กับไซเบอร์เยอะ บางที่อยู่หน้าจอคอมพิวเตอร์ 7 - 8 ชั่วโมง สิ่งที่ต้องทำคือการให้ท้องถิ่นหรือชุมชนพยายามช่วยกันดูแลถ้าใครมีแนวโน้มก็จะต้องให้ผู้ใหญ่เข้าไปดูแล เพื่อไม่ให้ลุกลาม โดยขณะนี้มีมติของสหประชาชาติว่า ให้ทุกประเทศออกกฎหมายหรือพยายามดูแลเด็กหรือกลุ่มเสี่ยงที่เดินทางเข้าไปในซีเรียหรืออิรัก แต่ประเทศไทยยังไม่ถึงขั้นนั้น แต่ก็ควรจะระวังเพราะมีอยู่ในประเทศไทย ผลที่เกิดขึ้นหากมีการก่อการร้ายทางไซเบอร์ผลทางกายภาพ เช่นทำลายระบบสาธารณูปโภคทั้งหลายให้เกิดความเสียหายเกี่ยวกับ โรงพยาบาล การผลิตน้ำ โรงไฟฟ้า และผลกระทบทางด้านจิตใจ" (สัญญา, นามสมมติ, สัมภาษณ์, 10 กรกฎาคม 58)

"เทคโนโลยีด้านไซเบอร์ มีการพัฒนามากมาย เทคโนโลยีต่างๆ ง่ายและเร็วขึ้น ถ้าไปใช้ในทางการก่อการร้ายก็จะเสียหายได้เร็วและเป็นมุมกว้างได้ ผู้ก่อการร้ายมีลักษณะเด่นคือต้องรู้

เทคโนโลยี อาจศึกษาข้อมูล เทคนิควิธีการซึ่งเป็นใครก็ได้แต่ต้องรู้เทคโนโลยี" (วรรณี, นามสมมติ, สัมภาษณ์, 13 กรกฎาคม 58)

บทสรุปผลจากการศึกษาพบข้อสรุป 2 ประเด็นดังนี้ 1.การก่อการร้ายทางไซเบอร์ เป็นการกระทำที่ก่อให้เกิดความเสียหาย ก่อให้เกิดความหวาดกลัว ตื่นตระหนกโดยมีการนำไซเบอร์มาเป็นเครื่องมือในการก่อการร้าย โดยมีเหตุจูงใจทางการเมือง เป็นสำคัญ สิ่งที่ค้นพบคือ ประเทศไทยยังไม่มีสถานการณ์หรือเหตุจูงใจที่นำไปสู่การก่อการร้ายทางไซเบอร์ ส่วนใหญ่เป็นการกระทำของแฮกเกอร์ เช่น การขโมยข้อมูลหน้าเว็บไซต์ของหน่วยงานราชการ ธนาคารหรือสถาบันทางการเงิน เพื่อแสดงออกถึงความสนุกสนาน พอใจ ทำให้เป็นที่รู้จักว่ามีศักยภาพในด้านนี้ 2.การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย จากการวิจัยสิ่งที่ค้นพบคือ ประเทศไทยมีการตื่นตัวและตระหนักในเรื่องของการต่อต้านการก่อการร้ายทางไซเบอร์ แต่มีการดำเนินการแบบแยกส่วน มีหน่วยงานที่การตระหนักในความปลอดภัยทางไซเบอร์คือ หน่วยทหาร ตำรวจและหน่วยงานของภาคเอกชนบางส่วนที่เกี่ยวข้องกับการเงิน เช่น ธนาคารพาณิชย์ต่างๆ สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์แห่งประเทศไทย (ก.ล.ต.) เป็นต้น

สรุปข้อมูลเชิงคุณภาพได้ดังนี้ การก่อการร้ายหมายถึง กระทำการใด ๆ เพื่อให้เกิดความหวาดกลัว การใช้ความรุนแรงหรือขู่ว่าจะใช้ความรุนแรงเพื่อให้เกิดความตื่นตระหนก โดยมีเหตุจูงใจทางการเมือง ทั้งนี้เพื่อนำไปสู่การเปลี่ยนแปลงในทางสังคมทางการเมือง และทางเศรษฐกิจ วิธีการก่อการร้ายทางไซเบอร์ มีวิธีการดังนี้1.ผู้ก่อการร้ายซึ่งต้องมีความรู้ทางไซเบอร์หรือเทคโนโลยี ศึกษาข้อมูลที่เกี่ยวกับเป้าหมายที่ต้องการจะกระทำ 2.สร้างหรือพัฒนาเครื่องมือให้ตรงกับความต้องการต่อเป้าหมาย เครื่องมือที่สำคัญของการก่อการร้ายทางไซเบอร์คืออินเทอร์เน็ต 3. ระดมคนหรือหาสมาชิกที่มีแนวความคิดแนวทางเดียวกัน 4.ระดมเงินทุนในการสนับสนุน 5. ปฏิบัติการตามวัตถุประสงค์ที่วางไว้เพื่อมุ่งเป้าหมายทางการเมืองปัจจัยที่เกี่ยวข้องกับแรงจูงใจในการก่อการร้ายทางไซเบอร์ด้วยประเทศไทยเป็นประเทศเปิดเสรี เปิดรับนักท่องเที่ยวและมีนโยบายส่งเสริมให้เกิดการท่องเที่ยวในทุกที่โดยไม่มีข้อจำกัด ดังนั้นจึงเป็นเหมือนสวรรค์ของผู้ก่อการร้าย อีกทั้งการส่งเสริมการเปิดใช้อินเทอร์เน็ตในทุกที่ ทำให้ประชาชนขาดการตระหนักรู้ในเรื่องของการใช้ไซเบอร์ การก่อการร้ายทางไซเบอร์นั้นผู้ก่อการร้ายจะใช้เครื่องมือทางไซเบอร์ที่หาง่ายและใช้เครื่องมือได้ทุกที่ ไม่ว่าจะเป็นโทรศัพท์มือถือ แท็บเล็ต คอมพิวเตอร์ ที่สามารถเชื่อมต่ออินเทอร์เน็ตได้ทำให้คนเข้าถึงได้ง่ายและเชื่อง่ายขึ้น แรงจูงใจที่นำไซเบอร์มาก่อการร้าย ผู้เชี่ยวชาญมองว่าเป็นเรื่องเงินเป็นสำคัญ รองลองมาเป็นเรื่องของแนวคิด อุดมการณ์ทางการเมืองหรือทางศาสนา หรือแม้แต่ความไม่พอใจต่อหน่วยงานหรือองค์กร แต่ปัจจัยที่สำคัญที่ผู้เชี่ยวชาญมองต่างกันคือ แรงจูงใจที่สำคัญต่อการกระทำที่เป็นการก่อการร้ายจะต้องเป็นการกระทำที่มาจากแรงจูงใจทาง

เมืองเป็นสำคัญ จึงเห็นได้ว่า ความเข้าใจในความหมายของการก่อการร้ายที่แตกต่างกัน นำไปสู่การอธิบายแรงจูงใจของการก่อการร้ายที่ต่างกันด้วย เมื่ออธิบายความเข้าใจแรงจูงใจการก่อการร้ายทางไซเบอร์ จึงไม่ได้มีการให้คำจำกัดความที่ชัดเจนปัญหาที่สำคัญของการต่อต้านการก่อการร้ายเกิดจากแนวคิดของการก่อการร้าย และความหมาย และความไม่รู้ถึงความรุนแรงอันเกิดจากการก่อการร้ายของคนในประเทศใครคือผู้ก่อการร้าย และอะไรคือการก่อการร้าย เนื่องจากภัยการก่อการร้ายเป็นเรื่องไกลตัวและยังไม่มีการสร้างความตระหนักอย่างชัดเจน

ความก้าวหน้าทางไซเบอร์คือ เทคโนโลยีที่มีอินเทอร์เน็ต เพื่อเชื่อมต่อการสื่อสารได้ทุกที่ทุกเวลา ไม่ว่าจะอยู่ที่ใดบนโลก สะดวก รวดเร็ว และไซเบอร์มีความสำคัญอย่างมากต่อการดำรงชีวิตในปัจจุบัน โดยมีเครื่องมือที่ใช้ในการติดต่อสื่อสาร ไม่ว่าจะเป็น คอมพิวเตอร์ โทรศัพท์มือถือ หรือ แท็บเล็ตเป็นต้น ความก้าวหน้าทางไซเบอร์ต้องมีความเร็วสูง มีระบบปฏิบัติการที่ดีและมีประสิทธิภาพและสามารถเข้าถึงได้ผู้ก่อการร้ายแสวงหาโอกาสจากประเทศไทยในหลายด้านเพื่อก่อการร้าย ประเด็นสำคัญที่พบได้คือ ประเทศไทยเป็นประเทศที่เปิดเสรี และประชาชนมีการต้อนรับชาวต่างประเทศ มีการยิ้มแย้มแจ่มใสและต้อนรับผู้อื่นจึงเหมือนกับเป็นสวรรค์ของผู้ก่อการร้าย ส่วนใหญ่ผู้ก่อการร้ายจะใช้ประเทศไทยเป็นฐานในการเตรียมการก่อการร้ายไปยังประเทศที่สาม หรือประเทศที่เป็นเป้าหมายมากกว่า และประเทศไทยไม่มีมาตรการในการป้องกันความปลอดภัยทางไซเบอร์ ประชาชนยังไม่ความตระหนักรู้ต่อภัยคุกคามทางไซเบอร์ จึงทำให้มีการใช้อย่างไม่ระแวดระวังเครื่องมือทางไซเบอร์ที่นำมาใช้ในการก่อการร้ายในปัจจุบัน คือ โทรศัพท์มือถือ แท็บเล็ต คอมพิวเตอร์ หรืออุปกรณ์ที่สามารถเชื่อมต่ออินเทอร์เน็ตได้และสามารถใช้งานได้ทุกที่ อย่างสะดวกและรวดเร็ว การเชื่อมต่ออินเทอร์เน็ตที่มีความเร็วสูงและมีระบบปฏิบัติการที่มีประสิทธิภาพจะช่วยการปฏิบัติการได้อย่างมีประสิทธิภาพ นอกจากนี้ ประเด็นสำคัญที่ค้นพบคือการใช้สังคมออนไลน์ทั้งกล่องข้อความ ไลน์ ทวิสเตอร์ เป็นต้น เพื่อใช้ในการติดต่อสื่อสารกันทั่วโลกและใช้เป็นช่องทางในการเผยแพร่แนวคิด วิดีโอ เพื่อให้เกิดความเชื่อ ต่อบุคคล ต่อสมาชิกในกลุ่มหรือ เชื่อมโยงไปยังดึงปลุกระดมคนเพื่อนำมาสู่การก่อการร้ายได้ การก่อการร้ายทางไซเบอร์และการต่อต้านการก่อการร้ายทางไซเบอร์ สรุปได้ 2 ประเด็นดังนี้

1.การก่อการร้ายทางไซเบอร์ เป็นการกระทำที่ก่อให้เกิดความเสียหาย ก่อให้เกิดความหวาดกลัว ตื่นตระหนกโดยมีการนำไซเบอร์มาเป็นเครื่องมือในการก่อการร้าย โดยมีเหตุจูงใจทางการเมือง เป็นสำคัญ สิ่งที่ค้นพบคือ ประเทศไทยยังไม่มีสถานการณ์หรือเหตุจูงใจที่นำไปสู่การก่อการร้ายทางไซเบอร์ ส่วนใหญ่เป็นการกระทำของแฮกเกอร์ เช่น การแฮกหน้าเว็บไซต์ของหน่วยงานราชการ ธนาคารหรือสถาบันทางการเงิน เพื่อแสดงออกถึงความสนุกสนาน พอใจ ทำให้เป็นที่รู้จักว่ามีศักยภาพในด้านนี้

2.การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย จากการวิจัยสิ่งที่ค้นพบคือ ประเทศไทยมีการตื่นตัวและตระหนักในเรื่องของการต่อต้านการก่อการร้ายทางไซเบอร์ แต่มีการดำเนินการแบบแยกส่วน มีหน่วยงานที่การตระหนักในความปลอดภัยทางไซเบอร์คือ หน่วยทหาร ตำรวจและหน่วยงานของภาคเอกชนบางส่วนที่เกี่ยวข้องกับการเงิน เช่น ธนาคารพาณิชย์ต่างๆ สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์แห่งประเทศไทย (ก.ล.ต.) เป็นต้น การสัมภาษณ์เกี่ยวกับความก้าวหน้าทางไซเบอร์ การนำไซเบอร์มาเป็นเครื่องมือในการก่อการร้าย การก่อการร้ายการก่อการร้ายทางไซเบอร์ ปัญหาในการจัดการกับการก่อการร้ายความก้าวหน้าทางไซเบอร์แรงจูงใจในการก่อการร้ายและการแสวงหาโอกาสในการก่อการร้ายทางไซเบอร์ การนำไซเบอร์มาเป็นเครื่องมือในการก่อการร้ายและการต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย สังเคราะห์สรุปผลดังนี้

ตารางที่ 4 การสังเคราะห์ข้อมูลประเด็นที่เกี่ยวข้องกับการก่อการร้ายและการต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย

ประเด็นที่เกี่ยวข้องกับการก่อการร้ายและการต่อต้านการก่อการร้ายทางไซเบอร์	ผู้เชี่ยวชาญ									
	คนที่ 1	คนที่ 2	คนที่ 3	คนที่ 4	คนที่ 5	คนที่ 6	คนที่ 7	คนที่ 8	คนที่ 9	คนที่10
ความก้าวหน้าทางไซเบอร์คือการพัฒนาเทคโนโลยีที่สามารถเชื่อมต่อกันได้อย่างรวดเร็ว	✓	✓		✓	✓		✓		✓	
ความก้าวหน้าทางไซเบอร์คือการนำอุปกรณ์สื่อสารที่เชื่อมต่ออินเทอร์เน็ตและมีความเร็วสูง	✓	✓	✓	✓	✓		✓	✓	✓	
ประเทศไทยมีนโยบายเปิดเสรีเน้นการส่งเสริมการท่องเที่ยว นโยบายการเข้าถึงอินเทอร์เน็ตได้มากขึ้น	✓		✓					✓	✓	✓
แรงจูงใจในการก่อการร้ายที่สำคัญคือเงิน แนวคิดและอุดมการณ์ รวมทั้งเครื่องมือในการก่อการร้ายที่หาง่าย	✓	✓	✓	✓	✓		✓			

ประเด็นที่เกี่ยวข้องกับการก่อการร้ายและการต่อต้านการก่อการร้ายทางไซเบอร์	ผู้เชี่ยวชาญ									
	คนที่ 1	คนที่ 2	คนที่ 3	คนที่ 4	คนที่ 5	คนที่ 6	คนที่ 7	คนที่ 8	คนที่ 9	คนที่10
การก่อการร้ายคือ การกระทำที่ทำให้เกิดความเสียหายทั้งระดับบุคคลและระดับประเทศ ส่วนใหญ่เป็นประเด็นทางการเมือง		✓	✓	✓					✓	✓
การก่อการร้ายทางไซเบอร์คือ การนำเอาไซเบอร์มาเป็นเครื่องมือในการก่อการร้ายโดยมีแรงจูงใจทางการเมืองเป็นหลัก			✓	✓	✓			✓	✓	✓
วิธีปฏิบัติการหลักของการก่อการร้ายทางไซเบอร์คือ ศึกษาข้อมูลที่ต้องการเจาะช่องโหว่ หาเครื่องมือในการทำลายและดำเนินการก่อการร้ายทางไซเบอร์		✓	✓	✓	✓	✓	✓	✓		
ประเทศไทยยังไม่มีการสร้างการตระหนักรู้ทางไซเบอร์และการก่อการร้ายทางไซเบอร์มีผลต่อความเสียหายทั้งระดับบุคคลและระดับประเทศ	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
ประเทศไทยยังไม่มีการจัดรูปแบบการศึกษาที่เน้นความรู้ทางไซเบอร์และส่งเสริมงานวิจัยเพื่อพัฒนาองค์ความรู้ทางไซเบอร์	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
ประเทศไทยยังไม่มีกฎหมายเพื่อดูแลป้องกันและควบคุมการดำเนินการทางไซเบอร์และบังคับใช้อย่างแท้จริง	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

ประเด็นที่เกี่ยวข้องกับการก่อการร้ายและการต่อต้านการก่อการร้ายทางไซเบอร์	ผู้เชี่ยวชาญ									
	คนที่ 1	คนที่ 2	คนที่ 3	คนที่ 4	คนที่ 5	คนที่ 6	คนที่ 7	คนที่ 8	คนที่ 9	คนที่10
ประเทศไทยยังไม่มีหน่วยงานหรือองค์กรที่เป็นเจ้าภาพหลักเพื่อดูแล ติดตามและควบคุมการดำเนินการรวมถึงแก้ปัญหาทางไซเบอร์ทั้งหมด	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
การป้องกันทางไซเบอร์ของประเทศไทยต้องเกิดจากความร่วมมือกันระหว่างหน่วยงานทั้งภาครัฐและเอกชนและภาคประชาชนทั้งประเทศ	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
การพัฒนาทางไซเบอร์อย่างรวดเร็วส่งผลต่อการนำมาเป็นเครื่องมือทางการก่อการร้ายในอนาคตที่มีอานุภาพร้ายแรงอย่างงแน่นอน	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

จากการสัมภาษณ์ผู้เชี่ยวชาญที่เกี่ยวข้องกับการมีบทบาทหรือเกี่ยวข้องกับการดำเนินงานการพัฒนาทางไซเบอร์และมีความรู้ความเชี่ยวชาญในการกำหนดยุทธศาสตร์ทางเทคโนโลยีทั้งหมด (จำนวน 10 คน) และนำมาข้อมูลทั้งหมดมาสังเคราะห์เพื่อกำหนดประเด็นที่เกี่ยวข้องกับการก่อการร้ายและการต่อต้านการก่อการร้ายทางไซเบอร์มี 2 ส่วนดังนี้

ในส่วนแรกพบว่า มีประเด็นของการสังเคราะห์ข้อมูลรวม 6 ประเด็น ที่มีผู้เชี่ยวชาญมีความเห็นพ้องต้องกันดังต่อไปนี้ ประเทศไทยยังไม่มีการสร้างการตระหนักรู้ทางไซเบอร์และการก่อการร้ายทางไซเบอร์มีผลต่อความเสียหายทั้งระดับบุคคลและระดับประเทศประเทศไทยยังไม่มีการจัดรูปแบบการศึกษาที่เน้นความรู้ทางไซเบอร์และส่งเสริมงานวิจัยเพื่อพัฒนาองค์ความรู้ทางไซเบอร์ประเทศไทยยังไม่มีกฎหมายเพื่อดูแล ป้องกันและควบคุมการดำเนินการทางไซเบอร์และบังคับใช้อย่างแท้จริงประเทศไทยยังไม่มีหน่วยงานหรือองค์กรที่เป็นเจ้าภาพหลักเพื่อดูแล ติดตามและควบคุมการดำเนินการรวมถึงแก้ปัญหาทางไซเบอร์ทั้งหมดการป้องกันทางไซเบอร์ของประเทศไทยต้องเกิดจากความร่วมมือกันระหว่างหน่วยงานทั้งภาครัฐและเอกชนและภาคประชาชนทั้งประเทศและการพัฒนาทางไซเบอร์อย่างรวดเร็วส่งผลต่อการนำมาเป็นเครื่องมือทางการก่อการ

ร้ายในอนาคตที่มีอานุภาพร้ายแรงอย่างแน่นอน จึงสรุปได้ว่า ในทั้ง 6 ประเด็นนี้ผู้เชี่ยวชาญมีความเห็นพ้องต้องกันเพื่อนำมากำหนดเป็นประเด็นยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์

ส่วนที่สอง พบว่า มีประเด็นของการสังเคราะห์ข้อมูล รวม 7ประเด็น ที่มีผู้เชี่ยวชาญมีความเห็นบางส่วนที่แสดงความคิดเห็นและบางส่วนไม่ได้มีความคิดเห็นพ้องต้องกัน ดังต่อไปนี้ ความก้าวหน้าทางไซเบอร์คือการพัฒนาเทคโนโลยีที่สามารถเชื่อมต่อกันได้อย่างรวดเร็วจำนวน 6 คน ความก้าวหน้าทางไซเบอร์คือการนำอุปกรณ์สื่อสารที่เชื่อมต่ออินเทอร์เน็ตและมีความเร็วสูง จำนวน 8 คน ประเทศไทยมีนโยบายเปิดเสรีเน้นการส่งเสริมการท่องเที่ยว นโยบายการเข้าถึงอินเทอร์เน็ตได้มากขึ้นจำนวน 5 คน แรงจูงใจในการก่อการร้ายที่สำคัญคือเงิน แนวคิดและอุดมการณ์ รวมทั้งเครื่องมือในการก่อการร้ายที่หาง่าย จำนวน 6 คน การก่อการร้ายคือ การกระทำที่ทำให้เกิดความเสียหายทั้งระดับบุคคลและระดับประเทศ ส่วนใหญ่เป็นประเด็นทางการเมือง จำนวน 5 คน การก่อการร้ายทางไซเบอร์คือ การนำเอาไซเบอร์มาเป็นเครื่องมือในการก่อการร้าย โดยมีแรงจูงใจทางการเมืองเป็นหลักจำนวน 6 คนและวิธีปฏิบัติการหลักของการก่อการร้ายทางไซเบอร์คือ ศึกษาข้อมูลที่ต้องการ เจาะช่องโหว่ หาเครื่องมือในการทำลายและดำเนินการก่อการร้ายทางไซเบอร์จำนวน 7 คน

มีข้อสรุปดังนี้ ประเด็นที่ผู้เชี่ยวชาญให้ความเห็นพ้องกัน จำนวน 5 คน มี 3 ประเด็นคือ ประเทศไทยมีนโยบายเปิดเสรีเน้นการส่งเสริมการท่องเที่ยว นโยบายการเข้าถึงอินเทอร์เน็ตได้มากขึ้นแรงจูงใจในการก่อการร้ายที่สำคัญคือเงิน แนวคิดและอุดมการณ์ รวมทั้งเครื่องมือในการก่อการร้ายที่หาง่ายและการก่อการร้ายคือ การกระทำที่ทำให้เกิดความเสียหายทั้งระดับบุคคลและระดับประเทศ ส่วนใหญ่เป็นประเด็นทางการเมืองสรุปได้ว่า การเข้าใจความหมายของการก่อการร้าย มีการกระทำให้เกิดความเสียหายโดยเป็นประเด็นทางการเมืองยังมีความคิดเห็นที่ไม่สอดคล้องกัน แรงจูงใจในการก่อการร้าย ส่วนหนึ่งเป็นมุมมองที่มาจากความต้องการเงินเป็นสำคัญ ในการก่อการร้ายต้องมีเหตุจูงใจทางการเมือง ในประเด็นนี้แตกต่างจากแนวคิดของ Central Intelligence Agency (CIA) นิยามว่า “การก่อการร้ายหมายถึง ปฏิบัติการรุนแรงที่มีการคิดและการเตรียมการไว้ล่วงหน้า โดยที่มีเหตุจูงใจทางการเมือง กระทำต่อเป้าหมาย ซึ่งไม่ได้มีส่วนเกี่ยวข้องกับสงคราม และไม่มีศักยภาพในการทำการรบโดยกลุ่มขบวนการที่มิได้เป็นตัวแทนของรัฐในทางการเมืองระหว่างประเทศ หรือโดยกลุ่มสายลับของรัฐที่กระทำการในทางลับ” (ธันยวัต ชูส่งแสง, 2547, หน้า 1) จึงเป็นข้อสรุปได้ว่า การนิยามความหมาย หรือการทำความเข้าใจในความหมาย การอธิบายในการก่อการร้ายต้องเป็นไปในทิศทางเดียวกัน จึงจะสามารถสร้างความเข้าใจและกำหนดเป็นยุทธศาสตร์ในการต่อต้านการก่อการร้ายได้

ประเด็นที่ผู้เชี่ยวชาญให้ความเห็นพ้องกัน จำนวน 6 คน มี 2 ประเด็น คือความก้าวหน้าทางไซเบอร์คือการพัฒนาเทคโนโลยีที่สามารถเชื่อมต่อกันได้อย่างรวดเร็วและวิธีปฏิบัติการหลักของการก่อการร้ายทางไซเบอร์คือ ศึกษาข้อมูลที่ต้องการ เจาะช่องโหว่ หาเครื่องมือในการทำลายและดำเนินการก่อการร้ายทางไซเบอร์ สรุปได้ว่า ความเข้าใจต่อความหมายของความก้าวหน้าทางไซเบอร์มีส่วนสำคัญต่อการพัฒนาทางเทคโนโลยีให้ทันต่อความเป็นโลกาภิวัตน์ อีกทั้งวิธีปฏิบัติการหลักของการก่อการร้ายทางไซเบอร์ก็มีความแตกต่างจากการก่อการร้ายทั่วไป ที่จะต้องเป็นผู้ก่อการร้ายที่มีความเชี่ยวชาญทางเทคโนโลยีและไซเบอร์ อีกทั้งยังต้องศึกษาวิธีการอย่างรอบคอบเพื่อไม่ให้เกิดความผิดพลาดเพราะเป้าหมายมีความเฉพาะเจาะจงมาก และเมื่อกระทำการก่อการร้ายทางไซเบอร์แล้ว จะส่งผลต่อความเสียหายและรุนแรงอย่างมหาศาลและประเด็นที่ผู้เชี่ยวชาญไม่ได้เห็นพ้องต้องกันทั้งหมด ในจำนวน 7 คน และ 8 คนคือ การก่อการร้ายทางไซเบอร์คือ การนำเอาไซเบอร์มาเป็นเครื่องมือในการก่อการร้ายโดยมีแรงจูงใจทางการเมืองเป็นหลักและความก้าวหน้าทางไซเบอร์คือการนำอุปกรณ์สื่อสารที่เชื่อมต่ออินเทอร์เน็ตและมีความเร็วสูงสรุปได้ว่า การสร้างความเข้าใจต่อการนำเอาไซเบอร์มาก่อการร้ายต้องเป็นวัตถุประสงค์ทางการเมืองเป็นหลักและการจะสามารถก่อการร้ายได้นั้นความก้าวหน้าทางไซเบอร์มีส่วนสำคัญอีกทั้งยังต้องเป็นประเทศที่มีการพัฒนาทางไซเบอร์ มีการใช้อุปกรณ์ที่ทันสมัย และมีการเชื่อมต่ออินเทอร์เน็ตและมีความเร็วสูง

ตารางที่ 5 สรุปความคิดเห็นของผู้สัมภาษณ์

ประเด็นของการสังเคราะห์ข้อมูลรวม 6 ประเด็น ที่มีผู้เชี่ยวชาญมีความเห็นพ้องต้องกัน	ผู้ที่ให้สัมภาษณ์	ข้อสรุป
-ประเทศไทยยังไม่มีการสร้างการตระหนักรู้ทางไซเบอร์และการก่อการร้ายทางไซเบอร์มีผลต่อความเสียหายทั้งระดับบุคคลและระดับประเทศ ประเด็นที่ 2ประเทศไทยยังไม่มีการจัดรูปแบบการศึกษาที่เน้นความรู้ทางไซเบอร์และส่งเสริมงานวิจัยเพื่อพัฒนาองค์ความรู้ทางไซเบอร์ -ประเทศไทยยังไม่มีกฎหมายเพื่อดูแล ป้องกันและควบคุมการดำเนินการทางไซเบอร์และ	ผู้ให้สัมภาษณ์คนที่ 1 – 10	ในทั้ง 6 ประเด็นนี้ผู้เชี่ยวชาญมีความเห็นพ้องต้องกันว่า ประเทศไทยยังคงไม่มีประเด็นเหล่านี้จึงสามารถนำมากำหนดเป็นประเด็นยุทธศาสตร์เพื่อการต่อต้านการก่อการร้ายทางไซเบอร์

ประเด็นของการสังเคราะห์ข้อมูลรวม 6 ประเด็น ที่มีผู้เชี่ยวชาญมีความเห็นพ้องต้องกัน	ผู้ที่ให้สัมภาษณ์	ข้อสรุป
บังคับใช้อย่างแท้จริง - ประเทศไทยยังไม่มีหน่วยงานหรือองค์กรที่เป็นเจ้าภาพหลักเพื่อดูแล ติดตามและควบคุมการดำเนินการรวมถึงแก้ปัญหาทางไซเบอร์ทั้งหมด - การป้องกันทางไซเบอร์ของประเทศไทยต้องเกิดจากความร่วมมือกันระหว่างหน่วยงานทั้งภาครัฐและเอกชนและภาคประชาชนทั้งประเทศ - การพัฒนาทางไซเบอร์อย่างรวดเร็วส่งผลต่อการนำมาเป็นเครื่องมือทางการก่อการร้ายในอนาคตที่มีอานุภาพร้ายแรงอย่างแน่นอน		
-ประเทศไทยมีนโยบายเปิดเสรีเน้นการส่งเสริมการท่องเที่ยว นโยบายการเข้าถึงอินเทอร์เน็ตได้มากขึ้น - แรงจูงใจในการก่อการร้ายที่สำคัญคือเงิน แนวคิดและอุดมการณ์ รวมทั้งเครื่องมือในการก่อการร้ายที่หาง่าย - การก่อการร้ายคือ การกระทำที่ทำให้เกิดความเสียหายทั้งระดับบุคคลและระดับประเทศ	จำนวน 5 คน	การนิยามความหมาย หรือการทำความเข้าใจในความหมาย การอธิบายในการก่อการร้ายต้องเป็นไปในทิศทางเดียวกัน จึงจะสามารถสร้างความเข้าใจและกำหนดเป็นยุทธศาสตร์ในการต่อต้านการก่อการร้ายได้
-ความก้าวหน้าทางไซเบอร์คือการพัฒนาเทคโนโลยีที่สามารถเชื่อมต่อกันได้อย่างรวดเร็ว - วิธีปฏิบัติการหลักของการก่อการร้ายทางไซเบอร์คือ ศึกษาข้อมูลที่ต้องการ เจาะช่องโหว่ หาเครื่องมือในการทำลายและดำเนินการก่อการร้ายทางไซเบอร์	จำนวน 6 คน	ความเข้าใจต่อความหมายของความก้าวหน้าทางไซเบอร์มีส่วนสำคัญต่อการพัฒนาทางเทคโนโลยีให้ทันต่อความเป็นโลกาภิวัตน์และวิธีปฏิบัติการหลักของการก่อการร้ายทางไซเบอร์ก็มีความแตกต่างจากการก่อการร้ายทั่วไป ที่จะต้องเป็นผู้ก่อการร้ายที่มีความเชี่ยวชาญทาง

ประเด็นของการสังเคราะห์ข้อมูลรวม 6 ประเด็น ที่มีผู้เชี่ยวชาญมีความเห็นพ้องต้องกัน	ผู้ที่ให้สัมภาษณ์	ข้อสรุป
		เทคโนโลยีและไซเบอร์ อีกทั้งยังต้องศึกษาวิธีการอย่างรอบคอบเพื่อไม่ให้เกิดความผิดพลาดเพราะเป้าหมายมีความเฉพาะเจาะจงมาก และเมื่อกระทำการก่อการร้ายทางไซเบอร์แล้วจะส่งผลต่อความเสียหายและรุนแรงอย่างมหาศาล
-การก่อการร้ายทางไซเบอร์คือ การนำเอาไซเบอร์มาเป็นเครื่องมือในการก่อการร้ายโดยมีแรงจูงใจทางการเมืองเป็นหลัก - ความก้าวหน้าทางไซเบอร์คือการนำอุปกรณ์สื่อสารที่เชื่อมต่ออินเทอร์เน็ตและมีความเร็วสูง	จำนวน 7 คน และจำนวน 8 คน	การสร้างความเข้าใจต่อการนำเอาไซเบอร์มาก่อการร้ายต้องเป็นวัตถุประสงค์ทางการเมืองเป็นหลัก และการจะสามารถก่อการร้ายได้นั้น ความก้าวหน้าทางไซเบอร์มีส่วนสำคัญอีกทั้งยังต้องเป็นประเทศที่มีการพัฒนาทางไซเบอร์ มีการใช้อุปกรณ์ที่ทันสมัย และมีการเชื่อมต่ออินเทอร์เน็ตและมีความเร็วสูง

จากทั้งสองประเด็นที่มีการนำข้อมูลจากการสัมภาษณ์มาสังเคราะห์เพื่อนำมาเป็นประเด็นในการกำหนดยุทธศาสตร์พบได้ว่า ประเทศไทยยังไม่มีผู้รู้หรือผู้เชี่ยวชาญที่สามารถอธิบายหรือให้ความหมายต่อความเข้าใจของไซเบอร์ ความก้าวหน้าทางไซเบอร์ การก่อการร้ายและ การนำไซเบอร์มาเป็นเครื่องมือในการก่อการร้าย จึงจำเป็นอย่างยิ่งที่จะต้องมีการพัฒนา ศึกษาวิจัยและสร้างความเข้าใจให้เกิดขึ้นกับคนในประเทศไทยอย่างเป็นระบบ

สอดคล้องกับการวิจัยเชิงปริมาณดังนี้การวิจัยเรื่องยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย ได้ดำเนินการเก็บรวบรวมข้อมูลจากประชากรโดยอาศัยอยู่ในกรุงเทพมหานคร กลุ่มตัวอย่างจำนวน 690 คนสรุปผลการวิเคราะห์เป็นตารางการวิเคราะห์ข้อมูลแผนภูมิและคำอธิบาย แบ่งเป็น 3 ส่วนดังนี้

ส่วนที่ 1 ข้อมูลทั่วไปของกลุ่มตัวอย่างได้แก่ เพศ อายุ การศึกษา อาชีพ และรายได้

ส่วนที่ 2 ความคิดเห็นต่อความก้าวหน้าทางไซเบอร์และลักษณะการก่อการร้ายทาง

ไซเบอร์และนำมาเป็นเครื่องมือทางยุทธศาสตร์ในการก่อการร้าย

ส่วนที่ 3 ความคิดเห็นต่อยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์

ส่วนที่ 4 การวิเคราะห์ความสัมพันธ์ระหว่างปัจจัยส่วนบุคคลกับประเด็นความก้าวหน้าทางยุทธศาสตร์และการนำยุทธศาสตร์มาเป็นเครื่องมือในการก่อการร้ายทางไซเบอร์และยุทธศาสตร์การต่อต้านการต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย

ส่วนที่ 5 การวิเคราะห์ความคิดเห็นความสัมพันธ์ระหว่างอาชีพกับยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทยและข้อเสนอแนะ

โดยสัญลักษณ์ที่ใช้ในการแสดงผล มีดังนี้

SD หมายถึง ส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation)

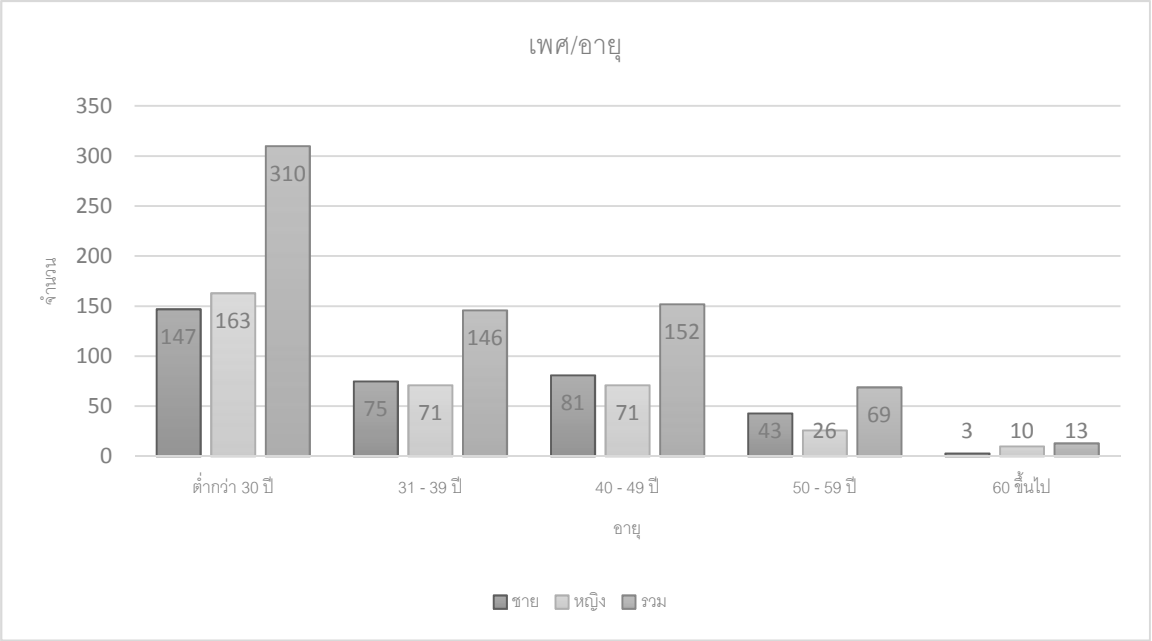
n หมายถึง ขนาดตัวอย่าง (Sample Size)

ส่วนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

ตารางที่ 6 จำแนกจำนวนของกลุ่มตัวอย่างเพศและอายุ(n = 690 คน)

เพศ/อายุ	อายุ					รวม
	ต่ำกว่า 30 ปี	31 – 39 ปี	40 – 49 ปี	50 – 59 ปี	60 ปีขึ้นไป	
ชาย	147	75	81	43	3	349
หญิง	163	71	71	26	10	341
รวม	310	146	152	69	13	690

จากตารางที่ 6 กลุ่มตัวอย่างมีจำนวนของเพศชายมากกว่าเพศหญิงเพศชายมีจำนวน 349 คนและเพศหญิงมีจำนวน 341 คน โดยกลุ่มตัวอย่างที่มีอายุต่ำกว่า 30 ปี มีจำนวนของเพศหญิงมากว่าเพศชาย เพศหญิงมีจำนวน163 คน เพศชายมีจำนวน 147 คน และกลุ่มตัวอย่างที่มีอายุมากกว่า 60 ปี มีจำนวนเพศหญิงมากกว่าเพศชาย เพศหญิงมีจำนวน 10 คน และเพศชายมีจำนวน 3คน

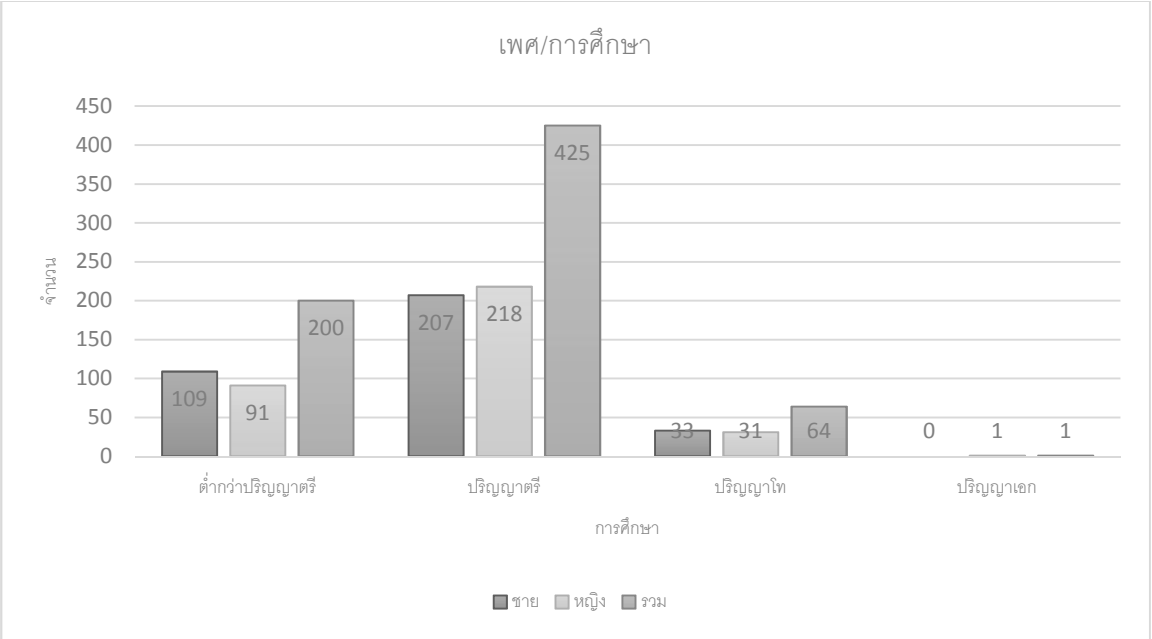


ภาพที่ จำแนกจำนวนของกลุ่มตัวอย่างเพศและอายุ

ตารางที่ 7 จำนวนของกลุ่มตัวอย่างจำแนกตามเพศและการศึกษา(n = 690 คน)

เพศ/ การศึกษา	การศึกษา				รวม
	ต่ำกว่าปริญญาตรี	ปริญญาตรี	ปริญญาโท	ปริญญาเอก	
ชาย	109	207	33	0	349
หญิง	91	218	31	1	341
รวม	200	425	64	1	690

จากตารางที่ 7 กลุ่มตัวอย่างมีจำนวนของผู้ที่มีการศึกษาระดับปริญญาตรีเป็นเพศชายมากกว่าเพศหญิง กลุ่มผู้ตอบแบบสอบถามปริญญาตรีเป็นเพศหญิงจำนวน 218 คน และเป็นเพศชายจำนวน 207 คน

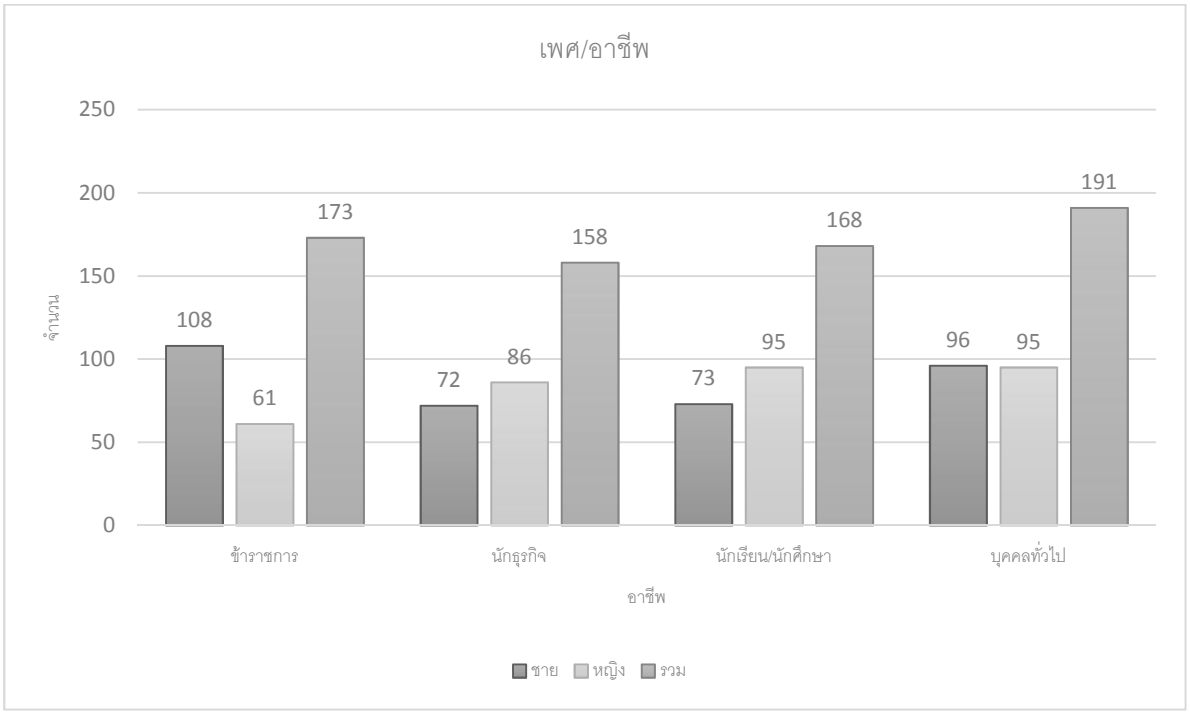


ภาพที่ จำแนกจำนวนของกลุ่มตัวอย่างเพศและการศึกษา

ตารางที่ 8จำนวนของกลุ่มตัวอย่างจำแนกตามเพศและอาชีพ(n = 690 คน)

เพศ/อาชีพ	อาชีพ				รวม
	ข้าราชการ	นักธุรกิจ	นักเรียน/นักศึกษา	บุคคลทั่วไป	
ชาย	108	72	73	96	349
หญิง	61	86	95	95	341
รวม	173	158	168	191	690

จากตารางที่ 8กลุ่มตัวอย่างมีจำนวนของผู้ที่มีอาชีพข้าราชการเป็นเพศชาย จำนวน 108 คน และเป็นเพศหญิง จำนวน 61 คน รวมจำนวน 173 คน และ ผู้ที่เป็นบุคคลทั่วไป เป็นเพศชาย จำนวน 96คนและเป็นเพศหญิง จำนวน 95 คน รวมจำนวน 191 คน ที่ตอบแบบสอบถามมากที่สุด

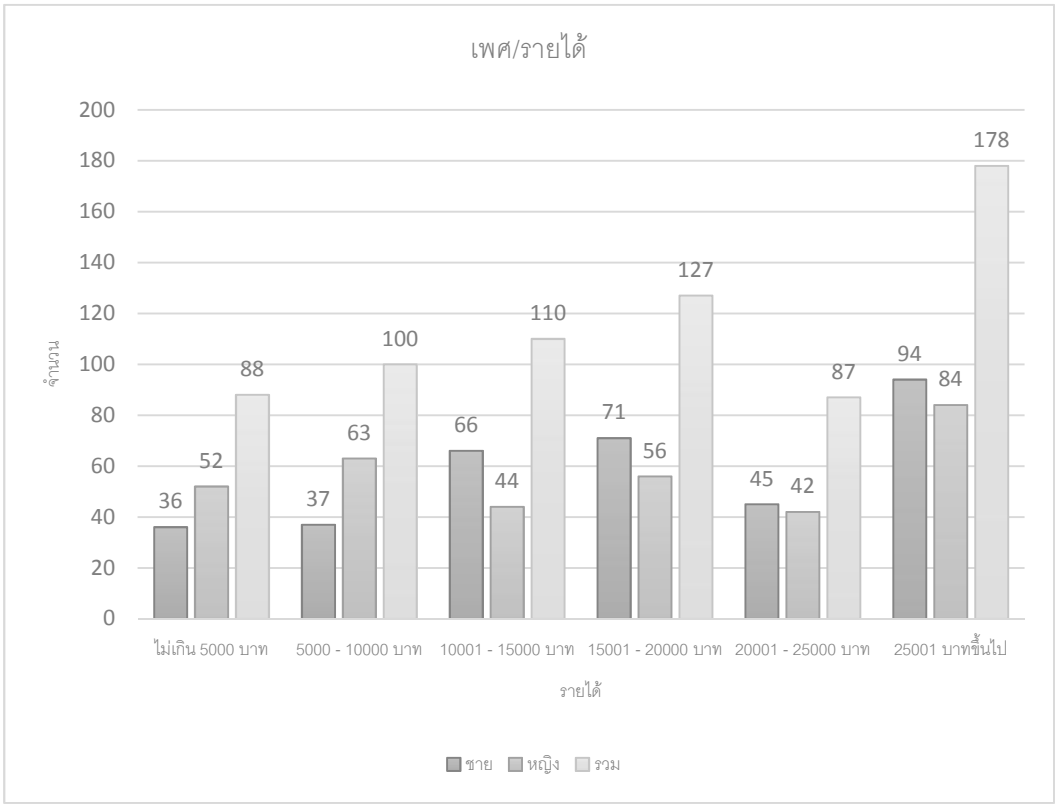


ภาพที่ จำแนกจำนวนของกลุ่มตัวอย่างเพศและอาชีพ

ตารางที่ 9 จำนวนของกลุ่มตัวอย่างจำแนกตามเพศและรายได้(n = 690 คน)

เพศ/รายได้	รายได้						รวม
	ไม่เกิน 5000 บาท	5001 – 10000 บาท	10001 – 15000 บาท	15001 – 20000 บาท	20001 – 25000 บาท	25001 บาทขึ้นไป	
ชาย	36	37	66	71	45	94	349
หญิง	52	63	44	56	42	84	341
รวม	88	100	110	127	87	178	690

จากตารางที่ 9 กลุ่มตัวอย่างมีจำนวนของผู้ที่มีรายได้สูง 25001 บาทขึ้นไป เป็นเพศชาย จำนวน 94 คน และเพศหญิง จำนวน 84 คน รวม จำนวน 178 คน สูงที่สุด รองลงมา รายได้ 15001 – 20000 บาทขึ้นไป เป็นเพศชาย จำนวน 71 คน และเป็นเพศหญิงจำนวน 56 คน รวมจำนวน 127 คน และรายได้ 10001– 15000 บาท เป็นเพศชาย จำนวน66 คน และเป็นเพศหญิงจำนวน 44 คน รวม จำนวน 110 คน ตามลำดับ



ภาพที่ จำแนกจำนวนของกลุ่มตัวอย่างเพศและรายได้

ส่วนที่ 2 ความคิดเห็นต่อความก้าวหน้าทางไซเบอร์และลักษณะการก่อการร้ายทางไซเบอร์และนำมาเป็นเครื่องมือทางยุทธศาสตร์ในการก่อการร้าย

ตารางที่ 10 การนำเสนอระดับความคิดเห็นจำแนกตามประเด็นความก้าวหน้าทางไซเบอร์

ประเด็น(n=690)	ระดับความคิดเห็น (ความถี่)					รวม	ค่าเฉลี่ย	SD	ระดับ
	1	2	3	4	5				
ความก้าวหน้าทางไซเบอร์									
1.การใช้โทรศัพท์มือถือ Tablet คอมพิวเตอร์และเครื่องมืออื่น ๆ ที่สามารถเชื่อมต่ออินเทอร์เน็ตพร้อมทั้งมีความเร็วสูงเป็นความก้าวหน้าทางไซเบอร์	0	5	72	365	248	690	4.24	0.66	มากที่สุด
2.Application ของโทรศัพท์มือถือที่สามารถอำนวยความสะดวกและมีการเชื่อมต่ออย่างรวดเร็วส่งผลต่อความก้าวหน้าทางไซเบอร์	0	3	99	350	238	690	4.21	0.68	มากที่สุด
3.จุดเชื่อมต่ออินเทอร์เน็ตสาธารณะและเน็ตเวิร์คความเร็วสูงจะส่งผลให้สังคมเครือข่าย, โทรศัพท์มือถือและการให้บริการจัดเก็บข้อมูลบนอินเทอร์เน็ต เกิดการขยายตัวและแพร่หลายเข้าถึงคนไทยทุกคน	2	25	138	307	218	690	4.04	0.83	มาก
4.ความก้าวหน้าทางไซเบอร์ คือการพัฒนาทางเทคโนโลยีที่สามารถเชื่อมต่อกันได้อย่างรวดเร็วสะดวกขึ้น ทำให้ทุกคนติดต่อกันได้ไม่ว่าจะอยู่ที่ใดในโลก	1	12	99	347	231	690	4.16	0.73	มาก

ประเด็น(n=690)	ระดับความคิดเห็น (ความถี่)					รวม	ค่าเฉลี่ย	SD	ระดับ
	1	2	3	4	5				
ความก้าวหน้าทางไซเบอร์									
5.การพัฒนาของแพลตฟอร์ม (Platform) หรือระบบปฏิบัติการสามารถที่จะพัฒนาไปสู่ระบบเว็บ 3.0 และ 4.0 ที่สามารถตัดสินใจแทนมนุษย์ในอนาคต	4	28	239	300	119	690	3.74	0.80	มาก
6.ปัจจุบันนี้คนไทยจะสามารถเชื่อมต่อออนไลน์กับโลกเสมือนทำให้รู้สึกเท่าเทียมกับคนทั่วโลก สามารถเข้าถึงแพลตฟอร์มพื้นฐานสารสนเทศและข้อมูลทุกอย่างในทางออนไลน์ได้	8	28	174	314	166	690	3.88	0.86	มาก
ภาพรวม	15	101	821	1983	1220	4140	4.04	0.54	มาก

จากตารางที่ 10 ระดับความคิดเห็นต่อความก้าวหน้าทางไซเบอร์และลักษณะการก่อการร้ายทางไซเบอร์และนำมาเป็นเครื่องมือทางยุทธศาสตร์ในการก่อการร้ายโดยภาพรวมพบว่า กลุ่มตัวอย่างมีความคิดเห็นในระดับมาก เมื่อพิจารณาเป็นรายประเด็น พบว่า ประเด็นความก้าวหน้าทางไซเบอร์ กลุ่มตัวอย่างมีความคิดเห็นในระดับมาก โดยมีค่าเฉลี่ย 4.04 ส่วนเบี่ยงเบนมาตรฐาน 0.54 เมื่อพิจารณาเป็นรายข้อพบว่า ข้อที่มีระดับความคิดเห็นสูง 3 อันดับแรก คือ

1. ข้อที่กลุ่มตัวอย่างมีความคิดเห็นสูงที่สุด คือการใช้โทรศัพท์มือถือแท็บเล็ตคอมพิวเตอร์และเครื่องมืออื่นๆ ที่สามารถเชื่อมต่ออินเทอร์เน็ตพร้อมทั้งมีความเร็วสูงเป็นความก้าวหน้าทางไซเบอร์มีความคิดเห็นในระดับมากที่สุด โดยมีค่าเฉลี่ย4.24 ส่วนเบี่ยงเบนมาตรฐาน 0.66

2. ข้อที่กลุ่มตัวอย่างมีความคิดเห็นสูงอันดับเป็นที่สอง คือ Application ของโทรศัพท์มือถือที่สามารถอำนวยความสะดวกและมีการเชื่อมต่ออย่างรวดเร็ว ส่งผลต่อความก้าวหน้าทางไซเบอร์มีความคิดเห็นในระดับมากที่สุด โดยมีค่าเฉลี่ย 4.21 ส่วนเบี่ยงเบนมาตรฐาน 0.68

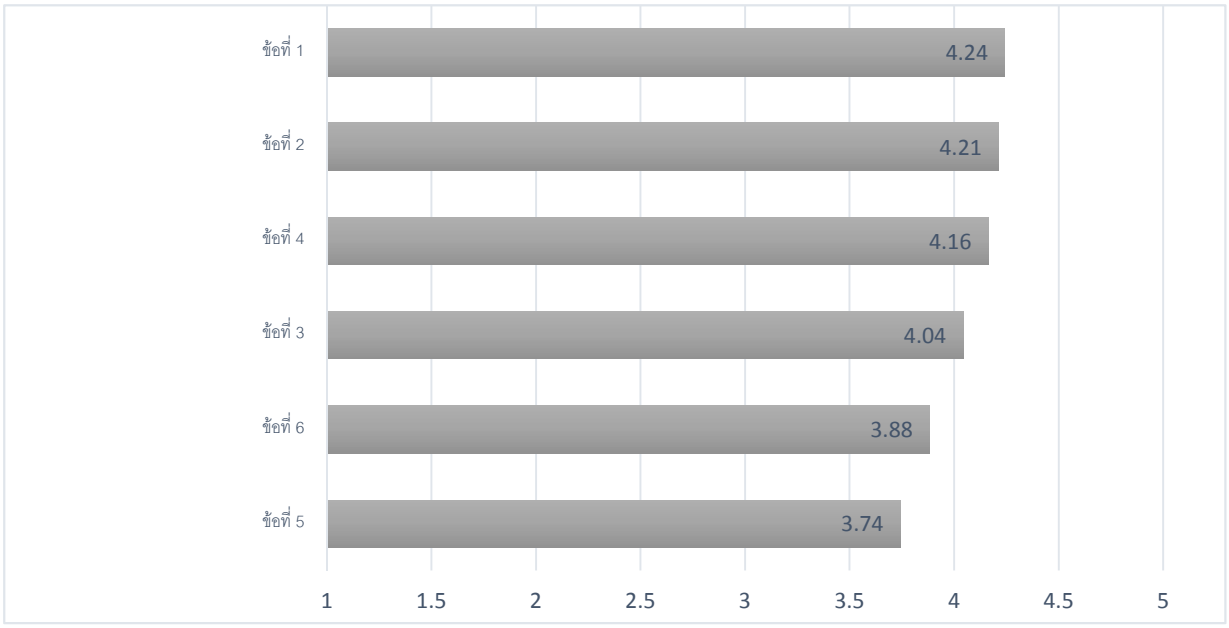
3. ข้อที่กลุ่มตัวอย่างมีความคิดเห็นสูงอันดับเป็นที่สาม คือ ความก้าวหน้าทางไซเบอร์ คือ การพัฒนาทางเทคโนโลยีที่สามารถเชื่อมต่อกันได้อย่างรวดเร็วสะดวกขึ้น ทำให้ทุกคนติดต่อกันได้ไม่ว่าจะอยู่ที่ใดในโลกมีความคิดเห็นในระดับมาก โดยมีค่าเฉลี่ย 4.16 ส่วนเบี่ยงเบนมาตรฐาน 0.73

ข้อที่มีระดับความคิดเห็นต่ำ 3 อันดับแรก คือ

1. ข้อที่กลุ่มตัวอย่างมีความคิดเห็นต่ำที่สุด คือ การพัฒนาของแพลตฟอร์ม (Platform) หรือระบบปฏิบัติการสามารถที่จะพัฒนาไปสู่ระบบเว็บ 3.0 และ 4.0 ที่สามารถตัดสินใจแทนมนุษย์ในอนาคต มีความคิดเห็นในระดับมาก โดยมีค่าเฉลี่ย 3.74 ส่วนเบี่ยงเบนมาตรฐาน 0.80

2. ข้อที่กลุ่มตัวอย่างมีความคิดเห็นต่ำเป็นอันดับที่สอง คือ ปัจจุบันนี้คนไทยจะสามารถเชื่อมต่อออนไลน์กับโลกเสมือนทำให้รู้สึกเท่าเทียมกับคนทั่วโลก สามารถเข้าถึงแพลตฟอร์มพื้นฐาน สารสนเทศและข้อมูลทุกอย่างในทางออนไลน์ได้ มีความคิดเห็นในระดับมาก โดยมีค่าเฉลี่ย 3.88 ส่วนเบี่ยงเบนมาตรฐาน 0.86

3. ข้อที่กลุ่มตัวอย่างมีความคิดเห็นต่ำเป็นอันดับที่สาม คือ จุดเชื่อมต่ออินเทอร์เน็ตสาธารณะและเน็ตเวิร์คความเร็วสูงจะส่งผลให้สังคมเครือข่ายโทรศัพท์มือถือและการให้บริการจัดเก็บข้อมูลบนอินเทอร์เน็ต เกิดการขยายตัวและแพร่หลายเข้าถึงคนไทยทุกคน มีความคิดเห็นในระดับมาก โดยมีค่าเฉลี่ย 4.04 ส่วนเบี่ยงเบนมาตรฐาน 0.83



ภาพที่ ระดับความคิดเห็นจำแนกตามประเด็นความก้าวหน้าทางไซเบอร์

ตารางที่ 11 การนำเสนอระดับความคิดเห็นจำแนกตามประเด็นการลักษณะการก่อการร้ายทางไซเบอร์และนำมาเป็นเครื่องมือทางยุทธศาสตร์ในการก่อการร้าย

ประเด็นยุทธศาสตร์ (n=690)	ระดับความคิดเห็น (ความถี่)					รวม	ค่าเฉลี่ย	SD	ระดับ
	1	2	3	4	5				
ลักษณะการก่อการร้ายทางไซเบอร์และนำมาเป็นเครื่องมือทางยุทธศาสตร์ในการก่อการร้าย									
7.การก่อการร้ายทางไซเบอร์ คือ การนำไซเบอร์มาเป็นเครื่องมือในการก่อการร้ายโดยมีวัตถุประสงค์เพื่อให้เกิดความรุนแรง รู้สึกหวาดกลัว คุกคามรัฐบาลหรือกลุ่มสังคมใด ๆ โดยมีแรงจูงใจทางการเมืองเป็นหลัก	3	27	170	365	565	690	3.86	0.76	มาก
8.การก่อการร้ายทางไซเบอร์เป็นการใช้เครื่องมือทางเทคโนโลยี เช่น โทรศัพท์มือถือ คอมพิวเตอร์ หรือเครื่องมือประเภทอื่น ๆ ที่เชื่อมต่อทางอินเทอร์เน็ตเพื่อการก่อการร้าย	3	22	171	351	143	690	3.90	0.76	มาก
9.อินเทอร์เน็ตเป็นช่องทางที่สำคัญที่ใช้ในการก่อการร้าย เช่น ลักลอบขโมยข้อมูลข่าวสารเพื่อมุ่งเป้าทางการเมือง ปล่อยไวรัสเพื่อทำลายระบบต่าง	3	33	163	335	156	690	3.90	0.81	มาก
10.การก่อการร้ายทางไซเบอร์เป็นการกระทำเพื่อความสนุกความพึงพอใจและสร้างชื่อเสียงให้กับผู้กระทำโดยมีแรงจูงใจประสงค์ทางการเมืองเป็นสำคัญ	7	60	241	274	108	690	3.62	0.88	มาก

