การรับมือของภาครัฐกับการก่อการร้ายทางไซเบอร์ในประเทศไทย

น.ส.นัทธมน เพชรกล้า

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาศิลปศาสตรดุษฎีบัณฑิต
สาขาวิชาอาชญาวิทยาและงานยุติธรรม ภาควิชาสังคมวิทยาและมานุษยวิทยา
คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2564

Government sector's Response in Counter-Cyber-Terrorism in Thailand

Miss Natthamon Petchkla

A Dissertation Submitted in Partial Fulfillment of the Requirements
for the Degree of Doctor of Philosophy in Criminology and Criminal Justice
Department of Sociology and Anthropology
FACULTY OF POLITICAL SCIENCE
Chulalongkorn University
Academic Year 2021

หัวข้อวิทยานิพนธ์	การรับมือของภาครัฐกับการก่อการร้ายทางไซเบอร์ในประเทศไทย
โดย	น.ส.นัทธมน เพชรกล้า
สาขาวิชา	อาชญาวิทยาและงานยุติธรรม
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	รองศาสตราจารย์ ดร.สุมนทิพย์ จิตสว่าง

คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาศิลปศาสตรดุษฎีบัณฑิต

..... คณบดีคณะรัฐศาสตร์
(รองศาสตราจารย์ ดร.เอก ตั้งทรัพย์วัฒนา)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(รองศาสตราจารย์ ดร.ศรีสมบัติ โชคประจักษ์ชัด)

..... อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(รองศาสตราจารย์ ดร.สุมนทิพย์ จิตสว่าง)

..... กรรมการ
(รองศาสตราจารย์วันชัย มีชาติ)

..... กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.ฐิติยา เพชรมุนี)

..... กรรมการภายนอกมหาวิทยาลัย
(พล.ต.ต.ดร.พรชัย ขันตี)

นัทธมน เพชรกล้า : การรับมือของภาครัฐกับการก่อการร้ายทางไซเบอร์ในประเทศไทย. (Government sector's Response in Counter-Cyber-Terrorism in Thailand) อ.ที่ปรึกษาหลัก : รศ. ดร.สุมนทิพย์ จิตสว่าง

นับตั้งแต่อินเทอร์เน็ตถูกคิดค้นขึ้นได้ส่งผลกระทบต่อการเปลี่ยนแปลงอย่างรวดเร็วจากความก้าวหน้าของเทคโนโลยีในโลกไซเบอร์ ปัญหาสำคัญที่สังคมกำลังเผชิญอยู่ในขณะนี้คือการเพิ่มขึ้นของการโจมตีทางไซเบอร์ ซึ่งสามารถเชื่อมโยงกับการก่อการร้ายทางไซเบอร์ แต่ละประเทศในโลกกำลังเริ่มที่จะจัดการกับข้อกังวลของการก่อการร้ายทางอินเทอร์เน็ตซึ่งเป็นวิธีการใหม่ในการบรรลุเป้าหมายทางการเมือง ประเทศไทยเป็นหนึ่งที่กำลังตื่นตระหนกและให้ความสนใจในประเด็นนี้ แต่เนื่องด้วยข้อจำกัดหลาย ๆ ประการจึงทำให้ความก้าวหน้าในการจัดการกับประเด็นนี้มีไม่มากนักเมื่อเทียบกับประเทศอื่น ๆ เพื่อตอบสนองต่อสถานการณ์การก่อการร้ายทางไซเบอร์ในประเทศไทยและสถานการณ์ที่อาจจะเกิดขึ้นในประเทศไทยในอนาคต วิจัยนี้จะทบทวนคำจำกัดความของคำว่าการก่อการร้ายทางไซเบอร์เพื่อกำหนดทิศทางการทำนโยบาย และแผนการเตรียมการของหน่วยงานของรัฐต่าง ๆ ที่มีความเสี่ยงของการก่อการร้ายทางไซเบอร์ไปในทางที่ถูกต้อง โดยการใช้เครื่องมือวิจัยในการศึกษาเอกสารและสัมภาษณ์เชิงลึกกับเจ้าหน้าที่ที่ทำงานด้ายไซเบอร์ของแต่ละองค์กร เพื่ออธิบายสถานการณ์การก่อการร้ายทางไซเบอร์และวิธีจัดการกับมันในอนาคต

ผลการศึกษาพบว่าสถานการณ์การก่อการร้ายไซเบอร์ในประเทศไทยนั้นเป็นเพียงแค่ภัยคุกคามทางไซเบอร์เท่านั้น แต่ถึงอย่างไรก็ตามหน่วยงานภาครัฐของไทยก็มีศักยภาพในเรื่องของการออกกฎหมาย การใช้งบประมาณ และการเข้าถึงทางเทคโนโลยีอย่างปลอดภัยสำหรับประชาชน หากพิจารณาไปยังจุดอ่อนพบว่าประเทศไทยยังต้องมีการปรับปรุงในเรื่องของการบังคับใช้กฎหมาย ข้อบกพร่องทางเทคโนโลยี และจำนวนบุคลากรที่มีความรู้ความสามารถ เพื่อลดจุดอ่อนที่กล่าวมา รัฐบาลจำเป็นต้องสร้างสภาพแวดล้อมที่ไม่เอื้ออำนวยต่อการกระทำความผิดทางไซเบอร์ สร้างช่องทางทางอินเทอร์เน็ตใหม่ โดยที่รัฐสามารถควบคุมช่องทางทางไซเบอร์ได้ เพิ่มหลักสูตรความมั่นคงไซเบอร์ในโรงเรียนและมหาวิทยาลัย สร้างเครือข่ายสำรองกับประเทศอื่น ๆ หรือกับภาคเอกชนอื่น ๆ เพื่อรองรับการโจมตี

สาขาวิชา	อาชญาวิทยาและงานยุติธรรม	ลายมือชื่อนิสิต .....
ปีการศึกษา	2564	ลายมือชื่อ อ.ที่ปรึกษาหลัก .....

6181362224 : MAJOR CRIMINOLOGY AND CRIMINAL JUSTICE
KEYWORD: Cyberterrorism, Computer crimes

Natthamon Petchkla : Government sector's Response in Counter-Cyber-Terrorism in Thailand . Advisor: Assoc. Prof. SUMONTHIP CHITSAWANG, Ph.D.

Since the internet was invented, the global community has been rapidly changed by the advance of technology in cyberspace. A prominent issue now confronting society though, is the increase of cyberattacks which can be linked to cyber-terrorism. Individual countries in the world are now starting to address the concerns of cyberterrorism as a new means to achieve political goals. Thailand is one of these countries that has just started to pay this issue attention, but is not as advanced in dealing with the issue as some other nations are. In order to respond to the current cyber-terrorism situation in Thailand, this research will review the definition of cyber terrorism to examine the current cyber situation. Furthermore, it will study all the preparation of various government agencies at the risk of cyber. The methods that have been used in this research are studying documents and conducting in-depth interviews with cybersecurity staff of each organization to describe the situation and how to deal with cyber-terrorism in Thailand.

The results revealed that the cyber-terrorism situation in Thailand is merely a cyber-threat. However, Thai government agencies have the potential to enact laws. Moreover, budget use and secure access to technology for citizens. Considering the weaknesses, Thailand still needs to improve in law enforcement, technology flaw and the number of the government officers who are specialize in cyber security in order to mitigate the aforementioned weaknesses. Government needs to create an unfavorable environment for cyber-crimes. Creating a new internet channel whereby the state can control cyber channels. Increasing cybersecurity courses in schools and universities. Also building a backup network with other countries or with other private sectors to respond the attack.

Field of Study:	Criminology and Criminal Justice	Student's Signature .....
Academic Year:	2021	Advisor's Signature .....

กิตติกรรมประกาศ

วิทยานิพนธ์หัวข้อเรื่อง การรับมือของภาครัฐกับการก่อการร้ายไซเบอร์ในประเทศไทย สำเร็จขึ้นได้มาจากการทุ่มเทกายและใจของผู้วิจัย อาจารย์ที่ปรึกษา คณะกรรมการสอบวิทยานิพนธ์ โครงการปริญญาเอกกาญจนาภิเษก (คปก.) สำนักงานกองทุนสนับสนุนการวิจัย และสำนักงานกองทุนสนับสนุนการวิจัย (สกว.) ผู้วิจัยขอขอบพระคุณรองศาสตราจารย์ ดร.สุมนทิพย์ จิตสว่าง อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก ที่ให้คำปรึกษาในการทำวิจัยตลอดมา รองศาสตราจารย์ ดร.ศรีสมบัติ โชคประจักษ์ชัด ประธานกรรมการ ที่มอบคำแนะนำที่มีประโยชน์ทำให้งานวิจัยมีความสมบูรณ์มากขึ้น นอกจากนี้ขอขอบพระคุณ รองศาสตราจารย์วันชัย มีชาติ ผู้ช่วยศาสตราจารย์ ดร.ฐิติยา เพชรมุนี พล.ต.ต.ดร.พรชัย ขันตี ซึ่งเป็น กรรมการ และกรรมการภายนอกมหาวิทยาลัยที่เสียสละเวลาในการอ่านวิทยานิพนธ์และให้คำแนะนำเพื่อให้วิทยานิพนธ์เล่มนี้ลุล่วงไปได้ด้วยดี

ในส่วนของข้อมูลสำหรับวิทยานิพนธ์เล่มนี้ ผู้วิจัยขอขอบพระคุณผู้ให้ข้อมูลสำคัญจากทุกหน่วยงานของภาครัฐ รวมไปถึงคณะอาจารย์แห่งมหาวิทยาลัย Sheffield สหราชอาณาจักร ที่มอบความรู้ที่เป็นประโยชน์อย่างมากกับวิทยานิพนธ์ชิ้นนี้ และเปิดโอกาสให้ผู้วิจัยได้ออกไปสัมผัสบรรยากาศในต่างประเทศที่ทำให้ผู้วิจัยมีกำลังใจที่จะมุ่งมั่นทำงานให้สำเร็จ

ผู้วิจัยขอขอบพระคุณครอบครัว พ่อ แม่ และพี่ไซม่อน ที่สนับสนุนทั้งงบประมาณ กำลังใจ และสถานที่พักอาศัยระหว่างการเก็บข้อมูลเพื่อให้งานวิจัย และสำคัญที่สุดผู้วิจัยต้องขอบคุณตัวเองเป็นอย่างมากที่ไม่ท้อแท้ใน

การทำวิทยานิพนธ์ ผู้วิจัยหวังว่าผลงานชิ้นนี้จะมีคุณค่าและเป็นประโยชน์ต่อสังคมไม่มากก็น้อย และเป็นประโยชน์ต่อหน่วยงานที่เกี่ยวข้องในการศึกษาค้นคว้าต่อไป

นัทธมน เพชรกล้า

สารบัญ

หน้า

สารบัญตาราง

หน้า

สารบัญภาพ

หน้า

บทที่ 1

บทนำ

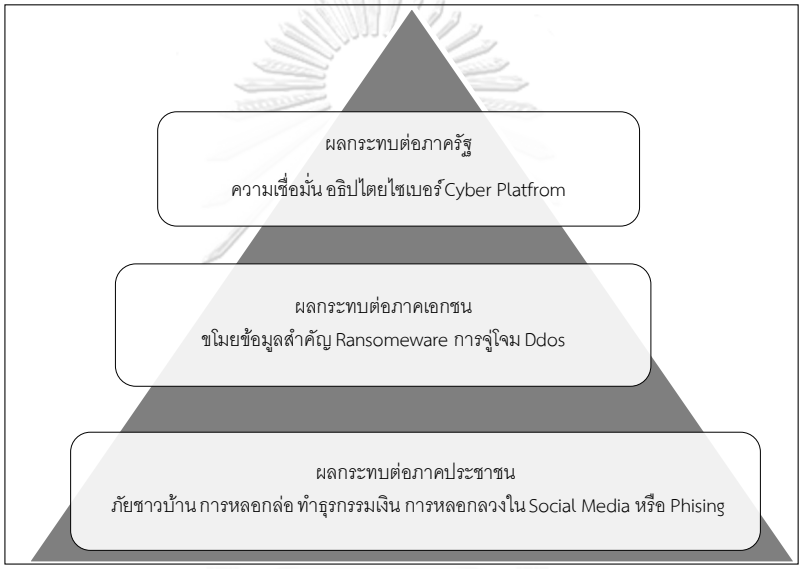
1.1 ที่มาและความสำคัญของปัญหา

ที่มาของงานวิจัยเกิดขึ้นจากวิวัฒนาการ (Evolution) ของอาชญากรรมที่มีรูปแบบเปลี่ยนไปจากการก่ออาชญากรรมแบบดั้งเดิม (Traditional Crime) ไปสู่การก่ออาชญากรรมแบบใหม่ (Non – Traditional Crime) หรือ อาชญากรรมไซเบอร์ (Cyber Crime) ตามบริบทของสังคมที่มีเทคโนโลยีในการขับเคลื่อน การก่อการร้ายทางไซเบอร์ (Cyber-Terrorism) ถือเป็นรูปแบบหนึ่งของอาชญากรรมไซเบอร์ ที่สามารถสร้างความหวาดกลัวได้มากกว่าการก่อการร้ายแบบธรรมดา ด้วยเหตุนี้จึงเป็นที่มาของงานวิจัยที่มุ่งประเด็นความสนใจไปยังการใช้กลยุทธ์ดั้งเดิมของการก่อการร้ายภายใต้เครื่องมือรูปแบบใหม่ที่สามารถก้าวข้ามความเป็นเขตแดนของรัฐชาติผ่านเครือข่ายของคอมพิวเตอร์ และนอกจากนี้การศึกษาทิศทางการก่อการร้ายทางไซเบอร์ยังไม่ค่อยมีแพร่หลายนักในประเทศไทย และเทคนิคใหม่ของผู้ก่อการร้ายนั้นจะก่อให้เกิดผลกระทบอย่างมหาศาลโดยที่ไม่ต้องลงทุนอย่างมากมาย และเหตุนี้จึงเป็นสิ่งจำเป็นที่งานวิจัยนี้จะต้องเร่งศึกษาเพื่อเสนอวิธีรับมือและป้องกันให้กับรัฐบาล โดยวิธีการแสวงหาความจริงเพื่อตอบคำถามของวิจัยเล่มนี้จะทำโดยการศึกษาวิธีการโจมตีในรูปแบบของการก่อการร้ายทางไซเบอร์เพื่อที่จะบรรลุจุดประสงค์ที่วางไว้

ในปัจจุบันรูปแบบของอาชญากรรมเกือบทุกประเภทสามารถเกิดขึ้นได้บนโครงข่ายอินเทอร์เน็ต ทำให้ภัยคุกคามนั้นมีความหลากหลายและยากที่จะป้องกัน ภัยคุกคามที่เกิดขึ้นปัจจุบันจะใช้พื้นที่ทางไซเบอร์ (Cyber Space) เป็นเครื่องมือในการโจมตี ก่ออาชญากรรมหลายประเภท เช่น การปลอมแปลง บิดเบือนข้อมูล การฉ้อโกงเงิน ขโมยข้อมูลส่วนตัว มากไปกว่านั้นอินเทอร์เน็ตยังเปิดช่องว่างให้กับโจรผู้ร้ายที่ใช้เป็นเครื่องมือในการล่อลวงเด็กและเยาวชน ไม่ว่าจะเป็นการเผยแพร่คลิปอนาจารหรือการค้ามนุษย์

นอกจากนี้ภัยคุกคามทางอินเทอร์เน็ตยังรวมไปถึงการโจมตีในระดับประเทศ การโจมตีจากรัฐบาลประเทศอื่นผ่านการโจรกรรมข้อมูลเพื่อจุดประสงค์ของการสืบเสาะข้อมูลลับ หรือเพื่อเข้ามาต่อรอง ประนีประนอม และควบคุมฝ่ายตรงข้ามกับรัฐบาลของตน โดยสามารถใช้วิธีการที่แตกต่างกัน เช่น การใช้มัลแวร์ (Malware) หมายถึงการรูปแบบหนึ่งของซอฟต์แวร์ ที่เป็นอันตรายต่อผู้ที่ได้รับ เช่น ไวรัส และ Ransomware การใช้เทคนิค Phishing เพื่อสร้างแรงจูงใจในการเปิดไฟล์ (ที่มีมัลแวร์อันตรายแนบไว้) การโจมตีเซิร์ฟเวอร์โดยการเขียนโปรแกรมที่ใช้สื่อสารกับฐานข้อมูลภายใน

เซิร์ฟเวอร์ด้วยเทคนิค SQL ที่จะสามารถเปิดโอกาสให้ผลกระทบที่มีจะเกิดกับระบบโดยตรง ส่วนใหญ่มักจะใช้จู่โจมกับหน่วยงานที่เป็นสถาบันทางการเงิน ในขณะเดียวกันการโจมตียังมีในรูปแบบของการโจมตีผู้ใช้งานเว็บไซต์ผ่านการใช้โค้ด XSS (Cross-Site Scripting) เพื่อให้ผู้ใช้ได้รับผลกระทบโดยตรง นอกจากนี้ยังมีวิธีดั้งเดิมที่ใช้ในการจู่โจมระบบ เช่น การแฮกข้อมูล (Hack) และการโจมตีแบบ DoS (Denial of Service) ที่ทำให้การบริการต่าง ๆ ไม่สามารถใช้งานได้ โดยเฉพาะหน่วยงานเกี่ยวกับสาธารณูปโภคสำคัญ (Critical Infrastructure) ส่งผลให้ประชาชนในประเทศเดือดร้อน ดังจะเห็นได้จากลำดับขั้นของภัยคุกคามในภาพ



รูปที่ 1 ผลกระทบของภัยคุกคามทางไซเบอร์

การโจมตีผ่านช่องทางอินเทอร์เน็ตมีการพัฒนาความรุนแรงมากขึ้นตั้งแต่ในทศวรรษ 1950 เทคโนโลยีถูกนำมาพัฒนาเกิดเป็นอาวุธนิวเคลียร์ สหรัฐอเมริกานำอาวุธนิวเคลียร์ข้าประจำการอย่างเป็นระบบภายใต้พื้นฐานทางเทคโนโลยี เรียกอาวุธทางเทคโนโลยีสารสนเทศนี้ว่า “ลอจิก บอมบ์” หรือ ซอฟต์แวร์ชุดคำสั่งที่ปิดระบบหรือเครือข่าย และ/หรือลบข้อมูลหรือซอฟต์แวร์ในเครือข่าย ใช้เพื่อลอบวางระเบิดเสมือนจริงในประเทศอื่น เหตุการณ์ครั้งประวัติศาสตร์ที่ถูกจารึกไว้ในชื่อของ “The Original Logic Bomb” (คลาร์ก, 2555) สมัยสงครามเย็นเมื่อปี 1982 หน่วย CIA ของสหรัฐอเมริกาถูกกล่าวหาว่าเป็นผู้คิดระบบในการทำลายท่อส่งก๊าซไซบีเรียที่จะนำก๊าซไปยังประเทศรัสเซียโดยไม่ต้องใช้ระเบิดในเชิงกายภาพ แต่เป็นเพียงแค่การใช้รหัสคอมพิวเตอร์มุ่งเจาะทำลายระบบ การระเบิดครั้งนี้เป็นครั้งแรกในประวัติศาสตร์การก่อการร้ายไซเบอร์ที่ส่งผลต่อความเสียหายเชิงกายภาพ ภัยคุกคามไซเบอร์ยังคงพัฒนาขีดความสามารถในการทำลายอย่างต่อเนื่อง สงครามไซเบอร์ครั้งใหญ่อีก

ครั้งหนึ่งในประวัติศาสตร์ นั่นคือ สงครามเว็บครั้งที่ 1 (Web War One) สงครามครั้งนี้เกิดขึ้นกับประเทศเอสโตเนีย ในปี 2007 ถูกโจมตีด้วยระบบคำสั่ง ดีดีโอเอส (Distribute Denial of Service: DDOS) หรือการโจมตีเซิร์ฟเวอร์ด้วยการระดมคำสั่งเป็นสาเหตุทำให้การบริการโดยโครงข่ายอินเทอร์เน็ตทั้งหมดถูกระงับประชาชนเอสโตเนียไม่สามารถใช้บริการธนาคารออนไลน์, เว็บไซต์สื่อหรือบริการอิเล็กทรอนิกส์ของรัฐบาลได้ หลังเอสโตเนีย โดนโจมตี องค์การสนธิสัญญาแอตแลนติกเหนือหรือนาโต (NATO) จัดตั้งศูนย์กลางกลาโหมเพื่อป้องกันภัยไซเบอร์ ดำเนินการอย่างเป็นทางการเมื่อ 2008(คลาร์ก, 2555)

สถานการณ์ภัยคุกคามไซเบอร์ในประเทศไทยเห็นได้ชัดเจนจากเหตุการณ์ล่าสุดของการโจมตีโรงพยาบาลสระบุรีที่ถูกไวรัสเรียกค่าไถ่กว่า 6 หมื่นล้านบาท จากการสอบเบื้องต้นพบว่าเป็นมัลแวร์จากยุโรปทำให้เกิดสถานการณ์วุ่นวายในโรงพยาบาล ไม่ว่าจะเป็นข้อมูลของผู้ป่วย ระบบการสั่งยา ระบบการจ่ายค่ารักษาพยาบาล (ทีเอ็นเอ็น, 2563) นอกจากนี้ยังมีเหตุการณ์ในอดีตที่กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) ถูกโจมตีผ่านปฏิบัติการ DDoS เหตุการณ์การกดปุ่ม F5 หรือปุ่มรีเฟรชติดกันหลาย ๆ ครั้งเพื่อให้ระบบเกิดความสับสนเป็นวิธีเชิงสัญลักษณ์ ซึ่งเป็นรูปแบบที่ใกล้เคียงกับการก่อการร้ายไซเบอร์มากที่สุด โดยหลังจากที่มีการแชร์ข้อความในสื่อสังคมออนไลน์ให้ประชาชนรวมตัวกันต่อต้านระบบซิงเกิลเกตเวย์ (Single Gateway) เพื่อควบคุมอินเทอร์เน็ตของประเทศ โดยให้ผู้ที่มีแนวคิดเดียวกันใช้อินเทอร์เน็ตเปิดเว็บไซต์เป้าหมายก่อนที่จะกดปุ่ม F5 หรือปุ่มรีเฟรชพร้อมกันหลาย ๆ ครั้งเพื่อทำให้เว็บไซต์ไม่สามารถรองรับการเข้าชมของคนจำนวนมาก เป็นเหตุทำให้เว็บไซต์ล่ม จากเหตุการณ์นี้มีการตั้งสมติฐานว่าเป็นการกระทำของคนไทยหรือเป็นฝีมือของชาวต่างชาติ

นอกจากเหตุการณ์ข้างต้น ยังมีการโจมตีรูปแบบอื่น ๆ ที่แตกต่างออกไป เช่น ปฏิบัติการข่าวสาร (Information Operations: IO) เป็นการเข้าไปเปลี่ยนแปลงข่าวสารเพื่อให้ประชาชนเกิดความเข้าใจผิดในการรับรู้ บางครั้งอาจทวีความรุนแรงขึ้นเป็นในระดับของสงคราม IO เช่น การพยายามจะบิดเบียนข้อมูลของฝั่งภาครัฐและยุยงให้เกิดความปั่นป่วนในหมู่ประชาชนส่งผลให้ความเชื่อมั่นกับรัฐบาลลดลง (ณัฐโชติ ดุสิตานนท์ & เสฏฐวุฒิ แสนนาม, 2563)

จากสถิติการแจ้งเหตุภัยคุกคามด้าน ไซเบอร์ที่เกิดขึ้นในประเทศไทยโดยจำแนก ประเภทภัยคุกคามออกเป็น 9 ประเภท (สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน), 2562) พบการแจ้งเหตุภัยคุกคาม ทั้งสิ้น 3,797 เรื่องโดยสามารถจัดลำดับตามจำนวนเหตุภัยคุกคามที่ ได้รับแจ้งออกเป็นประเภทใหญ่ ๆ ได้โดยภัยคุกคามส่วนใหญ่ประมาณร้อยละ 26.9 (จำนวน 1,021 เรื่อง) เป็นภัยคุกคามที่เกิดจากโปรแกรมหรือซอฟต์แวร์ที่ถูกพัฒนาขึ้นเพื่อส่ง ให้เกิดผลลัพธ์ ที่ไม่พึงประสงค์กับผู้ใช้งานหรือระบบ (Malicious Code) และประมาณร้อยละ 26.9 (จำนวน 1,021 เรื่อง) เป็นภัยคุกคามที่เกิดกับระบบที่ถูกบุกรุก/เจาะเข้าระบบได้สำเร็จและระบบถูก ครอบครองโดยผู้ที่ไม่ได้รับ

อนุญาต (Intrusions) ในส่วนภัยคุกคามที่รองลงมาประมาณร้อยละ 26.4 (จำนวน 1,002 เรื่อง)เป็นภัยคุกคามภัยที่เกิดจากการฉ้อฉลฉ้อโกงหรือการหลอกลวงเพื่อผลประโยชน์ (Fraud) และลำดับสุดท้ายประมาณร้อยละ 18.6 (จำนวน 706 เรื่อง) เป็นภัยคุกคาม ที่เกิดจากความพยายามจะบุกรุก/เจาะเข้าระบบ (Intrusion Attempts) (ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย) (สำนักงานรัฐบาลอิเล็กทรอนิกส์, 2562)

จากการศึกษาผ่านการติดตามข่าวสาร ประเทศไทยเป็นประเทศหนึ่งที่มีความตระหนักรู้ในเรื่องของภัยคุกคามทางไซเบอร์เห็นได้จากการออกพระราชบัญญัติความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 ("การออกพระราชบัญญัติความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562," 2562) การตั้งหน่วยงาน ประเทศไทยมีการเตรียมตัวรับมือกับภัยคุกคามไซเบอร์โดยทั้งในรูปแบบของนโยบายรัฐและกฎหมาย มีกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นหน่วยงานหลักในการออกกฎเกณฑ์ควบคุม ดูแล ภารกิจที่เกี่ยวข้องกับไซเบอร์ทั้งหมด มีพระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ซึ่งเป็นกลไกเฝ้าระวัง ป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ที่อาจเกิดกับระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศสำคัญ (CII) และส่งผลเสียหายในระดับประเทศ นอกจากนี้ยังมีการจัดตั้งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กปช.) คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยทางไซเบอร์ (กกช.) คณะกรรมการส่งเสริมการรักษาความมั่นคงปลอดภัยไซเบอร์โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (กสส.) จัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และคณะกรรมการกำกับดูแลสำนักงาน กำหนดกรอบนโยบายและแผน แนวทางการบริหารจัดการ กำหนดโครงสร้างพื้นฐานสำคัญทางสารสนเทศและแนวทางการประสานงานแนวทางการรับมือภัยคุกคามทางไซเบอร์ (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน), 2561) นอกจากนี้ยังกำหนดบทลงโทษซึ่งประกอบไปด้วยบทกำหนดโทษเจ้าหน้าที่และพนักงานสอบสวน บทกำหนดโทษหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ บทกำหนดโทษผู้กระทำความผิด ฝ่าฝืน ขัดขวาง และไม่ปฏิบัติตามคำสั่งคณะกรรมการ

แต่อย่างไรก็ตามการออกพระราชบัญญัติความมั่นคงปลอดภัยทางไซเบอร์ ยังไม่สามารถที่จะกำหนดได้ว่าประเทศไทยมีการเตรียมความพร้อมรับมือกับการก่อการร้ายที่เหมาะสมและเพื่อการศึกษาถึงประสิทธิภาพของการเตรียมการรับมือภัยคุกคามทางไซเบอร์ในรูปแบบการก่อการร้ายนั้น ผู้วิจัยจึงเลือกศึกษาหน่วยงานที่มีความเสี่ยงที่จะเป็นเป้าหมายให้กับผู้ก่อการร้ายทางไซเบอร์ อันได้แก่ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กระทรวงยุติธรรม สภาความมั่นคงแห่งชาติ กระทรวงสาธารณสุข การไฟฟ้าส่วนภูมิภาค กสทช. ธนาคารแห่งประเทศไทย หน่วยงานเหล่านี้มีความสำคัญที่คอยควบคุมการใช้ปัจจัยพื้นฐานของประชาชน เพราะฉะนั้นการศึกษาความตระหนักรู้ของหน่วยงาน

เหล่านี้จะช่วยให้สามารถแสดงให้เห็นถึงระดับการเตรียมพร้อมรับมือภัยคุกคามจากไซเบอร์ในรูปแบบของการก่อการร้ายได้อย่างดี

1.2 โจทย์วิจัยและปัญหาวิจัย

1. ศักยภาพการรักษาความมั่นคงปลอดภัย ป้องกัน ปราบปราม และรับมือภัยคุกคามด้านการก่อการร้ายไซเบอร์ของหน่วยงานภาครัฐไทยในปัจจุบันเป็นอย่างไร
2. แนวทางการรักษาความมั่นคงปลอดภัย ป้องกัน ปราบปราม และรับมือภัยคุกคามด้านการก่อการร้ายไซเบอร์ของหน่วยภาครัฐไทยในปัจจุบันเป็นอย่างไร
3. หน่วยงานภาครัฐด้านการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์ หน่วยงานด้านการปราบปรามภัยคุกคามไซเบอร์ และหน่วยงานที่มีความเสี่ยงต่อภัยคุกคามไซเบอร์รวมทั้ง เจ้าหน้าที่ภาครัฐ ควรมีแนวทางในการรับมือการก่อการร้ายไซเบอร์และพัฒนาแนวทางนั้นให้เกิดประสิทธิภาพอย่างไร

1.3 วัตถุประสงค์

1. เพื่อศึกษาศักยภาพการรักษาความมั่นคงปลอดภัย ป้องกัน ปราบปราม และรับมือภัยคุกคามด้านการก่อการร้ายไซเบอร์ของหน่วยงานภาครัฐไทยในปัจจุบัน
2. เพื่อศึกษาแนวทางการรักษาความมั่นคงปลอดภัย ป้องกัน ปราบปราม และรับมือภัยคุกคามด้านการก่อการร้ายไซเบอร์ของหน่วยงานภาครัฐไทยในปัจจุบัน
3. เพื่อศึกษาการรับมือภัยคุกคามจากการก่อการร้ายไซเบอร์ของหน่วยงานภาครัฐไทยในปัจจุบัน

1.4 ขอบเขตการวิจัย

ศึกษาศักยภาพการรักษาความมั่นคงปลอดภัย ป้องกัน ปราบปราม และรับมือภัยคุกคามจากการก่อการร้ายไซเบอร์ (Cyber Terrorism) ที่เกิดขึ้นกับหน่วยงานภาครัฐไทย ณ ปัจจุบัน ศึกษาแผนการเตรียมรับมือของหน่วยงานต่าง ๆ ของรัฐบาลที่มีความเสี่ยงต่อการเกิดการก่อการร้ายไซเบอร์ รวมไปถึงศึกษาความตระหนักรู้ของเจ้าหน้าที่มีส่วนเกี่ยวข้อง เพื่อนำมาคาดการณ์สถานการณ์การก่อการร้ายทางไซเบอร์ที่จะเกิดกับประเทศไทยในอนาคต

1.5 นิยามศัพท์ที่ใช้ในงานวิจัย

1. การก่อการร้ายไซเบอร์ หมายถึง การใช้คอมพิวเตอร์เป็นเครื่องมือรวมทั้งเป็นเป้าหมายในการก่อการร้าย โดยมีการเตรียมตัวและมีผลประโยชน์ทางการเมืองเป็นแรงกระตุ้นในการจู่โจมระบบ ขโมย บิดเบือนข้อมูล หรือทำลาย ในระบบคอมพิวเตอร์ ที่ส่งผลให้เกิดความเสียหายต่อผู้บริสุทธิ์ (คลาร์ก, 2563)

2. หน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ หรือ “Critical Infrastructure (CI)” คือ องค์กรหรือส่วนงานหนึ่งส่วนงานใดของหน่วยงานนั้นมีผลเกี่ยวเนื่องสำคัญต่อความมั่นคงหรือความสงบเรียบร้อยของประเทศหรือต่อสาธารณชน เช่น หน่วยงานด้านความมั่นคงของรัฐ, หน่วยงานด้านบริการภาครัฐที่สำคัญ, หน่วยงานด้านการเงินการธนาคาร, หน่วยงานด้านเทคโนโลยีสารสนเทศและโทรคมนาคม (อีทีดีเอ, 2561)

3. คณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช) หรือภาษาอังกฤษเรียกว่า National Cyber Security Committee (NCSC) มีอำนาจหน้าที่สำคัญในการเสนอนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ กำหนดนโยบายารบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จัดทำแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์เสนอต่อคณะรัฐมนตรีสำหรับเป็นแผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ในสถานการณ์ปกติและในสถานการณ์ที่อาจเกิดหรือเกิดภัยคุกคามทางไซเบอร์ กำหนดมาตรฐานและแนวทางการส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ สร้างมาตรฐานกำหนดมาตรฐานขั้นต่ำที่เกี่ยวข้องกับคอมพิวเตอร์ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ รวมถึงส่งเสริมการรับรองมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานเอกชน ("การออกพระราชบัญญัติความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562," 2562)

4. ศักยภาพในการรับมือภัยคุกคามทางไซเบอร์ คือ ความสามารถสูงสุดที่เป็นไปได้ในการรับมือภัยคุกคามทางไซเบอร์ที่ได้กล่าวถึงในการทำวิจัยฉบับนี้ ประกอบไปด้วยศักยภาพทางด้านกฎหมายและกลยุทธ์ ศักยภาพในการบังคับใช้กฎหมายและกลยุทธ์ ศักยภาพของทรัพยากรบุคคล ศักยภาพของเทคโนโลยีและงบประมาณ (Denning, 2001)

1.6 ประโยชน์ที่คาดว่าจะได้รับ

1. สามารถประเมินศักยภาพของหน่วยงานภาครัฐด้านการกำกับดูแลความมั่นคงปลอดภัยไซเบอร์หน่วยงานด้านการป้องกันและปราบปรามภัยคุกคามไซเบอร์ และหน่วยงานที่มีความเสี่ยงต่อภัยคุกคามด้านการก่อการร้ายไซเบอร์ของไทยในปัจจุบัน

2. สามารถประเมินนโยบายการรักษาความมั่นคงปลอดภัย ป้องกัน ปราบปราม และรับมือการก่อการร้ายไซเบอร์ของหน่วยงานภาครัฐ

3. สามารถเรียนรู้แก้ไขจุดบกพร่องและส่งเสริมศักยภาพของหน่วยงานภาครัฐในการรักษาความมั่นคงปลอดภัย ป้องกัน ปราบปราม และรับมือการก่อการร้ายไซเบอร์

4. นำผลที่ได้ไปพัฒนานโยบายการรักษาความมั่นคงปลอดภัย ป้องกัน ปราบปราม และรับมือการก่อการร้ายไซเบอร์ที่จะเกิดขึ้นได้ในอนาคต

บทที่ 2

แนวคิด ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

สิ่งที่เปลี่ยนแปลงอย่างเป็นที่ประจักษ์ในศตวรรษที่ 21 นั่นคือโลกคู่ขนานที่เปรียบเสมือนโลกความจริงในทุก ๆ มิติ สังคม เศรษฐกิจ หรือการเมือง จะได้รับอิทธิพลจากอินเทอร์เน็ต ซึ่งบางครั้งอาจจะถูกมองว่าอินเทอร์เน็ตจะเอื้อประโยชน์ต่อสังคมทำให้การติดต่อสื่อสารรวดเร็วและสะดวกมากขึ้น แต่ในความสะดวกรวดเร็วนั้นอาจเป็นเหมือนดาบสองคมแก่สังคมที่อนุญาตให้คนร้ายแสวงหาผลประโยชน์โดยใช้อินเทอร์เน็ตเป็นเครื่องมือในการหลอกลวงประชาชน ส่งผลให้รัฐบาลจะเป็นต้องตั้งมาตรการในการสอดส่องดูแลพฤติกรรมการกระทำความผิดทางไซเบอร์ที่จะส่งผลให้เกิดความเสียหายทั้งทางชีวิตและทรัพย์สิน

ความรุนแรงที่เกิดขึ้นจากภัยทางไซเบอร์มีทั้งในระดับเล็กน้อยไปจนไปถึงภัยระดับชาติ ความขัดแย้งที่เกิดขึ้นไม่ว่าจะด้วยวัตถุประสงค์การเมือง เศรษฐกิจ หรือ สังคม จะใช้ไซเบอร์ (Cyberspace) เป็นเครื่องมือและเป็นพื้นที่ในการสู้รบ โจมตี ก่อการร้าย รวมไปถึงการก่อสงคราม โดยพื้นฐานแล้วลักษณะภัยคุกคามเหล่านี้จะไม่เปลี่ยนแต่จะได้รับแรงสนับสนุนจากไซเบอร์ทำให้ โจรผู้ร้ายสามารถก่ออาชญากรรมได้รวดเร็วมากขึ้น และสร้างผลกระทบได้รุนแรงและแม่นยำกว่าที่ผ่านมา การป้องกันระบบความปลอดภัยทางไซเบอร์จึงเป็นเรื่องที่ยากต่อการควบคุม เพราะความเป็นพลวัตรของโลกไซเบอร์ที่มีการเปลี่ยนแปลงตลอดเวลาทำให้การวางแผนยุทธศาสตร์และกลยุทธ์ไม่มีความเสถียร ดังนั้นศึกษาการโจมตีทางไซเบอร์ (Cyber Attack) เพื่อนำมาจัดแยกแยะประเภทและหาความหมายให้ผู้ที่ไม่มีความรู้เฉพาะทางด้านไซเบอร์เข้าใจและเตรียมรับมือการโจมตีทางไซเบอร์ (Cyber Attack) ได้มากที่สุด ในบทนี้จะนำประเด็นทั้งหมดที่เกี่ยวข้อกับการศึกษาความตระหนักรู้ของภาครัฐในการรับมือกับการก่อการร้ายทางไซเบอร์ มานำเสนอ ดังนี้

1. นิยามการก่อการร้ายสากล (Definitions of Terrorism)
2. นิยามการก่อการร้ายไซเบอร์ (Definitions of Cyber Terrorism)
3. องค์กรอาชญากรรมข้ามชาติและการก่อการร้ายทางไซเบอร์ (Organizational Cyber Terrorism)
4. จิตวิทยากับการก่อการร้ายไซเบอร์ (The Psychology of Cyber-Terrorism)
5. ทฤษฎีอาชญาวิทยาและทฤษฎีการก่อการร้ายกับไซเบอร์ (Criminology Theories and Terrorism Theories)

6. โครงสร้างพื้นฐานสำคัญของประเทศและการก่อการร้ายไซเบอร์ (Critical National Infrastructure and Cyber terrorism)

7. ประวัติศาสตร์การโจมตีไซเบอร์และประเภทของการโจมตี (History of Cyber-Terrorism and Types of Attacks)

8. สถานการณ์การก่อการร้ายไซเบอร์ในต่างประเทศ (Assessing the Risks of Cyber Terrorism in Global Context)

9. สถานการณ์และยุทธศาสตร์การต่อต้านการก่อการร้ายไซเบอร์ของประเทศไทย (Cyber Security situation and Strategies for Thailand)

2.1 นิยามการก่อการร้ายสากล (Definitions of Terrorism)

นิยามของการก่อการร้ายในทางวิชาการมีความกระจัดกระจาย แตกต่างตามจุดมุ่งหมายของแต่ละสำนักกล่าวได้ว่า นิยามการก่อการร้ายนั้นยังไม่เป็นสากล และยังเป็นประเด็นที่โต้แย้งกันอยู่ในปัจจุบันนี้ (Schmid, 2011) นักวิชาการในสาขาสังคมศาสตร์ได้พัฒนานิยามการก่อการร้ายให้เหมาะสมกับรูปแบบ (Models) ที่ใช้สำหรับการทำวิจัยในเฉพาะสาขา ทำให้บางครั้งความหมายและนิยามของการร้ายแตกต่างออกไป เช่น ตำรวจมองว่า การก่อการร้ายเป็นปัญหาทางทหาร (Military Problem) ในขณะเดียวกัน ทหารกลับมองว่าปัญหาการก่อการร้ายเป็นปัญหาของกระบวนการยุติธรรม (Criminal Justice) นักกฎหมายก็จะให้นิยามการก่อการร้ายไปในทางกฎหมายทั่วไป (Legal Definition) ส่วนพนักงานอัยการก็จะมองในมองของ ประมวลกฎหมายอาญา (Criminal Codes) จึงเป็นสาเหตุให้ความหมายของการก่อการร้ายขึ้นอยู่กับมุมมองและทัศนคติของแต่ละสายอาชีพ จากแนวทางการให้คำจำกัดความแต่ละแบบสามารถสรุปได้ดังตารางที่ 1

ตารางที่ 1 คำจำกัดความการก่อการร้าย

ประเภท (Type)	คำจำกัดความ (Definition)
แบบธรรมดาทั่วไป	ความรุนแรงที่เกิดจากการตั้งใจกระทำขึ้นเพื่อมุ่งหวังให้เกิดความกลัวเกิดการเปลี่ยนแปลงขึ้น
ในแง่กฎหมาย	ความรุนแรงทางด้านอาชญากรรมที่ละเมิดต่อกฎหมายอาญาและรัฐมีมาตรการลงโทษกำหนดไว้
เชิงวิเคราะห์	มีปัจจัยทางด้านการเมืองและสังคมโดยเฉพาะอยู่เบื้องหลังการโจมตีหรือการกระทำการองผู้ก่อการร้ายแต่ละคน
รัฐสนับสนุน	รัฐเล็ก ๆ ที่ใช้กลุ่มก่อการร้ายไปดำเนินการในรัฐอื่น และกรณีรัฐในค่ายคอมมิวนิสต์โจมตีหรือทำลายผลประโยชน์องค่ายตะวันตก
รัฐ	การใช้กำลังอำนาจของรัฐบาลทำให้เกิดความหวานกลัวหรือความกดดันหมู่ของประชาชนตนเองเพื่อให้เชื่อฟังและอยู่ภายใต้อำนาจ

ที่มา: Schmid (2011)

ปัญหาต่าง ๆ ที่เกี่ยวข้องกับการตีความคำนิยามการก่อการร้ายยังคงมีความคลุมเครือ คำจำกัดความที่มีอยู่ยังมีทั้งจุดอ่อนและข้อจำกัด Laqueur ได้กล่าวถึงการให้ความหมายของการก่อการร้ายว่าไม่มีคำจำกัดความใดเป็นความมาตรฐานและแต่ละแนวทางก็ปะปนไปด้วยอคติทางการเมืองเป็นพื้นฐาน ความเห็นนี้สอดคล้องกับที่ Schmid ได้กล่าวไว้ ซึ่งผลวิเคราะห์ปรากฏดังข้อต่อไปนี้ (Schmid, 2011)

หลังจากการวิเคราะห์ ค้นคว้า คำจำกัดความของการก่อการร้ายมีมากกว่า 100 ความหมาย Alex Schmid สรุปความได้ดังนี้

1. ลัทธิการก่อการร้ายเป็นแนวคิดทางนามธรรมไม่มีรูปธรรม
2. ความหมายอย่างหนึ่งอย่างใดไม่สามารถใช้แทนความหมายที่เป็นไปได้สำหรับถ้อยคำนี้ในทุกกรณี
3. คำจำกัดความที่แตกต่างกันอย่างมากมายนี้จะมีองค์ประกอบเหมือนกันด้วย

4. ความหมายของการก่อการร้ายจะเป็นความหมายที่ได้จากเหยื่อซึ่งเป็นเป้าหมายเป็นผู้ให้ความหมายหรือกำหนดขึ้น

ในส่วนถัดไปจะพิจารณาแนวทางกฎหมายอาญาและรัฐธรรมนูญแห่งราชอาณาจักรไทย มาใช้เป็นการประกอบการวิเคราะห์เป็นสำคัญ

ประเด็นสำคัญของการนิยามการก่อการร้ายทางการเมืองอยู่ที่การใช้วิธีการรุนแรงเพื่อจุดมุ่งหมายทางการเมือง กล่าวได้ว่า การที่คนร้ายทำร้ายเจ้าหน้าที่รัฐให้ถึงแก่ความตายในขณะปล้นทรัพย์โดยไม่มีจุดมุ่งหมายทางการเมือง ย่อมไม่ใช่การก่อการร้ายทางการเมือง แต่การลอบยิงเจ้าหน้าที่ของรัฐเพื่อสร้างความหวาดกลัวแก่ประชาชน โดยหวังบ่อนทำลายอำนาจรัฐย่อมเป็นการก่อการร้ายทางการเมือง ดังที่มาตรา 133 ตามประมวลกฎหมายอาญา บัญญัติไว้ว่า

ผู้ใดใช้กำลังประทุษร้ายหรือข่มขู่ว่าจะใช้กำลังประทุษร้ายเพื่อ

1. ล้มล้างหรือเปลี่ยนแปลงรัฐธรรมนูญ

2. ล้มล้างอำนาจนิติบัญญัติ อำนาจบริหาร และอำนาจตุลาการแห่งรัฐธรรมนูญหรือให้ใช้อำนาจดังกล่าวแล้วไม่ได้ หรือ

3. แบ่งแยกราชอาณาจักร หรือยึดอำนาจปกครองในส่วนหนึ่งส่วนใดแห่งราชอาณาจักร ผู้นั้น กระทำความผิดฐานกบฏ

การก่อการร้ายทางการเมืองมีลักษณะแตกต่างจากอาชญากรรมองค์กร ถึงแม้อาชญากรรมองค์กรจะมีการใช้ความรุนแรงแต่ก็ทำไปเพื่อผลประโยชน์ของกลุ่มเท่านั้น นอกจากนี้การก่อการร้ายทางการเมืองยังแตกต่างจากการกระทำรุนแรงโดยผู้วิกลจริตที่ไม่ได้มีจุดมุ่งหมายใด ๆ ทางการเมืองเช่นกัน

จุดหมายปลายทางของการก่อการร้ายทางการเมือง คือ การปฏิวัติเพื่อล้มล้างอำนาจของรัฐบาลที่ปกครองอยู่ แต่เป็นที่สังเกตว่า กลุ่มก่อการร้ายจำนวนไม่น้อยที่ไม่มีสมรรถนะเพียงพอที่จะล้มล้างอำนาจรัฐเพื่อสถาปนารัฐบาลใหม่ กลุ่มก่อการร้ายที่สมรรถนะต่ำเหล่านี้จึงได้รับขนานนามว่า “กลุ่มก่อการร้ายที่เป็นรองด้านปฏิวัติ” อย่างที่ Walter ได้จำแนกกระบวนการก่อการร้ายทางการเมืองได้เป็น 3 ขั้นตอน (Walter, 1969) คือ

1. การใช้ความรุนแรงหรือขู่ว่าจะใช้ความรุนแรง

2. ปฏิกิริยาตอบโต้ทางอารมณ์ต่อความรุนแรงหรือการขู่ใช้ความรุนแรงนั้น

3. ผลทางสังคมที่มาจากความรุนแรงและปฏิกิริยาตอบโต้

กล่าวได้ว่ากระบวนการก่อการร้ายไม่ได้ให้ความสำคัญต่อการใช้ความรุนแรงโดยตรง แต่ให้ความสำคัญต่อผลกระทบทางอารมณ์ที่มีต่อมวลชนจากการใช้ความรุนแรง กล่าวอีกในหนึ่ง การสร้างความหวาดกลัว เป็นหัวใจของการก่อการร้าย เพราะฉะนั้น การที่ผู้ก่อการร้ายวางระเบิดสถานที่ไม่ได้

มีจุดประสงค์เพียงแค่ทำลายทรัพย์ของชีวิตคนเพียงอย่างเดียว แต่กลับต้องการที่จะสร้างความหวาดหลัว ให้ประชาชนรู้สึกไม่มั่นคง ไม่เชื่อมั่นต่อรัฐบาล

อย่างไรก็ตาม การก่อการร้าย นั้นสามารถอธิบายถึงการต่อต้านหรือการตอบโต้การกระทำของฝ่ายรัฐบาล ซึ่งเรียกว่า การก่อความไม่สงบ (Insurgency) ถึงแม้จะมีลักษณะเดียวกับการก่อการร้าย แต่โดยความหมายแล้วมีระดับความรุนแรงน้อยกว่า สำหรับจุดมุ่งหมายโดยรวมนั้นยังคงเดิม คือ ต้องการล้มล้างอำนาจรัฐที่มีอยู่เดิม การไม่ยอมรับการปกครองโดยรัฐบาล แต่เพียงการก่อความไม่สงบอยู่ในช่วงของความขัดแย้งระดับต่ำ ซึ่งสามารถอธิบายการกระทำต่าง ๆ (Mickolus, 1978) ได้ดังนี้

การก่อความไม่สงบ (Insurgency) คือ การเคลื่อนไหวของกระบวนการที่มุ่งประสงค์จะล้มล้างอำนาจรัฐที่มีอยู่เดิม เป้าหมายอาจจำกัดอยู่ที่การแยกตัวออกจากการควบคุมของรัฐบาล จนถึงการเข้ายึดอำนาจรัฐ มีการต่อสู้ ใช้อาวุธทำลายฝั่งตรงข้ามแต่มีความรุนแรงไม่เท่ากับสงครามกลางเมือง (Mickolus, 1978)

การบ่อนทำลาย (Subversion) คือ การกระทำที่บั่นทอนอำนาจทางทหาร เศรษฐกิจ การเมือง สังคม หรือกำลังใจของฝ่ายรัฐบาล โดยใช้ความรุนแรงหรือแทรกซึมเข้าไปทำลายล้าง เพื่อการชักจูงให้เป็นไปตามแผนที่วางไว้ (Mickolus, 1978)

การก่อความวุ่นวายของประชาชน (Civil Disturbance) คือ การใช้ประชาชน มวลชน ในการก่อความวุ่นวาย ขัดขวางการปฏิบัติงานของรัฐ เพื่อบั่นทอนการสนับสนุนของรัฐบาล เป็นการกระทำที่แสดงให้เห็นถึงความอ่อนแอของรัฐบาล ทั้งนี้การกระทำอาจจะไม่ใช่การกระทำต่อหน้าแต่เป็นการจัดตั้งหน่วยใต้ดินเพื่อยุยง ชะลอการทำงานของข้าราชการไม่ให้รัฐบาลดำเนินงานได้ (Mickolus, 1978)

การก่อจลาจล (Riot) คือ การก่อความวุ่นวายของประชาชนที่ใช้ความรุนแรงต่อหน้าโดยไม่คำนึงถึงกฎหมาย กระทบกระเทือนถึงความสงบเรียบร้อยของบ้านเมือง (Mickolus, 1978)

การก่อวินาศกรรม (Sabotage) คือ การปฏิบัติการที่มีความประสงค์ในการทำลาย เข้าแทรกแซง การป้องกันประเทศ โดยการทำลายนี้มีวัตถุประสงค์เพื่อการสงคราม (Mickolus, 1978)

สงครามกองโจร (Guerrilla Warfare) คือ การปฏิบัติการของทหาร/แบบทหารในดินแดนของข้าศึก หรือที่ข้าศึกยึดครองอยู่ ด้วยการใช้กำลังไม่ตามแบบ ซึ่งส่วนใหญ่กระทำโดยประชาชนในท้องถิ่นและเป็นการปฏิบัติด้วยความรวดเร็วในระยะเวลาอันสั้น โดยใช้การจู่โจม คล่องแคล่ว และแนบเนียน เป็นการสนับสนุนจากประชาชนในท้องถิ่นหรือกองกำลังจากนอกประเทศ (Mickolus, 1978)

การก่อการร้าย (Terrorism) คือ การใช้ความรุนแรง หรือข่มขู่ว่าจะใช้ความรุนแรง ซึ่งมีการวางแผนไว้ล่วงหน้า เพื่อบรรลุ เป้าหมายทางการเมือง ศาสนา สังคม อุดมการณ์ โดยสร้างความหวาดกลัวให้กับประชาชนเพื่อให้มีความไม่มั่นใจต่อรัฐบาล (Mickolus, 1978)

โดยสรุปคำนิยามของการก่อความรุนแรงที่แตกต่างกันจะขึ้นอยู่กับหลายปัจจัย ไม่ว่าจะเป็น วิธีการ เทคนิค การรบ จุดประสงค์ ความเสียหาย แต่ก็ยังมีจุดร่วมเหมือนกันเช่น จุดประสงค์ทางการเมือง การแย่งอำนาจจากรัฐบาล

การก่อการร้ายแบบดั้งเดิมได้สร้างผลกระทบที่รุนแรงกับสังคมโลกตั้งแต่เหตุการณ์โจมตีตึกแฝดที่สหรัฐอเมริกาและระเบิดครั้งใหญ่ที่ลอนดอน สหราชอาณาจักร ค.ศ. 2005 ความกลัวการก่อการร้ายยกระดับเพิ่มขึ้นอย่างทวีคูณ (Jones, 2005) ในเกือบทุกประเทศจึงมีการนิยามการก่อการร้ายของตนเองให้เหมาะสมกับบริบทและสภาพสังคมของตนและเพื่อความถูกต้องในการบังคับตามกฎหมาย

กระทรวงกลาโหมของสหรัฐอเมริกานิยามการก่อการร้าย คือ การใช้ความรุนแรงกระทำการที่ผิดกฎหมาย ส่วนใหญ่มีแรงขับเคลื่อนจากศาสนา การเมือง ความเชื่อ และอุดมคติ ที่ฝังรากลึกของความกลัวบังคับให้รัฐบาลต้องทำตามเป้าของกลุ่มก่อการร้ายที่วางไว้ส่วนใหญ่จะเป็นเป้าหมายทางการเมือง (Gordon & Ford, 2002) FBI เห็นด้วยกับนิยามนี้แต่มีการปรับความหมายให้สอดคล้องกับบทบาทหน้าที่ขององค์กรมากขึ้น

คณะมนตรีความมั่นคงแห่งสหประชาชาติ (United Nations Security Council; UNSC) ได้ให้คำนิยามการก่อการร้ายว่าเป็นการก่ออาชญากรรมที่เป็นภัยต่อประชาชน มีการเตรียมการมาเป็นอย่างดีเพื่อก่อให้เกิดความสูญเสียด้วยวัตถุประสงค์ที่ต้องการยั่วยุให้เกิดความโกลาหลภายในรัฐด้วยการสร้างความกลัว จากคำนิยามนี้ไม่ได้อธิบายถึงความกดดันจากสถานการณ์ทางการเมือง ศาสนา เชื้อชาติ อุดมการณ์ หรือความเชื่อใด ๆ (Campbell, 2010)

สหราชอาณาจักรให้คำนิยามการก่อการร้ายเป็นไปตาม Section 1 ของ The Terrorism Act 2000 หมายถึง การกระทำที่อยู่ในขอบเขตเหล่านี้

1. การกระทำที่ถูกออกแบบเพื่อข่มขู่รัฐบาล หรือ สาธารณะ
2. การกระทำที่ทำเพื่อจุดประสงค์ทางการเมือง ศาสนา หรือ อุดมการณ์
3. เกี่ยวข้องกับความรุนแรงที่เป็นภัยต่อมนุษย์
4. เกี่ยวข้องกับความรุนแรงที่เป็นภัยต่อทรัพย์สิน
5. ทำให้ประชาชนถึงแก่ความตาย
6. ก่อให้เกิดความเสี่ยงต่อสุขภาพหรือความปลอดภัยต่อสาธารณะ
7. ก่อให้เกิดการขัดขวางการทำงานของระบบอิเล็กทรอนิกส์

เพื่อที่จะทำความเข้าใจการก่อการร้ายไซเบอร์แบบองค์รวม จำเป็นที่จะต้องทำความเข้าใจการก่อการร้ายแบบดั้งเดิมเพื่อเป็นพื้นฐานหลักในการนำไปวิเคราะห์ต่อไป จากการศึกษารวบรวมนิยามทั้งหมดของการก่อการร้ายพบว่า องค์ประกอบหลัก คือ การกระทำที่รุนแรง ส่งผลให้เกิดความเสียหายต่อชีวิตและทรัพย์สิน เป็นความตั้งใจที่จะข่มขู่รัฐ หรือ สังคม เพื่อให้ปฏิบัติตามวัตถุประสงค์ทางการเมือง ศาสนา และอุดมการณ์ของกลุ่มใดกลุ่มหนึ่ง (Matusitz, 2008)

การก่อการร้ายไซเบอร์เป็นวิวัฒนาการที่ต่อยอดจากการก่อการร้ายโดยใช้ระบบและเครือข่ายคอมพิวเตอร์อยู่ภายในพื้นที่ไซเบอร์ (Cyberspace) การก่อการร้ายแบบดั้งเดิมจะเกิดขึ้นในพื้นที่ทางกายภาพ (Physical Space) (Matusitz, 2008) ใช้อาวุธดั้งเดิมในการสร้างความกลัวให้กับเหยื่อ และเหมือนกับการก่อการร้ายทั่วไปการก่อการร้ายไซเบอร์ใช้วิธีแบบเดิมแต่เปลี่ยนแปลงในส่วนของพื้นที่การก่ออาชญากรรมเป็นพื้นที่ Digital และเปลี่ยนอาวุธธรรมดากลายเป็นไวรัสคอมพิวเตอร์ (Reyes, Brittson, O'Shea, & Steele, 2011)

การก่อการร้ายแบบดั้งเดิมมีกระบวนการคัดสรรค์ผู้ก่อการร้ายที่เป็นคนในพื้นที่เพื่อที่จะเข้าใจภูมิศาสตร์ของแต่ละพื้นที่ที่ต้องการจะโจมตี ซึ่งวิธีนี้จะแตกต่างกับการก่อการร้ายไซเบอร์ที่ไม่จำเป็นต้องใช้คนในพื้นที่เพราะเครือข่ายอินเทอร์เน็ตสามารถเข้าถึงได้ทุกที่และแม่นยำ โดยไม่จำเป็นต้องใช้สายลับในการเก็บข้อมูลเพราะไซเบอร์นั้นจะเข้าถึงแหล่งข้อมูลได้อย่างสะดวกและง่ายดาย

โดยสรุปแล้วเพื่อความชัดเจนในการนิยาม การก่อการร้าย หมายถึง การใช้ความรุนแรง หรือข่มขู่ว่าจะใช้ความรุนแรง ซึ่งมีการวางแผนไว้ล่วงหน้า เพื่อบรรลุ เป้าหมายทางการเมือง ศาสนา สังคม อุดมการณ์ โดยสร้างความหวาดกลัวให้กับประชาชนเพื่อให้ขาดความมั่นใจต่อรัฐบาล

2.2 นิยามการก่อการร้ายไซเบอร์ (Definition of Cyber Terrorism)

การก่อการร้ายทางไซเบอร์ส่วนใหญ่จะใช้ความกลัวผ่านช่องทางสื่อออนไลน์ (Online Media) เพื่อเป็นการกระตุ้นและแพร่กระจ่ายข่าวได้อย่างรวดเร็ว แต่รูปแบบของการก่อการร้ายนั้นยังคงเดิม เปรียบเสมือนเหล้าเก่าในขวดใหม่ (Green, 2020: pp. 11-18) ที่เปลี่ยนไปในลักษณะภายนอกเท่านั้น การก่อการร้ายไซเบอร์ในปัจจุบันอาจผสมผสานรูปแบบของเทคโนโลยีคอมพิวเตอร์เข้ามาใช้ในการก่อวินาศกรรม เช่น การจี้ปล้นเครื่องบินโดยการเจาะระบบคอมพิวเตอร์การบิน การโจมตีระบบควบคุมโรงงานอาวุธนิวเคลียร์ และควบคุมระบบทหารผ่านทางเครือข่ายคอมพิวเตอร์ทั่วโลก การก่อการร้ายไซเบอร์ถือเป็นภัยคุกคามรูปแบบใหม่ที่รัฐบาลในแต่ละประเทศจะต้องเตรียมตัว ซึ่งการก่อการร้ายแบบเก่านั้นอาจต่างกันในเรื่องของการขาดการเชื่อมโยงแบบโลกาภิวัฒน์

การให้นิยามการก่อการร้ายที่กล่าวมายังมีข้อถกเถียงทางด้านวิชาการที่ยังไม่สามารถสรุปได้ การก่อการร้ายไซเบอร์ที่มีส่วนผสมของเทคโนโลยีมาเกี่ยวข้อง ทำให้คำนิยามของการก่อการร้ายในรูปแบบของไซเบอร์นั้นมีความยากยิ่งขึ้น มีนักวิชาการหลายฝ่ายพยายามหาข้อตกลงร่วมกันในการให้นิยาม โดย Denning ให้ความหมายของการก่อการร้ายไซเบอร์ คือ การใช้คอมพิวเตอร์เป็นทั้งเครื่องมือและเป้าหมายในการก่อการร้าย (Denning, 2020) โดยมีการเตรียมตัวและมีผลประโยชน์ทางการเมืองเป็นแรงกระตุ้นในการจู่โจมระบบ ขโมย บิดเบือนข้อมูล หรือทำลาย ในระบบคอมพิวเตอร์ ที่ส่งผลให้เกิดความเสียหายต่อผู้บริสุทธิ์ แต่อย่างไรก็ตาม Dawn โต้แย้งว่าการก่อการร้ายไซเบอร์นั้นเป็นการทำลายระบบคอมพิวเตอร์อย่างรุนแรงประเภทหนึ่งที่ส่งผลต่อการขับเคลื่อนประเทศ ผู้ช่วยผู้อำนวยการฝ่าย Cyber-Division ของ FBI กล่าวเสริมว่า การก่อการร้ายเป็นการก่ออาชญากรรมประเภทหนึ่งที่ใช้คอมพิวเตอร์และความสามารถทางการสื่อสารเทคโนโลยีเป็นตัวบ่อนทำลายก่อให้เกิดความเสียหายอย่างรุนแรง เกิดความขัดข้องในการบริหารงานระดับประเทศ เพื่อจุดประสงค์ที่จะสร้างความกลัว ความรู้สึกสับสนและไม่ปลอดภัยกับประชาชน โดยการขู่บังคับนี้มีเป้าหมายให้รัฐบาลยอมกระทำตามข้อตกลงทางการเมืองที่กลุ่มตนยื่นเสนอให้ ทั้งนี้ อาจจะเป็นในเรื่องของการเมือง สังคม และอุดมการณ์ของแต่ละกลุ่มนั้น (Denning, 2020) Denning กล่าวเพิ่มเติมในคำนิยามของการก่อการร้ายว่าเป็นการผสมผสานระหว่างพื้นที่ไซเบอร์ (Cyberspace) กับการก่อการร้าย (Terrorism) โดยหากพิจารณาจากความหมายแรก พื้นที่ไซเบอร์ (Cyberspace) สามารถตีความได้ถึงการเปรียบเปรยจากนวนิยายแนววิทยาศาสตร์ที่พยายามอธิบายถึงพื้นที่ที่ไม่อยู่ในเชิงกายภาพถูกสร้างจากคอมพิวเตอร์ และจะเกิดขึ้นได้เฉพาะในสภาพแวดล้อม ที่เป็นโครงข่ายคอมพิวเตอร์เท่านั้น โดยที่ผู้ใช้จะต้องเป็นผู้ควบคุมทิศทางผ่านการใช้คีย์บอร์ด (Keyboard) และการเคลื่อนที่ของเม้าส์ (Mouse) พื้นที่ไซเบอร์ (Cyberspace) นั้นไม่มีอยู่ในความเป็นจริง Kenney เห็นด้วยว่า การก่อการร้ายไซเบอร์จะเกิดขึ้นได้เฉพาะในโลกของไซเบอร์ เหมือนกับ สงครามไซเบอร์ (Cyber War) การแฮกข้อมูล (Hacktivism) และการลักลอบเข้าสู่ข้อมูล (Unauthorized Assess) ทั่วไป (Kenney, 2015: pp. 111-128)

จากการศึกษานิยามทั้งหมด สามารถสรุปได้ว่า การก่อการร้ายไซเบอร์นั้นจะเกิดในพื้นที่ไซเบอร์(Cyberspace) และใช้ระบบคอมพิวเตอร์ (Computer System) ในการดำเนินการ การกระทำนี้จะทำให้เกิดความกลัวและความรุนแรงหรือเป็นอันตรายกับร่างกายหรือทรัพย์สินผู้อื่น และสุดท้ายจะต้องขับเคลื่อนโดยจุดประสงค์ของการเมือง ศาสนา และอุดมการณ์ ในกรณีนี้ผู้ก่อการร้ายจะถูกมองว่าใช้คอมพิวเตอร์เป็นอาวุธ

จากการศึกษา ค้นหาความหมาย มีการตีความการก่อการร้ายไซเบอร์มากมายที่แตกต่างกัน บางสำนักให้ความหมายการก่อการร้ายไซเบอร์ คือ การใช้คอมพิวเตอร์เป็นอาวุธของผู้ก่อการร้าย

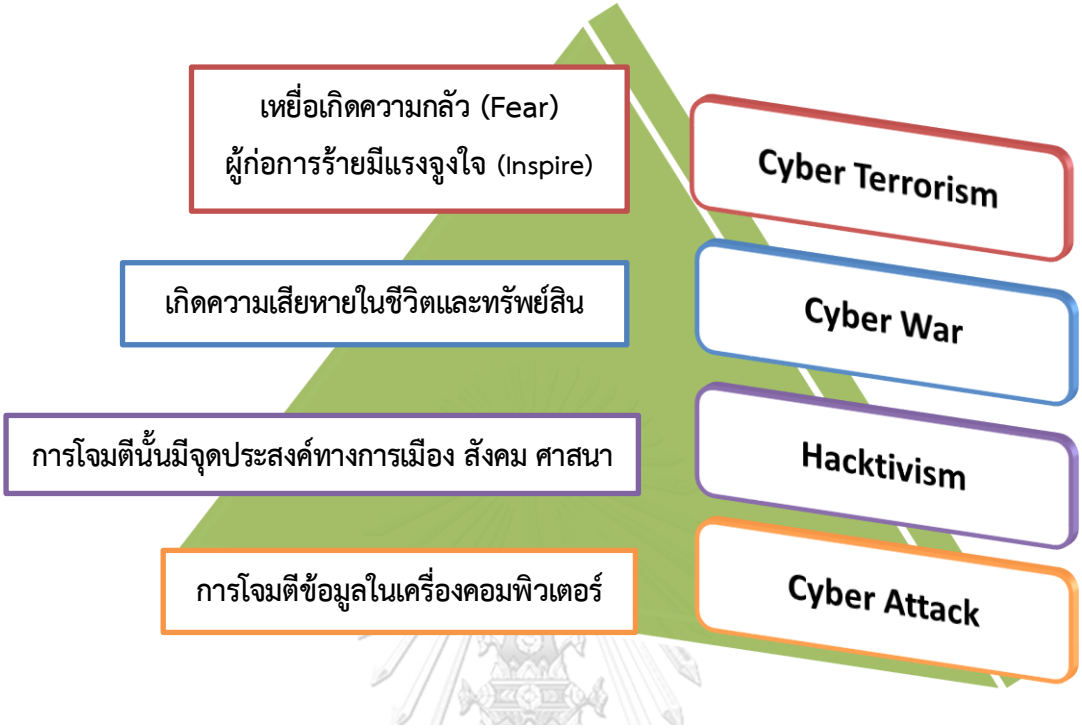
ก่อให้เกิดผลกระทบวงกว้าง เกิดความสูญเสีย ถึงแม้ว่าไวรัสจะไม่ได้อยู่ในโลกแห่งความจริง แต่ก็ถือเป็นความเสี่ยงและภัยคุกคามที่จะทำให้เกิดการโจมตีทางไซเบอร์ Kenney ได้ให้คำนิยามของการก่อการร้ายไซเบอร์ที่ครบสมบูรณ์แบบไว้ใน งานวิจัยของเขา เรื่อง Cyber Terrorism in Post- Stuxnet World ได้แบ่งระดับความหมายของของปรากฏการณ์ทางไซเบอร์ไว้เป็นประเภท คือ การจู่โจมทางไซเบอร์ (Cyber Attack) การแฮก (Hacktivism) สงครามไซเบอร์ (Cyber Warfare) และการก่อการร้ายไซเบอร์ (Cyber Terrorism) (Kenney, 2015) จากการเปรียบเทียบคำนิยามกับนักวิชาการสำนักอื่น ๆ ถือว่าคำนิยามของ Kenney มีความครอบคลุมและใกล้เคียงกับการโจมตีทางไซเบอร์มากที่สุด

คำนิยามแบ่งเป็น 4 องค์ประกอบ ดังนี้

1. การโจมตีข้อมูลในเครื่องคอมพิวเตอร์
2. การโจมตีนั้นมีจุดประสงค์ทางการเมือง สังคม ศาสนา และอุดมการณ์ ของกลุ่มใดกลุ่มหนึ่ง
3. เกิดความเสียหายในชีวิตและทรัพย์สินอย่างมหาศาล
4. เกิดความกลัวกับเหยื่อ ผลจากการข่มขู่ทำให้เหยื่อยอมปฏิบัติตาม

ปรากฏการณ์แต่ละประเภทที่ได้กล่าวล้วนมีจุดประสงค์ตรงกับองค์ประกอบหนึ่งในสี่ประการข้างต้น ยกตัวอย่างเช่น เป้าหมายของ การแฮก (Hacktivism) จะสอดคล้องกับอุดมการณ์ทางการเมือง ความต้องการที่จะควบคุมรัฐบาล ส่วนเป้าหมายของการก่อการร้ายไซเบอร์ (Cyber Terrorism) จะสอดคล้องกับการข่มขู่ ทำให้เกิดความกลัวต่อเหยื่อและเกิดแรงจูงใจให้กับผู้ก่อการร้ายให้มีความฮึกเหิมที่จะกระทำ

จากองค์ประกอบทั้ง 4 ประการรวมกันเป็นเป้าประสงค์หลักในการก่อการร้ายแบบดั้งเดิมและการก่อการร้ายไซเบอร์ โดยสรุปแล้ว การก่อการร้ายไซเบอร์จะต้องเป็นไปตามองค์ประกอบข้างต้นที่เกิดจากการโจมตีของคอมพิวเตอร์ เกิดความเสียหายทางกายภาพ ทำให้ประชาชนหวาดกลัวและยอมทำตามแนวทางของผู้ก่อการร้ายที่วางไว้ ส่วนใหญ่จะเป็นเรื่องของการเมือง สังคม ศาสนา และอุดมการณ์ของกลุ่ม



รูปที่ 2 องค์ประกอบของภัยคุกคามทางไซเบอร์

ถึงแม้อาชญากรรมไซเบอร์จะเป็นอาชญากรรมรูปแบบใหม่แต่ก็ยังมีรากฐานดั้งเดิมมาจากอาชญากรรมธรรมดาที่เกิดทั่วไป การวิเคราะห์อาชญากรรมไม่ว่าจะตั้งแต่ยุคคลาสสิก (Classical School) ที่มุ่งเน้นการกระทำของมนุษย์ที่อยู่ร่วมกันในสังคมว่ามนุษย์จะประกอบอาชญากรรมเพราะมนุษย์มีเจตจำนงอิสระ หรือ Free Will (Hollin, 2013) ผ่านการไตร่ตรองถึงผลดีและผลเสียที่จะเกิดขึ้นแล้วว่าสิ่งที่กำลังจะกระทำไปนั้นก่อให้เกิดประโยชน์มากกว่าโทษ สำนักคลาสสิกเห็นว่าการลงโทษผู้กระทำความผิดจะต้องเหมาะสมกับความผิดของอาชญากรและข้อจำกัดของมนุษย์ โดยการลงโทษจะต้องประกอบด้วย ความรวดเร็วในการรับโทษ (Swiftness) ความแน่นอนที่จะได้รับโทษ (Certainty) และการบังคับใช้บทลงโทษที่เคร่งครัด (Severity) เพื่อผู้กระทำความผิดจะได้สำนึกในสิ่งที่กระทำไป (Hollin, 2013) การลงโทษจะต้องไม่น้อยเกินไปหรือไม่มากเกินไป แนวคิดเจตจำนงอิสระจึงสามารถนำมาอธิบายอาชญากรรมทางไซเบอร์ได้ จากการวิเคราะห์การกระทำของบุคคลที่กระทำความผิดมีแนวโน้มมากขึ้นเพราะความสะดวกของการใช้โลกไซเบอร์เป็นเครื่องมือ และความสะดวกเหล่านี้อาจจะเป็นตัวขัดเกลาให้ผู้กระทำความผิดและบริบทของสังคมที่เปลี่ยนไปทำให้เกิดการชั่งน้ำหนักของประโยชน์และโทษในสิ่งที่กระทำใช้เวลาลดลงและไม่แม่นยำ จึงทำให้ผู้กระทำความผิด

ส่วนมากตัดสินใจกระทำอย่างง่ายดาย โดยปราศจากการคำนึงถึงโทษที่จะได้รับ นอกจากนี้การก่อการร้ายไซเบอร์ยังมีลักษณะพิเศษอยู่สองลักษณะ นั่นคือ

1. ช่องว่างของไซเบอร์ (Vulnerability) ช่องว่างของไซเบอร์ทำให้ผู้จู่โจมสามารถเข้ามาขโมย บิดเบือนเปลี่ยนแปลง และทำลายข้อมูลที่เก็บไว้ในพื้นที่ระหว่างคอมพิวเตอร์ ความรวดเร็วของไซเบอร์เป็นอุปสรรคในการป้องกันและรับมือกับภัยคุกคาม จึงต้องมีการพัฒนากลวิธีรับมือให้เท่าทันกับผู้โจมตีเพราะ Virus ในปัจจุบันส่วนมากมีการพัฒนาอยู่ตลอดเวลา ทำให้ผู้โจมตีมีหนทางในการเข้าถึงระบบได้ง่ายขึ้นและยากที่เจ้าของระบบจะป้องกัน (Eom, Kim, Kim, & Chung, 2012)

2. การเพิ่มขึ้นของตัวแสดงที่ไม่ใช่รัฐ (The Rise of Non-State Actors) พื้นที่ของไซเบอร์เปิดโอกาสการมีส่วนร่วมแก่ตัวแสดงที่ไม่ใช่รัฐ (Non-State Actors) มากขึ้น ในอดีตรัฐบาลมีอำนาจในการยับยั้งควบคุมไม่ให้ความขัดแย้งลุกลามกลายเป็นความขัดแย้งระหว่างประเทศ (International Conflict) แต่โลกาภิวัฒน์และอินเทอร์เน็ตได้เพิ่มช่องทางการเข้าถึงให้กับทุกระดับอย่างเท่าเทียม การเปลี่ยนผ่านของวัฒนธรรมย่อยออนไลน์ทำให้เกิดพื้นที่ที่ไร้ขอบเขตและเป็นผลให้การทูตระหว่างประเทศไม่สามารถควบคุมได้

โดยสรุปแล้วจากการพิจารณาองค์ประกอบความหมายของการก่อการร้ายไซเบอร์ คือ การใช้คอมพิวเตอร์เป็นเครื่องมือรวมทั้งเป็นเป้าหมายในการก่อการร้าย โดยมีการเตรียมตัวและมีผลประโยชน์ทางการเมืองเป็นแรงกระตุ้นในการจู่โจมระบบ ขโมย บิดเบือนข้อมูล หรือทำลาย ในระบบคอมพิวเตอร์ ที่ส่งผลให้เกิดความเสียหายต่อผู้บริสุทธิ์

2.3 องค์กรอาชญากรรมข้ามชาติและการก่อการร้ายทางไซเบอร์ (Organizational Cyber Terrorism)

องค์กรอาชญากรรมข้ามชาติและการก่อการร้ายไซเบอร์มีความเชื่อมโยงกันในชนิดที่ปฏิเสธไม่ได้ ลักษณะของการก่อการร้ายไซเบอร์ถึงแม้บางครั้งจะเป็นการกระทำของคนเพียงคนเดียวที่มีทักษะเชี่ยวชาญในระบบคอมพิวเตอร์เจาะทำลายระบบก่อให้เกิดความเสียหายมหาศาลตามที่เป็นข่าว แต่โดยส่วนมากผู้ก่อการร้ายเหล่านั้นจะได้รับการสนับสนุนจากองค์กรและเครือข่ายที่จะสามารถทำให้เกิดการแลกเปลี่ยนทางเทคโนโลยีที่มีความก้าวหน้ามากพอที่จะเจาะเข้าระบบสำคัญของภาครัฐได้

ตามอนุสัญญาสหประชาชาติว่าด้วยการต่อต้านองค์กรอาชญากรรมที่จัดตั้งในลักษณะองค์กร ค.ศ. 2000 องค์กรอาชญากรรมข้ามชาติ หมายความถึง กลุ่มของบุคคลตั้งแต่ 3 คนขึ้นไปที่ไม่ได้จัดตั้งขึ้นโดยความบังเอิญเพื่อกระทำความผิด และไม่จำเป็นต้องมีการกำหนดบทบาทของสมาชิกอย่างเป็น

ทางการ ไม่จำเป็นต้องมีความต่อเนื่องของการเป็นสมาชิกหรือมีโครงสร้างที่พัฒนาแล้ว แต่ต้องดำรงอยู่เป็นระยะเวลาหนึ่งและมีการประสานดำเนินงานระหว่างกันและมีเป้าหมายในการกระทำความผิดและการกระทำเช่นนี้จะได้รับโทษในการจำคุก อย่างน้อย 4 ปีหรือโทษที่รุนแรงกว่านั้นอย่างหนึ่งหรือมากกว่า การรวมกลุ่มเป็นอาชญากรรมสามารถกระทำในรัฐมากกว่าหนึ่งรัฐ หรือกระทำในรัฐหนึ่งแต่มีส่วนสำคัญของการเตรียมการ การวางแผน การสั่งการ หรือการควบคุมเกิดขึ้นในอีกรัฐหนึ่ง หรือมีผลกระทบอย่าง สำคัญในอีกรัฐหนึ่ง หรือกระทำในรัฐหนึ่งแต่เกี่ยวข้องกับองค์กรอาชญากรรมซึ่งเกี่ยวข้องกับกิจกรรมที่เป็นความผิดอาญาในรัฐมากกว่าหนึ่งรัฐ สำหรับในประเทศไทย องค์กรอาชญากรรมข้ามชาติถูกนิยามในมาตรา 3 แห่งพระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ.2556 ว่า “องค์กรอาชญากรรมข้ามชาติ หมายถึง คณะบุคคลตั้งแต่สามคนขึ้นไปที่รวมตัวกันช่วงระยะเวลาหนึ่งและ ร่วมกันกระทำการใด โดยมีวัตถุประสงค์เพื่อกระทำความผิดอาญาที่กฎหมายกำหนดโทษจำคุกขั้นสูงตั้งแต่ 4 ปี ขึ้นไปหรือโทษสถานที่หนักกว่านั้นเพื่อให้ได้มาซึ่งผลประโยชน์ทางการเงิน ทรัพย์สิน หรือผลประโยชน์ทางวัตถุ อย่างอื่นไม่ว่าโดยทางตรงหรือทางอ้อม ซึ่งการกระทำความผิดทางอาญาได้กระทำลงมากกว่าในหนึ่งรัฐ หรือมีส่วนใดส่วนหนึ่งของการกระทำผิดหรือผลกระทบเกี่ยวข้องตังแต่ 2 รัฐ ขึ้นไป” องค์กรอาชญากรรมข้ามชาติสามารถก่ออาชญากรรมได้หลายลักษณะ ไม่ว่าจะเป็นอาชญากรรมสิ่งแวดล้อม การลักลอบค้าไม้ผิดกฎหมาย การลักลอบค้าอาวุธเถื่อน การลักลอบค้างาช้าง เครือข่ายการค้ามนุษย์ การค้าสัตว์ป่าเป็นต้น โดยภาพรวมแล้วองค์กรอาชญากรรมข้ามชาติจะมีลักษณะพื้นที่ (วรรณวิภา เมืองถ้า, 2551) ดังต่อไปนี้

1. องค์กรอาชญากรรมข้ามชาติจะมีเงินและอำนาจเป็นแรงจูงใจในการผลักดันองค์กร ไม่ได้ดำเนินการองค์กรโดยอาศัยแรงผลักดันจากอุดมการณ์และไม่มีเป้าหมายทางการเมือง
2. มีการดำเนินงานอย่างต่อเนื่องตลอดการเป็นสมาชิกขององค์กรอาชญากรรม
3. มีสมาชิกจำกัดเฉพาะกลุ่มใดกลุ่มหนึ่ง
4. มีการจัดลำดับชั้นของสมาชิกภายในองค์กรอาชญากรรม
5. มีการกำหนดหน้าที่และการแบ่งงานกันทำอย่างชัดเจน
6. การดำเนินงานขององค์กรอาชญากรรมมักจะใช้ความรุนแรง และการติดสินบนเป็นวิธีการดำเนินการเพื่อให้บรรลุภารกิจขององค์กร
7. วัตถุประสงค์หนึ่งขององค์กรอาชญากรรมคือการสามารถผูกขาดธุรกิจใน

ตารางที่ 2 เปรียบเทียบลักษณะที่เชื่อมโยงและแตกต่างระหว่างองค์กรอาชญากรรมข้ามชาติและการก่อการร้ายไซเบอร์

องค์กรอาชญากรรมข้ามชาติ	การก่อการร้ายไซเบอร์
- มีเงินและอำนาจเป็นแรงจูงใจ	- ผลักดันจากอุดมการณ์และเป้าหมายทางการเมือง
- ดำเนินงานอย่างต่อเนื่องตลอดการเป็นสมาชิก	- รวมกลุ่มเป็นเครือข่ายตามภารกิจ
- มีสมาชิกจำกัดเฉพาะกลุ่มใดกลุ่มหนึ่ง	- ไม่มีการจำกัดเฉพาะสมาชิกเพราะการสื่อสารที่ไร้พรมแดน
- มีการจัดลำดับชั้นของสมาชิก	- มีการจัดลำดับชั้นของสมาชิก เป็นองค์กรแบบหลวม
- กำหนดหน้าที่และการแบ่งงานกันทำอย่างชัดเจน	- หนึ่งคนสามารถทำได้หลายหน้าที่
- ใช้ความรุนแรง และการติดสินบนเพื่อให้บรรลุภารกิจ	- ใช้ความรุนแรง และจู่โจมโดยไม่ต้องติดสินบน
- การสามารถผูกขาดธุรกิจในพื้นที่คือวัตถุประสงค์หนึ่ง	- มีแต่วัตถุประสงค์ทางการเมืองและอุดมการณ์เฉพาะกลุ่ม

จากตารางที่ 2 แสดงว่าอาชญากรรมทั้งสองประเภทมีความคล้ายคลึงและแตกต่างกัน โครงสร้างขององค์กรอาชญากรรมข้ามชาติจะเป็นส่วนหนึ่งของการก่อการร้ายไซเบอร์ที่แปรเปลี่ยนรูปแบบมา การรับมือกับการก่อการร้ายไซเบอร์อาจจะต้องศึกษาการรับมือกับ กลไกป้องกันและปราบปรามองค์กรอาชญากรรมข้ามชาติควบคู่กันไปด้วยจึงจะเป็นประโยชน์ เช่น การกำหนดความผิดอาญาและบทกำหนดโทษ การสืบสวนสอบสวนคดีความผิดฐานมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ และการสร้างความร่วมมือที่เป็นประโยชน์ต่อการดำเนินคดีระหว่างประเทศ

2.4 จิตวิทยากับการก่อการร้ายไซเบอร์ (The Psychology of Cyber-Terrorism)

ในปัจจุบันรูปแบบของอาชญากรรมเกือบทุกประเภทสามารถเกิดขึ้นได้บนโครงข่ายอินเทอร์เน็ต ทำให้ภัยคุกคามนั้นมีความหลากหลายและยากที่จะป้องกัน ภัยคุกคามที่เกิดขึ้นปัจจุบันจะใช้พื้นที่ทางไซเบอร์ (Cyber Space) เป็นเครื่องมือในการโจมตี ก่ออาชญากรรมหลายประเภท เช่น การปลอมแปลง บิดเบือนข้อมูล การฉ้อโกงเงิน ขโมยข้อมูลส่วนตัว มากไปกว่านั้นอินเทอร์เน็ตยังเปิดช่องว่างให้กับโจรผู้ร้ายที่ใช้เป็นเครื่องมือในการล่อลวงเด็กและเยาวชน ไม่ว่าจะเป็นการเผยแพร่คลิปอนาจารหรือการค้ามนุษย์

นอกจากนี้ภัยคุกคามทางอินเทอร์เน็ตยังรวมไปถึงการโจมตีในระดับประเทศ การโจมตีจากรัฐบาลประเทศอื่นผ่านการโจรกรรมข้อมูลเพื่อจุดประสงค์ของการสืบเสาะข้อมูลลับ หรือเพื่อเข้ามาต่อรอง ประนีประนอม และควบคุมฝ่ายตรงข้ามกับรัฐบาลของตน โดยสามารถใช้วิธีการแฮกข้อมูล (Hack) ทำให้การบริการต่าง ๆ ไม่สามารถใช้งานได้ โดยเฉพาะหน่วยงานเกี่ยวกับสาธารณูปโภคสำคัญ (Critical Infrastructure) ส่งผลให้ประชาชนในประเทศเดือดร้อน

นอกจากนี้พื้นที่ทางไซเบอร์ (Cyber Space) ยังถูกใช้ในการเผยแพร่ข่าวสารปลอม (Propaganda) ขัดเกลาให้คนมีแนวความคิดรุนแรง (Radicalize Potential Supporters) เป็นแหล่งรวบรวมเงินทุนสนับสนุน (Raise Fund) หรือใช้เป็นเครื่องมือในการติดต่อสื่อสารผู้ก่อการร้ายด้วยกันเอง (Communicate Plan) จุดประสงค์เพื่อสร้างความหวาดกลัว (Fear) ให้กับประชาชน

การก่อการร้ายไซเบอร์ในปัจจุบันมีแนวคิดแบบซับซ้อน เป็นการก่อการร้ายที่มุ่งเป้าทำให้ประชาชนบริสุทธิ์หวาดกลัว หากมีการพิจารณาจากองค์ประกอบโดยละเอียด ผู้ก่อการร้ายพยายามใช้ความกลัว (Fear) ของประชาชนเป็นเครื่องมือในการบรรลุความสำเร็จ แต่ความกลัวนั้นเป็นสิ่งนามธรรม (Abstract) ขึ้นอยู่กับตัวบุคคล มีลักษณะเป็นวัตถุวิสัย (Subjective) จึงยากที่จะหามาตรวัดในการวัดความกลัว เมื่อหลักการของการก่อการร้าย คือ ความกลัว การศึกษาความกลัวจึงเป็นสิ่งจำเป็นและเป็นพื้นฐานในการทำความเข้าใจการก่อการร้ายต่อไป

ความกลัวเป็นความรู้สึกไม่มั่นคงทางอารมณ์สิ่งที่เกิดขึ้นภายนอก ความกลัวเป็นธรรมชาติของมนุษย์ และเป็นความรู้สึกที่อยู่คู่กับการดำเนินชีวิตมนุษย์ ทุกคนล้วนมีความกลัวในบางสิ่งบางอย่าง ด้วยกันทั้งสิ้น เช่น กลัวสัตว์ที่ดุร้าย เพราะเกรงว่าจะถูกทำอันตราย กลัวภัยธรรมชาติเพราะเป็นสิ่งที่ เราควบคุมไม่ได้ กลัวการเปลี่ยนแปลง เพราะไม่รู้อนาคตจะเป็นเช่นไร กลัวการพลัดพรากจากคนรัก เพราะไม่ต้องการอยู่อย่างโดดเดี่ยวอ้างว้าง กลัวความเจ็บปวดจากอุบัติเหตุและโรคภัยไข้เจ็บ หรือ แม้กระทั่งกลัวความตาย เพราะไม่รู้ว่าตายแล้วจะไปที่ใด ความกลัวจะส่งผลดีกับเรา หาก

เรากลัวอย่างมีเหตุผล กลัวในสิ่งที่ควรกลัว เช่น หากเรากลัวอุบัติเหตุ เราจะทำสิ่งต่าง ๆ ด้วยความไม่ประมาท หากเรากลัวการถูกลงโทษ เราจะไม่ทำผิดกฎระเบียบ ไม่ทำความชั่วร้าย

ในทางตรงกันข้าม ความกลัวจะส่งผลร้ายกับเราหากเรากลัวอย่างไร้เหตุผล กลัวในสิ่งที่ไม่ควรกลัว เช่น กลัวความมืด กลัวผี (เกรียงศักดิ์ เจริญวงศ์ศักดิ์, 2539) อีกทั้งความกลัวเป็นปฏิกิริยาการตอบสนองตามธรรมชาติ ที่มีต่อภัยคุกคามทั้งที่เกิดขึ้นจริงหรือ เกิดจากจินตนาการ (Gullone, 2000) ในต่างประเทศนั้นมักทำการศึกษาวิจัยเกี่ยวกับความ กลัว โดยมุ่งเน้นไปที่ความกลัว 2 ประเภท คือ ความกลัวที่เป็นปกติ (Normal Fear) และความกลัวทาง คลินิก (Clinical Fear) หรือ โฟเบีย (Phobia) โดยความกลัวจะเป็นพื้นฐานของสิ่งมีชีวิต เป็นส่วนสำคัญ ที่ทำให้เกิดการปรับตัวของพัฒนาการมนุษย์ และเกี่ยวข้องกับการมีชีวิตอยู่รอด (Gullone & Moore, 2000: pp. 393-407)

ความหมายของความกลัวจากพจนานุกรมบัณฑิตยสถาน พ.ศ. 2542 ได้ให้ความหมายว่าเป็นความรู้สึกไม่อยากประสบสิ่งที่ไม่ดีแก่ตัวหรือความรู้สึกหวาดกลัวเพราะคาดว่าจะประสบภัย และบุคคลจะแสดงออกเมื่อตระหนักถึงอันตรายที่เกิดขึ้นกับตนเอง (ภัสยกร เลาสวัสดิกุล, 2557: น. 11)

โดยความกลัวที่กล่าวไว้นั้นสามารถนำเป็นเครื่องมือที่ใช้ในการก่อการร้าย (Terrorism) ตั้งแต่ในสมัยยุคแห่งความหวาดกลัวของฝรั่งเศส (The Reign of Terror) ระหว่างการปฏิวัติครั้งใหญ่ในปี ค.ศ. 1789-1794 โดยรัฐของฝรั่งเศสในนำวิธีอันป่าเถื่อนมาใช้ เพื่อให้ฝ่ายตรงข้ามหวาดกลัว ดังนั้นความหมายดั้งเดิมของการก่อการร้ายจึงหมายถึง ผู้ครองอำนาจรัฐหรือผู้ที่กำลังยึดอำนาจรัฐใช้กำลังก่อความหวาดกลัวเพื่อวัตถุประสงค์ทางการเมือง (Campbell, 2010) อย่างไรก็ตามแนวความคิดทางด้านก่อการร้ายได้วิวัฒนาการไปมากจนทำให้ความหมายของการก่อการร้ายเปลี่ยนไปจากเดิม นอกจากนี้ยังแพร่ระบาดก่อให้เกิดการเปลี่ยนแปลงในสังคมระหว่างประเทศโดยใช้รูปแบบในการต่อรองกับรัฐ หรือบีบบังคับให้รัฐทำตามเงื่อนไขความต้องการของกลุ่มซึ่งกลายมาเป็นลัทธิที่ปรากฏขึ้นในสังคมระหว่างประเทศ เรียกว่า ลัทธิการก่อการร้าย (Terrorism) การก่อการร้ายนั้นไม่ใช่สงครามที่จะเผชิญหน้ากันโดยตรง แต่เป็นกลยุทธ์ที่ถูกนำมาใช้เป็นเครื่องมือในการสร้างความกลัว

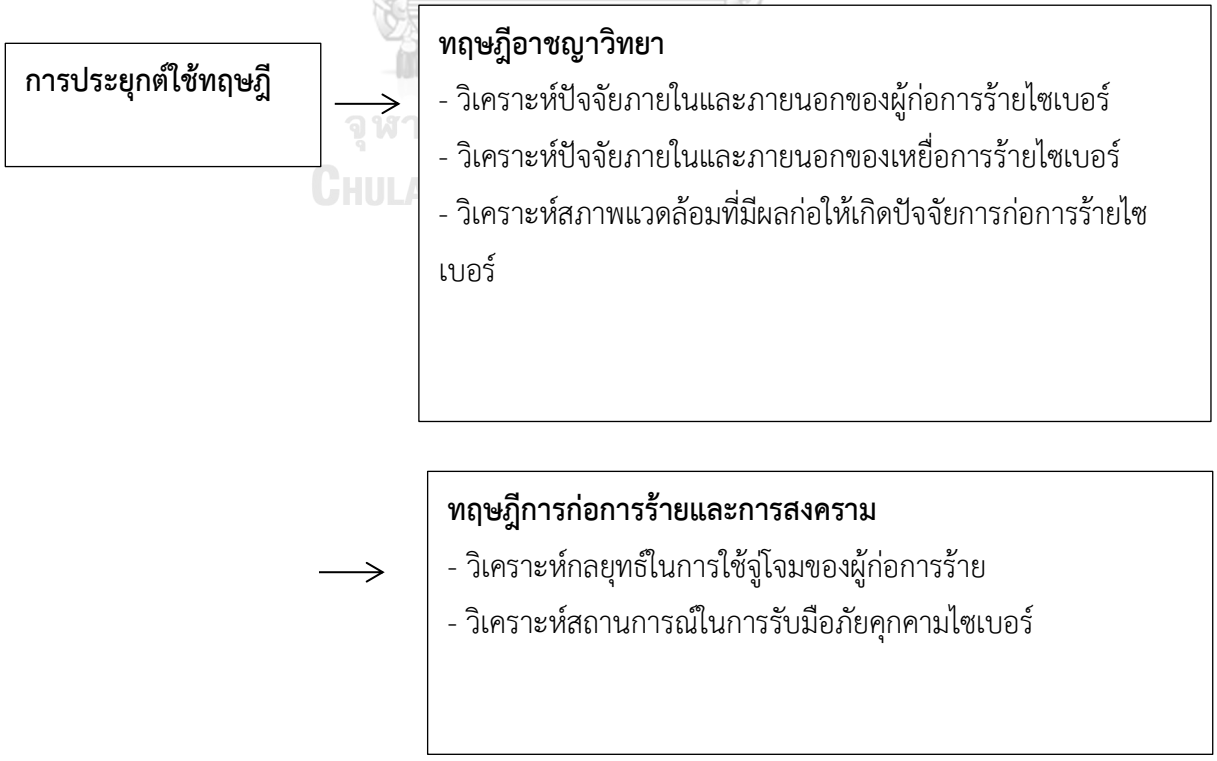
2.5 ทฤษฎีอาชญาวิทยาและทฤษฎีการก่อการร้ายกับไซเบอร์ (Criminology Theories and Terrorism Theories)

นับตั้งแต่ปี 2004 Facebook ถูกก่อตั้งขึ้นโดยกลุ่มนักศึกษามหาวิทยาลัยฮาร์วาร์ด Facebook เป็นเครือข่ายสังคมออนไลน์ที่ใหญ่และทรงอิทธิพลที่สุดเครือข่ายหนึ่งของโลกได้ถือกำเนิดขึ้น ในช่วงเริ่มต้น Facebook เป็นเพียงพื้นที่แลกเปลี่ยนข้อมูลข่าวสารกันระหว่างหมู่นักศึกษา

มหาวิทยาลัย (Croft, 2007) แต่ต่อมาเครือข่ายสังคมออนไลน์ดังกล่าวได้ปรับเปลี่ยนและพัฒนาจนมีบทบาทเชื่อมประสานให้ผู้คนทั้งที่ใกล้ชิดกันหรือห่างกันคนละมุมโลกสามารถติดต่อถึงกันได้อย่างง่ายขึ้น เครือข่ายสังคมออนไลน์กลายเป็นพื้นที่ใหม่ที่ได้รับความนิยมอย่างรวดเร็วสำหรับการพบปะ นัดหมาย ไต่ถามสารทุกข์สุขดิบ และแลกเปลี่ยนความคิดเห็น โดยไม่อยู่ภายใต้ข้อจำกัดทางด้านสถานที่หรือเวลา

นอกจากการพบปะแลกเปลี่ยนความคิดเห็น ปัจจุบัน Facebook ยังเป็นอีกสื่อหนึ่งที่มีอิทธิพลต่อการเปลี่ยนแปลงทางพฤติกรรมของผู้คนในสังคม ทั้งในเชิงจิตวิทยาและสังคมวิทยา (Madalena, 2011) ความเปลี่ยนแปลงทางพฤติกรรมประการหนึ่งที่ผู้เขียนสนใจคือ ผลกระทบจากความตึงเครียดของผู้คนในสังคมจากการใช้เครือข่ายสังคมออนไลน์

ผู้วิจัยได้ยกตัวอย่างเรื่องราวของ Facebook เพื่อแสดงให้เห็นว่าเทคโนโลยีกำลังเข้ามาเป็นส่วนหนึ่งของชีวิตมนุษย์ในการหล่อหลอมความคิด การตัดสินใจ มนุษย์มีความตระหนักรู้โดยมีเทคโนโลยีเป็นหนึ่งในการประกอบสร้าง ดังนั้นการจะศึกษาการกระทำความผิดโดยใช้เทคโนโลยีเป็นเครื่องมือสามารถนำทฤษฎีอาชญาวิทยาแบบดั้งเดิมมาประยุกต์ใช้ในการอธิบายเหตุผลหรือแรงจูงใจที่มนุษย์จะตัดสินใจกระทำความผิดได้ และเพื่อให้มีความลึกซึ้งในการวิเคราะห์ผู้วิจัยจะนำ ทฤษฎีอาชญาวิทยาและทฤษฎีการก่อการร้ายและสงครามมาอธิบายเพื่อให้กระบวนการที่เกิดขึ้นมีมิติมากขึ้นโดยจะแสดงให้เห็นดังนี้



รูปที่ 3 การประยุกต์ใช้ทฤษฎีอาชญาวิทยาและทฤษฎีการก่อการร้ายและสงคราม

2.5.1 ทฤษฎีอาชญาวิทยากับผู้ก่อการร้ายไซเบอร์

2.5.1.1 ทฤษฎีความตึงเครียดในสังคมกับไซเบอร์ (Strain Theory)

ไม่ว่าจะเป็นพื้นที่ไซเบอร์หรือพื้นที่กายภาพ ทั้งสองพื้นที่ถือว่าเป็นพื้นที่ทางสังคมเช่นเดียวกัน ดังนั้นแนวคิดทฤษฎีที่อธิบายสังคมบนพื้นที่กายภาพ ก็ย่อมนำมาศึกษาสังคมบนพื้นที่ไซเบอร์ได้เช่นกัน ทฤษฎีอาชญาวิทยาที่สามารถอธิบายพฤติกรรมในโลกไซเบอร์ได้ คือ ทฤษฎีความตึงเครียด (Strain Theory)

ทฤษฎีความตึงเครียด เป็นทฤษฎีที่คิดขึ้นโดย Robert K. Merton มีรากฐานแนวคิดมาจากทฤษฎีสภาวะไร้กฎเกณฑ์ (Anomie Theory) ของ Emile Durkheim นักสังคมวิทยาชาวฝรั่งเศสที่อธิบายว่า อาชญากรรมรวมถึงการกระทำอัตวินิบาตกรรมหรือฆ่าตัวตายนั้นเกิดจากการเปลี่ยนแปลงทางสังคมอย่างรวดเร็วในช่วงเวลาใดเวลาหนึ่ง เป็นเหตุให้สมาชิกในสังคมบางรายปรับตัวไม่ทันต่อการเปลี่ยนแปลงนั้น นำไปสู่ความหดหู่ กดดัน และการฆ่าตัวตายได้ในที่สุด (Tibbetts & Rivera, 2015: pp. 167-180) ตัวอย่างที่เห็นได้คือการที่บุคคลต้องอยู่ในสังคมที่ไม่มีความแน่นอน ไม่ว่าจะเป็นเรื่องของเศรษฐกิจการเมืองที่มีความแปรปรวน ทำให้สถานภาพของบุคคลนั้นมีความเปลี่ยนแปลงอยู่เสมอ บุคคลนั้นอาจมีความตึงเครียดเกิดขึ้นในสภาวการณ์ดังกล่าวและง่ายต่อการตัดสินใจก่ออาชญากรรม หรือการตัดสินใจฆ่าตัวตายเนื่องจากหาทางออกไม่ได้ ซึ่งถือเป็นอาชญากรรมประเภทหนึ่งเช่นกัน (อาชญากรรมที่ไม่มีเหยื่อ – Victimless Crime)

Merton ได้นำแนวคิดดังกล่าวมาพัฒนากลายเป็นทฤษฎีความตึงเครียด ซึ่งอธิบายว่าโดยทั่วไปแล้ว สมาชิกในทุกสังคมจะถูกกำหนดให้มีเป้าหมายในชีวิตซึ่งเป็นที่ยอมรับจากสังคม (Conventional Goals) โดยต้องมีวิธีการหรือแนวทางในการไปสู่เป้าหมายนั้นโดยวิธีการที่เป็นที่ยอมรับของสังคม (Conventional Means) ด้วยเช่นกัน จากลักษณะทางสังคมดังกล่าวจึงก่อให้เกิดความเครียดหรือความกดดันในการบรรลุถึงเป้าหมายที่สังคมได้วางไว้ อันนำไปสู่วิธีการในการปรับตัวของสมาชิกในสังคมที่มีต่อสภาพความกดดันเหล่านั้น ด้วยเหตุนี้ Merton จึงได้แบ่งพฤติกรรมของสมาชิกในสังคมออกเป็น 5 กลุ่มประเภท (Tibbetts & Rivera, 2015) กล่าวคือ

Conformity ซึ่งเป็นกลุ่มที่ยอมรับเป้าหมายที่สังคมวางไว้ และยอมรับในแนวทางที่เป็นบรรทัดฐานของสังคมในการไปสู่เป้าหมายนั้น เช่น หากอยากร่ำรวยก็เลือกที่จะทำงานหนัก หากมองในมุมมองของอาชญากรรมไซเบอร์ ผู้ที่ใช้เทคโนโลยีอย่างถูกต้องอยู่ในกรอบที่รัฐบาลกำหนดไว้

Innovation เป็นกลุ่มที่ยอมรับเป้าหมาย แต่ปฏิเสธแนวทางที่สังคมยอมรับ กลุ่มนี้จึงจัดว่าเป็นกลุ่มที่มีแนวโน้มในการก่อให้เกิดอาชญากรรม ยกตัวอย่างเช่น อยากร่ำรวย แต่ไม่อยากทำงานหนัก จึงเลือกที่จะประกอบอาชญากรรม เพื่อให้ตนเองประสบผลสำเร็จในเป้าหมาย

ที่ตนเองโดยที่ไม่คำนึงถึงผู้อื่น คนกลุ่มนี้เปรียบได้กับแฮกเกอร์ที่ปฏิบัติตัวนอกกรอบ โจมตีรัฐบาล ใช้เทคโนโลยีในทางที่ผิด

Ritualism เป็นกลุ่มที่เลือกที่จะปฏิเสธเป้าหมายของสังคม แต่ยอมรับหรือทำตัวให้สอดคล้องกับแนวทางที่เป็นบรรทัดฐานของสังคมได้ ยกตัวอย่างเช่น ผู้ที่อยู่ในกลุ่มนี้อาจจะอยากร่ำรวย หรืออยากมีชื่อเสียง ตามเป้าหมายทั่วไปที่สังคมได้วางไว้ แต่ก็เลือกที่จะปฏิบัติตามกฎเกณฑ์ของสังคมเพื่อไม่ให้เกิดปัญหาใด ๆ ทั้งต่อตนเองและต่อสังคม ในกรณีนี้อาจเป็นผู้ที่มีแนวคิดต่อต้านรัฐบาล แต่เลือกที่จะนิ่งเฉยและปฏิบัติตัวตามกรอบที่วางไว้

Retreatism เป็นกลุ่มที่ปฏิเสธทั้งเป้าหมายและแนวทางที่สังคมยอมรับ เช่น คนที่ไม่ต้องการประสบความสำเร็จตามเป้าหมายใด ๆ ของสังคม รวมถึงไม่ต้องการประกอบอาชีพการงาน เลือกที่จะแยกตัวโดดเดี่ยวไร้บ้าน (Homeless) หรือออกจากสังคมไปอยู่ในที่ที่ไม่ต้องมีการติดต่อปฏิสัมพันธ์กับมนุษย์ อาจนำมาเชื่อมโยงในแง่ของผู้ที่ปฏิเสธเทคโนโลยี ไม่ต้องการสิ่งใหม่ ๆ อาจถูกมองว่าเป็นพวกล้าหลัง

Rebellion เป็นกลุ่มที่เข้าใจทั้งเป้าหมายและแนวทางทั่วไปที่สังคมยอมรับ แต่เลือกที่จะไม่ดำเนินตามเป้าหมายและแนวทางนั้น โดยจะใช้แนวทางอื่นที่ตนเองเห็นสมควรแทน ซึ่งในกลุ่มนี้มักจะได้แก่พวกนักปฏิวัติ หรือพวกผู้ก่อการร้าย ในที่นี้อาจมองเป็นพวกแฮกเกอร์ที่มีอุดมการณ์

ทฤษฎีความตึงเครียดที่ได้กล่าวโดยสรุปนี้ เป็นทฤษฎีทางสังคมวิทยาที่อธิบายถึงสาเหตุของการกระทำความผิดหรือการเกิดอาชญากรรมบนพื้นที่ทางสังคมในโลกความเป็นจริงได้เป็นอย่างดี โดยเมื่อพิจารณาแล้วจะเห็นได้ว่า สมาชิกของสังคมที่ถูกจัดอยู่ในกลุ่ม Innovation นั้น เป็นกลุ่มที่มีแนวโน้มที่จะก่ออาชญากรรมมากกว่ากลุ่มอื่น ๆ ซึ่งหากนำทฤษฎีดังกล่าวมาอธิบายต่อลักษณะพฤติกรรมของมนุษย์บนสังคมไซเบอร์จะแตกต่างออกไปดังที่จะกล่าวในประเด็นถัดไป

สมาชิกในสังคมไซเบอร์ก็มีการกำหนดเป้าหมายหรือค่านิยมทางสังคมเช่นเดียวกันกับในสังคมบนพื้นที่จริง และต่างก็ต้องมีแนวทางในการปรับเปลี่ยนตนเอง เพื่อให้บรรลุถึงเป้าหมายหรือค่านิยมนั้น การที่ผู้ใช้แต่ละคนต่างมุ่งนำเสนอเฉพาะด้านดี ๆ ของตนผ่านทางพื้นที่เสมือนจริงดังกล่าว ในอีกด้านหนึ่งย่อมก่อให้เกิดเป้าหมายหรือค่านิยมบนพื้นที่ไซเบอร์เช่นกัน โดยเป้าหมายทางสังคมจะถูกกำหนดร่วมกันอย่างไม่เป็นทางการหรืออาจไม่ตั้งใจ แนวความคิดเช่นนี้อาจเกิดขึ้นได้ทั้งในบุคคลทั่วไปและอาจเปลี่ยนผันความคิดของบุคคลเหล่านั้นให้กลายเป็นอาชญากรไซเบอร์หากถูกกดดันจากสังคมมากไป

จากเป้าหมายหรือการสร้างค่านิยมทางสังคมดังกล่าว เมื่อนำมาพิจารณาโดยอาศัยทฤษฎีของ Merton จะเห็นได้ว่า สมาชิกที่อยู่ในสังคมไซเบอร์ก็ย่อมสามารถถูกแบ่งออกได้

เป็น 5 ลักษณะเช่นเดียวกัน โดยอาจมีบางกลุ่มที่ยอมรับในเป้าหมายหรือค่านิยมนั้นรวมทั้งยึดในวิธีการที่เป็นที่ยอมรับของสังคม เพื่อบรรลุสู่เป้าหมายหรือค่านิยมดังกล่าว แต่ขณะเดียวกันกับที่สมาชิกอีกหลายคนของสังคมไม่อาจที่จะไปสู่เป้าหมายนั้นได้ด้วยวิธีการเช่นเดียวกันนั้น ก็ต้องแสวงหาวิธีการต่าง ๆ ที่อาจไม่เป็นที่ยอมรับได้ของสังคม ประกอบกับลักษณะพิเศษของเครือข่ายสังคมไซเบอร์บางอย่างที่เอื้อต่อพฤติกรรมเบี่ยงเบน (Deviant Behavior) ได้ง่าย เช่น การไม่อาจระบุได้แน่ชัดว่าสิ่งที่แต่ละคนโพสต์ลงไปนั้นมีความจริงแท้มากน้อยแค่ไหนซึ่งบางครั้งอาจเป็นเพียงแค่การหลอกลวงเพื่อสร้างภาพให้ได้รับการยอมรับหรือมีตัวตนบนพื้นที่เสมือนจริงเท่านั้น หรืออาจจะนำไปสู่การก่ออาชญากรรมที่มีความร้ายแรงมากขึ้น โดยเฉพาะอย่างยิ่งสมาชิกของสังคมในกลุ่ม Innovation ซึ่งตามทฤษฎีของ Merton แล้วจัดว่าเป็นกลุ่มที่ยอมรับในเป้าหมายทางค่านิยมของสังคมไซเบอร์ โดยเชื่อว่าคนที่ได้ชื่อว่าประสบความสำเร็จในชีวิตนั้นจะต้องมีความร่ำรวย ได้รับความยอมรับจากสังคม มีรูปแบบการใช้ชีวิตที่หรูหรา แต่เนื่องจากในกลุ่มดังกล่าวเลือกที่จะปฏิเสธการปฏิบัติตามแนวทางที่สังคมยอมรับ ดังนั้นบุคคลในกลุ่มดังกล่าวจึงมีแนวโน้มที่จะใช้ช่องทางบนพื้นที่ไซเบอร์ในการกระทำความผิดลักษณะต่าง ๆ ซึ่งใช้เทคโนโลยีคอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด ได้แก่ การหลอกลวงบนพื้นที่ไซเบอร์ (Cyber Fraud) การคุกคามบนพื้นที่ไซเบอร์ (Cyber Harassment) การปลอมตัวเป็นคนอื่นบนพื้นที่ไซเบอร์ (Cyber Impersonating) หรือแม้แต่การลักลอบเจาะระบบคอมพิวเตอร์ (Hack) เพื่อเปลี่ยนแปลงแก้ไขข้อมูลทางคอมพิวเตอร์ เป็นต้น แต่ในบางครั้งการกระทำความผิดทางไซเบอร์ไม่ได้เกิดแค่เพียงในกลุ่ม Innovation เท่านั้น แต่ยังสามารถปรากฏให้เห็นในกลุ่มของ Rebellion โดยเฉพาะผู้ก่อการร้ายไซเบอร์ซึ่งอาจมีเป้าหมายและแนวทางแตกต่างจากที่สังคมยอมรับ แต่ไม่อาจตีความว่าเป้าหมายและแนวทางเหล่านั้นผิด เช่น ผู้ก่อการร้ายที่มีความเห็นต่างจากรัฐบาล รวมกลุ่มกันกด F5 เพื่อโจมตีเวปไซต์ของรัฐบาลไม่ให้สามารถใช้งานได้ เป็นการแสดงออกเชิงสัญลักษณ์

นอกจากนี้ ลักษณะของเป้าหมายหรือค่านิยมทางสังคมไซเบอร์ ยังมีข้อที่แตกต่างจากสังคมบนพื้นที่กายภาพที่สำคัญอีกประการหนึ่งคือ โดยลักษณะของเนื้อหาที่มีการเผยแพร่ผ่านทางสังคมไซเบอร์มีลักษณะพิเศษที่รวดเร็ว ดังนั้น เป้าหมายหรือค่านิยมทางสังคมไซเบอร์บางอย่างก็อาจจะอยู่ในลักษณะที่มาเร็วไปเร็วเช่นกัน โดยอาจเป็นเพียงเป้าหมายทางค่านิยมที่คงอยู่เฉพาะช่วงเวลาสั้น ๆ และเมื่อถึงช่วงระยะเวลาหนึ่งเป้าหมายทางสังคมนั้นก็อาจเกิดการเปลี่ยนแปลงหรือพ้นสมัย ดังนั้นด้วยลักษณะของความไม่นิ่งและเปลี่ยนแปลงอย่างรวดเร็วของค่านิยมบนสังคมไซเบอร์อาจก่อให้เกิดปัญหาการปรับตัวในทุกกลุ่มสมาชิก โดยเฉพาะอย่างยิ่งในกลุ่ม Conformity ซึ่งเชื่อว่าเป็นกลุ่มที่มีแนวโน้มในการก่ออาชญากรรมต่ำที่สุดหากว่าอยู่ในพื้นที่ทางสังคมจริง เนื่องจากเป็นกลุ่มที่มีลักษณะในการยอมรับค่านิยมของสังคมและยินยอมปฏิบัติตามวิถีทางของสังคมในการ

บรรลุต่อเป้าหมายนั้น แต่เมื่อเกิดความเปลี่ยนแปลงทางเป้าหมายอย่างรวดเร็วดังเช่นลักษณะของค่านิยมบนสังคมไซเบอร์ ก็อาจส่งผลให้บุคคลในกลุ่มดังกล่าวไม่สามารถปฏิบัติตามวิถีทางที่ควรจะเป็นได้เสมอไป และอาจเปลี่ยนตัวเองให้มาก่ออาชญากรรม เนื่องจากไม่สามารถไปสู่เป้าหมายของสังคมที่มีความหลากหลายและมีความเปลี่ยนแปลงอย่างรวดเร็วได้ทัน นอกจากนี้ในลักษณะการเปลี่ยนแปลงเป้าหมายดังกล่าว หากว่ารวดเร็วเกินไป จนทำให้สมาชิกบางคนในสังคมไซเบอร์อาจปรับตัวไม่ทัน ก็อาจเกิดปัญหาในเรื่องของความหดหู่ทางอารมณ์ อันนำไปสู่การฆ่าตัวตาย ซึ่งอาจเรียกได้ว่าเป็นลักษณะของ Cyber Anomie อีกด้วย

2.5.1.2 ทฤษฎีปฏิสัมพันธ์เชิงสัญลักษณ์กับไซเบอร์ (Symbolic Interaction Theory)

เหตุการณ์ที่เกิดจากการโทรแจ้งเหตุเท็จกับเจ้าหน้าที่กลายเป็นเหตุการณ์ที่ถูกลืมและไม่เกิดขึ้นบ่อยนัก หลังจากที่ยุคดิจิทัลเข้ามาแทนที่ เหตุการณ์นี้อาจเป็นเรื่องง่ายสำหรับเจ้าหน้าที่เพราะแค่เพียงวางสายโทรศัพท์ ผู้ก่อกวนก็ไม่สามารถดำเนินภารกิจต่อได้ แต่อย่างไรก็ตามการโทรแจ้งความเท็จได้พัฒนารูปแบบตามกระแสในยุคปัจจุบันโดยนำเอาเทคโนโลยีมาใช้เป็นเครื่องมือสร้างเหตุการณ์ขึ้นมาเพื่อหลอกลวงให้ผู้ที่เป็นเหยื่อตายใจ ส่วนใหญ่ผู้กระทำจะมีวัตถุประสงค์เพื่อแกล้งเหยื่อด้วยความสนุกสนานเท่านั้น คลิปวีดีโอส่วนใหญ่สามารถพบได้ตามช่อง YouTube Chanel เพจ Facebook ต่าง ๆ เพื่อให้นำมาซึ่งกระแสความนิยมผ่านยอด Like ยิ่งมีผู้คนสนใจมากเท่าไหร่ ก็จะยิ่งทำให้คลิป วิดีโอเหล่านี้มีเพิ่มขึ้นมากเท่านั้น

หากเหตุการณ์ข้างต้นนั้นไม่เพียงแต่เป็นการสร้างความสนุกสนาน แต่ยังสร้างความเดือดร้อนให้ผู้อื่นที่ถูกโยงเข้าสู่เหตุการณ์โดยไม่ตั้งใจ เช่น การโทรศัพท์แจ้งความเท็จกับหน่วย SWAT (Special Weapons and Tactics) ของสหรัฐอเมริกา เพื่อกล่าวหาว่ามีผู้กำลังคิดจะก่อการร้าย เหตุการณ์รูปแบบนี้เกิดขึ้นส่วนใหญ่กับผู้มีประวัติเล่นวีดีโอเกมส์ออนไลน์ โดยจะใช้ หน่วย SWAT เป็นส่วนหนึ่งในการเล่นเกมส์ นักอาชญาวิทยาให้ความสนใจน้อยมากกับการก่ออาชญากรรมในรูปแบบนี้ โดยเฉพาะอย่างยิ่งการนำเทคโนโลยีมาใช้เป็นเครื่องมือเพื่อเพิ่มเติมความซับซ้อนทำให้เกิดเป็นสภาวะฉุกเฉิน และส่งผลต่อการเกิดอาชญากรรมได้ง่ายขึ้น เงื่อนไขเหล่านี้สามารถใช้ทฤษฎีทางสังคมวิทยาและอาชญาวิทยาเข้ามาอธิบายได้ เช่น วิธีการทางปรากฏการณ์วิทยา ของ Jack Katz (Katz, 1988) ที่พยายามจะอธิบายอารมณ์ของผู้ก่ออาชญากรรม ณ ที่เกิดเหตุจะเป็นแรงจูงใจหลักที่จะทำให้อาชญากรรมเกิดขึ้น

ผู้ก่ออาชญากรรมจะพยายามเข้าถึงที่อยู่ของเหยื่อในทุกรูปแบบไม่ว่าจะเป็นการแกะรอยจาก Call ID เพื่อหาถึงสถานที่ที่สัญญาณโทรศัพท์ส่งมา เมื่อได้ที่อยู่ของเหยื่อแล้วจะพยายามสร้างเรื่องเพื่อเรียกร้องความสนใจกับ หน่วย SWAT เช่น เกิดเหตุการณ์โจมตีสาธารณชนโดย

อาวุธที่มีความร้ายแรงสูง ภายใต้สถานการณ์ที่กดดัน หน่วย SWAT จึงจำเป็นต้องเร่งการตัดสินใจ บุกเข้าไปช่วยเหลือตัวประกันที่ผู้ก่ออาชญากรรมได้สร้างเรื่องไว้ การทำงานของหน่วย SWAT นั้นไม่จำเป็นต้องมีใบอนุญาตก่อนที่จะเข้าไปยังสถานที่ส่วนบุคคลใด ๆ เพราะฉะนั้น ทุกครั้งก่อนที่หน่วย SWAT ตัดสินใจจะโจมตีจะมีสมมติฐานเสมอว่าผู้แจ้งเหตุต้องการความช่วยเหลือจริงไม่ใช่การสร้างสถานการณ์ (Technocrime and criminological theory, 2018)

ผู้ก่ออาชญากรรมต้องมีทักษะ Social Engineering หรือที่มีภาษาไทยเรียกว่า “วิศวกรรมสังคม” เป็นศิลปะการของแฮกเกอร์ใช้หลอกลวงผู้คนเพื่อผลประโยชน์ที่ต้องการผ่านการค้นไปถึงจุดอ่อน ความไม่รู้ ไม่เข้าใจ หรือความประมาท สิ่งเหล่านี้เป็นปัจจัยต่อการก่ออาชญากรรมที่สำเร็จ เมื่อเทียบกับการโจมตีรูปแบบอื่น ๆ ของไซเบอร์ โดยเฉพาะกับผู้ที่ไม่มีความรู้ทางด้านความมั่นคงปลอดภัย ถึงแม้พวกเขาเหล่านี้จะรู้ตัวผู้ก่ออาชญากรรมแต่อาชญากรก็ยังมีทักษะที่แนบเนียนในการหลอกล่อขอข้อมูลส่วนตัวโดยที่เหยื่อไม่รู้ตัว (Wall, 2007) เห็นได้ชัดว่าทักษะที่สำคัญที่สุดคือ ทักษะสื่อสารที่เป็นทักษะทางสังคม (Soft Skill) ผสมผสานกับทักษะทางคอมพิวเตอร์ที่สามารถควบคุมสถานการณ์ตรงหน้าให้เหยื่อคล้อยตามได้ ผู้ก่ออาชญากรรมจะเข้าถึงข้อมูลส่วนตัว เลขที่บ้าน เบอร์โทรศัพท์ ผ่านการใช้ ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider for Information) คือ บริษัทที่ให้ลูกค้าสามารถเข้าถึงอินเทอร์เน็ต เช่น TOT, True, หรือ CAT โดยผู้ให้บริการจะเชื่อมโยงลูกค้าเข้ากับเทคโนโลยีรับส่งข้อมูลที่เหมาะสมในการส่งผ่านอุปกรณ์อินเทอร์เน็ต เมื่อหน่วย SWAT ได้รับข้อมูลเหล่านั้นก็จะส่งกองกำลังมุ่งตรงไปยังผู้ต้องสงสัยทันที และหากเรื่องราวเกิดบานปลายหน่วย SWAT เองจะเป็นผู้ต้องรับผิดชอบกับการจู่โจมที่ผิดพลาดครั้งนี้

เหตุการณ์เช่นนี้ยังไม่เคยได้รับรายงานจากว่าเกิดขึ้นในประเทศไทย แต่ก็มีความเป็นไปได้ในอนาคตที่ผู้ก่อการร้ายซึ่งจะมาจากความตั้งใจหรือไม่ตั้งใจก็ดีจะตัดสินใจก่ออาชญากรรมแบบนี้ขึ้นเพราะพฤติกรรมการเลียนแบบ การใช้การกระทำเชิงสัญลักษณ์สร้างตัวตนให้กับตนเองและเพื่อมุ่งร้ายกับคนอื่นจะเป็นวิธีที่ง่ายขึ้นเมื่ออยู่ในโลกดิจิทัล โดยสามารถประยุกต์ใช้หลักทางทฤษฎีปฏิสัมพันธ์เชิงสัญลักษณ์ของ George Herbert Mead (Cronk, 2006b) ที่ได้ให้ความสนใจพฤติกรรมและตัวตนเชิงสังคมของมนุษย์โดยตัวตนของมนุษย์นั้นมีทั้งแบบเป็นผู้กระทำสามารถควบคุมตัวเองได้ ผู้ถูกกระทำ และในแบบของตัวตนที่เกิดจากการปฏิสัมพันธ์ระหว่างตัวเองกับคนอื่นในสังคม การสร้างเหตุการณ์ขึ้นมาเพื่อทำร้ายผู้อื่นนั้นจึงเป็นการจำลองเชิงสัญลักษณ์ที่เล่นกับตัวตนและความรู้สึกของผู้ที่ถูกกระทำ การที่หน่วย SWAT ตัดสินใจที่จะจู่โจมผู้ที่ถูกกล่าวหาเป็นเพียงเพราะว่าพวกเขาถูกฝึกให้มีความคุ้นชินกับการตอบโต้เชิงสัญญะที่ได้เรียนรู้จากสังคม การกระทำเช่นนี้สามารถตอบได้ในแนวคิดของ Charles Cooley ที่ได้กล่าวว่ามนุษย์มักจะมองเห็นตัวตนที่สะท้อนผ่านกระจกเงา (Looking-Glass Self) (Cooley, 1894) ที่เป็นวิถีทางที่จะดำรงตัวตนผ่าน

ภาพสะท้อนที่คนอื่นตั้งความหวังไว้ นั่นแสดงให้เห็นถึงอิทธิพลของสังคมที่กำหนดตัวตนของบุคคล การที่ภาพจะสะท้อนจากสิ่งที่ผู้อื่นเห็นตัวตนของเราจะเป็นผลมาจากการที่ตัวเราให้คุณค่ากับสิ่งนั้น ดังนั้นมนุษย์จึงโน้มเอียงเข้าสู่ความหมายของสังคมที่เกิดขึ้นในบริบทของการมีปฏิสัมพันธ์ทางสังคม ระหว่างตัวตนกับสังคมจนเป็นเหตุให้การตัดสินใจนั้นเกิดขึ้นจากความคุ้นชินและด้วยสาเหตุอิทธิพล ของโลกดิจิทัลจะทำให้ปฏิสัมพันธ์เชิงสัญลักษณ์มีความคลุมเครือจนทำให้เกิดเหตุการณ์ที่ผิดพลาด เหล่านั้น

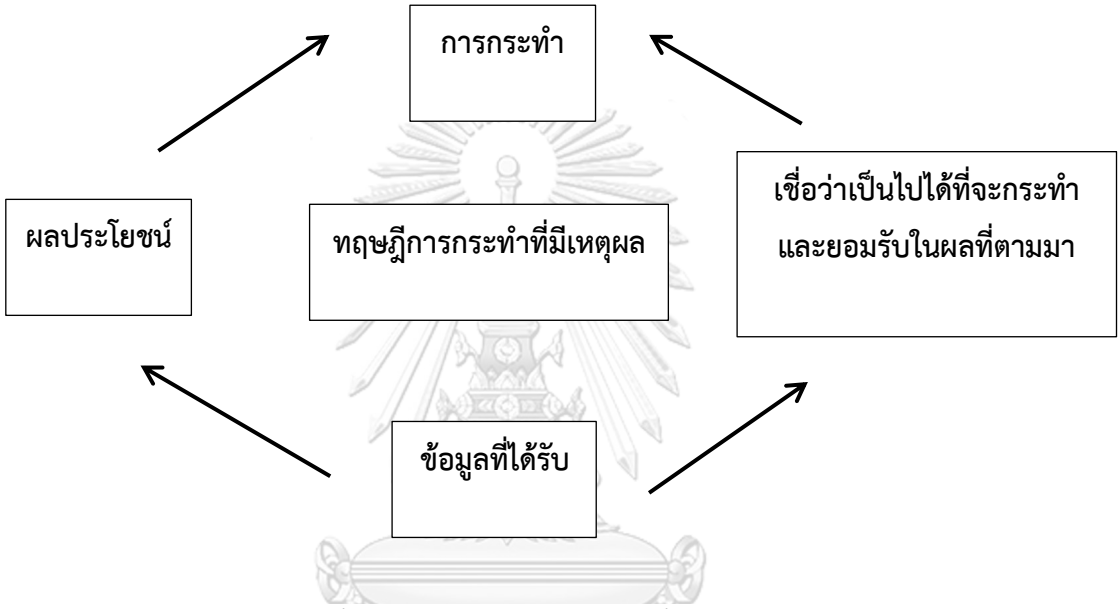
2.5.1.3 กลุ่มทฤษฎีพฤติกรรมผู้ก่อการร้ายไซเบอร์

ในการก่อการร้ายหรือการกระทำความผิด ผู้กระทำสามารถเป็นได้ในรูปแบบของบุคคลและรูปแบบขององค์กร โดยทั้ง 2 รูปแบบนั้นจะมีพฤติกรรมในการจูงใจที่ต่างกัน ในรูปแบบของบุคคลนักวิชาการเชื่อว่ามีสาเหตุมาจากปัจจัยหลายประการ โดยทฤษฎีที่มีความสัมพันธ์อย่างใกล้ชิดกับพฤติกรรมของผู้ก่อการร้ายหรือผู้กระทำความผิด อาจแบ่งได้เป็น 3 ทฤษฎี ดังต่อไปนี้

1) ทฤษฎีที่เกี่ยวกับเจตจำนงในการเลือก (Choice Theory) ซึ่งประกอบด้วยทฤษฎีเจตจำนงอิสระ (Free Will Theory) โดยทฤษฎีนี้มีแนวคิดว่ามนุษย์โดยธรรมชาติเป็นผู้ที่มีเหตุผล (Rational) แต่ในขณะเดียวกันก็ยึดถือประโยชน์ส่วนตัวเป็นที่ตั้ง (Utilitarian) นอกจากนี้ ยังมีความยึดมั่นในเรื่องสุขนิยม (Hedonistic) ดังนั้น เมื่อมนุษย์มีเหตุผล มนุษย์จึงมีเจตจำนงอิสระในการตัดสินใจเลือกที่จะทำหรือไม่ทำสิ่งใดสิ่งใดสิ่งหนึ่ง ดังนั้นการแสดงออกของพฤติกรรมใดพฤติกรรมหนึ่งของมนุษย์จึงขึ้นอยู่กับการชั่งน้ำหนักระหว่างความสุขหรือประโยชน์ที่จะได้รับกับความทุกข์หรือผลร้ายที่จะตามมา ซึ่งตามหลักแล้วนั้นมนุษย์ทุกคนย่อมมองหาและเลือกที่จะมีความสุข โดยพยายามหลีกเลี่ยงในสิ่งที่จะก่อให้เกิดความทุกข์ ดังนั้น ทฤษฎีนี้สามารถใช้ได้กับอาชญากรทั่วไปและผู้ก่อการร้ายไซเบอร์เพราะในเบื้องลึกแล้วจิตใจมนุษย์ จะสามารถตัดสินใจได้ง่ายขึ้นเมื่อสถานการณ์บีบบังคับให้ตัดสินใจ ยิ่งในโลกยุคดิจิทัลกระแสความเร็วที่เกิดขึ้นจะยิ่งทำให้มนุษย์เลือกในสิ่งที่เป็นประโยชน์กับตนเองง่ายขึ้น เพราะฉะนั้น Free Will ของมนุษย์จึงได้รับการกระตุ้นจากเทคโนโลยีให้ขาดการยับยั้งชั่งใจ การจะกำหนดบทลงโทษกับผู้ที่มีความคิดเช่นนี้อาจจะต้องใช้วิธีเด็ดขาดและใช้ได้อย่างทั่วถึงกับทุกฐานความผิดที่เกิดขึ้นจากเทคโนโลยี (Let the Punishment Fit the Crime) (Cronk, 2006a)

2) ทฤษฎีทางเลือกหรือทฤษฎีการกระทำที่มีเหตุผล (Rational Choice Theory) หากพิจารณาแล้วทฤษฎีนี้มีความคล้ายคลึงกับทฤษฎีเจตจำนงอิสระ เป็นทฤษฎีสำนักอาชญาวิทยายุค Classic โดยทฤษฎีทางเลือกหรือทฤษฎีการกระทำที่มีเหตุผลจะมีความเชื่อที่ว่าอาชญากรหรือผู้ก่อการร้ายมีเหตุผลและสามารถเลือกที่จะใช้มัน โดยอาชญากรหรือผู้ก่อการร้ายจะสามารถประเมินความเสี่ยงที่จะเกิดขึ้นด้วยการไตร่ตรอง พิจารณา และชั่งน้ำหนักสิ่งที่จะกระทำ โดย

จะพิจารณาระหว่างเหตุผลส่วนตัว อารมณ์ กิเลส ความอยากได้อยากมี ความแค้น ความโกรธกับการได้มาซึ่งผลประโยชน์เหล่านั้น เพราะฉะนั้นอาชญากรหรือผู้ก่อการร้ายในสำนักคิดนี้จึงเป็นผู้ที่มีเหตุผลสามารถประเมินประโยชน์ที่ได้รับและผลที่ตามมาจากการประกอบอาชญากรรมได้ ดังนั้นเหตุผลจึงทำให้มนุษย์เลือกที่จะกระทำอย่างมีเหตุผลและหลีกเลี่ยงความเสี่ยงหรือหายนะที่จะเกิดกับตนเองหรือการใช้ตนเองเป็นศูนย์กลาง (Cronk, 2006c)



รูปที่ 4 อธิบายทฤษฎีการกระทำที่มีเหตุผล

ที่มา: Cronk (2006c)

3) ทฤษฎีกิจวัตรประจำวัน (Routine Activities Theory) ทฤษฎีนี้เป็นทฤษฎีหนึ่งที่มีความคล้ายคลึงกับทฤษฎีข้างต้นที่ได้กล่าวมา แต่จะแตกต่างกันในเรื่องของการเพิ่มปัจจัยในการก่ออาชญากรรมหรือการก่อการร้าย โดยผู้ที่ต้องการจะก่ออาชญากรรมจะเลือกเหยื่อที่มีความเหมาะสม มีพฤติกรรมทำอะไรซ้ำ ๆ กันทุกวันจนเป็นกิจวัตร หากมีโอกาสหรือเหยื่อนั้นขาดผู้ปกป้อง เป็นเหยื่อที่อ่อนแอก็จะโจมตีได้ง่าย หลักคิดของทฤษฎีนี้สามารถใช้ได้กับการก่อการร้ายทางไซเบอร์เพราะหากประกอบไปด้วยผู้กระทำที่มีความตั้งใจ เหยื่อที่มีความอ่อนแอ มีช่องว่างในการโจมตี ผู้ก่อการร้ายจะหาช่องทางในการโจมตีได้ไม่ยาก ตัวอย่างเช่น การละเลยในเรื่องของการรักษาความปลอดภัยของระบบไซเบอร์ของหน่วยงานรัฐ อาจจะจะเปิดโอกาสให้ผู้ก่อการร้ายเข้ามาควบคุมระบบเหล่านั้นได้โดยไม่ทันได้ตั้งตัว จากการวิเคราะห์ตามทฤษฎีนี้แล้วเชื่อว่าหากมีการเพิ่มคนดูแล (Guardian) จะลดเป้าประสงค์หรือเป้าหมายในการโจมตีได้มากขึ้น (วรรณฉัตรตร พวยพุ้ง, 2555)

4) ทฤษฎีการข่มขู่ยับยั้ง (Deterrence Theory) ทฤษฎีนี้สามารถประยุกต์ใช้กับการก่อการร้ายไซเบอร์ได้เป็นอย่างดี โดยทฤษฎีนี้มองว่าการจะป้องกันไม่ให้เกิดการกระทำความผิดหรือการก่อการร้ายไซเบอร์ได้นั้นจะต้องใช้หลักการข่มขู่ยับยั้งทั่วไป (General Deterrence) และการข่มขู่ยับยั้งเฉพาะราย (Specific Deterrence) (Kabanda, 2018)

รูปที่ 5 อธิบายการประยุกต์ใช้ทฤษฎีการข่มขู่ยับยั้งกับการรับมือก่อการร้ายไซเบอร์
ที่มา: Kabanda (2018)

จากรูปที่ 5 สามารถแบ่งวิธีการป้องกันออกเป็น 4 ประเภท (Kabanda, 2018) นั่นคือ การข่มขู่ยับยั้งจะต้องอาศัยความตระหนักรู้ การอบรม นโยบายจากผู้บริหารที่จะนำไปบังคับใช้ ในเรื่องการป้องกันจะต้องพึ่งพาการป้องกันเชิงกายภาพที่เป็นรูปธรรมจับต้องได้ เครื่องมือที่ทันสมัย และ Firewalls ที่ช่วยในการป้องกันไวรัส สำหรับการตรวจจับ จะมาในรูปแบบของระบบควบคุมที่จะต้องมีการสอดส่องสอดแนมอยู่ตลอดเวลา ส่วนสุดท้าย คือ การรักษาเยียวยาหมายถึงการใช้ระบบกฎหมายการลงโทษภายในและภายนอก

สำหรับผู้กระทำผิดในรูปแบบขององค์กรนั้นสามารถวิเคราะห์ได้ตั้งแต่รูปแบบของการจัดตั้งองค์กร เช่น การรวมตัวกันเป็นองค์กรแบบอุปถัมภ์เป็นการรวมกลุ่มบุคคลที่มีโครงสร้างความสัมพันธ์อย่างหลวม ๆ เพื่อประโยชน์ของกลุ่ม ผู้อุปถัมภ์อาจมีความสัมพันธ์กับเจ้าหน้าที่ภาครัฐจึงสามารถลักลอบเข้าระบบโครงสร้างอินเทอร์เน็ตโดยปราศจากอำนาจได้ รูปแบบองค์กรนี้บางครั้งได้การสนับสนุนทางด้านเศรษฐกิจและการเมือง รูปแบบความสัมพันธ์ของเครือญาติ

มีลักษณะคล้ายระบบสังคม มีโครงสร้างที่เป็นอิสระจากตัวบุคคล กลุ่มโครงสร้างนี้มีความสัมพันธ์และมีผลประโยชน์ร่วมกันทำให้มีเป้าหมายในการโจมตีระบบทางไซเบอร์เดียวกัน พฤติกรรมขององค์กรอาชญากรรมไม่ว่าจะเป็นดั้งเดิมหรือในโลกไซเบอร์ สมาชิกขององค์กรจะมีเลียนแบบพฤติกรรมซึ่งกันและกัน ตามทฤษฎีการเรียนรู้ทางสังคม (Social Learning Theory) Tarde ให้ข้อสังเกตว่า บุคคลจะเลียนแบบประเพณีของบุคคลอื่นตามกลุ่มคนที่ใกล้ชิด ผู้ที่มีฐานะต่ำกว่าจะเลียนแบบผ็ที่มีฐานะสูงกว่า และเรียนรู้พฤติกรรมใหม่ ๆ ถ้าพฤติกรรมแบบเก่า ๆ ขัดแย้งกัน (อัณณพ ชูบำรุง, 2532)

ผู้กระทำในรูปแบบขององค์กรจะมีพฤติกรรมซับซ้อนมากกว่าผู้กระทำแบบบุคคล พฤติกรรมในการตัดสินใจกระทำความผิดจะต้องได้รับความเห็นจากสายบังคับบัญชาหรือสมาชิกในกลุ่ม ความอิสระในการเลือกกระทำจะมีน้อยกว่า ความเด็ดขาดในการเลือกกระทำก็เช่นกัน ดังนั้นในการโจมตีแต่ละครั้งจะต้องใช้เวลานานในการเตรียมการ ต้องมีความรอบคอบมากว่าผู้กระทำแบบบุคคล และเป้าหมายที่ผู้กระทำแบบองค์กรอาชญกรรามจะเลือกนั้นจะต้องใช้ทักษะทางคอมพิวเตอร์สูงกว่าผู้กระทำแบบบุคคล

2.5.1.4 ทฤษฎีที่เกี่ยวกับอุปนิสัยของผู้ก่อการร้าย (Trait Theories)

Sigmund Freud บิดาแห่งนักคิดเกี่ยวกับอุปนิสัยได้นำการศึกษาด้านจิตวิทยามาวิเคราะห์มาอธิบายถึงสาเหตุของอาชญากรรมและการกระทำผิด การวิเคราะห์นี้อาศัยหลักจิตวิทยา (Psychology) และจิตเวชศาสตร์ (Psychiatry) ใช้หลักปรัชญาในการรักษา (Treatment) Freud เชื่อว่าความก้าวร้าวกับความรุนแรงเป็นสัญชาตญาณดิบของมนุษย์ แนวคิดเรื่องโครงสร้างของบุคลิกภาพของ Freud ประกอบไปด้วย 3 ส่วน คือ

รูปที่ 6 อธิบายแนวคิดโครงสร้างของบุคลิกภาพของ Freud

ที่มา: วรรณฉัตรตร พวยพุ้ง (2555)

ตามแนวคิด ของ Freud นั้น Ego จะอยู่กลางระหว่างความขัดแย้งของสัญชาตญาณดิบ (Id) และการควบคุมของ Superego มนุษย์สามารถกลั่นกรองการกระทำโดยการประสานระหว่าง Ego และ Id โดยมี Superego เข้ามาเป็นส่วนหนึ่ง และเมื่อใดที่ Ego ไม่สามารถประนีประนอมระหว่าง Id และอยู่เหนือการควบคุมของ Superego ก็จะเกิดความขัดแย้งขึ้น ถ้า Id มีความหนักแน่นมากกว่าจะทำให้มนุษย์เลือกที่ใช้สัญชาตญาณดิบตามใจตนก่อให้เกิดการกระทำที่ไม่ถูกต้อง แต่อย่างไรก็ตามถ้า Superego มีพลังเหนือ Id การกระทำเหล่านั้นก็จะไม่เกิดขึ้น ดังนั้นจึงมีข้อสันนิษฐานว่าการกระทำความผิด จะมาจากปัญหาทางอารมณ์ (Emotional Problem Theories) หรือเหตุการณ์ซึ่งสามารถกระตุ้นให้มนุษย์ไม่สามารถควบคุมได้และตัดสินใจกระทำไปเพราะใช้อารมณ์ (วรรณฉัตรตร พวยพุ้ง, 2555)

บางครั้งกลุ่มทฤษฎีนี้เชื่อว่าการกระทำความผิดของคนเกิดจากปัญหาทางชีวภาพร่างกายที่ผิดปกติจนไม่สามารถที่จะยับยั้งได้ เช่น การที่จิตผิดปกติ (Mental Disorder Theories) ในแบบที่จิตผิดปกติจากสมองที่ผิดปกติ (Organic Disorder) ซึ่งจะเกี่ยวกับสมองโดยตรง และในแบบจิตผิดปกติจากระบบการทำงานของสมองผิดปกติ (Functional Disorder) คือเกิดจากระบบการทำงานของ ประสาทการรับรู้ (Cognitive) การเข้าใจ (Perceptual) ไม่สามารถทำหน้าที่ได้ทำให้เกิดอาการประสาทหลอน (Psychosis) วิตกกังวล (Neurosis) และในแบบสุดท้ายคือการเป็นปรปักษ์ต่อสังคม (Sociopathy Theory) ซึ่งเป็นอาการของความเจ็บป่วยและสามารถก่อให้เกิดการกระทำความผิดได้ ถือว่าอาการเป็นปรปักษ์กับสังคมนั้นจะเกิดขึ้นได้กับทุกคน แต่อาการที่เกิดขึ้นอย่างรุนแรงนั้นจะเกิดขึ้นกับคนที่ป่วยเท่านั้น

นอกจากที่ได้กล่าวถึงอาการความผิดปกติข้างต้นแล้ว ผู้ก่อการร้ายไซเบอร์สามารถมีพฤติกรรม การโยนความผิดอย่างที่ David Matza และ Gresham Sykes (กฤษมันต์ วัฒนาณรงค์, 2553) ได้กล่าวถึง แนวคิดที่เชื่อว่าผู้กระทำความผิดจะมองตัวเองเป็นศูนย์กลางและพยายามจะโยนการรับผิดชอบไปยังผู้อื่น โดยพยายามทำให้เขาดูถูกต้อง ตัวอย่างเช่น การพยายามผลักความผิดที่เกิดขึ้นไปยังรัฐ โดยกล่าวหาว่ารัฐเป็นผู้ที่จะต้องรับผิดชอบกับเรื่องที่ตนคิดว่าเป็นเรื่องที่ไม่ยุติธรรมสำหรับตน มีผู้ก่อการร้ายหลายกลุ่มที่พยายามใช้ข้อนี้ในการปรักปรำและเป็นเหตุให้ทำร้ายคนผู้บริสุทธิ์เพื่อข่มขู่รัฐให้กระทำตามสิ่งที่ตนคิดว่าถูกต้อง

กลุ่มทฤษฎีเกี่ยวกับอุปนิสัยยังกล่าวถึงทฤษฎีการเลียนแบบ (Theory of imitation) Jean Gabriel Tarde นักอาชญาวิทยา ได้อธิบายการเลียนแบบว่าเป็นสาเหตุหนึ่งในการกระทำความผิด โดยมีกฎอยู่ 3 ประการด้วยกัน นั่นคือ 1) การเลียนแบบพฤติกรรมระหว่างผู้ที่มีความสัมพันธ์ใกล้ชิดกัน เช่น กลุ่มเพื่อนแฮกเกอร์ 2) การเลียนแบบจากผู้ที่มีสถานะเหนือกว่าตน เช่น

การเลียนแบบผู้ที่อยู่ในองค์กรและมีลำดับบังคับบัญชาที่เหนือกว่าตน หากผู้นั้นปฏิบัติตัวไม่ดีแต่ยังได้รับการเคารพ นับหน้าถือตา จะยิ่งเป็นตัวกระตุ้นให้ผู้น้อยปฏิบัติตาม ในที่นี้หากผู้นั้นมีพฤติกรรมในการฉ้อฉลองค์กรโดยใช้เทคโนโลยีเป็นเครื่องมือจะยิ่งทำให้ผู้น้อยที่คอยสังเกตสามารถเลียนแบบพฤติกรรมได้ง่าย 3) การเลียนแบบพฤติกรรมใหม่ตาม “กฎของการแทรกแทน” (Law of Insertion) ของ Tarde (Williams, 2007) เช่น การเลียนแบบพฤติกรรมที่เหนือไปกว่าพฤติกรรมที่ตนได้ทำผิดในตอนแรก เมื่อมีครั้งแรกย่อมมีครั้งที่สอง เช่น จากการขโมยข้อมูลธรรมดากลายเป็นพัฒนาทักษะเพื่อลักลอบเข้าระบบ ทักษะแบบนี้สามารถเกิดขึ้นได้จากการเลียนแบบสื่อประเภทต่าง ๆ เช่น ภาพยนตร์ YouTube หรือคลิปวีดิโอต่าง ๆ ที่มีในอินเทอร์เน็ต (Williams, 2007)

2.5.1.5 ทฤษฎีการแก้ตัว (Techniques of Neutralization)

นักอาชญาวิทยา Gresham Sykes และ David Matza เสนอทฤษฎีนี้ขึ้นมาเพื่อแสดงให้เห็นว่า แรงจูงใจ แรงผลักดัน การหาเหตุผลเข้าข้างตนเอง มีเทคนิคการวางตัวเป็นกลางถือเป็นการองค์ประกอบสำคัญที่เป็นประโยชน์ในต่อการละเมิดกฎหมาย มนุษย์จะใช้เหตุผลเพื่อให้ได้สิ่งที่ดีที่สุดและให้เสียน้อยที่สุด (กฤษมันต์ วัฒนาณรงค์, 2553) โดยเทคนิคที่ใช้แก้ตัว ได้แก่

1) อ้างว่าตกอยู่ในภาวะจำต้องทำ (Denial of responsibility) เช่น การลอกข้อสอบเพื่อนและอ้างว่าต้องทำเพื่อให้ตนเองจบ

2) อ้างว่าไม่ได้ทำให้ใครเดือดร้อน (Denial of injury) เช่น การลอกข้อสอบเป็นสิ่งที่เพื่อนเต็มใจและไม่ได้ทำให้เพื่อนเดือนร้อน

3) อ้างว่าเหยื่อสมควรที่จะเป็นเช่นนั้น (Denial of the victim) เช่น เมื่อมีเหตุผลที่เข้าข้างตนเอง การขัดขืนของเหยื่อจึงเป็นสิ่งที่ไม่ถูกต้อง และการกระทำที่ตนลงมือทำกับเหยื่อจึงไม่ใช่สิ่งที่ผิดอะไร

4) อ้างกล่าวโทษว่ามีผู้อื่นเลวร้ายกว่า (Condemnation of the condemners) เช่น การทำร้ายเหยื่อของตนอาจเทียบไม่ได้กับการตีรันฟันแทงของเด็กอื่นๆ มักจะหาข้ออ้างในเหตุการณ์ที่ไม่เกี่ยวข้องมาเปรียบเทียบ

5) อ้างเหตุผลดีกว่ามาหักล้าง (Appeal to higher loyalties) เช่น การลอกสอบของตนทำให้ตนจบ มีงานมีการทำ ไม่ต้องเติบโตไปเป็นอาญชรในอนาคต

ทฤษฎีนี้จัดอยู่ในกลุ่มทฤษฎีกระบวนการทางสังคม (Social Process) หรือทฤษฎีการเรียนรู้ (Learning Theory) มีการเรียนรู้เรื่องแรงจูงใจ เหตุผลของการกระทำผิด ค่านิยมที่ชื่นชอบการกระทำผิด โดยสรุปแล้วทฤษฎีแสดงให้เห็นว่าอาชญากรมักจะไม่เห็นว่าสิ่งที่ตนทำลงไปเป็นสิ่งผิดแต่กลับเป็นสิ่งที่ตนเองจะต้องกระทำเพื่อความอยู่รอดของตน ในโลกของไซเบอร์ก็เช่นกัน (กฤษมันต์ วัฒนาณรงค์, 2553) ผู้กระทำจะเปรียบเสมือนใส่หน้ากากไว้ตลอดเวลาเพราะฉะนั้นเวลากระทำ

ความผิดจะง่ายกว่าโลกในความจริง เมื่อตนถูกโลกแห่งความจริงบีบคั้น เช่น ยากจน ไม่มีเงินทอง การโตรกรรมในโลกของไซเบอร์คือทางออก การใช้ไซเบอร์เปรียบเสมือนหน้ากากที่ปิดบังตนเอาไว้จนทำให้ตนไม่รู้สึกว่าที่กระทำไปนั่นไม่ใช่ความผิดโดยมีเหตุผลความจำเป็นมาสนับสนุน ยิ่งเป็นกรณีที่เหยื่อสมยอมด้วยแล้วก็มักจะโทษว่าเหยื่อสมควรที่จะเป็นเช่นนั้น (Denial of the victim)

2.5.2 ทฤษฎีอาชญาวิทยากับเหยื่อการร้ายไซเบอร์

หากใช้กลุ่มทฤษฎียุคปฏิฐานนิยม (Positivist School in Criminology) มาวิเคราะห์พฤติกรรมของเหยื่ออาชญากรรม Lombroso ได้ให้ความเห็นว่า “การกระทำความผิดของอาชญากรแสดงออกมาเพราะตกอยู่ภายใต้การกดดันของเหยื่อ ที่มีการยั่วยุอารมณ์” Garofaro ให้ข้อสังเกตเป็นในทางเดียวกันกับ Lombroso ว่า “การกระทำของเหยื่อในบางกรณีเป็นต้นเหตุยั่วยุให้มีการประกอบ อาชญากรรมขึ้น”เนื่องจากเป็นการศึกษาเพียงด้านเดียวของผู้กระทำความผิด จึงไม่อาจสรุปได้ว่าเหยื่อมีบทบาทสำคัญในการก่ออาชญากรรม Wolfgang นักอาชญาวิทยาในยุคต่อมาได้ศึกษาผู้เสียหายเพื่อหาสาเหตุของอาชญากรรม จึงทำให้เป็นจุดเริ่มต้นในการศึกษาเหยื่ออย่างจริงจังในยุคต่อ ๆ มา (สถาบันวิจัยรพีพัฒนศักดิ์, 2553)

การให้คำนิยาม “เหยื่อ” “ผู้เสียหาย” “เหยื่ออาชญากรรม” มีความหมายกว้างโดยหมายถึงเหยื่อทุกประเภท จนกระทั่งในปี 1948 Hana Von Hentig บิดาของแห่งเหยื่อวิทยาได้ให้คำจำกัดความที่ชัดเจนของคำว่าเหยื่อในมุมมองอาชญาวิทยา Hana Von Hentig มองว่าเหยื่อที่ถูกทำร้ายมีส่วนที่ยั่วยุให้อาชญากรมีความโมโหและกระทำในสิ่งที่ไม่สามารถควบคุมได้ เหยื่อส่วนใหญ่มักจะเป็นเพศหญิง คนแก่และเด็กที่มีความอ่อนแอ คนกลุ่มน้อย เหยื่อส่วนใหญ่มีจะมีลักษณะซึมเศร้าหดหู่ จากโดยกระทำ ในช่วงกลางทศวรรษ 1940 Benjamin Mendelsohn นักเหยื่อวิทยาและอดีตทนายความ เขาสนใจในประเด็นเรื่องความสัมพันธ์ระหว่างเหยื่อและอาชญากรโดยการสัมภาษณ์ และได้ข้อสรุปว่า (สถาบันวิจัยรพีพัฒนศักดิ์, 2553)

1. เหยื่อที่บริสุทธิ์โดยแท้จริง (Completely Innocent Victim) เป็นเหยื่อที่ไม่มีส่วนเกี่ยวข้องใด ๆ ต่อการถูกเป็นเหยื่อ ส่วนใหญ่ที่มักจะเกิดกับธรรมชาติของเหยื่อที่มีลักษณะอ่อนแอ เช่น เด็ก คนชรา

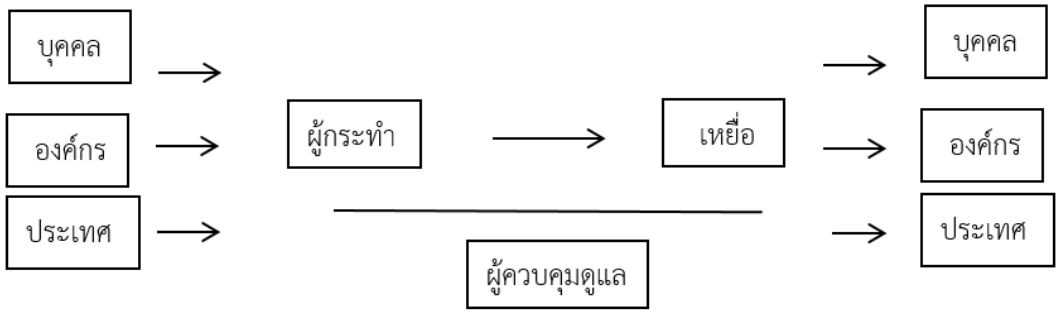
2. เหยื่อที่มีความผิดเล็กน้อย (Victim with Minor Guilt) เหยื่อที่มีความเขลาและถูกกระตุ้นให้ทำในสิ่งที่ผิดและต้องรับกรรมจากการกระทำนั้น

3. เหยื่อที่มีความผิดเท่ากับอาชญากร (The Vitcimas Guiltyasthe Offender) ส่วนใหญ่เหยื่อประเภทนี้จะเป็นเหยื่อที่มีความสมัครใจที่จะกระทำความผิดที่เกิดกับร่างกายของตน เช่น การฆ่าตัวตาย

4. เหยื่อที่มีความผิดมากที่สุด (The Most Guilty Victim) เหยื่อที่ก้าวร้าว รุนแรง จึงเป็นเหตุทำให้ถูกทำร้ายหรือโดนฆ่า

5. เหยื่อปลอม (The Simulating Victim) คือ เหยื่อที่ไม่ได้ถูกทำร้ายจริง แต่สร้างภาพว่าตนเองถูกทำร้าย หรือมาจากคนที่มีจิตผิดปกติ

โดยสรุปแล้ว “เหยื่อหรือผู้เสียหายจากอาชญากรรม” หมายถึง บุคคล กลุ่มบุคคล หรือองค์กรที่ได้รับความเสียหายไม่ว่า จะเป็นการบาดเจ็บทางร่างกายหรือสภาพจิตใจ ความเจ็บปวดทางอารมณ์ ความรู้สึกนึกคิด ความสูญเสียทาง เศรษฐกิจหรือสิทธิขั้นพื้นฐานโดยเป็นผลจากการกระทำหรือละเว้น การกระทำซึ่งเป็นการละเมิด ต่อกฎหมายอาญาหรือกฎหมายที่บัญญัติให้การใช้อำนาจหน้าที่โดยมิชอบเป็นความผิดทางอาญา อันเป็นกฎหมายของประเทศสมาชิกนั้น ๆ และยังหมายถึงครอบครัวหรือทายาทของผู้เสียหาย ตลอดจนบุคคลที่ได้รับความเสียหายจากการเข้าไปช่วยเหลือผู้เสียหายให้พ้นจากภัยอันตรายหรือป้องกันการกระทำร้ายนั้น (สถาบันวิจัยรพีพัฒนศักดิ์, 2553)



รูปที่ 7 กระบวนวิธีการวิจัยของการศึกษาการรับมือการก่อการร้ายไซเบอร์ในประเทศไทย

ในการวิเคราะห์เหยื่อจากการก่อการร้ายไซเบอร์หรือเหยื่อจากภัยคุกคามไซเบอร์ สามารถวิเคราะห์ผ่านทฤษฎีอาชญาวิทยา สามารถแยกประเภทของเหยื่อที่เป็นในรูปแบบบุคคล องค์กร และเหยื่อในระดับประเทศ โดยจะใช้ทฤษฎีกิจวัตรประจำวัน และ ทฤษฎีการมีส่วนร่วมของเหยื่อ วิเคราะห์ ดังนี้

1. ทฤษฎีกิจวัตรประจำวัน (Routine Activities Theory)

ทฤษฎีที่พัฒนาขึ้นเมื่อนักอาชญาวิทยาสนใจเหยื่อและสนใจที่จะอธิบายสาเหตุของอาชญากรรมโดยศึกษาเหยื่อมากขึ้น ทฤษฎีนี้พัฒนามาจาก Cohen และ Felson ทฤษฎีนี้สามารถนำมาประยุกต์ใช้กับการก่อการร้ายไซเบอร์และภัยคุกคามไซเบอร์ได้ โดยมองว่าเหยื่อที่มีความอ่อนแอจะมีแนวโน้มที่จะเป็นเหยื่อของการก่อการร้ายไซเบอร์ได้ จากองค์ประกอบสามประการในการเกิดอาชญากรรม คือ ผู้กระทำที่มีแรงจูงแจง เหยื่อที่มีความเหมาะสม และขาดผู้ดูแลที่มีประสิทธิภาพ หากมุ่งเน้นไปยังประเด็นเรื่องเหยื่อที่มีความเหมาะสม อาจจำแนกได้ 3 ประเภท คือ คน สิ่งของ และสถานที่ โดยสิ่งที่เคยตกเป็นเหยื่อมาแล้วจะสามารถตกเป็นเหยื่อได้อีกครั้ง ผู้ใช้งานคอมพิวเตอร์มีโอกาสตกเป็นเหยื่อของภัยคุกคามประเภทนี้ได้มากที่สุด เพราะคนที่ใช้คอมพิวเตอร์ส่วนใหญ่จะขาดความตระหนักรู้ในเรื่องความปลอดภัยของระบบคอมพิวเตอร์ หรือระบบรักษาความปลอดภัยเองก็มีข้อเสียข้อบกพร่องเป็นเป้าหมายของการโจมตี การป้องกันไม่ให้เกิดภัยคุกคามไซเบอร์หรือการปิดโอกาสของการตกเป็นเหยื่อเป็นวิธีที่มีประสิทธิภาพสูงสุด มากกว่าที่จะให้เหยื่องดทำกิจวัตรประจำวันแบบเดิม แต่จะต้องทำโดยการลดช่องว่างโดยการใช้ระบบรักษาความปลอดภัยดิจิทัล (Digital Guardian) ที่เพียงพอ เหยื่อเองจะต้องมีความตระหนักรู้ในตนเอง เช่น การระวังในการเข้าเวปไซต์ผิดปกติเพราะเสี่ยงต่อการได้รับไวรัส ความมั่นคงปลอดภัยของการตั้งรหัสผ่านที่ไม่ควรใช้รหัสเดียวกันทั้งหมด

1.1 คนร้าย/แฮกเกอร์

คนร้ายในบริบทของแฮกเกอร์มีความต้องการที่แตกต่างจากคนร้ายแบบดั้งเดิม มีลักษณะที่เปลี่ยนไปจากเดิมคือปัจจัยทางเทคโนโลยีที่ไร้พรหมแดน การเข้าถึงได้ง่ายไม่จำเป็นต้องมีต้นทุนมากมาย ดังนั้นทำให้คนร้ายส่วนมากเป็นมือสมัครเล่น สามารถเข้าถึงได้และมีจำนวนเพิ่มมากขึ้น การกระทำส่วนใหญ่จึงส่งผลเสียในลักษณะที่ค่อนข้างน้อง มีแนวโน้มเป็นรายบุคคลมากกว่าที่จะเป็นในรูปแบบองค์กรขนาดใหญ่เพราะองค์กรลักษณะแบบนั้นจะมีระบบการป้องกันที่ดียากต่อการที่คนร้ายมือใหม่จะเข้าถึงได้

1.2 เหยื่อ/เป้าหมาย

เหยื่อหรือเป้าหมายจะมีความแตกต่างไปจากอาชญากรรมธรรมดา เนื่องจากผู้ที่จะโดนแฮกได้นั้นต้องมีการเข้าถึงเทคโนโลยีได้ มีความรู้ในเทคโนโลยีในระดับหนึ่งแต่ยังไม่เพียงพอจ่อการที่จะป้องป้องตนเองขากผู้ร้าย และยังขาดซึ่งความตระหนักรู้ถึงภัยคุมคามทางเทคโนโลยีที่สามารถเกิดขึ้นได้ในทุกที่ทุกเวลา เหยื่อในปัจจุบันมีมากขึ้นเนื่องจากการเข้าถึงเทคโนโลยีทำได้ง่าย เช่นการเข้าเวปไซต์ต่างๆและกรอกข้อมูลส่วนตัวโดยไม่ได้ทันระวัง หรือการเลือกเชื่อในข้อมูลที่ไม่เป็นความจริง และตกเป็นเหยื่อยของผู้ร้ายได้ง่าย

1.3 โอกาสหรือเวลาและสถานที่

เมื่อกล่าวถึงโอกาสเป็นสิ่งที่สำคัญในโลกของไซเบอร์เพราะในทุกช่วงเวลาคือโอกาสที่ผู้ร้ายจะกระทำได้ทุกเมื่อ โดยเฉพาะในเวลาที่เหยื่อทีเวลาส่วนตัวในโลกของไซเบอร์มากเท่าไหร่จะยิ่งเป็นเป้าหมายและเพิ่มโอกาสให้กับผู้ร้ายมากเท่านั้น เวลาที่เหยื่อมักถูกเป็นเป้าคือช่วงเวลาที่เหยื่อมีความเหนื่อยหน่ายกับเทคโนโลยีหรือเวลาที่จำกัดในการตัดสินใจทำธุรกรรมทางเทคโนโลยี เวลาเหล่านี้จะเป็นช่องว่างให้กับผู้ร้ายในการขโมยข้อสำคัญหรือหลอกลวงเหยื่อได้ในระยะเวลาอันสั้น

วิธีการรับมือตามทฤษฎีกิจวัตรประจำวันสามารถช่วยเหลือเหยื่อผ่านการสร้างระบบป้องกันที่แข็งแรง เพิ่มสายด่วนทางเทคโนโลยีในการช่วยเหลือเพื่อที่จะแนะนำวิธีการในการรับมือของเหยื่อต่อผู้ร้ายได้ทันท่วงที นอกจากนี้เหยื่อส่วนมากมักจะเป็นผู้ที่ขาดความรู้ทางเทคโนโลยีเพราะฉะนั้นการมีผู้รู้เป็นที่ปรึกษาในการทำธุรกรรมต่างๆ จึงเป็นสิ่งจำเป็นเช่นการที่ลูกหลานจะต้องคอยเป็นหูเป็นตาให้กับผู้ใหญ่ ผู้ปกครองให้ใช้เทคโนโลยีอย่างถูกต้อง การดูแลเรื่องพาสเวิร์ดต่างๆควรมีการเปลี่ยนพาสเวิร์ดในทุกๆ 3 เดือน เพื่อป้องกันการเข้าถึงของผู้ร้ายการตัดโอกาสของผู้ร้ายไม่ให้เข้าถึงเป็นวิธีที่สำคัญที่สุด ต่อมาคือการลดความอ่อนแอของเหยื่อและตัดแรงกระตุ้นในการกระทำของผู้ร้ายหรือแฮกเกอร์โดยบังคับใช้กฎหมายที่มีประสิทธิภาพ

2. ทฤษฎีการมีส่วนร่วมของเหยื่อ (Victim Precipitation)

ทฤษฎีนี้เชื่อว่าเหยื่อมีส่วนเกี่ยวข้องที่ทำให้เกิดเหตุอาชญากรรม อาจจะไม่ใช่การยั่วยุโดยตรง แต่เป็นทางอ้อม เช่น ความอิจฉา ริษยา ที่ผู้กระทำมีต่อเหยื่อ ไม่ว่าจะเป็นทางธุรกิจผลประโยชน์ทางการเมืองหรือความเกลียดชัง มีทั้งในระดับปัจเจก ระดับองค์กร และระดับประเทศ ลักษณะการกระทำเช่นนี้มีความใกล้เคียงกับการก่อการร้ายไซเบอร์ ที่ผู้กระทำจะต้องมีการวางแผนไตร่ตรอง อย่างดีก่อนที่จะตัดสินใจกระทำ บางครั้งอาจเกิดขึ้นโดยที่เหยื่อไม่จำเป็นต้องยั่วยุต่อหน้าหรือยั่วยุทางตรง แต่การกระทำมาจากความอิจฉาของฝ่ายตรงข้ามหรือการกลัวว่าอีกฝ่ายจะได้เปรียบในเรื่องผลประโยชน์ โดยเหยื่อมีพฤติกรรมที่แสดงออก 2 ประเภท นั่นคือ เหยื่อที่มีลักษณะ Active Precipitation หรือ เหยื่อที่มีลักษณะอยู่เฉย (Passive Precipitation) ตามที่ได้กล่าวไว้ข้างต้น (วรรณ นิศาสุขสวัสดิ์, 2562)

เหยื่อจากการก่อการร้ายไซเบอร์มักจะเป็นในรูปแบบของ Passive Precipitation โดยเฉพาะเหยื่อในระดับปัจเจกบุคคล เพราะส่วนใหญ่จะมาจากความเพิกเฉย ละเลย ของเหยื่อเองที่ไม่ระวังตัวเป็นเหตุให้เกิดช่องว่างในการโจมตีของผู้ประสงค์ร้าย แต่ในระดับประเทศบางครั้งอาจเกิดจากการยั่วยุของฝ่ายใดฝ่ายหนึ่งเป็นเหตุทำให้ความขัดแย้งที่รุนแรงและสงผลให้เกิดการก่อการร้ายไซเบอร์หรือสงครามไซเบอร์ในที่สุด เช่น การยั่วยุของอิหร่านที่มีต่อสหรัฐอเมริกา การยั่วยุของประเทศรัสเซียที่มีต่ออดีตประเทศโซเวียต

และอย่างที่เห็นได้ชัดในปัจจุบันสงครามระหว่างรัสเซียและยูเครนที่เกิดขึ้นมาเป็นช่วงเวลาหลายสัปดาห์ส่วนใหญ่มาตรการที่ถูกใช้จะเป็นในเชิงการข่มขู่และกดดันทางเศรษฐกิจและไซเบอร์ เหยื่อในฐานะของรัฐชาติอย่างเป็นเทศยูเครนอาจถูกมองได้ว่าเป็นส่วนหนึ่งที่ทำให้รัสเซียเกิดปัญหาเนื่องจากยูเครนมีความต้องการที่จะเป็นส่วนหนึ่งขององค์การ NATO ซึ่งอาจถูกมองเป็นการชักศึกเข้าบ้านของรัสเซียเพราสหรัฐสามารถที่จะวางฐานทัพในประเทศสมาชิกของ NATO ได้ ซึ่งเป็นจุดฉนวนที่ทำให้รัสเซียไม่พอใจ

แต่อย่างไรก็ตามการที่รัสเซียเริ่มประกาศสงครามกับยูเครนและทำร้ายผู้บริสุทธิ์ก่อนนั้นถือเป็นเรื่องที่ผิดตามหลักมนุยธรรม แต่การที่รัสเซียใช้สงครามไซเบอร์เป็นส่วนหนึ่งของสงครามครั้งนี้ยังไม่สามารถที่จะตอบได้ว่าผิดหลักมนุษยธรรมหรือไม่และการที่ประเทศต่าง ๆ ร่วมมือกันตอบโต้รัสเซียที่กระทำต่อยูเครนด้วยการโจมตีทางไซเบอร์นั้นถือเป็นการป้องกันตนเองหรือไม่และเหยื่อในสถานการณ์นี้มีจำนวนมากเท่าใด ทฤษฎีจำเป็นต้องขยายความในเรื่องของประเภทของเหยื่อว่าเป็นเหยื่อในรูปแบบใด สถานการณ์ใด และวิธีการตอบโต้ของเหยื่อที่มีต่อผู้กระทำนั้นถูกต้องหรือไม่ จึงจะสามารถอธิบายปรากฏการณ์ทางไซเบอร์ได้อย่างชัดเจน

2.5.3 ทฤษฎีสงครามในเชิงป้องกัน

หลังจากที่ได้วิเคราะห์ปัจจัยที่จะทำให้เกิดการก่อการร้ายในระดับปัจเจกแล้วนั้น สิ่งที่สำคัญประการต่อมาคือการวิเคราะห์กลวิธีในการนำเทคโนโลยีมาใช้ในการก่อการร้ายหรือการทำให้เกิดสงคราม สำหรับหลักการทำสงครามหรือตำราที่จะใช้ประกอบนั้นมีหลายตำรา ต่างขึ้นอยู่กับบริบทของพื้นที่ที่ใช้ในการทำสงคราม ทักษะของผู้ที่ใช้ หรือสถานการณ์ ณ ขณะนั้น แต่สำหรับโลกไซเบอร์ปัจจัยบางอย่างย่อมเปลี่ยนไป เช่น ปัจจัยในเชิงพื้นที่ที่ไม่ว่าสนามรบที่ใดในโลกใบนี้ย่อมเหมือนกัน เป็นการรบที่ไร้พรมแดน แต่บางสิ่งบางอย่างที่ตำราสงครามดั้งเดิมจะนำมาใช้กับการก่อการร้ายไซเบอร์ได้ อาจจะเป็นในเรื่องทักษะของนักรบ และเช่นเดียวกันกับการก่อการร้ายไซเบอร์ก็ย่อมมีแนวทางที่ไม่ต่างจากการทำสงครามมากนักโดยหลักการทั่วไปของการทำสงครามนั้นจะเสนอให้เห็นต่อไป

“หลักการสงคราม คือ หลักการพื้นฐานในการดำเนินสงคราม ที่แต่ละประเทศกำหนดให้หน่วยทหารของตนยึดถือเป็นแนวทางในการวางแผน และอำนวยการปฏิบัติการรบเพื่อให้บรรลุความสำเร็จของการดำเนินสงครามเป็นส่วนรวม” การกำหนดหลักการสงครามของประเทศใดประเทศหนึ่ง จะต้องผ่านกระบวนการศึกษา วิเคราะห์ บทเรียนจากกรบในอดีต ทั้งของกองทัพของตนเอง และกองทัพประเทศอื่น ๆ ประกอบการคาดการณ์รูปแบบของสงครามที่มีโอกาสที่จะเกิดขึ้นในอนาคต นำมาประมวลเป็นหลักการสงครามที่ใช้เป็นกรอบของแนวคิด สำหรับการรบของกองทัพ

ประเทศนั้น ๆ โดยยึดถือเป็นหลักที่ใช้ปฏิบัติ 10 หลักการ ตามที่ วชิรศักดิ์ พูสิทธิ์ ได้กล่าวไว้ในหลักการทำสงครามในศตวรรษที่ 21 (วชิรศักธิ์ พูสิทธิ์, 2557) ได้แก่

1. การจู่โจมต้องมีจุดมุ่งหมายที่ชัดเจน (Objective) การจู่โจมใด ๆ ก็แล้วแต่หากขาดจุดมุ่งหมายที่ชัดเจนก็ไม่สามารถที่จะบรรลุวัตถุประสงค์ทางการเมืองที่วางไว้ได้ โดยกลยุทธ์ในที่นี้จะให้ความกระจ่างและชัดเจนต่อการกำหนดเป้าหมายหรือวัตถุประสงค์ ทั้งในระดับ ยุทธศาสตร์ชาติ ยุทธศาสตร์ทหาร หรือแม้กระทั่ง ในยุทธวิธี การกำหนดความชัดเจนของความมุ่งหมายเป็นเรื่องที่ทำให้การปฏิบัติในทุกส่วนของหน่วยระดับรองลงมามีความเข้าใจตรงกัน และไม่สับสนที่จะนำไปปฏิบัติที่สำคัญการรักษาซึ่งจุดมุ่งหมายเดียวกันจะย่อมทำให้เกิดความกลมเกลียวและนำมาซึ่งผลลัพธ์เดียวกัน

หากจะเชื่อมโยงถึงการก่อการร้ายทางไซเบอร์บางครั้งผู้ก่อการร้ายไม่ได้มีเป้าหมายหลักในการจู่โจมเป็นแค่การกระทำที่ใช้เพื่อความสนุกเท่านั้น การก่อการร้ายในรูปแบบนี้จึงไม่ได้เป็นการก่อการร้ายที่มีเป้าหมายชัดเจน ส่วนมากมักจะมุ่งโจมตีในระดับปัจเจกเท่านั้น

รูปที่ 8 องค์ประกอบในการก่อสงคราม

ที่มา: Handel (1997)

2. การจู่โจมเชิงรุก (Offensive) ในการจู่โจมใดก็ตาม ผู้ที่โจมตีย่อมปรารถนาที่จะชนะสงคราม ดังนั้นฝ่ายที่เริ่มก่อนมักจะมีการเตรียมตัวมาเป็นอย่างดี และจะเตรียมการปฏิบัติที่จะนำมาซึ่งชัยชนะได้ดังนั้นการชิงความได้เปรียบด้วยการริเริ่มที่จะโจมตีก่อนและสามารถขยายผลความมุ่งมั่นนั้นได้ จะถึงหลักในการรุก ซึ่งเป็นหลักการที่จะนำไปสู่การบรรลุความมุ่งหมายตามหลักการ

สงครามในข้อหนึ่ง ทั้งนี้อยู่ที่ความได้เปรียบของแต่ละฝ่ายซึ่งถ้าฝ่ายใดสามารถดำรงความริเริ่มโดยใช้หลักการรุกได้ ก็จะเป็นผู้ที่กำหนดฝ่ายตรงข้าม กรณีเช่นนี้เห็นได้จากการที่อิหร่านพยายามที่จะเป็นฝ่ายรุกโจมตีไซเบอร์กับอเมริกาก่อนที่ตนจะโดนโจมตี เช่นเดียวกันกับเกาหลีเหนือที่พยามจะเป็นฝ่ายรุกก่อนเช่นกัน ผู้ที่เป็นฝ่ายรุกจะสามารถดำเนินการตามที่เราต้องการได้ หรือเรียกว่าการเป็นผู้กำหนดทิศทางและกำหนดปัญหาให้กับฝ่ายตรงข้ามเป็นผู้แก้ ไม่ใช่ให้ฝ่ายตรงข้ามเป็นผู้กำหนดปัญหาให้เราเป็นผู้แก้

3. หลักการรวมพลหรือทรัพยากร (Mass) หลักการรวมพลหรือทรัพยากรในที่นี้คือในการปฏิบัติแต่ละครั้ง จะต้องมุ่งให้เกิดอำนาจกำลังรบสูงสุด นั่นหมายความว่าการรวมกันอยู่เป็นกลุ่มจะมีพลังมากกว่าการแยกกัน หากมีทรัพยากรที่ต้องใช้ในการโจมตีก็จำเป็นที่จะต้องนำมารวมกันให้ได้มากที่สุด สามารถเปรียบเทียบได้กับกองทัพไซเบอร์ของนานาประเทศที่จะต้องมีการตั้งศูนย์และรวบรวมกำลังผลให้ได้มากที่สุดเพื่อป้องกันไม่ให้เกิดภัยคุกคามที่ไม่สามารถคาดการณ์ได้ ดังนั้นการรวมทรัพยากรเข้าไว้ในส่วนกลางจะทำให้บรรลุความสำเร็จ ถ้าในระดับยุทธศาสตร์ของชาตินั่นแปลความว่าคือการใช้พลังอำนาจของชาติทั้งมวลในสัดส่วนสูงสุด ใช้ผู้ที่เชี่ยวชาญทางไซเบอร์รวมกันในสัดส่วนที่สูงที่สุดเมื่อเกิดผลกระทบต่อปัญหาที่สั่นคลอนต่อความมั่นคงของชาติ

4. หลักการออมกำลัง (Economy of Force) ตามทฤษฎีการจู่โจมในสงคราม การออมกำลังเป็นสิ่งจำเป็นเมื่อยามเกิดวิกฤติหรือแผนไม่ได้เป็นไปตามที่คาดไว้ แต่ในอีกแง่หนึ่งการออมกำลังในแง่นี้หมายถึงหลักการที่จะต้องใช้กำลังน้อยการปฏิบัติที่เป็นรอง ในการจู่โจมนั้นย่อมต้องมีหลายภารกิจ และจะต้องแยกให้ชัดเจนว่าอันไหนคือภารกิจหลักหรือภารกิจรอง ในการจะปฏิบัติภารกิจรองนั้นจะต้องสงวนกำลังทั้งหมดไว้สนับสนุนเพื่อจะต้องทุ่มเทกำลังในการปฏิบัติภารกิจหลัก หรือกล่าวได้ว่าการกระทำใดที่เป็นเรื่องรอง จะใช้ทรัพยากรที่มีอยู่ในอัตราส่วนที่น้อยที่สุดเข้ากระทำเพื่อออมทรัพยากรที่มีอยู่อย่างจำกัดไว้ กลยุทธ์ข้อนี้อาจจะแตกต่างกับกับบริบททางไซเบอร์เพราะในการสู้ผ่านเทคโนโลยีนั้นเป็นเสมือนตัวแทน การจะสำรองทรัพยากรไว้อาจจะนำมาใช้ในแง่ของการฟื้นตัวของสาธารณูปโภคต่าง ๆ เมื่อโดนโจมตีแล้วเสียหาย เพราะฉะนั้นในแง่ของไซเบอร์การออมกำลังหรือสำรองทรัพยากรจึงเป็นกลยุทธ์เชิงรับมากกว่า

5. หลักการดำเนินกลยุทธ์ (Maneuver) หลักการของข้อนี้มีความซับซ้อนมากหากต้องเปรียบกับการโจมตีในโลกไซเบอร์เพราะเปรียบเสมือนการบังคับฝ่ายศัตรูที่อยู่ในฐานะที่เสียเปรียบ โดยการใช้อำนาจของผู้ได้เปรียบมุ่งโจมตีฝ่ายตรงข้ามที่กำลังอ่อนแอแบบประกบจุดตามกลยุทธ์ที่ได้วางไว้ การเคลื่อนย้ายกำลังจู่โจมจุดอ่อนของฝ่ายตรงข้าม ทำให้ศัตรูเสียเปรียบและสามารถเอาชนะศัตรูได้ การกระทำเช่นนี้มักจะเป็นเชิงเทคนิค เช่น การใช้ไวรัส Trojan ในการเข้าไป

อยู่ในอุปกรณ์ของฝ่ายศัตรูทั้งที่ศัตรูรู้ตัวแต่ก็สายไปเมื่อไวรัสนั้นเริ่มทำงานโดยการโจมตีจุดอ่อนของฝ่ายตรงข้ามทันที (Zhenfang, 2015)

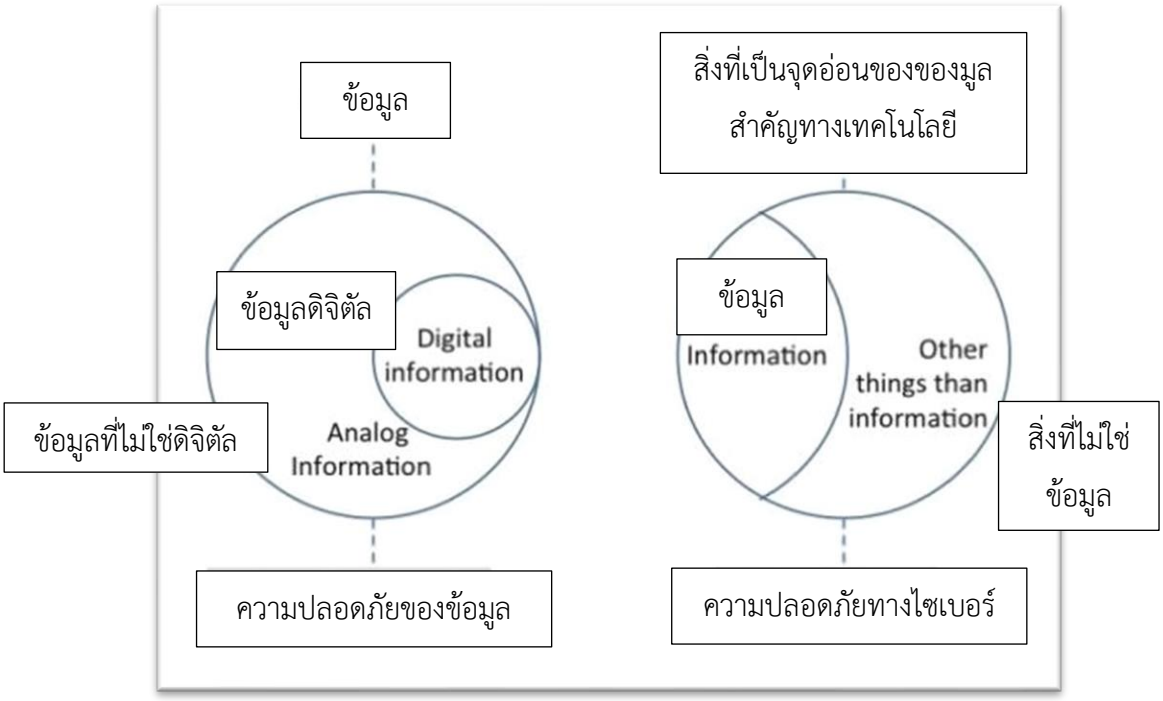
6. หลักเอกภาพในการบังคับบัญชา (Unity of Command) หลักนี้สามารถใช้ได้ในกลุ่มการโจมตีทุกรูปแบบ โดยจะช่วยลดความสับสนในการบังคับบัญชา จัดให้มีอำนาจในการสั่งการภายใต้ผู้บังคับบัญชาคนเดียว นั่นหมายถึงปฏิบัติการใด ๆ ในแต่ละครั้งจะต้องมีผู้ที่รับผิดชอบเพียงคนเดียว หลักการบังคับบัญชาแบบนี้สามารถพบเห็นได้ในประเทศที่สามารถควบคุมได้อย่างเบ็ดเสร็จ เช่น เกาหลีเหนือ หรืออิหร่านที่กองกำลังไซเบอร์ของตนจะขึ้นตรงอยู่กับผู้บังคับบัญชาซึ่งเป็นหัวหน้าสูงสุดเพียงเท่านั้นเพราะจะทำให้สามารถสั่งการได้ทันที และง่ายต่อการจู่โจมและการตัดสินใจ

7. หลักการจู่โจม (Surprise) หลักการในข้อนี้เป็นหลักการเชิงเทคนิคคือ การจู่โจมฝ่ายตรงข้าม ณ เวลา และสถานที่ ในลักษณะทันทีจนฝ่ายตรงข้ามไม่ทันตั้งตัว เมื่อฝ่ายศัตรูไม่ทันได้คาดคิดก็จะไม่มีโอกาสตอบโต้หรือเตรียมการในการตั้งรับ ปัจจัยที่จะก่อให้เกิดการจู่โจม ได้แก่ ความรวดเร็ว และทำในสิ่งที่ศัตรูคาดไม่ถึง ในอดีตหลักการสงครามข้อนี้ถูกนำมาใช้เพื่อช่วยยุติการรบในครั้งนั้นโดยเร็ว ซึ่งบางครั้งเป็นการแก้จุดตาย (Deadlock) ของการใช้กำลังจากทั้งสองฝ่าย จากตำราดั้งเดิมสามารถนำมาประยุกต์ใช้กับการก่อการร้ายหรือสงครามไซเบอร์ เช่นการโจมตีหน่วย SWAT ที่เคยกล่าวไว้ในก่อนหน้าว่าหน่วย SWAT นั้นไม่มีเวลาในการตัดสินใจมากนัก และการโจมตีในรูปแบบใหม่ ๆ ที่พบเจอในปัจจุบันจะทำให้ฝ่ายที่ถูกโจมตีไม่สามารถคาดการณ์ได้ตลอดเวลา ด้วยเหตุเช่นนี้จึงทำให้การโจมตีไซเบอร์เป็นเรื่องที่อันตรายและยิ่งเพิ่มทวีความรุนแรงมากขึ้นเพราะไม่สามารถรับมือได้

8. หลักความง่าย (Simplicity) คือ การดำเนินการในเรื่องของยุทธศาสตร์การทำแผนที่ไม่มีความคลุมเครือ ชัดแจ้ง และชัดเจน ง่ายต่อความเข้าใจ หรือรวมไปถึงคำสั่งจากผู้บังคับบัญชาที่สามารถสั่งการแล้วทำให้เกิดความเข้าใจตรงกันทุกภาคส่วนมาใช้ในการบัญชาการ ข้อดีของหลักนี้จะทำให้กองกำลังสามารถที่จะเดินไปด้วยกันและเป็นหนึ่งเดียวกันได้ สามารถใช้ได้ทั้งการโจมตีแบบดั้งเดิมและแบบไซเบอร์มีความสอดคล้องกับหลักเอกภาพในการบังคับบัญชาและหลักการจู่โจมที่มีจุดมุ่งหมายชัดเจน ความง่ายจะเป็นหลักประกันที่ทำให้ทุกระดับมีเป้าหมายเดียวกัน

9. หลักการรักษาความปลอดภัย (Security) คือ หลักการที่มีเพื่อ ลดความเสี่ยง ความประมาท เลินเล่อ ของฝ่ายตนในการปฏิบัติกับฝ่ายตรงข้าม เป็นกลยุทธ์ที่ตั้งรับ ปกปิดความลับและจุดอ่อนที่ฝ่ายตนมีไม่ให้ฝ่ายศัตรูล่วงรู้ และการรักษาความปลอดนี้ก็ไม่ควรจะมีการป่าวประกาศว่าฝ่ายตนมีอะไร เพื่อป้องกันไม่ให้ความลับรั่วไหลและป้องกันไม่ให้ฝ่ายตรงข้ามใช้ประโยชน์จากจุดอ่อนที่เรามีการรักษาความปลอดภัยจากการจู่โจมไซเบอร์เป็นประเด็นใหญ่นอกจากจะต้องปกปิดจุดอ่อนของตนเองแล้ว ยังต้องคำนึงถึงหลักการทำงานร่วมกันในรูปแบบของภาคี เครือข่ายการ

ส่งเสริมให้ความรู้กับบุคลากรให้รับรู้ถึงสถานการณ์ไซเบอร์ที่เกิดขึ้น ไปจนถึงโครงสร้างขององค์กรที่มีแผนรองรับภัยคุกคามไซเบอร์นั้นไว้แล้ว



รูปที่ 9 เทคนิคการป้องกันข้อมูลในรูปแบบของ Information Security และ Cyber Security

ที่มา: Handel (1997)

รูปที่ 9 แสดงให้เห็นถึงเทคนิคการป้องกันข้อมูลในรูปแบบของ Information Security และ Cyber Security ซึ่งมีความแตกต่างกัน ในส่วนของ Information Security จะประกอบไปด้วยข้อมูลแบบ Analog และ Digital ในส่วนของ Cyber Security จะประกอบด้วยข้อมูล (Information) และสิ่งที่ไม่ได้เป็นข้อมูล (Other Things than Information) เช่น สิ่งของทางกายภาพ ยานพาหนะ สัญาณไฟจราจร เครื่องใช้ไฟฟ้า ซึ่งทั้งหมดนี้จำเป็นจะต้องได้รับการรักษาความปลอดภัยทั้งสิ้น (Handel, 1997)

10. หลักการต่อสู้แบบทำลายล้าง (Total Annihilation) หลักการนี้เป็นการผนึกกำลังเพื่อป้องกันประเทศจากข้าศึกทั้งมวลเข้าด้วยกันโดยใช้กองทัพเป็นแกนกลาง หลักการในข้อนี้คือการจัดให้มีกำลังประจำถิ่น กำลังประชาชนเข้ามามีส่วนร่วมในการป้องกันประเทศ วัตถุประสงค์ของการใช้ยุทธศาสตร์นี้คือ การสร้างความพร้อมในการที่จะเผชิญต่อภัยคุกคามไม่ว่ารูปแบบใดก็ตาม โดยเพิ่มสภาพความพร้อมรบและขยายกำลังเต็มขนาดได้อย่างรวดเร็ว ในทางยุทธศาสตร์ หลักการนี้เป็นการแสดงเจตนารมณ์ ของประชาชนในการที่จะรักษาเอกราช และ อธิปไตยของชาติ ซึ่งเป็นสิ่งที่ต้องใช้ความพยายามร่วมกัน ของประชาชนทุกสาขาอาชีพ และกองทัพ จากหลักการข้างต้นแสดงให้เห็น

ว่าหากประชาชนรวมเป็นหนึ่งเดียวกับกองทัพจะทำให้การต่อสู้มีโอกาสจะชนะฝ่ายตรงข้ามมากขึ้น เช่นเดียวกันกับภัยจู่โจมไซเบอร์ หากภาคประชาชนและภาคส่วนอื่น ๆ ทั้งหมดมีความตระหนักรู้ในเรื่องของภัยไซเบอร์จะทำให้กองกำลังของประเทศมีความแข็งแกร่งมากขึ้น การโต้ตอบกับศัตรูจะทำได้ง่ายและเป็นไปอย่างหนักแน่น ทั้งนี้รัฐบาลจะต้องสั่งการเตรียมพร้อมรับมือกับภัยคุกคามไซเบอร์ โดยจะต้องมีสายบังคับบัญชาที่ชัดเจน มีวัตถุประสงค์ที่ชัดเจน คำสั่งที่ออกมาต้องง่ายต่อการเข้าใจ

นอกจากนี้ในการทำสงครามใด ๆ ยังต้องอาศัยกลยุทธ์ในการริเริ่ม (INITIATIVE) ใช้ทดแทน “หลักการรุก” (Offensive) เข้าควบคุมสถานการณ์เพื่อชิงความได้เปรียบ การริเริ่มที่นำมาใช้แทนการรุกนี้จะเป็นการเปิดกว้างในการวางยุทธศาสตร์การรบ ซึ่งจะต้องใช้เวลาในการศึกษาหา “สาเหตุ” (Causes) และ “ผล” (Effect) เพื่อประมาณการณ์ถึงแนวโน้มที่อาจเป็นไปได้ ดังนั้น ผู้วางยุทธศาสตร์จะต้องคำนึงถึงกลยุทธ์แนวรุกและแนวรับเพื่อพร้อมกับการหาสาเหตุและผลกระทบที่จะตามมา นักยุทธศาสตร์ต้องเตรียมข้อมูล วิเคราะห์ ศึกษาสภาวะแวดล้อมทางยุทธศาสตร์ (Strategic Environment) พร้อมทั้งสามารถกำหนดผู้รับผิดชอบแผนการนั้น ๆ ได้อย่างชัดเจน โดยเฉพาะการวางยุทธศาสตร์การรบในยุคข้อมูลข่าวสารดิจิทัล

การรอให้ฝ่ายตรงข้ามจู่โจมก่อนย่อมส่งผลให้เกิดการเสียเปรียบเป็นอย่างมาก เนื่องจากในปัจจุบัน การไหลของข้อมูลเกิดขึ้นอย่างรวดเร็ว ดังนั้น การเป็นผู้ควบคุมสถานการณ์ได้ก่อน จะทำให้สามารถกำหนดและควบคุมสภาวะแวดล้อมของสถานการณ์เอาไว้ได้ หมายความว่าฝ่ายตรงข้ามจำเป็นจะต้องปรับเปลี่ยนวิถีทางของตนให้สอดคล้องกับสถานการณ์ ที่ผู้ได้เปรียบเป็นฝ่ายกำหนด เห็นได้ชัดว่าจุดเริ่มต้นนั้นสามารถกำหนดชะตากรรมของการรบได้ ผู้ที่ได้เปรียบคือผู้ที่มีความแข็งแกร่งและสามารถเริ่มเกมส์ได้ก่อน สงครามไซเบอร์ก็เช่นกัน การเริ่มต้นควรมากับความพร้อมและอำนาจการต่อรองในระดับสูงเพื่อสร้างความเกรงกลัวให้กับฝ่ายตรงข้ามไม่ให้กล้าเข้ามาจู่โจม

สิ่งที่ยังเป็นปัญหาของการก่อการร้ายของโลกปัจจุบันคือการหาจุดร่วมในการให้ความหมายของการกระทำ ซึ่งปัจจุบันมี 3 สำนักหลักที่พยายามวิเคราะห์การก่อการร้ายไซเบอร์ 1) สำนักแรกมีแนวคิดที่ว่าการก่อการร้ายไซเบอร์เป็นเรื่องเล็กและอันตรายน้อยกว่าการก่อการร้ายแบบดั้งเดิม แต่อย่างไรก็ตามความเห็นของสำนักที่สองกลับตรงกันข้ามกับสำนักที่หนึ่งโดยสิ้นเชิง 2) สำนักที่สองมีความเชื่อว่าการก่อการร้ายไซเบอร์จะนำมาซึ่งการสูญสิ้นของโลกใบนี้ได้ และสำนักสุดท้าย 3) สำนักนี้เชื่อว่าคำนิยามที่มีอยู่ในปัจจุบันนั้นแคบเกินไปที่จะกำหนดว่าการกระทำใด ๆ ของผู้ก่อการร้ายโดยใช้คอมพิวเตอร์เป็นอาวุธจะสามารถเรียกการกระทำนั้นว่า การก่อการร้ายไซเบอร์ได้ (Thruelsen, 2006)

2.6 โครงสร้างพื้นฐานสำคัญของประเทศ (Critical National Infrastructure) และการก่อการร้ายไซเบอร์ (Critical National Infrastructure and Cyber Terrorism)

นักวิชาการมีความเชื่อว่าเป้าหมายของการก่อการร้ายไซเบอร์ คือ การมุ่งโจมตีโครงสร้างพื้นฐานสำคัญของประเทศ หรือ Critical National Infrastructure เพื่อสร้างความหวาดกลัวให้กับประชาชน ในขณะที่คนบางส่วนเชื่อว่า หากการโจมตีโครงสร้างพื้นฐานสำคัญของประเทศนั้นไม่ได้สร้างความหาดกลัวต่อประชาชน การกระทำเหล่านั้นไม่ถือว่าเป็นการก่อการร้ายไซเบอร์ นักวิชาการหลายฝ่ายเห็นด้วยกับประโยคนี้ ในปี 2003 เกิดเหตุการณ์ไฟดับใน 8 มลรัฐ ทางเกาะตอนเหนือของสหรัฐอเมริกา ทำให้ประชาชนที่อาศัยอยู่ในมลรัฐเหล่านั้นกว่า 45 ล้านคน ไม่มีฟ้าฟ้าใช้ ต้องอยู่ท่ามกลางความมืดกว่า 7 ชั่วโมง แต่เหตุการณ์ครั้งนี้กลับไม่ได้สร้างความกลัวให้กับประชาชนเท่าใดนัก เพราะถือว่าเป็นเรื่องที่สามารถเกิดขึ้นได้ และเหตุไฟดับครั้งนี้ไม่ได้ถูกระบุว่าเป็นการก่อการร้ายด้วยเหตุผลที่ว่าอาจเป็นความผิดพลาดของระบบไฟฟ้าเท่านั้น

ตัวอย่างที่สำคัญอีกประการหนึ่งของการโจมตีโครงสร้างพื้นฐานสำคัญของประเทศ คือการจู่โจมทางไซเบอร์โดยการควบคุมการจราจรทางอากาศที่จะทำให้เกิดความเสียหายครั้งยิ่งใหญ่ หากใช้รูปแบบของการก่อการร้าย 9/11 ที่เคยโด่งดังทั่วโลก อย่างไรก็ตามการจู่โจมทางไซเบอร์นั้นอาจจะทำได้ยากขึ้นเพราะปัจจุบันการติดต่อสื่อสารทางอากาศยังจำเป็นต้องใช้คนเป็นสื่อกลางระหว่างระบบคอมพิวเตอร์การบินและนักบิน ไม่ใช่การบังคับเครื่องบินผ่านเครือข่ายคอมพิวเตอร์โดยตรง

ยังมีเหตุการณ์หนึ่งที่สะท้อนให้เห็นความร้ายแรงของปัญหาการก่อการร้ายไซเบอร์ได้ดี นั่นคือ การจู่โจมระบบในขั้นตอนการผลิตอาหาร ผู้ก่อการร้ายสามารถเจาะระบบการควบคุมของโรงงานหรืออุตสาหกรรมอาหาร ที่จะต้องใช้วัตถุดิบบางประเภทในการผลิต หากระบบถูกจู่โจมมีการเปลี่ยนแปลงขั้นตอนหรือวัตถุดิบในการทำอาหารนั้น ๆ เข้าไป เช่น การใส่สารเคมีในส่วนผสมที่เป็นอันตรายต่อชีวิต ลงในกระบวนการผลิตอาหารจำนวนมาก กรณีนี้อาจทำให้ประชาชนผู้บริโภคเป็นอันตรายโดยไม่รู้ตัว และผู้ประกอบการอาจจะโดนจับกุมโดยรัฐบาลในข้อหาที่ตนเองไม่ได้ก่อ เมื่ออาหารที่ออกมาจากกระบวนการผลิตนั้นถูกนำจำหน่ายสู่ตลาด ขั้นตอนการกวาดล้างผลิตภัณฑ์ที่เจือปนจะทำได้ยากยิ่งขึ้น

จากตัวอย่างที่กล่าวมาแสดงให้เห็นว่าโครงสร้างพื้นฐานสำคัญของประเทศ (Critical National Infrastructure) ควรมีการเพิ่มประสิทธิภาพในการป้องกันความปลอดภัยให้มากขึ้น เพื่อลดผลกระทบที่อาจจะทำให้เกิดความเสียหายต่อประชาชนในระดับมหภาคได้ (Jones, 2005)

2.7 ประวัติศาสตร์การโจมตีไซเบอร์และประเภทของการโจมตี (History of Cyber-Terrorism and Types of Attacks)

2.7.1 The Original Logic Bomb 1982

เมื่อประวัติศาสตร์ต้องจารึกการก่อการร้ายในรูปโฉมใหม่ การก่อการร้ายไซเบอร์จึงเป็นสถานการณ์หนึ่งที่จะต้องถูกจารึกไว้ให้เห็นถึงความร้ายแรงของเทคโนโลยี การโจมตีที่ส่งผลกระทบครั้งรุนแรงในยุคเริ่มต้นของประวัติศาสตร์การก่อการร้ายไซเบอร์ รู้จักในชื่อของ “The Original Logic Bomb” เหตุการณ์นี้เกิดขึ้นในยุคสงครามเย็น ปี 1982 หน่วย CIA ของสหรัฐอเมริกาถูกกล่าวหาว่าเป็นผู้จู่โจมท่อส่งก๊าซไซบีเรียที่ขนส่งก๊าซไปยังรัสเซียโดยปราศจากการใช้วิธีโจมตีแบบเดิม ๆ เช่น ระเบิด หรือ มิสไซล์ แต่กลับใช้การเขียนโค้ชโปรแกรมคอมพิวเตอร์เพื่อควบคุมการปฏิบัติการของระบบท่อก๊าซที่เรียกว่า “Logic Bomb” หรือซอฟต์แวร์ ชุดคำสั่งที่ปิดระบบและลบข้อมูลซอฟต์แวร์ในเครือข่ายการโจมตี ใช้เพื่อลอบวางระเบิดเสมือนจริง การใช้ Logic Bomb ไม่สามารถใช้วิธีป้องกันเดียวกับอาวุธนิวเคลียร์ เพราะปฏิบัติการไซเบอร์แบบนี้อยู่ในมุมมืดเหมือนการใช้กลยุทธ์การก่อการร้ายในการโจมตี เมื่อเปรียบเทียบกับความร้ายแรงของสงครามเย็นแล้ว การใช้ Logic Bomb มีความรุนแรงมากกว่าหลายเท่า (Carr, 2012)

ไซบีเรียอาจเป็นถูกมองเป็นพื้นที่ที่หนาวเหน็บและไร้ซึ่งทรัพยากร แต่ในความเป็นจริงนั้นไซบีเรียมีก๊าซธรรมชาติขนาดใหญ่ ก๊าซนี้ถูกนำส่งไปยังกรุงมอสโก ประเทศรัสเซีย การขนส่งจากตะวันออกเฉียงเหนือของประเทศมายังเมืองหลวงของรัสเซียเป็นระยะทางที่ยาวไกลและยังสร้างปัญหาให้แก่รัสเซียตลอดมา ถึงแม้สหภาพโซเวียตมีบุคลากรที่มีความรู้ทางวิศวกรรมสูง แต่ยังขาดผู้ที่มีความเชี่ยวชาญด้านคอมพิวเตอร์ที่จะสร้างระบบป้องกันทางเทคโนโลยีได้อย่างรัดกุม จึงเป็นผลให้สหภาพโซเวียตต้องพึ่งพิงบริษัทสัญชาติแคนนาดาในการสร้างระบบป้องกันทางเทคโนโลยี

ในช่วงเดือนตุลาคม ปี 1982 การระเบิดของท่อส่งก๊าซธรรมชาติเป็นเหตุการณ์ 1 ใน 7 ของการระเบิดที่ร้ายแรงที่สุดในประวัติศาสตร์โดยความรุนแรงนั้นเทียบเท่ากับการทิ้งระเบิดปรมาณู (The Atomic Bomb) ที่ประเทศญี่ปุ่นช่วงสงครามโลกครั้งที่สอง การเล่าขานถึงสาเหตุของการระเบิดท่อก๊าซไซบีเรียนั้นมีมากมาย โดยข้อกล่าวหาที่มีความน่าเชื่อถือมากที่สุดคือ การจู่โจมของสหรัฐอเมริกาผ่านหน่วย CIA หลักฐานหลักที่สนับสนุนแนวคิดนี้คือการที่กลุ่มสายลับรัสเซียที่มีชื่อว่า Vladimir Vetrov สามารถขโมยเอกสารลับของสหรัฐอเมริกาผ่านระบบของสายลับฝรั่งเศสที่มีการแลกเปลี่ยนข้อมูลกับหน่วยงาน CIA ของสหรัฐอเมริกาถึงกระบวนการโจมตีระบบท่อก๊าซ “ระบบ

ซอฟแวร์ที่ควบคุมกลไกของท่อก๊าซ หัวสูบ กังหัน ถูกตั้งค่าให้ทำงานผิดพลาด หลังจากการรบกวนการทำงานในครั้งแรกทำให้เกิดการตั้งค่าความเร็วของหัวสูบและความดันของท่อส่งก๊าซใหม่ที่เกินกำลังจะรับได้ เป็นผลทำให้ชิ้นส่วนข้อต่อของท่อก๊าซหลุดออกมาและเกิดการระเบิดในที่สุด ” (Lichfield, 2009) แต่อย่างไรก็ตามยังมีหลักฐานบางอย่างแสดงให้เห็นว่าเหตุการณ์ครั้งนี้เป็นข้อบกพร่องของของท่อก๊าซที่เกิดการรั่วและทำให้ความดันที่มีอยู่เพิ่มมากขึ้นจนเป็นเหตุให้ท่อก๊าซระเบิด

สำหรับข้อกล่าวหาที่มีต่อ CIA กลับสร้างความน่าเชื่อถือมากยิ่งขึ้นเมื่อสายลับฝั่งรัสเซียค้นพบว่าทั้งหมดเป็นแผนของสหรัฐอเมริกา รัสเซียเปิดเผยว่าตนได้บุกเข้าไปขโมยข้อมูลลับของสหรัฐอเมริกาผ่านระบบและการกระทำครั้งเปิดโอกาสให้สหรัฐอเมริกาปล่อยไวรัส Trojan horse เข้ามาในระบบซอฟแวร์ของรัสเซีย ไวรัสที่ติดเข้ามานั้นทำให้สหรัฐอเมริกาล่วงรู้ระบบการทำงานของท่อก๊าซไซบีเรียทั้งหมด (Reed, 2004) แต่อย่างไรก็ตามการกล่าวหาว่า CIA เป็นผู้อยู่เบื้องหลังการระเบิดท่อก๊าซไซบีเรียยังเป็นได้แค่สมมติฐานเพราะยังไม่มีหลักฐานเพียงพอที่จะเอาผิดได้ แต่สำหรับการศึกษาถึงความร้ายแรงของไวรัสคอมพิวเตอร์ที่เกิดขึ้นนั้นเป็นเรื่องที่น่าสนใจและควรจารึกไว้ในประวัติศาสตร์การก่อการร้ายไซเบอร์

2.7.2 Operation Titan Rain 2003

ปฏิบัติการ Titan Rain เกิดขึ้นในปี 2003 เมื่อสหรัฐเมริกาเปิดเผยการถูกโจมตีระบบไซเบอร์ทั้งประเทศสหรัฐอเมริกา โดยการโจมตีครั้งนี้เกิดถูกกล่าวหาว่าเป็นการกระทำของกองทัพประเทศมหาอำนาจทางตะวันออกอย่างจีน สิ่งที่สำคัญที่สุดของเหตุการณ์คือการโจมตีไม่ได้มาจากแฮกเกอร์ธรรมดาเพียงไม่กี่คนแต่เป็นการกรพทำของกองทัพจากรัฐซึ่งถูกกล่าวหาว่าเป็นฝีมือของประเทศจีน การจู่โจมครั้งนี้ไม่ได้ทำลายเพียงแค่ Department of Defense (DoD) ของสหรัฐอเมริกาเท่านั้น แต่ยังรวมไปถึง Ministry of Defense ของสหราชอาณาจักร การโจมตีที่เกิดขึ้นในอังกฤษสร้างความเสียหายไปยังสถานการณ์สำคัญในปี 2006 ที่ระบบคอมพิวเตอร์ของ The House of Commons ถูกระงับจากการโจมตี แต่อย่างไรก็ตามรัฐบาลจีนปฏิเสธทุกข้อกล่าวหาในการโจมตีแต่กลับให้ข้อสังเกตว่าผู้ก่อการร้ายนั้นใช้คอมพิวเตอร์และเวปไซต์จากประเทศจีนกระทำสิ่งเหลานั้น เป็นที่ทราบกันดีว่าระบบคอมพิวเตอร์ในประเทศจีนนั่นมีระบบการป้องกันไม่เพียงพอและง่ายต่อแฮกเกอร์ที่จะใช้เป็นเครื่องมือ ถึงแม้จีนจะมีข้ออ้างดังกล่าวแต่ก็ไม่สามารถโน้มน้าวให้น่าเชื่อถือได้เพราะปฏิบัติการ Titan Rain เป็นปฏิบัติการขนาดใหญ่ที่จะต้องใช้แฮกเกอร์ผู้เชี่ยวชาญหลายคนร่วมมือการใช้คอมพิวเตอร์ในเครือข่ายประเทศจีน ปฏิบัติการนี้จะต้องอาศัยความอดทน ความร่วมมือ และสายลำดับบังคับบัญชาขององค์กร

แต่ในที่สุดปฏิบัติการนี้สร้างความขัดแย้งอย่างเป็นรูปธรรมระหว่างสหรัฐอเมริกาและประเทศจีน เพราะการโจมตีนี้สร้างความเสียหายให้กับองค์กรสำคัญ ๆ ของสหรัฐอเมริกา เช่น องค์กร NASA และ FBI ซึ่งปฏิบัติการแบบนี้ไม่สามารถกระทำได้ผ่านแฮกเกอร์อิสระ แต่จะต้องกระทำผ่านหน่วยงานกองทัพของจีนเท่านั้น จุดเริ่มต้นของปฏิบัติการ Titan Rain เป็นเหตุการณ์แรกที่สหรัฐเริ่มตั้งข้อสงสัยกับประเทศจีนและยังคอยจับตาดูความเคลื่อนไหวอยู่ตลอดมา และเหตุการณ์ครั้งนี้ยังคงเป็นเหตุการณ์แรกที่ทำให้ทุกประเทศเริ่มตระหนักถึงภัยคุกคามไซเบอร์ (Cyware Social, 2016)

2.7.3 Mimetic สู่ Mimetic 2000

จากงานวิจัยของ Greenberg (1995) แสดงให้เห็นว่า แบตเตอร์รี่ ของ MacBook สามารถจูโจมผ่านตัวควบคุมแบตเตอร์รี่ที่จะควบคุมระดับอุณหภูมิและพลังงานที่ใช้ เมื่อตัวควบคุมทำงานผิดพลาด แบตเตอร์รี่จะไม่สามารถใช้งานได้ ในตอนท้ายของงานวิจัยยังเสริมไว้อีกว่า หากโชคร้ายแบตเตอรี่อาจจะเกิดการระเบิดได้ และแนวความคิดนี้เองที่ถูกนำมาเชื่อมโยงการทำงานของไวรัสกลายเป็นข่าวพาดหัวหนังสือพิมพ์ Weekly World News ในปี 2000 ที่ว่า แฮกเกอร์สามารถเปลี่ยนคอมพิวเตอร์ที่บ้านของคุณให้กลายเป็นระเบิดได้ (“Hackers can turn your home computer in to a BOMB”)

หลังจากนั้นไม่นาน YouTube ได้อัพโหลดคลิปวิดีโอ การปล่อยไวรัสที่เป็นที่มาของการระเบิดในแบตเตอร์รี่ลิเทียม ซึ่งเป็นส่วนหนึ่งของอุปกรณ์อิเล็กทรอนิกส์ เช่น คอมพิวเตอร์ โทรศัพท์มือถือ สร้างความตอกย้ำในหมู่ประชาชนถึงความร้ายแรงของการโจมตีทางไซเบอร์

ในปี 1994 มีผู้ใช้อินเทอร์เน็ตทั้งหมดกว่า 25 ล้านคน ซึ่งเทียบเป็นร้อยละ 0.4 ของประชากรทั้งโลก ซึ่งในขณะนั้น Social Media ยังไม่มีขึ้นในระบบอินเทอร์เน็ต ประชาชนใช้ยังอีเมล์ในการติดต่อสื่อสาร ในปี 1994 อีเมล์มีคำเตือนให้กับผู้ที่ใช้ในกรณีระวังการโจมตีของไวรัส (Virus) ชื่อ Good Times ที่มีอยู่ในอินเทอร์เน็ต คำเตือนของผู้เชี่ยวชาญได้บอกไว้ว่าหากผู้ใดได้รับอีเมล์ที่มีชื่อว่า Good Times ผู้นั้นจำเป็นจะต้องรีบลบทันทีเพราะหากอีเมล์นี้ถูกเปิดขึ้นมาจะสามารถทำลายข้อมูลทั้งหมดในคอมพิวเตอร์ของผู้ใช้ ที่มากไปกว่านั้นอีเมล์ Good Times ยังสามารถขอให้ผู้ใช้นั้นส่งต่อเพื่อเป็นการแพร่กระจายไวรัสตัวนี้ไปยังผู้ใช้อื่น ๆ อีกด้วย นี่จึงเป็นสาเหตุทำให้ไวรัสชนิดนี้แพร่ระบาดไปทั่วโลก

Good Times เป็นไวรัสหลอกลวงชนิดหนึ่ง ที่รู้จักในชื่อของ Hoax Virus แต่ปัจจุบันนี้ไวรัสหลอกลวง Hoax ได้แพร่กระจายไปตามอีเมล์ทั่วโลก จากคอมพิวเตอร์เครื่องหนึ่งไปยังอีกเครื่องหนึ่ง ทำลายข้อมูลส่วนตัวภายในคอมพิวเตอร์นั้น ๆ เป็นการสร้างความหวาดกลัวที่มองไม่

เห็นในสังคม ไวรัส Good Times เป็นไวรัสที่ถูกส่งต่อคนหนึ่งไปสู่อีกคนหนึ่ง เป็นวิธีเดียวกันกับไวรัสทั่วไป แต่ลักษณะเด่นของไวรัสตัวนี้คือการเล่นกับจิตวิทยาความรู้สึกของมนุษย์ (Human Mind) ที่รู้จักในชื่อของ Mimetic Virus (Skoudis & Zeltser, 2004) ตามทฤษฎีของ Mimetic มีขึ้นในสมัยกรีกโบราณ นักปรัชญาในสมัยนั้นให้ความหมาย Mimetic ว่าคือการเลียนแบบ (imitation) การล้อเลียน (Mimicry) ท่าทางการแสดงออก (The Act of Expression) หรือการแสดงตัวตน (Presentation of the Self) (Gebauer & Wulf, 1995: p. 17) และมากกว่าการส่งข้อความระหว่างบุคคลหนึ่งถึงบุคคลหนึ่ง ไวรัส Good Times ยังสร้างความกลัวจากบุคคลหนึ่งสู่บุคคลหนึ่ง เป็นการแพร่ระบาดทางความคิด ที่ทำให้ทุกคนเชื่อว่า ไวรัส Good Times จะสามารถทำลายข้อมูลในเครื่องคอมพิวเตอร์ได้ จึงทำให้ผู้คนที่รับรู้เรื่องราวเหล่านี้มีการเตือนผู้ใช้คนอื่น ๆ ผ่านช่องทางทางอีเมล์ ความเชื่อหนึ่งที่ปรากฏให้เห็นชัดคือ หากผู้ที่ได้รับอีเมล์ ไวรัส Good Times และ ได้ Activated ไวรัสตัวนี้เรียบร้อยแล้วนั้นจะสามารถทำลายระบบ hard drive เครื่องอุปกรณ์ภายนอกได้ และทั้งหมดนี้คือความสำเร็จของไวรัส Good Times ที่ใช้เทคนิคในการหลอกลวงจากการพูด ๆ ต่อ ๆ กัน ผ่านทางอีเมล์ (Pseudo-Ttechnical Babble) (Gebauer & Wulf, 1995) เปรียบ เสมือนกับดักแห่งความกลัวในโลกไซเบอร์

สัญลักษณ์ หรือ Meme เป็นแนวความคิด พฤติกรรม ที่แพร่ระบาดจากคนสู่คนภายในวัฒนธรรมเดียวกันเพื่อสืบสานต่อวัฒนธรรมหรือแนวคิดนั้น ๆ ให้มีอยู่ต่อไป จากรุ่นสู่รุ่น ที่ Richard Dawkins ได้เขียนไว้ในทฤษฎีของเขา “Culture is transmitted through units known as memes.”(Gebauer & Wulf, 1995) การแพร่ระบาดของ Meme สามารถพบเจอได้ในโลกอินเทอร์เน็ตในปัจจุบัน วิธีการแพร่จะเป็นไปอย่างรวดเร็วจากคนหนึ่งสู่อีกคนหนึ่ง ผ่าน Email Blog Forum หรือ สื่อสังคมออนไลน์ ในตลอด 20 ปีที่ผ่านมา ตั้งแต่ ไวรัส Good Times ได้ถูกคิดค้นมา จำนวนของผู้ใช้อินเทอร์เน็ตมีมากขึ้น โดยในขณะนี้มีมากถึง 3 ล้านล้านคน คิดได้เป็น ร้อยละ 40 ของประชากรทั้งโลก เพียงแค่ประชากรในประเทศอังกฤษประเทศเดียวนั้นมีมากถึง 57 ล้านคนซึ่งคิดเป็นร้อยละ 89.9 ของจำนวนประชากรทั้งประเทศ ในปี 2017 หากคิดจากจำนวนประชากรทั้งหมดบนโลกใบนี้ อาจเทียบได้เป็น 1 ใน 4 ของประชากรทั้งหมดที่เข้าถึงสื่อสังคมออนไลน์ และมีแนวโน้มจะเพิ่มขึ้นเป็น 1 ใน 3 ในอนาคตอันใกล้ (Marketer, 2013) การเพิ่มขึ้นของจำนวนผู้ใช้อินเทอร์เน็ตอย่างรวดเร็ว จะยิ่งเพิ่มความซับซ้อนของการทำงานไวรัสมากยิ่งขึ้นและยากที่จะควบคุม

2.7.4 Web War One 2007 (สงครามไซเบอร์ประเทศเอสโตเนีย)

สงครามไซเบอร์เปลี่ยนโลกในครั้งนี้เกิดขึ้นในปี 2007 ช่วงเวลาฤดูใบไม้ผลิของประเทศติดทะเลบอลติก ความขัดข้องของระบบเทคโนโลยีโครงสร้างสาธารณูปโภคพื้นฐานประเทศ

เอสโตเนียทั้งประเทศทำให้เกิดความโกลาหลวุ่นวาย การโจมตีระบบในครั้งนี้ทำให้ความสัมพันธ์ระหว่างรัสเซียและเอสโตเนียเกิดความสั่นคลอนจากความขัดแย้งดั้งเดิมระหว่างประเทศอดีตสหภาพโซเวียต รัสเซียและเอสโตเนียเป็นปัญหาที่ยังไม่จบสิ้น เอสโตเนียเป็นประเทศแรกที่สามารถปลดแอกตัวเองออกจากการเป็นอาณานิคมแต่ยังถูกกดดันให้เข้าเป็นส่วนหนึ่งของสหภาพโซเวียตตลอดมา เอสโตเนีย พยายามหาทางลบล้างสัญลักษณ์ที่บ่งบอกถึงการถูกบีบเป็นส่วนหนึ่งของโซเวียต ในขณะที่รัสเซียพยายามที่จะบีบบังคับจึงทำให้เกิดความขัดแย้งกันอย่างรุนแรง ภายหลังความขัดแย้งขยายเขตแดนไปสู่พื้นที่ไซเบอร์ เอสโตเนียโดนโจมตีด้วยคำสั่ง Distribute Denial of Service-DDOS ทำให้ประเทศตกอยู่ท่ามกลางความชะงักงันของระบบ ทุกอย่างหยุดนิ่ง ระบบทุกระบบทางไซเบอร์ของเอสโตเนียถูกทำลายดั่งกับการชัทดาวน์คอมพิวเตอร์

เอสโตเนียเป็นประเทศแรกที่เป็นผู้นำด้านระบบคอมพิวเตอร์ของยุโรป ผู้ริเริ่ม E-Government และ การเลือกตั้งผ่านอินเทอร์เน็ต ชาวเอสโตเนียมีความคุ้นเคยกับ Skype มากกว่าการใช้สัญญาณโทรศัพท์ ธุรกรรมทางการเงินทั้งหมดของประเทศถูกใช้ผ่านระบบออนไลน์ และการดำรงชีวิตของประชาชนชาวเอสโตเนียต่างขึ้นอยู่กับระบบอินเทอร์เน็ต ด้วยเหตุผลต่าง ๆ เหล่านี้จึงทำให้ยากต่อการจินตนาการว่าการที่เอสโตเนียจะอยู่โดยปราศจากอินเทอร์เน็ตจะมีสภาพอย่างไร การโจมตีเกิดขึ้นอย่างต่อเนื่องโดยระบบอินเทอร์เน็ตจากทั่วโลกมุ่งโจมตีระบบ อินเทอร์เน็ตเอสโตเนีย ระบบสารสนเทศออนไลน์ของประเทศถูกทำให้ล่มและคนในประเทศไม่สามารถติดต่อสื่อสารซึ่งกันและกันได้

สืนามิของการจู่โจมระบบทำให้เกิดการพัฒนาเป็น Botnet ซึ่งเป็นกลุ่มของอุปกรณ์ที่ติดมัลแวร์และถูกเปลี่ยนเป็น Bot (ย่อมาจาก Robot) และการที่มี Botnet หลาย ๆ ตัวจะทำให้เกิดเป็นอาวุธทำลายระบบเครือข่ายของตน ในช่วงเวลาไม่กี่วัน Botnet โจมตีธนาคาร การออกกาศสัญญาณโทรทัศน์ ตำรวจ และรัฐบาลแห่งชาติ เครือข่ายของระบบรัฐสภาและกระทรวงต่าง ๆ ถูกรบกวนโดย Botnet สายด่วนโทรแจ้งเหตุแห่งชาติถูกบล็อคไม่ให้สามารถติดต่อได้ การตั้งรับของประเทศเอสโตเนียไม่สามารถตอบสนองได้อย่างร้อยเปอร์เซ็น จุดมุ่งหมายในการโจมตีประเทศเอสโตเนียครั้งนี้คือการทำให้ทั้งประเทศถูกตัดขาดจากโลกภายนอก และการขอความช่วยเหลือจากประเทศต่าง ๆ ก็ดูจะเหมือนเป็นไปได้ยากเมื่อเอสโตเนียกำลังโดนกลบลงดิน

ในความโชคร้ายยังคงมีความโชคดี เอสโตเนียมีพันธมิตรกับบริษัทอินเทอร์เน็ตอิสระสัญชาติสวีเดนซึ่งเป็นบริษัทที่ให้บริการผ่าน i.root-servers.net ผู้ซึ่งเป็นส่วนหนึ่งของการควบคุมระบบอินเทอร์เน็ตในระดับโลกบริษัท Netnod ยังคงสามารถให้สัญญาณเครือข่ายได้บางส่วน ผู้บริหารสูงสุดของบริษัท Netnod ร่วมเข้าหารือกับผู้นำของประเทศเอสโตเนียเพื่อช่วยเหลือ

เหตุการณ์เบื้องต้น การช่วยเหลือของบริษัท Netnod ทำให้เกิดการชักจูงบริษัทผู้ให้สัญญาติอินเทอร์เน็ตทั่วโลกช่วยกันหยุดการโจมตีจากผู้ก่อการร้าย

รัสเซียปฏิเสธทุกข้อกล่าวหาที่เกี่ยวข้องกับการอยู่เบื้องหลังการโจมตีในครั้งนี้ แต่รัฐมนตรีว่าการกระทรวงการต่างประเทศของเอสโตเนีย Urmas Paet ประณามการกระทำครั้งนี้ว่าทำให้สหภาพยุโรปตกอยู่สถานการณ์ลำบากเพราะรัสเซียโจมตีเอสโตเนีย รัสเซียตอบโต้ข้อกล่าวหาดังกล่าวโดยการคว่ำบาตรเอสโตเนียทั้งในด้านเศรษฐกิจและการทูต รัสเซียยกเลิกการเดินทางและการขนส่งวัตถุดิบทางรถไฟจากกรุงมอสโกไปกรุงทาลินเมืองหลวงประเทศเอสโตเนีย สงครามเวปครั้งแรก (Web War I) (O'Neill, 2020) สร้างความตึงเครียดกับรัสเซียและประเทศข้างเคียง งบประมาณทางการทหารเพิ่มมากขึ้น เอสโตเนียเป็นประเทศสมาชิกของ the North Atlantic Treaty Organization หรือองค์กร NATO พันธมิตรทางทหารที่ยิ่งใหญ่ที่สุดในโลก การท้าทายโดยการจู่โจมในครั้งนี้เปรียบได้เหมือนการทดสอบศักยภาพทางทหารขององค์กร NATO ในการรับมือภับคุกคามไซเบอร์

เอสโตเนียเปรียบเทียบการจู่โจมครั้งนี้เหมือนการกระทำของผู้ก่อการร้ายที่กระตุ้นถึงศักยภาพในการตั้งรับภัยคุกคามไซเบอร์ขององค์กร NATO และผลของการจู่โจมทำให้เห็นว่าประเทศสมาชิกยังไม่มีความพร้อมในการรับมือกับภัยคุกคามประเภทนี้เพราะยังไม่เคยเกิดขึ้นมาก่อน ยังไม่มีตำราที่กล่าวถึงคู่มือในการตอบโต้ แม้กระทั่งการเตรียมพร้อมระดับยุทธศาสตร์และกลยุทธ์ทางเทคนิค ภัยคุกคามที่เกิดขึ้นยังอยู่ในเขตแดนความคลุมเครือว่าจะสามารถเรียกการกระทำเหล่านี้ว่า “สงคราม” ได้หรือไม่ องค์กร NATO ได้รับผลกระทบจากการโจมตีของ Botnet อย่างจริงจังเพราะเครือข่ายไซเบอร์ของเอสโตเนียนั้นเป็นส่วนหนึ่งของเครือข่าย NATO หนึ่งปีหลังเหตุการณ์นี้ทำให้องค์กร NATO ตั้งหน่วยงานเฉพาะเพื่อรับมือกับภัยคุกคามทางไซเบอร์ในเมืองหลวงของประเทศเอสโตเนีย

โดยสรุปแล้วการโจมตีโครงสร้างเครือข่ายของเอสโตเนียนั้นถูกตระหนักว่าเป็นการโจมตีทางไซเบอร์ครั้งแรกที่รุนแรงและมีความชัดเจนมากกว่า The Original Logic Bomb ที่ยังอยู่ในความคลุมเครือและยังไม่สามารถสรุปสาเหตุได้ แต่การโจมตีประเทศเอสโตเนียในครั้งนี้ยังคงเป็นแค่จุดเริ่มต้นเพราะยังมีการโจมตีอีกมากมายในช่วงที่ผ่านมาสามารถเรียกได้ว่าโฉมหน้าของความรุนแรงจากภัยคุกคามไซเบอร์เป็นอย่างไร

2.7.5 Stuxnet 2010

ขบวนการเคลื่อนไหวในสังคมในปลายศตวรรษที่ 20 แนวความคิดสมัยใหม่ได้ฝังรากลึกเกี่ยวกับแนวคิดของยุคสมัยแห่งความอิสระในสังคมออนไลน์ ในขณะนี้ผู้คนกำลังอาศัยอยู่ในโลก

ของคอมพิวเตอร์ที่เสมือนจริง การก่อการร้ายทางไซเบอร์มีอิทธิพลอย่างสูงในการสร้างความโกลาหลให้กับรัฐสมัยใหม่ ที่จะทวีความรุนแรงและก่อความสับสนวุ่นวายมากยิ่งขึ้น (Kushner, 2013) หากเทียบกับการก่อการร้ายแบบดั้งเดิมที่เกิดในโลกกายภาพ การก่อการร้ายจะมีลักษณะเชิงเดี่ยว (Single) เกิดขึ้นที่ใดจะส่งผลกระทบ ณ ที่นั่นเพียงแห่งเดียว ตรงกันข้ามกับการก่อการร้ายในพื้นที่ไซเบอร์ที่ไม่ได้ถูกจำกัดในเรื่องของเขตแดนหรือภูมิศาสตร์ใด ๆ และด้วยเหตุผลดังกล่าวนั้นจึงส่งผลให้การก่อการร้ายที่เกิดขึ้น ณ ที่หนึ่งจะส่งผลกระทบได้อีกในหลาย ๆ ที่ตามเครือข่ายอินเทอร์เน็ตที่เชื่อมต่อ เท่าที่ผู้ก่อการร้ายต้องการ

ไวรัสคอมพิวเตอร์ที่ถูกใช้เป็นเครื่องมือของผู้ใช้คอมพิวเตอร์ในทุก ๆ ระดับ ตั้งแต่ประชาชนทั่วไป ไปจนถึงแฮกเกอร์ผู้ชำนาญการ ผลกระทบของไวรัสเกิดขึ้นได้ตั้งแต่การสร้างความรำคาญ ก่อกวนระบบไปจนถึงการทำลายข้อมูลทั้งระบบ แต่อย่างไรก็ตามไวรัสคอมพิวเตอร์ส่วนบุคคลจะไม่ก่อให้เกิดความเสียหายเชิงกายภาพ จนกระทั่งการเกิดขึ้นของ Stuxnet

Stuxnet เป็นโปรแกรมมุ่งร้ายที่มาในรูปแบบของการโจมตีที่ก่อให้เกิดผลกระทบเชิงกายภาพ ทำลาย hardware ที่เชื่อมต่อกับระบบ ไวรัสตัวนี้ถูกคิดค้นเมื่อเดือน มิถุนายน ปี 2010 มีวัตถุประสงค์ในการทำลาย จู่โจมระบบการควบคุมอุตสาหกรรม Programmable logic controller (PLC) ที่ควบคุมโรงงานยูเรเนียมซึ่งเป็นแหล่งผลิตนิวเคลียร์ของอิหร่าน การจู่โจมจะเริ่มจากการบิดเบือน Software Code ของโรงงานทำให้การหมุนของเครื่องแยกวัตถุมีระดับแรงขึ้นจนทำให้เกิดการแยกกันของชิ้นส่วน (Kushner, 2013) Stuxnet เป็นไวรัสตัวแรกที่ทำให้โลกรู้ว่าไซเบอร์สามารถทำไปใช้เป็นอาวุธในการทำลายล้างเชิงกายภาพได้

จากที่กล่าวมาข้างต้นนั้น เห็นได้ชัดเจนว่าไวรัสสามารถสร้างความกลัวอย่างมากมายมหาศาลให้กับมนุษย์ การสื่อสารของประชาชนที่ใช้อินเทอร์เน็ตสามารถส่งต่อไวรัสได้อย่างรวดเร็ว ตัวอย่างเช่น ไวรัส Good Times ที่เป็นไวรัสหลอกลวงและแพร่กระจายได้ไปทั่วโลกได้อย่างรวดเร็ว การใช้ไวรัสไม่จำเป็นต้องมีทักษะด้านคอมพิวเตอร์ระดับสูง การสร้างไวรัสจะไม่มีขอบเขตเป้าหมายที่แน่นอน แต่จะเป็นการสุ่มเลือกเป้าหมายจะกระทั่งแพร่กระจายไปในสื่อออนไลน์ สู่โลกแห่งความจริง

การก่อการร้ายจะใช้วิธีในการสื่อสารโดยเฉพาะการถ่ายทอดผ่านข้อความสร้างอุดมการณ์ไปยังคนหมู่มากในขณะเดียวกันเป็นการสร้างความกลัวแพร่ผ่านในเวปไซต์ และสื่อสังคมออนไลน์ต่าง ๆ วิธีการก่อการร้ายแบบนี้ไม่จำเป็นที่จะต้องอาศัยการทำลายเชิงกายภาพตราบใดที่ความกลัวนั้นยังฝังลึกลงไปในเป้าหมาย

ความกังวลที่เคยเกิดขึ้นในอดีตกำลังจะเกิดขึ้นจริงในปัจจุบัน การโจมตีเพียงแค่การกดปุ่มแต่สามารถที่จะทำลายล้างทั้งโลกได้ การผสมผสานของศาสตร์ทางวิทยาศาสตร์คอมพิวเตอร์

และศาสตร์ทางสังคมในเรื่องของการใช้กลยุทธ์เพื่อบรรลุเป้าหมายเป็นเรื่องละเอียดอ่อน แต่หากกระทำสำเร็จผลกระทบที่ตามมาอาจจะสร้างความเสียหายที่ไม่อาจประเมินค่าได้

2.7.6 ประเภทของการโจมตีไซเบอร์

การโจมตีทางไซเบอร์มีหลายรูปแบบแต่ไม่มีรูปแบบใดที่เหมือนกัน การเลือกใช้ประเภทของการโจมตีขึ้นอยู่กับเหยื่อและสถานการณ์ อาชญากรรมไซเบอร์ การก่อการร้ายไซเบอร์ และสงครามไซเบอร์ ถึงแม้จะอยู่ในขอบเขตความเป็นไซเบอร์แต่ก็มีความแตกต่างกันในการใช้กลยุทธ์ในการโจมตี เมื่อผู้วิจัยต้องศึกษาการก่อการร้ายไซเบอร์ รูปแบบการโจมตีที่ถูกนำมาใช้มากที่สุดสามารถแบ่งได้ 6 ประเภท ดังนี้

2.7.6.1 Malware

Malware มัลแวร์ คือ โปรแกรมชนิดหนึ่งที่ถูกสร้างขึ้นมาเพื่อประสงค์ร้ายต่อคอมพิวเตอร์ ซึ่งปัจจุบัน Malware ยังถูกแบ่งประเภทออกมาอีกมากมายตามลักษณะพิเศษ (Paul, 2012) เช่น

1) Bot คือ ซอฟต์แวร์ชนิดหนึ่งที่สามารถทำงานได้แบบอัตโนมัติ โดย Bot ในที่นี้คือชนิด เดียวกับ Botnets ที่ทำลายเครือข่ายของประเทศเอสโตเนีย ผู้ก่อการร้ายใช้ Bot เพื่อการโจมตีแบบ DDoS ทำให้ระบบถูกรบกวนและไม่สามารถทำงานได้

2) Ransomware คือ มัลแวร์ที่จะทำให้การเข้ารหัสไฟล์ไม่สามารถใช้งานได้ และหากว่าผู้ใช้ต้องการจะใช้งานไฟล์นั้นได้อีกครั้ง จำเป็นต้องจ่ายเงินค่าไถ่ให้กับแฮกเกอร์หรือผู้ก่อการร้ายเพื่อถอดรหัสไฟล์เหล่านั้น คล้ายกับการเรียกค่าไถ่แบบดั้งเดิม

3) Virus คือ มัลแวร์ชนิดหนึ่งที่สามารถสำเนาตัวเองกระจายไปยังเครื่องอื่น ๆ หรือเข้าไปติดอยู่ในเครื่องคอมพิวเตอร์ โดยผ่าน ไฟล์ประเภทต่าง ๆ หรือการนำเอาแผ่นดิสก์หรือแฟลชไดร์ฟที่ติดไวรัสจากเครื่องหนึ่งไปใช้กับอีกเครื่องหนึ่ง เมื่อติดไวรัสแล้วจะส่งผลให้การทำงานของเครื่องคอมพิวเตอร์ช้าลง คอมพิวเตอร์อาจถูกขโมยข้อมูล หรือหยุดทำงานตลอดเวลา

4) Worm เป็นมัลแวร์ที่ถูกใช้บ่อยที่สุด มัลแวร์ทำงานด้วยวิธีการแพร่กระจายผ่านระบบเน็ตเวิร์ค ผ่านทางช่องโหว่ของระบบปฏิบัติการ เพื่อสร้างความเสียหาย ลบไฟล์ หรือขโมยข้อมูล หนอนคอมพิวเตอร์ชนิดนี้ใช้วิธีแพร่กระจายผ่านการส่งอีเมล์แนบไฟล์ที่มีมัลแวร์หรือหนอนคอมพิวเตอร์อยู่ไปยังคอมพิวเตอร์ที่ถูกติดตั้งโดยมัลแวร์

5) Trojan Horse มัลแวร์ม้าเมืองทรอย ที่ใช้กลยุทธ์เดียวกับม้าไม้ที่ถูกส่งเข้าไปยังเมืองทรอย โดยเพื่อเข้าไปควบคุม ทำลาย หรือขโมยข้อมูลจากระบบ มัลแวร์ตัวนี้แกล้งทำเป็นโปรแกรมปกติ เพื่อหลอกให้ผู้ใช้ดาวน์โหลดมาใช้งาน ภายหลังการใช้งานหรือติดตั้งแล้วจะเปิด

ช่องโหว่ระบบถูกควมคุมหรือขโมยข้อมูลแบบไม่ทันตั้งตัว Trojan Horse ถูกอ้างว่าใช้ใน The Original Logic Bomb ที่รัสเซียลักลอบเข้าระบบของสหรัฐและได้รับมัลแวร์ตัวนี้มาทำให้ระบบการขนส่งท่อก๊าซไซบีเรียระเบิด

6) Bug เป็นมัลแวร์ที่เกิดจากการที่โปรแกรมเมอร์วางระบบความผิดพลาด หรือบางครั้งเกิดจากความผิดพลาดของผู้ใช้งาน จนเป็นช่องโหว่ให้แฮกเกอร์หรือผู้ก่อการร้ายเข้าไปโจมตีระบบได้

7) Spyware มัลแวร์สายลับที่ทำหน้าที่เก็บข้อมูลการใช้งานต่าง ๆ ของเครื่องที่ถูกติดตั้ง และส่งไปยังแฮกเกอร์หรือผู้ก่อการร้าย มัลแวร์ชนิดนี้ยังสามารถเก็บข้อมูลจากคีย์บอร์ดที่ผู้ใช้พิมพ์ พร้อมกับบันทึกหน้าจอพร้อมกันโดยไม่รู้ตัว

นักวิชาการเชื่อว่า Malware เป็นรูปแบบภัยคุกคามยุคบุกเบิก เป็นซอฟแวร์ที่อันตรายกับผู้ที่ได้รับ หากมี Malware อยู่ในเครื่องจะสามารถสร้างความเสียหายได้ ไม่ว่าจะเป็นการขโมยข้อมูล การควนคุมระบบข้อมูล การระบาดของไวรัส WAnnaCry ที่สร้างความเสียหายให้กับสหรัฐอเมริกา อังกฤษ จีน รัสเซีย อิตาลี หรือการใช้ Ransomware เรียกค่าไถ่จากโรงพยาบาลสระบุรี มีการระบุว่าการถูกโจมตีด้วย Malware มีมากกว่า 75,000 ครั้ง ทั่วโลก การทำงานของ Malware ส่วนมากจะเป็นการแฝงตัวเข้ามาในระบบเพื่อให้ผู้ใช้ได้ติดตั้งซอฟแวร์ที่ผิดปกติตัวนี้ แม้กระทั่งการดาวน์โหลดไฟล์ Word และ PDF ยังเป็นสามารถให้เกิดการแอบแฝงของของ Malware ได้อย่างง่ายดาย (Monster Connect, 2009) Malware สามารถแบ่งประเภทโดยละเอียดได้ ดังนี้

2.7.6.2 Phishing

โดยทั่วไปผู้ใช้งานในไซเบอร์จะมีความตระหนักถึงภัยคุกคาม โดยที่พวกเขาจะไม่เปิดไฟล์หรือดาวน์โหลดไฟล์ที่ไม่รู้จักหรือมีความเสี่ยงต่อคอมพิวเตอร์ ด้วยเหตุนี้เทคนิค Phishing จึงถูกคิดค้นเพื่อเป็นเทคนิคจูงใจให้ผู้ใช้ระบบเปิดไฟล์ที่มีความเสี่ยง และเมื่อผู้ใช้เชื่อและเปิดไฟล์เหล่านั้น “มัลแวร์” จะถูกติดตั้งและพร้อมโจมตีคอมพิวเตอร์ทันที เทคนิคที่น่าสนใจของ Phishing คือการปลอมแปลงส่งอีเมล์จากคนที่รู้จักหรือคนที่ผู้ใช้งานเชื่อถือพร้อมแนบไฟล์แฝงที่เป็นมัลแวร์อันตราย เช่น การส่งอีเมล์แจ้งขอเปลี่ยนรหัสใหม่พร้อมให้กรอกข้อมูลส่วนตัว โดยเป็นกับดักให้ผู้ใช้ขาดความตระหนักคิดและกรอกข้อมูลเหล่านั้นโดยไม่รู้ตัว

2.7.6.3 Denial of Service (DoS)

การโจมตีแบบ Denial of Service (DoS) สามารถเปรียบเปรยกับทางด่วนแห่งหนึ่งที่มีการกำหนดขนาดและจำนวนยานพาหนะที่ใช้วิ่งบนทางด่วนแห่งนี้ แต่เมื่อจำนวนยานพาหนะที่มีเกิดมากกว่าจะนวนที่กำหนดไว้ จะทำให้ทางด่วนแห่งนั้นไม่สามารถใช้การได้ ด้วยวิธีเดียวกันนี้ Denial of Service (DoS) เป็นวิธีที่ระดมกันเข้าเวปไซร์มากเกินไปจนทำให้เวปไซต์ไม่

สามารถใช้การได้ หรือบางครั้งภัยคุกคามจาก Denial of Service (DoS) เป็นผลจากความผิดปกติของเซิร์ฟเวอร์ ภัยในรูปแบบของ Denial of Service (DoS) เคยเกิดขึ้นที่ประเทศไทย ในครั้งนั้นมีการโจมตีโดยการกด F5 ถล่มเวปไซต์กระทรวง ICT เพื่อเป็นสัญลักษณ์ต่อต้าน Single Gateway หรือเหตุการณ์โจมตีเครือข่ายของเอสโตเนียที่ใช้ Botnets ดำเนินการโจมตีแบบ Denial of Service (DoS) โดย Botnets นั้นสามารถส่งข้อมูลจำนวนมากไปยังเซิร์ฟเวอร์ของศัตรูและเป็นผลให้เซิร์ฟเวอร์ไม่สามารถใช้การได้ในที่สุด (CISA, 2009)

2.7.6.4 SQL Injection Attack

ภาษาของโปรแกรมที่เขียนเพื่อสื่อสารกับฐานข้อมูลภายในเซิร์ฟเวอร์ โดยเมื่อเกิดการโจมตีภาษาของโปรแกรมชนิดนี้จะสื่อสารโดยตรงกับเซิร์ฟเวอร์และจะส่งผลกระทบนั้นถึงเซิร์ฟเวอร์หรือเวปไซต์โดยตรง ภัยคุกคามรูปแบบนี้เป็นที่น่ากังวลต่อองค์กรใหญ่ เพราะภายในเซิร์ฟเวอร์ขององค์กรจะมีข้อมูลมากมายที่สำคัญ และเมื่อข้อมูลสำคัญถูกจู่โจม SQL จะสามารถสร้างความเสียหายในระยะยาว

2.7.6.5 Cross-Site Scripting (XSS)

การโจมตีแบบ Cross-Site Scripting (XSS) ใช้วิธีเดียวกันกับ SQL แต่จะแตกต่างกันที่เป้าหมาย โดย Cross-Site Scripting (XSS) จะมุ่งเป้าไปที่ผู้ใช้เวปไซต์ แต่ไม่สร้างความเสียหายให้กับเวปไซต์ที่เป็นช่องทางเชื่อมต่อ วิธีการโจมตีจะมาในรูปแบบของ Code แอบแฝงที่มีอยู่หน้าเวปไซต์เพื่อให้ผู้ใช้กด วิธีการแบบ XSS จะสามารถลดทอนความน่าเชื่อถือของเวปไซต์เหล่านั้นเมื่อผู้เข้าใช้ถูกโจมตีด้วยไวรัสนี้ (Dandecha, 2019)

2.7.6.6 Session Hijacking และ MitM

คือการโจมตีแบบแทรกกลางโดยมีแฮกเกอร์ผู้ไม่หวังดีเข้ามาแอบสังเกตการณ์สนทนาและเป็นผู้รับส่งข้อมูลในการสนทนา เรียกดูเครือข่าย IP และพาสเวิร์ดโดยที่ผู้สนทนาไม่รู้ตัว แฮกเกอร์นั้นสามารถใช้การจับรหัสและเปลี่ยนแปลง บิดเบือนข้อมูลเป็นอย่างอื่น เพื่อสร้างความเข้าใจผิดต่อคู่สนทนาได้ การโจมตีแบบนี้สร้างความเสียหายเป็นอย่างมากหากข้อมูลข้อผู้สนทนานั้นเป็นความลับหรือเป็นผลสำคัญต่อการเปลี่ยนแปลงในระดับประเทศ ในการป้องกันไม่ให้เกิดการแทรกกลาง จำเป็นจะต้องสร้างมาตราการความปลอดภัยระหว่างการแลกเปลี่ยนข้อมูลต้นฉบับให้เป็นข้อมูลที่ถูกเข้ารหัสเพื่อไม่ให้เกิดการโจมตีดักจับและเปลี่ยนแปลงข้อมูล

2.8 สถานการณ์การก่อการร้ายไซเบอร์ในต่างประเทศ (Assessing the Risks of Cyber Terrorism in Global Context)

2.8.1 การดำเนินการเรื่องการต่อต้านการก่อการร้ายไซเบอร์ในกรอบสหประชาชาติ

เลขาธิการคณะทำงานดำเนินการต่อต้านการก่อการร้าย คณะทำงานว่าด้วยการต่อต้านการใช้อินเทอร์เน็ตเพื่อการก่อการร้าย (Secretary-General's Counter-Terrorism Implementation Task Force The Working Group on Countering the Use of the Internet for Terrorist Purposes of the Counter-Terrorism Implementation Task Force) มีวัตถุประสงค์เพื่อประสานงานให้กับสหประชาชาติเพื่อสนับสนุนให้ประเทศทั่วโลกมียุทธศาสตร์การต่อต้านการก่อการร้ายไซเบอร์ที่มีประสิทธิภาพซึ่งได้รับการรับรองจากสมัชชาใหญ่แห่งสหประชาชาติในมติ 60/288 โดยประเทศสมาชิกมีมติให้"ทุกประเทศประสานความร่วมมือในระดับนานาชาติและระดับภูมิภาคเพื่อต่อต้านการก่อการร้ายในทุกรูปแบบโดยเฉพาะการใช้อินเทอร์เน็ตเป็นเครื่องมือสำหรับต่อต้านการแพร่กระจายของการก่อการร้าย โดยภาครัฐอาจต้องการความช่วยเหลือในเรื่องนี้" (UnITed naTIons CoUnTer-TerrorIsm ImplemenTaTIon Task ForCe, 2019)

คณะทำงานฯ ได้ระบุประเด็นสำคัญสำหรับการอภิปราย ซึ่งเป็นประเด็นทางกฎหมาย ปัญหาทางเทคนิคและการใช้อินเตอร์เน็ตระหว่างประเทศได้อย่างมีประสิทธิภาพมากขึ้นเพื่อต่อต้านการก่อการร้าย โดยเฉพาะอย่างยิ่งการบังคับใช้ของกฎหมายของประเทศสมาชิกให้เข้มงวด และตรวจแสดงให้เห็นว่าความผิดฐานการใช้อินเทอร์เน็ตเป็นเครื่องมือในการก่อการร้าย ควรจะมีโทษสูงสุดเพื่อให้เห็นตัวอย่างแก่ผู้กระทำความผิด

ในขณะเดียวกัน สำนักงานต่อต้านการก่อการร้ายแห่งสหประชาชาติ (UNOCT) ก็มีบทบาทในการริเริ่มการใช้เทคโนโลยีใหม่ ใช้โซเชียลมีเดียเพื่อรวบรวมข้อมูล Open Source และหลักฐานดิจิทัลเพื่อต่อต้านการก่อการร้ายที่มาจากความคลั่งไคล้รุนแรง โดยเฉพาะอย่างยิ่งโครงการความปลอดภัยทางไซเบอร์ที่มีจุดมุ่งหมายเพื่อเพิ่มขีดความสามารถของประเทศสมาชิกและองค์กรเอกชนในการป้องกันการโจมตีทางไซเบอร์ที่มุ่งโครงสร้างพื้นฐานที่สำคัญ

ตารางที่ 3 การเปรียบเทียบการเตรียมความพร้อมรับมือภัยคุกคามไซเบอร์ของแต่ละประเทศ

ข้อปฏิบัติ	Singapore	North Korea	South Asia	US	UK	Iran	Russia
ความตระหนักรู้และการอบรม	/	/	/	/	/	/	/

ความต่อเนื่องของแผนยุทธศาสตร์	/	-	/	/	-	/	/
ความปลอดภัยของข้อมูล	/	/	-	-	/	-	/
ระบบปฏิบัติการต่อต้านการก่อการร้ายไซเบอร์	/	-	/	/	/	/	/
การบูรณาการข้อมูลระหว่างหน่วยงาน	/	/	-	/	/	-	/
การบริหารจัดการวิกฤติ	/	/	/	/	/	-	/
การส่งเสริมความร่วมมือกับกันระหว่างประเทศ	/	/	/	/	/	-	-
การบังคับใช้กฎหมายไซเบอร์	/	/	/	/	/	/	/

ที่มา: ThaiCERT (2018)

2.8.2 การก่อการร้ายไซเบอร์ประเทศสิงคโปร์

ประเทศสิงคโปร์มีนโยบายอย่างเป็นทางการในการต่อต้านการก่อการร้ายทางไซเบอร์ตั้งแต่ในปี 2018 ชื่อว่า National Cyber Security Master Plan 2018 เป็นทิศทางที่ใช้แนะนำภาครัฐ ภาคเอกชน ภาคประชาชนในการรับมือกับภัยคุกคามไซเบอร์ สิงคโปร์บังคับใช้กฎหมายการใช้คอมพิวเตอร์ในทางที่ผิดและความมั่นคงปลอดภัยทางคอมพิวเตอร์ ปี 2017 (Computer Misuse and Cyber Security Act 2017) (อินโดแปซิฟิก ดีเฟนส์, 2560) พระราชบัญญัตินี้ให้ผู้มีอำนาจเป็นคนกำหนดมาตรฐานในการป้องกัน จัดการดูแล ควบคุม และตอบโต้กับภัยคุกคามทางไซเบอร์ พระราชบัญญัตินี้นำไปใช้กับการปกป้องข้อมูลสาธารณูปโภคสำคัญต่าง ๆ ของประเทศและเรื่องปกป้องข้อมูลส่วนบุคคลที่เริ่มบังคับใช้ตั้งแต่ปี 2012

ในปี 2019 สิงคโปร์วางแผนที่จะเพิ่มการป้องกันการโจมตีทางไซเบอร์ในขณะนี้เนื่องจากการรั่วไหลของข้อมูล สิงคโปร์วางแผนที่จะก่อตั้งองค์กรการป้องกันทางไซเบอร์เพื่อเสริมสร้างการป้องกันการโจมตีทางออนไลน์โดยรัฐมนตรีว่าการกระทรวงกลาโหมสิงคโปร์ได้ให้เป้าหมายของการก่อตั้งครั้งนี้ว่าเป็นการก่อตั้งกองกำลังการป้องกันทางไซเบอร์จำนวน 2,600 คน ซึ่งเป็นการเพิ่มขึ้นอย่างมากจากระดับปัจจุบัน เพื่อทำการป้องกันการโจมตีทางไซเบอร์ตลอด 24 ชั่วโมง นักรบไซเบอร์ของสิงคโปร์จะต้องมีทักษะในระดับสูงเนื่องจากความถี่และความซับซ้อนของการโจมตีทางไซเบอร์ที่เพิ่มสูงขึ้นและจะต้องผ่านการคัดสรรและต้องรับผิดชอบอย่างสูง เมื่อเทียบกับนักรบหน่วยอื่น ขณะนี้องค์กรการป้องกันทางไซเบอร์ของสิงคโปร์ประกอบด้วย 4 กลุ่ม ได้แก่ กองความมั่นคงทางไซเบอร์ซึ่งเป็นหน่วยตอบสนองการปฏิบัติการ กรมนโยบายและแผนงาน กรมตรวจการความมั่นคงทางไซเบอร์เพื่อประเมินความเสี่ยง และกลุ่มการป้องกันทางไซเบอร์

2.8.2.1 ยุทธศาสตร์การป้องกันภัยคุกคามไซเบอร์ของประเทศสิงคโปร์

สิงคโปร์สามารถตามยุทธวิธีและปฏิบัติการของผู้รุกรานในโลกไซเบอร์ได้อย่างเท่าทัน มีการศึกษาตามทฤษฎีในรูปแบบของการทำสงครามและการก่อการร้าย นอกจากนี้สิงคโปร์ยังวางแผนที่จะเพิ่มการฝึกอบรมในสาขาการป้องกันทางไซเบอร์เพื่อป้อนบุคลากรให้กับองค์กร นักรบไซเบอร์รุ่นใหม่ของสิงคโปร์จะประกอบด้วยทหารจากกองทัพแห่งชาติและผู้ที่พิจารณาแล้วว่าพร้อมสำหรับการทำงานหลังผ่านกระบวนการคัดสรรซึ่งรวมถึงการแข่งขัน การทดสอบ และแม้แต่การเข้าค่ายไซเบอร์ นักรบไซเบอร์รุ่นใหม่ของกองทัพสิงคโปร์จะตรวจสอบเครือข่ายและระบบตอบสนองต่อเหตุการณ์ต่าง ๆ ที่เกิดขึ้น ดำเนินการวิเคราะห์ด้านนิติวิทยาศาสตร์ และปกป้องโครงสร้างพื้นฐานของข้อมูลที่สนับสนุนเครือข่ายที่สำคัญของสิงคโปร์ เนื่องจากสิงคโปร์ตระหนักแล้วว่าภัยไซเบอร์เป็นภัยที่ใกล้ตัว การที่แฮกเกอร์สามารถจู่โจมระบบการเข้าถึงอินเทอร์เน็ตของกองทัพสิงคโปร์ได้ มาจากการโจมตีที่มีเป้าหมายและได้รับการวางแผนเป็นอย่างดี ดังนั้นเพื่อไม่ให้เกิด

เหตุการณ์เช่นนี้ขึ้น สิงคโปร์จึงมีแนวทางการป้องกันภัยคุกคามทางไซเบอร์ตามยุทธศาสตร์หลักในการรับมือ4 ข้อ (CSA, 2016) ดังนี้

1) กลยุทธ์ในการฟื้นตัวสาธารณูปโภคที่สำคัญของประเทศ

(1) สร้างระบบป้องกันให้กับบริการสำคัญต่าง ๆ

(2) เพิ่มความสามารถที่จะตอบโต้ภัยคุกคามที่จะเกิดขึ้นอย่างแม่นยำ

(3) สร้างความเข้มแข็งให้กับระบบรักษาความปลอดภัยไซเบอร์ในอยู่ในธรรมาภิบาลและกรอบของกฎหมาย

(4) สร้างระบบความปลอดภัยให้กับรัฐบาลโดยการสร้างความสามารถในการตรวจจับไวรัสแปลกปลอม

2) สร้างความปลอดภัยในพื้นที่ไซเบอร์

(1) ตอบโต้กับภัยคุกคามทางไซเบอร์โดยแผน National Cybercrime Action Plan (NCAP)

(2) สร้างความมั่นใจให้กับองค์กรการต่อต้านภัยคุกคามทางไซเบอร์ของสิงคโปร์ด้วยการแสดงให้เห็นถึง Data Protection Trust marks

(3) ส่งเสริมให้มีการรายงานข้อมูลที่เป็นประโยชน์ต่อการป้องกันภัยคุกคามอยู่ตลอดเวลา

3) พัฒนาความมั่นคงปลอดภัยของนิเวศวิทยาทางไซเบอร์

(1) จูงใจให้ผู้เชี่ยวชาญทางไซเบอร์เข้ามาเป็นส่วนหนึ่งของการทำงานกับรัฐบาล เช่น เปิดสถาบันการสอน เปิดหลักสูตรที่น่าสนใจพร้อมกับการให้ใบประกาศนียบัตรเมื่อจบหลักสูตร

(2) สนับสนุนธุรกิจ Start Up ที่จะสามารถพัฒนาให้เป็นเครือข่ายป้องกันไซเบอร์ได้ในอนาคต

(3) เป็นพันธมิตรกับบริษัทท้องถิ่น (Local Company) ที่มีความรู้ด้านไซเบอร์และสามารถแก้ไขสถานการณ์สำคัญได้ในอนาคต

4) เพิ่มความเข้มแข็งให้กับพันธมิตรต่างชาติในการป้องกันภัยคุกคามจากไซเบอร์

(1) รวมกลุ่มการแก้ปัญหาภัยคุกคามไซเบอร์ภายในกลุ่มประเทศอาเซียนและภาคีต่างชาติอื่น ๆ

(2) สร้างภาวะความเป็นผู้นำทางด้านไซเบอร์ให้กับกลุ่มประเทศเพื่อนบ้าน

(3) แลกเปลี่ยนข้อมูลระหว่างกัน เช่น มีการจัดสัมมนา จัดเวทีแสดงผลงาน สร้างห้อง Lab จำลองเพื่อเป็นแหล่งให้ความรู้กับกลุ่มประเทศเพื่อนบ้าน

(4) แลกเปลี่ยนนวัตกรรมกับประเทศเพื่อนบ้าน กลุ่มประเทศสมาชิกอาเซียน และภาคีต่างชาติอื่น ๆ เพื่อให้มีความสัมพันธ์ระหว่างประเทศที่แข็งแรง และจะเป็นผลดีเมื่อมีภัยคุกคาม ประเทศพันธมิตรจะคอยช่วยสอดส่องดูแล

2.8.2.2 กฎหมายควบคุมไซเบอร์ของประเทศสิงคโปร์

กฎหมายเฉพาะที่ประเทศสิงคโปร์มีเพื่อรับมือกับความผิดทางไซเบอร์คือ กฎหมายการใช้คอมพิวเตอร์ในทางที่มิชอบและความมั่นคงปลอดภัยทางไซเบอร์ ปี 1993 และมีการเพิ่มเติมในปี 2007 และ 2017 โดยมีการกำหนดความผิดไว้ 7 ประเภท (คณาธิป ทองรวีวงศ์, 2563) คือ

1) การเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจ

2) การเข้าถึงด้วยเจตนาหรือสนับสนุนให้เกิดการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

3) การแก้ไขข้อมูลคอมพิวเตอร์โดยปราศจากอำนาจ

4) การใช้หรือดักรับบริการทางคอมพิวเตอร์โดยปราศจากอำนาจ

5) การขัดขวางการใช้คอมพิวเตอร์โดยปราศจากอำนาจ

6) การเปิดเผยรหัสสำหรับการเข้าถึงโดยปราศจากอำนาจ

7) การได้มา เก็บรักษาไว้ จัดหาให้ เสนอจัดหาให้ ส่งต่อ หรือทำให้ปรากฏโดยวิธีใด ๆ ซึ่งข้อมูลดังกล่าวจากการกระทำอันเป็นความผิดตามกฎหมาย

กฎหมายในประเภทที่ยกตัวอย่างนี้ครอบคลุมถึงการใช้ไซเบอร์เพื่อเป็นอาวุธโจมตีตามรูปแบบของภัยคุกคามที่เกิดขึ้นบ่อยในปัจจุบัน กฎหมายเหล่านี้สามารถเอาผิดกับอาชญากรไซเบอร์ทั่วไปและอาชญากรไซเบอร์ที่มีความเชี่ยวชาญและร่วมกระทำกันเป็นองค์กร

2.8.3 การก่อการร้ายไซเบอร์ของสาธารณรัฐประชาธิปไตยประชาชนเกาหลี

“Cyber warfare, along with nuclear weapons and missiles, is an ‘all-purpose sword’ that guarantees our military’s capability to strike relentlessly.” -Kim Jong-un-- (Tai, 2019)

ประโยคนี้ทำให้ผู้เชี่ยวชาญหลายท่านตั้งคำถามว่าความสามารถในการก่อสงครามไซเบอร์ของเกาหลีเหนือนั้นร้ายแรงเท่ากับความสามารถในการก่อสงครามนิวเคลียร์หรือไม่ เกาหลีเหนือมีท่าทีจะนำเครื่องมือทางไซเบอร์มาเป็นอาวุธในการโจมตีและสามารถแทนที่อาวุธนิวเคลียร์ที่

เกาหลีเหนือครอบครองเพื่อข่มขู่ต่างชาติได้ แต่อย่างไรก็ตาม อาวุธทั้ง 2 ประเภทจะก่อให้เกิดความเสียหายและสร้างความกังวลให้กับนานาประเทศเป็นอย่างมาก

ความแตกต่างประการหนึ่งระหว่างอาวุธนิวเคลียร์และอาวุธไซเบอร์นั้น คือ เกาหลีเหนือไม่สามารถโจมตีด้วยอาวุธนิวเคลียร์ได้ก่อนเพราะจะถูกตราหน้าว่าเป็นผู้ก่อสงคราม ส่งผลต่อภาพลักษณ์ของประเทศและสร้างความไม่พอใจต่อนานาชาติ แต่สำหรับอาวุธทางไซเบอร์นั้นมีวิธีการใช้ที่ง่ายและศัตรูส่วนใหญ่จะไม่รู้ตัว เช่นการใช้การต่อสู้แบบสงครามกองโจร (Guerilla Tactics) ซึ่งเป็นวิธีที่เหมาะกับการใช้ขโมยข้อมูล จู่โจมระบบอิเล็กทรอนิกส์ และระบบทางการเงิน ได้อย่างเงียบ ๆ เริ่มตั้งแต่ในทศวรรษที่ 2010 แฮกเกอร์จากเกาหลีเหนือได้เริ่มจู่โจมระบบบ่อยขึ้น จากหนึ่งครั้งในปี 2015 ไปสู่ 4 ครั้งในปี 2017 และเพิ่มขึ้นทุกปีนับตั้งแต่นั้นเป็นต้นมา เมื่อเดือนตุลาคม 2019 ผู้ต้องสงสัยชาวเกาหลีเหนือกว่า 30 คนถูกตั้งข้อหาว่าเป็นผู้ลอบเข้าระบบเพื่อขโมยข้อมูลเกี่ยวกับอาวุธสงครามที่ใช้ในการรบทางอากาศ ผ่านทางระบบคอมพิวเตอร์ของเกาหลีใต้ สองเดือนถัดมายังพบว่า แฮกเกอร์ชาวเกาหลีเหนือยังได้ขโมยข้อมูลส่วนตัวของชาวเกาหลีใต้กว่า 1,000 คน จาก Refugee Resettlement Centre ที่จะสร้างความเดือดร้อนให้กับครอบครัวและเพื่อนของพวกเขา (Tai, 2019)

พบว่าแรงจูงใจส่วนใหญ่ตั้งแต่แรกเริ่มของ แฮกเกอร์ชาวเกาหลีเหนือ คือเงินและการทำลายล้างระบบความมั่นคงของรัฐบาลประเกาหลีใต้ ถึงแม้ว่าประเทศเกาหลีเหนือนั้นจะเป็นประเทศที่ยากจนและมีข้อจำกัดในเรื่องเทคโนโลยี คนส่วนน้อยในประเทศยังต้องเข้าระบบอินทราเน็ตของประเทศที่ชื่อว่า “Kwangmyong” แต่ความสามารถทางไซเบอร์ของเกาหลีเหนือยังถูกมองว่าซับซ้อนพัฒนาได้อย่างรวดเร็ว (Tai, 2019)

ในยุคสมัยของโซเวียต เกาหลีเหนือยังไม่สามารถที่จะผลิตโทรทัศน์แบบสีได้ แต่พวกเขาสามารถที่จะผลิตอาวุธนิวเคลียร์และคิดค้น พัฒนาการสำรวจทางอากาศ ยิ่งเป็นสิ่งที่เน้นย้ำว่า หากประเทศเผด็จการอย่างเกาหลีเหนือต้องการจะบรรลุวัตถุประสงค์ที่ตนวางไว้ พวกเขาจะตักตวงประโยชน์จากทรัพยากรมนุษย์ จนกว่าจะได้สิ่งนั้นมา เกาหลีเหนือคิดค้นอาวุธทางไซเบอร์ตั้งแต่ปี 1990 และส่งนักเรียนที่อัจฉริยะทางคอมพิวเตอร์ไปเรียนในมหาวิทยาลัยในประเทศจีนที่ติดอันดับ จนทำให้เกาหลีเหนือมีแฮกเกอร์ของกองทัพกว่า 6,000 คน และความสามารถทางไซเบอร์ของพวกเขาเป็นได้ทั้งอาวุธและแหล่งรายได้ของประเทศ

2.8.3.1 ยุทธศาสตร์ทางไซเบอร์ของเกาหลีเหนือ

เป็นที่น่ากังวลว่า ไม่ว่าจะเป็นภาครัฐหรือหน่วยงานความมั่นคงของประเทศต่าง ๆ ยังไม่สามารถที่จะป้องกันภัยทางไซเบอร์จากเกาหลีเหนือได้ โดยมีข้อมูลอ้างว่าแม้แต่ธนาคารที่มีหน่วยป้องกันในระดับสูงยังไม่สามารถต้านทานภัยจากเกาหลีเหนือ อย่างเช่นในกรณีของจู่โจม

ระบบ Sony Pictures Entertainment นั้น FBI ได้ให้ข้อสังเกตว่าแฮกเกอร์ส่วนใหญ่สามารถจู่โจมระบบได้ประสบผลสำเร็จกว่าร้อยละ 90 ถึงแม้การคุกคามในปัจจุบันจะเป็นการจู่โจมที่ไม่ซับซ้อนและผู้โจมตีไม่จำเป็นจะต้องมีทักษะสูง แต่ก็พิสูจน์ให้เห็นว่าการจู่โจมเหล่านี้สามารถทำลายระบบสำคัญต่าง ๆ ของรัฐได้ โดยจะเริ่มจาก การจู่โจมแบบ Denial-of-Service บนเวปไซต์ และเริ่มพัฒนาการโจมตีให้ซับซ้อนและเป็นระบบมากขึ้นในช่วงเวลา 5 ปี และยังไม่มีหน่วยงานใดสามารถยับยั้งและป้องกันเกาหลีเหนือจากสงครามไซเบอร์ได้ เช่นเดียวกับสงครามนิวเคลียร์ (Tai, 2019)

นักวิชาการหลายท่านตั้งคำถามว่าเพราะเหตุใดการจู่โจมทางไซเบอร์ของเกาหลีเหนือถึงไม่ถูกยกระดับให้เป็นการโจมตีในระดับสูง นั่นเป็นเพราะการเจรจาถึงสันติภาพของไซเบอร์นั้นมีความความยากเนื่องจากการโจมตีมีรูปแบบที่หลากหลายและยากที่จะควบคุม มากไปกว่านั้น ยังไม่มีกฎเกณฑ์สากลใด ๆ ที่สามารถควบคุมสงครามไซเบอร์ได้ ปัจจัยสำคัญที่ทำให้ยากต่อการควบคุมสงครามไซเบอร์ที่จะเกิดขึ้นจากเกาหลีเหนือคือการปกครองภายใต้ระบบเผด็จการ ถึงแม้จะสนธิสัญญาการปลดอาวุธกับนานาประเทศ ก็ไม่ได้หมายความว่าเกาหลีหนีจะสามารถปฏิบัติตามกฎได้ทั้งหมดเพราะการคงไว้ซึ่งอาวุธทางไซเบอร์ถือเป็นหลักประกันให้แก่ประเทศ ดังนั้นจึงควรมีการสังเกตพฤติกรรมของแฮกเกอร์เกาหลีเหนืออย่างใกล้ชิด

2.8.3.2 กฎหมายและนโยบายควบคุมไซเบอร์ของประเทศเกาหลีเหนือ

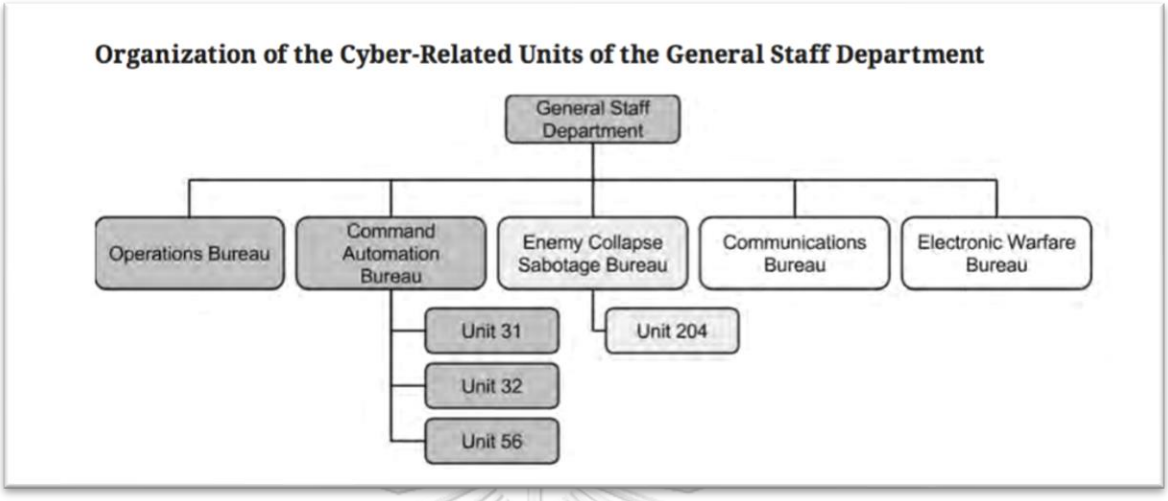
การศึกษานโยบายและการออกกฎหมายของประเทศเกาหลีเหนือเป็นเรื่องที่มีความท้าทายเป็นอย่างมาก เนื่องจากเกาหลีเหนือเป็นประเทศปิด ทำให้นโยบายและกฎหมายภายในประเทศไม่สามารถแพร่หลายในสังคมนานาชาติได้ การศึกษามตราการ นโยบาย ในการควบคุมภัยคุมคามทางไซเบอร์สามารถศึกษาได้จากเอกสารต่างชาติที่ถูกตีพิมพ์เป็นภาษาอังกฤษ ดังนี้

มาตรการในการควบคุมภัยคุกคามทางไซเบอร์ของเกาหลีเหนือส่วนใหญ่จะมุ่งเน้นในการรักษาความปลอดภัยระหว่างประเทศ การกำหนดนโยบายจะเป็นการวางยุทธศาสตร์เชิงรุกในการก่อสงครามไซเบอร์ เกาหลีเหนือตระหนักว่าการใช้ไซเบอร์เป็นเครื่องมือในการโจมตีมีต้นทุนที่ถูกและนำมาซึ่งผลลัพธ์ที่ยิ่งใหญ่ อีกทั้งยังรอดพ้นจากข้อครหาต่าง ๆ จากสังคมโลก นโยบายส่วนใหญ่ที่เกาหลีเกนือใช้ในการโจมตีทางไซเบอร์จะเป็นการจู่โจมระยะสั้น โดยสร้างสถานการณ์ให้มีความเป็นการต่อสู่เชิงอสมมาตร (Asymmetric Attack) โดยที่เกาหลีเหนือจะเป็นฝ่ายได้เปรียบในการโจมตีเสมอ การโจมตีไซเบอร์ของเกาหลีเหนือจะเน้นในเรื่องข้อมูลข่าวสาผ่านช่องทางเครือข่ายคอมพิวเตอร์และการติดต่อสื่อสารของคนผ่านช่องทางอินเทอร์เน็ตในภาพรวมแล้วเกาหลีเหนือจะให้ความระมัดระวังในเรื่องของการเข้าถึงข้อมูลหรือเข้าถึงระบบความมั่นคงของรัฐโดยปราศจากอำนาจการออกกฎหมายควบคุมจึงให้นิยามของการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ได้ชัดเจนในเรื่องของการเข้าถึงข้อมูล ข้อมูลสำคัญในที่นี้ยังคงรวมไปถึงข้อมูลที่ใช้ในระบบโครงสร้างสาธารณูปโภค

พื้นฐานสำคัญของประเทศ ที่จะช่วยให้องค์กรต่าง ๆ ของเกาหลีใต้นำกรอบแนวคิดคำนิยามนี้ไปกำหนดกฎย่อยในการเข้าถึงข้อมูลที่มีความเป็นส่วนตัว ทรัพย์สินทางปัญญา และความอิสระในการแสดงความคิดเห็น ประชาชนในประเทศเกาหลีเหนือไม่สามารถใช้อินเทอร์เน็ตโดยปราศจากตัวตนเพื่อป้องกันไม่ให้เกิดความบิดเบือนทางข้อมูลในโลกไซเบอร์

หน่วยงานหลักที่เป็นผู้กำหนดกฎเกณฑ์ทางไซเบอร์ของเกลหลีเหนือคือ the DPRK's Reconnaissance General bureau (RGB) (정찰총국) หน่วยงานนี้มีบทบาทเป็นศูนย์กลางสำคัญที่จะดำเนินนโยบายต่าง ๆ ทางไซเบอร์ในระดับนานาชาติ ในปี 2009 ถึงปี 2010 RGB พัฒนากองทัพไซเบอร์ของเกาหลีเหนือให้มีจำนวนมากขึ้นเป็นสองเท่า รวมทั้งมีผลงานในการโจมตีทางไซเบอร์ในระดับนานาชาติต่าง ๆ อีกมากมาย RGB ทำงานร่วมกันระหว่าง Korean Worker's Party (KWP) และ the Ministry of People's Armed Forces (MPAF) ซึ่งเป็นหน่วยงานความมั่นคงปลอดภัยหลักของประเทศ โดยผู้นสูงสุดของ RGB คือ General Kim Yong-Chol ตั้งแต่ปี 2009 (Jun, LaFoy, & Sohn, 2015)

นอกจาก Reconnaissance General Bureau (RGB) เกาหลีเหนือยังองค์กรที่ทำหน้าที่เป็นฝ่ายปฏิบัตินั้นคือ General Staff Department of the Korean People's army หรือ GSD (총참모부) หน่วยงานนี้มีการแบ่งโครงสร้างในการโจมตีและโต้ตอบภัยคุกคามทางไซเบอร์ที่ชัดเจน และรายงานการปฏิบัติงานขึ้นตรงกับ Kim Il-Sung ผู้นำสูงสุดของเกาหลีเหนือ ภารกิจของ GSD ที่จะต้องรับผิดชอบได้แก่ ความมั่นคงปลอดภัยของข้อมูลสำคัญ ความปลอดภัยในการติดต่อสื่อสารของประชาชน สงครามอิเล็กทรอนิกส์ และปฏิบัติการด้านจิตวิทยา โดยในโครงสร้างองค์กร GSD จะประกอบไปด้วย Operations Bureau หน่วยวางแผนและยุทธศาสตร์องค์กร Command Automation Bureau (지휘자동화국) หน่วยปฏิบัติการด้านไซเบอร์และระบบเครือข่ายคอมพิวเตอร์ Enemy Collapse Sabotage Bureau ปฏิบัติการทางด้านข้อมูลข่าวสารสงครามเชิงจิตวิทยา และการสร้างโฆษณาชวนเชื่อ Communications Bureau เป็นหน่วยงานกลางในการประสานงานระหว่าง GSD กับหน่วยงานอื่น ๆ ของรัฐบาลเกาหลีเหนือ รวมทั้งเป็นหน่วยที่คอยดูแลรักษาความปลอดภัยในการติดต่อสื่อสารของประชาชนในประเทศ หน่วยงานสุดท้าย Electronic Warfare Bureau คือ หน่วยงานที่คอยจู่โจม ขัดขวาง และทำลายเครือข่ายและระบบควบคุมทางทหารของประเทศศัตรูผ่านช่องทางอิเล็กทรอนิกส์ (Jun et al., 2015)



รูปที่ 10 โครงสร้างองค์กร General Staff Department of the Korean People's Army

ที่มา: Jun et al. (2015)

2.8.4 การก่อการร้ายไซเบอร์ของประเทศในเอเชียใต้

2.8.4.1 ประเทศอินเดีย

การใช้เทคโนโลยีของผู้ก่อการร้ายในการโจมตีมุมไบในเดือนพฤศจิกายน ปี ค.ศ. 2008 ส่งผลกระทบถึงการใช้กฎหมายเพื่อดำเนินคดีกับผู้ก่อการร้ายที่ใช้เทคโนโลยีเพื่อวางแผนและดำเนินการโจมตี อินเดียยอมรับการแก้ไขกฎหมาย IT กว่า 2000 ฉบับ ในเดือนธันวาคม ค.ศ. 2008 และเช่นเดียวกับประเทศปากีสถานและบังคลาเทศที่ต้องมีการปรับใช้กฎหมายที่คล้ายกัน

หลังจากเกิดเหตุการณ์ก่อการร้ายในครั้งนั้น ประเทศอินเดียและปากีสถานทำให้ผู้ก่อการร้ายในโลกไซเบอร์ได้รับการลงโทษสูงสุด คือ การประหารชีวิต และเป็นจุดเริ่มต้นของการให้คำจำกัดความของการก่อการร้ายทางไซเบอร์ในบริบททางกฎหมายอย่างจริงจัง มาตรการของรัฐบาลอินเดียเพื่อป้องกันการใช้เทคโนโลยีโดยผู้ก่อการร้ายถูกกล่าวถึงในบริบทของระบอบประชาธิปไตยที่ต้องการรักษาความปลอดภัยให้สมดุลกับความเป็นส่วนตัวและเสรีภาพของพลเมือง

ประเทศอินเดียพบกับการก่อการร้ายครั้งใหญ่ ที่รู้จักในชื่อของ เหตุการณ์ 26/11 การโจมตีที่มุมไบครั้งนั้นผู้ก่อการร้ายได้มุ่งโจมตีโดยใช้ระเบิด ณ โรงแรม Mumbai Taj ก่อให้เกิดความเสียหายต่อชีวิตและทรัพย์สินเป็นอย่างมาก การก่อการร้ายในครั้งนี้ทราบภายหลังว่ามีการใช้ไซเบอร์เป็นเครื่องมือในการก่อระเบิด โดยการรวบรวมข้อมูลผ่านช่องทางออนไลน์และแพร่ข้อมูลสร้างความกลัวให้กับประชาชนโดยขัดขวางการรักษาความปลอดภัยของรัฐในระบบไซเบอร์

หลังจากเหตุการณ์ก่อความไม่สงบในครั้งนั้นเป็นเหตุทำให้ประเทศอินเดียต้องเริ่มการแก้ไขกฎหมายพระราชบัญญัติ The Information Technology Act 2000 ให้มีความเฉพาะเจาะจงมากขึ้นที่จะรับมือกับการก่อการร้ายทางไซเบอร์ได้ บทบัญญัติมาตราที่ 66F กล่าวถึงการนิยามการก่อการร้ายทางไซเบอร์ในความหมายที่กว้างเกินไป และวางกำหนดโทษตามตัวแสดงที่กระทำผิดในรูปแบบอาชญากรรมไซเบอร์เท่านั้นแต่ความหมายและคำจำกัดความของคำว่าอาชญากรรมไซเบอร์ (Cyber Terrorism) ในบทบัญญัติยังไม่มีความชัดเจนเพียงพอ และเพื่อจะทำให้ตัวบทกฎหมายในส่วนการก่อการร้ายมีความชัดเจนและมีประสิทธิภาพมากขึ้น รัฐบาลอินเดียได้ตั้งชุดกฎหมาย ปี 2011 ซึ่งมีความตั้งใจจะอุดช่องว่างกฎหมายทั้งปวง จากการศึกษาช่องว่างทางกฎหมายของประเทศอินเดีย พบว่า มีปัญหาในขอบเขต (Reich, 2012) ดังนี้

1. มายาคติและความจริงของการก่อการร้ายทางไซเบอร์
2. ประสิทธิภาพทางกฎหมายที่จะจัดการกับประเด็นการก่อการร้ายทางไซเบอร์
3. การบังคับใช้กฎหมายที่มีประสิทธิภาพจริงหรือไม่

2.8.4.2 ประเทศศรีลังกา

การก่อการร้ายที่มุ่งโจมตีโบสถ์คริสต์และโรงแรมในศรีลังกาเมื่อวันอาทิตย์ที่ 21 เมษายน ค.ศ. 2019 มีผู้เสียชีวิตจำนวน 359 คน ชี้ให้เห็นถึงระดับความรุนแรงและซับซ้อน โดยหลังจากการก่อเหตุ เจ้าหน้าที่ระดับสูงได้ชี้แจงว่าเหตุการณ์ครั้งนี้เกิดขึ้นโดยกลุ่มก่อการร้ายภายนอก คือ กลุ่ม IS และผู้ร่วมก่อการร้ายส่วนใหญ่มาจากครอบครัวชนชั้นกลางและชนชั้นสูง มีการศึกษาดี นักวิชาการได้ให้ข้อสังเกตว่าการก่อการร้ายในครั้งนี้เป็นการก่อการร้ายแบบไฮบริดที่ผสานกันลงตัวระหว่างการก่อการร้ายแบบเก่าและแบบใหม่โดยใช้เทคโนโลยีเป็นเครื่องมือ การก่อการร้ายแบบนี้จะเป็นรูปแบบที่จะกระทำมากขึ้นในอนาคต มีลักษณะที่ตรวจจับยาก ไม่สามารถหาเบาะแสได้ตามหลักฐานทั่วไปเพราะผู้ก่อการร้ายติดต่อสื่อสารผ่านทางเทคโนโลยีและจิตวิญญาณร่วมที่ไร้พรหมแดน

การก่อการร้ายที่โบสถ์คริสต์และโรงแรมในศรีลังกาเริ่มต้นจากการปลุกระดมจากโซเชียลที่สามารถเข้าถึงประชาชนได้ทุกกลุ่มหากมีอินเทอร์เน็ต หรือเรียกได้ว่าการ “ระบาดทางอารมณ์” ผ่านสื่อสังคมออนไลน์นั้นก่อให้เกิดผลกระทบที่รุนแรงเป็นอย่างมาก การประสานงานกับเครือข่ายแนวคิดเดียวกันจึงทำให้เป็นไปได้อย่างรวดเร็ว รวมไปถึงภาวะในการตัดสินใจของคนกลุ่มนี้ก็สามารถทำได้โดยไม่ตั้งอาศัยการยับยั้งชั่งใจใด ๆ

พื้นที่ทางไซเบอร์ถูกนำมาใช้เป็นเครื่องมือในการก่อการร้ายของกลุ่ม The Liberation Tigers of Tamil Eelam (LTTE) ที่ต่อสู้กับรัฐบาลศรีลังกา โดยมีกลยุทธ์สำคัญในการหาแหล่งทุนสนับสนุนกลุ่มก่อการร้ายผ่านทางไซเบอร์ สร้างข่าวลือ โฆษณาชวนเชื่อ ยุแยงให้ผู้คน

แตกแยก และสร้างความเข้าใจผิดให้กับนานาประเทศเรื่องของการกดขี่ข่มเหงชนกลุ่มน้อยโดยรัฐ กลุ่ม LTTE ยังพยายามที่จะแฮกข้อมูลสำคัญและ เว็บไซต์ของรัฐบาลหลายครั้ง Concannon และ McKeever ให้ความเห็นว่า กลุ่ม LTTE เป็นกลุ่มการก่อการร้ายกลุ่มแรกที่ใช้อินเทอร์เน็ตเป็นเครื่องมือในการก่อการร้าย ในปี 1988 โดยพยายามที่จะโจมตีระบบของสถานทูตศรีลังกาด้วยการถล่มส่งอีเมล์กว่า 800 ครั้งต่อวันเป็นเวลา 2 อาทิตย์ ทำให้ระบบอีเมล์ของสถานทูตไม่สามารถใช้การได้ โดยมีข้อความว่า “We are the Internet Black Tigers and we’re doing this to interrupt your communications” (Reich, 2012) โดย Intelligence Department ของศรีลังกาได้ประกาศว่าการกระทำนี้เป็นการกระทำของการก่อการร้ายทางไซเบอร์ครั้งแรกของประเทศศรีลังกา และเมื่อวันที่ 1 เดือน พฤษภาคม ปี 2009 กลุ่ม LTTE ได้โจมตีรัฐบาลศรีลังกาทางไซเบอร์อีกครั้งโดยการสร้างโฆษณาชวนเชื่อเพื่อยุยงให้เกิดความแตกแยกของประชาชนผ่านทางเวปไซต์ของรัฐบาล เหตุการณ์ครั้งนี้ทำให้รัฐบาลศรีลังกากลับมาสนใจเรื่องความมั่นคงปลอดภัยของข้อมูลมากขึ้น

1) ยุทธศาสตร์การรับมือการก่อการร้ายไซเบอร์ของรัฐบาลศรีลังกา

เมื่อการต่อสู้ทางไซเบอร์ของกลุ่ม LTTE ถูกตีตราว่าเป็นภัยต่อความมั่นคงของรัฐ การปฏิบัติการทางทหารเพื่อต่อต้านกลุ่ม LTTE จึงเกิดขึ้น ประการแรก รัฐบาลศรีลังกาใช้ความรุนแรงและข่มขู่กลุ่ม LTTE เพื่อต่อต้านการโฆษณาชวนเชื่อที่กลุ่ม LTTE ได้สร้างขึ้นบนอินเทอร์เน็ต เป้าหมายหลักของรัฐบาลคือการกำจัดเวปไซต์ www.tamilnet.com เนื่องจากเป็นเวปไซต์หนึ่งที่สื่อใช้อ้างถึงมากที่สุด สื่อต่างประเทศอย่าง Vidanage ชี้ให้เห็นว่า “รัฐบาลศรีลังกาได้เริ่มต้นสงครามไซเบอร์ใต้ดินกับเว็บไซต์สำนักงานใหญ่ของ LTTE เนื่องจากรัฐบาลขาดความเชี่ยวชาญในการโจมตีรูปแบบของแฮกเกอร์บนเว็บไซต์จึงต้องขอความช่วยเหลือจากสหรัฐฯ ในการส่งทีมงานลับไปเพื่อโจมตีเว็บไซต์สำนักงานใหญ่ของ LTTE” (Karatzogianni, 2009) (Vidanage ใน Karatzogianni) นอกจากนี้ Vidanage ยังชี้ให้เห็นว่า รัฐบาลศรีลังกาพยายามทำทุกวิถีทางที่จะจำกัดบทบาทในโลกไซเบอร์ของกลุ่ม LTTE และทั้งยังมี ข่าวลือในการสังหารหัวหน้าบรรณาธิการของเวปไซต์อีกด้วย สิ่งเหล่านี้คือสัญญาณบางอย่างที่แสดงให้เห็นว่ารัฐบาลกำลังรุกล้ำและแย่งชิงพื้นที่สื่อของกลุ่ม LTTE บนอินเทอร์เน็ต

ดังนั้นการศึกษาของ Vidanage จึงสรุปอย่างชัดเจนว่ารัฐบาลศรีลังกาอยู่เบื้องหลังการปิดปากผู้ที่เกี่ยวข้องกับเวปไซต์ www.tamilnet.com ด้วยวิธีที่รุนแรง แต่อย่างไรก็ตาม รัฐมนตรีว่าการกระทรวงโทรคมนาคมของศรีลังกาได้ออกมาประณามการฆ่าบรรณาธิการของเว็บไซต์นั้น แต่ก็ยังกล่าวต่อไปอีกว่า“ฉันก็ยังจะอยากจ้างแฮกเกอร์ที่สามารถปิดการใช้งานของ TamilNet ได้” สิ่งที่รัฐมนตรีกล่าวอาจจะเป็นสัญญะภายในที่แสดงออกให้เห็นว่าเขาเองก็ไม่ได้พอใจนักกับการกระทำของแฮกเกอร์เหล่านั้น แต่สิ่งที่ศรีลังกาต้องการจริง ๆ ณ ตอนนี้คือ การสามารถ

คาดการณ์ล่วงหน้าได้เกี่ยวกับภัยคุกคามที่จะมีต่อรัฐบาลศรีลังกา ในอนาคตจากเวปไซต์ www.tamilnet.com” (Karatzogianni, 2009)

ในช่วงสุดท้ายของสงคราม Eelam ปี 2006-2009 การสื่อสารทางอินเทอร์เน็ตของกลุ่ม LTTE ถูกยับยั้งโดยรัฐบาล มีการดำเนินการทางกฎหมายเพื่อควบคุมการใช้อินเทอร์เน็ตในคาเฟ่ โดยรัฐบาลได้ออกมาตรการหลัก อาทิ เจ้าของร้านอินเทอร์เน็ตจะต้องลงทะเบียนข้อมูลของผู้ใช้และทำตามคำสั่งของรัฐบาล นอกจากนั้นข่าวของเว็บไซต์ LTTE หรือการรายงานข่าวใด ๆ ที่สนับสนุนอุดมการณ์ต่อต้านรัฐ ก็จะถูกลบไปจากพื้นที่ไซเบอร์ของศรีลังกา

2) กฎหมายควบคุมไซเบอร์ของกลุ่มประเทศในเอเชียใต้

หลังจากประเทศในเอเชียใต้เผชิญกับการก่อการร้ายไซเบอร์ อินเดียจึงริเริ่มแก้ไข The Information Technology Act 2000 ฉบับบเพิ่มเติม ปี 2008 โดยเพิ่มมาตรา 66F (Punishment for Cyber Terrorism) เพื่อรับมือการก่อการร้ายไซเบอร์ มีรายละเอียด (สาวตรี สุขศรี, 2563) ดังนี้

(1) ผู้ใดมีความตั้งใจที่จะคุกคามความเป็นอันหนึ่งอันเดียวกัน ความมั่นคงหรืออำนาจอธิปไตยของอินเดีย หรือโจมตีเพื่อสร้างความหวาดกลัวในหมู่ประชาชนชนหรือส่วนใดส่วนหนึ่งของประชาชนโดย

(ก) การปฏิเสธ หรือทำให้เกิดการปฏิเสธการเข้าถึงของบุคคลใด ๆ ที่ได้รับอนุญาตให้เข้าถึงทรัพยากรคอมพิวเตอร์ หรือ

(ข) พยายามเจาะหรือเข้าถึงทรัพยากรคอมพิวเตอร์โดยไม่ได้รับอนุญาต หรือเข้าถึงเกินกว่าที่ได้รับอนุญาต หรือ

(ค) แพร่กระจาย หรือก่อให้เกิดการแพร่กระจายวิ่งปนเปื้อนในคอมพิวเตอร์และโดยวิธีการดังกล่าวทำให้เกิด หรือมีแนวโน้มทำให้บุคคลเสียชีวิต บาดเจ็บหรือทำให้เสียหายหรือทำให้บริการที่จำเป็นต่อการดำรงชีวิตของชุมชนต้องหยุดลงหรือส่งผลกระทบต่อโครงสร้างพื้นฐานของข้อมูลที่สำคัญที่ระบุไว้ในมาตรา 70

(2) ผู้ใดมีตระหนักรู้ หรือทำโดยเจตนา แทรกซึม เข้าถึงทรัพยากรคอมพิวเตอร์โดยไม่ได้รับอนุญาต หรือเกินไปกว่าที่ได้รับอนุญาต และโดยวิธีการดังกล่าวจะได้เข้าถึงสารสนเทศ ข้อมูล หรือฐานข้อมูลคอมพิวเตอร์ที่ถูกจำกัดไว้ด้วยเหตุผลด้านความปลอดภัยของรัฐ หรือความสัมพันธ์ระหว่างประเทศ หรือสารสนเทศ ข้อมูล หรือ ฐานข้อมูลคอมพิวเตอร์ที่ถูกจำกัดไว้ด้วยเหตุผลเพราะเชื่อว่าการได้ไปซึ่งข้อมูลเหล่านั้น อาจถูกนำไปใช้เพื่อก่อให้เกิด หรือมีแนวโน้มที่จะทำให้เกิดความเสียหายต่อผลประโยชน์ของอธิปไตย และความมั่นคงของอินเดีย ต่อความสัมพันธ์กับต่างประเทศ ต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน หรือเกี่ยวกับการดูหมิ่นศาล การ

หมิ่นประมาทหรือยั่วยุให้กระทำความผิด หรือทำไปเพื่อผลประโยชน์ของต่างประเทศ กลุ่มบุคคล หรืออื่น ๆ

(3) ผู้ใดที่กระทำ หรือสมคบคิดที่จะกระทำการก่อการร้ายในโลกไซเบอร์ ต้องถูกลงโทษด้วยการจำคุกซึ่งอาจขยายถึงการจำคุกตลอดชีวิต

ประเทศอินเดียมีการใช้กฎหมายที่มุ่งเน้นถึงการกระทำความผิดที่เข้าถึงโดยปราศจากอำนาจ เช่น การขโมยข้อมูล การโจทตีให้เกิดความเสียหายต่อระบบหรือข้อมูลคอมพิวเตอร์ โดยเฉพาะในมาตราที่ 66F ที่มุ่งหมายต่อการกระทำความผิดที่ส่งผลเสียต่อรัฐ ทั้งที่ตั้งใจที่ก่อให้เกิดความสูญเสียในระดับบุคคลทั่วไปและเพื่อสร้างความหวาดกลัวให้เกิดกับประชาชนและสังคม ที่เป็นองค์ประกอบสำคัญในการก่อการร้าย