ประเด็นยุทธศาสตร์ (n=690)	ระดับความคิดเห็น (ความถี่)					รวม	ค่าเฉลี่ย	SD	ระดับ
	1	2	3	4	5				
ลักษณะการก่อการร้ายทางไซเบอร์และนำมาเป็นเครื่องมือทางยุทธศาสตร์ในการก่อการร้าย									
11.การหลอกลวงทางโทรศัพท์ เช่น การหลอกให้โอนเงินไปให้การหลอกลวงว่าได้รับรางวัล หรือ การหลอกลวงโดยขู่ว่าเป็นหนี้บัตรเครดิต พูดจาหว่านล้อมให้ไปทำธุรกรรมทางตู้เอทีเอ็ม ฯ เป็นวิธีการที่นำไปสู่การก่อการร้ายได้	6	35	188	311	150	690	3.84	0.85	มาก
12.การก่อการร้ายทางไซเบอร์ในประเทศไทย เป้าหมายที่สำคัญคือความต้องการทำลายหรือสร้างความเสียหาย ความหวาดกลัว ที่มีวัตถุประสงค์ทางการเมืองเป็นสำคัญ	5	43	230	288	124	690	3.71	0.86	มาก
13.วิธีการปฏิบัติการหลักของการก่อการร้ายทาง ไซเบอร์คือ ศึกษาข้อมูลที่ต้องการเจาะช่องโหว่หาเครื่องมือในการทำลาย และดำเนินการก่อการร้ายทางไซเบอร์	3	30	199	339	119	690	3.79	0.79	มาก
14.การใช้ไซเบอร์เป็นเครื่องมือเช่น การโฆษณาชวนเชื่อ การชักจูง สาธิตวิดีโอการสอนให้ทำอุปกรณ์วางเพลิงและวัตถุระเบิด สามารถเป็นสาเหตุของก่อการร้ายได้	5	46	186	316	137	690	3.79	0.86	มาก

ประเด็นยุทธศาสตร์ (n=690)	ระดับความคิดเห็น (ความถี่)					รวม	ค่าเฉลี่ย	SD	ระดับ
	1	2	3	4	5				
ลักษณะการก่อการร้ายทางไซเบอร์และนำมาเป็นเครื่องมือทางยุทธศาสตร์ในการก่อการร้าย									
15.การเผยแพร่วิดีโอเพื่อถ่ายทอดแนวคิด, อุดมการณ์, วิธีการก่อการร้ายเพื่อการโน้มน้าวให้เกิดการชักจูงใจให้เชื่อสามารถนำไปสู่การก่อการร้ายได้	8	41	197	326	118	690	3.74	0.85	มาก
16.การดักฟังทางอิเล็กทรอนิกส์เป็นวิธีการของการก่อการร้าย เช่น ความต้องการข้อมูลทางการเมือง, ทางอุตสาหกรรม, ทางความมั่นคงของประเทศ เป็นต้น	7	38	179	330	136	690	3.80	0.85	มาก
17.การใช้เทคโนโลยีสารสนเทศทางไซเบอร์ในการขู่เข็ญ, ล่วงละเมิดและคุกคามจากข้อมูลข่าวสาร เป็นวิธีในการก่อการร้าย	10	48	215	295	122	690	3.72	0.87	มาก
18.กลุ่มผู้ก่อการร้ายใช้วิธีการที่รุนแรงในการก่อวินาศกรรมที่มีความหลากหลายมากขึ้น เช่น ระเบิดพลีชีพ อากาศยานไร้คนขับ การสอดแนมข้อมูล การปล่อยไวรัสเพื่อทำลายโครงสร้างพื้นฐานของประเทศ	6	34	178	311	161	690	3.86	0.86	มาก
19.ผู้ก่อการร้ายทางไซเบอร์ สามารถเป็นใครก็ได้ขอให้มีความรู้ทางไซเบอร์ และทางเทคโนโลยี ก็สามารถก่อการร้ายทางไซเบอร์ได้	7	36	201	308	138	690	3.79	0.87	มาก

ประเด็นยุทธศาสตร์ (n=690)	ระดับความคิดเห็น (ความถี่)					รวม	ค่าเฉลี่ย	SD	ระดับ
	1	2	3	4	5				
ลักษณะการก่อการร้ายทางไซเบอร์และนำมาเป็นเครื่องมือทางยุทธศาสตร์ในการก่อการร้าย									
20.กฎหมายที่เกี่ยวกับไซเบอร์ เพื่อดูแล ป้องกัน และควบคุมการดำเนินการทางไซเบอร์ยังไม่ครอบคลุมและบังคับใช้อย่างแท้จริง	8	37	165	303	177	690	3.89	0.88	มาก
21.ประเทศไทยยังไม่มีหน่วยงานหรือองค์กรที่เป็นเจ้าภาพหลักเพื่อดูแล ติดตามและควบคุมการดำเนินการรวมถึงการแก้ปัญหาทางไซเบอร์ทั้งหมด	11	28	182	321	148	690	3.84	0.86	มาก
22.การป้องกันทางไซเบอร์ของประเทศไทยต้องเกิดจากความร่วมมือกันระหว่างหน่วยงาน ทั้งภาครัฐ เอกชน และประชาชนทั้งประเทศ	4	20	177	293	196	690	3.97	0.83	มาก
23.ผลที่เกิดขึ้นจากการก่อการร้ายทางไซเบอร์ ส่งผลต่อความเสียหายทั้งทางกายภาพ และรุนแรงในระดับความมั่นคงของประเทศไทย	4	31	182	341	159	690	3.88	0.82	มาก
24.เป้าหมายของการก่อการร้ายทางไซเบอร์ในอนาคต คือ การพัฒนาไซเบอร์ให้มีความสามารถในการใช้เป็นเครื่องมือต่อการก่อการร้ายทางการเมืองในระดับประเทศหรือระหว่างประเทศ ซึ่งยากต่อการป้องกันและควบคุมได้	5	30	182	336	137	690	3.85	0.82	มาก

ประเด็นยุทธศาสตร์ (n=690)	ระดับความคิดเห็น (ความถี่)					รวม	ค่าเฉลี่ย	SD	ระดับ
	1	2	3	4	5				
ลักษณะการก่อการร้ายทางไซเบอร์และนำมาเป็นเครื่องมือทางยุทธศาสตร์ในการก่อการร้าย									
25.การพัฒนาทางไซเบอร์อย่างรวดเร็วจะส่งผลต่อการนำมาใช้เป็นเครื่องมือในก่อการร้ายในอนาคตอย่างแน่นอน	5	40	184	307	154	690	3.83	0.85	มาก
รวม	110	649	3590	6110	3148	13607	3.82	0.56	มาก

จากตารางที่11 ประเด็นลักษณะการก่อการร้ายทางไซเบอร์และนำมาเป็นเครื่องมือทางยุทธศาสตร์ในการก่อการร้ายกลุ่มตัวอย่างมีความคิดเห็นในระดับมาก โดยมีค่าเฉลี่ย 3.82 ส่วนเบี่ยงเบนมาตรฐาน 0.56เมื่อพิจารณาเป็นรายข้อพบว่า ข้อที่มีระดับความคิดเห็นสูง 3 อันดับแรก คือ

1. ข้อที่กลุ่มตัวอย่างมีความคิดเห็นสูงที่สุด คือ การป้องกันทางไซเบอร์ของประเทศไทยต้องเกิดจากความร่วมมือกันระหว่างหน่วยงาน ทั้งภาครัฐ เอกชน และประชาชนทั้งประเทศ มีความคิดเห็นในระดับมาก โดยมีค่าเฉลี่ย 3.97 ส่วนเบี่ยงเบนมาตรฐาน 0.83

2. ข้อที่กลุ่มตัวอย่างมีความคิดเห็นสูงเป็นอันดับที่สอง คือ การก่อการร้ายทางไซเบอร์เป็นการใช้เครื่องมือทางเทคโนโลยี เช่น โทรศัพท์มือถือ คอมพิวเตอร์ หรือเครื่องมือประเภทอื่น ๆ ที่เชื่อมต่อทางอินเทอร์เน็ตเพื่อการก่อการร้าย/อินเทอร์เน็ตเป็นช่องทางที่สำคัญที่ใช้ในการก่อการร้าย เช่น ลักลอบขโมยข้อมูลข่าวสารเพื่อมุ่งเป้าทางการเมือง ปล่อยไวรัสเพื่อทำลายระบบต่าง ๆมีความคิดเห็นในระดับมาก โดยมีค่าเฉลี่ย 3.90 เท่ากัน ส่วนเบี่ยงเบนมาตรฐาน 0.76และ 0.81 ตามลำดับ

3. ข้อที่กลุ่มตัวอย่างมีความคิดเห็นสูงเป็นอันดับที่สาม คือ กฎหมายที่เกี่ยวกับไซเบอร์เพื่อดูแล ป้องกัน และควบคุมการดำเนินการทางไซเบอร์ยังไม่ครอบคลุมและบังคับใช้อย่างแท้จริง มีความคิดเห็นในระดับมาก โดยมีค่าเฉลี่ย 3.89 ส่วนเบี่ยงเบนมาตรฐาน 0.88

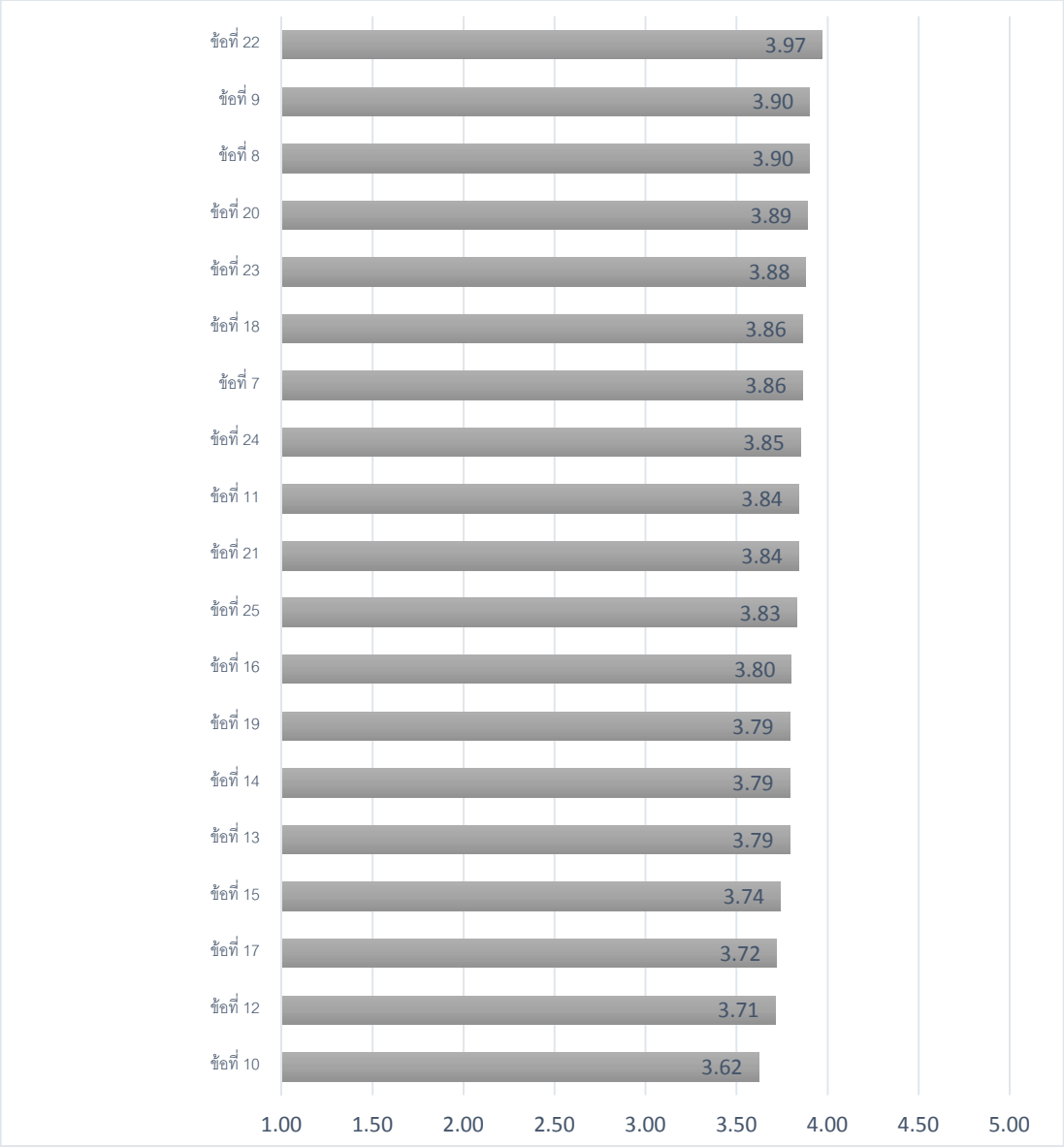
ข้อที่มีระดับความคิดเห็นต่ำ 3 อันดับแรก คือ

1. ข้อที่กลุ่มตัวอย่างมีความคิดเห็นต่ำที่สุด คือ การก่อการร้ายทางไซเบอร์เป็นการกระทำเพื่อความสนุกความพึงพอใจและสร้างชื่อเสียงให้กับผู้กระทำโดยมีแรงจูงใจประสงค์ทางการเมืองเป็นสำคัญ มีความคิดเห็นในระดับมาก โดยมีค่าเฉลี่ย 3.62 ส่วนเบี่ยงเบนมาตรฐาน 0.88

2. ข้อที่กลุ่มตัวอย่างมีความคิดเห็นต่ำเป็นอันดับที่สอง คือ การก่อการร้ายทางไซเบอร์ในประเทศไทย เป้าหมายที่สำคัญคือ ความต้องการทำลายหรือสร้างความเสียหาย ความหวาดกลัว ที่มี

วัตถุประสงค์ทางการเมืองเป็นสำคัญ มีความคิดเห็นในระดับมาก โดยมีค่าเฉลี่ย 3.71 ส่วนเบี่ยงเบนมาตรฐาน 0.68

3. ข้อที่กลุ่มตัวอย่างมีความคิดเห็นต่ำเป็นอันดับที่สาม คือ การใช้เทคโนโลยีสารสนเทศทางไซเบอร์ในการขู่เข็ญ ล่วงละเมิดและคุกคามจากข้อมูลข่าวสาร เป็นวิธีในการก่อการร้าย มีความคิดเห็นในระดับมาก โดยมีค่าเฉลี่ย 3.72 ส่วนเบี่ยงเบนมาตรฐาน 0.87



ภาพที่ ระดับความคิดเห็นจำแนกตามประเด็นลักษณะการก่อการร้ายทางไซเบอร์ (Cyber) และนำมาเป็นเครื่องมือทางยุทธศาสตร์ในการก่อการร้าย

ส่วนที่ 3 ความคิดเห็นต่อยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย

ตารางที่ 12 การนำเสนอระดับความคิดเห็นจำแนกตามประเด็นยุทธศาสตร์

ประเด็นยุทธศาสตร์ (n=690)	ระดับความคิดเห็น (ความถี่)					รวม	ค่าเฉลี่ย	SD	ระดับ
	1	2	3	4	5				
R: Research ยุทธศาสตร์การเสริมสร้างงานวิจัยเพื่อการพัฒนาทางไซเบอร์	9	14	141	350	176	690	3.98	0.79	มาก
E: Education ยุทธศาสตร์การจัดการศึกษาในการสร้างพื้นฐานของประชาชนในประเทศไทย	8	21	147	334	180	690	3.97	0.81	มาก
A: Awareness ยุทธศาสตร์การสร้างการตระหนักรู้ทางไซเบอร์ให้กับประชาชน	12	19	155	320	184	690	3.95	0.83	มาก
D: Developmentยุทธศาสตร์การพัฒนาความก้าวหน้าทางไซเบอร์	5	17	150	326	192	690	4.00	0.80	มาก
C: Coordinateยุทธศาสตร์การส่งเสริมความร่วมมือระหว่างภาครัฐ เอกชน และภาคประชาชน	6	28	136	298	222	690	4.02	0.85	มาก
L: Law ยุทธศาสตร์การกำหนดใช้กฎหมายทางไซเบอร์และการบังคับใช้กับประชาชน	11	38	161	311	169	690	3.88	0.89	มาก
I: Integration ยุทธศาสตร์การใช้การบูรณาการร่วมกันเพื่อการแบ่งปันข้อมูล	6	30	153	321	180	690	3.93	0.84	มาก
P: Perception Prepares and Protect ยุทธศาสตร์การรับรู้ทางไซเบอร์ร่วมกันตระเตรียมและปกป้องทางไซเบอร์	12	43	139	297	199	690	3.92	0.92	มาก
ภาพรวม	69	210	1182	2557	1502	5520	3.96	0.67	มาก

จากตารางที่ 12 ระดับความคิดเห็นต่อประเด็นยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์โดยภาพรวมพบว่า กลุ่มตัวอย่างมีความคิดเห็นในระดับมาก โดยมีค่าเฉลี่ย 3.96 ส่วนเบี่ยงเบนมาตรฐาน 0.67

เมื่อพิจารณาเป็นรายประเด็น พบว่า ข้อที่มีระดับความคิดเห็นสูงเรียงลำดับลงไปน้อยที่สุด คือ

1. ข้อที่กลุ่มตัวอย่างมีความคิดเห็นสูงที่สุด คือC: Coordinateยุทธศาสตร์การส่งเสริมความร่วมมือระหว่างภาครัฐ เอกชน และภาคประชาชนมีความคิดเห็นในระดับมาก โดยมีค่าเฉลี่ย 4.02 ส่วนเบี่ยงเบนมาตรฐาน 0.85

2. ข้อที่กลุ่มตัวอย่างมีความคิดเห็นเป็นอันดับที่สองคือ D: Developmentยุทธศาสตร์การพัฒนาความก้าวหน้าทางไซเบอร์ มีความคิดเห็นในระดับมาก โดยมีค่าเฉลี่ย 4.00 ส่วนเบี่ยงเบนมาตรฐาน 0.80

3. ข้อที่กลุ่มตัวอย่างมีความคิดเห็นเป็นอันดับที่สามคือ R: Research ยุทธศาสตร์การเสริมสร้างงานวิจัยเพื่อการพัฒนาทางไซเบอร์ มีความคิดเห็นในระดับมาก โดยมีค่าเฉลี่ย 3.98 ส่วนเบี่ยงเบนมาตรฐาน 0.79

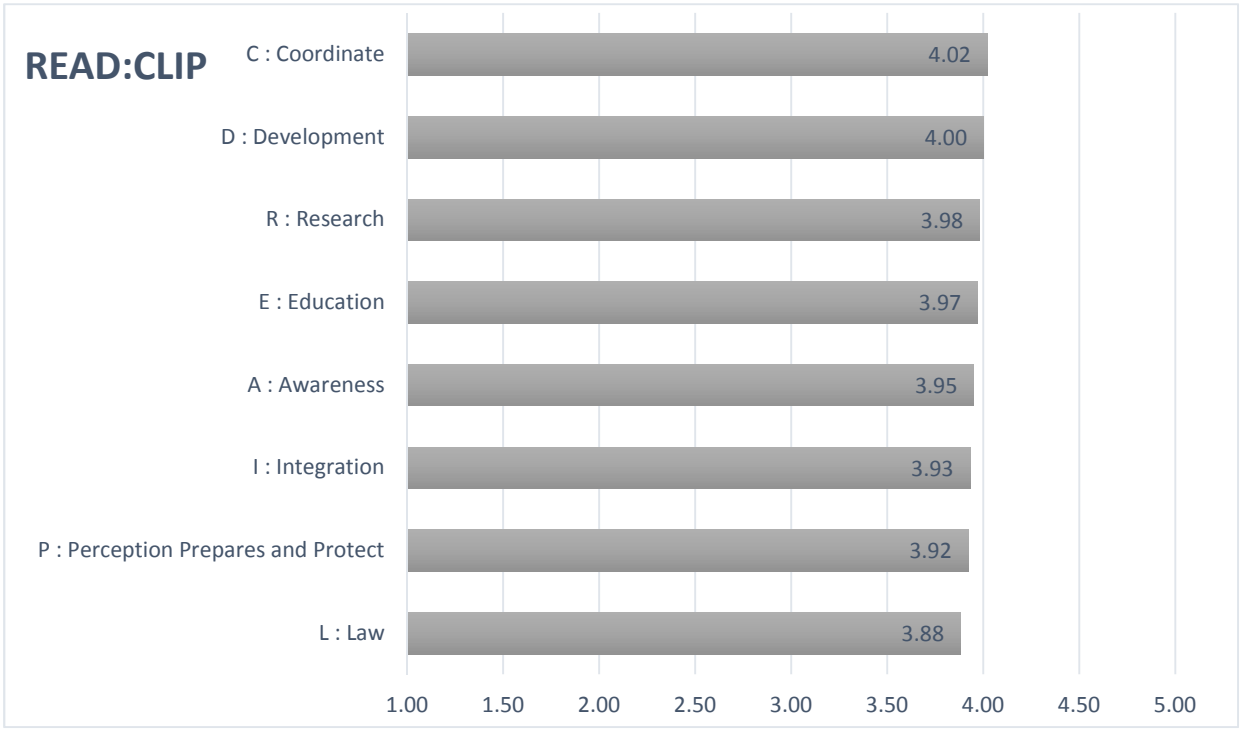
4. ข้อที่กลุ่มตัวอย่างมีความคิดเห็นเป็นอันดับที่สี่คือ E: Education ยุทธศาสตร์การจัดการศึกษาในการสร้างพื้นฐานของประชาชนในประเทศไทย มีความคิดเห็นในระดับมาก โดยมีค่าเฉลี่ย 3.97 ส่วนเบี่ยงเบนมาตรฐาน 0.81

5. ข้อที่กลุ่มตัวอย่างมีความคิดเห็นเป็นอันดับที่ห้าคือ A: Awareness ยุทธศาสตร์การสร้างการตระหนักรู้ทางไซเบอร์ให้กับประชาชน มีความคิดเห็นในระดับมาก โดยมีค่าเฉลี่ย 3.95 ส่วนเบี่ยงเบนมาตรฐาน 0.83

6. ข้อที่กลุ่มตัวอย่างมีความคิดเห็นเป็นอันดับที่หกคือ I: Integration ยุทธศาสตร์การใช้การบูรณาการร่วมกันเพื่อการแบ่งปันข้อมูล มีความคิดเห็นในระดับมาก โดยมีค่าเฉลี่ย 3.93 ส่วนเบี่ยงเบนมาตรฐาน 0.84

7. ข้อที่กลุ่มตัวอย่างมีความคิดเห็นเป็นอันดับที่เจ็ดคือ P: Perception Prepares and Protect ยุทธศาสตร์การรับรู้ทางไซเบอร์ร่วมกัน ตระเตรียมและปกป้องทางไซเบอร์ มีความคิดเห็นในระดับมาก โดยมีค่าเฉลี่ย 3.92 ส่วนเบี่ยงเบนมาตรฐาน 0.92

8. ข้อที่กลุ่มตัวอย่างมีความคิดเห็นน้อยที่สุดคือ L: Law ยุทธศาสตร์การกำหนดใช้กฎหมายทางไซเบอร์และการบังคับใช้กับประชาชน มีความคิดเห็นในระดับมาก โดยมีค่าเฉลี่ย 3.88 ส่วนเบี่ยงเบนมาตรฐาน 0.89



ภาพที่ ระดับความคิดเห็นจำแนกตามประเด็นยุทธศาสตร์

ส่วนที่ 4 ผลการวิเคราะห์ปัจจัยส่วนบุคคลกับประเด็นความก้าวหน้าทางไซเบอร์และการนำยุทธศาสตร์มาเป็นเครื่องมือในการก่อการร้ายในประเทศไทย

ตารางที่ 13 การนำเสนอการวิเคราะห์ปัจจัยส่วนบุคคลกับประเด็นความก้าวหน้าทางไซเบอร์

ลำดับที่	ประเด็นความก้าวหน้าทางไซเบอร์	ปัจจัยส่วนบุคคล				
		เพศ (t– test)	อายุ (t–test)	การศึกษา (t– test)	อาชีพ (t– test)	รายได้ (t–test)
1	การใช้โทรศัพท์มือถือ แท็บเล็ต คอมพิวเตอร์และเครื่องมืออื่น ๆ ที่สามารถเชื่อมต่ออินเทอร์เน็ตพร้อมทั้งมีความเร็วสูงเป็นความก้าวหน้าทางไซเบอร์	.860	.258	1.090	3.949	3.035
2	Application ของโทรศัพท์มือถือที่สามารถอำนวยความสะดวกและมีการเชื่อมต่ออย่างรวดเร็วส่งผลต่อความก้าวหน้าทางไซเบอร์	2.179	1.502	2.412	.731	1.264
3	จุดเชื่อมต่ออินเทอร์เน็ตสาธารณะและเน็ตเวิร์คความเร็วสูงจะส่งผลให้สังคมเครือข่าย, โทรศัพท์มือถือและการให้บริการจัดเก็บข้อมูลบนอินเทอร์เน็ตเกิดการขยายตัวและแพร่หลายเข้าถึงคนไทยทุกคน	3.102	.935	.376	.293	.464
4	ความก้าวหน้าทางไซเบอร์ คือการพัฒนาทางเทคโนโลยีที่สามารถเชื่อมต่อกันได้อย่างรวดเร็วสะดวกขึ้น ทำให้ทุกคนติดต่อกันได้ไม่ว่าจะอยู่ที่ใดในโลก	.460	1.735	1.995	2.576	2.001
5	การพัฒนาของแพลตฟอร์ม (Platform) หรือระบบปฏิบัติการสามารถที่จะพัฒนาไปสู่ระบบเว็บ 3.0 และ 4.0 ที่สามารถตัดสินใจแทนมนุษย์ในอนาคต	.611	1.164	2.626	1.610	2.567

ลำดับที่	ประเด็นความก้าวหน้าทางไซเบอร์	ปัจจัยส่วนบุคคล				
		เพศ (t– test)	อายุ (t–test)	การศึกษา (t– test)	อาชีพ (t– test)	รายได้ (t–test)
6	ปัจจุบันนี้คนไทยจะสามารถเชื่อมต่อออนไลน์กับโลกเสมือนทำให้รู้สึกเท่าเทียมกับคนทั่วโลก สามารถเข้าถึงแพลตฟอร์มพื้นฐาน สารสนเทศและข้อมูลทุกอย่างในทางออนไลน์ได้	2.887	1.650	.140	1.240	1.166

จากตารางที่13 จากการทดสอบสมมุติฐานพบว่าความคิดเห็นของปัจจัยส่วนบุคคลด้านเพศ ด้านอายุและด้านการศึกษา มีผลต่อความก้าวหน้าทางไซเบอร์ การแสดงความคิดเห็นอย่างมีนัยสำคัญที่ 0.05

ตารางที่ 14การนำเสนอการวิเคราะห์ปัจจัยส่วนบุคคลกับประเด็นลักษณะการก่อการร้ายทางไซเบอร์ (Cyber) และนำมาเป็นเครื่องมือยุทธศาสตร์ในการก่อการร้าย

ลำดับที่	ประเด็นลักษณะการก่อการร้ายทางไซเบอร์ (Cyber) และนำมาเป็นเครื่องมือยุทธศาสตร์ในการก่อการร้าย	ปัจจัยส่วนบุคคล				
		เพศ (t– test)	อายุ (t-test)	การศึกษา (t– test)	อาชีพ (t– test)	รายได้ (t - test)
7	การก่อการร้ายทางไซเบอร์ คือ การนำไซเบอร์มาเป็นเครื่องมือในการก่อการร้ายโดยมีวัตถุประสงค์เพื่อให้เกิดความรุนแรง รู้สึกหวาดกลัว คุกคามรัฐบาลหรือกลุ่มสังคมใด ๆ โดยมีแรงจูงใจทางการเมืองเป็นหลัก	2.213	1.933	2.002	1.253	2.139
8	การก่อการร้ายทางไซเบอร์เป็นการใช้เครื่องมือทางเทคโนโลยี เช่น โทรศัพท์มือถือ คอมพิวเตอร์ หรือเครื่องมือประเภทอื่น ๆ ที่เชื่อมต่อทางอินเทอร์เน็ตเพื่อการก่อการร้าย	8.608	.998	2.458	.600	.862
9	อินเทอร์เน็ตเป็นช่องทางที่สำคัญที่ใช้ในการก่อการร้าย เช่น ลักลอบขโมยข้อมูลข่าวสารเพื่อมุ่งเป้าทางการเมือง ปล่อยไวรัสเพื่อทำลายระบบต่าง ๆ	4.261	.555	1.941	.956	.528
10	การก่อการร้ายทางไซเบอร์เป็นการกระทำเพื่อความสนุกความพึงพอใจและสร้างชื่อเสียงให้กับผู้กระทำโดยมีแรงจูงใจประสงค์ทางการเมืองเป็นสำคัญ	2.681	1.727	1.129	.815	.587
11	การหลอกลวงทางโทรศัพท์ เช่น การหลอกให้โอนเงินไปให้การหลอกลวงว่าได้รับรางวัล หรือ การหลอกลวงโดยขู่ว่า	1.182	1.769	1.357	.296	1.070

ลำดับที่	ประเด็นลักษณะการก่อการร้ายทางไซเบอร์ (Cyber) และนำมาเป็นเครื่องมือยุทธศาสตร์ในการก่อการร้าย	ปัจจัยส่วนบุคคล				
		เพศ (t– test)	อายุ (t-test)	การศึกษา (t– test)	อาชีพ (t– test)	รายได้ (t - test)
	เป็นหนี้บัตรเครดิต พูดจาหว่านล้อมให้ไปทำธุรกรรมทางตู้เอทีเอ็ม ฯ เป็นวิธีการที่นำไปสู่การก่อการร้ายได้					
12	การก่อการร้ายทางไซเบอร์ในประเทศไทย เป้าหมายที่สำคัญคือ ความต้องการทำลายหรือสร้างความเสียหาย ความหวาดกลัว ที่มีวัตถุประสงค์ทางการเมืองเป็นสำคัญ	7.272	2.006	.839	.727	2.257
13	วิธีการปฏิบัติการหลักของการก่อการร้ายทาง ไซเบอร์คือ ศึกษาข้อมูลที่ต้องการเจาะช่องโหว่หาเครื่องมือในการทำลายและดำเนินการก่อการร้ายทางไซเบอร์	7.641	.946	2.329	.763	1.951
14	การใช้ไซเบอร์เป็นเครื่องมือเช่น การโฆษณาชวนเชื่อ การชักจูง สาธิตวิดีโอการสอนให้ทำอุปกรณ์วางเพลิงและวัตถุระเบิด สามารถเป็นสาเหตุของก่อการร้ายได้	1.537	.537	1.475	.590	2.062
15	การเผยแพร่วิดีโอเพื่อถ่ายทอดแนวคิดอุดมการณ์ วิธีการก่อการร้ายเพื่อการโน้มน้าวให้เกิดการชักจูงใจให้เชื่อสามารถนำไปสู่การก่อการร้ายได้	2.951	1.957	1.096	.188	.909
16	การดักฟังทางอิเล็กทรอนิกส์เป็นวิธีการของการก่อการร้าย เช่น ความต้องการข้อมูลทางการเมือง ทางอุตสาหกรรม ทางความมั่นคงของประเทศ เป็นต้น	.997	1.491	1.913	.088	.306

ลำดับที่	ประเด็นลักษณะการก่อการร้ายทางไซเบอร์ (Cyber) และนำมาเป็นเครื่องมือยุทธศาสตร์ในการก่อการร้าย	ปัจจัยส่วนบุคคล				
		เพศ (t– test)	อายุ (t-test)	การศึกษา (t– test)	อาชีพ (t– test)	รายได้ (t - test)
17	การใช้เทคโนโลยีสารสนเทศทางไซเบอร์ในการขู่เข็ญ ล่วงละเมิดและคุกคามจากข้อมูลข่าวสาร เป็นวิธีในการก่อการร้าย	4.999	1.330	.422	1.507	1.448
18	กลุ่มผู้ก่อการร้ายใช้วิธีการที่รุนแรงในการก่อวินาศกรรมที่มีความหลากหลายมากขึ้น เช่น ระเบิดพลีชีพ อากาศยานไร้คนขับ การสอดแนมข้อมูล การปล่อยไวรัสเพื่อทำลายโครงสร้างพื้นฐานของประเทศ	4.850	.687	3.862	.193	1.044
19	ผู้ก่อการร้ายทางไซเบอร์ สามารถเป็นใครก็ได้ขอให้มีความรู้ทางไซเบอร์ และทางเทคโนโลยี ก็สามารถก่อการร้ายทางไซเบอร์ได้	4.565	.831	1.731	1.087	1.486
20	กฎหมายที่เกี่ยวกับไซเบอร์ เพื่อดูแลป้องกันและควบคุมการดำเนินการทางไซเบอร์ยังไม่ครอบคลุมและบังคับใช้อย่างแท้จริง	3.935	.766	1.624	.520	2.768
21	ประเทศไทยยังไม่มีหน่วยงานหรือองค์กรที่เป็นเจ้าภาพหลักเพื่อดูแลติดตามและควบคุมการดำเนินการรวมถึงการแก้ปัญหาทางไซเบอร์ทั้งหมด	2.368	.139	2.477	2.327	.581
22	การป้องกันทางไซเบอร์ของประเทศไทยต้องเกิดจากความร่วมมือกันระหว่างหน่วยงาน ทั้งภาครัฐ เอกชน และประชาชนทั้งประเทศ	.809	1.991	1.476	2.213	1.375

ลำดับที่	ประเด็นลักษณะการก่อการร้ายทางไซเบอร์ (Cyber) และนำมาเป็นเครื่องมือยุทธศาสตร์ในการก่อการร้าย	ปัจจัยส่วนบุคคล				
		เพศ (t– test)	อายุ (t-test)	การศึกษา (t– test)	อาชีพ (t– test)	รายได้ (t - test)
23	ผลที่เกิดขึ้นจากการก่อการร้ายทางไซเบอร์ ส่งผลต่อความเสียหายทั้งทางกายภาพ และรุนแรงในระดับความมั่นคงของประเทศไทย	3.311	.627	1.202	1.166	.346
24	เป้าหมายของการก่อการร้ายทางไซเบอร์ในอนาคต คือ การพัฒนาไซเบอร์ให้มีความสามารถในการใช้เป็นเครื่องมือต่อการก่อการร้ายทางการเมืองในระดับประเทศหรือระหว่างประเทศ ซึ่งยากต่อการป้องกันและควบคุมได้	.621	.761	2.129	1.507	1.069
25	การพัฒนาทางไซเบอร์อย่างรวดเร็วจะส่งผลต่อการนำมาใช้เป็นเครื่องมือในก่อการร้ายในอนาคตอย่างแน่นอน	3.441	1.067	2.546	1.150	1.049

จากตารางที่ 14จากการทดสอบสมมุติฐานพบว่าความคิดเห็นของปัจจัยส่วนบุคคลด้านอายุและด้านอาชีพ มีผลต่อการนำยุทธศาสตร์มาเป็นเครื่องมือในการก่อการร้ายทางไซเบอร์ในประเทศไทยการแสดงความคิดเห็นอย่างมีนัยสำคัญที่ 0.05 ส่วนปัจจัยด้านเพศ ด้านการศึกษาและด้านรายได้ การแสดงความคิดเห็นอย่างไม่มีนัยสำคัญที่ 0.05แสดงว่าไม่มีผลต่อการนำยุทธศาสตร์มาเป็นเครื่องมือในการก่อการร้ายทางไซเบอร์ในประเทศไทย

ตารางที่15 การนำเสนอการวิเคราะห์ข้อมูลปัจจัยส่วนบุคคลกับประเด็นยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย

ลำดับที่	ประเด็นยุทธศาสตร์การต่อต้านการก่อการร้ายในประเทศไทย	ปัจจัยส่วนบุคคล				
		เพศ (t–test)	อายุ (t– test)	การศึกษา (t– test)	อาชีพ (t– test)	รายได้ (t-test)
1	R : Research ยุทธศาสตร์การเสริมสร้างงานวิจัยเพื่อการพัฒนาทางไซเบอร์	3.848	1.983	1.932	3.061	2.509
2	E : Education ยุทธศาสตร์การจัดการศึกษาในการสร้างพื้นฐานของประชาชนในประเทศไทย	.188	.845	2.326	.344	.702
3	A : Awareness ยุทธศาสตร์การสร้างการตระหนักรู้ทางไซเบอร์ให้กับประชาชน	.052	1.664	1.838	.643	.956
4	D : Developmentยุทธศาสตร์การพัฒนาความก้าวหน้าทางไซเบอร์	.232	1.771	1.077	.277	1.085
5	C : Coordinateยุทธศาสตร์การส่งเสริมความร่วมมือระหว่างภาครัฐ เอกชน และภาคประชาชน	1.273	1.155	2.365	.442	1.401
6	L : Law ยุทธศาสตร์การกำหนดใช้กฎหมายทางไซเบอร์และการบังคับใช้กับประชาชน	2.461	.867	2.370	.053	2.880
7	I : Integration ยุทธศาสตร์การใช้การบูรณาการร่วมกันเพื่อการแบ่งปันข้อมูล	.060	.383	3.850	1.112	2.542
8	P : Perception Prepares and Protect ยุทธศาสตร์การรับรู้ทางไซเบอร์ร่วมกันตระเตรียมและปกป้องทางไซเบอร์	0.53	1.839	2.114	.518	1.452

จากตารางที่15 จากการทดสอบสมมุติฐานพบว่าความคิดเห็นของปัจจัยส่วนบุคคลด้านเพศและด้านอายุ มีผลต่อนำยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์มาปรับใช้ในประเทศไทยการแสดงความคิดเห็นอย่างมีนัยสำคัญที่ 0.05ส่วนปัจจัยด้านการศึกษา ด้านอาชีพและด้านรายได้การแสดงความคิดเห็นอย่างไม่มีนัยสำคัญที่ 0.05แสดงว่าไม่มีผลต่อการนำยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์มาปรับใช้ในประเทศไทย

ตารางที่ 16 ความคิดเห็นเพื่อกำหนดยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์

ข้อเสนอแนะ	จำนวน	ร้อยละ
1.ควรจัดตั้งหน่วยงาน หรือองค์กรโดยตรงในการกำกับดูแลโดยเฉพาะ และบังคับกฎหมายอย่างจริงจัง	30	44.78
2. อยากให้มีการพัฒนาระบบป้องกันให้มากกว่านี้	10	14.93
3. รัฐควรส่งเสริมให้เยาวชนประชาชน ตระหนักถึงการใช้งานของโลกไซเบอร์อย่างลึกซึ้ง และนำมาใช้เป็นกลไกสำคัญในการป้องกันการก่อการร้ายทางไซเบอร์ และกฎหมายอย่างชัดเจน	9	13.43
4. ควรร่วมมือกันระหว่างภาครัฐและประชาชนอย่างจริงจังโดยสามารถเข้าถึงได้ง่าย เพื่อช่วยเหลือในการตรวจสอบ	5	7.46
5. ควรใช้ไซเบอร์ในการวิจัยและศึกษาให้ถูกต้อง เกิดประโยชน์ต่อสังคม และส่วนรวม	2	2.99
6. พัฒนาโลกไซเบอร์โดยคำนึงถึงการใช้พลังงานทางเลือกการประหยัดพลังงานและอุปกรณ์ เป็นแนวทางในการพัฒนา	2	2.99
7. พัฒนาโลกไซเบอร์ให้มีความทันสมัยมากขึ้น	2	2.99
8. อยากให้ข้อมูลของเครือข่ายตำรวจสามารถเชื่อมโยงแลกเปลี่ยนและตรวจสอบข้อมูลการก่อการร้ายได้ง่าย	1	1.49
9. ควรมีการประชาสัมพันธ์ยุทธศาสตร์ให้ทั่วถึง	1	1.49
10. ควรมีวิจารณญาณในการเสพสื่อจากอินเตอร์เน็ต	1	1.49
11. ควรพัฒนาเครือข่ายออนไลน์ด้านสารสนเทศ ข่าวสารบ้านเมือง เพื่อการเข้าถึงสื่อต่าง ๆ ได้ครอบคลุมมากขึ้น	1	1.49
12. ควรมีการอบรมแก่ผู้ตรวจสอบเกี่ยวกับไซเบอร์ เพื่อ	1	1.49

ข้อเสนอแนะ	จำนวน	ร้อยละ
ป้องกันปัญหาการก่อการร้ายทางไซเบอร์		
13. ควรมีการจำกัดขอบเขตในการเข้าใช้โลกไซเบอร์ ไม่ให้สามารถเจาะข้อมูลเชิงลึกเพื่อก่อการร้ายทางไซเบอร์	1	1.49
14. ให้ขึ้นทะเบียนจากหมายเลขบัตรประจำตัวประชาชน	1	1.49
ภาพรวม	67	100.00

จากตารางที่ 16 แสดงข้อเสนอแนะของกลุ่มตัวอย่างต่อประเด็นยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ พบว่า ควรจัดตั้งหน่วยงาน หรือองค์กรโดยตรงในการกำกับดูแลโดยเฉพาะ และบังคับกฎหมายอย่างจริงจัง มากที่สุด จำนวน 30 คน คิดเป็นร้อยละ 44.78 รองลงมาคือ อยากให้มีการพัฒนาระบบป้องกันให้มากกว่านี้ จำนวน 10 คน คิดเป็นร้อยละ 14.93 รัฐควรส่งเสริมให้เยาวชน ประชาชน ตระหนักถึงการใช้งานของโลกไซเบอร์อย่างลึกซึ้ง และนำมาใช้เป็นกลไกสำคัญในการป้องกันการก่อการร้ายทางไซเบอร์ และกฎหมายอย่างชัดเจน จำนวน 9 คน คิดเป็นร้อยละ 13.43 ควรร่วมมือกันระหว่างภาครัฐและประชาชนอย่างจริงจัง โดยสามารถเข้าถึงได้ง่าย เพื่อช่วยเหลือในการตรวจสอบ จำนวน 5 คน คิดเป็นร้อยละ 7.46 ควรใช้ไซเบอร์ในการวิจัยและศึกษาให้ถูกต้อง เกิดประโยชน์ต่อสังคม และส่วนรวม/พัฒนาโลกไซเบอร์โดยคำนึงถึงการใช้พลังงานทางเลือก การประหยัดพลังงานและอุปกรณ์ เป็นแนวทางในการพัฒนา/พัฒนาโลกไซเบอร์ให้มีความทันสมัยมากขึ้น จำนวนข้อละ 2 คน คิดเป็นร้อยละ 2.99 ของแต่ละข้อ ให้ขึ้นทะเบียนจากหมายเลขบัตรประจำตัวประชาชน/อยากให้ข้อมูลของเครือข่ายตำรวจสามารถเชื่อมโยง แลกเปลี่ยนและตรวจสอบข้อมูลการก่อการร้ายได้ง่ายยิ่งขึ้น/ควรมีการประชาสัมพันธ์ยุทธศาสตร์ให้ทั่วถึง/ควรมีวิจารณญาณในการเสพสื่อจากอินเตอร์เน็ต/ควรพัฒนาเครือข่ายออนไลน์ด้านสารสนเทศ ข่าวสารบ้านเมือง เพื่อการเข้าถึงสื่อต่าง ๆ ได้ครอบคลุมมากขึ้น/ควรมีการอบรมแก่ผู้ตรวจสอบเกี่ยวกับไซเบอร์ เพื่อป้องกันปัญหาการก่อการร้ายทางไซเบอร์/ควรมีการจำกัดขอบเขตในการเข้าใช้โลกไซเบอร์ ไม่ให้สามารถเจาะข้อมูลเชิงลึกเพื่อก่อการร้ายทางไซเบอร์จำนวนข้อละ 1 คน คิดเป็นร้อยละ 1.49 ของแต่ละข้อ

สรุปผลการทดสอบสมมุติฐานการวิจัย

จากสมมติฐานข้อที่ 1 พบว่า ข้อเท็จจริง เชิงคุณภาพ พบว่า จากการค้นคว้าเอกสารและงานวิจัยที่เกี่ยวข้องและผู้ให้สัมภาษณ์ให้ความคิดเห็นในประเด็นของความก้าวหน้าทางไซเบอร์สอดคล้องไปในทางเดียวกันว่า การก่อการร้ายได้นำความก้าวหน้าทางเทคโนโลยีที่มีความก้าวหน้า

สูงจะฉวยโอกาสเอาความก้าวหน้าทางไซเบอร์มาใช้ในการก่อการร้าย เมื่อความก้าวหน้าทางไซเบอร์มีการพัฒนาอย่างรวดเร็วและมีเครื่องมือที่สามารถนำมาใช้เพื่อประโยชน์ในการก่อการร้าย ทั้ง คอมพิวเตอร์ โทรศัพท์มือถือ แท็บเล็ต คอมพิวเตอร์ หรืออุปกรณ์ที่สามารถเชื่อมต่ออินเทอร์เน็ตได้ และการนำสังคมออนไลน์ทั้ง เฟซบุ๊กไลน์ทวิสเตอร์ที่มีการติดต่อสื่อสารกันทั่วโลก มาใช้เป็นช่องทางของการนำไปสู่การก่อการร้าย

ข้อเท็จจริง เชิงปริมาณ พบว่า จากการทดสอบสมมุติฐาน ด้วยสถิติทดสอบ t – test ความคิดเห็นของเพศ และอายุ มีการแสดงความคิดเห็นอย่างมีนัยสำคัญที่ 0.05 นำมาสู่ข้อสรุป ดังนี้ การก่อการร้ายที่มีความก้าวหน้าทางเทคโนโลยีสูงจะนำเอาความก้าวหน้าทางไซเบอร์มาฉวยโอกาสในการก่อการร้ายเพื่อเป็นประโยชน์ในการก่อการร้าย สอดคล้องกับความคิดเห็นของกลุ่มตัวอย่างจำนวน 690 คน แสดงความคิดเห็นอย่างมีนัยสำคัญที่ 0.05 สรุปผลได้ว่า การก่อการร้ายมีเทคโนโลยีความก้าวหน้าสูงกว่าความก้าวหน้าทางไซเบอร์จะฉวยโอกาสนำความก้าวหน้าทางไซเบอร์เพื่อนำมาใช้ประโยชน์ในการการก่อการร้าย การก่อการร้ายที่มีการใช้เทคโนโลยีความก้าวหน้าสูงเทียบเท่ากับความก้าวหน้าทางไซเบอร์จะฉวยโอกาสนำความก้าวหน้าทางไซเบอร์เพื่อมาใช้ประโยชน์ในการก่อการร้ายอย่างมีนัยสำคัญ

จากสมมติฐานข้อที่ 2 พบว่า ข้อเท็จจริง เชิงคุณภาพ พบว่า จากการค้นคว้าเอกสารและงานวิจัยที่เกี่ยวข้องและผู้ให้สัมภาษณ์ให้ความคิดเห็นในประเด็นประเทศไทยไม่มียุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์และมีความล้าหลังในประเด็นของความก้าวหน้าทางเทคโนโลยีและไซเบอร์ ผู้ก่อการร้ายทางไซเบอร์มียุทธศาสตร์ต่อการกระทำการก่อการร้ายปรับเปลี่ยนตลอดเวลา การแก้ปัญหาการก่อการร้ายของประเทศไทยเป็นการแก้ปัญหาเฉพาะหน้า มากกว่าการวางแนวทางป้องกัน ประเทศไทยมีบริบทของประเทศไทยที่ไม่ใช่เป้าหมายที่สำคัญของการ ก่อการร้าย แต่สามารถเป็นฐานหรือช่องทางในการดำเนินการได้ การจัดการปัญหาการก่อการร้ายจึงความต้องมีความแตกต่างจากประเทศอื่นๆ จากบริบทของประเทศที่มีความแตกต่างกัน

ข้อเท็จจริง เชิงปริมาณ พบว่าจากการทดสอบสมมุติฐาน ด้วยสถิติทดสอบ t – test ความคิดเห็นของเพศและอายุ มีการแสดงความคิดเห็นอย่างมีนัยสำคัญที่ 0.05 นำมาสู่ข้อสรุป ดังนี้ ประเทศไทยมีการพัฒนาความก้าวหน้าทางไซเบอร์แต่น้อยกว่าผู้ใช้ยุทธศาสตร์การก่อการร้าย ควรมีการป้องกันการก่อการร้าย และจัดการปัญหาการก่อการร้ายที่มีความแตกต่างจากประเทศอื่นๆ โดยพิจารณาจากบริบทของประเทศไทยเพื่อจัดทำยุทธศาสตร์ของการต่อต้านการก่อการร้ายทางไซเบอร์ (Cyber) ในประเทศไทยสอดคล้องกับความคิดเห็นของกลุ่มตัวอย่างจำนวน 690 คน แสดงความคิดเห็นอย่างมีนัยสำคัญที่ 0.05สรุปผลได้ว่า ประเทศไทยมีความล้าหลังกว่าผู้ใช้ยุทธศาสตร์การก่อการร้ายแนวทางการพัฒนาหรือการต่อต้านการก่อการร้ายเป็นการแก้ไขมากกว่าการป้องกัน

การจัดการปัญหาการก่อการร้ายควรแตกต่าง เพื่อจัดทำยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ (Cyber) ในประเทศไทย

จากสมมติฐานข้อที่ 3 ข้อเท็จจริง เชิงคุณภาพ พบว่าจากการค้นคว้าเอกสารและงานวิจัยที่เกี่ยวข้องและผู้ให้สัมภาษณ์ให้ความคิดเห็นในประเด็น ประเทศไทยยังไม่มีสถานการณ์ที่สามารถเชื่อมโยงไปสู่การก่อการร้ายทางไซเบอร์ได้ กระบวนการคิดเพื่อวิเคราะห์หรือประเมินการก่อการร้ายต้องมีรูปแบบที่ทำให้เกิดการเรียนรู้ต่อสถานการณ์ของการก่อการร้ายและให้ทุกภาคส่วนมีความร่วมมือกันในการต่อต้านหรือป้องกันการก่อการร้าย

ข้อเท็จจริง เชิงปริมาณ พบว่าจากการทดสอบสมมุติฐาน ด้วยสถิติทดสอบ t – testความคิดเห็นของเพศ และอายุ มีการแสดงความคิดเห็นอย่างมีนัยสำคัญที่ 0.05 นำมาสู่ข้อสรุป ดังนี้ ประเทศไทยต้องมีเครื่องมือที่ช่วยในการวิเคราะห์หรือประเมินสถานการณ์ของการก่อการร้ายที่สะท้อนในเชิงความคิดเพื่อให้ทุกภาคส่วนได้เกิดการเรียนรู้ต่อการเกิดสถานการณ์การก่อการร้าย สอดคล้องกับความคิดเห็นของกลุ่มตัวอย่างจำนวน 690 คน แสดงความคิดเห็นอย่างมีนัยสำคัญที่ 0.05สรุปผลได้ว่า การวิเคราะห์หรือประเมินการก่อการร้ายเครื่องมือที่ใช้ต้องมีวิธีการเรียนรู้ที่สะท้อนในรูปแบบเชิงความคิดที่ต่อต้านหรือป้องกันการก่อการร้ายได้

ตารางที่ 17 วิเคราะห์ อุปสรรค โอกาส จุดอ่อนและจุดแข็งของประเทศไทย (TOWS)

วิเคราะห์ อุปสรรค โอกาส จุดอ่อนและจุดแข็งของประเทศไทย (TOWS)	
อุปสรรค Threats	**โอกาส Opportunity**
1.เศรษฐกิจของโลกมีความผันผวนและไม่มั่นคง 2.ความแปรปรวนของสภาพภูมิอากาศของโลก 3.สถานการณ์การก่อการร้ายที่คุกคามไปทั่วโลก 4.กลุ่มก่อการร้ายมีความเข็มแข็งมากขึ้น 5.การพัฒนาของอาวุธที่มีอานุภาพร้ายแรง เช่น อาวุธชีวภาพ อาวุธนิวเคลียร์ 6.ประเทศมหาอำนาจและประเทศในกลุ่มนับถือศาสนาอิสลาม สร้างความเข็มแข็งและสะสมพลังทางทหารที่มีแสนยานุภาพมาก	1.การสร้างความร่วมมือในภูมิภาคจากการเปิดประตูสู่อาเซียน 2.การขยายตลาดการลงทุนไปยังประเทศเพื่อนบ้าน 3.ความได้เปรียบในการเป็นฐานการผลิตภาคการเกษตร 4.ประเทศไทยส่งเสริมภาคบริการและการท่องเที่ยว 5.โลกไซเบอร์มีเครือข่ายที่ครอบคลุมทั่วโลก
จุดแข็ง Strength	จุดอ่อน Weakness
1.วัฒนธรรมของประเทศไทยที่มีความเข้มแข็ง	1.การเมืองของประเทศไทยยังไม่มั่นคง

วิเคราะห์ อุปสรรค โอกาส จุดอ่อนและจุดแข็งของประเทศไทย (TOWS)	
2.ประเทศไทยเป็นมิตรกับทุกประเทศ 3.ประเทศไทยยังคงมีทั้งระบบเกษตรกรรมและอุตสาหกรรม 4.คนไทยเป็นมิตรและเข้ากันได้ดีกับคนทุกชนชาติ 5.ประเทศไทยสามารถปรับตัวให้มีความพร้อมรับกับทุกสถานการณ์	2.ความเหลื่อมล้ำของรายได้ของประชากรภายในประเทศ 3.ปัญหาความยากจนที่ครอบคลุมในประชากรระดับล่าง 4.ความเป็นระบบอุปถัมภ์ที่มีอย่างถาวรในสังคมไทย 5.ปัญหาคอร์รัปชั่นในประเทศไทย 6.ประเทศไทยเป็นสังคมผู้สูงอายุ

ตารางที่ 18 สรุปการวิเคราะห์กลยุทธ์

สรุปการวิเคราะห์กลยุทธ์		
TOWS Matrix	โอกาส Opportunity	อุปสรรค Threats
	1.การสร้างความร่วมมือในภูมิภาคจากการเปิดประตูสู่อาเซียน 2.การขยายตลาดการลงทุนไปยังประเทศเพื่อนบ้าน 3.ความได้เปรียบในการเป็นฐานการผลิตภาคการเกษตร 4.ประเทศไทยส่งเสริมภาคบริการและการท่องเที่ยว 5.โลกไซเบอร์มีเครือข่ายที่ครอบคลุมทั่วโลก	1.เศรษฐกิจของโลกมีความผันผวนและไม่มั่นคง 2.ความแปรปรวนของสภาพภูมิอากาศของโลก 3.สถานการณ์การก่อการร้ายที่คุกคามไปทั่วโลก 4.กลุ่มก่อการร้ายมีความเข็มแข็งมากขึ้น 5.การพัฒนาของอาวุธที่มีอานุภาพร้ายแรง เช่น อาวุธชีวภาพ อาวุธนิวเคลียร์ 6.ประเทศมหาอำนาจและประเทศในกลุ่มนับถือศาสนาอิสลาม สร้างความเข็มแข็งและสะสม

สรุปการวิเคราะห์กลยุทธ์		
		พลังทางทหารที่มีแสนยานุภาพมาก
จุดแข็ง Strength	กลยุทธ์เชิงรุก SO	กลยุทธ์เชิงป้องกัน ST
1.วัฒนธรรมของประเทศไทยที่มีความเข้มแข็ง 2.ประเทศไทยเป็นมิตรกับทุกประเทศ 3.ประเทศไทยยังคงมีทั้งระบบเกษตรกรรมและอุตสาหกรรม 4.คนไทยเป็นมิตรและเข้ากันได้ดีกับคนทุกชนชาติ 5.ประเทศไทยสามารถปรับตัวให้มีความพร้อมรับกับทุกสถานการณ์	S1.วัฒนธรรมของประเทศไทยที่มีความเข้มแข็ง S2.ประเทศไทยเป็นมิตรกับทุกประเทศ S3.ประเทศไทยยังคงมีทั้งระบบเกษตรกรรมและอุตสาหกรรม S4.คนไทยเป็นมิตรและเข้ากันได้ดีกับคนทุกชนชาติ S5.ประเทศไทยสามารถปรับตัวให้มีความพร้อมรับกับทุกสถานการณ์ O1.การสร้างความร่วมมือในภูมิภาคจากการเปิดประตูสู่อาเซียน O2.การขยายตลาดการลงทุนไปยังประเทศเพื่อนบ้าน O3.ความได้เปรียบในการเป็นฐานการผลิตภาคการเกษตร O4.ประเทศไทยส่งเสริมภาคบริการและการท่องเที่ยว	S1.วัฒนธรรมของประเทศไทยที่มีความเข้มแข็ง S2.ประเทศไทยเป็นมิตรกับทุกประเทศ S3.ประเทศไทยยังคงมีทั้งระบบเกษตรกรรมและอุตสาหกรรม S4.คนไทยเป็นมิตรและเข้ากันได้ดีกับคนทุกชนชาติ S5.ประเทศไทยสามารถปรับตัวให้มีความพร้อมรับกับทุกสถานการณ์ T1.เศรษฐกิจของโลกมีความผันผวนและไม่มั่นคง T2.ความแปรปรวนของสภาพภูมิอากาศของโลก T3.สถานการณ์การก่อการร้ายที่คุกคามไปทั่วโลก T4.กลุ่มก่อการร้ายมีความเข็มแข็งมากขึ้น T5.การพัฒนาของอาวุธที่มีอานุภาพร้ายแรง เช่น

สรุปการวิเคราะห์กลยุทธ์		
	O5. โลกไซเบอร์มีเครือข่ายที่ครอบคลุมทั่วโลก	อาวุธชีวภาพ อาวุธนิวเคลียร์ T6. ประเทศมหาอำนาจและประเทศในกลุ่มนับถือศาสนาอิสลาม สร้างความเข็มแข็งและสะสมพลังทางทหารที่มีแสนยานุภาพมาก
จุดอ่อน Weakness	กลยุทธ์เชิงแก้ไข WO	กลยุทธ์เชิงรับ WT
1.การเมืองของประเทศไทยยังไม่มั่นคง **2.ความเหลื่อมล้ำของรายได้ของประชากรภายในประเทศ** **3.ปัญหาความยากจนที่ครอบคลุมในประชากรระดับล่าง** **4.ความเป็นระบบอุปถัมภ์ที่มีอย่างถาวรในสังคมไทย** **5.ปัญหาคอร์รัปชั่นในประเทศไทย** **6.ประเทศไทยเป็นสังคมผู้สูงอายุ**	W1. การเมืองของประเทศไทยยังไม่มั่นคง W2. ความเหลื่อมล้ำของรายได้ของประชากรภายในประเทศ W3. ปัญหาความยากจนที่ครอบคลุมในประชากรระดับล่าง W4. ความเป็นระบบอุปถัมภ์ที่มีอย่างถาวรในสังคมไทย W5. ปัญหาคอร์รัปชั่นในประเทศไทย W6.ประเทศไทยเป็นสังคมผู้สูงอายุ O1. การสร้างความร่วมมือในภูมิภาคจากการเปิดประตูสู่อาเซียน O2. การขยายตลาดการลงทุนไปยังประเทศเพื่อน	W1.การเมืองของประเทศไทยยังไม่มั่นคง W2. ความเหลื่อมล้ำของรายได้ของประชากรภายในประเทศ W3.ปัญหาความยากจนที่ครอบคลุมในประชากรระดับล่าง W4. ความเป็นระบบอุปถัมภ์ที่มีอย่างถาวรในสังคมไทย W5.ปัญหาคอร์รัปชั่นในประเทศไทย W6. ประเทศไทยเป็นสังคมผู้สูงอายุ T1.เศรษฐกิจของโลกมีความผันผวนและไม่มั่นคง T2. ความแปรปรวนของสภาพภูมิอากาศของโลก