2.8.5 การก่อการร้ายไซเบอร์ของประเทศสหรัฐอเมริกา

สหรัฐอเมริกามีความเสี่ยงต่อภัยคุกคามทางไซเบอร์เนื่องจากประชาชนมากกว่าร้อยละ 70 สามารถเข้าถึงอินเทอร์เน็ตซึ่งเป็นการควบคุมได้ยาก โครงสร้างพื้นฐานเกือบทั้งหมดของประเทศอเมริกาขึ้นอยู่กับระบบไซเบอร์ ไม่ว่าจะเป็นระบบการขนส่ง ระบบธนาคาร ระบบการรักษาพยาบาล หรือโครงสร้างสาธารณูปโภค เช่น ไฟฟ้า ประปา ด้วยเหตุนี้จึงทำให้สหรัฐคำนึงถึงการรักษาความปลอดภัยของระบบไซเบอร์เป็นอย่างดี นอกจากนี้กองทัพสหรัฐฯ ยังมีแถลงการณ์ว่า ภัยคุกคามทางไซเบอร์เป็นภัยคุกคามที่อาจส่งผลกระทบถึงสามในสี่ของผลประโยชน์หลักของชาติ ได้แก่ สถานภาพทางเศรษฐกิจ ความมั่นคง ความเป็นระเบียบของชาติ

ภายคุกคามครั้งแรกของสหรัฐอเมริกาเกิดขึ้นครั้งแรกในปี 2010 เมื่อสหรัฐฯ เข้าสู่สงครามไซเบอร์ โดยประกาศขีดความสามารถทางไซเบอร์ของกองทัพเรือ กองทัพอากาศ และกองทัพบก เข้าเป็นหนึ่งเดียวกันภายใต้อำนาจของ U. S. Cyber Command โดยหลังจากนั้นสหรัฐฯ ได้เพิ่มกำลังของเจ้าหน้าที่ด้านไซเบอร์กว่าเกือบ 2,000 คน ในปี 2014 และเพิ่มจำนวนอีกว่า 4,000 คน ภายใน 2 ปีต่อมา อเมริกาประกาศสงครามไซเบอร์เป็นกลยุทธ์ที่เรียกว่า “The Best Defense is a Good Offense” หรือ “การป้องกันเชิงรุกทางไซเบอร์” และยกระดับการก่อการร้ายทางไซเบอร์ให้เป็นการก่อการร้ายที่แรงกว่า al-Qaeda บารัค โอบามา อดีตประธานาธิบดีของสหรัฐอเมริกาให้ความสำคัญถึงโครงสร้างพื้นฐานดิจิทัลว่าเป็นยุทธศาสตร์ของชาติและก่อให้เกิดกลยุทธ์และแผนแม่บทย่อยต่าง ๆ ตามมาเพื่อป้องกันการถูกจู่โจม (CSIS, 2020)

ภัยคุกคามทางไซเบอร์ล่าสุดที่สหรัฐเจอเกิดขึ้นเมื่อเดือนพฤษภาคม ปี 2020 สหรัฐฯ กล่าวหาว่าจีนได้พยายามขโมยงานวิจัยที่เกี่ยวกับการศึกษาเกี่ยวกับวัคซีนรักษาโรคติดเชื้อไวรัสโคโรนา 2019 ที่เก็บไว้ในฐานข้อมูล Big Data ของสหรัฐอเมริกา (CSIS, 2020) สำนักงานสอบสวนกลาง

(Federal Bureau of Investigation: FBI) รายงานว่า ได้มีความพยายามที่จะจู่โจมระบบฐานข้อมูลวิจัยวัคซีนของสหรัฐ โดยระบุว่ารัฐบาลจีนเป็นผู้ก่อการครั้งนี้ แต่โฆษกรัฐบาลได้ออกมาปฏิเสธการกระทำดังกล่าว การเกิดโรคระบาดนี้สร้างความบาดหมางให้กับทั้งสองประเทศเป็นอย่างมาก และพร้อมกล่าวหาว่าฝ่ายเป็นผู้เริ่มการเกิดขึ้นของไวรัสครั้งนี้ The Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency (CISA) ของประเทศสหรัฐฯ ได้ออกคำเตือนอย่างเป็นทางการกับสัญญาณการก่อการร้ายทางไซเบอร์ที่จีนเป็นผู้ต้องสงสัย โดยรายละเอียดการโจมตีปรากฏว่า ผู้โจมตีกำลังแอบเฝ้าสังเกตข้อมูลความเคลื่อนไหวของหน่วยงานสาธารณสุขในอเมริกาและพยายามขโมยสิทธิบัตรที่อเมริกากำลังจะจดทะเบียนกับวัคซีนรักษาโรค ติดเชื้อ Covid 19 จีนและสหรัฐมีความบาดหมางในเรื่องของสงครามไซเบอร์กันมานาน ตั้งแต่ในปี 2009 ซึ่งรัฐบาลจีนถูกสหรัฐฯ กล่าวหาว่า เป็นตัวการหลักในการแทรกซึมเข้าระบบและขโมยข้อมูลสำคัญของเครื่องบินรบ Lockheed Martin F-35 Fighter Jet หลังจากที่จีนประกาศว่าจะพัฒนาเครื่องบินรบชนิดใหม่ the Shenyang J-31 ที่มีฟังก์ชันเหมือนกับ เครื่องบินรบ Lockheed Martin F-35 ที่มากกว่านั้น หน่วยข่าวกรองของสหรัฐฯ ให้ข้อมูลว่ารัฐบาลจีนพยายามจะขโมยเทคโนโลยีและข้อมูลสำคัญทางไซเบอร์ทุกอย่างที่สหรัฐฯมี เพื่อนำมาพัฒนาเทคโนโลยีของตนเอง (BBC NEWS, 2020)

2.8.5.1 การรับมือการก่อการร้ายไซเบอร์ของสหรัฐอเมริกา

สหรัฐฯ มีแผนการป้องกันภัยคุกคามทางไซเบอร์โดยให้การรักษาความปลอดภัยทางไซเบอร์มีความสำคัญเป็นอันดับหนึ่งและเป็นสิ่งที่สหรัฐฯต้องทำอย่างเร่งด่วน ในปัจจุบันกระทรวงความมั่นคงแห่งมาตุภูมิ (The Department of Homeland Security) เป็นกระทรวงที่ได้รับอำนาจในการดูแลระบบรักษาความปลอดภัยของไซเบอร์ทั้งหมด โดยเฉพาะโครงสร้างสาธารณูปโภคพื้นฐานที่สำคัญ โดยกระทรวงความมั่นคงแห่งมาตุภูมิจะเป็นหน่วยนำและประสานงานกับหน่วยงานอื่น ๆ ของรัฐบาลให้ทำแผนแม่บทย่อยเพื่อปฏิบัติตามแผนยุทธศาสตร์ใหญ่ที่กระทรวงเป็นผู้กำหนด นอกจากนี้กระทรวงยังเป็นผู้ควบคุมการดำเนินนโยบายของ ศูนย์รักษาความมั่นคงปลอดภัยด้านไซเบอร์แห่งชาติ (National Cyber Security Center) อีกกรอบหนึ่งด้วย นอกจากนี้กระทรวงกลาโหมของสหรัฐฯ ยังมีบทบาทสำคัญร่วมในการควบคุมระบบรักษาความปลอดภัยทางไซเบอร์โดยร่วมมือกับภาคเอกชนในการแบ่งปันข้อมูลสำคัญ รวมไปถึงการบูรณาการข้อมูลกับหน่วยข่าวกรอง และ National Cyber Investigative Joint Task Force หรือ หน่วยเฉพาะกิจร่วมด้านการสืบสวนสอบสวนด้านไซเบอร์แห่งชาติของสหรัฐฯ ร่วมเป็นส่วนหนึ่งในการดำเนินนโยบาย โดยหน่วยเฉพาะกิจร่วมด้านการสืบสวนสอบสวนด้านไซเบอร์แห่งชาติยังสามารถบังคับใช้กรอบทางไซเบอร์กับหน่วยงานของสหรัฐฯทั่วประเทศ (Cilluffo, 2017)

ยุทธศาสตร์การรักษาความปลดภัยทางไซเบอร์ของสหรัฐเมริกาสามารถแบ่งเป็นประเด็นสำคัญได้ดังนี้

1) ขยายการเตือนภัยทางไซเบอร์และสร้างข้อมูลเครือข่ายเพื่อสนับสนุนการจัดการภัยคุกคาม

2) พัฒนาให้เกิดการแบ่งปันข้อมูลระหว่างภาครัฐและเอกชนเพื่อเฝ้าระวังภัย

3) บังคับใช้แผนการป้องกันภัยคุกตามทางไซเบอร์อย่างต่อเนื่องและบังคับใช้ทั่วทุกพื้นที่

4) ปรับปรุงการรับมือภัยคุกคามไซเบอร์ในประเทศ

2.8.5.2 กฎหมายควบคุมไซเบอร์ของประเทศสหรัฐอเมริกา

สหรัฐอเมริกาเป็นประเทศผู้นำในการรับมือการก่อการร้ายหลังจากเหตุการณ์ 9/11 ในปี 2001 สหรัฐได้ออกกฎหมายภายใต้ชื่อของ The USA Patriot Act 2001 ซึ่งเป็นกฎหมายแห่งการเริ่มต้นในการรับมือกับภายคุกคาม ในกฎหมายฉบับนี้ยังมีวัตถุประสงค์ในการเฝ้าระวังภัยที่จะเกิดขึ้นทางไซเบอร์และพร้อมที่จะอาศัยอำนาจในการตัดช่องทางต่างของผู้ก่อการร้ายผ่านช่องทางอินเทอร์เน็ต ในมาตราที่ 814 กำหนดถึงการยับยั้งและป้องกันการก่อการร้ายไซเบอร์ มีผลเป็นการแก้เพิ่มเติมมาตรา 1030 ของ Title 18, The United Code ที่เกี่ยวข้องกับการฉ้อโกงทางคอมพิวเตอร์ ผู้กระทำความผิดตามมาตรนี้มีโทษตั้งแต่ปรับ จำคุกไม่เกิน 5 ปี 10 ปี และสูงสุดจำคุกไม่เกิน 20 ปี ทั้งนี้ขึ้นอยู่กับรูปแบบของการกระทำความผิดและความเสียหายที่เกิดขึ้น (สาวตรี สุขศรี, 2563)

นอกจากนี้สหรัฐฯ ยังมีรัฐบัญญัติว่าด้วยการกระทำโดยมิชอบและฉ้อโกงทางคอมพิวเตอร์เป็นกฎหมายเฉพาะในระดับรัฐบาลกลางที่กำหนดฐานความผิดเกี่ยวกับผู้ที่กระทำความผิดทางไซเบอร์ (The Computer Fraud and Abuse Act) ประกอบด้วยความผิด 7 ฐาน (คณาธิป ทองรวีวงศ์, 2563) ดังนี้

1) ฐานโจรกรรมข้อมูลข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องกับความมั่นคงของชาติมีองค์ประกอบความผิด คือ เข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจหรือเกินขอบเขตอำนาจให้ได้มาซึ่งข้อมูลที่จะนำไปใช้ให้เกิดความเสียหายต่อรัฐ หรืออาจนำไปใช้กับรัฐบาลต่างชาติ

2) ฐานโจรกรรมข้อมูลข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องกับการเงิน ประกอบไปด้วยองค์ประกอบ ความผิดสำคัญคือ เข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจหรือเกินขอบเขตอำนาจให้ได้มาซึ่งข้อมูลเกี่ยวกับสถาบันทางการเงิน ข้อมูลสถานะการเงินของผู้บริโภค

3) ฐานเข้าถึงโดยมิชอบซึ่งคอมพิวเตอร์ของหน่วยงานรัฐมีองค์ประกอบความผิดคือ เข้าถึงคอมพิวเตอร์ที่ไม่ใช่สาธารณะ แต่เป็นคอมพิวเตอร์หน่วยงานของรัฐและส่งผลกระทบต่อการใช้คอมพิวเตอร์ดังกล่าวของรัฐบาล

4) ฐานฉ้อโกงหลอกลวงทางคอมพิวเตอร์ มีองค์ประกอบความผิดสำคัญคือเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจหรือเกินขอบอำนาจ ฉ้อโกงและได้มาซึ่งสิ่งใดที่มีคุณค่า

5) ฐานทำให้เสียหายต่อคอมพิวเตอร์ มีองค์ประกอบสำคัญคือเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจหรือเกินขอบเขตอำนาจ ส่งโปรแกรม ข้อมูล คำสั่ง ทำให้เกิดความเสียหายต่อคอมพิวเตอร์

6) ฐานได้มาซึ่งรหัสผ่านหรือข้อมูลที่อาจนำไปสู่การเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจ มีองค์ประกอบความผิดที่สำคัญคือ ผู้ใดรู้และมีเจตนาหลอกลวงเกี่ยวกับการได้มาซึ่งรหัสผ่านหรือข้อมูลอื่นที่คล้ายคลึงกันซึ่งอาจนำไปสู่การเข้าถึงคอมพิวเตอร์โดยปราศจากอำนาจ

7) ฐานกรรโชกทรัพย์ไซเบอร์ มีองค์ประกอบความผิดที่สำคัญคือ ผู้ใดโดยเจตนาเพื่อกรรโชกเงินหรือสิ่งอื่นอันมีคุณค่าจากผู้อื่น กระทำการส่งการสื่อสารที่มีเนื้อหา ข่มขู่ว่าจะกระทำความเสียหายต่อคอมพิวเตอร์ที่ได้รับการคุ้มครองตามกฎหมายนี้

ความผิดทางคอมพิวเตอร์ตามรัฐบัญญัติว่าด้วยการกระทำโดยมิชอบและฉ้อโกงทางคอมพิวเตอร์นี้จะมุ่งเน้นไปยังขอบเขตของคอมพิวเตอร์ที่ได้รับการคุ้มครอง ซึ่งหมายถึงคอมพิวเตอร์ที่ใช้โดยรัฐบาลหรือสถาบันของรัฐ เมื่อการกระทำอันเป็นความผิดนั้นส่งผลกระทบต่อการใช้งานคอมพิวเตอร์ของสถาบันนั้น หรือคอมพิวเตอร์ถูกใช้หรือส่งผลกระทบต่อการสื่อสารระหว่างรัฐหรือการค้าระหว่างประเทศ รวมถึงคอมพิวเตอร์ที่ตั้งอยู่นอกสหรัฐอเมริกาซึ่งถูกใช้ในลักษณะกระทบการสื่อสารระหว่างรัฐหรือการค้าระหว่างประเทศ รัฐบัญญัติว่าด้วยการกระทำโดยมิชอบและฉ้อโกงทางคอมพิวเตอร์ หรือ The Computer Fraud and Abuse Act เป็นกฎหมายระดับรัฐบาลกลางโดยในแต่ละมลรัฐจะมีกฎหมายควบคุมกระทำความผิดที่เกี่ยวกับคอมพิวเตอร์ของตนอยู่แล้ว แต่จะสามารถบังคับใช้ได้แค่เขตของมลรัฐเท่านั้น และมีบัญญัติลักษณะความผิดของโทษที่แตกต่างกัน แต่จะอาศัยกรอบหลักในการนิยามความผิดที่เกี่ยวข้องกับ คอมพิวเตอร์ตามรัฐบัญญัติว่าด้วยการกระทำโดยมิชอบและฉ้อโกงทางคอมพิวเตอร์

นอกจากนี้สหรัฐยังมีกฎหมายที่บังคับใช้เมื่อเกิดการก่อการร้ายไซเบอร์ระหว่างประเทศ อาทิ ประเทศเกาหลีเหนือที่มีการมุ่งโจมตีสหรัฐอเมริกาอยู่บ่อยครั้ง สหรัฐจึงมีการระงับข้อพิพาททางกฎหมายโดยการบังคับ ลงโทษประเทศเกาหลีเหนือตาม The North Korean Sanctions and Policy Enhancement Act 2016 ที่สหรัฐฯสามารถลงโทษทางกฎหมายสำหรับ

องค์กรหรือบุคคลที่จัดหาข้อมูลสำคัญสนับสนุนให้เกาหลีเหนือสามารถกระทำการสำคัญที่เป็นการโจมตีภายใต้ขอบเขตความมั่นคงทางไซเบอร์ โดยวัตถประสงค์ของกฎหมายฉบับนี้เพื่อที่จะระงับการใช้ความรุนแรงหรือวิธีทางทหารตอบโต้การโจมตีของเกาหลีเหนือ ต้องการที่จะใช้วิธีทางการทูตในการเจรจาต่อรองกับรัฐบาลเกาหลีเหนือ และเพื่อช่วยประชาชนเกาหลีเหนือให้พ้นจากการคุกคามทางสิทธิและเสรีภาพจากรัฐบาล

The North Korean Sanctions and Policy Enhancement Act 2016 ฉบับนี้ครอบคลุมไปถึงการป้องกันการกระทำสำคัญของเกาหลีเหนือที่เป็นภัยต่อความมั่นคงทางไซเบอร์ของประเทศ (มาตรา 12) Significant Activities Undermining Cybersecurity โดยนิยามคำว่า “การกระทำสำคัญที่เป็นภัยต่อความมั่นคงทางไซเบอร์” ประกอบไปด้วยความพยายามที่จะกระทำการเหล่านี้ (Congress.Gov, 2016)

1) ปฏิเสธการเข้าถึง ทำให้ช้าลง ขัดขวาง หรือทำลาย ข้อมูลและการสื่อสารทางระบบเทคโนโลยีหรือเครือข่าย

2) แอบอ้างหรือลักลอบนำเอาข้อมูลออกจากระบบหรือเครือข่ายโดยปราศจากอำนาจ ผ่านการใช้การโจมตีของ มัลแวร์ (Malware Attacks) การใช้ Denial of Service และการกระทำประเภทอื่นที่กำหนดไว้ในกฎหมาย

สหรัฐอเมริกามีความรอบคอบในการออกกฎหมายเตรียมพร้อมรับมือกับภัยคุกคามไซเบอร์โดยกฎหมายที่ออกนั้นมีทั้งในระดับบุคคล องค์กร และครอบคลุมไปถึงระดับความสัมพันธ์ระหว่างประเทศ สหรัฐอเมริกาอาจมีความคุ้นชินกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นจึงทำให้รัฐบาลไม่ประมาทที่จะกำหนดทิศทางในการจัดการกับผู้ร้าย

2.8.6 การก่อการร้ายไซเบอร์ของสหราชอาณาจักร

ผู้ก่อการร้ายมากมายที่มีแผนการมุ่งโจมตีประเทศอังกฤษไม่เว้นแม้แต่การใช้เทคโนโลยีในการจู่โจม ผู้ก่อการร้ายเหล่านี้จะมาในรูปแบบของแฮกเกอร์ต่างชาติที่มีทรัพยากรเพียบพร้อมในการจารกรรม การก่อการร้ายมักจะพุ่งเป้าไปที่รัฐบาล กองทัพ หน่วยงานที่เกี่ยวข้องกับเศรษฐกิจและประชาชนทั่วไป วิธีจู่โจมเริ่มจากการขโมยข้อมูลสำคัญ เช่น ผลการวิจัยที่มีประโยชน์ โครงการที่สำคัญทางเศรษฐกิจ ในปี 2017 National Health Service หรือ NHS และรัฐสภาของอังกฤษได้รับการจู่โจมอย่างหนักหน่วง โดย Jeremy Fleming ผู้อำนวยการของ the British Government Communications Headquarters (GCHQ) ได้รายงานว่ามีการโจมตีที่สำคัญมากถึง 600 ครั้งเพียงแค่ใน 1 ปี โดยเมื่อเดือนพฤษภาคม ปี 2017 ผู้ก่อการร้ายได้ลักลอบเข้าระบบของ NHS เพื่อสลับสับเปลี่ยนนัดของคนไข้แต่ละโรงพยาบาลให้เกิดความสับสนวุ่นวายนี่เป็นแค่ส่วนหนึ่งที่

ชี้ให้เห็นว่าภัยคุกคามทางไซเบอร์นั้นใกล้ตัวชาวอังกฤษมากกว่าที่คิด นอกจากนี้ผู้ก่อการร้ายยังมีวิธีอื่น ๆ ที่แตกต่างออกไป เช่น การขโมยข้อมูลที่เป็นความลับและมาเปิดเผยต่อสาธารณชนเพื่อยุยง โน้มน้าวให้ประชาชนเชื่อในฝั่งตรงข้ามกับรัฐบาล (GCHO, 2016)

2.8.6.1 ยุทธศาสตร์การรับมือภัยคุกคามของสหราชอาณาจักร

อังกฤษตั้งศูนย์ดำเนินงานต่อต้านภัยคุกคามไซเบอร์ ที่เรียกว่า National Cyber Security Center (NSCS) มีภารกิจหลักในการให้ความปลอดภัยกับองค์กรต่าง ๆ ทั้งภาครัฐ ภาคเอกชน และประชาชนในการใช้งานอินเทอร์เน็ตอย่างปลอดภัย เมื่อมีเหตุภัยคุกคามเกิดขึ้น NSCS จะให้คำแนะนำไปยังหน่วยงานนั้น ๆ ไปทันที โดย NSCS จะนำผู้เชี่ยวชาญทางด้านเทคโนโลยีทางอุตสาหกรรมและสาธารณูปโภคมาเป็นผู้ปฏิบัติงานหลักพร้อมด้วยมีทีมที่ปรึกษาผู้เชี่ยวชาญทางกฎหมาย หน่วยข่าวกรอง และผู้ที่เชียวชาญจากต่างชาติร่วมด้วยในช่วงแรกหลังจากที่ NSCS ก่อตั้ง การดำเนินงานของหน่วยงานสามารถจัดการกับ Website Phishing ซึ่งทำให้ชาวอังกฤษตกเป็นเหยื่อกว่าพันราย โดยการโจมตีดังกล่าวได้รับความช่วยเหลือจากแฮกเกอร์ของรัฐพันธมิตร เมื่อปี 2018 NSCS สามารถทำลายหน่วยงานที่ปลอมแปลงชื่อเพื่อแสวงหาผลประโยชน์จากอินเทอร์เน็ตกว่า 140,000 หน่วยงาน และเพื่อการป้องกันภัยคุกคามในระยะยาว NSCS ได้สร้าง เครื่องหมายโดเมนของรัฐบาล เพื่อเป็นสัญลักษณ์ในการกรองความน่าเชื่อถือของอีเมล์ที่ส่งเข้ามา หน่วยงาน NSCS เป็นหน่วยงานกลางที่รัฐบาลกลางตั้งขึ้นเพื่อกำกับดูแลความเรียบร้อยในโลกของไซเบอร์ (พิพัทธ์ เพิ่มพันธุ์, 2561) หน่วยงานนี้มีหน้าที่ที่จะรักษาความสงบและป้องกันระบบเศรษฐกิจขนาดใหญ่ของอังกฤษที่วางอยู่ในโลกดิจิทัลผ่านการรักษาความปลอดภัยทางไซเบอร์ โดยองค์กรมีวิสัยทัศน์ วัตถุประสงค์ และพันธกิจ ดังนี้

NSCS มีวิสัยทัศน์ที่มุ่งหมายที่จะทำให้สหราชอาณาจักรมีระบบเศรษฐกิจและสังคมที่ปลอดภัยท่ามกลางกระแสความเปลี่ยนแปลงทางไซเบอร์ โดยการบริหารจะต้องเป็นไปตามหลักค่านิยมความเชื่อหลักแห่งเสรีภาพ ความเสมอภาค โปร่งใส และภายใต้หลักนิติธรรมแห่งรัฐ โดยมีวัตถุประสงค์:

1) สหราชอาณาจักรจะต้องเป็นประเทศที่ปลอดภัย สามารถจัดการควบคุมภัยคุกคามจากไซเบอร์ได้และสร้างความเชื่อมั่นให้กับนานาประเทศ

2) สหราชอาณาจักรมีความยืดหยุ่นในการรับมือการโจมตีทางไซเบอร์มากขึ้นและสามารถปกป้องผลประโยชน์ของประเทศในโลกไซเบอร์ได้ดีขึ้น

3) สหราชอาณาจักรจะช่วยสร้างโลกไซเบอร์ให้โปร่งใส มั่นคงและหลากหลาย ซึ่งสาธารณชนในสหราชอาณาจักรสามารถใช้งานได้อย่างปลอดภัย

4) สหราชอาณาจักรมีความรู้ ทักษะ และขีดความสามารถที่จำเป็นเพื่อเป็นแนวทางในการจัดการความเสี่ยงทางไซเบอร์ได้อย่างสมบูรณ์

นอกจากนี้หน่วยงาน NSCS ซึ่งเป็นหน่วยงานกลางที่รัฐบาลกลางตั้งขึ้นเพื่อกำกับดูแลความเรียบร้อยในโลกของไซเบอร์จะต้องมีหลักปฏิบัติโดยคำนึงว่าระบบเครือข่ายทั้งหมดในโลกยุคโลกาภิวัตน์อาจมีความเสี่ยงที่จะถูกการโจมตีทางไซเบอร์ด้วยความผันผวนของเทคโนโลยีจึงเป็นการยากต่อการตรวจจับ ทำให้ไม่มีความปลอดภัยแน่นอน ดังนั้นสหราชอาณาจักรจะใช้วิธีจัดการกับความเสี่ยงเพื่อจัดลำดับความสำคัญการตอบสนองที่หน่วยงานมีไว้รองรับ ถึงแม้ว่าสหราชอาณาจักรจะมีผู้นำระดับชาติที่แข็งแกร่ง แต่รัฐบาลก็ไม่สามารถที่จะบริหารงานได้เพียงลำพัง ดังนั้นรัฐบาลจำเป็นต้องประเมินศักยภาพของตน รู้ขีดจำกัดของความสามารถในโลกไซเบอร์ เพื่อให้โครงสร้างพื้นฐานบางอย่างถูกดำเนินการป้องกันโดยเอกชนและผู้ที่มีความเชี่ยวชาญดำเนินการให้ทันต่อการคุกคาม ในอีกแง่มุมหนึ่งธรรมชาติของอินเทอร์เน็ตเป็นไปในรูปแบบที่นอกเหนือความเป็นรัฐชาติ เป็นภัยคุกคามข้ามพรมแดน ดังนั้น สหราชอาณาจักรจึงไม่สามารถดำเนินการทุกอย่างต่อไปได้ด้วยตนเอง และจำเป็นที่จะต้องหาพันธมิตรกับประเทศอื่น ๆ ที่สามารถแบ่งปัน แลกเปลี่ยนความคิดเห็นในมุมมองที่สหราชอาณาจักรละเลยไป สหราชอาณาจักรยังคงพิจารณาในประเด็นความมั่นคงของรัฐชาติและปัญหาการละเมิดสิทธิส่วนบุคคลเป็นอย่างดี ดังนั้นสหราชอาณาจักรจึงพยายามที่จะใช้นโยบายในการเข้าถึงข้อมูลความมั่นคงของชาติที่จะละเมิดสิทธิส่วนบุคคลน้อยที่สุดเพื่อเป็นไปตามหลักเสรีภาพขั้นพื้นฐานของประชาชน ในเวทีนานาชาติ สหราชอาณาจักรได้ดำเนินการพัฒนาบรรทัดฐานของพฤติกรรมที่ยอมรับได้ในโลกไซเบอร์ โดยเริ่มจากความเชื่อที่ว่าพฤติกรรมที่ไม่สามารถยอมรับได้ในแบบออฟไลน์นั้นก็ไม่ควรเป็นที่ยอมรับในทางออนไลน์โดยจุดยืนของสหราชอาณาจักรจะปฏิบัติไปตามกรอบหลักการที่เสนอโดยรัฐมนตรีต่างประเทศของสหราชอาณาจักร ดังนี้

1) รัฐบาลต้องดำเนินการที่เกี่ยวกับไซเบอร์การอย่างเป็นสัดส่วนเพื่อให้สอดคล้องกับกฎหมายระดับชาติและนานาชาติ

2) ประชาชนทุกคนจะต้องมีความสามารถในด้านของทักษะเทคโนโลยีและผู้ใช้ไซเบอร์ทุกคนจะต้องมีเคารพในความหลากหลายทั้งด้านภาษา วัฒนธรรม และความคิด

3) ความมั่นใจที่จะสร้างให้โลกไซเบอร์เปิดกว้างต่อนวัตกรรมและการไหลเวียนของความคิด ข้อมูลและการแสดงออกอย่างเสรี

4) ความต้องการที่จะทำให้แน่ใจว่าไซเบอร์สเปซยังคงเปิดกว้างต่อนวัตกรรมและการไหลเวียนของความคิดข้อมูลและการแสดงออกอย่างเสรี

5) ผู้ใช้ในโลกไซเบอร์จะต้องเคารพสิทธิส่วนบุคคลของความเป็นส่วนตัวและเพื่อให้การป้องกันที่เหมาะสมกับทรัพย์สินทางปัญญา

6) ส่งเสริมให้ทุกภาคส่วนทำงานร่วมกันเพื่อรับมือกับภัยคุกคามจากอาชญากรที่ทำหน้าที่ออนไลน์

7) ส่งเสริมสภาพแวดล้อมการแข่งขันเพื่อให้มั่นใจว่าผลตอบแทนจากการลงทุนในเครือข่ายมีความยุติธรรม เพื่อที่จะบรรลุวิสัยทัศน์ตามกรอบหลักการข้างต้น ภาครัฐ ภาคเอกชน และประชาชน จะต้องทำงานร่วมกัน เพื่อที่ทุกคนจะได้รับประโยชน์จากการใช้อินเทอร์เน็ตในพื้นที่ไซเบอร์ร่วมกัน ดังนั้นทุกภาคส่วนจึงมีหน้าที่รับผิดชอบในการช่วยปกป้อง และสอดส่องดูแลซึ่งกันและกัน บุคคลทั่วไปหรือประชาชนทั่วไปมีบทบาทสำคัญในดูแลสอดส่องโลกไซเบอร์ให้เป็นสถานที่ปลอดภัยในการทำธุรกิจและใช้ชีวิต โดยประชาชนจะต้องรู้วิธีป้องกันตนเองจากภัยคุกคามทางออนไลน์ในระดับพื้นฐานว่าทำอย่างไรประชาชนเหล่านั้นจะสามารถเข้าถึงข้อมูลที่ถูกต้องและทันสมัยเกี่ยวกับภัยคุกคามออนไลน์ที่พวกเขาจะต้องเผชิญในอนาคต นอกจากนี้ยังจะต้องให้ความรู้ประชาชนในเรื่องเทคนิคและวิธีปฏิบัติเมื่อพวกเขาตกอยู่ในสถานการณ์ภัยคุกคาม

โดยพื้นฐานแล้วประชาชนทั่วไปจะต้องระมัดระวังเกี่ยวกับการใส่ข้อมูลส่วนบุคคลหรือข้อมูลที่ละเอียดอ่อนบนอินเทอร์เน็ต ควรระวังสิ่งที่แนบมากับอีเมลหรือลิงก์จากผู้ส่งที่ไม่รู้จัก และการดาวน์โหลดไฟล์จากเว็บไซต์ที่ไม่น่าเชื่อถือ หากทุกภาคส่วนสามารถช่วยกันสอดส่องและสามารถระบุภัยคุกคามในพื้นที่ไซเบอร์ เช่น รายงานปัญหาที่พบเจอ สามารถระบุเว็บไซต์ที่หลอกลวง จะทำให้รัฐบาลสามารถทำงานได้ง่ายขึ้น ในส่วนของรัฐบาลมีหน้าที่รักษาความปลอดภัยในการใช้อินเทอร์เน็ตของประชาชน เช่น การป้องกันรหัสผ่าน การปรับปรุงซอฟต์แวร์ รวมไปถึงติดตั้งโปรแกรมต่อต้านมัลแวร์เพื่อช่วยป้องกันไม่ให้ผู้อื่นใช้คอมพิวเตอร์เพื่อเพิ่มการคุกคามได้ ผู้ใช้ไซเบอร์ทุกคนควรตระหนักรู้ในหน้าที่ของตน ผู้คนที่มีหน้าที่รับผิดชอบในโลกออฟไลน์ก็ย่อมต้องมีหน้าที่รับผิดชอบต่อพฤติกรรมของตนเองในโลกไซเบอร์เช่นกัน (Cabinet Office, 2020)

2.8.6.2 กฎหมายควบคุมไซเบอร์ของประเทศสหราชอาณาจักร

สหราชอาณาจักรกมีพระราชบัญญัติการก่อการร้ายภายใต้ชื่อของ The Terrorism Act 2000 ที่รวมถึงภัยคุกคามที่มาในรูปแบบของการทำลายระบบอิเล็กทรอนิกส์อย่างร้ายแรงแสดงให้เห็นว่าสหราชอาณาจักรได้ตระหนักถึงการก่อการร้ายไซเบอร์ตั้งแต่ในช่วงปี 2000 ในปี 2006 สหราชอาณาจักรได้แก้ไขเพิ่มเติมกฎหมายฉบับนี้ภายใต้ชื่อของ The Terrorism Act 2006 โดยเพิ่มเติมฐานความผิดใหม่ ๆ เช่น ฐานส่งเสริมให้เกิดการก่อการร้าย ฐานเชิดชูการก่อการร้าย ฐานเผยแพร่หรือแจกจ่ายเอกสารของผู้ก่อการร้ายไม่ว่าโดยวิธีใด ๆ รวมไปถึงวิธีทางอิเล็กฏทรอนิกส์ นอกจากนี้สหราชอาณาจักรยังออกพระราชบัญญัติเพิ่มเติมอีก 2 ฉบับ ได้แก่ พระราชบัญญัติว่าด้วยการระงับทรัพย์สินของผู้ก่อการร้ายในปี 2020 และ พระราชบัญญัติว่าด้วยป้องกันและสอบสวนการก่อการร้ายในปี 2011 อีกด้วย (สาวตรี สุขศรี, 2563)

สหราชอาณาจักรมีกฎหมายจัดการกับผู้กระทำความผิดทางคอมพิวเตอร์ผ่านพระราชบัญญัติการใช้คอมพิวเตอร์โดยมิชอบ (Computer Misuse Act) ประกอบไปด้วยความผิดหลัก 3 ฐานด้วยกัน (Legislation.gov.uk, 2007)

1) การเข้าถึงโดยปราศจากอำนาจ (Unathorized Access to Computer Material) มาตรา 1

มีองค์ประกอบความผิดที่สำคัญคือ ทำให้คอมพิวเตอร์ปฏิบัติการใด ๆ ด้วยเจตนาเข้าถึงโปรแกรมหรือข้อมูลใด ๆ ที่เก็บอยู่ในคอมพิวเตอร์โดยปราศจากอำนาจ และในขณะที่ผู้กระทำรู้ถึงการกระทำดังกล่าว

2) การเข้าถึงโดยปราศจากอำนาจด้วยเจตนากระทำความผิด (Unathorized Access with intent to commit or facilitate of further offences) ตามมาตรา 2

องค์ประกอบของความผิดที่สำคัญคือ การกระทำการเข้าถึงโดยปราศจากอำนาจด้วยเจตนาที่กระทำความผิดอื่น (Futher Offences) เจตนาอำนวยความสะดวกสำหรับการกระทำความผิดดังกล่าว ซึ่งเป็นความผิดที่กฎหมายกำหนดไว้ ผู้กระทำอายุ 21 ปี และ 18 ปีสำหรับอังกฤษและเวลส์ ซึ่งไม่มีประวัติกระทำความผิดมาก่อน จะต้องได้รับโทษจำคุกเป็นเวลา 5 ปี

3) การทำให้เสียหายซึ่งข้อมูลคอมพิวเตอร์โดยปราศจากอำนาจ (Unathorized Acts with intent to impair, or with recklessness as to impairing, operation of computer) มาตรา 3

องค์ประกอบของความผิดที่สำคัญคือ การกระทำใด ๆ โดยปราศจากอำนาจอันเกี่ยวข้องกับคอมพิวเตอร์ โดยในขณะกระทำผู้กระทำรู้ว่าตนปราศจากอำนาจและมีเจตนากระทำการต่อไปนี้

(ก) ทำให้เสียหาย (Impair) ต่อการปฏิบัติการของคอมพิวเตอร์

(ข) ป้องกันหรือขัดขวางการเข้าถึงโปรแกรมหรือข้อมูลใด ๆ ที่เก็บไว้ในคอมพิวเตอร์

(ค) ทำให้เสียหายต่อการดำเนินการของโปรแกรมใด ๆ หรือความน่าเชื่อถือได้ของข้อมูลใด ๆ

(ง) ทำให้สิ่งตาม (ก) - (ค) ถูกกระทำขึ้น

2.8.7 การก่อการร้ายไซเบอร์ในประเทศอิหร่าน

อิหร่าน เป็นหนึ่งในประเทศที่มีชื่อเสียงในเรื่องการปฏิบัติการการโจมตีทางไซเบอร์ โดยสถานการณ์ที่เกิดขึ้นส่วนหนึ่งมุ่งประเด็นในเรื่องการขยายวงจากการโจมตีทางไซเบอร์ (Cyber

Attacks) ไปสู่สงครามไซเบอร์ (Cyber War) เต็มรูปแบบทำให้เกิดเป้าหมายในการปฏิบัติการหลากหลายเป้าหมาย และความซับซ้อนอย่าง Hybrid War อิหร่านถูกมองว่าเป็นประเทศที่พยายามจะก่อสงครามกองโจรมุ่งโจมตีสหรัฐอเมริกา จนแม้กระทั่งปัจจุบันอิหร่านยังพยายามใช้ไซเบอร์จู่โจมโรงพลังงานนิวเคลียร์หรือแม้กระทั่งลอบสังหารทหารรายสำคัญของสหรัฐฯ โดยการใช้ โดรน จนทำให้ทั้งสองประเทศเกิดความขัดแย้งอย่างไม่สิ้นสุด ในอดีตอิหร่านได้โจมตีทางไซเบอร์มุ่งเป้าหมายเป็นเขื่อนของอเมริกา ระบบการเงินและเครือข่ายของรัฐบาล ซึ่งในขณะนั้นผลกระทบอาจเกิดขึ้นในระยะสั้น ภารกิจ Operation Ababil เป็นที่รู้จักดีว่าเป็นการโจมตีระบบการเงินอเมริกา มีเป้าหมายเป็นสถาบันการเงินที่ใหญ่ที่สุดของประเทศ

อิหร่านยังเคยโจมตีทางไซเบอร์โดยการใช้ Malware Shamoon โจมตีบริษัท น้ำมันรายใหญ่ซึ่งลบข้อมูลจากคอมพิวเตอร์หลายพันเครื่องส่งผลให้เกิดค่าเสียหายมากมาย กระทบต่อราคาน้ำมันหรืออุปทานน้ำมันทั่วโลก นอกจากนี้อิหร่านเองจะเคยถูกโจมตีโดยการทำลายข้อมูลจนสูญเสียการควบคุมของระบบส่งผลกระทบทางกายภาพ อย่างเช่นกรณีที่อิหร่านโดนโจมตีด้วย Stuxnet โปรแกรมที่ดำเนินการโดยสหรัฐอเมริกาและอิสราเอลทำให้เกิดความเสียหายอย่างมากต่อเครื่องหมุนเหวี่ยงนิวเคลียร์ของอิหร่านที่เชื่อว่าเป็นโครงการพัฒนานิวเคลียร์ทางการทหารของอิหร่าน การที่จะรับมือภัยคุ้มคามทางไซเบอร์ของอิหร่านนั้นจำเป็นจะต้องใช้หน่วยข่าวกรองที่มีความเชี่ยวชาญในการสอดแนม กฎหมายที่สามารถเอาผิดกับผู้ก่อการร้ายไซเบอร์ที่ไร้พรมแดน

2.8.7.1 การรับมือภัยก่อการร้ายไซเบอร์ของประเทศอิหร่าน

ประเทศอิหร่านให้อำนาจกับกองทัพไซเบอร์หรือ Iranian Cyber Army ซึ่งเป็นกลุ่มแฮกเกอร์ของรัฐสามารถติดต่อประสานงานกับรัฐบาลอย่างถูกกฎหมายและขึ้นตรงกับผู้นำสูงสุดของประเทศอิหร่าน (Supreme Leader of Iran) หน่วยงานนี้ถูกสร้างขึ้นในปี 2005 โดยกลุ่ม Tehran Bureau ซึ่งมีผู้นำคือ Mohammad Hussein Tajik สมาชิกของกลุ่มนี้ได้อ้างว่าการจู่โจมทางอินเทอร์เน็ตหลายครั้งเป็นการกระทำของพวกเขาตั้งแต่ในปี 2009 การจู่โจมส่วนมากพบใน Baidu and Twitter การจู่โจม Baidu นี้เป็นเหตุที่ทำให้เกิดสงครามที่เรียกว่า Sino-Iranian Hacker War ที่มีการจู่โจม International Atomic Energy Agency องค์กรนิวเคลียร์นานาชาติ จากที่กล่าวมาทั้งหมดนี้เห็นได้ว่า อิหร่านมักจะเป็นประเทศผู้ริเริ่มการโจมตีซึ่งเป็นการประกาศตนว่า เป็นผู้มีอำนาจทางสงครามไซเบอร์ ในปี 2013 Institute for National Security Studiesลงความเห็นว่า Islamic Revolutionary Guards กองกำลังทางไซเบอร์ของอิหร่านเป็นกองทัพไซเบอร์ที่ยิ่งใหญ่เป็นอันดับที่ 4 ของโลก ยุทธศาสตร์การป้องกันภัยคุกคามทางไซเบอร์ของอิหร่านส่วนใหญ่จะขึ้นอยู่กับกลุ่มภายใต้อำนาจของรัฐ มีความคล่องแคล่วและรวดเร็วในการตัดสินใจเพราะมีอำนาจการสั่งการโดยตรงจากผู้นำสูงสุดเพียงคนเดียว (Doffman, 2019)

2.8.7.2 กฎหมายควบคุมไซเบอร์ของประเทศอิหร่าน

ประเทศอิหร่านมีกฎหมายที่ควบคุมดูแลการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ทั้งหมด 56 มาตรา ในส่วนแรกเป็นเป็นเรื่องที่ว่าด้วยอาชญากรรมและการกำหนดโทษ ส่วนที่สอง คือกฎหมายวิธีพิจารณาความแพ่ง และส่วนที่สามคือ ข้อบังคับต่าง ๆ โดยสามารถยกตัวอย่างมาตราที่สำคัญที่ใช้ในการจัดการกับอาชญากรหรือผู้ก่อการร้ายไซเบอร์ (Free Word Centre, 2012) ดังนี้

บทที่ 1 อาชญากรรมต่อความเป็นส่วนตัวของข้อมูลคอมพิวเตอร์และระบบโทรคมนาคม

มาตรา 1 การเข้าถึงข้อมูลคอมพิวเตอร์และระบบโทรคมนาคมโดยผิดกฎหมายซึ่งได้รับการคุ้มครองโดย“ มาตรการรักษาความปลอดภัย บทบัญญัติของมาตรา 1 มีเพื่อกำหนดเป้าหมายบุคคลที่ครอบครองข้อมูลที่มีผลต่อความมั่นคงของรัฐบาล บุคคลเหล่านั้นอาจจะถูกปราบปรามเนื่องจากข้อมูลเหล่านั้นได้มาจากการละเมิดมาตรการรักษาความปลอดภัย (Free Word Centre, 2012)

มาตรา 2 อาชญากรรมไซเบอร์ที่เกี่ยวข้องกับ "การสอดแนมที่ผิดกฎหมาย" โดยที่อาชญากรสามารถเข้าถึงเนื้อหาที่ผิดกฎหมายผ่านการสื่อสารแบบ "ไม่เปิดเผยต่อสาธารณะ" ทางคอมพิวเตอร์โทรคมนาคม มาตรานี้มีวัตถุประสงค์ป้องกันไม่ให้บุคคลใด ๆ ที่ไม่มีอำนาจสามารถดักฟังการสื่อสารระหว่างบุคคลหรือบุคคลสาธารณะ (Free Word Centre, 2012)

มาตรา 3 อาชญากรรมไซเบอร์ที่เกี่ยวข้องกับ “การจารกรรมคอมพิวเตอร์” ซึ่งอาชญากรสามารถเข้าถึงและแบ่งปันข้อมูลที่เป็นความลับของรัฐบาล โทษต่ำที่สุดของผู้กระทำผิดมาตรานี้จะถูกคุมขังขั้นต่ำเป็นระยะเวลา 3 -5 ปี และมากที่สุดคือ 10 – 15 ปี (Free Word Centre, 2012)

บทที่ 2 อาชญากรรมต่อความถูกต้องและแท้จริงของข้อมูลคอมพิวเตอร์และระบบโทรคมนาคม มาตรา 6 อาชญากรรมไซเบอร์ประกอบด้วยความผิดที่มี “การฉ้อโกง” โดยไม่ต้องมีการพิสูจน์ว่ามี

เจตนาหรือไม่ และข้อ 6a ที่เกี่ยวข้องกับข้อมูลที่ “เชื่อถือได้” ในขณะที่ 6b เกี่ยวข้องกับข้อมูลทั้งหมดที่มีอยู่บนหน่วยความจำส่วนกลาง หน่วยประมวลผล และชิปของคอมพิวเตอร์หรือระบบโทรคมนาคม (Free Word Centre, 2012)

มาตรา 9 อาชญากรรมทางไซเบอร์ในทางอาญาที่เกี่ยวข้องกับการถ่ายโอน แจกจ่าย ยับยั้ง หรือทำให้ข้อมูลของคอมพิวเตอร์หรือระบบโทรคมนาคมของผู้อื่นหรือทำให้การทำงานเสียหาย (Free Word Centre, 2012)

มาตรา 10 อาชญากรรมไซเบอร์ที่ปกปิดข้อมูล เปลี่ยนรหัสผ่านและ / หรือเข้ารหัสข้อมูลที่ปราศจากอำนาจในการเข้าถึงข้อมูลคอมพิวเตอร์และระบบโทรคมนาคมนั้น (Free Word Centre, 2012)

บทที่ 3 ข้อบังคับอื่น ๆ

มาตรา 52 มอบหมายให้กระทรวงยุติธรรมและกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารมีภารกิจในการพัฒนาความร่วมมือระหว่างประเทศในการก่ออาชญากรรมคอมพิวเตอร์ (Free Word Centre, 2012)

มาตรา 53 ในกรณีที่มีการใช้คอมพิวเตอร์หรือระบบโทรคมนาคมในการก่ออาชญากรรมที่ไม่อยู่ภายใต้กฎหมายว่าด้วยอาชญากรรมคอมพิวเตอร์ จะสามารถดำเนินการได้ตามกฎหมายอาญาที่มีอยู่ มาตรา 53 แสดงให้เห็นว่าอิหร่านมีวิธีการทางเลือกมากมายในการจัดการกับผู้ที่กระทำความผิดเกี่ยวกับคอมพิวเตอร์ด้วย การแก้ไขกฎหมายปฏิรูปรัฐธรรมนูญของอิหร่านกฎหมายสื่อมวลชนปี 1986 และประมวลกฎหมายอาญาอิสลาม (Free Word Center, 2012)

ในภาพรวมแล้วกฎหมายที่อิหร่านได้กำหนดไว้ ยังไม่มีคำนิยามที่ชัดเจนเกี่ยวกับการเข้าถึงข้อมูลหรือระบบคอมพิวเตอร์โดยทางที่มิชอบด้วยกฎหมาย ข้อมูลที่เป็นความลับและการขัดขวางการทำงานของระบบคอมพิวเตอร์ และส่งผลให้เกิดปัญหาที่ตามมาในการตีความทางกฎหมาย มากไปกว่านั้นในตัวบทกฎหมายยังปรากฏให้เห็นอีกว่า กฎหมายอาชญากรรมไซเบอร์ไม่ได้ระบุถึงโทษของอาชญากรที่มีเจตนาหรือไม่มีเจตนาเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ ดังนั้นโทษที่ใช้สำหรับการกระทำทั้งสองประเภทจึงมีระดับเดียวกัน (Free Word Center, 2012)

2.8.8 การก่อการร้ายไซเบอร์ในประเทศรัสเซีย

รัสเซียเป็นอีกประเทศหนึ่งที่ถูกกล่าวหาบ่อยครั้งว่าเป็นผู้ใช้ไซเบอร์ในการรุกรานชาติอื่นก่อน โดยเฉพาะการโจมตีที่จะต้องอาศัยผู้เชี่ยวชาญระบบคอมพิวเตอร์โดยเฉพาะการเจาะระบบแบบ DoS ใช้เทคนิคโฆษณาชวนเชื่อในสมัยสงครามเย็น เป็นการแพร่กระจายข่าวลวงผ่านระบบอินเตอร์เน็ต สนับสนุนกลุ่มตน มีการใช้เทคโนโลยีที่ชื่อว่า “SORM” ซึ่งเป็นการก่อกวนกลุ่มผู้ที่ไม่เห็นด้วยกับรัฐบาลด้านไซเบอร์ สำหรับรัสเซียนั้นรัฐบาลมีศักยภาพมากในการควบคุมเทคโนโลยีไซเบอร์ เพราะฉะนั้นหากมีการก่อกวนจากกลุ่มชน รัฐบาลจะเป็นผู้แสดงและตรวจจับผู้ที่ปลุกปั่น การดำเนินการดังกล่าวเป็นของหน่วยงานข่าวกรองสัญชาติรัสเซีย เป็นหน่วยงานด้านความมั่นคงของมีชื่อเรียกว่า Federal Security Service: FSB ซึ่งในอดีตเคยเป็นส่วนหนึ่งของแผนกที่ 16 ของหน่วยเคจีบี (KGB) ในขณะที่หน่วยงานอื่น ๆ อยู่ภายใต้การควบคุมของกระทรวงมหาดไทยและกิจการทางทหารของรัสเซีย

การก่อการร้ายที่รัสเซียแตกต่างจากประเทศอื่น เนื่องจากรัสเซียเป็นประเทศสหพันธรัฐการเกิดความร่วมมือกับประเทศเพื่อนบ้านซึ่งเคยเป็นหนึ่งในประเทศโซเวียต จึงเป็นเรื่องง่ายที่รัสเซียจะพัฒนาความก้าวหน้าทางไซเบอร์ ยกตัวอย่างการเกิดการก่อการร้ายในรูปแบบไซเบอร์ของประเทศลัตเวีย โดยในการก่อการร้ายนั้นไม่ได้เป็นการก่อการร้ายแบบองค์กรอาชญากรรมแต่เป็นการก่อการร้ายในระดับบุคคลที่มีความร่วมมือและเต็มใจที่จะช่วยรัสเซีย การก่อการร้ายครั้งนี้มุ่งโจมตีประเทศจอร์เจีย โดยประเทศอเมริกาได้ให้ข้อสังเกตว่าการจู่โจมมาจากคอมพิวเตอร์ส่วนบุคคล ไม่มีส่วนเกี่ยวข้องใด ๆ กับภาครัฐของรัสเซียที่ถูกกล่าวหา นอกจากนี้ยูเครนและลัตเวียยังร่วมมือให้การช่วยเหลือรัสเซียในสงคราม South Ossetia War ในปี 2008 การโจมตีจะใช้กองทัพซอมบี้ (Zombie Army) โดยอาศัยนักเจาะระบบคอมพิวเตอร์ที่จะถูกควบคุมโดยหน่วยงานลับหลายหน่วยงาน เช่น ในเหตุการณ์จับตัวประกันในโรงหนังกลางกรุงมอสโคว์ ในปี 2002 โดยรัสเซียได้ใช้อาวุธไซเบอร์ที่เรียกว่า “Snake” จะทำให้เกิดความเสียหายต่อระบบเครือข่ายของรัฐ Hacker ชาวรัสเซียจะแสวงหาประโยชน์จากข้อบกพร่อง (Bug) ในโปรแกรม Microsoft Windows และโปรแกรมอื่น ๆ เพื่อหาความลับที่รัฐบาลเก็บไว้ สิ่งเหล่านี้เกิดขึ้นกับองค์การ นาโต้ (NATO) สหภาพยุโรป (European Union) และบริษัทต่าง ๆ ที่อยู่ในสายพลังงานและโทรคมนาคม ด้วยเหตุนี้ทำให้เชื่อได้ว่าเหตุการณ์ไฟฟ้าดับในยูเครนเกิดจากการโจมตีด้านไซเบอร์ของรัสเซีย มีรัฐบาลรัสเซียอยู่เบื้องหลัง การกระทำครั้งนี้ใช้การโจมตีแบบ Malware เข้าทำลายเครือข่ายระบบไฟฟ้าของยูเครนในเดือนธันวาคม ปี 2005 (กรมพัฒนาสังคมและสวัสดิการ, 2563)

2.8.8.1 การรับมือก่อการร้ายไซเบอร์ของประเทศรัสเซีย

ประเทศรัสเซียมีนโยบาย ITC Security หรือ การรักษาความปลอดภัย Information-Communication Technology ที่เป็นปัจจัยหนึ่งที่จะทำให้เศรษฐกิจของรัสเซียมีความมั่นคงและน่าเชื่อถือ มีนโยบายถือเก็บทะเบียนรายชื่อของผู้ที่เป็นนักเจาะระบบคอมพิวเตอร์ของรัสเซียไว้เพื่อสามารถควบคุมมิให้เกิดการจู่โจมจากกลุ่มคนเหล่านั้น แต่ยังไม่สามารถทำได้อย่างสมบูรณ์เพราะในบางครั้งยังยากที่จะหาหลักฐานในการจับกุมและไม่สามารถตามรอยผู้ใช้ได้ การวิเคราะห์ทางสถิติของรัสเซียแสดงให้เห็นว่า รัสเซียมีแนวโน้มการโจมตีในระบบดิจิทัลสูงขึ้น ในช่วง 17 ปีที่ผ่านมา (2001-2018) จำนวนอาชญากรรมที่ใช้เทคโนโลยีการสื่อสารโทรคมนาคมเพิ่มขึ้นจาก 1,300 เป็น 174,674 ครั้ง จนถึงปัจจุบัน มีการลงทะเบียนความผิดทางอาญา 97,524 ครั้งซึ่งมากกว่าร้อยละ 53 ในปี 2018 ส่วนใหญ่ระบุว่าเป็นการฉ้อโกง (ร้อยละ 52) การโจรกรรม (ร้อยละ 19) และการค้ายาเสพติด (ร้อยละ 11) นอกจากนี้ยังมีการเข้าถึงข้อมูลคอมพิวเตอร์ การสร้างและแจกจ่ายซอฟต์แวร์ที่เป็นอันตราย การบุกรุกระบบชำระเงินทางอิเล็กทรอนิกส์ และการแจกจ่ายสื่อลามกที่เกี่ยวข้องกับผู้เยาว์

เหตุที่เพิ่มขึ้นของการจู่โจมทางไซเบอร์นั้นเกิดจากการขยายตัวของอินเทอร์เน็ต ทำให้มีจำนวนผู้ใช้อินเทอร์เน็ตเพิ่มขึ้นอย่างมีนัยสำคัญจาก 35 ล้านคน ในปี 2007 เป็น 92.8 ล้านคนในปี 2018 หรือเพิ่มขึ้นจากร้อยละ 25 เป็นร้อยละ 76 ของประชากรประเทศ ในเมื่อปีที่แล้วการมีส่วนร่วมของอินเทอร์เน็ตรัสเซีย (RuNet) ต่อเศรษฐกิจของประเทศนั้นอยู่ที่ 4 ล้านล้านรูเบิลหรือ 60 ล้านดอลลาร์ตามที่สมาคมสื่อสารอิเล็กทรอนิกส์แห่งรัสเซียระบุปัญหาหลักของรัสเซียในการรับมือคือ การเพิ่มขึ้นของตัวแสดงภายนอกและการขาดผู้เชี่ยวชาญทางระบบดิจิทัลเฉพาะด้าน การประเมินนี้แสดงให้เห็นว่าทั้งระบบและผู้ประกอบการภาครัฐควรใช้มาตรการขั้นพื้นฐานบังคับดังนี้

1) เพิ่มความปลอดภัยของโครงสร้างพื้นฐานข้อมูลที่สำคัญและความมั่นคงของการทำงาน

2) เพิ่มการคุ้มครองประชาชนจากเหตุฉุกเฉินที่เกิดจากจู่โจมเทคโนโลยีสารสนเทศและโครงสร้างพื้นฐานที่สำคัญ

3) ปรับปรุงการป้องกันอาชญากรรมที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและโครงสร้างพื้นฐานที่สำคัญและต่อต้านการละเมิดดังกล่าว

ในเดือนพฤษภาคม 2562 ประธานาธิบดี วลาดิมีร์ ปูติน ได้ลงนามใน “Internet Isolation Bill” ซึ่งมีไว้เพื่อความมั่นคงของระบบอินเทอร์เน็ตในรัสเซียในกรณีที่ถูกตัดการเชื่อมต่อจาก World Wide Web มาตรการนี้มีผลบังคับใช้ในวันที่ 1 พฤศจิกายน 2019 กำหนดให้ผู้ให้บริการอินเทอร์เน็ตติดตั้งอุปกรณ์เพื่อกำหนดเส้นทางการเข้าชมเว็บของรัสเซียผ่านเซิร์ฟเวอร์ในประเทศ ข้อดีของ “Internet Isolation Bill” อาจทำหน้าที่รักษาความปลอดภัยทางดิจิทัลจากการประกอบความผิดทางอาญา แต่ในขณะเดียวกันก็เป็นการจำกัดการเข้าถึงพื้นที่ข้อมูลระหว่างประเทศ รัสเซียเป็นประเทศเดียวที่เข้าร่วมในสภายุโรปที่ไม่ได้ลงนามในอนุสัญญาบูดาเปสต์ว่าด้วยอาชญากรรมไซเบอร์ (EST ฉบับที่ 185, 2001) เหตุผลหลักคือการที่ Paragraph 32 ของอนุสัญญาอนุญาตให้มีการเข้าถึงข้อมูลคอมพิวเตอร์ในลักษณะเฉพาะทางทางอาชญากรรมและความมั่นคงทางไซเบอร์โดยหน่วยข่าวกรองของประเทศอื่น ๆ ทำให้รัสเซียต้องเตรียมร่างอนุสัญญาฉบับใหม่เพื่อมาแก้ไขและเสนอต่อสมัชชาใหญ่แห่งสหประชาชาติเกี่ยวกับการต่อต้านอาชญากรรมทางดิจิทัล โดยทั้งนี้สหประชาชาติได้ให้การรับรองมติที่เสนอโดยรัสเซีย ภายใต้ชื่อ “Countering the use of information and communications technologies for criminal purposes” มีจุดมุ่งหมายเพื่อปกป้องข้อมูลที่เรียกว่าสิทธิพิเศษของรัฐในขณะที่ส่งเสริมฉันทามติระดับโลกและการหาแนวทางที่เป็นรูปธรรมและในทางปฏิบัติเพื่อต่อต้านอาชญากรรมไซเบอร์ ในเวลาต่อมา สนธิสัญญา “Cooperation in Combating Cybercrime” ถูกลงนามตามมาในเดือนกันยายน 2018 เพื่อที่จะสร้างความมั่นใจว่า

ระบบการป้องกันและระบบการตรวจจับ การสอบสวนมีประสิทธิภาพ นอกจากนี้ยังมีการกำหนดรูปแบบหลักของความร่วมมือซึ่งกันและกันคือการแลกเปลี่ยนข้อมูลเกี่ยวกับการจู่โจมที่เกิดขึ้น เพื่อช่วยในการรับมือการโจมตี และการดำเนินงานพิเศษด้านความช่วยเหลือในการฝึกอบรมและพัฒนาวิชาชีพของเจ้าหน้าที่บังคับใช้กฎหมาย (Sukharenko, 2019)

ความแตกต่างของการให้ความหมายของคำว่าการก่อการร้ายไซเบอร์ของรัสเซียคือ การมุ่งเน้นไปยังสงครามและการก่อการร้ายเชิงข้อมูลข่าวสาร หรือ Information Warfare ซึ่งเป็นปัจจัยที่มีพลังสำหรับการก่อการร้ายไซเบอร์ หากฝ่ายใดควบคุมข้อมูลข่าวสารได้ ฝ่ายนั้นก็จะเป็นผู้ชนะ โดยรัฐบาลรัสเซียจะใช้กลยุทธ์ในแบบ Defensive Action ปกป้องข้อมูลข่าวสาร โดยเฉพาะบทบาทของ Social Media ที่รัฐบาลจะต้องคอยระวังการที่ศัตรูจะมาในรูปแบบของการโฆษณาชวนเชื่อและการบิดเบือนข้อมูลข่าวสาร ตามที่ได้กล่าวไว้ข้างต้น รัสเซียออกข้อห้ามจำกัดการไม่มีตัวตนในอินเทอร์เน็ต (Anonymity) รัฐบาลรัสเซียใช้เทคโนโลยีที่เพื่อจำกัดเนื้อหาและการไหลของข้อมูลภายในระบบไซเบอร์ของรัสเซีย รัฐบาลรัสเซียสามารถกรองเนื้อหาเว็บไซต์ได้และมีข้อห้ามไม่ให้เด็กสามารถเข้าถึงอินเทอร์เน็ต รัฐบาลรัสเซียได้ออกกฎหมายเปิดใช้งาน “Roskomnadzor” (Medvedev, 2015) เพื่อขึ้นบัญชีดำสำหรับเว็บไซต์ของผู้กระทำความผิด ภายใน 3 ปีหลังจากนั้น รัฐบาลได้ขยายอำนาจเพื่ออนุญาตให้มีการปิดเว็บไซต์ที่ถือว่าเป็นภัยคุกคามต่อชาติ รัสเซียมีมาตรการในการรับมือที่เป็นแนวคิดหลักสามารถแบ่งออกมาได้ 4 ประการ ดังนี้

1) เพิ่มความรู้ในโลกไซเบอร์ให้กับประชาชน (การตระหนักถึงภัยคุกคามและวิธีการป้องกันระบบ)

2) การบังคับเปิดเผยข้อมูลที่เกี่ยวกับเหตุการณ์ไซเบอร์ที่เป็นประเด็นความมั่นคงระดับชาติ

3) การปรับปรุงกระบวนการช่วยเหลือทางกฎหมายระหว่างประเทศและระดับชาติ การออกกฎหมายเกี่ยวกับองค์ประกอบของการก่อการร้ายไซเบอร์และขั้นตอนการสืบสวน

4) การขยายความร่วมมือแบบสามทางระหว่าง บริษัท / องค์กรไซเบอร์ผู้เชี่ยวชาญด้านความปลอดภัยและหน่วยงานบังคับใช้กฎหมาย

2.8.8.2 กฎหมายควบคุมไซเบอร์ของประเทศรัสเซีย

ความหมายเกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของรัสเซีย ถูกเขียนไว้ในประมวลกฎหมายอาญาเป็นกลุ่มของฐานความผิดในหมวดที่เกี่ยวข้องกับความผิดต่อความสงบเรียบร้อยของสาธารณะประกอบไปด้วย 3 ฐานความผิด ดังนี้

1) มีองค์ประกอบความผิดคือ ผู้ใดเข้าถึงข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกัน หากการกรทำนั้นมีลักษณะของการทำลาย สกัดกั้น แก้ไข ทำสำเนาข้อมูลคอมพิวเตอร์

2) มีองค์ประกอบความผิดคือ สร้างใช้เผยแพร่ โปรแกรมหรือข้อมูลคอมพิวเตอร์อื่น ซึ่งทำให้เกิดความเสียหาย สกัดกั้น แก้ไข สำเนา ข้อมูลคอมพิวเตอร์ หรือทำให้ระบบรักษาความมั่นคงปลอดภัยเสียหายไม่สามารถใช้งานได้

3) มีองค์ประกอบความผิดคือ ฝ่าฝืนกฎเกณฑ์ ในการปฏิบัติงานที่เกี่ยวกับการประมวลข้อมูลคอมพิวเตอร์หรือฝ่าฝืนกฎเกณฑ์เกี่ยวกับการทำงานของระบบโทรคมนาคมและการสื่อสาร โดยการกระทำนั้นทำให้เกิดความเสียหาย สกัดกั้น แก้ไข สำเนา ข้อมูลคอมพิวเตอร์

กฎหมายที่เกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ของรัสเซียครอบคลุมถึงการเฝ้าระวังโปรแกรมคอมพิวเตอร์ที่จะก่อให้เกิดความเสียหายต่อระบบ ไม่ว่าจะเป็นมัลแวร์ (Malware) การโจมตีผ่าน Denial of Service-DDOS โดยกฎหมายของรัสเซียนั้นจะไม่แบ่งแยกฐานความผิดที่มุ่งทำลายข้อมูลและมุ่งทำลายระบบ ถือว่าความผิดทั้งสองประเภทนั้นอยู่ในฐานเดียวกัน (คณาธิป ทองรวีวงศ์, 2563)

2.8.9 การวิเคราะห์ความเหมือนและแตกต่างของสถานการณ์และการรับมือภัยคุกคามทางไซเบอร์ในต่างประเทศและประเทศไทย

จากการศึกษาสถานการณ์การก่อการร้ายไซเบอร์พร้อมด้วยการเตรียมการรับมือภัยคุกคามที่กำลังเกิดขึ้นในประเทศต่าง ๆ ที่ผู้วิจัยได้เลือกสรรมาศึกษาเพราะมีความโดดเด่นในเรื่องของเทคโนโลยีผสานกับระบบการปกครองของประเทศนั้น ๆ ที่จะนำไปสู่การตัดสินใจที่จะออกนโยบายเพื่อเตรียมพร้อมและป้องกันไม่ให้เกิดการก่อการร้ายไซเบอร์ที่มีผลกระทบมหาศาล ในที่นี้ผู้วิจัยเลือกศึกษาประเทศที่มีศักยภาพทางเทคโนโลยี เช่น สหรัฐอเมริกา สหราชอาณาจักร ที่เป็นประเทศมหาอำนาจ มีระบบการปกครองเป็นแบบประชาธิปไตย มีการออกนโยบายการตั้งรับอย่างชัดเจนเน้นการกระจายตัวของการตั้งรับโดยรัฐบาลมีบทบาทสำคัญในการควบคุม แต่ภาคเอกชนและประชาชนก็มีบทบาทไม่น้อยไปกว่ารัฐในการสนับสนุนเทคโนโลยีที่ทันสมัย ให้ความสำคัญกับประเด็นความมั่นคงแห่งรัฐและความส่วนตัวของประชาชนทัดเทียมกัน ประเทศที่มีลักษณะในการรับมือภัยคุกคามไซเบอร์ที่คล้ายกับสองประเทศข้างต้นนั้น คือ ประเทศสิงคโปร์ ที่มีแนวโน้มจะพัฒนาศักยภาพด้านเทคโนโลยีให้ทัดเทียมกับประเทศมหาอำนาจ ถึงแม้สิงคโปร์จะเป็นประเทศเล็ก ๆ แต่ก็สามารถพัฒนาบุคลากรให้มีความพร้อมเพียงพอที่จะรับมือภัยคุกคามเฉกเช่นสองประเทศที่กล่าวมาได้ ส่วนประเทศรัสเซีย เกาหลีเหนือ จีน และอิหร่านนั้น มีความพร้อมทางเทคโนโลยีไม่น้อยไปกว่าประเทศมหาอำนาจอื่น ๆ แต่สิ่งที่แตกต่างออกไปคือนโยบายทางไซเบอร์ของประเทศเหล่านี้จะมีลักษณะเชิงรุก มากกว่าที่จะตั้งรับ โดยหากพิจารณาถึงโครงสร้างของหน่วยงานที่ดูแลควบคุมระบบไซเบอร์ของกลุ่มประเทศนี้จะมีลักษณะของเส้นสายบังคับบัญชาที่ชัดเจน โดยส่วนมากผู้นำสูงสุดจะเป็น

ผู้บังคับบัญชาและสามารถสั่งการได้อย่างเด็ดขาด ทำให้ลักษณะของกองกำลังมีความเข้มแข็ง รัฐบาลจะให้ความเข้มข้นในการคัดสรรกำลังคนที่มีความสามารถเพื่อเข้ามาอบรม บางครั้งอาจส่งบุคลากรของตนไปเรียนรู้กับประเทศเพื่อนบ้านที่เป็นพันธมิตรกัน ประเทศเหล่านี้มักจะมีกรอบความร่วมมือเฉพาะกลุ่มประเทศพันธมิตรของตนเอง เช่น เกาหลีเหนือกับจีน รัสเซียและกลุ่มประเทศโซเวียต อิหร่านและกลุ่มประเทศในตะวันออกกลาง สำหรับกลุ่มประเทศในเอเชียใต้ เช่น อินเดีย ศรีลังกา นั้นมีความคุ้นชินและเชี่ยวชาญกับระบบไซเบอร์ ทำให้การพัฒนานโยบายเป็นเรื่องที่ต่อเนื่อง การก่อการร้ายที่ Mumbai ทำให้อินเดียมีความตื่นตัวในเรื่องการก่อการร้ายไซเบอร์มากขึ้น รัฐบาลอินเดียให้ความสนใจในการพัฒนาระบบกฎหมายเพื่อสามารถนำมาใช้จัดการกับผู้ก่อการร้ายไซเบอร์ได้

สำหรับประเทศไทยนั้นถือว่าเป็นการเริ่มต้นใหม่ในยุคดิจิทัล การเปลี่ยนแปลงของไทยเห็นได้ชัดจากนโยบายไทยแลนด์ 4.0 ที่พยายามผลักดันการดำเนินการของรัฐเกือบทุกประเภทให้อยู่ในระบบดิจิทัล แต่ทั้งนี้ประเทศไทยยังไม่มีความพร้อมที่จะรับมือกับภัยคุกคามที่จะเกิดขึ้นในระบบไซเบอร์ได้อย่างเต็มรูปแบบ เพราะไม่ว่าจะเป็นผู้เชี่ยวชาญทางไซเบอร์ที่มีน้อย การขาดความตระหนักรู้ในเรื่องการก่อการร้ายไซเบอร์และภัยคุกคามในรูปแบบต่าง ๆ ทำให้บางหน่วยงานละเลยที่จะออกนโยบายจริงจังกับเรื่องเหล่านี้ แต่อย่างไรก็ตามในช่วงสองถึงสามปีที่ผ่านมา รัฐบาลเริ่มมีการจัดตั้งหน่วยงานที่จะเข้ามากำกับควบคุมระบบไซเบอร์ที่ชัดเจน ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย หรือ “ไทยเซิร์ต” (Thailand Computer Emergency Response Team: ThaiCERT) ถือเป็นการผลักดันระบบการรักษาความปลอดภัยที่ควบคู่กันไปกับการพัฒนาในระบบ 4.0 บุคลากรของไทยได้รับการส่งเสริมมากขึ้นในด้านเทคโนโลยีพื้นฐานเพื่อให้มีความรู้เบื้องต้นในการจัดการกับภัยคุกคามที่อาจจะเกิดขึ้นได้ ในส่วนเรื่องกฎหมาย รัฐบาลได้พยายามกำหนดบทลงโทษผ่านทางพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ว่าผู้ที่กระทำความผิดผ่านการใช้คอมพิวเตอร์จะต้องได้รับโทษไม่ต่างจากผู้กระทำผิดแบบดั้งเดิม เพื่อให้การอธิบายสถานการณ์ภัยคุกคามไซเบอร์ที่ประเทศไทยต้องเผชิญและเปรียบเทียบความพร้อมในการรับมือภัยคุกคามกับต่างประเทศ ผู้วิจัยจึงขอยกตารางข้อปฏิบัติที่ประเทศไทยและต่างประเทศใช้ดำเนินการ ดังนี้

ตารางที่ 4 ข้อปฏิบัติที่ประเทศไทยและต่างประเทศ

ข้อปฏิบัติ	Singapore	North Korea	South Asia	US	UK	Iran	Russia	Thailand
ความตระหนักรู้และการอบรม	/	/	/	/	/	/	/	/
ความต่อเนื่องของแผนยุทธศาสตร์	/	-	/	/	-	/	/	-
ความปลอดภัยของข้อมูล	/	/	-	-	/	-	/	-
ระบบปฏิบัติการต่อต้านการก่อการร้ายไซเบอร์	/	-	/	/	/	/	/	/
การบูรณาการข้อมูลระหว่างหน่วยงาน	/	/	-	/	/	-	/	-
การบริหารจัดการวิกฤติ	/	/	/	/	/	-	/	/
การส่งเสริมความร่วมมือกับกันระหว่างประเทศ	/	/	/	/	/	-	-	/
การบังคับใช้กฎหมายไซเบอร์	/	/	/	/	/	/	/	/

2.9 สถานการณ์และยุทธศาสตร์การต่อต้านการก่อการร้ายไซเบอร์ของประเทศไทย (Cyber Security Situation and Strategies for Thailand)

ประเทศไทยเป็นประเทศหนึ่งที่มีผู้ใช้อินเทอร์เน็ตกว่าร้อยละ 70 ของประชากรทั้งหมด และโครงสร้างสาธารณูปโภคพื้นฐานของประเทศส่วนใหญ่ขึ้นอยู่กับระบบดิจิทัล เมื่อพิจารณาแผนนโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม ดังนี้

1. ผลักดันให้พัฒนาโครงสร้างพื้นฐานดิจิทัลประสิทธิภาพสูงให้ครอบคลุมทั่วประเทศ
2. ขับเคลื่อนเศรษฐกิจด้วยเทคโนโลยีดิจิทัล
3. สร้างสังคมคุณภาพที่ทั่วถึงเท่าเทียมด้วยเทคโนโลยีดิจิทัล
4. ปรับเปลี่ยนภาครัฐสู่การเป็นรัฐบาลดิจิทัล
5. พัฒนากำลังคนให้พร้อมเข้าสู่ยุคเศรษฐกิจและสังคมดิจิทัล
6. สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล

จะเห็นได้ว่าแผนทั้งหมดที่วางไว้เป็นการพยายามผลักดันให้การบริหารภาครัฐทั้งหมดเข้าสู่ระบบดิจิทัล ในกรณีนี้จึงเกิดประเด็นคำถามว่าประเทศไทยมีความพร้อมหรือความตระหนักรู้เพียงพอหรือไม่กับการเข้าสู่สังคมดิจิทัลอย่างเต็มรูปแบบ ดังนั้นในส่วนนี้จะนำเสนอถึงแผนการเตรียมความพร้อมและการรับมือกับภัยคุกคามทางไซเบอร์ของแต่ละหน่วยงานที่มีความเสี่ยงต่อการโจมตี

รัฐบาลไทยได้ประกาศใช้ระเบียบสำนักนายกรัฐมนตรีว่าด้วยคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560 เพื่อการเตรียมการเพื่อรับมือกับการโจมตีไซเบอร์ในภาครัฐ ภาคเอกชน และภาคประชาสังคม โดยมีมาตรการป้องกัน ดังนี้

1. รัฐบาลได้แต่งตั้งกรรมการผู้ทรงคุณวุฒิในคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เมื่อวันที่ 24 เมษายน 2561

2. รัฐบาลได้ยกร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... ซึ่งคณะรัฐมนตรีมีมติอนุมัติหลักการร่างพระราชบัญญัติฉบับนี้เมื่อวันที่ 6 มกราคม 2558 และการเสนอร่างกฎหมายตามบทบัญญัติมาตรา 77 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560

3. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้จัดประชุมคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ครั้งที่ 1/2561 โดยมีพลเอก ประยุทธ์ จันทร์โอชา นายกรัฐมนตรี เป็นประธานในการประชุมครั้งนี้ได้พิจารณาใน 4 ประเด็น คือ

1) กรอบแนวคิดนโยบายและแผนระดับชาติ เพื่อปกป้อง รับมือ ป้องกัน และลดความเสี่ยง และให้มีความสอดคล้องไปในทิศทางเดียวกัน

2) แนวทาง การกำหนดโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศและแนวปฏิบัติเพื่อตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์

3) แนวทางการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ระยะเร่งด่วน

4) แนวทางการจัดตั้งหน่วยประสานงานกลางและหน่วยงานเผชิญเหตุด้านความมั่นคงปลอดภัยไซเบอร์ชั่วคราว เพื่อให้ความมั่นคงปลอดภัยไซเบอร์ของชาติอยู่ในระดับมาตรฐานสากล

จากการประชุมสามารถสรุปผลในการดำเนินการได้ ดังนี้

1. มีมติเห็นชอบให้จัดกลุ่มโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (Critical Information Infrastructure: CII) 6 กลุ่ม (อริย์ธัช แก้วเกาะสะบ้า, 2558) คือ

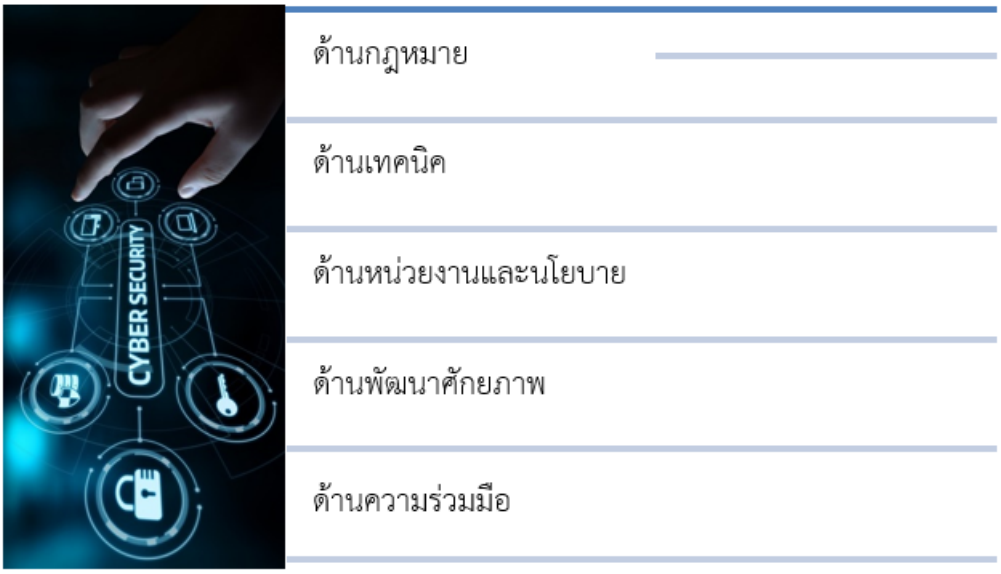
รูปที่ 11 กลุ่มโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ
(Critical Information Infrastructure: CII)
ที่มา: อริย์ธัช แก้วเกาะสะบ้า (2558)

2. ยกระดับการพัฒนาบุคลากรทางด้านไซเบอร์ มีการเตรียมความพร้อมยกระดับแผนการทำงาน ร่วมกัน 8 ด้าน ที่สอดคล้องกับแผนยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560-2564 (อริย์ธัช แก้วเกาะสะบ้า, 2558) คือ

รูปที่ 12 การเตรียมความพร้อมยกระดับแผนการทำงาน ร่วมกัน 8 ด้าน

ที่มา: อริย์ธัช แก้วเกาะสะบ้า (2558)

3. ประเทศไทยได้ถูกจัดการจัดอันดับด้านความมั่นคงปลอดภัยไซเบอร์เปรียบเทียบในระดับนานาชาตินั้น ในปี 2560 สหภาพโทรคมนาคมระหว่างประเทศได้สำรวจระดับความจริงจัง ในการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ของแต่ละประเทศ โดยพิจารณาจากมาตรการ 5 ด้าน (อริย์ธัช แก้วเกาะสะบ้า, 2558) ได้แก่



รูปที่ 13 มาตรการ 5 ด้านของความมั่นคงปลอดภัยไซเบอร์ของแต่ละประเทศ
ที่มา: อริย์ธัช แก้วเกาะสะบ้า (2558)

ซึ่งพบว่า ประเทศไทยอยู่ในอันดับที่ 22 จาก 194 ประเทศ ขณะเดียวกันเปรียบเทียบกับประเทศสมาชิกในกลุ่มอาเซียน ประเทศไทยอยู่อันดับที่ 3 รองจากประเทศสิงคโปร์ และประเทศมาเลเซีย ซึ่งกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และหน่วยงาน ที่เกี่ยวข้องจะช่วยกันขับเคลื่อนให้ประเทศไทยอยู่ใน 20 อันดับแรกของประเทศที่มีความพร้อมด้านไซเบอร์

1) ด้านการพัฒนาบุคลากรความมั่นคงปลอดภัยไซเบอร์ ประเทศไทยได้รับการสนับสนุนจากประเทศญี่ปุ่นเป็นอย่างมาก โดยได้จัดตั้ง “ศูนย์ความร่วมมืออาเซียน-ญี่ปุ่น เพื่อพัฒนาบุคลากรความมั่นคงปลอดภัยไซเบอร์ (ASEAN-Japan Cyber security Capacity Building Centre) ประเทศไทยยังได้รับเลือกให้เป็นเจ้าภาพจัดตั้งศูนย์ฯ ตามมติที่ประชุม TELMIN-Japan และได้มีการเปิดศูนย์ความร่วมมืออาเซียน-ญี่ปุ่น อย่างเป็นทางการเมื่อเดือนมิถุนายน พ.ศ. 2561 ซึ่งเจ้าภาพหลักในการดำเนินงานได้มอบหมายให้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมและสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ หรือ ETDA เป็นผู้ดำเนินการ ทั้งนี้โดยได้รับการสนับสนุนจากประเทศญี่ปุ่นทั้งด้านงบประมาณและองค์ความรู้ต่าง ๆ ด้วยเหตุนี้ประเทศไทยจึงได้รับการพัฒนาให้ประเทศที่อยู่ในอันดับที่ 20 ของโลกที่มีความจริงจังทางด้านไซเบอร์ และสามารถผลิตบุคลากรที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยทางไซเบอร์เพิ่มขึ้นอีก 1,000 คน โดยความร่วมมือของภาครัฐ ภาคเอกชน และสถาบันการศึกษา

2) การสร้างหน่วยงานประสานงานกลาง โดยมอบหมายให้สานักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ทำหน้าที่เป็นหน่วยประสานงานกลางเป็นการชั่วคราวระหว่างจัดตั้ง (Cyber Security Agency) เพื่อรับมือกับภัยคุกคามทางไซเบอร์ และทางานร่วมกับหน่วยงานที่เกี่ยวข้อง ลดความเสี่ยงจากการถูกโจมตีทางไซเบอร์ (อริย์ธัช แก้วเกาะสะบ้า, 2558)

เพื่อให้การศึกษาเป็นไปตามวัตถุประสงค์ที่วางไว้ เพื่อที่จะศึกษาสถานการณ์ไซเบอร์ในประเทศไทยให้มีความลึกซึ้งมากขึ้นและเข้าใจถึงสถานการณ์การเตรียมพร้อมรับมือของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ (Critical National Infrastructure) และหน่วยงานที่มีหน้าที่หลักในการป้องกันและรักษาความมั่นคงทางไซเบอร์ รวมไปถึงการตระหนักรู้ของบุคลากรทุกระดับ การวิเคราะห์วรรณกรรมในบทนี้จะขอแสดงการเตียมพร้อมรับมือภัยคุกคามทางไวเบอร์ซึ่งแสดงให้เห็นถึงความตระหนักรู้ของหน่วยงานที่มีความเสี่ยงสูง ที่ผู้วิจัยได้เลือกศึกษาทั้งหมด 8 หน่วยงาน ได้แก่ สภาความมั่นคงแห่งชาติ ธนาคารแห่งประเทศไทย หน่วยงานกำกับดูแลกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ การไฟฟ้าส่วนภูมิภาค กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กระทรวงยุติธรรม กองทัพไทย กระทรวงสาธารณสุข ดังนี้

2.9.1 สภาความมั่นคงแห่งชาติ

สภาความมั่นคงแห่งชาติได้ประเมินสถานการณ์ปัจจุบันของประเทศไทย โดยประกอบไปด้วยการประเมินความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ทั้งหมด 5 ด้าน คือ ด้านความพร้อมด้านมาตรการทางกฎหมายและระเบียบปฏิบัติ ด้านความพร้อมด้านกลไกทางเทคนิคเพื่อรับมือกับภัยคุกคามทางไซเบอร์ ด้านความพร้อมทางด้านบุคลากร ด้านความพร้อมของระบบและเทคโนโลยี และด้านความพร้อมด้านงานสืบสวน งานการข่าวและการข่าวกรองทางไซเบอร์ มีรายละเอียด ดังนี้

2.9.1.1 ความพร้อมด้านมาตรการทางกฎหมายและระเบียบปฏิบัติ

ประเทศไทยมีความพร้อมด้านมาตรการทางกฎหมายและระเบียบปฏิบัติโดยมีกฎหมายหลายฉบับได้กำหนดมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไว้ แบ่งออกได้เป็น 3 กลุ่ม (สำนักงานสภาความมั่นคงแห่งชาติ, 2560) คือ

1) กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กำหนดไว้เพื่อลดความเสี่ยงและทำให้เกิดความน่าเชื่อถือเมื่อมีการใช้ระบบคอมพิวเตอร์หรือระบบอินเทอร์เน็ตในการทำธุรกรรมทางอิเล็กทรอนิกส์ซึ่งครอบคลุมทั้งในการพาณิชย์อิเล็กทรอนิกส์ รวมไปจนถึงการให้บริการทางอิเล็กทรอนิกส์ของรัฐหรือในงานรัฐบาลอิเล็กทรอนิกส์นั้นมีความมั่นคงปลอดภัย ตลอดจนกำหนดให้หน่วยงานที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศ (Critical Information Infrastructure Protection) ต้องปฏิบัติตามมาตรการด้านความมั่นคงปลอดภัย และต่อมาก็ได้มี

การตรากฎหมายจัดตั้งสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ. (Electronic Transactions Development Agency: ETDA) มีหน้าที่ในการกำกับดูแลและสนับสนุนการบริการต่าง ๆ ที่เกี่ยวข้องกับธุรกรรมออนไลน์ โดยยึดหลักตามกฎหมาย รวมถึงวิเคราะห์ และรับรองความสอดคล้องและถูกต้องตามมาตรฐานที่กำหนดไว้ รวมทั้งร่วมมือกับองค์กรหรือหน่วยงานทั้งในและต่างประเทศ นอกจากนี้ประเทศไทยยังมีความพยายามที่จะยกระดับทักษะผู้เชี่ยวชาญทางด้านความมั่นคงปลอดภัยไซเบอร์ รวมทั้งทำหน้าที่ดูแลศูนย์ประสานความมั่นคงปลอดภัยไซเบอร์ (ThaiCERT)

2) กฎหมายระดับอนุบัญญัติ เป็นกฎหมายลูกที่ดูแลการทำธุรกรรมด้านธุรกิจ การเงิน มีมาตรฐานการกำกับดูแลตลาดเงินโดยธนาคารแห่งประเทศไทยและตลาดทุนโดยสำนักงานคณะกรรมการหลักทรัพย์และตลาดหลักทรัพย์แห่งประเทศไทย รวมทั้งในการกำกับดูแลธุรกิจประกันภัยโดยสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เพื่อให้บริการของผู้ประกอบการในภาคเศรษฐกิจที่มีการกำกับดูแลนั้นมีความมั่นคงปลอดภัย

3) พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ซึ่งดูแลควบคุม ตั้งแต่การเข้าถึงระบบข้อมูลของผู้อื่นโดยมิชอบ แก้ไข บิดเบียนข้อมูลจนเป็นเหตุให้ผู้อื่นเสียหาย ส่งอีเมล์ spam รบกวนผู้อื่น หรือรบกวนระบบหน่วยงานจนเป็นเหตุให้หน่วยงานมิสามารถทำงานได้ ลักลอบเข้าระบบความมั่นคงของรัฐ นำข้อมูลที่ผิดกฎหมายมาเผยแพร่ โดยการกด Like หรือ Share ถือเป็นกระบวนการหนึ่งในการผลแพร่ ตัดต่อ บิดเบือนรูปภาพเป็นเหตุให้ผู้อื่นมีความรับรู้ที่ผิด แสดงความเห็นที่ผิดต่อ พ.ร.บ. ละเมิดลิขสิทธิ์ผลงานของผู้อื่น นอกจากนี้พระราชบัญญัติยังกำหนดบทลงโทษสำหรับผู้กระทำความผิดข้างต้น และมอบสำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นหน่วยงานที่คอยสอดส่องดูแลและป้องกันไม่ให้เกิดการกระทำความผิดทางไซเบอร์ซึ่งเป็นหน่วยงานหลักที่คอยกำกับดูแลในเชิงนโยบาย นอกจากนี้ยังมอบให้สำนักงานตำรวจแห่งชาติ โดยกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี กระทรวงยุติธรรม โดยสำนักคดีเทคโนโลยีและสารสนเทศสังกัดกรมสอบสวนคดีพิเศษ (DSI) สำนักงานป้องกันและปราบปรามการฟอกเงิน ส่วนตรวจสอบการกระทำความผิดทางเทคโนโลยีศูนย์เทคโนโลยีสารสนเทศ เป็นหน่วยงานลำดับถัดไปในการควบคุมดูแล

เห็นได้ว่าประเทศไทยมีความเตรียมพร้อมรับมือทางทางกฎหมายเพื่อลดการเกิดขึ้นของภัยคุกคามทางไซเบอร์ได้อย่างทันยุคทันสมัย แต่อย่างไรก็ตามยังไม่มีนโยบายส่งเสริมการสร้างผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยอย่างจริงจัง และยังขาดการกำหนดบทลงโทษที่ควบคุมจึงจำเป็นจะต้องยกระดับความเข้มแข็ง สร้างหน่วยงานความมั่นคงทางไซเบอร์โดยมีนโยบายและเป้าหมายเชิงรุกเพื่อเตรียมพร้อมสำหรับการทำสงครามไซเบอร์ในอนาคต ประเทศไทยยังต้องการผู้เชี่ยวชาญทางไซเบอร์ นักรบไซเบอร์เพื่อสร้างกองทัพไซเบอร์ที่เป็นรูปธรรม นอกจากนี้ยังต้องการ

เครือข่ายพันธมิตรไซเบอร์กับต่างชาติที่เหนียวแน่นเพื่อให้เกิดความยืดหยุ่นเมื่อมีภัยคุกคามเข้ามา เพราะภาวะวิกฤติเหล่านั้นอาจส่งผลกระทบอย่างมีนัยสำคัญและรุนแรง

ทั้งนี้ประเทศไทยควรกระชับสัมพันธ์ระหว่างพันธมิตรไซเบอร์ในภูมิภาคเอเชียและกลุ่มประเทศสมาชิกอาเซียน พร้อมสร้างบรรทัดฐานในการบริหารจัดการพื้นที่ทางไซเบอร์ให้ชัดเจนในระดับภูมิภาคต่อไป

2.9.1.2 ความพร้อมด้านกลไกทางเทคนิคเพื่อรับมือภัยคุกคามทางไซเบอร์

กลไกหรือเทคนิคเพื่อรับมือภัยคุกคามทางไซเบอร์ของแต่ละประเทศแตกต่างกันขึ้นอยู่กับสภาพความพร้อมของโครงสร้างทางดิจิทัล ประเทศไทยเป็นประเทศที่มีความพร้อมอยู่ในระดับกลาง เทคนิคการป้องกันเชิงรุกอย่างที่สหรัฐอเมริกาหรืออิหร่านนำมาใช้นั้นอาจจะยังไม่เหมาะสม แต่อย่างไรก็ตาม ประเทศไทยในฐานะที่เป็นประเทศสมาชิกขององค์กรด้านการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ทั้งในระดับภูมิภาค (APCERT/Asia Pacific Computer Emergency Response Team) และระดับสากล (FIRST/Forum of Incident Response and Security Teams) จึงได้ก่อตั้ง ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (The Computer Emergency Response Team) หรือ ThaiCERT มีภารกิจในการประสานงานระหว่างหน่วยงานต่างประเทศที่เป็นสมาชิกขององค์กรกับหน่วยงานในประเทศ ทั้งภาครัฐ เอกชน มหาวิทยาลัย ผู้ให้บริการอินเทอร์เน็ต หรือผู้เกี่ยวข้องในการตอบสนองและจัดการกับเหตุการณ์ความมั่นคงปลอดภัยที่ได้รับแจ้ง ในขณะนี้ ThaiCERT ถูกย้ายมาสังกัดอยู่ภายใต้ สำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์ หรือ สพธอ.

2.9.1.3 ความพร้อมทางด้านบุคลากร

ความพร้อมทางด้านบุคลากรจะมาพร้อมกับความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ทั้งในการปฏิบัติและด้านนโยบาย บุคลากรต้องความเชี่ยวชาญเฉพาะทางด้านเทคโนโลยี ซึ่งจากการศึกษาพบว่ากว่าร้อยละ 50 หน่วยงานรัฐและเอกชนยังไม่มีการจัดระบบที่พัฒนาบุคลากรให้มีความรู้เรื่องความมั่นคงปลอดภัยไซเบอร์ และให้บุคลากรยังไม่มีแรงจูงใจที่ต้องการเรียนรู้เรื่องของความมั่นคงปลอดภัยทางไซเบอร์ เช่น คอร์สเรียนเพื่อเสริมความสามารถและศักยภาพให้กับตนเอง เช่น เมื่อผ่านเกณฑ์การสอบวัดระดับความรู้เบื้องต้นในการรักษาความมั่นคงปลอดภัยไซเบอร์ก็จะต้องได้รับการยกย่อง หรือมีการปรับตำแหน่งให้พนักงานคนนั้น มากไปกว่านั้นควรต้องส่งเสริมให้มีการจัดสอบวัดระดับความรู้ที่ได้รับการยอมรับในระดับสากล และควรบรรจุไว้ให้กับหน่วยบริหารทรัพยากรส่วนบุคคลเพื่อไว้ใช้ในการพิจารณาคัดเลือกบุคลากรที่มีความสามารถในด้านนี้เข้ามาทำงาน สำนักงานคณะกรรมการข้าราชการพลเรือน (สำนักงาน ก.พ.) จำเป็นจะต้องมีส่วนร่วมในการบรรจุคุณสมบัติเหล่านี้ในการพิจารณาข้าราชการที่มีความเชี่ยวชาญเข้ามาเป็นส่วนหนึ่งของหน่วยงาน นอกจากนี้รัฐยังสามารถปรับปรุง Job Profiles ให้ทันสมัยและมี Digital Skills เป็นหนึ่งในทักษะพื้นฐาน กำหนด

ตำแหน่งหน้าที่ใหม่ที่สามารถสนับสนุนกลยุทธ์องค์กร เช่น data scientists, user interface designers, digital innovation manager เป็นต้น

2.9.1.4 ความพร้อมของระบบและเทคโนโลยี

ประเทศไทยมีนโยบาย “ประเทศไทย 4.0” เพื่อยกระดับความสามารถในการแข่งขันของประเทศ ซึ่งเป็นผลจากบทบาทของดิจิทัลที่เพิ่มขึ้นในด้านสังคมเศรษฐกิจและด้านเทคโนโลยี การเปลี่ยนแปลงสู่ยุค 4.0 นี้ เป็นการผสมผสานเทคโนโลยีการผลิตและเทคโนโลยีการสื่อสารเข้าด้วยกัน ได้แก่ Big Data and Analytics, Clouds, Internet of Things (IoT), Cyber Security, Simulation, Augmented Reality, Additive Manufacturing, Autonomous Robot, Horizontal and Vertical System Integration (จารุวัฒน์ เศวตพัชราภรณ์ & วรภพ ตันติวาณิชชากร, 2560) การเปลี่ยนแปลงสู่ยุค 4.0 ของประเทศไทยจะเน้นไปในส่วนของการกระตุ้นเศรษฐกิจ การใช้เทคโนโลยีลดต้นทุนในการผลิต เพื่อสามารถทำให้ผลิตสินค้าได้คุ้มทุนมากขึ้น ในด้านการเงิน ธนาคารแห่งประเทศไทยก็ตระหนักถึงภัยคุกคามทางไซเบอร์โดยได้กำหนดแบบประเมินความเสี่ยงทางไซเบอร์เพื่อให้องค์กรได้รู้จุดบกพร่องของตน และยกระดับการรักษาความปลอดภัยในส่วนตรงนั้นขึ้นได้ โดยธนาคารแห่งประเทศไทยได้ประเมินความเสี่ยงใน 2 ส่วนหลัก คือ ความเสี่ยงตั้งแต่ตั้งต้นด้านไซเบอร์ และ การบริหารจัดการความเสี่ยงและมาตรการควบคุมด้านการรักษาความปลอดภัยที่พึงมีจากการศึกษาจากนโยบายของหน่วยงานที่มีความเสี่ยงต่อการเป็นกลุ่มเป้าหมายของผู้ก่อการร้ายไซเบอร์ทำให้ทราบว่าหน่วยงานเหล่านี้มีความตระหนักรู้ถึงภัยไซเบอร์และมีวิธีเตรียมความพร้อมได้เป็นอย่างดี

2.9.1.5 ความพร้อมด้านงานสืบสวน

ประเทศไทยมีหน่วยงานด้านความมั่นคงหลายหน่วยงาน โดยแต่ละหน่วยงานนั้นมีความพยายามที่จะบูรณาการข้อมูลซึ่งกันและกัน ยกตัวอย่างเช่น งานข่าวกรองทางไซเบอร์กับตำรวจ งานด้านกระบวนการยุติธรรม การสอบสวนคดีพิเศษ ข้อมูลของผู้ต้องขัง ผู้ที่ถูกคุมประพฤติ ข้อมูลบางส่วนถูกบรรจุในฐานข้อมูล Big Data เพื่อสามารถที่จะนำข้อมูลเหล่านี้ไปวิเคราะห์และทำนายอนาคตได้อีกด้วย แต่อย่างไรก็ตามเมื่อบรรจุข้อมูลเหล่านี้ลงในพื้นที่ไซเบอร์ การตระหนักถึงความปลอดภัยของข้อมูลจึงเป็นสิ่งสำคัญ ดังนั้น ทั้งในเรื่องความปลอดภัยของข้อมูลส่วนตัวจะต้องไม่ให้เกิดการรั่วไหลออกไป (ธนาคารแห่งประเทศไทย, 2562)

2.9.2 ธนาคารแห่งประเทศไทย

ธนาคารแห่งประเทศไทยตระหนักดีว่าสถาบันทางการเงินใช้เทคโนโลยีเป็นหลักในการขับเคลื่อนประเทศ ทำให้ต้องเผชิญกับภัยไซเบอร์ที่ไม่สามารถหลีกเลี่ยงได้ ดังนั้นสถาบันการเงินอย่างธนาคารแห่งประเทศไทยจำเป็นจะต้องมีแผนรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่เข้มงวด

โดยธนาคารแห่งประเทศไทยจะประเมินความเสี่ยงของภัยคุกคามทางไซเบอร์ใน 2 ส่วนหลัก คือ ความเสี่ยงตั้งแต่ตั้งต้นด้านไซเบอร์ และการบริหารจัดการความเสี่ยงและมาตรการควบคุมด้านการรักษาความปลอดภัยที่พึงมี

2.9.2.1 การประเมินความเสี่ยงตั้งต้นด้านไซเบอร์ (Cyber Inherent Risk Assessment) ธนาคารแห่งประเทศไทยมีโอกาสเผชิญกับภัยคุกคามทางไซเบอร์อย่างหลีกเลี่ยงไม่ได้ จึงจำเป็นจะต้องวางแผนการประเมินการประเมินความเสี่ยงพื้นฐานทางไซเบอร์ใน 5 ด้าน ดังนี้

1) ขอบเขต ประเภท และปริมาณการใช้เทคโนโลยีสารสนเทศรูปแบบต่าง ๆ รวมถึงลักษณะ

2) การติดต่อสื่อสาร การเชื่อมโยงระบบของเทคโนโลยีทั้งภายในและภายนอกองค์กร

3) ความหลากหลายของของช่องทางการใช้อิเล็กทรอนิกส์

4) รูปแบบ ปริมาณ และความซับซ้อนของผลิตภัณฑ์หรือบริการ จำนวนลูกค้าหรือปริมาณการใช้งาน

5) ขนาดและลักษณะเฉพาะขององค์กร เช่น จำนวนสาขาหรือบริษัทที่อยู่ในเครือต่างประเทศ การใช้

6) ปริมาณ IT outsourcing

7) ประวัติการถูกภัยคุกคามทางไซเบอร์ซึ่งเป็นปัจจัยบ่งชี้ถึงเป้าหมายในการโจมตี

2.9.2.2 แนวทางการบริหารจัดการความเสี่ยงและมาตรการควบคุมด้านการรักษาความปลอดภัยที่พึงมี (Maturity Level) เป็นการประเมินการบริหารจัดการและการควบคุมความเสี่ยงภัยทางไซเบอร์ว่าอยู่ในระดับที่สอดรับกับความเสี่ยงที่มี หรือมีช่องว่างในเรื่องใดบ้าง โดยประเมินใน 6 ด้าน ดังนี้

1) กรอบกำกับดูแล (Governance)

2) การระบุความเสี่ยง (Risk Identification)

3) การป้องกัน (Protection)

4) การเฝ้าระวังและการตรวจจับ (Detection)

5) การตอบสนองต่อเหตุการณ์และการกู้คืน (Respond and Recovery)

6) การบริหารความเสี่ยงด้านภัยคุกคามที่เกิดจากหน่วยงานภายนอก (Third Party Risk Management)

โดยระดับความเสี่ยงจากภัยคุกตามไซเบอร์แบ่งเป็น 3 ระดับ ได้แก่ Baseline, Intermediate และ Advanced Maturity สอดคล้องกับระดับความเสี่ยงไซเบอร์ที่สถาบันทางการเงินมี ดังนี้

ตารางที่ 5 การบริหารจัดการความเสี่ยงไซเบอร์

ระดับความเสี่ยง	การบริหารจัดการความเสี่ยงไซเบอร์
ต่ำ	สำนักงานควรปฏิบัติได้ตามมาตรการที่ ธปท. กำหนดสำหรับระดับ Baseline Maturity
ปานกลาง	สำนักงานควรปฏิบัติได้ตามมาตรการที่ ธปท. กำหนดสำหรับระดับ Baseline และ Intermediate Maturity
สูง	สำนักงานควรปฏิบัติได้ตามมาตรการที่ ธปท. กำหนดสำหรับระดับ Baseline Intermediate และ Advanced Maturity

สถาบันทางการเงินจะมีการประเมินความเสี่ยงไซเบอร์อย่างน้อยปีละ 1 ครั้ง โดยเมื่อมีการเปลี่ยนแปลงทางโครงสร้างด้านระบบเทคโนโลยีสารสนเทศอย่างมีนัยยะสำคัญ หน่วยงานบริหารความเสี่ยง หน่วยงานกำกับการปฏิบัติตามหลักเกณฑ์ และหน่วยงานตรวจสอบภายในของสถาบันการเงินจะมีส่วนร่วมกำกับดูแลสถานบันการเงินในการประเมินตามกรอบความพร้อมในการรับมือภัยคุกคามทางไซเบอร์ และจะต้องส่งผลประเมินมายังฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ เป็นประจำทุกปี

2.9.3 หน่วยงานกำกับดูแลกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ

หน่วยงานกำกับดูแลกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติหรือ กสทช. ประเมินสถานการณ์ไซเบอร์ของประเทศไทยในช่วงสองศตวรรษที่ผ่านมาอย่างก้าวกระโดดโดยประเทศไทยได้เริ่มเปลี่ยนแปลงระบบการบริหารนำเข้าสู่ระบบดิจิทัล ทั้งนี้ จะต้องสร้างความเชื่อมั่นให้กับประเทศไทยว่ามีระบบการบริหารจัดการความเสี่ยงและมาตรการควบคุมด้านการรักษาความปลอดภัยที่พึงมี สิ่งที่ประเทศไทยเผชิญคือการปฏิวัติทางดิจิทัล (Digital Revolution) ซึ่งมีเทคโนโลยีเป็นตัวแปรสำคัญที่ทำให้เศรษฐกิจและสังคมของประเทศขับเคลื่อนได้ ท่ามกลางการปฏิวัติเทคโนโลยีประเทศไทยจะต้องพัฒนาฮาร์ดแวร์หรือซอร์ฟแวร์ที่มีความปลอดภัย ที่

นอกเหนือไปจากการให้ความสะดวกเพื่อรองรับกับการขยายตัวของอินเทอร์เน็ตซึ่งเป็นตัวที่ขยายขอบเขตของภัยคุกคามทางไซเบอร์ จากสภาพแวดล้อมที่ สำนัก กสทช. ได้ประเมินสรุปให้เห็นว่าประเทศไทยจะต้องมีแนวทางในการรับมือ ดังนี้

1. ประเทศไทยจะต้องประเมินขนาดและลักษณะของภัยคุกคามทางไซเบอร์พร้อมทั้งช่องโหว่จากการใช้เทคโนโลยีที่ประเทศประสบอยู่

2. ภาครัฐต้องเป็นผู้นำในการเปลี่ยนแปลงโดยยกระดับขีดสมรรถนะด้านความมั่นคงปลอดภัยไซเบอร์และจะต้องควบคุมและแทรกแซงด้านเศรษฐกิจและการลงทุน

3. สร้างความร่วมมือกับทุกภาคส่วนให้ตระหนักถึงความมั่นคงปลอดภัยทางไซเบอร์ และจะต้องมีหน่วยกลางของรัฐบาลทำหน้าที่ควบคุมและประสานงานด้านความมั่นคงและปลอดภัยทางไซเบอร์ของแต่ละหน่วยงานด้วย โดยมีกระบวนการสู่ความมั่นคงทางไซเบอร์ ดังนี้

รูปที่ 14 กระบวนการสู่ความมั่นคงทางไซเบอร์

1) การบริหารจัดการความเสี่ยงของระบบอินเทอร์เน็ต

ผู้บริหารจะต้องมีนโยบายสั่งการให้องค์กรต้องมีการบริหารจัดการความเสี่ยงต้องมีประกาศจริงจังและมีการสื่อสารที่ชัดเจนโดยเฉพาะการสร้างวิสัยทัศน์และมีเป้าหมายสำหรับเจ้าหน้าที่และผู้เกี่ยวข้องทุกคนเข้าใจและสามารถปฏิบัติตามได้ ตระหนักถึงแนวทางนี้และเข้าใจถึงวิธีการตัดสินใจและความเสี่ยงต่าง ๆ ที่อาจจะเกิดขึ้น

2) ความพร้อมของบุคลากรที่ใช้ระบบ

ความพร้อมในที่นี้ครอบคลุมไปถึงผู้ใช้ที่มีสิทธิพิเศษในการเข้าถึงข้อมูลสำคัญของหน่วยงาน บางครั้งการกระทำของผู้ใช้อาจเป็นการละเมิดสิทธิส่วนบุคคล ดังนั้นหน่วยงานควร

ระบุถึงขอบเขตหน้าที่และสิทธิ์ในการเข้ารหัสตามที่มีชื่อระบุไว้เท่านั้น นอกจากตัวองค์กรเองจะต้องกำหนดขอบเขตแล้ว ในส่วนของตัวบุคคลก็จำเป็นที่ต้องตระหนักรู้ในตนเองว่ามีขอบเขตหน้าที่เพียงใดในการเฝ้าระวังการเข้าระบบและการปกป้องข้อมูลองค์กรรั่วไหล

3) การติดตามและการควบคุมเครื่องมืออิเล็กทรอนิกส์

การเฝ้าติดตามระบบเป็นวิธีที่ดีที่สุดที่ป้องกันไม่ให้เกิดภัยคุกคามทางไซเบอร์การตรวจสอบ (มหิตถีห์ จักราบาตร, 2560) อย่างต่อเนื่องก็เป็นปัจจัยสำคัญประการหนึ่งที่จะสามารถตอบสนองภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที อุปกรณ์อิเล็กทรอนิกส์ที่สามารถถอดเคลื่อนย้ายได้มีโอกาสที่จะแพร่ไวรัสที่มุ่งทำลายระบบได้สูง การกระทำเช่นนี้อาจเป็นไปโดยตั้งใจหรือไม่ได้ตั้งใจดังนั้นหน่วยงานควรมีกฎที่ชัดเจนเพื่อป้องกันการเคลื่อนย้ายอุปกรณ์อุปกรณ์อิเล็กทรอนิกส์หรือการเข้าระบบผ่านรหัสของผู้อื่นตามความอำเภอใจ (มหิตถีห์ จักราบาตร, 2560)

หากพิจารณาในแผนยุทธศาสตร์ที่ 3 ของสำนักงาน กสทช. ฉบับ 2 (พ.ศ. 2561-2564) ที่มุ่งเสริม สร้างความเข้มแข็งด้านดิจิทัลเพื่อการพัฒนาประเทศอย่างยั่งยืน แผนยุทธศาสตร์นี้มีความสอดคล้องและแสดงให้เห็นถึงความตระหนักรู้ถึงภัยคุกคามของไซเบอร์ โดยมีเป้าประสงค์ยกระดับการเข้าถึงการใช้ประโยชน์จากดิจิทัล รวมทั้งส่งเสริมการวิจัยและพัฒนานวัตกรรมดิจิทัล สร้างพื้นฐาน ความรู้ความเข้าใจ (Digital Literacy) การใช้ประโยชน์จากเทคโนโลยีและอุปกรณ์สื่อสารอย่างถูกวิธี สร้างความมั่นคงปลอดภัยทางไซเบอร์ให้กับประชาชนให้มีความเชื่อมั่นในการใช้บริการ ตลอดจนสร้างเครือข่ายความร่วมมือและการใช้ประโยชน์จากเครือข่ายความร่วมมือต่าง ๆ ในการกำกับดูแลเพื่อปกป้องคุ้มครองผลประโยชน์ประชาชน เพื่อให้การศึกษานโยบายของ สำนักกสทช. ให้มีความละเอียดมากยิ่งขึ้น จึงขอยกตัวกรอบการดำเนินการของกลยุทธ์ที่ 3.2 และ 3.4 ดังต่อไปนี้

กลยุทธ์ที่ 3.2 ส่งเสริมให้ประชาชนมีความรู้ความเข้าใจและสามารถใช้ประโยชน์จากเทคโนโลยีดิจิทัลได้ถูกวิธี และมีความมั่นใจทางไซเบอร์จะประกอบด้วยแนวทางการดำเนินการดังนี้

1. ศึกษาและประเมินความรู้ความเข้าใจดิจิทัล (Digital Literacy) ของประชาชน
2. กำหนดกรอบและขอบเขตของความรู้ความเข้าใจดิจิทัล (Digital Literacy) ที่จำเป็นที่ประชาชนจะต้องได้รับ การพัฒนาโดยคำนึงถึงความแตกต่างของประชากร เช่น เพศ อายุ การศึกษาทักษะ เป็นต้น โดยมีเป้าหมายเพื่อให้ ประชาชนมีความรู้ความเข้าใจและสามารถใช้ประโยชน์จาก เทคโนโลยีดิจิทัล (Digital Literacy) ในชีวิตประจำวัน
3. พัฒนาสาระความรู้สื่อและช่องทางในการส่งผ่านความรู้ไปยังประชาชน ที่มีความเหมาะสมตามกลุ่มประชากร
4. ติดตามและประเมินความรู้ความเข้าใจดิจิทัล (Digital Literacy) ของประชาชน

กลยุทธ์ที่ 3.4 เสริมสร้างการสร้างเครือข่ายและความร่วมมือระหว่างรัฐ ภาคเอกชน และภาคประชาสังคม ในการดูแลการประกอบการฯ เพื่อปกป้องคุ้มครองผลประโยชน์ของประชาชน

1. ติดตามและประเมินสถานการณ์แนวโน้มและทิศทางการประกอบกิจการฯ เพื่อนำไปสู่การระบุหน่วยงานที่ มีความเกี่ยวข้องกับการกำกับดูแลการประกอบกิจการฯ ทั้งที่เป็นหน่วยงานภายในประเทศและภายนอกประเทศ

2. ศึกษาบทบาทและบริบทการดำเนินงานของหน่วยงานที่เกี่ยวข้องกับการกำกับดูแลฯ และกำหนดทิศทาง และขอบเขตของการประสานความร่วมมือกับหน่วยงานที่เกี่ยวข้อง

3. ให้ความสำคัญกับการแสวงหาจุดมุ่งหมายร่วมกัน (Purpose) การกำหนดความเชื่อพื้นฐานในการทำงานร่วมกัน (Principle) การกำหนดความสามารถที่ต้องมีร่วมกัน (Capability) การกำหนดบทบาทความรับผิดชอบของแต่ละฝ่ายและความสัมพันธ์ที่มีต่อกัน (Concept) การกำหนดกฎระเบียบและโครงสร้างที่จะใช้ยึดโยงความสัมพันธ์ที่มีต่อกัน (Structure) และการกำหนดโครงการหรือกิจกรรมที่ จะดำเนินการร่วมกัน (Practice) กับหน่วยงานที่เป็นเป้าหมาย ของการสร้างเครือข่ายและความร่วมมือ

4. จัดทำข้อตกลงความร่วมมืออย่างเป็นทางการและมีการกำหนดระบบและกลไกการประสานความร่วมมือ ระหว่างกันในการกำกับดูแลการประกอบกิจการฯ รวมถึง การมีระบบและกลไกในการสนับสนุนการดำเนินงานและการ แก้ไขปัญหาระหว่างหน่วยงาน ดำเนินการตามข้อตกลงความร่วมมืออย่างจริงจังและมีการติดตามประเมินผล (สำนักงานคณะกรรมการกิจการกระจายเสียงกิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ, 2562)

ทั้งสองกลยุทธ์นี้เป็นกลวิธีเบื้องต้นที่แสดงให้เห็นว่า สำนัก กสทช. มีความพร้อมและความตระหนักรู้กับภัยของไซเบอร์ที่กำลังจะเกิดขึ้นโดยจะเป็นการสร้างความเชื่อมั่นและการสร้างเครือข่ายเป็นนโยบายตั้งรับเมื่อมีภัยคุกคามทางไซเบอร์

2.9.4 การไฟฟ้าส่วนภูมิภาค

จาก พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ที่กำหนดให้โครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานภาครัฐมีมาตรฐานและมีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์มีการเฝ้าระวังภัยคุกคามและมีแผนรับมือเพื่อกู้คืนระบบให้กลับมาทำงานได้ตามปกติ และมีการร่วมมือและประสานงานกับสำนักงานรักษาความมั่นคงปลอดภัยไซเบอร์นั้น ทำให้การไฟฟ้าส่วนภูมิภาคกำหนดทิศทางการปรับเปลี่ยน “PEA Digital Transformation” โดยให้มีการพัฒนาขีดความสามารถทางด้านธุรกิจและทางด้านเทคโนโลยีดิจิทัล ของ กฟภ.โดยกำหนดยุทธศาสตร์ดิจิทัลของ กฟภ. 5 ด้าน ดังนี้

1. ยกระดับระบบไฟฟ้าให้เป็นเลิศด้วยดิจิทัล เสริมสร้างโครงข่ายระบบไฟฟ้าด้วยเทคโนโลยีดิจิทัล พัฒนาขีดความสามารถการวิเคราะห์ข้อมูลในการบริหารโครงข่ายอย่างมีประสิทธิภาพเพิ่มเสถียรภาพของระบบไฟฟ้าและการบริการที่เป็นเลิศ

2. เชื่อมโยงลูกค้าด้วยเทคโนโลยียกระดับการให้บริการลูกค้าด้วยการสร้างความผูกพันธ์ที่ดีกับลูกค้าดิจิทัลในโลกแห่งการเชื่อมต่อสร้างความประทับใจแก่ประสบการณ์ในการใช้บริการรวมไปถึงการเสริมสร้างภาพลักษณ์และความเชื่อมั่นผ่านเทคโนโลยีดิจิทัล

3. ปรับเปลี่ยนสู่องค์กรสมัยใหม่เพิ่มความคล่องตัวรวดเร็วและมีประสิทธิภาพในการดำเนินธุรกิจกฟภ.โดยใช้เทคโนโลยีดิจิทัลปรับเปลี่ยนและสนับสนุนการดำเนินงานภายในสร้างวัฒนธรรมการเป็นเพื่อนคู่คิด

4. เสริมสร้างบุคลากรแห่งอนาคตพัฒนาศักยภาพของทรัพยากรบุคคลเพื่อเตรียมความพร้อมในการทำงานยุคดิจิทัลรวมถึงการพัฒนาทักษะในการใช้เทคโนโลยีดิจิทัลเพื่อรองรับการทำงานและการเปลี่ยนแปลงของธุรกิจ

5. แพลตฟอร์มดิจิทัล สร้างแพลตฟอร์มดิจิทัลของ กฟภ. ที่สนับสนุนการดำเนินงานทั้งองค์กรให้มีมาตรฐานและมีความมั่นคง ปลอดภัยรองรับการเติบโตของธุรกิจ

ทั้งนี้การไฟฟ้าในฐานะเป็นหน่วยงานสาธารณูปโภคพื้นฐานขนาดใหญ่จึงมีแผนการที่จะดูแลความปลอดภัยไซเบอร์ โดยมี 5 ขั้นตอน ดังนี้ 1) ผู้นำมีความชัดเจนในทิศทางการบริหารสามารถตัดสินใจได้อย่างเฉียบขาดเมื่ออยู่ในวิกฤติและสามารถนำ กฟภ. เข้าสู่ Digital Unity ตามแผนที่กำหนดไว้ได้ 2) จัดตั้งโครงสร้างดิจิทัลที่ชัดเจนภายในองค์กรและปรับปรุงกฎระเบียบให้สอดคล้องกับการทำงานเพื่อผลักดันให้แผนสามารถดำเนินการไปได้ 3) ร่วมมือกับพันธมิตรที่จะเข้ามาแลกเปลี่ยนความรู้ใหม่ ๆ 4) สร้างวัฒนธรรมองค์กรให้มีความคุ้นชินและมีความระมัดระวังให้ใช้ไซเบอร์อย่างปลอดภัย 5) สร้างทักษะความสามารถใหม่ให้กับบุคลากรในเรื่องการใช้เทคโนโลยี

การไฟฟ้าส่วนภูมิภาคมีความตระหนักถึงความสำคัญในการรักษาความมั่นคงปลอดภัยเว็บไซต์เพื่อปกป้องข้อมูลของผู้ใช้บริการจากการถูกทำลาย หรือบุกรุกจากผู้ไม่หวังดี หรือผู้ที่ไม่มีสิทธิ์ในการเข้าถึงข้อมูล จึงได้กำหนดมาตรการรักษาความมั่นคงปลอดภัยเว็บไซต์ โดยใช้มาตรฐานการรักษาความปลอดภัยของข้อมูลขั้นสูง ด้วยเทคโนโลยี Secured Socket Layer (SSL) ซึ่งเป็นเทคโนโลยีในการเข้าสู่ข้อมูลผ่านรหัสที่ระดับ 128 bits (128-bits Encryption) เพื่อเข้ารหัสข้อมูลที่ถูกส่งผ่านเครือข่ายอินเทอร์เน็ตในทุกครั้งที่มีการทำธุรกรรมทางการเงินผ่านเครือข่ายอินเทอร์เน็ตของการไฟฟ้าส่วนภูมิภาค ทำให้ผู้ที่ดักจับข้อมูลระหว่างทางไม่สามารถนำข้อมูลไปใช้ต่อได้ โดยจะใช้การเข้ารหัสเป็นหลักในการรักษาความปลอดภัยของข้อมูล

นอกจากมาตรการ และวิธีการรักษาความมั่นคงปลอดภัยโดยทั่วไปที่กล่าวข้างต้นแล้ว การไฟฟ้าส่วนภูมิภาคยังใช้เทคโนโลยีระดับสูงดังต่อไปนี้เพื่อปกป้องข้อมูลส่วนตัวของท่าน

1. Firewall เป็นระบบซอฟท์แวร์ที่จะอนุญาตให้เฉพาะผู้ที่มีสิทธิ หรือผู้ที่การไฟฟ้าส่วนภูมิภาคอนุมัติเท่านั้นจึงจะผ่าน Fire Wall เพื่อเข้าถึงข้อมูลได้

2. Scan Virus นอกจากเครื่องคอมพิวเตอร์ทุกเครื่องที่ให้บริการจะมีการติดตั้ง Software ป้องกัน Virus ที่มีประสิทธิภาพสูงและ Update อย่างสม่ำเสมอแล้ว การไฟฟ้าส่วนภูมิภาคยังได้ติดตั้ง Scan Virus Software บนเครื่อง Server โดยเฉพาะอีกด้วย

3. Cookies เป็นไฟล์คอมพิวเตอร์เล็ก ๆ ที่จะทำการเก็บข้อมูลชั่วคราวที่จำเป็น ลงในเครื่องคอมพิวเตอร์ของผู้ขอใช้บริการ เพื่อความสะดวกและรวดเร็วในการติดต่อสื่อสาร อย่างไรก็ตามการไฟฟ้าส่วนภูมิภาคตระหนักถึงความเป็นส่วนตัวของ ผู้ใช้บริการเป็นอย่างดี จึงหลีกเลี่ยงการใช้ Cookies แต่ถ้าหากมีความจำเป็น ต้องใช้ Cookies บริษัทจะพิจารณาอย่างรอบคอบ และตระหนักถึงความปลอดภัย และความเป็นส่วนตัวของผู้ขอรับบริการเป็นหลัก

4. Auto Log off ในการใช้บริการของการไฟฟ้าส่วนภูมิภาค หลังจากเลิกการใช้งานควร Log off ทุกครั้ง กรณีที่ผู้ใช้บริการลืม Log off ระบบจะทำการ Log off ให้โดยอัตโนมัติภายในเวลาที่เหมาะสมของแต่ละบริการ ทั้งนี้เพื่อความปลอดภัยของผู้ใช้บริการเอง(การไฟฟ้าส่วนภูมิภาค, 2562)

นอกจากนี้ ทั้งการไฟฟ้าภูมิภาคและการไฟฟ้านครหลวงยังมีการจัดการความเสี่ยงเรื่องการจู่โจมความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ทั้งระบบควบคุมการส่งจ่าย พลังไฟฟ้า (SCADA/EMS) และระบบเทคโนโลยีสารสนเทศอื่น ๆ โดยตรวจเยี่ยมและมีข้อเสนอแนะให้เพิ่มมาตรการป้องกัน การถูกโจมตีทั้งทางไซเบอร์และทางกายภาพ รวมทั้งเร่งรัดให้มีการจัดตั้ง Computer Security Incident Response Team (CSIRT) และมุ่งเน้นการพัฒนาความรู้ความสามารถ และส่งเสริมบุคลากรให้มีทักษะทางด้านความมั่นคงไซเบอร์ทั้งปัจจุบันและอนานคต (วันชัย เจยีรวัฒนาวิทย์, 2562)

2.9.5 กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้รับมอบหมายให้รับผิดชอบเสริมสร้างความมั่นคงทางเทคโนโลยีสารสนเทศและไซเบอร์ โดยแบ่งเป็นแนวทางดังนี้

1) ป้องกันภัยคุกคามด้านไซเบอร์ สงครามไซเบอร์ และเสริมสร้างความปลอดภัยระบบเทคโนโลยีสารสนเทศ โดยบูรณาการการจัดการความมั่นคงปลอดภัยทางไซเบอร์ระหว่างหน่วยงานภาครัฐ การประสานความร่วมมือและเสริมสร้างเครือข่ายกับภาคเอกชน ภาควิชาการ บุคลากร องค์กรและผู้เชี่ยวชาญด้านการรักษาความมั่นคงทางไซเบอร์ การเสริมสร้างความร่วมมือระหว่างประเทศ การเฝ้าระวังและการพัฒนาระบบป้องกัน การโจมตีระบบสารสนเทศ การพัฒนา

ความพร้อมต่อสงครามไซเบอร์ การปกป้องโครงสร้างพื้นฐานสำคัญด้านสารสนเทศของประเทศ การกู้คืนข้อมูล ระบบ/เครือข่ายและการพัฒนามาตรฐานด้านความปลอดภัยในทุกด้าน

2) พัฒนาการบังคับใช้กฎหมาย โดยการพัฒนาระเบียบและกฎมายเพื่อความมั่นคงปลอดภัยไซเบอร์และการพัฒนาเทคโนโลยีสำหรับงานสืบสวนและป้องกันอาชญากรรมทางไซเบอร์ ให้สามารถลดภัยคุกคามหรือขีดอันตรายที่ส่งผลกระทบกับบุคคล ข้อมูลและระบบเทคโนโลยีสารสนเทศ โดยเฉพาะที่อยู่ในรูปของการทำธุรกรรมทางอิเล็กทรอนิกส์ การละเมิดทรัพย์สินทางปัญญา การโจรกรรมข้อมูลสารสนเทศ การละเมิดสิทธิเสรีภาพของบุคคล การกรรโชกข้อมูลสารสนเทศ การกระทำผิดตลอดจนการก่อวินาศกรรมหรือทำลายระบบสารสนเทศ รวมถึงการสร้างความตระหนักรู้ให้กับประชาชนเกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์

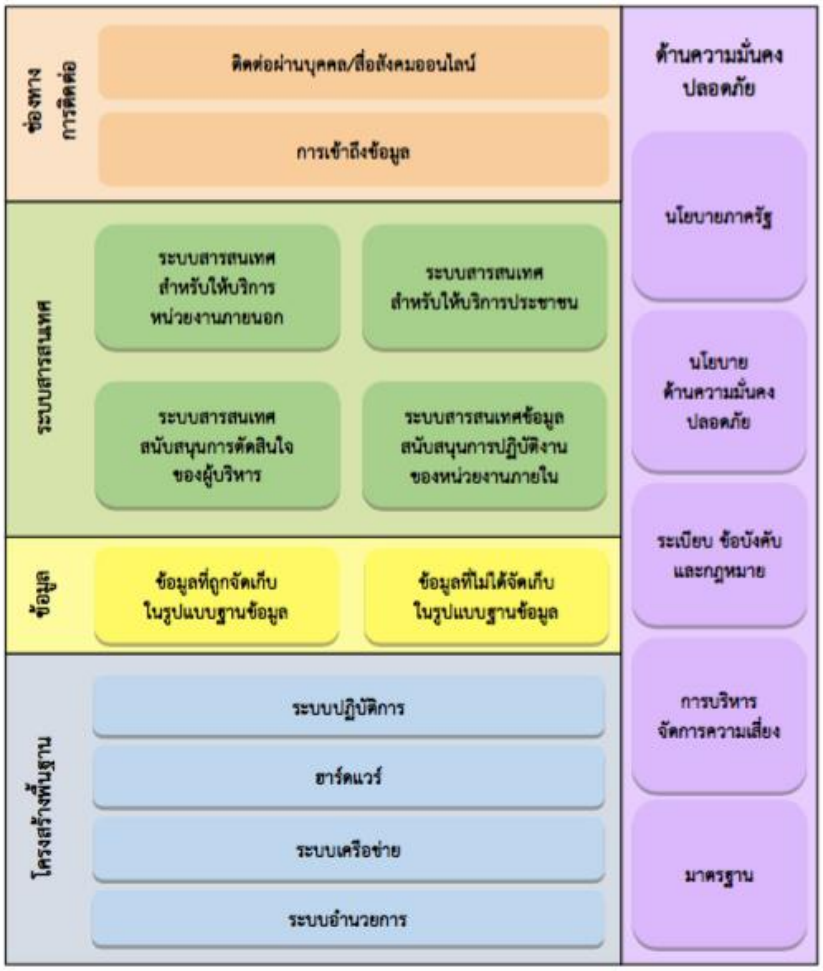
3) พัฒนาศักยภาพทางด้านเทคโนโลยีสารสนเทศ โดยส่งเสริมการวิจัย พัฒนา และจดสิทธิบัตรเทคโนโลยีสารสนเทศที่ผลิตโดยคนไทย การวิจัยและพัฒนาเพื่อความมั่นคงปลอดภัยไซเบอร์ การบูรณาการเชื่อมโยงระบบฐานข้อมูลรัฐ การพัฒนาระบบรัฐบาลอิเล็กทรอนิกส์แบบบูรณาการ รวมถึงการใช้ระบบรัฐบาลอิเล็กทรอนิกส์ เครือข่ายสื่อสารข้อมูลเชื่อมโยงหน่วยงานภาครัฐ (GIN) ระบบคลาวด์ภาครัฐ (G-Cloud) ตลอดจนการพัฒนาบุคลากรภาครัฐ องค์กรทุกภาคส่วนที่เกี่ยวข้องให้มีความรู้ความชำนาญด้านระบบเทคโนโลยีสารสนเทศและการรักษาความปลอดภัยทางไซเบอร์ เพื่อให้บุคลากรภาครัฐและองค์กรทุกภาคส่วนที่เกี่ยวข้องมีข้อมูลข่าวสารและความรู้ทางด้านเทคโนโลยีที่ทันสมัย และการรักษาความมั่นคงปลอดภัยไซเบอร์ในเชิงปริมาณ คุณภาพ อย่างต่อเนื่อง

4) พัฒนาระบบการเตรียมพร้อมแห่งชาติเพื่อเสริมสร้างความมั่นคงของชาติ โดยจัดให้มีระบบสั่งการที่มีเอกภาพ สามารถบูรณาการและผนึกกำลังทุกภาคส่วนที่เกี่ยวข้องในการบริหารจัดการภัยในเชิงรุก ทั้งการแจ้งเตือนภัย การป้องกันภัย การระงับภัย การบรรเทาภัย และการฟื้นฟูผลที่เกิดขึ้น รวมไปถึงการ ส่งเสริมและสนับสนุนการมีส่วนร่วมของทุกภาคส่วนในการเตรียมพร้อมเผชิญภัยพิบัติและพัฒนาและสนับสนุนการมีระบบฐานข้อมูลเฝ้าระวังและเตรียมพร้อมด้านภัยพิบัติที่ทันสมัยพร้อมระบบสำรอง ที่สามารถเอื้อต่อการเตือนภัยล่วงหน้าอย่างรวดเร็วและมีประสิทธิภาพ (กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, 2561)

2.9.6 กระทรวงยุติธรรม

กระทรวงยุติธรรมเห็นถึงความสำคัญของการนำเทคโนโลยีดิจิทัลมาใช้เพื่อเพิ่มศักยภาพการทำงานของกระทรวงยุติธรรมโดยใช้เทคโนโลยีในการบริหารจัดการ ให้บริการประชาชนสอดคล้องกับความก้าวหน้าของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว แต่อย่างไรก็ตามก็ไม่ได้ละเลยความมั่นคงปลอดภัยในการใช้เทคโนโลยี จึงได้กำหนดวิสัยทัศน์ ยุทธศาสตร์ แผนงาน โดย

แสดงให้เห็นผ่านโครงสร้างดิจิทัลขององค์กร เพื่อติดตามและประเมินผลการพัฒนาเทคโนโลยีดิจิทัลของกระทรวงยุติธรรม ดังนี้



รูปที่ 15 ออกแบบสถาปัตยกรรมองค์กรในด้านต่าง ๆ (Enterprise Reference Models)

ที่มา: สำนักงานปลัดกระทรวงยุติธรรม (2560)

การออกแบบสถาปัตยกรรมองค์กรในอนาคตของกระทรวงยุติธรรม ได้ออกแบบสถาปัตยกรรมองค์กรในด้านต่าง ๆ (Enterprise Reference Models) โดยแบ่งเป็น 5 ด้าน (สำนักงานปลัดกระทรวงยุติธรรม, 2560) ได้แก่

1) ด้านช่องทางการติดต่อ (Channel) หมายถึง ช่องทางที่จะสามารถติดต่อ หรือการให้บริการประชาชนที่เข้ามารับการบริการกับส่วนราชการในสังกัดกระทรวงยุติธรรมได้อย่างสะดวก และรวดเร็วยิ่งขึ้น อาทิ การติดต่อหน่วยงานโดยตรง การติดต่อผ่านหน้าเว็บไซต์ของส่วนราชการ

2) ด้านระบบสารสนเทศ (Application) หมายถึง การพัฒนาระบบสารสนเทศและการนา ระบบสารสนเทศส่วนกลาง (Common) มาใช้สนับสนุนการปฏิบัติงาน และการให้บริการ อาทิ ระบบสารสนเทศที่รองรับการปฏิบัติงาน ระบบสารสนเทศที่สามารถใช้ข้อมูลร่วมกัน ระหว่างส่วนราชการในสังกัดกระทรวงยุติธรรม ระบบวิเคราะห์สนับสนุนการตัดสินใจของผู้บริหารและผู้ปฏิบัติงาน ระบบข้อมูลเชิงพื้นที่ของส่วนราชการในสังกัดกระทรวงยุติธรรม และระบบ การให้บริการกับหน่วยงานภายนอกและประชาชน

3) ด้านข้อมูล (Data) หมายถึง ข้อมูลสำหรับบริหารจัดการในภาพรวมระดับกระทรวง อาทิ ข้อมูลทรัพยากรบุคคล งบประมาณ การเงินการบัญชี พัสดุครุภัณฑ์ ยุทธศาสตร์และแผนงาน ซึ่งสามารถจัดเก็บได้ 2 แบบ คือ จัดเก็บในฐานข้อมูล และไม่ถูกจัดเก็บในฐานข้อมูล

4) ด้านโครงสร้างพื้นฐาน (Infrastructure) หมายถึง การรองรับระบบสารสนเทศและการให้บริการ สนับสนุนการปฏิบัติงาน ซึ่งระบบดังกล่าวเน้นการใช้งานและการนำเข้าข้อมูลผ่านอุปกรณ์เคลื่อนที่ไร้สาย ระบบเครือข่ายหลัก และระบบการรองข้อมูล ควรได้รับการปรับปรุงและเสริมประสิทธิภาพ เพื่อรองรับการเชื่อมโยงของข้อมูลที่จะมีปริมาณเพิ่มสูงขึ้นในอนาคต ดังนั้นโครงสร้างพื้นฐานควรรองรับการเติบโตของข้อมูลที่มหาศาล (Big Data)

5) ด้านความมั่นคงปลอดภัย (Security) หมายถึง การประเมินความเสี่ยงทั้งในกระบวนการบริหารจัดการปฏิบัติงาน ระบบสารสนเทศ และโครงสร้างพื้นฐาน ให้เป็นไปตามมาตรฐานสากล รวมถึงพัฒนาปรับปรุงด้านกฎหมาย กฎระเบียบ ข้อบังคับและนโยบายที่สนับสนุนการปฏิบัติงานผ่านทางเทคโนโลยีดิจิทัล รวมถึงการมีมาตรฐานทางด้านการจัดเก็บและรูปแบบข้อมูลที่มีมาตรฐานเดียวกัน (Data Standard) ทำให้เกิดข้อมูลที่มีประสิทธิภาพต่อการใช้งานในอนาคต

โดยแต่ละมุมมองของโครงสร้างดิจิทัลขององค์กรนั้น จะมีมุมมองต่อแบบจำลอง (Enterprise Reference Model) ที่แตกต่างกัน แสดงดังภาพ

ตารางที่ 6 แบบจำลอง Enterprise Reference Model

มุมมอง	ด้านโครงสร้างพื้นฐาน	ด้านข้อมูล	ด้านระบบสารสนเทศ	ด้านความมั่นคงปลอดภัย
ผู้บริหาร	ระบบปฏิบัติการ/Hardware ระบบเครือข่าย/ระบบอำนวยการ	- จัดเก็บแบบฐานข้อมูล - ไม่ได้จัดเก็บแบบฐานข้อมูล	สนับสนุนการตัดสินใจของผู้บริหาร	นโยบายรัฐ/ ระเบียบข้อบังคับ กฎหมาย / นโยบายความมั่นคงปลอดภัย/การบริหารจัดการความเสี่ยง/มาตรฐาน
หน่วยงานภายนอก		- จัดเก็บแบบฐานข้อมูล	ให้บริการหน่วยงานภายนอก	นโยบายรัฐ/ ระเบียบข้อบังคับ กฎหมาย/ นโยบายความมั่นคงปลอดภัย/การบริหารจัดการความเสี่ยง/มาตรฐาน
ส่วนราชการในสังกัดกระทรวงยุติธรรม	ระบบปฏิบัติการ/Hardware ระบบเครือข่าย/ระบบอำนวยการ	- จัดเก็บแบบฐานข้อมูล - ไม่ได้จัดเก็บแบบฐานข้อมูล	สนับสนุนงานหน่วยงานภายใน	นโยบายรัฐ/ ระเบียบข้อบังคับ กฎหมาย / นโยบายความมั่นคงปลอดภัย/การบริหารจัดการความเสี่ยง/มาตรฐาน
ประชาชน		- จัดเก็บแบบฐานข้อมูล	ให้บริการประชาชน	นโยบายรัฐ/ ระเบียบข้อบังคับ กฎหมาย / นโยบายความมั่นคงปลอดภัย/การบริหารจัดการความเสี่ยง/มาตรฐาน

ที่มา: สำนักงานปลัดกระทรวงยุติธรรม, 2560

ระบบคลาวด์ของกระทรวงยุติธรรม (MOJ Cloud) มีวัตถุประสงค์เพื่อให้บริการกับส่วนราชการและมีกรอบแนวทางเพื่อให้ส่วนราชการในสังกัดกระทรวงยุติธรรมนำไปประยุกต์ใช้ในการจัดทำ ทบทวน และปรับปรุงสถาปัตยกรรมองค์กรของแต่ละส่วนราชการโดยสิ่งที่ส่วนราชการในสังกัดกระทรวงยุติธรรมต้องเตรียมการตามแผนปฏิบัติการดิจิทัลของกระทรวงยุติธรรม ในส่วนสถาปัตยกรรมองค์กรมี (สำนักงานปลัดกระทรวงยุติธรรม, 2560) ดังต่อไปนี้

1) ศึกษา วิเคราะห์ภารกิจ/หน้าที่หลัก และประเมินสถานภาพด้านเทคโนโลยีดิจิทัลที่สนับสนุนภารกิจ/หน้าที่หลักของส่วนราชการในสังกัดกระทรวงยุติธรรม

2) ออกแบบสถาปัตยกรรมองค์กรปัจจุบัน (As-Is) ของส่วนราชการในสังกัดกระทรวงยุติธรรมโดยครอบคลุมสถาปัตยกรรมด้านธุรกิจ สถาปัตยกรรมด้านข้อมูล สถาปัตยกรรมระบบงาน และสถาปัตยกรรมด้านเทคนิค

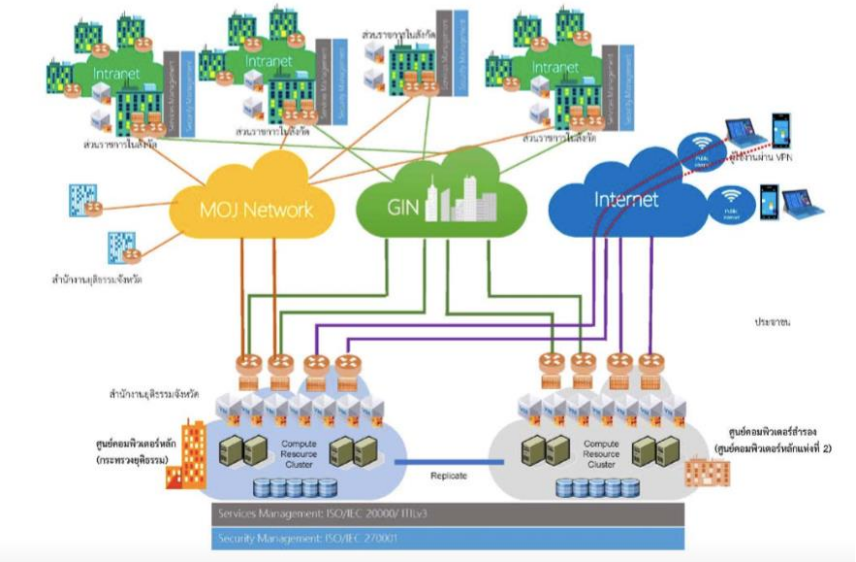
3) ออกแบบสถาปัตยกรรมองค์กรอนาคต (To-Be) เพื่อการบริการด้านเทคโนโลยีดิจิทัล โดยครอบคลุมสถาปัตยกรรมด้านธุรกิจ สถาปัตยกรรมด้านข้อมูล สถาปัตยกรรมระบบงาน และสถาปัตยกรรมด้านเทคนิคที่สอดคล้องกับกรอบแนวทางการจัดทาสถาปัตยกรรมองค์กร ด้านเทคโนโลยีดิจิทัลของกระทรวงยุติธรรม

4) วิเคราะห์เปรียบเทียบช่องว่าง (Gap Analysis) ระหว่างสถาปัตยกรรมองค์กรปัจจุบัน และสถาปัตยกรรมองค์กรอนาคตที่ออกแบบ เพื่อรองรับการปฏิบัติงานในอนาคต

5) กำหนดแผนงานด้านการพัฒนาเทคโนโลยีดิจิทัล เพื่อสนับสนุนการนาสถาปัตยกรรมองค์กรไปสู่การใช้งานจริง

6) ติดตามและประเมินผลทบทวนการจัดทำสถาปัตยกรรมองค์กรของส่วนราชการในสังกัดกระทรวงยุติธรรม

กระทรวงยุติธรรมมีระบบโครงสร้างพื้นฐานเทคโนโลยีดิจิทัลหลักของกระทรวง (MOJ Cloud) ถือว่าเป็นระบบโครงสร้างพื้นฐานเทคโนโลยีดิจิทัลหลัก ที่มีการบูรณาการทั้งในด้านการใช้งานโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล ด้านการเชื่อมโยงระบบสารสนเทศและแพลตฟอร์ม ด้านข้อมูล ตลอดจนด้านบริการดิจิทัล ดังนั้นทิศทางการพัฒนาโครงสร้างพื้นฐานเทคโนโลยีดิจิทัลของกระทรวงจะเน้น การจัดเตรียมระบบโครงสร้างพื้นฐานเทคโนโลยีดิจิทัลสำหรับการให้บริการ MOJ Cloud และการสร้าง ระบบเครือข่ายสื่อสารข้อมูลในการเชื่อมโยงหน่วยงาน และเพื่อการบริการดิจิทัลโดยใช้ MOJ Cloud เป็นศูนย์กลาง โดยสถาปัตยกรรมระบบโครงสร้างพื้นฐานเทคโนโลยีดิจิทัลของกระทรวงยุติธรรม สามารถแสดงได้ตามภาพ



รูปที่ 16 สถาปัตยกรรมระบบโครงสร้างพื้นฐานเทคโนโลยีดิจิทัล
ของกระทรวงยุติธรรม

ที่มา: สำนักงานปลัดกระทรวงยุติธรรม (2560)

นอกจากนี้กระทรวงยุติธรรมยังมีมาตรการในการป้องกันภัยคุกคามทางไซเบอร์เชิงเทคนิคอย่างครอบคลุม โดยแบ่งออกเป็น 4 กรอบ (สำนักงานปลัดกระทรวงยุติธรรม, 2560) ดังนี้

1. การบริหารจัดการการรักษาความมั่นคงปลอดภัยเทคโนโลยีดิจิทัล
2. ระบบเครือข่ายศูนย์คอมพิวเตอร์
3. การบริหารจัดการระบบรักษาความมั่นคงปลอดภัยแบบรวมศูนย์
4. การให้บริการระบบสารสนเทศ

ตารางที่ 7 มาตรการในการป้องกันภัยคุกคามทางไซเบอร์เชิงเทคนิค

การบริหารจัดการการรักษาความมั่นคงปลอดภัยเทคโนโลยีดิจิทัล		
Security Management การบริหารจัดการการรักษาความมั่นคงปลอดภัยเทคโนโลยีดิจิทัล	ก่อน ระหว่างและหลังเกิดเหตุ	การวางนโยบายกระบวนการ มาตรการ ในการบริหารจัดการการรักษาความมั่นคงปลอดภัยเทคโนโลยีดิจิทัลอย่างเป็นระบบ
ระบบเครือข่ายศูนย์คอมพิวเตอร์		
Firewall Segmentation การกรองแบบ Stateful และการตรวจสอบโปรโตคอล	ก่อนเกิดเหตุ	การเข้าถึงที่ไม่ได้รับอนุญาต และแพคเก็ตที่มีรูปแบบไม่ถูกต้อง
Anti-Malware ระบุ บล็อก และวิเคราราะห์ไฟล์และการส่ง-ที่เป็นอันตราย	ก่อน ระหว่างและหลังเกิดเหตุ	การกระจายมัลแวร์ผ่านเครือข่ายหรือระหว่างเซิร์ฟเวอร์และอุปกรณ์
Intrusion Detection and Prevention การระบุการโจมตีด้วยลายมือชื่อและการวิเคราะห์ความผิดปกติ	ก่อนเกิดเหตุ	การโจมตีโดยใช้เวิร์มไวรัสหรือเทคนิคอื่น ๆ
VPN Concentrator การเข้าถึงระยะไกลแบบเข้ารหัส	ก่อนเกิดเหตุ	บริการที่เปิดเผยและการโจรกรรมข้อมูล
Flow Analytics การวิเคราะห์ข้อมูล Meta Data ของการรับส่งข้อมูลเครือข่ายเพื่อระบุเหตุการณ์ด้านความปลอดภัย	ระหว่าง และหลังเกิดเหตุ	กิจกรรมที่เป็นอันตรายดำเนินการผ่านเทคนิคที่ต่างกันโดยทั่วไปโดยอาชญากรไซเบอร์ผ่านทางอินเทอร์เน็ตหรือเครือข่ายอื่น ๆ
DDoS Protection ป้องกันรูปแบบการโจมตี DDoS	ก่อน ระหว่างและหลังเกิดเหตุ	การโจมตี DDoS ที่มาจากหลายแหล่งจำนวนมากเพื่อประสงค์จะทำลายการให้บริการ
DNS-Based Advanced Threat Solution บล็อกกิจกรรมอินเทอร์เน็ตทั้งหมดที่กำหนดไว้ในโดเมน ที่เป็น	ก่อนเกิดเหตุ	มัลแวร์ ฟิชชิ่ง การควบคุมการ Call Back บนพอร์ต หรือโปรโตคอลใด ๆ