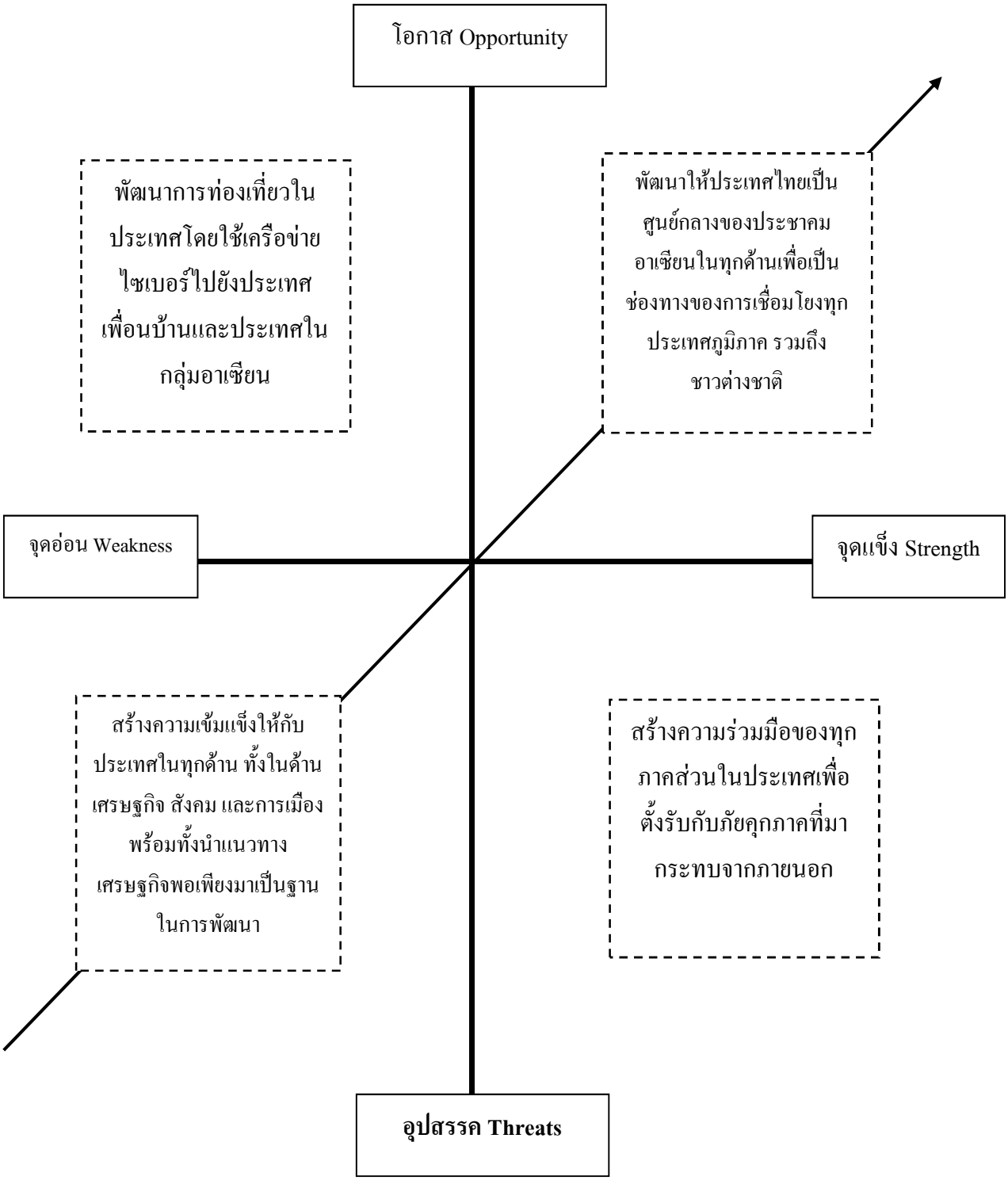
สรุปการวิเคราะห์กลยุทธ์		
	บ้าน O3. ความได้เปรียบในการเป็นฐานการผลิตภาคการเกษตร O4.ประเทศไทยส่งเสริมภาคบริการและการท่องเที่ยว O5.โลกไซเบอร์มีเครือข่ายที่ครอบคลุมทั่วโลก	T3. สถานการณ์การก่อการร้ายที่คุกคามไปทั่วโลก T4. กลุ่มก่อการร้ายมีความเข็มแข็งมากขึ้น T5. การพัฒนาของอาวุธที่มีอานุภาพร้ายแรง เช่น อาวุธชีวภาพ อาวุธนิวเคลียร์ T6. ประเทศมหาอำนาจและประเทศในกลุ่มนับถือศาสนาอิสลาม สร้างความเข็มแข็งและสะสมพลังทางทหารที่มีแสนยานุภาพมาก

กลยุทธ์เชิงรุก SO คือ พัฒนาให้ประเทศไทยเป็นศูนย์กลางของประชาคมอาเซียนในทุกด้านเพื่อเป็นช่องทางของการเชื่อมโยงทุกประเทศภูมิภาค รวมถึงชาวต่างชาติ

กลยุทธ์เชิงป้องกัน ST คือ สร้างความร่วมมือของทุกภาคส่วนในประเทศเพื่อตั้งรับกับภัยคุกภาคที่มากระทบจากภายนอก

กลยุทธ์เชิงแก้ไข WO คือ พัฒนาการท่องเที่ยวในประเทศโดยใช้เครือข่ายไซเบอร์ไปยังประเทศเพื่อนบ้านและประเทศในกลุ่มอาเซียน

กลยุทธ์เชิงรับ WT คือ สร้างความเข้มแข็งให้กับประเทศในทุกด้าน ทั้งในด้านเศรษฐกิจ สังคม และการเมือง พร้อมทั้งนำแนวทางเศรษฐกิจพอเพียงมาเป็นฐานในการพัฒนา



ภาพที่ 9 ภาพรวมของการวิเคราะห์สถานการณ์ (Scenario Analysis)

สรุปภาพรวมของการสร้างภาพอนาคต (Scenario Analysis)

การสร้างภาพอนาคต (Scenario Analysis) สามารถสรุปเป็นสถานการณ์ได้ 4 สถานการณ์ดังนี้

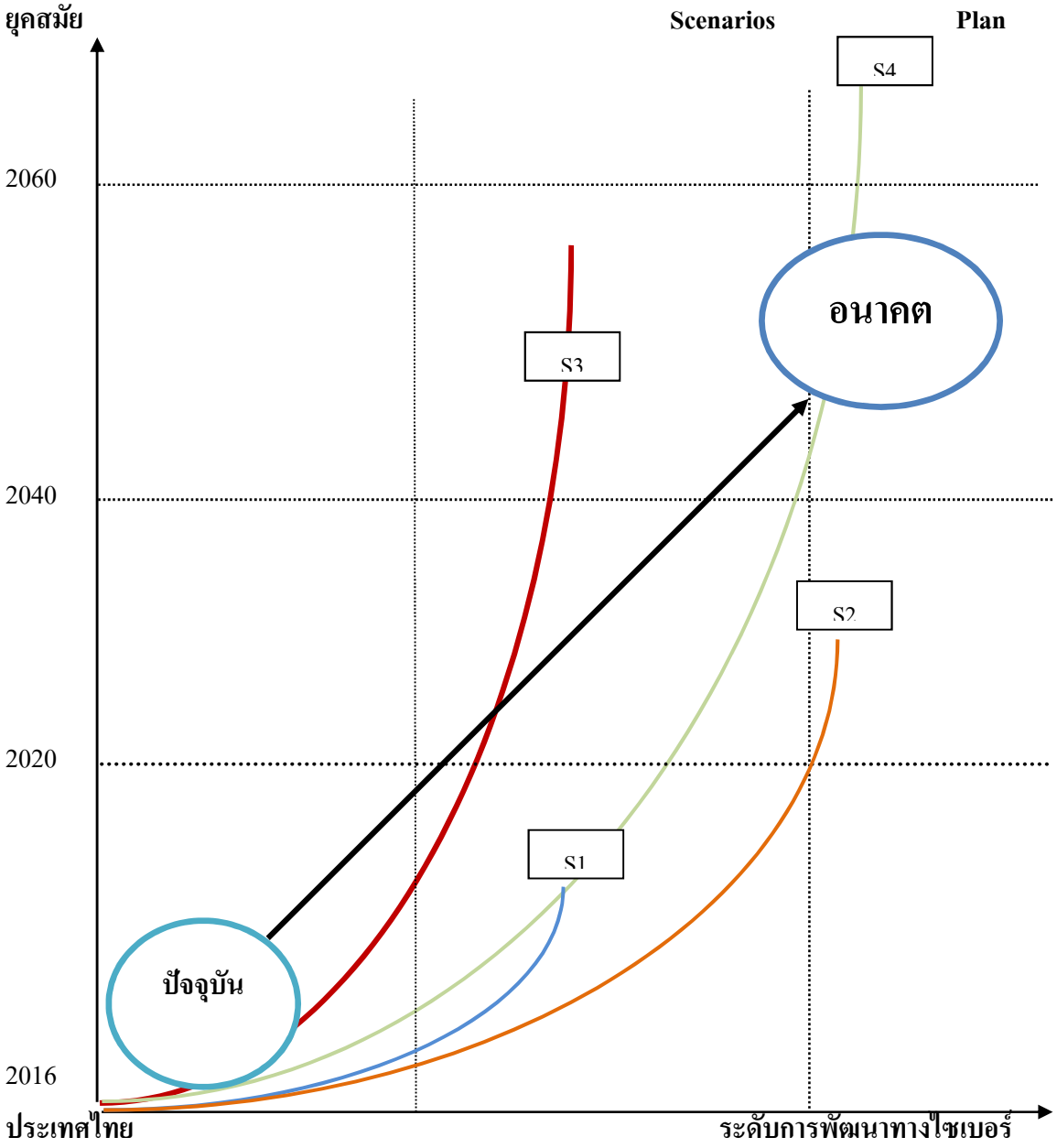
สถานการณ์ที่ 1 (S1) สถานการณ์การก่อการร้ายของโลกจะทวีความรุนแรงเพิ่มมากขึ้น กลุ่มประเทศยุโรปและประเทศมหาอำนาจที่มีแนวทางของการต่อต้านการก่อการร้ายจะเป็นเป้าหมายของการถูกโจมตีด้วยอาวุธที่มีอานุภาพร้ายแรง และนำมาซึ่งความสูญเสียอย่างมาก การเตรียมความพร้อมต่อการป้องกัน และการตอบโต้ด้วยพลังอำนาจแห่งชาติจะมากขึ้นตามไปด้วย ประเทศไทยจะไม่เป็นเป้าหมายของการก่อการร้ายด้วยความเป็นมิตรกับประเทศเพื่อนบ้าน และมีนโยบายในการเปิดประเทศเสรีประชาธิปไตยเพื่อการส่งเสริมการท่องเที่ยว

สถานการณ์ที่ 2 (S2) ประเทศไทยมีการจัดตั้งหน่วยงานทั้งภาครัฐ เอกชน เพื่อร่วมมือกันดำเนินการในการต่อต้านการก่อการร้ายและป้องกันประเทศต่อภัยคุกคามในการก่อการร้าย อนาคตข้างหน้าประเทศไทยจะมีหน่วยงานที่มีความเข้มแข็งต่อการต่อต้านการก่อการร้ายที่มีประสิทธิภาพ

สถานการณ์ที่ 3 (S3) ประเทศไทยให้ความสำคัญต่อการก่อการร้ายทางไซเบอร์มากขึ้น รวมทั้งให้ความสำคัญต่อการก่อการร้ายที่มีไซเบอร์เป็นเครื่องมือ ประชาชนมีความตื่นตัวในการป้องกันการก่อการร้ายทางไซเบอร์มากขึ้น

สถานการณ์ที่ 4 (S4) ประเทศไทยมีความก้าวหน้าทางไซเบอร์ มีการพัฒนาในหลายด้านเพื่อเป็นแนวทางในการป้องกันและต่อต้านการก่อการร้ายตามบริบทของประเทศไทย

ผลของการศึกษาวิจัยนำสู่กรอบยุทธศาสตร์ ดังนี้



ภาพที่ 10 ผลของการศึกษาวิจัยนำสู่กรอบยุทธศาสตร์

สรุปกระบวนการศึกษาวิจัยเป็นข้อค้นพบดังนี้

สภาพแวดล้อมของโลกในปัจจุบันเปลี่ยนแปลงไปตามโลกาภิวัตน์และความเจริญทางเทคโนโลยี การเปลี่ยนแปลงที่เกิดขึ้นนำไปสู่ผลกระทบทางการเมือง เศรษฐกิจและสังคม ที่มาจากความขัดแย้งในเรื่องผลประโยชน์ และโลกไร้พรมแดนที่ประเทศไทยหรือรัฐใดครองเทคโนโลยีครองข้อมูลข่าวสารก็จะครอบครองผลประโยชน์ที่เหนือกว่าประเทศหรือรัฐที่ด้อยความเจริญกว่า ทางเทคโนโลยีไซเบอร์ได้ถูกจัดให้เป็นอีกหนึ่งสนามรบ เพิ่มจากการรบทางบก ทางน้ำและทางอากาศ ซึ่งในปัจจุบันทางการทหารมี 5 ยุทธบริเวณ คือพื้นดิน ทะเล อากาศ อวกาศและไซเบอร์สเปซการพัฒนาเทคโนโลยีต่างๆ ที่เกี่ยวข้องกับความมั่นคงของชาติทั้งการเมือง เศรษฐกิจ สังคม และการทหาร ประเทศใดมีความเจริญก้าวหน้าในการพัฒนาเทคโนโลยีที่ทันสมัยกว่า ย่อมได้เปรียบเรื่องศักยภาพและพลังอำนาจ ในด้านการเมืองก็จะทำให้เกิดเสถียรภาพและความมั่นคงทางการเมืองเพื่อเสริมสร้างความเชื่อมั่น ความเชื่อถือของรัฐบาลในการปกครองและการบริหารประเทศ การเจรจาต่อรองและรักษาผลประโยชน์ของชาติ (National Interest) ด้านเศรษฐกิจจะเห็นได้ชัดในการพัฒนาความเจริญก้าวหน้าของประเทศ ด้านสังคมก็จะเสริมสร้างความเป็นปึกแผ่นและภูมิคุ้มกันให้กับประชาชน และด้านการทหารก็จะเป็นการเสริมสร้างศักยภาพทางการสงคราม และพลังด้านการรบที่สูงกว่าเมื่อการพัฒนาทางเทคโนโลยีมีความเจริญมากขึ้น จะนำมาสู่การพัฒนาของเครื่องมือที่จะนำมาก่อการร้าย

ทฤษฎีการต่อต้านการก่อการร้ายของมาร์ธา เครนชอร์ จะประกอบด้วย 1. การต่อต้านการก่อการร้ายแบบป้องกันโดยการมุ่งเน้นการสร้างอุปสรรคระหว่างผู้ก่อการร้ายกับเป้าหมาย ซึ่งในการสร้างอุปสรรคหมายถึงการสร้างมาตรการในการป้องกัน สร้างศักยภาพในการให้หน่วยงานบังคับใช้กฎหมาย โดยแนวคิดเบื้องหลังแนวทางป้องกันนี้เกิดจากความเชื่อที่ว่า การก่อการร้ายไม่อาจถูกขจัดหมดไปได้อย่างสิ้นเชิง เป้าหมายของการลดการก่อการร้าย คือการลดระดับความรุนแรงลงสู่จุดที่ไม่ทำให้รัฐบาลต้องทุ่มเททรัพยากรในการดำเนินการมากจนกระทบต่อการดำเนินนโยบาย 2. การตอบสนองแบบบริหารจัดการครอบคลุมการวางแผนเชิงเหตุและแง่มุมในเชิงปฏิบัติของนโยบายสาธารณะในระหว่างหรือภายหลังเกิดเหตุโจมตี 3. มาตรการมุ่งเน้นการตอบโต้ โดยตอบสนองต่อการปฏิบัติของผู้ก่อการร้าย

ข้อสรุปเชิงคุณภาพ การก่อการร้ายหมายถึง กระทำการใด ๆ เพื่อให้เกิดความหวาดกลัว การใช้ความรุนแรงหรือขู่ว่าจะใช้ความรุนแรงเพื่อให้เกิดความตื่นตระหนก โดยมีเหตุจูงใจทางการเมือง ทั้งนี้เพื่อนำไปสู่การเปลี่ยนแปลงในทางสังคมทางการเมือง และทางเศรษฐกิจวิธีการก่อการร้ายทางไซเบอร์ มีวิธีการดังนี้ 1. ผู้ก่อการร้ายซึ่งต้องมีความรู้ทางไซเบอร์หรือเทคโนโลยี ศึกษาข้อมูลที่เกี่ยวกับเป้าหมายที่ต้องการจะกระทำ 2. สร้างหรือพัฒนาเครื่องมือให้ตรงกับความต้องการ

ต่อเป้าหมาย เครื่องมือที่สำคัญของการก่อการร้ายทางไซเบอร์คืออินเทอร์เน็ต 3. ระดมคนหรือหาสมาชิกที่มีแนวความคิดแนวทางเดียวกัน 4. ระดมเงินทุนในการสนับสนุน 5.ปฏิบัติการตามวัตถุประสงค์ที่วางไว้เพื่อมุ่งเป้าหมายทางการเมืองปัจจัยที่เกี่ยวข้องกับแรงจูงใจในการก่อการร้ายทางไซเบอร์ด้วยประเทศไทยเป็นประเทศเปิดเสรี เปิดรับนักท่องเที่ยวและมีนโยบายส่งเสริมให้เกิดการท่องเที่ยวในทุกที่โดยไม่มีข้อจำกัด ดังนั้นจึงเป็นเหมือนสวรรค์ของผู้ก่อการร้าย อีกทั้งการส่งเสริมการเปิดใช้อินเทอร์เน็ตในทุกที่ ทำให้ประชาชนขาดการตระหนักรู้ในเรื่องของการใช้ไซเบอร์ การก่อการร้ายทางไซเบอร์นั้นผู้ก่อการร้ายจะใช้เครื่องมือทางไซเบอร์ที่หาง่ายและใช้เครื่องมือได้ทุกที่ ไม่ว่าจะเป็นโทรศัพท์มือถือ แท็บเล็ต คอมพิวเตอร์ ที่สามารถเชื่อมต่ออินเทอร์เน็ตได้ทำให้คนเข้าถึงได้ง่ายและเชื่อง่ายขึ้น แรงจูงใจที่นำไซเบอร์มาก่อการร้าย ผู้เชี่ยวชาญมองว่าเป็นเรื่องเงินเป็นสำคัญ รองลองมาเป็นเรื่องของแนวคิด อุดมการณ์ทางการเมืองหรือทางศาสนา หรือแม้แต่ความไม่พอใจต่อหน่วยงานหรือองค์กร แต่ปัจจัยที่สำคัญที่ผู้เชี่ยวชาญมองต่างกันคือ แรงจูงใจที่สำคัญต่อการกระทำที่เป็นการก่อการร้ายจะต้องเป็นการกระทำที่มาจากแรงจูงใจทางเมืองเป็นสำคัญ จึงเห็นได้ว่า ความเข้าใจในความหมายของการก่อการร้ายที่แตกต่างกัน นำไปสู่การอธิบายแรงจูงใจของการก่อการร้ายที่ต่างกันด้วย เมื่ออธิบายความเข้าใจแรงจูงใจการก่อการร้ายทางไซเบอร์ จึงไม่ได้มีการให้คำจำกัดความที่ชัดเจนปัญหาที่สำคัญของการต่อต้านการก่อการร้ายเกิดจากแนวคิดของการก่อการร้าย และความหมาย และความไม่รู้ถึงความรุนแรงอันเกิดจากการก่อการร้ายของคนในประเทศใครคือผู้ก่อการร้าย และอะไรคือการก่อการร้าย เนื่องจากภัยการก่อการร้ายเป็นเรื่องไกลตัวและยังไม่มีการสร้างความตระหนักอย่างชัดเจน

ความก้าวหน้าทางไซเบอร์คือ เทคโนโลยีที่มีอินเทอร์เน็ต เพื่อเชื่อมต่อการสื่อสารได้ทุกที่ทุกเวลา ไม่ว่าจะอยู่ที่ใดบนโลก สะดวก รวดเร็ว และไซเบอร์มีความสำคัญอย่างมากต่อการดำรงชีวิตในปัจจุบัน โดยมีเครื่องมือที่ใช้ในการติดต่อสื่อสาร ไม่ว่าจะเป็น คอมพิวเตอร์ โทรศัพท์มือถือ หรือ Tablet เป็นต้น และความก้าวหน้าทางไซเบอร์ต้องมีความเร็วสูง มีระบบปฏิบัติการที่ดีและมีประสิทธิภาพและสามารถเข้าถึงได้ผู้ก่อการร้ายแสวงหาโอกาสจากประเทศไทยในหลายด้านเพื่อก่อการร้าย ประเด็นสำคัญที่พบได้คือ ประเทศไทยเป็นประเทศที่เปิดเสรี และประชาชนมีการต้อนรับชาวต่างประเทศ มีการยิ้มแย้มแจ่มใสและต้อนรับผู้อื่นจึงเหมือนกับเป็นสวรรค์ของผู้ก่อการร้าย ส่วนใหญ่ผู้ก่อการร้ายจะใช้ประเทศไทยเป็นฐานในการเตรียมการก่อการร้ายไปยังประเทศที่สาม หรือประเทศที่เป็นเป้าหมายมากกว่า และประเทศไทยไม่มีมาตรการในการป้องกันความปลอดภัยทางไซเบอร์ ประชาชนยังไม่ความตระหนักรู้ต่อภัยคุกคามทางไซเบอร์ จึงทำให้มีการใช้อย่างไม่ระแวดระวังเครื่องมือทางไซเบอร์ที่นำมาใช้ในการก่อการร้ายในปัจจุบัน คือ โทรศัพท์มือถือ แท็บเล็ต คอมพิวเตอร์ หรืออุปกรณ์ที่สามารถเชื่อมต่ออินเทอร์เน็ตได้

และสามารถใช้งานได้ทุกที่ อย่างสะดวกและรวดเร็ว การเชื่อมต่ออินเทอร์เน็ตที่มีความเร็วสูงและมีระบบปฏิบัติการที่มีประสิทธิภาพจะช่วยการปฏิบัติการได้อย่างมีประสิทธิภาพ นอกจากนี้ ประเด็นสำคัญที่ค้นพบคือการใช้สังคมออนไลน์ทั้งกล่องข้อความ ไลน์ ทวิสเตอร์เป็นต้น เพื่อใช้ในการติดต่อสื่อสารกันทั่วโลกและใช้เป็นช่องทางในการเผยแพร่แนวคิด วิดีโอ เพื่อให้เกิดความเชื่อ ต่อบุคคล ต่อสมาชิกในกลุ่มหรือ เชื่อมโยงไปยังดึงปลุกระดมคนเพื่อนำมาสู่การก่อการร้ายได้การก่อการร้ายทางไซเบอร์และการต่อต้านการก่อการร้ายทางไซเบอร์ สรุปได้ 2 ประเด็นดังนี้

1. การก่อการร้ายทางไซเบอร์ เป็นการกระทำที่ก่อให้เกิดความเสียหาย ก่อให้เกิดความหวาดกลัว ตื่นตระหนกโดยมีการนำไซเบอร์มาเป็นเครื่องมือในการก่อการร้าย โดยมีเหตุจูงใจทางการเมือง เป็นสำคัญ สิ่งที่ค้นพบคือ ประเทศไทยยังไม่มีสถานการณ์หรือเหตุจูงใจที่นำไปสู่การก่อการร้ายทางไซเบอร์ ส่วนใหญ่เป็นการกระทำของแฮกเกอร์ เช่น การแฮกหน้าเว็บไซต์ของหน่วยงานราชการ ธนาคารหรือสถาบันทางการเงิน เพื่อแสดงออกถึงความสนุกสนาน พอใจ ทำให้เป็นที่รู้จักว่ามีศักยภาพในด้านนี้

2. การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย จากการวิจัยสิ่งที่ค้นพบคือ ประเทศไทยมีการตื่นตัวและตระหนักในเรื่องของการต่อต้านการก่อการร้ายทางไซเบอร์ แต่มีการดำเนินการแบบแยกส่วน มีหน่วยงานที่การตระหนักในความปลอดภัยทางไซเบอร์คือ หน่วยทหาร ตำรวจและหน่วยงานของภาคเอกชนบางส่วนที่เกี่ยวข้องกับการเงิน เช่น ธนาคารพาณิชย์ต่างๆ สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์แห่งประเทศไทย (ก.ล.ต.) เป็นต้น

ข้อสรุปจากเทคนิคเดลฟาย จากการนำข้อมูลจากการสัมภาษณ์ในเชิงคุณภาพมาสังเคราะห์เพื่อจัดทำแบบสอบถามไปยังผู้เชี่ยวชาญได้ผลสรุปดังนี้ ประเทศไทยยังไม่มีการสร้างการตระหนักรู้ทางไซเบอร์ การก่อการร้ายทางไซเบอร์มีผลต่อความเสียหายระดับบุคคลและระดับประเทศ ประเทศไทยยังไม่มีการจัดรูปแบบการศึกษาที่เน้นความรู้ทางไซเบอร์ การส่งเสริมการวิจัยเพื่อพัฒนาองค์ความรู้ทางไซเบอร์ ประเทศไทยยังไม่มีกฎหมายเพื่อดูแล ป้องกันและควบคุมการดำเนินการทางไซเบอร์และบังคับใช้อย่างแท้จริง ประเทศไทยยังไม่มีหน่วยงานหรือองค์กรที่เป็นเจ้าภาพหลักเพื่อดูแล ติดตามและควบคุมการดำเนินการทางไซเบอร์ทั้งหมด การพัฒนาทางไซเบอร์ที่รวดเร็วส่งผลต่อการนำมาเป็นเครื่องมือทางการก่อการร้ายในอนาคตที่มีอานุภาพร้ายแรงอย่างแน่นอน และการป้องกันทางไซเบอร์ของประเทศไทยต้องเกิดจากความร่วมมือระหว่างหน่วยงานทั้งภาครัฐ ภาคเอกชนและภาคประชาชนทั้งประเทศ

ข้อสรุปเชิงปริมาณ ความก้าวหน้าทางไซเบอร์ พบว่า ข้อที่มีระดับความคิดเห็นสูง 3 อันดับแรกคือ 1. การใช้โทรศัพท์มือถือแท็บเล็ตคอมพิวเตอร์และเครื่องมืออื่นๆ ที่สามารถเชื่อมต่ออินเทอร์เน็ตพร้อมทั้งมีความเร็วสูงเป็นความก้าวหน้าทางไซเบอร์ 2. Application ของโทรศัพท์มือถือ

ที่สามารถอำนวยความสะดวกและมีการเชื่อมต่ออย่างรวดเร็วส่งผลต่อความก้าวหน้าทางไซเบอร์3. ความก้าวหน้าทางไซเบอร์ คือการพัฒนาทางเทคโนโลยีที่สามารถเชื่อมต่อกันได้อย่างรวดเร็ว สะดวกขึ้น ทำให้ทุกคนติดต่อกันได้ไม่ว่าจะอยู่ที่ใดในโลก

ลักษณะการก่อการร้ายทางไซเบอร์และนำมาเป็นเครื่องมือทางยุทธศาสตร์ในการก่อการร้ายพบว่าข้อที่มีระดับความคิดเห็นสูง 3 อันดับแรกคือ 1. การป้องกันทางไซเบอร์ของประเทศไทยต้องเกิดจากความร่วมมือกันระหว่างหน่วยงาน ทั้งภาครัฐ ภาคเอกชนและประชาชนทั้งประเทศ 2. การก่อการร้ายทางไซเบอร์เป็นการใช้เครื่องมือทางเทคโนโลยี เช่น โทรศัพท์มือถือ คอมพิวเตอร์ หรือเครื่องมือประเภทอื่น ๆ ที่เชื่อมต่อทางอินเทอร์เน็ตเพื่อการก่อการร้าย/อินเทอร์เน็ตเป็นช่องทางที่สำคัญที่ใช้ในการก่อการร้าย เช่น ลักลอบขโมยข้อมูลข่าวสารเพื่อมุ่งเป้าทางการเมือง ปล่อยไวรัสเพื่อทำลายระบบ 3. กฎหมายที่เกี่ยวกับไซเบอร์ เพื่อดูแล ป้องกัน และควบคุมการดำเนินการทางไซเบอร์ยังไม่ครอบคลุมและบังคับใช้อย่างแท้จริง

ข้อค้นพบ ความก้าวหน้าทางไซเบอร์คือการพัฒนาทางเทคโนโลยีที่สามารถเชื่อมต่อกันได้อย่างรวดเร็วสะดวกขึ้น ทำให้ทุกคนติดต่อกันได้ไม่ว่าจะอยู่ที่ใดในโลกการก่อการร้ายทางไซเบอร์เป็นการใช้เครื่องมือทางเทคโนโลยี เช่น โทรศัพท์มือถือ คอมพิวเตอร์ หรือเครื่องมือประเภทอื่น ๆ ที่เชื่อมต่อทางอินเทอร์เน็ตเพื่อการก่อการร้ายและอินเทอร์เน็ตเป็นช่องทางที่สำคัญที่ใช้ในการก่อการร้าย เช่น ลักลอบขโมยข้อมูลข่าวสารเพื่อมุ่งเป้าทางการเมือง และปล่อยไวรัสเพื่อทำลายระบบต่าง ๆการป้องกันทางไซเบอร์ของประเทศไทยต้องเกิดจากความร่วมมือกันระหว่างหน่วยงาน ทั้งภาครัฐ เอกชนและประชาชนทั้งประเทศและประเทศไทยต้องมีกฎหมายที่เกี่ยวกับไซเบอร์ เพื่อดูแล ป้องกัน และควบคุมการดำเนินการทางไซเบอร์เพื่อให้ครอบคลุมและบังคับใช้อย่างแท้จริง

การพัฒนายุทธศาสตร์การต่อต้านการก่อการร้ายในประเทศไทยนำเสนอยุทธศาสตร์ในการต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย ดังนี้ยุทธศาสตร์ READ: CLIP ประกอบด้วย

ยุทธศาสตร์ที่ 1 Research ยุทธศาสตร์การเสริมสร้างการวิจัยเพื่อการพัฒนาทางไซเบอร์

ยุทธศาสตร์ที่ 2 Education ยุทธศาสตร์การจัดการศึกษาในการสร้างพื้นฐานของประชาชนในประเทศไทย

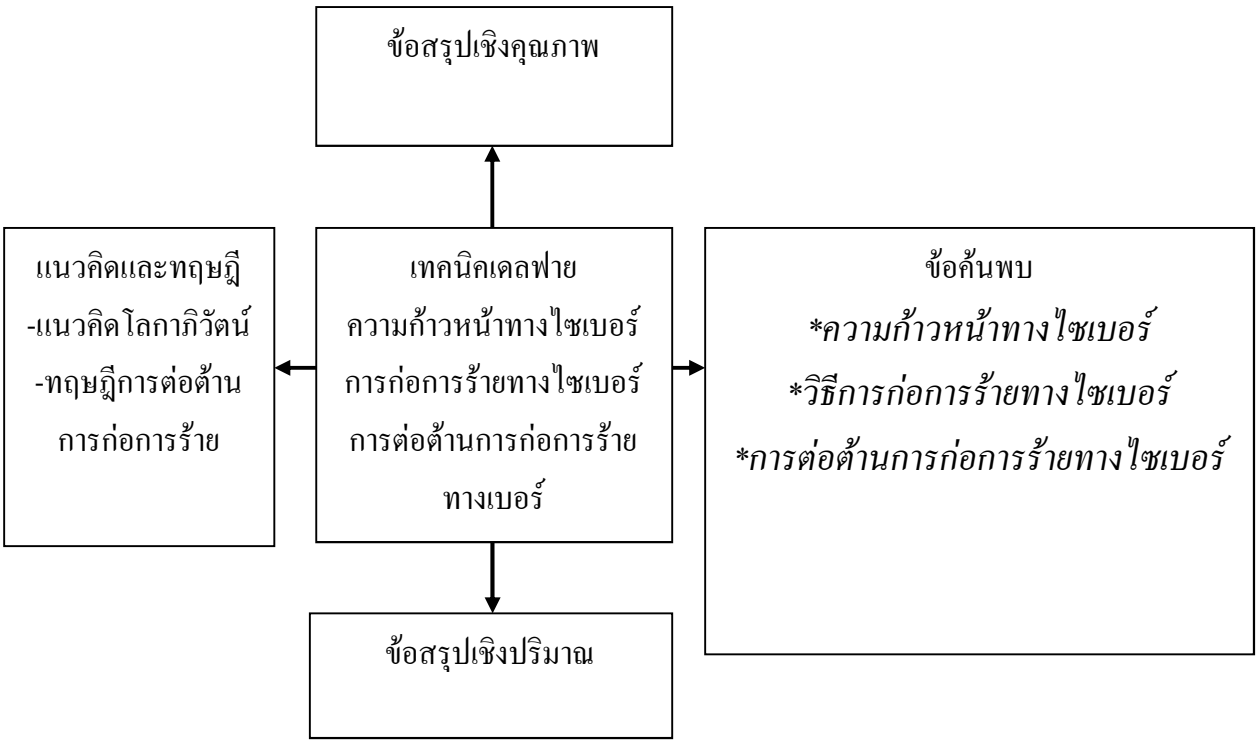
ยุทธศาสตร์ที่ 3 Awareness ยุทธศาสตร์การสร้างการตระหนักรู้ทางไซเบอร์ให้กับประชาชน ยุทธศาสตร์ที่ 4 Development ยุทธศาสตร์การพัฒนาความก้าวหน้าทางไซเบอร์

ยุทธศาสตร์ที่ 5 Coordinate ยุทธศาสตร์การส่งเสริมความร่วมมือระหว่างภาครัฐ ภาคเอกชน และภาคประชาชน

ยุทธศาสตร์ที่ 6 Law ยุทธศาสตร์การกำหนดใช้กฎหมายทางไซเบอร์และการบังคับใช้กับประชาชน

ยุทธศาสตร์ที่ 7 Integration ยุทธศาสตร์การใช้บูรณาการร่วมกันเพื่อแบ่งปันข้อมูล

ยุทธศาสตร์ที่ 8 Perception prepares and protect ยุทธศาสตร์การรับรู้ทางไซเบอร์ร่วมกัน ตระเตรียมและปกป้องทางไซเบอร์



บทที่ 5
ยุทธศาสตร์ในการต่อต้านการก่อการร้ายทางไซเบอร์ของประเทศไทย

การวิจัยเรื่อง ยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทยโดยมีวัตถุประสงค์การวิจัยดังนี้ 1. เพื่อศึกษาความก้าวหน้าทางไซเบอร์ที่มีการนำมาใช้เป็นเครื่องมือทางยุทธศาสตร์ในการก่อการร้ายในประเทศไทย 2. เพื่อศึกษาลักษณะการก่อการร้ายโดยใช้ไซเบอร์มาเป็นเครื่องมือทางยุทธศาสตร์ในการก่อการร้ายของประเทศไทยและวิเคราะห์ประเมินการก่อการร้ายทางไซเบอร์ในประเทศไทยโดยใช้การวิเคราะห์จุดแข็ง จุดอ่อน โอกาสและอุปสรรควิธีการวิเคราะห์สถานการณ์และองค์กรแห่งการเรียนรู้ 3. เพื่อพัฒนายุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย ผู้วิจัยแบ่งผลการวิเคราะห์ข้อมูลของการศึกษาโดยใช้แนวความคิดที่จะนำไปสู่การวิเคราะห์ยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ของประเทศไทยดังนี้

สภาพแวดล้อมและสถานการณ์โลกภายใต้โลกาภิวัตน์

สถานการณ์ความมั่นคงของประเทศไทยประสบปัญหาความมั่นคงภายในประเทศเนื่องจากสภาพการณ์ความขัดแย้งทางการเมืองที่ยังต้องแก้ไขปัญหากันอย่างต่อเนื่อง การก่อความไม่สงบในจังหวัดชายแดนภาคใต้ ปัญหาอาชญากรรมข้ามชาติ ปัญหาความยากจน ปัญหาของการทำลายสิ่งแวดล้อมและระบบนิเวศน์ทางบกและทางทะเล สาธารณภัยและอุบัติภัยต่าง ๆ ซึ่งมีผลกระทบต่อสภาพสังคมโดยรวม และผลประโยชน์แห่งชาติที่ส่งผลกระทบต่อสภาพสังคมโดยรวม ไม่ว่าจะเป็นขบวนการค้ายาเสพติด ขบวนการค้ามนุษย์ การฟอกเงิน การค้าสินค้าเลี่ยงภาษีและสิ่งผิดกฎหมาย ราคาน้ำมันผันแปร ทำให้ประชาชนได้รับความเดือดร้อน นอกจากนี้การก่อการร้ายข้ามชาติที่แพร่ขยายไปยังทุกพื้นที่ทั่วโลก โดยเฉพาะอย่างยิ่งพื้นที่อันเป็นผลประโยชน์ของประเทศมหาอำนาจ หรือพลเมืองของประเทศมหาอำนาจเข้าไปเกี่ยวข้อง ประเทศไทยอาจจะได้รับผลกระทบทั้งทางตรงและทางอ้อมจากการก่อการร้ายแม้ว่าประเทศไทยจะไม่ใช่เป้าหมายโดยตรงของการก่อการร้ายสากล แต่ประเทศไทยมีการเข้าร่วมเป็นพันธมิตรกับสหรัฐอเมริกาและประเทศอื่น ๆ รวมทั้งเป็นภาคีอนุสัญญาการต่อต้านการก่อการร้ายสากล ตลอดจนนโยบายของประเทศไทยต่อการเปิดประเทศ ส่งเสริมการท่องเที่ยว ทำให้เป็นดินแดนเสรีในการเดินทางผ่านเข้าและออก กลุ่มก่อการร้ายมักใช้เป็นเส้นทางผ่าน หรือพักพิง นัดพบหรือใช้เป็นสถานที่ในการประกอบวัสดุที่เกี่ยวข้องกับการก่อการร้ายได้ ผลกระทบที่เกิดขึ้นประเทศไทยไม่สามารถหลีกเลี่ยงได้ ทางด้านการเมืองประเทศไทยโดยรัฐบาลต้องสนับสนุนสหรัฐอเมริกาและพันธมิตรยุโรปตะวันออก ตาม

จุดยืนในการก่อการร้ายสากล และตามพันธกรณี แต่การดำเนินนโยบาย การปฏิบัติจะต้องไม่ตกเป็นเป้าการโจมตีแก้แค้นขององค์กรหรือเครือข่ายการก่อการร้าย การปฏิบัติการภายในประเทศของไทย เหตุการณ์ที่กระทบกับประเทศไทยโดยตรง ได้แก่ การทำลายสถานที่ เป้าหมายต่อบุคคลสำคัญ ประชาชนและทรัพย์สินของประเทศ จะใช้นโยบายไม่ยินยอมต่อข้อเรียกร้องแต่ถ้าเป็นการกระทำที่มีผลต่อส่วนรวม ต่อสถานที่ บุคคลสำคัญต่างประเทศที่เกิดขึ้นในประเทศไทย จะยึดถือนโยบายพิจารณาร่วมกันกับผู้แทนของรัฐบาลประเทศนั้น ๆ แต่จะต้องไม่ขัดต่อนโยบายหลักของประเทศไทย และจะต้องไม่กระทบกระเทือนต่อผลประโยชน์แห่งชาติ ในกรณีที่ต้องใช้กำลังในแก้ไขปัญหา จะต้องใช้กำลังของหน่วยพิเศษของประเทศไทยเป็นหลัก หากจะต้องใช้กำลังของต่างประเทศเข้าร่วมจะต้องได้รับการอนุมัติก่อน หากเหตุการณ์นั้นเกิดนอกประเทศและมาสิ้นสุดในประเทศไทย ถือว่าเป็นเรื่องที่เกิดขึ้นในประเทศไทย ในส่วนของการปฏิบัติการภายนอกประเทศแต่เป็นผลกระทบที่เกิดขึ้นในประเทศไทยโดยตรง เช่น ต่อสถานทูตและบุคคลสำคัญของประเทศยังคงใช้นโยบายไม่ยินยอมต่อข้อเรียกร้อง กำลังที่ใช้แก้ไขปัญหาอาจจะเป็นมิตรประเทศ แต่ต้องมีเจ้าหน้าที่ของไทยร่วมด้วย

สภาพแวดล้อมของโลกในปัจจุบันเปลี่ยนแปลงไปตามโลกาภิวัตน์และความเจริญทางเทคโนโลยี การเปลี่ยนแปลงที่เกิดขึ้นนำไปสู่ผลกระทบทางการเมือง เศรษฐกิจและสังคม ที่มาจากความขัดแย้งในเรื่องผลประโยชน์ และโลกไร้พรมแดนที่ประเทศไทยหรือรัฐใดครองเทคโนโลยีครองข้อมูลข่าวสารก็จะครอบครองผลประโยชน์ที่เหนือกว่าประเทศหรือรัฐที่ด้อยความเจริญกว่าทางเทคโนโลยีไซเบอร์ได้ถูกจัดให้เป็นอีกหนึ่งสนามรบ เพิ่มจากการรบทางบก ทางน้ำและทางอากาศ ซึ่งในปัจจุบันทางการทหารมี 5 ยุทธบริเวณ คือพื้นดิน ทะเล อากาศ อวกาศและไซเบอร์สเปซการพัฒนาเทคโนโลยีต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงของชาติทั้งการเมือง เศรษฐกิจ สังคม และการทหาร ประเทศใดมีความเจริญก้าวหน้าในการพัฒนาเทคโนโลยีที่ทันสมัยกว่า ย่อมได้เปรียบเรื่องศักยภาพและพลังอำนาจ ในด้านการเมืองก็จะทำให้เกิดเสถียรภาพและความมั่นคงทางการเมืองเพื่อเสริมสร้างความเชื่อมั่น ความเชื่อถือของรัฐบาลในการปกครองและการบริหารประเทศ การเจรจาต่อรองและรักษาผลประโยชน์ของชาติ ด้านเศรษฐกิจจะเห็นได้ชัดในการพัฒนาความเจริญก้าวหน้าของประเทศ ด้านสังคมก็จะเสริมสร้างความเป็นปึกแผ่นและภูมิคุ้มกันให้กับประชาชน และด้านการทหารก็จะเป็นการเสริมสร้างศักยภาพทางการสงคราม และพลังด้านการรบที่สูงกว่า

บทสรุปสถานการณ์ประเทศไทยยังคงเป็นเหตุการณ์ที่ยังไม่สามารถวางใจได้ สอดคล้องกับสถานการณ์การก่อการร้ายยังคงเกิดขึ้นต่อเนื่อง สถานการณ์ความมั่นคงยังคงเป็นปัญหาที่ทุกประเทศทั่วโลกต้องพึงระวังการใช้เทคโนโลยีสมัยใหม่นำมาเป็นเครื่องมือที่ทรงพลังให้ประชาชน

ไว้ใช้เพื่อเป้าหมายของตนเอง การนำเทคโนโลยีก็ช่วยให้มนุษย์สร้างสรรค์สิ่งต่างๆได้อย่างมหัศจรรย์ แต่บางครั้งเทคโนโลยีก็เป็นเครื่องมือของการทำลายล้างได้อย่างเกินความคาดหมาย ปัจจุบันนี้สิ่งที่หลีกเลี่ยงไม่ได้คือ การนำอินเทอร์เน็ตมาเชื่อมต่อการสื่อสารออนไลน์ซึ่งเอื้อประโยชน์ต่อผู้ก่อการร้ายและพวกหัวรุนแรงกลุ่มต่าง ๆ เมื่อมีการแพร่หลายมากขึ้นความเสี่ยงดังกล่าวก็เพิ่มมากขึ้นด้วย การโจมตีของผู้ก่อการร้ายทางไซเบอร์ไม่จำกัดอยู่แค่การรบกวนระบบหรือปิดเครือข่ายโครงสร้างพื้นฐาน ผู้ก่อการร้ายที่ลักลอบขนยาเสพติด ค้ายา หรืออาชญากรจะนำเครื่องมือทางไซเบอร์มาใช้เพื่อกระทำการก่อการร้ายได้มีอานุภาพร้ายแรงยิ่งขึ้น ความชำนาญในการใช้สื่อของผู้ก่อการร้ายเป็นคุณลักษณะสำคัญที่สุด

แนวโน้มการก่อการร้ายในอนาคต

แนวโน้มของการก่อการร้ายในอนาคตและมาตรการในการต่อต้านการก่อการร้ายเพื่อคาดการณ์หรือทำนายแนวโน้มการก่อการร้ายรัฐจะได้เตรียมการตอบโต้และต่อต้านได้อย่างทันท่วงที การก่อการร้ายมีความสลับซับซ้อนมากยิ่งขึ้นและมีความอันตรายมากยิ่งขึ้นด้วย นอกเหนือจากวิธีการและรูปแบบอย่างเดิม ๆ ที่ยังคงใช้อยู่แล้ว การขยายแนวทางหรือเครือข่ายและมีการเคลื่อนไหวอยู่ตลอดเวลา เมื่อผู้ก่อการร้ายมีการจัดองค์กรที่ดี มีความรู้อย่างลึกซึ้งเกี่ยวกับเทคโนโลยีทางการสื่อสาร คอมพิวเตอร์ วัตถุระเบิด เคมี ชีวะ และนิวเคลียร์มีการสร้างสมาชิกไว้ทั่วโลก โดยเฉพาะการใช้เทคโนโลยีเป็นส่วนหนึ่งของการเพิ่มประสิทธิภาพด้วยการเข้ารหัส และใช้อินเทอร์เน็ตแพร่ข่าวอย่างรวดเร็ว ภัยคุกคามสูงสุดจากการก่อการร้ายน่าจะเป็นการ นำระเบิดแรงสูง การใช้รังสีและนิวเคลียร์ การใช้อาวุธชีวภาพ อาวุธเคมีและการโจมตีเครือข่ายอินเทอร์เน็ต อาวุธอานุภาพทำลายล้างสูง ออกแบบมาเพื่อทำให้เกิดการสูญเสียเป็นกลุ่มก้อน และการทำลายล้าง แต่ก็เป็นโอกาสที่ยากที่ผู้ก่อการร้ายจะมีอาวุธนิวเคลียร์ ชีวะ เคมีโดยตรง ส่วนใหญ่เป็นการใช้กัมมันตภาพรังสี สารเคมี และเชื้อโรคในการก่อวินาศกรรม อาวุธที่มีการทำลายล้างสูงคือการใช้รังสีและนิวเคลียร์ การใช้อาวุธชีวะ และการใช้อาวุธเคมี

หากเกิดการใช้อาวุธโดยใช้รังสีและนิวเคลียร์ การใช้อาวุธชีวะ และการใช้อาวุธเคมี ผู้ที่ได้รับผลกระทบโดยตรงคือชีวิตมนุษย์และก่อให้เกิดปัญหาต่าง ๆ อีกมากมายตามมา ชีวิตมนุษย์ก็จะเกิดวิกฤตการณ์ที่โรงพยาบาลต่างๆผู้ที่สัมผัสและรับผลจากการเผยแพร่กระจายของรังสี ชีวะหรือสารพิษจำนวนมากเกินกว่าที่โรงพยาบาลจะรองรับผู้ป่วย ปัญหาการขาดแคลนเตียงผู้ป่วย ขาดแคลนยาปฏิชีวนะ เครื่องช่วยหายใจ เวชภัณฑ์บำบัดโรค และผลข้างเคียง บุคลากรทางการแพทย์มีจำนวนไม่เพียงพอที่สำคัญที่อาจเกิดคือ ความไม่พอใจของประชาชน การตื่นตระหนกจากความหวาดกลัวสารพิษและปัญหาการระบาดของโรค สิ่งเหล่านี้ถ้าเกิดขึ้นโดยกลุ่มผู้ก่อการร้าย หลาย

คนคิดว่าการเตรียมการเพื่อรองรับสถานการณ์การก่อการร้ายทางรังสีและนิวเคลียร์ การก่อการร้ายทางอาวุธชีวะ การก่อการร้ายทางอาวุธชีวะทำได้ยาก เพราะความหลากหลายของชนิดเชื้อโรค และสารเคมีรวมถึงวัสดุกัมมันตรังสี และหากเตรียมการรองรับถานการณ์นี้ให้ดีต้องมีค่าใช้จ่ายสูง และทรัพยากรที่ใช้เพื่อเตรียมการมีจำนวนไม่มาก แต่หลายคนเชื่อว่าเหตุการณ์ก่อการร้ายลักษณะนี้เกิดขึ้นได้ยาก โอกาสเกิดขึ้นน้อย ทำให้ไม่คุ้มค่าการลงทุน (ศูนย์ศึกษาการก่อการร้าย, 2549, หน้า 8 – 9) นอกจากการเผยแพร่กระจายของอาวุธต่าง ๆ ในการทำลายล้างมวลชน ความเจริญก้าวหน้าของเทคโนโลยีก็มาพร้อมกับความเสื่อมของสังคม สังคมที่เปราะบางขาดสายสัมพันธ์ทางสังคมที่แนบแน่น ถูกโจมตีได้ง่าย ทั้งจากกลุ่มที่คลั่งลัทธิ ผู้ก่อการร้าย และองค์การก่อการร้ายสากล ตลอดจนพวกโรคจิตและพวกอารมณ์วิปริตสามารถก่อเหตุร้ายต่อสังคมได้ไม่ว่าจะทางใดทางหนึ่ง นอกจากนี้การดำเนินธุรกิจ ธุรกรรมต่างๆ ตลอดจนถึงการจัดเก็บข้อมูลด้วยไฟฟ้าและซ่อมแซมและกอบกู้ระบบดังกล่าว การวิเคราะห์ข้อมูลและการส่งข้อมูลทางอิเล็กทรอนิกส์ ส่วนใหญ่ของหน่วยราชการและรัฐบาล รวมถึงหน่วยงานด้านความมั่นคง ธนาคารพาณิชย์ การขนส่ง งานทางวิทยาศาสตร์ ตลอดจนกิจกรรมต่างๆของบุคคลต่างพึ่งพิงระบบ ออนไลน์หรืออาศัยเครือข่าย อาณาเขตพื้นที่ต่างๆ ของการดำเนินชีวิตของประชาชนที่มีวิถีผูกพันกับสิ่งดังกล่าวที่จะตกอยู่ในอันตรายและการก่อวินาศกรรม โดยบรรดาแฮกเกอร์คอมพิวเตอร์ และการก่อวินาศกรรมที่เป็นความร่วมมือกันสามารถที่จะปฏิบัติการกับประเทศใดประเทศหนึ่งได้ การทำให้ระบบไฟฟ้าหรือระบบอิเล็กทรอนิกส์สูญเสีย หรือเกิดแรงเสียดทาน ทำให้เกิดอาการไร้ความสามารถเป็นอัมพาต นำไปสู่การก่อการร้ายด้านข้อมูลและสงครามไซเบอร์ และการแพร่เชื้อโรคไวรัสในระบบเครือข่ายคอมพิวเตอร์ การสร้างความปั่นป่วนหรือความอลหม่านในเครือข่ายเป็นสิ่งที่เกือบจะไม่มีข้อจำกัดและถูกโจมตีได้ง่ายเพิ่มขึ้นทุกวัน พลังอำนาจในการทำลายล้างสูงกว่าอาวุธที่ใช้ในการก่อการร้ายอื่น ๆ (ศูนย์ศึกษาการก่อการร้าย, 2549, หน้า 21)

เหตุที่นำไปสู่การก่อการร้ายส่วนหนึ่งเกิดจากความอ่อนแอของสังคม การพึ่งพาระบบเศรษฐกิจแบบทุนนิยมทำให้ทุกคนในสังคมเห็นแก่ตัว สะสมทุนและความสุขทางวัตถุ สังคมเสื่อมทรามลงความยึดมั่นผูกพันต่อสัญลักษณ์ทางสังคมและโยงใยทางสังคมเห็นว่าตัวเองต่ำต้อยจะเกิดอารมณ์หวั่นไหวพร้อมที่จะเรียกร้องความทัดเทียมให้แก่ตนเอง ยิ่งในสังคมที่ค่าของเงินมาเป็นเกณฑ์วัดมาตรฐานความเป็นอยู่ในสังคม และช่วงโอกาสของการก้าวสู่การเลื่อนชั้นทางสังคม บุคคลเหล่านี้พร้อมจะเข้าสู่สถานการณ์ที่ก้าวร้าวเพื่อทำลาย แบ็คเมล์ หรือเรียกร้องให้รัฐหรือสังคมต้องให้ในสิ่งใดเป็นการตอบแทน พร้อมกับเข้าขบวนการก่อการร้าย และองค์การก่อการร้ายชักนำผู้ด้อยโอกาสเข้าสู่การสอดแนม จารชน นักก่อวินาศกรรม อาชญากร หัวขโมยต่างๆ ทางด้านอิเล็กทรอนิกส์และหากผู้มีแรงกระตุ้นทางการเมืองต่างๆรวมถึงผู้แบ่งแยก การใช้วิธีการต่างๆ ที่จะ

ทำให้ศัตรูอ่อนกำลังลงด้วยการก่อการร้าย การเลือกการทำลายล้าง และการสร้างความเสียหายอาจสอดคล้องกับความเชื่อเกี่ยวกับคำพยากรณ์ นำไปสู่ความเชื่อในเรื่องการทำลายล้าง โดยการใช้ความรุนแรงแบบสุดโต่ง พร้อมที่จะทำให้เกิดความเสียหายอย่างมหาศาลการก่อวินาศกรรมโดยใช้อินเทอร์เน็ตด้วยการโจมตีต่าง ๆ เช่น การทิ้งระเบิด จดหมายหรือเมล์ อาจใช้ข้อความซ้ำไปยังจดหมายอิเล็กทรอนิกส์โดยปฏิเสธไม่ให้ผู้ใช้ชอบธรรมเข้าถึงที่อยู่หรือเว็บไซต์นั้นหรือทำให้ระบบที่ใช้อยู่หยุดทำงานจากข้อมูลที่ส่งเข้าไปมากเกินไป การทำลาย การลบ หรือเปลี่ยนแปลงข้อมูล การกดรหัสผ่าน และการหลอกลวงด้วยเทคนิคต่าง ๆ สื่อภาพลามกอนาจาร การพนันบนอินเทอร์เน็ต การฉ้อโกง การฟอกเงินเป็นต้น

ในปัจจุบันวิธีการของการก่อการร้ายได้มีการพัฒนารูปแบบการก่อการร้ายทางไซเบอร์โลกหลังเหตุการณ์ 11 กันยายน จะเห็นได้ว่าประเทศที่มีสิทธิเสรีภาพ ยังคงต้องพึ่งพาระบบที่ช่วยเพิ่มประสิทธิภาพของการตรวจสอบและรักษาความมั่นคงของประเทศ ยิ่งเมื่อเหตุการณ์สะเทือนขวัญส่งผลกระทบต่อประชาชน ทำให้ประชาชนยอมเสียสละความอิสรเสรี เพื่อยอมรับการตรวจสอบกิจกรรมบนโลกออนไลน์ที่เข้มงวดมากขึ้น มาตรการในการต่อต้านก่อการร้าย เป็นมาตรการในการลดความสามารถและลดความเป็นไปได้ของการเกิดการร้าย รวมทั้งเทคนิคการป้องกันการเกิดอาชญากรรมและวิธีการตรวจสอบก่อนเกิดเหตุการณ์ มาตรการตอบโต้เป็นมาตรการต่อเหตุการณ์ที่เกิดขึ้น ขึ้นอยู่กับการวางแผน การปฏิบัติการทางยุทธวิธีภายหลังเกิดเหตุการณ์ และเป็นการทำให้โอกาสที่ผู้ก่อการร้ายปฏิบัติการสำเร็จลดลง (กองข่าวกองทัพภาคที่ 2, ม.ป.ป., หน้า 17 อ้างถึงใน ดุสิต น้ำฝน, 2549, หน้า 34) ในขณะที่ผู้ก่อการร้ายไม่ได้ยึดหลักกฎหมายและความถูกต้องและปฏิบัติการด้วยความโหดเหี้ยมทารุณ แม้ทรัพยากรมีจำกัด แต่ก็สามารถนำจุดอ่อนของฝ่ายเจ้าหน้าที่ของรัฐมาใช้ประโยชน์ได้ ทั้งยังสามารถสร้างเครือข่ายและรักษาการริเริ่มทำให้เครื่องมือในการต่อสู้การก่อการร้ายต้องใช้ทรัพยากรมหาศาล เครื่องมือที่ใช้ในการต่อต้านการก่อการร้ายได้แก่ นโยบายทางการทูตเพื่อสร้างพันธมิตร และเสียงสนับสนุนในเวทีการเมืองระหว่างประเทศ เพื่อความชอบธรรมในการดำเนินการต่อต้านการก่อการร้าย กฎหมายที่ดำเนินคดีกับผู้ก่อการร้ายในศาลยุติธรรม การควบคุมแหล่งเงินด้วยการตัดวงจรของเงินสนับสนุน การใช้กำลังทหาร การข่าวกรอง และการนำยุทธศาสตร์ผสมเครื่องมือทุกชนิดมารวมกันใช้ให้เกิดศักยภาพสูงสุด(กองข่าวกองทัพภาคที่ 2, ม.ป.ป., หน้า 17- 21 อ้างถึงใน ดุสิต น้ำฝน, 2549, หน้า 34 - 35)

สรุปแนวโน้มการก่อการร้ายในอนาคตจะใช้เครื่องมือและอาวุธที่หลากหลายโดยเฉพาะอุปกรณ์ต่างๆ ที่สามารถหาได้ง่าย มีราคาถูก และก่อให้เกิดผลสัมฤทธิ์ได้อย่างดีเยี่ยม การใช้เทคโนโลยีเข้ามาช่วยในการผลิตและเผยแพร่ข้อมูลข่าวสารในการก่อการร้าย การผลิตอาวุธที่มาทำลายล้าง การใช้สารพิษที่หาซื้อได้ง่าย การใช้อาวุธนิวเคลียร์ ถ้าหากมีโอกาสอันเหมาะก็จะใช้

ยุทธวิธีแบบเดิมไม่ว่าจะเป็นการลอบวางระเบิดการปล้นยึดยาน โดยสาร การลักพาตัว การข่มขู่ การลอบสังหาร การบุกโจมตีด้วยอาวุธ การจับตัวประกัน การซุ่มยิง การกระทำต่อเป้าหมายจะไม่เลือกหรือคำนึงศีลธรรม ประชาชนทั่วไปสามารถเป็นเป้าหมายของการก่อการร้ายได้ทั้งหมด และทันทีเพื่อหวังผลในการสร้างความหวาดกลัวและมีผลในวงกว้างการใช้ไซเบอร์มาเป็นเครื่องมือในการก่อการร้ายมีประสิทธิภาพร้ายแรง แฮกเกอร์ที่มีความรู้และผู้เชี่ยวชาญด้านคอมพิวเตอร์จะเพิ่มขีดความสามารถให้กับกลุ่มผู้ก่อการร้าย เมื่อกลุ่มผู้ก่อการร้ายคิดค้นวิธีการใหม่ๆ ยุทธศาสตร์การต่อต้านการก่อการร้ายจะต้องปรับตัวตาม การลงโทษสถานเบาอาจไม่เพียงพอต่อความผิดของผู้ก่อการร้าย การเปลี่ยนแปลงที่สำคัญของยุทธศาสตร์การต่อต้านการก่อการร้ายในอนาคตจะไม่เกี่ยวข้องเพียงการบุกทลายหรือการตรวจสอบโทรศัพท์มือถือ แต่จะมุ่งเน้นที่การลดทอนความเสี่ยงของประชากรที่ใช้เทคโนโลยีชีวิตประจำวัน

การจัดการกับปัญหาการก่อการร้าย

การจัดการปัญหาการก่อการร้ายแต่ละประเทศมีมุมมองหรือวิธีการในการจัดการกับปัญหาการก่อการร้ายที่แตกต่างกัน จากการให้ความหมายของการก่อการร้ายที่แตกต่างกันในแต่ละประเทศ บางประเทศให้ความหมายของการก่อการร้ายว่า เป็นผู้ก่อการร้าย บางประเทศอาจมีมุมมองต่อผู้ก่อการร้ายว่าเป็นนักต่อสู้เพื่อนำมาซึ่งสันติภาพ นอกจากนั้นนโยบายของแต่ละประเทศในการปฏิบัติต่อผู้ก่อการร้ายที่แตกต่างกัน บางประเทศเลือกที่จะติดต่อหรือวางตัวเป็นกลางกับองค์กรก่อการร้ายซึ่งอาจมีผลประโยชน์ร่วมกัน บางส่วนเป็นเรื่องของการจำกัดความรุนแรงในประเทศของตน หรืออาจเป็นการไม่หวังผลใดก็ตาม ในขณะที่บางประเทศเลือกที่จะต่อต้านการก่อการร้ายอย่างเปิดเผย เมื่อต้องการผลประโยชน์ในความร่วมมือระหว่างสองประเทศที่มีนโยบายต่อต้านการก่อการร้ายที่แตกต่างกัน จึงเป็นเรื่องยากในการปฏิบัติให้เป็นรูปธรรม สิทธิเสรีภาพของประชาชนก็เป็นสิ่งสำคัญที่ต้องพิจารณา แต่ละประเทศจึงต้องพยายามที่จะสร้างระบบรักษาความปลอดภัยและความมั่นคงภายในรัฐและการต่อต้านการก่อการร้าย อาจจะละเมิดสิทธิเสรีภาพของประชาชน ซึ่งหากเลือกที่จะใช้วิธีการออกกฎหมายและระเบียบเพื่อเอื้ออำนวยความสะดวกของเจ้าหน้าที่ของรัฐในการสืบ ติดตาม เสาะแสวงหาข่าวและการตอบโต้องค์กรก่อการร้ายอาจนำไปสู่การละเมิดสิทธิเสรีภาพของประชาชนในรัฐไม่ว่าจะเป็นการดักฟังโทรศัพท์ ดังอย่างที่เห็นได้ชัดกรณีนายเอ็ดวาร์ด สโนเดน ได้ออกมาเปิดเผยถึงโครงการลับของหน่วยงานด้านความมั่นคงของสหรัฐอเมริกาที่มีการเชื่อมโยงและเข้าถึงระบบของผู้บริหารรายใหญ่ ๆ ของสหรัฐอเมริกา ซึ่งไม่ใช่เพียงแค่ประเทศสหรัฐอเมริกาที่มีโครงการลับลักษณะนี้ ในอังกฤษ รัสเซีย ตะวันออกกลาง จีนและอีกในหลายๆประเทศก็ล้วนแล้วแต่มีโครงการลักษณะดังนี้เพื่อให้สามารถเข้าถึงข้อมูลอันอาจเป็น

ประโยชน์ต่อศักยภาพในการทำสงครามไซเบอร์และในการเฝ้าระวังการก่อการร้ายข้อมูลที่นำมาเปิดเผย เป็นต้น การตรวจสอบการใช้อินเทอร์เน็ต และตรวจสอบข้อความในอีเมล์ของผู้ต้องสงสัย การตรวจสอบการหมุนเวียนของกระแสเงิน ที่เชื่อว่ามีส่วนเกี่ยวข้องกับการก่อการร้าย การขยายความหมายของการก่อการร้ายและเพิ่มบทลงโทษแก่ผู้ก่อการร้ายและผู้ที่ทำให้ความช่วยเหลือหรือสนับสนุนการก่อการร้ายทั้งหมดอาจส่งผลให้รัฐมีเครื่องมือที่จะใช้ต่อต้านและตอบโต้การก่อการร้ายมากขึ้น

ประเทศที่เลือกการต่อต้านการก่อการร้ายจะต้องกำหนดวิธีการบรรลุผลในการกระทำ คือ ยุทธศาสตร์และเครื่องมือในการต่อสู้การก่อการร้าย ยุทธศาสตร์จะต้องครอบคลุมประเด็นต่อไปนี้จึงจะเป็นยุทธศาสตร์แห่งความสำเร็จ คือ ปกป้อง (Deter) การก่อการร้ายในอนาคตและลด (Diminish) สาเหตุพื้นฐานของการก่อการร้าย ซึ่งเป็นความพยายามในระยะยาว นอกจากนี้ต้องใช้ทั้งในเชิงรุกในการเอาชนะภัยคุกคามจากการก่อการร้ายและเชิงรับในการป้องกันด้วยการประเมินความเสี่ยงต่อเป้าหมายที่เปราะบางถูกกระทำได้ง่ายและการจัดการกับผลที่ตามมา เพื่อไปสู่การปราศจากการก่อการร้ายหรือลัทธิ องค์กรและขบวนการในการก่อการร้ายลดลง (ศูนย์พลเรือนและทหารสัมพันธ์, 2548, หน้า 34 – 35)

ในแง่ของกฎหมายและระเบียบต่างๆที่เกี่ยวข้องกับไซเบอร์ พบว่า ประเทศไทยไม่มีระเบียบและกฎหมายต่างๆที่ชัดเจน โดยเฉพาะกฎหมายและระเบียบที่จำเป็นในยุคของโลกไซเบอร์สเปซ (Cyber Space) ในส่วนของกฎหมายที่เกี่ยวข้องมีดังนี้ การปกป้องข้อมูลส่วนบุคคล การป้องกันทรัพย์สินทางปัญญา ความปลอดภัยทางไซเบอร์ การป้องกันหรือกฎหมายที่เกี่ยวกับอาชญากรรมทางไซเบอร์ รวมถึงกฎหมายทั้งพหุภาคีและทวิภาคี ความร่วมมือกับต่างประเทศ รวมถึงประเทศในอาเซียนในเรื่องการป้องกันการก่อการร้ายทางไซเบอร์ ประเทศไทยยังไม่มีกฎหมายเฉพาะในเรื่องของการปกป้องข้อมูลส่วนบุคคล และกฎหมายที่เกี่ยวข้องกับอาชญากรรม และ การต่อต้านหรือป้องกันการก่อการร้ายทางไซเบอร์ ซึ่งมีความจำเป็นอย่างยิ่ง ต่อโลกในศตวรรษที่ 21 นี้ อีกทั้งยังต้องเพิ่มการกำหนดแนวทางปฏิบัติที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศ เช่น การใช้เทคโนโลยีคลาวด์ สื่อสังคมออนไลน์ และการจัดการข้อมูลจำนวนมหาศาล ก็ยังไม่ชัดเจนในแนวทางปฏิบัติ

ประเทศไทยมีการแก้ไขกฎหมายเพิ่มเติมประมวลกฎหมายอาญาโดยได้บัญญัติความผิดเกี่ยวกับการก่อการร้ายและกำหนดโทษในการกระทำความผิดไว้ในมาตรา 135/1 – 135/4 โดยเมื่อพิจารณาเจตนารมณ์ของการบัญญัติความผิดเกี่ยวกับการก่อการร้ายดังนี้ลักษณะ 1/1 ความผิดเกี่ยวกับการก่อการร้าย มาตรา 135/1 ผู้ใดกระทำความผิดอาญาดังต่อไปนี้

ใช้กำลังประทุษร้าย หรือกระทำการใดอันก่อให้เกิดอันตรายต่อชีวิต หรืออันตรายอย่างร้ายแรงต่อร่างกายหรือเสรีภาพของบุคคลอื่น กระทำการอันใดก่อให้เกิดความเสียหายอย่างร้ายแรงแก่ระบบการขนส่งสาธารณะ ระบบโทรคมนาคม หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะกระทำการอันใดก่อเกิดความเสียหายแก่ทรัพย์สินของรัฐหนึ่งรัฐใด หรือบุคคลใดหรือต่อสิ่งแวดล้อมอันก่อให้เกิดหรือน่าจะก่อให้เกิดความเสียหายทางเศรษฐกิจถ้าการกระทำนั้นได้กระทำโดยมีจุดมุ่งหมายเพื่อขู่เข็ญหรือบังคับรัฐบาลไทย รัฐบาลต่างประเทศหรือองค์กรระหว่างประเทศให้กระทำหรือไม่ กระทำการอันใดอันก่อให้เกิดความเสียหายอย่างร้ายแรง ต้องระวางโทษประหารชีวิต จำคุกตลอดชีวิต หรือจำคุกตั้งแต่สามปีถึงยี่สิบปีและปรับตั้งแต่หกหมื่นบาทถึงหนึ่งล้านบาท

มาตรา 135/2 (1) ขู่เข็ญว่าจะกระทำการก่อการร้าย โดยมีพฤติกรรมอันควรเชื่อว่าบุคคลนั้นจะกระทำตามที่ขู่เข็ญจริงหรือ (2) สะสมกำลังพลหรืออาวุธจัดหาหรือรวบรวมทรัพย์สินให้หรือรับการฝึกการก่อการร้าย หรือกระทำความผิดใดๆ อันเป็นส่วนของการวางแผนเพื่อการก่อการร้ายหรือยุยงประชาชนให้เข้ามีส่วนร่วมในการก่อการร้ายสองถึงสี่ปี ปรับตั้งแต่สี่หมื่นบาท ถึงสองแสนบาท

มาตรา 135/3 ผู้ใดสนับสนุนในการกระทำความผิดตามมาตรา 135/1 และ 135/2 ต้องระวางโทษเช่นเดียวกัน

มาตรา 135/4 ผู้ใดเป็นสมาชิกของคณะบุคคลซึ่งมีมติหรือประกาศภายใต้คณะมนตรีความมั่นคงแห่งสหประชาชาติ

ในการระบุการกระทำความผิดในการก่อการร้ายตามมาตรา 135/1 -138/4 เป็นการกล่าวเพียงภาพกว้างในประเด็นของการก่อการร้าย แต่ยังไม่ได้เฉพาะไปยังลักษณะ ประเภท และการกล่าวถึงความผิดในการก่อการร้ายทางไซเบอร์

บทสรุปในการจัดการปัญหาของการก่อการร้าย ในแต่ละประเทศความท้าทายของการดำเนินการคือ การหยุดยั้งการก่อการร้ายหรือการลดควบคุมไม่ให้เกิดลัทธิองค์การก่อการร้ายเพิ่มมากขึ้น สิ่งสำคัญคือการวางยุทธศาสตร์ที่เหมาะสมต่อการดำเนินการในการจัดการปัญหาในแต่ละรัฐ ด้านการศึกษาบริบทของแต่ละประเทศที่แตกต่างกันและการให้คำนิยามหรือความหมายของแต่ละประเทศ นโยบายการจัดการปัญหาภายในประเทศ และวิธีการที่จะบรรลุผลในการกระทำ การมีและใช้ทรัพยากรความเชื่อมต่อระหว่างนโยบายและการปฏิบัติ ยุทธศาสตร์การใช้กองกำลัง มิติทางยุทธการการปฏิบัติการ ยุทธวิธีและเทคนิคต่าง ๆ เพื่อให้การก่อการร้ายลดน้อยลง

แนวคิดและทฤษฎีเกี่ยวกับการต่อต้านการก่อการร้าย

จากการศึกษาถึงแนวทางและมาตรการในการต่อต้านการก่อการร้ายจะเห็นได้ว่า การต่อต้านการก่อการร้ายจะใช้เครื่องมือสำคัญคือการผสมผสานกันของทุกเครื่องมือ ทั้งทางการทูต การทหาร การข่าวกรอง การเมืองและกฎหมาย รวมถึงสร้างความร่วมมือจากประชาสังคม นอกจากนั้นการกำหนดยุทธศาสตร์ในการจัดการปัญหา จะนำมาซึ่งความสำเร็จในการต่อต้านการก่อการร้ายและ ในการต่อต้านการก่อการร้ายมีทฤษฎีที่ใช้ประกอบการต่อต้านการก่อการร้ายของมาร์ธาเครนชอร์แอล. พอลบรีเมอร์และไบรอัน เจนกินส์ (Crenshaw, 2006) ดังนี้

1. การต่อต้านการก่อการร้ายแบบป้องกัน

แนวทางการต่อต้านการก่อการร้ายแบบป้องกัน หรือ Preventive counter – terrorism มุ่งเน้นการสร้างอุปสรรคระหว่างผู้ก่อการร้ายกับเป้าหมาย ซึ่งอุปสรรคเหล่านี้อาจอยู่ในรูปแบบของมาตรการป้องกัน การสร้างศักยภาพของหน่วยงานบังคับใช้กฎหมายหรือการปฏิรูปกฎหมาย เป็นต้น โดยแนวคิดเบื้องหลังแนวทางป้องกันนี้เกิดจากความเชื่อที่ว่า การก่อการร้ายไม่อาจถูกขจัดหมดไปได้อย่างสิ้นเชิง ดังนั้นเป้าหมายการต่อต้านการก่อการร้ายคือ การลดระดับความรุนแรงลงสู่จุดที่ไม่ทำให้รัฐบาลต้องทุ่มเททรัพยากรในการดำเนินการจนกระทบต่อการดำเนินนโยบายในด้านอื่นๆ ทฤษฎีการป้องกันการก่อการร้ายที่ดีที่สุดเป็นของมาร์ธา เครนชอร์ (Martha Crenshaw) ศาสตราจารย์ด้านการก่อการร้ายแห่งมหาวิทยาลัยสแตนฟอร์ด ซึ่งพิจารณาการต่อต้านการก่อการร้ายจากมุมมองของวิธีการและองค์การ การต่อต้านการก่อการร้าย จากมุมมองของวิธีการมี 2 หนทาง ได้แก่ การป้องกัน (Defense) และการป้องปราม (Deterrence) โดยมีจุดหมายในการลดโอกาสความสำเร็จในการก่อเหตุของผู้ก่อการร้าย แต่การป้องกันโดยใช้การขัดขวางโดยใช้กำลังเพื่อมิให้ผู้ก่อการร้ายบรรลุเป้าหมายทางกายภาพ มาตรการป้องกันอาจเป็นทั้งเชิงรุก เช่น การใช้กำลังโจมตีกลุ่มก่อการร้าย ที่อยู่ในขั้นตอนสุดท้ายของการวางแผนก่อเหตุและเชิงรับ ซึ่งมิใช่การใช้กำลังอย่างเปิดเผย เช่น การเพิ่มความเข้มงวดในการควบคุมชายแดน ส่วนการป้องปรามเน้นที่การเพิ่มต้นทุนของการก่อการร้ายเพื่อกระตุ้นให้ผู้ก่อการร้ายเลือกหนทางเลือกทางการเมืองอื่น แนวทางการป้องปรามที่มักนิยมใช้คือ การปฏิเสธ (Denial) และการตอบโต้ (Retaliation) โดยการปฏิเสธมีความคล้ายคลึงในทางปฏิบัติกับการป้องกันเชิงรับ แต่ไม่เน้นทำให้การก่อการร้ายเป็นไปไม่ได้ เพียงแค่เพิ่มต้นทุนของการใช้แนวทางการก่อการร้าย ขณะที่การตอบโต้เป็นการกระทำที่ตรงไปตรงมา ซึ่งรัฐต้องตระหนักว่า การตอบโต้ของรัฐอาจเป็นเป้าหมายทางยุทธศาสตร์ในการก่อเหตุของผู้ก่อการร้าย ปัญหาสำคัญที่รัฐประสบปัญหาหากใช้แนวทางที่กระตุ้นให้ผู้ก่อการร้ายเลือกทางเลือกอื่นทดแทนคือ การก่อเหตุมีอัตราสูงเพิ่มมากขึ้น หากกลุ่มผู้ก่อการร้ายมีการเปลี่ยนยุทธวิธี เช่นรอเวลาจนกว่าการก่อการร้ายจะมีต้นทุนต่ำลง หรือการหันไปโจมตีพลเรือนซึ่งไม่สามารถ

ป้องกันตนเองได้ ดังนั้นรัฐจึงควรพยายามทำให้วิธีการโจมตีอื่นยากลำบากขึ้น หรือทำลายทรัพยากรทั้งคน เงินทุน และเครื่องมือของกลุ่มก่อการร้ายด้วย

การต่อต้านการก่อการร้ายตามแนวทางองค์กรจึงมุ่งที่วิธีการที่รัฐจะสร้างให้เกิดการแตกแยกภายในกลุ่มก่อการร้าย ซึ่งเครนชอร์ระบุว่า อาจกระทำได้ทั้งทางออก (Exit) และการส่งเสียง (Voice)โดยทางออกเกิดขึ้นเมื่อสมาชิกคนหนึ่งหรือสมาชิกกลุ่มเล็ก ตัดสินใจลาออกจากกลุ่มหรือแยกตัวออกมาตั้งกลุ่มใหม่ หรือเข้าร่วมกับกลุ่มตรงข้ามกับกลุ่มเดิม ส่วนการส่งเสียงนั้นเกี่ยวข้องกับกระบวนการแสดงความคิดเห็นที่แตกต่างของสมาชิกมีความคิดเห็นคล้อยตามกัน

ดังนั้น จุดอ่อนสำคัญของกลุ่มก่อการร้ายจึงอยู่ที่ความไม่สามารถในการดึงดูดและรักษาสมาชิกไว้ในองค์กรมากกว่าการไม่สามารถในการบรรลุเป้าหมายทางการเมือง การต่อต้านการก่อการร้ายจึงควรให้ความสำคัญกับอัตราการคัดสรรและรักษาสมาชิกของกลุ่มก่อการร้าย โดยช่องทางที่รัฐอาจสนับสนุนให้ผู้ก่อการร้ายละทิ้งกลุ่มก่อการร้ายหรือไม่เข้าร่วมกับกลุ่มก่อการร้ายได้

2.การตอบสนองแบบบริหารจัดการ (Managerial response)

การตอบสนองแบบการบริหารจัดการ ครอบคลุมการวางแผนเผชิญเหตุและแง่มุมในเชิงปฏิบัติของนโยบายสาธารณะในระหว่างหรือภายหลังเกิดเหตุโจมตี เช่น การทำระบบไฟฟ้าสนามบิน การขนส่งให้สามารถดำเนินการได้ตามปกติ และการรักษาพยาบาลผู้บาดเจ็บ รวมถึงทฤษฎีการตอบสนองทางการเมืองต่อการก่อการร้าย โดยในการตอบสนองทางการเมือง

บรีเมอร์ (Bremer, 1998) ระบุว่า แทนที่จะเข้าไปปฏิบัติการต่อต้านกลุ่มก่อการร้ายโดยตรงเพียงอย่างเดียว วัตถุประสงค์ของการต่อต้านการก่อการร้าย ควรอยู่ที่การสร้างสภาพแวดล้อมทางการเมือง เศรษฐกิจและจิตวิทยา ที่เป็นศัตรูต่อการดำเนินงานของกลุ่มก่อการร้าย หากแต่เป็น “ชุมชนรัฐและสภาพแวดล้อมทางยุทธศาสตร์ที่ผู้ก่อการร้ายปฏิบัติการ” ทัศนะของบรีเมอร์สะท้อนจุดสำคัญของการต่อต้านการก่อการร้ายของสหรัฐอเมริกาที่เน้นการกดดันรัฐที่สนับสนุนการก่อการร้ายและทำลายความชอบธรรมของการใช้การก่อการร้ายในฐานะเครื่องมือทางการเมือง

3. มาตรการมุ่งเน้นการตอบโต้

มาตรการมุ่งเน้นการตอบโต้ (Response – oriented measures) มีนัยยะของการตอบสนองต่อการปฏิบัติของผู้ก่อการร้าย โดยไบรอัน เจนกินส์ (Brian Jenkins) เห็นว่ารูปแบบและความรุนแรงในการตอบโต้ของรัฐขึ้นอยู่กับความเข้าใจสภาพเนื้อแท้ของปัญหา โดยหากรัฐไม่เข้าใจปัญหาก็อาจทำให้ตกหลุมพรางของกลุ่มก่อการร้าย ดังนั้นการเข้าใจปัญหาอย่างถ่องแท้ทำให้สามารถแก้ไขปัญหาได้ตรงจุดด้านเครน ชอร์ระบุว่า รัฐสามารถมีมุมมองต่อผู้ก่อการร้ายที่ถูกจับกุมใน 3 ลักษณะ ได้แก่อาชญากรทางการเมือง อาชญากรทั่วไป และนักโทษสงคราม ซึ่งแต่ละมุมมอง

จะสะท้อนยุทธศาสตร์เฉพาะในการต่อต้านการก่อการร้าย เรียงจากการกดดันทางการเมือง การบังคับใช้กฎหมายและการตอบโต้ด้วยกำลังทหาร อย่างไรก็ตามระบอบการปกครองของรัฐเป็นข้อจำกัดสำคัญของปฏิบัติการต่อต้านการก่อการร้าย เช่น ประเทศที่ปกครองด้วยระบอบประชาธิปไตยจะต้องปฏิบัติการในกรอบรูปแบบที่สังคมยอมรับได้ ปัจจัยที่ตัดสินการตอบโต้ของรัฐประกอบด้วยข้อตกลงทางการเมืองในรัฐบาล ทัศนะของนานาชาติและ กองทัพ โดยเฉพาะความใกล้ชิดของกองทัพต่อการตัดสินใจของรัฐวัฒนธรรมในเชิงสถาบันของกองทัพและศักยภาพของยุทโธปกรณ์

จากบริบทของประเทศไทยจะเห็นได้ว่าสอดคล้องกับ ทฤษฎีการต่อต้านการร้ายแบบป้องกัน การตอบสนองแบบบริหารจัดการและมาตรการมุ่งเน้นการตอบโต้ ของมาร์ธา เครนชอร์ แอล พอล บรีเมอร์และไบรอัน เจนกินส์ ด้วยประเทศไทยยังไม่ได้เป็นกลุ่มประเทศที่ถูกโจมตีด้วยการก่อการร้าย ถึงแม้ว่าจะมีเหตุการณ์ที่นำไปสู่กระบวนการวิเคราะห์ถึงสถานการณ์ของการก่อการร้ายก็ตาม สิ่งค้นพบของนักวิจัยคือ ประเทศไทยควรมุ่งเน้นแนวทางของการต่อต้านการก่อการร้ายแบบป้องกัน มุ่งเน้นการสร้างมาตรการป้องกันให้เกิดขึ้นภายในประเทศ โดยพัฒนาตั้งแต่ระดับบุคคล หน่วยงาน องค์กรทั้งภาครัฐและหน่วยงานภาคเอกชน รวมถึงประชาสังคมต่างๆ ให้มีความเข้าใจต่อการก่อการร้ายอย่างจริงจัง และมีการกำหนดแนวทางอย่างเป็นรูปธรรม อีกทั้งสร้างศักยภาพของบุคคล หน่วยงานที่เกี่ยวข้องกับการต่อต้านการก่อการร้าย การกำหนดกฎหมายและการบังคับใช้กฎหมายที่เกี่ยวข้องให้มีบทลงโทษที่ชัดเจน เพื่อลดระดับความรุนแรงลงสู่จุดที่ไม่ทำให้รัฐบาลต้องทุ่มเททรัพยากรในการดำเนินการอย่างมากจนกระทบต่อการดำเนินนโยบายด้านอื่นหรือเป็นการทำให้ต้นทุนของการก่อการร้ายสูงมากขึ้น แนวทางการป้องกันเน้นการเพิ่มต้นทุนการก่อการก่อการร้ายหรือสร้างความแตกแยกภายในกลุ่มก่อการร้าย เช่น ให้สมาชิกมีความหวาดระแวงขึ้นในกลุ่ม วิธีการที่สามารถทำได้ขั้นต้นตามทฤษฎีคือ การป้องกัน (Defense) และการป้องปราม (Deterrence) โดยการป้องกันเป็นการขัดขวางโดยใช้กำลัง เพื่อมิให้ผู้ก่อการร้ายบรรลุเป้าหมายทางกายภาพ การต่อต้านการก่อการร้ายแบบปกป้อง เน้นการสร้างสภาพแวดล้อมทางการเมือง ทางเศรษฐกิจ และสังคมวิทยาที่ไม่เอื้อต่อการทำงานของกลุ่มผู้ก่อการร้าย ส่วนการปราบปราม โดยเน้นการเพิ่มขีดความสามารถในกำลังทางทหาร และพลังอำนาจแห่งชาติ ส่วนแนวทางสุดท้ายคือ การตอบโต้ มุ่งเน้นการเผชิญเหตุ และการลดผลกระทบภายหลังเกิดเหตุ เช่น การฟื้นฟูสภาพหลังเหตุการณ์ที่เกิดขึ้น และการเยียวยาหลังสถานการณ์ ในประเทศไทยควรเพิ่มแนวทางการป้องกันการก่อการร้ายทางไซเบอร์ด้วยการกำหนดให้มีความร่วมมือกันในระดับหน่วยงานที่เกี่ยวข้องกับไซเบอร์เพื่อประสานความร่วมมือ กำหนดแนวทางและสร้างพลังอำนาจเพื่อป้องกันการโจมตีทางไซเบอร์ โดยเป็นการป้องกันในเชิงรับ ส่วนการป้องปราม คือการปฏิเสธและการตอบโต้ ประเทศ

ไทยสามารถดำเนินการต่อต้านการก่อการร้ายทางไซเบอร์โดยการปฏิเสธได้ เช่น การไม่ให้การสนับสนุนแนวทางของการก่อการร้าย การประกาศนโยบายต่อการต่อต้านการก่อการร้ายที่ชัดเจน ในส่วนของการตอบโต้นั้นยังคงเป็นแนวทางที่ประเทศไทยยังต้องพัฒนาอีกหลายทาง เช่น กำลังคน วัสดุอุปกรณ์ที่ใช้ในการต่อต้านก่อการร้าย เงินทุนในการพัฒนาประเทศและส่งเสริมทางด้านนี้ และการบริหารจัดการต่อปัญหาที่เกิดขึ้นเพื่อไม่ให้มีการดำเนินการด้านก่อการร้ายได้

การวิเคราะห์ยุทธศาสตร์ต่อการดำเนินการต่อต้านการก่อการร้ายทางไซเบอร์และบทบาทของประเทศไทย

การศึกษาเกี่ยวกับยุทธศาสตร์การต่อต้านการก่อการร้าย แนวทางการป้องกัน การดำเนินการต่อต้านขององค์กรก่อการร้ายของประเทศไทยและต่างประเทศ สังเคราะห์สรุปผลดังนี้

ตารางที่ 18 สังเคราะห์ยุทธศาสตร์การต่อต้านการก่อการร้าย

ยุทธศาสตร์ต่อต้านการก่อการร้าย	แนวทางที่เกี่ยวข้องในการต่อต้านก่อการร้ายทางไซเบอร์*		
	การต่อต้านแบบป้องกัน	การตอบสนองแบบบริหารจัดการ	มาตรการมุ่งเน้นการตอบโต้
ยุทธศาสตร์ของสหรัฐอเมริกาในการต่อต้านการก่อการร้ายของบารัค โอบามา กำหนดยุทธศาสตร์ 4 มิติ คือ -การเอาชนะองค์กรก่อการร้าย -การไม่เป็นแหล่งเงินทุน/ที่หลบภัย -การลดสภาวะแอบแฝงของการก่อการร้าย -การปกป้องประชาชนและผลประโยชน์	✓	✓	✓
นโยบายการต่อต้านการก่อการร้ายของบิลคลินตัน ปี 1995 ระบุขั้นตอนการ	✓	✓	✓

ยุทธศาสตร์ต่อต้านการก่อการร้าย	แนวทางที่เกี่ยวข้องในการต่อต้านก่อการร้ายทางไซเบอร์*		
	การต่อต้านแบบป้องกัน	การตอบสนองแบบบริหารจัดการ	มาตรการมุ่งเน้นการตอบโต้
ดำเนินงานดังนี้ -การลดจุดอ่อนจุดล่อแหลม -การป้องปรามการก่อการร้าย -การตอบโต้การก่อการร้าย -การป้องกันมิให้กลุ่มก่อการร้ายได้มาซึ่งอาวุธที่มีอานุภาพการทำลายล้างสูง ยุทธศาสตร์การต่อต้านการก่อการร้าย 8 ประการดังนี้ -คุ้มครองพลเมืองมาตุภูมิและผลประโยชน์ของสหรัฐ -ขัดขวาง ลดระดับ แยกออก และทำลายอัลกออิดะห์กับกลุ่มและบุคคลที่เชื่อมโยง -ป้องกันการพัฒนา การได้มาและการใช้อาวุธที่มีอานุภาพการทำล้างสูง -ทำลายแห่งพักพิงของผู้ก่อการร้าย -สร้างพันธมิตรและศักยภาพการต่อต้านการก่อก่อการร้ายที่ยั่งยืน -ลดระดับความเชื่อมโยงระหว่างอัลกออิดะห์กับกลุ่มบุคคลที่เชื่อมโยงกับอัลกออิดะห์ - ต่อต้านยุทธศาสตร์ของกับอัลกออิดะห์			

ยุทธศาสตร์ต่อต้านการก่อการร้าย	แนวทางที่เกี่ยวข้องในการต่อต้านก่อการร้ายทางไซเบอร์*		
	การต่อต้านแบบป้องกัน	การตอบสนองแบบบริหารจัดการ	มาตรการมุ่งเน้นการตอบโต้
และผลกระทบ รวมทั้งลดโอกาสในการแสวงหาประโยชน์จากความรุนแรงในภูมิภาค -ขัดขวางวิธีการที่ผู้ก่อการร้ายอาจใช้ เช่น การเรียกค่าไถ่ การรับเงินทุนสนับสนุนจากภายนอก			
ยุทธศาสตร์ต่อต้านการก่อการร้ายของประเทศออสเตรเลีย Counter – Terrorism White Paper 2010 ระบุถึงองค์ประกอบ 4 ด้านดังนี้ Analysis การวิเคราะห์ภัยคุกคามด้วยข้อมูลและการข่าว Protection การดำเนินมาตรการเพื่อป้องกันประเทศและประชาชนให้ปลอดภัยจากการก่อการร้าย รวมถึงลดความเสี่ยงจากการถูกโจมตี Response การตอบโต้อย่างเหมาะสมและทันเวลา เมื่อเกิดเหตุภัยคุกคามจากการก่อการร้าย ตลอดจนการดำเนินคดีต่อผู้กระทำผิด Resilience การสร้างชุมชนเข้มแข็งให้สามารถต่อต้านการใช้ความรุนแรงหรือ	✓	✓	✓

ยุทธศาสตร์ต่อต้านการก่อการร้าย	แนวทางที่เกี่ยวข้องในการต่อต้านก่อการร้ายทางไซเบอร์*		
	การต่อต้านแบบป้องกัน	การตอบสนองแบบบริหารจัดการ	มาตรการมุ่งเน้นการตอบโต้
การก่อการร้าย			
Cyber Security Strategy of Estonia 2008 -Application of a graduated system of security measures in Estonia -Development of Estonia's expertise in and high awareness of information security to the highest Standard of excellence -Development of an appropriate regulatory and legal framework to support the secure and seamless operability of information systems -promoting international co-operation aimed at strengthening global cyber security	✓	✓	
National Cyber Security Strategy of TURKEY 2013 – 2014 Strategic Cyber Security Actions Regulatory Measures Activities to help judicial process Establishing the National Cyber Incidents	✓	✓	

ยุทธศาสตร์ต่อต้านการก่อการร้าย	แนวทางที่เกี่ยวข้องในการต่อต้านก่อการร้ายทางไซเบอร์*		
	การต่อต้านแบบป้องกัน	การตอบสนองแบบบริหารจัดการ	มาตรการมุ่งเน้นการตอบโต้
Response Organization Strengthening the National Cyber Security Infrastructure Human Resources Education and Awareness Raising Activities in the Field of Cyber Security Developing National Technologies in the field of Cyber Security Extending the Scope of National Cyber Security Mechanisms			
ยุทธศาสตร์การต่อต้านการก่อการร้ายของสหราชอาณาจักรยุทธศาสตร์ต่อต้านการก่อการร้ายหลักมีแนวทางการปฏิบัติตามหลักการ 4Ps ได้แก่ Pursue การติดตามกลุ่มก่อการร้าย เพื่อยับยั้งการถูกโจมตี เช่นการพัฒนางานข่าวกรอง รวมถึงกฎหมาย Prevent ป้องกันมิให้ประชาชนเป็นผู้ก่อการร้าย หรือสนับสนุนแนวคิดนิยมความรุนแรง Protect การเสริมสร้างเกราะป้องกันจากการโจมตี เช่น การเพิ่มขีดความสามารถใน	✓	✓	✓

ยุทธศาสตร์ต่อต้านการก่อการร้าย	แนวทางที่เกี่ยวข้องในการต่อต้านก่อการร้ายทางไซเบอร์*		
	การต่อต้านแบบป้องกัน	การตอบสนองแบบบริหารจัดการ	มาตรการมุ่งเน้นการตอบโต้
การรับมือกับการก่อการร้าย Prepare การลดผลกระทบจากเหตุการณ์ที่ไม่สามารถป้องกันได้ โดยเตรียมความพร้อมในการให้ความช่วยเหลือรวมถึงการฟื้นฟูหลังเหตุการณ์			
The UK Cyber Security Strategy November 2011 Objective 1: The UK to tackle cybercrime and be one of the most secure places in the world to do business in cyberspace Objective 2: The UK to be more resilient to cyberattacks and better able to protect our interests in cyberspace Objective 3: The UK to helped shape an open, stable and vibrant cyberspace which the UK public can use safely and that supports open societies Objective 4: The UK to have the cross – cutting knowledge, skills and capability its needs to underpin all our cyber security objectives	✓	✓	✓
The UK Cyber Security Strategy	✓	✓	✓

ยุทธศาสตร์ต่อต้านการก่อการร้าย	แนวทางที่เกี่ยวข้องในการต่อต้านก่อการร้ายทางไซเบอร์*		
	การต่อต้านแบบป้องกัน	การตอบสนองแบบบริหารจัดการ	มาตรการมุ่งเน้นการตอบโต้
November 2013 -Making the UK one of the most secure place in the world to do business in cyberspace -Making the UK more resilient to Cyber Attack and better able to protect our interests in cyberspace -Helping shape an open, vibrant and stable cyberspace that support open societies -building the UK's cyber security knowledge, skill and capability			
The Cyber Security Strategy of Finland Security cyber largely relies on the exchange of information which, at the international level, is best achieved through co – operation networks. Such networks bolster the ability to take immediate actions in ensuring cyber security and combat Cyber Crime. The professional co – operation networks of the public and private sectors allow for the exchange of expert information on cyber	✓	✓	✓

ยุทธศาสตร์ต่อต้านการก่อการร้าย	แนวทางที่เกี่ยวข้องในการต่อต้านก่อการร้ายทางไซเบอร์*		
	การต่อต้านแบบป้องกัน	การตอบสนองแบบบริหารจัดการ	มาตรการมุ่งเน้นการตอบโต้
security requires close co – operation between the networks which deal with international data security, cyber defence and law enforcement. The most significant of these include the international network of national CERTs, the network of government CERTs, (GovCERT), Interpol and Europol in law enforcement, and organizations dealing with Critical information Infrastructure Protection.			
ยุทธศาสตร์การต่อต้านการก่อการร้ายของประเทศอินโดนีเซียปี 2006 -การป้องกัน ได้แก่ การแก้ไขปัญหารากเหง้าที่เป็นต้นเหตุของการก่อการร้าย - การปราบปราม โดยใช้วิธีการทางทหาร การตัดการสนับสนุนทางการเงิน การบังคับใช้กฎหมาย ตลอดจนการประสานงานระหว่างหน่วยงานที่เกี่ยวข้องอย่างมีประสิทธิภาพ - การสร้างการตระหนักและการเตรียมความพร้อมในหมู่ประชาชนอย่างกว้างขวาง - การปกป้องสถานที่ สาธารณูปโภคหรือ	✓	✓	✓

ยุทธศาสตร์ต่อต้านการก่อการร้าย	แนวทางที่เกี่ยวข้องในการต่อต้านก่อการร้ายทางไซเบอร์*		
	การต่อต้านแบบป้องกัน	การตอบสนองแบบบริหารจัดการ	มาตรการมุ่งเน้นการตอบโต้
วัตถุที่มีความสำคัญหรือเสี่ยงที่จะตกเป็นเป้าหมายการโจมตี			
ประเทศไทย			
นโยบายการแก้ไขปัญหาพรรคคอมมิวนิสต์แห่งประเทศไทย เมื่อวันที่ 23 เม.ย. 2523 พล.อ.เปรม ติลสูนานนท์ นายกรัฐมนตรีลงนามในคำสั่งสำนักนายกรัฐมนตรีที่ 66/2523 เรื่อง นโยบายการต่อสู้เพื่อเอาชนะคอมมิวนิสต์ ประเด็นสำคัญคือการใช้การเมืองนำการทหาร มุ่งเน้นขจัดความไม่เป็นธรรมในสังคม และปฏิบัติต่อผู้ก่อการร้ายคอมมิวนิสต์หรือผู้ที่หลงผิดที่เข้ามอบตัว หรือที่จับได้อย่างเพื่อนประชาชนร่วมชาติ คำสั่งนี้ถือเป็นจุดเปลี่ยนที่สำคัญจากนโยบายขวาจัดของรัฐบาลก่อนหน้ามาเป็นการประนีประนอม	✓	✓	
ยุทธศาสตร์การแก้ไขปัญหาพรรคคอมมิวนิสต์แห่งประเทศไทยพ.ศ. 2537 1.ใช้แนวทาง พลเรือน – ตำรวจ – ทหาร โดยมีประชาชน (เป้าหมาย) ของปฏิบัติการ 2.ส่งเสริมความเข้าใจระหว่างรัฐบาลและ	✓	✓	

ยุทธศาสตร์ต่อต้านการก่อการร้าย	แนวทางที่เกี่ยวข้องในการต่อต้านก่อการร้ายทางไซเบอร์*		
	การต่อต้านแบบป้องกัน	การตอบสนองแบบบริหารจัดการ	มาตรการมุ่งเน้นการตอบโต้
ประชาชน โดยเฉพาะที่อยู่ในชนบท โดยภาครัฐต้องสร้างความเชื่อมั่นให้ประชาชนเห็นถึงความจริงใจของเจ้าหน้าที่			
นโยบายการก่อการร้ายและแก้ ไขการก่อการร้ายฉบับปี 2545 1. พัฒนาประสิทธิภาพงานข่าวกรองและจัดระบบประสานงานข่าว 2. ปรับปรุงกฎหมายให้สอดคล้องกับสภาพปัญหาและสถานการณ์ 3. พัฒนาบุคลากร ระบบข้อมูลข่าวสารและองค์ความรู้ 4. ปลุกจิตสำนึกภาคประชาชนให้มีส่วนร่วมในการหาข่าว และเป็นเครือข่ายชุมชน 5. ลดปัจจัยและเงื่อนไข ที่เอื้อให้บุคลากรบางกลุ่มถูกชักจูงเข้าร่วมกลุ่มก่อการร้ายและการปราบปรามขบวนการอาชญากรรมข้ามชาติ 6. ประสานแผนเตรียมความพร้อมทรัพยากร จัดระบบการประสานงานและฝึกซ้อมการปฏิบัติ 7. กระชับและขยายความร่วมมือในระดับภูมิภาค จัดตั้งกลไกประสานและช่อง	✓	✓	

ยุทธศาสตร์ต่อต้านการก่อการร้าย	แนวทางที่เกี่ยวข้องในการต่อต้านก่อการร้ายทางไซเบอร์*		
	การต่อต้านแบบป้องกัน	การตอบสนองแบบบริหารจัดการ	มาตรการมุ่งเน้นการตอบโต้
ทางการติดต่อสื่อสาร 8. ร่วมมือกับประชาคมระหว่างประเทศและปฏิบัติตามพันธกรณีระหว่างประเทศภายใต้กรอบสหประชาชาติ โดยคำนึงถึงผลประโยชน์และความมั่นคงของชาติเป็นสำคัญ			
พ.ร.บ.ว่าด้วยการจัดระเบียบราชการด้านเทคโนโลยีสารสนเทศและการสื่อสารของกระทรวงกลาโหม -กำหนดให้กระทรวงฯ ดำเนินการเกี่ยวกับระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการบริหารงานทั่วไป ให้สามารถติดต่อเชื่อมโยง แลกเปลี่ยนข้อมูลข่าวสารระหว่างหน่วยงานต่างๆ		✓	
แผนยุทธศาสตร์การพัฒนาเทคโนโลยีสารสนเทศและการสื่อสารกองทัพไทย พ.ศ. 2557 - 2561 ยุทธศาสตร์ที่ 1พัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารให้มีความมั่นคงปลอดภัยและมีประสิทธิภาพ ยุทธศาสตร์ที่ 2 พัฒนาระบบเทคโนโลยี		✓	

ยุทธศาสตร์ต่อต้านการก่อการร้าย	แนวทางที่เกี่ยวข้องในการต่อต้านก่อการร้ายทางไซเบอร์*		
	การต่อต้านแบบป้องกัน	การตอบสนองแบบบริหารจัดการ	มาตรการมุ่งเน้นการตอบโต้
สารสนเทศ เพื่อการบูรณาการข้อมูลร่วมกันอย่างมีประสิทธิภาพ ยุทธศาสตร์ที่ 3 พัฒนาระบบเทคโนโลยีสารสนเทศ สนับสนุนอำนวยการ การใช้กำลังกองทัพและการยุทธร่วมกันอย่างมีประสิทธิภาพ ยุทธศาสตร์ที่ 4 พัฒนาและส่งเสริมการเรียนรู้ของกำลังพลเพื่อมุ่งไปสู่การพึ่งตนเอง			
กรอบนโยบายเทคโนโลยีสารสนเทศและการสื่อสาร ระยะพ.ศ. 2554 – 2563 ของประเทศไทยหรือกรอบนโยบาย ICT 2020 ประกอบด้วย 7 ยุทธศาสตร์ ดังนี้ ยุทธศาสตร์ที่ 1 พัฒนาโครงสร้างพื้นฐาน ICT ให้มีความทันสมัย มีการกระจายอย่างทั่วถึงและมีความปลอดภัย ยุทธศาสตร์ที่ 2 พัฒนาทุนมนุษย์ที่มีความสามารถในการสร้างสรรค์และใช้สารสนเทศอย่างมีประสิทธิภาพ ยุทธศาสตร์ที่ 3 พัฒนาทุนมนุษย์ที่มีความสามารถในการสร้างสรรค์และใช้สารสนเทศอย่างมีประสิทธิภาพ		✓	

ยุทธศาสตร์ต่อต้านการก่อการร้าย	แนวทางที่เกี่ยวข้องในการต่อต้านก่อการร้ายทางไซเบอร์*		
	การต่อต้านแบบป้องกัน	การตอบสนองแบบบริหารจัดการ	มาตรการมุ่งเน้นการตอบโต้
ยุทธศาสตร์ที่ 4 ยกระดับขีดความสามารถในการแข่งขันอุตสาหกรรม ICT ยุทธศาสตร์ที่ 5 ใช้ ICTเพื่อสร้างนวัตกรรมบริการของภาครัฐ ยุทธศาสตร์ที่ 6 พัฒนาและประยุกต์ใช้ ICT เพื่อสร้างความเข้มแข็งของภาคการผลิต ยุทธศาสตร์ที่ 7 พัฒนาและประยุกต์ใช้ ICT เพื่อลดความเหลื่อมล้ำในสังคม ยุทธศาสตร์ที่ 8 พัฒนาและประยุกต์ใช้ ICT เพื่อพัฒนาเศรษฐกิจและสังคมที่เป็นมิตรกับสิ่งแวดล้อม			
แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารของประชาคมอาเซียนสู่ 2015(ASAN ICT Master plan 2015) มีเป้าหมายการพัฒนาดังนี้ ยุทธศาสตร์ที่ 1 การเปลี่ยนแปลงทางเศรษฐกิจเป็นการเตรียมความพร้อมด้านสภาพแวดล้อมให้เหมาะกับการทำธุรกิจเพื่อที่จะดึงดูดการค้า การลงทุนและการสร้างธุรกิจในสาขาเทคโนโลยีสารสนเทศและการสื่อสาร ยุทธศาสตร์ที่ 2 การมีส่วนร่วมของ		✓	

ยุทธศาสตร์ต่อต้านการก่อการร้าย	แนวทางที่เกี่ยวข้องในการต่อต้านก่อการร้ายทางไซเบอร์*		
	การต่อต้านแบบป้องกัน	การตอบสนองแบบบริหารจัดการ	มาตรการมุ่งเน้นการตอบโต้
ประชาชนและการสร้างศักยภาพให้แก่ประชาชน เป็นการปรับปรุงคุณภาพชีวิตของประชาชนผ่านการเข้าถึง ICT อย่างทั่วถึงและเท่าเทียมในราคาที่เหมาะสม			
ยุทธศาสตร์ที่ 3 การสร้างนวัตกรรมคือการส่งเสริมอุตสาหกรรมเทคโนโลยีสารสนเทศและการสื่อสารเพื่อสิ่งแวดล้อมโดยใช้ความคิดสร้างสรรค์และความแปลกใหม่ รวมทั้งส่งเสริมงานวิจัยพัฒนานวัตกรรมเพื่อมุ่งสู่ความเป็นเลิศทางวิชาการ			
ยุทธศาสตร์ที่ 4 การพัฒนาโครงสร้างพื้นฐานเพื่อสนับสนุนการให้บริการเทคโนโลยีสารสนเทศและการสื่อสารต่างๆ ให้ครอบคลุมทั่วทุกชุมชนในอาเซียน			
ยุทธศาสตร์ที่ 5 การพัฒนาทุนมนุษย์เป็นการพัฒนาทรัพยากรธรรมมนุษย์ให้มีทักษะและความสามารถด้าน ICT เพื่อสนับสนุนการเจริญเติบโตของภาคอุตสาหกรรม ICT และช่วยส่งเสริมอุตสาหกรรมอื่น ๆ ในภาคเศรษฐกิจ			
ยุทธศาสตร์ที่ 6 การลดช่องว่างด้านดิจิตอล			

ยุทธศาสตร์ต่อต้านการก่อการร้าย	แนวทางที่เกี่ยวข้องในการต่อต้านก่อการร้ายทางไซเบอร์*		
	การต่อต้านแบบป้องกัน	การตอบสนองแบบบริหารจัดการ	มาตรการมุ่งเน้นการตอบโต้
เพื่อการพัฒนาและส่งเสริมการนำ ICT ไปใช้ให้เกิดประโยชน์ในชีวิตประจำวันเพื่อสร้างอาชีพ			
แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร (ฉบับที่ 3) ระยะ พ.ศ.2554 – 2563 มียุทธศาสตร์ดังนี้ ยุทธศาสตร์ที่ 1พัฒนาทุนมนุษย์ให้มีความรอบรู้ เข้าถึง มีส่วนร่วมในการพัฒนาและใช้ประโยชน์จากระบบ ICT ได้อย่างรู้เท่าทันในการสร้างสรรค์นวัตกรรม เพื่อดำรงชีวิตและการประกอบอาชีพ ยุทธศาสตร์ที่ 2พัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่พอเพียงและคุ้มค่า ยุทธศาสตร์ที่ 3การพัฒนาบริการอิเล็กทรอนิกส์ของภาครัฐอย่างฉลาดทั้งในประเทศและระดับภูมิภาคสากล โดยให้ชุมชนและท้องถิ่นมีส่วนร่วมในการพัฒนาในแนวทางนวัตกรรมและมีความมั่นคงปลอดภัย ยุทธศาสตร์ที่ 4 พัฒนาขีดความสามารถทางธุรกิจ ส่งเสริมให้มีการประยุกต์ใช้ ICT เพื่อให้มีศักยภาพในการแข่งขันในตลาดใน	✓	✓	

ยุทธศาสตร์ต่อต้านการก่อการร้าย	แนวทางที่เกี่ยวข้องในการต่อต้านก่อการร้ายทางไซเบอร์*		
	การต่อต้านแบบป้องกัน	การตอบสนองแบบบริหารจัดการ	มาตรการมุ่งเน้นการตอบโต้
ระดับภูมิภาคและระดับสากล			
ยุทธศาสตร์การบูรณาการรัฐบาลอิเล็กทรอนิกส์ E - Government ยุทธศาสตร์ที่ 1 พัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารเป็นโครงข่ายสื่อสารข้อมูลภาครัฐ ยุทธศาสตร์ที่ 2 การเพิ่มประสิทธิภาพของรัฐบาลอิเล็กทรอนิกส์ ยุทธศาสตร์ที่ 3 การสนับสนุนการบริการอิเล็กทรอนิกส์		✓	
แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการศึกษา กระทรวงศึกษาธิการ พ.ศ. 2557 – 2559 ยุทธศาสตร์ที่ 1 ยกระดับความสามารถของผู้สอนและบุคลากรทางการศึกษาในการใช้ ICTเพื่อการศึกษา ยุทธศาสตร์ที่ 2 ส่งเสริมระบบการสนับสนุนการเรียนการสอนแบบอิเล็กทรอนิกส์ เพื่อพัฒนาผู้เรียน ยุทธศาสตร์ที่ 3 พัฒนาโครงสร้างพื้นฐาน ICTเพื่อขยายโอการการเข้าถึงบริการทางการศึกษาและการเรียนรู้ตลอดชีวิต	✓	✓	

ยุทธศาสตร์ต่อต้านการก่อการร้าย	แนวทางที่เกี่ยวข้องในการต่อต้านก่อการร้ายทางไซเบอร์*		
	การต่อต้านแบบป้องกัน	การตอบสนองแบบบริหารจัดการ	มาตรการมุ่งเน้นการตอบโต้
ยุทธศาสตร์ที่ 4 พัฒนาระบบ ICT เพื่อสนับสนุนการบริหารจัดการและการบริการ ยุทธศาสตร์ที่ 5 ส่งเสริมการวิจัยและพัฒนาองค์ความรู้ด้านเทคโนโลยีและนวัตกรรมเพื่อการศึกษา			
ยุทธศาสตร์ไซเบอร์ของกระทรวงเทคโนโลยีและสารสนเทศประเทศไทย ยุทธศาสตร์ที่ 1การประสานความร่วมมือระหว่างภาครัฐและเอกชนเพื่อความมั่นคงปลอดภัยไซเบอร์ ยุทธศาสตร์ที่ 2 การสร้างความตระหนักและรอบรู้ด้านความมั่นคงปลอดภัย ไซเบอร์ ยุทธศาสตร์ที่ 3 การพัฒนาระเบียบและกฎหมายเพื่อความมั่นคงปลอดภัยไซเบอร์ ยุทธศาสตร์ที่ 4 การวิจัยและพัฒนาเพื่อความมั่นคงปลอดภัยไซเบอร์ ยุทธศาสตร์ที่ 5 การประสานความร่วมมือระหว่างประเทศเพื่อความมั่นคงปลอดภัยไซเบอร์	✓	✓	

ยุทธศาสตร์ต่อต้านการก่อการร้าย	แนวทางที่เกี่ยวข้องในการต่อต้านก่อการร้ายทางไซเบอร์*		
	การต่อต้านแบบป้องกัน	การตอบสนองแบบบริหารจัดการ	มาตรการมุ่งเน้นการตอบโต้
ยุทธศาสตร์ไซเบอร์ของคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ประเทศ ประกอบด้วย	✓	✓	
ยุทธศาสตร์หลัก 3 ด้านแรก และยุทธศาสตร์รองอีก 5 ด้านคือ			
ยุทธศาสตร์ที่ 1 การบูรณาการจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย			
ยุทธศาสตร์ที่ 2 การสร้างศักยภาพในการตอบสนองต่อสถานการณ์ฉุกเฉินความมั่นคงปลอดภัยไซเบอร์			
ยุทธศาสตร์ที่ 3 การป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศไทย			
ยุทธศาสตร์ที่ 4 การประสานความร่วมมือระหว่างภาครัฐและเอกชนเพื่อความมั่นคงปลอดภัยไซเบอร์			
ยุทธศาสตร์ที่ 5 การสร้างความตระหนักและรอบรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์			
ยุทธศาสตร์ที่ 6 การพัฒนาระเบียบและกฎหมายเพื่อความมั่นคงปลอดภัยไซเบอร์			
ยุทธศาสตร์ที่ 7 การวิจัยและพัฒนาเพื่อ			

ยุทธศาสตร์ต่อต้านการก่อการร้าย	แนวทางที่เกี่ยวข้องในการต่อต้านก่อการร้ายทางไซเบอร์*		
	การต่อต้านแบบป้องกัน	การตอบสนองแบบบริหารจัดการ	มาตรการมุ่งเน้นการตอบโต้
ความมั่นคงปลอดภัยไซเบอร์			
ยุทธศาสตร์ที่ 8 การประสานความร่วมมือระหว่างประเทศเพื่อความมั่นคงปลอดภัยไซเบอร์			

*จากทฤษฎีการต่อต้านการก่อการร้ายแบบป้องกันของ Martha Crenshaw L. Paul Bremer และ Brian Jenkins

จากการศึกษาเกี่ยวกับเรื่องยุทธศาสตร์การต่อต้านการก่อการร้าย แนวทางการป้องกันต่อต้านการดำเนินการต่อองค์กรก่อการร้ายของประเทศไทยและต่างประเทศ พบว่า นโยบายการต่อต้านการก่อการร้ายของบิล คลินตัน ปี 1995 มีการดำเนินการต่อต้านการก่อการร้าย ป้องกันโดยเน้นการลดระดับความเชื่อมโยงระหว่างอัลกออิดะห์กับกลุ่มบุคคล มุ่งเน้นการตอบโต้ ทำลายแหล่งพักพิงของกลุ่มผู้ก่อการร้าย ส่วนของบารัค โอบามา มุ่งเน้นการตอบโต้โดยการเอาชนะองค์กรก่อการร้าย ตอบสนองแบบบริหารจัดการ การไม่เป็นแหล่งเงินทุนหรือที่หลบภัยและการปกป้องผลประโยชน์ของประชาชน

ประเทศออสเตรเลีย มียุทธศาสตร์การต่อต้านการก่อการร้าย ในปี 2010 เน้นการต่อต้านการก่อการร้ายทั้ง 3 แนวทาง การต่อต้านแบบป้องกัน มีการดำเนินมาตรการเพื่อป้องกันประเทศและประชาชนให้ปลอดภัยจากการก่อการร้าย รวมถึงลดความเสี่ยงจากการถูกโจมตี แต่สิ่งที่น่าสนใจคือมาตรการการตอบโต้ เน้นการตอบโต้อย่างเหมาะสมและทันเวลาเมื่อเกิดเหตุภัยคุกคามจากการก่อการร้าย

ประเทศเอสโทเนีย ประกาศเอกราชครั้งแรกในปี พ.ศ.2461 ก่อนจะถูกยึดครองโดยสหภาพโซเวียต นาซีเยอรมัน และสหภาพโซเวียตอีกครั้งหลังสงครามโลกครั้งที่สอง เอสโทเนียกลับมาเป็นรัฐเอกราชอีกครั้งหลังการล่มสลายของสหภาพโซเวียต ได้กำหนดยุทธศาสตร์ความมั่นคงทางไซเบอร์ โดยมีมาตรการแบบบริหารจัดการโดยการส่งเสริมความร่วมมือระหว่างประเทศที่มุ่งเสริมสร้างการศึกษาความปลอดภัยในโลกไซเบอร์ทั่วโลก การต่อต้านแบบป้องกัน มี

ยุทธศาสตร์การกำกับดูแลกฎหมายที่เหมาะสมเพื่อสนับสนุนการทำงานที่ปลอดภัยและราบรื่นของระบบสารสนเทศ

ประเทศอินโดนีเซีย มีการกำหนดยุทธศาสตร์การต่อต้านการก่อการร้าย ปี 2006 เน้นการป้องกันโดยการแก้ไขปัญหาที่รากเหง้าที่เป็นต้นเหตุของการก่อการร้าย การปกป้องสถานที่สาธารณูปโภคหรือวัตถุที่มีความสำคัญหรือเสี่ยงที่จะตกเป็นเป้าหมายการโจมตี การตอบสนองแบบบริหารจัดการ เน้นการสร้างการตระหนักและการเตรียมความพร้อมในหมู่ประชาชนอย่างกว้างขวาง

ประเทศตุรกี กำหนดยุทธศาสตร์ความมั่นคงทางไซเบอร์ ในระหว่างปี 2013 – 2014 เน้นมาตรการแบบป้องกัน โดยการเสริมสร้างโครงสร้างพื้นฐานการรักษาความปลอดภัยไซเบอร์แห่งชาติ พัฒนาเทคโนโลยีในการรักษาความปลอดภัยทางไซเบอร์ ส่วนการตอบสนองการบริหารจัดการ เน้นการสร้างความตระหนักกิจกรรมในด้านการรักษาความปลอดภัยทางไซเบอร์

ประเทศอังกฤษ มียุทธศาสตร์การต่อต้านการก่อการร้าย มีแนวทางในการต่อต้านการก่อการร้ายทั้ง 3 ทาง ป้องกันโดยไม่ให้ประชาชนเป็นผู้ก่อการร้ายหรือสนับสนุนแนวคิดนิยมหัวรุนแรง แนวทางการตอบสนองการบริหารจัดการ การเสริมสร้างเกราะป้องกันจากการโจมตีและการตอบโต้ การติดตามกลุ่มผู้ก่อการร้ายเพื่อยับยั้งการถูกโจมตีและลดผลกระทบจากเหตุการณ์ที่ไม่สามารถป้องกันได้ โดยมีการเตรียมความพร้อมในการช่วยเหลือรวมถึงการฟื้นฟูหลังเหตุการณ์ ในส่วนของยุทธศาสตร์ความมั่นคงทางไซเบอร์ของประเทศอังกฤษ พบว่า ในปี 2011 และปี 2013 มีการกำหนดยุทธศาสตร์ในทิศทางเดียวกัน ป้องกันโดยการสร้างความรู้ด้านความปลอดภัยไซเบอร์มีความรู้และทักษะ ความสามารถ มุ่งเน้นการตอบโต้ โดยมีความยืดหยุ่นมากขึ้นในการโจมตีทางไซเบอร์และสามารถที่จะปกป้องผลประโยชน์ของประเทศในโลกไซเบอร์

ประเทศฟินแลนด์ มียุทธศาสตร์ในการสร้างความมั่นคงทางไซเบอร์ โดยมีการป้องกันโดยการอาศัยการแลกเปลี่ยนข้อมูล ในระดับนานาชาติสร้างความร่วมมือและเครือข่าย สนับสนุนความสามารถในการดำเนินการได้ทันทีในการรักษาความมั่นคงปลอดภัย และสร้างเครือข่ายระหว่างประเทศในการบังคับใช้กฎหมายและองค์กรที่เกี่ยวข้องเพื่อป้องกันโครงสร้างพื้นฐาน

จากตารางการสังเคราะห์จะเห็นได้ว่า หลายประเทศมีความพร้อมและเตรียมการในการต่อต้านการก่อการร้าย โดยมีการกำหนดยุทธศาสตร์อย่างเป็นรูปธรรม และให้ความสำคัญกับยุทธศาสตร์ความมั่นคงทางไซเบอร์ แต่ก็ยังคงไม่มียุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ที่ชัดเจน

ในส่วนของประเทศไทยมีนโยบายการแก้ไขปัญหาพรรคคอมมิวนิสต์แห่งประเทศไทย ปี 2523 เน้นการขจัดความไม่เป็นธรรมในสังคม และยุทธศาสตร์การแก้ไขปัญหาพรรคคอมมิวนิสต์

แห่งประเทศไทย ปี 2537 เน้นการส่งเสริมความเข้าใจระหว่างรัฐบาลและประชาชน ส่วนนโยบายการก่อการร้ายและแก้ไขการก่อการร้ายฉบับปี 2545 เน้นการป้องกันพัฒนาประสิทธิภาพของงานข่าวกรอง จัดระบบประสานงานข่าว ปลุกจิตสำนึกภาคประชาชนให้มีส่วนร่วมในการหาข่าวและเป็นเครือข่าวชุมชน ส่วนพ.ร.บ.ว่าด้วยการจัดระเบียบราชการด้านเทคโนโลยีสารสนเทศและการสื่อสารของกระทรวงกลาโหม

แผนยุทธศาสตร์การพัฒนาเทคโนโลยีสารสนเทศและการสื่อสารกองทัพไทย พ.ศ. 2557 – 2561กรอบนโยบายเทคโนโลยีสารสนเทศและการสื่อสาร ระยะพ.ศ. 2554 – 2563 ของประเทศไทยหรือกรอบนโยบาย ICT 2020 แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารของประชาคมอาเซียนสู่ 2015 (ASAN ICT Master plan 2015) แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร (ฉบับที่ 3) ระยะ พ.ศ.2554 – 2563 ยุทธศาสตร์การบูรณาการรัฐบาลอิเล็กทรอนิกส์ E - Government และแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการศึกษา กระทรวงศึกษาธิการ พ.ศ. 2557 – 2559 มีแนวทางการกำหนดยุทธศาสตร์การในแนวทางการตอบสนองแบบบริหารจัดการทั้งสิ้น แต่ในปี 2556 ได้กำหนดยุทธศาสตร์ไซเบอร์ของคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ การตอบสนองแบบบริหารจัดการ โดยการสร้างศักยภาพในการตอบสนองต่อสถานการณ์ฉุกเฉินความมั่นคงไซเบอร์และการป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศไทย ต่างกับยุทธศาสตร์ไซเบอร์ของกระทรวงเทคโนโลยีและสารสนเทศแห่งประเทศไทย มุ่งเน้นการป้องกัน โดยการประสานความร่วมมือระหว่างรัฐและเอกชนเพื่อความมั่นคงปลอดภัยไซเบอร์ สร้างความตระหนักและรอบรู้ทางไซเบอร์ ด้านการตอบสนองแบบบริหารจัดการ เน้นการพัฒนาระเบียบและกฎหมาย และการวิจัยและพัฒนา เพื่อความมั่นคงปลอดภัยทางไซเบอร์

สิ่งที่ค้นพบ การสังเคราะห์ข้อมูลประเทศไทยยังไม่ให้ความสำคัญต่อการก่อการร้ายทางไซเบอร์ ด้วยเพราะยังไม่มีสถานการณ์เกิดขึ้นในประเทศไทยจึงยังไม่มีการกำหนดในแผนการพัฒนาทางเทคโนโลยีสารสนเทศและยุทธศาสตร์ทางไซเบอร์อีกทั้งประเทศไทยยังขาดการร่วมมือกันระหว่างองค์กรทั้งภาครัฐ ภาคเอกชนและภาคประชาชน และการแบ่งปันข้อมูลข่าวสารร่วมกันเพื่อแบ่งปันข้อมูล รวมทั้งการจัดการศึกษาที่เป็นรากฐานของการเรียนรู้ในการสร้างพื้นฐานของประชาชน

จุดแข็ง จุดอ่อน โอกาสและอุปสรรคที่มีต่อการเกิดการก่อการร้ายทางไซเบอร์รวมทั้งวิเคราะห์ผลกระทบของประเทศไทยที่มีต่อการเกิดการก่อการร้ายต่อการป้องกันการก่อการร้ายทางไซเบอร์ในประเทศไทย

ส่วนที่ 1 การวิเคราะห์จุดแข็ง จุดอ่อน โอกาสและอุปสรรคที่มีต่อการเกิดการก่อการร้ายทางไซเบอร์

จุดแข็งมีดังนี้

1. ประเทศไทยเป็นมิตรกับประเทศทั้งในภูมิภาคอาเซียนและประเทศอื่นในโลกทำให้เราไม่เป็นเป้าหมายของการก่อการร้าย

2. ประเทศไทยเรียนรู้การนำเอาความรู้จากหลายๆ ประเทศมาพัฒนาทางเทคโนโลยี

3. ประเทศไทยยังมีวิถีของการเป็นประเทศเกษตรกรรมกับอุตสาหกรรมรวมกัน

4. ประเทศไทยมีหน่วยงานที่จัดตั้งขึ้นเพื่อดูแลทางไซเบอร์ทั้งภาครัฐและภาคเอกชน

จุดอ่อนมีดังนี้

1. ประชาชนยังไม่มีความตระหนักต่อภัยคุกคามทางไซเบอร์

2. ระบบคอมพิวเตอร์มีช่องโหว่ทำให้ง่ายต่อการถูกโจมตี

3. ประเทศไทยยังไม่มีกฎหมายที่สามารถบังคับและควบคุมการใช้ทางไซเบอร์

4. ไม่มีหน่วยงานกลางในการประสานงานทางด้านไซเบอร์

5. ประเทศไทยยังคงมีการเมืองที่ไม่มั่นคง และต้องอยู่ภายใต้กฎอัยการศึก

6. ประเทศไทยยังไม่มีโครงข่ายพื้นฐานที่สามารถเชื่อมต่อกันทั้งหมด และความเร็วของพื้นที่ไม่ทั่วทั้งประเทศ

7. ประเทศไทยยังขาดบุคลากรที่มีความเชี่ยวชาญทางไซเบอร์และเทคโนโลยี

8. ผู้บริหารระดับสูงของประเทศยังไม่มีความเข้าใจและไม่ให้ความสำคัญต่อการป้องกันการก่อการร้ายทางไซเบอร์มีช่องว่างของช่วงอายุทำให้เกิดปัญหาต่อระบบการทำงาน