ตารางที่ 7 มาตรการในการป้องกันภัยคุกคามทางไซเบอร์เชิงเทคนิค (ต่อ)

การบริหารจัดการระบบรักษาความมั่นคงปลอดภัยแบบรวมศูนย์		
Policy/Configuration การกำหนดนโยบายและจัดการโครงสร้างพื้นฐานแบบครบวงจรและการตรวจสอบการปฏิบัติตามข้อกำหนด	ก่อนและระหว่าง เกิดเหตุ	การเข้ายึดครองโครงสร้างพื้นฐานหรืออุปกรณ์
Time Synchronization การปรับเทียบนาฬิกาอุปกรณ์	ก่อนเกิดเหตุ	
Monitoring การเฝ้าระวังและตรวจสอบการจราจรเครือข่าย	ก่อน ระหว่างและหลังเกิดเหตุ	กิจกรรมที่เป็นอันตรายดำเนินการผ่านเทคนิคที่ต่างกันโดยทั่วไปโดยอาชญากรไซเบอร์ผ่านทางอินเทอร์เน็ตหรือเครือข่ายอื่น ๆ
Anomaly Detection การระบุโฮสต์ที่ติดไวรัสและการสแกนหาโฮสต์ที่มีช่องโหว่อื่น ๆ	ก่อนและระหว่าง เกิดเหตุ	การรับส่งข้อมูลของวอร์ม ที่มีพฤติกรรมในการพยายามสแกนการทำงานของระบบ
Analysis/Correlation การจัดการเหตุการณ์ความปลอดภัยของข้อมูลแบบเรียลไทม์	ระหว่างและหลังเกิดเหตุ	การโจมตีที่มีรูปแบบและพฤติกรรมที่หลากหลาย
Vulnerability Management การสแกนและบริหารจัดการช่องโหว่ของระบบฯ	ก่อน ระหว่างและหลังเกิดเหตุ	อุปกรณ์ที่เป็นอันตรายที่เชื่อมต่อกับโครงสร้างพื้นฐาน
Logging/ Reporting รวบรวมข้อมูลเหตุการณ์จากส่วนกลาง	ก่อน ระหว่างและหลังเกิดเหตุ	การเข้าถึงเครือข่ายหรือการกำหนดค่าโดยไม่ได้รับอนุญาต

ตารางที่ 7 มาตรการในการป้องกันภัยคุกคามทางไซเบอร์เชิงเทคนิค (ต่อ)

การให้บริการระบบสารสนเทศ		
Web Application Firewall การเฝ้าระวังและตรวจสอบ Application ชั้นสูง	ก่อน ระหว่างและหลังเกิดเหตุ	การโจมตี Application ที่พัฒนาไม่ดี
Web Security การเฝ้าระวังและตรวจการเข้าถึงอินเทอร์เน็ตบนเว็บ	ระหว่างและหลังเกิดเหตุ	การแทรกซึมและกิจกรรมที่เป็นอันตรายดำเนินการผ่านเทคนิคที่ต่างกันผ่านทาง HTTP
Server-Based Security ซอฟต์แวร์รักษาความปลอดภัย เพื่อปกป้องเครื่องแม่ข่าย	ก่อน ระหว่างและหลังเกิดเหตุ	ไวรัสหรือมัลแวร์ที่คุกคามระบบ
Application Visibility Control การตรวจสอบข้อมูล Packet เชิงลึก (Deep Packet inspection: DPI) ของการรับส่งข้อมูลของแอปพลิเคชัน	ระหว่าง และหลังเกิดเหตุ	เครื่องมือโจมตีซ่อนตัวอยู่ในแอปพลิเคชันที่ได้รับอนุญาต
TLS/SSL Encryption Offload ฮาร์ดแวร์ที่ช่วยเพิ่มประสิทธิภาพการเข้ารหัสข้อมูล	ก่อนเกิดเหตุ	การขโมยข้อมูลที่ไม่ได้เข้ารหัส
Email Security การตรวจสอบคุณภาพและป้องกัน e-mail	ระหว่าง และหลังเกิดเหตุ	การแทรกซึมและกิจกรรม ที่เป็นอันตรายดำเนินการผ่านเทคนิคที่ต่างกันผ่านทาง e-mail

การเฝ้าระวังทั้ง 4 กรอบที่เห็นจากในภาพนั้นแสดงถึงความพร้อมของกระทรวงยุติธรรมในเชิงเทคนิคที่สามารถนำผู้เชี่ยวชาญมาวิเคราะห์เครื่องมือที่จะสามารถใช้จริงได้ในการขับเคลื่อนองค์กร มาตรการการป้องกันที่สอดรับไปกับภัยคุกคามที่เกิดขึ้นพร้อมทั้งสามารถกำหนดรูปแบบการป้องกันที่มีก่อนหลังจะสามารถทำให้ทั้งเจ้าหน้าที่หรือผู้ที่มีความรู้ทั่วไปสามารถเห็นภาพรวมของยุทธศาสตร์การเฝ้าระวังภัยคุกคามไซเบอร์ของกระทรวงยุติธรรมได้มากขึ้น

2.9.7 กองทัพไทยกับยุทธศาสตร์รับมือภัยคุกคามไซเบอร์

สถานการณ์การเปลี่ยนแปลงของเทคโนโลยีในปัจจุบัน ส่งผลต่อความมั่นคงของประเทศไทย อย่างที่เห็นได้ชัดเจน ตั้งแต่รูปแบบของการใช้ชีวิตประจำวัน ความน่าเชื่อถือทางเศรษฐกิจ สังคมการและการเมือง ทำให้ประเทศต้องปรับตัวรับกับความมั่นคงรูปแบบใหม่ อย่างที่เห็นในต่างประเทศ การจูโจมจะมาในลักษณะการจารกรรม การก่อการร้าย ในวิถีของโลกดิจิทัล สาเหตุเหล่านี้ทำให้ประเทศไทยมีความตระหนักถึงศักยภาพทางไซเบอร์ที่มีต่อความมั่นคงของชาติมากยิ่งขึ้น ขณะนี้หลายประเทศทั่วโลกพยายามพัฒนาขีดความสามารถในโลกดิจิทัลของตนเพื่อประกาศว่าตนมีศักยภาพที่จะสร้างความได้เปรียบในการแข่งขัน อย่างไรก็ตาม หากยิ่งต้องพึ่งพาไซเบอร์มากเพียงใดก็จะยิ่งเป็นการเพิ่มโอกาสเสี่ยงที่จะเกิดเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงของชาติจากไซเบอร์มากขึ้น เพราะลักษณะสำคัญของไซเบอร์คือความเร็วในการแพร่กระจาย และปราศจากพรมแดนในการจู่โจม (ธาราทิพย์ กัลยาณมิตร, 2560) ดังนั้นกองทัพไทยจึงมีการเตรียมการดำเนินการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ดังนี้

กระทรวงกลาโหมและกองบัญชาการกองทัพไทยได้ตั้งหน่วยงานสำคัญเพื่อปฏิบัติการในมิติไซเบอร์ในแง่ของการรับมือกับภัยคุกคามรูปแบบใหม่ ได้แก่

1. ศูนย์ไซเบอร์ กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม กระทรวงกลาโหม (ศซบ.ทสอ.กห.) จัดตั้งขึ้นเมื่อ 1 ต.ค. 2558 ตามยุทธศาสตร์ไซเบอร์เพื่อการป้องกันประเทศกระทรวงกลาโหม พ.ศ. 2558 เพื่อให้เป็นหน่วยงานหลักประสานงานด้านไซเบอร์ในภาพรวมของกระทรวงกลาโหมเชื่อมโยงนโยบายด้านไซเบอร์กับระดับรัฐบาลและนำไปสู่การดำเนินการของหน่วยไซเบอร์ระดับปฏิบัติและดำเนินการสร้างความร่วมมือด้านไซเบอร์กับหน่วยงานรัฐและภาคเอกชนที่เกี่ยวข้องทั้งในและต่างประเทศ

2. กองปฏิบัติการสงครามเครือข่าย สำนักปฏิบัติการ กรมยุทธการทหาร (กสค.สปก.ยก.ทหาร) จัดตั้งขึ้นเมื่อ พ.ค. 2556 โดยสภากลาโหมมีมติอนุมัติให้กองทัพไทยจัดตั้งหน่วยงานรับผิดชอบทางด้านไซเบอร์ โดยกองมีความรับผิดชอบหลักในการจัดการและบูรณาการการปฏิบัติทางไซเบอร์ในระดับกองทัพไทย เช่น จัดทำยุทธศาสตร์การปฏิบัติการไซเบอร์ของกองทัพไทย และ

มีหน้าที่รับผิดชอบในฐานะเป็นองค์ประกอบหนึ่งของศูนย์ประสานการรักษาความปลอดภัยระบบคอมพิวเตอร์กระทรวงกลาโหม (MODCERT)

3. กองรักษาความปลอดภัยสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร (กรส.ศทศ.สส.ทหาร) มีหน้าที่ในการดำเนินการตรวจสอบ วิเคราะห์ ป้องกัน กู้คืน และประเมินผลการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ จัดทำแนวทาง หลักการ ระเบียบ มาตรการ และแผนการดำาเนินงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศรวมทั้งพิจารณาเสนอแนะ การดำเนินการต่อภัยคุกคามที่มีผลกระทบต่อระบบสารสนเทศของกองทัพไทย และมีหน้าที่รับผิดชอบในฐานะเป็นองค์ประกอบหนึ่งของศูนย์ประสานการรักษาความปลอดภัยระบบคอมพิวเตอร์กระทรวงกลาโหม (MODCERT)

จากศูนย์ไซเบอร์ที่ได้กล่าวมานั้นแสดงให้เห็นว่าปัจจุบันกองบัญชาการกองทัพไทยมีหน่วยงานหลักที่รับผิดชอบด้านความมั่นคงปลอดภัยทางไซเบอร์อยู่ 2 หน่วยงาน คือ กองปฏิบัติการสงครามเครือข่าย สำนักปฏิบัติการ กรมยุทธการทหารและกองรักษาความปลอดภัยสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร ซึ่งทั้ง 2 หน่วยงานมีภารกิจทางด้านไซเบอร์ที่ต้องรับผิดชอบเหมือนกันแต่มีสายการบังคับบัญชาที่แยกกัน ด้วยสาเหตุที่มีภารกิจใกล้เคียงกัน ผู้บริหารจึงเห็นถึงความเชื่อมโยงระหว่างทั้งสองหน่วยงาน จึงปรับเปลี่ยนโครงสร้างของทั้งสองหน่วยงานดังกล่าวให้เป็น“ศูนย์ไซเบอร์ทหาร”ขึ้นตรงกับสำนักผู้บัญชาการทหารสูงสุด

เมื่อมีโครงสร้างที่พร้อมปฏิบัติงานแล้ว กองทัพไทยยังมีแนวทางการพัฒนาด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ผ่านการออกนโยบาย ดังนี้

1. นโยบายการสร้างความร่วมมือทางไซเบอร์ระหว่างประเทศ ผ่านการสร้างเครือข่ายของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (CERT) ในแต่ละประเทศทั้งใน กลุ่มประเทศสมาชิกอาเซียน ระดับภูมิภาคเอเชีย และนอกประเทศในภูมิภาคอื่น ๆ โดยเน้นความร่วมมือและการตอบสนองต่อสถานการณ์ฉุกเฉินทางไซเบอร์ เมื่อมีเหตุการณ์ฉุกเฉินประเทศไทยจะสามารถรับมือได้ทันท่วงที เพราะการทำางานร่วมกันจะเป็นจุดแข็งต่อการตอบสนองต่อภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ ทั้งนี้ ยังสามารถแลกเปลี่ยนข้อมูล นวัตกรรมที่จำเป็นในการรับมือภัยคุกคามได้อีกด้วย และในอนาคตการร่วมมือจะแปรรูปไปเป็นความร่วมมือด้านไซเบอร์ระดับภูมิภาคและระดับโลกอย่างเป็นรูปธรรม

2. นโยบายการเชื่อมโยงการทำงานด้านไซเบอร์ในภาพรวมทั้งในส่วนของกระทรวงกลาโหมและกองบัญชาการกองทัพไทย ซึ่งทั้งสองหน่วยงานนั้นเป็นทั้งหน่วยนโยบายและหน่วยปฏิบัติ ทั้งนี้ยังรวมไปถึงการปฏิบัติงานยามปกติและการปฏิบัติในสถานการณ์วิกฤติ การมี Cyber Command จึงเป็นสิ่งสำคัญ เมื่อเกิดสงครามไซเบอร์ (Cyber War) การมีเอกภาพในการ

บังคับบัญชา (Unity of Command) จะทำให้กำลังพลของนักรบไซเบอร์สามารถปฏิบัติงานได้ตามวัตถประสงค์ได้อย่างเต็มที่

3. นโยบายรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ที่สร้างความความเข้าใจถึงบริบทและความรุนแรงของภัยคุกคามด้านไซเบอร์ เข้าใจภาพใหญ่ของภัยคุกคามที่กำลังจะเกิดขึ้นในอนาคตว่ามีความหลากหลายเพียงใด และจำเป็นจะต้องสร้างความต่อเนื่องในบทบาทหน้าที่ของตนในทุกตำแหน่งระดับชั้น ทุกภาคส่วนของรัฐ ไม่ว่าจะเป็นกระทรวงกลาโหม กระทรวงมหาดไทย กระทรวงยุติธรรม กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ฯลฯ

4. นโยบายการผลักดันให้เรื่องความมั่นคงทางไซเบอร์ไปบรรจุในแผนป้องกันประเทศ หรือแผนต่าง ๆ ที่จัดทำขึ้นเพื่อนำมาเป็นกรอบการปฏิบัติในกองทัพไทย โดยให้ถือว่างานด้านความมั่นคงปลอดภัยทางไซเบอร์ในปัจจุบันนั้นไม่นับว่าเป็นงานทางเทคนิคหรือนโยบาย จำเป็นจะต้องมีแผนต่าง ๆ มารองรับความมั่นคงปลอดภัยทางไซเบอร์

เมื่อกองทัพมีแนวนโยบายเป็นกรอบใหญ่ในการปฏิบัติงานแล้ว กลยุทธ์ย่อยที่ตามจึงจำเป็นจะต้องสอดคล้องกับแนวปฏิบัติใหญ่โดยสามารถแบ่งได้เป็น กลยุทธ์เชิงรุก (Offensive Tactics) และกลยุทธ์เชิงรับ (Defensive Tactics) ดังนี้

1. กลยุทธ์เชิงรุก (Offensive Tactics)

1) การสร้างเครือข่ายไซเบอร์ในภาพรวม ความมั่นคงปลอดภัยด้านไซเบอร์นั้นอาศัยการแก้ปัญหาด้วยความร่วมมือที่เป็นทีม ไม่ว่าจะเป็นกระทรวงกลาโหมหรือกองบัญชาการกองทัพไทยที่จะต้องเป็นหนึ่งเดียวกันในด้านไซเบอร์ และจำเป็นจะต้องหารือในฐานะของทีมประเทศไทยอีกด้วย ซึ่งจะต้องสามารถบูรณาการการทำงานร่วมกันได้

2) การส่งเสริมให้หน่วยงานทหารในการวิจัยที่เกี่ยวข้องกับไซเบอร์ของกองทัพโดยหน่วยงานที่มีศักยภาพในการทำวิจัย ได้แก่ กรมวิทยาศาสตร์และเทคโนโลยีกลาโหม สถาบันเทคโนโลยีป้องกันประเทศ โดยทั้งสองหน่วยงานนี้ควรสามารถทำการวิจัยที่สามารถนำไปใช้ประโยชน์ได้ในอนาคต

3) การสนับสนุนด้านการข่าว โดยเฉพาะหน่วยข่าวแห่งชาติ ฝ่ายพลเรือน หรือกรมข่าวทหาร ศูนย์รักษาความปลอดภัย เป้นต้น ที่ต้องคอยสอดส่องดูแลความเคลื่อนไหว (Cyber Intelligence) ของสถานการณ์ที่เกิดขึ้น เพื่อนำไปจัดทำแผนการบริหารจัดการกับภัยคุกคามในอนาคต

4) การหาเจ้าภาพหลักในการฝึกร่วมกันระหว่างหน่วยงานด้านไซเบอร์ของกองทัพโดยหน่วยงานหลักจะต้องพิจารณามอบอำนาจเจ้าภาพผู้ประสานงานมีเครื่องมือที่ชัดเจนที่จะสามารถรวมหน่วยงานที่เกี่ยวข้องในการฝึกปฏิบัติด้วยกันได้ นอกจากนี้ควรจะต้องมีการฝึกร่วมกันเมื่อเกิดสถานการณ์ฉุกเฉินทางไซเบอร์ เพื่อเตรียมพร้อมโยกย้ายกำลังได้ตลอดเวลา

5) เพื่อสร้างความสอดคล้องกับโยบายที่วางไว้ รัฐบาลนำเรื่องไซเบอร์บรรจุเป็นวิชาในหลักสูตรโรงเรียนทหารทุกระดับทุกเหล่าทัพหน่วยงาน ควรประกอบไปด้วยวิชาการเรียนพื้นฐาน วิชาเรียนแบบภาคปฏิบัติ เชิงเทคนิค รวมไปถึงการเวทีแลกเปลี่ยนความคิดเห็นทางวิชาการที่เกี่ยวข้องกับประเด็นด้านไซเบอร์ลงไปในหลักสูตร เพื่อเป็นการสร้างความตระหนักรู้ตั้งแต่ต้นก่อนที่จะรับเข้ามาปฏิบัติงานจริง

2. กลยุทธ์เชิงรับ (Defensive Tactics)

1) การสร้างความตระหนักรู้ (Awareness) ให้กับผู้เกี่ยวข้อง เจ้าหน้าที่ กำลังพลและประชาชนทั่วไป กลุ่มคนที่ได้กล่าวมานั้นจะต้องมีคือความตระหนักรู้ต่อภัยคุกคามจากไซเบอร์ โดยจะต้องเรียนรู้ตั้งแต่ภัยคุกคามตั้งแต่ในระดับเล็กน้อย เช่น การใช้สื่อสังคมออนไลน์ การใช้จดหมายอิเล็กทรอนิกส์ (Email) การทำธุรกรรมทางการเงิน ไปจนถึงภัยคุกคามระดับที่เป็นความมั่นคงสูงของประเทศ ความตระหนักรู้เบื้องต้นนั้นจะช่วยให้เกิดความระวังตัวในการดำเนินชีวิตในโลกดิจิทัลมากขึ้น

2) การเตรียมความพร้อมในการตอบสนองต่อสถานการณ์ฉุกเฉินได้ทันท่วงทีและฟื้นคืนระบบกลับสู่ภาวะปกติโดยเร็วที่สุด (Cyber Resilience) กลยุทธ์ในข้อนี้จะถูกใช้เมื่อกองทัพถูกโจมตีโดยอาวุธทางไซเบอร์แล้วจำเป็นจะต้องฟื้นตัวหลังการโจมตีให้ได้เร็วที่สุดเพื่อทำให้ประเทศสามารถดำเนินการต่อไปได้ ทั้งนี้เนื่องจากความเสี่ยงทางไซเบอร์นั้นสามารถเกิดขึ้นได้ตลอดเวลาและไม่มีขอบเขตในการขวางกั้น ดังนั้นกองทัพจำเป็นจะต้องเน้นกลยุทธ์เชิงรับด้านนี้มากที่สุด

3) หน่วยงานทางด้านไซเบอร์ควรมีกระบวนการรับมือกับภัยคุกคามด้านไซเบอร์หลายรูปแบบธรรมชาติของภัยคุกคามทางไซเบอร์นั้น มีการเคลื่อนไหวแบบไม่หยุดนิ่ง (Dynamic) ดังนั้น วิธีการรับมือ คือ ต้องสามารถนำไปใช้ได้ (Practical) และพร้อมรับมือในหลายรูปแบบ

4) การผลิตและพัฒนาบุคลากรด้านไซเบอร์กองทัพควรต้องผลิตบุคลากรด้านไซเบอร์เพิ่มเติม ด้วยการคัดเลือกกำลังพลที่มีพื้นฐานความรู้ด้านไซเบอร์ออกมาฝึกฝนและพัฒนาให้สามารถปฏิบัติงานด้านไซเบอร์ได้ โดยอาจใช้ช่องทางที่กองทัพมีอยู่ รวมไปถึงการแบ่งปันข้อมูลระหว่างหน่วยงานในประเด็นที่เกี่ยวข้องกับไซเบอร์หน่วยงานต่าง ๆ ควรเปิดเผย/ให้ข้อมูลการถูกแฮกหรือการโจรกรรมข้อมูลให้กับหน่วยงานกลางทางด้านไซเบอร์ เพื่อที่จะช่วยกันอุดรอยรั่วที่เกิดขึ้นและนำมาใช้เป็นบทเรียนในครั้งต่อไป (ธาราทิพย์ กัลยาณมิตร, 2560)

นอกจากกลยุทธ์เชิงรุกและเชิงรับที่ได้กล่าวมานั้นกองทัพยังมีการดำเนินงานในด้านการพัฒนา Hardware ของระบบคอมพิวเตอร์ เช่น การวิเคราะห์ การบริหารความเสี่ยงด้านความปลอดภัยของโครงสร้างพื้นฐาน เทคโนโลยีสารสนเทศ กองทัพสามารถตรวจรหัสหาช่องโหว่หรือ

จุดบกพร่องของตนได้ โดยในบางครั้งกองทัพอาจจำเป็นจะต้องพึ่งพิง Outsourcing เพื่อเพิ่มประสิทธิภาพและอุดช่องว่างความปลอดภัยทางไซเบอร์ หากมีเหตุการณ์ฉุกเฉินใด ๆ จะมี Computer Security Incident Response Team เข้ามาประเมินสถานการณ์ โดยเฉพาะสถานการณ์ด้านการข่าว ทั้งนี้ยังมีการเตรียมห้องปฏิบัติการ Cyber เพื่อจัดตั้งหน่วย SOC (Security Operation Center) ที่มีการจัดเวรยามเฝ้าระวังตลอด 24 ชั่วโมง

กองทัพยังมีการฝึกอบรมผ่านการทำ Workshop ให้กับเจ้าหน้าที่ในกองทัพให้รู้จักสิ่งบอกเหตุ ระดับของภัยคุกคามไซเบอร์ เพื่อสามารถส่งสัญญาณภัยคุกคามที่ตรวจพบต่อไปยังหน่วยงานที่รับผิดชอบต่อไปได้ รวมไปถึงการจัดให้มีกองทุนสำหรับการศึกษา ฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์สำหรับผู้มีศักยภาพให้ได้มีโอกาสเรียนรู้ในต่างประเทศ ในภาพรวมของกองทัพนั้น การตอบสนองต่อภัยคุกคามทางไซเบอร์ยังเป็นไปในทิศทางที่ดี โดยเฉพาะด้าน Cyber security แต่ยังขาดศักยภาพในการปฏิบัติการตามกลยุทธ์เชิงรุก เนื่องจากไม่มีกำลังพลที่เชี่ยวชาญทางไซเบอร์เพียงพอ

2.9.8 กระทรวงสาธารณสุขกับการรับมือภัยคุกคามไซเบอร์

การเข้าสู่ระบบเศรษฐกิจและสังคมเทคโนโลยีดิจิทัลส่งผลให้เกิดการเปลี่ยนแปลงทั้งโครงสร้างและรูปแบบกิจกรรมการดำเนินงานในทุกภาคส่วน โดยเฉพาะการที่ประชาชนจะได้รับบริการทางการแพทย์และสุขภาพที่ทันสมัย ทั่วถึงและเท่าเทียม สามารถพัฒนาระบบบริการสุขภาพอย่างมีประสิทธิภาพ กระทรวงสาธารณสุข ได้ผลักดันการขับเคลื่อนระบบสุขภาพด้วยเทคโนโลยีดิจิทัลผ่านยุทธศาสตร์เทคโนโลยีสารสนเทศสุขภาพ (e Health Strategy) มุ่งเน้นการพัฒนาที่สอดรับกับแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม (Digital Economy) และยังพิจารณาจากปัจจัยที่เกี่ยวข้อง รวมทั้งความสอดคล้องกับยุทธศาสตร์เทคโนโลยีดิจิทัลและ e Health ในระดับสากลเพื่อตอบปัญหาความท้าทายด้านสาธารณสุขในหลาย ๆ ด้าน เช่น

1. หน่วยบริการในสังกัดกระทรวงสาธารณสุขสามารถเชื่อมโยงกันด้วยเครือข่ายภายใน (MoPH Intranet) ได้อย่างปลอดภัยและได้มาตรฐานสากล
2. การขยายบริการ Internet ความเร็วสูง แบบพิเศษ ให้กับโรงพยาบาลส่งเสริมสุขภาพตำบลทุกแห่งทั่วประเทศ
3. การเชื่อมโยงเครือข่ายสารสนเทศภาครัฐ (GIN) ให้ครอบคลุมโรงพยาบาลชุมชนทุกแห่งทั่วประเทศ
4. การจัดการระบบสำรองข้อมูลของโรงพยาบาลศูนย์/ทั่วไปทุกแห่งทั่วประเทศ
5. การจัดต้นแบบระบบบริการด้านสุขภาพอัจฉริยะ (Smart Service: PHRs, EMR, Registration) รวมถึงผลิตภัณฑ์สุขภาพในหน่วยบริการที่มีความพร้อม

6. การออกกฎหมายในระบบสุขภาพที่ทันสมัยเชื่อมโยงกับการดำเนินงานของแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม

7. การบริหารจัดการ Health Digital Literacy ขนาดใหญ่เป็นแหล่งรวบรวมความรู้สุขภาพที่เหมาะสมกับประเทศไทย ประชาชนเข้าถึงและใช้ประโยชน์ได้อย่างสะดวกรวดเร็ว ช่วยตอบปัญหา คลายความสงสัย ป้องกันการเข้าใจผิดที่อาจก่อให้เกิดความเสี่ยงด้านสุขภาพ ยับยั้งการแพร่กระจายข้อมูลที่บิดเบือนในโลกโซเชียลได้ทันต่อสถานการณ์

8. การจัดให้มีระบบ Tele Health ที่มีคุณภาพสนับสนุนการให้บริการตรวจวินิจฉัยและให้คำปรึกษาระหว่างแพทย์ผู้เชี่ยวชาญกับแพทย์ในโรงพยาบาลที่ห่างไกล โดยเฉพาะโรงพยาบาลชายขอบจังหวัด

9. การพัฒนาบุคลากรในระบบสุขภาพให้มีศักยภาพในการใช้เทคโนโลยีดิจิทัลมาปรับกระบวนการทำงานให้มีประสิทธิภาพดียิ่งขึ้น

10. การบูรณาการเชื่อมโยงข้อมูลที่เกี่ยวข้องกับระบบสุขภาพร่วมกันระหว่างหน่วยงานในกระทรวงสาธารณสุข

e Health ที่จะกล่าวถึง ประกอบไปด้วย “e” และ “Health” “Health หรือ สุขภาพ” คือ ภาวะที่มีความพร้อมสมบูรณ์ทั้งทางร่างกายและจิตใจ การดูแลตนเอง การดูแลคนที่เรารัก และได้รับการดูแล “e” คือ electronic technology เช่น computer โทรศัพท์มือถือและแท็ปเล็ต อินเตอร์เน็ต และ Social Media “IT” คือ Information Technology หรือเทคโนโลยีสารสนเทศเมื่อเอามารวมกัน ก็คือ e Health หรือ Health IT ซึ่งก็คือเทคโนโลยีและบริการ ICT ที่เชื่อมโยงระหว่างผู้ให้บริการด้านสุขภาพและประชาชน เพื่อให้สามารถเข้าถึงบริการสุขภาพได้อย่างมีประสิทธิภาพ ทั่วถึง เป็นธรรมและปลอดภัย (สำนักงานปลัดกระทรวงสาธารณสุข ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร, 2560)

โครงการ e Health ได้รูปแบบมาจากการศึกษา การเชื่อมโยงข้อมูลสุขภาพของประเทศเอสโตเนีย (Estonia Healthcare) พบว่าประเทศเอสโตเนียมีประชากร ประมาณ 1.3 ล้านคน และเคยถูกโจมตีทาง cyber ในปี 2007 ส่งผลให้ระบบเทคโนโลยีสารสนเทศของรัฐบาลล้มเหลวทั้งหมด จึงพัฒนารูปแบบการจัดเก็บข้อมูลด้วย Cloud computing และใช้เทคโนโลยี Blockchain เพื่อการบริหารจัดการและสำรองข้อมูลอย่างปลอดภัย โดยเก็บข้อมูลทุกประเภทรวมถึงข้อมูลด้านสุขภาพของประชาชนในรูปอิเล็คทรอนิคส์ เน้นความปลอดภัยของข้อมูล ตามสากล คือ CIA ประกอบด้วย ความมั่นใจ (Confidentiality) ความสมบูรณ์(Integrity) และความพร้อมใช้งาน (Availability) ความสมบูรณ์ของระบบ(System Integrity) และความสมบูรณ์ของการดำเนินการ (Operational integrity) ความสมบูรณ์ของกระบวนการ (Process Integrity) คือ การพิสูจน์แหล่งที่มาของข้อมูล ระบบสามารถประกันการสื่อข้อมูลจะเป็นเรื่องที่มีประสิทธิภาพ ความถูกต้อง

ของข้อมูลผู้รับบริการ ร่วมกับความรอบคอบและโปร่งใสของผู้ปฏิบัติงานจะช่วยลดค่าใช้จ่าย ด้านสุขภาพ

eHealth Estonia ทำงานบน Backbone ที่เรียกว่า X-road ทำหน้าที่รับส่งข้อมูลระหว่างระบบคอมพิวเตอร์ต่าง ๆ อย่างเป็นอิสระต่อกัน แม้คอมพิวเตอร์แต่ละระบบจะใช้เทคโนโลยีแตกต่างกัน โดยอาศัยตัวแปลง (adapter) เพื่อให้สามารถรับส่งข้อมูลในรูปแบบที่ X-road เข้าใจ ด้วยเซิร์ฟเวอร์ที่มีความปลอดภัย (secure server) และหลักการเก็บข้อมูลแบบกระจาย (Distributed) จึงทำให้สามารถขยายจำนวนข้อมูลได้โดยไม่มีขีดจำกัด ความสำเร็จของเอสโตเนียเกิดจากการทำงานร่วมกัน ของ X-road, e-identity และ blockchain ร่วมกับความสามารถของรัฐในการเก็บข้อมูล ด้วยความโปร่งใส ประชาชนรู้ว่ารัฐเข้าถึงข้อมูลของตนประเภทใดบ้าง การนำเทคโนโลยี Blockchain มาปรับใช้ในประเทศไทย อาจพบข้อจำกัด เนื่องจาก

1. กฎหมายเทคโนโลยี ที่มีใช้ในปัจจุบัน ไม่มีส่วนใดเข้าได้กับ Blockchain
2. Blockchain ต้องปรับให้เป็นเข้ากันได้ กับระบบสุขภาพที่มีขนาดใหญ่ขึ้น
3. Blockchain ต้องอาศัยความเร็วในการประมวลผลอย่างน้อย 100 มิลลิวินาที
4. ด้านความรับผิดชอบของการบันทึก เคลื่อนย้ายและวางแผนใช้งานข้อมูลในอนาคต

สถานการณ์ปัจจุบันที่กระทรวงสาธารณสุขกำลังเผชิญอยู่ คือ การปฏิวัติดิจิทัลสร้างการทดแทนการทำงานบนข้อมูลเชิงเส้นไปสู่การหมุนเวียนและใช้ข้อมูลหลายมิติพร้อม ๆ กันโดยมีเส้นทางสำคัญไปสู่จุดหมายดังกล่าว คือ ระบบอัจฉริยะในการประมวลผลเพื่อการตัดสินใจอย่างมีประสิทธิภาพ ความโปร่งใสและธรรมภิบาลของข้อมูลมีความน่าเชื่อถือ การปฏิวัติดิจิทัลทำให้เกิดนวัตกรรมเปลี่ยนแปลงโลกสำคัญ 4 เรื่อง คือ

1. ปัญญาประดิษฐ์ (Artificial Intelligence: AI) เป็นเทคโนโลยีใหม่ที่สามารถทำการตัดสินใจและตอบสนองภายในเสี้ยววินาทีด้วยโปรแกรมการตัดสินใจจากประสบการณ์ที่เก็บรวบรวมในฐานข้อมูลคุณภาพขนาดใหญ่ (Big data) การใช้เทคโนโลยีปัญญาประดิษฐ์ของเหมาะสมกับระบบบริการทางการแพทย์ เช่น ผู้ช่วยในโรงพยาบาลเช่น โปรแกรม IBM Watson ที่เข้ามามีบทบาทสำคัญในการบริหารจัดการข้อมูลของผู้ป่วยและช่วยในการตัดสินใจทางการแพทย์

2. บล็อกเชน (Blockchain) คือ เทคโนโลยีที่ใช้บันทึกข้อมูลแบบกระจาย (distributed ledger) เพื่อแก้ปัญหาความไม่ปลอดภัยในการเชื่อมต่อข้อมูลความท้าทายของการใช้ blockchain ในระบบข้อมูลสุขภาพและการแพทย์ที่มีหลายภาคส่วน คือ ปัจจุบัน blockchain ยังไม่มี standard platform จึงยังไม่สามารถเชื่อมต่อข้ามเครือข่ายได้ ความท้าทายด้านการตรวจสอบข้อมูลในทางการแพทย์ที่มีปริมาณมากพร้อมกันทั้งเครือข่ายตลอด 24 ชั่วโมง จำเป็นต้องใช้คอมพิวเตอร์ที่มีศักยภาพสูงมาก

3. การประมวลผลแบบกลุ่มเมฆ (Cloud Computing) คือระบบโปรแกรมคอมพิวเตอร์ที่ประมวลผลบนเครือข่ายอินเทอร์เน็ตแทนเครื่องคอมพิวเตอร์เป็นลักษณะการทำงานที่ใช้ทรัพยากรมากมายบนเครือข่ายอินเทอร์เน็ต เช่น พื้นที่เก็บข้อมูล โปรแกรมต่าง ๆ ผ่านอุปกรณ์คอมพิวเตอร์ที่สามารถเชื่อมต่ออินเทอร์เน็ตได้จึงสามารถเข้าถึงข้อมูลล่าสุดในระบบจากที่ใดก็ได้ ผ่านอุปกรณ์ ลดค่าใช้จ่ายในการดูแล Software และ Server ของแต่ละหน่วยงาน ความท้าทายของ cloud computing คือ หากอินเตอร์เน็ตที่มีความเร็วต่ำระบบจะไม่สามารถทำงานได้

4. Big Data Analytics คือ เทคโนโลยีจัดการประมวลและวิเคราะห์ข้อมูลที่มีปริมาณมหาศาล (High Volume) มีความหลากหลาย (High Variety) ทั้งข้อมูลที่เป็นข้อความ ตัวเลข ภาพ และข้อมูลอื่น ๆ และจัดการข้อมูลที่มีการเปลี่ยนแปลงเคลื่อนไหวต่อเนื่องตลอดเวลา (High Velocity) จนไม่สามารถจัดการด้วยวิธีทั่วไปได้อย่างรวดเร็วสามารถหยิบข้อมูลที่มีความไม่ชัดเจนและตรวจสอบข้อมูลที่บันทึกผิดพลาดได้แต่ไม่สามารถแก้ปัญหาความจงใจบันทึกผิดพลาดจากการขาดความรับผิดชอบ (Accountability) ได้ (กองยุทธศาสตร์และแผนงาน, 2561) ข้อมูลที่เก็บนั้นจะมีในรูปแบบ ข้อมูลเชิงพฤติกรรม เช่น การรับประทานอาหาร การออกกำลังกาย ภาพถ่ายทางการแพทย์ เวชระเบียนที่เป็นลายมือบันทึกเสียง รายละเอียดการตรวจรักษา เป็นต้น

เนื่องจากความเสี่ยงที่จะเกิดขึ้นกับระบบไซเบอร์ของสาธารณสุขนั้นมีมากและยังส่งผลกระทบอีกมหาศาล กระทรวงสาธารณสุขจึงมีแผนการรับมือ ดังนี้

มาตรการทางไซเบอร์ที่กระทรวงใช้อยู่ในปัจจุบันประกอบด้วย การจัดตั้งทีมเฝ้าระวัง Cyber Security 24 ชั่วโมง สำหรับเครือข่ายหลัก มีแนวปฏิบัติให้แก่หน่วยงาน กรณีเร่งด่วนเมื่อเกิดเหตุ พร้อมทั้งมีแนวทางการป้องกัน เพิ่มบทบาท CIO ทุกระดับในการบริหารจัดการคุณภาพระบบ IT มีแผนบริหารความต่อเนื่อง และปฏิบัติตามนโยบายด้านความมั่นคง ปลอดภัยสารสนเทศกระทรวงสาธารณสุข นอกจากนี้ยังแผนมาตรการไซเบอร์ในอนาคตโดยการเพิ่มประสิทธิภาพระบบ Cyber Security ในทุกหน่วยงาน พัฒนาทักษะด้าน Cyber Security แก่บุคลากรในกระทรวงสาธารณสุข จัดตั้งศูนย์เฝ้าระวัง Cyber Security ด้านสาธารณสุข (Health-CERT) ร่วมกับ ETDA จัดทำแผนปฏิบัติการประเมินช่องโหว่ทุกหน่วยงาน (โอภาส การย์กวินพงศ์, 2560)

2.10 งานวิจัยที่เกี่ยวข้อง

งานวิจัยส่วนใหญ่ที่มีประเด็นเกี่ยวข้องกับภัยคุกคามทางไซเบอร์จะเป็นในรูปแบบของการประเมินหน่วยงานทางเทคนิคและกลยุทธ์ โดยจะแบ่งเป็นฝ่ายทหารและฝ่ายพลเรือน สำหรับฝ่ายทหารนั้นงานวิจัยละการศึกษาส่วนมากจะครอบคลุมในส่วนของยุทธศาสตร์การทหาร การปฏิบัติการในสนามรบไซเบอร์ซึ่งจะแตกต่างกับงานวิจัยที่ศึกษาโดยพลเรือนซึ่งส่วนมากจะเน้นเรื่องยุทธศาสตร์

ในภาพรวม ถึงแม้จะเน้นในเรื่องการเพิ่มศักยภาพบุคลากรและความตระหนักรู้เหมือนกัน แต่สำหรับของพลเรือนยังขาดการเน้นเชิงลึกในเรื่องของกลยุท์เชิงรุกและเชิงรับที่จะนำไปสู่การบรรลุยุทธศาสตร์ที่วางไว้ ประเทศไทยมีการตั้งรับที่ดีแต่ยังขาดนโยบายเชิงรุกที่จะสร้างความเป็นหนึ่งในเรื่องไซเบอร์ หรือในอีกแง่หนึ่งคือสร้างความแข็งแกร่งให้แก่รัฐเพื่อข่มขู่ฝ่ายตรงข้ามที่จะเข้ามาโจมตี โดยในส่วนนี้จะขอยกงานวิจัยทั้งในส่วนที่ศึกษาโดยฝ่ายกองทัพและฝ่ายพลเรือนเพื่อให้เห็นถึงความแตกต่างและสามารถชี้ให้เห็นช่องว่างที่ต้องการเติมเต็มได้ ดังนี้

สงคราม ดอนนางพาและธนบดี ตันหยง เสนอวิจัยในหัวข้อ การพัฒนากำลังพลของกองทัพบกเพื่อรองรับสงครามไซเบอร์ เสนอวิทยาลัยเสนาธิการทหาร เพื่อประกอบการศึกษาตามหลักสูตรเสนาธิการทหาร รุ่นที่ 54 พ.ศ. 2556 (สงคราม ดอนนางพา & ธนบดี ตันหยง, 2556)

การวิจัยครั้งนี้มีความมุ่งหมายเพื่อหาแนวทางการพัฒนากำลังพลของกองทัพบกที่มีหน้าที่รับผิดชอบในสายงานเทคโนโลยีสารสนเทศโดยมุ่งไปที่ ศูนย์เทคโนโลยีสารสนเทศที่เป็นหน่วยขึ้นตรงของกรมการทหารสื่อสาร เป้าหมายของวิจัยชิ้นนี้ มุ่งตอบคำถามว่าหน่วยงานดังกล่าวมีขีดความสามารถที่จะปฏิบัติงานด้านสงครามไซเบอร์ได้หรือไม่ และถ้าหากต้องการพัฒนากำลังพลของหน่วยจะต้องพัฒนาไปในแนวทางใดจึงจะทำให้หน่วยสามารถมีประสิทธิภาพรองรับต่อภารกิจที่อาจเกิดขึ้นในงานสงครามไซเบอร์

โดยผู้วิจัยต้องการเสนอแนะหลักสูตรการเพิ่มพูนความรู้ทางด้านคอมพิวเตอร์ทางด้านต่าง ๆ ทั้งทางด้านงานเครือข่าย และระบบปฏิบัติการที่แตกต่างกัน งานวิจัยนี้เป็นการวิจัยเชิงคุณภาพซึ่งผู้วิจัยได้ดำเนินการวิจัยเชิงพรรณนา โดยการวิเคราะห์เอกสารที่เกี่ยวข้อง การสัมภาษณ์ผู้ทรงคุณวุฒิ รวมทั้งจากการสังเกตของผู้วิจัยเอง โดยผู้วิจัยได้ตั้งสมมติฐานงานวิจัยครั้งนี้ว่า “จะทำอย่างไรถึงจะสามารถพัฒนากำลังพลของหน่วยที่มีความรับผิดชอบในงานด้านเทคโนโลยีสารสนเทศให้สามารถปฏิบัติงานด้านสงครามไซเบอร์ได้อย่างมีประสิทธิภาพ แนวทางการศึกษาน่าจะไปในรูปแบบใดและอะไรจะเป็นตัวชี้วัดถึงความสำเร็จต่อแนวทางการพัฒนากำลังพลดังกล่าว”

ผลการวิจัยสรุปได้ว่าปัญหาเกิดจากการบรรจุกำลังพลที่มีความรู้และจบการศึกษาไม่ตรงกับตำแหน่งงานที่บรรจุทำให้กำลังพลไม่มีขีดความสามารถในการปฏิบัติงานตามวัตถุประสงค์ได้ ซึ่งสาเหตุนี้เป็นปัจจัยหลักต่อขีดความสามารถของหน่วยงาน ตลอดจนการฝึกอบรมที่มีอยู่ในปัจจุบันของหน่วยเพื่อเพิ่มพูนความรู้ก็จะเป็นโปรแกรมแอพพริเคชั่นซึ่งเป็นระดับของผู้ใช้งานเท่านั้น ไม่สามารถนำมาใช้ในงานของสงครามไซเบอร์ได้ งานวิจัยจึงเสนอแนะการแก้ไขปัญหาโดยมุ่งนำเอาหลักการพัฒนาทรัพยากรมนุษย์ที่หน่วยงานภายนอก หรือองค์กรต่าง ๆ นำมาใช้ โดยมีการนำเทคนิคของการฝึกอบรมและการประเมินผลงานในแต่ละขั้นมาเป็นตัวชี้วัดเพื่อชี้ให้เห็นถึงผลของความสำเร็จ ซึ่งตรงจุดนี้เป็นสิ่งสำคัญอย่างยิ่งต่อเป้าหมายและวัตถุประสงค์ที่วางไว้ในขั้นแรกของงานวิจัยเล่มนี้ ในส่วนข้อเสนอแนะนั้นเห็นควรวางแผนการพัฒนาโดยเสนอแผนพัฒนาที่ต้องคำนวนระยะเวลาที่ต้องการ

ผลิตบุคลากร ว่าควรใช้ระยะเวลากี่ปี และมีการวางเป้าหมายเพียงใด หรือทำแผนพัฒนาต่อเนื่องเพื่อผลิตบุคลากรตามเป้าหมายที่ได้วางไว้

ในประเด็นการพัฒนาบุคลากรทางไซเบอร์ ภัทราพร เรืองแสงศิลป์ (2550) ได้ทำการวิจัยเรื่องแนวทางการพัฒนาศักยภาพบุคลากรด้านเทคโนโลยีสารสนเทศในอุตสาหกรรมซอฟท์แวร์ อุตสาหกรรมซอฟท์แวร์ถือเป็นหนึ่งในห้าอุตสาหกรรมยุทธศาสตร์ของประเทศไทยที่มีความสำคัญต่อการพัฒนาประเทศ อุตสาหกรรมนี้ต้องใช้ทรัพยากรมนุษย์เป็นทรัพยากรหลักในการสร้างผลิตภัณฑ์ต่าง ๆ งานวิจัยชิ้นนี้ศึกษาแนวทางการพัฒนาบุคลากรด้านเทคโนโลยีสารสนเทศของประเทศสหรัฐอเมริกาเกี่ยวกับ คุณลักษณะ (ทักษะ ความรู้ ความสามารถ) ที่เหมาะสมของทรัพยากรมนุษย์ที่มีหน้าที่สร้างผลิตภัณฑ์ซอฟท์แวร์ เพื่อนำไปปรับประยุกต์ใช้เป็นแนวทางในการพัฒนาศักยภาพบุคลากรไทยได้ การศึกษาครั้งนี้มีวัตถุประสงค์เพื่อ

1. ศึกษาแนวทางของรัฐในการส่งเสริมสนับสนุนบุคลากรด้านเทคโนโลยีสารสนเทศในอุตสาหกรรมซอฟท์แวร์
2. ศึกษาแนวทางที่เหมาะสมในการพัฒนาบุคลากรเทคโนโลยีสารสนเทศในอุตสาหกรรมซอฟท์แวร์
3. ศึกษาถึงบทบาทของนักพัฒนาทรัพยากรมนุษย์

นอกจากเรื่องการพัฒนาบุคคลากรที่มีประสิทธิภาพแล้ว งานวิจัยเรื่องยุทธศาสตร์การพัฒนากำลังพล ของกองทัพไทยเพื่อต่อต้านภัยคุกคามไซเบอร์ในทศวรรษหน้าของ ปรัชญา ฮวดปากน้ำ เพื่อประกอบการศึกษาตามหลักสูตรเสนาธิการทหาร รุ่นที่ 57 พ.ศ. 2556 ยังชี้ให้เห็นถึงการพัฒนายุทธศาสตร์การสู้รบทางไซเบอร์ ซึ่งเป็นส่วนของกระบวนการ มีรายละเอียดดังนี้

การวิจัยเรื่องยุทธศาสตร์การพัฒนากำลังพลของกองทัพไทยเพื่อต่อต้านภัยคุกคามไซเบอร์ในทศวรรษหน้าเป็นการวิจัยเชิงคุณภาพ ประกอบด้วยการวิจัยเชิงเอกสาร และการสัมภาษณ์เชิงลึกมีวัตถุประสงค์เพื่อ (1) ศึกษาปัญหาความพร้อมด้านขีดสมรรถนะของกำลังพลกองทัพไทยสำหรับการต่อต้านภัยคุกคามไซเบอร์(2) ดำเนินการเตรียมแผนสำหรับการบูรณาการ ความรู้ ความสามารถ ทักษะ เจตคติ ให้กำลังพลของกองทัพไทยมีขีดสมรรถนะเพียงพอในการปฏิบัติการต่อต้านภัยคุกคามไซเบอร์และ (3) กำหนดยุทธศาสตร์แนวทางพัฒนากำลังพลกองทัพไทยสำหรับต่อต้านภัยคุกคามไซเบอร์ให้มีความพร้อมรับสถานการณ์ในห้วงสิบปีข้างหน้าการเก็บรวบรวมข้อมูล ดำเนินการโดยการรวบรวมจากเอกสารวิชาการด้านความมั่นคงปลอดภัยไซเบอร์และการสัมภาษณ์เชิงลึกจากผู้ให้ข้อมูลสำคัญ ได้แก่ ผู้เชี่ยวชาญจากภาคเอกชน และผู้รับผิดชอบโดยตรงจากกองบัญชาการกองทัพไทย กองทัพบก กองทัพเรือ กองทัพอากาศ นำมาวิเคราะห์จุดอ่อน จุดแข็ง โอกาส และอุปสรรค ภายใต้สภาวะแวดล้อมปัจจุบันและอนาคตในระยะสิบปีข้างหน้าเพื่อกำหนดเป็นยุทธศาสตร์ผลการวิจัยทำให้ทราบถึง

(1) ปัญหาความไม่พร้อมของหน่วยงานและกำลังพลของกองทัพไทยตลอดจนภัยคุกคามในปัจจุบันและแนวโน้มของภัยคุกคามที่จะเกิดขึ้นในอนาคตและส่งผลกระทบต่อความปลอดภัยของการใช้ข้อมูลข่าวสารในการปฏิบัติงานรักษาความมั่นคงของกองทัพไทยบนพื้นฐานของความปลอดภัยของข้อมูลหรือ Cia 3 ประการ ได้แก่ การรักษาความลับของข้อมูล การรักษาความคงสภาพของข้อมูลหรือความสมบูรณ์ของข้อมูล(Integrity) และความพร้อมใช้งานของข้อมูล (Availability) สิ่งที่จำเป็นอย่างยิ่งในการที่จะรับมือกับปัญหาหรือภัยคุกคามต่าง ๆ เหล่านี้ประการหนึ่ง คือ การสร้างความตระหนัก (Awareness) ให้แก่บุคลากรภายในองค์กร (2) การเตรียมแผนสำหรับการบูรณาการความรู้ ความสามารถ ทักษะ เจตคติ ให้กำลังพลของกองทัพไทยมีขีดสมรรถนะเพียงพอในการปฏิบัติการต่อต้านภัยคุกคามไซเบอร์โดยการเสริมสร้างองค์ความรู้ทั้งในด้านทฤษฎี และการฝึกฝนให้เกิดความเชี่ยวชาญในการปฏิบัติการต่อต้านภัยคุกคามไซเบอร์ ทั้งการป้องกัน (Prevent) ค้นหา (Detect) และตอบสนองเหตุการณ์ (Incident Response) ตลอดจนการปรับเจตคติให้กับกำลังพลของกองทัพมีความตื่นตัวเพิ่มความระมัดระวังในการปิดช่องโหว่ต่าง ๆ ทั้งในระหว่างการปฏิบัติงานและการใช้ชีวิตประจำวัน ไม่ให้ผู้ไม่ประสงค์ดีสามารถใช้ช่องทางไซเบอร์เข้าโจมตีได้โดยง่ายตลอดจนทราบถึงความจำเป็นในการปรับปรุงโครงสร้างหน่วยงานสงครามไซเบอร์ของกองทัพ จัดเตรียมสรรหาผลิตและพัฒนาบุคลากรสำหรับการต่อต้านภัยคุกคามไซเบอร์และ (3) ได้ยุทธศาสตร์แนวทางพัฒนากำลังพลกองทัพไทยสำหรับต่อต้านภัยคุกคามไซเบอร์ให้มีความพร้อมรับสถานการณ์ในห้วงสิบปีข้างหน้าโดยมีรูปแบบของยุทธศาสตร์และแผนการพัฒนากำลังพลของกองทัพไทยสำหรับต่อต้านภัยคุกคามไซเบอร์ (ปรัชญา ฮวดปากน้ำ, 2559)

และในประเด็นเดียวกันนั้น ชัยยศ ลิลิตวงษ์ ได้ศึกษาวิจัยเรื่อง “การเสริมสร้างศักยภาพไซเบอร์ในระดับกระทรวงกลาโหม” โดยศึกษาแนวคิดการดำเนินการไซเบอร์นานาประเทศ โดยเฉพาะสหประชาชาติ และสหรัฐอเมริกา สำหรับกระทรวงกลาโหมไทย ศูนย์บัญชาการไซเบอร์กลาโหมได้รับอนุมัติหลักการโดยรัฐมนตรีว่าการกระทรวงกลาโหมจัดตั้งหน่วยรับผิดชอบด้านไซเบอร์ของกระทรวงกลาโหมในลักษณะหน่วยบัญชาการไซเบอร์ (Cyber Command) ให้มีเอกภาพงานด้านไซเบอร์ในกระทรวงกลาโหม มีผังการจัดส่วนโครงสร้างศูนย์บัญชาการไซเบอร์กลาโหม ดังนี้

1) ส่วนบังคับบัญชาแบ่งเป็น กำลังพล งบประมาณ การเงิน ธุรการ 2) ส่วนแผนและยุทธศาสตร์แบ่งเป็น แผนและยุทธศาสตร์ไซเบอร์ติดตามสถานการณ์และอำนวยการยุทธ์ กฎหมายไซเบอร์ ปฏิบัติการข่าวสารไซเบอร์ 3) ส่วนปฏิบัติการไซเบอร์ แบ่งเป็น ป้องกัน โจมตีและแทรกซึมสืบสวน ชุดเผชิญเหตุ 4) ส่วนพัฒนาไซเบอร์ แบ่งเป็น พัฒนาหลักสูตรและฝึกอบรม จำลองยุทธศาสตร์ไซเบอร์ วิจัยและพัฒนาไซเบอร์ พัฒนาหลักนิยม ระเบียบปฏิบัติ มาตรฐานและต้องเชื่อมโยงความสัมพันธ์ด้านนโยบายและยุทธศาสตร์ไปถึง ศูนย์ปฏิบัติการไซเบอร์ ทั้งในส่วนของกองบัญชาการกองทัพไทย กองทัพบก กองทัพเรือ และกองทัพอากาศ ซึ่งต้องดำเนินการปรับ

โครงสร้างให้สอดคล้องตามภารกิจหน้าที่ อาจปรับเกลี่ยกำลังพล ทดลองปฏิบัติราชการ 6 - 12 เดือน ประเมินผลการปฏิบัติเป็นส่วนรวม นำเรียนผู้บังคับบัญชา เพื่อพิจารณาอนุมัติอัตราบรรจุจริงและจัดสรรงบประมาณสนับสนุนอย่างมั่นใจ ผลการวิจัยทำให้ทราบถึงภาพความขัดแย้งและการรักษาสันติภาพในยุทธบริเวณไซเบอร์ได้ระดับหนึ่ง และนำมาเป็นแนวทางในการยกร่างจัดทำยุทธศาสตร์ไซเบอร์กระทรวงกลาโหม และแผนการปฏิบัติไซเบอร์กระทรวงกลาโหม ให้สอดคล้องกับทิศทางของประชาคมไซเบอร์โลก ครอบคลุมตอบสนองภารกิจหลักของรัฐบาลเป็นสำคัญ โดยกำหนดกรอบระยะเวลา 3 ปีเป็นหลักการกว้าง ๆ ขอบเขตของงาน ความรับผิดชอบของหน่วยงานที่สามารถเข้าใจได้ในระดับกระทรวงกลาโหมและเหล่าทัพและได้ชี้ให้เห็นความสำคัญที่กระทรวงกลาโหมจำเป็นต้องเตรียมกำลังพลไซเบอร์พร้อมสิ่งอุปกรณ์รับมือกับภัยคุกคามไซเบอร์และสงครามไซเบอร์ที่ต้องการทรัพยากรและการสนับสนุนจากทุกภาคส่วน ไม่เช่นนั้นประเทศจะไม่มีขีดความสามารถต้านทาน/ตอบโต้เมื่อถูกโจมตีทางไซเบอร์จากปัญหาความขัดแย้งหรือสงครามใด ๆ

ในแง่มุมการศึกษาเกี่ยวกับภัยคุกคามทางไซเบอร์ในประเทศไทยที่ศึกษาในบริบทของพลเรือนจะมีข้อแตกต่างกันไป สามารถเห็นได้จากงานวิจัย ดังต่อไปนี้

หยาดพิรุณ นาชัยสินธุ์ ได้ศึกษาในหัวข้อเรื่อง ยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย (Strategies To Counter Cyber Terrorism In Thailand) คณะรัฐศาสตร์และนิติศาสตร์ มหาวิทยาลัยบูรพา การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อ 1) ศึกษาความก้าวหน้าทางไซเบอร์ที่มีการนำมาใช้เป็นเครื่องมือทางยุทธศาสตร์การก่อการร้ายในประเทศไทย 2) พัฒนายุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย การวิจัยครั้งนี้เป็นการวิจัยโดยใช้วิธีการศึกษาเชิงคุณภาพจากเทคนิคเดลฟายและการสัมภาษณ์เจาะลึก ประกอบด้วยผู้เชี่ยวชาญ 2 กลุ่ม คือ ผู้ที่มีบทบาทเกี่ยวข้องกับการดำเนินการหรือพัฒนาทางไซเบอร์ และผู้เชี่ยวชาญการกำหนดยุทธศาสตร์ทางเทคโนโลยีสารสนเทศ ทำการวิเคราะห์เนื้อหาและประเมินลักษณะการก่อการร้ายทางไซเบอร์ในประเทศไทย ผลการศึกษาพบว่า ความก้าวหน้าทางไซเบอร์คือ การพัฒนาทางเทคโนโลยีที่สามารถเชื่อมต่อกันได้อย่างรวดเร็วสะดวกขึ้น การก่อการร้ายทางไซเบอร์เป็นการใช้เครื่องมือทางเทคโนโลยี เช่น โทรศัพท์มือถือ คอมพิวเตอร์ แท็บเล็ตหรือเครื่องมือประเภทอื่น ๆ ที่เชื่อมต่อทางอินเทอร์เน็ตเพื่อการก่อการร้าย และอินเทอร์เน็ตเป็นช่องทางที่สำคัญที่ใช้ในการก่อการร้าย

โดยมีข้อค้นพบว่า ยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทยประกอบด้วย Read: Clip คือ 1. Research: ยุทธศาสตร์การเสริมสร้างการวิจัยเพื่อการพัฒนาทางไซเบอร์ 2. Education: ยุทธศาสตร์ การจัดการศึกษาในการสร้างพื้นฐานของประชาชนในประเทศไทย 3. Awareness: ยุทธศาสตร์การสร้างการตระหนักรู้ทางไซเบอร์ให้กับประชาชน 4. Development: ยุทธศาสตร์การพัฒนาความก้าวหน้าทางไซเบอร์ 5. Coordinate: ยุทธศาสตร์การส่งเสริมความร่วมมือระหว่างภาครัฐ ภาคเอกชน และภาคประชาชน 6. Law: ยุทธศาสตร์การกำหนดใช้กฎหมาย

ทางไซเบอร์และการบังคับใช้กับประชาชน 7. Integration: ยุทธศาสตร์การใช้การบูรณาการร่วมกันเพื่อแบ่งปันข้อมูล 8. Perception Prepares And Protect: ยุทธศาสตร์การรับรู้ทางไซเบอร์ร่วมกันตระเตรียมและปกป้องทางไซเบอร์ (หยาดพิรุณ นาชัยสินธุ์, 2560)

ในงานวิทยานิพนธ์เรื่อง ปัจจัยที่ส่งผลต่อพฤติกรรมการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ โดย ศิริรัตน์ ศรีสว่าง เสนอต่อ คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์การวิจัยครั้งนี้เป็นการศึกษาความสัมพันธ์เชิงสาเหตุ โดยมีวัตถุประสงค์เพื่อศึกษาปัจจัยที่ส่งผลต่อพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ เพื่อตรวจสอบความสอดคล้องของโมเดลกับข้อมูลเชิงประจักษ์ และเพื่อทดสอบความไม่แปรเปลี่ยนของโมเดลเชิงสาเหตุพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ระหว่างกลุ่มที่มีทักษะด้านเทคโนโลยีสารสนเทศและกลุ่มที่ไม่มีทักษะด้านเทคโนโลยีสารสนเทศ ข้อมูลที่ใช้ในการวิจัยเป็นข้อมูลที่รวบรวมผ่านแบบสอบถามจากผู้ใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลทั้งที่ใช้งานที่บ้านและที่ทำงานในประเทศไทยจำนวน 600 คน เครื่องมือที่ใช้ในการวิจัยเป็นแบบสอบถาม

ผลการวิจัยสรุปว่า พฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ได้รับอิทธิพลจากปัจจัยส่วนบุคคล ได้แก่ บุคลิกภาพแบบมีจิตสำนึก การรับรู้คุณค่าของข้อมูล และประสบการณ์ในอดีต รวมทั้งปัจจัยด้านสภาพแวดล้อม ได้แก่ การคล้อยตามกลุ่มอ้างอิง ความรู้ด้านความปลอดภัย และค่าใช้จ่ายในการป้องกัน โดยส่งผ่านการรับรู้ต่อสภาวะคุกคามการรับรู้ความสามารถในการจัดการกับภัยคุกคามและ แรงจูงใจในการป้องกัน โมเดลเชิงสาเหตุพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์ไม่มีความเปลี่ยนแปลงของรูปแบบโมเดลและค่าพารามิเตอร์ระหว่างกลุ่มที่มีทักษะด้านเทคโนโลยีสารสนเทศและกลุ่มที่ไม่มีทักษะด้านเทคโนโลยีสารสนเทศ (ศิริรัตน์ ศรีสว่าง, 2558) ผลของวิจัยนั้นแสดงให้เห็นว่าปัจจัยส่วนบุคคลมีอิทธิพลมากกว่า ดังนั้นการจะเพิ่มความตระหนักรู้อาจจะต้องมุ่งปัจจัยทางสังคม การปรับวัฒนธรรมองค์กรกระตุ้นบุคคลกรให้มีความตื่นตัวต่อภัยคุกคามที่เกิดขึ้น งานวิจัยนี้สามารถนำมาต่อยอดงานของผู้วิจัยที่กำลังศึกษาความพร้อมของหน่วยงานในภาครัฐกับการรับมือภัยคุกคามจากไซเบอร์โดยเน้นไปยังประเด็นการพัฒนาบุคลากร

งานวิจัยที่ทรงคุณค่าอีกเล่มหนึ่งเรื่อง ความรุนแรงร่วมสมัยในสังคมไทย: การก่อการร้ายในเมือง ของสุรชาติ บำรุงสุข และคณะ ที่มีความตระหนักถึงการสูญเสียที่เกิดขึ้นจากการก่อการร้ายในเหตุการณ์ 11 กันยายน 2001 ซึ่งเกิดกับมหานครขนาดใหญ่อย่างนิวยอร์กและเกิดกับอาคารของรัฐบาลในกรุงวอชิงตัน ดีซี แสดงให้เห็นถึงความเปลี่ยนแปลงครั้งยิ่งใหญ่ของการก่อการร้ายซึ่งจะเป็นจุดเริ่มต้นในการเข้าสู่การก่อการร้ายยุคใหม่ (The New Terrorism) โดยได้ทำลายข้อยกเว้นต่าง ๆ เช่น การทำลายเมืองอันเป็นที่ตั้งของหน่วยงานสำคัญซึ่งเคยได้รับการยกเว้นให้เคยเป็นเขตปลอดภัยเมื่อครั้งเกิดสงคราม การก่อการร้ายในรูปแบบใหม่นี้มุ่งเน้น ทำลายความมั่นคงมาตุภูมิ (Homeland

Security) ให้เกิดความสั่นคลอนจนทำให้ประชาชนเกิดความหวาดกลัว การโจมตีเมืองถือเป็นเป้าหมายอ่อน (Soft Targets) ที่มีความเปราะบางเพราะเป็นแหล่งวัฒนธรรม มีผู้คนอยู่อาศัย และไม่สามารถที่จะป้องกันการโจมตีจากการก่อการร้ายได้ และการจะสร้างเมืองให้เป็นเป้าหมายแข็ง (Hard Targets) ก็เป็นเรื่องยากในทางปฏิบัติ ดังนั้นประเด็นที่จะต้องตระหนักร่วมกันทั้งในทางบริบทและทฤษฎีคือ การสร้างความมั่นคงเมือง ที่เปรียบเสมือนโจทย์สำคัญของศตวรรษที่ 21 ที่ประเทศไทยอาจต้องเผชิญกับการเปลี่ยนเมืองเป็นสนามรบใหม่ในการทำสงครามของผู้ก่อการร้าย

การวิจัยนี้มีจุดประสงค์เพื่อ 1) ศึกษาปัญหาที่เมืองใหญ่ของโลกกำลังเผชิญกับภัยคุกคามในยุคปัจจุบันโดยเฉพาะจากการก่อการร้ายในพื้นที่เขตเมือง 2) ศึกษามาตรการ ยุทธศาสตร์ และนโยบายในการเสริมสร้างความมั่นคงปลอดภัยในเมือง รวมถึงการป้องกันละป้องปรามการก่อการร้ายในประเทศต่าง ๆ และ 3) แสวงหาข้อคิด บทเรียน รวมถึงแนวปฏิบัติที่ดีให้กับหน่วยงานภาคปฏิบัติในการป้องกันเมืองจากการก่อการร้ายที่เกิดขึ้นในโลกร่วมสมัย การวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ โดยสำรวจเอกสารประกอบกับการสนทนากลุ่ม และสัมภาษณ์เชิงลึก การเลือกกลุ่มผู้ให้ข้อมูลสำคัญสำหรับการวิจัยในครั้งนี้ใช้วิธีสุ่มตัวอย่างแบบเจาะจง โดยพิจารณาและตัดสินใจเลือกผู้ให้ข้อมูลให้สอดคล้องกับคำถามและวัตถุประสงค์การวิจัย โดยจะเป็นผู้ทรงคุณวุฒิที่มีความเชี่ยวชาญ และประสบการณ์ในเรื่องการก่อการร้ายและต่อต้านการก่อการร้าย จากนั้นทำการวิเคราะห์เนื้อหาและสรุปข้อเสนอแนะหรือแนวทางปฏิบัติสำหรับการเสริมสร้างความมั่นคงปลอดภัยในเมืองไทย

ผลการศึกษาพบว่า 1) เมืองทั่วทุกมุมโลกเป็นเป้าหมายหลักของการก่อการร้าย 2) ความรุนแรงและการก่อการร้ายในเมืองนำมาซึ่งการเปลี่ยนแปลงแบบแผนของสงครามในโลกร่วมสมัย และทำให้สงครามเป็นลักษณะอสมมาตร ทั้งในลักษณะของมิติคู่สงคราม การรบ กฎสงคราม เครื่องมือและนิยามของชัยชนะ 3) การก่อการร้ายในเมืองยังสะท้อนให้เห็นถึงความเปลี่ยนแปลงของการก่อการร้ายทั้งในแง่ของพื้นที่ ของความรุนแรง และคุณลักษณะของผู้ก่อเหตุ นอกจากนี้งานวิจัยยังมีข้อเสนอแนะเชิงนโยบายเพื่อเสริมสร้างความมั่นคงปลอดภัยของเมืองและการป้องกันการก่อการร้ายปผ่านการเตรียมการใน 3 ส่วน คือ 1) การเตรียมความพร้อมของเมือง 2) การเตรียมความพร้อมของเจ้าหน้าที่ตำรวจ และ 3) การเตรียมพร้อมด้านงานข่าวกรองในการรับมือการก่อการร้าย

งานวิจัยเล่มนี้สามารถนำมาต่อยอดโดยเปรียบเสมือนการเปิดทางให้แนวคิดการก่อการร้ายรูปแบบใหม่ที่มุ่งโจมตีเมืองหรือที่ที่มีความเปราะบางเปรียบได้เช่นโครงสร้างพื้นฐานสาธารณูปโภคสำคัญของประเทศที่ผู้ก่อการ้ายโดยเฉพาะไซเบอร์มุ่งที่จะโจมตีเพราะจะทำให้เกิดผลเสียหายอันมหาศาลตามมา (สุรชาติ บำรุงสุข, ฉัตรพงษ์ ฉัตราคม, สัญญา ทองบุศย์, กุลนันทน์ คันธิก, & ศิบดี นพประเสริฐ, 2563)

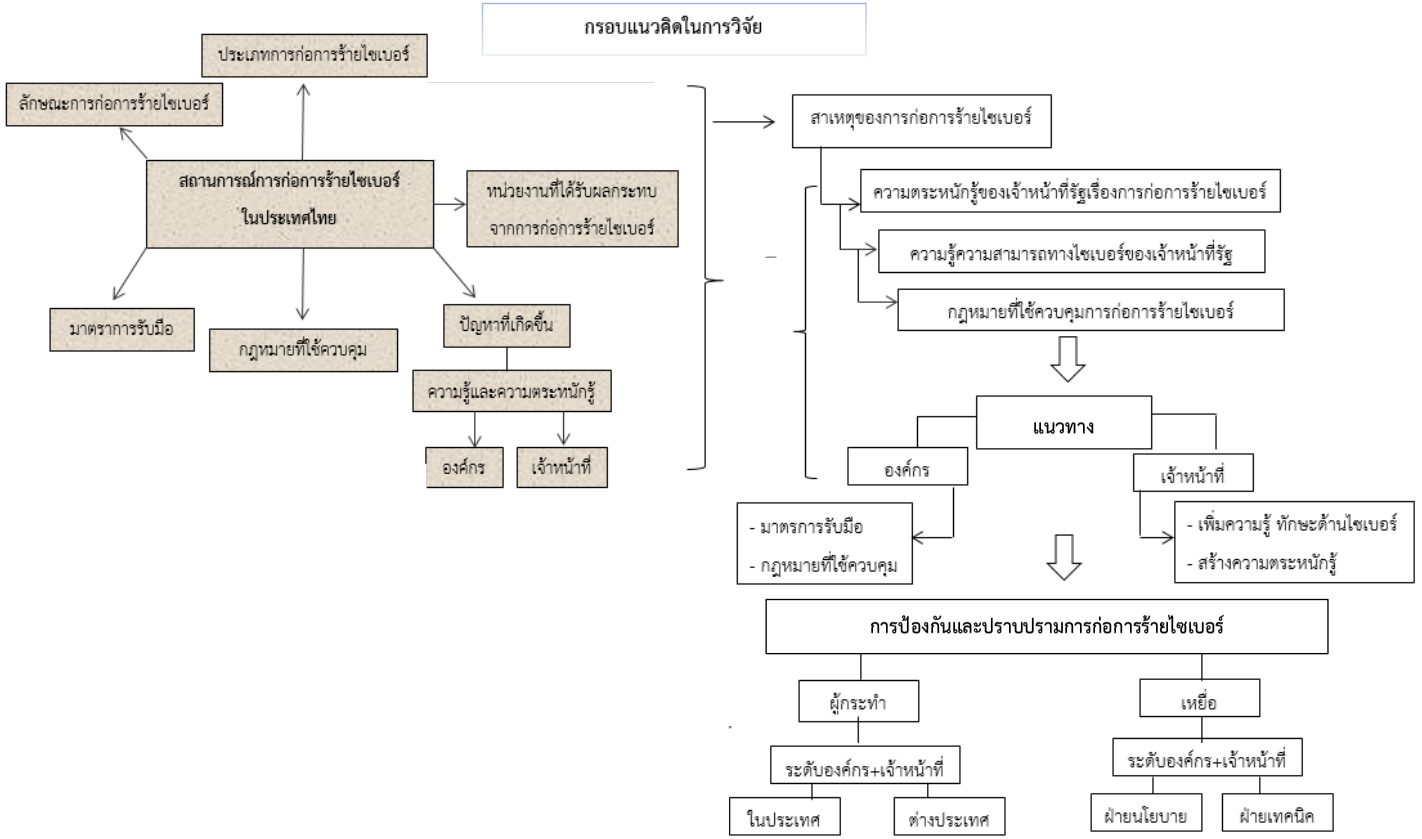
งานวิจัยชิ้นนี้จะไม่สามารถเติมเต็มช่องว่างทางการศึกษาได้หากปราศจากการศึกษาค้นคว้างานวิจัยในต่างประเทศควบคู่ไปด้วย งานวิจัยเกี่ยวกับภัยคุกคามทางไซเบอร์ในต่างประเทศมีในหลาย

ลักษณะไม่ว่าจะเป็นการศึกษาเชิงลึกในเชิงเทคนิคการทำงานของเทคโนโลยีในฐานะเครื่องของของผู้ก่อการร้าย การศึกษานิยามที่ชัดเจนของการก่อการร้ายไซเบอร์ ผลกระทบที่มีต่อประชาชนหรือความมั่นคงของรัฐ ไปจนถึงการศึกษาความตระหนักรู้ ความกลัว และอิทธิพลของการก่อการร้ายไซเบอร์ที่มีต่อประชาชนและหน่วยงานทั้งภาครัฐและเอกชนโดยมีรายละเอียด ดังนี้

Lee Jarvis And Stuart Macdonald (2014) ได้ศึกษาวิจัยเรื่อง Locating Cyber-Terrorism: How Terrorism Researchers Use And View The Cyber Lexicon วิจัยชิ้นนี้ได้สำรวจแนวคิดเรื่องการก่อการร้ายทางไซเบอร์จากนักวิจัยที่ทำงานในขอบข่ายเกี่ยวกับภัยคุกคามทางไซเบอร์กว่า 24 ประเทศทั่วโลก เป้าหมายของงานวิจัย คือ การแลกเปลี่ยนความรู้และมีส่วนร่วมในการศึกษารายละเอียดในพื้นที่ไซเบอร์โดยการสำรวจขอบเขตการก่อการร้ายทางไซเบอร์ที่มีอยู่ในโลกปัจจุบัน โดยเน้นคำถามสองข้อหลักคือแนวคิดการก่อการร้ายไซเบอร์ยังติดอยู่กับมายาคติการก่อการร้ายแบบเดิม และการนำไปสู่การเกิดสงคามไซเบอร์ในอนาคตได้อย่างไร ส่วนประการที่สองคือ แนวคิดเหล่านี้จะนำไปใช้ประโยชน์อย่างไรในเวทีการวิจัยระดับโลก จากการศึกษาได้หรือไม่ หลังจากได้ทำการศึกษาวิจัยแล้วมีข้อค้นพบว่าในประการแรก ผู้เชี่ยวชาญที่เกี่ยวข้องในขอบเขตของการก่อการร้ายไซเบอร์มีความคุ้นชินกับมายาคติแบบเดิมกับการก่อการร้าย และยังคงมีความคุมเคลือในเรื่องของการกำหนดนิยามของการก่อการร้ายไซเบอร์ ประการที่สองพบว่าผู้เชี่ยวชาญมีความคุ้นชินกับประเด็นการเกิดขึ้นของสงครามไซเบอร์ (Cyber Warfare) สงคราข่าวสาร (Information Warfare) และอาชญากรรมไซเบอร์ (Cybercrime) แต่อย่างไรก็ตามจากการศึกษาพบว่ายังความพยายามที่จะหลีกเลี่ยงที่จะกล่าวถึง จิฮัดจ์ในโลกไซเบอร์ (Cyber Jihad) และ การก่อการร้ายไซเบอร์แบบบริสุทธ์โดยไม่ขึ้นกับศาสตร์อื่น(Pure Cyber Terrorism) จากการสำรวจนำมาสู่ข้อสรุปและข้อเสนอแนะสำหรับการวิจัยในอนาคตไม่ว่าจะเป็นเรื่องการกำหนดนิยามที่ชัดเจนของการก่อการร้ายไซเบอร์ที่จะนำมาสู่การกำหนดความท้าทาย การกำหนดนโยบายของรัฐ เพราะในปัจจุบันคำว่าการก่อการร้ายไซเบอร์ถูกนำมาผูกกับความหมายเดิมจึงทำให้นโยบายที่จะนำมาใช้ควบคุมการก่อการร้ายไซเบอร์นั้นไร้ทิศทาง การก่อการร้ายควรถูกมองว่าเป็นพฤติกรรมอันตรายและน่ารังเกียจ ไม่ใช่แค่การนำนิยามของการก่อการร้ายมาผูก ยึดติดกับคำว่า วัตถุประสงค์ทางการเมืองเท่านั้น (Political Goals) เพราะการกำหนดเช่นนี้จะทำให้พฤติกรรมที่มีความรุนแรงใกล้เคียงแต่ไม่สามารถนับเป็นพฤติกรรมของการก่อการร้ายได้เพราะวัตถุประสงค์ที่ไม่เกี่ยวกับการเมือง(Lee & Macdonald, 2014) จากการศึกษางานวิจัยนี้เป็นข้อชี้แนะให้เห็นว่าช่องว่างของการทำวิจัยการก่อการร้ายไซเบอร์นั้นต้องคำนึงถึงนิยามของการก่อการร้ายเป็นหลักไม่เช่นนั้นแนวทางการรับมือที่ตามมาจะไร้ทิศทางเพราะไม่สามารถแยกประเภทของความรุนแรงได้

Janet J. Prichard และ Laurie E. Macdonald (2004) ได้เสนอชิ้นงานวิจัยในหัวข้อ Cyber Terrorism: A Study Of The Extent Of Coverage In Computer Science Textbooks

ให้กับมหาวิทยาลัย Bryant University ประเทศสหรัฐอเมริกา วิจัยเล่มนี้เริ่มต้นจะเหตุการณ์วันที่ 11 กันยายน 2001 ที่เป็นประวัติศาสตร์หน้าใหม่ของสหรัฐอเมริกที่เผชิญกับการก่อการร้าย หลังจากเหตุการณ์นี้เป็นเหตุให้รัฐบาลทุกประเทศต่างหามาตรการรองรับกับการก่อการร้ายและทบทวนนโยบายการควบคุมภัยคุกคามที่เกิดขึ้น นอกจากนี้จะเป็นจุดเริ่มต้นของการส่งเสริงการตระหนักรู้ที่มีต่อภัยคุกคามของการก่อการร้าย โดยเฉพาะเมื่อมีการเปลี่ยนแปลงของเทคโนโลยีที่ทำให้เกิดนิยามให้ขอการก่อการร้ายไซเบอร์ โดยในงานวิจัยของ Janet J. Prichard และ Laurie E. Macdonald ได้ให้คำนิยามการก่อการร้ายของการร้ายไซเบอร์ว่า “Cyber Terrorism Can Be Described As Politically Motivated Attacks In Cyberspace” นั่นคือ การก่อการร้ายที่มีแรงจูงใจทางการเมืองเกิดขึ้นในบริบทของไซเบอร์ ภัยคุกคามรูปแบบนี้จะนำมาซึ่งความเสียหายต่อเศรษฐกิจและสังคมเป็นอย่างมาก ในการก่อการร้ายไซเบอร์ที่ส่งผลกระทบในระดับประเทศส่วนใหญ่จะมาจากผู้ที่เชี่ยวชาญทางคอมพิวเตอร์เป็นผู้อยู่เบื้องหลัง จากสาเหตุนี้ทำให้วงการการศึกษาต้องขยายขอบเขตการเรียนรู้ให้ครอบคลุมถึงการใช้คอมพิวเตอร์เป็นเครื่องมือเพื่อที่จะสามารถควบคุมสถานการณ์ภัยคุกคามได้ โดยหัวข้อที่ได้รับความสนใจมากที่สุดในวงการศึกษา คือ Computer Security โดยเฉพาะ ภัยคุกคามในรูปแบบ การก่อการร้ายไซเบอร์ (Cyber Terrorism) ผู้วิจัยได้ทำการศึกษาแบบสุ่มตัวอย่างจากหนังสือเรียนในสาขา Computer Security ที่มีเนื้อหาเกี่ยวกับ การก่อการร้ายไซเบอร์ แต่พบว่าหนังสือเหล่านั้นไม่ได้มีการให้คำนิยามที่ชัดเจนและลึกซึ้งของการก่อการร้ายสำหรับอุตสาหกรรม It ดังนั้นในมุมมองของการส่งเสริมให้เกิดความตระหนักรู้จะต้องลงลึกไปถึงการควบคุมสื่อการสอนต่าง ๆ เช่น Textbook ที่จะต้องให้ความรู้นักเรียน นักศึกษา หรือผู้ที่สนใจได้อย่างชัดเจนและลึกซึ้ง และรวมไปถึงสื่อต่าง ๆ เช่น Websites วารสารออนไลน์ ที่จะสามารถให้ความรู้ในเรื่องการก่อการร้ายไซเบอร์ได้อีกด้วย (Janet & MacDonald, 2004) จากผลการวิจัยแสดงให้เห็นว่านอกจากจะต้องมีความชัดเจนในการให้คำนิยามแล้วนั้น ยังต้องเพิ่มความเข้มข้นในวงการวิชาการเพื่อที่จะผลิตสื่อที่มีความครอบคลุมในประเด็นการก่อการร้ายไซเบอร์ได้อย่างครบถ้วน



รูปที่ 17 กรอบแนวคิดในการวิจัย

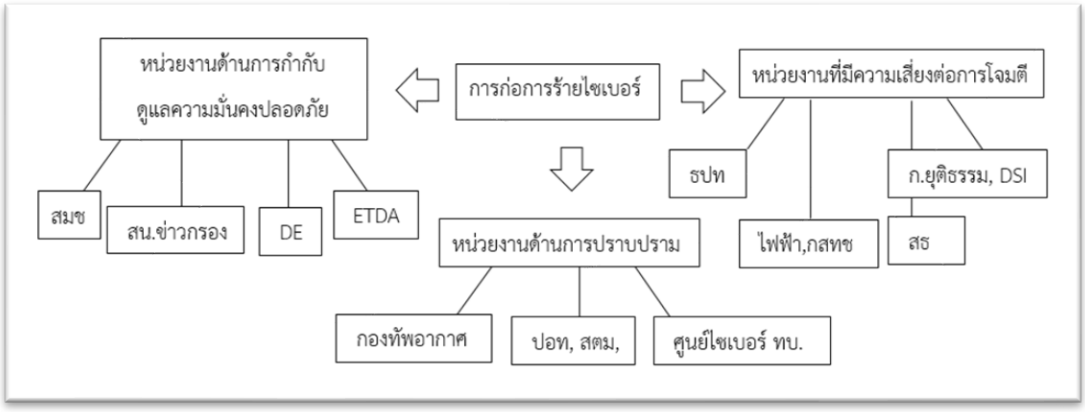
บทที่ 3

ระเบียบวิธีวิจัย

ในการดำเนินตามการศึกษาวิจัยเรื่องการศึกษาความตระหนักรู้ของภาครัฐในการรับมือกับการก่อการร้ายไซเบอร์นั้น โดยภาพรวมของการกำหนดระเบียบวิธีการวิจัยหรือกระบวนวิธีการวิจัย (Methodology) เป็นกระบวนวิธีการวิจัยเชิงคุณภาพ (Qualitative Research) ซึ่งประกอบด้วย การวิจัยเชิงเอกสาร (Documentary Research) และการสัมภาษณ์เชิงลึก (In-Depth Interview) และได้กำหนดกรอบและขอบเขตของระเบียบวิธีการวิจัยฯ เพื่อให้บรรลุวัตถุประสงค์ของการวิจัย 3 ข้อ ที่ต้องการจะศึกษา อันประกอบด้วย 1) เพื่อศึกษาสถานการณ์ภัยคุกคามด้านการก่อการร้ายไซเบอร์ของประเทศไทยในปัจจุบัน 2) เพื่อศึกษานโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์และความตระหนักรู้ถึงการก่อการร้ายไซเบอร์ของหน่วยงานภาครัฐและนำไปแก้ไขจุดบกพร่องและเสริมสร้างศักยภาพของรัฐบาลในการควบคุมการก่อการร้ายไซเบอร์ 3) เพื่อศึกษาการพัฒนานโยบายและยุทธศาสตร์การป้องกันและรับมือภัยคุกคามการก่อการร้ายไซเบอร์ที่จะเกิดขึ้นได้ในอนาคต จำเป็นจะต้องมีวิธีการเก็บรวบรวมข้อมูลทั้งปฐมภูมิและทุติยภูมิเพื่อหาความสัมพันธ์กันของผลลัพธ์ โดยวิธีวิจัยจะเป็นในเชิงคุณภาพที่จะใช้วิธีการสัมภาษณ์ผู้ที่เกี่ยวข้องกับการออกนโยบายการรับมือภัยคุกคามทางไซเบอร์ไปจนถึงผู้ที่รับนโยบายไปปฏิบัติใช้ นอกจากนี้จะรวบรวมข้อมูลผ่านการศึกษาบริบทของเหตุการณ์การก่อการร้ายในประเทศต่าง ๆ เพื่อนำมาเปรียบเทียบและคาดการณ์เหตุการณ์ที่มีแนวโน้มจะเกิดขึ้นกับประเทศไทย และมีระเบียบวิธีวิจัยดังนี้

3.1 วิธีการวิจัย

ผู้วิจัยได้กำหนดระเบียบวิธีการวิจัยหรือกระบวนวิธีการวิจัย (Methodology) โดยการใช้กระบวนวิธีการวิจัยเชิงคุณภาพ (Qualitative Research) โดยจะมีการศึกษาและวิเคราะห์ข้อมูลจากเอกสารหรือการวิจัยเชิงเอกสาร (Documentary Research) และกระบวนการสัมภาษณ์เชิงลึก (In-Depth Interview) มีรายละเอียดกรอบการศึกษาแยกประเภทตามหน่วยงานดังต่อไปนี้



รูปที่ 18 กระบวนวิธีการวิจัยของการศึกษาการรับมือการก่อการร้ายไซเบอร์ในประเทศ

3.1.1 การวิจัยเชิงเอกสาร (Documents)

ผู้วิจัยได้วิเคราะห์ข้อมูลจากเอกสาร (Documents) โดยการทบทวนวรรณกรรม แนวความคิด ทฤษฎี ที่เกี่ยวข้องกับการก่อการร้ายในบริบทดั้งเดิมเพื่อมาเปรียบเทียบความเปลี่ยนที่เกิดขึ้นกับการก่อการร้ายที่มีอยู่ในบริบทของโลกดิจิทัล เพื่อต่อต้านภัยคุกคามไซเบอร์ในประเทศไทยและรับมือกับภัยคุกคามไซเบอร์ที่จะมีในอนาคต ทั้งนี้ในกระบวนการการศึกษายังประกอบไปด้วยการวิเคราะห์ความคลุมเครือของนิยามการก่อการร้ายไซเบอร์ที่เป็นสาเหตุของความไม่ชัดเจนในนโยบายรับมือภัยคุกคาม รวมไปถึงการศึกษายุทธศาสตร์และกลยุทธ์ทั้งในทางพลเรือนและทางทหารเพื่อเห็นถึงความแตกต่างและช่องว่างของการออกนโยบายที่มี การศึกษาจะประกอบไปด้วยการทบทวนแผนการรับมือภัยคุกคามไซเบอร์ของหน่วยงานโครงสร้างสาธารณูปโภคพื้นฐานที่สำคัญและมีความเสี่ยงที่จะถูกโจมตี ทั้งหมดนี้เป็นการศึกษาแนวความคิดเบื้องต้นที่จะนำไปต่อยอดในการวิจัยได้ต่อไป

3.1.2 การสัมภาษณ์เชิงลึก (In-Depth Interview)

การสัมภาษณ์เชิงลึก (In-Depth Interview) ที่เป็นส่วนหนึ่งของการวิจัยเชิงคุณภาพ การวิจัยในครั้งนี้ผู้วิจัยได้กำหนดรูปแบบในการสัมภาษณ์ออกเป็น 2 ส่วน คือ การสัมภาษณ์แบบกำหนดโครงสร้างของคำถาม เพื่อนำไปใช้ในการสัมภาษณ์แบบชี้นำ (Guided Interview) และการสัมภาษณ์แบบไม่มีโครงสร้างหรือเป็นการสัมภาษณ์แบบปลายเปิด มีความยืดหยุ่นและเปิดกว้างหรือมีการนำคำสำคัญ (Keywords) มาใช้ประกอบในการชี้นำคำสัมภาษณ์ การสัมภาษณ์จะเริ่มจากการใช้คำถามที่มีลักษณะปลายเปิดเริ่มต้นในการสัมภาษณ์เพื่อให้ผู้ให้ข้อมูลสามารถให้ข้อมูลให้ได้มากที่สุด ซึ่งจะทำให้ได้ข้อมูลที่มีความหลากหลายในมิติต่าง ๆ และข้อเท็จจริงในทางปฏิบัติที่มีทั้งมิติของความความลึกและมิติของความกว้างของงานวิจัย เมื่อได้คำสำคัญจากการสัมภาษณ์ผู้ให้สัมภาษณ์แต่ละคน

ผู้วิจัยจะนำคำสำคัญไปกำหนดโครงสร้างของคำถาม เพื่อนำไปใช้ในการสัมภาษณ์แบบชี้นำเพื่อสามารถตีกรอบคำตอบที่ผู้วิจัยต้องการได้

3.1.3 ผู้ให้ข้อมูลสำคัญ (Key Informant)

ผู้ให้ข้อมูลสำคัญที่นำมาใช้ในการวิจัยครั้งนี้ กำหนดจากผู้ทรงคุณวุฒิ และบุคคลที่มีความสำคัญหรือมีส่วนเกี่ยวข้องกับการออกนโยบายเพื่อรับมือกับภัยคุกคามไซเบอร์ที่มีต่อหน่วยงานที่เป็นโครงสร้างสาธารณูปโภคพื้นฐานที่มีความเสี่ยง รวมไปถึงผู้รับนโยบายมาปฏิบัติเพื่อให้ทราบถึงแนวความคิดในทางปรัชญาตลอดจนแนวความคิดและทัศนคติ และความตระหนักรู้ โดยการคัดเลือกผู้ให้ข้อมูลสำคัญนี้ทำโดยวิธีการสุ่มตัวอย่างแบบเจาะจง (Purposive Random) อันเป็นการเลือกตัวอย่างที่ผู้วิจัยได้ดำเนินการพิจารณาเลือกตัวอย่างด้วยตนเอง โดยให้สอดคล้องกับวัตถุประสงค์และแนวทาง เพื่อที่จะได้นำข้อมูลที่ได้รับจากวิธีการวิจัยเชิงคุณภาพ (Qualitative Research) ดังกล่าวมาวิเคราะห์ผลจนได้ข้อสรุปต่อไป โดยผู้ให้ข้อมูลสำคัญสำหรับการสัมภาษณ์เชิงลึกประกอบด้วย ผู้ให้นโยบาย ผู้ปฏิบัติ ผู้ทรงคุณวุฒิ และบุคคลที่มีความสำคัญหรือมีส่วนเกี่ยวข้องกับการรับมือภัยคุกคามทางไซเบอร์ ดังต่อไปนี้

1. บุคลากรผู้ที่มีความรู้ความเชี่ยวชาญในส่วนของการกำหนดยุทธศาสตร์ไซเบอร์ในหน่วยงานภาครัฐ จำนวน 11 คน (ด้านนโยบาย) ประกอบด้วย กระทรวงดิจิทัลและเทคโนโลยี จำนวน 1 คน สภาความมั่นคงแห่งชาติ จำนวน 1 คน สำนักข่าวกรอง 1 คน สพธอ. 1 คน ศูนย์ไซเบอร์กองทัพบก จำนวน 1 คน กองทัพอากาศ 1 คน กระทรวงยุติธรรม 1 คน การไฟฟ้าส่วนภูมิภาค 1 คน หน่วยงานกำกับดูแลกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติหรือ กสทช.1 คน กระทรวงสาธารณสุข 1 คน ธนาคารแห่งประเทศไทย 1 คน

2. บุคลากรผู้ที่มีความรู้ความเชี่ยวชาญ ในการรับนโยบายไซเบอร์มาปฏิบัติในหน่วยงานภาครัฐ จำนวน 11 คน (ด้านเทคนิค) ประกอบด้วย กระทรวงดิจิทัลและเทคโนโลยี จำนวน 1 คน หน่วยงานความมั่นคงแห่งชาติ จำนวน 1 คน ศูนย์ไซเบอร์กองทัพบก จำนวน 1 คน กองทัพอากาศ 1 คน กระทรวงยุติธรรม 1 คน กรมสอบสวนคดีพิเศษ 1 คน การไฟฟ้าส่วนภูมิภาค 1 คน หน่วยงานกำกับดูแลกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติหรือ กสทช. 1 คน กระทรวงสาธารณสุข 1 คน ธนาคารแห่งประเทศไทย 1 คน กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี 1 คน

3. ผู้ทรงคุณวุฒิที่มีความเชี่ยวชาญด้านการรับมือการก่อการร้ายไซเบอร์ จำนวน 1 คน

4. ผู้ทรงคุณวุฒิที่มีความเชี่ยวชาญด้านการรับมือการก่อการร้ายและสงคราม จำนวน 1 คน

5. ผู้บริหารที่มีความเกี่ยวข้องกับการรับมือการก่อการร้ายไซเบอร์ในประเทศไทย จำนวน 1 คน

6. ข้อมูลทั่วไปบุคลากรที่ปฏิบัติหน้าที่ด้านยุทธศาสตร์ไซเบอร์และด้านเทคนิคไซเบอร์ของแต่ละหน่วยงาน ผู้บริหารและอาจารย์ผู้ที่มีความเชี่ยวชาญด้านไซเบอร์และการก่อการร้าย 9 คน

ตารางที่ 8 ผู้ให้ข้อมูลสำคัญ

ผู้ให้ข้อมูลสำคัญ	ตำแหน่ง/ความเชี่ยวชาญ	สังกัด	ประสบการณ์การทำงาน
ผู้ให้ข้อมูลสำคัญ ที่ 1	ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ	สำนักปลัดกระทรวงยุติธรรม	- ประสบการณ์ด้านเทคโนโลยีคอมพิวเตอร์ 12 ปี - ประสบการณ์ด้านการบริหาร 5 ปี เคยดำรงตำแหน่งหัวหน้ากลุ่มงานความปลอดภัยไซเบอร์
ผู้ให้ข้อมูลสำคัญ ที่ 2	เจ้าหน้าที่ทางด้านเทคนิค ศูนย์เทคโนโลยีสารสนเทศ	สำนักปลัดกระทรวงยุติธรรม	- ประสบการณ์ด้านคอมพิวเตอร์และเทคโนโลยี การรับมือการจู่โจมทางไซเบอร์ 6 ปี
ผู้ให้ข้อมูลสำคัญ ที่ 3	เจ้าหน้าที่ทางด้านนโยบาย ศูนย์เทคโนโลยีสารสนเทศ	สำนักปลัดกระทรวงสาธารณสุข	- ประสบการณ์ด้านคอมพิวเตอร์และเทคโนโลยี ผลงาน application “หมอพร้อม”
ผู้ให้ข้อมูลสำคัญ ที่ 4	เจ้าหน้าที่ทางด้านเทคนิค ศูนย์เทคโนโลยีสารสนเทศ	สำนักปลัดกระทรวงสาธารณสุข	- ประสบการณ์ด้านคอมพิวเตอร์และเทคโนโลยี - ดูแลด้านการ backup ข้อมูลแก่โรงพยาบาลเครือข่าย
ผู้ให้ข้อมูลสำคัญ ที่ 5	เจ้าหน้าที่ Cyber Security Section	ธนาคารแห่งประเทศไทย	เชี่ยวชาญด้าน Cyber Security
ผู้ให้ข้อมูลสำคัญ ที่ 6	เจ้าหน้าที่ Cyber Security Section	ธนาคารแห่งประเทศไทย	เชี่ยวชาญด้าน Cyber Security
ผู้ให้ข้อมูลสำคัญ ที่ 7	เจ้าหน้าที่ Cyber Security Section	ธนาคารแห่งประเทศไทย	เชี่ยวชาญด้าน Cyber Security
ผู้ให้ข้อมูลสำคัญ ที่ 8	ผกก. กลุ่มงานสนับสนุนคดีเทคโนโลยี	ปอท.	สืบสวนและพิสูจน์พยานหลักฐานคดีเทคโนโลยีตั้งแต่ปี 2555 - ปัจจุบัน

ตารางที่ 8 ผู้ให้ข้อมูลสำคัญ (ต่อ)

ผู้ให้ข้อมูลสำคัญ	ตำแหน่ง/ความเชี่ยวชาญ	สังกัด	ประสบการณ์การทำงาน
ผู้ให้ข้อมูลสำคัญ ที่ 9	เจ้าหน้าที่ทางด้านเทคนิค สำนักเทคโนโลยีสารสนเทศ	กสทช.	มีความเชี่ยวชาญทางด้านเทคนิคการรับมือการจู่โจมทางไซเบอร์
ผู้ให้ข้อมูลสำคัญ ที่ 10	เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศ	สำนักข่าวกรองแห่งชาติ	มีความเชี่ยวชาญทางด้านการข่าวและความมั่นคงปลอดภัยทางไซเบอร์
ผู้ให้ข้อมูลสำคัญ ที่ 11	เจ้าหน้าที่ทางด้านเทคนิค ศูนย์เทคโนโลยีสารสนเทศ	สำนักข่าวกรองแห่งชาติ	ทำงานเฉพาะด้านความมั่นคงทางไซเบอร์ 5 ปี มีหน้าที่วิเคราะห์และตรวจจับภัยคุกคามทางไซเบอร์
ผู้ให้ข้อมูลสำคัญ ที่ 12	นายทหารปฏิบัติการไซเบอร์	ศูนย์ไซเบอร์ กองทัพอากาศ	มีความเชี่ยวชาญทางด้านเทคนิคการรับมือการจู่โจมทางไซเบอร์
ผู้ให้ข้อมูลสำคัญ ที่ 13	เจ้าหน้าที่ ศูนย์ไซเบอร์ กองทัพอากาศ	ศูนย์ไซเบอร์ กองทัพอากาศ	เคยแข่งขัน Cyber Contest และจัดอบรมด้านไซเบอร์
ผู้ให้ข้อมูลสำคัญ ที่ 14	เจ้าหน้าที่ ศูนย์ไซเบอร์ กองทัพบก	ศูนย์ไซเบอร์ กองทัพบก	มีความเชี่ยวชาญทางด้านเทคนิคการรับมือการจู่โจมทางไซเบอร์
ผู้ให้ข้อมูลสำคัญ ที่ 15	ผู้อำนวยการกองปฏิบัติการไซเบอร์	สกมช. กระทรวงดิจิทัลฯ	เคยทำงานศูนย์ไซเบอร์ กองทัพอากาศ
ผู้ให้ข้อมูลสำคัญ ที่ 16	รองผู้กำกับการ ช่วยราชการ สกมช.	สกมช. กระทรวงดิจิทัลฯ	เคยทำงานด้านคดีเทคโนโลยี
ผู้ให้ข้อมูลสำคัญ ที่ 17	นักวิเคราะห์นโยบายและแผนปฏิบัติการ	สมช.	วิเคราะห์แผนและนโยบายความมั่นคงทางไซเบอร์
ผู้ให้ข้อมูลสำคัญ ที่ 18	นักวิเคราะห์นโยบายและแผนปฏิบัติการ	สมช.	วิเคราะห์แผนและนโยบายความมั่นคงทางไซเบอร์
ผู้ให้ข้อมูลสำคัญ ที่ 19	นักวิเคราะห์นโยบายและแผนชำนาญการ	สมช.	จัดทำแผนยุทธศาสตร์การก่อการร้ายสากลและอาชญากรรมข้ามชาติ ปี 2547-2556
ผู้ให้ข้อมูลสำคัญ ที่ 20	เจ้าหน้าที่กองเทคโนโลยีสารสนเทศ	การไฟฟ้าฝ่ายผลิต	วิศวกรระดับ 11 ของการไฟฟ้า
ผู้ให้ข้อมูลสำคัญ ที่ 21	เจ้าหน้าที่กองเทคโนโลยีสารสนเทศ	การไฟฟ้าฝ่ายผลิต	วิศวกรระดับ 11 ของการไฟฟ้า

ตารางที่ 8 ผู้ให้ข้อมูลสำคัญ (ต่อ)

ผู้ให้ข้อมูลสำคัญ	ตำแหน่ง/ความเชี่ยวชาญ	สังกัด	ประสบการณ์การทำงาน
ผู้ให้ข้อมูลสำคัญ ที่ 22	อาจารย์ประจำคณะรัฐศาสตร์	มหาวิทยาลัย สุโขทัยธรรมธิราช	เชี่ยชาญทางด้านการก่อการร้ายโดยเฉพาะกรณี 3 จังหวัดชายแดนภาคใต้
ผู้ให้ข้อมูลสำคัญ ที่ 23	อาจารย์ประจำคณะคณะพัฒนาทรัพยากรมนุษย์	อาจารย์มหาวิทยาลัย NIDA	เชี่ยวชาญทางด้านวิศวกรรมเทคโนโลยีและเคยเป็นผู้พัฒนา software ของบริษัทญี่ปุ่น
ผู้ให้ข้อมูลสำคัญ ที่ 24	ผู้อำนวยการศูนย์มุสลิมศึกษา เชี่ยวชาญโลกตะวันออกกลางและการก่อการร้ายแบบดั้งเดิม	จุฬาลงกรณ์มหาวิทยาลัย	มีความเชี่ยวชาญด้านโลกตะวันออกกลางเป็นเวลา 20 ปี ตีพิมพ์หนังสือเรื่อง การก่อการร้าย:มุมมองโลกมุสลิม
ผู้ให้ข้อมูลสำคัญ ที่ 25	ผู้เชี่ยวชาญด้านไซเบอร์ของรัฐสภา วิทยากรพิเศษโรงเรียนตำรวจ	สังกัดอิสระ	เชี่ยวชาญทางด้านวิศวกรรมเทคโนโลยีและเคยเป็นผู้พัฒนา software ผู้ศึกษาและตีพิมพ์บทความทางด้านความมั่นคงปลอดภัยไซเบอร์
ผู้ให้ข้อมูลสำคัญ ที่ 26	อาจารย์ประจำภาควิชากฎหมายระหว่างเทศ	มหาวิทยาลัย Sheffield	เชี่ยวชาญทางด้านกฎหมายระหว่างเทศด้านไซเบอร์และผู้เขียนตำรา cyber espionage
ผู้ให้ข้อมูลสำคัญ ที่ 27	อาจารย์ประจำภาควิชากฎหมายระหว่างเทศและความมั่นคงปลอดภัยไซเบอร์	มหาวิทยาลัย Sheffield	เชี่ยวชาญทางด้านกฎหมายระหว่างเทศและอาชญากรรม ผู้ทรงคุณวุฒิทางด้านกฎหมายระหว่างประเทศของ UN
ผู้ให้ข้อมูลสำคัญ ที่ 28	อาจารย์ประจำภาควิชากฎหมายระหว่างเทศและกฎหมายประเทศอินเดีย	มหาวิทยาลัย Sheffield	เชี่ยวชาญทางด้านกฎหมายระหว่างเทศและอาชญากรรมของเอเชียตะวันออก เอเชียใต้
ผู้ให้ข้อมูลสำคัญ ที่ 29	อาจารย์ประจำภาควิชากฎหมายระหว่างเทศและความมั่นคงปลอดภัยไซเบอร์	มหาวิทยาลัย Sheffield	เชี่ยวชาญทางด้านกฎหมายกฎหมายระหว่างเทศและความมั่นคงปลอดภัยไซเบอร์

ตารางที่ 8 ผู้ให้ข้อมูลสำคัญ (ต่อ)

ผู้ให้ข้อมูลสำคัญ	ตำแหน่ง/ความเชี่ยวชาญ	สังกัด	ประสบการณ์การทำงาน
ผู้ให้ข้อมูลสำคัญ ที่ 30	เชี่ยวชาญทางด้านแผนความมั่นคงทางไซเบอร์	รัฐบาลอังกฤษ	นักวิชาการอิสระ นักวิเคราะห์แผนความมั่นคงแห่งชาติ
ผู้ให้ข้อมูลสำคัญ ที่ 31	นักวิเคราะห์แผนความมั่นคงนอกเวลา	รัฐบาลอังกฤษ	นักวิชาการอิสระ นักวิเคราะห์แผนความมั่นคงแห่งชาติด้านไซเบอร์
ผู้ให้ข้อมูลสำคัญ ที่ 32	นักศึกษาปริญญาเอก	คณะวิศวกรรมไซเบอร์มหาวิทยา UCL	เชี่ยวชาญทางแผนการป้องกันและการรับมือทางไซเบอร์
ผู้ให้ข้อมูลสำคัญ ที่ 33	นักศึกษาปริญญาเอก	คณะวิศวกรรมไซเบอร์มหาวิทยา UCL	เชี่ยวชาญทางด้านธุรกิจและอุตสาหกรรมทางไซเบอร์และความตระหนักรู้ของพนักงานในองค์กรณ์
ผู้ให้ข้อมูลสำคัญ ที่ 34	ผู้บริหาร	บริษัทเอกชนทางด้านไซเบอร์	เชี่ยวชาญทางการใช้ไซเบอร์ทางการบินและต่อยอดเทคโนโลยี

3.2 การสร้างและพัฒนาคุณภาพเครื่องมือ

การดำเนินการวิจัยด้วยการสัมภาษณ์ผู้เชี่ยวชาญเพื่อทำการรวบรวมข้อมูลและความคิดเห็นที่เป็นประโยชน์ต่อการศึกษาในครั้งนี้จะมีลักษณะเฉพาะคือ การสัมภาษณ์เชิงลึกแบบรายบุคคล เพื่อหลีกเลี่ยงการเผชิญหน้ากันระหว่างผู้เชี่ยวชาญแต่ละท่าน ทำให้ผู้เชี่ยวชาญแต่ละท่านปราศจากการชี้นำจากกลุ่มและไม่อยู่ในอิทธิพลทางความคิดเห็นของผู้เชี่ยวชาญท่านอื่น เครื่องมือเป็นแบบสัมภาษณ์เกี่ยวกับความก้าวหน้าทางไซเบอร์ ลักษณะการก่อการร้ายทางไซเบอร์ และการนำไซเบอร์มาเป็นเครื่องมือทางยุทธศาสตร์ในการก่อการร้าย พัฒนาเครื่องมือโดยวิธีการยกร่างแบบสัมภาษณ์ นำแบบสัมภาษณ์ให้อาจารย์ ที่ปรึกษาให้ข้อเสนอแนะ ปรับปรุงแบบสัมภาษณ์ตามข้อเสนอแนะของอาจารย์ที่ปรึกษาทดลองสัมภาษณ์ บุคคลผู้ที่ไม่ใช่ผู้ทรงคุณวุฒิในครั้งนี้และปรับปรุงอีกครั้ง โดยในการสัมภาษณ์จะครอบคลุมประเด็นสำคัญ ดังนี้

ข้อคำถามสำหรับนำไปใช้ในการสัมภาษณ์เชิงลึกครั้งนี้ ได้ดำเนินการออกแบบการวิจัย (Research Design) หรือการสร้างแบบสัมภาษณ์ โดยการสร้างแบบสัมภาษณ์แบบกึ่งโครงสร้าง หรือเป็นกระบวนวิธีการสัมภาษณ์ที่มีรูปแบบหรือมีลักษณะที่ไม่เป็นมาตรฐาน (Unstructured or Unstandardized Interview) และการสัมภาษณ์แบบชี้นำ (Guided Interview) ซึ่งในการกำหนดโครงสร้างของคำถามนั้น ประกอบไปด้วยคำถาม จำนวน 3 ตอนดังนี้

ตอนที่ 1 ข้อมูลทั่วไปของผู้ให้สัมภาษณ์

ตอนที่ 2 ประกอบด้วยข้อคำถามสำคัญสำหรับ นำมาใช้วิเคราะห์ข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ ดังนี้

1. สภาพปัญหาความพร้อมด้านขีดสมรรถนะของหน่วยงานสำหรับการต่อต้านภัยคุกคามไซเบอร์

2. สภาพปัญหาหรืออุปสรรคในการจัดทำแผนยุทธศาสตร์ สำหรับการส่งเสริมความรู้ความสามารถ ทักษะ ทัศนคติ ให้บุคลากรให้มีขีดสมรรถนะเพียงพอในการปฏิบัติการต่อต้านภัยคุกคามไซเบอร์

3. แนวทางกำหนดยุทธศาสตร์การพัฒนาบุคลากรทั้งที่มีความเชี่ยวชาญและบุคลากรทั่วไปสำหรับต่อต้านภัยคุกคามไซเบอร์

ตอนที่ 3 ความคิดเห็นและข้อเสนอแนะอื่น ๆ

3.3 การเก็บรวบรวมข้อมูล

การวิจัยครั้งนี้ ได้กำหนดกระบวนการหรือแนวทางในการเก็บรวบรวมข้อมูลใน 2 ลักษณะ ประกอบด้วย 1) เก็บรวบรวมข้อมูลจากการศึกษาค้นคว้าข้อมูลจากเอกสารทางวิชาการและข้อมูลจากสื่อเทคโนโลยีสารสนเทศ 2) เก็บรวบรวมข้อมูลจากการสัมภาษณ์เชิงลึกผู้ให้ข้อมูลสำคัญ สรุปได้ดังนี้

3.3.1 การเก็บรวบรวมข้อมูลจากการศึกษาค้นคว้าข้อมูลจากเอกสารทางวิชาการ และข้อมูลจากสื่อเทคโนโลยีสารสนเทศ

ผู้ศึกษาได้ดำเนินกระบวนการในการเก็บรวบรวมข้อมูลจากแผนยุทธศาสตร์และแนวทางการรับมือจากหน่วยงานโครงสร้างพื้นฐานที่สำคัญของประเทศที่มีโอกาสตกเป็นเป้าหมายในการโจทตีทางไซเบอร์ ข้อมูลสถานการณ์ภัยคุกคามที่เกิดขึ้นในต่างประเทศรวมถึงแนวทางการรับมือของประเทศต่าง ๆ ข้อมูลเหล่านี้จะถูกค้นหาโดยเฉพาะจากแหล่งข้อมูลทางเว็บไซต์ที่ปรากฏบนอินเทอร์เน็ต เพื่อเก็บรวบรวมข้อมูลในระดับทุติยภูมิ (secondary data) ประเภทต่าง ๆ ไม่ว่าจะเป็นข้อมูลจากเอกสารทางวิชาการ รายงานการศึกษาวิจัยและผลงานวิจัยประเภทต่าง ๆ เป็นต้น เพื่อนำมาใช้เป็นแนวทางในการออกแบบหรือสร้างแบบสัมภาษณ์เชิงลึกรวมทั้งเพื่อนำมาใช้เป็นส่วนประกอบในกระบวนการวิเคราะห์และประมวลผลข้อมูลในการวิจัยในส่วนต่อไปนี้

3.3.2 การเก็บรวบรวมข้อมูลจากการสัมภาษณ์เชิงลึกผู้ให้ข้อมูลสำคัญ

ผู้วิจัยได้กำหนดการเก็บรวบรวมข้อมูลโดยการขอความร่วมมือ จากองค์กรหรือบุคคลที่เป็นกลุ่มตัวอย่างของการวิจัยครั้งนี้ เพื่อการขอสัมภาษณ์อย่างเป็นทางการและไม่เป็นทางการ ไม่ว่าจะเป็นผู้บริหาร ผู้ที่มีส่วนเกี่ยวข้องในการออกยุทธศาสตร์และนำยุทธศาสตร์ไปปฏิบัติ รวมไปถึงผู้ทรงคุณวุฒิ ที่มีส่วนเกี่ยวข้องกับการสร้างความตระหนักรู้และการรับมือภัยคุกคามไซเบอร์ในรูปแบบการก่อการร้าย ทั้งนี้ ในกระบวนการสัมภาษณ์เชิงลึกนั้น ผู้วิจัยจะดำเนินการบันทึกข้อมูลโดยวิธีการจดบันทึกข้อมูลของผู้มีส่วนร่วมในการวิจัยโดยการขออนุญาตอย่างเป็นทางการก่อนการสัมภาษณ์เพื่อนำมาใช้ในกระบวนการตรวจสอบและตรวจทานความ ถูกต้องย้อนกลับในภายหลังได้

3.4 การวิเคราะห์ข้อมูล

ผู้วิจัยจะวิเคราะห์ข้อมูลที่ได้จากการสัมภาษณ์เชิงลึก (In-Depth Interview) ประมวลผลข้อมูล ร่วมกับการศึกษาค้นคว้าข้อมูลจากเอกสาร (Documentary Research) ผู้วิจัยใช้การวิเคราะห์แบบอุปนัยโดยผู้วิจัยยังจะนำข้อมูลที่ได้มาจดบันทึกเป็นระบบโดยจำแนกว่าใครพูดอะไร และนำมาหาความหมาย แยกแยะองค์ประกอบที่เชื่อมโยง ความสัมพันธ์ของข้อมูลเพื่อ อธิบายความสัมพันธ์ของข้อมูลที่รวบรวมมาจากการสัมภาษณ์ โดยผู้วิจัยจะเก็บรวบรวมข้อมูลไปพร้อมกับการวิเคราะห์ทุกครั้งเพื่อให้ได้ข้อมูลที่ถูกต้องครบถ้วนและสมบูรณ์ ตามประเด็นที่ต้องการ นอกจากนี้จะวิเคราะห์ข้อมูลโดยพิจารณา ประเด็นหลัก (Major Themes) ที่พบในข้อมูลที่ได้รับจากการ สัมภาษณ์ทั้งหมด จากนั้นจะนำประเด็นหลัก (Major Themes) มาพิจารณาแบ่งแยกออกเป็นประเด็นย่อย (Sub-Themes) และหัวข้อย่อย (Categories) หลังจากนั้นผู้วิจัยใช้การวิเคราะห์ข้อมูลโดยการจำแนกชนิดของข้อมูลช่วยการจำแนกชนิดของข้อมูล กรอบในการจำแนกตาม ประเด็นที่เกี่ยว ข้องกับความก้าวหน้าทางไซเบอร์ ลักษณะของการก่อการร้าย การก่อการร้ายทางไซเบอร์การนำไซเบอร์มาเป็นเครื่องมือทางยุทธศาสตร์ในการก่อการร้าย การต่อต้านการก่อการร้ายทางไซเบอร์ของ ประเทศอันเป็นแนวทางประการสำคัญที่สามารถนำไปสู่การจัดทำข้อเสนอแนะในการกำหนดยุทธศาสตร์การสร้างความตระหนักรู้เพื่อรับมือกับภัยคุกคามไซเบอร์ในบริบทของประเทศไทยได้ในอนาคต

3.5 ระยะเวลาที่ใช้ในการวิจัย

ผู้วิจัยจะดำเนินการวิจัยตั้งแต่เดือน สิงหาคม 2563 ถึง กรกฎาคม 2565

3.6 จริยธรรมในการวิจัย

ในการศึกษาวิจัยครั้งนี้ ทางผู้วิจัยได้ตระหนักถึงจริยธรรมในการวิจัย ซึ่งในการเก็บข้อมูลในแต่ละครั้ง จะต้องได้รับอนุญาตและความยินยอมจากผู้ให้ข้อมูล จากวิธีการสัมภาษณ์เชิงลึก (In-Depth Interview) ผลจากการวิจัยจะไม่ทำให้เกิดความเสียหายแก่ผู้ให้ข้อมูล และต้องเสนอทางมหาวิทยาลัยให้พิจารณาอนุมัติ ออกจดหมายชี้แจง สำหรับกลุ่มตัวอย่างที่เป็นหน่วยงาน ในองค์กรภาครัฐ ผู้วิจัยจะต้องได้รับความยินยอมในการเปิดเผย ชื่อของหน่วยงาน ในบางประเด็นที่มีความเกี่ยวเนื่องทางกฎหมาย จะมีการพิทักษ์สิทธิป้องกันความเสี่ยงและการรักษาความลับของหน่วยงานภาครัฐบาล หากแต่จะมีการนำเสนอข้อมูลในภาพรวมเพื่อปกป้องผู้ให้ข้อมูล

3.7 อุปสรรคในการเก็บรวบรวมข้อมูล

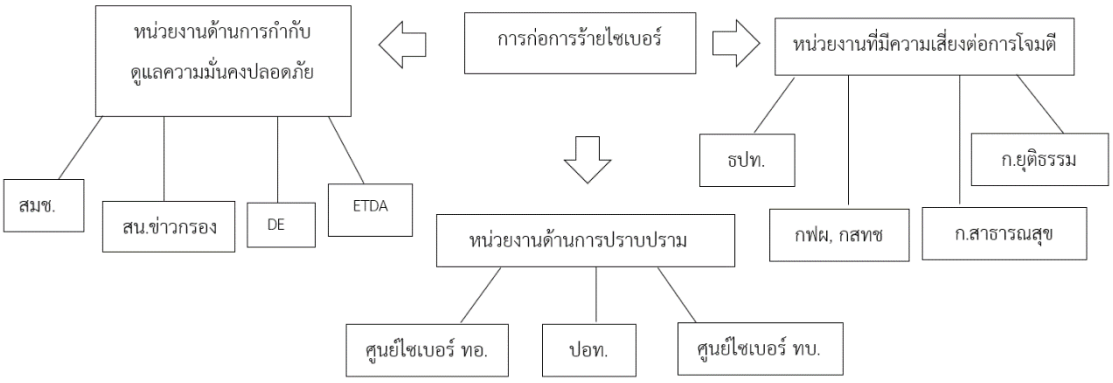
ในช่วงเวลาที่เป็นอุปสรรคจากภัยคุกคามทางโรคระบาดทำให้ผู้ให้ข้องและผู้ต้องการข้อมูลไปสามารถพบปะและสนทนาได้อย่างต่อหน้าหรือไม่ได้มีโอกาสในการเยี่ยมชมการทำงานที่แท้จริงขององค์กรนั้นๆ แต่ที่สำคัญที่สุดผู้วิจัยได้ใช้เวลาการส่งจดหมายและจดหมายอิเล็กทรอนิกส์ในเพื่อความรวดเร็วในการหาข้อมูล และผลตอบรับจากหน่วยต่างๆในการให้ความรู้และให้ข้อมูลนั้นเป็นไปด้วยความราบรื่นโดยแต่ละฝ่ายที่เกี่ยวข้อจะมีการประสานต่อไปเรื่อยยังผู้ที่ถูกมอบหมายให้ภูกสัมภาษณ์และผู้ที่ถูกสัมภาษณ์เองก็เป็นผู้มีประสบการณ์จริงสามารถให้ความรู้ได้อย่างแท้จริง การสัมภาษณ์ส่วนใหญ่จะถูกสัมภาษณ์ทางโทรศัพท์และ Google Meet ซึ่งง่ายและสะดวกทั้งสองฝ่ายและสามารถที่จะรักษาความสัมพันธ์ระหว่าผู้ให้ข้อมูลและผู้ต้องการข้อมูลได้ต่อไปในอนาคจ ซึ่งความสัมพันธ์ลักษณะนี้จะมีความสำคัญมากในการวิจัยในระดับต่างประเทศที่ผู้วิจัยได้ไปร่ำเรียนมา

บทที่ 4

ผลการศึกษาและการอภิปรายผลการศึกษา

การศึกษาเรื่อง การรับมือของภาครัฐกับการก่อการร้ายทางไซเบอร์ในประเทศไทย เป็นการวิเคราะห์การรับมือภัยคุมคามทางไซเบอร์ของภาครัฐในรูปแบบของการก่อการร้ายของหน่วยงานต่างๆ ที่มีความสำคัญเชิงโครงสร้างพื้นฐาน สาธารณูปโภคสำคัญของประเทศไทย โดยจะเริ่มศึกษาตั้งแต่คำนิยามของการก่อการร้ายไซเบอร์ให้มีความชัดเจนเพื่อที่จะสามารถอธิบายสถานการณ์และศักยภาพในการรับมือการก่อการร้ายไซเบอร์ของประเทศไทยนั้นเป็นเช่นใด และเพื่อให้การศึกษานั้นมีความคมชัดและเข้าใจง่าย โดยงานวิจัยเล่มนี้มีวัตถุประสงค์เพื่อศึกษาศักยภาพการรักษาความมั่นคงปลอดภัย ป้องกัน ปราบปราม และรับมือภัยคุกคามด้านการก่อการร้ายไซเบอร์ของหน่วยงานภาครัฐไทย และอีกทั้งยังเพื่อศึกษาแนวทางการรักษาความมั่นคงปลอดภัย และรับมือภัยคุกคามด้านการก่อการร้ายไซเบอร์ของหน่วยงานภาครัฐไทยในปัจจุบัน

จากการนำเสนอผลการศึกษาดังกล่าวได้กล่าวได้จากการวิเคราะห์และสังเคราะห์โดยอาศัยข้อมูลเชิงคุณภาพจากการสัมภาษณ์เชิงลึกมาวิเคราะห์เนื้อหาจากผู้ที่ปฏิบัติงานทั้งในทางนโยบายและทางเทคนิคในหน่วยงานรัฐมีมีความเสี่ยงต่อการถูกโจมตี หน่วยงานภาครัฐที่มีหน้าที่ดูแลความมั่นคงปลอดภัย และหน่วยงานด้านการปราบปราม ดังรูปที่ 19



รูปที่ 19 แผนภาพหน่วยงานสำคัญของภาครัฐไทย

แต่อย่างไรก็ตามในการนำเสนอผลการศึกษาดังกล่าวข้อมูลที่ได้นั้นอาศัยการถ่ายทอดข้อมูลจากประสบการณ์ในเรื่องของรูปแบบการก่อการร้ายที่เกิดขึ้นในประเทศไทย การสัมภาษณ์เชิงลึกจากผู้ที่มีประสบการณ์การทำงานทางด้านไซเบอร์ทั้งทางเทคนิคและนโยบายของแต่ละหน่วยงานข้างต้น รวม

ไปถึงการสัมภาษณ์ผู้เชี่ยวชาญซึ่งเป็นอาจารย์มหาวิทยาลัยที่มีความรู้ทางด้านเทคโนโลยี ความมั่นคงปลอดภัยไซเบอร์ และอาจารย์มหาวิทยาลัยที่มีความรู้ทางด้านการก่อการร้ายแบบดั้งเดิม เพื่อสังเคราะห์นำออกมาเป็นข้อมูลประกอบกับวิเคราะห์จากเอกสารสำคัญ นโยบายและแผน รวมไปถึงผลงานทางวิชาการต่างๆ ทั้งในประเทศไทยและต่างประเทศและคัดกรองความจริงและประเมินศักยภาพของหน่วยงานที่มีส่วนเกี่ยวข้องในประเทศสามารถดำเนินไปได้อย่างมีประสิทธิภาพและในขณะเดียวกัน ผู้วิจัยจะนำทฤษฎีทางอาชญาวิทยาและทฤษฎีทางสงครามและการก่อการร้ายมาประกอบในการวิเคราะห์เครื่องมือและแนวนโยบายต่างๆ ของแต่ละหน่วยงานที่มีอยู่ในขณะนี้เพื่อมาวิเคราะห์ว่าเพียงพอต่อการรับมือการก่อการร้ายไซเบอร์ที่จะเกิดขึ้นได้หรือไม่

ผลการศึกษาที่ประกอบไปด้วยการนำเสนอใน 4 ส่วน

1. สถานการณ์การก่อการร้ายไซเบอร์ในประเทศไทยและการให้คำนิยามและความสำคัญของการก่อการร้ายไซเบอร์

2. ศักยภาพในการรับมือการก่อการร้ายไซเบอร์และผลกระทบจากการก่อการร้ายไซเบอร์ในประเทศไทยของหน่วยงานต่างๆ ที่มีหน้าที่รักษาความมั่นคงปลอดภัย หน่วยงานที่มีการปราบปรามทางไซเบอร์และหน่วยงานที่มีความเสี่ยงที่จะถูกโจมตีทางไซเบอร์

3. แนวโน้มที่จะเกิดการก่อการร้ายไซเบอร์รวมไปถึงรูปแบบที่จะเกิดขึ้นในประเทศไทยในอนาคต

4. การอภิปรายผลการศึกษา

4.1 ข้อมูลทั่วไปของผู้ให้ข้อมูลสำคัญ

จากการสัมภาษณ์ผู้ให้ข้อมูลสำคัญทั้งหมด 34 คน แบ่งออกเป็นสายงานนโยบายและสายงานปฏิบัติการเชี่ยวชาญด้านเทคโนโลยี และสายงานวิชาการ ตามหน่วยงานที่ได้สรุปไว้ข้างต้น ผู้ให้ข้อมูลสำคัญในสายงานนโยบายและสายงานปฏิบัติการเชี่ยวชาญด้านเทคโนโลยีส่วนใหญ่มีอายุระหว่าง 35 – 55 ปี ส่วนน้อยที่มีอายุ 25 – 30 ปี โดยจบการศึกษาจากคณะวิศวกรรมศาสตร์คอมพิวเตอร์และวิทยาศาสตร์คอมพิวเตอร์จากมหาวิทยาลัยในประเทศเป็นส่วนใหญ่ มีเพียง 2 ท่านที่มาจากมหาวิทยาลัยในต่างประเทศ อายุงานและประสบการณ์ที่มีดดยภาพรวมตั้งแต่ 5 – 12 ปี และมีผลงานสำคัญๆ ต่างทางด้านเทคโนโลยีและระบบป้องกันความปลอดภัยทางไซเบอร์

สำหรับสายงานวิชาการนั้นผู้ให้ข้อมูลสำคัญทั้งหมดจบการศึกษาจากต่างประเทศประกอบไปด้วยสหราชอาณาจักร อินเดีย และญี่ปุ่น มีพื้นฐานความรู้ตั้งแต่ทางด้านเทคโนโลยีไซเบอร์ การก่อการร้าย สงครามไซเบอร์ และกฎหมายระหว่างประเทศด้านความปลอดภัยทางไซเบอร์ ข้อมูลบางส่วนมาจากการที่นักวิจัยได้ค้นคว้าจากตำราและวารสารทั้งภาษาไทยและ

ภาษาอังกฤษรวมไปถึง การจัดกิจกรรมเชิงวิชาการ การสัมมนาทั้งในรูปแบบปกติและรูปแบบออนไลน์ เรื่องของภัยคุกตามทางไซเบอร์และการรับมือของแต่ละภาคส่วนในต่างประเทศ

4.2 การให้คำนิยามสถานการณ์การก่อการร้ายไซเบอร์ในประเทศไทย

ในขณะที่ “การก่อการร้ายไซเบอร์” เป็นภัยคุกคามสำหรับหลายๆ ประเทศ แต่สำหรับประเทศไทยนั้นการก่อการร้ายไซเบอร์ยังเป็นเรื่องใหม่ที่ยังไม่เคยเกิดขึ้น บุคลากรที่ปฏิบัติงานทางด้านนโยบายเห็นว่า การก่อการร้ายนั้นเป็นเรื่องที่ซับซ้อน ต้องประกอบไปด้วยวัตถุประสงค์ทางการเมือง หรือการพยายามที่จะสร้างความเสื่อมเสียให้กับรัฐบาล หากมองให้ลึกไปกว่านั้นการก่อการร้ายไซเบอร์ยิ่งเป็นเรื่องที่ลึกซึ้ง ผู้ก่อการร้ายจะต้องมีทักษะทางด้านคอมพิวเตอร์ในระดับที่เชี่ยวชาญจึงจะสามารถเจาะเข้าระบบข้อมูลของรัฐได้ ซึ่งปัจจุบันรัฐบาลมีระบบความมั่นคงทางไซเบอร์ที่แข็งแกร่ง ข้อมูลที่ตรงกันจากผู้ให้สัมภาษณ์ไม่ว่าจะเป็นผู้ที่เชี่ยวชาญทางด้านเทคนิคหรือนโยบายไซเบอร์ต่างเห็นว่าการจู่โจมทางไซเบอร์ในปัจจุบันเป็นเพียงแค่การจู่โจมในระดับที่ไม่ได้สร้างความเสียหายหรือสร้างผลกระทบในระดับมหภาค การจู่โจมในแต่ละครั้งมาในรูปแบบของ Ransomware หรือไวรัสเรียกค่าไถ่รองลงมาคือ Phishing Mail คือ คำที่ใช้เรียกเทคนิคการหลอกลวงโดยใช้อีเมล์หรือหน้าเว็บไซต์ปลอมเพื่อให้ได้มา ซึ่งข้อมูล เช่น ชื่อผู้ใช้ รหัสผ่าน หรือข้อมูลส่วนบุคคลอื่น ๆ (ThaiCERT,2021) เพื่อนำข้อมูลที่ได้ไปใช้ในการเข้าถึงระบบโดยไม่ได้ รับอนุญาต การจู่โจมรูปแบบนี้เกิดจากความไม่ระมัดระวังหรือการขาดความตระหนักรู้ของผู้ปฏิบัติงาน และภัยรูปแบบที่หน่วยงานภาครัฐเจอมากเป็นลำดับที่ 3 คือ การบิดเบือนข้อมูลหน้าเว็ปไซต์หลักของหน่วยงาน ทำให้หน่วยงานภาครัฐขาดความน่าเชื่อถือ แต่รูปแบบภัยทั้งหมดที่กล่าวมานั้นเป็นเพียงแค่การจู่โจมจากผู้ไม่หวังดีซึ่งไม่จำเป็นต้องใช้ทักษะมากนัก การจู่โจมมาจากทั้งในประเทศและจากต่างประเทศหากพิจารณาจาก IP Address ของเครื่องคอมพิวเตอร์ แต่ส่วนใหญ่นั้นจะมาจากผู้ก่อกวนในประเทศเป็นส่วนใหญ่ (ThaiCERT, 2021) ภัยไซเบอร์ที่ได้กล่าวไว้ข้างต้นจึงเป็นแค่เพียงการก่อกวนถึงแม้จะมีเป้าหมายมุ่งทำลายรัฐบาลแต่ระดับของการโจมตีนั้นยังคงอยู่ในระดับที่สามารถรับมือได้ จึงไม่สามารถสรุปได้ว่าภัยคุกคามทางไซเบอร์ที่หน่วยงานภาครัฐของไทยประสบพบเจอนั้นเป็นภัยในระดับการก่อการร้ายที่จะต้องสร้างความเสียหายในระดับประเทศ ระดับมหภาค โดยสรุปแล้วภัยคุกคามทางไซเบอร์ที่หน่วยงานภาครัฐประสบพบเจอในปัจจุบันจึงยังไม่สามารถเรียกว่าเป็นการก่อการร้ายไซเบอร์ อนึ่ง ผู้ให้ข้อมูลสำคัญได้ให้ข้อมูลในประเด็นของสถานการณ์ภัยคุกคามทางไซเบอร์ไว้ ดังนี้

“ขอยอมรับว่าภัยทางไซเบอร์ปัจจุบันมีเข้ามาในหลายรูปแบบและมีแนวโน้มที่เพิ่มมากขึ้น แต่ภัยเหล่านั้นไม่สามารถที่จะเรียกว่าการก่อการร้ายได้เนื่องจากผลกระทบที่เกิดขึ้นจากการจู่โจมมีไม่มากนัก และระบบความมั่นคงทางไซเบอร์ของหน่วยงานภาครัฐของไทยก็สามาถที่จะรับมือภัยคุกคามเหล่านั้นได้อย่างดี โดยเฉพาะในระบบทางการเงิน ที่มีความแข็งแกร่ง”

ผู้ให้ข้อมูลสำคัญ ที่ 5 (ผู้ให้ข้อมูลในตัวแทนของธนาคารแห่งประเทศไทย)

“เราคงยังไม่สามารถใช้คำว่าการก่อการร้ายไซเบอร์ได้ในสถานการณ์ปัจจุบันของประเทสไทยเพราภัยตุกคามส่วนใหญ่ล้วนมาจากผู้จู่โจมที่มีทักษะทางคอมพิวเตอร์ไม่มากนัก แบะมีเพียงแค่จุดประสงค์ที่จะลองของกับหน่วยงานรัฐเท่านั้น ระบรักษาความมั่นคงทางไซเบอร์ของกองทัพอากาศมีความมั่นคงในระดับหนึ่ง เรามีการตั้งศูนย์ควบคุมภัยที่จะเกิดขึ้นจากไซเบอร์ปฏิบัติงาน 24 ชั่วโมง เพื่อที่จะสามารถสกัดสิ่งที่ผิดปกติที่มีจุดประสงค์เข้ามาจู่โจมฐานข้อมูลที่ควบคุมการจารจรทางอากาศได้ทันท่วงที”

ผู้ให้ข้อมูลสำคัญ ที่ 13
(ผู้ให้ข้อมูลสำคัญในฐานะผู้ปฏิบัติงานในศูนย์ไซเบอร์กองทัพอากาศ)

“สำหรับกองทัพบกเอง ถือว่าเป็นหน่วยงานความมั่นคงที่จะต้องมีระบบป้องกันเป็นอย่างสูงไม่ว่าจะเป็นในพื้นที่ทางกายภาพหรือในพื้นที่ไซเบอร์ แต่อย่างไรภัยคุกคามที่เราเจอได้มากที่สุดการแสกนหาช่องโหว่เพื่อเข้ามาในระบบและนำข้อมูลจากเราไป แต่ยังไม่เคยมีผู้คุกคามทางไซเบอร์คนใดสามารถที่จะเอาข้อมูลของเราไปได้ การทำให้ระบบคอมพิวเตอร์ปั่นป่วนหรือล่มก็ยังไม่เคยเกิดขึ้นกับกองทัพบก แต่มีบางอย่างที่เกี่ยวข้องกับการก่อการร้ายทางไซเบอร์เล็กน้อย เช่น คดีชาวเมียนมาร์ที่เคยตกเป็นผู้ต้องหาในคดีฆ่าข่มขืนที่เกาะเต่า สร้างความโกรธค้นให้ชาวเมียนมาร์จนทำให้ผู้ก่อความไปสงบกลุ่มหนึ่งก่อการโจมตีทางไซเบอร์ผ่านการเปลี่ยนหน้าเว็บไซต์ขององค์กรบริหารส่วนตำบลแห่งหนึ่ง ซึ่งการโจมจีทางไซเบอร์ในลักษณะนี้มีวัตถุประสงค์ทางการเมือง คล้ายกับเงื่อนไขในการก่อการร้าย แต่ผลที่เกิดขึ้นมันคงยังเล็กน้อยเกินไปที่จะเรียกว่าการก่อการร้าย”

ผู้ให้ข้อมูลสำคัญ ที่ 14
(ผู้ให้ข้อมูลสำคัญในฐานะผู้ปฏิบัติงานในศูนย์ไซเบอร์กองทัพบก)

“ภัยไซเบอร์ที่หน่วยงานพบเจอมากที่สุดคือการพยายามบิดเบือนของมูลหน้าเวปไซต์ อย่างที่ทราบกันว่า กสทช. เป็นหน่วยงานที่มีหน้าที่ดูแลและควบคุมระบบความมั่นคง ทั้งหมดที่เกี่ยวกับโทรคมนาคมและการเผยแพร่ข้อมูลข่าวสารของภาครัฐ การที่ ผู้ก่อกวนมุ่งโจมตีเวปไซต์เพื่อให้เกิดความบิดเบือนข้อมูลของรัฐบาลและสร้างความ เข้าใจผิดให้กับประชาชน จึงเป็นเทคนิคหนึ่งที่ทีมของเราจะต้องป้องกันไม่ให้เกิดขึ้น อีก แต่การกระทำเหล่านี้ก็ไม่ได้จะสรุปว่าเป็นการก่อการร้ายไซเบอร์อย่างเต็มรูปแบบ เนื่องจากผลกระทบที่เกิดขึ้นนั้นยังคงเล็กน้อยเมื่อต้องเทียบกับการก่อการร้ายระดับ นานาชาติ”

ผู้ให้ข้อมูลสำคัญ ที่ 9
(ผู้ให้ข้อมูลสำคัญในฐานะเจ้าหน้าที่ทางด้านเทคนิค สำนักเทคโนโลยีสารสนเทศ. กสทช.)