9. โครงสร้างทางสาธารณูปโภคด้านไซเบอร์ ด้านอินเทอร์เน็ตต้องพัฒนาอีกมาก

10. การขาดระบบแบ็คอัพ (back up) ข้อมูลเมื่อเกิดปัญหาขัดข้องซึ่งต้องพัฒนาให้แข็งแรงกว่านี้

11. ต้องมีการสนับสนุนงบประมาณในการพัฒนาและป้องกันการก่อการร้ายทางไซเบอร์

12. ประเทศไทยยังไม่ได้ให้ความสำคัญกับการลงทุนเรื่องระบบการป้องกันการก่อการร้ายทางไซเบอร์

13. การขาดประชาสัมพันธ์หรือวิธีการในการสร้างให้คนไทยตระหนักรู้ถึงภัยในการก่อการร้ายทางไซเบอร์ หรือการใช้ไซเบอร์อย่างถูกต้องซึ่งเป็นเรื่องใกล้ตัว

14. ปัญหาของอาชญากรรมไซเบอร์ประชาชนมองว่าเป็นเรื่องไกลตัวมองว่าเป็นหน้าที่ของรัฐจัดการกับปัญหาอาชญากรรม

15. ประเทศไทยยังต้องพัฒนาเทคโนโลยีให้มีประสิทธิภาพและมีการบริหารจัดการที่ดี เพียงพอและทรัพยากรของเมืองไทยยังไม่พร้อม ไม่เพียงพอ

16. ประเทศไทยยังไม่มีระบบการจัดระเบียบและเก็บหลักฐานข้อมูล (Law full intercepts) และไม่มีหน่วยงานรองรับการดำเนินการในการทางไซเบอร์

โอกาสมีดังนี้

1. ประเทศไทยมีการสร้างภูมิคุ้มกันไม่ให้เป็นฐานในการโจมตีทางไซเบอร์

2. สังคมไทยมีสิ่งอำนวยความสะดวกและประชาชนพร้อมปรับตัวได้ตลอดเวลา

3. ประเทศไทยมีนโยบายในการส่งเสริมการพัฒนาด้านโครงสร้างพื้นฐาน

4. ประเทศไทยมีคนรุ่นใหม่ที่มีความสนใจและมีความรู้ทางไซเบอร์

5. มีนโยบายในส่งเสริมการพัฒนาทางเทคโนโลยีไซเบอร์และมีนโยบายของประเทศไทยสนับสนุนให้เข้าสู่โลกของอินเทอร์เน็ต

6. ประเทศไทยส่งเสริมให้คนไทยเข้าถึงข้อมูลได้ง่ายมากขึ้น

7. ประเทศไทยมีโอกาสในการพัฒนาเทคโนโลยีทางไซเบอร์อีกมากมาย เช่นการใช้ไซเบอร์เพื่อการเกษตรกรรม

อุปสรรคมีดังนี้

1. แนวทางการทำงานของคนไทยคือ คนคิดไม่ได้ทำ คนทำไม่ได้คิด

2. ประเทศไทยให้ความสำคัญกับระบบเครือข่ายมากกว่าฐานความรู้ประเทศไทยยังคงมีวิธีการทำงานแบบเครือข่ายและระบบอุปถัมภ์ในการทำงาน

3. การสนับสนุนในด้านงบประมาณในการดำเนินการมีไม่เพียงพอ

4. โครงสร้างพื้นฐานของประเทศไทยยังเป็นระบบเก่ายังไม่พัฒนาสมบูรณ์แบบ

5. ประชาชนยังไม่มีความรู้ ความไม่เข้าใจเรื่องไซเบอร์อีกมาก

6. โครงสร้างพื้นฐานที่รองรับการขยายตัวทางไซเบอร์ยังต้องพัฒนาอีกมาก

ตารางที่ 19 การวิเคราะห์ SWOT การต่อต้านการก่อการร้ายทางไซเบอร์ของประเทศไทย

การวิเคราะห์ SWOT การต่อต้านการก่อการร้ายทางไซเบอร์ของประเทศไทย	
จุดแข็ง (S)	จุดอ่อน (W)
S1.ประเทศไทยเป็นมิตรกับประเทศทั้งในภูมิภาคอาเซียนและประเทศอื่นในโลก ทำให้เราไม่เป็นเป้าหมายของการก่อการร้าย S2. ประเทศไทยเรียนรู้การนำเอาความรู้ของหลายๆ ประเทศมาพัฒนาทางเทคโนโลยี	W1.ประชาชนยังไม่มีความตระหนักต่อภัยคุกคามทางไซเบอร์ W2.ระบบคอมพิวเตอร์มีช่องโหว่ทำให้ง่ายต่อการถูกโจมตี W3.ประเทศไทยยังไม่มีกฎหมายที่สามารถ

การวิเคราะห์ SWOT การต่อต้านการก่อการร้ายทางไซเบอร์ของประเทศไทย	
S3.ประเทศไทยยังมีวิถีของการเป็นประเทศเกษตรกรรมกับอุตสาหกรรมรวมกัน S4.ประเทศไทยมีหน่วยงานที่จัดตั้งขึ้นเพื่อดูแลทาง ไซเบอร์ทั้งภาครัฐและเอกชน	บังคับและควบคุมการใช้ทางไซเบอร์ W4.ไม่มีหน่วยงานกลางในการประสานงานทางด้านไซเบอร์ W5.ประเทศไทยยังคงมีการเมืองที่ไม่มั่นคง และต้องอยู่ภายใต้กฎอัยการศึก W6.ประเทศไทยยังไม่มีโครงข่ายพื้นฐานที่สามารถเชื่อมต่อกันทั้งหมด และความเร็วของพื้นที่ไม่ทั่วทั้งประเทศ W7. ประเทศไทยยังขาดบุคลากรที่มีความเชี่ยวชาญทางไซเบอร์และเทคโนโลยี W8. ผู้บริหารระดับสูงของประเทศยังไม่มีความเข้าใจและไม่ให้ความสำคัญต่อการป้องกันการก่อการร้ายทางไซเบอร์มีช่องว่างของช่วงอายุทำให้เกิดปัญหาต่อระบบการทำงาน W9.โครงสร้างทางสาธารณูปโภคด้านไซเบอร์ด้านอินเทอร์เน็ตต้องพัฒนาอีกมาก W10. การขาดระบบแบคอัพ (back up) ข้อมูลเมื่อเกิดปัญหาขัดข้องซึ่งต้องพัฒนาให้แข็งแรงกว่านี้ W11.ต้องมีการสนับสนุนงบประมาณในการพัฒนาและป้องกันการก่อการร้ายทางไซเบอร์ W12.ประเทศไทยยังไม่ได้ให้ความสำคัญกับการลงทุนเรื่องระบบการป้องกันการก่อการร้ายทางไซเบอร์ W13.การขาดประชาสัมพันธ์หรือวิธีการในการสร้างให้คนไทยตระหนักรู้ถึงภัยในการก่อการร้ายทางไซเบอร์ หรือการใช้ไซเบอร์อย่างถูกต้องซึ่งเป็นเรื่องใกล้ตัว W14.ปัญหาของอาชญากรรมไซเบอร์ประชาชน

การวิเคราะห์ SWOT การต่อต้านการก่อการร้ายทางไซเบอร์ของประเทศไทย	
	มองว่าเป็นเรื่องไกลตัวและมองว่าเป็นหน้าที่ของรัฐจัดการกับปัญหาอาชญากรรม W15.ประเทศไทยยังต้องพัฒนาเทคโนโลยีให้มีประสิทธิภาพและมีการบริหารจัดการที่ดี เพียงพอและทรัพยากรของเมืองไทยยังไม่พร้อม ไม่เพียงพอ W16.ประเทศไทยยังไม่มีระบบการจัดระเบียบและการเก็บหลักฐานข้อมูล(Law Full Intercepts)และไม่มีหน่วยงานรองรับการดำเนินการในการทางไซเบอร์
โอกาส (O)	อุปสรรค (T)
O1.ประเทศไทยมีการสร้างภูมิคุ้มกันไม่ให้เป็นฐานในการโจมตีทางไซเบอร์ O2.สังคมไทยมีสิ่งอำนวยความสะดวกและประชาชนพร้อมปรับตัวได้ตลอดเวลา O3.ประเทศไทยมีนโยบายในการส่งเสริมการพัฒนาด้านโครงสร้างพื้นฐาน O4.ประเทศไทยมีคนรุ่นใหม่มีความสนใจและมีความรู้ทางไซเบอร์ O5.ประเทศไทยมีนโยบายในส่งเสริมการพัฒนาทางเทคโนโลยีไซเบอร์และมีนโยบายของประเทศไทยสนับสนุนให้เข้าสู่โลกของอินเทอร์เน็ต O6.ประเทศไทยส่งเสริมให้คนไทยเข้าถึงข้อมูลได้ง่ายมากขึ้น O7.ประเทศไทยมีโอกาสในการพัฒนาเทคโนโลยีทางไซเบอร์อีกมากมาย เช่นการใช้ไซเบอร์เพื่อการเกษตรกรรม	T1.แนวทางการทำงานของคนไทยคือ คนคิดไม่ได้ทำ คนทำไม่ได้คิด T2.ประเทศไทยให้ความสำคัญกับระบบเครือข่ายมากกว่าฐานความรู้ประเทศไทยยังคงมีวิธีการทำงานแบบเครือข่ายและระบบอุปถัมภ์ในการทำงาน T3.การสนับสนุนในด้านงบประมาณในการดำเนินการมีไม่เพียงพอ T4.โครงสร้างพื้นฐานของประเทศไทยยังเป็นระบบเก่ายังไม่พัฒนาสมบูรณ์แบบ T5.ประชาชนยังไม่มีความรู้ ความไม่เข้าใจเรื่องไซเบอร์อีกมาก T6.โครงสร้างพื้นฐานของประเทศที่รองรับการขยายตัวทางไซเบอร์ยังไม่มีความพร้อมต่อการพัฒนา

การกำหนดยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย

1. ผลการวิเคราะห์ จุดแข็ง จุดอ่อน โอกาสและอุปสรรครวมทั้งวิเคราะห์ผลกระทบของประเทศไทยที่มีต่อการเกิดการก่อการร้ายและการป้องกันการก่อการร้ายทางไซเบอร์ในประเทศไทยสภาพแวดล้อมที่มีผลต่อการดำเนินการของประเทศไทยต่อการต่อต้านการก่อการร้าย

ด้านเศรษฐกิจ

ในปัจจุบันจะพบได้ว่า สภาวะทางเศรษฐกิจของประเทศไทย เกิดการตื่นตัวต่อการรวมกลุ่มของประชาคมอาเซียน รวมทั้งประเทศไทยต้องปรับตัวเข้าสู่เศรษฐกิจโลก โดยการรวมกลุ่มเศรษฐกิจเพื่อให้เกิดการลื่นไหลในภูมิภาคอาเซียนทั้งในเรื่องของข้อมูลข่าวสารและการค้าเสรี การบริการและการท่องเที่ยว ประเทศไทยจึงจำเป็นต้องปรับตัวเพื่อให้สอดคล้องกับเศรษฐกิจโลกที่มีแนวโน้มของการขยายตัวที่ลดลง อีกทั้งปัญหาทางเศรษฐกิจที่เกิดขึ้นกับประเทศมหาอำนาจต่างๆ ผลปรากฏที่เกิดจากการรวมกลุ่มทางเศรษฐกิจ ได้แก่ การเคลื่อนย้ายของแรงงาน ธุรกิจอุตสาหกรรม การลงทุนกับต่างประเทศ สิ่งที่เป็นตัวชี้วัดสำคัญของการเติบโตทางเศรษฐกิจคือ การบริการ อุตสาหกรรม และการลงทุน ต่างมุ่งเน้นการเพิ่มประสิทธิภาพและการสร้างนวัตกรรม โดยการนำเทคโนโลยีสารสนเทศและการสื่อสารมาเป็นเครื่องมือในการช่วยพัฒนาทางด้านเศรษฐกิจ เมื่อนำเอาเทคโนโลยีสารสนเทศมาใช้เป็นเครื่องมือในการสร้างการเติบโต จำเป็นอย่างยิ่งที่จะต้องพัฒนาความรู้ทางเทคโนโลยี รวมทั้งการสร้างความตระหนักรู้เพื่อไม่ให้หลงกลต่อการหลอกลวงทางเศรษฐกิจ และไม่ตกเป็นเหยื่อของการก่อการร้าย

ด้านสังคม

สภาพสังคมของประเทศไทย ยังมีอิทธิพลหรือถูกครอบงำแนวความคิดแบบทุนนิยมที่เป็นผลกระทบมาจากระบบทุนนิยมในกระแสโลกาภิวัตน์ ทำให้คนไทยได้รับอิทธิพลที่ส่งผลกระทบต่อวิถีชีวิต การอพยพย้ายถิ่นของประชากรวัยแรงงานมาทำงานในเมือง มีผลต่อการเปลี่ยนแปลงโครงสร้างของประชากร ทำให้เกิดชุมชนแออัด คุณภาพชีวิตลดน้อยลง แต่ในภาคชนบทขาดประชากรวัยแรงงาน สถานการณ์ของการเข้าสู่สังคมผู้สูงอายุ รวมถึงประเทศไทยยังคงมีปัญหาสังคมอีกมาก เช่นปัญหาการค้ามนุษย์ ปัญหาของแรงงานผิดกฎหมาย ปัญหาของโรคระบาด อาชญากรรมที่นำไปสู่การก่อการร้าย ปัจจุบันสิ่งที่ต้องเตรียมความพร้อมของประเทศไทยคือ การเติบโตอย่างรวมเร็วของการพัฒนาเทคโนโลยี การใช้สื่อสังคมออนไลน์เทคโนโลยีสารสนเทศเป็นเครื่องมือที่ช่วยให้มนุษย์ในศตวรรษที่ 21 มีอิสระที่จะเลือกกระทำการใดๆ โดยปัจเจกชนทั่วไป รวมถึงชุมชนและท้องถิ่นสามารถเข้าถึงข้อมูลและข่าวสารและมีส่วนร่วมในกิจกรรมต่างๆในโลกออนไลน์ในการดำเนินชีวิต ภาครัฐและภาคเอกชนได้นำรูปแบบของ E – Service เป็นกลไกหลักใน

การทำงานและเป็นศูนย์กลางในการพัฒนาในทุก ๆ ด้าน การที่ประชาชนสามารถเข้าถึงข้อมูลต่างๆ ได้ เป็นประโยชน์ต่อตนเอง และช่วยทำให้การทำงานของรัฐมีความโปร่งใส ตรวจสอบได้ ประชาชนมีโอกาสในการเข้าถึงข้อมูลข่าวสารผ่านระบบอิเล็กทรอนิกส์ แต่ในทางตรงกันข้าม การมีใช้เทคโนโลยีที่มากเกินไปส่งผลต่อการควบคุมการใช้งานระบบออนไลน์ของรัฐ ประชาชนในการสื่อสารออนไลน์ติดต่อสื่อสารถึงกันและใช้เป็นเครื่องมือในการกระทำในทางที่ผิดมากขึ้น เช่น การละเมิดความเป็นส่วนบุคคลของผู้อื่น การนำมาเป็นเครื่องมือเพื่อการก่อการร้ายได้ ก่อให้เกิดผลกระทบต่อความสงบเรียบร้อยและศีลธรรมของสังคมไทย

ด้านการเมือง

สภาพทางการเมืองของประเทศไทย มีการปฏิรูปในเชิงโครงสร้าง และความเชื่อมั่นของประชาชนต่อระบบการเมือง พรรคการเมืองที่มีบทบาทหลักมีจำนวนน้อยลงประชาชนยังขาดความเชื่อมั่นต่อระบบการเมือง การเมืองไร้เสถียรภาพ ส่งผลให้การเมืองมีรูปแบบของการแข่งขันเชิงนโยบาย การมีส่วนร่วมของประชาชนหรือการเมืองภาคประชาชนมีบทบาทสูงขึ้น เห็นได้จากสถานการณ์ทางการเมืองที่ผ่านมา ระบบการเมืองขาดการถ่วงดุล การขาดความสามัคคี ประชาชนแตกแยก จนทำให้สถานภาพทางการเมืองของไทยขาดเสถียรภาพอย่างสิ้นเชิง อีกทั้งความเป็นโลกาภิวัตน์ทำให้การกำหนด กติกา วิถีและระบอบประชาธิปไตยในเวทีการเมืองโลก ส่งผลต่อความเปราะบางทางการเมืองของประเทศไทย ปัจจุบันจะเห็นได้ว่าประชาชนมีความสนใจทางการเมืองมากขึ้น จากการเข้าถึงโลกของอินเทอร์เน็ตและการสื่อสารได้อย่างรวดเร็ว สามารถนำเทคโนโลยีมาใช้เพื่อการติดตามความเคลื่อนไหว แสดงความคิดเห็นและเป็นส่วนหนึ่งของระบบทางการเมืองได้หลายๆ ทาง แต่ในทางตรงกันข้ามกัน อินเทอร์เน็ตส่งผลในทางลบได้เช่นเดียวกัน เมื่อประชาชนใช้อินเทอร์เน็ตในการหลอกลวง หรือข่มขู่ หรือเป็นเครื่องมือในการนำมาสู่การปลุกระดมมวลชน สร้างข้อมูลเท็จ เพื่อการก่อการร้ายได้

จากสภาพแวดล้อมทั้ง 3 ด้านคือด้านเศรษฐกิจ ด้านสังคม และด้านการเมืองของประเทศไทย โดยภาพรวม พบว่าทุกสภาพแวดล้อมทุกด้านเอื้อต่อการกระทำในการก่อการร้ายได้

2.การกำหนดยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ของประเทศไทย จากการวิเคราะห์ จุดแข็ง จุดอ่อน โอกาสและอุปสรรค และวิเคราะห์แนวทาง/มาตรการของการต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย เพื่อให้ได้ยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ของประเทศไทย

การนำเสนอยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์โดยเทคนิคเดลฟาย การสัมภาษณ์ผู้เชี่ยวชาญ จำนวน 10 ท่าน ผู้วิจัยได้หาแนวทางเพื่อประโยชน์จากจุดแข็ง หาแนวทางลดจุดอ่อน หาแนวทางเพื่อค้นหาโอกาส และแนวทางเพื่อเอาชนะภัยคุกคาม จากนั้นจึงจับคู่จุดแข็ง

หลัก – โอกาสหลัก (SO) การจับคู่จุดแข็งหลัก – ภาวะคุกคามหลัก (ST) การจับคู่จุดอ่อนหลัก – โอกาสหลัก (WO) และการจับคู่จุดอ่อนหลัก - ภาวะคุกคามหลัก (WT) เพื่อจัดทำยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย ซึ่งจากการวิเคราะห์ความสัมพันธ์ระหว่างจุดแข็งกับโอกาส จุดแข็งกับภาวะคุกคาม จุดอ่อนกับโอกาส และจุดอ่อนกับภาวะคุกคาม ผลของการวิเคราะห์ความสัมพันธ์ในข้อมูลแต่ละคู่ดังกล่าว ทำให้เกิดยุทธศาสตร์สามารถแบ่งออกได้เป็น 4 ประเภทดังนี้

1. ยุทธศาสตร์เชิงรุก (SO Strategy)
2. ยุทธศาสตร์เชิงป้องกัน (ST Strategy)
3. ยุทธศาสตร์เชิงแก้ไข (WO Strategy)
4. ยุทธศาสตร์เชิงรับ (WT Strategy)

หลังจากนั้นผู้วิจัยได้นำเสนอยุทธศาสตร์ในการต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทยต่อผู้เชี่ยวชาญเพื่อทำการปรับแก้ไขตามคำแนะนำ เพื่อให้ได้ยุทธศาสตร์ในการต่อต้านการก่อการร้ายทางไซเบอร์ ซึ่งนำเสนอผลการศึกษาดังนี้

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

จุดแข็งหลัก – โอกาสหลัก (SO)

Integration ยุทธศาสตร์การใช้การบูรณาการร่วมกันเพื่อแบ่งปันข้อมูล (SO)

แนวทางหรือมาตรการ

1. จัดตั้งหน่วยงานกลาง มีหน้าที่ในการดูแล ดำเนินการทางด้านไซเบอร์ มีการแบ่งปันข้อมูลร่วมกันเพื่อประโยชน์ของประชาชน รวมทั้งมีการบูรณาการการทำงานร่วมกัน อีกทั้งระบุโอกาส และความท้าทายในการเพิ่มขีดความสมารถของกลไกการตอบสนองต่อการร้าย

2. สร้างฐานข้อมูลกลางเพื่อรวบรวมข้อมูลสำคัญจากทุกภาคส่วน รวมทั้งมีการควบคุมดูแลเพื่อไม่ให้ข้อมูลถูกเผยแพร่ เปิดโอกาสให้ทุกหน่วยงานที่เกี่ยวข้องกับไซเบอร์สามารถดึงข้อมูลไปใช้ในทางที่ถูกต้อง

3. จัดตั้งศูนย์ข่าวกรองทางไซเบอร์ เพื่อทำงานด้านการข่าวทางไซเบอร์ แบ่งปันข้อมูลข่าวสาร และประสานงานความร่วมมือระหว่างหน่วยงาน

Coordinate ยุทธศาสตร์การส่งเสริมความร่วมมือระหว่างภาครัฐภาคเอกชนและภาคประชาชน(SO)

แนวทางหรือมาตรการ

1. มีการเสริมสร้างความเข้าใจร่วมกันในการกำหนด นิยาม ความหมายของไซเบอร์ การก่อการร้ายและการก่อการร้ายทางไซเบอร์

2. มีการกำหนดนโยบาย แนวทางและแผนปฏิบัติการที่ชัดเจนเพื่อให้เกิดการแปลงแผนไปสู่กลยุทธ์และไปสู่การปฏิบัติตามวิสัยทัศน์ พันธกิจและเป้าประสงค์ที่กำหนดไว้อย่างมีประสิทธิภาพ

3. กำหนดกลไกในการทบทวน ติดตาม และประเมินความเสี่ยงต่อการนำแผนไปปรับใช้เพื่อปรับแนวทางให้มีความเหมาะสมตามสถานการณ์ใหม่หรือสถานการณ์ที่แตกต่าง

จุดแข็งหลัก – ภาวะคุกคามหลัก (ST)

Perception prepares and protect ยุทธศาสตร์การรับรู้ทางไซเบอร์ร่วมกัน ตระเตรียม และปกป้องทางไซเบอร์ (ST)

แนวทางหรือมาตรการ

1. ปลูกฝังทัศนคติและแนวทางการใช้ไซเบอร์ที่เป็นรูปธรรมเพื่อให้ประชาชนมีการรับรู้ต่อการใช้ไซเบอร์ในทางที่ถูกต้อง

2. สร้างการมีส่วนร่วมของประชาชน รวมทั้งวิธีการในการตระเตรียมตนเองเพื่อให้เกิดการปฏิบัติอย่างรู้เท่าทัน

3. สร้างมุมมองต่อการสอดส่องดูแลและป้องกันที่ดีในการดำรงชีวิตประจำวัน ให้มีภูมิคุ้มกันตนเองต่อการใช้ไซเบอร์

Research ยุทธศาสตร์การเสริมสร้างงานวิจัยเพื่อการพัฒนาทางไซเบอร์ (ST)

แนวทางหรือมาตรการ

1. มีการส่งเสริมให้ประชาชน นักวิชาการ หรือภาคเอกชนมีความสนใจในประเด็นทางไซเบอร์และการก่อการร้ายทางไซเบอร์มากขึ้น ให้ครอบคลุมทุกด้าน

2. สนับสนุนด้านงบประมาณด้านการวิจัยทางไซเบอร์เพื่อสร้างแรงจูงใจให้กับนักวิจัยทางไซเบอร์อย่างมีประสิทธิภาพ

จุดอ่อนหลัก – โอกาสหลัก (WO)

Development ยุทธศาสตร์การพัฒนาความก้าวหน้าทางไซเบอร์ (WO)

แนวทางหรือมาตรการ

1. มีการจัดตั้งหน่วยงานการพัฒนาทางไซเบอร์เพื่อพัฒนาระบบสารสนเทศและการรักษาความปลอดภัยทางไซเบอร์ข้อมูลข่าวสาร

2. จัดฝึกอบรมให้ความรู้ สนับสนุนการจัดสอบเพื่อให้บุคลากรผ่านเกณฑ์มาตรฐานสากล สนับสนุนการวิจัยสร้างองค์ความรู้ใหม่ทางไซเบอร์

3. พัฒนาบุคลากรให้มีความเชี่ยวชาญในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ รวมทั้งสร้างแรงจูงใจในการจงรักภักดีและทำงานเพื่อประเทศชาติเพื่อป้องกันสมองไหลไปยังต่างประเทศ

Awareness ยุทธศาสตร์การสร้างการตระหนักรู้ทางไซเบอร์ให้กับประชาชน (WO)

แนวทางหรือมาตรการ

1. สนับสนุนให้ประชาชนมีการสร้างความรู้ ความเข้าใจที่ดีต่อการใช้ไซเบอร์ รวมทั้งมีการถ่ายทอดความรู้ ความเข้าใจที่ดีต่อการใช้ไซเบอร์ รวมทั้งมีการถ่ายทอดความรู้ความเข้าใจจากรุ่นไปสู่รุ่น

2. เผยแพร่ความรู้และประชาสัมพันธ์ให้ประชาชนมีการใช้ไซเบอร์รวมทั้งตระหนักถึงการใช้ไซเบอร์อย่างถูกต้องเพื่อป้องกันการนำมาเป็นเครื่องมือในการก่อการร้าย

จุดอ่อนหลัก - ภาวะคุกคามหลัก (WT)

L – Law ยุทธศาสตร์การกำหนดใช้กฎหมายทางไซเบอร์และการบังคับใช้กับประชาชน (WT)

แนวทางหรือมาตรการ

1.กำหนดกฎหมาย กฎระเบียบ ขั้นตอน ที่เกี่ยวข้องกับการใช้ไซเบอร์ ความมั่นคงทางไซเบอร์และการต่อต้านการก่อการร้ายทางไซเบอร์อย่างครอบคลุม

2.กำหนดแนวทางที่ชัดเจนต่อการบังคับใช้กฎหมาย พร้อมทั้ง มาตรการ บทลงโทษต่อการกระทำอันเกี่ยวข้องกับก่อการร้าย

Education ยุทธศาสตร์การจัดการศึกษาในการสร้างพื้นฐานของประชาชนในประเทศไทย (WT)

แนวทางหรือมาตรการ

1.กำหนดหลักสูตรที่เกี่ยวกับไซเบอร์ในทุกระดับเพื่อให้เยาวชนได้มีรากฐานของการศึกษาและเข้าใจต่อการใช้ไซเบอร์อย่างถูกต้อง

2.พัฒนาหลักสูตรในระดับอุดมศึกษาเพื่อพัฒนาองค์ความรู้ทางไซเบอร์ให้สามารถนำความรู้ไปใช้อย่างครอบคลุมและมีประสิทธิภาพในทุก ๆ ด้าน

ตารางที่ 20 ยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย

ยุทธศาสตร์การต่อต้านการก่อการร้ายในประเทศไทย	แนวทางหรือมาตรการ	SWOT
I – Integration ยุทธศาสตร์การใช้การบูรณาการร่วมกันเพื่อแบ่งปันข้อมูล(SO)	1.จัดตั้งหน่วยงานกลาง มีหน้าที่ในการดูแล ดำเนินการทางด้านไซเบอร์ มีการแบ่งปันข้อมูลร่วมกันเพื่อประโยชน์ของประชาชน รวมทั้งมีการบูรณาการการทำงานร่วมกัน อีกทั้งระบุโอกาส และความท้าทายในการเพิ่มขีดความสามารถของกลไกการตอบสนองต่อการร้าย 2.สร้างฐานข้อมูลกลางเพื่อรวบรวมข้อมูลสำคัญจากทุกภาคส่วน รวมทั้งมีการควบคุมดูแลเพื่อไม่ให้ข้อมูลถูกเผยแพร่ เปิดโอกาสให้ทุกหน่วยงานที่เกี่ยวข้องกับไซเบอร์สามารถดึงข้อมูลไปใช้ในทางที่ถูกต้อง 3. จัดตั้งศูนย์ข่าวกรองทางไซเบอร์ เพื่อทำงานด้านการข่าวทางไซเบอร์ แบ่งปันข้อมูลข่าวสาร และประสานงานความร่วมมือระหว่างหน่วยงาน	O1 O3 O5 S1 S4
C – Coordinate ยุทธศาสตร์การส่งเสริมความร่วมมือระหว่างภาครัฐ ภาคเอกชน และภาคประชาชน	1.มีการเสริมสร้างความเข้าใจร่วมกันในการกำหนด นิยาม ความหมายของไซเบอร์ การก่อการร้ายและการก่อการร้ายทางไซเบอร์	

ยุทธศาสตร์การต่อต้านการก่อการร้ายในประเทศไทย	แนวทางหรือมาตรการ	SWOT
(SO)	2.มีการกำหนดนโยบาย แนวทางและแผนปฏิบัติการที่ชัดเจนเพื่อให้เกิดการแปลงแผนไปสู่กลยุทธ์และไปสู่การปฏิบัติตามวิสัยทัศน์ พันธกิจและเป้าประสงค์ที่กำหนดไว้อย่างมีประสิทธิภาพ 3.กำหนดกลไกในการทบทวน ติดตามและประเมินความเสี่ยงต่อการนำแผนไปปรับใช้เพื่อปรับแนวทางให้มีความเหมาะสมตามสถานการณ์ใหม่หรือสถานการณ์ที่แตกต่าง	
P – Perception Prepares and Protect ยุทธศาสตร์การรับรู้ทางไซเบอร์ร่วมกัน ตระเตรียม และปกป้องทางไซเบอร์ (ST)	1.ปลูกฝังทัศนคติและแนวทางการใช้ไซเบอร์ที่เป็นรูปธรรมเพื่อให้ประชาชนมีการรับรู้ต่อการใช้ไซเบอร์ในทางที่ถูกต้อง 2.สร้างการมีส่วนร่วมของประชาชนรวมทั้งวิธีการในการตระเตรียมตนเองเพื่อให้เกิดการปฏิบัติอย่างรู้เท่าทัน 3.สร้างมุมมองต่อการสอดส่องดูแลและป้องกันที่ดีในการดำรงชีวิตประจำวัน ให้มีภูมิคุ้มกันตนเองต่อการใช้ไซเบอร์	S2 S3 S4 T4 T5 T6
R : Research ยุทธศาสตร์การเสริมสร้างงานวิจัยเพื่อการพัฒนาทางไซเบอร์ (ST)	1.มีการส่งเสริมให้ประชาชน นักวิชาการหรือภาคเอกชนมีความสนใจในประเด็นทางไซเบอร์และการก่อการร้ายทางไซเบอร์มากขึ้น ให้ครอบคลุมทุกด้าน 2.สนับสนุนด้านงบประมาณด้านการวิจัยทางไซเบอร์เพื่อสร้างแรงจูงใจให้กับ	

ยุทธศาสตร์การต่อต้านการก่อการร้ายในประเทศไทย	แนวทางหรือมาตรการ	SWOT
	นักวิจัยทางไซเบอร์อย่างมีประสิทธิภาพ	
D : Development ยุทธศาสตร์การพัฒนาความก้าวหน้าทางไซเบอร์ (WO)	1.มีการจัดตั้งหน่วยงานการพัฒนาทางไซเบอร์เพื่อพัฒนาระบบสารสนเทศและการรักษาความปลอดภัยทางไซเบอร์ข้อมูลข่าวสาร 2.จัดฝึกอบรมให้ความรู้ สนับสนุนการจัดสอบเพื่อให้บุคลากรผ่านเกณฑ์มาตรฐานสากล สนับสนุนการวิจัยสร้างองค์ความรู้ใหม่ทางไซเบอร์ 3.พัฒนาบุคลากรให้มีความเชี่ยวชาญในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ รวมทั้งสร้างแรงจูงใจในการจงรักภักดีและทำงานเพื่อประเทศชาติเพื่อป้องกันสมองไหลไปยังต่างประเทศ	O2 O3 O4 O5 O7 W1 W3 W4 W7
A : Awareness ยุทธศาสตร์การสร้างการตระหนักรู้ทางไซเบอร์ให้กับประชาชน(WO)	1.สนับสนุนให้ประชาชนมีการสร้างความรู้ ความเข้าใจที่ดีต่อการใช้ไซเบอร์ รวมทั้งมีการถ่ายทอดความรู้ ความเข้าใจที่ดีต่อการใช้ไซเบอร์ รวมทั้งมีการถ่ายทอดความรู้ความเข้าใจจากรุ่นไปสู่รุ่น 2.เผยแพร่ความรู้และประชาสัมพันธ์ให้ประชาชนมีการใช้ไซเบอร์รวมทั้งตระหนักถึงการใช้ไซเบอร์อย่างถูกต้องเพื่อป้องกันการนำมาเป็นเครื่องมือในการก่อการร้าย	
L – Law	1.กำหนดกฎหมาย กฎระเบียบ ขั้นตอน ที่เกี่ยวข้องกับการใช้ไซเบอร์ ความมั่นคง	W1 W3 W9 W11

ยุทธศาสตร์การต่อต้านการก่อการร้ายในประเทศไทย	แนวทางหรือมาตรการ	SWOT
ยุทธศาสตร์การกำหนดใช้กฎหมายทางไซเบอร์และการบังคับใช้กับประชาชน(WT)	ทางไซเบอร์และการต่อต้านการก่อการร้ายทางไซเบอร์อย่างครอบคลุม 2.กำหนดแนวทางที่ชัดเจนต่อการบังคับใช้กฎหมาย พร้อมทั้ง มาตรการบทลงโทษต่อการกระทำอันเกี่ยวข้องกับก่อการร้าย	W12 T4 T6
E : Education ยุทธศาสตร์การจัดการศึกษาในการสร้างพื้นฐานของประชาชนในประเทศไทย(WT)	1.กำหนดหลักสูตรที่เกี่ยวกับไซเบอร์ในทุกระดับเพื่อให้เยาวชนได้มีรากฐานของการศึกษาและเข้าใจต่อการใช้ไซเบอร์อย่างถูกต้อง 2.พัฒนาหลักสูตรในระดับอุดมศึกษาเพื่อพัฒนาองค์ความรู้ทางไซเบอร์ให้สามารถนำความรู้ไปใช้อย่างครอบคลุมและมีประสิทธิภาพในทุก ๆ ด้าน	

การวิเคราะห์ภาพอนาคตโดยวิธีการวิเคราะห์สถานการณ์และองค์กรแห่งการเรียนรู้

1. การวิเคราะห์สถานการณ์การก่อการร้ายและการก่อการร้ายทางไซเบอร์ (Scenario analysis)สามารถวิเคราะห์เป็น 3 ประเด็นดังนี้

1. กระแสโลก

สถานการณ์ของการก่อการร้ายเริ่มมีความรุนแรงเพิ่มมากขึ้นเป็นทวีคูณ จากกลุ่มก่อการร้ายที่มีความพยายามในการแสดงบทบาทให้เป็นที่ประจักษ์ต่อประชาคมโลก เช่น กลุ่มเคร่งศาสนาสุดโต่ง หรือกลุ่มมุสลิมหัวรุนแรงต่าง ๆ ในศตวรรษที่ 21 นี้มีสถานการณ์รุนแรงที่เกิดขึ้นบทโลก ที่สร้างความสะพรึงกลัว สืบเนื่องมาจากการก่อการร้ายเมื่อ 11 กันยายน 2001 ที่ผ่านมา ประธานาธิบดี บารัคโอบามา ผู้นำสหรัฐอเมริกาเตรียมแผนยุทธศาสตร์ต่อต้านการติดอาวุธไอเอส ในวันที่ 10 กันยายน หลังจากสหรัฐอเมริกาขยายการปฏิบัติการโจมตีทางอากาศในอิรักที่เริ่มตั้งแต่ 8 สิงหาคม โดยเริ่มด้วยการโจมตีกลุ่มไอเอสอย่างหนักและรุนแรงมากขึ้นเชื่อมโยงกับการเกิด

สถานการณ์การก่อการร้ายที่ฝรั่งเศสเมื่อวันที่ 13 พฤศจิกายน 2558 ที่ผ่านมา เมื่อประธานาธิบดี นาย ฟรองซัวร์ โอลลองด์ ประธานาธิบดีฝรั่งเศส ประกาศเมื่อวันที่ 18 กันยายน 2557 ว่า รัฐบาลฝรั่งเศส จะส่งเครื่องบินไปให้ความช่วยเหลือรัฐบาลอิรัก ในการปราบปรามกลุ่มรัฐอิสลาม (ไอเอส) พร้อม ทั้งกำชับว่า กองทัพฝรั่งเศสจะไม่โจมตีภาคพื้นดิน หลังจากผู้นำฝรั่งเศสออกมาประกาศเพียง 1 วัน เครื่องบินรบของกองทัพฝรั่งเศสได้เริ่มเปิดฉากโจมตีทางอากาศต่อฐานที่มั่นของกลุ่มไอเอส เมื่อ ประเทศฝรั่งเศสประกาศอย่างชัดเจนต่อการต่อต้านการก่อการร้ายนำมาสู่การถูกโจมตี เมื่อวันที่ 13 พฤศจิกายนที่ผ่านมาถือว่าเป็นการก่อการร้ายที่ร้ายแรงที่สุดที่เคยเกิดขึ้นในประเทศฝรั่งเศส จนทำ ให้มีผู้เสียชีวิตและบาดเจ็บเป็นจำนวนมาก อันเป็นสาเหตุจากการที่รัฐบาลฝรั่งเศสตัดสินใจเข้าร่วม การโจมตีกลุ่มไอเอสในซีเรีย จะเห็นได้ว่าการก่อการ้ายในครั้งนี้ แตกต่างจากการก่อการร้ายในอดีต เป็นการกระทำที่มุ่งเป้าต่อเป้าหมายที่เป็นประชาชนทั่วไป การโจมตีมุ่งไปยังเป้าหมายที่เป็น เป้าหมายอ่อน (Soft target) เช่น โรงละคร สนามกีฬาหรือแหล่งบันเทิงต่างๆ เมื่อกระทำการแล้วจะ มีเป้าหมายในวงกว้าง มีการแพร่กระจายข่าวไปทั่วโลก สร้างความหวาดกลัวและสร้างความตก ตะลึงไปยังประชาชนทั่วโลกอีกด้วย การกระทำของกลุ่มก่อการร้ายไอเอสในครั้งนี้ คงปฏิเสธไม่ได้ ว่า เหตุเพราะการร่วมปฏิบัติการทางทหารของกองทัพฝรั่งเศสในการโจมตีอิรักและซีเรีย ทำให้ ฝรั่งเศสกลายเป็นเป้าหมายสำคัญของกลุ่มก่อการร้าย และประเด็นที่สำคัญคือ การดำเนินการของ กองทัพพันธมิตร ที่มีสหรัฐอเมริกาเป็นผู้นำในการเปิดฉากโจมตีกลุ่มไอเอสในอิรักและซีเรีย จนทำ ให้กลุ่มไอเอส ประกาศว่าจะปลุกระดมสมาชิกให้สังหารชาวอเมริกันและยุโรป โดยเฉพาะชาว ฝรั่งเศสให้ได้ ความท้าทายของการก่อการร้ายในอนาคตจะเป็นการพัฒนาเครือข่ายโดยใช้ไซเบอร์ มาเป็นส่วนในการเชื่อมโยงของกลุ่มผู้ก่อการร้ายในการสื่อสาร ติดต่อระหว่างกัน มีการระดม สมาชิกจากหลายประเทศทั่วโลก เพื่อเดินทางเข้ามาเป็นสมาชิกหรือใช้การสั่งการโดยมีเทคโนโลยี รวมทั้งพัฒนาอาวุธที่มีอานุภาพร้ายแรงมากยิ่งขึ้น เพื่อปฏิบัติการในการก่อการร้าย ภัยคุกคามทาง ไซเบอร์ จะเกิดขึ้นเมื่อผู้ก่อการร้ายใช้ประโยชน์จากอาวุธไซเบอร์ในการก่อวินาศกรรม โดยอาจมี การมุ่งเป้าไปที่การทำลายที่มีผลกระทบในวงกว้าง เช่น การทำลายระบบโครงข่ายกระแสไฟฟ้า การ โจมตีระบบโครงข่ายสื่อสาร หรือแม้กระทั่งการโจมตีระบบต่างๆ ที่ใช้ในด้านการทหาร ซึ่งก็อาจ เกิดขึ้นได้ในปัจจุบันนี้ หลายประเทศได้ให้ความสำคัญต่อการจัดตั้งกองทัพไซเบอร์ เพื่อพัฒนา ศักยภาพของทหารต่อการทำสงครามไซเบอร์ และปฏิบัติการควบคู่ไปกับการทำสงครามแบบปกติ เพื่อพัฒนาให้มีความแข็งแกร่งมากยิ่งขึ้น

2. กระแสโลกาภิวัตน์

ในกระแสของการเปลี่ยนแปลงในยุคโลกาภิวิตน์เกิดความเชื่อมโยงอย่างสลับซับซ้อน และต่อเนื่องกันในหลายมิติทั้งด้านเศรษฐกิจ สังคม การเมือง สิ่งแวดล้อม วิทยาศาสตร์และ

เทคโนโลยี แต่สิ่งหนึ่งที่ประชาคมโลกไม่อาจปฏิเสธได้คือภัยคุกคามความมั่นคงจากผู้ก่อการร้าย สถานการณ์ก่อการร้ายไม่ได้จำกัดอยู่เฉพาะภูมิภาคใดภูมิภาคหนึ่งเท่านั้น แต่เป็นการกระจายไปยังทุกพื้นที่ทั่วโลก ภัยคุกคามความมั่นคงที่แปรเปลี่ยนรูปแบบจากภัยคุกคามแบบดั้งเดิม (Traditional threats) เป็นลักษณะของ ภัยคุกคามไม่ตามแบบ (Non – traditional threats) ซึ่งทุกประเทศทั่วโลกต้องเผชิญอย่างหลีกเลี่ยงไม่ได้ การใช้สังคมออนไลน์ (Social network)จะถูกนำมาใช้ในทางการเมืองเพิ่มมากขึ้น ทั้งการโฆษณา ประชาสัมพันธ์มากขึ้น การใช้ในการกระทำความผิด การล้วงข้อมูลลับ การก่ออาชญากรรม การสร้างอาวุธไซเบอร์ ซึ่งเป็นซอฟแวร์ที่ใช้ในการโจมตีระบบของฝ่ายตรงข้าม ซึ่งโดยส่วนใหญ่เป็นเครื่องมือหรือซอฟแวร์ที่แฮกเกอร์สร้างหรือพัฒนาขึ้นมาเพื่อเจาะระบบต่าง ๆ ซึ่งเครื่องมือนี้สามารถนำมาใช้ในการปฏิบัติการโจมตีทางทหารได้เฉกเช่นเดียวกัน

3.กระแสในประเทศ

กลุ่มก่อการร้ายมีแนวโน้มขยายเครือข่ายเข้ามาในภูมิภาคเอเชียตะวันออกเฉียงใต้มากขึ้น เพื่อใช้เป็นแหล่งพักพิง ซ่องสุมและหรือเป็นแหล่งกบดาน เป็นเส้นทางการลำเลียงอาวุธ แม้ว่าประเทศไทยยังมิใช่ประเทศที่เป็นเป้าหมายโดยตรงของการก่อการร้ายและไม่ได้เป็นคู่กรณีของกลุ่มก่อการร้ายโดยเฉพาะก็ตาม แต่ด้วยประเทศไทยมีการเปิดเป็นประเทศเสรีประชาธิปไตย ที่เป็นศูนย์กลางของภูมิภาคตะวันออกเฉียงใต้ โดยเฉพาะมีนโยบายส่งเสริมการท่องเที่ยวและมีเส้นทางการบินที่เชื่อมโยงกันทั่วโลก ทำให้สามารถเดินทางเข้าออกได้ง่าย
ประเทศไทยมีสถานการณ์การก่อการร้ายที่เกิดขึ้น มีการจัดอันดับของประเทศที่มีความน่าเป็นห่วงต่อสถานการณ์การก่อการร้าย โดยสถาบันเศรษฐศาสตร์และสันติภาพ (Institute for Economics and Peace : IEP) ร่วมกับกลุ่มวิชาการระหว่างประเทศ เผยรายงานดัชนีก่อการร้ายโลก หรือ2015 Global Terrorism Index ซึ่งประเมินความเสียหายที่เกี่ยวข้องกับการก่อการร้ายในปี 2557 จากการสำรวจพบว่าใน 162 ประเทศทั่วโลก ประเทศไทยถูกจัดอยู่ในอันดับที่ 10 รองจาก อิรัก อัฟกานิสถาน ไนจีเรีย ปากีสถาน ซีเรีย อินเดีย เยเมน โซมาเลียและลิเบีย ในปีที่ผ่านมามีผู้เสียชีวิตจากเหตุการณ์ที่เกี่ยวข้องกับการก่อการร้ายในประเทศไทย จำนวน 156 ราย เพิ่มขึ้นจากปีก่อนหน้าร้อยละ 16 แต่ก็ยังคงน้อยกว่าตัวเลขสูงสุด 255 ราย เมื่อปี 2552 โดยความสูญเสียมาจากเหตุความไม่สงบในจังหวัดชายแดนภาคใต้ ขณะที่การก่อเหตุในกรุงเทพมหานครในปี 2557 อยู่ที่ 58 ครั้ง เพิ่มขึ้น 5 เท่าจากปีก่อนหน้า

ความท้าทายของการต่อต้านการก่อการร้ายในภูมิภาคเอเชียตะวันออกเฉียงใต้ นอกจากจะเป็นการก่อการร้ายที่เป็นภัยคุกคามเพียงแค่ในภูมิภาคเท่านั้น แต่เป็นความท้ายทายในทุก ๆที่มีการก่อการร้าย โดยมีความท้าทายในเรื่องของการก่อการร้ายทางไซเบอร์ทั้งเป็นส่วนของสังคม

ออนไลน์ที่สามารถก่อให้เกิดการกระทำที่มีความรุนแรงและสามารถกระทำพฤติกรรมที่มีความรุนแรงได้ด้วยตนเองและนำเอาเทคโนโลยีที่มีความรุนแรงและทันสมัยมาใช้มากขึ้น

4.ทิศทางของประเทศไทย

ประเทศไทยมีการดำเนินการโดยรัฐบาลมีการความเห็นชอบในการจัดตั้ง แผนการต่อต้านการต่อก่อการร้ายสากลเพื่อให้มีหน่วยงานที่พร้อมในการปฏิบัติการในภาวะฉุกเฉิน และสามารถควบคุมสถานการณ์ไม่ให้เลวร้ายลงไปกว่าเดิมและสร้างความมั่นใจให้กับประชาชน รัฐบาลมีมติเห็นชอบในการลงนามการให้สัตยาบันในอนุสัญญา BIMSTEC ว่าด้วยความร่วมมือในการต่อต้านการก่อการร้ายสากล องค์การอาชญากรรมข้ามชาติ และการลักลอบค้ายาเสพติดของสำนักงานสภาคามมั่นคงแห่งชาติ (สมช.) เมื่อปลายเดือนธันวาคม 2557 ในส่วนของการป้องกันการก่อการร้ายทางไซเบอร์ กองทัพไทยมีการจัดตั้งหน่วยงานที่ดูแลทางด้านไซเบอร์ดังนี้

กองทัพบก (ทบ.) มีศูนย์ไซเบอร์ กรมทหารสื่อสาร ศูนย์เทคโนโลยีทางทหาร(ศศท.)

กองทัพเรือ (ทร.)มีกรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ

กองทัพอากาศ (ทอ.)มีกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ

สำนักงานตำรวจแห่งชาติ มีสำนักงานเทคโนโลยีสารสนเทศและการสื่อสาร (สทส.)

กระทรวงกลาโหมจัดตั้ง กองสงครามไซเบอร์

ความท้าทายในเรื่องของก่อการร้ายทางไซเบอร์ทั้งสังคมออนไลน์ และเครือข่ายสังคม (Social Network) มีการนำเทคโนโลยีที่ทันสมัยและการกระทำที่มีความซับซ้อนมากขึ้น

2. ประเมินผลจากการวิเคราะห์สภาพแวดล้อมของประเทศไทย

ตารางที่ 21 การวิเคราะห์สภาพแวดล้อมของประเทศไทย

จุดแข็ง (Strength)	จุดอ่อน(Weaknesses)
1.ประเทศไทยเป็นมิตรกับประเทศทั้งในภูมิภาคอาเซียนและประเทศอื่นในโลก ทำให้เราไม่เป็นเป้าหมายของการก่อการร้าย 2. ประเทศไทยเรียนรู้การนำเอาความรู้ของหลายๆ ประเทศมาพัฒนาทางเทคโนโลยี 3.ประเทศไทยยังมีวิถีของการเป็นประเทศเกษตรกรรมกับอุตสาหกรรมรวมกัน	1.ประชาชนยังไม่มีความตระหนักต่อภัยคุกคามทางไซเบอร์ 2. ระบบคอมพิวเตอร์มีช่องโหว่ทำให้ง่ายต่อการถูกโจมตี 3.ประเทศไทยยังไม่มีกฎหมายที่สามารถบังคับและควบคุมการใช้ทางไซเบอร์ 4.ไม่มีหน่วยงานกลางในการประสานงาน

4.ประเทศไทยมีหน่วยงานที่จัดตั้งขึ้นเพื่อดูแลทางไซเบอร์ทั้งภาครัฐและเอกชน	ทางด้านไซเบอร์ 5.ประเทศไทยยังคงมีการเมืองที่ไม่มั่นคง และต้องอยู่ภายใต้กฎอัยการศึก 6.ประเทศไทยยังไม่มีโครงข่ายพื้นฐานที่สามารถเชื่อมต่อกันทั้งหมด และความเร็วของพื้นที่ไม่ทั่วทั้งประเทศ 7. ประเทศไทยยังขาดบุคลากรที่มีความเชี่ยวชาญทางไซเบอร์และเทคโนโลยี
โอกาส (Opportunities)	อุปสรรค (Threats)
1.ประเทศไทยมีการสร้างภูมิคุ้มกันไม่ให้เป็นฐานในการโจมตีทางไซเบอร์ 2.สังคมไทยมีสิ่งอำนวยความสะดวกและประชาชนพร้อมปรับตัวได้ตลอดเวลา 3.ประเทศไทยมีนโยบายในการส่งเสริมการพัฒนาด้านโครงสร้างพื้นฐาน 4.ประเทศไทยมีคนรุ่นใหม่มีความสนใจและมีความรู้ทางไซเบอร์ 5.ประเทศไทยมีนโยบายในส่งเสริมการพัฒนาทางเทคโนโลยีไซเบอร์และมีนโยบายของประเทศไทยสนับสนุนให้เข้าสู่โลกของอินเทอร์เน็ต 6.ประเทศไทยส่งเสริมให้คนไทยเข้าถึงข้อมูลได้ง่ายมากขึ้น 7.ประเทศไทยมีโอกาสในการพัฒนาเทคโนโลยีทางไซเบอร์อีกมากมาย เช่นการใช้ไซเบอร์เพื่อการเกษตรกรรม	1.แนวทางการทำงานของคนไทยคือ คนคิดไม่ได้ทำ คนทำไม่ได้คิด 2. ประเทศไทยให้ความสำคัญกับระบบเครือข่ายมากกว่าฐานความรู้ประเทศไทยยังคงมีวิธีการทำงานแบบเครือข่ายและระบบอุปถัมภ์ในการทำงาน 3.การสนับสนุนในด้านงบประมาณในการดำเนินการมีไม่เพียงพอ 4.โครงสร้างพื้นฐานของประเทศไทยยังเป็นระบบเก่ายังไม่พัฒนาสมบูรณ์แบบ 5.ประชาชนยังไม่มีความรู้ ความไม่เข้าใจเรื่องไซเบอร์อีกมาก 6.โครงสร้างพื้นฐานของประเทศที่รองรับการขยายตัวทางไซเบอร์ยังไม่มีความพร้อมต่อการพัฒนา

3.ประเมินสถานการณ์ในการวางจุดที่มั่น (Position) ของประเทศไทย

ตารางที่ 22 การวิเคราะห์สถานการณ์ (Scenario Analysis) จากคำถาม 7 ข้อดังนี้

คำถาม	คำตอบ
1.การก่อการร้ายในอนาคตเป็นอย่างไร	1.1 การก่อการร้ายจะมีความรุนแรงมากขึ้นจากกลุ่มหัวรุนแรง เคร่งศาสนาที่ขยายสมาชิกที่มาจากการระดมคนจากทั่วโลก ด้วยการชักจูงผู้ที่มีความคิด อุดมการณ์ในทิศทางเดียวกัน เพื่อสร้างฐานของกลุ่มก่อการร้าย 1.2 วิธีการในการก่อการร้ายจะมีวิธีการที่เกินความคาดหมาย เปลี่ยนจุดก่อเหตุเป็น Soft Target มากขึ้นและใช้ไซเบอร์มาดำเนินการด้วยเทคโนโลยีที่ทันสมัยและใช้ทุนน้อยกว่าอาวุธอื่น
2.ประเทศไทยมีการดำเนินการอย่างไรต่อการเกิดการก่อการร้ายในโลก	2.1 ประเทศไทยมีจุดยืนที่ชัดเจนต่อการแสดงออกในการต่อต้านการก่อการร้ายสากลและมีทิศทางในการสร้างพลังอำนาจแห่งชาติให้เข็มแข็งเพื่อป้องกันก่อการร้าย
3.ทิศทางของประเทศไทยต่อการต่อต้านการก่อการร้ายทางไซเบอร์ในอนาคต	3.1 ประเทศไทยควรพัฒนาศักยภาพความพร้อมในการปฏิบัติการต่อการต่อต้านการก่อการ้ายทางไซเบอร์และสงครามไซเบอร์ คือ บุคลากร เทคโนโลยี และการจัดองค์กร และสร้างความพร้อมให้ประชาชนมีการตระหนักรู้และป้องกันการก่อการร้ายทางไซเบอร์
4.ไซเบอร์จะเป็นเครื่องมือที่สำคัญต่อการนำมาเป็นเครื่องมือในการก่อการร้ายในอนาคต	4.1 เทคโนโลยีสารสนเทศและคอมพิวเตอร์จะมีการพัฒนาอย่างต่อเนื่อง มีการประยุกต์ใช้ในทุกภาคส่วน ไปจนถึงเทคโนโลยีอวกาศและในทางการทหาร ประเด็นสำคัญคือการพัฒนาอาวุธยุทโธปกรณ์ต่างๆ มาปฏิบัติการทางทหารในอนาคต
5.การก่อการร้ายทางไซเบอร์จะเป็นการกระทำที่มีอานุภาพร้ายแรง	5.1 อาวุธทางไซเบอร์ จะมีอานุภาพร้ายแรง ถ้ามีคนรู้จักใช้วิธี เป็นซอฟแวร์ที่ผู้ก่อการร้ายใช้ในการโจมตีระบบ

คำถาม	คำตอบ
	ของฝ่ายตรงกันข้าม ซึ่งเป็นเครื่องมือที่แฮกเกอร์พัฒนาขึ้นเพื่อใช้ในการเจาะระบบต่าง ๆ และสามารถนำมาใช้เพื่อปฏิบัติการทางทหารได้ และแฮกเกอร์ยังสามารถพัฒนา อาวุธไซเบอร์เพื่อนำมาปฏิบัติการเฉพาะอย่างได้
6. ถ้ามองไปในอนาคต อะไรคือสิ่งที่สำคัญที่ประเทศไทยต้องทำโดยเร็วที่สุดต่อการดำเนินการต่อต้านการก่อการร้ายทางไซเบอร์	6.1 ประเทศไทยยังไม่เป็นเป้าหมายต่อการก่อการร้ายทางไซเบอร์ แต่สิ่งสำคัญที่ต้องทำอย่างเร่งด่วนคือการสร้างองค์กรหรือหน่วยงานเฉพาะที่มีการดำเนินการทางด้านยุทธศาสตร์ นโยบาย แผนงานเพื่อกำหนดทิศทางของการป้องกันและต่อต้านการก่อการร้ายทางไซเบอร์ในอนาคต
7.ประเทศไทยควรมีหรือควรทำเป็นอันดับแรกของการต่อต้านการก่อการร้ายทางไซเบอร์	7.1ประเทศไทยควรสร้างความร่วมมือกันในทุกภาคส่วนเพื่อสร้างความเข็มแข็งให้กับการป้องกันและต่อต้านการก่อการร้ายทางไซเบอร์ในอนาคต 7.2 ประเทศไทยมีการพัฒนาประเทศให้มีความก้าวหน้าทางไซเบอร์ในหลายด้าน เช่นการพัฒนาการศึกษา พัฒนาการวิจัย การพัฒนาอาวุธและพัฒนาระบบป้องกัน รวมถึงการฟื้นฟูหลังจาการเกิดสถานการณ์การก่อการร้ายทางไซเบอร์

สรุปภาพรวมของการวิเคราะห์สถานการณ์(Scenario Analysis)

การวิเคราะห์สถานการณ์(Scenario Analysis) สามารถสรุปเป็นสถานการณ์ได้ 4 สถานการณ์ดังนี้

สถานการณ์ที่ 1 สถานการณ์การก่อการร้ายของโลกจะทวีความรุนแรงเพิ่มมากขึ้น กลุ่มประเทศยุโรปและประเทศมหาอำนาจที่มีแนวทางของการต่อต้านการก่อการร้ายจะเป็นเป้าหมายของการถูกโจมตีด้วยอาวุธที่มีอานุภาพร้ายแรง และนำมาซึ่งความสูญเสียอย่างมาก การเตรียมความพร้อมต่อการป้องกัน และการตอบโต้ด้วยพลังอำนาจแห่งชาติจะมากขึ้นตามไปด้วย ประเทศไทยจะ

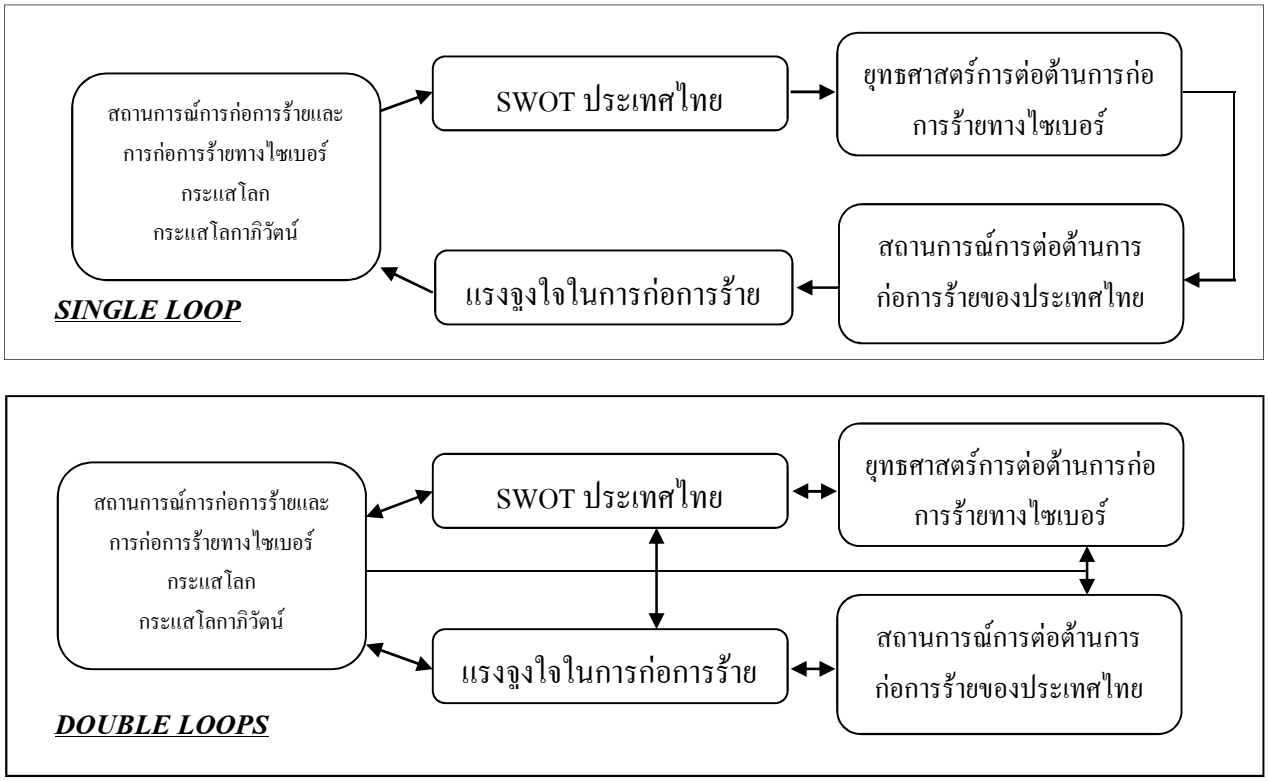
ไม่เป็นเป้าหมายของการก่อการร้ายด้วยความเป็นมิตรกับประเทศเพื่อนบ้าน และมีนโยบายในการเปิดประเทศเสรีประชาธิปไตยเพื่อการส่งเสริมการท่องเที่ยว