“การก่อการร้ายไซเบอร์หากพิจารณาถึงเงื่อนไขแล้วคงยากที่จะบอกว่าประเทศไทย เคยประสบพบเจอกับสิ่งเหล่านี้หรือไม่ แต่สิ่งที่เกิดขึ้นแน่นอนนั้นเราอาจจะเรียกว่า เป็นคุกคามทางไซเบอร์ที่สามารถเกิดขึ้นได้ทุกวินาที บางทีมาจากคนที่มีอุดมการณ์ และบางครั้งอาจเป็นมือสมัครเล่นที่ต้องการสร้างสถานการณ์เท่านั้นหลายหน่วยงาน ในประเทศถูกโจมตีผ่านระบบไซเบอร์แต่บางครั้งเปรียบเสมือนภายที่มองไม่เห็น เพราะเราจะสมารถตรวจจับได้ว่ามีใครที่พยายามรุกล้ำเข้ามาในระบบ แต่เราไม่ สามารถทราบได้เลยว่าเขาเหล่านั้นเอาข้อมูลอะไรไปได้บ้าง แต่ผลที่เกิดขึ้นก็ไม่ได้ รุนแรงเพียงพอที่จะสามารถเรียกได้ว่าเป็นการก่อการร้ายไซเบอร์”

ผู้ให้ข้อมูลสำคัญ ที่ 19
(นักวิเคราะห์นโยบายและแผนชำนาญการสภาความมั่นคงแห่งชาติ)

“การก่อการร้ายไซเบอร์มีอยู่จริง แต่เพียงแค่เราไม่สามมารถที่จะจับต้องได้อย่างเป็น รูปธรรมเฉกเช่นการก่อการร้ายในรูปแบบดั้งเดิม การก่อการร้ายไซเบอร์อย่างที่ทราบกัน ว่าผู้ก่อการร้ายจะใช้เครื่องมือทางไซเบอร์โจมตีฝ่ายตรงข้ามซึ่งมีเป้าหมายเป็นไซเบอร์ ด้วยกัน แต่การก่อการร้ายไซเบอร์นั้นทำได้ง่าย บางครั้งการโจมตีอาจไม่ต้องใช้ทักษะมาก แต่อย่างไรก็ตามการก่อการร้ายนั้นจะต้องมีวัตถุประสงค์ทางการเมืองที่ชัดเจน ซึ่งถ้าหาก มองในมุมนี้คงไม่สามารถสรุปว่าการจู่โจมที่เกิดขึ้นในไซเบอร์เป็นการก่อการร้ายหรือ อาจจะเป็นเพียงแค่การจู่โจมธรรมดาเพื่อให้ได้ผลประโยชน์เฉพาะกลุ่มของตน”

ผู้ให้ข้อมูลสำคัญ ที่ 23
(อาจารย์ประจำคณะคณะพัฒนาทรัพยากรมนุษย์)

“การก่อการร้าย เป็นคำที่มีปัญหามากๆ และผมเลือกที่จะใช้คำอื่นที่แสดงถึงกิจกรรมที่โหดร้ายแทนการก่อการร้าย เช่น ระเบิดก็เรียกว่าระเบิด ก่อวินาศกรรมก็คือก่อวินาศกรรม มีอาวุธก็คือมีอาวุธ เพราะคำว่าก่อการร้ายไม่ได้บอกอะไร มันแค่การบอกว่าสิ่งเหล่านั้นร้าย เป็นสิ่งที่ไม่ดี แต่คำกลางก็คือ การก่อการร้าย คือ การกระทำที่รุนแรง สร้างความสะพรึงกลัวในวงกว้างต่อผู้คน พลเรือน มุ่งที่จะตอบโจทย์เป้าหมายทางการเมือง หรือเปลี่ยนแปลงระเบียบทางสังคมบางอย่าง แต่อย่างไรก็ตามก็ไม่ได้เป็นความหมายที่ทุกคนยอมรับได้ทั่วกันเสมอไป แต่เพียงยอมรับร่วมกันได้มากที่สุด”

ผู้ให้ข้อมูลสำคัญ ที่ 22 (อาจารย์ประจำคณะรัฐศาสตร์)

4.3 คำนิยามการก่อการร้ายไซเบอร์

ข้อมูลสำคัญจากผู้ที่มีความสามารถและเชี่ยวชาญทางด้านไซเบอร์ แสดงให้เห็นถึงการให้ข้อมูลที่เป็นไปในทิศทางเดียวกันว่าประเทศไทยยังไม่มีประสบการณ์ในการรับมือกับการก่อการร้ายไซเบอร์ที่แท้จริงแต่สิ่งที่ประเทศไทยประสบพบเจอนั้นคือภัยคุกคามทางไซเบอร์ที่หน่วยงานสามารถรับมือได้ จากนิยามและสภาพปัญหาที่เกิดขึ้นกับประเทศไทยในประเด็นการก่อการร้ายสามารถสรุปได้ ดังนี้

การก่อการร้ายคือการทำให้เกิดความเสียหายอย่างร้ายแรงกับระบบขนส่ง ระบบสาธารณูปโภค ระบบโทรนคมนาคม ซึ่งเป็นเหตุทำให้ประชาชน คนบริสุทธิ์ ได้รับผลกระทบ การกระทำเหล่านี้จะต้องมีจุดประสงค์ทางการเมือง เพื่อทำลายความน่าเชื่อถือจากรัฐบาล ตามประมวลกฎหมายอาญา มาตรา 135/1 พ.ศ. 2546 (ความผิดฐานก่อการร้ายในประเทศไทย) การกระทำความผิดข้างต้นถือได้ว่าเป็นการก่อการร้าย

จากการให้การนิยามของผู้ให้ข้อมูลสำคัญคน ที่ 24 และ ผู้ให้ข้อมูลสำคัญคน ที่ 22 มีความคล้ายคลึงกันและหนักแน่นในความหมายของคำว่าก่อการร้ายในรูปแบบดั้งเดิม ผู้ให้ข้อมูลยังเสริมอีกว่าการก่อการร้ายนั้นเกิดขึ้นกับประเทศไทยมานาน แต่เนื่องด้วยเงื่อนไขต่างๆ จึงไม่สามารถเรียกว่าเป็นผู้ก่อการร้ายได้ แต่เป็นได้แค่เพียงผู้ก่อความไม่สงบเท่านั้น แต่อย่างไรก็ตาม การกระทำ วิธีการ และผลกระทบนั้นอยู่ในเงื่อนไขของการนิยามคำว่าการก่อการร้ายทั้งหมด เนื่องจากเทคโนโลยีเข้ามามีบทบาทในโลกปัจจุบันมากขึ้น บริบทของความรุนแรงจึงเปลี่ยนไป การก่อการร้ายได้ถูกเชื่อมโยงกับไซเบอร์ซึ่งรวมไปถึงอุปกรณ์อิเล็กทรอนิกส์ต่าง ๆ ที่สามารถเชื่อมต่อกับโครงข่ายอินเทอร์เน็ตได้ หากเชื่อมโยงไปยังประมวลกฎหมายอาญา มาตรา 135/1 พ.ศ.2546 ข้างต้นก็สามารถตีความได้ว่า ผู้ใดที่ใช้อุปกรณ์ทางไซเบอร์ทำให้เกิดความเสียหายอย่างร้ายแรงกับระบบอิเล็กทรอนิกส์ในการขนส่ง ระบบสาธารณูปโภค ระบบโทรนคมนาคม ซึ่งเป็นเหตุทำให้ประชาชน คนบริสุทธิ์ ได้รับผลกระทบ การ

กระทำเหล่านี้จะต้องมีจุดประสงค์ทางการเมือง เพื่อทำลายความน่าเชื่อถือของรัฐบาล จะถือว่าเป็นการก่อการร้ายก่อการร้ายไซเบอร์ ดังนั้นรัฐบาลจึงนิยามการก่อการร้ายไซเบอร์ให้มีความเชื่อมโยงกับประมวลกฎหมายดังกล่าวเพื่อให้พร้อมเตรียมรับกับภัยคุกคามทางไซเบอร์ที่จะมาถึง รัฐบาลได้ออก พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ 2562 ซึ่งได้กำหนดให้มี คณะกรรมการการรักษาความมั่นคง ปลอดภัยไซเบอร์แห่งชาติ หรือ กมช. (National Cyber Security Committee: NCSC) เพื่อเป็นหน่วยงานหลักในการกำหนดนโยบาย โดยจะวิเคราะห์ถึงโครงสร้างการทำงานและหน้าที่ของหน่วยงานนี้ในส่วนต่อไป

4.3.1 คำนิยามการก่อการร้ายไซเบอร์ตามแนวความคิดของแต่ละหน่วยงาน

4.3.1.1 หน่วยงานด้านการกำกับดูแลความมั่นคงปลอดภัย

การก่อการร้ายไซเบอร์ หมายถึง การใช้คอมพิวเตอร์หรือระบบอิเล็กทรอนิกส์ที่มีการเชื่อมโยงกับโครงข่ายทางอินเทอร์เน็ตจู่โจมหน่วยงานภาครัฐโดยวิธีในรูปแบบการก่อการร้าย เช่น การโจมตีระบบไม่ให้สามารถใช้งานได้ การข้อมูลข้อมูลจากระบบจนเกิดความเสียหายที่รุนแรง โดยเป้าหมายในการโจมตีนั้นจะต้องอยู่ใน cyber space เท่านั้นถึงจะเรียกได้ว่าเป็นการจู่โจมทางไซเบอร์ที่แท้จริง และจุดประสงค์ของการจู่โจมนั้นจะต้องเป็นจุดประสงค์ทางการเมือง ต้องการบิดเบือนข้อเท็จจริงของรัฐบาล หรือแม้กระทั้งทำให้ระบบความมั่นคงของรัฐล้มเหลวไม่ว่าจะเป็นระบบสาธารณูปโภคสำคัญของประเทศที่จะก่อให้เกิดความเสียหายอย่างรุนแรงต่อประชาชนอันบริสุทธิ์เพื่อให้เพื่อผู้ที่จู่โจมได้รับความพึงพอใจในจุดประสงค์ที่ตนเองต้องการ

4.3.1.2 หน่วยงานการปราบกราบการก่อการร้าย

การก่อการร้ายไซเบอร์ หมายถึง การใช้กลวิธีในการก่อการร้ายมาประยุกต์ใช้กับระบบเทคโนโลยีในปัจจุบันเพื่อโจมต่อรับบความมั่นคงของรัฐบาล โดยเฉพาะความมั่นคงทางการทหาร ให้เกิดความเสียหายรุนแรงและก่อให้เกิดความเสื่อมเสียต่อภาพลักษณ์ความมั่นคงของประเทศ การกระทำของผู้ก่อการร้ายจะสามารถกระทำโดยเป็นกลุ่มหรือเป็นบุคคล จะมีฐานที่ตั้งในการก่อการร้ายภายในประเทศหรือนอกประเทศไทยได้ และการก่อการร้ายนั้นจะต้องเกิดผลในระดับรุนแรงกับประชาชนผู้บริสุทธิ์ ตรงตามคำนิยามของการก่อการร้ายแบบดั้งเดิม

4.3.1.3 หน่วยงานที่มีความเสี่ยงต่อการโจมตี

การก่อการร้ายไซเบอร์ หมายถึง การที่ผู้ก่อการร้ายมีวัตถุประสงค์ที่จะคุกคามภาครัฐเพื่อให้ได้มาซึ่งผลประโยชน์ของตน โดยมีวิธีการจู่โจมภาครัฐภายใต้ระบบคอมพิวเตอร์และโครงข่ายอินเทอร์เน็ตเพื่อทำลายข้อมูลของฝั่งตรงข้าม หรือขู่คุกคามเพื่อให้รัฐยอมเสียค่าใช้จ่ายเพื่อให้บรรลุวัตถุประสงค์ของเป้าหมายในกลุ่มตน วิธีการที่ใช้ในการก่อการร้ายส่วนมากจะทำให้ระบบของภาครัฐเสียจนทำให้ประชาชนไม่สามารถใช้งานได้

จากภาพสรุปของการนิยามการก่อการร้ายทั้งหมดของหน่วยงานภาครัฐทั้ง 3 ประเภท ซึ่งมีความคล้ายคลึงกันในส่วนของการใช้วัตถุประสงค์ทางการเมืองเป็นที่ตั้ง ใช้วิธีการก่อการร้ายแบบดั้งเดิม เช่น การทำลายผู้บริสุทธิ์ การทำลายความน่าเชื่อถือของภาครัฐ บิดเบือนข้อมูลที่ถูกต้อง ผ่านทางการใช้เทคโนโลยี และอุปกรณ์ไซเบอร์ในการดจมตีอีกฝ่ายหนึ่งเมื่อให้ได้มาซึ่งผลประโยชนของกลุ่มตน แต่ความเสียหายนั้นจะต้องเป็นในระดับที่รุนแรง

4.3.2 คำนิยามการก่อการร้ายไซเบอร์ประเทศไทยกับคำนิยามการก่อการร้ายในระดับนานาชาติ

จากคำนิยามจองสหประขาชาติ การก่อการร้ายไซเบอร์คือการอาชญากรรมทางไซเบอร์จู่โจมเพื่อวัตถุประสงค์ทางการเมือง ทำให้เกิดความกลัวแก่ประชาชน ขู่เข็น หรือบังคับรัฐบาลให้ยอมทำตามเป้าหมายของตนมิเช่นนั้น ผู้ก่อการร้ายจะใช้เหยื่อหรือประชาชนบริสุทธ์ของรัฐเป็นตัวประกัน (Denning, 2001) ประกอบกับการทำวิจัยของ Jarvis and Macdonald (2015) ผ่านโครงการร่วมกับ the global research community เรื่องแนวคิด “การก่อการร้ายไซเบอร์” (cyberterrorism) จากผู้ทำวิจัย 118 คน จาก 24 ประเทศทั่วโลก แต่ผลสรุปที่ได้นั้นยังคงมีความกำกวมอยู่ 3 ประการ คือ 1. ยังไม่สามารถหาความคล้องที่เป็นหนึ่งเดียวกันได้ในเรื่องของแนวคอดกรก่อการร้าย 2. การโต้แย้งเพื่อให้ได้มาถึงนิยามที่แท้จริงและสาเหตุการก่อการร้าย 3. การพยายามรวบรวมความคิดหรือแนวคิดเพื่อสร้างนิยามให้การก่อการ้ายมีเพียงหนึ่งเดียวในในมาตรฐานเดียวกัน

จากบทความของ ของ Jarvis and Macdonald (2015) มีองค์ประกอบ 3ประการที่จะต้องคำนึงถึง คือ 1. นักวิชาการให้ความหมายของคำว่าการก่อการร้ายไซเบอร์สอดคล้องในการออกนโยบายของผู้บริหารหรือไม่ 2. ลักษณะของการก่อการร้ายที่สำคัญคืออะไร และปัจจัยใดควรนำมาวิเคราะห์ในนิยาม 3. ความเหมาะสมในการให้คุณค่าของการใช้นิยามของการก่อการร้ายไซเบอร์เพื่อนำไปใช้ได้จริงในเหตุการณ์จู่โจมที่เกิดขึ้น

4.3.3 ข้อจำกัดในการให้คำนิยาม

จากการสำรวจนิยามจากนักวิชาการและผู้ทำวิจัยเกือบทั่วโลกกลับพบว่ายิ่งอธิบายนิยามของการก่อการร้ายมาเท่าไหร่จะทำให้การก่อการร้ายนั้นมีความลุ่มลึกและวกวนอยู่ในศาสตร์ของผู้เชี่ยวชาญในสาขานั้น ๆ ทำให้คำนิยามของการก่อการร้ายจึงไม่สามารถเป็นสากลได้ แม้กระทั่งอุปสรรคระหว่างความเชื่อ ศาสนา และเขตแดนระหว่างประเทศยังมีการจำกัดความหมายของนิยามการก่อการร้ายที่แตกต่างกันไป ยิ่งไปกว่านั้นการนิยามการก่อการร้ายแบบดั้งเดิมที่ยังดูคุมเครือเป็นผลทำให้การนิยามการก่อการร้ายไซเบอร์ที่ยังเกิดขึ้นไม่แพร่หลายมากนักประสบปัญหาในการให้คำนิยาม จากการศึกษาของ Jarvis and Macdonald (2015) พบว่าขอบเขตของการก่อการร้ายไซเบอร์

มีข้อโต้แย้งและมีความทับซ้อนในมุมมองของด้านการกมือง สังคม เศรษฐกิจ ศาสนา และสื่อสังคมออนไลน์ เกิดขึ้นตั้งแต่ในปี 1980 และการโต้แย้งทางวิชาการเรื่องคำนิยามครั้งนี้ก็ไม่สามารถที่จะหาข้อสรุปที่จะนำไปใช้จริงได้ การก่อการร้ายไซเบอร์นั้นจะต้องมีความรุนแรงมากถึงในระดับใด ใครคือผู้กระทำ และวิธีการที่ใช้จะเป็นเพียงแค่การจูงใจหรือการโจมตีผ่านโครงสร้างเครือข่ายจริงแต่เป็นเพียงแค่ผลประโยชน์ส่วนตัว ปราศจากอุดมการณ์หรือวัตถุประสงค์ทางการเมืองจะเป็นการก่อการร้ายไซเบอร์ได้หรือไม่ ในการศึกษาต่อไป Jarvis and Macdonald จึงพยายามสร้างขอบเขตของคำนิยามใน “ขอบเขตของการเมือง” เพื่อที่จะวางโครงสร้างของคำนิยามได้ชัดเจนขึ้น

การก่อการร้ายในรูปแบบขอบเขตของการเมือง การดำเนินการวิจัยเป็นไปในรูปแบบของแบบสอบถามของผู้ให้ข้อมูลหลักที่มีความเชี่ยวชายการก่อการร้ายในขอบเขตของการเมืองกว่า 200 คนและได้พบงานที่มีความน่าสนใจมากที่สุดงานหนึ่งชื่อว่า “The limitations of terrorism research” ดำเนินการวิจัยโดย Silke (2003) งานชิ้นนี้ให้ความสนใจในวิวัฒนาการของการก่อการร้ายหลังเหตุการณ์ 9/11 ที่ยังคงเป็นแหล่งอ้างอิงและเป็นแหล่งต้นกำเนิดของการศึกษาการก่อการร้ายยังสามารถเชื่อมโยงได้กับการก่อการร้ายไซเบอร์ได้อีกด้วย โยการค้นหานิยามของการก่อการร้ายไซเบอร์นั้นจะเริ่มจาก 2 คำถาม คือ 1. การก่อการร้ายไซเบอร์คืออะไรและควรมีนิยามแบบไหน 2. การก่อการร้ายไซเบอร์เหมือนหรือแตกต่างจากการใช้ความรุนแรงทางไซเบอร์รูปแบบอื่นๆ อย่างไร เช่นการมีลักาณะพิเศษที่สามารถระบุว่าเป็นการก่อการร้ายไซเบอร์ได้เลยหรือไม่ หรือภายใต้คำนิยามของการก่อการร้ายไซเบอร์นั้นมีองค์ประกอบไปด้วยพฤติกรมมหรือรูปแบบการใช้ความรุนแรงต่าง ๆ ที่กล่าวมา

เพื่อความชัดเจนการศึกษานี้จึงแบ่งแนวคิดนิยามการก่อการร้ายไซเบอร์เป็น 2 แนวคิด แนวคิดแรกเป็นแนวคิดแบบเฉพาะเจาะจง (Narrow View) คำนิยามจึงมีความใกล้เคียงกับคำนินามการก่อการร้ายทั่วไปที่มีวัตถุประสงค์ทางการเมืองเป็นที่ตั้งหรือมีจุดมุ่งหมายทำร้ายประชาชนคนบริสุทธิ์สำหรับแนวคิดที่สองเป็นแนวคิดในมุมมองกว้าง (Broader View) คำนิยามจะรวมรูปแบบการก่อการร้ายที่ใช้อินเทอร์เน็ต หรือการใช้เทคโนโลยีสารสนเทศเป็นเครื่องมือของผู้ก่อการร้าย Talihärm ได้ให้ความหมายของความเหมือนและความแตกต่างของนิยามแบบเฉพาะเจาะจง (narrow view) ที่ใช้เป้าหมายของการก่อการร้ายเป็นตัววัด และ นิยามมุมมองกว้าง (Broader View) ที่ใช้เครื่องมือในการก่อการร้ายเป็นตัววัด (Talihärm, 2010: pp. 59-74, 63-64) ดังนี้

การก่อการร้ายไซเบอร์ คือ การกระทำที่ประกอบด้วยวัตถุประสงค์ทางการเมือง สังคม และอุดมการณ์จู่โจมเน็ตเวิร์ค คอมพิวเตอร์ และข้อมูลสารสนเทศต่าง ๆ ไม่ว่าการกระทำเหล่านั้นจะเป็นการกระทำผ่านช่องทางไซเบอร์หรือช่องทางทางกายภาพก็ตาม หากเกิดความเสียหายต่อประเทศหรือผู้คนบริสุทธิ์ ก็จะถือว่าเป็นการก่อการร้ายไซเบอร์ (Narrow View) แต่ในอีกแง่หนึ่งทุกการกระทำที่ผ่านการใช้ช่องทางไซเบอร์และอินเทอร์เน็ตเพื่อเช่นเป็นเครื่องมือในการก่อการร้ายสำเร็จก็

ถือว่าเป็นการก่อการร้ายทางไซเบอร์เช่นกัน (Broader View) และการใช้ช่องทางทางอินเทอร์เน็ตเป็นเครื่องมือนั้นจำเป็นจะต้องอาศัยเงินสนับสนุนที่เพียงพอ การร่วมมือระหว่างกลุ่มบุคคลที่มีความเชื่อและอุดมคติเดียวกันเพื่อสร้างโฆษณาชวนเชื่อให้กับผู้ใช้อินเทอร์เน็ตอื่นๆ มีความเลื่อมใสและมีความเชื่อเดียวกันกับสิ่งที่กลุ่มผู้ก่อการร้ายต้องการ

Denning (2001) ให้คำนิยามการก่อการร้ายไซเบอร์ในมุมของ the US House of Representatives ว่าการก่อการร้ายไซเบอร์ คือ การมาบรรจบกันระหว่างการก่อการร้ายในโลกของไซเบอร์ โดยการใช้วิธีการจู่โจมที่ผิดกฎหมายมุ่งเป้าหมายไปยังคอมพิวเตอร์ โครงข่ายอินเทอร์เน็ต และข้อมูลสารสนเทศที่อยู่ในระบบโครงข่ายนั้นๆ การกรทำจะทำเพื่อข่มขู่รัฐบาลหรือประชาชนให้มีความหวาดกลัวเพื่อให้บรรลุจุดประสงค์ทางการเมืองหรือสังคม และที่มากกว่านั้นการก่อการร้ายไซเบอร์จะมีลักษณะที่ส่งผลทำให้เกิดความเสียหายไม่ว่าจะเป็นรายบุคคล ทรัพย์สิน และสร้างความเสียหายที่เพียงพอให้เกิดความกลัว ไม่ว่าจะเป็น การทำให้เกิดการบาดเจ็บตามร่างกาย อาจจะถึงแก่ความตาย การเกิดระเบิดกับโครงสร้างพื้นฐานสำคัญ การตูโจมหรือปล้นเครื่องบิน การทำให้น้ำประปามีความปนเปื้อน หรือแม้กระทั่งการทำให้เกิดความเสียหายทางเศรษฐกิจ ความเสียหายเหล่านี้ขึ้นอยู่กับระดับความรุนแรงที่เกิดขึ้น ทั้งนี้ไม่รวมถึงการก่อกวนหรือจู่โจมการบริการที่ไม่ได้มีความสำคัญต่อการดำรงชีวิตขั้นพื้นฐานของประชาชน

คำนิยามผู้ก่อการร้ายไซเบอร์

ดังคำนิยามข้างต้นนี้มีความใกล้เคียงกับข้อมูลที่ได้จากการสัมภาษณ์ผู้เชี่ยวชาญทั้งสิบกว่าคนสำคัญของภาครัฐจะนำมาใช้เป็นมาตรวัดว่าการก่อการร้ายในนิยามของงานวิจัยเล่มนี้คืออะไร แต่ข้อจำกัดเพียงบางข้อ อย่างเช่น การมุ่งเป้าหมายของการก่อการร้ายไซเบอร์นั้นควรพิจารณาเฉพาะข้อมูลทางเทคโนโลยีสารสนเทศเท่านั้นหรือไม่ เมื่อคำนึงถึงนิยามการก่อการร้ายไซเบอร์ ผู้ก่อการร้ายไซเบอร์ในที่นี้ อาจรวมไปถึง คนสอดแนมทางไซเบอร์ อาชญากรไซเบอร์ ผู้จู่โจมไซเบอร์ หรือแม้กระทั่งแฮกเกอร์สมัครเล่นหรือมืออาชีพ ที่มีจุดประสงค์ที่จะทำลายระบบคอมพิวเตอร์ ขโมยข้อมูลส่วนบุคคล ข้อมูลลับทางการค้าทางเศรษฐกิจ การระงับการบริการต่างๆ ปล่อยไวรัสในระบบคอมพิวเตอร์ ปลอมแปลงธุรกรรมทางการเงิน หรือแม้กรทั่งใช้วิธีคุกคามส่วนบุคคลหรือนิติบุคคล การกระทำเหล่านี้มีบ่อเกิดที่ง่ายและสร้างพลังอันยิ่งใหญ่ให้กับผู้ก่อการร้ายไซเบอร์ในอนาคตเพราะมีเว็บไซต์นับพันเว็บไซต์ที่คอยอำนวยความสะดวกให้กับและให้ทักษะกับผู้จู่โจมทางไซเบอร์มือใหม่ให้เป็นผู้ที่มีความเชี่ยวชาญได้ในอนาคตโดยไม่ต้องแม้กระทั่งค่าใช้จ่ายใด ๆ

ผลกระทบจากการก่อการร้ายไซเบอร์ จะประกอบไปด้วยการพิจารณาสภาพเงื่อนไขของอุปกรณ์ที่ใช้และความร้ายแรงที่ส่งผลต่อร่างกายและจิตใจของมนุษย์ เพื่อที่จะทำให้เข้าใจมากขึ้น การก่อการร้ายนั้นรวมไปถึงการกระทำออฟไลน์ หรือส่งผลกระบไปยังโลกแห่งความจริงและเกิดความ

เสียหายที่มากกว่าข้อมูลสารสนเทศในระบบคอมพิวเตอร์ นิยามการก่อการร้ายไซเบอร์ในมุมมองนี้มีความเป็นเอกลักษณ์และไม่สามารถพบได้ตามวารสารวิชาการทางด้านการก่อการร้ายไซเบอร์ทั่วไป

Weimann (2005: pp. 129-149) ให้ข้อจำกัดของคำนิยามการก่อการร้ายในแนวคิดของการใช้โครงข่ายคอมพิวเตอร์เป็นอุปกรณ์ในการทำลายสาธารณูปโภคสำคัญของประเทศเพื่อให้เกิดความเสียหายคำนิยามนี้มีความคล้ายกันในแนวความคิดของผู้เชี่ยวชาญทางด้านเทคนิคละผู้กำหนดนโยบายทางไซเบอร์ในหน่วยงานด้านการกำกับดูแลความมั่นคงปลอดภัย เช่น สภาความมั่นคงแห่งชาติ และหน่วยงานที่มีความเสี่ยงต่อการโจมตี เช่น การไฟฟ้าส่วนผลิต กระทรวงสาธารณสุข และกระทรวงยุติธรรม สาเหตุที่หน่วยงานประเภทนี้มีแนวความคิดที่คล้ายกันเพราะเป็นลักษณะของหน่วยงานเองเป็นหน่วยงานที่เป็นกลุ่มเสี่ยงและเป็นหน่วยงานความมั่นคงหรือควบคุมสาธารณูปโภคสำคัญของประเทศ เพราะฉะนั้นความหวาดกลัวที่ถูกสร้างขึ้นจากผู้ก่อการร้ายไซเบอร์อาจใช้เรียกเป็นคำนิยามสำหรับหน่วยงานเหล่านี้ได้

Hua and Bapna (2012: pp. 102-114) ให้คำนิยามการก่อการร้ายไซเบอร์เพิ่มเติมว่าเป็นกิจกรรมที่กระทำด้วยระบบคอมพิวเตอร์ อินเทอร์เน็ต และเทคโนโลยีสารสนเทศ มีจุดมุ่งหมายทางการเมือง ต้องการบิดเบือนความน่าเชื่อถือของรัฐบาล เป็นผลที่ทำให้เกิดความรุนแรงเสียหายทั้งในเชิงในเชิงกายภาพและสร้างความหวาดกลัวให้ประชาชนเหมือนกลยุทธ์ที่ใช้กับการก่อการร้ายแบบดั้งเดิม แนวคิดการกำหนดคำนิยามของ Hua and Bapna มีความคล้ายคลึงกับผู้กำหนดนโยบายของหน่วยงานด้านฝ่ายปราบปราบ เช่น ศูนย์ไซเบอร์กองทัพบก ศูนย์ไซเบอร์กองทัพอากาศ และยังมีความคล้ายคลึงกับแนวคิดของผู้กำหนดนโยบายทางไซเบอร์ของหน่วยงานด้านการกำกับดูแลความมั่นคงปลอดภัย คือ สำนักข่าวกรองแห่งชาติ และ กสทช. พร้อมถึงอาจารย์ผู้มีความเชี่ยวชาญทางด้านการก่อการร้ายแบบดั้งเดิมซึ่งจะมีแนวคิดพื้นฐานที่อ้างถึงกลยุทธ์การก่อการร้ายแบบเก่า แต่เพียงแค่การก่อการร้ายไซเบอร์นั้นเป็นเพียงแค่การเปลี่ยนแปลงการใช้อาวุธจาก ดาบ ปืน หรือ ระเบิดมาเป็น ระบบเครือข่ายคอมพิวเตอร์ในการทำลาย แนวคิดการให้นิยามการก่อการร้ายแบบนี้มักสนใจถึงจิตวิทยาในการใช้ของผู้ก่อการร้ายไซเบอร์ ผู้ก่อการร้ายจะต้องมีอุดมการณ์ที่ชัดเจนเพียงพอที่จะโน้มน้าวให้คนส่วนใหญ่เชื่อในสิ่งที่พวกตนต้องการหรือหมดความเชื่อถือต่อรัฐบาล และเมื่อนั้นรัฐบาลจึงถึงว่าเป็นภัยคุกคามแบบหนึ่งในรูปแบบการก่อการร้ายไซเบอร์ จึงมีการตั้งหน่วยงานไซเบอร์ขึ้นมาโดยเฉพาะเพื่อสอดส่องการกระทำที่เข้าข่ายกับนิยามข้างต้นหรือที่เรียกว่า (Information Operation: IO) หรือยุทธการทางข้อมูลข่าวสารเพื่อสอดแนมและระวังการใส่ร้ายหรือบิดเบือนรัฐบาลผ่านช่องทางอินเทอร์เน็ต แนวคิดนิยามการก่อการร้ายไซเบอร์ในรูปแบบนี้จึงมีความใกล้เคียงกับกลยุทธ์การใช้แรงจูงใจเพื่อสร้างกลุ่มคนที่มีแนวคิดอุดมการณ์เดียวให้เปลี่ยนความเชื่อตามเป้าหมายของผู้ก่อกรร้ายไซเบอร์ การกระทำเชิงจิตวิทยาในรูปแบบนี้จึงเป็นคุณลักษณะเด่นของการก่อการร้ายไซเบอร์และทำ

ให้วิธีการรับมือของการก่อการร้ายในแนวคิดนี้มีความแตกต่างไปจากการรับมือการก่อการร้ายในการให้นิยามแบบอื่น

โดยสรุปนิยามการก่อการร้ายไซเบอร์จากการค้นคว้าหาข้อมูลจากเอกสารและจากการสัมภาษณ์มีทั้งความเหมือนและความแตกต่างกันดังนี้

ตารางที่ 9 นิยามการก่อการร้ายไซเบอร์จากการค้นคว้าหาข้อมูลจากเอกสารและจากการสัมภาษณ์

แหล่งที่มาของข้อมูล	ค้นคว้าเอกสาร	การสัมภาษณ์
1. ตัวแสดง	ตัวแสดงมีการระบุได้อย่างชัดเจนว่าเป็นผู้กระทำประเภทใดถึงสามารถเรียกว่าผู้ก่อการร้าย	ตัวแสดงมีความยืดหยุดไม่สามารถเรียกว่าผู้ก่อการร้ายแต่จะเรียกตามการกระทำของตัวแสดงที่เกิดขึ้น เช่น การแฮกจะเรียกผู้กระทำว่าแฮกเกอร์ไม่ใช่ผู้ก่อการร้ายถึงแม้จะมีส่วนประกอบครบถ้วนตามนิยาม
2. วิธีการ	เน้นวิธีการลับหลัง โจมตีทำร้ายผู้บริสุทธิ์ ทำลายสาธารณูปโภคสำคัญต่าง ๆ หรืออาวุธนิวเคลียร์ผ่านช่องทางทางไซเบอร์	ใช้วิธีการชักจูงผ่านทางโซเชียลมีเดียให้ประชาชนมีความเชื่อในแบบเดียวกัน
3. ความรุนแรง	ความรุนแรงส่งผลกระทบในระดับโลกหรือระหว่างประเทศมหา อำนาจ ผลเสียทางการเงินมีมูลค่าหลายล้านดอลลาร์เน้นการเมืองระหว่างประเทศ เช่น สหรัฐกับอิหร่าน จีนกับฝรั่งเศส รัสเซียกับสหราชอาณาจักร	เกิดความเสียหายในระดับท้องถิ่นหรือส่วนบุคคลเป็นส่วนใหญ่
4. จุดประสงค์ทางการเมือง	องค์ประกอบในข้อนี้เป็นส่วนสำคัญโดยเอกสารต่าง ๆ จะเน้นเรื่องจุดประสงค์ทางการเมืองระหว่างประเทศมากกว่าการ	จุดประสงค์ทางการเมืองในที่นี้โดยส่วนใหญ่จะหมายถึงการบิดเบือนข้อมูลหรือการใส่ร้ายรัฐบาลและทำให้สถาบันความ

ตารางที่ 9 นิยามการก่อการร้ายไซเบอร์จากการค้นคว้าหาข้อมูลจากเอกสารและจากการสัมภาษณ์ (ต่อ)

แหล่งที่มาของข้อมูล	ค้นคว้าเอกสาร	การสัมภาษณ์
	บิดเบือนข้อมูลเพื่อทำให้คนในประเทศหลงเชื่อ การทำลายสาธารณูปโภคต่าง ๆ ที่ส่งผลให้คนบริสุทธิ์ถูกทำลายถือเป็นการขู่รัฐบาลประเทศนั้น	มั่นคงของรัฐเสื่อมเสีย เหตุการณ์เหล่านั้นจะถูกตั้งข้อสังเกตว่าเป็นการก่อการร้ายในสายตาผู้สัมภาษณ์ ส่วนการทำลายสาธารณูปโภคสำคัญนั้นก็เป็นส่วนหนึ่งแต่ประเทศไทยยังไม่พบเจอสิ่งเหล่านั้น

จุดร่วมกันของนิยามการก่อการร้ายไซเบอร์จากการค้นคว้าหาข้อมูลจากเอกสารและการสัมภาษณ์ คือ การก่อการร้ายไซเบอร์ต้องประกอบไปด้วยจุดประสงค์ทางการเมืองเป็นหลัก

จุดแตกต่างระหว่างนิยามการก่อการร้ายไซเบอร์จากการค้นคว้าหาข้อมูลจากเอกสารและการสัมภาษณ์จะเน้นนิยามที่มีความผูกพันธ์ด้วยกฎหมาย แต่จากการสัมภาษณ์บุคคากรจากภาครัฐไทยนั้นไม่ได้กล่าวถึงประเด็นในส่วนนี้ แต่จะมีเพียงมุมมองของนักวิชาการจากต่างประเทศที่จะให้ความสำคัญสอดคล้องไปกับนิยามทางด้านกฎหมายด้วย

นิยามเป็นจุดเริ่มต้นที่สำคัญในการต่อยอดของการรับมือการก่อการร้ายไซเบอร์ต่อไปของแต่ละองค์กร จากการสัมภาษณ์เชิงลึกและการศึกษาข้อมูลเชิงเอกสารจึงสามารถแสดงให้ถึงสภาพปัญหาของการให้คำนิยามและการรับมือของการก่อการร้ายดังนี้

1. แนวความคิดเชิงนโยบายของหน่วยงานให้ความหมายของการก่อการร้ายไซเบอร์คลุมเครือ

การเริ่มต้นจากคำนิยามเป็นสิ่งที่สำคัญมากในที่ทำให้นักวางแผนนโยบายทางไซเบอร์ขององค์กรนำแผนไปใช้ได้เกิดประสิทธิภาพหรือไม่ การการสัมภาษณ์เชิงลึกทราบว่าร้อยละ 90 ของผู้ร่างนโยบายทางเทคโนโลยีของหน่วยงานจะมีพื้นฐานทางคอมพิวเตอร์อย่างน้อยคือการจบจากคณะวิศวกรรมศาสตร์และคณะวิทยาศาสตร์คอมพิวเตอร์ ทำให้พวกเขาเหล่านั้นสามารถเข้าใจความเป็นเทคโนโลยีได้เป็นอย่างดีและสามารถสั่งการและเขียนนโยบายให้กับเจ้าหน้าที่ผู้ที่มีทักษะทางเทคโนโลยีได้อย่างเข้าใจ แต่อย่างไรก็ตามหากการมองจากภาพรวมการจัดการปัญหาทางไซเบอร์มีหลายระดับ และการขาดการให้คำนิยามที่ชัดเจนของคำว่าการก่อการร้ายไซเบอร์ไม่ว่าจะเป็นลักษณะของการกระทำ หรือระดับความรุนแรงของเหตุที่เกิดขึ้นจึงไม่สามารถทำให้เจ้าหน้าที่ทางเทคนิคเข้าใจ

ได้ว่าการก่อการร้ายนั้นคืออะไร และการรับมือที่มีอยู่นั้นเป็นเพียงแค่การรับมืออาชญากรรมไซเบอร์หรือไม่

2. ลักษณะของการก่อการร้ายและอาชญกรรมทางไซเบอร์มีความคล้ายคลึงกัน

อย่างที่ได้กล่าวไปข้างต้นว่าลักษณะของการก่อการร้ายแลอาชญากรรมไซเบอร์มีความคล้ายคลึงกันและการจะแบ่งแยกระหว่างการก่อการร้ายและอาชญกรรมไซเบอร์ได้นั้นจะต้องพิจารณาภายใต้ 4 องค์ประกอบ นั่นคือ ระดับความรุนแรง จุดประสงค์ทางการเมืองหรืออุดมการณ์ของผู้กระทำ เกิดความรุนแรงต่อผู้บริสุทธิ์ และเป็นการสร้างการขับเคลื่อนเพื่อให้เกิดการปกครองรูปแบบใหม่มีการใช้จิตวิทยาในการชักนำ รวมกลุ่มผู้ที่มีอุดมการณ์เดียวกัน ซึ่งจะแตกต่างกับการจู่โจมหรืออาชญากรรมไซเบอร์ธรรมดาที่เป็นเพียงผู้ที่มีทักษะทางด้านคอมพิวเตอร์ไม่สูงมากนักและเป็นการกระทำเป็นครั้งคราว ไม่ได้มีจุดประสงค์ที่จะทำลายสถาบันใดสถาบันหนึ่งอย่างชัดเจน การสอบถามจึงทำให้ทราบว่าปัจจุบันนั้นการจู่โจมทางไซเบอร์หรือคอมพิวเตอร์นั้นมีทุกวินาทีแต่ถ้าหากถามถึงการก่อการร้ายไซเบอร์ที่เต็มรูปแบบนั้นก็ยังไม่มีหน่วยงานใดเคยประสบพบเจอ ในบางความเห็นของผู้เชี่ยวชาญนั้นคิดว่าการใช้เทคโนโลยีของประเทศไทยยังไม่ใช่ช่องทางหลักในการบริหารงานสำคัญ การขโมยข้อมูลสำคัญหรือการทำลายระบบจึงมีน้อยหรือไม่ผู้ก่อการร้ายอาจใช้แค่ประเทศไทยนั้นเป็นเพียงแค่ทางผ่านในการก่อการร้ายเท่านั้น

3. การนำนโยบายในเชิงการก่อการร้ายไซเบอร์ไม่สามารถนำไปใช้จริงในเหตุการณ์ต่าง ๆ ที่มีแนวโน้มที่จะเกิดขึ้นในอนาคตได้

หน่วยงานทุกหน่วยงานในประเทศไทยมีความตระหนักถึงภัยทางไซเบอร์และการคุกคามทางไซเบอร์ในระดับที่ดี มีการส่งรายงานประจำประจำปี แก่ ETDA เพื่อประเมินภัยคุกคามทางไซเบอร์ที่แต่ละหน่วยงานนั้นเจอ แต่เราสำหรับนโยบายและพระราชบัญญัติที่ออกมานั้นจะไม่ครอบคลุมถึงการก่อการร้ายไซเบอร์ เพราะยังไม่สามารถใช้คำนิยามที่คลุมคลุมและเหมาะสมได้ ดังนั้น การรับมือของประเทศไทยในขณะนี้จึงเป็นการปะติดปะต่อภาพของภัยคุกคามทางไซเบอร์ในระดับเล็กน้อยเพื่อสร้างความหมายที่แท้จริงของการก่อการร้ายไซเบอร์

โดยสรุปแล้วนิยามการก่อการร้ายไซเบอร์ยังคงไม่มีความชัดเจนในหน่วยงานของประเทศไทยแม้กระทั่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 นั้นยังไม่ได้มีการบัญญัติถึงการก่อการร้ายทางไซเบอร์ ทำให้การรับมือหรือวางนโยบายของเรื่องการก่อการร้ายไซเบอร์เป็นเรื่องที่ยังคุมเครือและไม่สามารำแผนนโยบายไปปฏิบัติใช้ได้จริง

4.4 การรับมือสถานการณ์ภัยคุกคามทางไซเบอร์

สถานการณ์ภัยคุกคามทางไซเบอร์ของประเทศไทยส่วนมากยังไม่สามารถยกระดับได้ว่าเป็นการก่อการร้ายทางไซเบอร์ จากการประมวลผลและวิเคราะห์จากบทสัมภาษณ์ของบุคคลกรที่มีความเชี่ยวชาญจากหน่วยงานภาครัฐ ไม่ว่าจะเป็นหน่วยงานที่ทำหน้าที่ดูแลควบคุมภัยคุกคามทางไซเบอร์ หน่วยงานที่เป็นเป้าหมายสำคัญในการจู่โจมทางไซเบอร์ หรือ หน่วยสาธารณูปโภคสำคัญต่าง ๆ และหน่วยงานทางทหารที่ทำหน้าที่ป้องกันภัยคุกคามภัยไซเบอร์ในระดับชาติ ต่างมีความเห็นไปในทางเดียวกันว่า ภัยคุกคามส่วนใหญ่แล้วเป็นภัยคุกคามที่เกิดจากมัลแวร์ โดยการใช้มัลแวร์เรียกค่าไถ่โจมตีมายังระบบคอมพิวเตอร์ของผู้ใช้งาน และการปลอมแปลงอีเมลหลอกลวงส่งเอกสารแนบที่แฝงมัลแวร์เข้ามาเพื่อจารกรรมข้อมูลสำคัญในองค์กรความเสียหายที่เกิดขึ้นกับองค์กรยังมีไม่มากนัก โดยหากวัดตามมาตรการของ สกมช. ยังถือว่าอยู่ในระดับไม่ร้ายแรง ดังรูปที่ 20 (คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ, 2564)

รูปที่ 20 ระดับของภัยคุกคามทางไซเบอร์
ที่มา: ThaiCERT(2018)

เป็นภัยคุกคามทางไซเบอร์ที่ทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศหรือการให้บริการของรัฐด้อยประสิทธิภาพลง นอกจากการจะมีการจู่โจมโดยใช้ช่องว่างทางระบบแล้ว ภัยคุกคามทางไซเบอร์ของประเทศไทยยังมาจากการที่ผู้จู่โจมใช้ช่องว่างจะการขาดความตระตระหนักรู้จากบุคลากร ภัยคุกคามประเภทนี้เกิดขึ้นส่วนใหญ่กับบุคลากรที่ยังขาดความ

ตระหนักรู้ทางด้านไซเบอร์ ตัวอย่างเช่น ภัยคุกคามที่เกิดขึ้นกับธนาคารบางสาขาหรือโรงพยาบาล เครือข่ายที่ภารกิจหลักของเจ้าหน้าที่นั้นมีมากจึงอาจเกิดความบกพร้องหรือขาดความตระหนักรู้ทางด้านเทคโนโลยี แต่อย่างไรก็ตามภัยคุกคามทั้งสองประเภทดังกล่าวเกิดขึ้นบ่อยครั้งกับหน่วยงานภาครัฐ หากพิจารณาในกรณีที่หน่วยงานสามารถตรวจจับได้สามารถเฉลี่ยได้วันละ 150 ครั้งต่อวัน สำหรับหน่วยงานที่เป็นเป้าหมายหรือสาธารณูปโภคสำคัญ หรือแม้แต่กระทั่งหน่วยงานความมั่นคงไม่ว่าจะเป็นฝ่ายพลเรือนหรือทหารจะประสบพบเจอภัยคุกคามในแบบเดียวกัน แต่ด้วยความสามารถในการรับมือของหน่วยงานนั้นทำให้การตรวจจับในแต่ละครั้งไม่เกิดความเสียหายในระดับรุนแรงแต่ก็ไม่สามารถทราบว่าข้อมูลที่ผู้จู่โจมได้ไปนั้นคืออะไร ภัยคุกคามในประเทศไทยส่วนใหญ่ที่เกิดขึ้นกับหน่วยงานภาครัฐจะถูกแจ้งไปยัง ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) เพื่อให้เข้ามาควบคุมดูแลและฟื้นฟูระบบ จากการเก็บข้อมูลทั้งหมดทราบว่าหน่วยงานที่มีรายงานการถูกโจมตีน้อยที่สุดได้แก่ กระทรวงยุติธรรม กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี และสำนักงานรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ซึ่งเฉลี่ยเดือนละ 1 ครั้ง

จากการประเมินสถานการณ์จากผู้เชี่ยวชาญทั้งด้านเทคนิคและด้านนโยบายทางไซเบอร์สามารถสรุปได้ว่าหน่วยงานภาครัฐในประเทศยังพบเพียงแค่ปัญหาเล็กน้อย โดยภัยคุกคามที่มีความคล้ายคลึงการนิยามการก่อการร้ายมากที่สุดมี 3 เหตุการณ์ จากบทสัมภาษณ์ของผู้เชี่ยวชาญจากหน่วยงานที่แตกต่างกัน ดังนี้

> *“ครั้งที่คดีความเรื่องชาวเมียนมา 2 คนที่ถูกศาลฎีกาตัดสินประหารชีวิตในข้อหาฆาตกรรมนักท่องเที่ยวชาวอังกฤษที่เกาะเต่า จ.สุราษฎร์ธานี ครั้งนั้นชาวเมียนมามีความคับแค้นข้องใจในคดีและคิดว่าชาวเมียนมาทั้ง 2 คนนั้นเป็นเพียงแพะรับบาปเท่านั้น หลังจากนั้นจึงมีแฮคเกอร์ชาวเมียนมากลุ่มรวมกลุ่มกันโจมตีเวปไซต์หน้าเพจของหน่วยงานราชการไทย โดยการเปลี่ยนหน้าเพจเป็นรูปที่ไม่เหมาะสมกับเวปไซร์ของ องค์การบริหารส่วนตำบลเกาะเต่า การโจมตีครั้งนั้นผู้โจมตีทางไซเบอร์มีวัตถุประสงค์ทางการเมืองอย่างชัดเจน มีความต้องการที่จะบิดเบือนและทำให้หน่วยงานของรัฐสูญเสียความน่าเชื่อถือและใช้วิธีและกลยุทธ์ในรูปแบบการก่อการร้ายแต่ผลที่เกิดขึ้นนั้นไม่ได้เกิดความเสียหายในระดับรุนแรง ผมคิดว่าเหตุการณ์นี้มีความใกล้เคียงกับการก่อการร้ายมากที่สุดแต่ก็ยังไม่ถือว่าเป็นการก่อการร้ายทางไซเบอร์ที่รุนแรงมากนัก”*
>
> ผู้ให้ข้อมูลสำคัญคนที่ 14 (เจ้าหน้าที่ศูนย์ไซเบอร์กองทัพบก)

“โรงพยาบาลสระบุรี โดน ransomware!!! เรียกค่าไถ่ ยังคงเป็นเคสการโจมตีทางไซเบอร์ที่เป็นข่าวดังนช่วงระยะหนึ่งเมื่อกันยายน 2563 โดยโรงพยาบาลสระบุรี ซึ่งเป็นโรงพยาบาลประจำจังหวัดได้ออกประกาศว่าระบบของโรงพยาบาลไม่สามารถใช้ได้จึงทำให้เกิดความล่าช้า ในครั้งนี้เกลุ่มแฮกเกอร์ เรียกค่าไถ่กว่าจำนวน 200,000 บิตคอยน์ หรือประมาณ 63,000 ล้านบาท เพื่อจะให้ระบบของโรงพยาบาลกลับมาใช้งานได้แต่เนื่องจากทางโรงพยาบาลได้ backup ข้อมูลไว้ย้อนหลังตั้งแต่ 2548 ซึ่งเป็นเวลา 5 ปี จึงทำให้ผู้บริหารไม่จำเป็นต้องเสียเงินจำนวนมหาศาลเพื่อแลกกับข้อมูลคนไข้ แต่การแก้ไขในครั้งนั้นใช้เวลาเพียงแค่ 3 วันระบบก็สามารถกลับมาใช้งานดังเดิมได้ ความสำเร็จในครั้งส่วนหนึ่งเป็นผลงานของไทยเสิร์ตที่เข้ามาช่วยเหลือ”

ผู้ให้ข้อมูลสำคัญคนที่ 3 (เจ้าหน้าที่ทางด้านนโยบาย สป.สธ)

“คดีแฮกเกอร์บุกเจาะข้อมูลบริษัท Sony Picture สร้างความเสียหายหลายล้านดอลลาร์สหรัฐฯ เป็นคดีใหญ่ระดับโลกและสืบเสาะต้นเหตุได้ว่าผู้โจมตีได้เปิดโรงแรมหรูที่ประเทศไทยเป็นฐานในการจู่โจม เหตุการณ์นี้แสดงให้เห็นว่าประเทศไทยก็เป็นส่วนหนึ่งในการก่อการร้ายไซเบอร์ข้ามชาติได้ และการหาเบาะแสหรือการจับกุมก็เป็นไปได้ยากเพราะฉะนั้นการที่ประเทศไทยไทยจะเป็นกลายเป็นเหยื่อหรือถูกพาดพิงก็เป็นเรื่องที่จะเกิดขึ้นง่ายในอนาคต”

ผู้ให้ข้อมูลสำคัญคนที่ 15 (ผู้อำนวยการกองปฏิบัติการไซเบอร์ สกมช.)

“คดีที่เป็นภัยคุกคามจ่อประเทศไทยจริง ๆ นั้นมีน้อยมา และไม่ได้สร้างความเสียหายให้กับประเทศในระดับความรุนแรงมากมายหมาศาล ประเทศไทยยังคงรับมือภัยคุกคามที่เกิดจากภัยไซเบอร์โดยส่วนใหญ่จะเป็นในรูปแบบปัจเจกได้ดีและสามารถช่วยเหลือ แก้ไขปัญหา กู้คืนข้อมูลได้ทัน”

ผู้ให้ข้อมูลสำคัญคนที่ 8 (ผกก. กลุ่มงานสนับสนุนคดีเทคโนโลยี ปอท.)

เพื่อเป็นการสรุปความคิดเห็นของการก่อการร้ายในประเทศจากผู้ให้ข้อมูลทั้ง 3 กลุ่ม จึงสามารถแสดงตามตารางที่ 10 ดังนี้

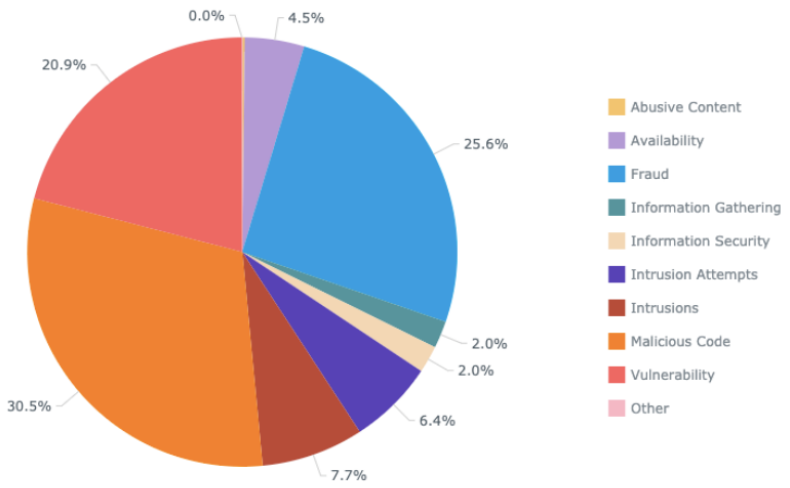
ตารางที่ 10 แสดงแนวคิดความคิดเห็นของการก่อการร้ายในประเทศ

หน่วยงาน	แนวความคิดเห็นที่เหมือกัน	แนวความคิดเห็นที่ต่างกัน
หน่วยงานควบคุมดูแล	- จุดประสงค์ทางการเมืองของผู้ก่อการร้าย - ยังไม่มีผู้ก่อการร้ายทางไซเบอร์ที่แท้จริงในประเทศไทย - ใช้วิธีการก่อการร้ายแบบกองโจร ทำลายผู้บริสุทธิ์	- ผลกระทบที่เกิดขึ้นจะต้องสร้างความเสียหายทั้งภาครัฐและประชาชน
หน่วยงานปราบปรามด้านทหาร	- จุดประสงค์ทางการเมืองของผู้ก่อการร้าย - ใช้วิธีการก่อการร้ายแบบกองโจร ทำลายผู้บริสุทธิ์	- ผลกระทบที่เกิดขึ้นจะต้องมีผลกระทบต่อสถาบันหลักของสถาบัน - มีผู้ก่อการร้ายที่แท้จริงเกิดขึ้นในประเทศไทย แต่การก่อการร้ายนั้นอาจไม่มีผลกระทบในระดับสูง
หน่วยงานที่เป็นเป้าหมายของผู้ก่อการร้าย	- จุดประสงค์ทางการเมืองของผู้ก่อการร้าย - ใช้วิธีการก่อการร้ายแบบกองโจร ทำลายผู้บริสุทธิ์	- ความเสียหายที่หายที่เกิดขึ้นจะต้องมีผลกระทบต่อประชาชนเป็นหลัก

4.4.1 สถานการณ์ภัยคุกคามทางไซเบอร์ในประเทศไทย

ในปัจจุบันประเทศไทยพบว่ามีภัยคุกคามทางไซเบอร์ 4 ย้อนหลังอยู่ประมาณที่จำนวน 2000 กว่าครั้งและภัยคุกคามที่พบส่วนใหญ่คือความพยายามที่จะเจาะระบบทางไซเบอร์ การหลอกลวง การใช้ช่องว่างทางระบบคอมพิวเตอร์เพื่อเข้าโจมตี และ การใช้ Malicious code ในการสร้างความวุ่นวาย โดยในปีหลัง ๆ นั้นการพัฒนาของภัยคุกคามเน้นไปที่ การใช้ Malicious code ในการสร้างความวุ่นวายมากที่สุด และ การใช้ช่องว่างทางคอมพิวเตอร์เพื่อจู่โจม คือ ร้อยละ 30.5 และ 41 ตามลำดับ (ThaiCERT, 2021)

จำแนกตามประเภทภัยคุกคาม



รูปที่ 21 แสดงจำนวนประเภทภัยคุกคามในปี พ.ศ. 2563

ที่มา: ThaiCERT (2021)

ภัยคุกตามที่แยกให้เห็นนั้นพบว่า การใช้ Malicious code มีร้อยละ 30.5 คิด 687 ครั้งต่อปี นอกจากนั้นยังมีการใช้จุดอ่อนหรือช่องโหว่ หมายถึง สภาพแวดหรือสภาวะที่เป็นข้อบกพร่องหรือไม่สมบูรณ์นำไปสู่การจู่โจมระบบก็เป็นสาเหตุหลักใกล้เคียงกับ การใช้ Malicious code ส่วนในเรื่องการหลอกลวงก็ยังคงเป็นภัยคุกตามร่วมสมัยที่ยังคงพบเจออยู่ในปัจจัยสังเกตเห็นได้จากตารางข้างล่างนี้

ตารางที่ 11 แสดงจำนวนสถิติภัยคุกคามในปี พ.ศ. 2563 (ข้อมูลจากการสัมภาษณ์)

สถิติภัยคุกคาม ประจำปี พ.ศ. 2563

ประเภทภัยคุกคาม / เดือน	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	รวม
Abusive content	0	0	1	1	0	1	0	0	0	0	0	1	**4**
Availability	10	19	19	9	12	26	2	0	0	2	0	2	**101**
Fraud	50	52	76	103	38	27	22	61	24	35	35	53	**576**
Information gathering	3	0	9	3	1	8	6	6	2	1	4	3	**46**
Information security	11	0	0	1	4	10	0	2	0	2	13	3	**46**
Intrusion Attempts	22	30	6	3	5	6	2	10	23	4	10	24	**145**
Intrusions	51	10	13	4	4	14	4	2	17	28	12	14	**173**
Malicious code	84	101	94	91	84	77	22	23	26	40	24	21	**687**
Vulnerability	31	27	1	3	109	109	94	14	7	14	51	11	**471**
Other	1	0	0	0	0	0	0	0	0	0	0	0	**1**
รวม	**263**	**239**	**219**	**218**	**257**	**278**	**152**	**118**	**99**	**126**	**149**	**132**	**2250**

ที่มา: ThaiCERT (2021)

ต่อมาใน พ.ศ. 2564 ภัยคุกคามของประเทศไทยยังคงอยู่ที่จำนวน 1336 ครั้ง แต่เนื่องจากข้อมูลนี้เก็บได้เพียงแค่เดือนสิงหาคม ในตัวข้อมูลเลยไม่สมบูรณ์มากนัก แต่สิ่งที่แตกต่างจากปี พ.ศ. 2563 นั่นก็คือ การใช้จุดอ่อนหรือช่องโหว่มีมากที่สุดมีจำนวน 548 ครั้ง โดยทั่วไปข่าวสารเกี่ยวกับช่องโหว่ มักจะได้มาจาก เจ้าของผลิตภัณฑ์หรือ เว็บไซต์ทางด้านความมั่นคงปลอดภัย และการไม่ติดตั้งโปรแกรมต่อต้านไวรัสก็เป็นสาเหตุสำคัญที่ทำให้ข้อมูลเสียหายและข้อมูลถูกขโมย ทั้งหมดมาจากการขาดความตระหนักรู้ของผู้ใช้

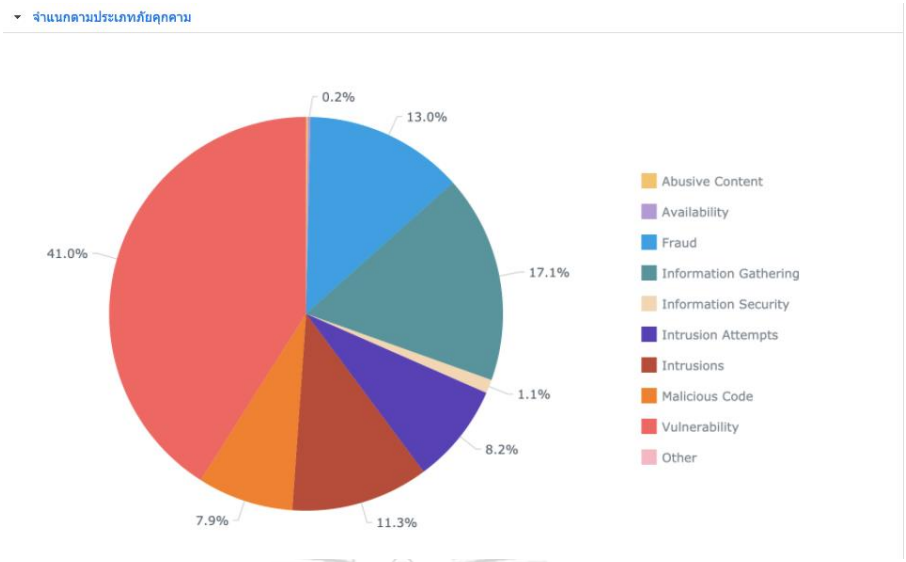
ตารางที่ 12 แสดงจำนวนสถิติภัยคุกคามในปี พ.ศ. 2564 (ข้อมูลจากการสัมภาษณ์)

สถิติภัยคุกคาม ประจำปี พ.ศ. 2564

ประเภทภัยคุกคาม / เดือน	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	รวม
Abusive Content	0	1	0	0	0	1	0	0	0	0	0	0	**2**
Availability	0	0	1	0	1	0	1	0	0	0	0	0	**3**
Fraud	46	20	26	16	27	16	13	10	0	0	0	0	**174**
Information Gathering	12	24	49	25	29	27	42	20	0	0	0	0	**228**
Information Security	4	5	0	0	2	2	0	2	0	0	0	0	**15**
Intrusion Attempts	21	15	25	20	14	5	6	4	0	0	0	0	**110**
Intrusions	32	27	29	8	15	15	11	14	0	0	0	0	**151**
Malicious Code	8	29	21	10	12	9	11	5	0	0	0	0	**105**
Vulnerability	31	5	121	64	81	94	77	75	0	0	0	0	**548**
Other	0	0	0	0	0	0	0	0	0	0	0	0	**0**
รวม	**154**	**126**	**272**	**143**	**181**	**169**	**161**	**130**	**0**	**0**	**0**	**0**	**1336**

ที่มา: ThaiCERT (2021)

นอกจากการใช้จุดอ่อนหรือช่องโหว่แล้ว ยังคงมีเรื่อง ความพยายามรวบรวมข้อมูลของระบบหรือ Information Gathering จำนวน 228 ครั้ง เป็นการพยายามรวบรวมข้อมูลจุดอ่อนของระบบเพื่อนำข้อมูลนั้นไปใช้หรือทำให้ข้อมูลเหล่านั้นเสียหาย ภัยนี้มีแนวโน้มเกิดขึ้นมาในปีปัจจุบัน เห็นได้จากแผนภาพวงกลมข้างล่าง



รูปที่ 22 แสดงจำนวนประเภทภัยคุกคามในปี พ.ศ. 2564 (ข้อมูลจากการสัมภาษณ์)
ที่มา: ThaiCERT (2021)

4.4.2 การรับมือภัยคุกคามทางไซเบอร์ในประเทศไทย

ในการวิจัยฉบับนี้ได้แบ่งกลุ่มการศึกษาหน่วยงานที่ได้รับผลกระทบและต้องรับมือการการก่อการร้ายไซเบอร์เป็น 3 ประเภท นั่นคือ หน่วยงานด้านการกำกับดูแลความมั่นคงปลอดภัย หน่วยงานด้านการปราบปราม หน่วยงานที่มีความเสี่ยงต่อการโจมตี เพื่อง่ายในการเข้าถึงการรับมือภัยการก่อการร้ายไซเบอร์และนโยบายของหน่วยงาน ดังนี้

4.4.2.1 หน่วยงานด้านการกำกับดูแลความมั่นคงปลอดภัย

การแบ่งหน่วยงานเป็นด้านการกำกับดูแลนั้นจะแสดงให้เห็นถึงศักยภาพของหน่วยงานที่สามารถมีเทคโนโลยีและบุคลากรที่มีความรู้ด้านเทคโนโลยีเพื่อสามารถรับกับการโจมตีทางไซเบอร์ได้ทัน เพราะฉะนั้นภารกิจหลักของหน่วยงานประเภทนี้คือการสอดส่อง ดูแล ควบคุมและแก้ปัญหาเมื่อมีการจู่โจมเกิดขึ้น ในที่นี้ผู้วิจัยได้สัมภาษณ์ สภาความมั่นคงแห่งชาติที่ดูแลความมั่นคงปลอดภัยทางด้าน สาธารณูปโภคและเทคโนโลยีสารสนเทศที่สำคัญของประเทศ สำนักงานข่าวกรองแห่งชาติ ในที่นี้ผู้วิจัยมีความเห็นว่าภัยคุกคามที่โจมตีประเทศไทยนั้นจะต้องมีการสกัดกั้นจากหน่วยงานที่มีความพร้อมเพราะฉะนั้นสำนักงานข่าวกรองจึงเป็นหน่วยงานแรกที่จะรับรู้เรื่องภัยตุกคามเหล่านี้ที่มาจากนอกประเทศและสามารถรายงานไปยังหน่วยปราบปรามได้ กระทรวงดิจิทัลเพื่อพัฒนาเศรษฐกิจและสังคม เป็นหน่วยงานหลักก่อนที่จะมีจุดกำเนิด สกช. ที่มีหน้าที่คอยควบคุมดูแลภัยคุกคามทางไซเบอร์เป็นหลัก กระทรวงดิจิทัลฯจึงเป็นกระทรวงที่เป็นผู้นำทั้งในด้านนโยบายเพื่อบังคับใช้กับหน่วยงานอื่น ๆ ให้อยู่ในระบบเดียวกันทั่วประเทศ สำหรับสำนักงานพัฒนาธุรกรรมทาง

อิเล็กทรอนิกส์ (องค์การมหาชน) เป็นหน่วยงานที่มีหน้าที่ดูแลควบคุมความมั่นคงปลอดภัยทางไซเบอร์เป็นหลักและมีส่วนขึ้นอยู่กับคณะกรรมการที่มาจากสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

สำหรับผลจากกการสัมภาษณ์เชิงลึกนั้นทราบว่าประเทศไทยมีเครือข่ายการควบคุมดูแลภัยคุกคามทางไซเบอร์ที่แข็งแกร่งในด้านนโยบาย คือ การมีพัฒนาการการดูแลและป้องกันด้านไซเบอร์ในมิติของกฎหมาย มิติด้านการเมือง และมิติด้านสังคม

1) มิติของกฎหมาย

ประเทศไทยเริ่มมีการใช้กฎหมายเข้ามาเป็นส่วนหนึ่งในการควบคุมดูแลการกระทำความผิดทางคอมพิวเตอร์ตั้งแต่ พ.ศ. 2550 โดยมีชื่อว่า พระราชบัญญัติว่าด้วยความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีผลบังคับใช้ตั้งแต่วันที่ 10 มิถุนายน 2550 แต่อย่างไรก็ตามภัยคุกคามทางคอมพิวเตอร์ที่เกิดขึ้นในประเทศไทย ณ ขณะนั้น จะเป็นในเชิงข้อมูลสารสนเทศ การใช้ข่าวปลอม การบิดเบือนข่าวสารที่มีผลต่อความมั่นคงของรัฐบาล (เสาวลักษณ์ ศรีสุวรรณ, 2564: น. 238-248) แนวคิดด้านภัยคุกคามตามกฎหมายขณะนั้นยังถูกจำกัดเป็นวงแคบเกี่ยวกับระบบคอมพิวเตอร์ หรือหมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงาน เข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ หรือการกล่าวถึงข้อมูลทางคอมพิวเตอร์ ผู้ให้บริการ และผู้ใช้บริการ โดยมีสาระหลักเกี่ยวกับการละเมิดเข้าถึงคอมพิวเตอร์โดยมิชอบ ทำให้เกิดความเสียหายทั้งในตัวระบบและข้อมูลมีการระวางโทษจำคุกไม่เกินและปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

ต่อมาประเทศไทยมีแก้ไขโดยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 เนื้อหาสาระในการแก้นั้นยังคงไว้ซึ่งแนวคิดเดิมแต่เพียงแค่เปลี่ยนใจความในเชิงเทคนิคด้านกฎหมาย และแก้ไขในบางมาตรา แต่ พระราชบัญญัติคอมพิวเจอร์ฉบับนี้นำไปสู่การออกพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ซึ่งมีพัฒนาการแตกต่างจาก พระราชบัญญัติคอมพิวเตอร์ทั้ง 2 ทั้งสองฉบับอย่างชัดเจน (สำนักงานสภาความมั่นคงแห่งชาติ, 2560) โดยมีแนวเป็นแนวคิดในการยกระดับของไทยในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อให้รับกับสภาพสังคมที่จะเข้าสู่ยุคดิจิทัลอย่างเต็มรูปแบบในอนาคต ดังนั้นจึงมีเป้าหมายหลักคือการสร้างความพร้อมของไทยในการรับมือกับ ภัยคุกคามทางไซเบอร์อย่างครอบคลุมรอบด้านมากที่สุดเท่าที่สภาวะแวดล้อมเอื้ออำนวย เพื่อเสริมขีดความสามารถของไทยในด้านนี้ที่มีอยู่แล้ว ให้เข้มแข็งยิ่งขึ้นโดยมุ่งเน้น การมีกลไกกลางในการบริหารจัดการการรักษา ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ การปกป้องโครงสร้างสาธารณูปโภค พื้นฐานและการสร้างความตระหนักในทุกภาคส่วนและความร่วมมือกับ ต่างประเทศ (สำนักงานสภาความมั่นคงแห่งชาติ, 2560) แต่ว่าด้วยพระราชบัญญัติฉบับนี้จำเป็นต้องมีการจำกัดสิทธิและเสรีภาพส่วนบุคคลเพื่อให้การรักษาความมั่นคง

ปลอดภัยไซเบอร์มีประสิทธิภาพและเพื่อให้มีมาตรการป้องกัน รับมือ และ ลดความเสี่ยงจากภัยคุกคามทางไซเบอร์อันกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ

สิ่งที่น่าสนใจของพระราชบัญญัติฉบับนี้คือการกล่าวถึง “การรักษาความมั่นคงปลอดภัยไซเบอร์” “ภัยคุกคามทางไซเบอร์” “ไซเบอร์” “หน่วยงานของรัฐ” “เหตุการณ์ที่เกี่ยงกับความมั่นคงปลอดภัยไซเบอร์”“มาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์” “โครงสร้างพื้นฐานสำคัญทางสารสนเทศ” “หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ” และ “หน่วยงานควบคุมหรือกากับดูแล” ซึ่งทั้งหมดสามารถขยายความได้ ดังนี้ (สำนักงานสภาความมั่นคงแห่งชาติ, 2560)

(1) “การรักษาความมั่นคงปลอดภัยไซเบอร์” หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้น เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อย ภายในประเทศ

(2) “ภัยคุกคามทางไซเบอร์” หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้าย ต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึง ที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทางานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือ ข้อมูลอื่นที่เกี่ยวข้อง

(3) “ไซเบอร์” หมายความรวมถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้ เครือข่ายคอมพิวเตอร์ระบบอินเทอร์เน็ตหรือโครงข่ายโทรคมนาคมรวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป

(4) “หน่วยงานของรัฐ” หมายความว่า ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจ องค์กรฝ่ายนิติบัญญัติ องค์กรฝ่ายตุลาการ องค์กรอิสระ องค์การมหาชนและหน่วยงานอื่น ของรัฐ

(5) “ประมวลแนวทางปฏิบัติ” หมายความว่า ระเบียบหรือหลักเกณฑ์ที่คณะกรรมการกากับดูแล ด้านความมั่นคงปลอดภัยไซเบอร์กำหนด

(6) “เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์” หมายความว่า เหตุการณ์ที่เกิดจากการกระทำหรือการดำเนินการใด ๆ ที่มิชอบซึ่งกระทำการผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ซึ่งอาจเกิดความเสียหายหรือผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือความมั่นคงปลอดภัย ไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

(7) “มาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์” หมายความว่า การแก้ไข ปัญหาความมั่นคงปลอดภัยไซเบอร์โดยใช้บุคลากร กระบวนการ และเทคโนโลยี โดยผ่านคอมพิวเตอร์ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ หรือบริการที่เกี่ยวกับคอมพิวเตอร์ใด ๆ เพื่อสร้างความมั่นใจ และเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

(8) “โครงสร้างพื้นฐานสำคัญทางสารสนเทศ” หมายความว่า คอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งหน่วยงานของรัฐหรือหน่วยงานเอกชนใช้ในกิจการของตนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็น ประโยชน์สาธารณะ

(9) “หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ” หมายความว่า หน่วยงานของรัฐหรือ หน่วยงานเอกชน ซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(10) “หน่วยงานควบคุมหรือกำกับดูแล” หมายความว่า หน่วยงานของรัฐ หน่วยงานเอกชน หรือ บุคคลซึ่งมีกฎหมายกำหนดให้มีหน้าที่และอำนาจในการควบคุมหรือกำกับดูแลการดำเนินกิจการของ หน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(11) “คณะกรรมการ” หมายความว่า คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

คำนิยามทั้งหมดนี้ทำให้เห็นถึงวิวัฒนาการที่เปลี่ยนไปของการร่างกฎหมายที่ให้ความสำคัญกับระบบไซเบอร์ตามยุคสมัย เพราะระบบไซเบอร์นั้นไม่ได้มีความระบบคอมพิวเตอร์เท่านั้นแต่ยังรวมไปถึงโครงข่ายอินเตอร์เน็ตที่อยู่ในรูปแบบ cloud หรือสายเคเบิลใต้มหาสมุทรที่ประเทศไทยจะต้องคำนึงถึงความปลอดภัยภัยใต้อาณาเขตระหว่างประเทศ นอกจากนี้ระบบไซเบอร์ยังเชื่อมโยงไปยังระบบสาธารณูปโภคที่สำคัญหรือระบบสารสนเทศที่สำคัญ การร่างพระราชบัญญัตินี้ขึ้นมาเพื่อให้เห็นความสำคัญของการรักษาความปลอดภัยของการใช้ชีวิตของประชาชนที่อาจเกิดผลกระทบได้หากมีการจู่โจมทางไซเบอร์

สิ่งที่น่าสนใจอีกประการหนึ่งของพระราชบัญญัติฉบับนี้ คือ การมี “คณะกรรมการ” หรือ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ที่จะประกอบด้วยคณะกรรมการด้านไซเบอร์ต่าง ๆ 3 คณะและจะกล่าวต่อในหัวข้อถัดไปนั้น ถือเป็นการสร้างศูนย์รวมผู้มีความรู้ความสามารถทางไซเบอร์ที่แท้จริงและจะคอยเป็นหน่วยงานเดียวที่มีอำนาจเบ็ดเสร็จในการตรวจตรา ดูแลรักษา ความมั่นคงปลอดภัยทางไซเบอร์ เพราะฉะนั้นไม่ว่าหน่วยงานนั้น

จะอยู่ในประเภทใดก็ตามก็จะถูกควบคุมภายใต้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาตินี้

ด้วยบทสรุปด้านกฎหมายทั้งหมดนี้นำไปสู่พัฒนาการทางด้านนิติวิธีที่นำมาจัดการกับการรับมือภัยคุกคามทางไซเบอร์ได้อย่างดี แต่อย่างไรก็ตามในตัวพระราชบัญญัตินั้นยังมิได้กล่าวถึง การก่อการร้ายทางไซเบอร์ อย่างเป็นกิจลักษณะ ดังนั้นหากกล่าวถึงการก่อการร้ายในรูปแบบนี้ก็จะทำให้เป็นเรื่องยากที่จะดำเนินคดีตามกฎหมายหรือแม้กระทั่งแต่นิยามของคำว่าการก่อการร้ายไซเบอร์นั้นควรที่จะมีบัญญัติไว้เพื่อรับมือกับการพัฒนาขึ้นต่อไปในอนาคต

2) มิติด้านการเมือง

การศึกษาสภาพการก่อการร้ายไซเบอร์ผ่านมิติมุมมองด้านการเมืองนั้นจะขาดการมองผ่านนโยบายสาธารณะไปไม่ได้ การออกนโยบาย นโยบายสาธารณะ (Public Policy) คืออะไรก็ตามที่รัฐบาลตัดสินใจเลือกที่จะกระทำหรือไม่กระทำ (Whatever governments choose to do or not to do) ซึ่งเป็นการพิจารณาในแง่ที่ว่าทำไมรัฐบาลจึงต้องดำเนินการนโยบายนั้นและนโยบายนั้นจะสร้างความแตกต่างอะไร ทั้งนี้ เพราะรัฐบาลมีหน้าที่ต้องทำหลายอย่าง (สุรศักดิ์ ชะมารัมย์, 2563) และในการรับผิดชอบการออกนโยบายที่เกี่ยวของกับไซเบอร์นั้น ได้แก่ 2 หน่วยงานหลัก คือ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมและสภาความมั่นคงแห่งชาติ โดยทั้งสองหน่วยงานมีหน้าที่รับผิดชอบที่แตกต่างกันโดยสภาความมั่นคงแห่งชาตินั้นจะมีบทบาทการดูแลในเรื่องปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศหรือ Critical Information Infrastructure (CII) ส่วนคือ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมนั้นมีหน้าที่ดูแลสาธารณูปโภคสำคัญ หรือ Critical Infrastructure (CI)

สภาความมั่นคงแห่งชาติมีหน้าที่ในการประเมินความพร้อมสภาพปัญหา และแนวโน้มของ ภัยคุกคามทางไซเบอร์ โดยสรุปดังนี้

(1) ประเมินความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์

แบ่งเป็น 4 ด้านหลัก คือ ความพร้อมด้านกลไกทางเทคนิคเพื่อรับมือกับภัยคุกคามทางไซเบอร์ ความพร้อมทางด้านบุคลากร ความพร้อมของระบบและเทคโนโลยี และความพร้อมด้านงานสืบสวน งานการข่าวและการข่าวกรองทางไซเบอร์

(1.1) ความพร้อมด้านกลไกทางเทคนิคเพื่อรับมือภัยคุกคามทางไซเบอร์ ในที่นี่สภาความมั่นคงแห่งชาติได้ร่วมมือกับหน่วยงานที่ชื่อว่า ศูนย์ประสานความมั่นคงปลอดภัยทางไซเบอร์ (The Computer Emergency Response Team) หรือไทยเซิร์ต (ThaiCERT) ของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ซึ่งจะมีความเกี่ยวโยงในฐานะประเภทหน่วยงานที่ควบคุมดูแลตามประเภทที่ผู้วิจัยได้จัดไว้ โดยไทยเซิร์ตนั้นมีหน้าที่ช่วยในการปกป้องและประสานการทำงานทั้งในด้านป้องกันและปราบปรามในทั้งสองบทบาท โดยอยู่ภายใต้

สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ทั้งนี้ยังมีการประสานงานร่วมกับกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทาง เทคโนโลยี ภายใต้สำนักงานตำรวจแห่งชาติ สำนักคดีเทคโนโลยีและสารสนเทศภายใต้กรมสอบสวนคดีพิเศษ กระทรวงยุติธรรม ศูนย์เทคโนโลยีสารสนเทศภายใต้ สำนักงานป้องกันและปราบปรามการฟอกเงินหรือธนาคารแห่งประเทศไทย อีกด้วย แต่เพียงเน้นนโยบายในเชิงการป้องกันมากกว่าการปราบปราม เพราะนโยบายและผู้ปฏิบัติในการปราบปรามนั้นจะอธิบายในประเภทหน่วยงานที่อยู่ในด้านการปราบปรามต่อไป เช่นกองทัพบก กองทัพอากาศ ที่มีการจัดตั้งศูนย์ไซเบอร์

(1.2) ความพร้อมทางด้านบุคลากร จากการสำรวจของสภาความมั่นคงแห่งชาติพบว่า กว่าร้อยละ 50 หน่วยงานทั้งรับและเอกชนจะไม่พบว่ามีการเตรียมการสำหรับการสร้างบุคลากรที่มีความพร้อมทางด้านไซเบอร์ และยังขาดแรงจูงใจกับบุคคลกรที่ทักษทางด้านไซเบอร์สูงเพราะเงินเดือนในหน่วยงานราชการนั้นยังมีผลตอบแทนน้อย ไม่เพียงพอเมื่อเทียบกับบริษัทเอกชนหรือการทำงานกับบริษัทต่างประเทศ

(1.3) ความพร้อมของระบบและเทคโนโลยี จากข้อมูลของสภาความในคงแห่งชาตินั้นประเทศไทยยังต้องพึ่งพิงเทคโนโลยีจากต่างชาติยังไม่สามารถคิดค้นนวัตกรรมใหม่ๆ ขึ้นได้เอง ทั้งนี้เนื่องจากการขาดการสนับสนุนทางการศึกษาอย่างจริงจังหรือการขาดความรู้และความเอาใจใส่ของบุคลากรที่มีต่อด้านเทคโนโลยี ดังนั้นสิ่งที่ประเทศไทยต้องวางกลยุทธ์คือการพัฒนาทักษะของนักเรียนนักศึกษาภายในชาติพร้อมทั้งการแลกเปลี่ยนความรู้การนานาชาติอีกด้วย

(1.4) ความพร้อมด้านงานสืบสวน งานการข่าวและการข่าวกรองทางไซเบอร์ สภาความมั่นคงแห่งชาติยังทำงานบูรณาการร่วมกับสำนักข่าวกรองแห่งชาติเพื่อหาข่าวทางไซเบอร์ ซึ่งเป็นหน่วยงานสำคัญดังที่ได้กล่าวไว้ในข้างต้นว่าภัยทางไซเบอร์นั้นหากมีต้นตอจากแหล่งข่าวที่น่าเชื่อถือได้ก็จะสามารถป้องกันภัยที่จะเกิดขึ้นและลดความเสียหายได้มากกว่าร้อยละ 50

(2) สภาพปัญหา และแนวโน้มของ ภัยคุกคามทางไซเบอร์

สภาพปัญหาที่เห็นได้ชัดในปัจจุบันคือการออกนโยบายทางด้านไซเบอร์ที่ไร้น้ำหนักการชั่งน้ำหนักความสำคัญระหว่างเรื่องปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศหรือ Critical Information Infrastructure (CII) ปกป้องโครงสร้างพื้นฐานสำคัญด้านสาธารณูปโภคสำคัญ หรือ Critical Infrastructure (CI) ในปัจจุบันนี้ประเทศไทยเน้นการออกนโยบายส่วนใหญ่ไปทางการปกป้องโครงสร้างพื้นฐานทางระบบสารสนเทศ (CII) เนื่องจากประชาชนในปัจจุบันใช้เครื่องมือสื่อสารและอินเทอร์เน็ตเป็นส่วนหนึ่งในชีวิตประจำวัน การสื่อสารผ่าน social media จึงมีความสำคัญที่จะต้องมีระบบการป้องกันไม่ให้มีการขโมยข้อมูลส่วนบุคคล หรือบิดเบือนข้อมูลที่เป็นภัยต่อความมั่นคงเหล่านั้น ดังนั้นในการวิเคราะห์ครั้งนี้จะส่งผลไปถึงปัจจัยทางสังคมที่หน่วยงานด้านการกำกับดูแลความมั่นคงปลอดภัยจะต้องคำนึง

“ดิฉันมองว่าในฐานะนักยุทธศาสตร์ นักวางแผน ประเทศไทยให้น้ำหนักกับความเป็นโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศหรือ critical information infrastructure (CII) มากเกินไป ถึงแม้การปกป้องข้อมูลข่าวสารเชิงสารสนเทศจะเป็นปัจจัยสำคัญและเป็นตัวแปรหลักทางด้านความมั่นคงของชาติ แต่เราก็ไม่ควรลืมการทุ่มเทให้กับระบบการรักษาสาธารณูปโภคที่สำคัญ เช่น Critical Infrastructure (CI)”

ผู้ให้ข้อมูลสำคัญ ที่ 17 (จากสภาความมั่นคงแห่งชาติ)

3) มิติด้านสังคม

ปัจจัยทางด้านสังคมนั้นสามารถมองในภาพรวมไปถึงการรักษาความมั่นคงปลอดภัยของประชาชนในชุมชนออนไลน์ ภัยคุกคาที่เกิดขึ้นกับเด็กในงามุมของการกระทำอนาจาร แต่การมองปัญหาเหล่านี้จะเป็นเพียงการวางยุทธศาสตร์ที่เป็นพียงแค่การรับมือภัยคุกคามทางไซเบอร์เท่านั้น ผลกระทบความมิติทางสังคมในเชิงปัจเจกยังคงไม่สามารถเชื่อมโยงไปยังการเกิดขึ้นของการก่อการร้ายไซเบอร์ได้ แต่อย่างไรก็ตามการวางนโยบายและยุทธศาสตร์ของธุรกิจสถาบันการเงินเป็นปัจจัยหนึ่งที่สำคัญต่อการเริ่มต้นแรงจูงใจให้กับผู้ที่มีแนวโน้มในการก่อการร้ายไซเบอร์เพื่อใช้เงินเป็นแรงจูงใจ

ระบบการเงิน ตลาดเงิน และสถาบันการเงินมีขอบเขตธุรกรรมที่เชื่อมโยงกันอย่างกว้างขวางและซับซ้อนเพิ่มมากขึ้นทั้งในประเทศและต่างประเทศทั่วโลก ตามนวัตกรรมทางการเงินและกระแสโลกาภิวัฒน์ ซึ่งก่อให้เกิดความเสี่ยงต่อเสถียรภาพของระบบสถาบันการเงิน (Systemic Risk) และความมั่นคงของสถาบันการเงินภายใต้หน้าที่การกำกับดูแลของธนาคารแห่งประเทศไทย

ปัจจุบันจากการเปิดเสรีทางการค้าและการเงิน ธนาคารพาณิชย์ไทยมีการเปิดสาขาและลงทุนในต่างประเทศเพิ่มมากขึ้น รวมถึงการทำธุรกรรมต่างๆ กับต่างประเทศ ในขณะเดียวกันธนาคารต่างชาติก็ได้มาเปิดสาขาหรือควบรวมและทำธุรกรรมกับธนาคารในประเทศไทยเพิ่มขึ้นด้วย นอกจากนี้ ธนาคารพาณิชย์หลายแห่งได้รับอนุญาตให้สามารถประกอบธุรกิจเป็นนายหน้าประกันภัย และขายผลิตภัณฑ์ด้านหลักทรัพย์ได้เพิ่มขึ้น ในด้านการกำกับดูแลของธปท. นั้น ครอบคลุมทั้งในระดับของธนาคารพาณิชย์และระดับกลุ่มธุรกิจทางการเงินของธนาคารพาณิชย์ ซึ่งรวมถึงบริษัทลูกที่มีหน่วยงานกำกับดูแลเฉพาะ เช่น บริษัทหลักทรัพย์ซึ่งอยู่ภายใต้การกำกับดูแลของสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (กลต.) และบริษัทประกันภันภัยซึ่งอยู่ภายใต้การกำกับดูแลของสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.) รวมอยู่ด้วย ทั้งนี้ ธนาคารแห่งประเทศไทยมีการประสานงานและขอความ

ร่วมมือระหว่างหน่วยงานกำกับดูแลอื่น ทั้งในระดับระหว่างประเทศและระดับภายในประเทศเพื่อความมีประสิทธิภาพในการกำกับดูแล ตรวจสอบ ป้องกันความเสี่ยง และแลกเปลี่ยนข้อมูลที่สำคัญจึงเป็นสิ่งจำเป็นในประเทศประกอบไปด้วย ก.ล.ต./ คปภ. ระหว่างประเทศ จะประกอบไปด้วยธนาคารกลาง / องค์กรกำกับดูแลอื่น ๆ (ธนาคารแห่งประเทศไทย, 2564)

ในด้านความมั่นคงปลอดภัยทางไซเบอร์ทั้ง 3 สถาบันธุรกิจทางการเงินมีการประสานงาน ร่วมมือ และมีการสัมมนาประจำปีในทุกปี เพื่อในการแบ่งปันข้อมูลความเสี่ยงและการเตรียมรับมือความเสี่ยง

> *“สถาบันธุรกิจทางการเงินทั้ง 3 หน่วยงานนี้มีการแลกเปลี่ยนข้อมูลกันอย่างดีในทุกความเสี่ยงทางไวเบอร์และมีการประกับต่างประเทศเพื่อให้รู้ก่อภัยจะมาถึง หากในแง่ที่มีปัญหาสำหรับสาขาทางธนาคารก็จะมีคนจาก ธปท. เองเข้าไปช่วยแก้ระบบทั้งที เรามีการเฝ้าระวังแบบ 24 ชั่วโมง และตั้งแต่มีการแต่งตั้งศูนย์ไซเบอร์ของธนาคารแห่งประเทศไทยมา ยังไม่เคยมีภัยคุกคามใดที่ร้ายแรงหรือยังไม่มีภัยคุกคามใดที่สามารถเรียกได้อย่างเต็มปากว่า คือการก่อการร้ายไซเบอร์ที่เกิดขึ้นกับสถาบันธุรกิจทางการเงิน ส่วนมากก็จะเป็นแค่ช่องโหว่ของระบบคอมพิวเตอร์ในการทำงาน หรือมัลแวร์ ไวรัส ต่างๆ ทั่วไป ซึ่งทาง ธปท. เองก็สามารถจัดการได้”*
>
> ผู้ให้ข้อมูลสำคัญ ที่ 5, 6, 7 (ผู้ให้ข้อมูลในตัวแทนของธนาคารแห่งประเทศไทย)

4) สรุปสภาพสถานการณ์การก่อการร้ายในกรอบของหน่วยงานด้านการกำกับดูแล

จากการสรุปภาพรวมการก่อการ้ายทางไซเบอร์ในทั้ง 3 มิติ อันได้แก่ มิติทางด้านกฎหมาย มิติทางด้านการเมือง และมิติทางด้านสังคมแล้วนั้น สามารถสรุปได้ว่าการบริหารจัดการหรือการรับมือทางการก่อการร้ายไซเบอร์นั้นยังเป็นเรื่องที่ยังไม่เคยเกิดขึ้น แต่ก็ไม่ได้หมายความว่าจะไม่เกิดขึ้นกับประเทศไทยในอนาคต เพราะฉะนั้นการประเมินสถานการทั้งมิติของกฎหมาย การเมือง และสังคม จะต้องมีความเข้มข้นมากกกว่านี้ เช่น การเพิ่มความสนใจไปยังโครงสร้างพื้นฐานสำคัญด้านสาธารณูปโภคสำคัญ (CI) ซึ่งเป็นโครงสร้างที่เปราะบางและเป็นเป้าหมายที่เสี่ยงต่อการก่อการร้ายมากที่สุด แต่อย่างไรก็ตามนั้นการปกป้องโครงสร้างพื้นฐานสำคัญด้าน (CII) ก็ยังคงจำเป็นในด้านการสร้างความมั่นคงต่อสถานบันของชาติ และการขับเคลื่อนยุทธศาสตร์ขอประเทศต่อไปในอนาคต

4.4.2.2 หน่วยงานด้านการปราบปราม

หน่วยงานด้านการปราบปรามที่งานวิจัยเล่มนี้กล่าวถึงคือหน่วยงานประเภทที่มีจุดประสงค์เพื่อรับมือกับการร้ายไซเบอร์โดยตรง มีกลยุทธ์ ยุทธศาสตร์ (Defensive) ตั้งรับป้องกันและตอบโต้ (Offensive) ได้อย่างเชี่ยวชาญ (อริย์ธัช แก้วเกาะสะบ้า, 2558) การวิจัยครั้งนี้จะเป็นการสัมภาษณ์เชิงลึกจากผู้มีความเชี่ยวชาญทางทางด้านนโยบายและทางด้านเทคนิคของกองทัพอากาศ รวมไปถึงผู้อำนวยการศูนย์ไซเบอร์ของกองทัพบก และผกก. กลุ่มงานสนับสนุนคดีเทคโนโลยีจากกองบังคับการปราบปรามารกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีด้วย

โดยจากการวิเคราะห์สภาพปัญหาการก่อการร้ายไซเบอร์ในมุมมองแนวคิดเชิงกลยุทธ์ทั้งป้องกันและปราบปรามจะเห็นได้ถึงความแตกต่างที่ชัดเจนกับหน่วยงานประเภทหน่วยงานด้านการกำกับดูแลความมั่นคงปลอดภัยที่จะมีลักษณะเป็นผู้ออกนโยบายมากกว่าที่จะเป็นผู้ปฏิบัติ ดังนั้นการวิเคราะห์การก่อการร้ายไซเบอร์ในมุมของหน่วยงานด้านการปราบปรามจึงมีแนวโน้มในด้านทางเทคนิคกลยุทธ์การต่อสู้แบบผสมผสานทั้งแบบดั้งเดิมและแบบใหม่ ในการวิเคราะห์นี้หน่วยงานด้านการปราบปรามมีอว่าการก่อการร้ายไซเบอร์เป็นภัยคุกคามที่เกิดขึ้นในระดับที่ไม่ได้รุนแรงมากนักเป็นหลัก เนื่องด้วยการเพิ่มขึ้นของพื้นที่การใช้เทคโนโลยีทำให้พื้นที่ของไซเบอร์มีการขยายขอบเขตประชาชนสามารถเข้าถึงระบบโครงข่ายอินเทอร์เน็ตได้อย่างง่ายดาย การจู่โจมทางไซเบอร์ในฐานะปัญหาระดับชาติจึงเป็นประเด็นที่นานาประเทศให้ความสนใจและเป็นพันธมิตรกัน ส่วนประเทศไทยนั้นก็มีพันธมิตรเป็นประเทศสหรัฐอเมริกา ญี่ปุ่น จีน ออสเตรเลีย เป็นหลัก (Campbell, 2010)

หากกล่าวถึงประเด็นการจู่โจมทางไซเบอร์ที่ไทยให้ความสนใจเป็นหลักคือการมองภาพของมหาอำนาจหลายประเทศ เช่น สหรัฐอเมริกา จีน และรัสเซีย ที่ยังไม่ได้มีอาวุธหรือเทคโนโลยีที่มีประสิทธิภาพเพียงพอที่จะสกัดกั้นหรือรู้ว่าฝ่ายใดเป็นผู้กระทำ หากเพียงว่าเราจะสามารถใช้กลยุทธ์การข่มขู่ยับยั้ง (deterrence) อย่างตำราสงครามฉบับเก่าที่สอนไว้ได้หรือไม่ เนื่องจากอาวุธที่ใช้ในสภาพแวดล้อมแบบดั้งเดิมกับอาวุธในโลกไซเบอร์นั้นมีความแตกต่างกัน หลาย ๆ ประเทศพยายามพัฒนาระบบป้องกันตนเองในพื้นที่ไซเบอร์เพื่อไม่ให้ผลประโยชน์ของตนเองตกอยู่กับประเทศหรือกลุ่มบุคคลอื่น การใช้ กลยุทธ์การข่มขู่ยับยั้ง (deterrence) ยังถูกนำมาใช้เพื่อข่มขู่ยับยั้งกับฝ่ายตรงข้ามแต่ต้องยอมรับว่าในโลกของไซเบอร์นั้นประสิทธิภาพของของ กลยุทธ์นี้ยังไม่มีประสิทธิภาพเท่าที่ควร ในแต่ละประเทศยังคงรักษาสถานะภาพของตนเองเพื่อไม่ให้เกิดการปะทะครั้งใช้ในดลกไซเบอร์รวมทั้งประเทศไทย (Campbell, 2010) เพราะทุกประเทศต่างรู้ดีว่าหากมีสงครามไซเบอร์ที่เต็มรู) แบบเกิดขึ้น ความสูญเสียจะมากกว่าสงครามนิวเคลียร์หลายเท่านัก

ประเทศไทยมองตัวแบบของสหรัฐอเมริกาและจีน ในกรณีที่มีการโจมตีทางไซเบอร์เกิดขึ้นเช่นมีการตัดระบบโครงข่ายอินเทอร์เน็ตของประเทศใดประเทศหนึ่ง กองกำลังไซเบอร์ของอีกประเทศหนึ่งก็จะตอบโต้โดยทันที มีหลายเหตุการณ์ที่เป็นฉนวนสำคัญในการเกิดสงครามไซเบอร์ เช่น การกล่าวหาว่าสหรัฐอเมริกาและอิสราเอลใช้ไวรัสที่ชื่อว่า Stuxnet โจมตีโรงงานนิวเคลียร์ของอิหร่าน แต่อย่างไรก็ตามก็ยังไม่มีหลักฐานที่ชัดเจนว่าสหรัฐอเมริกาและอิสราเอลเป็นผู้กระทำในเหตุการณ์นี้จริง เพราะมีบางหลักฐานกล่าวว่าท่อนำส่งในโรงงานนิวเคลียร์ของอิหร่านเกิดการรั่วเองและเป็นสาเหตุที่ทำให้โรงงานหยุดทำงาน ดังนั้นการที่อิหร่านจะเป็นผู้กล่าวหาสหรัฐและตอบโต้ทางไซเบอร์จนเกิดเป็นสงครามจึงเป็นสิ่งที่ยากเพราะแม้แต่อิหร่านเองก็ไม่สามารถที่จะหาสาเหตุต้นตอได้อย่างแท้จริง ด้วยสาเหตุนี้ทำให้แนวโน้มสภาพการก่อการร้ายมุ่งทำลายแบบรุนแรงจึงน้อยลงแต่ส่วนใหญ่จะมีแนวโน้มที่จะกระทำการแบบจู่โจมเป็นครั้งคราว เพราะการจู่โจมไซเบอร์ในระดับที่ไม่รุนแรงมากนัก เช่น การแฮกข้อมูลส่วนตัว การเรียกค่าไถ่ มีความเป็นไปได้สำหรับผู้กระทำและมีแรงจูงใจเป็นเงินหรือผลประโยชน์ที่ชัดเจน ปัจจุบันผู้คุกคามส่วนใหญ่จึงเลือกใช้ทักษะที่มีกระทำโดยปราศจากวัตถุประสงค์ทางการเมืองเพราะพวกเขาเหล่านั้นจะบรรลุวัตุประสงค์ได้ง่ายกว่า ดังนั้นการใช้กลยุทธ์ข่มขู่ยับยั้ง (deterrence) จึงควรนำมาทบทวนใหม่ (Campbell, 2010) และในการสร้างกลยุทธ์ใหม่โดยเฉพาะของประเทศไทยนั้นจำเป็นจะต้องมุ่งเป้าเฉพาะการศึกษาวัตถุประสงค์ของผู้กระทำเป็นรายบุคคลมากกว่าที่จะเป็นระดับรัฐชาติ และต้องศึกษาถึงวิธีที่พวกเขาเหล่านั้นตั้งใจที่จะทำให้บรรลุเป้าหมาย ควบคู่ไปกับการทบทวนกลยุทธ์ใหม่ๆทั้งหมดไปด้วยกัน

ในการวิเคราะห์สถานะการตั้งรับและการตอบโต้นั้นยังคงมีความเกี่ยวข้องกับหลักการข่มขู่ยับยั้ง (deterrence) ที่เป็นกลยุทธ์แบบดั้งเดิม โดยกลยุทธ์นี้มีแนวคิดที่จะทำลายความมั่นใจในการต่อสู้ของฝ่ายตรงข้ามจากการกระทำในสิ่งท่ายตรงข้ามไม่ต้องการหรือกลัวที่จะเกิดขึ้น หรืออาจจะเป็นการสร้างจินตนาการให้กับฝ่ายตรงข้ามมีความกลัวโดยไม่ต้องลงมือกระทำจริงเพื่อให้ฝ่ายตรงข้ามหยุดที่จะกระทำในสิ่งที่ตนเองต้องการ แนวคิดนี้ใช้ได้ดีในสมัยสงครามเย็น (Cold War) (Campbell, 2010) การข่มขู่นั้นบางครั้งอาจจะกระทำผ่านการลงโทษ โดยฝ่ายตรงข้ามจะคิดทบทวนว่าหากตนกระทำสิ่งที่คิดลงไป ผลที่จะตามมาจะรุนแรงมากกว่าสิ่งที่ตนจะรับไหว ทำให้ฝ่ายศัตรูหรือฝ่ายตรงข้ามไม่กล้าที่จะกระทำสิ่งเหล่านั้น เช่น การใช้บทบาททางการเมืองเหนือกองกำลังทางทหาร การศูนย์สถานะทางการเมืองจะทำให้กองกำลังทางทหารมีความตกต่ำลงอีกด้วย และการข่มขู่ประเภทนี้จะมีผลกับการข่มขู่ระหว่างรัฐด้วยกัน

ในขณะเดียวการการใช้หลักการข่มขู่ยับยั้ง (deterrence) ก็สามารถปรับใช้กับสถานการณ์ของประเทศไทยในลักษณะของการใช้กฎหมายเพื่อลงโทษ ปรับ และข่มขู่ ผู้กระทำความผิดทางไซเบอร์ได้ เช่น การมีกฎหมายปรับและจำคุกผู้ที่ตั้งใจทำให้ระบบ

คอมพิวเตอร์เสียหายหรือการขโมยข้อมูลส่วนบุคคล กฎหมายเหล่านี้ยังใช้ได้ผล แต่ในการสืบเสาะหาคนรับผิดในทางปฏิบัตินั้นยังเป็นเรื่องยากเพราะการทิ้งร่องรอยทางไซเบอร์นั้นแทบไม่สามารถพบได้

สำหรับหลักการข่มขู่ยับยั้ง (deterrence) อีกประเภทหนึ่งคือการที่ฝั่งใดฝั่งหนึ่งลงมือกระทำจริง และเห็นผลของการกระทำที่จะก่อให้เกิดความรุนแรงเสียหายมากกว่าจนทำให้ฝ่ายตรงข้ามยอมหยุดการกระทำที่ตนเองทำอยู่ เหมือนการที่ทั้งสองฝ่ายลงสนามจริงในการต่อสู้ โดยมีโมเดลมาตรฐานที่ว่า หากค่าความเสี่ยงมีความสัมพันธ์กับผลประโยชน์ที่คาดหวังไว้ ถ้า C+ R > B, เมื่อ C เท่ากับ ค่าความเสียหาย R เท่ากับ ค่าความเสี่ยง และ B คือ ผลประโยชน์ที่คาดว่าจะได้รับ ถ้าเท่ากับ ค่าความเสียหายบวกค่าความเสี่ยงและมีมากกว่า ผลประโยชน์ที่คาดว่าจะได้รับ การกระทำของฝ่ายนั้นจะหยุดลง การข่มขู่ประเภทนี้จะเกิดขึ้นได้จริงหรือมีประสิทธิภาพจริงก็ต่อเมื่อฝ่ายหนึ่งเห็นว่าผู้กระทำฝ่ายตรงข้ามมีความสามารถที่จะล้มล้างเกมรบได้จริงและเราจะต้องหยุดก่อนที่ความสูญเสียจะเกิดไปมากขึ้น (Campbell, 2010)

แต่อย่างไรก็ตามผู้ที่จะใช้กลยุทธ์เหล่านี้ก็จำเป็นที่ต้องพิจารณาว่าหลักการข่มขู่ยับยั้ง (deterrence) นี้ไม่ได้การันตีว่าสิ่งที่คิดไว้จะเกิดขึ้นจริง แผนอาจไม่บรรลุวัตถุประสงค์หากมีตัวแปรหรือปัจจัยอื่นมาขัดขวาง และปัญหาอีกประการหนึ่งที่กลยุทธ์แบบดั้งเดิมไม่สามารถประยุกต์ใช้กับการก่อการร้ายไซเบอร์ได้จริงนั้นคือสภาวะของความเป็นไซเบอร์มีความหลากหลายมาก เช่น พลังความน่ากลัวของไซเบอร์สามารถดับไฟฟ้าของเมืองทั้งเมืองได้ หรือเปิดปิดเขื่อนให้น้ำไหลท่วม ทำร้ายประชาชนคนบริสุทธิ์โดยไม่แบ่งแยก ดังนั้นการที่จะทำให้เกิดการล้มล้างจึงเป็นสิ่งที่อยุติธรรม ไม่เหมาะสม ผิดมนุษยธรรม และไม่น่าเชื่อถือ ประการต่อมาการประเมินความเสียหายของอาวุธทางไซเบอร์นั้นมีความแตกต่างจากอาวุธอื่นๆ เพราะอาวุธทางไซเบอร์เปรียบเสมือการล่องลอยในอากาศ ความสำเร็จของอาวุธทางไซเบอร์จะสามารถยืนยันประสิทธิของตนเองได้จริงหรือไม่ หรืออาจจะเกิดขึ้นเพราะฝั่งตรงข้ามมีรบบไซเบอร์ที่มีความผิดพลาดเกิดขึ้นเอง หากเปรียบเทียบกับความแม่นยำของอาวุธแบบดั้งเดิม เช่น เครื่องบินรบที่สามารถล็อกเป้าฝั่งตรงข้ามและทำลายได้อย่างเจาะจงแม่นยำ ต่างกับอาวุธไซเบอร์ที่ยังไม่สามารถควบคุมได้ร้อยเปอร์เซ็นต์ นอกจากนี้อาวุธไซเบอร์ยังหาง่ายหรือบริจาคจากประเทศคู่ตรงข้ามได้ง่าย ไม่ต้องมีหลักแหล่งหรือฐานทัพที่แน่นอน จึงทำให้มีความซับซ้อนและความยากที่จะใช้ทฤษฎีหรือกลยุทธ์เดิม ๆ ในการตอบโต้

นอกจากนี้ผู้เชี่ยวชาญทางด้านไซเบอร์ยังยกตัวอย่างสถาการณ์ที่เกิดขึ้นรอบโลกเพื่อเปรียบเทียบกับประเทศไทย ทำให้ผู้วิจัยได้วิเคราะห์ถึงความสัมพันธ์ระหว่างการใช้กลยุทธ์ในการยับยั้งการก่อการร้ายไซเบอร์ของประเทศมหาอำนาจต่างที่แสดงออกทางกองกำลังไซเบอร์ เช่น การใช้หลักการข่มขู่ยับยั้ง (deterrence) ไม่ประสบความสำเร็จในการใช้ในประเทศรัสเซียและสหรัฐอเมริกา เมื่อปี 2013 พบว่าหลังจากที่รัสเซียและสหรัฐอเมริกาได้ทำข้อตกลงและร่วมมือกันหยุดยั้งภัยคุกคามทางไซเบอร์ที่เกิดขึ้นและร่วมกันแบ่งปันข้อมูลที่ตนได้รับต่อกัน แต่ความร่วมมือนี้ไม่

เป็นผลเมื่อสหรัฐอเมริการู้ว่ารัสเซียพยายามที่จะใช้ไวรัสและมัลแวร์ต่าง ๆ โจมตีสหรัฐเมรอกาและประเทศพันธมิตร ความร่วมมือข้างต้นนั้นไม่เป็นผล รัสเซียยังคงมุ่งมั่นที่จะจู่โจมยูเครนโดยใช้วิธี denial-of-service หรือการทำให้ระบบเสียหายไม่สามารถทำงานต่อได้ และรัสเซียยังโดนกล่าวหาว่าเป็นผู้ทำให้ระบบการเลือกตั้งออนไลน์ในปี 2016 ถูกรบกวนและถูกนำข้อมูลไป สำหรับประเทศจีนมาหอำนาจในโลกตะวันออกก็พยายามที่จะแสดงจุดยืนว่าจะไม่เป็นผู้โจมตีหรือคุกคามชาติใดก่อน ประเทศจีนและสหรัฐอเมริกาได้ทำความร่วมมือเช่นเดียวกันว่าจะไม่มีการโจมตีทางไซเบอร์ซึ่งกันและกัน แต่ในผลสุดท้ายข้อมูลของสหรัฐอเมริกาได้ถูขโมยข้อมูลไปและสหรัฐอเมริกาได้สันนิฐานว่าเป็นการกระทำของประเทศจีนซึ่งสามารถขโมยข้อมูลส่วนบุคคลของเจ้าหน้าที่ของรัฐไปมากกว่า 20 ล้านคน ประเทศจีนใช้วิธีที่ตรงข้ามกับรัสเซีย คือ การใช้วิธีแทรกซึมไปกับระบบและขโมยข้อมูลที่เป็นประโยชน์ของตน ซึ่งต่างจากประเทศรัสเซียที่จะใช้วิธีจู่โจมแบบซึ่งหน้า

เกาหลีเหนือก็เป็นประเทศหนึ่งซึ่งมีความสามารถในด้านการจู่โจมทางไซเบอร์เป็นอย่างดี เกาหลีเหนือมีเป้าการโจมตีโดยเฉพาะสหรัฐอเมริกาและสาธารณรัฐเกาหลีใต้ และทฤษฎีการขมขู่ยั้งนั้นเหมือนว่าจะไม่สามารถใช้ได้กับเกาหลีเหนือ เกาหลีเหนือได้กระทำการจู่โจมบังคลาเทศโดยสามารถขโมยเงินที่มีมูลค่ากว่า 81 ล้านดอลลาร์ ถึงแม้ว่าเกาหลีเหนือจะ๔กลงทาจากสหประชาชาติในการกระทำเหล่านี้ แต่ก็ดูเหมือนว่ามาตรการที่สหประชาชาติทำกับเกาหลีเหนือนั้นไม่ได้ผลเท่ากับการยับยั้งการใช้อาวุธนิวเคลียร์ของเกาหลีเหนือ

จากเหตุการณ์จากทั่วโลกพบว่าภัยคุกคามทางไซเบอร์มีเพิ่มขึ้นและสร้างจุดอ่อนนให้กับมาตรการการป้องกันให้กับหน่วยปราบปรามทั่ว ประเทศไทยเองได้นำโมเดลของชาติต่างๆ มาพัฒนา ไม่ว่าจะเป็นการซื้อเทคโนโลยีใหม่ๆ การพัฒนาบุคคลาการให้มีความรู้ทางด้านไซเบอร์ และจูงใจพวกเขาเหล่านั้นเข้ามาร่วมงานกับภาครัฐ โดยกองทัพบกได้ตั้งศูนย์ไซเบอร์เพื่อจุดประสงค์ที่จะป้องป้องประเทศจากการคุกคามทางไซเบอร์โดยเฉพาะ ศูนย์ไซเบอร์ของกองทัพนั้นถึงแม้จะมีสายงานที่แยกกัน การบังคับบัญชาไม่ได้มาจากผู้บังคับบัญชาคนเดียวกัน แต่ศูนย์ไซเบอร์ของทุกเหล่าทัพจะมีการประชุมและแลกเปลี่ยนข้อมูลกันเป็นประจำ การรายงานผลจะมีในรูปแบบประจำปี และศูนย์ไซเบอร์นั้นจะมีหน่วยประจำที่จะคอยดูแลระบบตลอด 24 ชั่วโมง 7 วัน เพื่อลาดตระเวรตรวจสอบภัยคุกคามที่จะเกิดขึ้นกับกองทัพ หากวิเคราะห์ในบทบาทแล้วศูนย์กองทัพไซเบอร์จะเป้นสายงานที่แยกจากหน่วยงานดูแลควบคุมภัยคุกคามทางไซเบอร์ของพลเรือน แต่ก็ยังมีการประสานงานกันต่อเนื่องและในบางครั้งอาจจะต้องมีการขอความช่วยเหลือกัน

การจัดตั้งศูนย์ไซเบอร์กองทัพบก (Army Cyber Center) ขึ้นเพื่อปฏิบัติงานให้เป็นไปตามนโยบาย ของรัฐบาลโดยร่วมมือกับคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security: NCSC) จากเดิมที่เป็นแค่ศูนย์เทคโนโลยีทางทหาร (ศทท.) แต่

เนื่องจากกระแสสังคมที่เปลี่ยนไปกองทัพจึงเห็นว่าควรเพิ่มบทบาทหน้าที่การดูแลพื้นที่ทางไซเบอร์ให้กับกองทัพบกด้วย บทบาทสำคัญของศูนย์ไซเบอร์กองทัพมีดังนี้

1. ดูแลรักษาความสงบของพื้นที่ไซเบอร์ของประเทศ
2. ปกกันและปราบปราบภัยคุกคามทางไซเบอร์โดยเฉพาะทางทหารทั้งจากในและนอกประเทศ
3. รักษาความสงบของชาติ โดยประสารขอความร่วมมือต่างๆทั้งจากในและนอกประเทศเพื่อแลกเปลี่ยนข่าวสารภัยคุกคามทางไซเบอร์

ปัจจุบันศูนย์ไซเบอร์กองทัพมีหน้าที่หลัก 3 ประการที่จะต้องปฏิบัติผ่านกองปฏิบัติการไซเบอร์ เพื่อเฝ้าระวัง แจ้งเตือน และป้องกัน และแก้ปัญหาจากภัยคุกคามทางไซเบอร์ หรือเผชิญหน้าเหตุฉุกเฉิน กองรักษาความมั่นคงปลอดภัยไซเบอร์ ทำหน้าที่เสริมสร้างความรู้ความเข้าใจ ความตระหนักรู้ให้กับบุคลากร นอกจากนี้ยังต้องกำกับ ติดตาม ดูแลการปฏิบัติของหน่วยตามมาตรการการรักษาความมั่งคงปลอดภัย และกู้คืนความเสียหายให้ได้เร็วที่สุด ส่วนกองสุดท้ายนั้นคือกองสนับสนุนการปฏิบัติการข่าวสารไซเบอร์ เพื่อให้การสนับสนุนการปฏิบัติการข่าวสารของกองทัพบกและหน่วยที่เกี่ยวข้อง โดยทำหน้าที่เฝ้าระวัง แจ้งเตือนข้อมูลข่าวสารบนไซเบอร์ (อริย์ธัช แก้วเกาะสะบ้า, 2563)

ศูนย์ไซเบอร์กองทัพบกและกองทัพอากาศมีหลักการแนวคิด และกลยุทธ์แบบเดียวกัน แต่เพียงแตกต่างกันในเรื่อง domain หรือพื้นที่ที่ตนรับผิดชอบ เช่น ศูนย์ไซเบอร์กองทัพอากาศก็จะมีบทบาทคุมคุมไปถึงน่านฟ้าที่เป็นอาณาเขตของประเทศไทย หากมีสิ่งแปลกปลอมลุกล้ำเข้ามา เทคโนโลยีของกองทัพอากาศจะสามารถจับและสกัดดั้นไว้ก่อนได้ทันที แนวคิดในการตั้งรับของทางทหารนั้นสามารถแบ่งได้ ตามการวิเคราะห์ดังนี้

1) **การสร้างการรับรู้ในประสิทธิภาพของเทคโนโลยีในการตั้งรับ**

รัฐบาลไทยให้ความสำคัญกับกระแสความรุนแรงที่มีที่มาจากไซเบอร์เป็นอย่างมากทำให้มีการจัดซื้อเทคโนโลยี วัสดุ อุปกรณ์ต่าง ๆ ที่ทันสมัย เพื่อสกัดกั้นการจู่โจมทางไซเบอร์ทางในและนอกประเทศ ทั้งนี้ไทยจะมีความสามารถที่จะช่วยสอดส่องความผิดปกติที่เกิดขึ้นภายในอาณาเขตของประเทศเพื่อรายงานกับประเทศพันธมิตรก่อนที่จะเกิดการจู่โจมทางไซเบอร์ในประเทศต่าง ๆ การแสดงให้เห็นว่าประเทศไทยมีระบบที่ทันสมัย แน่นหนา และมั่นคงเป็นกลยุทยุทธ์ที่สามารถขมขวัญให้ศัตรูมิกล้าที่จะก่อการใหญ่ในระดับรัฐชาติ ถึงแม้ว่าบางครั้งคลังอาวุธทางไซเบอร์ของไทยอาจจะยังไม่ได้พัฒนาไปถึงขีดสุด แต่การสร้างการรับรู้จะเป็นตัวกระตุ้นให้ฝ่ายตรงข้ามกลัวที่จะกระทำ และไม่กล้าที่จะใช้ประเทศไทยเป็นฐานในการโจมตีทางไซเบอร์

“เรามีการสกัดจับ เฝ้าระวังตลอด 24 ชั่วโมง 7 วัน ทุกคนเป็นผู้เชี่ยวชาญทางด้านระบบ ครั้งหนึ่งเว็เคยได้รับแจ้งว่ามีกลุ่มผู้ก่อความไม่สงบทางไซเบอร์จากต่างประเทศที่จะใช้ประเทศไทยเป็นฐานในการโจมตีสหรัฐอเมริกา เนื่องด้วยการประสานงานกับชาติพันธมิตรและเทคโนโลยีที่พัฒนาทำให้เราสามารถสกัดจับกลุ่มผู้ก่อความไม่สงบนั้นได้ทัน”

ผู้ให้ข้อมูลสำคัญคนที่ 12 (จากศูนย์ไซเบอร์กองทัพอากาศ)

“ตั้งแต่ที่ผมทำงานมา น้อยมากที่จะมีกลุ่มผู้โจมตีใช้ประเทศไทยเป็นฐานในการโจมตีหรือก่อความไม่สงบทางไซเบอร์ไปยังประเทศอื่น อาจเป็นเพราะเทคโนโลยีที่เรามี และการสร้างความรับรู้ในฐานะประเทศที่ให้ความสนใจในไซเบอร์ ในฐานะรัฐชาติ กลุ่มผู้ก่อความไม่สงบจะต้องเลือกเป้าหมายที่อ่อนแอและระบบที่มีช่องโหว่เพื่อที่จะจับพวกเขาได้ยาก ประเทศไทยก็ไม่ใช่หนึ่งในประเทศเหล่านั้น”

ผู้ให้ข้อมูลสำคัญคนที่ 14 (จากศูนย์ไซเบอร์กองทัพบก)

2) การแสดงให้เห็นถึงกลยุทธ์เชิงรุก (Offensive) ของกองทัพ

กลยุทธ์เชิงรุกที่ทางกองทัพใช้นั้นสอดคล้องกับกลยุทธ์ในข้อแรก คือ การจะแสดงออกถึงแสงยานุภาพของอาวุธเพื่อให้ฝ่ายศัตรูกลัว จะต้องสร้างการรับรู้ว่าอาวุธทางไซเบอร์ที่เรามีนั้นแน่นหนาและพัฒนาไปถึงขั้นไหน หลักการนี้เป็นหลักการเดียวกันกับที่ใช้ในสงครามเย็นเพื่อสร้างความกลัวให้ศัตรู โดยจะไม่เกิดความเสียหาย ส่วนกลยุทธ์เชิงรุกในอีกประการหนึ่งคือการเลือกที่จะลงสนามและเปิดเกมส์ก่อมเพื่อที่จะให้ฝ่ายศัตรูเป็นผู้ตามเกมส์และเราจะเป็นผู้นำเกมส์นี้ หลักการนี้สามารถใช้ได้ร่วมสมัยไม่ว่าจะเป็นการรบแบบดั้งเดิมหรือไซเบอร์ก็ตาม แต่สิ่งที่สำคัญที่สุดคือการรักษาความลับของศักยภาพที่แท้จริงของกองกำลังไซเบอร์ในฐานะการป้องกันของรัฐชาติ แต่อย่างไรก็ตามกลยุทธ์นี้มีจุดอ่อน เพราะการวิเคราะห์ศักยภาพไซเบอร์ผ่านระบบคอมพิวเตอร์นั้นสามารถทำได้และอีกประการหนึ่งการใช้กลยุทธ์นี้อาจจะทำให้ถูกพิจารณาว่าเป็นการกระทำที่รุนแรงและผิดกฎหมาย

3) การตั้งกองปฏิบัติการเชิงรุกทางไซเบอร์

ในบางครั้งการใช้กลยุทธ์เชิงรุกก็เป็นอีกด้านหนึ่งที่จะใช้เพื่อเป็นการข่มขู่ฝั่งศัตรูที่จะทรัพยากรที่พวกเขามีเพื่อที่จะปกป้องการรุกรานที่จะเกิดขึ้น ดังนั้นการเก็บทรัพยากรส่วนหนึ่งเพื่อรับมือกับการรุกรานที่จะเกิดขึ้นนั้นจึงเป็นสิ่งสำคัญสำหรับฝ่ายศัตรู เช่น การแสดงให้เห็นถึงความสามารถและศักยภาพที่จะเพิ่มการต่อรองและยับยั้งความรุนแรงที่จะเกิดขึ้น กองปฏิบัติการเชิงรุกทางไซเบอร์นั้นควรจะมีวัตถุประสงค์ที่เฉพาะเจาะจง เพื่อที่จะไม่สร้างความ

รุนแรงและไม่สร้างความสูญเสียที่มากเกินไป ตัวอย่างที่แสดงให้เห็นกันมาแล้ว คือ ปฏิบัติการ Stuxnet ที่ไม่สามารถควบคุมความเสียหายจากปฏิบัติการเชิงรุกนี้ได้ ดังนั้น ผลจากการใช้การข่มขู่และยับยั้งควรต้องประกอบไปด้วยการแสดงให้เห็นถึงความน่าเชื่อถือของอาวุธไซเบอร์ที่จะมีผลกระทบที่อยู่ในขอบเขตที่รัฐชาติสามารถรับได้

4) การติดตั้งการตอบโต้การจู่โจมทางไซเบอร์อัตโนมัติ

การใช้หลักการนี้เพื่อการปกป้องและข่มขู่ยับยั้งฝ่ายตรงข้ามได้อย่างดี ยกตัวอย่างเช่นการติดตั้งระบบการตอบโต้อัตโนมัติ เมื่อฝ่ายตรงข้ามโจมตีทางไซเบอร์ระบบอัตโนมัตินี้จะตอบโต้โดยการใส่มัลแวร์เข้าไปในข้อมูลที่ฝ่ายตรงข้ามได้ไป และมัลแวร์ตัวนี้จะสามารถทำลายระบบไซเบอร์ของฝ่ายตรงข้าม หากฝ่ายตรงข้ามรู้ก่อนว่ามีการติดตั้งการตอบโต้การจู่โจมทางไซเบอร์อัตโนมัติอยู่นั้นก็จะรีบล้มเลิกการโจมตี แต่อีกแง่หนึ่งนั้นหากฝ่ายตรงข้ามมีความรู้ไม่มีเพียงพอก็จะสูญเสียการควบคุมระบบของตนเองและโดยกลายเป็นเหยื่อที่ถูกอีกฝ่ายกระทำแทน

5) การตั้งเป้าหมายป้องกันการสูญเสียที่รุนแรง

การตอบโต้ภัยคุกคามที่มาการจู่โจมทางไซเบอร์นั้นสามารถใช้อาวุธแบบดั้งเดิมและอาวุธนิวเคลียร์ได้แต่อย่างไรก็ตามการใช้อาวุธแบบดั้งเดิมนั้นไม่ควรเป็นตัวเลือกแรกในการใช้แต่แนวทางการโจมตีแบล้มล้างสามารถใช้พิจารณาในกรณีของการจู่โจมทางไซเบอร์แบบรุนแรงได้ เพราะการใช้อาวุธแบบเดิมจะทำให้สร้างความรุนแรงมากขึ้นเพราะเป็นการก่อเชื้อไฟทางกายภาพและความเสียหายที่รุนแรงทางกายภาพและมั่นใจว่าศัตรูจะไม่กล้าที่จะยอมรับความศูนย์เสียที่จะเกิดขึ้นเช่นกัน แต่วิธียังไม่เคยนำมาใช้ที่ใดบนโลกแม้แต่สหรัฐอเมริกาที่ยังไม่สามารถมั่นใจถึงความน่าเชื่อถือที่จะข่มขู่ยับยั้งฝ่ายตรงข้ามได้ ดังนั้นการที่จะประยุกต์ใช้วิธีนี้กับประเทศไทยเพราะอาวุธดั้งเดิมที่ประเทศไทยมีนั้นมีศักยภาพไม่มากพอที่จะข่มขู่ยับยั้งชาติอื่น

6) การสร้างสถานการณ์เพื่อตอบโต้การจรากรรมทางไซเบอร์

การสร้างสถานการณ์ถือเป็นกลยุทธ์หนึ่งที่สามารถสร้างความประณีประนอมกับฝ่ายศัตรูได้ เช่น การขโมยข้อมูลหรือทรัพย์สินทางปัญญา หรือความลับทางการค้า เช่น ประเทศจีนได้สร้างสถานการณ์หลอกลองเพื่อเป็นกับดักโดยเอกสารและข้อมูลทั้งหมดเป็นเอกสารปลอม และเมื่อข้อมูลเหล่านั้นถูกขโมยไปก็ไม่สามารถที่จะนำไปใช้กับระบบคอมพิวเตอร์แบบใดได้ทั้ง software หรือ hardware วิธีการนี้เป็นการประณีประนอมศัตรูและใช้และค่อยๆเป็นการตรวจจับผู้จู่โจมอย่างช้าๆ ระบบ malicious ในการจู่โจมกลับไป ดังนั้นฝ่ายตรงข้ามจะกลายเป็นเหยื่อทันที และเป็นการกระทำที่ไม่คุ้มที่จะเสี่ยง

6) การใช้กฎหมายอาญาในการสืบเสาะ

อย่างที่ทราบกันว่าหลายประเทศกำหนดให้การจู่โจมทางไซเบอร์เป็นการกระทำที่ผิดกฎหมายรวมทั้งประเทศไทยที่มีการกำหนดพระราชบัญญัติการกระทำ

ความผิดทางคอมพิวเตอร์จนมีการพัฒนามาเรื่อย ๆ จนกลายเป็นพระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ที่เป็นที่น่าสนใจในปัจจุบันในประเทศไทยการกระทำความผิดทางไซเบอร์ถือเป็นการกระทำความผิดกฎหมายที่โทษทั้งจำคุกและปรับ แต่การกระทำส่วนใหญ่จะมาในรูปของอาชญากรรมไซเบอร์มากว่าการต่อสู้อย่างชัดเจน แต่อย่างไรก็ตามอาชญกรรมทางไซเบอร์จะมีลักษณะที่ต่างออกไปจากอาชญากรรมธรรมดาที่กฎหมายจะตามทัน อาชญกรรมในอดีตสามารประเมินและสืบเสาะได้ตามหลักฐานที่ปรากฏอยู่และเป็นจุดแข็งที่จะทำให้การสืบเสาะหาต้นติผู้กระทำนั้นประสบความสำเร็จและสามารถขยายฐานการสืบเสาะไปยังเครือข่ายใหญ่ได้อีกด้วย แต่สำหรับอาชญากรรมไซเบอร์นั้นไม่สามารถที่จะหาหลักฐานใดๆที่จะทิ้งไว้ได้ ไม่ว่าจะเป็นลายนิ้วมือหรือชิ้นส่วนโค้ด malicious ที่เหลืออยู่ได้ว่ามาจากประเทสอะไรที่เป็นต้นกำเนิด ผู้กระทำอาจจะใช้ประเทศที่สามเป็นฐานการโจมตีเพื่อหลบหลีกการถูกจับกุม และอาจจะเลือกประเทศที่ยังไม่มีกฎหมายไซเบอร์ที่จริงจังเพื่อความปลอดภัยในการหลบหนีทางคดีของผู้กระทำ

แต่อย่างไรก็ตามลักษณะการจู่โจมและลักษณะของไวรัสที่ใช้ในการจู่ยังมีร่องรอยให้สหรัฐอเมริกาสามารถสืบเสาะได้ว่าการจู่โจมครั้งนี้มาจากประเทศอะไร ตัวอย่างเช่น เกาหลีเหนือจะมีมัลแวร์ลักษณะที่แตกต่างออกไปจากประเทศอื่นและสามารถทำให้สหรัฐจำได้และง่ายที่จะกล่าวหา นอกจากนี้สหรัฐใช้กฎหมายจัดการกับรัสเซียและจีนในปี 2014 และ 2017 ในข้อหาการจารกรรมทางเศรษฐกิจ เพราะเจอหลักฐานที่ผู้กระทำการจรากรรมใช้เป็น มัลแวร์ตัวเดียวกันกับฐานข้อมูลส่วนตัวเดิมเมื่อ 2 ปีที่แล้ว แฮกเกอร์จากจีนถูกจับและแฮกเกอร์ชาวรัสเซียถูกตักเตือนในการกระทำครั้งนี้ และถือเป็นการเตือนผู้ที่จะกระทำในอนาคต แต่อย่างไรก็ตามถ้าผู้กระทำทำในฐานะรัฐชาติการที่จะฟ้องร้องหรือใช้กฎหมายจัดการนั้นจะเป็นเรื่องที่ประเทศที่ถูกกล่าวหาจะปกป้องประชาชนของประเทศตัวเอง จึงเป็นเหตุให้วิธีการนี้มีจุดอ่อนมากมายเมื่อนำมาใช้กับกฎหมายนานาชาติ

7) การกำหนดโทษ

การกำหนดโทษนั้นสามารถเป็นกลยุทธ์ในการยับยั้งที่มีปนะสิทธิภาพ ยกตัวอย่าง เช่น การลงโทษเกาหลีเหนือจากการประกาศสงครามนิวเคลียร์ และทำให้เกาหลีเหนือทดลองอาวุธนิวเคลียร์ไม่สำเร็จ และมาตรการนี้ก็ยังสามารถใช้ได้ในการยับยั้งการสนับสนุนจากประเทศพันธมิตรของเกาหลีหนีเพื่อให้ให้ช่วยเหลือในการพัฒนาอาวุธทางไซเบอร์ได้ ประเทศที่ถูกกล่าวหานั้น ได้แก่ รัสเซีย อิหร่าน ที่ถูกกำหนดโทษในการช่วยเหลือนี้ และมากไปกว่านั้นมาตรการนี้มีจุดประสงค์ที่เฉพาะเจาะจงในการยับยั้งการกระทำในประเภทที่แตกต่างกัน และแน่นอนว่าอย่างไรก็ตามบทลงโทษนี้ก็ไม่สามารถยับยั้งการซื้อขายคอมพิวเตอร์หรือ software ซึ่งถือว่าเป็นอาวุธชนิดหนึ่งในการจู่โจมทางไซเบอร์ได้

8) การใช้ความตกลงระหว่างประเทศ

บรรทัดฐานระหว่างประเทศนั้นยอมรับในเรื่องของพื้นที่ทางไซเบอร์และมีความประสงค์ที่จะป้องกันไม่เกิดการจู่โจมทางไซเบอร์โดยการข่มขู่ยับยั้ง เช่นเดียวกับอาวุธชนิดอื่นในอดีต อาวุธทางไซเบอร์เป็นอาวุธที่ต้องห้ามเพราะอาวุธไซเบอร์สามารถทำให้ผู้จู่โจมสำเร็จในจุดประสงค์ที่ว่าไว้และได้สิ่งที่คาดหวัง รายงานจาก The United Nations Group of Governmental Experts ปี 2013 และ 2015 กล่าวสรุปถึงกฎหมายระหว่างประเทศ รวมไปถึง UN Charter ต่างนำไปใช้ควบคุมพื้นที่ทางไซเบอร์และมีข้อแนะนำไม่ให้มีการเกิดการตอบโต้ระหว่างรัฐชาติในประเด็นของการจู่โจมสาธารณูปโภคสำคัญต่าง ๆ NATO ได้เสนอ Tallinn Manuals ซึ่งเป็นบทนำของกฎหมายระหว่างประเทศสำหรับการป้องกันการเกิดสงครามไซเบอร์และปฏิบัติการสร้างความสงบ Tallinn Manuals มีจุดประสงค์ที่จะสร้างความเข้าใจร่วมกันเกี่ยวกับการกระทำไซเบอร์ใดสามารถทำได้(UnITed naTIons CoUnTer-TerrorIsm ImplemenTaTIon Task ForCe, 2019) แต่กฎหมายนี้ไม่ได้มีภาระผูกพัน เป็นเพียงการสร้างมาตรฐานที่สำคัญ และที่สำคัญความพยายามของประชาคมระหว่างประเทศนั้นเป็นการสร้างความเห็นร่วมกันบนพื้นฐานการกระทำทางไซเบอร์และจะถือเป็นการใช้แนวคิดแห่งการยับยั้งที่มีประสิทธิภาพประเภทนึ่งในการร่วมมือนี้

> *“ในประเทศไทยมีอาชญากรรมไซเบอร์ที่เกิดขึ้นกับประชาชนเพิ่มขึ้นในทุก ๆ วัน แต่มีรายงานน้อยมากที่จะเกิดกับหน่วยงานรัฐในระดับที่เกิดความสูญเสียที่รุนแรง มีบางครั้งที่เกิดช่อโหว่ของระบบคอมพิวเตอร์และมีการขโมยข้อมูลเกิดขึ้น หรือไม่ก็มีการบิดเบือนข้อมูลในเว็บไซต์ แต่ทาง ปอท. ก็สามารถรับมือได้”*
>
> ผู้ให้ข้อมูลสำคัญคนที่ 8 (ผู้ให้ข้อมูล จากกลุ่มงานสนับสนุนคดีเทคโนโลยีที่ ปอท.)

9) สรุปสภาพสถานการณ์การก่อการร้ายในกรอบของหน่วยงานด้านการปราบปราม

จากการวิเคราะห์นั้นแสดงให้เห็นว่าหน่วยงานด้านการปราบปราบมีแนวคิดด้านกลยุทธ์และการโจมตีโดยใช้หลักการยับยั้งขมขู่ (Deterrence) ฝ่ายตรงข้ามหรือพยายามแสดงอำนาจและประสิทธิภาพของเทคโนโลยีที่ตนมีเพื่อให้ยับยั้งการเกิดอาชญากรรมไซเบอร์ ถึงแม้สถานการณ์ในประเทศไทยตอนนี้ยังความรุนแรงไม่มากนักส่วนใหญ่เป็นการจู่โจมในระดับความรุนแรงน้อยบางครั้งผู้กระทำอาจไม่มีวัตถุประสงค์สำคัญใดเพียงแค่เป็นการสร้างความสนุกให้กับตนเท่านั้น และในส่วนเหตุการณ์ที่เกิดขึ้นระหว่างรัฐต่อรัฐนั้นในประเทศไทยสามารถนับได้เพียงไม่เกิน 3 ถึง 4 ครั้ง อย่างมากที่สุดก็เป็น การบิดเบือนเว็บไซต์ของหน่วยงานภาครัฐ จากคดีเกาะเต่า ซึ่งสร้าง

ความเกลียดชังให้กับกลุ่มแฮกเกอร์ของเมียนมาร์ มีวัตถุประสงค์ทางการเมืองเลยทำให้เกิดความวุ่นวายทางไซเบอร์ บิดเบือนข้อมูลหน้าเว็บไซต์ของภาครัฐ แต่อย่างไรก็ตามเหตุการณ์นี้ก็ไม่สามารถนับได้ว่าเป็นเหตุการณ์ระหว่างรัฐต่อรัฐเพราะรัฐบาลเมียนมาร์อาจไม่ได้มีส่วนรู้ร่วมคิดกับแฮกเกอร์กลุ่มนี้ด้วย

ในมุมมองของหน่วยงานด้านปราบปรามการสั่งซื้ออาวุธเทคโนโลยีใหม่ๆ ด้านไซเบอร์ถือเป็นสิ่งสำคัญที่จะยังยั้งคู่ต่อสู้และเช่นเดียวกันในด้านกองกำลังหรือผู้ที่มีความรู้ด้านไซเบอร์ ทางกองทัพได้มีการประกาศรับสมัครอยู่ตลอดเวลาเพื่อสร้างทีมที่มีประสิทธิภาพที่สุด การลาดตระเวรเชิงไซเบอร์ก็เช่นกันในฐานะกองทัพได้นำกลยุทธ์แบบเดิมซึ่งถือว่ายังสามารถนำมาประยุกต์ได้กับยุคไซเบอร์ กลยุทธ์เชิงรุกที่จะมีการลาดตระเวรตลอดทั้งวันทั้งคืนไม่มีแม้แต่วันหยุดเพื่อสกัดกั้นไม่ให้เกิดภัยคุกคามที่มาทางระบบคอมพิวเตอร์

นอกจากการใช้กลยุทธ์ต่าง ๆ ทางด้านทางทหารแล้วยังต้องใช้กลยุทธ์ทางการเมืองไม่ว่าจะเป็นการเข้าร่วมเป็นประเทศพันธมิตรกับนานาชาติ การแลกเปลี่ยนความรู้ เทคโนโลยี และข้อมูลต่างๆ การศึกษาการใช้กฎหมายระหว่างประเทศเพื่อไม่ให้เกิดช่องโหว่กับประเทศไทย และร่วมไปถึงการบังคับใช้กฎหมายภายในประเทศให้มีประสิทธิภาพอีกด้วย สภาพปัญหาอีกประการหนึ่งที่เกิดขึ้นกับหน่วยงานด้านการปราบปราม คือ การทุ่มเทกองกำลังไซเบอร์ไม่ตรงเป้าหมายโดยเนื่องจากการโจมตีไซเบอร์ส่วนใหญ่จะอยู่ในระดับความรุนแรงเล็กน้อยถึงปานกลางทำให้การแบ่งภารกิจในการทำงานนั้นให้ความสำคัญไปยังการโจมตีเชิงสาธารณูปโภคพื้นฐานทางสารสนเทศ CII ซึ่งเป็นงานของพลเรือน สิ่งนี้ทำให้เป้าประสงค์ของการจัดตั้งศูนย์มีความไขว้เขวไปบ้างเนื่องจากไม่ได้ระบุไว้อย่างชัดเจนในวัตถุประสงค์ที่ก่อตั้ง

4.4.2.3 หน่วยงานที่มีความเสี่ยงต่อการโจมตี

ผู้วิจัยแบ่งหน่วยงานที่มีความเสี่ยงต่อการโจมตีโดยคำนึงถึง ความเปราะบางการข้อมูลที่สำคัญและมีความเสี่ยงต่อการถูกโจรกรรม หรือเป็นหน่วยงานที่เป็นสาธารณูปโภคที่สำคัญของประเทศ (Critical National Infrastructure) ผู้วิจัยได้เลือกการสัมภาษณ์ผู้เชี่ยวชาญทั้งทางด้านนโยบายและด้านเทคโนโลยีโดยการสัมภาษณ์แบบเชิงลึกและเลือกหน่วยงานที่มีความเสี่ยงดังต่อไปนี้ กระทรวงสาธารณสุข กระทรวงยุติธรรม การไฟฟ้าฝ่ายผลิต ธนาคารแห่งประเทศไทย (สัมภาษณ์เชิงสาขาของธนาคาร) และ กสทช. จากการสัมภาษณ์ด้วยภาพรวมนั้นพบว่านักวางแผนนโยบายและผู้เชี่ยวชาญไซเบอร์ทางเทคนิคนั้นมีไม่เพียงพอเพราะในภารกิจหลักของหน่วยงานเหล่านี้ไม่ใช่ทางด้านไซเบอร์โดยเฉพาะแต่การมีศูนย์ไซเบอร์อยู่ข้างในองค์กรหรือเป็นส่วนหนึ่งนั้นจะเป็นการปกป้องความเสี่ยงที่จะเกิดขึ้นในเบื้องต้น

“ผมมองว่าองค์กรของเราเป้าประสงค์หลังคือการรักษาคนป่วย ละยิ่งโรงพยาบาลในเครือข่ายในต่างจังหวัดนั้นมีบุคลากรน้อย ผู้เชี่ยวชาญทางด้านไซเบอร์ก็ไม่มี หรือถ้ามีก็เป็นคนของโรงพยาบาลเอง ปกติภารกิจที่หนักอยู่แล้วก็ไม่สามารถที่จะดูแลเฝ้าระวังได้ทั้งหมด”

ผู้ให้ข้อมูลสำคัญคนที่ 3 (เจ้าหน้าที่ทางด้านนโยบาย สป.สธ)

การมีบุคลากรน้อยนั้นเป็นเพียงแค่ปัญหาหนึ่งเท่านั้น ถึงแม้ว่าสภาพการโจมตีทางไซเบอร์ในองค์กรที่มีความเสี่ยงข้างต้นนั้นจะมีเพิ่มมากขึ้นเรื่อย ๆ แต่ยังไม่พบเหตุการณ์ที่มีความรุนแรงที่ระดับที่ยังรับมือไม่ได้การโจมตีสถาบันการเงินตามสาขามีเกิดขึ้นอยู่บ่อยครั้ง แต่ส่วนใหญ่จะเกิดมาจากช่องโหว่ทางระบบคอมพิวเตอร์และมัลแวร์ซึ่งทางธนาคารแห่งประเทศไทยสามารถรับมือได้ ส่วนในด้านสาธารณสุขนั้นเคยเกิดการโจมตีระบบเพื่อเรียกค่าไถ่ครั้งใหญ่โดย Ransomware เป็นจำนวนเงินกว่าหกพันล้านบาท แต่กระทรวงสาธารณสุขได้ประกาศให้ทราบว่าได้มีการสำรองข้อมูลผู้ป่วยทั้งหมดในฐานข้อมูลกลาง รัฐบาลจึงไม่จำเป็นต้องจ่ายเงินเพื่อนำเอาข้อมูลกลับมา มีเพียงแต่ความสับสนวุ่นวายเล็กน้อยที่เกิดขึ้นในโรงพยาบาลที่ไม่สามารถทำให้ระบบทะเบียนคนไข้ทำงานได้ สำหรับกระทรวงยุติธรรมนั้น ในสำนักงานปลัดกระทรวงยุติธรรมยังไม่เกิดการโจมตีทางไซเบอร์ใด ๆ แต่จะมีเกิดขึ้นบ้างกับกรมราชทัณฑ์ที่เป็นกรมในสังกัด จากการสอบถามสัมภาษณ์ผู้เชี่ยวชาญทางไซเบอร์ที่ดูและระบบข้อมูลข้อราชทัณฑ์ด้วยนั้น ขณะนี้ก็มีการเตรียมสำรองข้อมูลที่เปราะบางและมีความเสี่ยงไว้ทั้งหมดในระบบ Big Data และจะใช้บล็อกเชนในการช่วยจัดลำดับข้อมูลของผู้ต้องขัง เนื่องจากก่อนหน้านี้มีการแฮกระบบของเว็บไซต์กรมราชทัณฑ์ ทำให้มีการเปลี่ยนแปลงซึ่งตัวเลข แต่อย่างไรก็ตามฝ่ายเทคโนโลยีของราชทัณฑ์ก็สามารถกู้คืนได้ทัน แต่เพียงไม่สามารถจับผู้กระทำความผิดได้ และสองหน่วยงานสุดท้าย การไฟฟ้าฝ่ายผลิตและ กสทช. นั้น จะมีความแตกต่างกับหน่วยงานข้างต้นเพราะจะมีศูนย์การรับมือไซเบอร์และฟื้นฟูสาธารณูปโภคที่สำคัญแบบพิเศษ โดยบุคลากรที่มีความเชี่ยวชาญ ตัวอย่างเช่น การไฟฟ้าฝ่ายผลิตจะมีวิธีการรับมือการก่อการร้ายไซ้บอร์อย่างชัดเจนแลพประสารงานกับหน่วยงานที่กำหับดูแลอย่าง สกมช. อยู่เสมอเพื่อรองรับความเสียหายหากมีการเกิดการโจมตี ไฟฟ้าดับจะสร้างความเสียหายให้กับประชาชนและประเทศเป็นอย่างสูง กสทช. จะมีหน่วยพิเศษที่ดูแลเฉพาะการดจมตีทางไซเบอร์กับสาธารณูปโภคเชิงสารสนเทศ (CI) เป็นการควบคุมข้อมูลข่าวสารไม่ให้เกิดการบิดเบือนและทำให้รัฐบาลเสียหายหรือสูญเสียความมั่นคง

1) สรุปสภาพปัญหาในด้านหน่วยงานที่มีความเสี่ยงต่อการโจมตี

สภาพปัญหาที่เกิดขึ้นจากภัยคุกคามทางไซเบอร์ที่เห็นได้ชัดเจนจากหน่วยงานที่มีความเสี่ยงต่อการโจมตีที่กล่าวไว้ข้างต้นสามารถสรุปได้ดังนี้

(1) ภารกิจทางไซเบอร์ไม่ใช่หน้าที่หลักขององค์กร

อย่างที่กล่าวไว้ในข้างต้นว่าหน่วยงานที่มีความเสี่ยงนั้นจะมีภารกิจหลักแยกตามวัตถุประสงค์ของหน่วยงานต่างกันไป เช่น กระทรวงสาธารณสุขมีภารกิจหลักในการดูแลรักษาคนไข้ การทำระบบหรือลงทะเบียนผู้ป่วยจึงเป็นงานที่มีความสำคัญรองลงมา กระทรวงยุติธรรมทำ หรือกรมราชทัณฑ์ก็เช่นกัน ภารกิจหลักของกรมคือการคืนคนดีสู่สังคม ดังนั้นการลงทะเบียนผู้ต้องขังหรือการจัดระเบียบรายชื่อผู้ต้องขังจึงเป็นงานที่ไม่ใช้วัตถุประสงค์หลักของหน่วยงาน ส่วนธนาคารบางสาขานั้นหากเกิดปัญหาก็รายงานไปยังผู้กำกับดูแลทันทีเพราะทางธนาคารแห่งประเทศไทยจะมีทีมไซเบอร์ที่เข้ามาช่วยได้ทัน

(2) บุคลากรมีไม่เพียงพอ

ต่อเนื่องจากสภาพปัญหาข้างต้นทำให้บุคลากรที่มีความรู้ทางไวเบอร์ที่จะสามารถพอแก้ไขปัญหาได้ทันท่วงทีนั้นมีไม่เพียงพอเพราะส่วนใหญ่การให้ความสำคัญของบุคลากรอยู่ที่ภารกิจหลักของหน่วยงานนั้นๆ ถึงแม้ว่าหลายหน่วยงานที่มีความเปราะบางและความเสี่ยงทางด้านข้อมูลจะมีศูนย์เทคโนโลยีสารสนเทศอยู่แต่บุคคลกรอาจจะต้องต้องมีภารกิจอื่นที่ไม่ได้เกี่ยวข้องกับการรับมือการจู่โจมไซเบอร์โดยตรง และหากบุคลากรมีหลากหลายหน้าที่จนไม่สามารถรับผิดชอบหน้าที่ของตนได้เต็มที่ก็จะทำให้ฟังก์ชันของหน่วยงานนั้นล้มเหลว

(3) การขาดเทคโนโลยีที่มีประสิทธิภาพ

เมื่อแต่ละหน่วยงานมีภารกิจหลักซึ่งไม่เกี่ยวข้องกับด้านเทคโนโลยี การทุ่มเทงบประมาณเป็นจำนวนมากเพื่อพัฒนาด้านเทคโนโลยีจึงเป็นเรื่องยาก เมื่อเทคโนโลยีไม่มีประสิทธิภาพเท่าที่ควรจึงจำเป็นจะต้องขอความช่วยเหลือจากหน่วยงานอื่น ๆ เมื่อมีภัยคุกคามที่เกิดขึ้น ในสภาพปัจจุบันบางหน่วยงานสาธารณูปโภคที่สำคัญได้แก่การไฟฟ้าฝ่ายผลิต กสทช หรือกระทรวงสาธารณสุข พยายามที่จะสนับสนุนงบประมาณด้านไซเบอร์หรือสนับสนุนบุคลากรให้มีความรู้ โดยส่งไปอบรมทางด้านเทคโนโลยีต่าง มีการตั้งศูนย์ไซเบอร์เพื่อแก้ไขปัญหาเบื้องต้นสำหรับหน่วยงาน ส่วนปัญหาที่ไม่สามารถรับมือได้ก็จะต้องติดต่อหน่วยงานด้านกำกับควบคุมดูแล เช่น สกมช. หรือ ThaiCERT เพื่อเข้ามาช่วยแก้ปัญหาต่อไป

(4) ความตระหนักรู้ของบุคลากรในองค์กร

เมื่อขาดบุคลากรที่มีความเชี่ยวชาญทางไซเบอร์และเทคโนโลยีที่ยังไม่ทันสมัย การเปลี่ยนพื้นฐานความคิดของคนในองค์กรกับการใช้เทคโนโลยีใหม่ ความยากไม่ได้มีแต่การพยายามชักจูงให้พวกเขาเหล่านั้นเข้าถึงและใช้เทคโนโลยีเหล่านั้นให้เป็นถึงแม้พวกเขาจะมีการต่อต้านเทคโนโลยี แต่สิ่งที่ยากไปกว่านั้นคือการสอนให้คนกลุ่มนั้นใช้เทคโนโลยีอย่างปลอดภัย เพราะปัญหาส่วนใหญ่ที่มาจากการขโมยข้อมูล หรือการโจมตีหน่วยงานสาธารณูปโภคสำคัญของรัฐ คือ ความผิดพลาดของบุคคลดรในองค์กรที่ไม่มีความตระหนักรู้ในเรื่องของเทคโนโลยี เช่น การใช้

พาสเวิร์ดที่เข้าถึงง่าย การใช้คอมพิวเตอร์ที่บ้านมาใส่ข้อมูลที่ทำงาน ปัญหาเหล่านี้ทำให้เกิดช่องโหว่ในระบบคอมพิวเตอร์และมีส่วนให้แฮกเกอร์สามารถจู่โจมได้

> *“ผมเห็นว่าคนหลาย ๆ คนยังไม่ยอมรับเทคโนโลยี พวกเขายังไม่เชื่อว่ามันสามารถใช้ประโยชน์ได้จริงหรือยืนยันตัวตนได้จริง ทางเดียวที่จะปรับความคิดเขาได้คือการบังคับให้เขาอยู่กับสิ่งแวดล้อมนั้นให้ได้ เราต้องไม่อ่อนข้อ ไม่มีข้อแม้ บอกว่าต้องทำคือต้องทำ มันงั้นงานก็ไม่เคลื่อน ระบบก็ยังวนเวียนอยู่แบบเดิม แต่ที่สำคัญ พวกเขาต้องรู้ด้วยว่าเมื่อใช้เทคโนโลยีแล้วจะใช้ยังไงถึงจะปลอดภัยไม่สร้างความเสียหายต่อองค์กร”*
>
> ผู้ให้ข้อมูลสำคัญคนที่ 2 (จากสำนักงานปลัดกระทรวงยุติธรรม)

(5) งบประมาณมีไม่เพียงพอ

สำหรับหน่วยงานที่มีความเสี่ยงนั้น จากการสัมภาษณ์ทำให้ทราบว่าการสนับสนุนด้านเทคโนโลยียังไม่ใช่เรื่องหลักที่ผู้บริหารจะใช้งบในการพัฒนา อย่างไรก็ตามตั้งแต่ปี 2019 เป็นต้นมา ผู้บริหารส่วนใหญ่ได้ทำตามนโยบายของภาครัฐที่มีการส่งเสริมให้ประเทศไทยมีความเป็นดิจิทัลหรือที่เรียกว่าระบบราชการแบบ 4.0 เมื่อมีการส่งเสริมด้านเทคโนโลยีเพื่อมาลดต้นทุนทั้งทรัพยากรบุคคล และทรัพยากรต่างๆในการทำงาน แนวความคิดในด้านการบริการองค์กรก็เปลี่ยนไป การใช้เทคโนโลยีที่ถูกต้องต้องมีความตระหนักรู้และพร้อมที่จะยอมรับ บางหน่วยงาอาจจะใช้งบประมาณส่วนใหญ่เพื่อพัฒนาภารกิจหลักของตนเอง แต่ก็ยังมีบางส่วนที่นำมาพัฒนาระบบเทคโนโลยีให้มีประสิทธิภาพมากขึ้น

> *“ผมเห็นว่างานเราควรพัฒนาระบบงานด้านเทคโนโลยีสารสนเทศให้ดี เราจะต้องมีงบประมาณที่เพียงพอที่จะสร้างฐานข้อมูลขนาดใหญ่และมีประสิทธิภาพเพื่อให้สามารถเก็บรายชื่อผู้ใช้บริการได้อย่างครบถ้วยเพราะหากเกิดปัญหาการเรียกค่าไถ่จากการขโมยข้อมูลก็จะเป็นผลดีกับองค์กรเองที่จะใช้หน่วยงานไอทีภายใต้ขององค์กรแก้ไขปัญหาเหล่านั้นได้ทัน”*
>
> ผู้ให้ข้อมูลสำคัญคนที่ 3 (จากสำนักงานปลัดกระทรวงติธรรม)

2) สรุปการรับมือการก่อการร้ายไซเบอร์ด้านหน่วยงานที่มีความเสี่ยงต่อการโจมตีในประเทศไทย

ณ ปัจจุบันประเทศไทยถือว่ากำลังเข้าสู่ความเป็นสังคมดิจิทัลอย่างค่อยเป็นค่อยไป หากประเมินจากความเป็นจริงภายใต้หลักฐานข้อมูลจากการสัมภาษณ์นั้นพบว่า

ภาคส่วนนโยบายไม่ว่าจะเป็นระดับรัฐ ระดับองค์กรทั้งเอกชนและราชการ หน่วยงานทางด้านทหาร หรือแม้แต่ประชาชนที่เป็นปัจเจกเองนั้นเริ่มมีความตระหนักและตื่นตัว เมื่อบทบาททางเทคโนโลยีมีมากขึ้นจึงทำให้คนในสังคมปฏิเสธไม่ได้ เทคโนโลยีมีทั้งประโยชน์และโทษหากนำมาใช้ในทางที่ผิด ประเทศไทยก็เป็นหนึ่งในประเทศที่ต้องเผชิญหน้ากับภัยคุกคามไซเบอร์อย่างหลีกเลี่ยงไม่ได้ แต่จากการวิเคราะห์องค์ประกอบต่าง ๆ ของภัยคุกคามทางไซเบอร์ที่ประเทศไทยเจอนั้นยังคงเป็นภัยคุกคามที่ไม่รุนแรงนัก ถึงแม้จะมีเพิ่มมากขึ้นทุกวันแต่หน่วยงานภาครัฐก็สามารถรับมือได้

ประเทศไทยกำลังเผชิญเป็นเพียงภัยคุกคามทางไซเบอร์เท่านั้น ไม่ถือเป็นการก่อการร้ายไซเบอร์เมื่อพิจารณาจากคำนิยามของก่อการร้ายนั้นจะต้องคำนึงภายใต้ 4 องค์ประกอบ นั่นคือ ระดับความรุนแรง จุดประสงค์ทางการเมืองหรืออุดมการณ์ของผู้กระทำเกิดความรุนแรงต่อผู้บริสุทธิ์ และเป็นการสร้างการขับเคลื่อนเพื่อให้เกิดการปกครองรูปแบบใหม่มีการใช้จิตวิทยาในการชักนำ รวมกลุ่มผู้ที่มีอุดมการณ์เดียวกัน ซึ่งจะแตกต่างกับการจูโจมหรืออาชญากรรมไซเบอร์ธรรมดาที่เป็นเพียงผู้ที่มีทักษะทางด้านคอมพิวเตอร์ไม่สูงมากนักและเป็นการกระทำเป็นครั้งคราวไม่ได้มีจุดประสงค์ที่จะทำลายสถาบันใดสถาบันหนึ่งอย่างชัดเจน