สถานการณ์ที่ 2 ประเทศไทยมีการจัดตั้งหน่วยงานทั้งภาครัฐ เอกชน เพื่อร่วมมือกันดำเนินการในการต่อต้านการก่อการร้ายและป้องกันประเทศต่อภัยคุกคามในการก่อการร้าย อนาคตข้างหน้าประเทศไทยจะมีหน่วยงานที่มีความเข้มแข็งต่อการต่อต้านการก่อการร้ายที่มีประสิทธิภาพ

สถานการณ์ที่ 3 ประเทศไทยให้ความสำคัญต่อการก่อการร้ายทางไซเบอร์มากขึ้น รวมทั้งให้ความสำคัญต่อการก่อการร้ายที่มีไซเบอร์เป็นเครื่องมือ ประชาชนมีความตื่นตัวในการป้องกันการก่อการร้ายทางไซเบอร์มากขึ้น

สถานการณ์ที่ 4 ประเทศไทยมีความก้าวหน้าทางไซเบอร์ มีการพัฒนาในหลายด้านเพื่อเป็นแนวทางในการป้องกันและต่อต้านการก่อการร้ายตามบริบทของประเทศไทย

4.สรุปภาพรวมของสถานการณ์การต่อต้านการก่อการร้ายของประเทศไทยและองค์กรแห่งการเรียนรู้LEARNING ORGANIZATION



ภาพที่ 10 ภาพรวมของสถานการณ์การต่อต้านการก่อการร้ายของประเทศไทยและองค์กรแห่งการเรียนรู้

การก่อการร้ายทางทางไซเบอร์ เป็นนำเอาเทคโนโลยีสารสนเทศและคอมพิวเตอร์มาเป็นเครื่องมือหรืออาวุธต่อการปฏิบัติการและทวีความรุนแรงเพิ่มมากขึ้นในอนาคต โลกกำลังเผชิญกับสถานการณ์การก่อการร้ายที่เกิดขึ้นจากกลุ่มผู้ก่อการร้ายที่มีแรงจูงใจต่อการดำเนินการก่อการร้ายและการปฏิบัติการต่างๆ จำเป็นต้องมีการนำเอาเทคโนโลยีสารสนเทศและการสื่อสารเข้ามาเป็นองค์ประกอบที่สำคัญ เช่นกองทัพต้องมีระบบบัญชาการและควบคุม ระบบเชื่อมโยงข้อมูล ระบบอาวุธยุทโธปกรณ์ระบบเรดาร์ ซึ่งการใช้ระบบเหล่านี้มีความเสี่ยงสูงต่อการถูกโจมตีผ่านทางไซเบอร์สเปซ จนนำไปสู่การเกิดสงครามรูปแบบใหม่ที่เรียกว่า สงครามไซเบอร์ ประเทศไทยแม้ว่าจะไม่ใช่เป้าหมายหลักแต่ควรมีการเตรียมความพร้อมต่อการเกิดการก่อการร้ายทางไซเบอร์ ด้วยความเสี่ยงเหล่านี้เกิดขึ้นได้เสมอประเทศไทยควรมีการทบทวนสภาพแวดล้อมของประเทศ วิเคราะห์แรงจูงใจของผู้ก่อการร้ายและปิดจุดอ่อนที่มีผลต่อช่องโหว่ และโอกาสที่เป็นสาเหตุของการก่อการร้ายทางไซเบอร์ได้ จนนำมาสู่สถานการณ์ในอนาคต สถานการณ์คือ

สถานการณ์ที่ 1 สถานการณ์การก่อการร้ายของโลกจะทวีความรุนแรงเพิ่มมากขึ้น กลุ่มประเทศยุโรปและประเทศมหาอำนาจที่มีแนวทางของการต่อต้านการก่อการร้ายจะเป็นเป้าหมายของการถูกโจมตีด้วยอาวุธที่มีอานุภาพร้ายแรง และนำมาซึ่งความสูญเสียอย่างมาก การเตรียมความพร้อมต่อการป้องกัน และการตอบโต้ด้วยพลังอำนาจแห่งชาติจะมากขึ้นตามไปด้วย ประเทศไทยจะไม่เป็นเป้าหมายของการก่อการร้ายด้วยความเป็นมิตรกับประเทศเพื่อนบ้าน และมีนโยบายในการเปิดประเทศเสรีประชาธิปไตยเพื่อการส่งเสริมการท่องเที่ยว สถานการณ์ที่ 2ประเทศไทยมีการจัดตั้งหน่วยงานทั้งภาครัฐ เอกชน เพื่อร่วมมือกันดำเนินการในการต่อต้านการก่อการร้ายและป้องกันประเทศต่อภัยคุกคามในการก่อการร้าย อนาคตข้างหน้าประเทศไทยจะมีหน่วยงานที่มีความเข้มแข็งต่อการต่อต้านการก่อการร้ายที่มีประสิทธิภาพสถานการณ์ที่ 3 ประเทศไทยให้ความสำคัญต่อการก่อการร้ายทางไซเบอร์มากขึ้น รวมทั้งให้ความสำคัญต่อการก่อการร้ายที่มีไซเบอร์เป็นเครื่องมือ ประชาชนมีความตื่นตัวในการป้องกันการก่อการร้ายทางไซเบอร์มากขึ้น และสถานการณ์ที่ 4ประเทศไทยมีความก้าวหน้าทางไซเบอร์ มีการพัฒนาในหลายด้านเพื่อเป็นแนวทางในการป้องกันและต่อต้านการก่อการร้ายตามบริบทของประเทศไทย โดยเรียงลำดับความสำคัญจากมากไปหาน้อย

การต่อต้านการก่อการร้ายทางไซเบอร์จำเป็นต้องมีการศึกษาและวิเคราะห์และสังเคราะห์สถานการณ์โดยการทบทวนสถานการณ์จากกระแสโลกกระแสโลกาภิวัตน์กระแสในประเทศและทิศทางของประเทศไทยอย่างต่อเนื่อง

ยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย

ความสอดคล้องและกระบวนการยกร่างจัดทำยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์

ยุทธศาสตร์ชาติ

1.ยุทธศาสตร์สร้างความมั่นคงให้กับประเทศ

2.ยุทธศาสตร์สร้างความสามารถในการแข่งขันของประเทศ

3.ยุทธศาสตร์สร้างโอกาสบนความเสมอภาคและเท่าเทียมกันทางสังคม

4.ยุทธศาสตร์การเติบโตบนคุณภาพชีวิตที่เป็นมิตรกับสิ่งแวดล้อม

5.ยุทศาสตร์การเพิ่มประสิทธิภาพของรัฐ

พลังอำนาจแห่งชาติ

ด้านการทูต (Diplomatic)

ด้านข่าวสาร/สารสนเทศ (Informational)

ด้านการทหาร (Military)

ด้านเศรษฐกิจ (Economic)

ด้านการเมือง (Politic)

ผลประโยชน์แห่งชาติ

1.การมีเอกราช อธิปไตยและบูรณภาพแห่งเขตอำนาจรัฐ

2.การดำรงอยู่อย่างมั่นคง ยั่งยืนของสถาบันหลักของชาติ

3.การดำรงอยู่อย่างมั่นคงของชาติและประชาชนจากภัยคุกคามทุกรูปแบบ

4.การอยู่ร่วมกันในชาติอย่างสันติสุข เป็นปึกแผ่น มั่นคงทางสังคม ท่ามกลางพหุสังคมและการมีเกียรติและศักดิ์ศรีของความเป็นมนุษย์

5.ความเจริญเติบโตของชาติ ความเป็นธรรม และความอยู่ดีมีสุขของประชาชน

6.ความยั่งยืนของฐานทรัพยากรธรรมชาติ สิ่งแวดล้อม ความมั่นคงทางพลังงาน อาหาร

7.การอยู่ร่วมกันอย่างสันติ ประสานสอดคล้องกันด้านความมั่นคง ในประชาคมอาเซียนและประชาคมโลกอย่างมีเกียรติและศักดิ์ศรี

วัตถุประสงค์ของชาติ

1. เพื่อส่งเสริมและรักษาไว้ซึ่งการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข

2. เพื่อเสริมสร้างจิตสำนึกของคนในชาติให้มีความจงรักภักดี และธำรงไว้ซึ่งสถาบันชาติ ศาสนา และพระมหากษัตริย์

3. เพื่อส่งเสริมและสนับสนุนการสร้างความปรองดอง ความเป็นธรรม และความสามัคคีของคนในชาติ

5.เพื่อพัฒนาศักยภาพของภาครัฐ และส่งเสริมบทบาทและความเข็มแข็งของทุกภาคส่วนในการรับมือกับภัยคุกคามทุกรูปแบบที่กระทบความมั่นคง

7.เพื่อพัฒนาศักยภาพการเตรียมความพร้อมของชาติในการเผชิญกับภาวะสงครามละวิกฤติการณ์ความมั่นคง อย่างมีเอกภาพและประสิทธิภาพ

8.เพื่อเสริมสร้างศักยภาพของกองทัพในการป้องกันประเทศ สนับสนุนภารกิจที่ไม่ใช่ช่วงสงคราม และสามารถผนึกกำลังของกองทัพทุกภาคส่วนในการเผชิญกับภัยคุกคามด้านการป้องกันประเทศทุกรูปแบบ

นโยบายความมั่นคงแห่งชาติ พ.ศ.2558 – 2564

นโยบายที่ 10 เสริมสร้างความมั่นคงทางเทคโนโลยีสารสนเทศและไซเบอร์

10.1ปกป้อง ป้องกัน ภัยคุกคามด้านไซเบอร์ สงครามไซเบอร์ และเสริมสร้างความปลอดภัยระบบเทคโนโลยีสารสนเทศ

10.2 พัฒนาการบังคับใช้กฎหมาย

10.3 พัฒนาการศักยภาพทางด้านเทคโนโลยีสารสนเทศ

นโยบายที่ 13 พัฒนาระบบการเตรียมความพร้อมแห่งชาติเพื่อเสริมสร้างความมั่นคงแห่งชาติ

13.1 พัฒนาระบบการเตรียมความพร้อมแห่งชาติ ให้ประสานสอดคล้องระหว่างแผนระดับชาติ ระดับจังหวัด ระดับท้องถิ่น และระดับชุมชน

13.2 จัดให้มีระบบสั่งการที่มีเอกภาพ

13.3 ส่งเสริมและสนับสนุนการมีส่วนร่วมทุกภาคส่วน

13.4 พัฒนาและสนับสนุนการมีระบบฐานข้อมูลเฝ้าระวังและเตรียมความพร้อมด้านภัยพิบัติที่ทันสมัย

นโยบายที่ 14 เสริมสร้างและพัฒนาศักยภาพในการป้องกันประเทศ

14.1 เสริมสร้างและพัฒนากองทัพให้มีโครงสร้างกำลังกองทัพ และยุทโธปกรณ์ที่เหมาะสม ทันสมัย

14.2 เสร้างสร้างและพัฒนาศักยภาพของชาติด้วยการผนึกกำลังจากทุกภาคส่วนในการป้องกันประเทศ และให้มีส่วนร่วมในการสนับสนุนการดำเนินงานของกองทัพตั้งแต่ในภาวะปกติ

14.3 เสริมสร้างความสัมพันธ์อันดี และความร่วมมือในทุกระดับกับกองทัพประเทศเพื่อนบ้าน

14.4 พัฒนาและนำศักยภาพของกองทัพในยามปกติเข้ามาสนับสนุนภารกิจนอกเหนือจากสงคราม

14.5 ส่งเสริมและพัฒนาวิทยาศาสตร์และเทคโนโลยีการป้องกันประเทศและความมั่นคง

นโยบายที่ 15 พัฒนาระบบข่าวกรองให้มีประสิทธิภาพ

15.1 ดำเนินงานข่าวกรองที่มีประสิทธิภาพและแจ้งเตือนภัยล่วงหน้าอย่างมีประสิทธิภาพ

15.2 เสริมสร้างความร่วมมืออย่างเป็นเอกภาพในประชาคมข่าวกรอง และหน่วยงานภาครัฐ รวมทั้งหน่วยข่างกรองต่างประเทศ และมีเครือข่ายด้านข้อมูลข่าวสารกับภาคเอกชนแบะประชาชน

15.3 เสริมสร้างและพัฒนาขีดความสามารถของระบบข่าวกรองอย่างต่อเนื่อง

แนวคิดเศรษฐกิจพอเพียง

เศรษฐกิจพอเพียง เป็นปรัชญาชี้แนวทางการดำรงชีวิตและการปฏิบัติตนของประชาชนในทุกระดับ ตั้งแต่ระดับครอบครัว ระดับชุมชน ไปจนถึงระดับรัฐทั้งในการพัฒนาและบริหารประเทศให้ดำเนินไปในทางสายกลาง โดยเฉพาะการพัฒนาเศรษฐกิจ ความพอเพียงหมายถึง ความพอประมาณ ความมีเหตุผล และการมีภูมิคุ้มกัน เพื่อให้สามารถป้องกันจากภัยที่มาจากการเปลี่ยนแปลงทั้งภายในและภายนอก โดยต้องประกอบด้วยเงื่อนไขความรู้ ประกอบด้วย รอบรู้ รอบคอบ ระมัดระวัง และเงื่อนไขคุณธรรม ประกอบด้วย ซื่อสัตย์ สุจริต ขยัน อดทนและแบ่งปัน

วิสัยทัศน์

ประเทศไทยมีศักยภาพในการสร้างภูมิคุ้มกันป้องกันและร่วมกันต่อต้านการก่อการร้ายทางไซเบอร์

พันธกิจ

สร้างฐานความรู้ทางไซเบอร์ให้กับประชาชนทุกระดับพร้อมทั้งมุ่งพัฒนาความเข็มแข็งทางไซเบอร์เพื่อความมั่นคงของประเทศไทย

เป้าประสงค์

เพื่อพัฒนาและเสริมสร้างความมั่นคงทางไซเบอร์ให้กับประเทศไทย

ยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย

ยุทธศาสตร์ที่ 1 Research ยุทธศาสตร์การเสริมสร้างงานวิจัยเพื่อการพัฒนาทางไซเบอร์

แนวทางหรือมาตรการ

1. มีการส่งเสริมให้ประชาชน นักวิชาการ หรือภาคเอกชนมีความสนใจในประเด็นทางไซเบอร์และการก่อการร้ายทางไซเบอร์มากขึ้น ให้ครอบคลุมทุกด้าน

2. สนับสนุนด้านงบประมาณด้านการวิจัยทางไซเบอร์เพื่อสร้างแรงจูงใจให้กับนักวิจัยทางไซเบอร์อย่างมีประสิทธิภาพ

ยุทธศาสตร์ที่ 2 Education ยุทธศาสตร์การจัดการศึกษาในการสร้างพื้นฐานของประชาชนในประเทศไทย

แนวทางหรือมาตรการ

1. กำหนดหลักสูตรที่เกี่ยวกับไซเบอร์ในทุกระดับเพื่อให้เยาวชนได้มีรากฐานของการศึกษาและเข้าใจต่อการใช้ไซเบอร์อย่างถูกต้อง

2. พัฒนาหลักสูตรในระดับอุดมศึกษาเพื่อพัฒนาองค์ความรู้ทางไซเบอร์ให้สามารถนำความรู้ไปใช้อย่างครอบคลุมและมีประสิทธิภาพในทุก ๆ ด้าน

ยุทธศาสตร์ที่ 3 Awareness ยุทธศาสตร์การสร้างการตระหนักรู้ทางไซเบอร์ให้กับประชาชน

แนวทางหรือมาตรการ

1. สนับสนุนให้ประชาชนมีการสร้างความรู้ ความเข้าใจที่ดีต่อการใช้ไซเบอร์ รวมทั้งมีการถ่ายทอดความรู้ ความเข้าใจที่ดีต่อการใช้ไซเบอร์ รวมทั้งมีการถ่ายทอดความรู้ความเข้าใจจากรุ่นไปสู่รุ่น

2. เผยแพร่ความรู้และประชาสัมพันธ์ให้ประชาชนมีการใช้ไซเบอร์รวมทั้งตระหนักถึงการใช้ไซเบอร์อย่างถูกต้องเพื่อป้องกันการนำมาเป็นเครื่องมือในการก่อการร้าย

ยุทธศาสตร์ที่ 4 Development ยุทธศาสตร์การพัฒนาความก้าวหน้าทางไซเบอร์

แนวทางหรือมาตรการ

1. มีการจัดตั้งหน่วยงานการพัฒนาทางไซเบอร์เพื่อพัฒนาระบบสารสนเทศและการรักษาความปลอดภัยทางไซเบอร์ข้อมูลข่าวสาร

2. จัดฝึกอบรมให้ความรู้ สนับสนุนการจัดสอบเพื่อให้บุคลากรผ่านเกณฑ์มาตรฐานสากล สนับสนุนการวิจัยสร้างองค์ความรู้ใหม่ทางไซเบอร์

3. พัฒนาบุคลากรให้มีความเชี่ยวชาญในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ รวมทั้งสร้างแรงจูงใจในการจงรักภักดีและทำงานเพื่อประเทศชาติเพื่อป้องกันสมองไหลไปยังต่างประเทศ

ยุทธศาสตร์ที่ 5 Coordinate ยุทธศาสตร์การส่งเสริมความร่วมมือระหว่างภาครัฐ ภาคเอกชน และภาคประชาชน

แนวทางหรือมาตรการ

1. มีการเสริมสร้างความเข้าใจร่วมกันในการกำหนด นิยาม ความหมายของไซเบอร์ การก่อการร้ายและการก่อการร้ายทางไซเบอร์

2. มีการกำหนดนโยบาย แนวทางและแผนปฏิบัติการที่ชัดเจนเพื่อให้เกิดการแปลงแผนไปสู่กลยุทธ์และไปสู่การปฏิบัติตามวิสัยทัศน์ พันธกิจและเป้าประสงค์ที่กำหนดไว้อย่างมีประสิทธิภาพ

3. กำหนดกลไกในการทบทวน ติดตาม และประเมินความเสี่ยงต่อการนำแผนไปปรับใช้เพื่อปรับแนวทางให้มีความเหมาะสมตามสถานการณ์ใหม่หรือสถานการณ์ที่แตกต่าง

ยุทธศาสตร์ที่ 6 Law ยุทธศาสตร์การกำหนดใช้กฎหมายทางไซเบอร์และการบังคับใช้กับประชาชน

แนวทางหรือมาตรการ

1. กำหนดกฎหมาย กฎระเบียบ ขั้นตอน ที่เกี่ยวข้องกับการใช้ไซเบอร์ ความมั่นคงทางไซเบอร์และการต่อต้านการก่อการร้ายทางไซเบอร์อย่างครอบคลุม

2. กำหนดแนวทางที่ชัดเจนต่อการบังคับใช้กฎหมาย พร้อมทั้ง มาตรการ บทลงโทษต่อการกระทำอันเกี่ยวข้องกับก่อการร้าย

ยุทธศาสตร์ที่ 7 Integrationยุทธศาสตร์การใช้การบูรณาการร่วมกันเพื่อแบ่งปันข้อมูล

แนวทางหรือมาตรการ

1. จัดตั้งหน่วยงานกลาง มีหน้าที่ในการดูแล ดำเนินการทางด้านไซเบอร์ มีการแบ่งปันข้อมูลร่วมกันเพื่อประโยชน์ของประชาชน รวมทั้งมีการบูรณาการการทำงานร่วมกัน อีกทั้งระบุโอกาส และความท้าทายในการเพิ่มขีดความสมารถของกลไกการตอบสนองต่อการร้าย

2. สร้างฐานข้อมูลกลางเพื่อรวบรวมข้อมูลสำคัญจากทุกภาคส่วน รวมทั้งมีการควบคุมดูแลเพื่อไม่ให้ข้อมูลถูกเผยแพร่ เปิดโอกาสให้ทุกหน่วยงานที่เกี่ยวข้องกับไซเบอร์สามารถดึงข้อมูลไปใช้ในทางที่ถูกต้อง

3. จัดตั้งศูนย์ข่าวกรองทางไซเบอร์ เพื่อทำงานด้านการข่าวทางไซเบอร์ แบ่งปันข้อมูลข่าวสาร และประสานงานความร่วมมือระหว่างหน่วยงาน

ยุทธศาสตร์ที่ 8 Perception Prepares and Protect ยุทธศาสตร์การรับรู้ทางไซเบอร์ร่วมกันตระเตรียม และปกป้องทางไซเบอร์

แนวทางหรือมาตรการ

1. ปลูกฝังทัศนคติและแนวทางการใช้ไซเบอร์ที่เป็นรูปธรรมเพื่อให้ประชาชนมีการรับรู้ต่อการใช้ไซเบอร์ในทางที่ถูกต้อง

2. สร้างการมีส่วนร่วมของประชาชน รวมทั้งวิธีการในการตระเตรียมตนเองเพื่อให้เกิดการปฏิบัติอย่างรู้เท่าทัน

ตารางที่ 23 การกำหนดยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย

ยุทธศาสตร์	วัตถุประสงค์	กลยุทธ์	แนวทาง	ตัวชี้วัดความสำเร็จ	หน่วยงานที่เป็นเจ้าภาพหลัก
ยุทธศาสตร์ที่ 1.Research ยุทธศาสตร์การเสริมสร้างงานวิจัยเพื่อการพัฒนาทางไซเบอร์	1. เพื่อให้มีการพัฒนาผลงานวิจัยทางไซเบอร์ให้เป็นที่ยอมรับในระดับชาติและนานาชาติ	กลยุทธ์ที่ 1 พัฒนางานวิจัยทางไซเบอร์	1.มีการส่งเสริมให้ประชาชนนักวิชาการหรือภาคเอกชนมีความสนใจในประเด็นทางไซเบอร์และการก่อการร้ายทางไซเบอร์มากขึ้นให้ครอบคลุมทุกด้าน 2.สนับสนุนด้านงบประมาณด้านการวิจัยทางไซเบอร์เพื่อสร้างแรงจูงใจให้กับนักวิจัยทางไซเบอร์อย่างมีประสิทธิภาพ	ร้อยละของงานวิจัยที่ได้รับการยอมรับในระดับชาติและนานาชาติ	สถาบันวิจัยแห่งชาติ มหาวิทยาลัย
ยุทธศาสตร์ที่ 2 Education ยุทธศาสตร์	1.เพื่อให้มีหลักสูตรการศึกษา	กลยุทธ์ที่ 1 จัดทำหลักสูตรเฉพาะเกี่ยวกับ	1.กำหนดหลักสูตรที่เกี่ยวกับไซ	จำนวนของหลักสูตรในแต่ละระดับ	กระทรวงศึกษาธิการ

ยุทธศาสตร์	วัตถุประสงค์	กลยุทธ์	แนวทาง	ตัวชี้วัดความสำเร็จ	หน่วยงานที่เป็นเจ้าภาพหลัก
การจัดการศึกษาในการสร้างพื้นฐานของประชาชนในประเทศไทย	ทางไซเบอร์ตั้งแต่ระดับประถมศึกษาจนถึงระดับอุดมศึกษา	ไซเบอร์กลยุทธ์ที่ 2 ติดตามและประเมินผลหลักสูตรทางไซเบอร์ เพื่อนำมาพัฒนาหลักสูตรทุก 5 ปี	เบอร์ในทุกระดับเพื่อให้เยาวชนได้มีรากฐานของการศึกษาและเข้าใจต่อการใช้ไซเบอร์อย่างถูกต้อง 2.พัฒนาหลักสูตรในระดับอุดมศึกษาเพื่อพัฒนาองค์ความรู้ทางไซเบอร์ให้สามารถนำความรู้ไปใช้อย่างครอบคลุมและมีประสิทธิภาพในทุก ๆ ด้าน	จำนวนครั้งของการติดตามประเมินผลหลักสูตร	
ยุทธศาสตร์ที่ 3 Awareness ยุทธศาสตร์การสร้างการตระหนักรู้ทางไซเบอร์ให้กับ	1.เพื่อให้ประชาชนมีความรู้ความเข้าใจต่อการใช้ไซเบอร์จนสามารถสร้างการ	กลยุทธ์ที่ 1 ส่งเสริมให้หน่วยงานภาครัฐ ภาคเอกชนการสร้างการตระหนักรู้ทาง	1.สนับสนุนให้ประชาชนมีการสร้างความรู้ ความเข้าใจที่ดีต่อการใช้ไซเบอร์ รวมทั้งมีการ	ร้อยละของความรู้ความเข้าใจทางไซเบอร์ จำนวนของโครงการที่มี	กระทรวงเทคโนโลยีและการสื่อสาร หน่วยงานภาครัฐทุกส่วน

ยุทธศาสตร์	วัตถุประสงค์	กลยุทธ์	แนวทาง	ตัวชี้วัดความสำเร็จ	หน่วยงานที่เป็นเจ้าภาพหลัก
ประชาชน	ป้องกันให้กับตนเองได้	ไซเบอร์กลยุทธ์ที่ 2 จัดทำโครงการทางไซเบอร์โดยสร้างความร่วมมือจากทุกภาคส่วนเพื่อสร้างความตระหนักรู้ให้กับประชาชน	ถ่ายทอดความรู้ความเข้าใจที่ดีต่อการใช้ไซเบอร์ รวมทั้งมีการถ่ายทอดความรู้ความเข้าใจจากรุ่นไปสู่รุ่น 2.เผยแพร่ความรู้และประชาสัมพันธ์ให้ประชาชนมีการใช้ไซเบอร์รวมทั้งตระหนักถึงการใช้ไซเบอร์อย่างถูกต้องเพื่อป้องกันการนำมาเป็นเครื่องมือในการก่อการร้าย	การสร้างการตระหนักรู้ทางไซเบอร์ให้กับประชาชน	
ยุทธศาสตร์ที่ 4 Development ยุทธศาสตร์การพัฒนาความก้าว	1.เพื่อให้หน่วยงานทุกภาคส่วนรวมทั้งภาคประชาชนมีส่วนในการ	กลยุทธ์ที่ 1 ให้มีหน่วยงานการพัฒนาทางไซเบอร์ให้มีความก้าวหน้าเทียบเท่ากับ	1.มีการจัดตั้งหน่วยงานการพัฒนาทางไซเบอร์เพื่อพัฒนาระบบสารสนเทศและ	สมรรถนะของหน่วยงานที่มีการพัฒนาความก้าวหน้าทางไซเบอร์ร้อยละของผู้	กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ยุทธศาสตร์	วัตถุประสงค์	กลยุทธ์	แนวทาง	ตัวชี้วัดความสำเร็จ	หน่วยงานที่เป็นเจ้าภาพหลัก
หน้าทางไซเบอร์	พัฒนาความก้าวหน้าทางไซเบอร์ในทุกด้าน	ประเทศเพื่อนบ้าน กลยุทธ์ที่ 2 การสร้างมาตรฐานความรู้เพื่อให้ตรงตามมาตรฐานสากล กลยุทธ์ที่ 3 ส่งเสริมให้บุคลากรมีความรู้และมีสมรรถนะทางไซเบอร์เทียบกับประเทศในอาเซียน	การรักษาความปลอดภัยทางไซเบอร์ข้อมูลข่าวสาร 2.จัดฝึกอบรมให้ความรู้สนับสนุนการจัดสอบเพื่อให้บุคลากรผ่านเกณฑ์มาตรฐานสากล สนับสนุนการวิจัยสร้างองค์ความรู้ใหม่ทางไซเบอร์ 3.พัฒนาบุคลากรให้มีความเชี่ยวชาญในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ รวมทั้งสร้างแรงจูงใจในการจงรักภักดีและทำงานเพื่อประเทศชาติ	ผ่านมาตรฐานสากลทางไซเบอร์จำนวนของบุคลากรที่มีความรู้และมีสมรรถนะทางไซเบอร์ที่ผ่านมาตรฐานสากล	

ยุทธศาสตร์	วัตถุประสงค์	กลยุทธ์	แนวทาง	ตัวชี้วัดความสำเร็จ	หน่วยงานที่เป็นเจ้าภาพหลัก
			เพื่อป้องกันสมองไหลไปยังต่างประเทศ		
ยุทธศาสตร์ที่ 5 Coordinate ยุทธศาสตร์การส่งเสริมความร่วมมือระหว่างภาครัฐ ภาคเอกชน และภาคประชาชน	1.เพื่อให้หน่วยงานทุกภาคส่วนรวมทั้งภาคประชาชนมีความร่วมมือป้องกันทางไซเบอร์อย่างเป็นรูปธรรม	กลยุทธ์ที่ 1 สร้างหรือพัฒนาให้มีองค์กรหน่วยงานที่เป็นแกนกลางในการร่วมมือกันทุกภาคส่วน กลยุทธ์ที่ 2 ส่งเสริมให้องค์กรทุกภาคส่วนที่มีส่วนเกี่ยวข้องทางไซเบอร์ปฏิบัติงานในทิศทางเดียวกัน กลยุทธ์ที่ 3 สร้างระบบการพัฒนาข้าราชการและบุคลากรส่วนงานไซเบอร์ให้มีศักยภาพในการปฏิบัติงาน	1.มีการเสริมสร้างความเข้าใจร่วมกันในการกำหนด นิยามความหมายของไซเบอร์ การก่อการร้ายและการก่อการร้ายทางไซเบอร์ 2.มีการกำหนดนโยบาย แนวทางและแผนปฏิบัติการที่ชัดเจนเพื่อให้เกิดการแปลงแผนไปสู่กลยุทธ์และไปสู่การปฏิบัติตามวิสัยทัศน์ พันธกิจและเป้าประสงค์ที่กำหนดไว้อย่างมีประสิทธิภาพ	จำนวนของโครงการที่มีการสร้างความร่วมมือกันของทุกภาคส่วน	รัฐบาล

ยุทธศาสตร์	วัตถุประสงค์	กลยุทธ์	แนวทาง	ตัวชี้วัดความสำเร็จ	หน่วยงานที่เป็นเจ้าภาพหลัก
		อย่างเป็นระบบ	3.กำหนดกลไกในการทบทวน ติดตาม และประเมินความเสี่ยงต่อการนำแผนไปปรับใช้เพื่อปรับแนวทางให้มีความเหมาะสมตามสถานการณ์ใหม่หรือสถานการณ์ที่แตกต่าง		
ยุทธศาสตร์ที่ 6 Law ยุทธศาสตร์การกำหนดใช้กฎหมายทางไซเบอร์และการบังคับใช้กับประชาชน	1.เพื่อให้มีกฎหมายไซเบอร์ของประเทศไทย	กลยุทธ์ที่ 1มีการพัฒนากฎหมายไซเบอร์และบังคับใช้อย่างเป็นรูปธรรม	1.กำหนดกฎหมายกฎระเบียบขั้นตอน ที่เกี่ยวข้องกับการใช้ไซเบอร์ความมั่นคงทางไซเบอร์และการต่อต้านการก่อการร้ายทางไซเบอร์อย่างครอบคลุม 2.กำหนด	ร้อยละของผู้มีความรู้เกี่ยวกับกฎหมายไซเบอร์ จำนวนของประชาชนที่รู้กฎหมายไซเบอร์	

ยุทธศาสตร์	วัตถุประสงค์	กลยุทธ์	แนวทาง	ตัวชี้วัดความสำเร็จ	หน่วยงานที่เป็นเจ้าภาพหลัก
			แนวทางที่ชัดเจนต่อการบังคับใช้กฎหมายพร้อมทั้งมาตรการบทลงโทษต่อการกระทำอันเกี่ยวข้องกับก่อการร้าย		
ยุทธศาสตร์ที่ 7 Integration ยุทธศาสตร์การใช้การบูรณาการร่วมกันเพื่อแบ่งปันข้อมูล	1.เพื่อให้มีระบบข้อมูลกลางเพื่อแบ่งปันข้อมูลข่าวสาร	กลยุทธ์ที่ 1 สร้างระบบข้อมูลกลาง	1.จัดตั้งหน่วยงานกลางมีหน้าที่ในการดูแลดำเนินการทางด้านไซเบอร์ มีการแบ่งปันข้อมูลร่วมกันเพื่อประโยชน์ของประชาชนรวมทั้งมีการบูรณาการการทำงานร่วมกัน อีกทั้งระบุโอกาสและความท้า	ร้อยละของจำนวนข้อมูลที่มีในระบบ	หน่วยข่าวกรองกองทัพสำนักงานตำรวจแห่งชาติและหน่วยงานที่รับผิดชอบเกี่ยวกับข้อมูล

ยุทธศาสตร์	วัตถุประสงค์	กลยุทธ์	แนวทาง	ตัวชี้วัดความสำเร็จ	หน่วยงานที่เป็นเจ้าภาพหลัก
			ทายในการเพิ่ม ขีดความ สามารถของ กลไกการ ตอบสนองต่อ การร้าย 2.สร้าง ฐานข้อมูล กลางเพื่อ รวบรวมข้อมูล สำคัญจากทุก ภาคส่วน รวมทั้งมีการ ควบคุมดูแล เพื่อไม่ให้ ข้อมูลถูก เผยแพร่ เปิด โอกาสให้ทุก หน่วยงานที่ เกี่ยวข้องกับไซ เบอร์สามารถ ดึงข้อมูลไปใช้ ในทางที่ ถูกต้อง 3. จัดตั้งศูนย์ ข่าวกรองทาง ไซเบอร์ เพื่อ		

ยุทธศาสตร์	วัตถุประสงค์	กลยุทธ์	แนวทาง	ตัวชี้วัดความสำเร็จ	หน่วยงานที่เป็นเจ้าภาพหลัก
			ทำงานด้านการข่าวทางไซเบอร์ แบ่งปันข้อมูลข่าวสาร และประสานงานความร่วมมือระหว่างหน่วยงาน		
ยุทธศาสตร์ที่ 8 Perception Prepares and Protect ยุทธศาสตร์การรับรู้ทางไซเบอร์ร่วมกันตระเตรียมและปกป้องทางไซเบอร์	1.เพื่อให้ประชาชนเกิดการรับรู้ร่วมกันตระเตรียมและป้องกันทางไซเบอร์	กลยุทธ์ที่ 1 พัฒนาและเสริมสร้างความรู้เรื่องไซเบอร์ที่เหมาะสมและจำเป็นกับประชาชน กลยุทธ์ที่ 2 เสริมสร้างจิตสำนึกและแนวทางการป้องกันตนเองเพื่อให้เกิดการป้องกันตนเอง	1.ปลูกฝังทัศนคติและแนวทางการใช้ไซเบอร์ที่เป็นรูปธรรมเพื่อให้ประชาชนมีการรับรู้ต่อการใช้ไซเบอร์ในทางที่ถูกต้อง 2.สร้างการมีส่วนร่วมของประชาชนรวมทั้งวิธีการในการตระเตรียมตนเองเพื่อให้เกิดการปฏิบัติ	ร้อยละของผู้ที่ได้รับความรู้ความเข้าใจในไซเบอร์ ร้อยละของจำนวนโครงการที่เสริมสร้างการมีส่วนร่วมในการป้องกันตนเองจากภัยไซเบอร์	กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร และหน่วยงานที่ดูแลทางไซเบอร์

ยุทธศาสตร์	วัตถุประสงค์	กลยุทธ์	แนวทาง	ตัวชี้วัดความสำเร็จ	หน่วยงานที่เป็นเจ้าภาพหลัก
			อย่างรู้เท่าทัน		

การศึกษาวิจัยได้ค้นพบกระบวนการจัดทำยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย ดังนี้ กำหนดรายละเอียดเป็นขั้นตอนดังนี้

ขั้นตอนที่ 1 ศึกษายุทธศาสตร์ชาติ พลังอำนาจแห่งชาติและผลประโยชน์แห่งชาติ เพื่อรักษาไว้ซึ่งความมั่นคงแห่งชาติ เป็นประการแรกของการก่อพื้นฐานของกระบวนยุทธศาสตร์ กระบวนการทางยุทธศาสตร์ประการแรกคือยุทธศาสตร์ชาติ ประกอบด้วย 5 ยุทธศาสตร์หลักคือ 1. ยุทธศาสตร์สร้างความมั่นคงให้กับประเทศ 2. ยุทธศาสตร์สร้างความสามารถในการแข่งขันของประเทศ 3. ยุทธศาสตร์สร้างโอกาสบนความเสมอภาคและเท่าเทียมกันทางสังคม 4. ยุทธศาสตร์การเติบโตบนคุณภาพชีวิตที่เป็นมิตรกับสิ่งแวดล้อม และ5. ยุทศาสตร์การเพิ่มประสิทธิภาพของรัฐ

ยุทธศาสตร์ชาติที่มีความเกี่ยวข้องเป็นยุทธศาสตร์การสร้างความมั่นคงให้กับประเทศด้วยความมั่นคงเป็นเรื่องที่มีผลกระทบต่อการพัฒนาในทุกมิติ สร้างความเชื่อมั่นกับนานาประเทศทั้งในด้านการเมือง เศรษฐกิจและสังคม กรอบแนวทางที่ต้องให้ความสำคัญเชื่อมโยงกับการต่อต้านการก่อการร้ายทางไซเบอร์ คือ พัฒนาระบบ กลไก มาตรการและความร่วมมือระหว่างประเทศ เพื่อป้องกันและแก้ปัญหาภัยคุกคามข้ามชาติ ลดผลประทบจากภัยก่อการร้ายและเสริมสร้างความมั่นคงทางเทคโนโลยีสารสนเทศและไซเบอร์

พลังอำนาจแห่งชาติ เป็นแรงเสริมในการช่วยในการสร้างกรอบยุทธศาสตร์ให้มีความมั่นคงในประเด็นของ ด้านข่าวสารและสารสนเทศ (Information)และผลประโยชน์แห่งชาติ มีความสอดคล้องในประเด็นของการอยู่ร่วมกันอย่างสันติ ประสานสอดคล้องกันด้านความมั่นคงในประชาคมอาเซียนและประชาคมโลกอย่างมีเกียรติและศักดิ์ศรี สอดคล้องกับวัตถุประสงค์ของชาติใน3 ข้อคือ ข้อ 5.เพื่อพัฒนาศักยภาพของภาครัฐ และส่งเสริมบทบาทและความเข็มแข็งของทุกภาคส่วนในการรับมือกับภัยคุกคามทุกรูปแบบที่กระทบความมั่นคง ข้อ 7.เพื่อพัฒนาศักยภาพการเตรียมความพร้อมของชาติในการเผชิญกับภาวะสงครามละวิกฤติการณ์ความมั่นคง อย่างมีเอกภาพและประสิทธิภาพและข้อ 8.เพื่อเสริมสร้างศักยภาพของกองทัพในการป้องกันประเทศ สนับสนุนภารกิจที่ไม่ใช่ช่วงสงครามและสามารถผนึกกำลังของกองทัพทุกภาคส่วนในการเผชิญกับภัยคุกคามด้านการป้องกันประเทศทุกรูปแบบ

แนวคิดเศรษฐกิจพอเพียง เป็นปรัชญาชี้แนวทางการดำรงชีวิตและการปฏิบัติตนของประชาชนในทุกระดับ ตั้งแต่ระดับครอบครัว ระดับชุมชน ไปจนถึงระดับรัฐทั้งในการพัฒนาและบริหารประเทศให้ดำเนินไปในทางสายกลาง โดยเฉพาะการพัฒนาเศรษฐกิจ ความพอเพียงหมายถึง ความพอประมาณ ความมีเหตุผล และการมีภูมิคุ้มกัน เพื่อให้สามารถป้องกันจากภัยที่มาจากการเปลี่ยนแปลงทั้งภายในและภายนอก โดยต้องประกอบด้วยเงื่อนไขความรู้ ประกอบด้วย รอบรู้ รอบคอบ ระมัดระวัง และเงื่อนไขคุณธรรม ประกอบด้วย ซื่อสัตย์ สุจริต ขยัน อดทนและแบ่งปัน ขั้นตอนที่ 2 กำหนดวิสัยทัศน์ พันธกิจ และเป้าประสงค์ วิเคราะห์สภาพแวดล้อมภายนอก และสภาพแวดล้อมภายใน SWOT และกำหนดยุทธศาสตร์ READ: CLIP และวิเคราะห์ 7's Mckinsey Modelขององค์กร ดังนี้

วิสัยทัศน์ คือ ประเทศไทยต้องมีศักยภาพในการสร้างภูมิคุ้มกันป้องกัน และร่วมกันต่อต้านการก่อการร้ายทางไซเบอร์

พันธกิจ คือ สร้างฐานความรู้ทางไซเบอร์ให้กับประชาชนทุกระดับพร้อมทั้งมุ่งพัฒนาความเข็มแข็งทางไซเบอร์เพื่อความมั่นคงของประเทศไทย

เป้าประสงค์ คือเพื่อพัฒนาและเสริมสร้างความมั่งคงทางไซเบอร์ให้กับประเทศไทย การวิเคราะห์สภาพแวดล้อมภายนอกและสภาพแวดล้อมภายใน เป็นการกำหนดอนาคตขององค์การ วิธีการที่ใช้เป็นการวิเคราะห์ SWOT คือ วิเคราะห์จุดแข็ง (Strength) และจุดอ่อน (Weakness) ต่อการก่อการร้ายทางไซเบอร์ในประเทศไทย รวมทั้ง โอกาส (Opportunity) และข้อจำกัดหรือภัยคุกคาม (Threat) จากภายนอก การวิเคราะห์สภาพแวดล้อมภายนอก ประกอบด้วย สภาพเศรษฐกิจ สังคม การเมือง ส่วนสภาพแวดล้อมภายในจะเป็นการกล่าวถึง การพัฒนาโครงสร้างพื้นฐาน การพัฒนาทางไซเบอร์ของประเทศไทย การขาดความพร้อมในการพัฒนาระบบไซเบอร์ จะเห็นได้ว่าสภาพแวดล้อมทั้งภายนอกและภายในนี้อาจเป็นได้ทั้งปัจจัยเกื้อหนุนหรือเป็นอุปสรรคต่อการต่อต้านการก่อการร้ายทางไซเบอร์

1.1 การกำหนดวิสัยทัศน์ (Vision) ผลจากการวิเคราะห์ SWOT จะนำไปสู่การกำหนดวิสัยทัศน์ ซึ่งเป็นภาพอนาคตที่ต้องการจะไปให้ถึง วิสัยทัศน์คือ ประเทศไทยต้องมีศักยภาพในการสร้างภูมิคุ้มกัน ป้องกันและร่วมกันต่อต้านการก่อการร้ายทางไซเบอร์

1.2 การกำหนดพันธกิจ (Mission) จะเป็นกล่าวถึงสิ่งที่ประเทศจะกระทำพันธกิจต้องเชื่อมโยงกับจุดมุ่งหมายหรือเหตุผลในการดำเนินการนั้น พันธกิจ คือ สร้างฐานความรู้ทางไซเบอร์ให้กับประชาชนทุกระดับพร้อมทั้งมุ่งพัฒนาความเข็มแข็งทางไซเบอร์เพื่อความมั่นคงของประเทศไทย

1.3 การกำหนดวัตถุประสงค์ (Objectives) เป็นผลที่ต้องการให้เกิดขึ้นในลักษณะจำเพาะเจาะจง จะเกิดขึ้นจากการดำเนินกิจกรรมตามที่ได้วางแผนไว้ วัตถุประสงค์จะต้องระบุว่าจะต้องทำอะไร ให้เมื่อไหร่เสร็จ และควรจะวัดได้ วัตถุประสงค์ขององค์การในทุระดับ เป้าประสงค์คือ เพื่อพัฒนาและเสริมสร้างความมั่งคงทางไซเบอร์ให้กับประเทศไทย

1.4 การกำหนดยุทธศาสตร์ เป็นวิธีการที่จะทำให้เกิดผลสำเร็จตามที่ตั้งเป้าหมายไว้ ยุทธศาสตร์การป้องกันภัยจากการก่อการร้ายจะต้องตอบสนองวัตถุประสงค์หลัก เพื่อป้องกันการโจมตีเป้าหมายสำคัญของประเทศที่จะส่งผลเสียหายต่อประเทศในระยะยาว ลดอันตรายที่เกิดจากการกระทำของผู้ร้าย และสามารถฟื้นฟูประเทศภายหลังจากการถูกกระทำให้สามารถกลับมาเหมือนเดิมได้อย่างรวดเร็ว ประเด็นสำคัญที่ต้องดำเนินการเป็นส่วนแรกคือการเตรียมการด้านการรักษาความปลอดภัย เตรียมการประเทศให้สามารถมีความพร้อมต่อการต่อต้านการก่อการร้าย ยุทธศาสตร์การต่อต้านการก่อการร้ายประกอบด้วย 8 ยุทธศาสตร์หลัก READ: CLIP

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

การวิเคราะห์ The 7's Mckinsey Model โดยวิเคราะห์เป็นประเด็นตามตัวแบบสถานการณ์ประเทศได้ดังนี้

1. ประเทศไทยมียุทธศาสตร์ (Strategy)ในการปฏิบัติตามแผนงานในการจัดการแก้ปัญหา การก่อการร้ายตามแผนงานจากการเตรียมการ ป้องกัน ต่อต้านและตอบโต้ จนถึงขั้นฟื้นฟู

2.โครงสร้าง (Structure) ของการมอบหมายงาน การแบ่งงาน ใช้โครงสร้างการจัดองค์การมีการทำงานตามสายการบังคับบัญชาและมีการสั่งการที่ตรงตามวัตถุประสงค์

3. ระบบขององค์การ (System) ตั้งแต่การวางแผน การอำนวยการ การประสานงานการดำเนินการด้านการข่าว และด้านอื่น ๆ

4. รูปแบบ (Style) ของการบริหารงานของผู้บริหารมีความเข้าใจในการก่อการร้าย การกระทำทางไซเบอร์ และการดำเนินการเพื่อการป้องกันการก่อการร้ายทางไซเบอร์อย่างแท้จริง

5. เจ้าหน้าที่ของคนในองค์การทำงานเป็นทีม (Staff) เข้าใจและสามารถปฏิบัติหน้าที่ได้อย่างมีประสิทธิภาพ

6. ทักษะขององค์การและคนในองค์การ (Skill) เจ้าหน้าที่ที่เกี่ยวข้องกับการดำเนินงานทางไซเบอร์ต้องได้รับการพัฒนาและถ่ายทอดองค์ความรู้ เทคโนโลยีที่ทันสมัยและการฝึกต่อต้านการก่อการร้ายที่ก่อให้เกิดความเชี่ยวชาญ

7. ค่านิยมร่วมกัน (Share Value) องค์การต้องสร้างค่านิยมต่อบุคลากรให้มีวัฒนธรรมองค์ในทิศทางเดียวกัน

Balanced Scorecard โดยวิเคราะห์เป็นประเด็นดังนี้

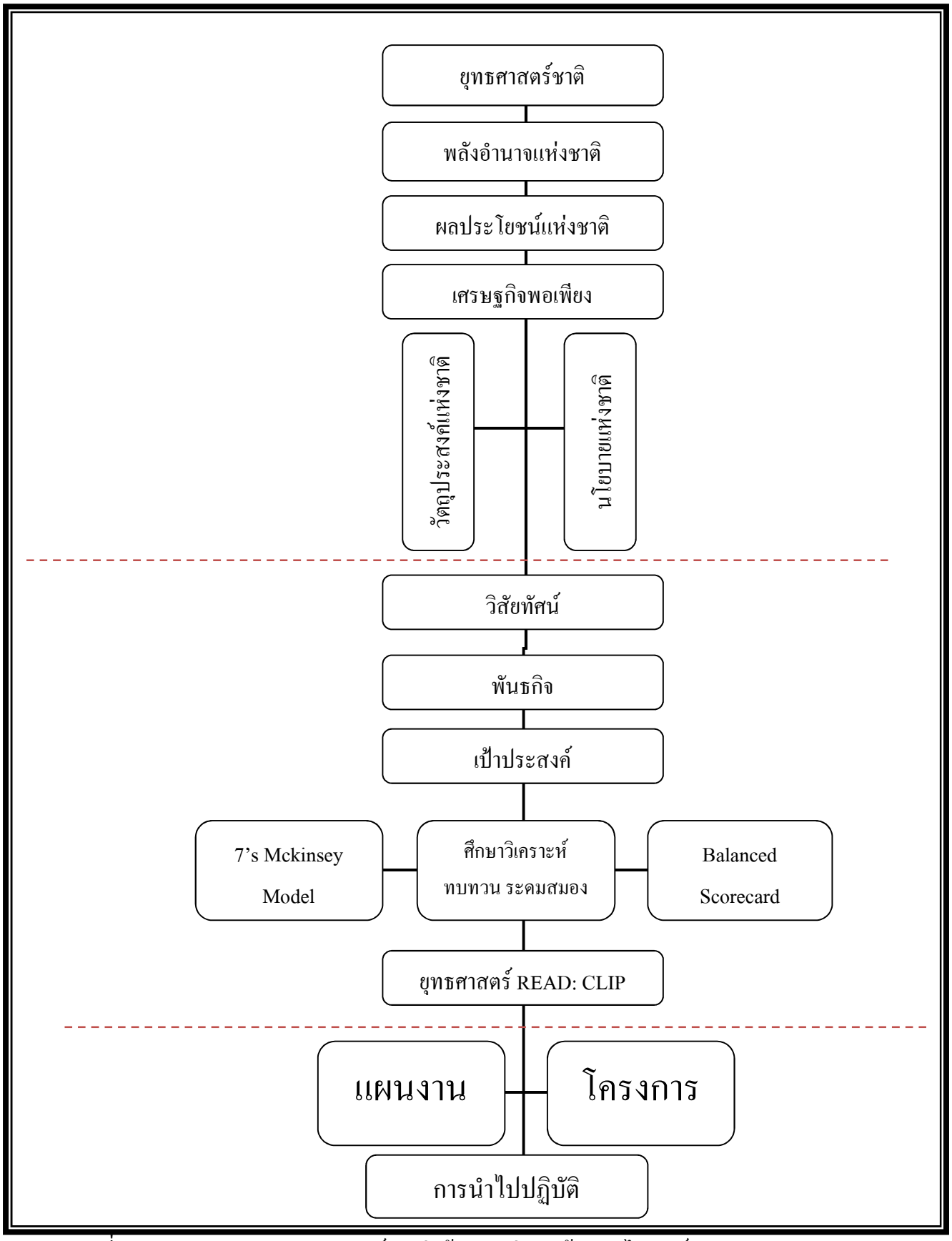
1.มุมมองด้านการเงิน (Financial perspective)

2.มุมมองด้านลูกค้า (Customer perspective)

3.มุมมองด้านกระบวนการของธุรกิจ (Business process perspective)

4.มุมมองด้านการเรียนรู้และการเติบโต (Learning and growth perspective)

ขั้นตอนที่3การกำหนดแผนงาน และโครงการเพื่อนำไปสู่การปฏิบัติ การกำหนดแผนงานจะทำให้องค์กรดำเนินงานให้เป็นไปในทิศทางเดียวกัน



ภาพที่ 11 กระบวนการจัดทำยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์

บทที่ 6
อธิปรายและสรุปผล

การวิจัยเรื่องยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย มีวัตถุประสงค์การวิจัยดังนี้1. เพื่อศึกษาความก้าวหน้าทางไซเบอร์ที่มีการนำมาใช้เป็นเครื่องมือทางยุทธศาสตร์ในการก่อการร้ายในประเทศไทย2.เพื่อศึกษาลักษณะการก่อการร้ายโดยใช้ไซเบอร์มาเป็นเครื่องมือทางยุทธศาสตร์ในการก่อการร้ายของประเทศไทยและวิเคราะห์ประเมินการก่อการร้ายทางไซเบอร์ในประเทศไทยโดยใช้การวิเคราะห์จุดแข็ง จุดอ่อน โอกาสและอุปสรรควิธีการวิเคราะห์สถานการณ์และองค์กรแห่งการเรียนรู้ 3. เพื่อพัฒนายุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย

ดำเนินการวิจัยด้วยการใช้เทคนิคเดลฟาย กำหนดและเตรียมกลุ่มผู้เชี่ยวชาญ สัมภาษณ์เชิงลึก จำนวน 10 คน กลุ่มแรกเป็นผู้ที่มีบทบาทเกี่ยวข้องกับการใช้ไซเบอร์ 4 คน กลุ่มที่สอง กลุ่มที่มีความเชี่ยวชาญในส่วนของการกำหนดยุทธศาสตร์ทางไซเบอร์ จำนวน 6 คน และทำการสัมภาษณ์ผู้เชี่ยวชาญ จากนั้นรวบรวมข้อมูลและจัดทำแบบสอบถามปลายปิดให้กลุ่มผู้เชี่ยวชาญในรอบที่สองและทำการสรุปผลที่ได้จากการศึกษา นำข้อมูลที่ได้มาจัดทำเป็นแบบสอบถามเชิงปริมาณ เพื่อกำหนดยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ของประเทศไทย และนำแบบสอบถามกับกลุ่มตัวอย่างจำนวน 690 คน ประกอบด้วย ข้าราชการ นักธุรกิจ นักเรียน/นักศึกษาและบุคคลทั่วไป นำข้อมูลที่ได้มาวิเคราะห์ทางสถิติ นำข้อมูลที่ได้ทั้งหมดมาปรับปรุงเป็นยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ของประเทศไทย

สรุปผลการวิจัย

สรุปผลการวิจัยตามวัตถุประสงค์ข้อที่ 1

1. ความก้าวหน้าทางไซเบอร์คือ เทคโนโลยีที่มีอินเทอร์เน็ต เพื่อเชื่อมต่อการสื่อสารได้ทุกที่ทุกเวลา ไม่ว่าจะอยู่ที่ใดบนโลก สะดวก รวดเร็วและไซเบอร์มีความสำคัญอย่างมากต่อการดำรงชีวิตในปัจจุบัน โดยมีเครื่องมือที่ใช้ในการติดต่อสื่อสาร ไม่ว่าจะเป็น คอมพิวเตอร์ โทรศัพท์มือถือ หรือ แท็บเล็ต เป็นต้น และความก้าวหน้าทางไซเบอร์ต้องมีความเร็วสูง มีระบบปฏิบัติการที่ดีและมีประสิทธิภาพสามารถเข้าถึงได้

2. ประเทศไทยมีโอกาสในการพัฒนาความก้าวหน้าทางไซเบอร์ได้อีกมาก บริบทของประเทศไทยยังคงเป็นประเทศที่ไม่ได้มีการใช้ไซเบอร์ทั้งระบบในโครงสร้างพื้นฐานและมีโอกาส

ในการพัฒนาทางไซเบอร์ด้วยปัจจัยหลายด้าน เช่น ความสามารถของคนรุ่นใหม่ที่มีความสนใจทางไซเบอร์ ความตื่นตัวต่อการเรียนรู้ทางไซเบอร์ การพัฒนาโครงสร้างพื้นฐานให้มีความพร้อม สามารถพัฒนาควบคู่ไปกับการใช้ไซเบอร์ และมีวิธีการป้องกันที่ดีต่อการก่อการร้าย

3. ประเทศไทยกล่าวได้ว่าแม้ไม่ใช่เป้าหมายโดยตรงของกลุ่มผู้ก่อการร้าย แต่อาจตกเป็นเป้าหมายสำหรับการปฏิบัติการของกลุ่มผู้ก่อการร้าย เนื่องจากประเทศไทยมีผลประโยชน์เกี่ยวข้องกับประเทศต่าง ๆ โดยเฉพาะประเทศตะวันตก ซึ่งเป็นเป้าหมายของกลุ่มผู้ก่อการร้ายจำนวนมาก โดยกลุ่มผู้ก่อการร้ายส่วนใหญ่ที่เข้ามาเคลื่อนไหวและปฏิบัติการในประเทศไทย จะใช้ประเทศไทยเป็นแหล่งที่หลบภัยและผลิตยุทโธปกรณ์ของกลุ่มผู้ก่อการร้าย อีกทั้งยังแสวงหาผลประโยชน์จากทางการเงิน การธนาคาร ประเทศไทยมีมาตรการที่ไม่รัดกุม เป็นช่องทางสนับสนุนทางการเงินของกลุ่มผู้ก่อการร้าย นอกจากนี้ การก่อการร้ายเชื่อมโยงกับการก่ออาชญากรรมประเภทอื่น ๆ ด้วย เช่น การลักลอบค้ายาเสพติด การค้าอาวุธ การฟอกเงินการปลอมแปลงเอกสารเดินทาง บัตรประจำตัวประชาชนหรือเอกสารราชการอื่นๆ ผู้ก่อการร้ายผลิตและลักลอบค้ายาเสพติดสามารถสร้างเงินและรายได้จำนวนมหาศาลให้กับผู้ก่อการร้าย และนำเงินที่ได้มาซื้ออาวุธหรือสร้างฐานกำลังเพื่อดำเนินการก่อการร้ายกับประเทศที่เป็นเป้าหมาย โดยมีวัตถุประสงค์ในการใช้ประเทศไทยเป็นฐานหรือศูนย์กลางในการจัดส่งอาวุธ หรือเป็นทางผ่านไปยังประเทศเป้าหมาย

4. การก่อการร้ายจะต้องมีเป้าหมาย วัตถุประสงค์และรูปแบบในการกระทำที่ชัดเจน ซึ่งกระทำได้จากบุคคล องค์กร หรือรัฐ แต่การก่อการร้ายทางไซเบอร์ มีหลากหลายรูปแบบทั้งประเภทที่กระทำโดยไม่ได้มุ่งหวังทำลายล้างหรือการกระทำที่สร้างความเสียหายต่อประเทศ โดยมีรูปแบบที่หลากหลายและซับซ้อน ซับซ้อน แม้ประเทศไทยจะไม่ใช่เป้าหมายของการก่อการร้ายโดยตรง แต่คนไทยก็ไม่มีการตระหนักต่อภัยของการก่อการร้ายในสถานการณ์การก่อการร้ายปกติ และการก่อการร้ายทางไซเบอร์ ประเทศไทยมีความพร้อมของการรับมือต่อการเกิดสถานการณ์จากหน่วยงานซึ่งมีหน้าที่ดูแลรับผิดชอบ แต่ก็ยังคงมีช่องโหว่ เช่น ทางด้านกฎหมาย ทางด้านของหน้าที่ในการดูแลและรับผิดชอบต่อการป้องกันการก่อการร้าย ผู้ก่อการร้ายสามารถใช้ช่องโหว่นี้ก่อการร้ายได้ทุกเมื่อ

5.ในศตวรรษที่ 21 นี้มีรูปแบบของการก่อการร้ายที่สังคมมีความตื่นตัวกับการป้องกันของการก่อการร้ายทางไซเบอร์ เป็นรูปแบบของการก่อการร้ายโดยมีการนำเทคโนโลยีสารสนเทศที่ทันสมัยนำมาเป็นเครื่องมือที่ช่วยให้กลุ่มก่อการร้ายสามารถดำเนินกิจกรรมต่าง ๆ ได้อย่างมีประสิทธิภาพ โดยใช้พลังอำนาจของเทคโนโลยีสารสนเทศเป็นแนวทางปฏิบัติหรือปรับองค์กรไปสู่รูปแบบใหม่การก่อการร้ายรูปแบบนี้อาศัยช่องว่างการขยายตัวของโลกสมัยใหม่ที่มีการเชื่อมโยงของข้อมูลข่าวสารผ่านระบบคอมพิวเตอร์ในระบบเครือข่าย จึงทำให้ผู้ก่อการร้ายสามารถ

ใช้ช่องทางนี้และผู้ใช้เทคโนโลยีสารสนเทศตกเป็นเป้าของการโจมตีทางไซเบอร์เพื่อทำลายหรือขัดขวางการทำงานระบบเครือข่ายคอมพิวเตอร์แบบต่างๆไม่ว่าจะเป็นเครือข่ายการสื่อสารหรือเครือข่ายระบบคอมพิวเตอร์ที่เกี่ยวข้องกับการทำงานขององค์กรขนาดใหญ่ การควบคุมโครงสร้างพื้นฐาน หรือระบบโครงสร้างความมั่นคงทางทหาร หรือการล้วงข้อมูลความมั่นคงของประเทศเป็นต้น โดยใช้วิธีการสร้างความเสียหาย ก่อให้เกิดความตื่นตระหนกต่อประชาชน และดึงดูดความสนใจของสื่อมวลชนหรือบุคคลต่าง ๆ ซึ่งคาดหมายว่า อนาคตจะมีการก่อการร้ายแบบการก่อการร้ายทางไซเบอร์และเป็นยุทธวิธีหนึ่งในการก่อการร้ายทางไซเบอร์

6. วิธีการก่อการร้ายทางไซเบอร์ มีวิธีการดังนี้ 1.ผู้ก่อการร้ายซึ่งต้องมีความรู้ทางไซเบอร์หรือเทคโนโลยี ศึกษาข้อมูลที่เกี่ยวกับเป้าหมายที่ต้องการจะกระทำ 2.สร้างหรือพัฒนาเครื่องมือให้ตรงกับความต้องการต่อเป้าหมาย เครื่องมือที่สำคัญของการก่อการร้ายทางไซเบอร์คืออินเทอร์เน็ต 3.ระดมคนหรือหาสมาชิกที่มีแนวความคิดแนวทางเดียวกัน 4.ระดมเงินทุนในการสนับสนุน 5. ปฏิบัติการตามวัตถุประสงค์ที่วางไว้เพื่อมุ่งเป้าหมายทางการเมือง

7.ปัจจัยที่เกี่ยวข้องกับแรงจูงใจในการก่อการร้ายทางไซเบอร์ด้วยประเทศไทยเป็นประเทศเปิดเสรี เปิดรับนักท่องเที่ยวและมีนโยบายส่งเสริมให้เกิดการท่องเที่ยวในทุกที่โดยไม่มีข้อจำกัด ดังนั้นจึงเป็นเหมือนสวรรค์ของผู้ก่อการร้าย อีกทั้งการส่งเสริมการเปิดใช้อินเทอร์เน็ตในทุกที่ ทำให้ประชาชนขาดการตระหนักรู้ในเรื่องของการใช้ไซเบอร์ การก่อการร้ายทางไซเบอร์นั้นผู้ก่อการร้ายจะใช้เครื่องมือทางไซเบอร์ที่หาง่ายและใช้เครื่องมือได้ทุกที่ ไม่ว่าจะเป็นโทรศัพท์มือถือ แท็บเล็ต คอมพิวเตอร์ ที่สามารถเชื่อมต่ออินเทอร์เน็ตได้ทำให้คนเข้าถึงได้ง่ายและเชื่องง่ายขึ้น แรงจูงใจที่นำไซเบอร์มาก่อการร้าย ผู้เชี่ยวชาญมองว่าเป็นเรื่องเงินเป็นสำคัญ รองลองมาเป็นเรื่องของแนวคิด อุดมการณ์ทางการเมืองหรือทางศาสนา หรือแม้แต่ความไม่พอใจต่อหน่วยงานหรือองค์กร แต่ปัจจัยที่สำคัญที่ผู้เชี่ยวชาญมองต่างกันคือ แรงจูงใจที่สำคัญต่อการกระทำที่เป็นการก่อการร้ายจะต้องเป็นการกระทำที่มาจากแรงจูงใจทางเมืองเป็นสำคัญ จึงเห็นได้ว่า ความเข้าใจในความหมายของการก่อการร้ายที่แตกต่างกัน นำไปสู่การอธิบายแรงจูงใจของการก่อการร้ายที่ต่างกันด้วย เมื่ออธิบายความเข้าใจแรงจูงใจการก่อการร้ายทางไซเบอร์ จึงไม่ได้มีการให้คำจำกัดความที่ชัดเจน

8.ผู้ก่อการร้ายแสวงหาโอกาสจากประเทศไทยในหลายด้านเพื่อก่อการร้าย ประเด็นสำคัญที่พบได้คือประเทศไทยเป็นประเทศที่เปิดเสรี และประชาชนมีการต้อนรับชาวต่างประเทศ มีการยิ้มแย้มแจ่มใสและต้อนรับผู้อื่นจึงเหมือนกับเป็นสวรรค์ของผู้ก่อการร้าย ส่วนใหญ่ผู้ก่อการร้ายจะใช้ประเทศไทยเป็นฐานในการเตรียมการก่อการร้ายไปยังประเทศที่สาม หรือประเทศที่เป็น

เป้าหมายมากกว่า และประเทศไทยไม่มีมาตรการในการป้องกันความปลอดภัยทางไซเบอร์ ประชาชนยังไม่มีการตระหนักรู้ต่อภัยคุกคามทางไซเบอร์ จึงทำให้มีการใช้อย่างไม่ระแวดระวัง

สอดคล้องกับข้อมูลเชิงปริมาณในประเด็นความก้าวหน้าทางไซเบอร์ กลุ่มตัวอย่างมีความคิดเห็นในระดับมากโดยมีค่าเฉลี่ย4.04 ส่วนเบี่ยงเบนมาตรฐาน 0.54เมื่อพิจารณาเป็นรายข้อ พบว่า ข้อที่มีระดับความคิดเห็นสูง 3 อันดับแรกคือ 1.กลุ่มตัวอย่างมีความคิดเห็นสูงที่สุดคือ การใช้โทรศัพท์มือถือ แท็บเล็ต คอมพิวเตอร์และเครื่องมืออื่นๆ ที่สามารถเชื่อมต่ออินเทอร์เน็ตพร้อมทั้งมีความเร็วสูงเป็นความก้าวหน้าทางไซเบอร์ มีความคิดเห็นในระดับมากที่สุด โดยมีค่าเฉลี่ย 4.24 ส่วนเบี่ยงเบนมาตรฐาน 0.66 2. กลุ่มตัวอย่างมีความคิดเห็นสูงอันดับเป็นที่สอง คือ Application ของโทรศัพท์มือถือที่สามารถอำนวยความสะดวกและมีการเชื่อมต่ออย่างรวดเร็ว ส่งผลต่อความก้าวหน้าทางไซเบอร์มีความคิดเห็นในระดับมากที่สุด โดยมีค่าเฉลี่ย 4.21ส่วนเบี่ยงเบนมาตรฐาน 0.68 และ3. กลุ่มตัวอย่างมีความคิดเห็นสูงอันดับเป็นที่สาม คือ ความก้าวหน้าทางไซเบอร์คือการพัฒนาทางเทคโนโลยีที่สามารถเชื่อมต่อกันได้อย่างรวดเร็วสะดวกขึ้นทำให้ทุกคนติดต่อกันได้ไม่ว่าจะอยู่ที่ใดในโลกมีความคิดเห็นในระดับมาก โดยมีค่าเฉลี่ย 4.16 ส่วนเบี่ยงเบนมาตรฐาน 0.73

สรุปผลการวิจัยตามวัตถุประสงค์ข้อที่ 2

1. การก่อการร้ายหมายถึง กระทำการใด ๆ เพื่อให้เกิดความหวาดกลัว การใช้ความรุนแรงหรือขู่ว่าจะใช้ความรุนแรงเพื่อให้เกิดความตื่นตระหนก โดยมีเหตุจูงใจทางการเมือง ทั้งนี้เพื่อนำไปสู่การเปลี่ยนแปลงในทางสังคมทางการเมือง และทางเศรษฐกิจ

2. ปัญหาที่สำคัญของการต่อต้านการก่อการร้ายเกิดจากแนวคิดของการก่อการร้าย ความหมาย และความไม่รู้ถึงความรุนแรงอันเกิดจากการก่อการร้ายของคนในประเทศใครคือผู้ก่อการร้าย และอะไรคือการก่อการร้าย เนื่องจากภัยการก่อการร้ายเป็นเรื่องไกลตัวและยังไม่มีการสร้างความตระหนักอย่างชัดเจน ดังนั้น มุมมองต่อการก่อการร้ายของแต่ละประเทศ มีการให้ความหมายและแนวคิดไปตามทิศทางของตนเอง ผู้ก่อการร้ายในมุมมองของประเทศหนึ่ง มองแตกต่างกับอีกประเทศหนึ่ง ที่มองว่าเป็นนักต่อสู้เพื่ออิสรภาพก็เป็นได้ การกระทำของการก่อการร้ายก็จะมีการแสดงออกที่แตกต่างกัน

3. นโยบายการต่อต้านการก่อการร้ายของประเทศมีความแตกต่างกันในการปฏิบัติต่อการกระทำของผู้ก่อการร้าย นโยบายของแต่ละประเทศจะตอบโต้ต่อการกระทำของผู้ก่อการร้ายในขั้นสูงสุดหรือต่อต้านการก่อการร้ายอย่างเปิดเผย แต่บางประเทศเลือกที่จะติดต่อหรือวางตัวเป็นกลางกับผู้ก่อการร้ายหรือองค์กรก่อการร้ายซึ่งอาจมีผลประโยชน์ร่วมกัน

4. ประเทศไทยปกครองแบบเสรีประชาธิปไตยการให้เสรีภาพไม่ว่าจะด้านใดๆ เป็นผลให้สิทธิเสรีภาพของประชาชนไม่มีขีดจำกัด โดยเฉพาะเสรีภาพทางสื่อ สื่อสารมวลชนเป็นตัวกลางในการนำเสนอข่าวสารความเป็นจริงให้กับประชาชน หากสื่อมีอิสระสูงก็อาจเป็นเครื่องมือที่ชี้นำให้ประชาชนหรือการนำเสนอข่าวสารบางอย่าง หากเอนเอียงไปในทางใดทางหนึ่งก็อาจเป็นเครื่องมือต่อผู้ก่อการร้ายในการรู้ถึงความเคลื่อนไหวและตอบโต้รัฐได้ง่ายขึ้น ประเด็นที่ต้องพิจารณาคือ ความพอดีของการกระจายสื่อและการควบคุมสื่อของรัฐบาล หากให้อิสระมากเกินไปก็เกินความพอดี หรือหากควบคุมมากเกินไปก็ไม่สามารถเป็นตัวกลางในการนำเสนอข่าวสารได้อย่างแท้จริง

5. ประเทศไทยให้ประชาชนมีสิทธิเสรีภาพมากตามระบอบประชาธิปไตย เมื่อรัฐพยายามจะสร้างแนวทางหรือระบบการรักษาความปลอดภัยและความมั่นคงภายในรัฐ และต่อต้านการก่อการร้าย หากว่ารัฐจะดำเนินการด้านการรักษาความปลอดภัยโดยการจัดระบบรักษาความปลอดภัยที่จะต่อต้านและตอบโต้การก่อการร้ายอย่างจริงจัง ออกกฎระเบียบเพื่อช่วยในการสืบติดตาม เสาะหา ในเรื่องของการข่าวและการตอบโต้ผู้ก่อการร้าย ก็ถือได้ว่าเป็นการนำไปสู่การละเมิดสิทธิเสรีภาพของประชาชน การกระทำอันนำไปสู่การละเมิดสิทธิเสรีภาพ

6. เครื่องมือทางไซเบอร์ที่นำมาใช้ในการก่อการร้ายในปัจจุบัน คือ โทรศัพท์มือถือ แท็บเล็ต คอมพิวเตอร์ หรืออุปกรณ์ที่สามารถเชื่อมต่ออินเทอร์เน็ตได้และสามารถใช้งานได้ทุกที่อย่างสะดวกและรวดเร็ว การเชื่อมต่ออินเทอร์เน็ตที่มีความเร็วสูงและมีระบบปฏิบัติการที่มีประสิทธิภาพจะช่วยการปฏิบัติการได้อย่างมีประสิทธิภาพ นอกจากนี้ ประเด็นสำคัญที่ค้นพบคือ การใช้สังคมออนไลน์ทั้ง ผู้ส่งสาร(Messengers) ไลน์ทวิสเตอร์เป็นต้น เพื่อใช้ในการติดต่อสื่อสารกันทั่วโลกและใช้เป็นช่องทางในการเผยแพร่แนวคิด วิดีโอ เพื่อให้เกิดความเชื่อต่อบุคคล ต่อสมาชิกในกลุ่มหรือเชื่อมโยงไปดึง ปลุกระดมคนเพื่อนำมาสู่การก่อการร้ายได้

7. การก่อการร้ายทางไซเบอร์ เป็นการกระทำที่ก่อให้เกิดความเสียหาย ก่อให้เกิดความหวาดกลัว ตื่นตระหนกโดยมีการนำไซเบอร์มาเป็นเครื่องมือในการก่อการร้าย โดยมีเหตุจูงใจทางการเมืองเป็นสำคัญ สิ่งที่ค้นพบคือ ประเทศไทยยังไม่มีสถานการณ์หรือมูลเหตุจูงใจที่นำไปสู่การก่อการร้ายทางไซเบอร์ ส่วนใหญ่เป็นการกระทำของแฮกเกอร์ เช่น การปิดและเปลี่ยนหน้าเว็บไซต์ของหน่วยงานราชการ ธนาคารหรือสถาบันทางการเงินเป็นสัญลักษณ์ของกลุ่ม เพื่อแสดงออกถึงความสนุกสนาน ความพอใจ ทำให้เป็นที่รู้จักว่ามีศักยภาพในด้านนี้

8.ในการจัดการปัญหาของการก่อการร้าย ในแต่ละประเทศความท้าทายของการดำเนินการคือ การหยุดยั้งการก่อการร้ายหรือการลดหรือควบคุมไม่ให้เกิดลัทธิ องค์การก่อการร้ายเพิ่มมากขึ้นได้อย่างไร สิ่งสำคัญคือการวางยุทธศาสตร์ที่เหมาะสมต่อการดำเนินการในการจัดการปัญหาในแต่

ละรัฐ ด้านการศึกษาบริบทของแต่ละประเทศที่แตกต่างกัน และการให้คำนิยามหรือความหมายของแต่ละประเทศ นโยบายการจัดการปัญหาภายในประเทศ และวิธีการที่จะบรรลุผลในการกระทำ การมีและใช้ทรัพยากรความเชื่อมต่อระหว่างนโยบายและการปฏิบัติ ยุทธศาสตร์การใช้กองกำลัง มิติทางยุทธการการปฏิบัติการ ยุทธวิธีและเทคนิคต่าง ๆ เพื่อให้การก่อการร้ายลดน้อยลง

9. การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย จากการวิจัยสิ่งที่ค้นพบคือ ประเทศไทยมีการตื่นตัวและตระหนักในความสำคัญของการต่อต้านการก่อการร้ายทางไซเบอร์ แต่มีการดำเนินการแบบแยกส่วน มีหน่วยงานที่ให้ความตระหนักต่อความปลอดภัยทางไซเบอร์คือ หน่วยทหาร ตำรวจและหน่วยงานของภาคเอกชน รวมทั้งหน่วยงานบางส่วนที่เกี่ยวข้องกับการเงิน เช่น ธนาคารพาณิชย์ต่างๆ สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์แห่งประเทศไทย (ก.ล.ต.)เป็นต้น

10. แนวโน้มการก่อการร้ายในอนาคตจะใช้เครื่องมือและอาวุธที่หลากหลายโดยเฉพาะอุปกรณ์ที่สามารถหาได้ง่าย มีราคาถูก และก่อให้เกิดผลสัมฤทธิ์ได้อย่างดีเยี่ยม การใช้เทคโนโลยีเข้ามาช่วยในการผลิตและเผยแพร่ข้อมูลข่าวสารในการก่อการร้าย การผลิตอาวุธที่มาทำลายล้าง การใช้สารพิษที่หาซื้อได้ง่าย การใช้อาวุธนิวเคลียร์ ถ้าหากมีโอกาสอันเหมาะสมก็จะใช้ยุทธวิธีแบบเดิมไม่ว่าจะเป็นการลอบวางระเบิดการปล้นยึดยานโดยสาร การลักพาตัว การข่มขู่ การลอบสังหาร การบุกโจมตีด้วยอาวุธ การจับตัวประกัน การซุ่มยิง การกระทำต่อเป้าหมายจะไม่เลือกหรือคำนึงศีลธรรมประชาชนทั่วไปสามารถเป็นเป้าหมายของการก่อการร้ายได้ทั้งหมด และทันทีเพื่อหวังผลในการสร้างความหวาดกลัวและมีผลในวงกว้าง

11. การใช้ไซเบอร์มาเป็นเครื่องมือในการก่อการร้ายมีประสิทธิภาพร้ายแรง แฮกเกอร์ที่มีความรู้และผู้เชี่ยวชาญด้านคอมพิวเตอร์จะเพิ่มขีดความสามารถให้กับกลุ่มผู้ก่อการร้าย เมื่อกลุ่มผู้ก่อการร้ายคิดค้นวิธีการใหม่ ยุทธศาสตร์การต่อต้านการก่อการร้ายจะต้องปรับตัวตาม การลงโทษสถานเบาอาจไม่เพียงพอต่อความผิดของผู้ก่อการร้าย การเปลี่ยนแปลงที่สำคัญของยุทธศาสตร์การต่อต้านการก่อการร้ายในอนาคตจะไม่เกี่ยวข้องเพียงการบุกทลายหรือการตรวจสอบโทรศัพท์มือถือแต่จะมุ่งเน้นที่การลดทอนความเสี่ยงของประชากรที่ใช้เทคโนโลยีในชีวิตประจำวัน

12. ประเทศไทยยังไม่มีกฎหมายและระเบียบต่างๆ ที่เกี่ยวข้องกับไซเบอร์ โดยเฉพาะกฎหมายและระเบียบที่จำเป็นในยุคของโลกไซเบอร์สเปซ โดยเฉพาะการกล่าวถึงการก่อการร้ายทางไซเบอร์ รวมทั้งการป้องกันหรือต่อต้านการก่อการร้ายทางไซเบอร์อย่างชัดเจนเกี่ยวกับการปกป้องข้อมูลส่วนบุคคล การป้องกันทรัพย์สินทางปัญญา ความปลอดภัยทางไซเบอร์ การป้องกันหรือกฎหมายที่เกี่ยวกับอาชญากรรมทางไซเบอร์ รวมถึงกฎหมายทั้งพหุภาคีและทวิภาคี ความร่วมมือกับต่างประเทศ รวมถึงประเทศในอาเซียนในเรื่องการป้องกันการก่อการร้ายทางไซเบอร์

ประเทศไทยยังไม่มีกฎหมายเฉพาะในเรื่องของการปกป้องข้อมูลส่วนบุคคล และกฎหมายที่เกี่ยวข้องกับอาชญากรรมและ การต่อต้านหรือป้องกันการก่อการร้ายทางไซเบอร์ ซึ่งมีความจำเป็นอย่างยิ่ง ต่อโลกในศตวรรษที่ 21 นี้ อีกทั้งยังต้องเพิ่มการกำหนดแนวทางปฏิบัติที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศ เช่น การใช้เทคโนโลยีคลาวด์ สื่อสังคมออนไลน์ และการจัดการข้อมูลจำนวนมหาศาล ก็ยังไม่ชัดเจนในแนวทางปฏิบัติ

สอดคล้องกับข้อมูลเชิงปริมาณในประเด็นลักษณะการก่อการร้ายทางไซเบอร์และนำมาเป็นเครื่องมือทางยุทธศาสตร์ในการก่อการร้ายกลุ่มตัวอย่างมีความคิดเห็นในระดับมาก โดยมีค่าเฉลี่ย 3.82 ส่วนเบี่ยงเบนมาตรฐาน0.56 เมื่อพิจารณาเป็นรายข้อพบว่าระดับความคิดเห็นสูงสุด 3อันดับแรกคือ 1. กลุ่มตัวอย่างมีความคิดเห็นสูงที่สุด คือ การป้องกันทางไซเบอร์ของประเทศไทยต้องเกิดจากความร่วมมือกันระหว่างหน่วยงาน ทั้งภาครัฐ เอกชน และประชาชนทั้งประเทศ มีความคิดเห็นในระดับมาก โดยมีค่าเฉลี่ย 3.97 ส่วนเบี่ยงเบนมาตรฐาน 0.83 2.ข้อที่กลุ่มตัวอย่างมีความคิดเห็นสูงเป็นอันดับที่สอง คือ การก่อการร้ายทางไซเบอร์เป็นการใช้เครื่องมือทางเทคโนโลยี เช่น โทรศัพท์มือถือ คอมพิวเตอร์หรือเครื่องมือประเภทอื่น ๆ ที่เชื่อมต่อทางอินเทอร์เน็ตเพื่อการก่อการร้าย/อินเทอร์เน็ตเป็นช่องทางที่สำคัญที่ใช้ในการก่อการร้าย เช่น ลักลอบขโมยข้อมูลข่าวสารเพื่อมุ่งเป้าทางการเมือง ปล่อยไวรัสเพื่อทำลายระบบต่าง ๆ มีความคิดเห็นในระดับมากโดยมีค่าเฉลี่ย 3.90 เท่ากัน ส่วนเบี่ยงเบนมาตรฐาน 0.76 และ 0.81 ตามลำดับและ 3. กลุ่มตัวอย่างมีความคิดเห็นสูงเป็นอันดับที่สาม คือ กฎหมายที่เกี่ยวกับไซเบอร์ เพื่อดูแล ป้องกัน และควบคุมการดำเนินการทางไซเบอร์ยังไม่ครอบคลุมและบังคับใช้อย่างแท้จริงมีความคิดเห็นในระดับมาก โดยมีค่าเฉลี่ย 3.89 ส่วนเบี่ยงเบนมาตรฐาน 0.88

การพัฒนายุทธศาสตร์การต่อต้านการก่อการร้ายในประเทศไทยนำเสนอยุทธศาสตร์ในการต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย ดังนี้

ยุทธศาสตร์ READ: CLIP ประกอบด้วย

ยุทธศาสตร์ที่ 1Research ยุทธศาสตร์การเสริมสร้างการวิจัยเพื่อการพัฒนาทางไซเบอร์

ยุทธศาสตร์ที่ 2Education ยุทธศาสตร์การจัดการศึกษาในการสร้างพื้นฐานของประชาชนในประเทศไทย

ยุทธศาสตร์ที่ 3Awareness ยุทธศาสตร์การสร้างการตระหนักรู้ทางไซเบอร์ให้กับประชาชน

ยุทธศาสตร์ที่ 4Development ยุทธศาสตร์การพัฒนาความก้าวหน้าทางไซเบอร์

ยุทธศาสตร์ที่ 5 Coordinate ยุทธศาสตร์การส่งเสริมความร่วมมือระหว่างภาครัฐ ภาคเอกชน และภาคประชาชน

ยุทธศาสตร์ที่ 6Law ยุทธศาสตร์การกำหนดใช้กฎหมายทางไซเบอร์และการบังคับใช้กับประชาชน

ยุทธศาสตร์ที่ 7 Integration ยุทธศาสตร์การใช้บูรณาการร่วมกันเพื่อแบ่งปันข้อมูล

ยุทธศาสตร์ที่**8**Perception Prepares and Protect ยุทธศาสตร์การรับรู้ทางไซเบอร์ร่วมกันตระเตรียมและปกป้องทางไซเบอร์

ยุทธศาสตร์ที่ 1 Research ยุทธศาสตร์การเสริมสร้างงานวิจัยเพื่อการพัฒนาทางไซเบอร์ (ST)

วัตถุประสงค์

1. เพื่อให้มีการพัฒนาผลงานวิจัยทางไซเบอร์ให้เป็นที่ยอมรับในระดับชาติและนานาชาติ

กลยุทธ์

กลยุทธ์ที่ 1 พัฒนางานวิจัยทางไซเบอร์

แนวทางหรือมาตรการ

1. มีการส่งเสริมให้ประชาชน นักวิชาการ หรือภาคเอกชนมีความสนใจในประเด็นทางไซเบอร์และการก่อการร้ายทางไซเบอร์มากขึ้นให้ครอบคลุมทุกด้าน

2. สนับสนุนด้านงบประมาณด้านการวิจัยทางไซเบอร์เพื่อสร้างแรงจูงใจให้กับนักวิจัยทางไซเบอร์อย่างมีประสิทธิภาพ

ยุทธศาสตร์ที่ 2 Education ยุทธศาสตร์การจัดการศึกษาในการสร้างพื้นฐานของประชาชนในประเทศไทย (WT)

วัตถุประสงค์

1. เพื่อให้มีหลักสูตรการศึกษาทางไซเบอร์ตั้งแต่ระดับประถมศึกษา จนถึงระดับอุดมศึกษา

กลยุทธ์ที่ 1กลยุทธ์ที่ 1จัดทำหลักสูตรเฉพาะเกี่ยวกับไซเบอร์

กลยุทธ์ที่ 2 ติดตามและประเมินผลหลักสูตรทางไซเบอร์ เพื่อนำมาพัฒนาหลักสูตรทุก 5 ปี

แนวทางหรือมาตรการ

1. กำหนดหลักสูตรที่เกี่ยวกับไซเบอร์ในทุกระดับเพื่อให้เยาวชนได้มีรากฐานของการศึกษาและเข้าใจต่อการใช้ไซเบอร์อย่างถูกต้อง

2. พัฒนาหลักสูตรในระดับอุดมศึกษาเพื่อพัฒนาองค์ความรู้ทางไซเบอร์ให้สามารถนำความรู้ไปใช้อย่างครอบคลุมและมีประสิทธิภาพในทุก ๆ ด้าน

ยุทธศาสตร์ที่ 3 Awareness ยุทธศาสตร์การสร้างการตระหนักรู้ทางไซเบอร์ให้กับประชาชน (WO)
วัตถุประสงค์

1.เพื่อให้ประชาชนมีความรู้ความเข้าใจต่อการใช้ไซเบอร์ จนสามารถสร้างการป้องกันให้กับตนเองได้

กลยุทธ์ที่ 1 ส่งเสริมให้หน่วยงานภาครัฐ ภาคเอกชนการสร้างการตระหนักรู้ทางไซเบอร์

กลยุทธ์ที่ 2 จัดทำโครงการทางไซเบอร์โดยสร้างความร่วมมือจากทุกภาคส่วนเพื่อสร้างความตระหนักรู้ให้กับประชาชน

แนวทางหรือมาตรการ

1. สนับสนุนให้ประชาชนมีการสร้างความรู้ ความเข้าใจที่ดีต่อการใช้ไซเบอร์ รวมทั้งมีการถ่ายทอดความรู้ ความเข้าใจที่ดีต่อการใช้ไซเบอร์ รวมทั้งมีการถ่ายทอดความรู้ความเข้าใจจากรุ่นไปสู่รุ่น

2. เผยแพร่ความรู้และประชาสัมพันธ์ให้ประชาชนมีการใช้ไซเบอร์รวมทั้งตระหนักถึงการใช้ไซเบอร์อย่างถูกต้องเพื่อป้องกันการนำมาเป็นเครื่องมือในการก่อการร้าย

ยุทธศาสตร์ที่ 4 Development ยุทธศาสตร์การพัฒนาความก้าวหน้าทางไซเบอร์ (WO)
วัตถุประสงค์

1. เพื่อให้หน่วยงานทุกภาคส่วน รวมทั้งภาคประชาชนมีส่วนในการพัฒนาความก้าวหน้าทางไซเบอร์ในทุกด้าน

กลยุทธ์ที่ 1 ส่งเสริมให้หน่วยงานภาครัฐ ภาคเอกชนการสร้างการตระหนักรู้ทางไซเบอร์

กลยุทธ์ที่ 2 จัดทำโครงการทางไซเบอร์โดยสร้างความร่วมมือจากทุกภาคส่วนเพื่อสร้างความตระหนักรู้ให้กับประชาชน

แนวทางหรือมาตรการ

1. มีการจัดตั้งหน่วยงานการพัฒนาทางไซเบอร์เพื่อพัฒนาระบบสารสนเทศและการรักษาความปลอดภัยทางไซเบอร์ข้อมูลข่าวสาร

2. จัดฝึกอบรมให้ความรู้ สนับสนุนการจัดสอบเพื่อให้บุคลากรผ่านเกณฑ์มาตรฐานสากล สนับสนุนการวิจัยสร้างองค์ความรู้ใหม่ทางไซเบอร์

3. พัฒนาบุคลากรให้มีความเชี่ยวชาญในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ รวมทั้งสร้างแรงจูงใจในการจงรักภักดีและทำงานเพื่อประเทศชาติเพื่อป้องกันสมองไหลไปยังต่างประเทศ

ยุทธศาสตร์ที่ 5 Coordinate ยุทธศาสตร์การส่งเสริมความร่วมมือระหว่างภาครัฐ ภาคเอกชน และภาคประชาชน (SO)

วัตถุประสงค์

1. เพื่อให้หน่วยงานทุกภาคส่วน รวมทั้งภาคประชาชนมีความร่วมมือป้องกันทางไซเบอร์อย่างเป็นรูปธรรม

กลยุทธ์ที่ 1 สร้างหรือพัฒนาให้มีองค์กรหน่วยงานที่เป็นแกนกลางในการร่วมมือกันทุกภาคส่วน

กลยุทธ์ที่ 2 ส่งเสริมให้องค์กรทุกภาคส่วนที่มีส่วนเกี่ยวข้องทางไซเบอร์ ปฏิบัติงานในทิศทางเดียวกัน

กลยุทธ์ที่ 3 สร้างระบบการพัฒนาข้าราชการและบุคลากรส่วนงานไซเบอร์ให้มีศักยภาพในการปฏิบัติงานอย่างเป็นระบบ

แนวทางหรือมาตรการ

1. มีการเสริมสร้างความเข้าใจร่วมกันในการกำหนด นิยาม ความหมายของไซเบอร์ การก่อการร้ายและการก่อการร้ายทางไซเบอร์

2. มีการกำหนดนโยบาย แนวทางและแผนปฏิบัติการที่ชัดเจนเพื่อให้เกิดการแปลงแผนไปสู่กลยุทธ์และไปสู่การปฏิบัติตามวิสัยทัศน์ พันธกิจและเป้าประสงค์ที่กำหนดไว้อย่างมีประสิทธิภาพ

3. กำหนดกลไกในการทบทวน ติดตาม และประเมินความเสี่ยงต่อการนำแผนไปปรับใช้เพื่อปรับแนวทางให้มีความเหมาะสมตามสถานการณ์ใหม่หรือสถานการณ์ที่แตกต่าง

ยุทธศาสตร์ที่ 6 Law ยุทธศาสตร์การกำหนดใช้กฎหมายทางไซเบอร์และการบังคับใช้กับประชาชน (WT)

วัตถุประสงค์

1. เพื่อให้มีกฎหมายไซเบอร์ของประเทศไทยบังคับใช้อย่างเป็นรูปธรรม

กลยุทธ์ที่ 1 มีการพัฒนากฎหมายไซเบอร์และไซเบอร์ ความมั่นคงทางไซเบอร์และการต่อต้านการก่อการร้ายทางไซเบอร์อย่างครอบคลุม

กลยุทธ์ที่ 2 กำหนดแนวทางที่ชัดเจนต่อการบังคับใช้กฎหมาย พร้อมทั้ง มาตรการ, บทลงโทษต่อการกระทำอันเกี่ยวข้องกับก่อการร้าย

แนวทางหรือมาตรการ

1. กำหนดกฎหมาย กฎระเบียบ ขั้นตอน ที่เกี่ยวข้องกับการใช้ไซเบอร์, ความมั่นคงทางไซเบอร์และการต่อต้านการก่อการร้ายทางไซเบอร์อย่างครอบคลุม

2. กำหนดแนวทางที่ชัดเจนต่อการบังคับใช้กฎหมาย พร้อมทั้ง มาตรการ, บทลงโทษต่อการกระทำอันเกี่ยวข้องกับก่อการร้าย

ยุทธศาสตร์ที่ 7 Integration ยุทธศาสตร์การใช้การบูรณาการร่วมกันเพื่อแบ่งปันข้อมูล (SO)

วัตถุประสงค์

1. เพื่อให้มีระบบข้อมูลกลางเพื่อแบ่งปันข้อมูลข่าวสาร

กลยุทธ์ที่ 1สร้างระบบข้อมูลกลาง

แนวทางหรือมาตรการ

1. จัดตั้งหน่วยงานกลาง มีหน้าที่ในการดูแล ดำเนินการทางด้านไซเบอร์ มีการแบ่งปันข้อมูลร่วมกันเพื่อประโยชน์ของประชาชน รวมทั้งมีการบูรณาการการทำงานร่วมกัน อีกทั้งระบุโอกาส และความท้าทายในการเพิ่มขีดความสมารถของกลไกการตอบสนองต่อการร้าย

2. สร้างฐานข้อมูลกลางเพื่อรวบรวมข้อมูลสำคัญจากทุกภาคส่วน รวมทั้งมีการควบคุมดูแลเพื่อไม่ให้ข้อมูลถูกเผยแพร่ เปิดโอกาสให้ทุกหน่วยงานที่เกี่ยวข้องกับไซเบอร์สามารถดึงข้อมูลไปใช้ในทางที่ถูกต้อง

3. จัดตั้งศูนย์ข่าวกรองทางไซเบอร์ เพื่อทำงานด้านการข่าวทางไซเบอร์, แบ่งปันข้อมูลข่าวสาร และประสานงานความร่วมมือระหว่างหน่วยงาน

ยุทธศาสตร์ที่ 8 Perception Prepares and Protect ยุทธศาสตร์การรับรู้ทางไซเบอร์ร่วมกันตระเตรียม และปกป้องทางไซเบอร์ (ST)

วัตถุประสงค์

1. เพื่อให้ประชาชนเกิดการรับรู้ร่วมกันตระเตรียมและป้องกันทางไซเบอร์

กลยุทธ์ที่ 1พัฒนาและเสริมสร้างความรู้เรื่องไซเบอร์ที่เหมาะสมและจำเป็นกับประชาชน

กลยุทธ์ที่ 2 เสริมสร้างจิตสำนึกและแนวทางการป้องกันตนเองเพื่อให้เกิดการป้องกันตนเอง

แนวทางหรือมาตรการ

1. ปลูกฝังทัศนคติและแนวทางการใช้ไซเบอร์ที่เป็นรูปธรรมเพื่อให้ประชาชนมีการรับรู้ต่อการใช้ไซเบอร์ในทางที่ถูกต้อง

2. สร้างการมีส่วนร่วมของประชาชน รวมทั้งวิธีการในการตระเตรียมตนเองเพื่อให้เกิดการปฏิบัติอย่างรู้เท่าทัน

3. สร้างมุมมองต่อการสอดส่องดูแลและป้องกันที่ดีในการดำรงชีวิตประจำวัน ให้มีภูมิคุ้มกันตนเองต่อการใช้ไซเบอร์

ระดับความคิดเห็นต่อประเด็นยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย ดังนี้

โดยภาพรวมพบว่า กลุ่มตัวอย่างมีความคิดเห็นในระดับมากโดยมีค่าเฉลี่ย 3.96 ส่วนเบี่ยงเบนมาตรฐาน 0.67 เมื่อพิจารณาเป็นรายประเด็น พบว่า ข้อที่มีระดับความคิดเห็นสูงเรียงลำดับลงไปน้อยที่สุด คือ1. กลุ่มตัวอย่างมีความคิดเห็นสูงที่สุด คือCoordinate ยุทธศาสตร์การส่งเสริมความร่วมมือระหว่างภาครัฐ ภาคเอกชน และภาคประชาชนมีความคิดเห็นในระดับมาก โดยมีค่าเฉลี่ย 4.02 ส่วนเบี่ยงเบนมาตรฐาน 0.85 กลุ่มตัวอย่างมีความคิดเห็นรองลงมาคือ Development ยุทธศาสตร์การพัฒนาความก้าวหน้าทางไซเบอร์ มีความคิดเห็นในระดับมาก โดยมีค่าเฉลี่ย 4.00 ส่วนเบี่ยงเบนมาตรฐาน 0.80 กลุ่มตัวอย่างมีความคิดเห็นเป็นอันดับที่สามคือ Research ยุทธศาสตร์การเสริมสร้างงานวิจัยเพื่อการพัฒนาทางไซเบอร์ มีความคิดเห็นในระดับมาก โดยมีค่าเฉลี่ย 3.98 ส่วนเบี่ยงเบนมาตรฐาน 0.79 กลุ่มตัวอย่างมีความคิดเห็นเป็นอันดับที่สี่คือ Education ยุทธศาสตร์การจัดการศึกษาในการสร้างพื้นฐานของประชาชนในประเทศไทย มีความคิดเห็นในระดับมากโดยมีค่าเฉลี่ย 3.97 ส่วนเบี่ยงเบนมาตรฐาน 0.81 กลุ่มตัวอย่างมีความคิดเห็นเป็นอันดับที่ห้าคือ Awareness ยุทธศาสตร์การสร้างการตระหนักรู้ทางไซเบอร์ให้กับประชาชน มีความคิดเห็นในระดับมาก โดยมีค่าเฉลี่ย 3.95 ส่วนเบี่ยงเบนมาตรฐาน 0.83 กลุ่มตัวอย่างมีความคิดเห็นเป็นอันดับที่หกคือ Integration ยุทธศาสตร์การใช้การบูรณาการร่วมกันเพื่อการแบ่งปันข้อมูล มีความคิดเห็นในระดับมาก โดยมีค่าเฉลี่ย 3.93 ส่วนเบี่ยงเบนมาตรฐาน 0.84 กลุ่มตัวอย่างมีความคิดเห็นเป็นอันดับที่เจ็ดคือ Perception Prepares and Protect ยุทธศาสตร์การรับรู้ทางไซเบอร์ร่วมกัน ตระเตรียมและปกป้องทางไซเบอร์ มีความคิดเห็นในระดับมาก โดยมีค่าเฉลี่ย 3.92 ส่วนเบี่ยงเบนมาตรฐาน 0.92 และกลุ่มตัวอย่างมีความคิดเห็นน้อยที่สุดคือ Law ยุทธศาสตร์การกำหนดใช้กฎหมายทางไซเบอร์และการบังคับใช้กับประชาชน มีความคิดเห็นในระดับมาก โดยมีค่าเฉลี่ย 3.88 ส่วนเบี่ยงเบนมาตรฐาน 0.89

การอภิปรายผลการวิจัย

การวิจัยเรื่องยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ ผลการศึกษาดังนี้ ความก้าวหน้าทางไซเบอร์ รูปแบบการก่อการร้ายทางไซเบอร์ โอกาสการก่อการร้ายทางไซเบอร์ในประเทศไทย เครื่องมือทางไซเบอร์ที่นำมาใช้ในการก่อการร้ายในประเทศไทย การก่อการร้ายทางไซเบอร์ การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย ยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย ประกอบด้วย

วิสัยทัศน์

ประเทศไทยมีศักยภาพในการสร้างภูมิคุ้มกันป้องกัน และร่วมกันต่อต้านการก่อการร้ายทางไซเบอร์

พันธกิจ

สร้างฐานความรู้ทางไซเบอร์ให้กับประชาชนทุกระดับพร้อมทั้งมุ่งพัฒนาความเข็มแข็งทางไซเบอร์เพื่อความมั่นคงของประเทศไทย

เป้าประสงค์

เพื่อพัฒนาและเสริมสร้างความมั่นคงทางไซเบอร์ให้กับประเทศไทย

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

ยุทธศาสตร์ที่ 8 Perception Prepares and Protect ยุทธศาสตร์การรับรู้ทางไซเบอร์ร่วมกันตระเตรียมและปกป้องทางไซเบอร์

จากการก่อการร้ายทางไซเบอร์ในประเทศไทยโดยใช้การวิเคราะห์จุดแข็ง จุดอ่อน โอกาส และอุปสรรควิธีการวิเคราะห์สถานการณ์และองค์การแห่งการเรียนรู้ เกิดข้อค้นพบที่นำมาอภิปรายดังนี้

1.ความก้าวหน้าทางไซเบอร์เป็นเทคโนโลยีที่มีอินเทอร์เน็ตเพื่อเชื่อมต่อการสื่อสารได้ทุกที่ทุกเวลาไม่ว่าจะอยู่ที่ใดบนโลก สะดวก รวดเร็วและไซเบอร์มีความสำคัญต่อการดำรงชีวิตของมนุษย์ โดยมีเครื่องมือที่ใช้ในการติดต่อสื่อสารเช่น คอมพิวเตอร์ โทรศัพท์มือถือหรือ แท็บเล็ต เป็นต้น สอดคล้องกับ หนังสือ Globalization ของ Malcolm Waters (2001) กล่าวว่า การอธิบายปรากฏการณ์ที่เชื่อมโยงสังคมและรัฐชาติเข้าไว้ด้วยกันทั่วโลก ความเป็นสากลนิยมการติดต่อสื่อสารที่เชื่อมต่อถึงกันโดยทั่วและการกระทำเหตุการณ์ที่ส่งผลกระทบหรือการร่วมมือของคนทั้งโลก ในความเป็นโลกาภิวัตน์ในศตวรรษที่ 21 นี้การนำเทคโนโลยีที่มีประสิทธิภาพและการ

สร้างเครือข่ายทางสังคม ทำให้โลกเปรียบเป็นโลกเสมือน สามารถเจอกันได้ รับรู้ความเคลื่อนไหว และสามารถเข้าถึงทุกมุมทั่วโลก โลกาภิวัตน์เป็นระบบวัฒนธรรมโลกที่พัฒนาขึ้นเพื่อตอบสนอง และเอื้ออำนวยต่อการเกิดขึ้นของระบบผูกขาดไร้พรมแดนเพื่อให้คนทั้งโลกขึ้นต่อวัฒนธรรมที่เรียกว่า Neo – westernization ที่เป็นการสร้างกระแสบริโภคนิยมทุกอย่างเป็นอเมริกา หรือญี่ปุ่น การเกิดกระแสบริโภคนิยมและการตามกระแสนั้นเป็นการรุกรานความเป็นท้องถิ่นและประเพณีดั้งเดิมของคนในพื้นที่ต่างๆ ของโลก และส่งผลกระทบในกลุ่มชาตินิยม ประเพณีนิยมและศาสนานิยม ส่งผลให้เกิดความไม่พอใจในกลุ่มมุสลิมหัวรุนแรงได้เนื่องจากกระแสโลกาภิวัตน์ จึงสามารถสรุปได้ว่า ความก้าวหน้าทางไซเบอร์ เป็นเทคโนโลยีที่เชื่อมต่อการสื่อสารได้ทุกที่ทุกเวลาไม่ว่าจะอยู่ที่ใดบนโลกสะดวก รวดเร็ว โดยมีเครื่องมือเพื่อการติดต่อสื่อสารเช่น คอมพิวเตอร์ โทรศัพท์มือถือหรือ แท็บเล็ต เป็นต้น ความก้าวหน้านี้ส่งผลให้ความเป็นโลกาภิวัตน์ในศตวรรษที่ 21 มีการนำเทคโนโลยีที่มีประสิทธิภาพและนำมาสร้างเครือข่ายทางสังคม ทำให้โลกเปรียบเป็นโลกเสมือนและการตามกระแสวัฒนธรรมบริโภคนิยมนำมาซึ่งความไม่พอใจของกลุ่มชาตินิยมเคร่งศาสนาและกลุ่มมุสลิมหัวรุนแรง กระทำการก่อการร้ายเพื่อวัตถุประสงค์ให้เกิดความรุนแรงและการก่อการร้ายในรูปแบบใหม่ในอนาคต

2.การก่อการร้ายทางไซเบอร์ เป็นรูปแบบของการก่อการร้ายโดยมีการนำเทคโนโลยีสารสนเทศที่ทันสมัยนำมาเป็นเครื่องมือที่ช่วยให้กลุ่มก่อการร้ายสามารถดำเนินกิจกรรมต่าง ๆ ผู้ก่อการร้ายสามารถใช้ช่องทางนี้และผู้ใช้เทคโนโลยีสารสนเทศตกเป็นเป้าของการโจมตี (Cyber attack) เพื่อทำลายหรือขัดขวางการทำงานระบบเครือข่ายคอมพิวเตอร์แบบต่างๆ ไม่ว่าจะเป็นเครือข่ายการสื่อสารหรือเครือข่ายระบบคอมพิวเตอร์ที่เกี่ยวข้องกับการทำงานขององค์กรขนาดใหญ่ การควบคุมโครงสร้างพื้นฐาน หรือระบบโครงสร้างความมั่นคงทางทหาร หรือการล้วงข้อมูลความมั่นคงของประเทศ เป็นต้น โดยใช้วิธีการสร้างความเสียหาย ก่อให้เกิดความตื่นตระหนกต่อประชาชนและดึงดูดความสนใจของสื่อมวลชนหรือบุคคลต่าง ๆ ซึ่งคาดหมายว่า อนาคตจะมีการก่อการร้ายทางไซเบอร์ (Cyber Terrorism) และเป็นยุทธวิธีในการก่อการร้าย การก่อการร้ายทางไซเบอร์สอดคล้องกับ Whitman & Mattord (2005) กล่าวว่า การก่อการร้ายทางไซเบอร์เป็นภัยคุกคามรูปแบบหนึ่ง กล่าวคือ เป็นการก่อการร้ายผ่านระบบเครือข่ายหรือเครือข่ายอินเทอร์เน็ต สอดคล้องกับ FBI ได้ให้คำนิยามของ ผู้ก่อการร้ายทางไซเบอร์ไว้ว่า เป็นการโจมตีแบบไตร่ตรองไว้ก่อน ต่อระบบสารสนเทศโดยกลุ่มบุคคลหรือตัวแทนที่ไม่เปิดเผยนาม ที่มีเหตุจูงใจจากประเด็นทางการเมืองในส่วนของวิธีการก่อการร้ายทางไซเบอร์ มีวิธีการดังนี้ 1. ผู้ก่อการร้ายซึ่งต้องมีความรู้ทางไซเบอร์หรือเทคโนโลยี ศึกษาข้อมูลที่เกี่ยวกับเป้าหมายที่ต้องการจะกระทำ 2. สร้างหรือพัฒนาเครื่องมือให้ตรงกับความต้องการต่อเป้าหมาย เครื่องมือที่สำคัญของการก่อการร้ายทางไซเบอร์คือ

อินเทอร์เน็ต 3. ระดมคนหรือหาสมาชิกที่มีแนวความคิดแนวทางเดียวกัน 4. ระดมเงินทุนในการสนับสนุน 5. ปฏิบัติการตามวัตถุประสงค์ที่วางไว้เพื่อมุ่งเป้าหมายทางการเมือง สอดคล้องกับ Ashraf Gobran (2015) เรื่องภัยคุกคามของผู้ก่อการร้ายทางไซเบอร์ พบว่า กลุ่มผู้ก่อการร้ายเริ่มต้นการปรับให้เข้ากันและยึดเอาความได้เปรียบของเครื่องมือทางไซเบอร์และความสามารถของเครื่องมือทางไซเบอร์ การคุกคามผู้ก่อการร้าย จะกระทำเพื่อการเติบโตของกลุ่มร่วมกัน ถึงแม้ว่าผู้ก่อการร้ายจะไม่มีฝีมือต่อการฆ่าคนอย่างรวดเร็วโดยตรงกับการใช้เครื่องมือทางไซเบอร์ การประทุษร้ายหรือการขัดขวางทางสังคม การโจมตีสามารถเป็นเหตุพอดีกับวัตถุประสงค์การดำเนินการ

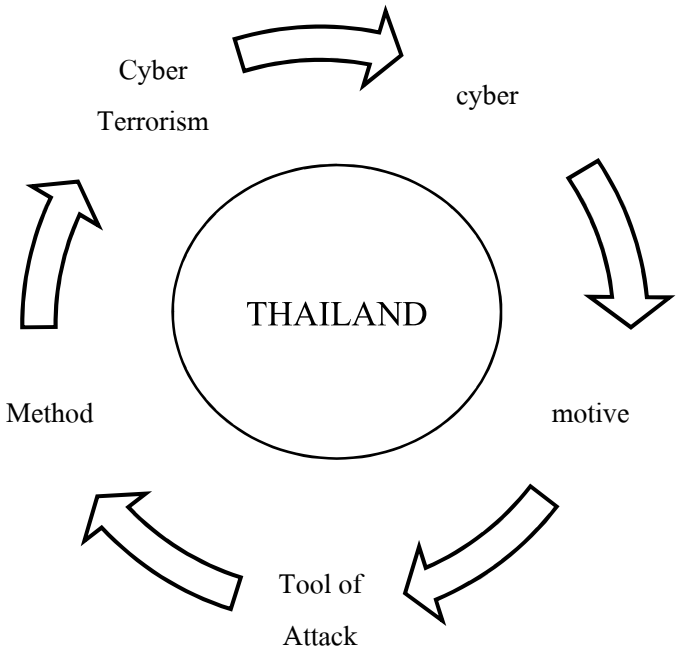
ปัจจัยที่เกี่ยวข้องกับแรงจูงใจและแสวงหาโอกาสในการก่อการร้ายทางไซเบอร์ด้วย ประเทศไทยเป็นประเทศเปิดเสรี เปิดรับนักท่องเที่ยวและมีนโยบายส่งเสริมให้เกิดการท่องเที่ยวในทุกที่โดยไม่มีข้อจำกัดส่วนใหญ่ผู้ก่อการร้ายจะใช้ประเทศไทยเป็นฐานในการเตรียมการก่อการร้ายไปยังประเทศที่สามหรือประเทศที่เป็นเป้าหมายมากกว่าและประเทศไทยไม่มีมาตรการในการป้องกันความปลอดภัยทางไซเบอร์ ประชาชนยังไม่มีการตระหนักรู้ต่อภัยคุกคามทางไซเบอร์ จึงทำให้มีการใช้อย่างไม่ระแวดระวังสอดคล้องกับจันทิมา เภาเจริญ (2550) วิจัยเรื่อง การก่อการร้ายสากลในเอเชียตะวันออกเฉียงใต้ ผลการวิจัยพบว่าแม้ประเทศไทยจะไม่ได้เกี่ยวข้องโดยตรงกับปัญหาและความขัดแย้งซึ่งเป็นสาเหตุของการก่อการร้ายสากล แต่กระนั้นการได้รับผลกระทบเป็นสิ่งที่ไม่อาจหลีกเลี่ยงได้ เพราะประเทศไทยมีความสัมพันธ์อันดีกับประเทศไทยที่เป็นเป้าหมายของการก่อการร้าย เช่นสหรัฐอเมริกา อิสราเอล ฯลฯ เนื่องจากว่าสถานทูต สถานกงสุล บริษัทการค้าและบริบทสายการบินต่าง ๆ ตั้งอยู่ในประเทศไทย ดังนั้นสถานที่เหล่านี้จึงเป็นเขตปริมณฑลในการปฏิบัติการก่อการร้ายแต่ยังไม่ใช่เป้าหมายในตัวของมันเอง ประเทศไทยจึงต้องร่วมมือไม่ว่าด้วยวิธีการใดกับประเทศต่าง ๆ ในการต่อต้านการก่อการร้าย เพราะการก่อการร้ายเป็นภัยคุกคามร่วมกันของชุมชนระหว่างประเทศ

ปัญหาที่สำคัญของการต่อต้านการก่อการร้ายเกิดจากแนวคิดของการก่อการร้าย ความหมาย และความไม่รู้ถึงความรุนแรงอันเกิดจากการก่อการร้ายของคนในประเทศใครคือผู้ก่อการร้าย และอะไรคือการก่อการร้าย เนื่องจากภัยการก่อการร้ายเป็นเรื่องไกลตัวและยังไม่มีการสร้างความตระหนักอย่างชัดเจน ดังนั้น มุมมองต่อการก่อการร้ายของแต่ละประเทศ มีการให้ความหมายและแนวคิดไปตามทิศทางของตนเอง สอดคล้องกับกมลนวล ศิลาพันธ์ (2556) วิจัยเรื่อง ความชัดเจนและความเหมาะสมในการกำหนดนิยามของการก่อการร้ายในประมวลกฎหมายอาญาของไทย พบว่า การบัญญัติความผิดฐานก่อการร้ายขึ้นใหม่ควรบัญญัติให้เป็นการกระทำความผิดอาญาที่โหดร้ายรุนแรง อันมีผลต่อการดำเนินชีวิตปกติสุขของประชาชนโดยทั่วไป จึงทำให้เกิด

ความรู้สึกหวาดกลัวและไม่ปลอดภัยของประชาชน อันเป็นวัตถุประสงค์หลักของผู้ก่อการร้าย การนิยามความหมายของการก่อการร้ายให้เป็นกลางเป็นที่ยอมรับทั่วไปอย่างเป็นสากลยังไม่สามารถทำได้ เพราะแต่ละประเทศยังยอมรับไม่ตรงกัน อีกทั้งคำนิยามของการก่อการร้ายระหว่างประเทศยังไม่ยุติบางประเทศเห็นว่าการต่อสู้เพื่ออิสรภาพไม่เป็นการก่อการร้ายระหว่างประเทศ ในขณะที่บางประเทศกลับเห็นว่า การกระทำดังกล่าวเป็นการก่อการร้ายระหว่างประเทศ สรุปได้ว่าการสร้างความเข้าใจต่อความหมาย การนิยามและการสร้างการตระหนักรู้ต่อการก่อการร้ายจึงเป็นสิ่งสำคัญที่ประชาชนไทยควรได้รับการส่งเสริม อีกทั้งในปัจจุบันประชาชนใช้ไซเบอร์เป็นเสมือนส่วนหนึ่งของชีวิตประจำวัน ซึ่งเป็นช่องทางหนึ่งที่เป็นช่องโหว่ของการนำมาซึ่งก่อการร้าย จึงต้องมีการส่งเสริมให้มีการสร้างความเข้าใจที่ถูกต้อง

การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย พบว่าประเทศไทยมีการตื่นตัวและตระหนักในเรื่องของการต่อต้านการก่อการร้ายทางไซเบอร์ แต่มีการดำเนินการแบบแยกส่วน มีหน่วยงานที่การตระหนักในความปลอดภัยทางไซเบอร์สอดคล้องกับดุสิต น้ำฝน (2549) วิจัยเรื่องการจัดตั้งองค์การชำนาญพิเศษเพื่อดำเนินการยุทธศาสตร์ต่อต้านการก่อการร้าย พบว่า เมื่อเกิดเหตุการณ์การก่อการร้ายในประเทศไทยในลักษณะที่มีความรุนแรงรวมถึงการก่อการร้ายรูปแบบใหม่ในอนาคต องค์การต่อต้านการก่อการร้ายจะไม่สามารถจัดการและปัญหาของโครงสร้างขององค์กรคือ องค์การมีสายการบังคับบัญชาและปฏิบัติตามคำสั่งองค์การสูงสุดเหนือขึ้นไป ต้องได้รับการอนุมิติในการเข้าจัดการกับปัญหาทุกครั้งและองค์การมีโครงสร้างหลวม บริหารงานยากขาดเอกภาพในการแก้ปัญหา อำนาจในการตัดสินใจและสั่งการด้านนโยบายไม่มีอิสระ สรุปได้ว่าประเทศไทยให้ความสำคัญต่อการก่อการร้ายในศตวรรษที่ 21 ที่มีความรุนแรงของการก่อการร้ายมากขึ้น โดยแนวทางหรือนโยบายของผู้บริหารที่มีทิศทางของการสร้างการตระหนักรู้ต่อภัยในการโจมตีของไซเบอร์ ประเด็นสำคัญคือการสร้างความชัดเจนหรือมีนโยบายต่อการดำเนินงานขององค์กรให้มีการดำเนินการไปในทิศทางเดียวกัน ลดปัญหาเรื่องระบบการทำงานที่มีระบบอุปถัมภ์การคอร์รัปชั่น สายการบังคับบัญชาที่มีมากจนเกิดความยุ่งยาก หากลดปัญหาเหล่านี้ได้จะทำให้การทำงานในการป้องกันหรือต่อต้านการก่อการร้ายมีประสิทธิภาพมากที่สุด

จากการวิจัยสรุปแนวคิดได้ดังนี้



ภาพที่ 12 Model 1: Circle of cyber Terrorism

Model 1 ผู้วิจัยได้พบว่า กระบวนการของการก่อการร้ายทางไซเบอร์เป็นนวัตกรรมที่เกิดขึ้นเป็นวัฏจักรของการก่อการร้ายทางไซเบอร์ ดังนี้

ลำดับแรก Cyber การพัฒนาของไซเบอร์ โลกไซเบอร์ (Cyber world) เป็นโลกของศตวรรษที่ 21 ที่ทุกคนเรียนรู้และก้าวตามความก้าวหน้าของไซเบอร์ในโลกของโลกาภิวัตน์ ไซเบอร์เป็นส่วนหนึ่งของเครือข่ายเชื่อมโยงตั้งแต่ระดับประเทศจนถึงระดับนานาชาติ ความรู้ที่เกี่ยวข้องกับเทคโนโลยี เครือข่ายคอมพิวเตอร์เป็นสิ่งที่จำเป็นกับมนุษย์ปัจจุบัน ความก้าวหน้าทางไซเบอร์คือเทคโนโลยีที่มีอินเทอร์เน็ต เพื่อเชื่อมต่อการสื่อสารของมนุษย์ให้สามารถติดต่อกันได้ทุกที่ทุกเวลาไม่ว่าจะอยู่ที่ใดบนโลก มีความสะดวก รวดเร็วและไซเบอร์ยังมีความสำคัญอย่างมากต่อการดำรงชีวิตของมนุษย์ในปัจจุบันและมากขึ้นเรื่อยๆ ในอนาคตข้างหน้า

ลำดับที่สอง Motive การนำไซเบอร์มาเป็นเครื่องมือในการก่อการร้ายจากปัจจัยที่เกี่ยวข้องกับแรงจูงใจในการก่อการร้ายทางไซเบอร์ดังนี้1.แรงจูงใจทางการเมือง 2.ศาสนาและอุดมการณ์ 3. แรงจูงใจทางการเงิน ประเทศไทยเป็นประเทศเปิดเสรี เปิดรับนักท่องเที่ยวและมีนโยบายส่งเสริมให้เกิดการท่องเที่ยวในทุกที่โดยไม่มีข้อจำกัด ดังนั้นจึงเป็นเหมือนสวรรค์ของผู้ก่อการร้าย อีกทั้งการส่งเสริมการเปิดใช้อินเทอร์เน็ตในทุกที่ ทำให้ประชาชนขาดการตระหนักรู้ในเรื่องของการใช้

ไซเบอร์ การก่อการร้ายทางไซเบอร์นั้นผู้ก่อการร้ายจะใช้เครื่องมือทางไซเบอร์ที่หาง่ายและใช้เครื่องมือได้ทุกที่ ไม่ว่าจะเป็นโทรศัพท์มือถือ แท็บเล็ต คอมพิวเตอร์ ที่สามารถเชื่อมต่ออินเทอร์เน็ตได้ทำให้คนเข้าถึงได้ง่ายและเชื่อง่ายขึ้น แรงจูงใจที่นำไซเบอร์มาก่อการร้าย เป็นเรื่องเงินเป็นสำคัญ รองลองมาเป็นเรื่องของแนวคิด อุดมการณ์ทางการเมืองหรือทางศาสนา หรือแม้แต่ความไม่พอใจต่อหน่วยงานหรือองค์กร แต่ปัจจัยที่สำคัญที่แตกต่างกันคือ แรงจูงใจที่สำคัญต่อการกระทำที่เป็นการก่อการร้ายจะต้องเป็นการกระทำที่มาจากแรงจูงใจทางเมืองเป็นสำคัญ จึงเห็นได้ว่าความเข้าใจในความหมายของการก่อการร้ายที่แตกต่างกัน นำไปสู่การอธิบายแรงจูงใจของการก่อการร้ายที่ต่างกันด้วย เมื่ออธิบายความเข้าใจแรงจูงใจการก่อการร้ายทางไซเบอร์ จึงไม่ได้มีการให้คำจำกัดความที่ชัดเจน

ลำดับที่สาม Tool of Attack โดยเครื่องมือที่ใช้ในการติดต่อสื่อสารประกอบด้วย คอมพิวเตอร์ โทรศัพท์มือถือ แท็บเล็ต(Tablet) หรืออุปกรณ์ที่สามารถเชื่อมต่ออินเทอร์เน็ตได้ และความก้าวหน้าทางไซเบอร์ต้องมีความความเร็วสูงเพื่อประโยชน์ในการเชื่อมต่อที่สะดวก รวดเร็ว มีระบบปฏิบัติการที่ดีและมีประสิทธิภาพและสามารถเข้าถึงได้ จากความก้าวหน้าทางไซเบอร์นำมาสู่การนำไซเบอร์มาใช้เป็นเครื่องมือในการโจมตีเครื่องมือทางไซเบอร์ที่นำมาใช้ในการก่อการร้ายในปัจจุบัน คือ โทรศัพท์มือถือ แท็บเล็ต คอมพิวเตอร์หรืออุปกรณ์ที่สามารถเชื่อมต่ออินเทอร์เน็ตได้และสามารถใช้งานได้ทุกที่ อย่างสะดวกและรวดเร็ว การเชื่อมต่ออินเทอร์เน็ตที่มีความเร็วสูงและมีระบบปฏิบัติการที่มีประสิทธิภาพจะช่วยการปฏิบัติการได้อย่างมีประสิทธิภาพ นอกจากนี้ ประเด็นสำคัญที่ค้นพบคือการใช้สังคมออนไลน์ทั้งกล่องข้อความ ไลน์ ทวิสเตอร์เป็นต้น รวมทั้งการใช้ การมีกลุ่มแฮกเกอร์เข้ามาโจมตีระบบได้ เช่นการจารกรรมข้อมูล การทำให้ระบบเครือข่ายคอมพิวเตอร์ไม่สามารถเข้าใช้งานได้ หรือการควบคุมและสั่งการไปยังเครื่องอื่นเพื่อปิดระบบ สร้างความเสียหายเพื่อใช้ในการติดต่อสื่อสารกันทั่วโลกและใช้เป็นช่องทางในการเผยแพร่แนวคิด วิดีโอเพื่อให้เกิดความเชื่อ ต่อบุคคล ต่อสมาชิกในกลุ่มหรือ เชื่อมโยงไปยังกลุ่ม ปลุกระดมคนเพื่อนำมาสู่การก่อการร้ายได้จากนั้นผู้ที่ไม่ประสงค์ดีจะมีวิธีการในการโจมตี

ลำดับที่สี่ Method การก่อการร้ายทางไซเบอร์กระทำได้โดยผู้ที่ไม่ประสงค์ดีใช้ไซเบอร์เป็นเครื่องมือในการก่อการร้าย มีลักษณะพิเศษต่างจากกลุ่มอื่นโดยจะต้องเป็นผู้เชี่ยวชาญหรือเป็นผู้รู้ทางด้านเทคโนโลยีหรือไซเบอร์ จึงจะสามารถปฏิบัติการได้ โดยมีวิธีดังนี้ วิธีการก่อการร้ายทางไซเบอร์