นำมาซึ่งปัญหาของการให้คำนิยามของการก่อการร้ายที่หน่วยงานแต่ละประเภทที่ผู้วิจัยได้แบ่งไว้ยังมีความคลุมเครือและมีนิยามไม่เหมือนกันขึ้นอยู่กับกรอบแนวคิดของหน่วยงานในแต่ละประเภท หน่วยงานด้านการกำกับดูแลความมั่นคงปลอดภัยนั้นมองว่าการก่อการร้ายเป็นคุกคามรูปแบบหนึ่งทางไซเบอร์ โดยจะมีวัตถุประสงค์ทางการเมือง โจมตีสาธารณูปโภคสำคัญทางสารสนเทศ (CII) และสาธารณูปโภคสำคัญของประเทศ(CI) โดยสภาความความมั่นคงแห่งชาติมีบทบาทในการเขียนนโยบายป้องกันภัยคุกคามทางไซเบอร์รูปแบบของสาธารณูปโภคสำคัญทางสารสนเทศ และกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมดูแลภัยคุกคามทางไซเบอร์ในรูปแบบสาธารณูปโภคสำคัญของประเทศ และมอบหมายให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ดำเนินการทำต่อไปในการสรุปการแบ่งภารกิจตามคำนิยามนั้นหน่วยงานประเภทนี้มีความเห็นตรงการว่าสำหรับในประเทศไทยยังไม่มีการก่อการร้ายไซเบอร์ในชนิดที่เต็มรูปแบบแต่จะมาเป็นภัยคุกคามทางไซเบอร์ชั่วครั้งชั่วคราวโดยผู้กระทำที่ไม่ใช่รัฐชาติมากกว่า

สำหรับนิยามของหน่วยงานด้านการปราบปรามซึ่งงานวิจัยเล่มนี้จะเน้นไปยังกองทัพและด้านการทหารมีความจริงจังกับการรับมือการก่อการร้ายทางไซเบอร์ โดยมีแผนและกลยุทธ์ในการรับมือที่ผสมผสานจากกลยุทธ์แบบดั้งเดิมมาประยุกต์ใช้กับพื้นที่สู้รบทางไซเบอร์ และเช่นเดียวกันนั้นหน่วยงานด้านการปราบปรามมองการก่อการร้ายไซเบอร์แบ่งเป็น 4 องค์ประกอบเหมือยอย่างข้างต้น แต่จะให้ความสำคัญกับการก่อการร้ายแบบรัฐชาติต่อรัฐชาติมากกว่า โดยจากคำนิยามแล้วประเทศไทยยังไม่เคยมีการก่อการร้ายไซเบอร์ตามนิยามที่อ้างไว้ กลยุทธ์ฝ่ายทหารจึงมีไว้เพื่อ

เตรียมพร้อมหากมีการเกิดการก่อการร้ายในอนาคตในระดับรุนแรงหน่วยปราบปราบก็มีได้แบ่งภารกิจงานขาดกับหน่วยงานของพลเรือน หน่วยงานทั้งสองประเภทยังคงมีการแลกเปลี่ยนข้อมูลและเทคโนโลยีซึ่งกันและกัน แต่จะเป็นข้อมูลคนละรูปแบบ

คำนิยามการก่อการร้ายสำหรับหน่วยงานสุดท้าย คือ หน่วยงานที่มีความเสี่ยงต่อการโจมตี จากการสัมภาษณ์พบว่าหน่วยงานประเภทนี้มีความเชื่อในด้านการก่อการร้ายไซเบอร์หลังจากที่ได้ศึกษาบทเรียนจากหลาย ๆ ประเทศไม่ว่าจะเป็น เอสโตเนีย สหรัฐอเมริกา รัสเซีย จีน หรือเกาหลีเหนือก็ตาม หน่วยงานมีความเชื่อว่าการก่อการร้ายที่เต็มรูปแบบจะเกิดขึ้นกับประเทศไทยจริงในอนาคตอันใกล้ เมื่อทุกอย่างเข้าสู่ระบบดิจิทัล ประกอบด้วยการที่รัฐบาลไทยก็มีการผลักดันให้ระบบราชการรวมไปถึงเอกจนและทุกหน่วยงานอยู่ในระบบโครงข่ายฐานข้อมูลขนาดใหญ่เพื่อความสะดวกและมีประสิทธิภาพในการบริหารประเทศ ปัจจุบันระบบธุรกรรมการเงินเกือบทั้งหมดตั้งอยู่บนพื้นที่ของไซเบอร์ การโอนเงินไปมาระหว่างปัจเจกต่อปัจเจก หรือปัจเจกผ่านสถาบันทางการเงินก็ตามจะถูกดูแลควบคุมผ่านรัฐเพื่อเป็นการเก็บข้อมูลรายได้ของประชาชนและไว้ประเมินสถานการณ์ทางเศรษฐกิจในอนาคต ในช่วงโรคระบาดโควิด 19 ระบบหมอพร้อมเป็นที่รู้จักในหมู่ของประชาชนในทุกชนชั้น ไม่ว่าจะเป็นระดับชนชั้นสูงหรือชนชั้นรากหญ้า คนทั้งที่อยู่ในเมืองหรืออยู่ในชนบทก็ตาม ทุกคนถูกบังคับด้วยสภาวแวดล้อมรอบข้างให้ใช้ชีวิตผลักดันโดยเทคโนโลยี ปัญหาที่เกิดขึ้นจากการพัฒนาระบบนั้นก็มีมากมายเพราะด้วยความเร่งรัด แต่ประเทสไทยยังถือเป็นประเทศที่โชคดีเพราะยังไม่มีการก่อการร้ายไซเบอร์ที่เต็มรูปแบบเกิดขึ้นกับระบบสาธารณูปโภคสำคัญต่างๆ ของประเทศ มีเพียงแต่การเรียกค่าไถ่ หรือขโมยข้อมูลที่มีความเสียหายเล็กน้อยเท่านั้น ดังนั้นการใช้สิ่งแวดล้อมเป็นแรงผลักดันในการพัฒนาระบบและเร่งเตรียมการรับมือการก่อการรไซเบอร์ที่กำลังจะเกิดขึ้นในอนาคตทำให้หลายหน่วยงานมีความตื่นตัวเช่น กฟฝ. ที่ให้ความสนใจและเตรียมพร้อมรับมือกับการก่อการร้ายเป็นอย่างดี

ถึงแม้หน่วยงานทั้ง 3 ประเภทจะมีแนวคิดที่ตรงกันว่า ณ ปัจจุบันประเทศไทยยังไม่มีประสบการณ์การรับมือการก่อการร้ายไซเบอร์อย่างเต็มรูปแบบ แต่ภัยคุกคามต่างๆที่เกิดขึ้นไม่ว่าจะเป็น มัลแวร์ทำลายระบบ การขโมยข้อมูลสำคัญ ไปจนถึงการเรียกค่าไถ่ถือเป็นสัญญาณสำคัญที่ประเทศไทยกำลังจะต้องเผชิญหน้ากับการก่อการ้ายไซเบอร์ในเร็ววันนี้

4.5 ศักยภาพในการรับมือคุกคามทางไซเบอร์

การรับมือทางเทคโนโลยีของประเทศไทยเริ่มต้นอย่างจริงจังในปี พ.ศ. 2539 หรือการรับมือเข้าสู่ยุคโลกเทคโนโลยี ปี 2000 กฎหมายฉบับแรกที่ถูกตราขึ้นคือ กฎหมายเทคโนโลยีสารสนเทศ (Information Law) ณ ขณะนั้นคณะรัฐมนตรีเห็นความสำคัญของโลกเทคโนโลยีจึงมีนโยบายแห่งชาติ

เพื่อพัฒนาเศรษฐกิจ สังคม อุตสาหกรรม และการค้า ให้มีความทันสมัย จึงได้มีการปฏิวัติเทคโนโลยีสารสนเทศขึ้นมาเป็นครั้งแรก โดยมีกฎหมายทั้งหมด 6 ฉบับ มีเนื้อหาคุ้มครองธุรกรรมทางอิเล็กทรอนิกส์ คุ้มครองข้อมูลส่วนบุคคล และกฎหมายเกี่ยวกับการโอนเงินทางอิเล็กทรอนิกส์ ซึ่งเป็นกฎหมายภายใต้รัฐธรรมนูญที่มุ่งเน้นการพัฒนาโครงสร้างพื้นฐานสารสนเทศให้ทั่วถึงและเท่าเทียมกัน

ในปี พ.ศ. 2541 รัฐบาลจัดตั้งระบบเทคโนโลยีอีกครั้งผ่าน “คณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ (National Information Technology Committee) หรือที่เรียกโดยย่อว่า" คณะกรรมการไอทีแห่งชาติ” คณะกรรมการชุดนี้ทำหน้าที่เป็นศูนย์ประสานความร่วมมือเกี่ยวกับสาธารณูปโภคพื้นฐานที่สำคัญของประเทศเพื่อทำให้ประชาชนมีการเข้าถึงอย่างเท่าเทียมกัน นอกจากนี้ภารกิจทางด้านกฎหมายทางเทคโนโลยีทั้งหมดก็ถูกโอนย้ายมายังคณะกรรมการนี้ โดยที่มีกระทรวง กระทรวงวิทยาศาสตร์ เทคโนโลยีและสิ่งแวดล้อมเป็นเลขานุการและขับเคลื่อนกฎหมายทางอิเล็กทรอนิกส์เบื้องต้นสำเร็จ (สุรภี, 2562)

รัฐบาลไทยไม่ได้หยุดยั้งการขับเคลื่อนการพัฒนาทางด้านการป้องกันความผิดพลาดที่เกิดจากระบบคอมพิวเตอร์ จากกฎหมายที่ร่างขึ้นในปี พ.ศ. 2541 ได้ออกเป็นพระราชบัญญัติที่ประชาชนส่วนใหญ่ได้บังคับใช้จริง 2 ฉบับ นั่นคือ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จากการวิเคราะห์พบว่ากฎหมายทั้ง 2 ฉบับเน้นการป้องกันเทคโนโลยีเชิงสารสนเทศ การคุ้มครองข้อมูลส่วนบุคคล และการทำธุรกรรมทางการเงิน ถึงแม้จะมีระบุถึงการโจมตีความมั่นคงของประเทศทางในทางเศรษฐกิจ สังคม และการเมือง แต่ยังไม่ได้ระบุถึงการโจมตีในด้านสาธารณูปโภคสำคัญอื่นๆในเชิงของการก่อการร้าย ถึงแม้ว่าการก่อการร้าย ณ ขณะนั้นยังคงเป็นประเทศระดับโลกเพราะเป็นผลมาจากเหตุการณ์หลัง 9/11 (ThaiCERT, 2018)

ต่อมาในปี พ.ศ. 2560 ประเทศไทยได้ออกปรับปรุง พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 มีการแก้ไขเพิ่มเติมจากฉบับปี พ.ศ. 2550 ไม่มากนัก โดยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 มีเนื้อหาใจความการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ การดักเข้าระบบคอมพิวเตอร์ การเข้าถึงข้อมูลของระบบคอมพิวเตอร์โดยไม่ชอบ มีการเปลี่ยนแปลงเพิ่มเติม เช่น การทำให้ข้อมูลผู้อื่นเสียหายโดยมิชอบ หรือทำให้ผู้อื่นไม่สามารถเข้าถึงข้อมูลของตนได้จะมีบทลงโทษต้องระวางโทษจำคุกไม่เกิน 5 ปี ปรับไม่เกิน 1 แสนบาท หรือทั้งจำทั้งปรับ นอกจากนี้ยังรวมไปถึงการกระทำที่ก่อกวนผ่านการส่งอีเมล์ไปให้ผู้อื่น การใช้ spam การบิดเบือนข้อมูลที่ส่งผลต่อความมั่นคงของชาติทางช่องทางออนไลน์ ไม่ว่าจะเป็น Facebook Instagram Line โพสต์ข้อมูลปลอม ทุจจริตหลอกลวง โพสต์ข้อมูลความผิดเกี่ยวกับความมั่นคงก่อการร้าย เผยแพร่ ส่งต่อข้อมูล ที่รู้แล้วว่าผิด ก็มีบทลงโทษเช่นกัน ต้องได้รับโทษจำคุกไม่เกิน 5 ปี ปรับไม่เกิน 1 แสนบาทหรือทั้งจำทั้งปรับ (ThaiCERT, 2018)

จากการสรุปโดยหลักการทั้งหมดของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 ก็พบว่ามีความครอบคลุมพอที่จะรับมือผู้ที่จะกระทำความผอดทางคอมพิวเตอร์เชิงสารสนเทศแต่แค่นั้นยังไม่เพียงพอต่อการป้องกันประเทศจากการคุกคามทางไซเบอร์ในเชิงโครงสร้างสำคัญหลักของสาธารรูปโภคต่าง ๆ เช่น การไฟฟ้า การคมนาคม การประปา ระบบสาธารณสุข เป็นต้น ด้วยสาเหตุนี้จึงเป็นที่มาให้เกิด พรบ.ความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เพื่อความคมชัดในการวิเคราะห์การรับมือการก่อการร้ายไซเบอร์ในประเทสไทย ผู้วิจัยจะนำ พรบ.ความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เป็นตัวตั้งในการวิเคราะห์ผ่านการเชื่อมโยงกลวิธีของหน่วยงานทั้ง 3 ประเภทข้างต้นที่เคยกล่าวไว้ได้แก่ หน่วยงานด้านรักษาความมั่นคงปลอดภัย หน่วยงานที่มีการปราบปรามทางไซเบอร์ และหน่วยงานที่มีความเสี่ยงที่จะถูกโจมตีทางไซเบอร์ โดยจะเริ่มต้นจากการอธิบาย พรบ.ความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และอธิบบายโครงสร้างพร้อมนโยบายยุทธศาสตร์ ของ คณะกรรมการที่ภายใต้การแต่งตั้งของ พรบ.ความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ว่ามีวิธีการรับมือกับการก่อการร้ายไซเบอร์ในประเทศไทยได้อย่างไร

พระราชบัญญัตินี้มีเพื่อเพื่อป้องกันหรือรับมือภัยคุกคามไซเบอร์ได้อย่างทันท่วงทีกฎหมายมีใจความหลักคือการตั้งหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและการแบ่งประเภทภัยคุกคามทางไซเบอร์เป็นหลายระดับเพื่อปกป้องระบบคอมพิวเตอร์และโครงข่ายอินเทอร์เน็ตของโครงสร้างสำคัญพื้นฐานทางสารสนเทศ หรือบริการที่สำคัญของประเทศที่มีความมั่นคงปลอดภัยโดยกำหนดให้โครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานภาครัฐมีมาตรฐานในการรักษาความมั่นคงปลอดภัยไซเบอร์ มีการเฝ้าระวังภัยคุกคามและมีแผนรับมือเพื่อกู้คืนระบบให้กลับมาทำงานได้ตามปกติและมีการร่วมมือและประสานงานกันและกับสำนักงานรักษาความมั่นคงปลอดภัยไซเบอร์เมื่อมีภัยร้ายแรงที่ทำให้การให้บริการที่สำคัญไม่สามารถทำงานได้จนเป็นผลกระทบต่อประชาชนจำนวนมาก

โครงสร้างของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ประกอบไปด้วย 2 ฝ่าย ดังนี้

1. หน่วยงานที่เป็นฝ่ายควบคุมดูแล (Regulator) มีหน้าที่ประมวลแนวทางปฏิบัติหรือตรวจสอบการปฏิบัติ ตรวจสอบขั้นต่ำลสั่งแก้ไข จะสนับสนุนด้วย หน่วยงานเฝ้าระวัง ติดตามตรวจสอบ เผชิญเหตุ เช่น ThaiCERT

2. หน่วยงานที่เป็นฝ่ายปฏิบัติ (Operator) มีหน้าที่กำหนดแผนรับมือตามมาตรฐานCOBIT หรือ ISO27001 ประเมินความเสี่ย หรือตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละหนึ่งครั้งหน่วยงานตรวจประเมินความเสี่ยงระบบ (Audit) ประมวลแนวทางปฏิบัติ (ThaiCERT, 2018)

4.5.1 การรับมือการก่อการร้ายไซเบอร์ของหน่วยงานที่มีความเสี่ยงต่อการโจมตีมีมาตรการในการดูแลความมั่นคงปลอดภัยไซเบอร์

1. การระบุ หรือ IDENTIFY

หน่วยงานต้องทำการระบุว่ากระบวนการดำเนินงานและทรัพย์สินสารสนเทศใดบ้างที่มีความเสี่ยงต่อการถูกโจมตีทางไซเบอร์และต้องได้รับการรักษาความมั่นคงปลอดภัยเพื่อบริหารจัดการความเสี่ยงด้านภัยคุกคามทางไซเบอร์ที่มีต่อระบบทรัพย์สิน ข้อมูล ของหน่วยงานได้อย่างเหมาะสม นอกจากนี้ยังต้องดูไปถึงสภาพแวดล้อมของธุรกิจ หลักธรรมาภิบาลของหน่วยงาน การจัดการความเสี่ยงที่คิดว่าจะประเชิญ และการประเมินความเสี่ยงเหล่านั้น

2. การป้องกัน หรือ PROTECT

หน่วยงานต้องมีมาตรการป้องกันที่เหมาะสมเพื่อจำกัดผลกระทบของเหตุการณ์ภัยคุกคามไซเบอร์ ซึ่งครอบคลุมถึงเรื่องการเข้าถึง การฝึกอบรมและการสร้าง ความตระหนักให้แก่เจ้าหน้าที่และผู้ที่เกี่ยวข้อง ความปลอดภัยของ ข้อมูล และมาตรการด้านความมั่นคงปลอดภัยต่าง ๆ ทั้งกระบวนการและวิธีปฏิบัติตลอดจนเทคโนโลยี หน่วยงานจะต้องหมั่นปรับปรับให้ระบบดูแลรักษาความมั่นคงปลอดภัยทางไซเบอร์ของตนใหม่อยู่ตลอดเวลาและสารมารถป้องกันหน่วยงานจากการจู่โจมได้

3. ตรวจจับ หรือ DETECT

หน่วยงานต้องมีกระบวนการติดตามเฝ้าระวังและตรวจจับเหตุการณ์ภัยคุกคามทางไซเบอร์อย่างต่อเนื่องและแจ้งเตือนถึงสิ่งที่ผิดปกติต่างๆ รวมถึงการติดตามเหตุการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นจากทั้งภายในและภายนอก วิเคราะห์จุดอ่อนหรือช่องโหว่ของภัยคุกคามที่เกิดขึ้นเพื่อเป็นข้อมูลประกอบในการพิจารณาทบทวนแนวทางการป้องกัน ความเสี่ยงและผลกระทบที่จะเกิดขึ้นกับหน่วยงานในอนาคต

4. การรับมือ หรือ RESPONSE

หน่วยงานจะต้องมีมาตรการป้องกันการลุกลามของภัยคุกคามการมี พร้อมทั้งการวิเคราะห์สาเหตุภัยคุกคามหรือตรวจพิสูจน์พยานหลักฐานดิจิทัลกำหนดมาตรการและกระบวนการรับมือภัยคุกคามไซเบอร์ที่ทันท่วงที รวมทั้งที่จะไม่ลืมที่จะมีการทดสอบ ปรับปรุงกลยุทธ์และแผนรับมือภัยคุกคามไซเบอร์อย่างสม่ำเสมอ และร่วมมือกับหน่วยงานที่เกี่ยวข้องทั้งภายในและภายนอกเกี่ยวกับแผนรับมือภัยคุกคามไซเบอร์

5. การฟื้นฟูหลังจากเกิดภัยคุกคามทางไซเบอร์ หรือ RECOVER

หน่วยงานจะต้องมีแผนกู้คืนระบบทั้งตอนเกิดเหตุและหลังเกิดเหตุนับเป็นช่วงระยะเวลาระยะสั้น ระยะกลาง และระยะยาม พร้อมทั้งปรับปรุงแผนการกู้คืนและกลยุทธ์อย่าง

สม่ำเสมอและมีการสื่อสารให้ผู้บริหารผู้ที่เกี่ยวข้องในองค์กรให้ทราบถึงวิธีการกู้คืนข้อมูลหลังจากที่ถูกจู่โจมทางไซเบอร์ (Moph, 2564)

สิ่งที่สำคัญของพระราชบัญญัติฉบับนี้ต่อมาคือการตั้ง สำนักงานคณะกรรมการการรักษา ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หรือ National Cyber Security Agency โดยมีหน้าที่ครอบคลุมในเรื่องการจัดทำนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์และแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา 9

ประสานงานการดำเนินการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ดำเนินการและประสานงานกับหน่วยงานของรัฐและเอกชนในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ ติดตาม วิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ ดำเนินการและให้ความร่วมมือหรือช่วยเหลือในการป้องกันรับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยเฉพาะภัยคุกคามทางไซเบอร์ที่กระทบหรือเกิดแก่โครงสร้างพื้นฐานสำคัญทางสารสนเทศ เสริมสร้างความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงการสร้างความตระหนักด้านสถานการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ร่วมกันเพื่อให้มีการดำเนินการเชิงปฏิบัติการที่มีลักษณะบูรณาการและเป็นปัจจุบัน

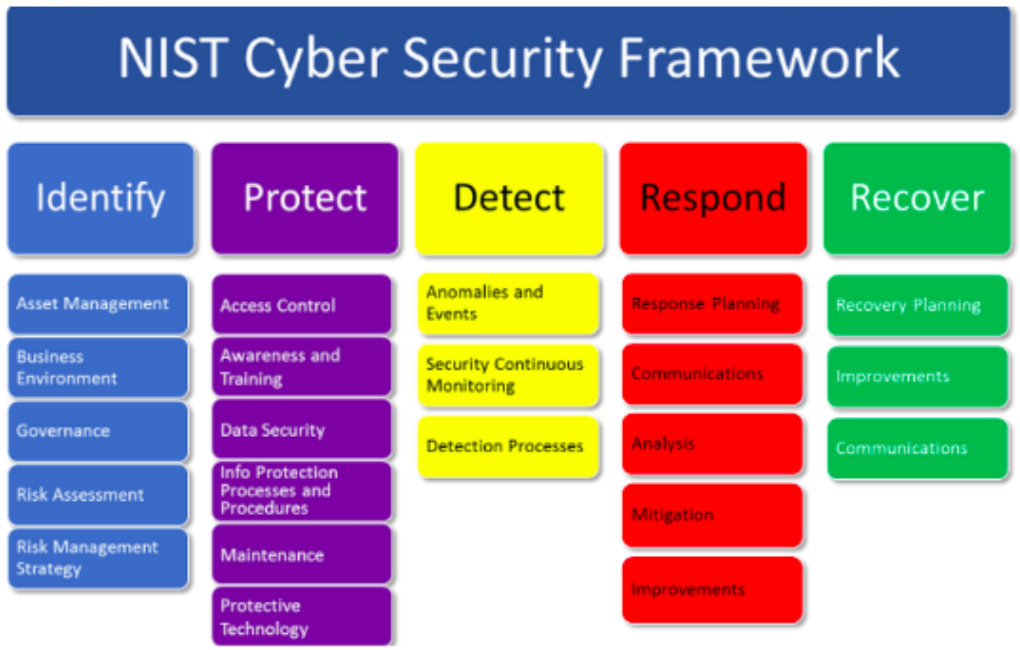
นอกจากนี้ยังเป็นศูนย์กลางในการรวบรวมและวิเคราะห์ข้อมูลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ รวมทั้งเผยแพร่ข้อมูลที่เกี่ยวข้องกับความเสี่ยงและเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่หน่วยงานของรัฐและหน่วยงานเอกชน เป็นศูนย์กลางในการประสานความร่วมมือระหว่างหน่วยงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานของรัฐและหน่วยงานเอกชน ทั้งในประเทศและต่างประเทศ ศึกษาและวิจัยข้อมูลที่จำเป็นสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อจัดทำข้อเสนอแนะเกี่ยวกับมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งดำเนินการอบรมและฝึกซ้อมการรับมือกับภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานที่เกี่ยวข้องเป็นประจำ รายงานความคืบหน้าและสถานการณ์เกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้ รวมทั้งปัญหาและอุปสรรค เสนอต่อคณะกรรมการเพื่อพิจารณาดำเนินการ ทั้งนี้ ตามระยะเวลาที่คณะกรรมการกำหนด เป็นต้น

จากการกำหนดหน้าที่พร้อมมาตราการที่มีเพื่อรักาความปลอดภัยทางไซเบอร์ข้างต้นทุกองค์กรจะต้องนำมาปรับใช้กับหน่วยงานของตนเอง โดยจะต้องมีแผนการรับมือกับภัยคุกคามทางไซเบอร์ทั้งหมดที่ประกอบไปด้วยกรอบแนวคิดทั้ง 5 ข้อที่เสนอในพระราชบัญญัติอันได้แก่ ระบุ ป้องกัน รับมือ ตรวจจับ และฟื้นฟู อยู่ในแผนการดำเนินงานขององค์กรนั้น ๆ โดยเฉพาะองค์กรที่มีความเสี่ยงต่อการโจมตีสูง

“ในฐานะที่เป็นตัวแทนของ กฟฝ. มีความเห็นว่า การไฟฟ้าเป็นสาธารณูปโภคที่สำคัญ เพราะฉะนั้นการที่เราต้องมือแผนการรับมือตามที่ สกมช. กำหนดถือเป็นสิ่งจำเป็นและหน่วยงานของเราก็ได้เตรียมพร้อมสำหรับการรับมือเหล่านั้นแล้ว”

ผู้ให้ข้อมูลคนสำคัญคนที่ 20 และ 21 (จาก การไฟฟ้าฝ่ายผลิตแห่งประเทศไทย)

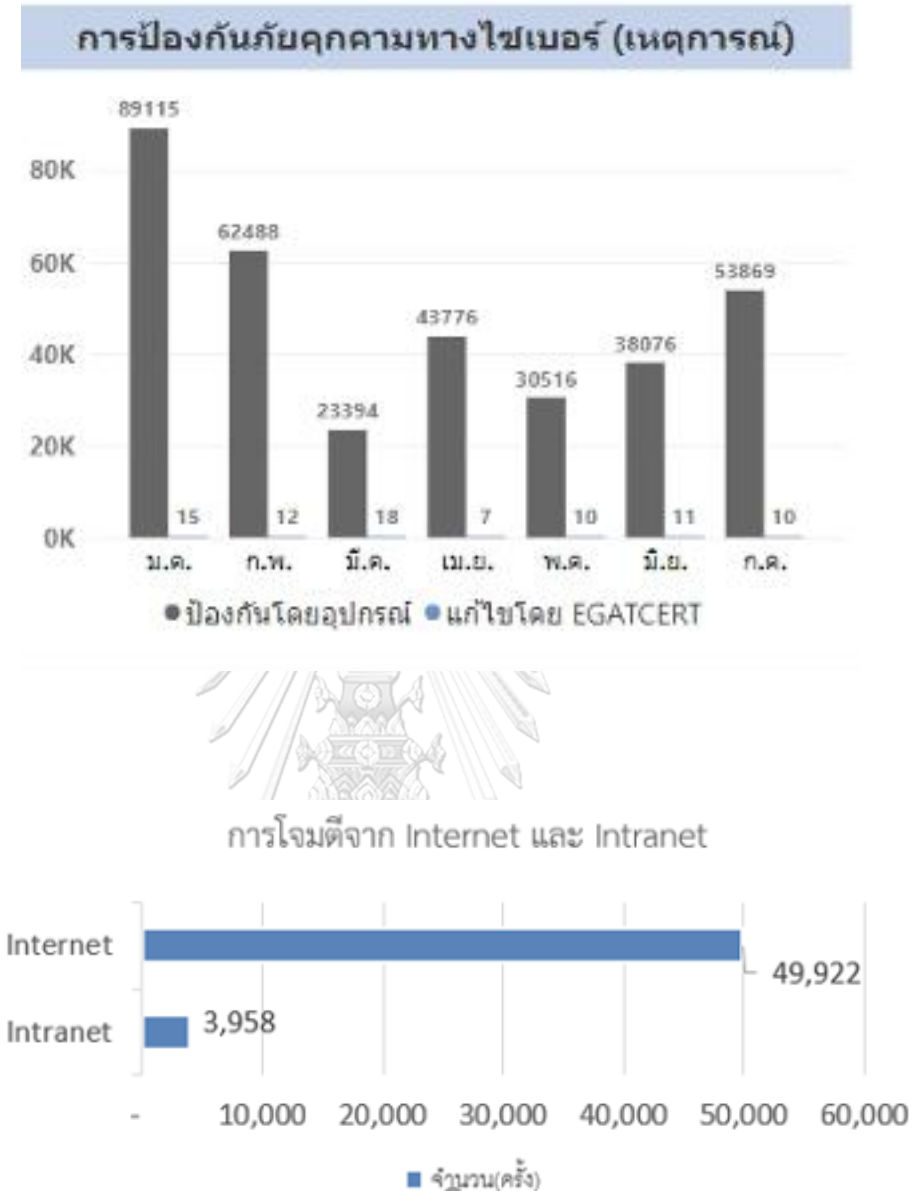
การไฟฟ้าฝ่ายผลิตแห่งประเทศไทยยึดหลักการตาม สกมช. ที่กำหนดไว้ตามกรอบ 5 ข้อ ดังนี้



รูปที่ 23 แผนภาพที่ได้จากการสัมภาษณ์เชิงลึกของการไฟฟ้าฝ่ายผลิต ส่วนใหญ่จะเป็นภัยคุกคามจากมัลแวร์ การพยายามบุกรุกเข้าระบบ และ การโจมตีความพร้อมใช้งาน

รูปที่ 24 แผนภาพจากการสัมภาษณ์การไฟฟ้าฝ่ายผลิตแห่งประเทศไทย (ข้อมูลจากการสัมภาษณ์)

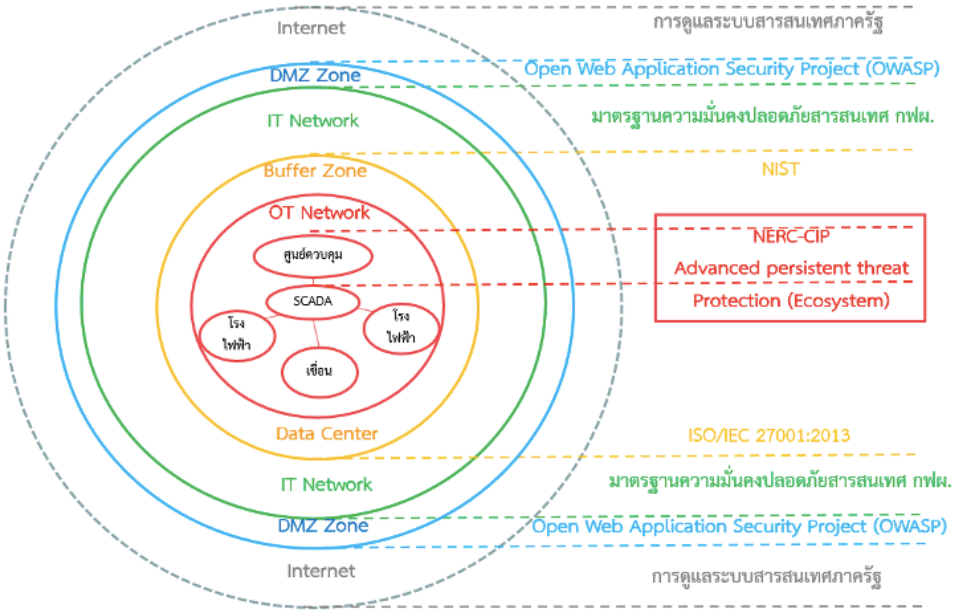
ส่วนใหญ่จากมาจากภัยคุกคามภัยนอกมากกว่าภายในทำให้การไฟฟ้าฝ่ายผลิตจำเป็นต้องมีการติดตั้งอุปกรณ์ป้องกันภัยคุกคามและการแก้ไขปัญหาด้วยการได้รับความร่วมมือจาก ThaiCERT สิ่งเหล่านี้สะท้อนให้เห็นว่าความผิดพลาดที่เป็นช่องโหว่เกิดจากภายในไม่ได้เป็นอุปสรรคกับการไฟฟ้าฝ่ายผลิต พนักงานหรือบุคลากรมีความตระรู้ในระบบคอมพิวเตอร์เป็นอย่างดี ส่วนในแผนภูมิแท่งที่แสดงไว้ด้านล่างนั้นบ่งบอกถึงภัยคุกคามที่เกิดขึ้นและอุปกรณ์ที่เป็นเทคโนโลยีสามารถสกัดจับหรือป้องกันไว้ได้ และร้อยละที่ปรากฏขึ้นนั้นเห็นได้ชัดเจนว่าอุปกรณ์ที่สกัดมีประสิทธิภาพมากพอที่จะไม่ต้องรอให้ทีมไอทีของการไฟฟ้าฝ่ายผลิตร่วมกับ ThaiCERT เข้ามาร่วมแก้ปัญหา



รูปที่ 26 แผนภาพระบบการป้องกันภัยคุกคามทางไซเบอร์ของการไฟฟ้าฝ่ายผลิตแห่งประเทศไทย (ข้อมูลจากการสัมภาษณ์)

6. เป้าหมายการโจมตี

ส่วนเป้าหมายการโจมตีนั้นในวงนอกสุดจะเกิดจากอินเทอร์เน็ตทั่วไปดูแลภายใต้ระบบสารสนเทศของภาครัฐ การโจมตีระดับที่ถัดมาคือการโจมตีผ่าน application และเป็นส่วนของโครงข่ายเทคโนโลยีสารสนเทศ เนื่องจากใกล้ระบบสำคัญมากที่สุดจะมีตัวกั้นเป็นศูนย์ข้อมูลของการไฟฟ้าและภายในที่สำคัญสุดนั้น คือ ศูนย์ควบคุมโรงไฟฟ้าทั่วประเทศรวมทั้งเขื่อนอีกด้วย เนื่องจากการไฟฟ้าส่วนผลิตนั้นเป็นหน่วยงานที่เปราะบางและเสี่ยงต่อการโจมตีมาก จึงทำให้ทั้งระบบเทคโนโลยีของหน่วยงานมีความพร้อมมากในด้านข้อมูลและเชิงเทคนิค



รูปที่ 27 แผนภาพจากการสัมภาษณ์การไฟฟ้าฝ่ายผลิตแห่งประเทศไทย (ข้อมูลจากการสัมภาษณ์)

7. การวัดระดับความรุนแรง

การวัดระดับความรุนแรงของเหตุการณ์ภายในปีนี้นั้นยังมีแนวโน้มระดับการโจมตีที่ต่ำมีระดับความรุนแรงในการโจมตีที่สูงแค่เพียง 3 ครั้งเท่านั้น ส่วนเกณฑ์ที่แยกระดับในการโจมตีนั้นได้อ้างตามตารางที่ 13

ตารางที่ 13 การสัมภาษณ์การไฟฟ้าฝ่ายผลิตแห่งประเทศไทย (ข้อมูลจากการสัมภาษณ์)

มุมมองการประเมินผลกระทบ	ผลกระทบระดับ (L-Low)	ผลกระระดับกลาง (M-Medium)	ผลกระทบระดับสูง (H-High)
1.ผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้ส่วนเสียที่อาจได้รับความเสียหายอื่น นอกจากร่างกายหรืออันตรายต่อชีวิตหรืออนามัย - จำนวนผู้ที่ได้รับผลกระทบมากกว่า 1 วัน- คำนวนความเสียหายโดยตรงเท่านั้น	จำนวนผู้ใช้บริการหรือผู้มีส่วนได้ส่วนเสียที่อาจได้รับผลกระทบมากกว่าหรือเท่ากับ 10,000 คนต่อวัน	จำนวนผู้ใช้บริการหรือผู้มีส่วนได้ส่วนเสียที่อาจได้รับผลกระทบมากกว่า 10,000 คนแต่มาก กว่าหรือเท่ากับ 100,000 ต่อวัน	จำนวนผู้ใช้บริการหรือผู้มีส่วนได้ส่วนเสียที่อาจได้รับผลกระทบมากกว่าหรือเท่ากับ 100,000 คนต่อวัน
2. ผลกระทบความมั่นคงของรัฐ	ไม่มีผลกระทบต่อความมั่นคงของรัฐ	-	มีผลกระทบต่อความมั่นคงของรัฐ

4.5.2 การรับมือการก่อการร้ายไซเบอร์ของหน่วยงานด้านการกำกับดูแลความมั่นคงปลอดภัย

เนื่องจากปัจจุบันภัยคุกคามทางไซเบอร์จากตัวแสดงที่ไม่ใช่รัฐชาติมีเพิ่มมากขึ้นทั้งในระดับโลกและส่งผลกระทบถึงประเทศไทย ด้วยลักษณะพิเศษที่ภัยคุกคามจากแฮกเกอร์ที่ไม่ได้มาจากภาครัฐมีคือความไร้พรมแดนในการจู่โจมโดยที่รัฐชาติไม่สามารถใช้กฎหมายของรัฐตนเอาผิดกับผู้ก่อการร้ายหรือผู้โจมตีเหล่านี้ได้ดังนี้สิ่งที่รัฐสามารถทำได้มี 2 วิธี คือ รัฐจะต้องรับผิดชอบกับการจู่โจมที่เกิดขึ้นภายในรัฐของตนและจะต้องอยู่ภายใต้การบังคับใช้และปกป้องของกฎหมายระหว่างประเทศ

ดังนั้นหน่วยงานด้านการกำกับดูแลความมั่นคงปลอดภัยนั้นมีแนวคิดในการรับมือทางด้านนโยบายตามรูปแบบของสหประชาชาติ หรือ United Nations Security Council S/RES/1373 (2001) ตามที่ Buchan (2016) ได้อ้างไว้ในงานเขียนของเขาว่า สหประชาชนมีกฎหมายระหว่างประเทศที่สามารถบังคับใช้ให้ประเทศต่างๆสามารถรับมือกับภัยคุกคามทางไซเบอร์

ที่มาจากผู้กระทำที่ไม่ใช่รัฐชาติได้ ในส่วนนี้จะวิเคราะห์ถึงบทบาทหน้าที่ของ หน่วยงานด้านการกำกับดูแลความมั่นคงปลอดภัยที่ใช้นโยบายปฏิบัติตามกฎหมายระหว่างประเทศทั้งของสหประชาชาติและ Tallin Manual ดังนี้

รัฐชาติมีบทบาททั้งตั้งรับและตอบโต้พร้อมทั้งดูแลความมั่นคงปลอดภัยของสาธารรูปโภคสำคัญของประเทศของตนเองและควรมีกฎหมายและบทลงโทษสำหรับผู้ที่กระทำความผิดทางไซเบอร์อย่างจริงจัง โดย 2 วิธีที่สำคัญที่สภาความมั่นคงแห่งชาตินำมาประยุกต์ใช้ มีดังนี้

1. รัฐบาลจะต้องรับผิดชอบต่อการกระทำที่เป็นการบุกรุกหรือโจมตีทางไซเบอร์ที่ไม่ได้เป็นภัยคุกคามระหว่างรัฐ

ผู้กระทำความผิดนั้นจะต้องมีการกระทำความผิดที่อยู่ภายใต้กฎหมายระหว่างประเทศทั้งนี้รวมไปถึงการใช้ไวรัสทางไซเบอร์เป็นเครื่องมือในการก่อการร้ายเพื่อจะสร้างความมีประสิทธิภาพภายใต้อำนาจของรัฐและกฎหมายระหว่างประเทศทางด้านเทคนิค แต่สิ่งที่ยังเป็นอุปสรรคอยู่ขณะนี้คือ การบุกรุกหรือโจมตีทางไซเบอร์นั้นไม่สามารถที่จะหาหลักฐานอย่างเป็นรูปธรรมได้ เพราะในห้วงพื้นที่ของไซเบอร์นั้นเปรียบเสมือนพื้นที่ว่างเปล่าเมื่ออุปกรณ์อิเล็กทรอนิกส์ (device) เชื่อมต่อกับอินเทอร์เน็ต (internet) หรือที่รู้จักในชื่อของอินเทอร์เน็ตโพรโทคอล (อังกฤษ: Internet Protocol: IP) หรือ เกณฑ์วิธีอินเทอร์เน็ต เป็นโพรโทคอลการสื่อสารที่สำคัญในการถ่ายทอดข้อมูลพื้นฐาน ถ้าไม่ถูกรับประกันโดยเครือข่าย IP นั้นจะไม่สามารถระบุตัวตนของผู้ส่งตัวจริงได้หรือรายละเอียดของผู้แต่จะเป็นเพียงข้อมูลพื้นฐานเท่านั้นที่จะสามารถบอกได้เช่น IP นี้ตั้งอยู่ที่ใดและมากไปกว่านั้นการใช้เทคโนโลยีเชิงเทคนิค เช่น Botnets หรือ ซอร์ฟแวร์ที่ไร้ตัวตน เช่น Virtual Private Networks (VPNs) ที่ประชาชนส่วนมากนิยมใช้ในการดาวโหลดภาพยนต์ที่ไม่ได้รับอนุญาตจากรัฐหือแอบใช่ทำในสิ่งที่ยังไม่รับรองทางกฎหมาย จะยิ่งทำให้การระบุหาตัวตนนั้นยากขึ้นไปอีกระดับ และที่สำคัญนั้นเทคนิคเหล่านี้สามารถหลอกได้ว่าสถานที่ตั้งของการจู่โจมอาจไม่ใช่ที่ตั้งของการจู่โจมจริงๆ เพราะผู้บุกรุกจะใช้ IP ที่ถูกกำหนดมาแล้วจากสถานที่หรือประเทศที่สาม เช่น การใช้ประเทสไทยเป็นสถานที่ในการจู้โจมทางไวเบอร์สหรัฐอเมริกา ทั้ง ๆ ที่ผู้จู่โจมนั้นไม่ใช่คนไทยและไม่ได้ทำในฐานะคนแต่เพียงใช้ประเทศไทยเป็นสถานที่ในการจู่โจมและเหตุผลที่เลือกประเทศไทยนั้นอาจเป็นเพราะเรามีช่องว่างทางกฎหมายที่ไม่สามารถเอาผิดหับผู้ก่อการร้ายเหล่านี้ได้ แต่หากเรานำกฎหมายระหว่างประเทศที่ใช้ครอบคลุมและป้องกันในส่วนของการโจมตีตรงนี้ได้ก็จะสามารถผิดช่องว่างหนึ่งในการจับกุมผู้ร้าย ซึ่งถ้า หน่วยงานปฏิบัติของไทยสามารถทราบสถานที่ก่อเหตุได้ก็จะสามารถจับตัวผู้ร้ายและสืบสวนไปถึงที่มาในโลกแห่งความจริง

“เคยมีเหตุการณ์ของบริษัท Sony Pictures ที่ถูกจู่โจมทั้งระบบจนล่มและเสียหายเป็นมูลค่าล้านล้านดอลลาร์สหรัฐ ทาง ThaiCert และ สกมช. ได้ร่วมมือกันหาผู้ร้านณ ห้องเช้าในตึกแห่งหนึ่งและพบว่าพวกเขาใช้สถานที่ของไทยเป็นสถานที่ในการจู่โจมเพื่อทำให้เกิดความเข้าใจผิด เพราะฉะนั้นหากมีการตรวจสอบที่ไม่ละเอียดมากพอจะให้ได้ว่าประเทสไทยจะเป็นประเทศที่จะถูกกล่าวหาว่าเป็นประเทศที่กระทำการก่อการร้ายในฐานรัฐชาติและใช้ IP ของประเทศไทย เหตุการณ์ครั้งนี้ทำให้หน่วยงานของเรามีชื่อเสียงเพราะสามารถพิสูจน์ได้ว่าประเทสไทยไม่ได้มีส่วนเกี่ยวข้องแต่อย่างใดแต่เป็นผู้ก่อการร้ายชาวรัสเซียเท่านั้นที่เข้ามาทำเพื่อหวังผลประโยชน์ แต่เราก็ไม่สามารถทราบได้อีกว่ารัฐบาลรัสเซียนั้นจะเป็นผู้อยู่เบื้อหลังเรื่องราวเหล่านี้หรือไม่หรือเป็นเพียงแค่กลุ่มที่ไม่อยู่ในฐานะตัวแสดงของรัฐเท่านั้น กฎหมายระหว่างประเทศสามารถนำมาใช้ได้ในกรณีนี้และกฎหมายของไทยเองก็สามารถนำมาบังคับใช้ได้เนื่องจากเกิดขึ้นในอนาเขตของประเทศไทย”

(ผู้ให้ข้อมูลสำคัญคนที่ 16 จากหน่วยงาน สกมช. และ ผู้ให้ข้อมูลสำคัญคนที่ 19 จากหน่วยงาน สมช.)

อย่างที่กล่าวไว้ข้างต้นนั้นการจะพัฒนาเทคโนโลยีที่มีความสามารถเพียงพอที่จะหาต้นสายปลายเหตุหรือสามารถระบุข้อมูลที่เป็นพิเศษเฉพาะตัวนั้นยังมีโอกาสพัฒนาได้ยาก แต่จะสามารถพัฒนาได้ในอานาคตเพื่อหาร่องรอยที่เชื่อถือได้จริง

2. รัฐจะต้องรับผิดชอบกับความล้มเหลวที่เกิดขึ้นหากเกิดเหตุการณ์คุกคามตามที่กฎหมาย

จารีตประเพณีระหว่างประเทศกำหนดไว้ ในที่นี้รวมไปถึงทั้งภัยคุกคามในรูปแบบเก่าและรูปแบบปัจจุบันที่จะต้องจัดการจับกุมกับผู้กระทำให้เข้าสู่กระบวนการให้ได้ เพราะเป็นข้อกำหนดในกฎหมายระหว่างประเทศว่าทุกประเทศนั้นจะต้องสามารถจัดการภัยคุกคามภายใต้อาณาเขตของตนให้ถูกต้องตามกฎหมายของรัฐตนเอง แต่ปัญหาของการจัดการกับผู้กระทำคือ ภายใต้กฎหมายระหว่างประเทศไม่ได้ระบุไว้ว่าหากเกิดเหตุการณ์ขึ้นที่ใดให้เป็นความรับผิดชอบของประเทศนั้น แต่สำหรับอุปสรรคทางไซเบอร์แล้ว รับไม่สามารถพิสูจน์ได้ว่าต้นเหตุที่แท้จริงจากตัวกระทำที่ไม่ใช่รัฐใช้ IP จากที่ใด และจนกว่าจะสืบทราบก็ทำให้ไม่ทันการที่ผู้กระทำจะหนีออกนอกประเทศนั้นแล้ว และอีกประการหนึ่งคือการที่กฎหมายระหว่างประเทศให้รัฐต้องออกมาตรการควบคุมที่มีประสิทธิภาพเอให้ประชาชนในระดับปัจเจกทุกคนอยู่ภายใต้การควบคุมของรัฐและข้อบังคับนี้ก็ไม่ได้เป็นการสร้างภาระให้รัฐในการที่จะปกป้องประชาชนของตนให้พ้นจากอันตรายภายในอนาเขตตนเองหรือต้องบรรเทาให้ภัยอันตรายนั้นน้อยลง

แต่อย่างไรก็ตามความพยายามที่จะทำให้กฎหมายระหว่างประเทศจะสามารถควบคุมภัยคุกคมที่ไรพรมแดนอย่างภัยคุกคามจากไซเบอร์ได้ กลไกทางกฎหมายที่จะปกป้องอาณาเขตของตนก็ยังไม่เพียงพอที่จะคุ้มตรองคนภายในประเทศหรือแม้กระทั่งกฎหมายระหว่างประเทศที่มีข้อบังคับและมีบทลงโทษก็ยังมีจุดอ่อนหรือช่องโหว่ให้ผู้กระทำผิดหลุดรอดมาได้ ในขณะที่ความไร้พรมแดนเป็นพื้นที่ใหม่ที่ยังไม่เคบมีผู้ใดเคยสัมผัสจึงเป็นเรื่องยากที่แต่ละรัฐชาติจะสามารถกลไกทางกฎหมายได้อย่างครอบคลุมและมีประสิทธิภาพ ดังนั้นสิ่งที่สามารถทำได้คือการป้องกันและการยับยั้งไม่ให้ภัยคุกคามเหล่านั้นเกิดขึ้น

4.5.2.1 การพัฒนาระบบการป้องกันและปราบในด้านกฎหมาย

การพัฒนาระบบทางกฎหมายและนโยบายนั้นจะต้องอาศัยการสร้างภูมิคุ้มกันคือการป้องกันและการตรวจตราอย่างละเอียดเพื่อไม่ให้เกิดภัยคุกคามขึ้นและพยายามผลักดันให้มีบทลงโทษผู้กระทำที่ไม่ใช่รัฐให้อยู่ภายใต้เขตของรัฐที่จะต้องรับผิดชอบต่อผลที่เกิดขึ้น มากไปกว่านั้นรัฐจะต้องควบคุมสาธารณูปโภคที่สำคัญโดยการสร้างกรอบระเบียบทางเทคโนโลยีให้สำหรับกรอกข้อมูลทุกอย่างให้กับรัฐ เช่น search engines ต่าง ๆ Internet Service Providers (ISPs) หรือ software providers ต่างๆ และในการปราบปราบภัยคุกคามทางไซเบอร์เหล่านั้นรัฐจำเป็นจะต้องร่างกฎหมายเพื่อกำหนดความผิดทางอาชญาแก่การกระทำแบบคุกคามทางไซเบอร์แต่ละประเภทหรือไม่หรือจะต้องประกอบไปด้วยบทลงโทษตามประเภทการกระทำผิดและสามารถนำไปปฏิบัติใช้จริงได้ แต่อย่างไรก็ตามที่รัฐจะดำเนินการไปถึงจุดนั้น รัฐจะต้องมีหน่วยในการรับมือได้ในทันทีที่มีชื่อว่า Computer Emergency Response Teams (CERTs) หรือที่ประเทศไทยมี ThaiCERTs ที่มีความรู้ความเชี่ยวชาญทางคอมพิวเตอร์โดยเฉพาะที่จะสามารถตรวจจับหรือปราบรามและทำให้ความร้ายแรงของไวรัสหรือภัยคุกคามนั้นลดลงได้ และรัฐจะต้องมีการแลกเปลี่ยนข้อมูลทางไซเบอร์ระหว่างกันทั้งโครงสร้างพื้นฐานสาธารณูปโภคสำคัญทั้งภาครัฐและเอกชน

ในช่วงต้นทศวรรษของปี 1960 รัฐพยายายามที่จะรวบรวมกฎหมายต่างๆ หรือสนธิสัญญาที่เกี่ยวกับการก่อการร้าย แต่ในครั้งนั้นยังไม่มีเรื่องราวที่เกี่ยวข้องกับการก่อการร้ายทางไซเบอร์จึงไม่ได้มีการบัญญัติเรื่องการก่อการร้ายไซเบอร์ไว้ในนั้นโดยเฉพาะ แต่คำนิยามของการก่อการร้ายไซเบอร์นั้นมีความกว้างเพียงพอและครอบคลุมในส่วนของการกระทำทางไซเบอร์ที่หมายถึงการใช้เทคโนโลยีเจาะระบบและสร้างความเสียหายให้เกิดขึ้น แต่ในปัจจุบันนี้มีการให้คำนิยามการกระทำของการก่อการร้ายไซเบอร์ที่ถูกใช้บังคับในข้อตกลงแบบผูกมัดระหว่างประเทศและสามารถใช้อำนาจทางศาลจัดการกับผู้กระทำผิดได้ภายใต้ Chapter VII of United Nations (UN) Charter, the Security Council หรือสภาความมั่นคงของสหประชาชาติ ที่จะบังคับให้ประเทศที่เป็นสมาชิกของสหประชาชาติต้องปฏิบัติตามมาตรการที่ UN กำหนดไว้ และเพื่อเป็นการป้องกันและแลกเปลี่ยนข้อมูลระหว่างประเทศ

สมาชิกให้เฝ้าระวังถึงภัยคุกคามทางไซเบอร์อีกด้วย โดยมีชื่อว่า counterterrorism measures หรือ มาตรการการรับมือการก่อการร้าย

จากมุมมองของผู้เขียนนั้นสาระสำคัญของของ the Convention on Cybercrime จะเฉพาะเจาะจงแค่อาชญากรรมไซเบอร์ธรรมดาเท่านั้น สนธิสัญญาต่างๆที่เกี่ยวข้องกับการต่อต้านการก่อการร้ายจากสภาความมั่นคงของสหประชาชาติได้ชี้ทิศทางเฉพาะประเภทของภัยคุกคามทางไซเบอร์ให้มีส่วนเกี่ยวกับกับการก่อการร้ายไซเบอร์ทั้งหมด ดังนั้นกฎหมายระหว่างประเทศจึงไม่สามารถระบุได้อย่างชัดเจนว่าการกระทำประเภทไหน ความรุนแรงขนาดใด ควรได้รับโทษเท่าใด ดังนั้นในส่วนนี้จึงจำเป้นที่จะต้องสรุปว่าองค์ประกอบอะไรบ้างที่ควรจะเป็นสิ่งสำคัญในการใช้เป็นกลไกปกป้องสาธารณูปโภคสำคัญทางไซเบอร์จากผู้กระทำที่ไม่ใช่รัฐชาติและเป็นการกระทำที่ไร้พรมแดน

1) องค์พื้นฐานความรู้

องค์พื้นฐานความรู้เป็นสิ่งสำคัญที่สุดในองค์ประกอบทั้งหมดเพราะรัฐจะต้องใช้องค์ความรู้ที่มีสกัดกั้นไม่ให้เกิดและปราบปรามไม่ให้เกิดขึ้น เพราะฉะนั้นรัฐจึงมีบทบาทสำคัญมากที่จะต้องมีเทคโนโลยีสำคัญเพื่อที่จะจะสอดส่องแต่ตรวจจับได้ว่า ภัยคุกคามนั้นจะมาจากนอกประเทศหรือในประเทศแต่รัฐจะต้องมีการติดตั้งเทคโนโลยีในการป้องกันไวรัสหรือมัลแวร์ต่างๆ ไม่ให้เข้าถึงสาธารณูประโภคสำคัญของประเทศก่อนที่จะเกิดเหตุการณ์ไม่สงบเกิดขึ้น แต่อย่างไรก็ตามก็ยังมีข้อถกเถียงว่าจะเป็นไปได้หรือไม่ที่รัฐจะสามารถป้องกันและสกัดกั้นภัยคุกคามเหล่านั้นได้ทั้งหมด จากการสัมภาษณ์ผู้เชี่ยวชาญในการทำ Tallinn Manual ยังไม่มีความคิดเห็นที่ถือเป็นที่สิ้นสุดว่านั้นคือข้อกำหนดที่รัฐจะต้องทำได้ ซึ่งบางครั้งรัฐอาจจะใช้ข้ออ้างในการขาดซึ่งองค์พื้นฐานความรู้ในการตรวจสอบได้ หรืออาจจะเรียกอีกอย่างว่า การขาดความตระหนักรู้ของรัฐ

2) ภารกิจและหน้าที่ในการป้องกันภัยคุกคาม (The Duty to Prevent)

เมื่อรัฐทราบถึงภัยคุกคามที่กำลังจะเกิดขึ้น รัฐจำเป็นจะต้องสามารถประเมินสถานการณ์ที่จะเกิดขึ้นได้และสามารถที่จะมีมาตรการที่จะรับมือและจะต้องถูกต้องตามทำนองครองธรรม ไม่ผิดต่อจริยธรรมที่จะตอบโต้ อย่างที่ทราบกันแล้วว่าข้อบังคับส่วนใหญ่ต้องการให้รัฐแต่ละรัฐใช้มาตรการตามกรอบของกฎหมายที่อยู่ภายอาณาเขตของตัวเองหรือการกระทำที่เกิดขึ้นภายในประเทศนั้น ในฐานะรัฐจะต้องทำให้ผลกระทบน้อยลงมากที่สุด รัฐจะต้องใช้ความสามารถสืบสวนและมีบทลงโทษสำหรับสิ่งที่ผู้ก่อการร้ายทำขึ้น รัฐจะต้องมีบทลงโทษที่จำเพาะผู้กระทำความผิดที่เป็นเหตุให้เกิดความเสียหายความรุนแรงต่อรัฐ หน้าทีในการสอบสวนสเหมือนหน้าที่ในการป้องกันอีกรูปแบบหนึ่ง

(1) ความสามารถในการรับมือของของรัฐ (State capacity)

ในความหมายของคำว่า ความสามารถรับมือภัยคุกคามไซเบอร์ของรัฐ นั้นหมายถึงการที่รับมีความพร้อมทางด้านทรัพยากรบุคคล อุปกรณ์เทคโนโลยีขั้นสูง งบประมาณในการจัดการกับภัยคุกคามเหล่านี้ได้ สิ่งเหล่านี้เรียกว่าเป็นเครื่องมือพื้นฐานสำหรับรัฐที่จะป้องกันภัยคุกคามทางไซเบอร์ ถึงแม้การป้องกันภัยคุกคามทางไซเบอร์จะมีความยาก เช่นการเข้าถึงง่ายของประชาชน การไม่สามารถระบุถึงตัวตนได้ แต่หากรัฐมีเทคโนโลยีใหม่ๆ ก็จะสามารถตามรอยผู้คุกคามเหล่านี้ได้ ตามกฎหมายระหว่างประเทศต้องการให้แต่ละรัฐมีการรับมือและเตรียมพร้อมกับก่อการร้ายที่กำลังจะมาถึงและไม่ปล่อยให้ภัยคุกคามเหล่านั้นเล็ดลอดออกมานอกประเทศได้ แต่ก่อนที่รัฐจะสามารถรับมือหรือมีทรัพยากรเหล่านี้ได้นั้น รับจะต้องพื้นฐานองค์ความรู้ที่ได้กล่าวไปในข้างต้นก่อนเพื่อพัฒนาทักษะของบุคลากรให้สามารถใช้ทรัพยากรได้อย่างคุ้มค่า

(2) ระดับความเสี่ยงของภัยคุกคาม (Degree of risk)

ระดับความเสี่ยงของภัยคุกคามทางไซเบอร์นั้นสามารถแบ่งได้เป็น 2 ระดับ โดยระดับแรกนั้นรัฐมองเห็นภัยคุกคามที่เกิดขึ้นเป็นเพียงภัยที่กำลังจะมาถึง แต่ยังไม่เกิดขึ้นจริง หากภัยมาถึงรัฐจำเป็นจะต้องใช้ทั้งความเร็วในการตั้งรับกับภัยที่คาดไม่ถึง และไม่สามารถคาดการณ์ความรุนแรงได้การเผชิญหน้านั้นจะใช้ความรวดเร็วในการพัฒนาเครื่องมือรับททือภัยคุกคามให้ผลที่เกิดขึ้นมีน้อยลง ส่วนความเสี่ยงในระดับที่สองนั้นคือความเสี่ยงที่เกิดขึ้นจริงและผลกระทบที่ตามมาว่าจะมีความรุนแรงมาเพียงใดและรัฐจะต้องป้องกันเพิ่มเติมจากการตั้งรับมือที่มีอยู่แล้วมากขึ้นเท่าใด และหลังจบเหตุการณ์เหล่านั้นรัฐจะต้องมีบทลงโทษที่ชัดเจน มีการเยียวยา และการฟื้นฟูสิ่งที่เสียหายเหล่านั้นให้กลับมาใช้งานได้เร็วยิ่งขึ้น

หากความเสียหายในที่นี้คือสาธารณูปโภคสำคัญของประเทศเกิดความเสียหายจนทำให้เกิดความสูญเสียต่อชีวิตของประชาชนเป็นจำนวนมาก ในกรณีนี้ “รัฐบาลจะต้องปิดระบบคอมพิวเตอร์ทั้งหมดของประเทศ” เพื่อไม่ให้เกิดความเสียหายมาไปกว่านั้น แต่ในความเป็นจริงแล้วหากเป็นการเกิดการจู่โจมข้ามรัฐก็จะเป็นไปได้ยากที่จะตรวจจับภัยคุกคามได้ และการปิดระบบโครงข่ายทางไซเบอร์ทุกอย่างก็ทำให้เกิดขึ้นซึ่งความเสียหายเช่นกันเพราะฉะนั้นรัฐจะต้องสามารถประเมินของเขตของความเสียหายเหล่านั้นได้ ก่อนที่จะตัดสินใจปิดระบบไซเบอร์ในจุดที่เกิดเหตุการณ์นั้นขึ้น

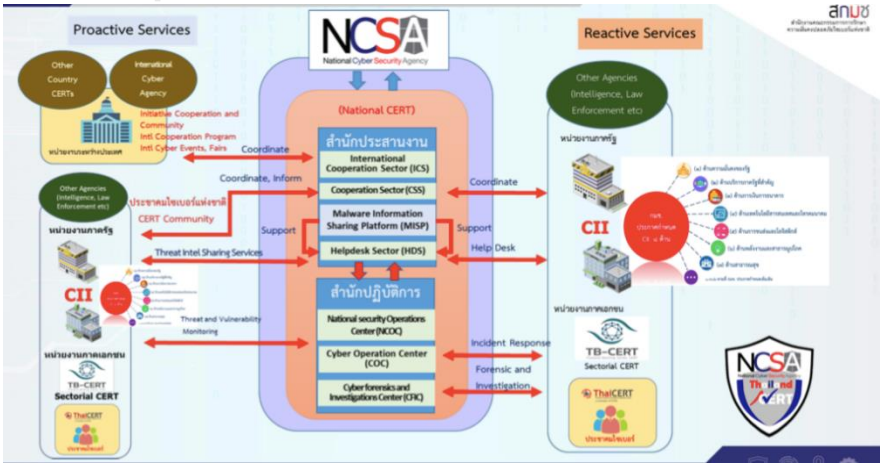
(3) ระดับความเสียหาย (Damage)

ข้อกำหนดที่เป็นพื้นฐานประการหนึ่งของกฎหมายระหว่างประเทศคือการที่รัฐละเมิดหรือฝ่าฝืนบรรทัดฐานที่อยู่ใต้ความรับผิดชอบของรัฐโดยละเลยสาเหตุที่จะทำให้เกิดความเสียหาย ซึ่งถือว่าข้อกำหนดนี้เป็นพื้นฐานที่จะสามารถใช้ได้กับการก่อการร้ายทางไซเบอร์ที่กำลังเกิดขึ้นในอนาคตได้ และกฎข้อนี้คือกฎข้อพื้นฐานแรกที่รัฐจะต้องนำมาปรับใช้

อย่างระมัดระวังและความรับผิดชอบของรัฐนั้นจะต้องขึ้นอยู่กับความเสียหายที่รุนแรงเท่านั้น และ The Tallinn Manual ก็มีความคิดเห็นในแบบเดียวกับกฎหมายระหว่างประเทศที่รับจะต้องรับผิดชอบกับความเสียหายที่รุนแรงโดยความรุนแรงนั้นไม่ใช่แค่ความเสียหายของสาธารณูปโภคสำคัญทางกายภาพเพียงอย่างเดียวแต่จะรวมไปถึงระบบโครงข่ายคอมพิวเตอร์ในพื้นที่ทางไซเบอร์ด้วย และหลังที่ความเสียหายเกิดขึ้นนั้นก็เป็นเพียงหน้าที่ของรัฐที่จะต้องประเมินความผิดพลาดที่เกิดขึ้นว่าการป้องกันภัยคุกคามของตนนั้นมีช่องโหว่อย่างไรและจะแก้ไขปรับปรุงเพื่อที่จะพร้อมรับมือตรงนั้นอย่างไร

เนื่องจากการนำโครงสร้างการและกรอบการรับมือทางไซเบอร์มาประยุกต์ใช้กับประเทศไทยหน่วยงานหลักคือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หรือ สกมช. มีแนวคิดดังนี้

ตามพระราชบัญญัติการรักษาความมั่นคง ปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2562ได้จัดตั้งสำนักงานคณะกรรมการการ รักษาความมั่นคงปลอดภัยไซเบอร์ แห่งชาติ หรือ สมกช. ให้ทำหน้าที่ กำหนดนโยบาย ระเบียบ มาตรการ มาตรฐานขั้นต่ำ แนวทางปฏิบัติใน การรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานภาครัฐและ ภาคเอกชนที่เป็นหน่วยงานโครงสร้าง พื้นฐานสำคัญทางสารสนเทศ ในการเฝ้าระวังป้องกันรับมือและลดความ เสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบและสร้างความ เดือดร้อนต่อประชาชน ตลอดจน ความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ โดยคำนึงถึงด้านสำคัญของความมั่นคง บริการภาครัฐที่สำคัญ การเงินการธนาคาร ขนส่งและโลจิสติกส์ เทคโนโลยีสารสนเทศ และโทรคมนาคม พลังงานและสาธารณูปโภคและสาธารณสุข โดยจะต้องมีการารเฝ้าระวัง การปกป้อง การรับมือ ลดความเสี่ยง



รูปที่ 28 แผนภาพการทำงานของ สกมช. (ข้อมูลจากการสัมภาษณ์)

นอกจากนี้ สกมช. จะต้องผลักดัน ThaiCERTs ระดับประเทศ ประสานงานระหว่างประเทศ และข้ามกลุ่มอุตสาหกรรมภายในประเทศ โดย CERTs ในกลุ่มนี้จะต้องดูแลโดย Regulator และจัดตั้ง CERTs ระดับหน่วยงาน มีหน้าที่ เฝ้าระวัง ตรวจจับภัยคุกคามทางไซเบอร์ รับมือ ประสานงาน จัดการสถานการณ์ภัยคุกคามทางไซเบอร์ เคราะห์ภัยคุกคามที่ซับซ้อนและมัลแวร์ ในระบบเจ้าหน้าหน้าที่สนับสนุนทางงเทคโนโลยีดูแลระบบจัดการระบบสารสนเทศ Information Sharing เจ้าหน้าที่สนับสนุนด้านการปฏิบัติการ CERTs Operations และจะต้องมีการจัดระบบฝึกอบรมให้บุคลากรทางไซเบอร์ สร้างความตระหนักด้านไซเบอร์ให้กับผู้ใช้งานทั่วไป โดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ

โดยความก้าวหน้าทางพระราชบัญญัติไซเบอร์นั้น ขณะนี้ตามมาตรา 9 จัดตั้งคณะกรรมการการรักษาความมั่นคง ปลอดภัยไซเบอร์แห่งชาติ (กมช.) ซึ่งได้จัดตั้งอย่างเป็นทางการเมื่อเดือนสิงหาคม 2564 โดยมีหน่วยงานควบคุมหรือกากับดูแล ตามมาตร 49 ทั้งหมด หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ Critical Information Infrastructure (CII) มาตรา 50 ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สาหรับหน่วยงาน CII หรือ “Sectorial CERT” มาตรา 60 รายละเอียดของลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ โดยทั้ง 3 มาตรานี้อยู่ภายใต้มาตรา 22 วรรคสองโดยมีการควบคุมดูแลของสำนักงานคณะกรรมการการรักษา ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และภายศูนย์ประสานการรักษาความมั่นคง ปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (National CERT) อีกชั้นหนึ่ง

หากพิจารณาถึงวิสัยทัศน์และภารกิจของสำนักงานคณะกรรมการการรักษา ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) จะเป็นผู้นำในการขับเคลื่อนในการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศ ที่มีประสิทธิภาพ พร้อมตอบสนอง ต่อภัยคุกคามไซเบอร์ทุกมิติ โดยมีภารกิจเสนอแนะ นโยบายฯ กำกับดูแล ให้ความร่วมมือฯ เผยแพร่ความรู้และพัฒนาบุคลากร และมีเป้าหมาย 5 ด้าน ดังนี้

เป้าหมายที่ 1 มีระบบบริหารจัดการด้าน ความมั่นคงปลอดภัยไซเบอร์ที่พร้อมรับมือต่อภัยคุกคามในทุกรูปแบบ

กลยุทธ์ที่สำคัญ: พัฒนาขีดความสามารถของสานักงานในการป้องกัน รับมือ เฝ้าระวัง และแก้ไขภัยคุกคามไซเบอร์ ศึกษาแนวโน้ม ทิศทาง และจัดทานโยบาย/แผน/กฎหมาย/กฎระเบียบ/ประกาศ/มาตรการ/มาตรฐาน ที่สนับสนุนการรักษา และส่งเสริมสนับสนุนงานวิจัยและพัฒนาเทคโนโลยีองค์ความรู้ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

เป้าหมายที่ 2 หน่วยงานภาครัฐและหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศมีการปกป้องและพร้อมตอบสนองต่อภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ

กลยุทธ์ที่สำคัญ: กำกับ ดูแล ให้หน่วยงานที่เกี่ยวข้อง สามารถป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามไซเบอร์ ความมั่นคงปลอดภัยทางไซเบอร์ระดับหน่วยงาน

เป้าหมายที่ 3 มีเครือข่ายความร่วมมือที่เข้มแข็งทั้งในประเทศและต่างประเทศ

กลยุทธ์ที่สำคัญ: สร้างเครือข่ายความร่วมมือเพื่อบูรณาการทางานร่วมกันรวมถึงส่งเสริมสนับสนุนการแลกเปลี่ยนข้อมูลภัยคุกคามไซเบอร์ทั้งในและต่างประเทศ

เป้าหมายที่ 4 มีบุคลากรไซเบอร์อย่างเพียงพอสอดรับกับความต้องการของประเทศ

กลยุทธ์ที่สำคัญ: พัฒนาศักยภาพและเพิ่มทักษะบุคลากรด้านการรักษา ความมั่นคงปลอดภัยไซเบอร์และสร้างบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

เป้าหมายที่ 5 หน่วยงานที่เกี่ยวข้องมีความตระหนัก รับรู้ และเข้าใจถึงความสำคัญในการรักษาความมั่นคงปลอดภัยทางไซเบอร์

กลยุทธ์ที่สำคัญ: สร้างความตระหนัก และการรับรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ นอกจากนี้ยังมีเป้าประสงค์หลักของโครงการเร่งรัดการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์

ระยะที่ 1 โดยมีผลลัพธ์คือเครื่องมือในการพัฒนาบุคลากรและมีบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ที่มีศักยภาพ มีหลักสูตรความมั่นคงปลอดภัยไซเบอร์ระดับพื้นฐาน หลักสูตรความมั่นคงปลอดภัยไซเบอร์ ระดับผู้เชี่ยวชาญ หลักสูตรระดับผู้เชี่ยวชาญภาคปฏิบัติ / เฉพาะด้าน และ หลักสูตร ความมั่นคง ปลอดภัยไซเบอร์ระดับผู้บริหาร โดยในขณะนี้ได้มีผู้เข้าร่วม ดังนี้ (ThaiCERT, 2018)

1. ผู้เข้าร่วมอบรมหลักสูตรระดับพื้นฐาน 2250 คน
2. ระดับผู้ปฏิบัติงาน 1250 คน
3. ระดับผู้เชี่ยวชาญ 300 คน
4. ระดับผู้บริหาร 50 คน

โดยทั้งหมดนี้จะเป็นกิจกรรมสร้างเครือข่าย ศึกษาดูงานในประเทศ สื่อประชาสัมพันธ์โครงการ clip และ infographic หรือ Social Media และงานแถลงข่าวโครงการ โดยหลักสูตรนั้นจะประกอบไปด้วยข้อสอบจริงและการเรียนผ่าน E-Learning ในระบบการเรียนนั้นจะประกอบไปด้วย (1) ระบบจัดบริหารจัดการผู้เข้าร่วมโครงการ ระบบบริการเนื้อหา E-Learning ระบบบริหารจัดการคลังข้อสอบ (2) ระบบการเรียนรู้แบบจำลองสถานการณ์ (3) ระบบจัดการด้านการเรียนรู้ เช่น ระบบจัดการฝึกอบรม Online Training ระบบจัดการการเรียนรู้ LMS

โครงการที่ สกมช. ได้ดำเนินการไปแล้วคือ การจัดการแข่งขัน Thailand Cyber Top Talent 2021สกมช. ร่วมกับ บริษัท หัวเหว่ย เทคโนโลยี (ประเทศไทย) จำกัด จะจัดการแข่งขันทักษะ ทางด้านCybersecurity ในชื่อ “Thailand Cyber Top Talent 2021” ให้กับนักเรียน

มัธยมศึกษา นักศึกษามหาวิทยาลัย และประชาชนทั่วไป เพื่อเป็นการส่งเสริมและต่อยอดความรู้ทาง Cybersecurity รวมทั้งเป็นการสร้างแรงงานทางด้าน Cybersecurity ออกสู่ตลาดแรงงาน และช่วยเพิ่มความตระหนักรับรู้เกี่ยวกับภัยคุกคามทางด้านไซเบอร์ให้กับบุคคลทั่วไปมากขึ้น รับสมัครผู้เข้าร่วม แข่งขันจากทั่วประเทศระดับมัธยม ระดับอุดมศึกษา ระดับประชาชนทั่วไป การจัดการแข่งขันแบ่งเป็น 3 ระดับ แข่งขันรอบแรก Online การแข่งขัน Final On-site รางวัลชนะเลิศ ระดับละ 3 อันดับ รวมมูลค่ากว่า 500,000 บาท เสร็จสิ้นไปเมื่อ 30 ตุลาคม 2564

4.5.3 การรับมือการก่อการร้ายไซเบอร์ของหน่วยการปราบปรามและป้องกัน

ภารกิจในการปกป้องไม่ให้ภัยคุกคามทางไซเบอร์เข้ามารุกรานประเทศไทยจะต้องเริ่มจากการแยกประเภทของภัยคุกคาม มาตรการป้องกันจึงจำเป็นจะต้องแยกเป็นภัยคุกคามทางไซเบอร์ (cyberattack) หรือ การตักตวงผลประโยชน์ทางไซเบอร์ (cyber exploitation) เพราะทั้งสองประเภทนี้บางครั้งมีความเหมือนกัน สิ่งที่จะต้องทำคือการสร้างแผนภาพให้ชัดเจนระบุได้ว่าคือภัยประเภทใด เป้าหมายสำคัญคือคนกลุ่มใด เก็บเป็นข้อมูล สิ่งที่สำคัญอีกประการหนึ่งที่ต้องคำนึงคือการประเมินผลของการบรรลุวัตถุประสงค์ทางการเมืองของผู้ก่อการร้ายต่ำไป เพราะผลจากการก่อการร้ายนั้นจะกระทบถึงความมั่นคงของประเทศ เศรษฐกิจ และสังคม แต่อย่างไรก็ตามผลจากการก่อการร้ายนั้นยากที่จะคาดการณ์ แม้แต่การก่อการร้ายแบบดั้งเดิมไม่ว่าจะเป็นในระดับเล็กน้อยไปจนถึงการก่อการร้ายในระดับประเทศเช่น เหตุการณ์ 9/11 ถึงแม้ว่าผลกระทบจากการก่อการร้ายจากไซเบอร์นั้นจะให้ผลที่ตรงข้ามกับและมักจะเกี่ยวข้องกับเทคโนโลยีเป็นพื้นฐานและเทคโนโลยีเพื่อการสื่อสาร สำหรับรูปแบบผลกระทบหรือแม้กระทั่งผลกระทบของการก่อการร้ายทางไซเบอร์จะมีความยากมากขึ้นในการคาดการณ์

สิ่งหนึ่งที่หน่วยการปราบปรามและป้องกันต้องกระทำคือวิธีการ “ผ่าตัด” หรือแบ่งย่อยภัยคุกคามคามทางไซเบอร์ให้อยู่ในรูปแบบของปัจเจกหรือกลุ่มเล็ก ๆ เพราะการแยกออกมาให้เห็นจะทำให้ผู้ก่อการร้ายมีความกดดันมากขึ้น การที่ผู้ก่อการร้ายสามารถรวมกลุ่มกันนั้นเปรียบเสมือนการสร้างเกราะป้องกันให้ตนเองและสร้างเครือข่ายในการหลบหนี การสร้างความกดดันให้ผู้ก่อการร้ายเช่นการข่มขู่ที่ได้กล้าวไปแล้วข้างต้นนั้นจะทำให้เกิดความกลัว แต่หากปฏิบัติการนี้ไม่สำเร็จ การใช้กำลังจะต้องเป็นสิ่งที่ตามมา

จากการศึกษาและสอบถามถึงเหตุการณ์ก่อการร้ายไซเบอร์นั้นส่วนใหญ่มักจะไม่พบความเสียหายเชิงกายภาพมากนัก แต่จะเกิดขึ้นกับความเสียหายในระบบโครงข่ายอินเทอร์เน็ต เพราะฉะนั้นนโยบายส่วนใหญ่จะพลาดการประมาณความเสียหายในเชิงกายภาพไม่เหมือนดังเช่นการก่อการร้ายแบบดั้งเดิม ดั้งนั้นหากนำกฎหมายมนุษยธรรมไม่สอดรับกับหลักการนี้จะมีช่องโหว่และไม่สามารถนำมาปรับใช้ได้ การบุกรุกทางไซเบอร์ยังคงเป็นภาพในอนาคตที่รัฐบาลและฝ่ายปราบปราม

ยังต้องจินตนาการที่จะต้องรับมือ ความซับซ้อนของไวรัสที่สามารถกระจายไปอย่างไร้พรมแดนจนไม่อาจใช้อำนาจทางกฎหมายสากลมารับรองการใช้กำลัง หากเกิดการคุกคามจากประเทศที่สามหรือประเทศที่ไม่มีส่วนเกี่ยวข้องหรือประเทศที่เป็นแค่ฐานทัพหรือทางผ่านเท่านั้น และการก่อการร้ายไซเบอร์นั้นจะเริ่มก่อตัวให้เห็นในเชิงกายภาพมากขึ้นเมื่อทุกสิ่งทุกอย่างบนโลกต้องพึ่งพิงการใช้อินเทอร์เน็ต

การแบ่งประเภทภัยคุกคามเพื่อรับมือ ประกอบไปด้วย ลักษณะของภัยคุกคามไซเบอร์ ตัวแสดงหรือผู้กระทำ เครื่องมือ เทคนิคในการโจมตี

1. จุดอ่อนใหม่ (New Vulnerabilities)

การเกิดขึ้นในโลกของไซเบอร์มักเปลี่ยนแปลงอยู่เสมอ จากการใช้คอมพิวเตอร์ธรรมดาเพื่ออำนวยความสะดวกในชีวิตประจำวัน และโลกใบนี้ก็ต้องอาศัยพึ่งพิงซึ่งเทคโนโลยีสมัยใหม่ อินเทอร์เน็ตกลายเป็นส่วนหนึ่งที่สำคัญของสังคมที่ประชาชนทุกส่วนจะต้องเข้าถึง ขณะนี้เรากำลังอยู่ในโลกของ Internet of Things ซึ่งหมายความว่าทุกอย่างบนโลกทุกเชื่อมต่อกับระบบอินเทอร์เน็ต ซึ่งความเสี่ยงนี้จะนำไปสู่การโจมตีสาธารณูปโภคสำคัญของประเทศ เช่น ระบบสาธารณสุข ระบบการขนส่ง ระบบไฟฟ้า ประปา และด้วยความที่สิ่งเหล่านี้มีความเป็นเอกเทศสูงคือทุกระบบในสาธารณูปโภคสำคัญของประเทศจะมีระบบเป็นของตนเองและไม่ได้มีการแบ่งปันข้อมูลใดๆจึงมีความเสี่ยงมากหากมีหน่วยใดหน่วยหนึ่งถูกโจมตีระบบและไม่มีหน่วยใดช่วยได้ทัน นี่จึงเป็นอาวุธใหม่ที่เปิดช่องว่างที่สำคัญให้กับรัฐชาติที่ต้องเตรียมตัวรับมือ

2. ความไร้พรมแดนและไร้ตัวตน (Boundlessness and Anonymity)

ในโลกไซเบอร์แล้วนั้นไม่มีการคำนึงถึงเรื่องเขตแดนเพราะเป็นเรื่องยากที่จะต้องจำกัดนิยามและระบุอาณาเขต ในโลกไซเบอร์ไม่เพียงแต่จะสามารถทำลายสาธารณูปโภคสำคัญของรัฐได้ แต่ยังสามารถชักจูงเรื่องเป็นแรงบันดาลใจให้คนทั่วโลกที่มีอุดมการณ์เดียวกันมารวมกลุ่มกัน ซึ่งความไร้ตัวตนนี้เป็นลักษณะที่น่ากลัวเพราะเราไม่สามารถทราบได้ว่า ใครคือผู้อยู่เบื้องหลังบัญชีเหล่านั้น และการจะจับกุมหรือหาหลักฐานสำหรับคนกระทำความผิดก็ไม่ใช่เรื่องง่ายอีกเช่นกันนี่คือความท้าทายของรัฐ หากมองในมุมของเทคโนโลยีสารสนเทศ การชื่อสื่อทางอินเทอร์ในโลกออนไลน์จะเป็นเรื่องที่รัฐทำได้ยากมากที่จะควบคุมการแสดงความคิดเห็นที่มีต่อรัฐอย่างอิสระ เพราะบางครั้งถือเป็นการละเมิดความเป็นส่วนตัวในพื้นที่ของตัวบุคคล

3. ความคลุมเครือในการรับผิดชอบของรัฐ (The Vagueness and Unclear Responsibilities)

เนื่องจากความไร้พรมแดนและไร้ตัวตนของผู้กระทำในโลกไซเบอร์จึงเป็นประเด็นให้ตั้งข้อสงสัยว่ารัฐควรจะต้องมีความรับผิดชอบในการกระทำเหล่านี้หรือไม่ และหากรัฐเองไม่ได้มีส่วนเกี่ยวข้องจะต้องมีมาตรการอย่างไรไม่ให้บุคคลที่สามเข้ามาก่อเหตุขอบเขตทางกายภาพของรัฐตนหรือ

แม้กระทั่งขอบเขตในไซเบอร์ก็ตาม นอกจากนี้ยังมีกฎหมายระหว่างประเทศกล่าวไว้ว่าหากมีการบุกรุกทางไซเบอร์รัฐนั้นจะต้องเป็นผู้ตรวจสอบและรับผิดชอบโดยมีบทลงโทษให้แก่ผู้กระทำความผิด ทั้งนี้รัฐจะต้องตั้งหน่วยงานเพื่อรับมือกับภัยคุกคามเหล่านั้นถ้ามีเหตุฉุกเฉิน เช่น การโจมตีระบบคอมพิวเตอร์สาธารณสุข โดยหน่วยงานแรกที่จะต้องรับผิดชอบคือทีมงานเทคโนโลยีสารสนเทศเบื้องต้นของกระทรวงสาธารณะสุขและหากไม่สามารถรับมือเบื้อต้นได้จะต้องติดต่อหน่วยงาน Computer Emergency Response Team ทีมสำหรับรับมือกับสถาณการณ์ฉุกเฉินที่เกี่ยวกับคอมพิวเตอร์ สำหรับประเทศไทยนั้นคือ (ThaiCERTs) นั่นเอง

4. อำนาจอธิปไตยของพื้นที่ทางไซเบอร์ (Sovereignty in Cyberspace)

ปัญหาหนึ่งที่เกิดขึ้นมาจากความไร้ตัวตนและไร้พรมแดนในโลกไซเบอร์นั้นคือการไม่สามารถระบุอำนาจอธิปไตยของรัฐชาติได้ เพื่อความปลอดภัยของผู้กระทำหรือจู่โจม พวกเขาจะหาช่อโหว่ด้วยการกระทำในภายนอกหรือรัฐที่ไม่เกี่ยวข้องโดยเฉพาะรัฐที่ไม่มีกฎหมายทางไซเบอร์รับรอง เพราะสุดท้ายแล้วรัฐก็ไม่สามารถที่จะตรวจจับหรือหาหลักฐานที่เกี่ยวข้องเพื่อจับกุมตัวได้จริงและรับเองก็ไม่สามารถกล่าวหาอีกรัฐหนึ่งว่าเป็นผู้กระทำได้เพราะไม่รู้ถึงแหล่งที่มาว่าตัวกระทำนั้นเป็นตัวแสดงที่ไม่ใช่รัฐหรือเป็นการสนับสนุนจากรัฐ ซึ่งสำคัญที่สุดคือการร่วมมือกันระหว่างรัฐในเชิงอำนาจทางศาลและกฎหมายเพื่อช่วยกันสอดส่องดูแลประชาชนของตนและประเทศสมาชิกให้ปลอดภัยจากภัยคุกคามทางไซเบอร์

5. ตัวแสดงและผลู้กระทำ (Actors and Terms)

การสามารถแยกแยะตัวแสดงหรือผู้กระทำในโลกไซเบอร์ได้นั้นจะเป็นประโยชน์กับรัฐในการสร้างกฎหมายและกำหนดนิยามในการจับกุมแลกำหนดบทลงโทษ โดยจากการสัมภาษณ์และการหาข้อมูลเชิงลึกสามารถแยกได้ดังนี้ (Buchan, 2016)

5.1 แฮกเกอร์ (Hackers)

แฮกเกอร์ คือ คนที่มีความชำนาญในการใช้คอมพิวเตอร์ไปในทางที่ผิดกฎหมาย เช่น การขโมยข้อมูลจากคอมพิวเตอร์ในเครือข่าย หรือแอบแก้ตัวเลขในธนาคารเพื่อถอนเงินออกมาใช้เองคำว่า hack อาจหมายถึงการแอบปรับแก้หรือดัดแปลงโปรแกรมคอมพิวเตอร์โดยไม่ถูกต้องตามกฎหมายและสามารถหาช่องโหว่ในระบบได้ ในความหมายนี้ระบุแฮกเกอร์ว่าเป็นปัจเจกบุคคลหรือปัจเจกบุคคลที่รวมกลุ่มกันและมีอุดมการณ์เดียวกัน แล้วสมาชิกในกลุ่มนั้นจะต้องเสียสละตนเองเพื่อเรียนรู้ทางไซเบอร์ให้ได้มากที่สุดโดยเฉพาะในทางเทคนิคและการเข้าถึงทรัพยากรทางเทคโนโลยีของภาครัฐ ผ่านทางการควบคุมซอฟแวร์

แต่อย่างไรก็ตามมุมมองโดยทั่วไปของแฮกเกอร์ได้เปลี่ยนไป ตั้งแต่การเกิดขึ้นครั้งแรกที่เรียกว่า การทดลองใช้โทรศัพท์ที่แฮกเกอร์มีจุดประสงค์ที่จะใช้โทรศัพท์ฟรีโดยไม่ต้องเสียเงิน และการพัฒนาต่อมาแฮกเกอร์ได้เรียนรู้และพัฒนาตนเองเมื่อ ระบบคอมพิวเตอร์เกิดขึ้น แฮก

เกอร์เริ่มที่จะใช้ทักษะในการแอบดูระบบเครือข่ายผู้อื่น ตั้งแต่ในยุคของอินเทอร์เน็ตและการมีอินเทอร์เน็ตเป็นกระแสหลักและใช้ คำศัพท์ แฮกเกอร์ ที่มีความหมายของอาชญากรรมซเบอร์ ต่อมาเมื่อแฮกเกอร์มีการรวมกลุ่มร่วมกันมาขึ้นจะก่อให้เกิดกิจกรรมที่ผิดกฎหมายที่เรียกว่า cracker หรือ แคร็กเกอร์ (อาชญากร) การก่ออาชญากรรมทางโลกไซเบอร์ มีลักษณะคล้ายกกับแฮกเกอร์แต่แตกต่างกันตรงความคิดและเจตนา แฮกเกอร์ คือผู้ที่นำความรู้ในการแฮกไปใช้ในทางที่มีประโยชน์ ส่วนแครกเกอร์ คือผู้ที่นำความรู้ในการแฮกไปใช้ในการทำความผิด เช่น การขโมยข้อมูล การทำลายข้อมูล หรือแม้กระทั่งการครอบครองคอมพิวเตอร์คนอื่น หากต้องให้ แคร็กเกอร์ และ แฮกเกอร์ ต้องอาศัยอยู่ในเรือลำเดียวกัน จะมีคำศัพท์ที่แบ่งแยกทั้ง 2 ประเภทนี้ คือ กลุ่มหมวกขาว (white hat) และ กลุ่มหมวกดำ (black hat) และบางครั้งทั้ง 2 คำศัพท์นี้มิอาจแยกอกจากกันได้สำหรับแฮกเกอร์บางประเภท จะถูกเรียกว่า กลุ่มหมวกเทา (grey hat) ที่จะมีจุดมุ่งหมายที่จะเอาผลประโยชน์ของผู้อื่นเป็นของตนเอง

สำหรับกลุ่มหมวกดำ (black hat) นั้นจะถูกมองว่าเป็นกลุ่มที่ผิดกฎหมายทำกิจกรรมที่เป็นภัยทางไซเบอร์ เช่น จู่โจม บุกรุก ระบบโครงข่ายไซเบอร์โดยมิได้รับอนุญาต ดังนั้นกลุ่มแฮกเกอร์จึงถูกมองว่าเป็นสามารถให้ความรู้แก่ภาครัฐได้ เพราะแฮกเกอร์ส่วนใหญ่จะมีความรู้และใช้ความรู้ส่วนนี้ช่วยเหลือรัฐบาลป้องกันภัยคุกคามทางไซเบอร์จากประเทศอื่น และเป็นที่ทราบกันว่ามีแนวโน้มที่แฮกเกอร์จะเปลี่ยนงานอดิเรกของตนเป็นงานในระดับชำนาญการในอนาคตและจะทำงานเป็นที่ปรึกษาทางอุตสาหกรรมซอฟแวร์และอินเทอร์เน็ต เช่น การสังเกตและป้องกันกลุ่มหมวกดำไม่ให้เข้ามาบุกรุก หรือระบุว่าแฮกเกอร์นั้นจะโจมตีสาธารณูปโภคอย่างไร และการแบ่งประเภทของแฮกเกอร์นั้นจะยิ่งช่วยให้ผู้อำนาจในการปฏิบัติการของรัฐเข้าถึงความเข้าใจของแฮกเกอร์มากขึ้นและใช้ประโยชน์จากแฮกเกอร์ได้ถูกต้อง ถึงแม้บางครั้งอาจจะดูไม่จำเป็นเพราะฉะนั้นวิจัยนี้จึงพยายามแยกแยะเพื่อให้เกิดความง่ายขึ้นในการป้องกันการบุกรุกทางไซเบอร์

5.2 แฮกเกอร์มือใหม่ (Script Kiddies)

แฮกเกอร์มือใหม่ที่ยังขาดความชำนาญในการเจาะระบบคอมพิวเตอร์ โดยปกติแล้ว Script Kiddies จะใช้โปรแกรมเจาะระบบที่ถูกพัฒนาโดย Hacker ที่มีความชำนาญสูงมาใช้เจาะระบบคอมพิวเตอร์ที่ตัวเองสนใจด้วยความอยากรู้อยากเห็น หรือทดลองความรู้ในการเจาะระบบของตนเอง แต่ยังมีทักษะเท่ากับผู้ที่เป็น Hacker แต่ถึงแม้ว่า คำนี้ Kiddies จะมีความหมายว่า เด็กสมัครเล่น แต่ก็ไม่ได้หมายความว่าจะต้องเป็นวัยรุ่นหรือเด็กเสมอไป แฮกเกอร์มือใหม่จะเริ่มต้นจากสิ่งง่ายๆที่ใช้อินเทอร์เน็ตเป็นเครื่องมือ และจะใช้การโจมตีแบบเน้นปริมาณมากกว่าคุณภาพ เช่น การถล่มเวปไซต์ด้วยการกด F5 เพื่อทำให้เวปไซต์นั้นล่มหรือการใช้ DDos ในการโจมตี

แฮกเกอร์อีกกลุ่มหนุ่งที่มีความเชื่อมโยงกับแฮกเกอร์กลุ่มนี้เรียกว่า Cybervigilantes หรือภาษาไทยสามารถอธิบายว่าเป็นการกระทำของการดำเนินศาลเตี้ยกิจกรรม

ผ่านทางอินเทอร์เน็ต ครอบคลุมไปถึงความตื่นตัวต่อการหลอกลวงอาชญากรรมและพฤติกรรมที่ไม่เกี่ยวข้องกับอินเทอร์เน็ตและกลุ่มนี้จะมีความพิเศษคือเป็น Anonymous กลุ่ม ที่ไร้ตัวตนหรือ Anonymous กลุ่มนี้จะมีการกระทำที่มีจุดม่งหมายทางการเมืองและต่อต้านอาชญากรรมแต่ในอีกด้านหนึ่งบางกลุ่มอาจจะมีการกระทำที่ผิดกฎหมาย เช่น การฟอกเงินเป็นหนึ่งในนั้น และหนึ่งในนั้นคือวิธีการที่กลุ่ม Cybervigilantes กระทำเป็นวิธีการที่ละเมิดความเป็นส่วนตัวของเป้าหมายซึ่งผิดต่อกฎหมายคุ้มครองสิทธิและเสรีภาพ และในที่สุดแล้วในกลุ่มของแฮกเกอร์มือใหม่ก็ยังขาดแรงจูงใจทางการเมืองที่ชัดเจนที่จะจัดกลุ่มได้ว่าเป็นผู้ก่อการร้าย

ขอบเขตที่เพิ่มขึ้นของความเข้าใจสื่อและการโต้ตอบทางออนไลน์ทำให้ผู้เฝ้าระวังใช้วิธีการที่เฉพาะเจาะจงกับอินเทอร์เน็ตเพื่อกระจายความยุติธรรมให้กับฝ่ายที่พวกเขาคิดว่าทุจริต แต่ไม่ได้ก่ออาชญากรรมอย่างเป็นทางการหรือไม่ได้รับการรับผิดชอบจากกระบวนการยุติธรรมทางอาญา

5.3 ผู้กระทำที่ไม่ใช่รัฐแต่มีเป้าหมายทางการเมือง (Nonstate actors with a Political Agenda)

ผู้กระทำที่ไม่ใช่รัฐอาจเป็นเรื่องง่ายที่จะเข้าถึงระบบโครงข่ายอินเทอร์เน็ตของแต่ละประเทศเพราะพวกเขาเหล่านั้นเปรียบเสมือนกลุ่มที่ไร้ตัวตนโดยใช้เครื่องมือทางไซเบอร์ต่อสู้เพื่อเป้าหมายทางการเมืองของรัฐนั้น บางครั้งการกระทำเหล่านี้อาจไม่ก่อให้เกิดอันตรายต่อประชาชนผู้บริสุทธิ์แต่เป็นการข่มขู่รัฐเสียมากกว่า การใช้เครื่องมือทางไซเบอร์ของคนกลุ่มนี้เป็นเรื่องง่ายและช่วยสนับสนุนให้การกระทำมุ่งสู่เป้าหมายได้เร็วขึ้น เพราะเครื่องมือทางไซเบอร์สามารถหาได้ง่ายและไม่ได้ใช้งบประมาณในการทำมากแต่สามารถทำให้เกิดผลที่หลากหลายไม่ว่าจะเป็นการขยายกลุ่มชายขอบ ชนกลุ่มน้อยให้มีพลังมากขึ้น และสามารถนำไปสู่การปฏิวัติทางการเมืองได้ การกระทำของคนกลุ่มนี้เริ่มตั้งแต่การใช้ความรู้ในเชิงสันติวิธีที่จะเผชิญหน้าและถอนรากถอนโคนและสร้างกองกำลังเป็นของตนเอง กลุ่มแรกที่ถูกยกขึ้นมาเป็นตัวอย่างในการเล่าถึงผู้กระทำที่ไม่ใช่รัฐ คือ Mexico's Zapatista กลุ่มชนที่เคลื่อนไหวโดยปฏิเสธการใช้ความรุนแรงแต่ใช้อินเทอร์เน็ตในการแสดงตัวตน บางครั้งสมาชิกในกลุ่มจะใช้ความสามารถทางด้านเทคโนโลยีสารสนเทศโจมตีเทคโนโลยีสารสนเทศของฝ่ายตรงข้าม ยกตัวอย่างเช่น การใช้เวปไซต์เพื่อทำให้รัฐเสียหาย หรือการเข้าไปทำลายเวปไซต์ของรัฐโดยการเปลี่ยนเนื้อหา ข้อมูล การกระทำเหล่านี้ไม่ได้ถูกเปรียบเทียบว่าเป็นการกรำทำที่ป่าเถื่อนแต่อย่างใด

ดังนั้นการใช้ช่องทางทางไซเบอร์เป็นเครื่องมือในทางการเมืองมีทั้งข้อดีและข้อเสีย เมื่อ server ถูกแฮก เวปไซต์ถูกโจมตี การให้บริการของรัฐเสียหายไม่สามารถใช้งานได้ หรือการจู่โจมแบบไม่ทันตั้งตัวของผู้ที่มีอุดมการณ์ทางการเมืองที่แตกต่าง การกระทำเหล่านี้จะถูกเรียกว่าเป็นการแฮก หรือ Hacktivism แต่หากการกระทำนั้นเป็นการสร้างข่าวปลอมชวนเชื่อประชาชนให้มี

ความเชื่อต่างจากรัฐ การกระทำเหล่านี้จะถูกเรียกว่า Webtism หากการกระทำของแฮกเกอร์นั้นเป็นการกระทำที่เชื่อว่าเกิดขึ้นเพราะรักชาติ แฮกเกอร์เหล่าจะใช้วิธีที่หลากหลายเช่นการใช้เทคนิคกองโจรหรือ guerilla และอีกวิธีหนึ่งคือการการก่อวินาศกรรม หรือ sabotage ในโลกไซเบอร์

ส่วนในการรับมือของภาครัฐนั้นสามารถทำได้ด้วยการจับกุมเป็นไปตามกฎหมายให้ให้ผู้กระทำผิดนั้นมาแลกเปลี่ยนความรู้ กลยุทธ์ หรือยุทธวิธีต่างๆ ที่ผู้กระทำผิดนำมาใช้เพื่อมาป้องกันประเทศของตน ในกรณีนี้เหตุการณ์การจู่โจมที่เกิดขึ้น ณ ประเทศเอสโตเนียสามารถยกเป็นเสหนึ่งที่สามารถเรียกว่าการก่อการร้ายได้

5.4 ผู้จัดการดูแลระบบและบริษัทรักษาความปลอดภัย (System Administrators and Cybersecurity Companies)

ผู้จัดการดูแลระบบคือผู้ที่มีความรู้ทางด้านเทคนิคที่จะคอยดูแลรักษาระบบเทคโนโลยีสารสนเทศ เช่น เว็ปไซต์ที่อยู่ภายใต้โครงข่ายอินเทอร์เน็ตทั้งหมด งานที่รับผิดชอบหลักคือการดูแลให้ระบบสามารถให้บริการได้และอยู่ภายใต้การควบคุม ภารกิจของงานขึ้นอยู่กับขนาดของธุรกิจนั้นๆ และงบประมาณที่ได้รับ รวมไปถึงความสำคัญของระบบไซเบอร์ที่จะต้องดูแล พวกเขาจะต้องสามารถสังเกตเห็นความผิดปกติหรือการรุกรานทางระบบได้ก่อนและในสายงานเหล่านี้ของพวกเขาจะต้องสามารถคาดการและจัดการการบุกรุกทางระบบที่เกิดขึ้นได้

ผู้ที่ปฏิบัติงานที่นี่นั้นจะต้องมีความรู้ความเชี่ยวชาญทางด้านไซเบอร์โดยเฉพาะซึ่งจะต้องมีชื่อเสียงเป็นที่ยอมรับหรือมีประกาศนียบัตรที่สามารถยืนยันได้จริงในสังคมออนไลน์ ถึงแม้ว่าจะไม่มีสนธิสัญญาระหว่างประเทศที่เป็นทางการถึงการร่วมมือกันในพื้นที่ทางไซเบอร์ถึงเรื่องการแลกเปลี่ยนผู้เชี่ยวชาญ แต่สำหรับในอนาคตแล้วการแลกเปลี่ยนผู้เชี่ยวชาญทางไซเบอร์จะช่วยปัญหาในการประสานงานระหว่างบุคคลที่เชี่ยวชาญและลดการเกิดภัยคุกคามทางไซเบอร์ได้

ผู้จัดการดูแลระบบนั้นจะได้รับการสนับสนุนจากศูนย์รักษาความปลอดภัยทางไซเบอร์ มีหน้าที่ดูแลควบคุมระบบทางไซเบอร์และตั้งรับโดยโปรแกรมป้องกันไวรัส โปรแกรมรักษาความปลอดภัยในซอฟแวร์ firewalls และระบบเตือนภัยต่างๆเกี่ยวกับภัยคุกคามทางไซเบอร์ และสำหรับในปัจจุบันนี้กระแสที่กล่าวมานั้นเรียกว่า “honey pots” ที่จะช่วยรวบรวมข้อมูลที่อัพเดตเกี่ยวกับโปรแกรม malicious และกิจกรรมต่างๆผ่านตอบโต้ต่อการโจมตีที่จะมาโจมที่ลูกค้าของเขา

5.5 ผู้ก่ออาชญากรรมทางไซเบอร์ (Cybercriminals)

อาชญากรคอมพิวเตอร์หรืออาชญากรทางไซเบอร์ตระหนักได้ว่าโครงข่ายทางอินเทอร์เน็ตหรือพื้นที่ทางไซเบอร์เป็นเรื่องมือที่สำคัญที่จะใช้แสวงหาผลประโยชน์ กรณีแรกของการก่ออาชญากรรมทางทางไซเบอร์ในช่วงปี 1987 โดยร้อยละ 5 ของเหยื่อจะเป็นองค์กรและบริษัท

ต่างๆ โดยหลังจากนั้นในช่วง 1990 มีผู้ใช้อินเทอร์เน็ตเพิ่มขึ้นกว่าล้านคน และมีรัฐบาลที่สนับสนุนการเติบโตของ e-commerce และการถ่ายโอนข้อมูลทางอินเทอร์เน็ต อาชญากรเริ่มโดยการส่งข้อความปลอมให้กับเหยื่อยเพื่อที่จะขโมยข้อมูลของบัตรเครดิต หรือการทำธุรกรรมการเงินกับธนาคารหรือการขโมยอัตลักษณ์ส่วนบุคคล แต่ในความเป็นจริงแล้วแฮกเกอร์จะมีแนวคิดว่าตนแตกต่างกับอาชญากรไซเบอร์ทั่วไป กล่าวคือ แฮกเกอร์ไม่ได้มีจุดประสงค์ที่เข้าไปตักตวงผลประโยชน์หรือตั้งใจทำเพื่อก่อให้เกิดความเสียหายจริง แต่อาชญากรคอมพิวเตอร์หรืออาชญากรทางไซเบอร์มีวัตถุประสงค์เหล่านั้นที่ใช้อุปกรณ์ทางไซเบอร์เดียวกันตั้งใจที่จะตักตวงผลประโยชน์จากเหยื่อ

ในทางกลับกันกลับมีกลุ่มแฮกเกอร์ที่พยายามก่อตั้งองค์กรเป็นของตนเองเพื่อรวบรวมผู้ที่มีความรู้ทางไซเบอร์มาอยู่ด้วยกันและร่วมกันก่ออาชญากรรมทางอินเทอร์เน็ต ไม่ว่าจะเป็นการขโมยขโมยอัตลักษณ์ส่วน การปล่อยไวรัสเพื่อให้เกิดความเสียหาย การขู่เรียกค่าไถ่ และตัวอย่างที่สำคัญที่สามารถเห็นได้คือ กลุ่ม Russian Business Network (RBN) ที่เป็นองค์กรขนาดใหญ่ทางไซเบอร์และมีจุดประสงค์ที่จะรุกรานหรือจู่โจมระบบเพื่อผลประโยชน์ของตนเอง หรือมีอำนาจขนาดที่สามารถควบคุมเทคโนโลยีสารสนเทศของประเทศได้ ดังนั้นจึงมีข้อสงสัยว่ากลุ่ม RBN นั้นมีจุดประสงค์ทางการเมืองและมีนักการเมืองสนับสนุนอยู่เบื้องหลังจนทำให้สมาชิกที่อยู่ใน RBN ไม่โดนจับกุม ตัวอย่างในการจู่โจมส่วนใหญ่จะเป็นการโจมตีสาธารณูปโภคสำคัญของประเทศและมีบริษัทเอกชนสนับสนุนด้านการเงินอยู่ หรือบางครั้งที่รัฐเป็นผู้สนับสนุนกลุ่มเหล่านี้ทางด้านการเงินเพราะรัฐและกลุ่มแฮกเกอร์มีผลประโยชน์ร่วมกัน หรือบางครั้งข้อขัดแย้งที่เกิดขึ้นอาจจะไม่ใช่ในรูปของการจู่โจมระบบเสมอไปแต่เป็นการใช้ความสัมพันธ์ทางการทูตเพื่อเจรจาต่อรองแทน

5.6 บริษัทเทคโนโลยีสารสนเทศ (ICT companies)

ตั้งแต่ช่องทางทางไซเบอร์สามารถถูกจับจองผ่านบริษัทเอกชนได้ การใช้ช่องทางเหล่านี้จึงทำให้เกิดอำนาจระหว่างบริษัทเอกชนและรัฐบาล ช่องทางทางไซเบอร์ให้โอกาสบริษัทstart-up ในการร่วมมือกับตลาดโลกเพื่อแลกเปลี่ยนความรู้กับนานาชาติผ่านอินเทอร์เน็ตซึ่งไม่จำเป็นต้องใช้งบประมาณมาก ซึ่งบริษัทเหล่านี้สามารถทำการค้าโดยไม่ต้องขึ้นอยู่กับกฎหมายระหว่างประเทศ สาเหตุนี้จึงเป็นสาเหตุสำคัญที่ทำให้บริษัทเหล่านี้มีอำนาจเหนือรัฐในการควบคุมนโยบายของรัฐ ยกตัวอย่าง เช่น Facebook Google YouTube หรือ Twitter ซึ่งเป็นบริษัทระดับชาติที่ยิ่งใหญ่และสามารถสร้างเครื่องมือทางเทคนิค เช่น การเป็นเทียบเสมือนการสร้าง กำแพงเมืองจีนที่เป็นที่ป้องกันภัยคุกคามได้ หรือ “Great Firewall of China”

5.7 ผู้กระทำที่เป็นรัฐและทีมรับมือภัยคุกคามฉุกเฉินทางไซเบอร์ (State Actors and CERTs)

ตั้งแต่กระแสการจู่โจมทางไซเบอร์เป็นปัญหาของรัฐตลอดมา รัฐได้นำกฎหมายซึ่งมีความสอดคล้องกับกฎหมายระหว่างประเทศมาบังคับใช้และมีการอบรมเจ้าหน้าผู้มี

อำนาจให้มีความรู้ทางด้านการรักษาความปลอดภัยทางไซเบอร์ แต่เนื่องจากระดับความรุนแรงของอาชญากรรมไซเบอร์ยังน้อยกว่าปริมาณที่เกิดขึ้นในสังคม การจับกุมผู้กระทำจึงยังมีน้อย แต่ในเมื่อรัฐได้ตระหนักถึงผลที่จะเกิดขึ้นและความรุนแรงที่จะมีมากขึ้นในอนาคต รัฐจึงสร้างกรอบแนวคิดทางด้านกฎหมายให้มีความรอบคอบและครอบคลุมมากขึ้น กฎหมายที่สร้างขึ้นนั้นมุ่งเป้าครอบคลุมไปถึงการจับกุมเชิงปัจเจกและและผู้กระทำที่ไม่ใช่รัฐ แต่อย่างไรก็ตามรัฐยังไม่สามารถแบ่งบทบาทของหน่วยงานที่นำกฎหมายไปปฏิบัติใช้ หน่วยข่าวกรองต่างๆ และกองทัพที่จะจัดการกับภัยคุมคามเหล่านี้ได้ เช่น หน่วยงานใดควรรับมือภัยคุกคามประเภทใดก่อนถึงจะสามารถสั่งการเจ้าหน้าที่ให้มาจับกุมได้ นอกจากนั้นรัฐยังไม่ทราบถึงจุดประสงค์ของการจู่โจมไซเบอร์ จึงไม่สามารถที่จะวิเคราะห์และสั่งการหน่วยงานได้ทัน เพราะฉะนั้น รัฐจำเป็นจะต้องแบ่งความรับผิดชอบให้กองทัพรับผิดชอบในส่วน การก่อการร้ายไซเบอร์ หรือ สงครามไซเบอร์ และแบ่งหน้าที่ให้กับหน่วยงานที่มีหน้าที่บังคับใช้กฎหมายมีหน้าที่ในการร่างนโยบายความมั่นคงแห่งชาติทางไซเบอร์ ส่วนอำนาจทางนิติองค์กรจะต้องทำข้อตกลงกับองค์กรระหว่างประเทศเพื่อสามารถแลกเปลี่ยนความรู้และอำนาจทางศาลได้ และหน่วยที่พร้อมรับมือกับเหตุการณ์ที่เกิดขึ้นทางไซเบอร์แบบฉุกเฉิน หรือที่เรียกว่า CERTs ซึ่งส่วนใหญ่มาจากภาคเอกชน ผู้เชี่ยวชาญจากอุตสาหกรรมไซเบอร์และมหาวิทยาลัยต่างๆ โดยหน้าที่ที่สำคัญของCERTsคือ ดูแลควบคุม ส่งสัญญาณเตือนหน่วยงานต่างหากเกิดภัยคุกคาม ให้ความช่วยเหลือต่างๆ และประสานงานร่วมมือกับหน่วยงานที่ต้องเผชิญกับปัญหาการจู่โจม แต่ปัญหาหนึ่งของการรุกรานทางไซเบอร์ไม่เพียงแค่การแบ่งแยกประเภทของการจู่โจม แต่เป็นปัญหาของการจู่โจมอาชญกรรมไซเบอร์อีกประการหนึ่งก็คือการใช้อำนาจทางศาลระหว่างประเทศซึ่งยังไม่เคยเกิดขึ้นในพื้นที่ ทางไซเบอร์ซึ่งเป็นพื้นที่ที่ไร้พรมแดน การขาดความรู้ของเจ้าหน้าที่ หรือการขาดการชักจูงผู้เชี่ยวชาญที่มีความรู้เข้ามาเป็นส่วนหนึ่งของทีม CERTs ด้วยเงินเดือนที่น้อยกว่าบริษัทเอกชนจึงทำให้พวกเขาเหล่านั้นเลือกที่จะไม่ทำงานกับรภาครัฐ ดังนั้น รัฐจึงต้องการความร่วมมือจากภาคเอกชนเพื่อเข้ามาทำงานให้ภาครัฐ

5.8 สื่อกระแสหลัก (The Mass Media)

สื่อกระแสหลักมีบทบาทสำคัญสำหรับการสร้างความตระหนักรู้ของการจู่โจมทางไซเบอร์ แต่ในปัจจุบันนี้การสร้างความตระหนักรู้ทางด้านนี้ยังไม่ใช่ประเด็นหลักหรือสำคัญมากนัก แต่อย่างไรก็ตามในทุกวันนี้ประชาชนยังต้องเผชิญปัญหาการหลอกลวงทางอินเทอร์เน็ตและเป็นข่าวใหญ่เมื่อรัฐบาลของสหรัฐนำประเด็นนี้มาเป็นวาระสำคัญในการกำหนดนโยบาย

แต่อย่างไรก็ตามสื่อกระแสหลักมีบทบาทสำคัญที่จะช่วยลดความรุนแรงปละช่วยโปรโหมดความรู้ให้กับประชาชน ด้วยเหตุผลหลายประการ เช่น สื่อกระแสกหลักสามารถเปิดเผยความลับ ความซับซ้อนของการรักษาความมั่นคงปลอดภัยไซเบอร์ได้ เพราะฉะนั้นแฮกเกอร์จะไม่ปฏิบัติการสำเร็จได้หากสื่อกระแสหลักคอยจับตาในประเด็นนี้ นอกจากนี้สื่อกระแสหลักจะ

นำเสนอเบื้อหลังทางการเมืองหรือการสื่อสารระหว่างประเทศที่จะเป็นเป้าหมายทำให้เกิดความตึงเครียดทางการเมืองหรือการทูตของทั้ง 2 ประเทศ และสุดท้ายแล้วนั้นสื่อกระแสหลักสามารถส่งอิทธิพลต่อสังคมได้อย่างดีไม่ว่าจะเป็นตัวเลือก พฤติกรรมของประชาชนที่ได้รับข้อมูลข่าวสาร หากสื่อสูญเสียความมั่นใจในการเป็นผู้นำทางเทคโนโลยีของประเทศแล้วจะส่งผลกระทบต่อเศรษฐกิจของประเทศอย่างหลีกเลี่ยงไม่ได้

6. เครื่องมือ (Tool)

เครื่องมือที่ใช้ในการจู่โจมในโลกของไซเบอร์นั้นมีหลายประเภทและแต่ละประเภทมีความรุนแรงแตกต่างกันไปตามระดับความซับซ้อนของเครื่องมือนั้นๆ และขึ้นอยู่กับทักษะที่มีของผู้จู่โจมและจุดประสงค์ในการใช้ ได้แก่

6.1 ไวรัส และ วอร์ม (Virus and Worms)

ไวรัสในคอมพิวเตอร์ทำงานเหมือนกับไวรัสที่ทำลายในตัวมนุษย์ผ่านการแฝงตัวเข้าไปในตัวมนุษย์ เข้าไปในอวัยวะสำคัญและทำให้ทำให้อวัยวะร่างกายส่วนนั้นเสียหายเพราะการกัดกินจากไวรัส เช่นเดียวกับไวรัสในคอมพิวเตอร์ ไวรัส จะติดเข้าไปในเครื่องคอมพิวเตอร์เหมือนกับการติดเชื่อไวรัส โปรแกรมหรือไฟล์ที่เป็นอันตรายจะทำให้เกิดความเสียหายและแพร่กระจายไปตามส่วนสำคัญอื่นๆของคอมพิวเตอร์จนทำให้คอมพิวเตอร์หรือระบบนั้นไม่สามารถใช้งานได้ หรือทำลายและลบข้อมูลในเครื่องนั้น ส่วนวอร์มนั้นจะเป็นไวรัสชนิดหนึ่งที่ยึดกับส่วนใดส่วนหนึ่งของระบบคอมพิวเตอร์ วอร์มสร้างมาจากโปรแกรมเล็กๆที่สามารถหลบหลีกการจับได้ วอร์มจะไม่สามารถทำงานได้ถ้าไม่มีกลไกในการที่เปิดระบบจากผู้สั่งการ วอร์มจะสามารถแพร่กระจายเหมือนโรคระบาดและจะทำลายระบบผ่านซอร์ฟแวร์ผ่านทางอีเมล์ วอร์มในปัจจุบันนั้นมีความสามารถสูงขึ้นกว่าวอร์มรุ่นเก่า เช่น วอร์มสามารถแพร่กระจายได้ง่ายแม้กระทั่งการเข้าเวปไซต์ต่าง ๆ วอร์มจะเข้าไปยังเวปไซต์หลักและจะคอยโจมตีผู้ที่เข้ามาเข้าเวปไซต์นั้น ยิ่งมีจำนวนผู้ใช้อินเทอร์เน็ตมากเท่าไหร่จะยิ่งทำให้เพิ่มการแพร่กระจายของวอร์มมากเท่านั้น

6.2 แบคดอร์ (Backdoor): Trojans and Rootkits

แบคดอร์ คือ รูรั่วในระบบซอร์ฟแวร์ที่ผู้สร้างจงใจสร้างเนื่องจากผู้สร้างต้องการให้ซอฟแวร์คอยส่งข้อมูลจากอุปกรณ์ที่มันติดตั้งอยู่กลับไปหาตน แต่กลับเป็นการเปิดโอกาสให้ผู้โจมตีเข้ามาในระบบได้เพื่อเอาข้อมูลหรือทำลายข้อมูล เมื่อนั้นแฮกเกอร์จะใช้วิธีเข้าประตูหลังเพื่อนำ ไวรัสและวอร์ม เข้าไปแพร่ระบายในระบบ แฮกเกอร์ก็สามารถใช้ Malware, Trojans, Rootkits (มัลแวร์ โทรจัน หรือชุดโปรแกรมที่สามารถซ่อนตัวอยู่ในคอมพิวเตอร์) เข้าไปแสวงหาประโยชน์ หรือใช้ Rootkit ในการซ่อน Malware ถูกออกแบบมาให้ฝังตัวอยู่ในชั้นของระบบคอมพิวเตอร์ที่โปรแกรมป้องกันไวรัสทั่วๆไปตรวจพบได้ยาก เมื่อคอมพิวเตอร์โดนแบค ดอร์ ติดเข้าในเครื่องแล้ว ผู้จู่โจมจะสามารถเข้ามาขโมยข้อมูลต่าง ๆของเครื่องได้ โดยที่เจ้าของระบบยังไม่ทันรู้ตัว การทำงานของแบ

คดอร์ จะทำงานทุกครั้งโดยเริ่มตั้งแต่เปิดเครื่องคอมพิวเตอร์และเมื่อขโมยข้อมูลสำเร็จแล้วนั้น ข้อมูลหรือหลักฐานต่าง ๆ สามารถถูกทำลายไม่ให้เหลือหลักฐานได้ และเหตุผลทั้งหมดนี้จึงเป็นสาเหตุให้ผู้ที่เป็นเจ้าของระบบไม่รู้ตัว

6.3 บ็อตเน็ต (Botnets)

บ็อต หรือ Bot มาจากคำว่า Robots ซึ่งเป็นชนิดหนึ่งของ Trojans โดยหากคอมพิวเตอร์ติดบ็อตเน็ตแล้ว นั่นแสดงว่าคอมพิวเตอร์ได้ติดมัลแวร์ หลังจากนั้นบอทจะสามารถติดต่อกับเซิร์ฟเวอร์ได้ทั้งในระยะไกลและระยะใกล้ และติดต่อกับบอทอื่นๆ ที่อยู่รอบๆได้เช่นกัน สาเหตุนี้ทำให้คอมพิวเตอร์ถูกควบคุมโดยผู้โจมตีเมื่อผู้โจมตีสามารถยึดครองระบบคอมพิวเตอร์และสั่งการระบบได้ก็จะสามารถโจมตีระบบอื่นๆ ได้เช่นกันซึ่งเป็นการเปลี่ยนคอมพิวเตอร์ทั่วไปให้เป็น “ซอมบี้” ที่ได้รับคำสั่งจากระยะไกลโดยไม่ได้รับความยินยอมจากเจ้าของระบบคอมพิวเตอร์ ในปี 2009 The Georgia Tech Information Security Center ประเมินว่า บ็อต กว่า 15% ของคอมพิวเตอร์ออนไลน์จะสามารถแปรเปลี่ยนไปเป็นกองทัพในสงครามไซเบอร์ได้ บ็อต สามารถสร้างความซับซ้อนได้ด้วยตนเอง สามารถบุกรุกระบบความมั่นคงทางไซเบอร์ และสามารถทำลายตัวเองเหมือนอาวุธนิวเคลียร์ ตัวอย่างการโจมตีที่สำคัญของ บ็อต คือ เมื่อปล่อย บ็อต ไว้ชั่วคราวเพียง 10 วันแต่ บ็อต สามารถเก็บข้อมูลได้มากกว่า 70 GB และสามารถเข้าถึงข้อมูลทางการเงินกว่า 8,310 บัญชี เข้าถึงบัตรเครดิตและเดบิตถึง 1,660 บัญชี และเข้าถึงข้อมูลผู้ใช้ถึง 297,962 คน (Kerschischnig, 2013: p. 106) (Kerschischnig, 2013, p. 106)

7. เทคนิค (Techniques)

เทคนิคที่จะกล่าวถึงนี้เปรียบเสมือนกลยุทธ์ในการโจมตีของผู้จู่โจมที่จะเลือกใช้อาวุธชนิดใดกับกลยุทธ์ใดในการโจมตี หรือวัตถุประสงค์และเป้าหมายในการโจมตีนั้นเป็นอย่างไรจึงจะเหมาะสมในการใช้วิธีเหล่านี้ ได้แก่

7.1 Distributed Denial-of-Service หรือ DoS Attacks

การโจมตีแบบนี้เป็นความพยายามที่จะทำให้เครื่องคอมพิวเตอร์หรือเครือข่ายอินเทอร์เน็ตสำหรับผู้ใช้ถูกทำลาย จนเป้าหมายไม่สามารถใช้บริการได้ เช่น ขัดขวางหรือชะลอการให้บริการของการเชื่อมโยงทางอินเทอร์เน็ต เป็นการโจมตีแบบกระจายทำให้ระบบนั้นไม่สามารถใช้ได้ชั่วคราว หรือทำให้ระบบนั้นช้าลง การโจมตีแบบนี้เคยเกิดขึ้นที่ประเทศไทย คือการกดโจมตีกระทรวงดิจิทัลโดยการกด F5 พร้อมกันหลาย ๆ เครื่องคอมพิวเตอร์จนทำให้เวปไซต์ของกระทรวงไม่สามารถใช้การได้ ThaiCERTs จึงต้องเข้าไปช่วยหยุดการโจมตีนี้

7.2 Infiltration หรือ เทคนิคการแทรกซึม

หากเปรียบเทียบกับสงครามในสนามรบรูปแบบเก่านั้นทหารจะใช้ยุทธวิธีการแทรกซึมที่มีขนาดเล็ก เคลื่อนตัวง่าย และสามารถรุกเข้าไปในพื้นที่ด้านของศัตรูโดยที่ศัตรูไม่รู้ตัว

และเลี่ยงที่จะเผชิญหน้าศัตรูเพื่อหลบหลีกการต่อสู้ที่ต้องทำให้เสียกำลังมาก และวางทัพหลังที่มีกองกำลังที่เข้มแข็งกว่าพร้อมอาวุธที่ครบมือเข้าไปทำลายศัตรู เช่นเดียวกันกับการแทรกซึมในระบบไซเบอร์ Infiltration เหมือนกับชิ้นส่วนเล็กๆของมัลแวร์ที่พยายามเข้าไปทำลายระบบคอมพิวเตอร์ของผู้ใช้โดยที่ผู้ใช้ไม่รู้ตัว Infiltration สามารถทำลานระบบทางกายภาพผ่านทางระบบซอฟแวร์นั้น ๆ เช่น การใช้ USB เสียบเข้าเครื่องคอมพิวเตอร์ ระบบสามารถถูกทำลายผ่าน Wi-fi หรือบางครั้งผ่านเป็นเพราะความไม่รอบคอมของผู้ใช้คอมพิวเตอร์ และยังมีอีกเทคนิคหนึ่งที่ไม่จำเป็นต้องใช้ Infiltration โดยตรง นั่นคือการขโมยข้อมูลจากผู้ใช้จากในถังขยะและเปลี่ยนหรือแทรกซึมไฟล์นั้นเพื่อเปิดโปงความลับของผู้ใช้งาน

อีกแง่หนึ่งของการใช้ Infiltration ในระยะไกลคือการแฮกระบบ Wi-fi ซึ่งมีมากมายหลายโดเมนในปัจจุบัน โดยเฉพาะการใช้ Wi-fi ในบ้าน และระบบ Wi-fi เหล่านั้นจะมีการป้องกันข้อมูลที่ต่ำ การแทรกซึมเข้าระบบ Wi-fi เหล่านี้จะมีประโยชน์ในสองแง่มุมคือจะสามารถเข้าได้ง่ายและจะไม่ทิ้งร่องรอยของผู้เข้าไป มากไปกว่านั้นแฮกเกอร์ยังใช้การแทรกซึมระบบจาก Wi-fi ส่วนบุคคลเข้าถึง Wi-fi ในระบบขแงบริษัทขนาดใหญ่หรือสามารถเข้าไปถึงภาครัฐได้ เทคนิคนี้เรียกว่า “dumpster diving” ยกตัวอย่าง เช่น ประเทสเยอรมันที่ถูกแฮกเกอร์ใช้วิธีแทรกซึมเข้าไปในระบบและควบคุมระบบการบินของสนามบินเยอรมัน สามารถสรุปได้ว่าการใช้ระบบ Wi-fi นั้นไม่ได้ปลอดภัยและกลับสร้างช่องโหว่มากมายให้กับแฮกเกอร์เพื่อเข้าแทรกซึมและโจมตี

7.3 Social Engineering หรือ วิศวกรรมสังคม

เหตุการณ์นี้จะเกิดขึ้นเมื่อปัจเจกบุคคลถูกหลอกลวงให้ป้อนข้อมูลสำคัญให้กับระบบ โดยผู้กระทำจะได้ประโยชน์จากข้อมูลเหล่านั้น ก่อนอื่นแล้วคำว่า วิศวกรรมสังคม นั้นหมายถึงการใช้วิธีทางจิตวิทยาแขนงหนึ่งมีเนื้อหาที่เป็นวิทยาศาสตร์อย่างมาก เกี่ยวกับ การรับรู้ข้อมูลของมนุษย์และการแสดงท่าทีต่อข้อมูลนั้น ซึ่งสามารถวิเคราะห์ด้วยสถิติและหาข้อสรุปด้วยวิธีทางวิทยาศาสตร์ได้ วิศวกรรมสังคมเกิดมาจากการนำเอาความรู้ทาง จิตวิทยา สังคมศาสตร์ รัฐศาสตร์ วิทยาศาสตร์คอมพิวเตอร์ และอีกหลายสิ่ง ซึ่งรวมไปถึงการศึกษา การออกแบบ การแก้ไข และการวางแผนพฤติกรรมมนุษย์ มาประยุกต์เข้าด้วยกัน การใช้ศาสตร์เหล่านี้จึงเป็นที่มาทำให้ผู้กระทำสามารถเข้าถึงและหลอกลวงผู้ใช้ได้ง่าย การทำให้ผู้ใช้นั้นเชื่อว่าข้อมูลที่ได้รับมานั้นน่าเชื่อถือ การส่งต่อข้อมูลเหล่านี้จะทำผ่านจาก email (phishing) ข้อความทางโทรศัพท์ (smishing) Voice-Over-IP-Services (vishing) โซเชียลมีเดียในปัจจุบันนั้นไม่ได้ช่วยป้องกันให้การหลอกลวงที่เกิดขึ้นมีน้อยลงมิหนำซ้ำกลับทำให้สถาการณ์เริ่มแย่ลง โดย BBC เผยแผ่ข้อมูลว่า การใช้บัญชีปลอมในโซเชียลมีเดียมีผลทำให้เกิดการลดความน่าเชื่อถือในโลกการค้า และแฮกเกอร์นั้นยังมุ่งเป้าไปยังกองทัพของรัฐนั้น ๆ ได้และเป็นสาเหตุให้เกิดการเพิ่มรุนแรงขึ้นมากอีกด้วย

7.4 การเข้าสู่ข้อมูล การสอดแนม และการรวบรวมข้อมูล Probing, Sniffing และ Mapping

การสอดแนม (Sniffing) หมายถึง การดักเพื่อแอบดูข้อมูลซึ่งจัดอยู่ในประเภทการดจมตีแบบสอดแนม ไม่ได้ใช้ความรุนแรงในการโจมตีหรือเป็นการโจมตีแบบพาสซีฟ (Passive) การกระทำเหล่านี้จะไม่เปลี่ยนแปลงหรือแก้ไขข้อมูล ตัวอย่างเช่น การดักอ่านข้อมูลในระหว่างการอ่านไฟล์ที่เก็บอยู่ในระบบเป็นวิธีเฝ้าดูข้อมูลบนเครือข่าย การเข้าระบบการรักษาข้อมูลผ่านรหัสจึงเป็นการเฝ้าระวังได้ เริ่มต้นด้วยแฮกเกอร์เฝ้าระวังประตูในการจะเข้าไปในระบบ ถ้าประตูระบบนั้นปิดอยู่ก็จะใช้วิธี การสอดแนม (Sniffing) หลังจากนั้นแฮกเกอร์จะพยายามเปิดประตูและพยายามมองให้เห็นว่ามีข้อมูลอะไรอยู่ในนั้นบ้าง (Probing) เมื่อประตูหลายบานถูกเปิดออกแฮกเกอร์จะทำการเชื่อมโยงข้อมูลทางหมดเข้าด้วยกัน (Mapping)

7.5 Anonymization Techniques หรือวิธีเทคนิคในการทำให้ไม่มีตัวตน

สิ่งที่ยากที่สุดในการควบคุมการบุกรุกในระบบไซเบอร์คือการสร้างความไร้ตัวตน ในที่นี้การใช้เทคนิคไร้ตัวตนนั้นจะเป็นกลวิธีที่ทำให้ผู้กระทำสารมารถหลบเลี่ยงการติดตามได้อย่างแนบเนียนมากขึ้น เช่น The Onion Router (TOR) ที่เป็นพื้นที่ให้เหล่าแฮกเกอร์สามารถใช้พื้นที่ได้อย่างอิสระโดยปราศจากความเสี่ยงในการถูกจับได้ The Onion Routerสามารถสร้างระบบนิรนามได้มากถึง 30,000 ระบบหรือคิดเป็น 3.4% ของเครือข่ายทางอินเทอร์เน็ต ระบบนี้สามารถถูกสกัดกั้นหรือยับยั้งได้ในประเทศที่มีการเมืองแบบอำนาจนิยามหรือเป็นรัฐบาลที่มีความเด็ดขาดโดยการใช้ อินเทอร์เน็ตที่ได้มาจากภาครัฐเท่านั้น แต่อย่างไรก็ตามสำหรับประเทศโลกเสรี การใช้เทคนิคนิรนามสามารถทำได้ง่ายเช่นการกระโดดไปมาระหว่างช่องทางในอินเทอร์เน็ต (hop) และการสร้างสถานที่ตั้งให้ตนเองเปรียบเสมือนตัวแทน proxies) ที่ไม่ใช่ตนให้ผู้ถูกกระทำเกิดความสับสน

โดยสรุปแล้วการจะเลือกใช้เทคนิคหรืออาวุธชนิดใดนั้นขึ้นอยู่กับความถนัดของผู้กระทำ วัตถุประสงค์ และเป้าหมายในการกระทำ แต่เทคนิคเหล่านี้จะมีการพัฒนาความซับซ้อนและมีประสิทธิภาพไปเรื่อยจนเปรียบเสมือนว่ารัฐกำลังตามหลักแฮกเกอร์ไปทุกๆหนึ่งก้าว เพราะฉะนั้นการเรียนรู้ที่จะแยกแยะอาวุธและเทคนิคในการใช้เพื่อจุดประสงค์ใดเป็นเรื่องสำคัญที่จะเข้าใจการกระทำของแฮกเกอร์ ดังนั้นแล้วนอกจากจะต้องศึกษานโยบาย หรือเทคโนโลยีแล้ว ยังต้องศึกษาถึงจิตวิทยาของแฮกเกอร์หรือพฤติกรรมของมนุษย์ในการเลือกกระทำสิ่งเหล่านี้ด้วย

4.6 การคาดการณ์สถานการณ์ที่จะเกิดขึ้นกับประเทศไทยโดยใช้โมเดลจากนานาชาติ

การจู่โจมทางไซเบอร์มีประวัติอย่างยาวนานโดยครั้งแรกที่สามารถเรียกความสนใจได้อย่างดีคือเมื่อกลางทศวรรษที่ 1990 เมื่ออินเทอร์เริ่มเติบโตและขยายพื้นที่การใช้เครือข่ายไปทั่วโลก มีหลาย

ปฏิบัติการที่เป็นสัญญาณว่าอินเทอร์เริ่มกลายเป็นเครื่องมือที่มีความร้ายแรงในอนาคต เช่น ปฏิบัติการ Moonlight Maze Solar Sunrise และ Rome Lab ที่ถือเป็นปฏิบัติระดับชาติในสงครามอ่าว 1990-1991 ที่พยายามแสดงให้เห็นแสงยานุภาพของความก้าวหน้าทาเทคโนโลยีทางทหาร เช่น Global Positioning Systems (GPS) ที่สามารถแสดงตำแหน่งของผู้ที่เราต้องการจะติดตามได้ แต่ในขณะนั้นส่วนใหญ่จะเป็นการต่อสู้แบบดั้งเดิม สำหรับการแฮกครั้งแรกเกิดขึ้นในสงคราม Kosovo ในปี 1999 สหรัฐฯเริ่มสงครามไซเบอร์เพื่อยับยั้งการสนับสนุนทางการเงินของเซอร์เบีย และในปี 2003 สหรัฐฯก็พยายามรุกรานอิรักและยับยั้งการสนับสนุนหรือตัดช่องทางทางการเงินของอิรักโดยเครื่องมือทางไซเบอร์อีกครั้ง แต่มีจุดมุ่งหมายน้อยนักที่จะโจตี ICT Infrastructure โครงสร้างพื้นฐานสารสนเทศ และการก่อการร้ายส่วนมากยังคงเป็นในรูปแบบเดิมเพราะยังไม่มีวิธีที่จะใช้เทคโนโลยีเข้าถึงในระบบของเทคโนโลยีระดับประเทศได้ (Karatzogianni, 2009)

ต่อมาในปี 2001 สหรัฐอเมริการเริ่มสงครามไซเบอร์กับประเทศจีนโดยการใช้ DoS สายลับของสหรัฐในอยู่ในประเทศจีนเผชิญหน้ากับอิสราเอลและปาเลสไตน์ การตอบโต้ครั้งใหญ่ของจีนที่มีต่อสหรัฐคือ Titan Rain สามารถสืบได้ว่าเป็นความพยายามของประเทศจีน แต่แฮกเกอร์ของประเทศจีนนั้นยังมีความสามารถไม่พอจึงทำปฏิบัติการดจมตีไม่สำเร็จและทิ้งร่องรอยว้ายโดยไม่ทราบว่าฝีมือคนที่ทำนั้นเป็นรัฐเองหรือตัวแทนที่ไม่ใช่รัฐ หลังจากนั้นเป็นต้นมาการถกเถียงเรื่องจุดมุ่งหมายทางการเมืองในการใช้ไซเบอร์เป็นเครื่องมือจึงเริ่มต้นขึ้นและเป็นหลักในการใช้วิเคราะห์ในการก่อการร้ายไซเบอร์ (Jones, 2005)

ประเทศไทยล้วนมีประสบการณ์ในการโดยแฮก การจูโจมแบบ DoS การโจมตีทางระบบการเงินการโจมตีเปลี่ยนแปลงข้อมูลหน้าเว็ปไซต์ หรือการเรียกค่าไถ่เพื่อแลกกับข้อมูล แต่อย่างไรก็ตามการโจมตีเหล่านี้ยังคงเป็นในระดับที่มีความเสียหายเล็กน้อยและไม่รุนแรง จึงไม่สามารถที่จะเรียกได้ว่าเป็นการก่อการร้ายทางไซเบอร์เบอร์ได้ ในส่วนนี้ผู้วิจัยจะนำโมเดลการเกิดขึ้นของการโจมตีทางไซเบอร์ของแต่ละประเทศที่เคยเกิดขึ้นและมีแนวโน้มที่จะเกิดกับประเทศไทยมาอธิบาย ตามลำดับดังนี้

1. สงครามไซเบอร์ Estonia 2007

สงครามไซเบอร์ที่เกิดขึ้นโดยการใช้ Botnet ในการโจมตีหน่วยงานโครงสร้างพื้นฐานสำคัญทั้งหมดของประเทศ Estonia ซึ่งประเทศนี้เป็นประเทศที่ระบบส่วนใหญ่พึ่งพิงกับอินเทอร์เน็ตและเทคโนโลยี การดจมตีครั้งนี้ทำให้ทั้งประเทศไม่สามารถใช้งานสาธารณูโภคทางไฟฟ้า การประปา การติดต่อสื่อสาร หรือการเดินทางต่างๆ ได้เลย CERT ของประเทศ Estonia ไม่สามารถี่จะควบคุมสถานการณ์ได้นวันแรก แต่อย่างไรก็ตาม CERT ได้ขอความช่วยเหลือจาก CEO ของ Netnod ในการช่วยลดความรุนแรงของการโจมตี ต่อมาภายในสองอาทิตย์การจู่โจมก็ได้สงบไป และสามารถสืบได้ว่าเป็นเพราะรัฐบาลรัสเซียที่พยายามจู่โจมแต่ก็ไม่สามารถหาความจริงหรือวัตุประสงค์ที่แท้จริงได้ การ

เกิดเหตุการณ์ครั้งนี้ทำให้ องค์กร NATO เคลื่อนไหวในกิจกรรมสร้างความมั่นคงปลอดภัยทางไซแบอร์ให้มีความเข้มแข็งมากกว่านี้ (Karatzogianni, 2009)

2. สิ่งที่ประเทศไทยสามารถเรียนรู้จากเหตุการณ์นี้

ประเทศไทยจะต้องมีทีม CERT ที่แข็งแรงและว่องไวต่อการจับตาความเคลื่อนไหวทางไซเบอร์ นอกจากนี้ CERT จะต้องมีเครือข่ายกับประเทศต่างๆ ไม่ว่าจะเป็นเอกชนหรือรูปแบบของรัฐเองเพื่อสามารถช่วยเหลือหรือส่งสัญญาณอินเทอร์เน็ตได้ทันการ การเรียนรู้ที่จะมีการเตรียมระบบสำรองจึงเป็นสิ่งสำคัญเช่นกันในการฟื้นฟู สาธารณูพื้นฐานสำคัญของประเทศเมื่อถูกโจมตี

3. สงคราม South Ossetia War 2008

ในระหว่างช่วงฤดูร้อนความตึงเครียดระหว่างสงครามรัสเซีย-จอร์เจีย โดยมีกลุ่มที่ต้องการแบ่งแยก Ossetian และ Abkhazian ได้พยายามต่อสู้ทางไซเบอร์กับรัสเซีย และได้รับผลกระทบต่างๆมากมายจากการโจมตีของไวรัส แต่ต่างจาก Estonia เพราะจอร์เจียนั้นยังมีระบบเทคโนโลยีทางไซเบอร์ที่ยังไม่เต็มรูปแบบ การเงิน การธนาคารเสียหายส่งผลไปถึงระบบคมนาคม การขาดความเชี่ยวชาญในด้านเทคโนโลยีนี้ทำให้เจอเจียร์ได้รับผลเสียหายจากสงครามไซเบอร์ค่อนข้างมาก สื่อหลักทางไซเบอร์ต่างๆ ไม่ว่าจะเป็น Facebook Instagram และ Twitter ได้รับผลกระทบทั้งหมด จุดอ่อนอย่างหนึ่งของจอร์เจียในครั้งนี้คือการขาดระบบเฝ้าระวังในระบบสาธารณูปโภคแบบสารสนเทศและเป้นจุดอ่อนในการโจมตีครั้งนี้ ดังนั้นการมีระบบ Internet gateway ที่ดีจะทำให้ประชาชนชนนั้นได้รับผลกระทบน้อยลงและรัฐบาลจะสามารถควบคุมสถานการณ์ได้ง่ายมากขึ้นไทย (Jones, 2005)

4. สิ่งที่ประเทศไทยสามารถเรียนรู้จากเหตุการณ์นี้

เนื่องจากประเทศจอร์เจียและประเทศไทยมีความสามารถในด้านเทคโนโลยีด้านไซเบอร์เท่ากัน แต่หากวัดในระการเฝ้าระวังทางด้านไซเบอร์เชิงสาธารณูปโภคทางสารสนเทศแล้วนั้นถือว่าประเทศไทยมีความพร้อมพร้อมกว่าประเทศจอร์เจียร์เป็นอย่างมาก จากการสัมภาษณ์ผู้เชี่ยวชาญต่างๆ จาก กสทช. หรือ สภาความมั่นคงแห่งชาตินั้นทราบว่าประเทศไทยมีความพร้อมทางด้านการเตรียมพร้อมและตอบโต้หากมีการต่อสู้หรือโจมตีทางด้านเทคโนโลยีสารสนเทศเป็นอย่างมาก จนบางครั้งประเทศไทยยังมีความสับสนว่าหน่วยงานใดควรรับผิดชอบเรื่องนี้อย่างจริงจังและจะต้องเพิ่มการเฝ้าระวังทางด้านสาธารณูปโภคสำคัญทางด้านการดำรงชีพพื้นฐานของประชาชนในมากขึ้น

5. สงคราม Kyrgyzstan 2009

สงครามในประเทศ Kyrgyzstan จะมีความสับสนในรูปแบบของสาธารณูปโภคพื้นฐานสำคัญในพื้นที่ของไซเบอร์ ในสงครามครั้งนี้ Kyrgyzstan ประสบกับการถูกชัดดาวน์ระบบเป็นเวลากว่าสัปดาห์ และรัฐบาลไม่ได้รับผลกระทบมากมายจากสงครามครั้งนี้อาจเป็นเพราะการจู่โจมจากอินเทอร์เน็ตที่มีความสามารถต่ำ และมีผลกรพทบกับประชาชนค่อนข้างน้อย การโจมตีของ

Kyrgyzstan ถือมีความซับซ้อนมากในเรื่องของจุดประสงค์ทางการเมืองและการจู่โจมครั้งนี้มีข้อสงสัยว่าอาจจะเป็นปฏิบัติที่ร่วมมือกับประธานาธิบดีคนก่อนเมื่อให้ขึ้นมาสู่อำนาจอีกครั้งและเป็นการจ้างและได้รับความร่วมมือกับรัฐบาลรัสเซียเพื่อเข้ามาควบคุมในอำนาจร่วมกับประธานาธิบดีคนเก่า (GCHO, 2016)

6. สิ่งที่ประเทศไทยสามารถเรียนรู้จากเหตุการณ์นี้

สิ่งที่ประเทศไทยได้เรียนรู้จากปฏิบัติการข้างต้นนี้ คือการจู่โจมทางไซเบอร์ที่มีวัตถุประสงค์ทางการเมืองโดยเฉพาะ การร่วมมือระหว่างนักการเมืองภายใน กลุ่มคนที่ไม่ใช่รัฐ และประเทศที่เป็นพื้นที่ที่สามทางไซเบอร์กับการเกี่ยวข้องซึ่งผลประโยชน์ สิ่งเหล่านี้สามารถเกิดขึ้นได้ในรูปแบบของการกดดันทางการเปลี่ยนแปลงสาธารณูปโภคพื้นฐานที่สำคัญและสาธารณูปโภคพื้นฐานทางสารสนเทศ ซึ่งเป็นการโน้มน้าวที่สำคัญและสามารถชักจูงผู้บริโภคเทคโนโลยีหรือผู้ใช้อินเทอร์ได้อย่างง่ายดายในการเปลี่ยนแปลงทางการเมือง

7. Tibetan Authorities

ผู้มีอำนาจใน Tibetan ถูกกล่าวหาว่าเป็นผู้ต้องสงสัยในการโจรกรรมทางไซเบอร์หลังจากสิบเดือนในการตรวจสอบพบว่า เครือข่ายคอมพิวเตอร์ทั้งหมดถูก Trojan อย่างน้อย 1,295 ระบบ และยังแพร่กระจายไปอีกยัง 103 ประเทศ ที่มีเป้าหมายมุ่งตรงไปยังกระทรวงการต่างประเทศ สถานทูต องค์กรต่างประเทศต่าง ๆ และรวมไปถึง NATO Headquarters และที่มากไปกว่านั้น Ghost Net ยังควบคุมไปยังการดาวน์โหลดในพื้นที่ออนไลน์ต่างๆ รวมไปถึงการอัพเดทระบบคอมพิวเตอร์ในตัวเอง (Jones, 2005)

แต่ถึงแม้ว่าหลักฐานทุกอย่างจะชี้ว่าประเทศจีนเป็นประเทศหลักในการกระทำครั้งนี้ แต่อย่างไรก็ตามหลักฐานต่างๆยังคงไม่เมืองพอที่จะไม่สามารถระบุได้ว่าเป็นรัฐบาลจีนหรือผู้กระทำที่ไม่ใช่รัฐ แต่ IP-address นั้นสามารถชีแจงได้ว่าเป็นการกระทำที่เกิดจากประเทศจีน

8. สิ่งที่ประเทศไทยสามารถเรียนรู้จากเหตุการณ์นี้

ข้อควรระวังสำหรับประเทศไทยคือการรักษาความปลอดภัยของระบบของตนเองและป้องกันการเป็นศัตรูกับประเทศอื่น ๆ ที่มีความสามารถในการโจมตีทางไซเบอร์ ที่สำคัญประเทศไทยควรสร้างความร่วมกับประเทศต่าง ๆในการแลกเปลี่ยนข้อมูลและเพื่อการช่วยเหลือได้ทันการเมื่อเกิดการจู่โจมทางไซเบอร์

9. Stuxnet 2010

เมื่อโรงงานนิวเคลียร์ ในประเทศอิหร่านถูกโจมตีโดยอาวุธไซเบอร์ที่เรียกว่าโทรจันที่ไม่มุ่งการจารกรรมล้วงข้อมูลเหมือนไวรัสคอมพิวเตอร์ทั่วไป แต่กลับมุ่ง “ทำลายล้าง” ระบบโรงงานอุตสาหกรรมที่เป็นเป้าหมายเฉพาะตัวและสามารถทะลุทะลวงเข้าไปได้ Stuxnet ถือเป็นไวรัสตัวแรกที่ถูกใช้เป็นอาวุธไซเบอร์ที่สามารถทำลายโครงสร้างพื้นฐานทางกายภาพได้จริง โครงการนี้เกิดจาก

หน่วยงาน US Strategic Command ซึ่งดูแลส่วนของหัวรบนิวเคลียร์นานาชาติเสนอให้ใช้กลยุทธ์เพื่อซื้อเวลาให้สามารถเข้าไปเจรจาทางการทูตได้มากขึ้น รวมถึงมีเวลาเพื่อให้ทางสหประชาชาติคว่ำบาตร และเรียกร้องให้อิหร่านลงนามใน Joint Comprehensive Plan of Action หรือแผนปฏิบัติการเบ็ดเสร็จร่วม ป้องกันไม่ให้มีการสร้างหัวรบนิวเคลียร์ขึ้น (ทีมมายด์อินไซต์, 2564) ซึ่งกลยุทธ์นี้คือการส่งไวรัสคอมพิวเตอร์เข้าไปก่อกวนโรงงานนิวเคลียร์ของอิหร่าน ไวรัสที่ว่านี้คือ Stuxnet ไวรัสชนิดหนอนคอมพิวเตอร์เป็นที่รู้จักกันดีในเรื่องการแพร่กระจายผ่านระบบเน็ตเวิร์คโดยทำหน้าที่ ทำให้เตาปั่น (Centrifuge) ที่ใช้แยกไอโซโทปของยูเรเนียม ปั่นเร็วขึ้นกว่าปกติ หลังจากนั้นก็ค่อยปล่อยให้ปั่นตามความเร็วเดิม ช่วงเดือนถัดมาทำให้เตาปั่น ปั่นช้าลงกว่าเดิมนาน 50 นาที แล้วปล่อยให้ปั่นตามปกติ วนซ้ำไปมาเรื่อย ๆ นานหลายเดือน จนในที่สุดเตาก็สามารถกลับมาปั่นทำงานปกติได้ ดังนั้นเจ้าหน้าที่จะไม่รู้เลยว่าโรงงานนิวเคลียร์กำลังตกอยู่ในความเสี่ยงร้ายแรง (ทีมมายด์อินไซต์, 2564)

10. สิ่งที่ประเทศไทยสามารถเรียนรู้จากเหตุการณ์นี้

เหตุการณ์นี้เป็นเหตุการณ์ที่เกิดระหว่างความขัดแย้งระหว่างประเทศสหรัฐฯและอิหร่าน ประเทศไทยสามารถเรียนรู้ได้จากการใช้ไวรัสที่ซับซ้อนตัวนี้ซึ่งมีผลต่อทางกายภาพจริง และเรียนรู้ว่าการรับมือของอิหร่านนั้นเป็นอย่างไร แต่ถึงแม้ว่าประเทศไทยจะยังไม่มีโรงงานนิวเคลียร์เป็นของตนเองแต่ประเทศไทยยังมีสาธารณูปโภคอื่นที่สำคัญต่างๆ ที่จะต้องป้องกันไม่ให้เกิดผลเสียกับประชาชน ทางที่ดีที่สุดคือการป้องกันไม่ให้โทรจันหรือไวรัสซับซ้อนตัวนี้เข้ามาทำลายในระบบ แต่ถ้าหากไม่สามารถป้องกันได้แล้ว ThaiCERT จะต้องเข้ามารับผิดชอบในเหตุการณ์ฉุกเฉินครั้งนี้ พร้อมทั้งร่วมมือกับหน่วยงานภายในที่ถูกโจมตีให้มีความรับเบื้องต้นในการสกัดกั้นและเตรียมพร้อมระบบ back up ข้อมูลต่างๆและให้การใช้บริการได้ปกติ(ทีมมายด์อินไซต์, 2564)

11. Operation Aurora- Google VS. China

Operation Aurora เป็นชุดของการโจมตีไซเบอร์ดำเนินการโดยภัยคุกคามถาวรขั้นสูงตั้งอยู่ในกรุงปักกิ่งประเทศจีน ซึ่งมีความผูกพันกับกองทัพปลดปล่อยประชาชน สิ่งนี้ถูกเปิดเผยต่อสาธารณะครั้งแรกโดย Google เมื่อวันที่ 12 มกราคม 2010 การโจมตีเริ่มขึ้นในกลางปี 2552 และดำเนินต่อไปจนถึงเดือนธันวาคม 2552 การโจมตีมีเป้าหมายไปที่องค์กรอื่น ๆ หลายสิบแห่ง อันเป็นผลมาจากการโจมตี Google นอกจากนี้ยังมีหลักฐานว่า Operation Aurora มีแผนที่จะใช้งานเครื่องมือเวอร์ชั่นที่ไม่มีการตรวจสอบได้อย่างสมบูรณ์ในประเทศจีน และยอมรับว่าหากไม่สามารถทำได้ก็จำเป็นจะต้องออกจากประเทศจีน แหล่งข่าวอย่างเป็นทางการของจีนอ้างว่านี่เป็นส่วนหนึ่งของกลยุทธ์ที่พัฒนาโดยรัฐบาลสหรัฐฯ (Jones, 2005)

การโจมตีเป็นชื่อ "Operation Aurora" พบว่า "Aurora" เป็นส่วนหนึ่งของเส้นทางไฟล์บนเครื่องของผู้โจมตีซึ่งรวมอยู่ในมัลแวร์เกี่ยวข้องกับการโจมตี จากข้อมูลอย่างเป็นทางการพบว่าเป้าหมายหลักของการโจมตีคือการเข้าถึงและอาจปรับเปลี่ยนที่เก็บซอร์สโค้ดที่บริษัทซึ่งจะสร้างความ

เสียหายด้านข้อมูลทางการเงินหรือข้อมูลส่วนบุคคลที่บริษัทมีและใช้เวลาและความพยายามอย่างมากในการปกป้อง ในการนี้ Google ได้ประกาศว่าบริษัทตนนั้นไม่เกี่ยวข้องกับรัฐบาลสหรัฐอเมริกาเพื่อที่จะใช้การลอยตัวนี้อยู่เหนือความขัดแย้งระหว่างรัฐซึ่งจะทำให้เกิดความรุนแรงมากกว่าเดิม (Gordon, & Ford, 2002)

12. กระแสต่าง ๆ ของสงครามไซเบอร์ในปัจจุบัน

เมื่ออินเทอร์เทอร์เน็ตมีความสำคัญมากขึ้นทั่วโลกและในประเทศไทยเองก็ตามปัญหาที่สำคัญคือความไม่แน่นอน ถึงการสัมภาษณ์จากทุกหน่วยงานจะมีความเห็นร่วมกันว่าประเทศไทยยังไม่เคยมีประสบการณ์กับการก่อการร้ายไซเบอร์ที่รุนแรง แต่แม้เพียงแค่ 0.01% ก็สามารถตีความว่าเป็นการเกิดขึ้นจริงของการก่อการร้ายทางไซเบอร์ได้ และหน่วยงานแงก็ไม่สามารถประเมินได้ถึงจุดประสงค์ของการกระทำและผลกระทบว่าจะร้ายแรงแค่ไหน ความคลุมเครือของสถานที่เกิด ข้อมูลระบุตัวตนของผู้กระทำ ผู้กระทำนั้นจะเป็นปัจเจกบุคคลหรือเป็นกลุ่ม จะสนับสนุนด้วยรัฐหรือไม่ใช่รัฐก็ตาม สุดท้ายแล้วเราไม่สามารถหาวิธีที่จะลงทาผู้กระทำโดยใช้อำนาจเหนือรัฐได้ คำถามที่ว่าสิ่งเหล่านี้ จะเกิดขึ้นเมื่อไหร่ ใครเป็นคนทำ ใช้กลยุทธ์ในการทำ และทำเพื่ออะไร ยังคงเป็นปัจจัยหลักในการพยากรณ์รูปแบบของการเกิดขึ้นของการจู่โจมทางไซเบอร์ในอนาคตโดยเฉพาะแรงจูงใจที่จะสามารถโน้มน้าวทางโลกไซเบอร์ได้ง่ายกว่าโลกที่แท้จริง (Green, 2020)

กระแสโลก ณ ตอนนี้การที่กลุ่มก่อการร้ายดั้งเดิม เช่น อัลกออิดะฮ์ พยายามที่จะหาเงินสนับสนุนการก่อการร้ายของตนผ่านการแฮกทางไซเบอร์ โดยที่นักวิชาการส่วนใหญ่กันเหไปสนใจในตลาดของการค้าขายเงินทางไซเบอร์เพื่อสามารถตัดโอกาสของผู้ก่อการร้ายเหล่านี้ได้ สหรัฐฯเป็นประเทศหนึ่งที่พยายามจะตัดเครือข่ายการแฮกของกลุ่มก่อการร้าย ไม่ว่าจะเป็นทางโลกตะวันออก เช่น เกาหลีเหนือพยายามจะส่ง Ransomware จู่โจมโรงพยาบาลในประเทศอังกฤษเพื่อเรียกค่าไถ่แต่ไวรัสเหล่านั้นกลับกลายเป็น WannaCry และทำลายระบบจองโรงพยาบาลประเทศอังกฤษเป็นเวลาสองอาทิตย์ แต่นโยบายของประเทศอังกฤษไม่มีนโยบายที่จะเงินเพื่อให้ได้ข้อมูลคืนมาเพราะตระหนักว่า อย่างไรก็ตามไม่มีอะไรการันตีว่าข้อมูลเหล่านั้นจะกลับมาได้จริง ส่วนสหรัฐอเมริกานั้นมีแนวโน้มที่จะไม่จ่ายค่าไถ่แต่ในที่สุดก็สามารถที่จะยอมจ่ายได้จริงซึ่งตรงข้ามกับประเทศรัสเซียที่มีแนวโน้มว่าจะจ่ายค่าไถ่แต่สุดท้ายก็ไม่จ่ายจริงๆ ทั้งหมดนี้ขึ้นอยู่กับนโยบายและยุทธศาสตร์ของประเทศ สหรัฐอเมริกายังโดนโจมตีจากประเทศเกาหลีเหนือโดยผ่านสงครามตัวแทนเช่นการเจาะระบบการเงินและการธนาคารของเกาหลีใต้ที่ส่งผลกระทบต่อประเทศสหรัฐฯ (Gordon, & Ford, 2002)

ประเทศไทยสามารถเรียนรู้จากประสบการณ์การเกิดสงครามไซเบอร์ การก่อการร้ายไซเบอร์ หรืออาชญากรรมไซเบอร์ต่างๆ จากบทเรียนของประเทศต่างๆที่เกิดขึ้นมาแล้ว และนำมาสร้างเป้นนโยบายของตนเองให้เป็นรูปธรรมและบังคับใช้ได้จริงโดยมีการซ้อมหรือหากหน่วยงานใดไม่มีการทำตามก็จะต้องมีบทลงโทษที่แน่นอน

4.7 การก่อการร้ายไซเบอร์ในอนาคต “The Future of Cyberterrorism”

ผู้ก่อการร้ายไซเบอร์จะมีแนวโน้มที่จะจู่โจมเครือข่ายธนาคาร และการธุรกรรมทางการเงินระหว่างประเทศ และจู่โจมตะกร้าเงินแลกเปลี่ยนระหว่างประเทศมากที่สุด ซึ่งจะทำให้ประชาชนในประเทศสูญเสียความมั่นใจในระบบเศรษฐกิจของประเทศ แต่ในการกระทำนี้จะส่งผลต่อองค์กรขนาดใหญ่หรือไม่นั้นยังไม่สามารถสรุปได้เพราะองค์กรขนาดใหญ่จะสามารถสกัดจับได้ทันก่อนที่จะทำให้เกิดความเสียหายเชิงโครงสร้าง แต่อย่างไรก็ตามการที่แฮกเกอร์ที่ไร้ตัวตนและมีแหล่งที่มาจากประเทศใดในโลกก็ได้จะสามารถทำให้ระบบเศรษฐกิจนั้นหยุดได้ชั่วคราวและการทำลายความมั่นคงนั้นจะสามารถเกิดขึ้นได้ในอนาคต (Denning, 2020) มากไปกว่านั้นการจู่โจมการจราจรทางอากาศ การควบคุมระบบสัญญาณทางอากาศ เป็นปัจจัยหนึ่งที่สามารถสร้างความขัดแย้งกันทางพลเรือนได้ ตัวอย่างที่สามารถเห็นได้ชัดเจนคือการควบคุมระบบเซ็นเซอร์ในห้องของกัปตันและการกระทำเช่นนี้สามารถทำได้กับระบบควบคุมรถไฟ นอกจากนี้ผู้ก่อการร้ายไซเบอร์สามารถเปลี่ยนระดับความดันของระบบท่อส่งแก๊สทำให้เกิดความล้มเหลวของระบบ และทำให้เกิดระเบิดและการเผาไหม้ได้ เฉกเช่นเดียวกับว่าเครื่องมือทางอิเล็กทรอนิกส์จะเป็นช่องโหว่ให้กับผู้ก่อการร้าย (Kenney, 2015) กระแสในอนาคตยังมีอีกมากมายที่รัฐบาลยังคาดไม่ถึงขึ้นอยู่กับความก้าวหน้าทางเทคโนโลยีและศักยภาพของผู้จู่โจม

4.7.1 ปัญหาที่ประเทศไทยกำลังเผชิญ

ประเทศไทยกำลังเผชิญปัญหาเหมือนประเทศอื่นๆในสังคมโลกไซเบอร์เพราะเมื่อนำอินเทอร์มาใช้มาขึ้นโดยที่คนส่วนใหญ่ขาดความตระหนักรู้ จากการวิเคราะห์ผลจากการสัมภาษณ์เชิงลึกทั้งหมดรวมถึงนโยบายต่างๆและการสัมมนา สามารถวิเคราะห์ปัญหาทั้งหมดได้ ดังนี้

1. ปัญหาด้านนโยบาย และการนำนโยบายไปสู่การปฏิบัติ

ปัญหาดั้งเดิมของประเทศไทยไม่ว่าจะเป็นนโยบายด้านใดก็ตาม สาเหตุหนึ่งที่ทำให้ประเทศไทยไม่ประสบความสำเร็จในการแก้ปัญหานั้นคือการไม่สามารถนำนโยบายไปปฏิบัติได้ เพราะไม่ได้มีคู่มือที่สามารถปรับใช้ได้กับทุกหน่วยงาน ระบบของแต่ละหน่วยงานมีความแตกต่างกัน จึงมีความยากที่จะนำกฎหรือมาตรฐานเดียวมาปรับใช้กับทุกๆหน่วยงาน ดังนั้นหน่วยงานที่ออกนโยบายต้องทำให้นโยบายนั้นมีชีวิตไม่ใช้แค่ตัวอย่างหนังสือในกระดาษ บางครั้งตเองมีการนำร่องกับหน่วยงานใดหน่วยงานหนึ่งก่อนที่จะนำนโยบายนี้มาใช้จริงกับหน่วยงานทั้งหมด

1.1 หน่วยงานด้านการกำกับดูแลความมั่นคง

หน่วยงานหลักด้านการออกนโยบายทางพลเรือน เพื่อสร้างความความใจให้หน่วยงานฝ่ายผลเรือนมีความความใจตรงกันหน่วยงานยังขาดการประสานซึ่งกันและกันไม่ว่าจะเป็นสภาความมั่นคงแห่งชาติ กระทรวงดิจิทัลฯ สกมช. หรือหน่วยงานทางด้านการเงิน เห็นได้ชัดว่าต่างฝ่ายต่างทำงานในภาคส่วนของตัวองจนลืมไปว่าการร่วมมือแลกเปลี่ยนเทคโนโลยีซึ่งกันและกันจะเป็นการสร้างความรู้สูงสุด บางหน่วยงานนำเสนอนโยบายเพียงแค่ในกระดาษ ซึ่งสร้างความเข้าใจยากแก่ผู้ปฏิบัติ

1.2 หน่วยงานด้านการปราบปราม

หน่วยงานนี้ใช้นโยบายที่ถูกร่างมาจากหน่วยงานด้านการกำกับดูแลความมั่นคงและมีนโยบายทางการทหารเป็นของตนเพราะฉะนั้น ปัญหาที่เห็นได้ชัดเจนคือต้องมีการทบทวนหรือไม่ว่านโยบายของฝ่ายพลเรือนและฝ่ายทหารนั้นต้องมีความเชื่อมโยงกันหรือไม่ หรือต้องมีการประเมินว่านดยบายของฝ่ายทหารที่วางไว้มีประสิทธิภาพมากแค่ไหนและมีทิศทางที่ถูกต้องหรือไม่เพื่อจะได้ปรับเปลี่ยนให้ถูกต้องตามสถานการณ์

1.3 หน่วยงานที่มีความเสี่ยงด้านการโจมตี

หน่วยงานประเภทนี้มีนโยบายที่ต้องทำตามหน่วยงานด้านการกำกับดูแลความมั่นคงซึ่งเป็นหน่วยงานสำหรับพลเรือนที่คอยดูแลสอดส่องไม่ให้เกิดความเสียหายต่อประชาชน เพราะฉะนั้นการมีคู่มือที่ทำให้ผู้ปฏิบัติเข้าใจง่ายและตรงตามภารกิจของแต่ละหน่วยงานจะเป็นประโยชน์มากขึ้น หน่วยงานด้านการกำกับดูแลความมั่นคงจะต้องศึกษาภารกิจของแต่ละหน่วยงารที่มีความเสี่ยงซึ่งได้มีข้อมูลเบื้องต้นเกี่ยวกับหน่วยงานข้างต้นแล้วในบทที่ 2 ดังนั้น สิ่งที่ควรพิจารณาต่อไปคือการสร้างนโยบายสำหรับแต่ละหน่วยงานที่มีความเสี่ยงและให้หน่วยงานนั้นปฏิบัติตามพร้อมประเมินผลมายังหน่วยงานด้านการกำกับดูแลความมั่นคงได้นำมาพิจารณาและแก้ไขต่อไป

2. ปัญหาการขาดบุคลากรที่เชี่ยวชาญทางเทคนิค

2.1 หน่วยงานด้านการกำกับดูแลความมั่นคง

ปัญหาดั้งเดิมของหน่วยงานด้านการกำกับดูแลความมั่นคงคือผู้ร่างนโยบายจำเป็นจะต้องมีความรู้ทางเทคนิคควบคู่ไปด้วยเพราะการจะสร้างระบบไซเบอร์ป้องกันความมั่นคงของประเทศนั้นจะต้องใช้มาตรการที่มีปะสิทธิภาพ การใช้ความรู้เรื่องนโยบายหรือความรู้ทางด้านรัฐศาสตร์เป็นทักษะที่จำเป็นแต่ทักษะทั้งสองอย่างนี้ไม่สามารถสร้างนโยบายที่มีประสทธิภาพได้ จากการสัมภาษณ์หน่วยงานด้านการกำกับดูแลความมั่นคงทำให้ทราบว่าขณะนี้ประเทศไทยกำลังขาดกำลังพลสำคัญที่มีความรู้ทางด้านไซเบอร์ในระดับนานาชาติ มหาวิทยาลัยส่วนใหญ่มีการเรียนการสอนเพียงแค่วิศวกรรมขั้นพื้นฐานทางคอมพิวเตอร์หรือวิทยาศาสตร์ทางคอมพิวเตอร์เท่านั้น สิ่งที่หน่วยงานด้านการกำกับดูแลความมั่นคงต้องการคือผู้เชี่ยวชาญทางด้านไซเบอร์ที่ร่วมสมัยเพื่อที่จะมา

สร้างความรู้ที่ถูกต้องและหาความรู้ใหม่ๆให้กับหน่วยงาน เช่น วิศวกรรมสังคมทางไซเบอร์ จิตวิทยาทางไซเบอร์ การป้องกันระบบสาธารณูปโภคสำคัญทางไซเบอร์ หรือการรับมือภัยคุกคามได้อย่างรวดเร็วตามสถานการณ์ที่เกิดขึ้นในปัจจุบัน

2.2 หน่วยงานด้านการปราบปราม

หน่วยงานด้านการปราบปรามเป็นหน่วยงานสำคัญที่จะต้องอาศัยผู้เชี่ยวชาญในการวิเคราะห์ภัยคุกคามที่กำลังเกิดขึ้นไม่ว่าจะเป็นทางเทคนิคหรือทางนกลยุทธ์ จึงเป็นที่สังเกตได้ชัดเจนว่าหน่วยงานปราบปรามโดยเฉพาะทางทหารมีเป้าหมายที่จะเพิ่มนโยบายหานักรบทางไซเบอร์เพิ่มมากขึ้น เช่นการเปิดรับสมัครทั้งทหารบก ทหารอากาศ แต่การรับสมัครเหล่านี้จำเป็นจะต้องรับบุคลากรที่มีความรู้จริงในตำแหน่งนั้นและมีความเชี่ยวชาญที่สามารถตามทันโลกปัจจุบันโดยเฉพาะในเรื่องของภาษาที่จะต้องสามารถใช้แลกเปลี่ยนกับหน่วยงานนานาชาติได้

2.3 หน่วยงานที่มีความเสี่ยงด้านการโจมตี

หน่วยงานที่มีความเสี่ยงจะมีภาระหน้าที่ที่แตกต่างจากหน่วยงานข้างต้นโดยส่วนมากหน่วยงานเหล่านี้มักมีหน้าที่ดูแลประและให้ประชาชนเป็นงานหลักแต่ภารกิจในเรื่องทางเทคโนโลยีเป็นงานรอง สิ่งที่จำเป็นคือการเพิ่มบุคลากรที่มีความรู้ทางด้านเทคโนโลยีและไซเบอร์ที่มีความร่วมสมัย ทันโลก สามารถมีความรู้เทียบเท่าเจ้าหน้าที่ ThaiCerts เพื่อที่จะสามารถติดต่อและประสานงานล่วงหน้าได้ทัน และอีกประการจะต้องมีความสามารถที่จะรับมือกับภัยคุกคามที่เกิดขึ้นเฉพาะหน้าได้อย่างรวดเร็ว ตรวจตรามิให้เกิดการจู่โจมทางไซเบอร์กับหน่วยงานได้ทัน อย่างน้อย 1-2 คน

3. ปัญหาด้านงบประมาณ

3.1 หน่วยงานด้านการกำกับดูแลความมั่นคง

ปัญหาด้านงบประมาณหน่วยงานด้านการกำกับดูแลความมั่นคงถือว่าไม่ใช่ปัญหาที่สำคัญมากนักสำหรับหน่วยงานเหล่านี้ เพราะรัฐบาลได้เล็งเห็นถึงความสำคัญของภัยคุกคามทางด้านไซเบอร์จึงได้ให้งบประมาณที่เพียงพอสำหรับหน่วยงานเหล่านี้ในการสร้างหน่วยงานใหม่ เช่น สกมช. เพื่อดูแลด้านนี้โดยเฉพาะ อยู่แค่เพียงว่าหน่วยงานเหล่านี้สามารถจัดสรรงบประมาณได้ถูกจุดประสงค์และกิจกรรมต่าง ๆ ที่เกิดขึ้นได้หรือไม่

3.2 หน่วยงานด้านการปราบปราม

หน่วยงานด้านการปราบปรามได้รับงบประมาณเพียงพอกับการรับมือภัยคุกคามทางไซเบอร์แต่ส่วนใหญ่ทางหน่วยงานจะทุ่มเทไปกับการซื้อเทคโนโลยีใหม่ๆ และไม่ได้ใช้เงินเพิ่มศักยภาพของบุคลากรเช่นการอบรมในระดับเชี่ยวชาญหรือเพิ่มเงินเดือนให้กับเจ้าหน้าที่ที่มีความรู้เฉพาะทางทางไซเบอร์เพื่อเพิ่มไม่ให้เกิดการสมองไหลไปยังภาคเอกชน เพราะความมั่นคงทางภาครัฐถือเป็นสิ่งสำคัญ

3.3 หน่วยงานที่มีความเสี่ยงด้านการโจมตี

หน่วยงานที่มีความเสี่ยงจะมีภาระหน้าที่ที่แตกต่างซึ่งมีหน้าที่เฉพาะทางของตน เช่น กระทรวงสาธารณสุขมีหน้าที่ในการดูแลรักษาผู้ป่วย การแบ่งงบประมาณมาเพื่อพัฒนาทางด้านเทคโนโลยีจึงเป็นเรื่องยากและไม่ตรงจุดประสงค์ ดังนั้นรัฐควรมีการพิจารณาตั้งงบประมาณพิเศษสำหรับหน่วยงานเหล่านี้เพื่อที่จะได้เพิ่มผู้ที่มีความเชี่ยวชาญโดยเฉพาะให้กับหน่วยงานเหล่านี้ในอนาคตด้วย

4. ปัญหาด้านวัฒนธรรมองค์กรและการตระหนักรู้

4.1 หน่วยงานด้านการกำกับดูแลความมั่นคง

ปัญหาการตระหนักรู้ของวัฒนธรรมองค์กรในประเทศไทยไม่ว่าจะเป็นองค์กรใดก็ตามมักจะพบความล้าหลังและการกลัวการเปลี่ยนแปลง แม้กระทั่งองค์กรที่เป็นหน่วยงานด้านการกำกับดูแลความมั่นคง จากการสัมภาษณ์พบว่าการวางนโยบายต่างๆในเรื่องการสร้างความตระหนักรู้ในรูปแบบขององค์กร เช่น การเพิ่มการอบรบทางด้านเทคโนโลยี การเพิ่มความระมัดให้กับเจ้าหน้าที่ในการใช้เทคโนโลยี การรักษาความลับ รหัสลับส่วนตัว หรือแม้กระทั้งคอมพิวเตอร์ในช่วงของการทำงานจากบ้าน ปัญหาสำคัญคือจะทำอย่างไรให้ความตระหนักรู้สามารถเกิดขึ้นได้จริงกับเจ้าหน้าที่ในทุกระดับเพื่อรับมือกับการเปลี่ยนแปลงทางเทคโนโลยีที่กำลังจะเกิดขึ้น

4.2 หน่วยงานด้านการปราบปราม

จากการสัมภาษณ์เชิงลึกทราบว่าปัญหาด้านการตระหนักรู้ไม่ใช้ปัญหาหลักขององค์กรเพราะบุคคลกรส่วนใหญ่ที่ทำงานจะต้องผ่านการอบรมทางคอมพิวเตอร์และมีความรู้ในระดับหนึ่งถึงจะสามารถอยู่ในองค์กรได้ ตัวอย่างเช่น กองทัพอากาศจะมีศูนย์ไซเบอร์ในสังกัดของตนและคัดเฉพาะบุคลากร ดังนั้นการมีความรู้ทางไซเบอร์เป็นพื้นฐานจึงทำให้พวกเขาสามารถมีความตระหนักรู้เป็นพื้นฐานหนึ่งในการทำงาน และการทำงานรักษาความมั่นคงในระดับประเทศนั้นจะต้องมีความมั่นคงและรอบคอบดังนั้นวัฒนธรรมองค์กรในเรื่องของการรักษาความปลอดภัยทางไซเบอร์จึงเป็นเรื่องที่สำคัญ

4.3 หน่วยงานที่มีความเสี่ยงด้านการโจมตี

ปัญหาการขาดความตระหนักรู้ทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และวัฒนธรรมองค์กรเป็นปัญหาใหญ่ที่ทำให้หน่วยงานที่มีความเสี่ยงด้านการโจมตีถูกโจมตีได้ง่ายเพราะเจ้าหน้าที่ส่วนใหญ่ที่ปฏิบัติหน้าที่จะตระหนักถึงภารกิจหลักขององค์กรในภาพรวมก่อนตระหนักถึงภัยคุกคามทางด้านไซเบอร์ เช่น กระทรวงสาธารณสุข กระทรวงยุติธรรม หรือ การไฟฟ้าฝ่ายผลิตก็ตาม เมื่อต้องเพิ่มภารกิจให้พวกเข้าจึงจำเป็นจะต้องลดภาระบางอย่างที่พวกเขามีและให้เวลาพวกเขาได้เรียนรู้

5. ปัญหาความซ้ำซ้อนของหน่วยงาน

5.1 หน่วยงานด้านการกำกับดูแลความมั่นคง

ภารกิจหลักของหน่วยงานด้านการกำกับดูแลความมั่นคงคือการรักษามาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ของฝ่ายพลเรือนและเตรียมการฟื้นฟูสภาพหลังจากโดยภัยคุกคามทางไซเบอร์ทำลาย ความซ้ำซ้อนของหน่วยงานนี้อาจจะทับซ้อนกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงานด้านการปราบปรามที่มีหน้าที่เพิ่มขึ้นในการดูแลสาธารณูปโภคสำคัญทางสารสนเทศซึ่งจะมีความซ้ำซ้อนกัน

5.2 หน่วยงานด้านการปราบปราม

เนื่องจากรัฐบาลมีความเห็นว่าสาธารณูปโภคทางสารสนเทศ เช่น การใช้โซเชียลมีเดียเป็นเหตุหนึ่งที่ทำให้รัฐเกิดความไม่มั่นคงจากประชาชนบางกลุ่ม และหวาดกลัวว่าประชาชนกลุ่มเหล่านี้จะใช้ช่องทางนี้เป็นการเผยแพร่อุดมการณ์การให้กับบุคคลทั่วไป จึงมอบหน้าที่เหล่านี้ให้หน่วยงานด้านการปราบปรามเข้าไปสืบเสาะในช่องทางการสื่อสารต่าง ๆ ซึ่งถือว่าเป็นงานที่ซ้ำซ้อนกับหน่วยงานด้านการกำกับดูแลความมั่นคงทางพลเรือนที่มีอยู่แล้ว

5.3 หน่วยงานที่มีความเสี่ยงด้านการโจมตี

ความซ้ำซ้อนที่เกิดขึ้นกับหน่วยงานที่มีความเสี่ยงด้านการโจมตียังไม่ปรากฏโดยตรงเพราะหน่วยงานเหล่านี้มีหน้าที่ทำตามหน่วยงานด้านการกำกับดูแลความมั่นคงและมีเจ้าหน้าที่บางส่วนจากหน่วยงานด้านการกำกับดูแลความมั่นคงเข้ามาเป็นส่วนหนึ่งขององค์กรเพราะมาอบรบและคอยรับมือภัยคุกคามที่หน่วยงานที่มีความเสี่ยงด้านการโจมตีไม่สามารถควบคุมได้

6. ปัญหาทางด้านกฎหมายและการบังคับใช้

6.1 หน่วยงานด้านการกำกับดูแลความมั่นคง

กฎหมายที่มีบทลงโทษสำหรับผู้ที่กระทำความผิดทางไซเบอร์ยังไม่สามารถบังคับใช้ได้อย่างเต็มที่เนื่องจากยังเป็นเรื่องใหม่และความไร้ตัวตนของผู้กระทำผิดยังคงเป็นข้อก็ตัวหนึ่งที่ไม่สามารถทำให้พวกเขาโดนจับได้ และหากผู้กระทเป็นตัวแสดงที่ไม่ใช่รัฐ หรือเป็นตัวแสดงจากรัฐที่สามจะทำให้เกิดความยุ่งยากมาขึ้นเพราะต้องอาศัยความร่วมมือจากกฎหมายระหว่างประเทศ

6.2 หน่วยงานด้านการปราบปราม

กฎหมายที่ใช้ลงโทษการจู่โจมทางการทหารส่วนใหญ่จะเป็นการตอบโต้กลับโดยไม่นับว่าเป็นการก่อความรุนแรงแต่เพื่อเป็นการป้องกันตัวเองไม่เห็นเกิดการจู่โจมในครั้งที่สองหรือสาม แต่อย่างไรก็ตามปัญหาที่เกิดขึ้นยังเชื่อมโยงอยู่กับกฎหมายระหว่างประเทศและกฎหมายมนุษย์ธรรมท์ไม่สามารถนำมาใช้ได้กับกรณีของการจู่โจมทางไซเบอร์

6.3 หน่วยงานที่มีความเสี่ยงด้านการโจมตี

กฎหมายที่บังคับกับหน่วยงานเหล่านี้ต้องมีผลมาจากหน่วยงานด้านการกำกับดูแลความมั่นคงซึ่งเป็นผู้ออกนโยบาย แต่สำหรับผู้จู่โจมนั้นจะได้รับโทษอย่างไรต่างขึ้นอยู่กับการกรพทำความเสียหายที่เกิดขึ้นแต่ทั้งนี้ทั้งนั้นยังไม่มีมาตรการที่กำหนดระดับความรุนแรงโดยตรง การปรับเงินหรือการจำคุกจึงเป็นเพียงบทลงโทษเล็กน้อยของผู้กระทำ

7. ปัญหาด้านผู้รับการแก้ไข (ผู้ก่อการร้ายทางไซเบอร์)

7.1 หน่วยงานด้านการกำกับดูแลความมั่นคง

หน่วยงานด้านการกำกับดูแลความมั่นคงมีบทลงโทษผู้กระทำความผิดที่มีประสิทธิภาพจริงหรือไม่ หรือมีการลดการกระทำความผิดซ้ำของผู้จู่โจมทางไซเบอร์ได้จริงหรือไม่ ยังคงเป็นคำถามถามที่จะต้องถกเถียงต่อไปถึงมาตรการที่จะต้องนำมาใช้เพื่อแก้ไขพฤติกรรมของผู้กระทำความผิดในอนาคตซึ่งอาจจะไม่เหมือนกับผู้ที่กระทำความผิดแบบธรรมดาทั่วไป

7.2 หน่วยงานด้านการปราบปราม

การแก้ไขผู้กระทำความผิดทางไซเบอร์ของมุมมองทางทหารมักจะเป็นในรูปแบบการโต้ตอบเพื่อเป็นการป้องกัน การข่มขู่เพื่อไม่ให้พวกเขาทำอีก เป็นกลยุทธ์เดียวกันกับการแก้ขพฤติกรรมของฝ่ายตรงข้างทางการทหารแบบดั้งเดิม เพราะฉะนั้นการแก้ไขฟื้นฟูผู้กระทำความผิดทางไซเบอร์ขึ้นอยู่กับพฤติกรรม เป้าหมาย ของแต่ละบุคคล ว่าจะจัดประเภทว่าเป็นภัยคุกคามแบบพลเรือนหรือแบบทางการทหารได้อย่างไร

7.3 หน่วยงานที่มีความเสี่ยงด้านการโจมตี

หน่วยงานเหล่านี้ถือว่าเป็นปลายน้ำไม่สามารถที่จะกำหนดได้ว่าผู้กระทำความผิดควรกระทำอย่างไร ถึงแม้กรมราชทัณฑ์จะสังกัดอยู่ภายใต้กระทรวงยุติธรรมและมีหน้าที่บำบัดแก้ไขคนกระทำความผิดแต่ก็ไม่ได้หมายความว่ากรมราชทัณฑ์จะสามารถออกกฎเกณฑ์ในการแก้ไขบำบัดได้ ดังนั้นหน้าที่เหล่านี้จึงขึ้นอยู่กับหน่วยงานด้านการกำกับดูแลความมั่นคงว่ามีความคิดเห็นอย่างไรและควรจะใช้บทลงโทษและการแก้ไขรูปแบบเดิมหรือไม่

8. ปัญหาด้านการร่วมมือระหว่างประเทศ

8.1 หน่วยงานด้านการกำกับดูแลความมั่นคง

หน่วยงานด้านการกำกับดูแลความมั่นคงมีความร่วมมือทางด้านการต่างประเทศในกรอบความร่วมมือทางไซเบอร์ได้ดีมากแต่ยังขาดการเป็นภาคีในการแลกเปลี่ยนความรู้ในอีกหลายองค์การที่จะต้องอาศัยคนที่มีความรู้จริงและเชี่ยวในเรื่องความมั่นคงทางไซเบอร์โดยตรง จากการสัมภาษณ์ทำให้ทราบว่าสภาความมั่นคงแห่งชาติมีความร่วมมืออย่างดีกับประเทศต่าง รงมถึงหน่วยงานอื่นๆที่อยู่ในกลุ่มของหน่วยงานด้านการกำกับดูแลความมั่นคงแต่หากมี

การเพิ่มความเข้มข้นที่มากกว่านี้เช่นการเพิ่มบุคลากรที่มีความเชี่ยวชาญทางด้านเทคนิคและนโยบายเพื่อเข้าร่วมในภาคีต่างๆจะเป็นสิ่งที่สามารถเติมเต็มปัญหาด้านการร่วมมือได้

8.2 หน่วยงานด้านการปราบปราม

หน่วยงานด้านการปราบปรามของประเทศไทยมีความร่วมมืออย่างดีกับต่างประเทศ เช่น การส่งทหารหรือข้าราชการไปอบรมเกี่ยวกับไซเบอร์ หรือมอบทุนให้กับนักศึกษาเพื่อกลับมาเป็นนักรบไซเบอร์ แต่ในกลุ่มของหน่วยงานด้านการปราบปรามนั้นจะมีขอบเขตของข้อมูลที่สามารถแลกได้มิฉะนั้นจะเป็นการเปิดเผยข้อมูลความมั่นคงระหว่างประเทศ ในรูปแบบของการร่วมมือมักจะมาในเรื่องของเทคนิค อุปกรณ์ ความรู้ต่างๆทางด้านเทคโนโลยีซึ่งจะไม่ได้เกี่ยวข้องกับกฎหมายระหว่างประเทศที่ใช้เพื่อควบคุมหรือปราบปรามประเทศอื่นๆ แต่อาจจะมีบางส่วนของหน่วยงานที่สามารถเข้าร่วมได้

8.3 หน่วยงานที่มีความเสี่ยงด้านการโจมตี

หน่วยงานที่มีความเสี่ยงเป็นหน่วยงานที่สำคัญที่สุดที่จะต้องอาศัยความร่วมมือหรือเข้าร่วมในองค์กรต่าง ๆ ระหว่างประเทศ รวมไปถึงความร่วมมือกับองค์กรเอกชนในประเทศไทยไม่ว่าจะเป็นองค์เอกชนที่มีสัญชาติไทยหรือต่างประเทศก็ตาม เพราะความร่วมมือเหล่านี้จะช่วยให้องค์กรสามารถเรียนรู้และรับมือกับกับสถานการณ์ทางไซเบอร์แบบได้ทันการณ์ด้วยเครื่องมือและความรู้ที่เป็นสมัยใหม่

9. ปัญหาด้านการทุจริตของเจ้าหน้าที่

9.1 หน่วยงานด้านการกำกับดูแลความมั่นคง

การทุจริตของเจ้าหน้าที่สามารถเกิดขึ้นได้ทุกเมื่อ ไม่ว่าจะเป็นในรูปแบบใดก็ตามเพราะฉะนั้นถ้าเจ้าหน้าที่ทุจริตในเรื่องงบประมาณหรือไม่ได้ทำงานให้เป็นไปตามแผนนโยบายที่วางไว้ หรือแม้เกระทั่งเป็นสายสืบให้กับกลุ่มแฮกเกอร์ต่างๆ อาจจะทำให้สถานการณ์ไซเบอร์ที่เกิดขึ้นในประเทศไทยมีความรุนแรงมากขึ้น เพราะเจ้าหน้าที่ในหน่วยงานด้านการกำกับดูแลความมั่นคงเปรียบเสมือนหน่วยงานหัวเรือใหญ่ในการนำประเทศไทยไปสู่จุดหมายที่ควรจะเป็น

9.2 หน่วยงานด้านการปราบปราม

หน่วยงานด้านการปราบปรามได้รับงบประมาณทางด้านไซเบอร์เพื่อนำไปพัฒนาอาวุธยุทโธปกรณ์ที่เหมาะสมให้มีความทันสมัยต่อโลก แต่หากเกิดการทุจริตของเจ้าหน้าที่จำนวนเงินนั้นเป็นวัตถุประสงค์เพื่อความมั่นคงทำให้ตรวจสอบยากว่าของที่ได้รับตรงตามความต้องการที่สั่งมาหรือไม่ อาจจะเป็นปัญที่สามารถเกิดขึ้นได้หากมีช่องว่างและยากต่อการตรวจสอบ

9.3 หน่วยงานที่มีความเสี่ยงด้านการโจมตี

หน่วยงานที่มีความเสี่ยงจะมีจะมีงบประมาณในด้านการพัฒนาระบบไอทีหรือระบบเทคโนโลยีสารสนเทศน้อยกว่าหน่วยงานประเภทอื่นเพราะฉะนั้นการทุจริตทางด้านการเงิน

อาจเกิดขึ้นได้น้อย แต่ความรุนแรงที่สามารถเกิดขึ้นได้คือการที่เจ้าหน้าที่สามารลักลอบเอาข้อมูลที่เป็นความลับไปขาย หรือกลายเป็นสายลับให้กับกลุ่มแฮกเกอร์เองเพื่อประโยชน์ส่วนตนจะเป็นเรื่องที่น่าเป็นห่วงอย่างยิ่ง

4.8 การวิเคราะห์การรับมือภัยคุกคามทางไซเบอร์จากปัจจัยอื่น ๆ

4.8.1 กฎหมายระว่างประเทศ

กรอบกฎหมายระหว่างประเทศเกี่ยวกับการก่อการร้ายนั้นมีมาก่อนเหตุการณ์ 9/11 จากตราสารระหว่างประเทศ 18 รายการ (รวมถึงการแก้ไขเพิ่มเติม) โดยนำมาใช้ตั้งแต่ปี 2506 มีอยู่ 13 รายการก่อนปี 2544 (Int'l Civil Aviation Org. [ICAO], 2010) แม้ว่าจะเห็นได้ชัดว่าการโจมตีเหตุการณ์ 11 กันยายนและเหตุการณ์อื่น ๆ ภายในสหรัฐอเมริกาเป็นตัวเร่งและกระตุ้นให้เกิดการพัฒนากฎหมายระหว่างประเทศที่จะมาช่วยป้องการการก่อการร้ายไม่ให้เกิดซ้ำอีก เช่น ตามอนุสัญญาว่าด้วยการปราบปรามการก่อการร้ายนิวเคลียร์ พ.ศ. 2548 และยุทธศาสตร์ต่อต้านการก่อการร้ายทั่วโลกขององค์การสหประชาชาติ พ.ศ. 2549 เอกสารเหล่านี้สร้างจากพื้นฐานทางกฎหมายที่มีอยู่ก่อนหน้านี้

ขอบเขตและหลักการทั่วไปของกฎหมายระหว่างประเทศที่เกี่ยวข้องกับการก่อการร้ายได้เปลี่ยนแปลงไปตั้งแต่เหตุการณ์ 9/11 สามารถอธิบายได้ว่า เนื่องจากองค์ประกอบบางอย่างไม่ได้เปลี่ยนแปลง เช่น ตามหลักฐานจากความล้มเหลวในการนำอนุสัญญาที่ครอบคลุมของสหประชาชาติว่าด้วยการก่อการร้ายระหว่างประเทศมาใช้ นำไปสู่ความคลุมเครือเหนือคำจำกัดความของการก่อการร้ายทั้งปวง ในขณะที่องค์ประกอบอื่นๆ เปลี่ยนไปอย่างมาก (เช่น แสดงการยอมรับโดยคณะมนตรีความมั่นคงแห่งสหประชาชาติ (UNSC) ในมติ 1368 และ 1373 ของสิทธิในการป้องกันตัวเองเพื่อตอบโต้การโจมตีของผู้ก่อการร้ายโดยผู้ไม่ฝักใฝ่ฝ่ายใด -ตัวแสดงของรัฐ) หากการโจมตีของผู้ก่อการร้ายในโลกไซเบอร์ทำอย่างน้อยถึงเกณฑ์เดียวกับการโจมตีเหตุการณ์ 9/11 มีเหตุผลร้ายแรงที่จะเชื่อว่าแนวทางทางกฎหมายจะเหมือนกับการโจมตีของอัลกออิดะห์: การพัฒนากฎหมายอย่างรวดเร็ว บนพื้นฐานของฐานที่มีอยู่แล้ว (Int'l Civil Aviation Org. [ICAO], 2010)

ผู้เขียนบางคนในปัจจุบันเชื่อว่าไม่มีภัยคุกคามจากการก่อการร้ายทางไซเบอร์ที่จะเกิดขึ้นจริง แต่เป็นความจริงจากการโจมตีทางไซเบอร์ ยังไม่ได้สร้างสถิติอย่างเป็นทางการในแง่ของจำนวนผู้เสียชีวิตที่ร้ายแรงและภายนอกนั้นคล้ายกับการโจมตีทางไซเบอร์ทั่วไป อันที่จริงมีช่องโหว่ขนาดใหญ่ระหว่างอันตรายที่สันนิษฐานไว้กับกิจกรรมการก่อการร้ายทางอินเทอร์เน็ตที่เป็นที่รู้จัก อย่างไรก็ตาม ด้วยวิวัฒนาการอย่างรวดเร็วของเทคโนโลยี จึงเป็นเพียงเรื่องของเวลา ก่อนอันตรายจากการก่อการร้ายในโลกไซเบอร์ที่คุกคามถึงชีวิตจะปรากฏขึ้น

การขาดคำจำกัดความของการก่อการร้ายที่เป็นที่ยอมรับในระดับสากลเป็นอุปสรรคในการอธิบายธรรมชาติของการก่อการร้ายทางอินเทอร์เน็ต โดยไม่กล่าวถึงการก่อการร้ายตามแบบแผน โดยทั่วไป จำเป็นต้องมีคำจำกัดความทั่วไปด้วยเหตุผลสองประการ: ประการแรก เพื่อกำหนดสถานะของกฎหมายจารีตประเพณีที่เกี่ยวข้องกับการใช้กำลังในการก่อการร้าย และประการที่สอง การทำให้การกระทำดังกล่าวเป็นอาชญากร กล่าวคือ เพื่อป้องกันการก่อการร้าย ประณาม และลงโทษ น่าสังเกตเช่นกันว่าความต้องการระหว่างประเทศในการส่งผู้ร้ายข้ามแดนผู้กระทำความผิดนั้นเกินกว่าแรงกดดันให้ส่งผู้ร้ายข้ามแดนผู้กระทำความผิดทั่วไป

อย่างไรก็ตาม จากมุมมองทางกฎหมาย ข้อเสนอแนะของอดีตเลขาธิการใหญ่นั้นสนับสนุนมากกว่าที่จะเป็นนวัตกรรม เนื่องจากมีคำจำกัดความหลักที่คล้ายคลึงกัน (บางส่วนคล้ายกับอนุสัญญาว่าด้วยการป้องกันและลงโทษการก่อการร้าย พ.ศ. 2480 ที่ไม่เคยมีผลใช้บังคับ) ที่มีอยู่ในร่างอนุสัญญาครอบคลุมเรื่องการก่อการร้ายระหว่างประเทศยังคงไม่เปลี่ยนแปลง ตั้งแต่ปี 2544 (U.N. Report of the Working Group, 2010)

บุคคลใดกระทำความผิดตามความหมายของอนุสัญญาฉบับปัจจุบัน หากบุคคลนั้นกระทำโดยมิชอบด้วยกฎหมายและโดยเจตนาไม่ว่าด้วยวิธีการใด ๆ

1. การเสียชีวิตหรือการบาดเจ็บทางร่างกายอย่างรุนแรงต่อบุคคลใด ๆ หรือ

2. ความเสียหายร้ายแรงต่อทรัพย์สินสาธารณะหรือส่วนตัว รวมทั้งสถานที่สาธารณะ สถานที่ราชการ สถานที่ราชการ ระบบขนส่งมวลชน สิ่งอำนวยความสะดวกโครงสร้างพื้นฐาน หรือต่อสิ่งแวดล้อม; หรือ

3. ความเสียหายต่อทรัพย์สิน สถานที่ สิ่งอำนวยความสะดวก หรือระบบที่อ้างถึงในวรรค 1(b) ของบทความปัจจุบันที่ส่งผลหรือมีแนวโน้มว่าจะส่งผลให้เกิดความสูญเสียทางเศรษฐกิจครั้งใหญ่เมื่อวัตถุประสงค์ของการกระทำโดยธรรมชาติหรือบริบทคือการข่มขู่ประชาชนหรือเพื่อบังคับให้รัฐบาลหรือองค์กรระหว่างประเทศทำหรืองดเว้นจากการกระทำใด ๆ

ข้อเสนอแนะต่าง ๆ ที่นักวิชาการจัดทำขึ้นเกี่ยวกับวิธีการให้คำจำกัดความแนวคิดนี้เป็นเพียงบางส่วนที่ทับซ้อนกันและมีขอบเขตจากคำแนะนำเหล่านั้นรวมถึงแง่มุมทางสังคม (การก่อการร้ายเกิดจาก “ความเห็นแก่ตัว การไม่อดทนอดกลั้น การขาดการสนทนาและความไร้มนุษยธรรม ความโลภและความรับผิดชอบ) หรือทางจิตวิทยา (การก่อการร้ายเป็นกลวิธีในการบีบบังคับการเปลี่ยนแปลงทางพฤติกรรมในปฏิปักษ์) สู่แนวทางทางกฎหมายที่ละเอียดถี่ถ้วน (“คนต้องแยกแยะระหว่างทัศนคติ [และ] วิธีการ” ของการก่อการร้าย)

อย่างไรก็ตาม คำถามก็คือว่าคำจำกัดความที่แนะนำนี้ทำให้ระบอบกฎหมายระหว่างประเทศที่มีอยู่แล้วคลายความผิดทางอาญาโดยไร้เหตุผลอย่างไร้เหตุผลหรือไม่ สิ่งนี้มีความเกี่ยวข้องอย่างยิ่งกับการโจมตีทางไซเบอร์ การกำหนด การก่อการร้ายไซเบอร์ เป็นตัวแปรตามสิ่งที่ทำให้การ

ก่อการร้ายในโลกไซเบอร์แตกต่างจากการก่อการร้ายทั่วไป คือการใช้เครือข่ายคอมพิวเตอร์ (ส่วนใหญ่เป็นอินเทอร์เน็ต) โดยพื้นฐานแล้วเป็นการใช้ลิงก์อิเล็กทรอนิกส์เพื่อดำเนินการโจมตีของผู้ก่อการร้าย ซึ่งมักเกี่ยวข้องกับโปรแกรมที่สร้างขึ้นเพื่อจุดประสงค์นั้น โปรแกรมเหล่านี้สามารถส่งไปยังปลายทางได้ผ่านทางอินเทอร์เน็ต อุปกรณ์จัดเก็บข้อมูลแบบพกพา (เช่น การ์ด USB) สัญญาณวิทยุไร้สาย หรือวิธีการอื่นๆ ที่คล้ายคลึงกัน การก่อการร้ายทางอินเทอร์เน็ตควรพิจารณาแยกจากการใช้อินเทอร์เน็ตของผู้ก่อการร้าย ซึ่งเกี่ยวข้องกับแง่มุมต่าง ๆ เช่น การสื่อสาร การสรรหาบุคลากร การระดมทุน การจัดระเบียบการโจมตีทางกายภาพ การโฆษณาชวนเชื่อ (รวมถึงในรูปแบบ "การแฮdข้อมูลด้วย") การยั่วยุให้เกิดการก่อการร้ายและคำขอโทษของการก่อการร้าย ในเวลาเดียวกัน การดำเนินการทางไซเบอร์บางอย่าง (เช่น การบุกรุกฐานข้อมูลโครงสร้างพื้นฐานที่สำคัญเพื่อรวบรวมข้อมูลเกี่ยวกับเป้าหมายที่มีช่องโหว่) อาจเป็นสาเหตุของกลุ่มหัวรุนแรงทางอินเทอร์เน็ต แต่ไม่ได้เป็นการกระทำของการก่อการร้ายทางไซเบอร์ด้วยตัวมันเอง นักวิชาการอย่าง Conway ยังเสนอให้แบ่งการโจมตีทางไซเบอร์ออกเป็น "การใช้" ทางอินเทอร์เน็ต (การแสดงความคิดและการสื่อสาร) "การใช้ในทางที่ผิด" (การรบกวนหรือประนีประนอมเว็บไซต์หรือโครงสร้างพื้นฐาน) "การใช้ที่ไม่เหมาะสม" (การใช้อินเทอร์เน็ตเพื่อ ก่อให้เกิดความเสียหายหรือมีส่วนร่วมในการโจรกรรม) และ“การก่อการร้ายทางอินเทอร์เน็ต” (Conway, 2003)

คำว่า "การก่อการร้ายทางอินเทอร์เน็ต" เกิดขึ้นก่อนเหตุการณ์ 9/11 แม้ว่าจะไม่มีคำจำกัดความสากลของ "การโจมตีทางไซเบอร์" และ "การก่อการร้าย" จึงส่งผลให้ผู้เชี่ยวชาญทุกคนนิยามคำศัพท์ของตนเอง การสื่อสารที่สับสนได้ทวีความรุนแรงมากขึ้น มีแนวโน้มที่จะถูกจำแนกให้เป็นการโจมตีทางไซเบอร์เล็กน้อยมากกว่าการเป็น “การก่อการร้ายทางอินเทอร์เน็ต” (Berner, 2003)

4.8.2 ประเด็นการก่อการร้ายไซเบอร์และความชอบธรรมตามกฎของสงคราม (CYBERTERRORISM AND JUS AD BELLUM)

การป้องกันตัวเองจากการก่อการร้าย (Self-Defense Against Terrorism)

รัฐบาลในปัจจุบันตระหนักถึงความเปราะบางของโครงสร้างพื้นฐานภายในประเทศและภัยคุกคามที่อาจเกิดขึ้นจากการก่อการร้ายทางอินเทอร์เน็ต อย่างไรก็ตามวิธีการใหม่ ๆ ในการโจมตีทางไซเบอร์กำลังถูกพัฒนาเพิ่มขึ้นเรื่อย ๆ (U.S. DEP’T OF DEF., 2006) จากการร่วมมือจากแฮกเกอร์ทั่วโลกความร่วมมือระหว่างรัฐที่ล้าหลัง ตัวอย่าง เช่น เมื่อคณะทำงานเฉพาะกิจเพื่อต่อต้านการก่อการร้ายของสหประชาชาติ (CTITF) ด้านการต่อต้านการใช้อินเทอร์เน็ตเพื่อจุดประสงค์ในการก่อการร้ายขอให้ประเทศต่างๆ ส่งรายงานปี 2552 มีเพียงสองรัฐเท่านั้นที่ระบุว่าการโจมตีทางไซเบอร์โดยผู้ก่อการร้ายเป็นหนึ่งในภัยคุกคามที่เกี่ยวข้องกับพวกเขา (U.N. Counter-Terrorism

Implementation Task Force, 2009) สิ่งนี้ตรงกันข้ามกับการพัฒนาอย่างรวดเร็วของความสามารถในการป้องกันทางไซเบอร์และการโจมตีทางไซเบอร์โดยสหรัฐอเมริกา จีน รัสเซีย อิหร่าน คิวบา อิสราเอล สหราชอาณาจักร และอื่นๆ โดยเสนอแนะว่ารัฐเหล่านี้สนับสนุนการใช้กำลังของตน สิทธิในการป้องกันตนเองส่วนบุคคล (ต่อต้านผู้ก่อการร้ายในโลกไซเบอร์) ต่อการดำเนินการร่วมกันในอนาคต

ในความเป็นจริง ประเทศสองประเทศที่โดดเด่นในด้านการใช้กำลังอย่างต่อเนื่องกับผู้ก่อการร้ายและรัฐที่ให้ที่พักพิงแก่พวกเขา คือ ประเทศอิสราเอลและประเทศสหรัฐอเมริกา ทั้งสองรัฐดำเนินการนอกเหนือภาระผูกพันทางกฎหมาย และถูกกล่าวหาว่าทั้งสองประเทศลงทุนอย่างหนักในการรณรงค์ต่อต้านการก่อการร้ายทางทหาร

แม้จะมีการประณามจากคณะมนตรีความมั่นคงในปฏิบัติการ "การป้องกันตัวเอง" ต่อการโจมตีของผู้ก่อการร้ายครั้งก่อน เช่น การจู่โจมสนามบินเบรุตในปี 2511 การบุกโจมตีเลบานอนในปี 2516 การทิ้งระเบิดของ PLO สำนักงานใหญ่ในตูนิเซียในปี 1985 และการลอบสังหาร Khalil al-Wazir ในปี 1988 อิสราเอลยังคงยืนหยัดโดยตำแหน่งในการตีความสิทธิ์ในการป้องกันตัวเองในวงกว้าง และมีแนวโน้มที่จะทำเช่นนั้นในส่วนที่เกี่ยวกับผู้ก่อการร้ายทางอินเทอร์เน็ตนัดหยุดงาน เช่นกัน แม้ว่าประชาคมระหว่างประเทศจะยังไม่มั่นใจกับข้อโต้แย้งของอิสราเอล แต่หลังจากเหตุการณ์ 9/11 ไม่ได้กีดกันอย่างชัดเจนถึงความเป็นไปได้ในการป้องกันตัวเองจากองค์กรต่าง ๆ เช่น ฮิซบอลเลาะห์และฮามาส (Van Steenberghe, 2010) และชอบที่จะจดจ่อกับประเด็นเรื่องสัดส่วนมากกว่าในการประเมินความถูกต้องตามกฎหมายของการโจมตีทางอากาศใกล้กับดามัสกัสในปี 2546 การรุกรานเลบานอนในปี 2549 (Tams, 2009) และการทิ้งระเบิดฉนวนกาซาในปี 2550-2555

การประณาม "การป้องกันตัวเอง" ของสหรัฐฯ ต่อผู้ก่อการร้ายไม่น่าจะเกิดขึ้นในคณะมนตรีความมั่นคงเนื่องจากการยับยั้งของสหรัฐฯ อย่างไรก็ตาม สมัชชาใหญ่สามารถผ่านมติ 41/38 ประณามการวางระเบิดของลิเบียจามาฮิริยาในปี 2529 เพื่อตอบสนองต่อการวางระเบิดดิสโก้เทคในกรุงเบอร์ลิน ปฏิบัติการ "ต่อต้านผู้ก่อการร้าย" ของสหรัฐอเมริกาในอิรักในปี 2536 เช่นเดียวกับในซูดานและอัฟกานิสถานในปี 2541 (Tams, 2009) ยังคงตั้งคำถามเกี่ยวกับความถูกต้องตามกฎหมายจนถึงปี 2544 เมื่อคณะมนตรีความมั่นคงตามมติ 1368 ระบุอย่างหนักแน่นว่าสหรัฐฯ มีสิทธิ์ เพื่อใช้การป้องกันตัวกับองค์กรก่อการร้าย สิ่งนี้ได้รับการยืนยันโดยการอนุมัติอย่างเงียบ ๆ ของประชาคมระหว่างประเทศเกี่ยวกับการรุกรานอัฟกานิสถานในปี 2544 และโดยทัศนคติทางกฎหมายที่นำมาใช้ในสหรัฐอเมริกาเอง (ประธานาธิบดีมีอำนาจทั้งตามรัฐธรรมนูญและตามกฎหมายในการใช้กองกำลังติดอาวุธในการปฏิบัติการทางทหาร ต่อต้านผู้ก่อการร้าย ภายในสหรัฐอเมริกา) (Tams, 2009) ซึ่งจะสะท้อนถึงการก่อการร้ายทางไซเบอร์อย่างหลีกเลี่ยงไม่ได้เช่นกัน

ประเทศอื่น ๆ ยังได้ใช้มาตรา 51 ของกฎบัตรสหประชาชาติ เพื่อแสดงเหตุผลในการโจมตีกลุ่มผู้ก่อการร้ายด้วยผลตอบรับที่หลากหลาย ตัวอย่างเช่น ปฏิกิริยาต่อการรุกรานของตุรกี

หลายครั้งในอิรักตอนเหนือในช่วงสองทศวรรษที่ผ่านมาเพื่อไล่ตามพรรคแรงงานเคอร์ดิสถานมีตั้งแต่ความเข้าใจไปจนถึง "ความเห็นอกเห็นใจและความห่วงใยปะปนกัน" (Van Steenberghe, 2010) ตัวอย่างเพิ่มเติมที่มีการใช้ข้อโต้แย้งในการป้องกันตัวเองในความสัมพันธ์กับผู้ก่อการร้าย รวมถึงการไล่ล่าของรัสเซียเพื่อขับไล่นักสู้เชเชนเข้าสู่จอร์เจีย การโจมตีของอิหร่านต่อฐานทัพมูจาฮีดินของอิรักและกลุ่มชาวเคิร์ดในอิรัก การมีส่วนร่วมของเอธิโอเปียในสงครามกลางเมืองโซมาเลียในปี 2549 คนโคลอมเบียการรุกรานดินแดนเอกวาดอร์ในปี 2551 เพื่อต่อสู้กับ FARC (Tams, 2009) และการไล่ล่าของ Al Shabaab ของเคนยาในปี 2554

แม้ว่าตัวอย่างเหล่านี้จะไม่เกี่ยวข้องกับผู้ก่อการร้ายทางไซเบอร์โดยตรง แต่ก็แสดงให้เห็นว่ารัฐอาจตอบสนองต่อการโจมตีทางไซเบอร์อย่างร้ายแรงจากผู้ที่ไม่ฝักใฝ่ฝ่ายใด สิ่งนี้มีความสำคัญอย่างยิ่ง เนื่องจากยังไม่มีประเทศใดประเทศหนึ่งที่ยอมรับความพยายามในการโจมตีทางไซเบอร์จนถึงทุกวันนี้ และคาดว่าผู้กระทำการที่ไม่ใช่ของรัฐมีแนวโน้มที่จะมีส่วนร่วมในกิจกรรมดังกล่าวมากกว่า จากมุมมองของกฎหมายระหว่างประเทศ การสร้างตราสินค้าให้กับกลุ่มหรือองค์กรที่มีความสามารถเชิงรุกทางไซเบอร์ “ผู้ก่อการร้าย” นั้นไม่เพียงพอ (Walter, 1969) เพื่อให้รัฐใช้สิทธิในการป้องกันตนเองจากกลุ่มผู้ก่อการร้ายทางอินเทอร์เน็ต ฝ่ายหลังควรเปิดตัว (หรือ เนื้อหามีแผนจะเปิดตัว) การจู่โจมทางอินเทอร์เน็ตที่จะถือเป็นทั้ง "การใช้กำลัง" ที่ผิดกฎหมายและ"การโจมตีด้วยอาวุธ"

แม้ว่า ICJ จะสรุปในคดีกำแพงว่า “มาตรา 51 ยอมรับการมีอยู่ของสิทธิในการป้องกันตัวเองโดยธรรมชาติในกรณีของการโจมตีด้วยอาวุธโดยรัฐหนึ่งกับอีกรัฐหนึ่ง” (Shiryaev, 2010) ศาลไม่ใส่ใจที่จะสังเกตว่าสิทธิที่จะปกป้อง ตนเองต่อต้านผู้กระทำการนอกภาครัฐที่ก้าวร้าวมีอยู่ในกฎหมายจารีตประเพณีระหว่างประเทศ (เช่น นอกมาตรา 51) ตั้งแต่สมัยโบราณ นอกจากนี้ ไม่มีข้อความในมาตรา 51 ที่ระบุว่า “การป้องกันตัวเองมีให้ใช้ได้ เฉพาะเมื่อมีการโจมตีด้วยอาวุธโดยรัฐ” (Shiryaev, 2010)

ในบริบทของการก่อการร้ายในโลกไซเบอร์ นี่หมายความว่าประเทศที่ควบคุม สนับสนุน ฉวยโอกาส หรือทนต่อการโจมตีของผู้ก่อการร้ายในโลกไซเบอร์ หากการโจมตีเล็ดลอดออกมาจากส่วนต่างๆ ของรัฐที่ล้มเหลวซึ่งรัฐบาลไม่สามารถควบคุมได้ ดินแดนเหล่านั้นก็จะถูกป้องกันตัวด้วยเช่นกัน แม้ว่าจะไม่น่าเป็นไปได้ แต่ปัญหาอาจเกิดขึ้นเมื่อรัฐบาลไม่ต้องการทนต่อการก่อการร้ายทางอินเทอร์เน็ต (เช่น รัฐบาลได้ให้สัตยาบันอนุสัญญาต่อต้านการก่อการร้ายที่เรียกร้องให้ส่งผู้ร้ายข้ามแดนหรือดำเนินคดี) แต่ไม่สามารถระบุตัวผู้กระทำความผิดได้ สิ่งนี้มีความเกี่ยวข้องโดยเฉพาะอย่างยิ่งหากมีการโจมตีทางไซเบอร์ที่ทำลายล้างโดยบุคคลเพียงคนเดียว การปฏิบัติการทางทหารกับส่วนต่างๆ ของประเทศในการไล่ล่าชายเพียงคนเดียวนั้นไม่เคยเกิดขึ้นมาก่อน (พิจารณา Osama bin Laden) แต่พวกเขาจะตั้งคำถามเกี่ยวกับความเหมาะสมอย่างหลีกเลี่ยงไม่ได้ เนื่องจาก

สถานการณ์ดังกล่าวไม่ครอบคลุมถึงกฎหมายระหว่างประเทศ รัฐเจ้าภาพจึงเหลือทางเลือกเดียวที่จะหันไปใช้คณะมนตรีความมั่นคง

4.8.3 การโจมตีด้วยอาวุธโดยผู้ก่อการร้ายทางไซเบอร์ (Armed Attacks by Cyberterrorists)

เมื่อพูดถึงขนาดของการโจมตีของผู้ก่อการร้ายในโลกไซเบอร์ที่จำเป็นในการไปถึงเกณฑ์ "การโจมตีด้วยอาวุธ" เราสามารถเทียบเคียงกับกรณีก่อนหน้านี้ได้ ตัวอย่างเช่น การควบคุมการบินเข้าไปในอาคารพลเรือนสอดคล้องกับเหตุการณ์ 9/11 ว่ารัฐเหยื่อควรมีสิทธิในการป้องกันตัว การจัดหาซอฟต์แวร์และ"การสนับสนุนอื่น ๆ " โดยรัฐเจ้าภาพจะไม่ถือเป็น"การโจมตีด้วยอาวุธ" (Watkin, 2004) แต่สิ่งนี้จะทำให้ประเทศเป็นผู้สนับสนุนการก่อการร้ายโดยรัฐทำให้รัฐเหยื่อหันไปใช้การป้องกันตัวกับมัน

ประชากรในวงกว้างมีศักยภาพที่จะสร้างความเสียหายต่อสิ่งแวดล้อมในอนาคต อาหาร และระบบนิเวศและก่อให้เกิดความบกพร่องทางพันธุกรรมและความเจ็บป่วยในรุ่นต่อๆ ไป" (Watkin, 2004) กรณีของการก่อการร้ายทางอินเทอร์เน็ตบางกรณีสามารถยกเว้นจากกรอบการป้องกันตัวเองได้อย่างปลอดภัย—เช่น การขโมยเงินทุนสำหรับองค์กรก่อการร้ายผ่านอินเทอร์เน็ตจะไม่ถึงระดับ "การใช้กำลัง" หรือการทำลายเครื่องหมุนเหวี่ยงในโรงงานเสริมสมรรถนะยูเรเนียมเพียงอย่างเดียวไม่สามารถเข้าถึงเกณฑ์ "การโจมตีด้วยอาวุธ" เนื่องจากความรุนแรงต่ำ ส่วนมากจะขึ้นอยู่กับสถานการณ์แต่ละอย่างของแต่ละสถานการณ์และส่วนใหญ่แล้วจะเป็นสถานการณ์ทางการเมือง อย่างไรก็ตาม จำเป็นอย่างยิ่งที่จะต้องรักษาเกณฑ์ที่เหมาะสมที่สุดสำหรับการอ้างสิทธิ์ในการป้องกันตัวเองในกฎหมายระหว่างประเทศ—เกณฑ์ที่ต่ำมากจะทำให้เส้นแบ่งระหว่างการขัดกันทางอาวุธและการบังคับใช้กฎหมายอาญาไม่ชัดเจน ในขณะที่เกณฑ์ที่สูงมากจะทำให้รัฐตกอยู่ในความเสี่ยง

เช่นเดียวกับกรณีของการโจมตีทางไซเบอร์ทั่วไป การป้องกันตัวเองจากการก่อการร้ายทางไซเบอร์จำเป็นต้องมีการตอบสนองตามความจำเป็นและเป็นสัดส่วน สิ่งนี้มีความสำคัญโดยเฉพาะอย่างยิ่งในแง่ของความไม่แน่นอนทางกฎหมายเกี่ยวกับการก่อการร้าย การโจมตีของผู้ก่อการร้ายประกอบด้วย "การกระทำที่คาดเดาไม่ได้ ฉับพลัน และทันที" เป็นส่วนใหญ่ การกระทำ "ป้องกัน" ที่ขัดแย้งกันในทางกฎหมาย เช่น การสังหารโดยมีเป้าหมายอาจถูกปฏิบัติต่อผู้ก่อการร้ายในโลกไซเบอร์ อาจถูกใช้ในกรอบของ "การทำสงครามกับการก่อการร้ายทางอินเทอร์เน็ต" ในอนาคต สิ่งนี้มีความเกี่ยวข้องโดยเฉพาะอย่างยิ่งเนื่องจากบางรัฐเริ่มอนุญาตให้ค้นหาคอมพิวเตอร์ของผู้ต้องสงสัยอาชญากรจากระยะไกล (Pradillo, 2011)

โดยทั่วไป การก่อการร้ายในโลกไซเบอร์เรียกร้องให้มีการตีความหลักการความจำเป็นและสัดส่วนใหม่อีกครั้งในมุมมองใหม่ ไม่เพียงแต่รัฐจะต้องแสดงหลักฐานที่ชัดเจนและ

น่าเชื่อถือเกี่ยวกับความจำเป็นในการใช้กำลังในการป้องกันตัวต่อการกระทำที่ติดตามไม่ได้ง่าย ๆ แต่ยังต้องอธิบายด้วยว่าเหตุใดบุคคลต่างๆ ซึ่งบางคนไม่เคยพกปืนติดตัว มือควรจะกำหนดเป้าหมายทางทหาร นอกจากนี้การขจัดความแตกต่างระหว่างการสงวนตัวและการป้องกันตัวล่วงหน้า เนื่องจากช่วงเวลาของ “ความฉับไว” นั้นไม่สามารถคาดเดาได้ จึงหันไปใช้การป้องกันตัวเองอย่างถูกกฎหมาย (Pradillo, 2011) ดังนั้น เป็นไปได้ก็ต่อเมื่อการโจมตีของผู้ก่อการร้ายในโลกไซเบอร์ยังคงเพิ่มขนาดขึ้นเรื่อย ๆ อาจถึงระดับ "การโจมตีด้วยอาวุธ" ในการโจมตีครั้งต่อไป หรือหากมีการโจมตีทางไซเบอร์และสถานะที่ร้ายแรงเหมือนกันเท่านั้น

4.8.4 การวิเคราะห์จากทฤษฎีเข็มทิ่ม (Needle-Prick Theory)

ก่อนที่อินเทอร์เน็ตจะกลายเป็นสากล อันโตนิโอ อ้างว่า “เพื่อให้เข้าข่ายเป็นการโจมตีด้วยอาวุธ กฎหมายระหว่างประเทศกำหนดให้การกระทำของผู้ก่อการร้ายเป็นส่วนหนึ่งของรูปแบบการก่อการร้ายที่รุนแรงอย่างสม่ำเสมอ แทนที่จะเป็นเพียงการโจมตีแบบโดดเดี่ยวหรือเป็นระยะๆ” (Cassese, 1989) เมื่อไซเบอร์สมัยใหม่มีการโจมตีแสดงถึงปรากฏการณ์ที่แตกต่างไปจากเดิมอย่างสิ้นเชิง ซึ่งเป็นรูปแบบต่อเนื่องของความพยายามในการเข้าสู่ระบบที่มีโอกาสประสบความสำเร็จค่อนข้างต่ำ ส่วนใหญ่เป็นเป้าหมายที่ "ร้ายแรง" แม้ว่าการแอบดูวัตถุระเบิดบนเครื่องบินอาจทำได้ง่ายกว่าการชนมันโดยใช้คอมพิวเตอร์ แต่การก่อการร้ายทางอินเทอร์เน็ตนั้นไม่ใช่สิ่งที่เป็นไปไม่ได้ และดังที่ได้กล่าวไว้ก่อนหน้านี้ จะมีความเป็นไปได้มากขึ้นเมื่อมีการพัฒนาเทคโนโลยี การก่อการร้ายทางไซเบอร์สามารถอยู่ในรูปแบบของการโจมตีทางไซเบอร์หลายครั้งกับเป้าหมายแบบสุ่ม (เช่น คอมพิวเตอร์ในโรงพยาบาลของประเทศ) เช่นเดียวกับในกรณีของการก่อการร้ายแบบดั้งเดิม

การโจมตีสามารถ "สะสมในลักษณะ” เนื่องจากเกี่ยวข้องกับการโจมตีของผู้ก่อการร้ายรายย่อยอย่างต่อเนื่อง อย่างไรก็ตาม ทฤษฎีเข็มทิ่ม (หรือการสะสมของทฤษฎีเหตุการณ์) ไม่เคยได้รับการรับรองอย่างเป็นทางการโดยคณะมนตรีความมั่นคง การวัดความรุนแรงของการโจมตีแต่ละครั้ง ควรพิจารณาถึงผลสะสมของการโจมตีแบบต่อเนื่องโดยแทนที่ไม่นับทันทีหลังจากการโจมตีครั้งเดียว ดังนั้นสิทธิในการป้องกันตัวเองยังคงมีอยู่และอนุญาตให้รัฐดำเนินการบังคับที่จำเป็นเพื่อยุติห่วงโซ่การโจมตี

ทฤษฎีนี้ยังกล่าวถึงในบริบทของการก่อการร้ายทางไซเบอร์ เนื่องจากอย่างน้อยสองรัฐที่มีความสามารถในการโจมตีทางไซเบอร์อย่างร้ายแรง ได้แก่ สหรัฐอเมริกาและอิสราเอล ที่ได้กล่าวไปแล้วนั้นได้หันไปใช้แนวทาง "ผลกระทบสะสม" โดยเฉพาะเพื่อตอบสนองต่อการกระทำของการโจมตีของผู้ก่อการร้ายในโลกไซเบอร์มีความเข้มข้นน้อยกว่าการโจมตีของผู้ก่อการร้ายแบบเดิม ๆ ดังนั้นจึงมีความเป็นไปได้มากกว่าที่ชุดของการโจมตีที่สร้างความเสียหาย (เช่น รูปแบบของการลอบ

สังหารแบบสุ่มโดยใช้คอมพิวเตอร์ทางการแพทย์-อุปกรณ์ในสถานะเดียว) สามารถกระตุ้นให้เหยื่อรัฐหันไปใช้หลักคำสอนของทฤษฎี

ในกรณีของการตอบสนองแบบปกติ การป้องกันตัวเองจากการก่อการร้ายทางอินเทอร์เน็ตนั้นมีความชั่วร้ายเหมือนกัน: การตอบสนองดูเหมือนเป็นการตอบโต้ มันจะข้ามพรมแดนที่ได้รับอนุญาตของการดำเนินการยึดหน่วงและจะไม่สมส่วนกับการโจมตีทางไซเบอร์โดยแยกตัว แม้ว่าทฤษฎีนี้จะได้รับการยอมรับในอนาคตในกฎหมายจารีตประเพณีระหว่างประเทศกับการก่อการร้ายทางไซเบอร์ จะถูกจำกัดไว้เช่นเดียวกันกับการป้องกันตัวเองแบบเดิม ๆ ความจำเป็น ความได้สัดส่วน การขาดวิธีการอื่นๆ ตลอดจนการหมดไปของสิทธิในการป้องกันตัวเองต่อไป คณะมนตรีความมั่นคงได้ดำเนินการแล้ว จนกว่า UNSC หรือ ICJ จะยอมรับความถูกต้องตามกฎหมายของวิธีการของทฤษฎีหรือจนกว่าจะมีหลักฐานเพียงพอที่จะชี้ให้เห็นว่าทฤษฎีนี้ถูกรวมเข้ากับกฎหมายจารีตประเพณีระหว่างประเทศ รวบรวมการโจมตีของผู้ก่อการร้ายในโลกไซเบอร์โดยขาดการโจมตีด้วยอาวุธเพื่อจุดประสงค์ในการปลุกระดม การป้องกันตัวเองจะยังคงผิดกฎหมาย

4.8.5 การก่อการร้ายในบริบทของกฎหมายมนุษยธรรมระหว่างประเทศ (CYBERTERRORISM AND JUS IN BELLO) ความซับซ้อนทั่วไป (General Complexities)

กฎหมายมนุษยธรรมระหว่างประเทศมีความเหมาะสมเพียงพอที่จะจัดให้มี “กรอบการกำกับดูแล” และ “กลไกที่มีประสิทธิภาพ” เพื่อลงโทษการก่อการร้าย Condorelli และ Naqvi กล่าวเสริมว่าประณามการก่อการร้ายในความขัดแย้งระหว่างประเทศและภายในและเสนอ ระบบการดำเนินคดีและการลงโทษผู้ที่กระทำความผิด (Condorelli & Naqvi, 2004) ซึ่งแตกต่างจากกฎหมายสิทธิมนุษยชน กฎหมายด้านมนุษยธรรมคำนึงถึงความรุนแรงหรือลักษณะที่เป็นระบบของการกระทำของผู้ก่อการร้ายที่เกิดขึ้นระหว่างความขัดแย้ง

เส้นแบ่งระหว่างการใช้กำลังและกฎหมายด้านมนุษยธรรมนั้นไม่ชัดเจน (Crawford, 2003) โดยธรรมชาติของการก่อการร้ายซึ่งอาจจะหรืออาจจะไม่เริ่มจากการขัดแย้งทางอาวุธ แต่ขึ้นอยู่กับสถานการณ์เฉพาะ บางครั้งการก่อการร้ายเพียงครั้งเดียวก็ไม่สามารถนับได้ ดังนั้น เราจึงต้องสันนิษฐานว่าการโจมตีของผู้ก่อการร้ายทางไซเบอร์เพียงครั้งเดียวไม่สามารถเริ่มต้นสงครามได้ แม้ว่าเหตุการณ์หลังเหตุการณ์ 9/11 จะบ่งบอกถึงสิ่งที่ตรงกันข้าม

ความซับซ้อนเพิ่มเติมยังมาจากลักษณะการโต้เถียงของปฏิบัติการต่อต้านการก่อการร้ายยังสอดคล้องกับความเข้าใจดั้งเดิมของสงครามเพียงบางส่วนเท่านั้น อย่างไรก็ตามยังคงชัดเจนว่ากฎหมายมนุษยธรรมระหว่างประเทศจะมีผลบังคับใช้ในสถานการณ์ที่ การโจมตีของผู้ก่อการร้ายใน

โลกไซเบอร์จะดำเนินการโดยเป็นส่วนหนึ่งของการสู้รบทางอาวุธ หรือหากทำให้เกิดความขัดแย้งกับตนเอง

ลักษณะพิเศษของการก่อการร้ายในกฎหมายมนุษยธรรมระหว่างประเทศ (Special Nature of Terrorism in International Humanitarian Law)

การก่อการร้ายเป็นสิ่งต้องห้ามเหมือนกับการขัดกันแย้งทางทหารภายในหรือระหว่างประเทศ เช่นเดียวกับการโจมตีอื่นๆ การก่อการร้ายทางอินเทอร์เน็ตที่รุนแรงนั้นขึ้นอยู่กับหลักการของความจำเป็น ความได้สัดส่วน ความเป็นมนุษย์ ความแตกต่าง ความเป็นกลาง และความกล้าหาญ ในเวลาเดียวกัน ระเบียบการของอนุสัญญาเจนีวาห้ามเฉพาะ (Husabø & Bruce, 2009) การก่อการร้าย และ การกระทำหรือการคุกคามของความรุนแรงซึ่งมีจุดประสงค์หลักคือการแพร่กระจายความหวาดกลัวในหมู่ประชากรพลเรือน

การกระทำของการก่อการร้ายเป็นคำกริยาที่แสดงออกว่าเป็นอาชญากรรมสงครามในกฎเกณฑ์ของ ICTR (Draft of Crimes Against the Peace and Security of Mankind, 1996) และประมวลกฎหมายอาญาต่อต้านสันติภาพและความมั่นคงของมนุษยชาติ (Draft of Crimes Against the Peace and Security of Mankind, 1996) แม้ว่าจะไม่มีความเกี่ยวข้องเพียงเล็กน้อยในบริบทของการโจมตีทางไซเบอร์และทำให้อาชญากรมีการกระทำแบบสุดโต่งโดยเฉพาะ—การจับตัวประกัน

การกระทำของผู้ก่อการร้ายทางไซเบอร์ในสงคราม

การก่อการร้ายทางไซเบอร์รวมถึงการกระทำทั้งหมดในระหว่างการสู้รบด้วยอาวุธที่ทำร้าย พยายามทำร้าย และคุกคามความรุนแรงต่อพลเรือนหรือบุคคลที่ไม่ได้ต่อสู้ดิ้นรน หากมีวัตถุประสงค์เพื่อข่มขู่ประชาชน การกระทำดังกล่าว อาจรวมถึงการก่อกวนคอมพิวเตอร์ทางการแพทย์ การจู่โจมทหารของศัตรูและการทิ้งระเบิดวัตถุพลเรือน ขัดขวางการจ่ายน้ำดื่ม และการปล่อยสารเคมีอันตรายในเขตเมือง แม้ว่าการกระทำเหล่านั้นจะไม่ทำให้มีผู้บาดเจ็บล้มตายก็ตาม (Schmitt, 2010) ต้องเป็นเจตนาโดยตรงที่จะข่มขู่ เนื่องจากการแพร่กระจายความหวาดกลัวโดยไม่ได้ตั้งใจในหมู่พลเรือนพลเรือนนั้นไม่ผิดกฎหมาย หากมีการใช้ความรุนแรงต่อเป้าหมายที่ชอบด้วยกฎหมาย (Chainoglou, 2010) ตัวอย่างเช่น กลยุทธ์ “shock and awe” ของชาวอเมริกันในช่วงแรกๆ ของปี 2546 อิรักการบุกรุกที่มุ่งเป้าไปที่กองทัพอิรักนั้นถูกกฎหมาย แม้ว่าประชากรพลเรือนจะมองว่าเป็นการก่อการร้ายก็ตาม (Whitaker, 2003)

การจัดการกับการโจมตีทางไซเบอร์ที่อาจรุนแรงต่อพลเรือนหรือบุคคลที่ต่อสู้ (ในรูปแบบของการกระทำและไม่ใช่การคุกคาม) จะต้องถือเป็นการก่อการร้ายในสมัยโบราณหากดำเนินการเพื่อบีบบังคับรัฐหรือองค์กรระหว่างประเทศ ในบริบทนี้ เราอาจพิจารณา ตัวอย่างเช่น การลอบสังหารบุคคลทางไซเบอร์ที่แยกตัวออกจากกัน (Schmitt, 2010) โดยใช้เครื่องกระตุ้นหัวใจด้วย

คอมพิวเตอร์ซึ่งทำหน้าที่เป็นข้อความถึงรัฐบาล เนื่องจากจำนวนประชากรทั่วไปที่ค่อนข้างต่ำจะมีอุปกรณ์ดังกล่าว มากกว่าที่จะเป็นการข่มขู่พลเรือนทั่วไป พระราชบัญญัตินี้จะเล่นตามภาระหน้าที่ของรัฐที่จะต้องประกันความปลอดภัยของพลเมืองของตน

ในระหว่างการขัดกันด้วยอาวุธ การกระทำของการก่อการร้ายตามแบบแผนผ่านพื้นที่ทางไซเบอร์สามารถถูกมองว่าเป็นอาชญากรรมส่วนบุคคลเท่านั้นหรือผ่านปริซึมของหลักการของความจำเป็น ความได้สัดส่วน มนุษยชาติ ความแตกต่าง ความเป็นกลาง และความกล้าหาญ อย่างไรก็ตาม มีความเป็นไปได้มากกว่าที่การก่อการร้ายทางไซเบอร์แบบโบราณและแบบเดิมจะทับซ้อนกันในสงคราม

บทความปัจจุบันกล่าวถึงประเด็นทางกฎหมายเกี่ยวกับการก่อการร้ายทางไซเบอร์ ในบทแรก ผู้เขียนอธิบายว่าเหตุใดการก่อการร้ายทางไซเบอร์จึงควรอธิบายว่าเป็น “การใช้เครือข่ายอิเล็กทรอนิกส์ในรูปแบบการโจมตีทางไซเบอร์เพื่อกระทำการ ก) การกระทำที่เป็นสาระสำคัญซึ่งเป็นเครื่องมือทางกฎหมายที่มีอยู่ซึ่งห้ามการก่อการร้าย หรือ ข) การกระทำของ การก่อการร้ายภายใต้กฎหมายจารีตประเพณีระหว่างประเทศ”(Condorelli & Naqvi, 2004) นอกจากนี้ด้วยการเน้นเป็นพิเศษในอนุสัญญาต่อต้านการก่อการร้ายที่มีอยู่และกฎหมายจารีตประเพณีระหว่างประเทศ ได้มีการแสดงให้เห็นว่าผู้กระทำการใดมีแนวโน้มที่จะมีส่วนร่วมในการก่อการร้ายทางอินเทอร์เน็ต (ผู้ดำเนินการที่ไม่ใช่ของรัฐ บริษัท และบุคคล) รวมถึงเป้าหมายที่ได้รับการคุ้มครองตามกฎหมาย และเป้าหมายใดที่ผู้ก่อการร้ายจะไล่ตาม

สองบทสุดท้ายเน้นที่การอนุญาตให้บุคคลตอบสนองต่อการก่อการร้ายทางอินเทอร์เน็ตและการบังคับใช้แนวคิดนี้กับ jus in bello ผู้เขียนตั้งข้อสังเกตว่าถึงแม้การป้องกันตัวเองโดยทั่วไปจะได้รับอนุญาตแต่ทฤษฎีทางกฎหมายที่ขัดแย้งกันจะมีปัญหาในการปรับตัวให้เข้ากับความเป็นจริงของการก่อการร้ายทางอินเทอร์เน็ตโดยไม่ได้รับการสนับสนุนจากนานาชาติ ผู้เขียนยังเน้นย้ำถึงสถานการณ์ที่ขัดแย้งกันของสองระบอบที่เกี่ยวกับการก่อการร้าย (แบบโบราณและแบบแผน) (Condorelli & Naqvi, 2004) ซึ่งอยู่ร่วมกันระหว่างความขัดแย้งทางอาวุธและผลกระทบต่อการก่อการร้ายทางไซเบอร์ การบรรจบกันของระบอบการปกครองเหล่านี้ในระดับการเมืองในอนาคตจะต้องมีการประสานงานทางกฎหมายขององค์กรระหว่างประเทศ

ทั้งหมดนี้แสดงให้เห็นว่าเหตุใดการก่อการร้ายตามแบบแผนของรัฐจึงควรถูกตัดออกว่าเป็นแนวคิดที่ปฏิบัติได้จริงในกฎหมายระหว่างประเทศ ในเวลาเดียวกัน การโต้แย้งในความเห็นชอบของข้อเสนอแนะขององค์กรการประชุมอิสลามที่จะกีดกันนักต่อสู้เพื่อเสรีภาพออกจากการบังคับใช้อนุสัญญาต่อต้านการก่อการร้าย รวมถึงการรักษาสิทธิ์ของเชลยศึกโดยผู้ก่อการร้ายทั่วไปในระหว่างสงคราม เช่นเดียวกับความคลาดเคลื่อนทางกฎหมายที่สร้างขึ้นโดยระบอบอนุสัญญาว่าด้วย

การก่อการร้าย ซึ่งทำให้นักสู้อิสระและกองโจรไซเบอร์ได้รับการคุ้มครองทางกฎหมายน้อยกว่ากองกำลังทหารของรัฐแม้จะมีสถานะเท่าเทียมกันภายใต้พิธีสารเพิ่มเติม

4.8.6 การวิเคราะห์แหล่งที่มาของรายได้จากการก่อการร้ายไซเบอร์

งานแรก ๆ เกี่ยวกับ 'ภัยคุกคามทางไซเบอร์' แสดงให้เห็นภาพแฮกเกอร์ ผู้ก่อการร้าย สายลับต่างประเทศ และแก๊งอาชญากร ที่พิมพ์คำสั่งสองสามคำลงในคอมพิวเตอร์สามารถควบคุมหรือทำลายโครงสร้างพื้นฐานที่สำคัญของทั้งประเทศได้ สถานการณ์ที่น่ากลัวนี้ไม่ได้รับการสนับสนุนจากหลักฐานใด ๆ กลุ่มผู้ก่อการร้ายอย่างอัลกออิดะห์ใช้อินเทอร์เน็ตเป็นจำนวนมาก แต่เป็นเครื่องมือสำหรับการสื่อสารภายในกลุ่ม การระดมทุน และการประชาสัมพันธ์ ผู้ก่อการร้ายทางไซเบอร์ยังสามารถใช้ประโยชน์จากอินเทอร์เน็ตเพื่อขโมยหมายเลขบัตรเครดิตหรือข้อมูลที่มีค่าเพื่อให้การสนับสนุนทางการเงินสำหรับการดำเนินงานของพวกเขา การก่อการร้ายทางไซเบอร์ได้รับความสนใจอย่างมาก แต่จนถึงปัจจุบัน การกระทำดังกล่าวไม่ได้มีความหมายอะไรมากไปกว่าการโฆษณาชวนเชื่อ การรวบรวมข่าวกรอง หรือกราฟิตีทางดิจิทัลที่เทียบเท่าโดยกลุ่มต่าง ๆ เข้ามาทำลายเว็บไซต์ของกันและกัน ไม่มีโครงสร้างพื้นฐานที่สำคัญถูกปิดโดยการโจมตีทางไซเบอร์ (Eom, Kim, & Chung, 2012)

ผู้ก่อการร้ายพยายามสร้างแถลงการณ์ทางการเมืองและสร้างความเสียหายทางจิตใจและร่างกายต่อเป้าหมาย หากการก่อการร้ายเป็นการใช้ความรุนแรงเพื่อให้ได้มาซึ่งวัตถุประสงค์ทางการเมือง ผู้ก่อการร้ายจะใช้อาวุธทางเศรษฐกิจที่มีผลกระทบแบบค่อยเป็นค่อยไปและสะสมจนมีประโยชน์ หนึ่งในคู่มือการฝึกอบรมของอัลกออิดะห์ “Military Studies in the Jihad Against the Tyrants” ตั้งข้อสังเกตว่าวัตถุระเบิดเป็นอาวุธที่ผู้ก่อการร้ายนิยมใช้ เพราะ “วัตถุระเบิดโจมตีศัตรูด้วยความสยดสยองและตกใจอย่างยิ่ง” (Eom, Kim, & Chung, 2012) การระเบิดนั้นรุนแรง สร้างความหวาดกลัวให้ศัตรู และสร้างความเสียหายถาวร การโจมตีทางไซเบอร์จะไม่มีผลกระทบทางการเมืองและละครแบบเดียวกับที่ผู้ก่อการร้ายแสวงหา การโจมตีทางไซเบอร์ที่เหยื่ออาจไม่สังเกตเห็นด้วยซ้ำ หรือเกิดจากความล่าช้าหรือไฟดับเป็นประจำ จะไม่ใช่อาวุธที่พวกเขาต้องการ หากการก่อการร้ายเป็นการกระทำที่รุนแรงเพื่อสร้างความตื่นตระหนกและบรรลุวัตถุทางการเมือง ผู้ก่อการร้ายจะพบว่าการใช้การก่อการร้ายทางไซเบอร์นั้นเป็นแหล่งเครื่องมือในการสะสมทุนเพื่อการก่อการร้ายจริงหรือการก่อการร้ายแบบดั้งเดิมจะมีประโยชน์และดูสมเหตุสมผลมากกว่า

4.8.7 การวิเคราะห์พฤติกรรมทางจิตวิทยาของแฮกเกอร์และการโจมตีทางไซเบอร์

คอมพิวเตอร์ไม่สามารถทำงานได้หากปราศจากเบื้องหลังที่อยู่ภายใต้การคิดวิเคราะห์ของมนุษย์เพราะฉะนั้นการวิเคราะห์การรู้คิด (cognitive) ของมนุษย์จึงเป็นสิ่งสำคัญประการหนึ่งที่จะ

เข้าใจได้ว่าการโจมตีครั้งนี้มีจุดประสงค์เพื่ออะไร ในประเด็นนี้ผู้วิจัยจะขอยกตัวอย่างง่ายๆที่เกิดขึ้นกับสหราชอาณาจักรเมื่อปี 2018 โรงพยาบาลในขึ้นกับสหราชอาณาจักรถูไวรัส WannaCry โจมตีจงไม่สามารถทำงานได้กว่าสองอาทิตย์ที่รัฐบาลจะสามารถกู้ระบบคืนได้ ความสูญเสียครั้งนี้นับเป็นพันล้านปอนด์ ผู้ป่วยและเจ้าหน้าที่จำเป็นต้องกลับไปใช้กระดาษในการทำงาน การจู่โจมครั้งนี้ถูกวิเคราะห์แล้วว่าเป็นการกระทำของประเทศเกาหลีเหนือที่ตั้งใจจะปล่อย Ransomware มาเพื่อขู่เรียกค่าไถ่เพื่อเป็นเงินสนับสนุนในการก่อการร้ายแต่ไวรัสนั้นเกิดผิดพลาดกลายเป็น WannaCry รัฐจึงไม่ได้เสียเงินให้กับเกาหลีเหนือเพื่อกู้ระบบคืน ถึงแม้ว่ารัฐจะจ่ายเงินก็ไม่ได้หมายความว่าจะได้ข้อมูลทั้งหมดคืน แต่สิ่งที่สำคัญที่สุดในการกระทำครั้งนี้คือวัตถุประสงค์ที่รัฐบาลอังกฤษไม่สามารถหาได้ว่าเพราะเหตุใดทำไมประเทศเกากลีเหนือจึงจู่โจมโรงพยาบาลในประเทศของตน และในกรณีนี้เองจึงเป็นข้อถกเถียงที่สำคัญว่าหากเรารู้จุดประสงค์ของผู้กระทำก็จะสามารถหาวิธีป้องกันได้ก่อนที่เหตุการณ์จะเกิดขึ้น ดังนั้นกระบวนการรู้คิดของมนุษย์ที่มีต่อการโจมตีทางไซเบอร์จึงนำเสนอได้ ดังนี้ (Doffman, 2019)

รูปแบบการจูงใจของกลุ่มการก่อการร้าย ISIS ที่สามารถใช้ระบบไซเบอร์เป็นเครื่องมือที่ใช้ในการหาทรัพยากรเพื่อสนับสนุนกลุ่มตน โดยมากที่สุด ISIS สามารถหาเงินสนับสนุนเป็นรายได้กว่า 2 พันล้านล้านดอลลาร์ จากการรวบรวมจาก การบริจาคจากบริษัทเอกชน ภาษี ค่าไถ่ และรายได้ทางการค้าขาย โบโกฮาราม ขบวนการก่อการร้ายในประเทศไนจีเรีย มีส่วนร่วมในการเพิ่มการลักพาตัวและรายได้จากการกรรโชกทรัพย์ ปล้นสะดม และขโมยจากธนาคาร อีกตัวอย่าง หนึ่งคือกลุ่ม Al-Shabaab ที่ได้เงินมาจากการใช้ช่องทางทางไซเบอร์ขโมยเงินภาษีนอกอาณาของรัฐตนเองและเงินจากธุรกิจและการค้าขานยต่างๆ นอกอาณาเขต

“People are the Achilles heel of cyberspace” เป็นสำนวนหนึ่งที่แปลว่าคนที่มีความแข็งแกร่งอย่างอคิลลีส ยังมีจุดอ่อนที่จะต้องปกป้องตลอดเวลา เช่น เดียวกันกับมนุษย์ในโลกไซเบอร์และมนุษย์ก็ตระหนักได้ว่าเพื่อที่จะปกป้องตนเอง ก็นจะเป็นที่จะต้องไล่ล่าโจมตีผู้อื่นก่อนที่ผู้อื่นจะไล่ล่าเรา (Doffman, 2019)

มนุษย์เป็นผู้เริ่มที่จะปกป้องตัวเองก่อนในความมั่นคงทางข้อมูลสารสนเทศในโลกไซเบอร์และจะเป็นคนสุดท้ายที่รับรู้ว่าตัวเองจะต้องตนจะต้องใช้การปกป้องตนเองเป็นวิธีสุดท้ายในการรักษาข้อมูลเทคโนโลยีสารสนเทศในโลกไซเบอร์เช่นกัน มนุษย์สร้าง Cyber Ecosystems ที่ซับซ้อนขึ้นมาและพื้นที่นี้กลายเป็นพื้นที่ของอาชญากรทางไซเบอร์ที่สามารถเข้ามาเพื่อตักตวงผลประโยชน์ได้ง่าย เช่น การขโมยข้อมูลส่วนบุคคล หรือข้อมูลความลับต่าง ๆ ของบริษัท เมื่อมีพื้นที่ให้เหล่าแฮกเกอร์นั้นอาศัยอยู่แฮกเกอร์หรืออาชญากรไซเบอร์ ณ ที่นี้จะรู้ถึงความซับซ้อนในความนึกคิดของมนุษย์และโจมตีมนุษย์ที่เป็นเหยื่อเหล่านั้นเพราะกิจกรรมของมนุษย์ในปัจจุบันนั้นไม่สามารถแยกออกได้จากโลกของไซแบอร์ละการรักษาความมั่นคงทางไซเบอร์และสิ่งที่ยากที่สุดคือการป้องกันการโจมตีเหล่านี้คือการขาดแนวทางในการแก้ปัญหาที่เชื่อมโยงกับการโจมตีเชิงแนวคิด

สิ่งที่แสดงให้เห็นว่ามนุษย์มีจุดอ่อนในโลกไซเบอร์ คือ

1. มากกว่า 80-90% ของการจู่โจมทางไซเบอร์ที่สำเร็จมาจากความผิดลาดของมนุษย์เอง
2. การจู่โจมทางไซเบอร์เกิดขึ้นในทุกๆ 39 วินาที
3. มากกว่า 230,000 มัลแวร์ถูกสร้างขึ้นในทุกๆวัน

ทั้งหมดนี้สร้างความเสียหายให้กับทั้งโลกในแต่ละประเทศเป็นมูลค่าตามประเทศดังนี้

1. สหรัฐอเมริกา สูญเสียเป็นมูลค่า 20.49 ล้านล้านปอนด์
2. จีน สูญเสียเป็นมูลค่า 13.4 ล้านล้านปอนด์
3. ญี่ปุ่น สูญเสียเป็นมูลค่า 4.97 ล้านล้านปอนด์
4. เยอรมัน สูญเสียเป็นมูลค่า 4.00 ล้านล้านปอนด์
5. สหราชอาณาจักร สูญเสียเป็นมูลค่า 2.83 ล้านล้านปอนด์
6. ฝรั่งเศส สูญเสียเป็นมูลค่า 2.78 ล้านล้านปอนด์
7. อินเดีย สูญเสียเป็นมูลค่า 2.27 ล้านล้านปอนด์
8. อิตาลี สูญเสียเป็นมูลค่า 2.07 ล้านล้านปอนด์
9. บราซิล สูญเสียเป็นมูลค่า 1.87 ล้านล้านปอนด์
10. แคนนาดา สูญเสียเป็นมูลค่า 1.71 ล้านล้านปอนด์

มีนักวิชาการหลายคนพยายามวิเคราะห์ว่าทำไมไซเบอร์ที่พยายามจู่โจมมนุษย์เพราะมนุษย์มีความเผลอเรอ ง่ายต่อการทำผิดพลาด ถือเป็นการเปิดช่องทางให้การโจมตีเกิดขึ้นง่าย สาเหตุนี้เป็นเพราะมนุษย์มีข้อจำกัดในเรื่องของความนึกคิดและทางกายภาพ หรือไม่เป็นความผิดพลาดที่องค์กรหรือหน่วยงานต่างๆไม่ได้ติดตั้งซอฟแวร์หรือไฟล์วอร์ลที่ไม่มีประสิทธิภาพจะทำให้มีช่องโหว่เกิดกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์และไม่สามารถป้องกันการจู่โจมได้ ต่อไปนี้จะเป็นการวิเคราะห์ข้อจำกัดของมนุษย์ที่มีต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์

1. อคติ (bias)

มนุษย์ล้วนมีอคติรวมถึงการเรียนรู้ในสิ่งใหม่ๆ มนุษย์จะมีความต่อต้านต่อสิ่งใหม่ ดังนั้นการเข้ามาของเทคโนโลยีจึงสร้างความเปลี่ยนแปลงให้กับคนรุ่นเก่าเป็นอย่างมากจึงไม่แปลกใจที่ว่าคนส่วนใหญ่จะมีอคติในการใช้และจะไม่รับข้อมูลใหม่ๆที่เข้ามา (Gullone, 2000) เมื่อเทคโนโลยีมีการพัฒนา ไวรัสต่างๆที่อาศัยช่องทางทางอินเทอร์เน็ตผ่านจากระบบคอมพิวเตอร์จึงเป็นการเปิดช่องว่างทำให้แฮกเกอร์สามารถเข้าโจมตีได้ หรือแม้กระทั่งอคติขององค์กรที่ไม่ให้ความสนใจหรือความตระหนักรู้ในเรื่องของความมั่นคงปลอดภัยไซเบอร์ จึงขาดการติดระบบป้องกันที่มีประสิทธิภาพทำให้แฮกเกอร์สามารถจู่โจมเข้ามาได้ง่าย

2. การกระตุ้นความสนใจ

ในประเด็นนี้จะกล่าวถึงมนุษย์จะมีความอยากรู้อยากเห็นเกี่ยวกับสิ่งที่เกิดขึ้นกับตนเองและผู้อื่นหรือหากแฮกเกอร์รู้ความสนใจหรือรู้จุดอ่อนของผู้ที่เป็นเหยื่อก็จะสามารถส่งอีเมล์ หรือที่เรียกกันว่า Phishing เป็นต้น ในการหลอกล่อให้เหยื่อตายใจและให้พาสเวิร์ดในที่สุด (Green, 2020) หลังจากนั้นแฮกเกอร์จะสามารถขโมยข้อมูลส่วนตัวหรือหลอกถามข้อมูลต่าง ๆ ด้วยความสมัครใจของตัวเหยื่อเองได้ เพราะฉะนั้นหลักการกระตุ้นความสนใจจึงเกี่ยวข้องกับวิธีเชิงจิตวิทยาที่สัมพันธ์กับแฮกเกอร์และเหยื่อ

3. พฤติกรรมส่วนตัว

มนุษย์ส่วนใหญ่จะเคยชินกับพฤติกรรมเดิม ๆ แต่ในขณะที่เทคโนโลยีมีการเปลี่ยนแปลงอยู่ทุกเวลา ดังนั้นการยึดติดกับพฤติกรรมเดิม ๆ จะทำให้เหยื่อส่วนใหญ่ตกเป็นเป้าหมายของแฮกเกอร์ได้ง่ายขึ้น เช่น การใช้ชีวิตเป็นกิจวัตรประจำวันหรืออธิบายตาม Routine Theory ที่ผู้กระทำความผิดจะสามารถสังเกตพฤติกรรมเหยื่อได้อย่างง่ายดาย และสามารถหาช่องว่างที่จะเข้าถึงระบบของเหยื่อนั้นได้ ดังนั้นการเปลี่ยนพฤติกรรมหรือการเพิ่มความระมัดระวังให้มากขึ้นจะทำให้ผู้กระทำความผิดหรือแฮกเกอร์ไม่สามารถหาช่องว่างในการโจมตีได้ (Green, 2020)

4. อิทธิพลในการตัดสินใจ ประกอบไปด้วยความเหนื่อย ความเครียด การเบี่ยงเบนทางความคิด ภาวะหมดไฟหรือหมดพลัง

ปัจจัยภายนอกของสิ่งแวดล้อมที่มีผลต่อปัจจัยภายในของมนุษย์ใช่ภาวะความกดดันจากที่ทำงาน จากครอบครัว จากการเรียน จะทำให้มนุษย์มีการใช่ความนึกคิดที่ผิดพลาดและเป็นสาเหตุให้เกิดผลเสียหรือข้อสำกัดในการตัดสินใจ เช่น ความเหนื่อย ความเครียด เป็นปัจจัยหลักที่สำคัญที่มนุษย์จะรู้สุขหมดไฟกับสิ่งที่ทำและจะเกิดการขาดความสนใจหรือการขาดความตระหนักรู้ในสิ่งใหม่ของเทคโนโลยีซึ่งมีผลให้เกิดช่องว่างสามารถทำให้แฮกเกอร์สามารถเข้ามาจูโจมได้ การเบี่ยงเบนทางความคิดก็เช่นกัน นั่นหมายถึงการสามารถโน้มน้าวให้เหยื่อเชื่อในสิ่งที่แฮกเกอร์หรือผู้กระทำความผิดคิดว่าตนนั้นทำถูกต้องแล้วและจะสามารถได้ประโยชน์จากการใช้เทคโนโลยีในทำในสิ่งที่ผิด ดังนั้น สิ่งที่ควรระวังคือการเฝ้าความนึกคิดของผู้เป็นเหนื่อยกับความพร้อมที่ต้องทันสมัยในโลกของไซเบอร์ (Karatzogianni, 2009)

แต่อย่างไรก็ตามความเกี่ยวข้องระหว่างความถึงคิดของเหยื่อให้ผู้ก่ออาชญากรรมทางไซเบอร์นั้นเป็นไปในทางเดียวกันนั่นคือ มนุษย์มักจะมีข้อจำกัดในการตัดสินใจ ไม่ว่าคุณจะเป็นเหยื่อหรือผู้กระทำแต่ข้อจำกัดที่เกิดขึ้นนั้นจะเกิดสามารถที่จะปรากฏได้ในผู้ถูกกระทำและผู้โดนกระทำเองและนั่นเปรียบเสมือนทางอกที่จะป้องกันการเกิดการจูโจมทางไซเบอร์ที่เกิดจากข้อจำกัดของอาชญากรในโลกเสมือนจริงนั่นเอง ทั้งหมดสามารถเชื่อมโยงกับแนวคิดและแสดงให้เห็นอย่างเป็นรูปธรรม ดังนี้

5. ความเหนื่อยล้า (Fatigue)

ความเหนื่อยล้าที่เกิดขึ้นในโลกไซเบอร์ในการรักาความมั่นคงปลอดภัยของระบบเป็นปัญหาที่ยังไม่สามารถแก้ได้ และยังคงวนเวียนอยู่กับการแก้ที่ปลายเหตุเพราะแฮกเกอร์มักจะมีเทคนิคที่ไปก่อนหน้าผู้ถูกโจมตีอยู่เสมอ เพราะฉะนั้นความเหนื่อยล้าที่เกิดขึ้นจึงทำให้เจ้าหน้าที่มีความท้อแท้ที่จะป้องกันหรือหาทางจับผู้กระทำความผิด โดยเฉพาะความเหนื่อยล้าในการรักษาความมั่นคงปลอดภัยที่มีช่องว่างอยู่เสมอ เมื่อหาช่องว่างได้ การตระหนักรู้เป็นสิ่งสำคัญในการควบคุมคนในการระวังตัว หรือการสร้างพาสเวิร์ดต่างๆ ให้ปลอดภัยเพื่อไม่ให้เกิดปัญหาภายหลัง (Karatzogianni, 2009) นอกจากนี้ความยากในการปฏิบัติการป้องกันละปราบปราม การสร้างนโยบายและการสร้างข้อบังคับให้ผู้ปฏิบัติจำเป็นจะต้องมีความชัดเจนสามารถโน้มน้าวให้ผู้คนสามารถปฏิบัติได้จริง เช่น การบังคับให้ผู้ใต้บังคับบัญชารักษาความลับข้อมูลออนไลน์ในระบบของตัวเอง โดยที่จะต้องไม่คอมพิวเตอร์ที่ทำงานมาใช้ส่วนตัว หรือเก็บรักษาพาสเวิร์ดของตนให้ดีเพื่อมิใครสามารถเข้ามาล่วงรู้ความลับของหน่วยงานตนได้ และนี่คือข้อจำกัดของมนุษย์ที่จะต้องแบ่งแยกระหว่างชีวิตจริงและชีวิตในโลกไซเบอร์

ในระดับที่สูงขึ้นไปการต่อสู้หรือสงครามทางไซเบอร์จะทำให้ผู้ปฏิบัติมีความเหนื่อยล้าที่จะต้องต่อสู้กับสิ่งที่เป็นนามปธรรมในรูปแบบทางกายภาพ เพราะบางครั้งการไร้จุดหมายหรือวัตถุประสงค์ที่ชัดเจนจะทำให้กองกำลังทางไซเบอร์ขาดอุดมการณ์และพลังในการต่อสู้ ดังนั้นการต่อสู้ทางไซเบอร์จึงไม่เหมือนกับการต่อสู้ในโลกของความจริง การปลุกพลังกองกำลังจึงเป็นไปได้ยากในโลกของไซเบอร์ ความไร้ซึ่งจุดหมายจึงทำให้เกิดความเหนื่อยล้าและท้อแท้

ความเหนื่อยล้าในการจัดการกับโลกไซเบอร์นั้นมีความซับซ้อนมากและยากแก่การเข้าใจในโลกแห่งความเป็นจริง โดยเฉพาะในในโลกแห่งความจริงที่มีพร้อมอุปสรรคในเรื่องโรคระบาดยิ่งทำให้ผู้ปฏิบัติด้ายไซเบอร์มีความท้อแท้และเหนื่อยมากขึ้นเพราะทุกอย่างจะต้องขึ้นกับโลกอินเทอร์เน็ต การเฝ้าระวังภัยต่างๆ ให้กับประชาชนผู้ใช้อินเทอร์เน็ตและการเฝ้าระวังการฝ่าฝืนของประชาชนจะทำให้เจ้าหน้าที่เหล่านี้มีความเหนื่อยล้ามากยิ่งขึ้น เช่น การรวมตัวกันของแฮกเกอร์ในรูปแบบขององค์กรจะมีมากขึ้น การรวม dark web ต่างๆ (Karatzogianni, 2009) การใช้อุปกรณ์ราคาถูกที่เอื้อเฟื้อต่อการเข้าถึงอินเทอร์เน็ตและเพิ่มอัตราการเกิดอาชญากรรม การยังอยู่ในรูปของคนนิรนามที่ไม่สามารถจับตัวตนได้จริง และการไม่สามารถป้องกันเหยื่อได้เพราะมีเหยื่อจำนวนมากที่พร้อมจะตกเป็นเป้าหมายในการก่ออาชญกรรมทางไซเบอร์

6. พฤติกรรมและความนึกคิดของแฮกเกอร์

การเชื่อมโยงระหว่างแฮกเกอร์และความนึกคิดในการต่ออาชญากรรมทางไซเบอร์เป็นสิ่งที่น่าสนใจและยังไม่เคยมีงานเขียนใดๆในประเทศไทยเคยศึกษา ดังนั้นในส่วนนี้จะอธิบายพฤติทางจิตวิทยาของแฮกเกอร์เพื่อแสดงออกถึงความเข้าใจในจุดประสงค์ในการก่ออาชญากรรม พฤติกรรมของ

แฮกเกอร์ส่วนใหญ่จะมุ่งสังเกตเหยื่อที่เป็นจุดอ่อนขององค์กร เพื่อใช่เหยื่อนั้นเป็นเครื่องมือเข้าถึงความลับขององค์กร ส่วนใหญ่องค์กรโดยทั่วไปจะขาดประสิทธิภาพในการลดการจู่โจมเมื่อเหยื่อเกิดความตื่นตระหนก แต่ในปัจจุบันมีระบบ Cognitive security ที่จะสามารถใช้ AI ในการควบคุมระบบวิเคราะห์พฤติกรรมของมนุษย์ที่เป็นอยู่อย่างมีรูปแบบซ้ำๆ กัน โดยระบบ Cognitive security จะสามารถสังเกตได้ว่าสิ่งที่ปลอมแปลงเข้ามานั้นเป็นภัยต่อองค์กรหรือไม่และระบบนี้จะมีประสิทธิภาพมากเมื่อมีการอัพเดทอยู่เรื่อย ๆ และจะสามารถปกป้องไม่ให้มีแฮกเกอร์สามารถหาช่องว่างจากระบบได้ ระบบ Cognitive security ถูกพัฒนามาจากการตรวจพบ Cognitive hacking ที่สามารถหลอกลวงเหยื่อเพื่อให้สามารถบอกข้อมูลความลับของตนและองค์กร โดยการหลอกล่อคนที่เต็มไปด้วยอคติประสบการณ์ดั้งเดิม และความตระหนักรู้ที่มีจำกัด จึงทำให้แฮกเกอร์สามารถควบคุมความคิดของบุคคลเหล่านี้จากการหาประโยชน์จากคนที่อ่อนแอและมีความบกพร่องทางเทคโนโลยี (Jarvis & Macdonald, 2015)

6.1 ประเภทของ Cognitive hacking

ประเภทแรก คือ Overt การใช้วิธีการจู่โจมแบบเปิดเผย เช่น Spoofing Mail คือเมล์ที่พยายามจะหลอกผู้รับว่าเมล์ถูกส่งมาจากบุคคลอีกคนหนึ่ง หรือเมล์ที่แอบอ้างอีเมล์แอดเดรสของผู้อื่นเป็นผู้ส่ง โดยผู้ส่ง Spoofing Mail มักมีจุดประสงค์เพื่อหลอกลวงเอาข้อมูลบางอย่างจากผู้รับ หรือเพื่อหลบหลีกการตรวจจับจากระบบกรองสแปม หรือการเปลี่ยนแปลงข้อมูลในสมุดบัญชีในการทำธุรกรรม

ประเภทแรก คือ Covert การใช้วิธีการจู่โจมแบบใช้วิธีภายในแบบไม่แสดงออกให้บุคคลภายนอกสังเกตเห็น เช่น Phishing เป็นหนึ่งในการหลอกลวงทางโลกออนไลน์ที่พบได้บ่อยที่สุด Phishing มีหลายรูปแบบ การหลอกลวงประเภทนี้มักจะเกี่ยวข้องกับการใช้กลอุบายหลอกล่อผู้ใช้งาน และการแอบอ้างเป็นเว็บไซต์ที่น่าเชื่อถือ เช่น เว็บไซต์ธนาคาร หรือบัญชีโซเชียลมีเดีย ซึ่งมักจะแตกต่างจากของจริง มีการเปลี่ยนชื่อในลิงก์เพียงเล็กน้อยทำให้เราไม่สังเกต บ่อยครั้งที่แฮกเกอร์ส่งอีเมลเพื่อขอให้คุณล็อกอินเข้าสู่ระบบธนาคาร หรือหน้าบัญชีอื่น ๆ เพื่อตรวจสอบหรือยืนยันข้อมูลของคุณพร้อมกับลิงก์ไปยังเพจปลอม แต่อย่างไรก็ตามเว็บไซต์ทางการดังกล่าวก็ไม่ต้องการให้เกิดการกระทำแบบนั้นเช่นกัน หรือ Smishing” หรือ SMS phishing คือการหลอกลวงทางข้อความ โดย scammers จะแอบอ้างตัวเองว่าเป็น บริษัทที่ถูกต้องตามกฎหมาย เพื่อพยายามขโมยข้อมูลส่วนตัวหรือข้อมูลทางการเงินของเหยื่อ ด้วยการส่ง notifications ไปที่โทรศัพท์ของเหยื่อบ่อยๆ (Jarvis & Macdonald, 2015)

การโจมตีในอีกรูปแบบหนึ่งคือ หรือ Vishing ด้วยเสียงเกี่ยวข้องกับผู้โทรที่ประสงค์ร้ายโดยอ้างว่ามาจากฝ่ายสนับสนุนด้านเทคนิคหน่วยงานของรัฐหรือองค์กรอื่น ๆ และพยายาม

ดึงข้อมูลส่วนบุคคลเช่นข้อมูลธนาคารหรือบัตรเครดิต Vishing ประเภทนี้ใช้ซอฟต์แวร์โฆษณาดิจิทัลเพื่อเผยแพร่โฆษณาที่ดูธรรมดาโดยมีโค้ดที่เป็นอันตรายฝังอยู่ภายใน

โดยสรุป การใช้ Cognitive hacking จะมีเทคนิคโดยมุ่งเน้นไปยังเจ้าหน้าที่ที่ไม่ได้รับการอบรมในเรื่องของเทคโนโลยี และเป็นส่วนสำคัญให้แฮกเกอร์มุ่งเป็นเป้าหมาย ดังนั้น แฮกเกอร์จะมุ่งเรียนรู้ไปยังเป้าหมายที่มีความเป็นไปได้ที่จะถูกหลอกได้ง่าย การใช้โซเชียลมีเดีย รูปภาพ หรืออินเทอร์เน็ตเป็นอุปกรณ์ในการหลอกลวง เลือกวิธีในการใช้ไม่ว่าจะเป็นการใช้วิธีการจู่โจมแบบเปิดเผยหรือการใช้วิธีการจู่โจมแบบใช้วิธีภายในแบบไม่แสดงออกเพื่อให้เหมาะกับเป้าหมาย ทำความเข้าใจเป้าหมาย โดยเฉพาะรูปแบบของพฤติกรรมและกระแสของสังคม และสุดท้ายคือการสร้างความเป็นมิตรและความไว้ใจเพื่อที่จะหลอกล่อเป้าหมายได้สำเร็จ (Dandecha, 2019).

สำหรับเหยื่อที่จะถูกหลอกลวงเป็นเป้าหมายแล้วจะต้องระวังในพฤติกรรมไม่ว่าจะเป็นความหุนหันพลันแล่น การควบคุมตนเอง การเชื่อหรือปฏิบัติตามในสิ่งที่เป็นกฎ เชื่อฟังต่อผู้บังคับบัญชาหรือกฎขององค์กร ความเชื่อใจที่มีต่อบุคคลอื่น คำเยินยอ การข่มขู่ และความใจเร็วของตนหรือการมีความเชื่อมั่นในตนเองน้อยเกินไป

การผสานความเข้าใจทางด้านจิตวิทยาและการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Campbell, 2010)

1. การสร้างการบูรณาการและเพิ่มความเป็นมืออาชีพในทางจิตวิทยา
2. ปรับปรุงความสัมพันธ์ระหว่างมนุษย์และคอมพิวเตอร์
3. เพิ่มพื้นที่ให้มนุษย์เป็นศูนย์กลางในการรักษาความมั่นคงปลอดภัยทางไซเบอร์
4. เข้าใจและลดแรงจูงใจทางลบในการปฏิบัติหน้าที่ของผู้ปฏิบัติงาน
5. ระบุได้ถึงการปฏิบัติการที่สำคัญ ภารกิจ หน้าที่ต่างๆในไซเบอร์ได้อย่างชัดเจน

4.9 วิเคราะห์ศักยภาพการรับมือภัยคุกคามทางไซเบอร์ของประเทศไทย

หน่วยงานในประเทศไทยมีศักยภาพเพียงพอต่อการรับมือภัยคุกคามทางไซเบอร์ ตลอดจนการก่อการร้ายไซเบอร์ สามารถประเมินศักยภาพการรับมือโดยพิจารณาจากแต่ละประเด็น ดังนี้

4.9.1 ศักยภาพที่เป็นจุดแข็ง

1) ด้านกฎหมาย

ประเทศไทยมีกฎหมายตั้งพระราชบัญญัติคอมพิวเตอร์ 2550 และพัฒนามาถึงพระราชบัญญัติความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 มีเนื้อความสำคัญในการตั้งหน่วยงานเพื่อให้ประเทศไทยมีการเตรียมตัวรับมือกับภัยคุกคามไซเบอร์โดยทั้งในรูปแบบของนโยบายรัฐและกฎหมาย มีกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นหน่วยงานหลักในการออกกฎเกณฑ์ ควบคุม ดูแล ภารกิจที่เกี่ยวข้องกับไซเบอร์ทั้งหมด มีพระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ซึ่งเป็นกลไกเฝ้าระวัง ป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ที่อาจเกิดกับระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศสำคัญ (CII) และส่งผลเสียหายในระดับประเทศ (สำนักงานรัฐบาลอิเล็กทรอนิกส์, 2562)

กฎหมายของประเทศไทยนั้นถูกพัฒนาให้ทันสมัยตลอดมาเพื่อให้สามารถจับผู้กระทำผิดไปรับโทษและเป็นกรอบในการใช้ควบคู่ไปกับนโยบายเชองปฏิบัติที่มอบหมายให้ทุกหน่วยเข้ามามีส่วนร่วม มีการประชาสัมพันธ์ที่เข้าถึงประชานเพื่อให้รับรู้ในประเด็นกฎหมายต่างๆ เหล่านี้

2) งบประมาณ

เนื่องจากประเทศไทยได้มีนโยบายในการจัดตั้งสำนักงานคณะกรรมการรักษาความปลอดภัยไซเบอร์แห่งชาติเมื่อไม่นานนัก ทำให้การได้รับงบประมาณครั้งนี้เป็นครั้ง มีมูลค่า 145.3499 ล้านบาท (สำนักงานรัฐบาลอิเล็กทรอนิกส์, 2562) นอกจากนี้จากข้อมูลการสัมภาษณ์โดยเฉพาะศูนย์ไซเบอร์กองทัพอากาศและธนาคารแห่งชาติจะมีการจัดสรรงบประมาณเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์อย่างเพียงพอที่จะลงทุนซื้ออุปกรณ์และเทคโนโลยีตรวจจับใหม่ๆ เพื่อให้ทันสมัยต่อการตรวจจับผู้ก่อการร้าย นอกจากนี้ยังมีงบประมาณบางส่วนที่เตรียมไว้ทุกปีเพื่อที่จะนำไปสงเสริมความร่วมมือทางไซเบอร์ระหว่างประเทศ การจัดสัมมนา การประชุมแลกเปลี่ยน การศึกษาต่อต่างประเทศแก่เจ้าหน้าที่ และการแลกเปลี่ยนอุปกรณ์ทางอิเล็กทรอนิกส์เพื่อกระชับความสัมพันธ์ระหว่างประเทศ เช่น ประเทศญี่ปุ่น ประเทศสหรัฐอเมริกา ประเทศออสเตรเลีย รวมไปถึงหน่วยงานอื่นๆ ของภาครัฐที่ยังได้จัดสรรงบประมาณเหล่านี้เพื่องานด้านรักษาความมั่นคงปลอดภัยทางไซเบอร์อีกด้วย

3) การเข้าถึงความรู้ทางเทคโนโลยีของประชาชน

รัฐบาลทุ่มเทงบประมาณให้หน่วยงานต่างๆ ในภาครัฐเพื่อสร้างความรู้พื้นฐานให้กับประชาชน เช่น การประชาสัมพันธ์อันตรายหรือภัยจากอินเทอร์เพื่อให้ประชาชนเป็นหูเป็นตาให้กับรัฐบาล และป้องกันตนเองไม่ให้เป็นเหยื่อทางไซเบอร์ ประชาชนมีความรู้เบื้องต้นหลังจากทราบว่าตนเองถูกหลอกทางไซเบอร์ก็จะเข้าแจ้งต่อหน่วยงานภาครัฐทันทีและเจ้าหน้าที่ก็สามารถช่วยได้ทัน

นอกจากนี้ยังมีประชาชนส่วนใหญ่ให้ความสนใจกับการเข้าร่วมกิจกรรมต่าง ๆ ของทางภาครัฐที่เกี่ยวของกับความมั่นคงปลอดภัยทางไซเบอร์ที่ภาครัฐจัดขึ้นเพื่อให้ความรู้และได้รับการตอบสนองอย่างดี

4.9.2 ข้อบกพร่องที่เป็นจุดอ่อน

1) การบังคับใช้กฎหมาย

จากข้อมูลทั้งหมดที่มีการศึกษาเรื่องกฎหมายในประเทศแสดงให้เห็นว่าประเทศไทยมีการพัฒนากฎหมายอยู่ตลอดเวลาเพื่อทำให้กฎหมายนั้นมีความสมัยใหม่ แต่อย่างไรก็ตามปัญหาที่เกิดขึ้นนั้นไม่ได้อยู่ที่ตัวบทของกฎหมายแต่เป็นในขั้นตอนของการใช้กฎหมายที่ผู้มีอำนาจในการบังใช้กฎหมายอาจจะใช้อำนาจนั้นไม่ชัดเจน หรือติดขัดจากปัญหาของเทคโนโลยีที่ไม่สามารถตรวจจับผู้ก่อการร้ายได้ทันท่วงที การมีจำนวนผู้กระทำผิดมากขึ้นตามจำนวนผู้ใช้อินเทอร์เน็ตที่เพิ่มขึ้นจึงทำให้ผู้ใช้อำนาจไม่สามารถดูแลควบคุมได้อย่างทั่วถึง เพราะฉะนั้นหากต้องการปรับปรุงการบังคับใช้กฎหมายเป็นไปอย่างถูกต้องจะต้องเริ่มจากการสร้างผู้บังคับใช้ที่มีความรู้อย่างสมบูรณ์และผลักดันให้มีความเพียบพร้อมทางเทคโนโลยี

2) ข้อบกพร่องทางเทคโนโลยี

จากข้อมูลการสัมภาษณ์แสดงให้เห็นถึงการจัดสรรงบประมาณมากมายเพื่อมาสนับสนุนความมั่นคงปลอดภัยทางไซเบอร์ แต่หน่วยงานส่วนให้ซึ่งมีภารกิจหลักเป็นของตนเอง เช่น กระทรวงสาธารณสุข การไฟฟ้าฝ่ายผลิต กระทรวงยุติธรรม ต่างมีภารกิจหลักที่มากมาย ทำให้บางครั้งงบประมาณเหล่านี้อาจไปไม่ถึงการปรับปรุงความมั่นคงปลอดภัยทางไซเบอร์ ถึงแม้ผู้บริหารจะให้ความสนใจถึงภัยคุกคามเหล่านี้อย่างจริงจังแต่ก็ยังมีภารกิจหลักของหน่วยงานที่จะต้องใช้งบประมาณมากกว่าการนำไปพัฒนาเทคโนโลยี มากไปกว่านั้นเทคโนโลยีมีการพัฒนาอยู่ตลอดเวลา การพลาดการอัพเดทในช่วงเวลาหนึ่งอาจทำให้การใช้เทคโนโลยีเหล่านี้มีการขาดตอนและจะต้องนำงบประมาณไปซื้ออุปกรณ์ใหม่ๆอยู่ตลอดเวลา การไม่ได้ใช้อุปกรณ์เหล่านี้อย่างสม่ำเสมอจะทำให้ไม่รู้ว่าเทคโนโลยีที่หน่วยงานกำลังใช้นั้นตกรุ่นไปแล้วหรือไม่

3) จำนวนบุคลากรที่มีความรู้ความสามารถ

จากข้อมูลการสัมภาษณ์รัฐบาลมีการสร้างการประชาสัมพันธ์และจัดกิจกรรมสร้างความรู้พื้นฐานให้กับประชาชนอยู่เสมอ แต่อย่างไรก็ตามบุคลากรที่มีความรู้เชี่ยวชาญเฉพาะด้านเทคโนโลยีกลับมีน้อย บางหน่วยงานมีเพียง 2-3 ท่าน เท่านั้น จำนวนบุคคลาการที่มีความรู้ความสามารถด้านความมั่นคงปลอดภัยไซเบอร์น้อยนั้นอาจเป็นเพราะรายได้ที่ไม่เพียงพอหรือไม่ดึงดูดเท่ากับเอกชนทุนการพัฒนาที่มีน้อยและเงื่อนไขที่มากมายของหน่วยงานรัฐทำเห็นผู้ที่มีความสามารถไม่ได้มองว่าเป็นโอกาส ดังนั้นหากรัฐต้องการให้การบังคับใช้กฎหมายมีประสิทธิภาพและการใช้เทคโนโลยีที่มีประสิทธิผลจึงจำเป็นจะต้องพัฒนาคนให้ได้มากที่สุด การสร้างแรงจูงใจเป็นสิ่งสำคัญ

ของการดึงดูดบุคลากรให้มาทำงานกับภาครัฐ และภาครัฐนั้นจะต้องจัดวางโครงสร้างหน่วยงานให้ดี เช่นแยกบุคลากรที่มีภารกิจสำคัญมีงานประจำออกจาก บุคลากรที่มีหน้าที่ทางไอทีเพื่อให้บุคคลกรทางไอทีนั้นมีเวลาในการทำงานด้านความมานคงปลอดภัยทางไซเบอร์อย่างเต็มที่

บทที่ 5

สรุปผลการศึกษาและข้อเสนอแนะ

จากผลการวิเคราะห์การศึกษาเรื่องการรับมือของภาครัฐกับการก่อการร้ายทางไซเบอร์ในประเทศไทย เป็นการวิเคราะห์การรับมือภัยคุมคามทางไซเบอร์ของภาครัฐในรูปแบบของการก่อการร้ายของหน่วยงานต่าง ๆ ที่มีผลกระทบต่อโครงสร้างพื้นฐาน สาธารณูปโภคสำคัญของประเทศไทย โดยจะเริ่มศึกษาตั้งแต่คำนิยามของการก่อการร้ายไซเบอร์ให้มีความชัดเจนเพื่อที่จะสามารถอธิบายสถานการณ์และศักยภาพในการรับมือการก่อการร้ายไซเบอร์ของประเทศไทยนั้นเป็นอย่างไร จากการรวบรวมข้อมูลจากการสัมภาษณ์เชิงลึกและการทำสัมภาษณ์แบบรวมกลุ่ม (focus group) ถึงนิยามของคำว่าการก่อการร้ายไซเบอร์ ดังนั้นในบทนี้จะสรุปผลการศึกษาทั้งหมดตามจุดประสงค์ที่วางไว้ พร้อมทั้งข้อเสนอแนะเชิงวิชาการและข้อเสนอแนะในการปฏิบัติ ดังต่อไปนี้

เพื่อตอบปัญหาตามจุดประสงค์ทั้งหมดที่ได้ตั้งไว้วิจัยเล่มนี้จะสรุปผลตามสถานการณ์การก่อการร้ายในประเทย การรับมือการก่อการร้ายในประเทศไทย และการกล่าวถึงอนาคตที่มีโอกาสจะเกิดขึ้นในเรื่องการก่อการร้ายไซเบอร์ ทั้งนี้อาจมีการเปรียบเทียบกับประเทศที่สำคัญและมีการพัฒนาทางด้านการรับมือการก่อการร้ายทางไซเบอร์ในโลกอีกด้วย

5.1 สถานการณ์ก่อการร้ายไซเบอร์ในประเทศไทย

จากวงสนทนาของผู้เชี่ยวชาญด้านไซเบอร์ ผู้เชี่ยวชาญด้านการก่อการร้าย และกฎหมายระหว่างประเทศ สามารถมองภาพของมุมมองการก่อการร้ายได้ในหลายมุมมองแต่จะต้องประกอบไปด้วย 4 องค์ประกอบหลัก คือ จุดประสงค์ของการกระทำ กลยุทธ์หรือวิธีในการกระทำ เป้าหมายที่มุ่งทำลายผู้บริสุทธิ์ เพื่อจุดประสงค์ที่แท้จริงคือเป้าหมายทางการเมือง การล้มล้าง การทำลายระบบเก่า บิดเบือนข้อมูลของรัฐ แต่อย่างไรก็ตามความซับซ้อนของโลกหรือพื้นที่ทางไซเบอร์ไปไกลจริงหว่านั้น โดยพิจารณาตามแต่ละมุมมอง โลกของไซเบอร์มีลักษณะพิเศษคือ ความไร้ตัวตน สามารถใช้ความว่างเปล่าหรือประเทศที่สามในการโจมตี การไม่สามารถหาคนที่กระทำความผิดได้เพราะไร้ซึ่งหลักฐานหรือไม่มีบทลงโทษระหว่างรัฐที่บังคับใช้ได้จริงถึงแม้จะมีข้อตกลงตามสนธิสัญญาระหว่างประเทศของสหประชาชาติก็ตาม ทั้งหมดนี้เกิดจากมุมมองที่แตกต่างกันของนักวิชาการที่มีหลายมุมมองขึ้นกับพื้นฐานความรู้ของตนเอง ประกอบไปด้วยกลุ่มผู้สนทนากลุ่มที่ 1 ที่เป็นชาวไทยและกลุ่มที่ 2 ที่เป็นชาวต่างชาติจากสหราชอาณาจักรฯ โดยรายละเอียดทั้งหมดนั้นสามารถสรุปได้ดังนี้

5.1.1 มุมองของการก่อการร้ายในประเทศไทย

เนื่องจากประเทศไทยให้ความสนใจในเรื่องของเทคโนโลยีและความรู้เรื่องภัยคุกคามทางไซเบอร์ทั้งในระดับเจ้าหน้าที่ธรรมดาและในระดับเจ้าหน้าที่ผู้ชำนาญการในเรื่องของไซเบอร์ของหน่วยงานอื่นๆ ความคิดในเรื่องของความตระหนักรู้ในการใช้เทคโนโลยีก็เช่นกัน การก่อการร้ายไซเบอร์ในมุมมองของประเทศไทยมักแฝงไปด้วย 2 มุมมอง โดยมุมมองแรกจะเกี่ยวข้องอาชญากรรมด้านการเงิน การฉ้อฉล การหลอกลวงเพื่องแสวงหาผลประโยชน์จากบุคคลทั่วไป หรือไปถึงในระดับองค์กรและส่งผลให้เกิดความเสียหายที่สูงมากขึ้น ในแง่มุมที่สองนโยบายการป้องกันการก่อการร้ายสำหรับประเทศไทยนั้นยังมุ่งเน้นไปยังสารธารณูปโภคพื้นฐานทางด้านสารสนเทศ เช่น การตรวจตราความเคลื่อนไหวในสื่อสังคมออนไลน์ความอ่อนไหวของสื่อออนไลน์ที่มีต่อความมั่นคงต่อสถาบันหลักของประเทศ ทำให้หน่วยงานด้านการกำกับดูแลความมั่นคงปลอดภัยได้รับภาระหน้าที่ในด้านเหล่านี้เป็นหลัก รวมไปถึงหน่วยงานด้านการปราบปรามที่จะต้องนำกำลังเข้ามาช่วยตรวจตราทางไซเบอร์เพื่อป้องกันไม่ให้เกิดการชักจูงหรือรวมกลุ่มทางไซเบอร์ที่อาจส่งผลให้เกิดการรวมกลุ่มจริงทางเชิงกายภาพซึ่งจะเป็นปัญหาต่อความมั่นคงของประเทศ

นโยบายทั้งหมดที่ถูกเสนอออกมานั้นสะท้อนมาจากมุมมองแนวคิดที่ประเทศไทยมีต่อการก่อการร้ายในแง่มุมออนไลน์ นั่นคือ ภาพลักษณ์ความมั่นคงของประเทศซึ่งให้ความสำคัญกับปัจจัยหลักปัจจัยที่หนึ่งขององค์ประกอบของความมั่นคงทางไซเบอร์มากที่สุด คือเป้าประสงค์ทางการเมืองของผู้ก่อการร้าย ส่วนในเรื่องของผลกระทบหลัก วิธีการในการก่อการร้าย หรือการทำร้ายประชาชนบริสุทธิ์ จะเป็นปัจจัยที่ตามมาในการส่งผลต่อนโยบาย จากการสัมภาษณ์ถึงมุมมองการก่อการร้ายไซเบอร์นั้นผู้เขียนได้เลือกการสัมภาษณ์เชิงลึกจากหน่วยงานที่เกี่ยวทั้งหมด 14 หน่วยงาน หน่วยงานที่ผู้วิจัยศึกษานั้นจะถูกแบ่งออกเป็น 3 ประเภทด้วยกัน คือ

หน่วยงานด้านการกำกับดูแลความมั่นคงปลอดภัย

1) กระทรวงดิจิทัลและเทคโนโลยีฯ
2) สภาความมั่นคงแห่งชาติ
3) สำนักข่าวกรองแห่งชาติ
4) สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

หน่วยงานด้านการปราบปราม

1) ศูนย์ไซเบอร์กองทัพบก
2) ศูนย์ไซเบอร์กองทัพอากาศ
3) กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี

หน่วยงานที่มีความเสี่ยงต่อการโจมตี

1) กระทรวงยุติธรรม

2) การไฟฟ้าส่วนภูมิภาค

3) หน่วยงานกำกับดูแลกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติหรือ กสทช.