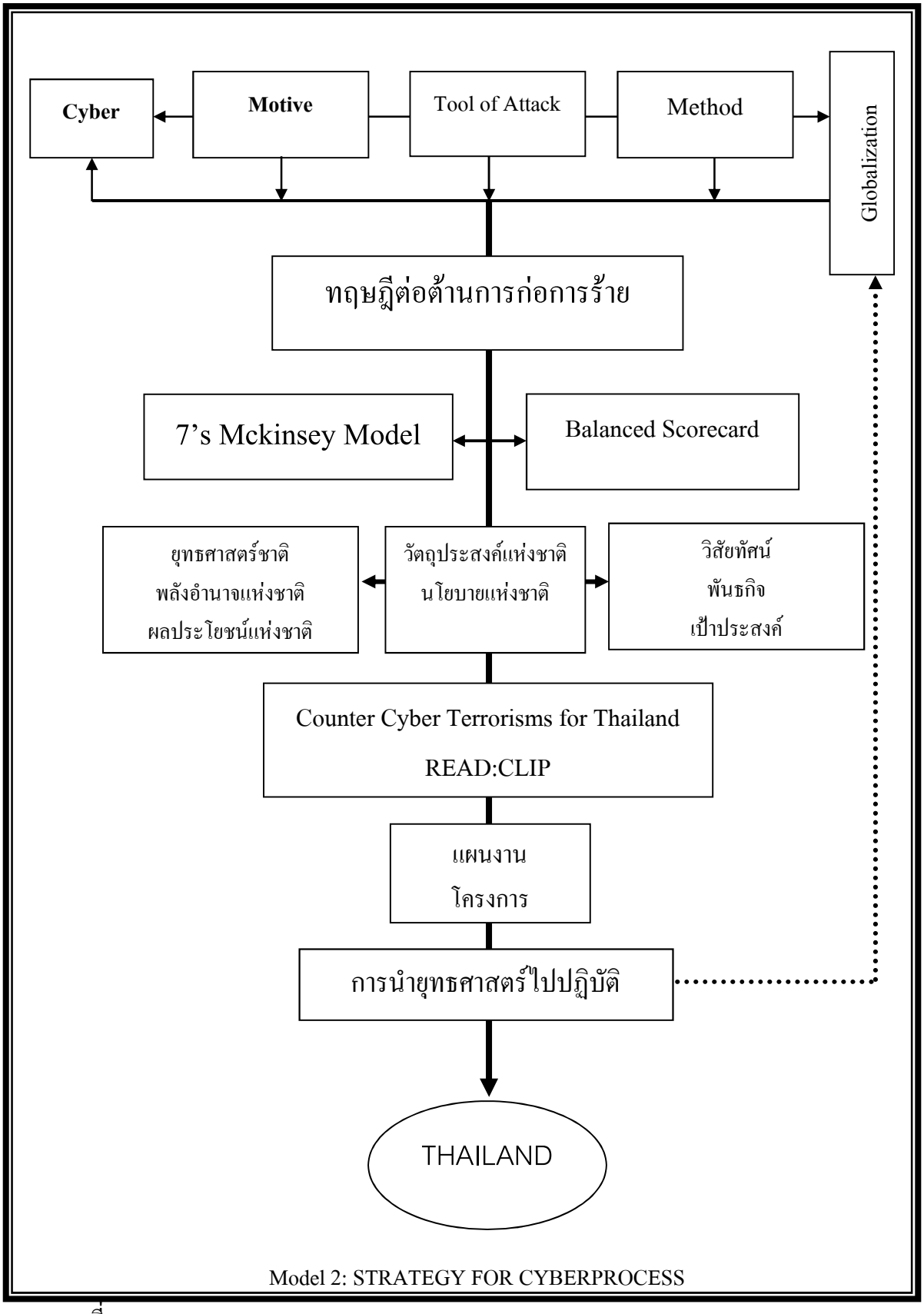
1.ผู้ก่อการร้ายซึ่งต้องมีความรู้ทางไซเบอร์หรือเทคโนโลยี ศึกษาข้อมูลที่เกี่ยวกับเป้าหมายที่ต้องการจะกระทำ2.สร้างหรือพัฒนาเครื่องมือให้ตรงกับความต้องการต่อเป้าหมาย เครื่องมือที่สำคัญของการก่อการร้ายทางไซเบอร์คืออินเทอร์เน็ต3.ระดมคนหรือหาสมาชิกที่มีแนวความคิด

แนวทางเดียวกัน 4.ระดมเงินทุนในการสนับสนุน 5.ปฏิบัติการตามวัตถุประสงค์ที่วางไว้เพื่อมุ่งเป้าหมายทางการเมือง

ลำดับที่ห้า Cyber Terrorism กลุ่มผู้ก่อการร้ายทางไซเบอร์จะนำช่องโหว่ของหน่วยงานหรือองค์กรที่ดูแลระบบทางด้านไซเบอร์โดยดำเนินการก่อการร้าย ซึ่งประเทศไทยปกครองแบบเสรีประชาธิปไตยการให้เสรีภาพไม่ว่าจะด้านใดๆ เป็นผลให้สิทธิเสรีภาพของประชาชนไม่มีขีดจำกัด โดยเฉพาะเสรีภาพทางสื่อ สื่อสารมวลชนเป็นตัวกลางในการนำเสนอข่าวสารความเป็นจริงให้กับประชาชน หากสื่อมีอิสระสูงก็อาจเป็นเครื่องมือที่ชี้นำให้ประชาชนหรือการนำเสนอข่าวสารบางอย่าง หากเอนเอียงไปในทางใดทางหนึ่งก็อาจเป็นเครื่องมือต่อผู้ก่อการร้ายในการรู้ถึงความเคลื่อนไหวและตอบโต้รัฐได้ง่ายขึ้น ประเด็นที่ต้องพิจารณาคือ การให้อิสระและสิทธิเสรีภาพแก่ประชาชนโดยไม่มีการควบคุม เป็นสิ่งที่ก่อให้เกิดผลสะท้อนกลับ การใช้เทคโนโลยีโดยเฉพาะในเรื่องของไซเบอร์ที่ไม่มีการควบคุม ประชาชนหรือองค์กรจะเป็นเหยื่อต่อการถูกทำลายหรือการโจมตีของผู้ก่อการร้ายได้

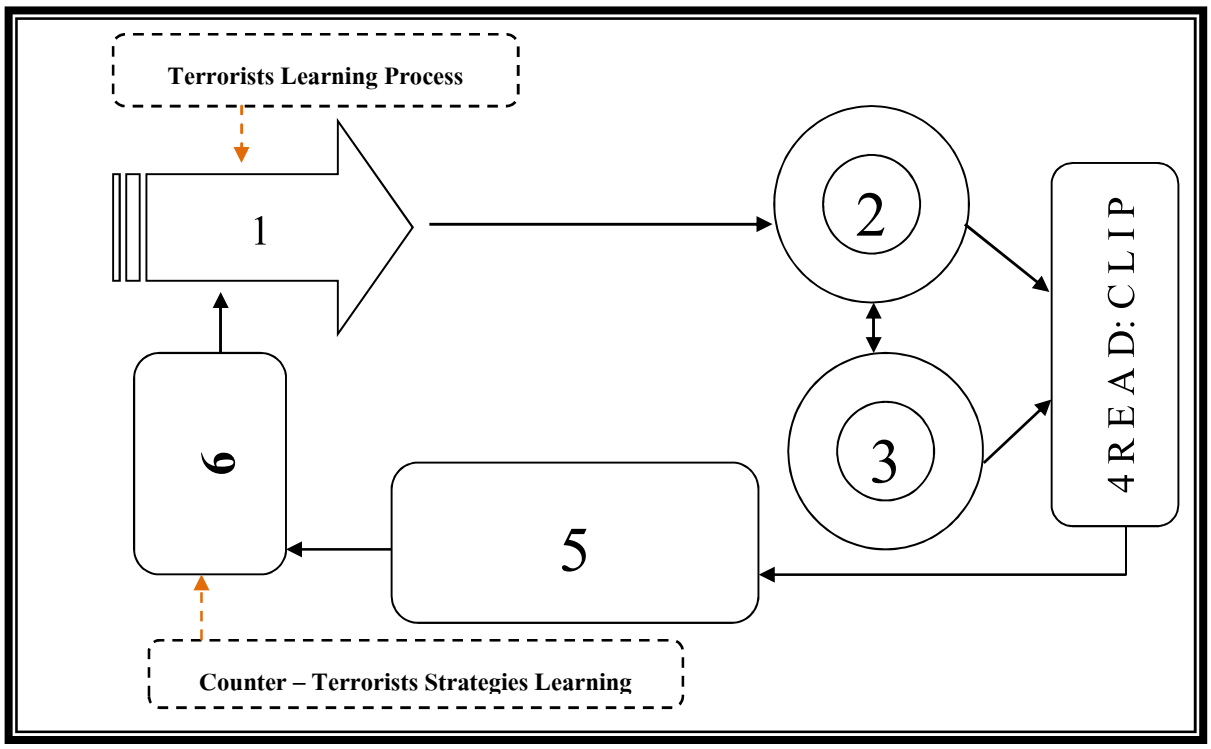
บทสรุป วัฏจักรการก่อการร้ายทางไซเบอร์เป็นนวัตกรรมที่เกิดขึ้นจากการเป็นโลกแห่งโลกาภิวัตน์ การพัฒนาความก้าวหน้าทางไซเบอร์ที่มีการเชื่อมโยงเครือข่ายทั้งโลกให้ติดต่อสื่อสารถึงกันได้อย่างง่ายดาย เมื่อเทคโนโลยี เครือข่ายและคอมพิวเตอร์ โทรศัพท์มือถือ แท็บเล็ต มีความจำเป็นต่อการดำรงชีวิตของมนุษย์ก็จะนำมาซึ่งภัยที่ใกล้ตัว แรงจูงใจที่สำคัญต่อการนำไซเบอร์มาเป็นเครื่องมือในการก่อการร้ายมาจากแรงจูงใจทางการเมือง แรงจูงใจทางศาสนาและอุดมการณ์และแรงจูงใจทางการเงิน สำหรับประเทศไทย แรงจูงใจที่ผู้ก่อการร้ายเข้ามาใช้ประเทศไทยเป็นฐานในการดำเนินการหรือเตรียมการเพื่อก่อการร้ายในประเทศโลกที่สาม ด้วยเหตุเพราะประเทศไทยมีโนโยบายของการเปิดเสรีทางด้านการท่องเที่ยว การค้า ต้อนรับชาวต่างประเทศอย่างมีมิตรไมตรี ทำให้เป็นเหมือนสวรรค์ของผู้ก่อการร้ายในการเข้ามาในประเทศไทย อีกทั้งยังมีนโยบายการส่งเสริมการใช้อินเทอร์เน็ตในทุกที่ ทำให้ประชาชนขาดความรู้ในเรื่องของไซเบอร์และการตระหนักรู้ทางไซเบอร์ เมื่อผู้ก่อการร้ายมีแรงจูงใจต่อการดำเนินการก่อการร้าย เครื่องมือที่ใช้ดำเนินการก่อการร้ายจึงมีความสำคัญ โดยเครื่องมือที่ใช้ในการติดต่อสื่อสารประกอบด้วย คอมพิวเตอร์ โทรศัพท์มือถือ แท็บเล็ตหรืออุปกรณ์ที่สามารถเชื่อมต่ออินเทอร์เน็ตได้ และความก้าวหน้าทางไซเบอร์ต้องมีความความเร็วสูงเพื่อประโยชน์ในการเชื่อมต่อที่สะดวก รวดเร็ว มีระบบปฏิบัติการที่ดีและมีประสิทธิภาพและสามารถเข้าถึงได้ จากความก้าวหน้าทางไซเบอร์นำมาสู่การนำไซเบอร์มาใช้เป็นเครื่องมือในการโจมตีเครื่องมือทางไซเบอร์ที่นำมาใช้ในการก่อการร้ายในปัจจุบันนอกจากนี้ ประเด็นสำคัญที่ค้นพบคือการใช้ โซเชียลมีเดีย (Social Media) ทั้ง ส่งข้อความทางเฟซบุ๊กไลน์ ทวิสเตอร์เป็นต้น รวมทั้งการใช้ การมีกลุ่มแฮกเกอร์เข้ามาโจมตีระบบได้ เช่นการ

จารกรรมข้อมูล การทำให้ระบบเครือข่ายคอมพิวเตอร์ไม่สามารถเข้าใช้งานได้ หรือการควบคุมและสั่งการไปยังเครื่องอื่นเพื่อปิดระบบ สร้างความเสียหายเพื่อใช้ในการติดต่อสื่อสารกันทั่วโลกและใช้เป็นช่องทางในการเผยแพร่แนวคิด วิดีโอ เพื่อให้เกิดความเชื่อ ต่อบุคคล ต่อสมาชิกในกลุ่มหรือเชื่อมโยงไปยังดึง ปลุกระดมคนเพื่อนำมาสู่การก่อการร้ายได้จากนั้นผู้ที่ไม่ประสงค์ดีจะมีวิธีการในการโจมตีโดยการโจมตีของผู้ก่อการร้ายมีวิธีในการดำเนินการที่แตกต่างจากการก่อการร้ายอื่นๆ ด้วยผู้ก่อการร้ายทางไซเบอร์ต้องมีความสามารถในการใช้เครื่องมือทางเทคโนโลยีและมีทักษะทางเทคโนโลยีรวมทั้งต้องมีความเข้าใจต่อเป้าหมายถึงผลลัพธ์ของความเสียหายที่จะเกิดขึ้นวิธีการก่อการร้ายทางไซเบอร์1.ผู้ก่อการร้ายซึ่งต้องมีความรู้ทางไซเบอร์หรือเทคโนโลยี ศึกษาข้อมูลที่เกี่ยวกับเป้าหมายที่ต้องการจะกระทำ2.สร้างหรือพัฒนาเครื่องมือให้ตรงกับความต้องการต่อเป้าหมาย เครื่องมือที่สำคัญของการก่อการร้ายทางไซเบอร์คืออินเทอร์เน็ต 3. ระดมคนหรือหาสมาชิกที่มีแนวความคิดแนวทางเดียวกัน 4.ระดมเงินทุนในการสนับสนุน 5.ปฏิบัติการตามวัตถุประสงค์ที่วางไว้เพื่อมุ่งเป้าหมายทางการเมือง จากวิธีการในการก่อการร้ายทางไซเบอร์จะนำมาใช้ผู้ก่อการร้ายจะมีแรงจูงใจการเกิดขึ้นของผู้ก่อการร้ายทางไซเบอร์ กลุ่มผู้ก่อการร้ายจะอาศัยช่องโหว่ของประเทศกลุ่มเป้าหมายที่โจมตี การก่อการร้ายในยุคโลกาภิวัฒน์ ศตวรรษที่ 21 เป็นรูปแบบการโจมตี วิธีการและกลุ่มเป้าหมายที่เปลี่ยนแปลงไปจากเดิม แต่ส่งผลกระทบต่อความสะพรึงกลัวของคนทั้งโลก แม้จะดำเนินการเพียงแค่ประเทศหรือกลุ่มประเทศเท่านั้น



Model 2: STRATEGY FOR CYBERPROCESS

ภาพที่ 13 Model 2: Strategy for cyber process



ภาพที่ 14 Model 3: COUNTER – TERRORISM LOOP MODEL

หมายเลข 1 ผู้ก่อการร้ายนำไซเบอร์มาเป็นเครื่องมือในการก่อการร้าย

การก่อการร้ายทางไซเบอร์ (Cyber - terrorism) เป็นวิธีการก่อการร้ายโดยโจมตีเป้าหมายเพื่อสร้างความเสียหายให้กับระบบแฟ้มข้อมูลหรือทำให้ระบบคอมพิวเตอร์เสียหาย เช่น การเข้าถึงข้อมูลเพื่อลักลอบแก้ไขทำลาย คัดลอก ทำให้คอมพิวเตอร์ทำงานผิดพลาด ซึ่งล้วนก่อให้เกิดความเสียหายมหาศาลอาทิ บิดเบือนข้อมูลหรือลบข้อมูลทางเศรษฐกิจในคอมพิวเตอร์ของประเทศเป้าหมายโอนเงินจากบัญชีธนาคารหนึ่งไปเข้าอีกบัญชีหนึ่งทำให้โปรแกรมควบคุมและสั่งการทางทหารใช้การไม่ได้เมื่อเกิดวิกฤตการณ์ระหว่างประเทศทำให้ไม่สามารถควบคุมดาวเทียมจากระยะไกลได้ด้วยคอมพิวเตอร์ ฯลฯ

หมายเลข 2 เป้าหมายโดยตรงของผู้ก่อการร้ายทางไซเบอร์

เป้าหมายโดยตรงของผู้ก่อการร้ายทางไซเบอร์คือ ไซเบอร์สเปซ (Cyber Space) เครือข่ายคอมพิวเตอร์ทั้งหลายที่มีอยู่ในโลกและเชื่อมต่อควบคุมอยู่ เป็นเครือข่ายเน็ตเวิร์คเพื่อให้ประชาชนสามารถเชื่อมต่อทั้งอินเทอร์เน็ต และเครือข่ายอื่น ๆ ในการทำธุรกรรม ซึ่งทำหน้าที่เสมือนเป็นทั้งผู้รับ – ส่ง ข้อมูล ทั้งธุรกรรมทางการเงิน การสนทนา พูดคุย รวมทั้งเครือข่ายของโครงสร้างพื้นฐานภายในประเทศที่ใช้ระบบคอมพิวเตอร์ควบคุมการทำงาน

หมายเลข 3 เป้าหมายสำรองผู้ก่อการรร้ายทางไซเบอร์

ผู้ก่อการร้ายทางไซเบอร์ พัฒนามาจากการเป็นอาชญากรรมทางไซเบอร์ ซึ่งกลายเป็นนักรบรับจ้างทางไซเบอร์ได้ คลาร์ก, ริชาร์ด เอ.(2555)อาชญากรทางไซเบอร์ใช้วิธีการแทรกซึมทั้งฮาร์ดแวร์และซอฟต์แวร์คอมพิวเตอร์ เพื่อลักลอบใส่รหัสที่ประสงค์ร้าย แทนที่จะเจาะระบบเพียงอย่างเดียว เช่น ในกรณีของการฉกหมายเลขบัตรเครดิต การหลอกลวงให้โอนเงิน เป็นต้น นอกจากนั้น การกระทำในรูปแบบอื่น ๆ ของผู้ก่อการร้าย เช่น กลุ่มไอเอสใช้การแสดงภาพวีดีโอฆ่าตัดคอเหยื่อผู้เคราะห์เพื่อแสดงออกกถึงความรุนแรงและแนวคิดที่เป็นปฏิปักษ์ต่อกลุ่มที่ต่อต้านและยังเป็นวิธีการชักจูงกลุ่มหรือสมาชิกที่เห็นด้วยให้เข้าร่วมกลุ่ม หมายเลข 4 ยุทธศาสตร์ READ: CLIP

ยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ คือการปกป้องและคุ้มครองให้กับประเทศ ประเทศไทยมีบริบทของประเทศที่แตกต่างจากประเทศอื่น ๆ เหตุผลที่สำคัญคือ เราควรกำหนดยุทธศาสตร์เพื่อป้องกันประเทศโดยคำนึงถึงบริบทของประเทศไทยเป็นหลัก การกำหนดยุทธศาสตร์ในเชิงป้องกัน จะเป็นเครื่องมือที่สำคัญเพื่อสร้างกรอบและแนวทางของการป้องกันเชิงรุกของการก่อการร้ายทางไซเบอร์ในอนาคต

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

ยุทธศาสตร์ที่ 8 Perception Prepares and Protect ยุทธศาสตร์การรับรู้ทางไซเบอร์ร่วมกันตระเตรียมและปกป้องทางไซเบอร์

หมายเลข 5 Cyber Innovation

กรอบของการป้องกันของประเทศไทยที่ดีคือการสร้างนวัตกรรมเพื่อนำมาเป็นเกราะป้องกันภัยจากการก่อการร้ายทางไซเบอร์ ประกอบด้วย

พัฒนาระบบเครือข่ายประชาชนสังคมออนไลน์

ปัจจุบันคนไทยใช้ Social Network และให้ความสำคัญกับการใช้สื่อออนไลน์ต่อการติดตามขาวสาร อัปเดทข้อมูลต่างๆ การสร้างนวัตกรรมด้วยการพัฒนาระบบเครือข่าย จัดทำเป็นโปรแกรมประยุกต์หรือแอพพลิเคชั่น (Application software) เพื่อช่วยให้ประชาชนที่ใช้เครื่องมือสื่อสาร เช่น โทรศัพท์มือถือ แท็บเล็ต เป็นต้น รายงานสถานการณ์ แจ้งข่าว ติดตาม ความเคลื่อนไหวที่เกี่ยวข้องกับการก่อการร้าย เพื่อเป็นแนวทางการป้องกันประเทศไทยที่สำคัญ

ภูมิคุ้มกันความพอเพียงของประเทศไทย

แนวทางปรัชญาเศรษฐกิจพอเพียง ในด้านการสร้างภูมิคุ้มกันที่ดี สิ่งสำคัญคือ การมีสติ สติเป็นการพิจารณาในสิ่งที่ระลึกรู้ในสิ่งที่ทำ เห็นถึงความเป็นจริง เห็นปัญหา ความเคลื่อนไหวหรือความผิดพลาดที่อาจเกิดขึ้น จะช่วยให้เกิดการยั้งคิด พร้อมรับกับการเปลี่ยนแปลงและแก้ไขปัญหาได้อย่างทันท่วงที เพื่อป้องกันความผิดพลาดต่าง ๆ การมีสติจะต้องฝึกฝนและปฏิบัติอย่างสม่ำเสมอ สร้างความร่วมมือระหว่างกลุ่มประเทศอาเซียน

การสร้างเกราะคุ้มกันที่ดีคือการร่วมมือกับพันธมิตรในกลุ่มประเทศอาเซียน เพื่อช่วยในเรื่องของข่าวกรอง ทำข้อตกลงร่วมกันในด้านของข้อมูลการก่อการร้ายทางไซเบอร์ ป้องกันการโจมตีต่อเครือข่ายภาครัฐและภาคเอกชนส่วนใหญ่ให้ได้

หมายเลข 6 แผนปรับปรุง ทบทวน และประเมินผลยุทธศาสตร์

การจัดทำยุทธศาสตร์ เพื่อให้ยุทธศาสตร์มีความทันสมัยและทันต่อเหตุการณ์หรือสถานการณ์ในแต่ละช่วงเวลา ต้องมีการประเมินผล ทบทวน และปรับปรุง กระบวนการประเมินผล (Biswas & Aggarwal : 63 อ้างถึงใน เยาวดี รางชัยกุล วิบูลย์ศรี,2549, น.7)ประกอบด้วยขั้นตอนที่สำคัญ 3 ขั้นตอนคือ

1.การเลือกสิ่งที่ต้องการประเมิน

2.การพัฒนาและใช้กระบวนการเพื่ออธิบายสิ่งที่ต้องการประเมินนั้นอย่างถูกต้อง แม่นยำ

3.สังเคราะห์หลักฐานที่เป็นผลจากกระบวนการเหล่านี้ไปสู่การตัดสินใจขั้นสุดท้าย

การทบทวนแผนยุทธศาสตร์จะทำให้เกิดกระบวนการพิจารณาและสร้างแนวทางป้องกันประเทศได้อย่างดี

จากกรอบความคิด 3: COUNTER – TERRORISM LOOP MODELประกอบด้วย ความก้าวหน้าทางไซเบอร์คือ เทคโนโลยีที่มีอินเทอร์เน็ต เพื่อเชื่อมต่อการสื่อสารได้ทุกที่ทุกเวลา

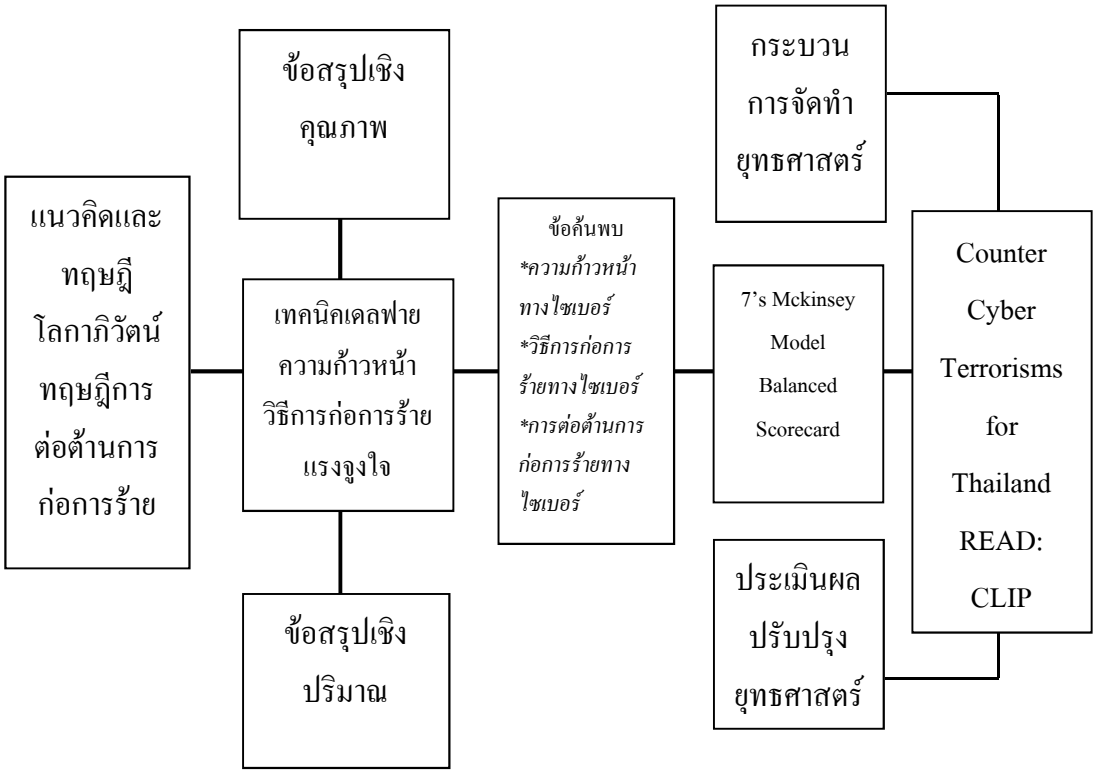
ไม่ว่าจะอยู่ที่ใดบนโลก สะดวก รวดเร็ว และไซเบอร์มีความสำคัญอย่างมากต่อการดำรงชีวิตในปัจจุบัน โดยมีเครื่องมือที่ใช้ในการติดต่อสื่อสาร ไม่ว่าจะเป็น คอมพิวเตอร์โทรศัพท์มือถือ หรือแท็บเล็ตเป็นต้น และความก้าวหน้าทางไซเบอร์ต้องมีความเร็วสูง มีระบบปฏิบัติการที่ดีและมีประสิทธิภาพและสามารถเข้าถึงได้ความก้าวหน้าทางไซเบอร์มีการพัฒนาอย่างรวดเร็ว จะเป็นแรงจูงใจที่สำคัญให้เกิดวธีการในการก่อการร้าย แรงจูงใจกระทำต่อเป้าหมาย มาจากแรงจูงใจทางการเมือง ศาสนา อุดมการณ์ และเงิน (โดยมีความมุ่งหวังในการนำเงินมาใช้เพื่อการก่อการร้าย) โดยผู้ก่อการร้ายใช้ไซเบอร์มาเป็นเครื่องมือในการดำเนินการก่อการร้าย โดยมีวิธีการที่แตกต่างจากการก่อการร้ายแบบปกติและกระทำต่อเป้าหมายที่เป็นพลังอำนาจแบบอ่อน (Soft Power) วิธีการก่อการร้ายทางไซเบอร์ 1.ผู้ก่อการร้ายซึ่งต้องมีความรู้ทางไซเบอร์หรือเทคโนโลยี ศึกษาข้อมูลที่เกี่ยวกับเป้าหมายที่ต้องการจะกระทำ2.สร้างหรือพัฒนาเครื่องมือให้ตรงกับความต้องการต่อเป้าหมาย เครื่องมือที่สำคัญของการก่อการร้ายทางไซเบอร์คืออินเทอร์เน็ต 3. ระดมคนหรือหาสมาชิกที่มีแนวความคิดแนวทางเดียวกัน 4.ระดมเงินทุนในการสนับสนุน 5.ปฏิบัติการตามวัตถุประสงค์ที่วางไว้เพื่อมุ่งเป้าหมายทางการเมือง เมื่อภัยก่อการร้ายคุกคามหรือโจมตีประเทศที่เป็นเป้าหมายสิ่งที่จะสามารถประการวิเคราะห์เพื่อให้ประเทศสามารถป้องกันตนเองหรือปลอดภัยจากการถูกคุกคามหรือโจมตีทางไซเบอร์ได้มีแนวคิดของทฤษฎีการต่อต้านการก่อการร้ายของมาร์ธา เครนชอร์ ได้กำหนดทฤษฎีการต่อต้านการก่อการร้ายมีรูปแบบการศึกษาในด้านการต่อต้านแบบป้องกันการตอบสนองแบบบริหารจัดการและมาตรการมุ่งเน้นการตอบโต้ประเทศไทยจำเป็นต้องมีการกำหนดยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ เพื่อเป็นกลยุทธ์ในการป้องกัน ต่อต้านและแก้ไขฟื้นฟู เมื่อเกิดการโจมตีทางไซเบอร์ อันประกอบด้วย Strategy READ: CLIP

บทสรุปการก่อการร้ายทางไซเบอร์เป็นภัยคุกคามรูปแบบหนึ่งที่ทั่วโลกให้ความสำคัญและเตรียมการรับมือกับภัยคุกคามจากการโจมตีทางไซเบอร์ ซึ่งเมื่อกลุ่มผู้ก่อการร้ายใช้ไซเบอร์เป็นเครื่องมือในการดำเนินการก่อการร้าย เพื่อมุ่งเป้าหมายทางการเมือง ความเสียหายอันเกิดจากการกระทำนี้ ไม่ว่าจะเป็นระบบสาธารณูปโภค โครงสร้างพื้นฐาน การพยาบาล ระบบการขนส่ง รวมทั้งระบบอื่น ๆ ที่จำเป็นจะต้องใช้คอมพิวเตอร์เข้ามาควบคุม อีกทั้งการดำเนินชีวิตประจำวันของมนุษย์ที่นำเอาความก้าวหน้าทางไซเบอร์เข้ามาเป็นอีกปัจจัยหนึ่งที่มีความสำคัญยิ่ง หากสิ่งเหล่านี้มีช่องโหว่ หรือกลุ่มผู้ก่อการร้ายสามารถเห็นถึงช่องทางของการก่อการร้ายได้ ก็จะฉวยโอกาสของการกระทำเพื่อมุ่งหวังไปยังหมายที่ไม่ใช่เพียงแค่กองทัพหรือการสู่รบแบบเผชิญหน้าแต่เป็นการกระทำไปยังประชาชน พลเรือน ที่ไม่มีโอกาสได้ต่อสู้หรือป้องกันตนเอง

การป้องกัน การต่อต้านหรือการเตรียมการ ป้องกันการก่อการร้ายทางไซเบอร์จะเกิดขึ้นมิได้หากผู้บริหารระดับสูง รัฐบาล ไม่เห้นความสำคัญและไม่ใช่เรื่องไกลตัวของประเทศไทยอีก

ต่อไป เพราะภัยคุกคามนี้จะเกิดขึ้นได้ทุกเมื่อ การต่อต้านหรือป้องกันการก่อการร้ายจะกระทำได้ต้องไม่ใช่การแก้ไขปัญหาแบบเฉพาะหน้าแต่เป็นการดำเนินการสร้างความเข้าใจในความหมายของการก่อการร้ายที่เป็นแนวทางเดียวกัน การสร้างความร่วมมือของหน่วยงานทุกภาคส่วน การสร้างการตระหนักรู้ให้กับประชาชน อีกทั้งการพัฒนาความก้าวหน้าทางไซเบอร์ของประเทศไทยอย่างต่อเนื่องจะทำให้ประเทศไทยสามารถป้องกันการก่อการร้ายโดยการส่งเสริมการวิจัยเพื่อเป็นฐานข้อมูลที่สำคัญต่อการพัฒนา ประเทศไทยเป็นประเทศที่เปิดเสรีทางด้านการท่องเที่ยว ให้สิทธิเสรีภาพแก่ประชาชน อีกทั้งยังเป็นสยามเมืองยิ้มที่พร้อมต้อนรับชาวต่างชาติที่เข้ามาในประเทศ ประเทศไทยไม่สามารถปิดกั้นนโยบายเหล่านี้ได้ด้วยเมื่อชาวต่างชาติเข้ามาในประเทศก็ถือเป็นรายได้หลักจากการท่องเที่ยว อีกทั้งประเทศไทยยังเป็นมิตรกับนานาประเทศ แต่ในสถานการณ์ที่ยากต่อการคาดเดาจึงจำเป็นที่ประเทศไทยจะต้องมียุทธศาสตร์เพื่อป้องกันการก่อการร้ายทางไซเบอร์ ซึ่งเป็นภัยคุกคามรูปแบบใหม่ที่หลายประเทศกำลังสะพรึงกลัวกับผลลัพธ์ที่จะเกิดขึ้น สิ่งสำคัญคือ คนไทยทั้งประเทศต้องให้ความสนใจและให้ความสำคัญต่อการใช้ไซเบอร์ และสามารถป้องกันตนเองเพื่อไม่ให้ตกเป็นเหยื่อของผู้ไม่หวังดีที่จะนำเอาไซเบอร์มาเป็นเครื่องมือในการก่อการร้ายได้

ข้อสรุปการอภิปรายผลการวิจัย



ข้อเสนอแนะ

ข้อเสนอแนะในเชิงนโยบายสาธารณะ

1. การสร้างเครือข่ายความร่วมมือทางด้านการต่อต้านการก่อการร้ายทางไซเบอร์ในกลุ่มอาเซียนโดยการจัดทำข้อตกลงหรือเครือข่ายความร่วมมือระหว่างกลุ่มประเทศ

2. ควรกำหนดแนวทางการต่อต้านการก่อการร้ายทางไซเบอร์ในระดับนานาชาติจากความร่วมมือในกลุ่มอาเซียน มีการประชุมร่วมกันโดยการหมุนเวียนเพื่อเป็นเจ้าภาพในแต่ละประเทศ

3. รัฐบาลควรมีการกำหนดคณะกรรมการกลางในระดับประเทศหรือหน่วยงานกลางในการประสานงานให้หน่วยงานทางยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์นำไปบรรจุในแผนยุทธศาสตร์ที่เกี่ยวข้องกับการต่อต้านการก่อการร้าย

4. ควรมีการกำหนดให้มีผู้บริหารระดับสูงเป็นประธานในการดูแลทางด้านความมั่นคงทางไซเบอร์และกำหนดเป็นแผนยุทธศาสตร์ทางไซเบอร์

5. ควรมีการกำหนดให้คณะกรรมการปรับปรุงความรู้และพัฒนาทักษะในด้านที่เกี่ยวข้อง เช่น ด้านการศึกษา ด้านเทคโนโลยี เพื่อให้มีความรู้และทักษะทัดเทียมกับผู้ก่อการร้ายได้

ข้อเสนอแนะในระดับปฏิบัติ

1. ต้องมีหน่วยงานในการทำงานทางด้านการต่อต้านการก่อการร้ายทางไซเบอร์ เช่น ตำรวจ ทหารหน่วยข่าวกรอง กำหนดแนวทางการเฝ้าระวังและกำหนดให้หน่วยงานสามารถดึงหรือได้รับข้อมูลและดำเนินการได้ในทางปฏิบัติ

2. หน่วยงานที่มีหน้าที่รับผิดชอบควรมีการกำหนดนโยบายและแนวทางที่สามารถแบ่งปันข้อมูลทั้งในส่วนของก่อนเกิดเหตุหรือหลังเกิดเหตุจากการถูกโจมตีทางไซเบอร์ได้อย่างรวดเร็ว เพื่อให้การแก้ไขปัญหาสามารถกระทำได้อย่างทันท่วงที

3. สถาบันทางสังคม ทั้งสถาบันการศึกษาและสถาบันครอบครัว ควรร่วมกันในการสร้างการตระหนักรู้ต่อภัยคุกคามทางไซเบอร์ รวมทั้งปลูกฝังให้คนในสังคมรู้ถึงภัยคุกคามที่ใกล้ตัวและเกิดขึ้นได้ทุกเมื่อ

4. ควรกำหนดแนวทางของการศึกษากฎหมายทางไซเบอร์และเรียนรู้ช่องทางเมื่อเกิดภัยคุกคามทางไซเบอร์ในการดำเนินการแก้ปัญหาอย่างเร่งด่วนและเป็นระบบให้แก่ประชาชน เพื่อไม่ให้ภัยคุกคามลุกลามจนกลายเป็นช่องโหว่ต่อผู้ไม่หวังดีนำไปสู่การก่อการร้ายได้

5. ควรมีการส่งเสริมหรือสร้างเครือข่ายความร่วมมือและรวมกลุ่มในระดับภูมิภาคหรือระดับชุมชนชุมชนเพื่อสร้างปราการป้องกันการถูกคุกคามทางไซเบอร์และเกิดการแลกเปลี่ยนข้อมูลกัน ระหว่างคนในชุมชน ชุมชนและหน่วยงานในระดับชุมชน ท้องถิ่น ไปสู่ระดับประเทศ

ข้อเสนอแนะเพื่อการวิจัยครั้งต่อไป

1. ควรมีการกำหนดนิยามของการก่อการร้ายทางไซเบอร์ให้มีความชัดเจน

2. ควรศึกษาพัฒนาการวิจัยในความก้าวหน้าทางไซเบอร์ เนื่องจากไซเบอร์ในอนาคต มีการเปลี่ยนแปลงอย่างต่อเนื่องและมีบทบาทต่อการดำรงชีวิตของประชาชน

3. ควรมีการศึกษาแนวทางการเชื่อมโยงขององค์กรที่เกี่ยวข้องกับการนำไซเบอร์และพัฒนาทางไซเบอร์ เพื่อสร้างความเข็มแข็งขององค์กรและสร้างเครือข่ายของหน่วยงานให้สามารถเชื่อมข้อมูลระหว่างกันได้

4. ยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ นี้เป็นองค์ความรู้ใหม่ ควรมีการนำไปใช้เพื่อให้สามารถต่อต้านการก่อการร้ายได้อย่างมีประสิทธิภาพ

บรรณานุกรม

กมลนวล ศิลาพันธ์. (2556). *ความชัดเจนและความเหมาะสมในการกำหนดนิยามของการก่อการร้ายในประมวลกฎหมายอาญาของไทย.* วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, สาขาวิชานิติศาสตร์, คณะนิติศาสตร์ปรีดี พนมยงค์, มหาวิทยาลัยธุรกิจบัณฑิต.

กรอบนโยบายเทคโนโลยีสารสนเทศและการสื่อสาร ระยะ พ.ศ. 2554 – 2563. (2550). เข้าถึงได้จาก http://www.thaiwebaccessibility.com/sites/default/files/content_types/webcontent/ict2020_book.pdf

กองข่าวกองทัพภาคที่ 2. (ม.ป.ป.) *การก่อการร้าย.* นครราชสีมา: เอกสารเผยแพร่ความรู้.

กัญญา โพธิวัฒน์.(2548). *ทีมผู้นำกับการเปลี่ยนแปลงในโรงเรียนประถมศึกษา: การศึกษาเพื่อสร้างทฤษฎีฐานราก.* วิทยานิพนธ์ดุษฎีบัณฑิต, สาขาวิชาการบริหารการศึกษา, คณะศึกษาศาสตร์, มหาวิทยาลัยขอนแก่น.

กีรติ ยศยิ่งยง. (2549). *การวางแผนการเปลี่ยนแปลงและการพัฒนาเชิงกลยุทธ์.* กรุงเทพฯ: มิสเตอร์ท๊อปปี้.

โกวิท วงศ์สุรวัฒน์. (2550). *การก่อการร้ายในเมืองกับสงครามกองโจร.* เข้าถึงได้จาก http://matichon.com

คณิต ณ นคร. (2547). *กฎหมายอาญาภาคทั่วไป* (พิมพ์ครั้งที่ 2). กรุงเทพฯ:วิญญูชน

คณิต ณ นคร. (2548). *ประมวลกฎหมายอาญา หลักกฎหมายและพื้นฐานการเข้าใจ* (พิมพ์ครั้งที่ 8). กรุงเทพฯ: วิญญูชน.

คลาร์ก, ริชาร์ด เอ. (2555). *สงครามไซเบอร์ – Cyber War***.** (ไพรัตน์ พงศ์พานิชย์, แปล) กรุงเทพฯ: มติชน.

โครินทร์ เฟื่องเกษม. (2541). *เอเชียตะวันออกเฉียงใต้: นโยบายต่างประเทศในยุคโลกาภิวัฒน์.* (พิมพ์ครั้งที่ 2). กรุงเทพฯ:โรงพิมพ์มหาวิทยาลัยธรรมศาสตร์.

จตุชัย แพงจันทร์. (2558). *ความปลอดภัยของข้อมูล Master in Security 3rd Edition.*นนทบุรี:ไอซีดีพรีเมียร์.

จิ๊กซอ. (2015).*10 การก่อการร้ายที่โลกต้องจำ.* เข้าถึงได้จาก http://www.247friend.net/blog/specialmaster/2015/05/11/entry-3

จันทิมา เภาเจริญ. (2550). *การก่อการร้ายสากลในเอเชียตะวันออกเฉียงใต้.* วิทยานิพนธ์ศิลปศาสตรมหาบัณฑิต, สาขาวิชารัฐศาสตร์, คณะรัฐศาสตร์, มหาวิทยาลัยรามคำแหง.

จุติ, “นามสมมติ” (2558, 7 กันยายน) สัมภาษณ์.

จุลชีพ ชินวรรณโณ. (2546). *ความมั่นคงในภูมิภาคเอเชียตะวันออกเฉียงใต้ในศตวรรษที่ 21: ประเทศไทยกับแนวคิดยุทธศาสตร์และความมั่นคงจากอดีตถึงปัจจุบัน.* กรุงเทพฯ: วิทยาลัยป้องกันราชอาณาจักร สถาบันวิชาการป้องกันประเทศ.

ชญาณ์พิมพ์ บัวดิษฐ์เดชา. (2551). *ความรับผิดทางอาญาของผู้คุกคามผู้อื่นโดยใช้อินเทอร์เน็ต.* วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, สาขาวิชานิติศาสตร์, คณะนิติศาสตร์, จุฬาลงกรณ์มหาวิทยาลัย.

ชรัติ อุ่มสัมฤทธิ์. (2550). *การนำเสนอยุทธศาสตร์การพัฒนาระบบการจัดการศึกษาระดับอุดมศึกษาของกองทัพบกเพื่อส่งเสริมความมั่นคงของชาติ.* ดุษฎีนิพนธ์ครุศาสตรดุษฎีบัณฑิต, สาขาวิชานโยบายการจัดการและความเป็นผู้นำทางการศึกษา, บัณฑิตวิทยาลัย, จุฬาลงกรณ์มหาวิทยาลัย.

ชัยอนันต์ สมุทวาณิช. (2544). *จากรัฐชาติสู่รัฐตลาด: แนวความคิดที่เกี่ยวกับรัฐและสังคมในยุคโลกานุวัตร.* กรุงเทพฯ: บ้านพระอาทิตย์.

ฐณภัทร แก้วโบราณ. (2557). *นโยบายรัสเซียต่อการแบ่งแยกดินแดนและการก่อการร้าย โดยกลุ่มกบฏเชชเนีย ระหว่างปี ค.ศ. 1991 – 2011.* วิทยานิพนธ์รัฐศาสตรมหาบัณฑิต, สาขาวิชารัฐศาสตร์, คณะรัฐศาสตร์, มหาวิทยาลัยรามคำแหง.

ดารณี พิมพ์ช่างทอง. (2552). *ระบบสารสนเทศในองค์กร.* กรุงเทพฯ: ทริปเพิ้ล กรุ๊ป.

ดุสิต น้ำฝน. (2549). *การจัดตั้งองค์การชำนาญพิเศษเพื่อดำเนินงานยุทธศาสตร์ต่อต้านการก่อการร้าย.* วิทยานิพนธ์รัฐศาสตรมหาบัณฑิต, สาขาวิชาการจัดการทรัพยากรเพื่อความมั่นคง, คณะมนุษยศาสตร์และสังคมศาสตร์, มหาวิทยาลัยบูรพา.

ดลยา เทียนทอง. (2549). “ข้อมูลเบื้องต้นเกี่ยวกับการก่อการร้าย” การก่อการร้ายร่วมสมัย (Contemporary Terrorism). *จุลสารความมั่นคงศึกษา,* 57, 7 – 12.

ดลยา เทียนทอง. (ม.ป.ป.). *การสำรวจข้อมูลเบื้องต้นเกี่ยวกับการก่อการร้าย.* กรุงเทพฯ: สถาบันเอเชียศึกษา, จุฬาลงกรณ์มหาวิทยาลัย.

ดำรงค์ วัฒนา. (2548). *ยุทธศาสตร์การบริหารภาครัฐ: หลักการและวิธีการ.* เข้าถึงได้จาก http://home.dsd.go.th/standard/.

ธเนศ ขำเกิด. (2541). องค์กรแห่งการเรียนรู้ (Learning Organization). *วารสารส่งเสริมเทคโนโลยี 25*(137), 171 – 174.

ธันยวัต ชูส่งแสง. (2547). *การก่อการร้ายในมุมมองของสหรัฐอเมริกา.* กรุงเทพฯ: กรมข่าวทหารอากาศ กองทัพอากาศ.

ธีรนันท์ นันทขว้าง. (2555*). ยุทธศาสตร์ – ยุทธศาสตร์ชาติ ความหมายของยุทธศาสตร์และยุทธศาสตร์ชาติ.* เข้าถึงได้จาก http:// tortaharn.net/downloadterrorism_Info_Age.pdf

บาร์เกอร์ โจนาธาน. (2548). *คู่มือศึกษาการก่อการร้ายแบบไม่งี่เง่า.* (เกษียร เตชะพีระ, แปล) กรุงเทพฯ: คบไฟ.

บุญรอด ศรีสมบัติ. (2548). *ยุทธศาสตร์ศึกษาเล่มที่ 3 คู่มือก่อการร้าย อัลเคด้า.* กรุงเทพฯ: สถาบันวิชาการทหารบกชั้นสูง.

บุญรอด ศรีสมบัติ, กิตติ์ธนทัต เลอวงศ์รัตน์,วิภูษณะ คล้ายมณี และเอื้อชาติ หนุนภักดี. (2555). *รู้เท่าทันการก่อการร้าย Knowing Terrorism.* กรุงเทพฯ: (ม.ป.ท.)

ปกรณ์ ปรียากรณ์. (2547). *การวางแผนกลยุทธ์.* กรุงเทพฯ: เสมาธรรม.

เปี่ยมพงศ์ นุ้ยบ้านด่าน. (2543). องค์กรแห่งการเรียนรู้. *วารสารการศึกษาพยาบาล*, *10*(3),13 – 17.

แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร (ฉบับที่ 3) ของประเทศไทย พ.ศ.2557 – 2561.(2557). เข้าถึงได้จาก www.itc.ddc.moph.go.th/file/it_plan_58.pdf

แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารแห่งประเทศไทย (ฉบับที่ 2) ของประเทศไทย พ.ศ.2552 – 2556. (2555). เข้าถึงได้จาก www.nstda.or.th › eBook

พนิดา พานิชกุล. (2553). *ความมั่นคงปลอดภัยของสารสนเทศและการจัดการ.* กรุงเทพฯ: เคทีพีคอมพ์แอนด์คอนซัลท์.

พงศธร สัตย์เจริญ. (2549). *กฎหมายกับการก่อการร้าย.* กรุงเทพฯ: สารชาวฟ้า.

เมธินี ไชยคุณา. (2553). *แนวคิดและองค์การก่อการร้ายระหว่างประเทศในประเทศอินโดนีเซียกับปฏิกิริยา ของออสเตรเลีย: กรณีศึกษาการลอบวางระเบิดบนเกาะบาหลี ค.ศ. 2002*. วิทยานิพนธ์ศิลปศาสตรมหาบัณฑิต, สาขาวิชาภูมิภาคศึกษา, บัณฑิตวิทยาลัย, มหาวิทยาลัยเชียงใหม่.

มงคล, “นามสมมติ” (2558, 27 พฤษภาคม) สัมภาษณ์.

มนตรี, “นามสมมติ” (2558, 11 พฤษภาคม) สัมภาษณ์.

ยอดชาย วิถีพานิช. (2558). *ไอเอส: กลุ่มก่อการร้ายที่โลกต้องจับตามอง.* เข้าถึงได้จาก www.Parliament.go.th>download>article.

เยาวดี รางชัยกุล วิบูรย์ศรี. (2549). *การประเมินโครงการ: แนวคิดและแนวปฏิบัติ.* กรุงเทพฯ: โรงพิมพ์จุฬาลงกรณ์มหาวิทยาลัย.

ระวิวรรณ ธรณี, ปราณี ประวิชพราหมณ์ และภาวิณี อุ่นวัฒนา. (2551). *ชีวิตที่พอเพียงในมุมมองของนักศึกษาภายใต้กระแสโลกาภิวัตน์*. กรุงเทพฯ: คณะศิลปะศาสตร์, มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร.

ราชบัณฑิตยสถาน. (2546). *พจนานุกรม ฉบับราชบัณฑิตยสถาน พ.ศ. 2542.* กรุงเทพฯ : ศิริวัฒนาอินเตอร์พริ้นท์.

ลิขิต ธีรเวคิน. (2554). *การปรับตัวในยุคโลกาภิวัตน์และการเตรียมตัวเข้าเป็นสมาชิกประชาคมอาเซียนของประเทศไทย.* เข้าถึงได้จากhttp://www.nubkk.nu.ac.th/handout_details.

วรกร โอภานันท์. (2544). *มาตรการทางกฎหมายในการต่อต้านการก่อการร้ายระหว่างประเทศ.* วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, สาขาวิชานิติศาสตร์, คณะนิติศาสตร์, มหาวิทยาลัยธรรมศาสตร์.

วรพจน์ วงศ์กิจรุ่งเรือง และอธิป จิตตฤกษ์. (2554). *ทักษะแห่งอนาคตใหม่: การศึกษาเพื่อศตวรรษที่ 21*. กรุงเทพฯ:โอเพ่นเวิลด์ส.

วรรณี แกมเกตุ. (2551). *วิธีวิทยาการวิจัยทางพฤติกรรมศาสตร์* (พิมพ์ครั้งที่ 2). กรุงเทพฯ: โรงพิมพ์จุฬาลงกรณ์มหาวิทยาลัย.

วรรณี, “นามสมมติ” (2558, 13 กรกฎาคม) สัมภาษณ์.

วิเชียร, “นามสมมติ” (2558, 26 พฤษภาคม) สัมภาษณ์.

วินาศกรรม 11 กันยายน พ.ศ.2554. (2558). เข้าถึงได้จาก www.th.Wikipedia.org/wiki/.

วิชัย ชูเชิด.(2547). *ความมั่นคงศึกษา.* ในเอกสารประกอบการศึกษา โรงเรียนเสนาธิการทหารบก (10). กรุงเทพฯ:สถาบันวิชาการทหารบกชั้นสูง.

วีรพล วรานนท์. (2547). *ยุทธศาสตร์และการกำหนดกำลังรบ.* กรุงเทพฯ: กราฟิคแมส.

วุฒิกรณ์ ชูวัฒนานุรักษ์. (2549). *การก่อการร้ายในเอเชียตะวันออกเฉียงใต้ในยุคหลังสงครามเย็น: วิเคราะห์แนวความคิด “การก่อการร้าย” และขบวนการก่อการร้ายในไทยและพิลิปปินส์.* ดุษฎีนิพนธ์รัฐศาสตรดุษฎีบัณฑิต, สาขาวิชารัฐศาสตร์, คณะรัฐศาสตร์, จุฬาลงกรณ์มหาวิยาลัย.

วงษ์พิทักษ์ เจียนเกาะ. (2550). *ประมวลกฎหมายอาญาของไทยกับกฎหมายระหว่างประเทศเกี่ยวกับการก่อการร้าย: ศึกษาเฉพาะกรณีอนุสัญญาระหว่างประเทศ ข้อตกลงและพิธีสารที่เกี่ยวข้อง*. วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, สาขาวิชานิติศาสตร์, บัณฑิตวิทยาลัย, มหาวิทยาลัยธุรกิจบัณฑิตย์.

วรนุช พุ่มเรือง. (2554). *บทบาทของปากีสถานในการต่อต้านการก่อการร้ายสมัยประธานาธิบดีเปอร์เวซมุชัรร๊อฟ(ค.ศ.1999 – 2008).* วิทยานิพนธ์รัฐศาสตรมหาบัณฑิต, สาขาวิชาการระหว่างประเทศและการทูต, คณะรัฐศาสตร์, มหาวิทยาลัยธรรมศาสตร์.

ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย. (2556). *Cyber Security is our Mission รายงานประจำปีไทยเซิร์ต 2556.* กรุงเทพฯ: ไทยเซิร์ต.

ศูนย์ศึกษาการก่อการร้าย. (2549).*การต่อต้านและการตอบโต้การก่อการร้าย.* เข้าถึงได้จาก www.geocities.com

ศูนย์พลเรือนและทหารสัมพันธ์ บัณฑิตวิทยาลัยราชนาวี รัฐแคลิฟอร์เนีย. (2548). *การตอบโต้ของทหารและพลเรือนและทหารต่อการก่อการร้าย*. ม.ป.ป.

สัญญา, “นามสมมติ” (2558, 10 กรกฎาคม) สัมภาษณ์.

สายฝน แสงสวัสดิ์. (2557). *ปัจจัยที่เกี่ยวข้องในการก่อการร้าย.* เข้าถึงได้จาก http://53011312366.blogspot.com/2012/09/blog-post_4205.html, 2557.

สุขุม เฉลยทรัพย์ และคณะ. (2551). *เทคโนโลยีสารสนเทศ.* (พิมพ์ครั้งที่ 6). กรุงเทพฯ: มหาวิทยาลัยราชภัฏสวนดุสิต

สุรินทร์ หิรัญบูรณะ. (2547). *ผ่าลัทธิก่อการร้าย: มหันตภัยของมนุษยชาติ.* กรุงเทพฯ: มติชน.

สุรศักดิ์, “นามสมมติ” (2558, 22 กรกฎาคม) สัมภาษณ์.

สมชัย, “นามสมมติ” (2558, 16 กรกฎาคม) สัมภาษณ์.

อโนทัย งามวิชัยกิจ. (2558). *การวิจัยแบบผสมผสานเชิงคุณภาพและเชิงปริมาณ.* เข้าถึงได้จาก https://www.tci-thaijo.org/index.php/stou-sms-pr/article/viewFile/33192/33209

อเนก เหล่าธรรมทัศน์. (2536). *ม็อบมือถือ:ชนชั้นกลางและนักธุรกิจกับการพัฒนาประชาธิปไตย.* กรุงเทพฯ: มติชน.

อัศวิน ศุกระศร. (2549). *ความผิดฐานการก่อการร้ายในประเทศไทย: มาตรการป้องกันและปราบปราม.*วิทยานิพนธ์นิติศาสตรมหาบัณฑิต, สาขาวิชานิติศาสตร์, คณะนิติศาสตร์, มหาวิทยาลัยธรรมศาสตร์.

อุนิยา เลิศโตมรสกุล. (2555). *อาชญากรรมและอาชญาวิทยา.* กรุงเทพ: โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.

เอริคชมิดท์และจาเร็ด โคเฮน. (2556). *ดิจิตัลเปลี่ยนโลก.* (สุทธวิชญ์ แสงดายดา, แปล) กรุงเทพฯ : โพสต์บุ๊กส์.

อวยพร, “นามสมมติ” (2558, 20 ตุลาคม) สัมภาษณ์.

Anthony, G. (2003). *The globalizing of modernity. in global transformations reader: Introduction to the globalization debate* (2rd ed). Cambridge: Polity Press.

Bremer, L. P. (1998). *The west’ counterterrorism strategy*. London: Frank Cass.

Bridgman, R. (1999). *Eyewitness: Technology.* New York: DK CHILDREN.

Boaz, G. (1998). *Defining terrorism: Is one man’s terrorist another man’s freedom fighter The International policy institute for counter – terrorism*. Retrived from

http://ict.org.il/.

Creswell, J. W., & Plano,V.L. (2007). *Designing and conducting mixed methods research*. (2nd ed). Thousand Oaks, CA: Sage publications.

Creswell, J. W. (2013). *Research design: Qualitative, quantitative and mixed methods approaches* (2nd ed). Thousand Oaks, CA: Sage publications.

Crenshaw, M. (1988). *Theories of terrorism: Instrumental and organizational Approaches, in David Rapoport (ed.) Inside Terrorist Organizations*. London: Frank Cass.

Crenshaw, M. (2006). The image of terrorism and the government's response to terrorism, In David C. Rapoport (ed.), *Terrorism: Critical Concepts in Political Science*. (pp. 13 – 31) London: Routledge.

Couloumbis,T. A., & Wolfe, J. H. (1978). *Introduction to international relations: power and justice*. New Jersey: Prentice Hall.

Coffey, A., & Atkinson, P. (1996). *Making sense of qualitative data: Complementary research strategies*. Thousand Oaks: Sage.

Daft, R. L. (1998). *Organization theory and design*. (6th ed). Ohio: South – Western College Publishing.

Daud, A. (2001). *Cyber – dissent in the middle east: A tool of political resistance.* Doctoral dissertation, School of Political and Policy, Claremont Graduate University.

EU Cyber security Dashboard - BSA. (n.d.). (2015, march 15). Retrieved from http:// www.bsa.org/~/media/Files/Policy/.../EU/study_eucybersecurity_en.pdf

Facebook statistics Thailand as ASEAN's top three. (2015, march 15). Retrieved from www.it24hrs.com/2015/facebook-population-aec-2015

Garvin, D. A. (1993). Building a learning organization. *Harvard Business Review on Knowledge Management*. Boston: Harvard Business school press.

Gary, G.S. (1990). *The political underprinning of terrorism, international terrorism characteristics,causes, controls, CharkesW.Kengley,JR*. NewYork: St.Martin's Press.

Geocities. (2004). *Terrorism studies.* Retrieved from http://www.geocities.com/terrorismstudies.

Giddens, A. (1990). *The Consequences of Modernity*. Cambridge: Polity.

Gobran, A. (2015). *Cyber terrorism threats*. Master of Science of Cyber security, ACapstone Project Submitted to the Faculty, Utica College.

Gray, C.F. & Larson, E.W. (2003). *Project management*. Singapore: Mcgraw Hill.

Gurr, R. T. (1988) Some Characteristics of Political Terrorism in the 1960s. In Stohl

Holton, R. (2000). Globalization´s cultural consequences, Annals of the American Academy of Political and Social Science , 570 (1), 140-152.

Morgenthau, H. J. (2005). *Politics among nations: The struggle for power and peace.*(7th ed). New York: Alfred A. Knopf.

Jonathan, R.W. (2000). *An introduction pacific grove, CA: brooks/cole publishing company, 1991.* (2nd ed). New Jersey: prentice Hall.

Kim, S.Y. (2010). *Cyber – surveillance: A case study in policy and development.* Doctoral dissertation, Faculty in Criminal Justice in partial fulfillment, The City University of New York.

Cronbach. L.J. (1974). *Essentials of phychological testing.* (3rd ed). New York: Harper & Row Publisners.

Lerche, C. O., & Said, A. A. (1995). *Concepts of international politics in global perspective.*(4th ed). New Jersey: Prentice Hall.

Lincoln, Y. S. & Guba, E. G. (1985). *Naturalistic inquiry.* Beverly Hills: Chicago.

Liotta, P.H., & Lloyd, R.M. (2004). *Strategy and force planning* (4rd ed). New York : Newport, RI Naval War College Press.

Resourcer material series no. 38 unafei. (1990). Retrived from https://www.ncjrs.gov/pdffiles

Rosenau, J. N. (1969). *Introduction: Political science in a shrinking world in linkage politics; essays on the convergence of national and international systems.* New York: The Free Press.

Burgelman, R.A, Christensen, C. M. & Wheelwright, S. C. (2008). *Strategic Management of Technology and Innovation*. McGraw-Hill: Irwin.

Neuman, W. (2000). *Social research methods: Qualitative and quantitative approach*. (4th ed). Boston: Allyn and Bacon.

Nye, J. (1995). *The case for deep engagement*. Foreign Affairs.74(4), 90 – 102.

Porter, M. (2001). *Strategy and the Internet*. Retrieved from https://hbr.org/2001/03/strategy-and-the-internet.

Said, A. A., & Lerche, C.O. (1970). *Concept of international politics*.(2rd ed). New Jersey: Prentice Hall.

Scholte, J.A. (2007). Defining globalization. Retrived from http:// www.clmeconomia.jccm.es.

Sharma, D.P. (2005). *The new terrorism: Islamist international*. New Delhi: A.P.H. Publishing Corporation.

Steve R. (2006). Social network analysis as an approach to combat terrorism: Past, present, And future research. Retrieved from http://www.search.proquest.com/openview/ dae6d26ba2112d9cda358bbde499ce7a/1?pq-origsite=gscholar

Snowden, A.M. (2015). *The perception of cyber threats and its associative relationship to the protection motivation theory and generational age groups: a Quantitative study*. Doctoral dissertation, Faculty in Business and Technology, Capella University

The Major Motivation behind Cyber Attacks. (2014). Retrieved from http://www.go-gulf.com/blog/cyber-crime.

The White House. (1996) *A national security strategy of engagement and enlargement.* Retrived from http;//www.fas.org/spp/military/docops/national/1996 stra.htm, February

The White House. (2002).T*he national security strategy of The United States of America*. Retrived from http://www.whitehouse.gov/nsc/nss.pdf>, September

Thornton, T. P. (2005). *Terror as a weapon of political agitation. In eckstein.* New York: Free Press of Glencoe.

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

Wilkinson, P. (1974).*Political terrorism*. London: Macmillan.

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

Ozeren, S. (2005).*Global response to cyber terrorism and Cybercrime: A matrix for international cooperation and vulnerability assessment.* Doctoral dissertation, Faculty in Information Science, University of North Texas.