4) กระทรวงสาธารณสุข

5) ธนาคารแห่งประเทศไทย

สถาบันวิชาการ

1) จุฬาลงกรณ์มหาวิทยาลัย

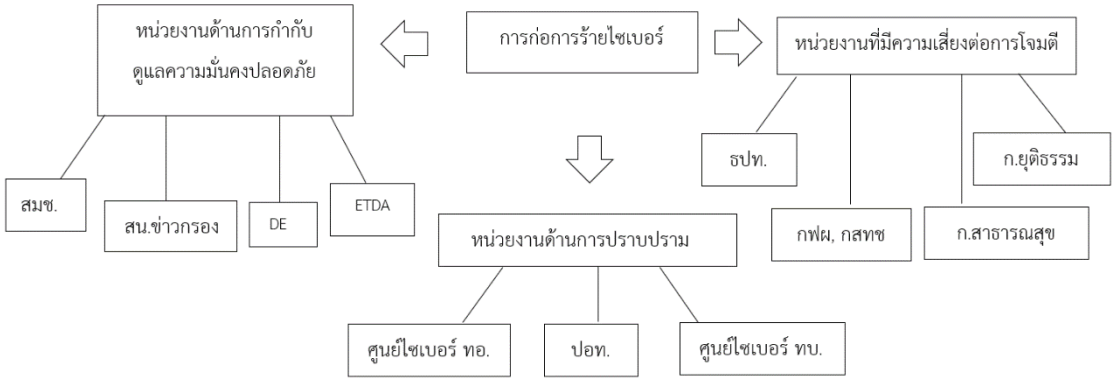
2) สถาบันบัณฑิตพัฒนาบริหารศาสตร์ (นิด้า) NIDA

เนื่องจากภาระหน้าที่ของแต่ละหน่วยงานมีความแตกต่างกัน มุมมองที่มีต่อการก่อการร้ายไซเบอร์จึงมีความแตกต่างกัน เช่น หน่วยงานด้านการกำกับดูแลความมั่นคงปลอดภัยมีแนวคิดว่าการใช้คอมพิวเตอร์หรือระบบอิเล็กทรอนิกส์ที่มีการเชื่อมโยงกับโครงข่ายทางอินเทอร์จูโจมหน่วยงานภาครัฐโดยวิธีในรูปแบบการก่อการร้าย เช่น การโจมตีระบบไม่ให้สามารถใช้งานได้ การข้อมูลข้อมูลจากระบบจนเกิดความเสียหายที่รุนแรง โดยเป้าหมายในการโจมตีนั้นจะต้องอยู่ในพื้นที่ไซเบอร์เท่านั้นถึงจะเรียกได้ว่าเป็นการจู่โจมทางไวเบอร์ที่แท้จริง และจุดประสงค์ของการจู่โจมนั้นจะต้องเป็นจุดประสงค์ทางการเมือง ต้องการบิดเบือนข้อเท็จจริงของรัฐบาล หรือแม้กระทั้งทำให้ระบบความมั่นคงของรัฐล้มเหลวไม่ว่าจะเป็นระบบสาธารณูปโภคสำคัญของประเทสที่จะก่อให้เกิดความเสียหายอย่างรุนแรงต่อประชาชนอันบริสุทธิ์เพื่อให้เพื่อผู้ที่จู่โจมได้รับความพึงพอใจในจุดประสงค์ที่ตนเองต้องการ

สำหรับหน่วยงานการปราบปรามการก่อการร้ายมองว่าการก่อการร้ายไซเบอร์หมายถึง การใช้กลวิธีในการก่อการร้ายมาประยุกต์ใช้กับระบบเทคโนโลยีในปัจจุบันเพื่อโจมต่อรับบความมั่นคงของรัฐบาล โดยเฉพาะความมั่นคงทางการทหาร ให้เกิดความเสียหายรุนแรงและก่อให้เกิดความเสื่อมเสียต่อภาพลักษณ์ความมั่นคงของประเทศ การกระทำของผู้ก่อการร้ายจะสามารถกระทำโดยเป็นกลุ่มหรือเป็นบุคคล จะมีฐานที่ตั้งในการก่อการร้ายภายในประเทศหรือนอกประเทศไทยได้ และการก่อการร้ายนั้นจะต้องเกิดผลในระดับรุนแรงกับประชาชนผู้บริสุทธิ์ ตรงตามคำนิยามของการก่อการร้ายแบบดั้งเดิม

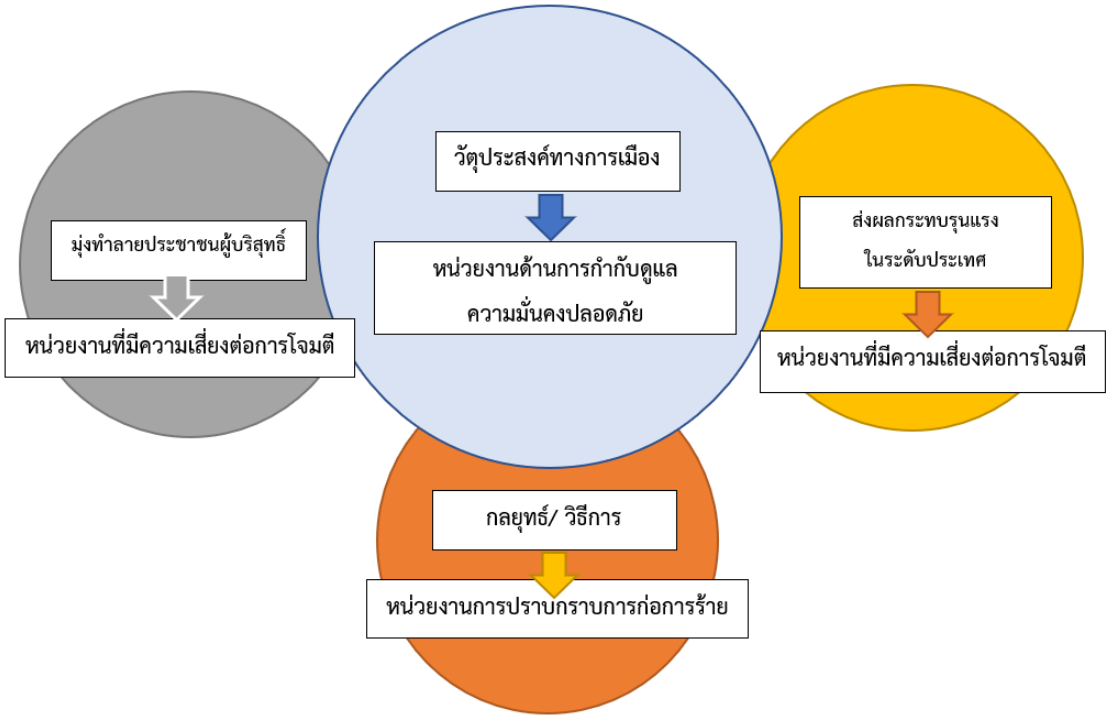
แต่สำหรับหน่วยงานที่มีความเสี่ยงต่อการโจมตีการก่อการร้ายไซเบอร์ หมายถึง การที่ผู้ก่อการร้ายมีวัตถุประสงค์ที่จะคุกคามภาครัฐเพื่อให้ได้มาซึ่งผลประโยชน์ของตน โดยมีวิธีการจู่โจมภาครัฐภายใต้ระบบคอมพิวเตอร์และโครงข่ายอินเทอร์เน็ตเพื่อทำลายข้อมูลของฝั่งตรงข้าม หรือขู่

คุกคามเพื่อให้รัฐยอมเสียค่าใช้จ่ายเพื่อให้บรรลุวัตถุประสงค์ของเป้าหมายในกลุ่มตน วิธีการที่ใช้ในการก่อการร้ายส่วนมากจะทำให้ระบบของภาครัฐเสียจนทำให้ประชาชนไม่สามารถใช้งานได้



รูปที่ 29 แผนภาพหน่วยงานสำคัญของภาครัฐไทย

เมื่อผสมผสานการให้คำนิยามของผู้เชี่ยวชาญที่ทำงานในหน่วยงานทั้ง 3 ประเภท และนักวิชาการจากมหาวิทยาที่มีความรู้เรื่องเหล่านี้สามารถสรุปได้ว่า ความคล้ายคลึงกันของนิยามของการก่อการร้ายที่มีส่วนเหมือนกันคือ การใช้วัตถุประสงค์ทางการเมืองเป็นที่ตั้ง ใช้วิธีการก่อการร้ายแบบดั้งเดิม เช่น การทำลายผู้บริสุทธิ์ การทำลายความน่าเชื่อถือของภาครัฐ บิดเบือนข้อมูลที่ถูกต้อง ผ่านทางการใช้เทคโนโลยี และอุปกรณ์ไซเบอร์ในการโจมตีอีกฝ่ายหนึ่งเมื่อให้ได้มาซึ่งผลประโยชนของกลุ่มตน แต่ความเสียหายนั้นจะต้องเป็นในระดับที่รุนแรง ความนิยามนี้มีความครบถ้วนมากที่สุดที่จะสามารถนำมาสรุปเป็นลักษณะการก่อการร้ายไซเบอร์ของประเทศไทยได้



รูปที่ 30 แผนภาพแสดงองค์ประกอบของนิยามการก่อการร้ายไซเบอร์
และมุมมองของแต่ละหน่วยงาน

5.1.2 มุมมองของการก่อการร้ายในต่างประเทศ

การก่อการร้ายไซเบอร์ คือ คือการโจมตีในพื้นที่ของไซเบอร์โดยใช้เครื่องมือทางไซเบอร์หรือใช้เครื่องมือทางกายภาพและส่งผลกระทบทำให้เกิดความรุนแรงทางกายภาพจริงทั้งนี้รวมไปถึงการทำลายในตัวระบบคอมพิวเตอร์เองด้วย การก่อการร้ายส่วนใหญ่ในต่างประเทศถูกมองว่าเป็นการก่อการร้ายจากภายนอกเขตรัฐชาติและการเข้าถึงข้อมูลส่วนตัวและการละเมิดลิขสิทธิ์ต่าง ๆ เป็นภัยที่รองลงมา ยกตัวอย่าง การก่อการร้ายในประเทศอังกฤษที่เคยประสบการจู่โจมทางไซเบอร์ในปี 2018 โดยการทำลายระบบเครือโรงพยาบาลทั่วประเทศ หรือ National Health Service (NHS) เป็นเวลากว่า 3 สัปดาห์ที่รัฐบาลอังกฤษจะสามารถกู้ระบบคืนได้ และ ณ ขณะนั้นทำให้เกิดความเสียหายกว่าล้านล้านบาท (CSIS, 2020) รัฐบาลอังกฤษเองพยายามที่จะกู้คืนข้อมูลจากไวรัสที่ถูกกล่าวหาว่าเป็นการกระทำของประเทศเกาหลีเหนือหน่วยสืบสวนเชื่อว่าไวรัสที่ส่งมานั้นเป็น Ransomware แต่เกิดความผิดพลาดทำให้กลายเป็น Trojan จึงทำให้รัฐบาลอังกฤษไม่ต้องเสียค่าไถ่และเช่นเดียวกันรูปแบบของ Ransomware ถูกวิเคราะห์ในส่วนต่อไป ในเหตุการณ์นี้รัฐบาลอังกฤษไม่มีนโยบายที่จะจ่ายค่าไถ่เพราะเนื่องจากว่าไม่สามารถมีสิ่งใดมาการันตีได้ถึงการได้กลับมาของข้อมูล

โดยสรุปแล้วหลังจากเหตุการณ์นี้เกิดขึ้นรัฐบาลอังกฤษเองยังไม่มีข้อมูลถึงแรงจูงใจในการกระทำของประเทศเกาหลีเหนือ ดังนั้นจึงไม่สามารถสรุปได้ว่าการกระทำครั้งนี้เป็นการก่อการร้ายจริงๆ เพราะจำเป็นจะต้องมีเป้าหมายทางการเมืองที่ชัดเจน หรือเพียงแค่รัฐบาลเกาหลีเหนือต้องการเพียงแค่เงินเพื่อมาสนับสนุนในการจู่โจมครั้งต่อๆไปเท่านั้น และถึงแม้ว่าจะรู้ว่ารัฐบาลเกาหลีเหนือเป็นผู้กระทำแต่ก็ไม่สามารถที่จะทำอะไรเป็นการตอบโต้ หรือใช้กฎหมายระหว่างประเทศโดยการคว่ำบาตรได้เพราะหลักฐานทางไซเบอร์ยังไม่สามารถใช้ได้จริงและไม่สามารถใช้กฎหมายระหว่างประเทศกดดันประเทศที่ไม่ได้เข้าร่วมกับสหประชาชาติได้ (Jun, LaFoy, & Sohn, 2015)

5.2 การอภิปรายการรับมือของภาครัฐ (Government Response)

การรับมือของภาครัฐของแต่ละประเทศมีความแต่ต่างกันเนื่องจากมุมมองที่มีต่อภัยคุกคามที่แตกต่างและระดับความรุนแรงที่เกิดขึ้น ดังนั้นเพื่อความชัดเจนในการอธิบายผู้วิจัยจะสรุปหัวข้อตามลำดับ ดังนี้

5.2.1 การป้องกันตัวเองและการจู่โจมทางไซเบอร์

หากมีการโจมตีเกิดขึ้นไม่ว่าจะเป็นในรูปแบบใดก็ตาม ประเทศที่ถูกโจมตีจะต้องตอบโต้กลับไปในรูปแบบใดรูปแบบหนึ่ง ขึ้นอยู่กับประสบการณ์ เทคโนโลยี ความรู้เฉพาะทาง หรือการใช้กฎหมายเป็นมาตรฐานในการตัดสินใจในการตอบโต้ หากเปรียบเทียบการจู่โจมในรูปแบบเดิมกับรูปแบบไซเบอร์นั้น ย่อมมีความแตกต่างกันมากไม่ว่าจะเป็นผู้กระทำที่ไม่สามารถระบุตัวได้ อาวุธที่มองไม่เห็นละไม่สามารถคาดการณ์ได้ รวมถึงความเสียหายที่เกิดขึ้นที่มักจะรุนแรงกว่าการจู่โจมในแบบเดิม ๆ ดังนั้น คำถามจึงถูกตั้งขึ้นมาว่าการที่ประเทศใดประเทศหนึ่งมีอาวุธทางไซเบอร์ที่รุนแรงเพื่อใช้เป็นเหตุผลในการป้องกันตนเองนั่นถูกหรือไม่ หรือการจู่โจมทางไซเบอร์กลับไปยังประเทศที่จู่โจมจะเป็นเรื่องที่ชอบธรรมหรือไม่ ยังไม่มีใครสามารถสรุปได้

ในมุมมองของประเทศอังกฤษซึ่งเป็นประเทศที่มีความพร้อมทางเทคโนโลยีและมีความเชี่ยวชาญมากประเทศหนึ่งในโลกให้ความสำคัญกับหลักกฎหมายที่จะใช้เป็นบรรทัดฐานในการตัดสินว่าการจู่โจมกลับแบบไซเบอร์นั้นมีความชอบธรรมเพียงใด ตามกฎหมายระหว่างประเทศและสนธิสัญญาที่ระบุไว้ในองค์กรสหประชาชาติได้กล่าวว่าการละเมิดต่อกฎหมายที่ป้องกันทางไซเบอร์ถือเป็นเรื่องที่ผิดประเทศที่เป็นผู้ก่อเหตุจะต้องถูกลงโทษ (Jarvis & Macdonald, 2015) แต่อย่างไรก็ตามในแง่การปฏิบัติแล้ว กฎหมายระหว่าประเทศไม่สามารถใช้ในการป้องกันไม่ให้เกิดการจู่โจมทางไซเบอร์ได้จริงเพราะกฎหมายที่สำคัญที่สุดคือกฎหมายภายในรัฐ และอีกประการที่สำคัญการจู่โจมทางไซเบอร์ยังไม่ถือว่าเป็นการละเมิดต่อกฎหมายมนุษยธรรม ซึ่งกฎหมายมนุษยธรรมมีเพื่อปกป้อง

คุ้มครองชีวิตและศักดิ์ศรีของผู้ที่ได้รับผลกระทบจากภัยการสู้รบสงครามและสถานการณ์รุนแรงที่เกี่ยวข้อง โดยไม่เลือกปฏิบัติเป็นกลางและเป็นอิสระ เพื่อบรรเทาทุกข์ในภาวะความขัดแย้งระดับระหว่างประเทศและพยายามป้องกันความเสียหายอันเกิดจากการสู้รบ ถึงแม้ว่ากฎหมายมนุษยธรรมจะมีความครบถ้วนแต่ยังไม่ได้รับการยอมรับให้ใช้กับความเสียหายที่เกิดกับโลกไซเบอร์ ตัวอย่างเช่น การใช้ไวรัสมุ่งทำลายระบบโรงพยาบาลเป็นผลให้เกิดความสับสนให้เกิดการสลับยาของผู้ป่วย ถึงแม้ผู้ป่วยจะได้รับผลกระทบจากเหตุการครั้งนี้แต่ไม่สามารถระบุได้ว่าการกระทำจู่โจมทางไซเบอร์เป็นการละเมิดกฎหมายมนุษยธรรม (Jarvis & Macdonald, 2015) ดังนั้น หากจะทำให้ปัญหาทางไซเบอร์ได้รับการตระหนักถึงความสำคัญมากกว่านี้ จำเป็นจะต้องอาศัยการร่วมมือกันระหว่างประเทศสร้างกฎหมายโดยระบุถึงการกรทำผิดทางไซเบอร์อย่างจริงจังและจะต้องประกอบไปด้วยบทลงโทษจริงที่ทุกประเทศจะต้องได้รับการลงโทษอย่างเท่าเทียมกัน

ในส่วนของประเทศไทยนั้นมีการเตรียมตัวต่อการก่อการร้ายไซเบอร์ในรูปแบบของการตั้งรับในเชิงนโยบายโดยเฉพาะการตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เพื่อเป็นหน่วยงานหลักสำหรับการจัดการรับมือ ป้องกันการก่อการร้ายโดยเฉพาะและหน่วยงานนี้ก็มีการเปิดตัวอย่างเป็นทางการในเดือนสิงหาคม 2564 ตามภารกิจหลักของสำนักงานแล้ว สกมช. จะเป็นหน่วยงานที่คอยควบคุม ทำหน้าที่เชิงปฏิบัติและตอบโต้ภัยคุกคามได้โดยทันทีผ่าน ThaiCERT ซึ่งมีผู้เชี่ยวชาญทางเทคนิคด้านคอมพิวเตอร์ในการรับมือตลอดเวลา ทีมของ สกมช. นั้นจะเป็นทั้งผู้ออกนโยบาย นำนโยบายไปให้ทุกส่วนปฏิบัติและสร้างมาตรฐานให้กับทุกหน่วยงานปฏิบัติงาน แต่ไม่รวมในส่วนของการดำเนินคดีตามความผิดของผู้กระทำเพราจะเป็นหน้าที่แยกของฝ่ายตุลาการ (ThaiCERT, 2018)

สิ่งที่ สกมช. จะสามารถปฏิบัติเพิ่มคือการเพิ่มฝ่ายด้านการวิจัยเพื่อเก็ยรวบรวมปัญหาสถิติจากหน่วยงานต่าง ๆ และนำมาวิเคราะห์ในอนาคตว่าการรับมือนั้นจะอยู่ในรูปแบบใดประเทศไทยควรมีการวางตำแหน่งกลยุทธ์ที่ชัดเจนว่าเราจะมีทิศทางตอบโต้กับภัยคุกคามแต่ละรูปแบบอย่างไร ดังที่ผู้วิจัยได้เสนอและแยกแยะไว้ในบทก่อนหน้าระหว่างเครื่องมือที่ใช้กับกลยุทธ์หรือวิธีที่ควรรับมือ

ตัวแสดงและผลู้กระทำ (Actors and Terms)

1) แฮกเกอร์ (Hackers)

คือ คนที่มีความชำนาญในการใช้คอมพิวเตอร์ไปในทางที่ผิดกฎหมาย เช่น การขโมยข้อมูลจากคอมพิวเตอร์ในเครือข่าย อาจหมายถึงการแอบปรับแก้หรือดัดแปลงโปรแกรมคอมพิวเตอร์โดยไม่ถูกต้องตามกฎหมายและสามารถหาช่องโหวในระบบได้ ในความหมายนี้ระบุแฮกเกอร์ว่าเป็นปัจเจกบุคคลหรือปัจเจกบุคคลที่รวมกลุ่มกันและมีอุดมการณ์เดียวกัน แล้วสมาชิกในกลุ่ม

นั้นจะต้องเสียสละตนเองเพื่อเรียนรู้ทางไซเบอร์ให้ได้มากที่สุดโดยเฉพาะในทางเทคนิคและการเข้าถึงทรัพยากรทางเทคโนโลยีของภาครัฐ ผ่านทางการควบคุมซอฟแวร์ (Hua & Bapna, 2012)

เครื่องมือ: ไวรัส และ วอร์ม (Virus and Worms) แบคดอร์ (Backdoor: Trojans and Rootkits) บ็อตเน็ต (Botnets)

วิธีการและกลยุทธ์: DoS Attacks เทคนิคการแทรกซึม การเข้าสู่ข้อมูล การสอดแนม และการรวบรวมข้อมูล เทคนิคในการทำให้ไม่มีตัวตน

วิธีการรับมือ: รัฐบาลควรให้ความสนใจแฮกเกอร์กลุ่มนี้เนื่องจากเป็นแฮกเกอร์ที่มีความรู้และมีความสามารถที่จะเจาะระบบได้จริง รับบาลควรมีรายชื่อผู้ที่สงสัยว่าจะเป็นฉอกเกอร์เพื่อที่จะสามารถตามถือความเคลื่อนไหวและสืบสาวไปยังแหล่งที่เป็นการรวมตัวกันได้ หากจับแฮกเกอร์เหล่านี้ได้ก็สามารถนำความรู้ของแฮกเกอร์เหล่านี้มาถ่ายทอดให้กับคนในองค์กรเพื่อเป็นประโยชน์ต่อรัฐบาล (Hua & Bapna, 2012)

2) แคร็กเกอร์ (Cracker) แครกเกอร์

คือผู้ที่นำความรู้ในการแฮกไปใช้ในการทำความผิดหรือจัดการคนแฮกเอร์ที่เป็นฝ่ายผิด เช่น การขโมยข้อมูล การทำลายข้อมูล หรือแม้กระทั่งการครอบครองคอมพิวเตอร์คนอื่น แบ่งแยกทั้ง 2 ประเภทนี้ คือ กลุ่มหมวกดำ (black hat) กลุ่มที่ผิดกฎหมายทำกิจกรรมที่เป็นภัยทางไซเบอร์ กลุ่มหมวกขาว (white hat) กลุ่มที่ใช้ความรู้ทางเทคโนโลยีมาช่วยเหลือผู้ที่ถูกจู่โจมจากกลุ่มหมวกดำซึ่งมีการกระทำที่ผิดกฎหมายและเป็นภัยทางไซเบอร์ กลุ่มหมวกเทา (grey hat) จะอยู่ระหว่างกลางแฮกเกอร์ทั้งสองแบบแต่มุ่งที่ผลประโยชน์มากที่สุด (Kabanda, 2018)

เครื่องมือ: ไวรัส และ วอร์ม (Virus and Worms) แบคดอร์ (Backdoor: Trojans and Rootkits) บ็อตเน็ต (Botnets)

วิธีการและกลยุทธ์: DoS Attacks เทคนิคการแทรกซึม การเข้าสู่ข้อมูล การสอดแนม และการรวบรวมข้อมูล เทคนิคในการทำให้ไม่มีตัวตน

วิธีการรับมือ: กลุ่มนี้มีความเชี่ยวชาญคล้ายกับแฮกเกอร์กลุ่มด้านบนแตกต่างที่อุดมการณ์เพราะฉะนั้นสิ่งที่รัฐบาลควรให้ความสนใจแฮกเกอร์กลุ่มนี้คือ การแยกแยะประเภทของแต่ละกลุ่มหมวกให้ชัดเจนเพื่อความชอบธรรมในการตัดสินความผิดของแต่ละฝ่าย ถึงบางฝ่ายจะมีแนวคิดที่ดีแต่วิธีการยังไม่ถูกต้องก็ยังไม่สามารถที่จะยอมรับได้ทั้งหมดว่าพวกเขาเหล่านั้นไม่ผิด การแบ่งกลุ่มและรายชื่อมนแต่ละกลุ่มจริงเป็นสิ่งสำคัญ (Kabanda, 2018)

3) แฮกเกอร์มือใหม่ (Script Kiddies)

แฮกเกอร์มือใหม่ที่ยังขาดความชำนาญในการเจาะระบบคอมพิวเตอร์ โดยปกติแล้ว Script Kiddies จะใช้โปรแกรมเจาะระบบที่ถูกพัฒนาโดย Hacker ที่มีความชำนาญสูงมาใช้เจาะ

ระบบคอมพิวเตอร์ที่ตัวเองสนใจด้วยความอยากรู้อยากเห็น หรือทดลองความรู้ในการเจาะระบบของตนเอง แต่ยังมีทักษะเท่ากับผู้ที่เป็น Hacker

เครื่องมือ: ไวรัส และ วอร์ม (Virus and Worms) แบคดอร์ (Backdoor: Trojans and Rootkits)

วิธีการและกลยุทธ์: DoS Attacks การเข้าสู่ข้อมูล การสอดแนม และการรวบรวมข้อมูล

วิธีการรับมือ: กลุ่มนี้อาจมีความเชี่ยวชาญน้อยกว่าแฮกเกทั่วไปซึ่งบางครั้งอาจไม่เป็นภัยต่อความมั่นคงของรัฐแต่สิ่งที่สำคัญที่รัฐควรให้ความสนใจคือ การดึงแฮกเกอร์มือใหม่เหล่านี้ออกมาจากวงจรหรือเครือข่ายหรือองค์กรที่เป็นการรวมตัวกันขนาดใหญ่เพื่อก่ออาชญากรรมทางไซเบอร์ การนำแฮกเกอร์มือใหม่เหล่านี้มาพัฒนาฝีมือโดยการอบรมกับฝ่ายภาครัฐหรือสร้างให้พวกเขาเป็นสายสืบในองค์ลับขนาดใหญ่ของแฮกเกอร์ในระดับนานาชาติต่อไปจะเป็นสิ่งที่นำมาใช้ประโยชน์ได้ในอนาคต(Kabanda, 2018)

4) แฮกเกอร์กลุ่ม Cybervigilantes

เป็นการกระทำของการดำเนินศาลเตี้ยกิจกรรมผ่านทางอินเทอร์เน็ต ครอบคลุมไปถึงความตื่นตัวต่อการหลอกลวงอาชญากรรมและพฤติกรรมที่ไม่เกี่ยวข้องกับอินเทอร์เน็ตและกลุ่มนี้จะมีความพิเศษคือเป็น Anonymous กลุ่ม ที่ไร้ตัวตนหรือ Anonymous กลุ่มนี้จะมีการกระทำที่มีจุดม่งหมายทางการเมืองและต่อต้านอาชญากรรมแต่ในอีกด้านหนึ่งบางกลุ่มอาจจะมีการกระทำที่ผิดกฎหมาย เช่น การฟอกเงินเป็นหนึ่งในนั้น และหนึ่งในนั้นคือวิธีการที่กลุ่ม Cybervigilantes กระทำเป็นวิธีการที่ละเมิดความเป็นส่วนตัวของเป้าหมายซึ่งผิดต่อกฎหมายคุ้มครองสิทธิและเสรีภาพ และในที่สุดแล้วในกลุ่มของแฮกเกอร์มือใหม่ก็ยังขาดแรงจูงใจทางการเมืองที่ชัดเจนที่จะจัดกลุ่มได้ว่าเป็นผู้ก่อการร้าย (Jun, LaFoy, & Sohn, 2015)

เครื่องมือ: ไวรัส และ วอร์ม (Virus and Worms) แบคดอร์ (Backdoor: Trojans and Rootkits) บ็อตเน็ต (Botnets)

วิธีการและกลยุทธ์: DoS Attacks เทคนิคการแทรกซึม วิศวกรรมสังคม การเข้าสู่ข้อมูล การสอดแนม และการรวบรวมข้อมูล เทคนิคในการทำให้ไม่มีตัวตน

วิธีการรับมือ: หากเปรียบเทียบจากทั้งสามกลุ่มข้างต้นแล้ว แฮกเกอร์กลุ่ม Cybervigilantes มีความเป็นอุดมการณ์และมีโครงสร้างการรวมตัวที่เหนียวแน่นที่สุด ดังนั้นการเชื่อมโยงแฮกเกอร์กลุ่มนี้กับการก่อการร้ายไซเบอร์ก็อาจจะเป็นเรื่องที่ทำได้เพราะกลยุทธ์ที่น่ากลัวของแฮกเกอร์กลุ่มนี้คือการใช้วิศวกรรมสังคมหรือการรื้อสร้างสังคมใหม่โดยใช้จิตวิทยาและเทคโนโลยีผสมเข้าด้วยกัน ดังนั้น รับบาลจะต้องให้อำนาจ สมช. และ สกมช. เป็นพิเศษในการตามหากลุ่มและ

รายชื่อของแฮกเกอร์กลุ่มนี้เพื่อจับตาความเคลื่อนไหวที่อาจจะเปลี่ยนแปลงจากกลุ่มเป้าหมายเดินแต่จะขยายความคิดและอุดมการณ์มากขึ้นในอนาคต (Jun, LaFoy & Sohn, 2015)

5) ผู้กระทำที่ไม่ใช่รัฐแต่มีเป้าหมายทางการเมือง (Nonstate actors with a Political Agenda)

ผู้กระทำที่ไม่ใช่รัฐอาจเป็นเรื่องง่ายที่พวกเขาจะเข้าถึงระบบโครงข่ายอินเทอร์เน็ตของแต่ละประเทศเพราะพวกเขาเหล่านั้นเปรียบเสมือนกลุ่มที่ไร้ตัวตนโดยใช้เครื่องมือทางไซเบอร์ต่อสู้เพื่อเป้าหมายทางการเมืองของรัฐนั้น บางครั้งการกระทำเหล่านี้อาจไม่ก่อให้เกิดอันตรายต่อประชาชนผู้บริสุทธิ์แต่เป็นการข่มขู่รัฐเสียมากกว่า การใช้เครื่องมือทางไซเบอร์ของคนกลุ่มนี้เป็นเรื่องง่ายและช่วยสนับสนุนให้การกระทำมุ่งสู่เป้าหมายได้เร็วขึ้น เพราะเครื่องมือทางไซเบอร์สามารถหาได้ง่ายและไม่ได้ใช้งบประมาณในการทำมากแต่สามารถทำให้เกิดผลที่หลากหลายไม่ว่าจะเป็นการขยายกลุ่มชายขอบ ชนกลุ่มน้อยให้มีพลังมากขึ้น และสามารถนำไปสู่การปฏิวัติทางการเมืองได้ การกระทำขอคนกลุ่มนี้เริ่มตั้งแต่การใช้ความรู้ในเชิงสันติวิธีที่จะเผชิญหน้าและถอนรากถอนโคนและสร้างกองกำลังเป็นของตนเอง การใช้เวปไซต์เพื่อทำให้รัฐเสียหาย หรือการเข้าไปทำลายเว็บไซต์ของรัฐโดยการเปลี่ยนเนื้อหา ข้อมูล การกระทำเหล่านี้ไม่ได้ถูกเปรียบเทียบว่าเป็นการกรำทำที่ป่าเถื่อนแต่อย่างใด (Talihärm, 2010)

เครื่องมือ: ไวรัส และ วอร์ม (Virus and Worms) แบคดอร์ (Backdoor: Trojans and Rootkits) บ็อตเน็ต (Botnets)

วิธีการและกลยุทธ์: DoS Attacks เทคนิคการแทรกซึม วิศวกรรมสังคม การเข้าสู่ข้อมูล การสอดแนม และการรวบรวมข้อมูล เทคนิคในการทำให้ไม่มีตัวตน

วิธีการรับมือ: ผู้กระทำที่ไม่ใช่รัฐแต่มีเป้าหมายทางการเมืองถือเป็นผู้ก่อการร้ายไซเบอร์กลุ่มใหญ่ที่น่ากลัวที่สุดเพราะรัฐบาลจะไม่สามารถสืบเสาะหรือกล่าวหากลุ่มเหล่านี้ได้ ซึ่งบางครั้งผู้กระทำที่ไม่ใช่รัฐนั้นอาจจะมีรัฐเบื้องหลังของสนับสนุนอยู่ไม่ว่าจะเป็นทางด้านการเงินเทคโนโลยี หรือลู่ทางในการเข้าถึงข้อมูล รัฐเหล่านี้พร้อมที่จะปกป้องกลุ่มผู้ก่อการร้ายกลุ่มนี้เพื่อผลประโยชน์ที่ตัวเองจะได้รับ ส่วนในเรื่องเครื่องมือที่ใช้ก็ขึ้นอยู่กับขนาดของกลุ่มผู้ก่อการร้ายหรือเป้าหมายที่จะโจมตี เครื่องมือที่ใช้จึงมีหลากหลายไม่ใช่แค่เพียงกลุ่มที่มีความเชี่ยวชาญเท่านั้นแต่ผู้กระทำที่ไม่ใช่รัฐบางกลุ่มอาจจะเป็นแค่กลุ่มเด็กฝึกหัดที่อาจจะต้องการความท้าทายแบบธรรมดาสำหรับวิธีการละกลยุทธ์ที่ใช้ส่วนใหญ่จะใช้อุดมการณ์ในการรวมกลุ่มและตั้งองค์กรขึ้นมา เมื่อองค์กรมีความแข็งแรงก็จะทำให้การแปลงตัวเป็นกลุ่มนิรนามทำได้ง่ายมากขึ้น (Talihärm, 2010)

สิ่งที่รัฐควรทำคือสร้างการป้องกันที่เข็มแข็งและระบบการป้องกันที่ไม่สามารถให้ผู้กระทำที่ไม่ใช่รัฐเข้าถึงระบบข้อมูลหรือโจมตีได้ ผู้กระทำที่ไม่ใช่รัฐนั้นยากที่จะหารายชื่อผู้ที่เกี่ยวข้องที่ แต่สิ่งที่สามารถทำได้คือการติดตามพฤติกรรมของแฮกเกอร์รายบุคคลที่มีความเชี่ยวชาญ

เพราะแฮกเกอร์กลุ่มนี้จะทำให้สามารสืบสาวไปยังต้นตอขององค์กร หรือใช้สายลับเหล่านี้ในการแทรกซึมผู้กระทำที่ไม่ใช่รัฐ หากรัฐโดยจู่โจมแล้ว สิ่งสำคัญที่ตามมาคือการสร้างทีมในการช่วยฟื้นฟูรวมไปถึงการร่วมมือกับองค์กรทางไซเบอร์ระหว่างประเทศเพื่อขอความช่วยเหลือจากพวกเขาได้ในทันเวลา

รูปที่ 31 ตัวแสดงและผู้กระทำ (Actors and Terms)

5.3 การรับมือเหตุการณ์ในอนาคต (Future Cyber Attack Response)

จากการวิเคราะห์ในบทที่ 4 การคาดการณ์เหตุการณ์ในอานาคตที่สามารถเกิดกับประเทศไทยโดยได้ถอดรูปแบบจากเหตุการณ์จู่โจมทางไซเบอร์ต่าง ๆ ที่เกิดในต่างประเทศ สามารถถอดบทเรียนและรับมือการเกิดขึ้นได้ดังนี้

5.3.1 สงครามไซเบอร์โดยการใช้ Botnet

สงครามไซเบอร์ที่เกิดขึ้นโดยการใช้ Botnet ในการโจมตีหน่วยงานโครงสร้างพื้นฐานสำคัญทั้งหมดของประเทศ ดังนั้น สกมช. และ ประเทศไทยจะต้องมีทีม ThaiCERT ที่แข็งแรงและว่องไวต่อการจับตาความเคลื่อนไหวทางไซเบอร์ นอกจากนี้ ThaiCERT จะต้องมีเครือข่ายกับประเทศต่างๆ ไม่ว่าจะเป็นเอกชนหรือรูปแบบของรัฐเองเพื่อสามารถช่วยเหลือหรือส่งสัญญาณอินเทอร์เน็ตได้ทันการ การเรียนรู้ที่จะมีการเตรียมระบบสำรองจึงเป็นสิ่งสำคัญเช่นกันในการฟื้นฟู สาธารณูพื้นฐานสำคัญของประเทศเมื่อถูกโจมตี ณ ขณะนี้ประเทศไทยยังคงเป็นประเทศที่มีความเป็นกึ่งเทคโนโลยี นั่นหมายความว่า หน่วยงานโครงสร้างพื้นฐานสำคัญบางส่วนยังคงใช้ระบบแบบเดิมโดยไม่ได้พึ่งเทคโนโลยีทั้งหมด นั่นหมายความว่าประเทศไทยยังสามารถสำรองข้อมูลและสามารถดำเนินการต่อได้ แต่หากเหตุการณ์นี้เกิดในวงกว้างกระทบกับหลายหน่วยงาน รัฐบาลอาจจะต้องให้ สกมช. และ ทีม ThaiCERT เพิ่มการอบรมให้แต่ละหน่วยงานหรือเพิ่มเจ้าหน้าที่จาก ThaiCERT แฝงตัวอยู่กับแต่ละหน่วยงานนั้น ที่มากไปกว่านั้นจุดประสงค์ของการจู่โจมนั่นคือการสร้างความหวาดกลัวให้กับประชาชน การหยุดชะงักของระบบสาธารณูปโภคทั้งหมดจะสร้างความตื่นตระหนกให้กับประชาชน รัฐบาลจำเป็นจะต้องสร้างหน่วยงานประสัมพันธ์ทางด้านไซเบอร์เพื่อลดความตื่นตระหนกและให้ประชาชนสามารถอยู่กับสภาวะที่เกิดขึ้นได้ (ThaiCERT, 2018)

5.3.2 สงครามไซเบอร์จากตัวแสดงที่เป็นรัฐ

การจู่โจมภายใต้ชื่อของรัฐชาติถือว่ามีความชัดเจนและมีจุดประสงค์ที่แน่นอนว่ารัฐชาติเหล่านั้นต้องการอะไร การตอบโต้ของประเทศไทยจึงสามารถทำได้ผ่านหัวหน้ารัฐบาล อาจจะเป็นในด้านการเจรจาทางการทูตเบื้องต้นแต่หากประเทศฝ่ายตรงข้ามไม่ยอมรับในข้อเสนอ รัฐบาลไทยอาจจะต้องกลับมาพิจารณาความสามารถทางด้านไซเบอร์ของชาติตน โดยเฉพาะกลยุทธีที่จะต้องใช้ในสงครามซึ่งขึ้นอยู่กับว่าประเทศที่ต่อรองด้วยนั้นมีความสามรถทางด้านเทคโนโลยีขนาดไหน หากมีมากประเทศไทยจะต้องปกป้องป้องสาธารณูปโภคที่สำคัญของตนก่อนและหากลยุทธ์ เช่น การโจรกรรม หรือ เทคนิคกองโจรไซเบอร์ แฝงตัวในกองทัพไซเบอร์ประเทศนั้นๆ หากเป็นประเทศที่มีเทคโนโลยีที่ต่ำกว่าประเทศไทย รัฐบาลไทยสามารถจู่โจมได้โดยใช้กลยุทธ์เชิงรุกพุ่งเป้าไปยังเป้าหมาย

โดยตรง เพื่อที่จะหยุดยั้งการจู่โจมจากประเทศเหล่านั้น ส่วนอีกทางเลือกหนึ่งคือการเลือกใช้กฎหมายระหว่างประเทศมาเป็นตัวกำหนดกฎเกณฑ์ในการต่อรองสำหรับทั้งสองฝ่าย หรือรัยกร้องขอความช่วยเหลือจากนานาชาติเพื่อข่ามาช่วยในการจู่โจมครั้งนี้

5.3.3 สงครามภายในของรัฐที่ใช้ไซเบอร์เป็นเครื่องมือ

สงครามในรูปแบบนี้มักจะมาพร้อมกับกลยุทธ์แบบกองโจรที่ใช้ในรูปแบบของไซเบอร์ ซึ่งรัฐบาลจะต้องระวังเป็นพิเศษในเรื่องของการใช้ช่องทางออนไลน์ในการรวมตัวกันของผู้ที่มีอุดมการณ์เดียวกัน ยกตัวอย่างเช่น ผู้ก่อความไม่สงบในสามจังหวัดชายแดนภาคใต้ที่จะใช้ช่องทางทางไซเบอร์ในการรวมตัวกันและใช้การจู่โจมทางการเงิน ไม่ว่าจะเป็นการแฮกบัญชีธนาคาร ฟิชชิ่งเมล์ หรือการหลอกเอาเงินในรูปแบบต่าง ๆ เป็นเงินในการสนับสนุนการก่อการร้ายต่อไป ช่องทางการหาเงินรูปแบบนี้ได้แรงบรรดาลใจมาจากกลุ่มก่อการร้ายระดับนานาชาติ หรือปะเทอย่างเกาหลีเหนือ และสิ่งที่รัฐบาลสามารถทำได้คือการร่วมมือกับสถาบันทางการเงินที่เป็นผู้บังคับดูแลกฎระเบียบธนาคารตามสาขาให้มีความรอบคอบ ร่วมมือกับประเทศต่างๆในการแลกเปลี่ยนข้อมูล รวมไปถึงสร้างความตระหนักรู้ทางการใช้ช่องทางทางออนไลน์ให้มากกว่านี้ (Husabø & Bruce, 2009)

สงครามภายในรัฐจะสามารถจัดการได้ง่ายกว่าเพราะสามารถใช้กฎหมายของรัฐชาติในการจับกุมผู้กระทำความผิดได้ แต่เมื่อจับได้แล้วสิ่งที่ควรทำต่อไปคือการร่วมมือกับสำนักงานป้องกันและปราบปรามการฟอกเงินแห่งชาติเพื่อติดตามที่มาของการใช้เงินเหล่านั้นเพื่อสืบไปยังแหล่งของการก่อการร้ายที่ใหญ่กว่า (Free Word Centre, 2012) แต่อย่างไรก็ตามสิ่งที่ผู้ก่อการร้ายต้องการส่วนใหญ่จะมาในรูปแบบของ Bitcoin ไม่ใช่เงินตราที่กำหนดใช้ภายในประเทศ เพราะฉะนั้นเงินตราอิเล็กทรอนิกส์จึงเป็นสิ่งที่ควรเฝ้าระวังหากมีการเรียกค่าไถ่เพื่อนำไปใช้จริง ประการที่สองรัฐควรมีการประชาสัมพันธ์และควบคุมช่องทางทางออนไลน์ให้ดีเพราะข้อความต่าง ๆ ที่ถูกโพสต์ขึ้นจะสามารถเป็นสื่อที่ดึงดูดให้คนทั่วไปที่ไม่มีความตระหนักรู้มาอยู่ร่วมกันได้

5.3.4 สงครามไซเบอร์ที่ตัวแสดงแทนไม่ใช่รัฐ

สิ่งที่ประเทศไทยได้เรียนรู้ คือการจู่โจมทางไซเบอร์ที่มีวัตถุประสงค์ทางการเมืองโดยเฉพาะ การร่วมมือระหว่างนักการเมืองภายใน กลุ่มคนที่ไม่ใช่รัฐ และประเทศที่เป็นพื้นที่ที่สามทางไซเบอร์กับการเกี่ยวข้องซึ่งผลประโยชน์ สิ่งเหล่านี้สามารถเกิดขึ้นได้ในรูปแบบของการกดดันทางการเปลี่ยนแปลงสาธารณูปโภคพื้นฐานที่สำคัญและสาธารณูปโภคพื้นฐานทางสารสนเทศ ซึ่งเป็นการโน้มน้าวที่สำคัญและสามารถชักจูงผู้บริโภคเทคโนโลยีหรือผู้ใช้อินเทอร์ได้อย่างง่ายดายในการเปลี่ยนแปลงทางการเมือง การจู่โจมจากตัวแสดงแทนที่ไม่ใช่รัฐจะสร้างปัญหากับรัฐชาติอย่างสูงเพราะไม่อาจทราบถึงข้อมูลอะไรได้เลย และที่สำคัญรัฐอาจไม่สามารถใช้กฎหมายของรัฐจับกุมพวก

เขาได้ การร่วมมือกับประเทศต่างๆยังคงต้องระวังตัวเพราะไม่สามารถรู้ได้ว่าประเทศใดคอยสนับสนุนและเป็นเบื้องหลังของการจู่โจมครั้งนี้

5.3.5 สงครามไซเบอร์กับผู้กระทำที่เป็นภาคเอกชนภายใต้สัญชาติรัฐ

สงครามไซเบอร์นี้อาจมีความซับซ้อนเนื่องจากไม่สามารถแยกได้ระหว่างบริษัทที่จดทะเบียนขึ้นอยู่ในรัฐชาติ หรือบริษัทเอกชนที่มีแนวคิดตรงข้ามกับรัฐชาติของตน ความขัดแย้งของประโยชน์ส่วนตัว (Kenney, 2015) เพราะฉะนั้นการตรวจจับเพื่อหาวัตถุประสงค์ที่แท้จริงจึงทำได้ยาก การรับมือกับบริษัทเอกชนนั้นจำเป็นต้องใช้การแสดงตัวของบริษัทเพื่อให้รู้ว่าตนไม่ได้รับการสนับสนุนโดยรัฐใด เพราะหากทราบว่าเป็นการสนับสนุนในฐานะรัฐจะทำให้ยิ่งเกิดความรุนแรงมากขึ้น กลายเป็นสงครามระหว่างประเทศได้ง่าย หากประเทศไทยต้องตกอยู่ในสถานการณ์เช่นนี้ อาจทำได้โดยการขอความช่วยเหลือจากชาติมหาอำนาจที่มีความรู้ทางเทคโนโลยีสูงมาเพื่อปราบปรามบริษัทเอกชน หรืออาจของความร่วมมือจากบริษัทเอกชนภายใต้การควบคุมของรัฐเองเพราะจะมีบุคลากรที่มีความรู้ความสามารถในการจัดการกับบริษัทเอกชนเหมือนกัน

5.3.6 สงครามไซเบอร์กับการต่อสู้ในรูปแบบของอาวุธนิวเคลียร์

ประเทศไทยสามารถเรียนรู้สงครามไซเบอร์ชนิดนี้ได้จากเหตุการณ์ Stuxnet ของสหรัฐกับอิหร่านว่าการใช้ไวรัสที่ซับซ้อนตัวนี้ซึ่งมีผลต่อทางกายภาพจริง และเรียนรู้ว่าการรับมือของอิหร่านนั้นเป็นอย่างไร แต่ถึงแม้ว่าประเทศไทยจะยังไม่มีโรงงานนิวเคลียร์เป็นของตนเองแต่ในอนาคตโรงงานนิวเคลียร์สามารถสร้างขึ้นในประเทศไทยได้ หรือไปถึงระบบท่อแก๊งใต้พื้นดินและมหาสมุทรที่ยังคงเป็นเป้าหมายในการก่อการร้าย (Kushner, 2013) การป้องกันไม่ให้เกิดผลเสียกับประชาชนทางที่ดีที่สุดคือการป้องกันไม่ให้ไวรัสซับซ้อนโทรจันเข้ามาทำลายในระบบ แต่ถ้าหากการดจมตีเกิดขึ้นจริง สิ่งที่ประเทศไทยต้องทำถัดมาคือการสร้างฐานหลับภัยใหกับประชาชนชนในบริเวณใกล้เคียงอย่างเพรียบพร้อม เพราะการรับมือที่ดีคือการที่มีการสูญเสียน้อยที่สุด ประเทศไทยยังไม่มีหลุ่มหลบภัยหรือสถานที่หลับภัยอย่างเป็นระบบเพราะฉะนั้นการสร้างสิ่งเหล่านี้ขึ้นมาจะเป็นประโยชน์กับประชาชนในอนาคตรวมถึงภัยพิบัติต่างๆที่จะเกิดขึ้นโดยที่ไม่ทันตั้งตัว

สำหรับการมองในแง่ของกลยุทธ์ การใช้กลยุทธ์ทางทหารหรือการป้องปรามนิวเคลียร์” (Nuclear Deterrence) ไม่สามารถนำมาประยุกต์ใช้กับสงครามไซเบอร์ได้เพราะความไร้ซึ่งพรมแดนและความไม่รู้ซึ่งความร้ายแรงของอาวุธและเขตแดนที่จะได้รับการโจมตีนั้นจะเป็นที่ใดจึงเป็นความยากที่จะใช้สมการในการข่มขู่เช่นอาวุธนิวเคลียร์ได้ เพราะฉะนั้นสิ่งที่ประเทศไทยสามารถทำได้ดีที่สุดคือการป้องกันไม่ให้เกิดการข่มขู่ที่สร้างความเสียหายเท่ากับการระเบิดของอาวุธนิวเคลียร์

นั่นคือการตรวจจับ การเฝ้าระวัง และการล่าตระเวรทางไซเบอร์ 24 ชั่วโมงในทุก ๆ วัน (Kushner, 2013)

5.4 ตัวอย่างสถานการณ์การก่อการร้ายไซเบอร์ในอนาคต

1) ผู้ก่อการร้ายไซเบอร์จะมีจุดประสงค์ที่จะจู่โจมเครือข่ายธนาคาร และการธุรกรรมทางการเงินระหว่างประเทศ และจู่โจมตะกร้าเงินแลกเปลี่ยนระหว่างประเทศมากที่สุด ซึ่งจะทำให้ประชาชนในประเทศสูญเสียความมั่นใจในระบบเศรษฐกิจของประเทศ แต่ในการกระทำนี้จะส่งผลต่อองค์กรขนาดใหญ่หรือไม่นั้นยังไม่สามารถสรุปได้เพราะองค์กรขนาดใหญ่จะสามารถสกัดจับได้ทันก่อนที่จะทำให้เกิดความเสียหายเชิงโครงสร้าง แต่อย่างไรก็ตามการที่แฮกเกอร์ที่ไร้ตัวตนและมีแหล่งที่มาจากประเทศใดในโลกก็ได้จะสามารถทำให้ระบบเศรษฐกิจนั้นหยุดได้ชั่วคราวและการทำลายความมั่นคงนั้นจะสามารถเกิดขึ้นได้ในอนาคต (Marketer, 2013)

2) ผู้ก่อการร้ายไซเบอร์จะมีแนวโน้มที่จู่โจมการจราจรทางอากาศ การควบคุมระบบสัญญาณทางอากาศ และสามารถสร้างความขัดแย้งกันทางพลเรือน ตัวอย่างที่สามารถเห็นได้ชัดเจนคือการควบคุมระบบเซ็นเซอร์ในห้องของกัปตันและการกระทำเช่นนี้สามารถทำได้กับระบบควบคุมรถไฟ(Paul, 2012)

3) ผู้ก่อการร้ายไซเบอร์สามารถที่จะเปลี่ยนตัวยาในโรงงานการผลิตยาและความเสียหายที่เกิดขึ้นนั้นจะรุนแรงจนไม่สามารถคาดเดาได้ (Moph, 2564)

4) ผู้ก่อการร้ายไซเบอร์สามารถเปลี่ยนระดับความดันของระบบท่อส่งแก๊สทำให้เกิดความล้มเหลวของระบบ และทำให้เกิดระเบิดและการเผาไหม้ได้ เฉกเช่นเดียวกับว่าเครื่องมือทางอิเล็กทรอนิกส์จะเป็นช่องโหว่ให้กับผู้ก่อการร้าย (Paul, 2012)

5) ผู้ก่อการร้ายสามารถสับเปลี่ยนข้อมูลในระบบคนเข้าเมืองเพื่อเอื้ออำนวยให้คนสามารถเข้าเมืองได้โดยผิดกฎหมาย (Kenney, 2015)

6) ผู้ก่อการร้ายสามารถเปิดระบบเรือนจำทั่วประเทศ เช่น เปิดประตูเรือนจำทั่วประเทศพร้อมกันจะเป็นการสร้างความชุลมุนแก่ประเทศที่สามารถควบคุมยาก (Kenney, 2015)

7) การล้มเหลวในการใช้ Appliances ต่างๆในมือถือเพราะขณะนี้ทุกอย่างขึ้นอยู่กับมือถือและสัญญาณอินเทอร์เน็ต หากระบบล่ม จะทำให้การใช้งานหยุดชะงัก ไม่ว่าจะเป็นการใช้ระบบโอนเงินออนไลน์ ระบบการรักษาความปลอดภัยต่างๆ ในมือถือส่วนบุคคล หากแฮกเกอร์สามารถขโมย password จากข้อมูลส่วนตัวได้จะทำให้เกิดความโกลาหลในการจัดการ (O'Neill, 2020)

8) การใช้ Artificial intelligence (AI) จนมีอำนาจเหนือคน AI สามารถสั่งให้คนทำในสิ่งที่ผิดพลาดหากคนส่วนใหญ่เชื่อในการทำงานของ AI เช่น AI อาจสั่งให้เด็กใช้นิ้วเขี่ยปลั๊กไฟ ซึ่งเด็กอาจไม่มีความรู้มากนัก หาก AI สั่งให้ทำอะไรก็จะทำตาม (Marketer, 2013)

9) Social media หรือสังคมออนไลน์จะเป็นช่องทางหลักในการจู่โจมบริษัทค้าขายต่างๆ เช่น การใช้ bots ในการเก็บข้อมูลลูกค้าของบริษัทต่าง ๆ และนำมาใช้ประโยชน์ต่อตัวเองและในที่สุด Social media จะเป็นช่องทางที่สำคัญในการสร้างไวรัสเพื่อเรียกค่าไถ่จากบริษัทโดยใช้ข้อมูลของลูกค้าเป็นตัวประกัน (O'Neill, 2020)

5.5 ประสิทธิภาพการใช้กฎหมายระหว่างประเทศและกฎหมายภายในประเทศ รับมือกับการก่อการร้ายไซเบอร์

5.5.1 กฎหมายระหว่างประเทศ jus ad bellum

ตามพื้นฐานดั้งเดิมแล้ว กฎหมายระหว่างประเทศมีไว้เพื่อรักษากฎเกณฑ์และมาตรฐานให้เกิดความสงบสุขของสังคมโลก เมื่อมีสงครามเกิดคิดภาพที่ปรากฏคือการสู้รบแบบเต็มกำกังไม่ว่าจะเป็นภาคพื้นดิน อากาศ หรือผืนน้ำ สร้างความสูญเสียมากมายในเชิงกายภาพ แต่เมื่อโลกปัจจุบันเปลี่ยนไปพื้นที่ในโลกไซเบอร์กลายมาเป็นพื้นที่หนึ่งในสนามรบ ดังนั้นคนส่วนใหญ่ยังคงไม่สามารถจินตนาการภาพของการของการสู้รบทางไซเบอร์ได้ อย่างมากจึงเป็นแค่การจู่โจมทางไซเบอร์เล็กๆน้อยๆ ไม่ว่าจะเป็นการใช้ไวรัสโจมตีระคอมพิวเตอร์ การขโมยข้อมูลส่วนตัวบนพื้นที่ออนไลน์ การหลอกลวงให้เสียเงิน การขู่เรียกค่าไถ่ แต่ในความเป็นจริงแล้วการสู้รบทางไซเบอร์มีความรุนแรงมากกว่านั้นและไม่สามารถเปรียบเทียบได้กับสงครามแบบดั้งเดิมซึ่งกฎหมายระหว่างประเทศได้เขียนไว้ได้อย่างสมบูรณ์

The NATO Cooperative Cyber Defence Centre of Excellence ยืนยันที่จะเสนอกฎหมายฉบับร่างในชื่อของ the Tallinn Manual 2.0. โดยกฎหมายร่างฉบับนี้ได้รวบรวมทฤษฎีที่สำคัญและเกี่ยวข้องกับสงครามไซเบอร์ต่างๆมากมายที่พอจะโน้มน้าวได้ว่าสถานการณ์ทางด้านกฎหมายระหว่างประเทศในปัจจุบันสามารถใช้ได้กับสงครามไซเบอร์หรือการก่อการร้ายไซเบอร์เองก็ตาม ด้วยเหตุผลดังกล่าว the Tallinn Manual 2.0 มีความตั้งใจที่อธิบายกฎเกณฑ์ที่กลายเป็นกฎหมายระหว่างประเทศแล้ว มากกว่าที่จะใช้ปฏิบัติจริงๆในฐานะทางกฎหมายทางเอกสารหรือเป็นสนธิสัญญาที่บังคับใช้จริง ๆ ประเทศอื่น ๆ ที่เป็นประเทศมหาอำนาจเช่น ประเทศรัสเซียหรือประเทศจีน ก็พยายามที่จะผลักดันกฎต่างๆที่เกิดขึ้นโลกไซเบอร์ไม่ว่าจะเป็นความร่วมมือของ the Shanghai Cooperation Organisation ในปี 2009 และ the International Information

Security Code of Conduct in September 2011 ปัญหาอยู่ที่ว่าการปรับปรุงหรือปรับเปลี่ยนกฎด้วยวิธีใดจึงจะทำให้กฎหมายระหว่างประเทศสามารถใช้ได้กับการจู่โจมที่เกิดขึ้นในโลกไซเบอร์ให้ได้ประสิทธิภาพมากที่สุด (Pradillo, 2011).

5.5.2 กฎของ International Humanitarian Law กับสงครามไซเบอร์

เมื่อพิจารณาระหว่างการจู่โจมทางไซเบอร์ หรือการจู่โจมแบบดั้งเดิม การกระทำทั้งสองนี้สามารถเปรียบเทียบในความเท่าเทียมได้หรือไม่ International Humanitarian Law จะสามารถใช้กับสถานการณ์ที่เกิดเหตุการณ์ความขัดแย้งทางทหาร เนื่องจากความหมายที่ล้าหลังนี้ได้กล่าวถึงการจู่โจมในรูปแบบดั้งเดิม แต่อย่างไรก็ตามการจู่โจมไซเบอร์ในปัจจุบันยังไม่รุนแรงถึงขึ้นที่จะเรียกได้ว่ารุนแรงเพียงพอที่จะเป็นจุดชนวน International Humanitarian Law ให้สามารถใช้การได้ ดังนั้นการจู่โจมทางไซเบอร์จำเป็นจะต้องมีความชัดเจนและสอดคล้องกับความเป็น International Humanitarian Law มากพอในปัจจุบัน (O'Neill, 2020)

ทั้งนี้เหตุการณ์ที่ไม่คาดฝันนั้นที่จะเกิดขึ้นกับประชาชนที่ได้รับผลกระทบจากการจู่โจมทางไซเบอร์สามารถเปรียบเทียบได้เท่ากับการจู่โจมแบบธรรมดาหรือแย่กว่าเท่านั้น

ในวรรคเจ็ดของ International Tribunal ระบุไว้ว่า การต่อสู้โดยกองกำลังในความขัดแย้งจะเกิดขึ้นเมื่อมีรัฐชาติใดรัฐชาติหนึ่งเป็นผู้สนับสนุนกองกำลังระหว่างรัฐ โดยเฉพาะในคำนิยามของคำว่ากองกำลังทางทหารนั้นไม่ได้คำนึงถึงการจู่โจมทางไซเบอร์ที่จะก่อความเสียหายด้านด้านกายภาพที่จะเป็นส่วนที่ทำให้กฎหมายฉบับนี้ใช้ได้ และประเด็นที่ว่าการจู่โจมทางไซเบอร์สามารถสร้างผลกระทบในโลกในทางกายภาพนั้นไม่สามารถถูกควบคุมภายใต้ International Humanitarian Law ได้ เพราะการจู่โจมทางไซเบอร์นั้นถูกเชื่อว่าไม่ทำให้เกิดความเสียหายทางกายภาพ การหยุดระบบการตราตารทางอากาศนั้นก็ยังสามารถทำได้ในหลายแง่มุม เช่น การเพิ่ม server หรือเปลี่ยน server เพื่อไม่ให้เกิดความเสียหาย โดยแยก server ไม่ให้เป็นอันเดียวกับของประชาชน (Pradillo, 2011; O'Neill, 2020)

เนื่องจากปราศจากความเห็นด้วยอย่างเป็นมติเอกฉันท์ระหว่างรัฐชาติในเรื่องของการจู่โจมทางไซเบอร์ที่มีผลทางกายภาพ เพราะฉะนั้นจึงทำให้ International Law ปราศจากกรอบแนวคิดที่คอยกำหนดหรือประเมินความเสียหายและระดับความเสียหายที่ชัดเจน แต่มีความพยายามหนึ่งที่เสนอการทดสอบแบบ “Functionality Test” ใน the Tallinn Manual ในการทดสอบเขียนไว้ว่า การพยายามที่จะขัดขวางการทำงานหรือทำให้การทำงานทางกายภาพของสาธารณูปโภคที่สำคัญเสียหายถือเป็นสิ่งที่สามารถเปรียบเทียบได้เท่ากับการต่อสู้แบบกองกำลังทางทหารทางกายภาพ (Rule 30, Para. 10 of the Tallinn Manual)

มาตรฐานการวัดนี้อาจจะเป็นบันไดขั้นแรกแต่ยังคงไม่สามารถไปไกลได้มากนักที่จะใช้กรอบแนวคิดนี้เกี่ยวกับการสร้างความเสียหายและเป็นจุดที่ทำให้ International Humanitarian Law สามรถใช้ได้การจู่โจมทางไซเบอร์นั้นจะต้องมีความจัดเจนเรื่องความเสียหายและระดับความรุนแรงที่ชัดเจนมากกว่านี้การหยุดยั้งระบบในระยะหนึ่งอาจจะยังไม่ได้สร้างความเสียหายทางกายภาพเท่ากับการจู่โจมแบบดั้งเดิม แต่บางครั้งผลจากกการต่อสู้ทางไซเบอร์อาจจะรุ่นแรงกว่าการจู่โจมแบบดั้งเดิมด้วยซ้ำและการปราศจากการควบคุมทางกฎหมายหรือไม่ได้อยู่ภายใต้การบังคับใช้ของ International Humanitarian Law อาจจะทำให้การจู่โจมทางไซเบอร์มีความรุนแรงมากขึ้น

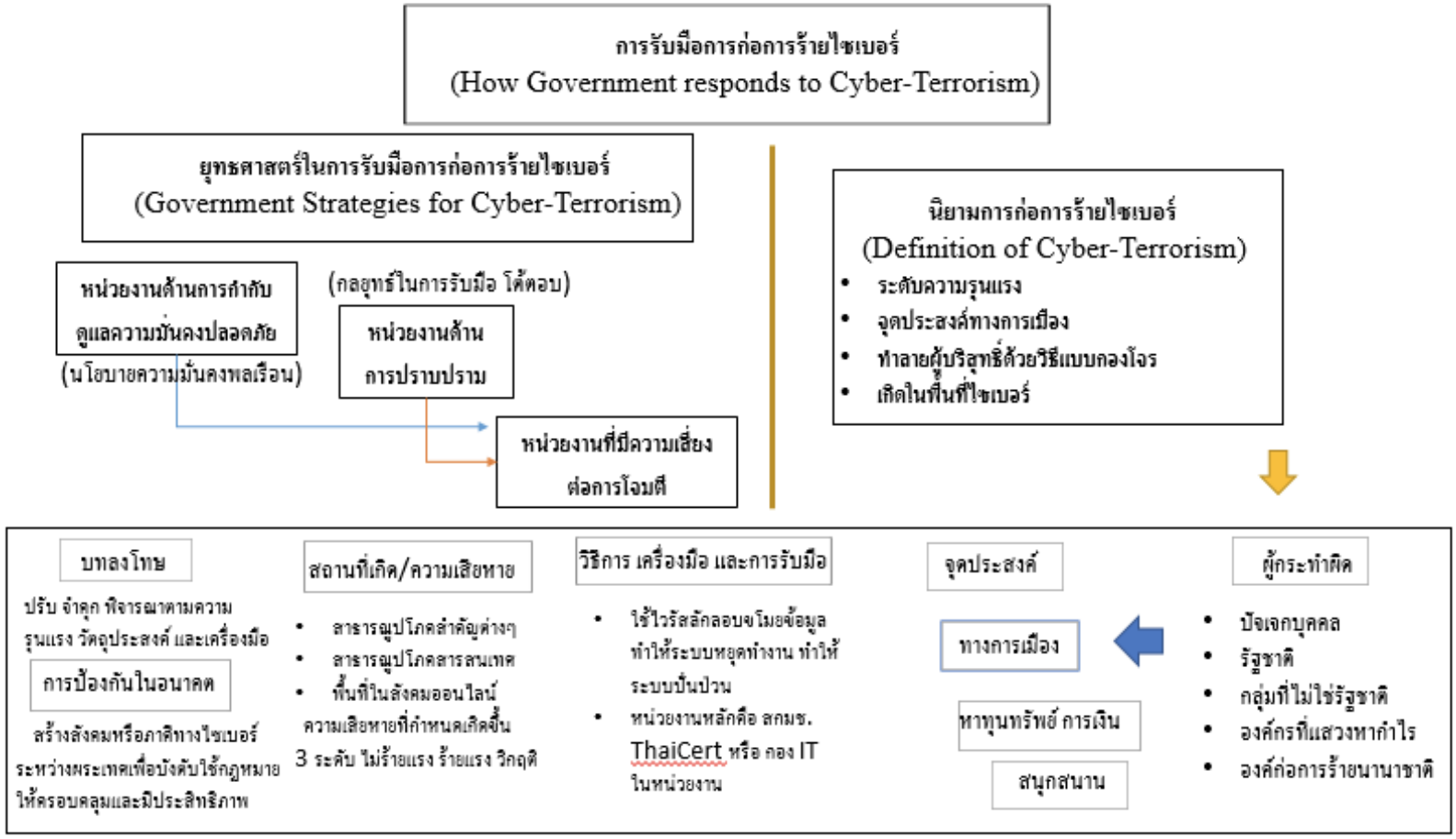
5.5.3 ปัญหาเรื่องอำนาจหน้าที่ที่ได้รับมอบหมาย (The Attribution Problem)

ตามที่ Common Article 2 ใน Geneva Conventions 1949 ได้กล่าวถึง ความขัดแย้งทางกองกำลังไว้ว่า International Humanitarian Law จะต้องสามารถใช้ได้ครอบคลุมทุกกรณีเมื่อเกิดสงคราม โดยสงครามในที่นี้หมายถึง การเกิดขึ้นซึ่งการสู้รบของอัครภาคีผู้ทำสัญญาทางการทูต (High Contracting Parties) ทั้งสองฝ่ายหรือมากกว่าสองฝ่าย ถึงแม้ว่าอีกฝ่ายจะมิได้คำนึงถึงก็ตาม ปัญหาที่เกิดขึ้นจากถ้อยคำนี้คือกลุ่มที่อยู่ในความขัดแย้งจะต้องเป็นส่วนหนึ่งของกองกำลังทางทหารของรัฐนั้นๆ ดังนั้นในกรณีนี้จึงไม่สามารถใช้กับการเกิดขึ้งของการจู่โจมทางไซเบอร์ได้ เพราะการจู่โจมทางไซเบอร์ไม่จำเป็นจะต้องมาจากกองกำลังทางทหารเท่านั้นเพราะแม้เพียงแต่ปัจเจกบุคคลก็สามารถที่จะประกาศสงครามกับประเทศมหาอำนาจได้ ดังนั้นจึงขึ้นอยู่กับการพิจารณาว่าหากมีการจู่โจมเกิดขึ้นจะเป็นเพียงแค่อาชญกรรมทางไซเบอร์ธรรมดาหรือการจู่โจมทางทหาร (Schmitt, 2010)

เมื่ออินเทอร์เน็ตพัฒนามากขึ้นเรื่อย ๆ การมีสมาคมที่ไร้ตัวตนจึงมีเพิ่มขึ้น และเป็นเรื่องยากที่จะใช้อำนาจทางกฎหมายกับการจู่โจมทางไซเบอร์ที่อยู่ภายในรัฐ ตัวอย่างที่เห็นได้ชัดคือการแฮก Solar-winds และ Water Plant ใน Florida ซึ่งมีหลักฐานชัดเจนว่าเป็นการกระทำที่มีวัตถุประสงค์ทางการเมืองแอบแฝงแต่พยามใช้ตัวแสดงอื่นในการบังหน้า ดังนั้นแม้ว่าประชาชนจะได้รับผลกระทบจากความรุนแรงครั้งนี้ แต่ก็ไม่สามารถใช้ International Humanitarian Law ในการจัดการได้เพราะยังมีความไม่ชัดเจนในอำนาจหน้าที่ที่ได้รับมอบหมายหรือการกล่าวถึงไซเบอ์ใน International Humanitarian Law อย่างชัดเจน เมื่อต้องย้อนกลับไปในปี 1945 นี่จึงควรเป็นเวลาที่รัฐชาตอทั้งหมายจะต้องร่วมมือการร่าง International Humanitarian Law ฉบับใหม่ที่ให้ความหมายกับสงครามไซเบอร์ การจู่โจมทางไซเบอร์ อาชญากรรมไซเบอร์ หรือการก่อการร้ายไซเบอร์ ได้อย่างชัดเจน (Schmitt, 2010)

การปรับปรุงกฎหมายภายในประเทศนั้นเป็นเรื่องที่ง่ายกว่ากฎหมายระหว่างประเทศเพราะเขตอำนาจรัฐชาติสามารถบังคับใช้ได้อย่างเด็ดขาด แต่สิ่งที่เกิดขึ้นคือประเทศไทยได้นำ

บทลงโทษสำหรับข้อหาการก่อการร้ายไซเบอร์มาใช้ลงโทษได้จริงหรือไม่ และหากกล่าวกระบวนการยุติธรรม การพัฒนาพฤติกรรมของผู้ต้องขังที่ทำผิดคดีนี้จะเป็นในรูปแบบใดเพราะพวกเขายังมีประโยชน์ต่อหน่วยงานต่างๆในการสร้างระบบป้องกันทางไซเบอร์หรือเป็นกองทัพทางไซเบอร์ให้กับรัฐ ดังนั้นสิ่งที่ประเทศไทยต้องทบทวนคือหลักสูตรในการพัฒนาพฤตินิสัยของผู้ต้องขังที่มาด้วยความผิดเหล่านี้เพราะจะให้พวกเขาเข้าไปรวมตัวกับผู้กระทำผิดเชิงกายภาพไม่ได้



รูปที่ 32 การรับมือการก่อการร้ายไซเบอร์

5.6 ข้อเสนอแนะ

จากวัตถุประสงค์ของการศึกษางานวิจัยเล่มนี้คือการค้นคว้าหาวิธีการรับมือทางการก่อการร้ายไซเบอร์ที่เหมาะมกับสถานการณ์ที่เกิดขึ้นกับประเทศไทย ณ ตอนนี้ จากการศึกษาประกอบไปด้วยวิธีการรวบรวมข้อมูลชั้นปฐมยภูมิและทุติยภูมิทั้งในรูปแบบภาษาไทยและภาษาอังกฤษ การสัมภาษณ์เชิงลึกจากผู้เชี่ยวชาญทางเทคนิคและผู้เชี่ยวชาญทางนโยบายทางไซเบอร์ของหน่วยงานภาครัฐและการสัมมนาต่าง ๆ เกี่ยวกับผลกระทบจากภัยคุกคามทางไซเบอร์

สิ่งสำคัญประการแรกของวิจัยเล่มนี้คือการตีความความหมายของการก่อการร้ายไซเบอร์เพื่อใช้ความหมายนั้นมาจำแนกแยกแยะการกระทำของผู้โจมตีทางหลาย เมื่อรัฐบาลสามารถกำหนดคำนิยามของการก่อการร้ายไซเบอร์ได้แล้ว สิ่งที่ตามมาคือการวิเคราะห์ผู้กระทำความผิด วิธีการที่ใช้ผู้ถูกกระทำหรือเหยื่อ ด้วยวิธีการผ่าตัด โดยจะเริ่มต้นแยกจากจำนวนชิ้นส่วนที่น้อยที่สุดนั่นคือจุดเริ่มต้น ผู้กระทำ พฤติกรรมทางจิตวิทยาที่ก่อให้เกิดการก่อการร้ายทางไซเบอร์ การวิเคราะห์ซึ่งวิธีการจะเป็นภารกิจของหน่วยปราบปรามที่จะต้องรู้ถึงจิตวิทยาของผู้กระทำให้การเลือกใช้เครื่องมือเพื่อสกัดจับได้ทันท่วงที สุดท้ายคือหน่วยงานที่เป็นสาธารณูปโภคสำคัญของประเทศ จากการสำภาษณ์และเก้บข้อมูลทราบว่าหน่วยงานประเภทนี้มีความพร้อมที่จะรับมือและคืนสภาพสู่ปกติได้อย่างมีประสิทธิ-พโดยการร่วมมือจาก สกมช. และ ThaiCERT แต่อย่างไรก็ตามในด้านของนโยบายประเทศไทยจะต้องให้ความร่วมมือกับภาคีหรือชุมชนระหว่างประเทศให้แนบแน่นพร้อมทั้งแบ่งปันข้อมูลต่างๆ เพื่อโชว์ศักยภาพว่าประเทศไทยนั้นมีกฎหมายรับรองที่จะจับกุมผู้คุกคามทางไซเบอร์ได้ตามกฎหมายภายในประเทศเพื่อลดความเสี่ยงของการเป็นประเทศที่ตกเป็นเป้าหมายของการตั้งฐานทัพในการโจมตี ถึงแม้ว่าประเทศไทยจะยังไม่เคยประสบกับการก่อการร้ายไซเบอร์แบบเต็มรูปแบบตามคำนิยาม แต่หน่วยงานต่าง ๆ ก็มีความพร้อมในการรับมือ ฟื้นฟู และป้องกันอย่างเต็มที่กับภัยคุกคามที่ชื่อว่า การก่อการร้ายไซเบอร์ ในอนาคต (ThaiCERT, 2018)

ในประเด็นการรับมือภัยคุกคามทางด้านไซเบอร์ เนื่องจากประเทศไม่ได้ให้ข้อจำกัดความการก่อการร้ายทางไซเบอร์ได้ตรงกับเหตุการณ์ที่เกิดขึ้นในประเทศไทย ดังนั้นเหตุการณ์การก่อการร้ายไซเบอร์จริง ๆ จึงไม่ได้มีขึ้น การรับมือของประเทศไทยจึงเป็นการรับมือภัยจูโจมตามลักษณะที่ผู้กระทำลงมือกระทำแตกต่างกันไป เช่น การจู่โจมโดยการแฮกข้อมูล การเรียกค่าไถ่ผ่าน ransomware ซึ่งแตกต่างจากการก่อการร้ายที่จะต้องประกอบไปด้วยวัตถุประสงค์ทางการเมืองและมีผลกระทบที่รุนแรงเป็นหลัก ดังนั้นการแก้ปัญหาทางเทคนิคจึงเป็นประเด็นที่สำคัญของประเทศไทย การสามารถแยกประเภทการจู่โจมต่าง ๆ ออกมาให้เห็นได้อย่างชัดเจนและเก็บข้อมูลด้วยระบบสถิติสามารถประเมินได้ว่าการจู่โจมแบบไหนมีแนวโน้มจะเกิดได้มากที่สุดและทีมผู้เชี่ยวชาญทางเทคนิคจะต้องมีการค้นคว้า ประสานงาน และเตรียมพร้อมรับมือกับภัยคุกคามประเภทนั้นได้ทันที

ประเด็นที่น่าสนใจในการอภิปรายคือ การใช้กฎหมายเข้ามาเป็นส่วนหนึ่งในการควบคุมไม่ให้เกิดการก่อการร้ายไซเบอร์ในอนาคต ซึ่งกฎหมายเหล่านี้ได้เกิดขึ้นในหลายๆประเทศ เช่น สหราชอาณาจักร สหรัฐอเมริกา จีน รัสเซีย หรืออินเดีย ที่เคยมีประวัติการก่อการร้ายทางไซเบอร์มาก่อน ประเทศไทยสามารถนำกฎหมายเหล่านั้นมาเป็นรูปแบบในการวิเคราะห์เพื่อปรับปรุงกฎหมายของตัวเองได้ กฎหมายปัจจุบันที่มีอยู่นั้นเป็นกฎหมายฉบับใหม่ครอบคลุมการกระทำที่เกิดขึ้นทางไซเบอร์ แต่อย่างไรก็ตามจำเป็นจะต้องมีการวิเคราะห์ไปยังตัวผู้กระทำที่แตกต่างกัน เช่นผู้กระทำที่เป็นตัวบุคคล ผู้กระทำที่เป็นรัฐชาติ และผู้กระทำที่เป็นองค์อิสระ ทั้งภายใต้อำนาจของรัฐชาติหรือนอกเหนืออำนาจของรัฐชาติ นอกจากนี้กำฆมายจะต้องมีความใกล้เคียงกับกฎหมายระหว่างประเทศเพื่อให้มีความสอดคล้องกันเมื่อต้องมีการจับผู้ร้ายในต่างประเทศเนื่องจากไซเบอร์สามารถเกิดขึ้นได้โดยไม่มีเขตแดน

การใช้อำนาจของกฎหมายปัจจุบันยังไม่พบผู้ที่ทำผิดในพระราชบัญญัติไซเบอร์ฉบับนี้ และยังไม่มีกระบวนการทำโทษใด ๆ ที่สามารถเป็นตัวชี้วัดว่าผู้กระทำผิดทางไซเบอร์มีการประพฤติตัวที่ดีขึ้นหลังจากเข้าสู่กระบวนการยุติธรรมหรืออยู่ภายใต้ระบบพัฒนาพฤตินิสัยของกรมราชทัณฑ์ ดังนี้ในส่วนนี้จริงเป็นประเด็นที่น่าคิดและวิจัยต่อไปว่า ระบบใดควรจะเป็นระบบที่ดีที่สุดที่จะสามารถทำให้ผู้กระทำความผิดมารับโทษและเกิดประโยชน์กับรัฐบาลและตัวผู้กระทำความผิดเอง

5.6.1 Pian Points ของการใช้เทคโนโลยีที่นำไปสู่การกำหนดนโยบาย

ในมุมมองของทหารและนโยบายการป้องกันประเทศทางการจูโจมไซเบอร์มีความแตกต่างกัน ฝ่ายนโยบายของประเทศไทยอาจจะมุ่งวิเคราะห์เป็นรายบุคคลมากกว่าเป็นกลุ่ม เพราะส่วนใหญ่เป้าหมายจะเป็นเชิงพานิชย์มากกว่าการขโมยทรัพย์สินทางปัญญาหรือละเมิดกฎหมายขโมยข้อมูล อาจจะใช้ศาสตร์ทางจิตทางวิทยาในการวิเคราะห์ โดยพบว่ามนุษย์มีอคติ (bias) ในการรับข่าวสารข้อมูลต่าง ๆ ดังนั้น หากข้อมูลที่ถูกส่งมาเป็นภัยต่อความมั่นคงแต่มนุษย์เลือกที่จะเชื่อ ไวรัสต่าง ๆ ที่อาศัยช่องทางทางอินเทอร์เน็ตผ่านจากระบบคอมพิวเตอร์จึงเป็นการเปิดช่องว่างทำให้แฮกเกอร์สามารถเข้าโจมตีได้ หรือแม้กระทั่งอคติขององค์กรที่ไม่ให้ความสนใจหรือความตระหนักรู้ในเรื่องของความมั่นคงปลอดภัยไซเบอร์ จึงขาดการติดระบบป้องกันที่มีประสิทธิภาพทำให้แฮกเกอร์สามารถจู่โจมเข้ามาได้ง่าย นอกจากนี้มนุษย์ยังมีความอยากรู้อยากเห็น การกระตุ้นความสนใจกับสิ่งที่เกิดขึ้นกับตนเองและผู้อื่นหรือหากแฮกเกอร์รู้ความสนใจหรือรู้จุดอ่อนของผู้ที่เป็นเหยื่อก็จะสามารถส่งอีเมล์ หรือที่เรียกกันว่า Phishing เป็นต้นในการหลอกล่อให้เหยื่อตายใจและให้พาสเวิร์ดในที่สุด หลังจากนั้นแฮกเกอร์จะสามารถขโมยข้อมูลส่วนตัวหรือหลอกถามข้อมูลต่างๆด้วยความสมัครใจของตัวเหยื่อเองได้ เพราะฉะนั้นหลักการกระตุ้นความสนใจจึงเกี่ยวข้องกับวิธีเชิงจิตวิทยาที่สัมพันธ์กับแฮกเกอร์และเหยื่อ (CISA, 2009)

ในส่วนของพฤติกรรมส่วนตัว มนุษย์ส่วนใหญ่จะเคยชินกับพฤติกรรมเดิม ๆ แต่ในขณะที่เทคโนโลยีมีการเปลี่ยนแปลงอยู่ทุกเวลา ดังนั้นการยึดติดกับพฤติกรรมเดิม ๆ จะทำให้เหยื่อส่วนใหญ่ตกเป็นเป้าหมายของแฮกเกอร์ได้ง่ายขึ้น เช่น การใช้ชีวิตเป็นกิจวัตรประจำวันหรืออธิบายตาม Routine Theory ที่ผู้กระทำความผิดจะสามารถสังเกตพฤติกรรมเหยื่อได้อย่างง่ายดาย และสามารถหาช่องว่างที่จะเข้าถึงระบบของเหยื่อนั้นได้ (Berner, 2003) ดังนั้น การเปลี่ยนพฤติกรรมหรือการเพิ่มความระมัดระวังให้มากขึ้นจะทำให้ผู้กระทำความผิดหรือแฮกเกอร์ไม่สามารถหาช่องว่างในการโจมตีได้

นอกจากอิทธิพลภายตัวของมนุษย์แล้วที่ทำให้เกิดข้อจำกัดในกรใช้เทคโนโลยี อิทธิพลภายนอกยังมีผลในการตัดสินใจ ประกอบไปด้วยความเหนื่อย ความเครียด การเบี่ยงเบนทางความคิด ภาวะหมดไฟหรือหมดพลังภาวะความกดดันจากที่ทำงาน จากครอบครัว จากการเรียน จะทำให้มนุษย์มีการใช่ความนึกคิดที่ผิดพลาดและเป็นสาเหตุให้เกิดผลเสียหรือข้อสำกัดในการตัดสินใจ ความเหนื่อยล้านี้จะทำให้เกิดการขาดความสนใจหรือการขาดความตระหนักรู้ในสิ่งใหม่ของเทคโนโลยี ซึ่งมีผลให้เกิดช่องว่างสามารถทำให้แฮกเกอร์สามารถเข้ามาจู่โจมได้ (Doffman, 2019) ด้วยเหตุผลที่เทคโนโลยีมีความเปลี่ยนแปลงอยู่ตลอดเวลาและมีการพัฒนาอยู่ตลอดเวลา การเรียนรู้ใหม่จึงมีขึ้นตลอดเวลา ดังนั้นการแก้ปัญหาให้ตรงจุดพร้อมเปลี่ยนแปลงปัจจัยที่เป็นอิทธิพลภายในและภายนอกจึงเป็นสิ่งสำคัญ แต่อย่างไรก็ตามความเกี่ยวข้องระหว่างความนึกคิดของเหยื่อและผู้ก่ออาชญากรรมทางไซเบอร์นั้นเป็นไปในทางเดียวกันนั่นคือ มนุษย์มักจะมีข้อจำกัดในการตัดสินใจ ไม่ว่าคุณจะเป็นเหยื่อหรือผู้กระทำแต่ข้อจำกัดที่เกิดขึ้นนั้นจะเกิดสามารถที่จะปรากฏได้ในผู้ถูกกระทำและผู้โดนกระทำเอง และนั่นเปรียบเสมือนทางออกที่จะป้องกันการเกิดการจู่โจมทางไซเบอร์ที่เกิดจากข้อจำกัดของอาชญากรในโลกเสมือนจริงนั่นเอง

โดยสรุปแล้วความเหนื่อยล้าในการจัดการกับโลกไซเบอร์นั้นมีความซับซ้อนมากและยากแก่การเข้าใจในโลกแห่งความเป็นจริง โดยเฉพาะในในโลกแห่งความจริงที่มีพร้อมอุปสรรคในเรื่องโรคระบาดยิ่งทำให้ผู้ปฏิบัติด้านไซเบอร์มีความท้อแท้และเหนื่อยมากขึ้นเพราะทุกอย่างจะต้องขึ้นกับโลกอินเทอร์เน็ต การเฝ้าระวังภัยต่าง ๆ ให้กับประชาชนผู้ใช้อินเทอร์เน็ตและการเฝ้าระวังการฝ่านฝืนของประชาชนจะทำให้เจ้าหน้าที่เหล่านี้มีความเหนื่อยล้ามากยิ่งขึ้น เช่น การรวมตัวกันของแฮกเกอร์ในรูปแบบขององค์กรจะมีมากขึ้น การรวม dark web ต่าง ๆ (Doffman, 2019) การใช้อุปกรณ์ราคาถูกที่เอื้อเฟื้อต่อการเข้าถึงอินเทอร์เน็ตและเพิ่มอัตราการเกิดอาชญากรรม การยังอยู่ในรูปของคนนิรนามที่ไม่สามารถจับตัวตนได้จริง และการไม่สามารถป้องกันเหยื่อได้เพราะมีเหยื่อจำนวนมากที่พร้อมจะตกเป็นเป้าหมายในการก่ออาชญกรรมทางไซเบอร์

5.6.2 การกำหนดนโยบายและการต่อยอดทางด้านวิชาการ

การเชื่อมโยงระหว่างแฮกเกอร์และความนึกคิดต่ออาชญากรรมทางไซเบอร์เป็นสิ่งที่น่าสนใจ จะสามารถรู้ได้หรือไม่เพราะเหตุใดแฮกเกอร์จึงต้องการจู่โจมคอมพิวเตอร์ของฝ่ายตรงข้าม การจู่โจมด้วยวัตถุประสงค์ทางการเมืองหรือจุดประสงค์ส่วนตัวจะใช้วิธีที่แตกต่างกันหรือไม่ ดังนั้น การอธิบายพฤติกรรมทางจิตวิทยาของแฮกเกอร์เพื่อแสดงออกถึงความเข้าใจในจุดประสงค์ในการก่ออาชญากรรมจึงเป็นสิ่งจำเป็น

จากการวิเคราะห์พฤติกรรมของแฮกเกอร์ในประเทศไทยจากการสัมภาษณ์ผู้ที่มีความรู้และเชี่ยวชาญทางเทคโนโลยี พฤติกรรมของแฮกเกอร์ส่วนใหญ่จะมุ่งสังเกตเหยื่อที่เป็นจุดอ่อนขององค์กร เพื่อใช้เหยื่อนั้นเป็นเครื่องมือเข้าถึงความลับขององค์กร ส่วนใหญ่องค์กรโดยทั่วไปจะขาดประสิทธิภาพในการควบคุมคนในองค์กรของตน เมื่อเหยื่อเกิดความตื่นตระหนก ก็ไม่มีแผนสำรองใดสามารถที่จะรับมือได้ แต่ในปัจจุบันมีระบบ Cognitive security ที่จะสามารถใช้ AI ในการควบคุมระบบวิเคราะห์พฤติกรรมของมนุษย์ที่เป็นอยู่อย่างมีรูปแบบซ้ำ ๆ กัน โดยระบบ Cognitive security จะสามารถสังเกตได้ว่าสิ่งที่ปลอมแปลงเข้ามานั้นเป็นภัยต่อองค์กรหรือไม่และระบบนี้จะมีประสิทธิภาพมากเมื่อมีการอัพเดทอยู่เรื่อย ๆ และจะสามารถปกป้องไม่ให้มีแฮกเกอร์สามารถหาช่องว่างจากระบบได้ ระบบ Cognitive security ถูกพัฒนามาจากการตรวจพบ Cognitive hacking ที่สามารถหลอกลวงเหยื่อเพื่อให้สามารถบอกข้อมูลความลับของตนและองค์กร โดยการหลอกล่อคนที่เต็มไปด้วยอคติ ประสบการณ์ดั้งเดิม และความตระหนักรู้ที่มีจำกัด จึงทำให้แฮกเกอร์สามารถควบคุมความคิดของบุคคลเหล่านี้จากการหาประโยชน์จากคนที่อ่อนแอและมีความบกพร่องทางเทคโนโลยี ไม่ว่าจะเป็น ประเภท Overt การใช้วิธีการจู่โจมแบบเปิดเผย เช่น Spoofing Mail หรือ Covert การใช้วิธีการจู่โจมแบบใช้วิธีภายในแบบไม่แสดงออกให้บุคคลภายนอกสังเกตเห็น เช่น Phishing เป็นหนึ่งในการหลอกลวงทางโลกออนไลน์ที่พบได้บ่อยที่สุด Phishing มีหลายรูปแบบ(Greenberg, 1995) การหลอกลวงประเภทนี้มักจะเกี่ยวข้องกับการใช้กลอุบายหลอกล่อผู้ใช้งาน และการแอบอ้างเป็นเว็บไซต์เพื่อพยายามขโมยข้อมูลส่วนตัวหรือข้อมูลทางการเงินของเหยื่อ ด้วยการส่ง notifications ไปที่โทรศัพท์ของเหยื่อบ่อย ๆ จากการวิเคราะห์จากทั้ง 2 ประเภทแฮกเกอร์ที่กระทำนั้นจะใช้เครื่องมือที่แตกต่างกันเพื่อวัตถุประสงค์ที่แตกต่างกัน แต่โดยทั้งสองประเภทแล้วหากบุคลากรมีความรู้เบื้องต้นด้านเทคโนโลยีจะทำให้สังเกตได้ว่ากำลังตกเป็นเหยื่อของแฮกเกอร์ และแฮกเกอร์เองก็จำเป็นที่จะต้องวิเคราะห์พฤติกรรมของแต่ละบุคคลเพื่อเลือกหาวิธีที่เหมาะสมกับเหยื่อแต่ละประเภท ทฤษฎีที่สามารถอธิบายได้ทางจิตวิทยา เช่น ทฤษฎีการเรียนรู้ (Learning theory) การเปลี่ยนแปลงพฤติกรรมซึ่งเนื่องมาจากประสบการณ์ของเหยื่อหรือแฮกเกอร์ กระบวนการที่ทำให้คนเปลี่ยนแปลงพฤติกรรม ความคิด คนสามารถเรียนได้จากการได้ยินการสัมผัส การอ่าน การใช้เทคโนโลยีการเรียนรู้ของเด็กและผู้ใหญ่จะต่างกัน (Greenberg, 1995) เด็กจะเรียนรู้ด้วยการเรียนใน

ห้องการซักถาม ผู้ใหญ่มักเรียนรู้ด้วยประสบการณ์ที่มีอยู่ แต่การเรียนรู้จะเกิดขึ้นจากประสบการณ์ที่ผู้สอนนำเสนอ ทั้งนี้จะมีการเสนอข้อเสนอแนะเชิงนโยบาย และข้อเสนอแนะทางด้านวิชาการควบคู่กันไป ดังนี้

5.7 ข้อเสนอแนะเชิงนโยบาย และการนำนโยบายไปสู่การปฏิบัติ

5.7.1 หน่วยงานด้านการกำกับดูแลความมั่นคง

1) ทิศทางและเป้าหมายของนโยบาย

หน่วยงานด้านการกำกับดูแลความมั่นคงจำเป็นจะต้องศึกษากฎหมายระหว่างประเทศและการบังคับใช้ของประเทศต่าง ๆ โดยผู้วิจัยได้นำเสนออย่างละเอียดของแต่ละประเทศที่มีความเชี่ยวชาญทางด้านไซเบอร์ไว้ในบทของการทบทวนวรรณกรรม ตัวอย่างเช่นการใช้กฎหมายของประเทศสหรัฐและประเทศตะวันออกกลางจะมีลักษณะที่แตกต่างกันขึ้นอยู่กับประสบการณ์ของแต่ละประเทศที่เจอกับการก่อการร้ายไซเบอร์ ดังนั้นประเทศไทยจะต้องมีจุดยืนนโยบายเป็นของตนเองเพื่อให้แสดงให้นานาชาติเห็นว่าประเทศไทยจะปฏิบัติอย่างไรกับผู้จู่โจมทางไซเบอร์ (Conway, 2003)

2) ทางเลือกในการนำไปปฏิบัติ

หน่วยงานด้านการกำกับดูแลความมั่นคงต้องทำการประสานหารือกับหน่วยงานฝ่ายกระบวนการยุติธรรม เช่น ศาล อัยการ กรมราชทัณฑ์ และตำรวจ เพื่อร่างนโยบายที่มีผลบังคับใช้จริงและร่วมกันคิดในการหาวิธีลงโทษตามความผิดของผู้จู่โจมทางไซเบอร์ เช่น ความผิดฐานคดีโจรกรรมข้อมูลสามารถนำไปฝึกฝนเพื่อช่วยรัฐบาลได้ หรือหากเป็นความผิดในฐานการจู่โจมสาธารณูปโภคสำคัญต่างๆ ก็สามารถให้ศาลพิจารณาถึงบทลงโทษและนำผู้กระทำความผิดเหล่านั้นไปเป็นส่วนหนึ่งของหน่วยงานรัฐบาลเพื่อรักษาความปลอดภัยเพราะผู้ที่จู่โจมนั้นมีความเชี่ยวชาญทางด้านเทคโนโลยี (Cooley, 1894)

3) ผลกระทบของนโยบาย

ผลกระทบที่จะเกิดขึ้นหากมีการปฏิบัติตามนโยบายข้างต้น จะทำให้มีความชัดเจนในการรับมือกับปัญหาการจู่โจมทางไซเบอร์ และเป็นทิศทางที่สำคัญทำให้สังคมโลกเห็นว่าประเทศไทยมีจุดยืนเป็นอย่างไร แต่นโยบายการรับมือนี้จะต้องทำอย่างเป็นรูปร่างโดยมีการออกกฎหมายและปฏิบัติใช้จริง อาจออกมาในรูปแบบของบทลงโทษที่มีอยู่ใน พรบ. ไซเบอร์ที่มีอยู่แล้วหรือเพิ่มเติมในส่วนของการอบรมตำรวจ อัยการ ผู้พิพากษา รวมไปถึงการคิดโปรแกรมการฟื้นฟูการกระทำความผิดของผู้ต้องขังร่วมกับกรมราชทัณฑ์ต่อไป (Cooley, 1894)

4) มาตรฐานหรือบรรทัดฐาน

มาตรฐานนี้ต้องใช้ระดับการวัดเดียวกันอย่างเสมอภาค เช่น มีการเก็บสถิติร่วมกันของสกมช. สมช. หน่วยข่าวกรอง ธนาคารแห่งชาติ ร่วมกับหน่วยงานในกระบวนการยุติธรรม เพื่อมาพิจารณาว่าจำนวนผู้กระทำความผิดมีเท่ากันหรือไม่และส่วนใดที่ยังไม่สามารถจับได้ หรือส่วนที่จับได้นั้นเป็นผู้กระทำความผิดประเภทใดมากที่สุด และได้รับบทลงโทษเป็นอัตราสัดส่วนเท่าใด รวมไปถึงการฟื้นฟูผู้กระทำความผิดประสบความสำเร็จไปแล้วกี่รายอาจใช้เกณฑ์การไม่กลับมากระทำผิดซ้ำภายในเวลา 3 ปี และหลังจากได้รับบทลงโทษและผู้กระทำความผิดนั้นสามารถกลับมาทำงานให้รัฐเป็นกรณีพิเศษได้หรือไม่ (Cooley, 1894)

5) การประเมินผลนโยบาย

การประเมินผลต้องขึ้นอยู่กับแต่ละหน่วยงานที่รับผิดชอบต่อภารกิจของตนเอง อาจจะประเมินโดยการยอมรับประเทศไทยในฐานะประเทศหนึ่งที่มีประสิทธิภาพในการควบคุมการจู่โจมทางไซเบอร์ การเข้าร่วมพันธกรณี หรือข้อตกลงนานาชาติต่าง ๆ โดยกำหนดจำนวนครั้งและควรทำให้ได้ร้อยละ 80 ปี ในส่วนจำนวนของผู้กระทำความผิดควรมีการประเมินถึงจำนวนตัวเลขที่ลดลงความรุนแรงในระดับสูงสุดไม่ควรเกิดมากกว่า 1 ครั้งต่อปี และความเสียหายที่เกิดขึ้นได้รับการฟื้นฟูกลับมาได้มากกว่าร้อยละ 80 ของความเสียหายทั้งหมด และควรมีการติดตามผู้กระทำความผิดหลังจากสิ้นสุดการลงโทษ หากสามารถกลับมาทำงานให้รัฐได้ผลดีหรือผลเสียที่ได้รับกลับมานั้นคุ้มค่ากับการให้โอกาสผู้กระทำความผิดเหล่านี้หรือไม่ (อีทีดีเอ, 2561)

5.7.2 หน่วยงานด้านการปราบปราม

1) ทิศทางและเป้าหมายของนโยบาย

หน่วยงานด้านการปราบปรามมีความเกี่ยวข้องกับความมั่นคงปลอดภัยด้านทางทหารและกลยุทธ์ยุทธวิธีต่าง ๆ ทางการรบ ทุกหน่วยงานมีกองปราบปรามทางด้านไซเบอร์เป็นของตนเองและมีแนวทางที่จะเพิ่มกำลังพลอย่างสูงสุดเพื่อให้เพียงพอกับการรักษาความปลอดภัยตลอด 24 ชั่วโมง (อีทีดีเอ, 2561) จากการวิเคราะห์การเปิดรับทรัพยากรบุคคลทางด้านไซเบอร์ควรมีแนวทางระบุศักยภาพของผู้สมัครที่มีความสามารถทางด้านไซเบอร์ที่มากกว่านี้และเพิ่มทักษะบางอย่าง เช่น ภาษาอังกฤษในระดับที่สามารถสื่อสารได้เพื่อเข้าประชุมแลกเปลี่ยนกับนานาชาติ การเพิ่มเงินเดือนให้สูงขึ้นเพื่อดึงดูดผู้ที่มีความสามารถให้อยู่กับองค์ต่อไป ในส่วนของทิศทางหน่วยงานด้านการปราบปรามควรมีทิศทางมาเน้นในด้านการป้องกันและรับมือเป็นหลักโดยเฉพาะปกป้องด้านสาธารณูปโภคที่สำคัญและปล่อยให้งานด้านการรักษาความปลอดภัยด้านสารสนเทศเป็นหน้าที่ของหน่วยงานด้านการกำกับดูแลความมั่นคง

2) ทางเลือกในการนำไปปฏิบัติ

ปรับนโยบายด้ายกลยุทธ์และยุทธศาสตร์ด้านกำลังพลโดนเพิ่มกำลังพลที่มีความสามารถอย่างน้อยในศูนย์บัญชาการต้องมีอยู่ไม่ต่ำกว่า 50 อัตรา และกระจายความรู้ไปยังส่วนภูมิภาคโดยการอบรมและแลกเปลี่ยนข้อมูลเพื่อให้ส่วนภูมิภาคมีความรู้เท่ากับส่วนกลาง (ดีเฟนส์, 2560) กลยุทธ์ที่ใช้ควรเป็นในรูปแบบของการป้องกัน สร้างแสงยานุภาพทางด้านไซเบอร์ให้มีความสามารถดังเช่นเดียวกับแสงยานุภาพทางด้านการทหารแบบดั้งเดิม และประสานความร่วมมือกับสี่เหล่าทัพทางด้านไซเบอร์เพื่อแลกเปลี่ยนข้อมูลให้ทันท่วงทีและควรมีการแลกเปลี่ยนข้อมูลกับทางภาคพลเรือนและภาคเอกชน

3) ผลกระทบของนโยบาย

ผลกระทบที่จะเกิดขึ้นหากมีการปฏิบัติตามนโยบายข้างต้น การรับมือทางด้านภัยคุกคามความมั่นคงทางด้านการทหารจะมีความพร้อม ผู้จูโจมทางไซเบอร์ไม่ว่าจะเป็นในแบบรัฐชาติ ประเทศที่สามหรือตัวแสดงที่ไม่ใช่รัฐชาติจะมีความยั้งคิดในการจูโจมประเทศไทยเพราะกลัวในแสงยานุภาพทางไซเบอร์ กฎหมายที่ครอบคลุม และความสามารถของบุคคลกรทางด้านการปราบปราม ภาคพลเรือน ภาคเอกชน และภาคประชาชนจะเกิดความเชื่อมั่นในส่วนของรัฐบาลว่ามีหน่วยงานปราบปรามที่เข้มแข็ง (ดีเฟนส์, 2560)

4) มาตรฐานหรือบรรทัดฐาน

มาตรฐานที่ต้องใช้จะต้องใช้มาตรฐานเดียวกันรวมทั้งสี่เหล่าทัพและหน่วยงานที่มีส่วนในการปราบปราม การจั้งมาตรฐานจำนวนกำลังพลทางไซเบอร์ต่อหน่วยความมั่นคงจะต้องมีผู้ที่มีความเชี่ยวชาญอย่างน้อยไม่ต่ำกว่า 50 คน หรือจะตั้งมาตรฐานในการสกัดภัยคุกคามทางไซเบอร์ในหนึ่งเดือนจะต้องสามารถทำได้หรือสกัดได้ไม่ต่ำกว่าร้อยละ 80 ต่อจำนวนครั้งทั้งหมด จะต้องมีการประชุมร่วมกันทางด้านไซเบอร์จากทุกภาคส่วนไม่ต่ำกว่าปีละ 1 ครั้ง และเก็บสถิติในเรื่องของการใช้กลยุทธ์ในการสกัดกั้น การปกป้องและปราบปรามในแต่ละครั้งว่าวิธีใดเป็นวิธีที่ได้ประสิทธิภาพมากที่สุด (อีทีดีเอ, 2561)

5) การประเมินผลนโยบาย

การประเมินผลผลต้องใช้รูปแบบการประเมินเดียวกันโดยกองเทคโนโลยีไซเบอร์จากแต่ละเหล่าทัพหรือหน่วยปราบปรามจะต้องนำไปปฏิบัติและประเมินจากมาตรฐานข้างต้นว่าสามารถทำได้จริงหรือไม่ และสามารถลดจำนวนครั้งการโจมตีได้เท่าไหร่ต่อปี ระดับความรุนแรงที่เกิดขึ้นเป็นเช่นไร น้อยลงหรือไม่โดยใช้มาตรฐานความสูญเสียในด้านจำนวนเงิน ความสูญทางทรัพยากร บุคคลกร และประชาชน เป็นตัววัด นอกจากนี้ควรมีการวัดความเชื่อมั่นของประชาชน และภาคพลเรือนรวมไปถึงเอกชนว่ามีความคิดเห็นอย่างไร มีระดับความเชื่อมั่นต่อองค์กรและประเทศในระดับใดจึงจะประสบความสำเร็จในนโยบาย (อีทีดีเอ, 2561)

5.7.3 หน่วยงานที่มีความเสี่ยงด้านการโจมตี

1) ทิศทางและเป้าหมายของนโยบาย

เนื่องจากหน่วยงานที่มีความเสี่ยงด้านการโจมตีมีความหลากหลายทางด้านภารกิจ ไม่ว่าจะเป็นหน่วยงานทางด้านสาธารณสุข ซึ่งมีหน้าที่หนักดูแลผู้ป่วย (โอภาส การย์กวินพงศ์, 2560) หน่วยงานด้านการไฟฟ้ามีหน้าที่นำจ่ายไฟฟ้าให้แต่ละครัวเรือและอุตสาหกรรม ธนาคารมีหน้าที่หลักในการลงทุนและดูแลลูกค้าเพื่อให้ได้ผลตอบแทนสูงสุด ตัวอย่างข้างต้นที่กล่าวมานี้ไม่ได้หน้าที่ที่เกี่ยวข้องกับไซเบอร์โดยตรงแต่ไซเบอร์กลับเป็นส่วนสำคัญที่พร้อมจะเป็นเครื่องมือที่ช่วยเหลือและทำลายหน่วยงานนั้น ๆ ได้อย่างไม่คาดคิด ดังนั้นทิศทางของหน่วยงานที่มีความเสี่ยงด้านการโจมตีจะต้องปฏิบัติตามหน่วยงานด้านการกำกับดูแลความมั่นคงตามแนวทางที่มีมาให้และให้ความสำคัญกับกองงานด้านเทคโนโลยีไซเบอร์รวมถึงการเพิ่มความตระหนักรู้ในส่วนบุคลากรเจ้าหน้าที่ให้มากขึ้น

2) ทางเลือกในการนำไปปฏิบัติ

หน่วยงานด้านการกำกับดูแลความมั่นคงต้องประสานการทำงานและร่วมมือกันวางระบบในองค์กรของหน่วยงานที่มีความเสี่ยงด้านการโจมตี โดยจะต้องเป็นไปตามมาตรฐานเดียวกัน การเตรียมพร้อมรับมือภัยคุกคามทางไซเบอร์ การเตรียมพร้อมฟื้นฟูระบบให้สามารถกลับมาใช้งานภายใน 24 ชั่วโมง เพื่อไม่ให้เกิดความเสียหายต่อประชาชาน นอกจากนี้หน่วยงานที่มีความเสี่ยงด้านการโจมตีจะต้องมีแผนในการอบรมบุคคลกรทุกฝ่ายให้เข้าใจนโยบายทางด้านไซเบอร์และสามารถเตรียมพร้อมต่อการจู่โจมได้ทุกเมื่อและทุกระดับ โดยการทำแผนรับมือภัยพิบัติทางไซเบอร์ส่งตาอไปยังหน่วยงานด้านการกำกับดูแลความมั่นคงให้ได้ประเมินถึงความพร้อม และจะต้องมีการมอบหมายบุคลากรของหน่วยตนให้เข้าร่วมกับกลุ่ม ThaiCERT เพื่อให้มีความรู้เบื้อต้นในการสกัดจับภัยคุกคามทางด้านไซเบอร์ (โอภาส การย์กวินพงศ์, 2560)

3) ผลกระทบของนโยบาย

ผลกระทบที่จะเกิดขึ้นหากมีการปฏิบัติตามนโยบายข้างต้น จะทำให้หน่วยงานที่มีความเสี่ยง ด้านการโจมตีมีความรู้เบื้องต้นและมีระบบพร้อมรับมือในการโจมตี บุคคลกรทั้งหมดที่ทำงานในหน่วยงานจะต้องมีความตระหนักรู้เรื่องภัยคุกคามทางไซเบอร์เบื้องต้นและสามารถรักษาความมั่นคงปลอดภัยของหน่วยงานของต้นได้ เมื่อหน่วยงานเหล่านี้มีความมั่นคงปลอดภัยทางไซเบอร์ได้ด้วยตนเองก็จะทำให้ประชาชนที่มาใช้บริการมีความมั่นใจในระบบขององค์กรนั้น ๆ (อริย์ธัช แก้วเกาะสะบ้า, 2558)

4) มาตรฐานหรือบรรทัดฐาน

มาตรฐานนี้ต้องใช้ระดับการวัดเดียวกันแต่อาจจะต้องปรับเปลี่ยนขึ้นอยู่กับหน่วยงานที่มีความเสี่ยง (Tams, 2009) เช่น ธนาคารสาขาต่าง ๆ จะต้องใช้มาตรฐานที่กำหนดจาก

ธนาคารแห่งประเทศไทย การไฟฟ้าส่วนผลิตจะต้องมีมาตรฐานเดียวกับการไฟฟ้าทั้งหมดทั่วประเทศ เพื่อการประสานและแลกเปลี่ยนข้อมูลกันโดยสะดวก กรมราชทัณฑ์ที่จะต้องมีมาตรการการดูแลผู้ต้องขังและระบบการคำนวณรายชื่อผู้ต้องขังและจำนวนปีที่มีการลงโทษก็จะต้องมีระบบที่ขึ้นกับ สกมช. เพื่อให้มีมาตรฐานตามที่ควารจะเป็น กระทรวงสาธารณสุขและโรงพยาบาลต่าง ๆ ก็เช่นกัน จะต้องปฏิบัติกองเทคโนโลยีของกระทรวงเพื่อให้โรงพยาบาลแม่ข่ายต่าง ๆ มีแนวทางในการป้องกันตนเองเบื้องต้นในการรับมือ

5) การประเมินผลนโยบาย

ผลประเมินของแต่ละหน่วยงานสามารถประเมินผ่าน สกมช. เพื่อเป็นพื้นฐานในการประเมินของหน่วยงานต่าง ๆ เป็นหลัก เช่น การเก็บสถิติภัยคุกคามที่เกิดขึ้นว่าส่วนมากเป็นรูปแบบใดและใช้เครื่องมือใดที่มีประสิทธิภาพที่สุดในการรับมือ (อริย์ธัช แก้วเกาะสะบ้า, 2558) ประเมินบุคคลกรและเจ้าหน้าที่ของหน่วยงานนั้น ๆ ว่ามีความตระหนักรู้ในเรื่องของความปลอดภัยไซเบอร์ในระดับใดเพื่อให้หน่วยงานนั้นมีความปลอดภัยจากการตกเป็นเหยื่อ นอกจากนี้ควรมีการสืบเสาะถึงจุดประสงค์ของการกระทำแต่ละครั้งหรือการจู่โจมแต่ละครั้งว่ามีความเกี่ยวข้องกับการเมืองหรือไม่ เป็นการก่อการร้ายไซเบอร์หรือไม่เพื่อเอาข้อมูลส่วนนี้มาวิเคราะห์ในอนาคตต่อไป

5.8 ข้อเสนอแนะเชิงวิชาการ

ในการศึกษาการก่อการร้ายไซเบอร์เป็นเรื่องใหม่และยังไม่เกิดขึ้นจริงในประเทศไทย จึงมีความยากในการค้นคว้าหาข้อมูลทางด้านวรรณกรรม และในการสัมภาษณ์ หรือเข้าร่วมสัมมานาหาข้อมูลเพิ่มเติม เพราะผู้ที่ตอบคำถามนั้นมีแนวคิดเรื่องการจู่โจมทางไซเบอร์มากกว่าการก่อการร้ายที่ยังเป็นรูปธรรม ทั้งสองอย่างนี้มีความใกล้เคียงกันแต่แตกต่างกันที่จุดประสงค์ของผู้กระทำและระดับความรุนแรง ดังนั้นหากมีการศึกษาเรื่องไซเบอร์ในครั้งต่อไป ควรจะต้องมีประเด็นดังนี้

1) ควรศึกษานิยามของการก่อการร้ายไซเบอร์โดยเฉพาะ เพราะหากมีนิยามที่ชัดเจนตั้งแต่ต้นจะทำให้การศึกษาปรากฏการณ์ที่ตามมานั้นมีความชัดเจนทั้งในเรื่องการร่างนโยบายและการแก้ปัญหา ทั้งนี้ต้องมีการสร้างมาตรฐานหรือประกอบคำนิยามใหม่ให้สามารถเป็นจุดเริ่มต้นของการศึกษาต่อไปได้

2) ควรศึกษากฎหมายระหว่างประเทศที่มีต่อการก่อการร้ายไซเบอร์ เพราะปัญหาที่ไม่สามารถแก้ไขได้ในปัจจุบันนี้คือการบังคับใช้กฎหมายระหว่างประเทศเพราะความเป็นไซเบอร์นั้นไม่มีขอบเขตที่จำกัด (Kerschischnig, 2013) หากผู้กระทำมีฐานที่ตั้งอยู่ที่ประเทศหนึ่งแต่ผลของการกระทำเกิดขึ้นในอีกประเทศหนึ่งการบังคับใช้กฎหมายจึงเป็นเรื่องที่ท้าทายและไม่สามารถเอาผิดกับ

การกระทำได้หากอีกรัฐหนึ่งไม่ให้ความร่วมมือ เพราะฉะนั้นการศึกษาการก่อการร้ายไซเบอร์ในเชิงของกฎหมายระหว่างประเทศจึงเป็นสิ่งสำคัญที่จะนำไปพัฒนาต่อ

3) ควรศึกษากฎหมายของประเทศไทยที่มีต่อการก่อการร้ายไซเบอร์อย่างละเอียด เพราะหากมีการก่อการร้ายไซเบอร์ขึ้นจริง ผู้ที่สมควรได้รับการลงโทษนั้นควรมีระดับการลงโทษที่แตกต่างกันขึ้นอยู่กับเครื่องมือ จุดประสงค์ และความรุนแรงที่เกิดขึ้น การจำคุกหรือการปรับเงินอาจไม่ใช่การแก้ไขปัญหาที่ถูกต้อง แต่ควรมีการหารือกับกระทรวงยุติธรรมหรือกรมราชทัณฑ์เพื่อให้มีแนวทางการแก้ปัญหาที่ถูกต้อง

4) ควรศึกษาจิตวิทยาที่มีต่อการก่อการร้ายไซเบอร์ เพราะการก่อการร้ายมีความเชื่อมโยงกับจิตวิทยาในเชิงศาสตร์ เช่นเดียวกับการก่อการร้ายไซเบอร์ที่แฮกเกอร์หรือผู้กระทำใช้ทฤษฎีเดียวกันในการสังเกตพฤติกรรมของเหยื่อและเลือกเหยื่อที่มีโอกาสเข้าถึงมาที่สุดเพื่อใช้เหยื่อนั้นทำลายองค์กรที่ต้องการ (Tams, 2009) หากใช้จิตวิทยาในการเข้าถึงแฮกเกอร์ได้จะสามารถที่จะทำนายพฤติกรรมต่อไปหรือเข้าถึงองค์ที่เป็นต้นตอของการก่อการร้ายไซเบอร์

5) ควรศึกษายุทธศาสตร์ที่มีต่อการก่อการร้ายไซเบอร์ เพราะการก่อการร้ายไม่ว่าจะเป็นในพื้นที่ใดก็ตามจะมีความเชื่อมโยงกับยุทธศาสตร์และกลยุทธ์ทางทหารที่จะต้องศึกษาอย่างจริงจัง เพราะยุทธศาสตร์และกลยุทธ์เหล่านี้จะสามารถบอกได้ถึงวิธีการรับมือในอนาคตต่อไป กลยุทธ์ในการใช้ไซเบอร์ได้ถูกนำเสนอไว้แล้วในงานวิจัยชิ้นนี้แต่เป็นเพียงการนำกลยุทธ์การก่อการร้ายทางกายภาพทั้งในอดีตและปัจจุบันมาประยุกต์ใช้กับกลยุทธ์ทางไซเบอร์เท่านั้น หากมีการศึกษาที่ลึกไปกว่านี้จะเป็นประโยชน์ในการรับมือทางด้านเทคนิคได้ (Weimann, 2005)

6) ควรศึกษาแหล่งงบประมาณของกลุ่มก่อการร้ายไซเบอร์ การก่อการร้ายไซเบอร์จำเป็นจะต้องมีผู้อยู่เบื้องหลังและในอนาคตนั้นไซเบอร์จะเป็นพื้นที่ในการหาช่องทางทางการเงินของผู้ก่อการร้ายในระดับนานาชาติได้ง่ายและประเทศต่างจะไม่สามารถนำกฎหมายที่มีอยู่มาใช้ในการจับกุมการก่อการร้ายทางไซเบอร์ได้เลยเพราะยังไม่มีหลักฐานใดที่เป็นผลทางกฎหมายและไม่มีกฎหมายระหว่างประเทศที่บังคับใช้ (Williams, 2007)

5.9 ข้อเสนอที่นำไปสู่การพัฒนาในอนาคตปรับใช้จากโมเดลต่างประเทศ

1) สร้างสภาพแวดล้อมที่ไม่เอื้ออำนวยต่อการกระทำความผิดทางไซเบอร์ ถอดรูปแบบการเรียนรู้จากประเทศอังกฤษ

ประเทศอังกฤษนั้นมีความตระหนักในเรื่องภัยไซเบอร์เป็นอย่างมาก มีการก่อตั้ง Internet Watch Foundation (IWF) การออกกฎบังคับเรื่องความปลอดภัยการใช้อินเทอร์เน็ตของเจ้าหน้าที่ที่มีส่วนเกี่ยวข้องกับข้อมูลของรัฐ ไม่ให้นำเครื่องคอมพิวเตอร์ของสำนักงานมาใช้ในพื้นที่ที่

นอกเหนือจากเขตของสำนักงาน และไม่อนุญาตให้เจ้าหน้าที่ทำงานกับเครื่องคอมพิวเตอร์ส่วนบุคคล เพราะจะทำให้ข้อมูลของรัฐรั่วไหล (LegislationGovUK, 2007) สิ่งที่ประเทศไทยสามารถทำได้คือ การสร้างสภาพแวดล้อมเหล่านี้โดยการออกกฎเป็นลายลักษณ์อักษร ถึงแม้ว่าจะมีบางหน่วยงานถูกกำชับไม่ให้นำเรื่องงานออกมาทำในสถานที่นอกเหนือสำนักงานโดยเฉพาะงานที่เป็นความลับจากหน่วยงานรัฐ แต่คำสั่งเหล่านั้นก็ยังเป็นเพียงแค่คำพูดไม่มีบทลงโทษที่ชัดเจน ดังนั้นประเด็นนี้ควรมี สกมช. เป็นหน่วยงานข้างต้นในการออกมาตรฐานแก่หน่วยงานต่าง ๆ ให้ปฏิบัติตามโดยจะต้องมีการแบ่งชั้นข้อมูลและขอบเขตงานที่ชัดเจนว่างานประเภทใดที่สามารถนำไปทำต่อนอกสถานที่ได้หรืองานประเภทใดไม่สามารถนำไปทำนอกสถานที่ได้ พร้อมกำหนดบทลงโทษให้เป็นลายลักษณ์อักษร พร้อมติดตั้งระบบตรวจสอบกับเครื่องคอมพิวเตอร์ของหน่วยงานรัฐเพื่อจับสัญญาณการทำงานนอกสถานที่

การสร้างสภาพแวดล้อมที่ไม่เอื้ออำนวยต่อการคุกคามทางไซเบอร์นั้นยังมีอีกหลายรูปแบบ แต่โดยส่วนมากรัฐบาลไทยได้เริ่มต้นในการบังคับใช้บ้างแล้วไม่ว่าจะเป็นในส่วนของกฎหมายไซเบอร์ การให้ความรู้แก่ประชาชนเรื่องการเข้าถึงข้อมูลทางอินเทอร์เน็ต การสร้างหน่วย Thaicert เพื่อรับมือภัยคุกคามได้ทันเวลา หรือติดต่อโทรศัพท์กับสำนักงานที่เกี่ยวข้องเพื่อให้ช่วยแก้ไขปัญหาการจู่โจมทางไซเบอร์ได้ทันท่วงที (Pradillo, 2011) สิ่งที่ประเทศไทยจำเป็นจะติ้งส่งเสริมมากขึ้นคือการให้ความรู้แก่ผู้บังคับใช้กฎหมายเพื่อให้กฎหมายที่สร้สงขึ้นมานั้นมีประสิทธิภาพ

2) สร้างช่องทางทางอินเทอร์เน็ตใหม่ โดยที่รัฐสามารถควบคุมช่องทางได้ทั้งหมด ถอดรูปแบบการเรียนรู้จากประเทศจีนและประเทศรัสเซีย

นโยบายนี้มีทั้งข้อดีและข้อเสียโดยข้อเสียนั้นหาก Gateway ล่มก็จะล่มกันหมดทั้งประเทศ เพราะจะไม่มี Gateway ตัวอื่นรองรับ - ผู้ใช้อินเทอร์เน็ตทั่วไปถูกจำกัดการใช้เครือข่ายกับต่างประเทศมากขึ้น และต้องระวังการเข้าถึงเนื้อหาที่ไม่เหมาะสมโดยไม่รู้ตัวเช่นกัน เช่น การถูกรัฐบาลบล็อก แบน แสกน การใช้งานอินเทอร์เน็ต เป็นการรุกล้ำความเป็นส่วนตัวของประชาชน แต่ในแง่ดีนั้นรัฐบาลจะสามารถควบคุมระบบได้ทั้งหมดและสามารถสอดได้อย่างมีประสิทธิภาพและสกัดกั้นไวรัสที่เป็นภัยได้อย่างทันเวลา ตัวอย่างเช่นประเทศรัสเซียที่มีช่องทางอินเทอร์เน็ตช่องทางเดียวควบคุมโดยรัฐ สามารถสกัดกั้นผู้ก่อกวนทางไซเบอร์ได้โดยง่ายเพราะลดความไร้ตัวตน (anonymity) ในโลกอินเทอร์เน็ต (Sukharenko, 2019) ถึงแม้ผู้ก่อกวนจะพยายามใช้เครื่องคอมพิวเตอร์ ณ ที่ใดหากสัญญาณนั้นผ่านช่องทางในประเทศรัสเซียรัฐบาลรัสเซียก็สามารถตรวจจับได้หมด เช่นเดียวกับรัฐบาลจีน ที่ไม่อนุญาตให้ช่องทางอินเทอร์เน็ตจากภายนอกเข้ามาใช้งานภายในประเทศได้เลย และคนในชาติเองก็ยังนิยมช่องทางอินเทอร์เน็ตที่รัฐบาลของตนเองได้ผลิตขึ้นมาเพราะฉะนั้นการจะโจมตีประเทศจีนทางไซเบอร์จึงไม่ใช่เรื่องง่าย ประเทศไทยหากต้องการทำรูปแบบเดียวกันนั้นจะต้องมั่นใจระบบของตนจะต้องมีความแข็งและมีประสิทธิภาพในการใช้งานมากเพียงพอติ่จำนวนประชากรเพื่อ

ไม่มีการล่มของสัญญาณได้ง่าย และนอกจากนี้ยังต่อทำความเข้าใจกับประชาชนในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์กับความเป็นส่วนตัวในโลกของอินเทอร์เน็ต (Skoudis & Zeltser, 2004)

3) เพิ่มหลักสูตรความมั่นคงไซเบอร์ในโรงเรียนและมหาวิทยาลัย ถอดรูปแบบการเรียนรู้จากประเทศญี่ปุ่น เกาหลีใต้ และจีน

จากการศึกษาเห็นได้ชัดว่ารัฐบาลประเทศญี่ปุ่นให้ความสนใจทางไซเบอร์เป็นอย่างมาก และมีทัศนวิสัยที่จะเป็นผู้นำทางไซเบอร์ในระดับภูมิภาค รัฐบาลญี่ปุ่นต่อการส่งเสริมความร่วมมือระหว่าอาเซียนและญี่ปุ่นในด้านไซเบอร์จึงได้สนับสนุนทางการศึกษาโดยตั้งศูนย์ความร่วมมืออาเซียน-ญี่ปุ่น เพื่อพัฒนาบุคลากรความมั่นคงปลอดภัยไซเบอร์ในกรุงเทพ โครงการพัฒนาศักยภาพทางไซเบอร์ของอาเซียนโดยความร่วมมือจากองค์การตำรวจสากลรัฐบาลญี่ปุ่นพยายามส่งสารว่าอินเทอร์เน็ต รวมถึงธุรกิจและธุรกรรมทางไซเบอร์ทั้งหมดเป็นโดเมนประเภทที่ใช้ร่วมกันทั่วโลก ญี่ปุ่นมีนโยบายอาชญากรรมทางไซเบอร์เป็นบทเรียนที่ได้เรียนรู้เพื่อต่อสู้อาชญากรรมทางไซเบอร์ การพัฒนาบุคลากร และมีแผนจะได้รับทุนจากกองทุนความร่วมมือญี่ปุ่น-อาเซียน ส่วนรัฐบาลจีนนั้นจีนมีการเตรียมเปิดตัวสถาบันการศึกษาด้านความปลอดภัยไซเบอร์ระดับโลก 6 สถาบัน ภายในอีก 5 ปี ประกอบไปด้วยอาจารย์และบุคลากรที่มีชื่อเสียง มีความสามารถเป็นที่ยอมรับในด้าน Cyber Security รวมไปถึงนักศึกษาที่เข้าเรียนที่นี่ต้องเป็นกลุ่มหัวกะทิ ซึ่งพวกเขาจะได้รับการศึกษาภายใต้การเรียนการสอนและอุปกรณ์การเรียนที่มีคุณภาพสูง (BBC NEWS, 2020) เช่นเดียวกันกับประเทศเกาหลีที่มีหลักสูตรประยุกต์ไซเบอร์ในการใช้ชีวิตประจำวันเพื่อสอนให้นักเรียนในทุกระดับชั้นเข้าใจในเบื้องต้น

ประเทศไทยควรต่อยอดหลักสูตรต่าง ๆ เหล่านี้โดยเน้นในการเริ่มต้นของสถาบันอุดมศึกษากำหนดให้มีหลักสูตรโดยเฉพาะและสร้างแรงจูงใจในการมอบทุนและมอบค่าใช้จ่ายให้ระหว่างเรียนเพื่อดึงดูดเด็กที่มีความสามารถ

4) สร้างเครือข่ายสำรองกับประเทศอื่น ๆ หรือกับภาคเอกชนอื่น ๆ เพื่อรองรับการโจมตี ถอดรูปแบบการเรียนรู้จากประเทศเอสโตเนีย

ประเทศเอสโตเนียเป็นประเทศที่ได้รับการยอมรับว่าตั้งอยู่ในสังคมออนไลน์อย่างเต็มรูปแบบ เพราะสาธารณูปโภคและระบบสำคัญ ๆ ต่าง ๆ ของประเทศ ไม่ว่าจะเป็น ระบบการศึกษา การสาธารณสุข หน่วยงานบริการของรัฐ การเงินธนาคาร ไปจนถึงการเลือกตั้ง ทุกอย่างตั้งอยู่บนอินเทอร์เน็ต ประชาชนจะใช้ชีวิตได้ง่ายขึ้นแต่ไม่อาจคาดคิดว่าเมื่อประเทศเอสโตเนียเกิดสงครามไซเบอร์จะทำให้ทุกระบบพื้นฐานของประเทศหยุดชะงักและไม่สามารถดำเนินกิจการการต่อไปได้เป็นเวลา 3 วัน และสิ่งที่สามารถช่วยให้รัฐบาลหาทางออกจากวิกฤตการณ์ครั้งนี้ได้คือการขอความช่วยเหลือจากบริษัทเครือข่ายอินเทอร์เน็ตเอกชนจากประเทศเพื่อนบ้านที่ทำให้ให้อินเทอร์เน็ตภายในประเทศได้รับการฟื้นฟู (Denning, 2020)

สิ่งที่ประเทศไทยได้เรียนรู้เป็นบทเรียนสำคัญในครั้งนี้คือการมีสัญญาณสำรองเพื่อช่วยในยามวิกฤต การผู้มิตรหรือการหา Partner กับเอกชนในประเทศต่าง ๆ ถือเป็นทางออกสำคัญ ทั้งนี้อาจทำได้ทั้งแบบที่เป็นทางการและไม่เป็นทางการ (Denning, 2020) โดยที่ประเทศไทยจะต้องมีวิธีที่จะแลกเปลี่ยนผลตอบแทนกับบริษัทเอกชนนั้นเพื่อจูงใจให้บริษัทเหล่านั้นเข้ามาช่วยเหลือในคราวยาก ลำบากโดยที่อีกฝ่ายก็ได้รับผลตอบแทนที่พึงพอใจ

บรรณานุกรม

กรมพัฒนาสังคมและสวัสดิการ. (2563). รูปแบบภัยคุกคามด้านไซเบอร์. สืบค้นจาก http://www.dsdw2016.dsdw.go.th/doc_pr/ndc_2560-2561/PDF/8498st/5.บทที่%203.pdf

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (2561). แผนปฏิบัติราชการ 4 ปี พ.ศ. 2562 - 2565 กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. สืบค้นจาก http://www.oic.go.th/FILEWEB/CABINFOCENTER3/DRAWER088/GENERAL/DATA0000/00000929.PDF

กฤษมันต์ วัฒนาณรงค์. (2553). ทฤษฎีการแก้ตัวกับการฉ้อฉลในการเรียน. สืบค้นจาก https://www.thairath.co.th/content/108668

กองยุทธศาสตร์และแผนงาน. (2561). เทคโนโลยีสารสนเทศ Digital Transformation. สืบค้นจาก http://164.115.25.41/expertcenter/wp-content/uploads/2018/conference/HPT3/Report/ G6.Paper-Digital-Transformation.pdf

การไฟฟ้าส่วนภูมิภาค. (2562). นโยบายการรักษาความมั่นคงปลอดภัยเว็บไซต์. สืบค้นจาก https://www.pea.co.th/นโยบายการรักษาความมั่นคงปลอดภัยเว็บไซต์

การออกพระราชบัญญัติความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562. (2562). *ราชกิจจานุเบกษา, 136*(69ก), 20-51.

เกรียงศักดิ์ เจริญวงศ์ศักดิ์. (2539). *เรียนรู้ วิถีสู่ความสำเร็จ* (พิมพ์ครั้งที่ 3). กรุงเทพฯ: ซัคเซสมีเดีย.

คณาธิป ทองรวีวงศ์. (2563). *กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ฯ*. กรุงเทพฯ: วิญญูชน.

คลาร์ก, ริชาร์ด เอ. (2563). *สงครามไซเบอร์ Cyber War*. กรุงเทพฯ: มติชน.

จารุวัฒน์ เศวตพัชราภรณ์ และวรภพ ตันติวาณิชชากร. (2560). การเตรียมความพร้อมก้าวสู่ยุคประเทศไทย 4.0. สืบค้นจาก https://www.thaiprint.org/2017/03/industrial-spending/vol113-industrial02/

ณัฐโชติ ดุสิตานนท์ และเสฏฐวุฒิ แสนนาม. (2563). Botnet of Things - ภัยคุกคามจาก Internet of Things และแนวทางการรับมือ. สืบค้นจาก https://www.thaicert.or.th/papers/general/2016/pa2016ge001.html

ทีเอ็นเอ็น. (2563). โรงพยาบาลสระบุรี ถูกไวรัสโจมตี เรียกค่าไถ่ 6.3 หมื่นล้านรับมือ. สืบค้นจาก https://www.tnnthailand.com/content/54304

ทีมมายด์อินไซต์. (2564). [Extreme History] Stuxnet Worm ไวรัสตัวแรกที่ถูกใช้เป็นอาวุธไซเบอร์ (แต่ช่วยหยุดสงครามโลกไว้ได้). สืบค้นจาก https://www.extremeit.com/extreme-history-stuxnet/

ธนาคารแห่งประเทศไทย. (2562). รอบการประเมินความพร้อมด้าน Cyber Resilience. สืบค้นจาก https://www.bot.or.th/Thai/FIPCS/Documents/FOG/2562/ThaiPDF/25620189.pdf

ธนาคารแห่งประเทศไทย. (2564). ความร่วมมือกับผู้กำกับดูแลอื่น. สืบค้นจาก https://www.bot.or.th/Thai/FinancialInstitutions/Sup_Co/Pages/default.aspx

ธาราทิพย์ กัลยาณมิตร. (2560). แนวทางการพัฒนากองทัพไทยด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์. สืบค้นจาก http://www.sscthailand.org/uploads_ssc/research_2018022615196280766225 17.pdf

ปรัชญา ฮวดปากน้ำ. (2559). ยุทธศาสตร์การพัฒนากำลังพลของกองทัพไทยเพื่อต่อต้านภัยคุกคามไซเบอร์ในทศวรรษหน้า. สืบค้นจาก http://jsc.rtarf.mi.th/research/sum_research/JSC_57/JSC5731.pdf

พิพัทธ์ เพิ่มพันธุ์. (2561). ศูนย์ไซเบอร์อังกฤษ หยุดยั้งการโจมตีทางไซเบอร์กว่า 1200 ครั้งในปีที่ผ่านมา. สืบค้นจาก https://www.theeleader.com/news-enterprise/ศูนย์ไซเบอร์อังกฤษ-nscs-stoped-phishing-attack/

ภัสยกร เลาสวัสดิกุล. (2557). *กลยุทธ์การบริหารสถาบันอุดมศึกษาเพื่อสร้างความเป็นพลเมืองของนิสิตนักศึกษา* (วิทยานิพนธ์ปริญญามหาบัณฑิต ไม่ได้ตีพิมพ์), จุฬาลงกรณ์มหาวิทยาลัย, กรุงเทพฯ.

มหิตถีห์ จักราบาตร. (2560). National Cybersecurity Strategy ยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. สืบค้นจาก https://www.nbtc.go.th/News/Information/National-Cybersecurity-Strategy-%E0%B8%A2%E0%B8%B8%E0%B8%97%E0%B8%98%E0%B8%.aspx.

วชิรศักธิ์ พูสิทธิ์. (2557). หลักการทำสงครามในศตวรรษที่ 21: การพิจารณาทางยุทธศาสตร์. สืบค้นจาก https://www.slideshare.net/washirasakpoosit/ss-30944385

วรรณ นิศาสุขสวัสดิ์. (2562). ปัญหากฎหมายเกี่ยวกับการคุ้มครองสิทธิผู้เสียหายในคดีอาญา ตามพระราชัญญัติค่าตอบแทนผู้เสียหายและค่าทดแทนและค่าใช้จ่ายแก่จำเลยในคดีอาญา พ.ศ. 2544 (แก้ไขเพิ่มเติม) (ฉบับที่ 2) พ.ศ. 2559. สืบค้นจาก http://dspace.spu.ac.th/bitstream/123456789/6429/7/7.บทที่%202%20%2B.pdf

วรรณฉัตรตร พวยพุ้ง. (2555). แนวคิดในการลงโทษเด็กและเยาวชน. สืบค้นจาก http://dspace.spu.ac.th/bitstream/123456789/3607/6/6chap2.pdf

วรรณวิภา เมืองถ้า. (2551). แนวคิดหลักทฤษฎี นิยามกฎหมายอาชญากรรมข้ามชาติ ชุดวิชา 41719 กฎหมายกระบวนการยุติธรรมเกี่ยวกับการควบคุม และปราบปรามอาชญากรรมในประเทศและข้ามชาติที่สำคัญ. สืบค้นจาก https://www.stou.ac.th/schoolsweb/law/UploadedFile/หน่วยที่%201.pdf

วันชัย เจยีรวัฒนาวิทย์. (2562). MEA-ICT roadmap going to MEA digital. สืบค้นจาก http://www.soe-d.com/images/downloads/SOED62_2.pdf

ศิริรัตน์ ศรีสว่าง. (2558). ปัจจัยที่ส่งผลต่อพฤติกรรมการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์. สืบค้นจาก http://ethesisarchive.library.tu.ac.th/thesis/2015/TU_2015_5302037337_3439_1883.pdf

สงคราม ดอนนางพา และธนบดี ตันหยง. (2556). การพัฒนากำลังพลของกองทัพบกเพื่อรองรับสงครามไซเบอร์. สืบค้นจากhttp://jsc.rtarf.mi.th/research/sum_research/JSC_54/JSC54_47.pdf

สถาบันวิจัยรพีพัฒนศักดิ์. (2553). สถาบันวิจัยรพีพัฒนศักดิ์การปฏิรูปกระบวนการยุติธรรมเพื่อสังคม. กรุงเทพฯ: ผู้แต่ง.

สาวตรี สุขศรี. (2563). *กฎหมายว่าด้วยอาชญากรรมคอมพิวเตอร์และอาชญากรรมไซเบอร์.* กรุงเทพฯ: คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์.

สำนักงานคณะกรรมการกิจการกระจายเสีย กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ. (2562). แผนยุทธศาสตร์ สำนักงาน กสทช. ฉบับ 2 (พ.ศ. 2561-2564). สืบค้นจาก https://www.nbtc.go.th/About/แผนปฏิบัติการ-สำนักงาน-กสทช-ประจำปี/37715.aspx

สำนักงานปลัดกระทรวงยุติธรรม. (2560). แผนปฏิบัติการดิจิทัลสำนักงานปลัดกระทรวงยุติธรรม พ.ศ. 2560 -2564. สืบค้นจาก http://www.oic.go.th/FILEWEB/CABINFOCENTER3/DRAWER088/GENERAL/DATA0000/00000929.PDF

สำนักงานปลัดกระทรวงสาธารณสุข, ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร. (2560). ยุทธศาสตร์เทคโนโลยีสารสนเทศสุขภาพ กระทรวงสาธารณสุข (2560 – 2569). สืบค้นจาก https://ict.moph.go.th/upload_file/files/eHealth_Strategy_THAI.pdf

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน). (2561). รายงานผลการดำเนินงานปีงบประมาณ พ.ศ. 2561 (รอบ 6 เดือนหลัง). สืบค้นจาก https://www.etda.or.th/content_files/19/files/O12-2561-6.v02.pdf

สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน). (2562). ความมั่นคงปลอดภัยทางไซเบอร์. สืบค้นจาก https://dga.or.th/upload/download/file_769c60982e4c374dcd33b41c29227a31.pdf

สำนักงานสภาความมั่นคงแห่งชาติ. (2560). ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560-2564. สืบค้นจาก http://www.nsc.go.th/wp-content/uploads/2018/08/strategyit60-64-1.pdf

สุรชาติ บำรุงสุข, ฉัตรพงษ์ ฉัตราคม, สัญญา ทองบุศย์, กุลนันทน์ คันธิก และศิบดี นพประเสริฐ. (2563). *ความรุนแรงร่วมสมัยในสังคมไทย:การก่อการร้ายในเมือง* (รายงานการวิจัย). กรุงเทพฯ: สำนักงานวิจัยแห่งชาติ.

สุรภี พิมพ์ละออ. (2562). กฎหมายเทคโนโลยีสารสนเทศของประเทศไทย. สืบค้นจาก https://sites.google.com/site/surapee389/kt-hmay-thekhnoloyi-sarsnthes-khxng-prathesthiy

สุรศักดิ์ ชะมารัมย์. (2563). แนวความคิด ตัวแบบ และทฤษฎีนโยบายสาธารณะ. สืบค้นจาก https://reru.ac.th/articles/images/vijai_19_09_59.pdf

เสาวลักษณ์ ศรีสุวรรณ. (2564). บรรณาธิการข่าวออนไลน์กับกฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ในประเทศไทย. *วารสารนิเทศศาสตร์ปริทัศน์, 24*(3), 238-248.

หยาดพิรุณ นาชัยสินธุ์. (2560). ยุทธศาสตร์การต่อต้านการก่อการร้ายทางไซเบอร์ในประเทศไทย. สืบค้นจาก https://webcache.googleusercontent.com/search?q=cache:vYbKEtgLhF8J

อริย์ธัช แก้วเกาะสะบ้า. (2558). คณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. สืบค้นจาก https://cdc.parliament.go.th/ewtadmin/ewt/parliament_parcy/ewt_w3c/ewt_dl_link.php?nid=50944

อัณณพ ชูบำรุง. (2532). *อาชญาวิทยาและอาชญากรรม.* กรุงเทพฯ: ภาควิชารัฐศาสตร์และรัฐประศาสนศาสตร์ คณะสังคมศาสตร์ มหาวิทยาลัยเกษตรศาสตร์.

อินโดแปซิฟิก ดีเฟนส์. (2560). สิงคโปร์เพิ่มการป้องกันทางไซเบอร์หลังการรั่วไหลของข้อมูล. สืบค้นจาก https://ipdefenseforum.com/th/สิงคโปร์เพิ่มการป้องกัน/

อีทีดีเอ. (2561). บทบาทหน้าที่ของกรรมการบริษัทในการกำกับดูแลเทคโนโลยีสารสนเทศตามกฎหมาย IT. สืบค้นจาก https://www.csmonitor.com/2001/0927/p16s2wogi.html.https://www.oic.or.th/sites/default/files/file_download/bthbaathhnaathiiainkaarkamkabduuaelethkhonolyiitaamkdhmaay_it_cchaak_dr.chaychna_etda_bryaayphaakhbaay.pdf

โอภาส การย์กวินพงศ์. (2560). ประเด็น Retreat สป.สธ. ข้อมูลและเทคโนโลยีสารสนเทศ. สืบค้นจาก http://203.157.155.38/plan2020/retreat0818/3ict.pdf

BBC NEWS. (2020). Coronavirus: US accuses China of hacking coronavirus research. Retrieved from https://www.bbc.com/news/world-us-canada-52656656

Berner, S. (2003). Cyber-terrorism: reality or paranoia? *SA Journal of Information Management, 5*(1).

Cabinet Office. (2020). The UK cyber security strategy protecting and promoting the UK in a digital world. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

Campbell, K. (2010). When is terrorist a subjective term? Retrieved from http://www.csmonitor.com

Carr, J. (2012). The myth of the CIA and the Trans-Siberian Pipeline Explosion Retrieved from http://jeffreycarr.blogspot.co.uk/2012/06/myth-of-cia-and-trans-siberian-pipeline.html

Cassese, A. (1989). The International Community's “Legal” Response to Terrorism. *International Comparative Law Quarterly, 38*(3), 589-608.

Chainoglou, K. (2010). An Assessment of Jus in Bello Issues Concerning Computer Network Attacks: A Threat Reflected in National Security Agendas. *Romanian J. Int'l L., 11*, 45.

Cilluffo, F. J. (2017). Emerging cyber threat to the United States. Retrieved from https://docs.house.gov/meetings/HM/HM09/20171012/106467/HHRG-115-HM09-Bio-CilluffoF-20171012.pdf

CISA. (2009). Understanding denial-of-service attacks. Retrieved from https://us-cert.cisa.gov/ncas/tips/ST04-015

Condorelli, L., & Naqvi, Y. Q. (2004). The war against terrorism and jus in bello: are the Geneva Conventions out of date? *Enforcing International Law Norms Against Terrorism, 37*.

Congress.Gov. (2016). North Korea sanctions and policy enhancement act of 2016. Retrieved from https://www.congress.gov/bill/114th-congress/house-bill/757/text

Conway, M. (2003). Terrorism and IT: Cyberterrorism and terrorist organisations online. Retrieved from https://doras.dcu.ie/502/1/terrorism_it_2003.pdf

Cooley, C. H. (1894). "The theory of transportation" Sociological theory and social research: Being selected papers of charles horton cooley. Retrieved from http://spartan.ac.brocku.ca/~lward/Cooley/Cooley_1894.html

Crawford, N. C. (2003). Just war theory and the US counterterror war. *Perspectives on Politics, 1*(1), 5-25.

Croft, C. (2007). A brief history of the facebook. Retrieved from http://www.meerutcollege.org/mcm_admin/upload/1587223450.pdf

Cronk, G. (2006a). Free will. Retrieved from https://www.iep.utm.edu/freewill/

Cronk, G. (2006b). George Herbert Mead (1863-1931). Retrieved from https://www.iep.utm.edu/mead/

Cronk, G. (2006c). Rational choice theory. Retrieved from https://www.iep.utm.edu/Rationalchoicetheory/

CSA. (2016). Singapore's cybersecurity strategy. Retrieved from https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy

CSIS. (2020). Significant cyber incidents. Retrieved from https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents

Cyware Social. (2016). Remembering operation titan rain. Retrieved from https://cyware.com/news/remembering-operation-titan-rain-c54ad3e4

Dandecha, W. (2019). Man-in-the-middle. Retrieved from https://cdt.wu.ac.th/?p=6803&lang=th

Denning, D. (2001). This narrow definition considers cyberterrorism. Retrieved from https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberterrorism.html

Denning, D. (2020). Cyberterrorism: Testimony before the special oversight panel on terrorism committee on armed services U.S. House of representatives. Retrieved from http://bit.ly/2Er9ZLt

Doffman, Z. (2019). Iran has launched ‘malicious’ new malware that wipes windows computers, warns ibm. Retrieved from https://www.forbes.com/sites/zakdoffman/2019/12/04/iranian-hackers-launch-malicious-new-wiper-malware-ibm-warns-of-destructive-attacks/#41967baa7ec2

Draft of Crimes Against the Peace and Security of Mankind. (1996). *Rep. of the Intl' Law Comm'n, 48th Sess., May 6- July 26, 1996, UN*

Eom, J.-H., Kim, N.-U., Kim, S.-H., & Chung, T.-M. (2012). *Cyber military strategy for cyberspace superiority in cyber warfare.* Paper presented at the Proceedings title: 2012 international conference on cyber security, cyber warfare and digital forensic (cybersec).

Free Word Centre. (2012). Islamic Republic of Iran: Computer crimes law. Retrieved from https://www.article19.org/data/files/medialibrary/2921/12-01-30-FINAL-iran-WEB%5B4%5D.pdf

GCHO. (2016). Cyber security. Retrieved from https://www.gchq.gov.uk/section/mission/cyber-security

Gebauer, G., & Wulf, C. (1995). *Mimesis: culture, art, society*. California: University of California Press.

Gordon, S., & Ford, R. (2002). Cyberterrorism? *Computers Security and Communication Networks, 21*(7), 636-647.

Green, J. (2020). The Myth of cyberterrorism. *Washington Monthly, 11*, 11-18.

Greenberg, M. A. (1995). Cognitive Processing of Traumas: the role of intrusive thoughts and reappraisals 1. *Journal of Applied Social Psychology, 25*(14), 1262-1296. doi:10.1111/j.1559-1816.1995.tb02618.x

Gullone, E. (2000). The development of normal fear: A century of research. *Clinical Psychology Review, 20*(4), 429-451.

Gullone, E., & Moore, S. (2000). Adolescent risk-taking and the five-factor model of personality. *Journal of Adolescence, 23*(4), 393-407.

Handel, M. I. (1997). Who is afraid of Carl von Clausewitz. *A Guide to the Perplexed*.

Hollin, C. R. (2013). *Psychology and crime: An introduction to criminological psychology*. New York, NY: Routledge.

Hua, J., & Bapna, S. (2012). How can we deter cyber terrorism? *Information Security Journal: A Global Perspective, 21*(2), 102-114.

Husabø, E. J., & Bruce, I. (2009). *Fighting terrorism through multilevel criminal legislation: Security Council Resolution 1373, the EU framework decision on*

combating terrorism and their implementation in Nordic, Dutch and German criminal law: Brill.

Int'l Civil Aviation Org. [ICAO]. (2010). Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation. *ICAO Doc, 10*(9960).

Janet, J. P., & MacDonald, L. E. (2004). Cyber terrorism: A study of the extent of coverage in computer science textbooks Retrieved from https://www.learn techlib.org/p/111454

Jarvis, L., & Macdonald, S. (2015). What is cyberterrorism? Findings from a survey of researchers. *Terrorism Political Violence, 27*(4), 657-678.

Jones, A. (2005). Cyber terrorism: fact or fiction. *Computer Fraud Security, 2005* (6), 4-7.

Jun, J., LaFoy, S., & Sohn, E. (2015). North Korea's cyber operations strategy and responses. Retrieved from http://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf

Kabanda, G. (2018). A cybersecurity culture framework and its impact on zimbabwean organizations. Retrieved from https://www.researchgate.net/publication/335292223_A_Cybersecurity_CultureFramework_and_Its_Impact_on_Zimbabwean_Organizations/figures?lo=1

Karatzogianni, A. (2009). Cyber Conflict and Global Politics. Retrieved from https://www.researchgate.net/publication/259850763_Cyber_Conflict_and_Global_Politics

Katz, J. (1988). *Seductions of crime: Moral and sensual attractions in doing evil*. New York, NY: Basic Books.

Kenney, M. (2015). Cyber-terrorism in a post-stuxnet world. *Orbis, 59*(1), 111-128.

Kerschischnig, G. (2013). Cyberthreats and International Law Cyberthreats and international law. *Journal of International and European Law, 29*(76), 106.

Kushner, D. (2013). The real story of stuxnet. *IEEE Spectrum, 3*(50), 48-53.

Lee, J., & Macdonald, S. (2014). Locating cyberterrorism: How terrorism researchers use and view the cyber lexicon. Retrieved from https://preventviolen textremism.info/sites/default/files/Locating%20Cyberterrorism-%20How%20Researchers%20Use%20and%20View%20the%20Cyber%20Lexicon.pdf

LegislationGovUK. (2007). Computer misuse act 1990. Retrieved from https://www.legislation.gov.uk/ukpga/1990/18/section/3

Lichfield, J. (2009). How the cold war was won... by the French Retrieved from http://www.independent.co.uk/news/world/politics/how-the-cold-war-was-won-by-the-french-1788720.html

Madalena, D. (2011). Facebook Impacts Our Social Behavior. Turns Out, We're Obsessed. Retrieved from https://siliconangle.com/2011/02/23/facebook-impacts-our-social-behavior-turns-out-were-obsessed/

Marketer, E. (2013). Social networking reaches nearly one in four around the world. Retrieved from http://emarketer.com

Matusitz, J. (2008). Cyberterrorism: Postmodern state of chaos. *Information Security Journal: A Global Perspective, 17*(4), 179-187.

Medvedev, S. A. (2015). Offense-defense theory analysis of Russian cyber capability. Retrieved from https://core.ac.uk/download/pdf/36737355.pdf

Mickolus, E. (1978). Trends in Transnational Terrorism. In M. H. Livingston (Ed.), *International terrorism in the contemporary world*. Westport, Conneticut: Greenwood Press.

Monster Connect. (2009). 7 รูปแบบทั่วไปของการโจมตี Cybersecurity. Retrieved from https://www.monsterconnect.co.th/7-common-types-of-cybersecurity-attacks/

Moph. (2564). Moph cybersecurity. Retrieved from https://hss.moph.go.th/fileupload/2564-278.pdf

O'Neill, P. H. (2020). The cyberattack that changed the world. Retrieved from https://www.dailydot.com/debug/web-war-cyberattack-russia-estonia/

Paul, N. D. (2012). Common malware types: Cybersecurity 101. Retrieved from https://www.veracode.com/blog/2012/10/common-malware-types-cybersecurity-101

Pradillo, J. C. O. (2011). Fighting against cybercrime in Europe: the admissibility of remote searches in Spain. *European Journal of Crime, Criminal Law and Criminal Justice, 19*, 363.

Reed, T. (2004). *At the Abyss: An insider's history of the cold war*. New York, NY: Ballantine Books.

Reich, P. C. (2012). Case study: India - terrorism and terrorist use of the internet/technology. Retrieved from https://waseda.pure.elsevier.com/en/publications/case-study-india-terrorism-and-terrorist-use-of-the-internettechn

Reyes, A., Brittson, R., O'Shea, K., & Steele, J. (2011). *Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors* Massachusetts, MA: Syngress.

Schmid, A. P. (2011). The Routlaedge handbook of terrorism research. Retrieved from https://www.routledge.com/Routledge-Handbook-of-Terrorism-and-Counterterrorism/Silke/p/book/9780367580520

Schmitt, M. N. (2010). Drone Attacks under the Jus ad Bellum and Jus in Bello: Clearing the 'fog of Law'. *Yearbook of International Humanitarian Law, 13*, 311-326.

Shiryaev, Y. (2010). Circumstances Surrounding the Separation Barrier and the Wall Case and their Relevance for the Israeli Right of Self-Defense. *Gonz. J. Int'l L., 14*, 1.

Silke, A. (2003). *Research on terrorism: Trends, achievements and failures*. Abindon: Routledge.

Skoudis, E., & Zeltser, L. (2004). *Malware: Fighting malicious code*. New Jersey, NJ: Prentice Hall Professional.

Sukharenko, A. N. (2019). Russian ITC security policy and cybercrime. Retrieved from https://www.ponarseurasia.org/sites/default/files/policy-memos-pdf/Pepm601_Sukharenko_July2019_4.pdf

Tai, C. (2019). North Korean cyberwarfare: as big a threat as its nuclear weapons?

Talihärm, A.-M. (2010). Cyberterrorism: in Theory or in Practice? *Defence Against Terrorism Review, 3*(2), 59-74.

Tams, C. J. (2009). The use of force against terrorists. *European Journal of International Law, 20*(2), 359-397.

Technocrime and criminological theory. (2018). (K. F. Steinmetz & M. Nobles Eds.). New York, NY: Routledge.

ThaiCERT. (2018). *Cybersecurity strategy for critical information infrastructure in Thailand*. Bangkok: Electronic Transactions Development Agency.

ThaiCERT. (2021). Incident report statistics 2021. Retrieved from https://www.etda.or.th/th/Our-Service/thaicert/stat.aspx

Thruelsen, P. D. (2006). *From soldier to civilian: Disarmament demobilisation reintegration in afghanistan*. Copenhagen: Danish Institute for International Studies.

Tibbetts, S. G., & Rivera, J. (2015). 11 Prenatal and perinatal factors in the development of persistent criminality. In *The development of criminal and antisocial behavior* (pp. 167-180). New York, NY: Springer.

U.N. Counter-Terrorism Implementation Task Force. (2009). Report on countering the use of the internet for terrorist purposes 3. Retrieved from http://www.un.org/en/terrorism/ctitf/pdfs/ctitf_internet_wg_2009_report.pdf

U.N. Report of the Working Group. (2010). Measures to Eliminate International Terrorism, U.N. GAOR, 65th Sess., art. Retrieved from https://www.un.org/en/ga/sixth/65/ElimIntTerror.shtml

UnITed naTIons CoUnTer-TerrorIsm ImplemenTaTIon Task ForCe. (2019). The use of the internet for terrorist purposes. Retrieved from https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

Van Steenberghe, R. (2010). Self-Defence in Response to Attacks by Non-state Actors in the Light of Recent State Practice: A Step Forward? *Leiden Journal of International Law, 23*(1), 183-208.

Wall, D. (2007). Cybercrime: The transformation of crime in the information age. *Polity, 4*.

Walter, E. V. (1969). *Terror and resistance: A study of political violence, with case studies of some primitive African communities* (Vol. 1). New York, NY: Oxford University Press.

Weimann, G. (2005). Cyberterrorism: The sum of all fears? *Studies in Conflict & Terrorism, 28*(2), 129-149.

Whitaker, B. (2003). Flags in the Dust, GUARDIAN. Retrieved from http://www.guardian.co.uk/world/2003/mar/24/worlddispatch.iraq.

Williams, G. (2007). Gabriel Tarde and the Imitation of Deviance. Retrieved from http://criminology.fsu.edu/crimtheory/tarde.htm

Zhenfang, Z. (2015). Study on computer trojan horse virus and its prevention. *International Journal of Engineering Applied Sciences 2*(8).

ภาคผนวก

คณะกรรมการพิจารณาจริยธรรมการวิจัยในคน กลุ่มสหสถาบัน ชุดที่ 2
สังคมศาสตร์ มนุษยศาสตร์ และศิลปกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
อาคารจามจุรี 1 ชั้น 1 ห้อง 114 ถนนพญาไท แขวงวังใหม่ เขตปทุมวัน กรุงเทพมหานคร 10330
โทรศัพท์ : 0 2218 3210-11 E-mail: curec2.ch1@chula.ac.th

COA No. 122/2564

ใบรับรองโครงการวิจัย

โครงการวิจัยที่ 073/64 การรับมือของภาครัฐกับการก่อการร้ายทางไซเบอร์ในประเทศไทย

ผู้วิจัยหลัก นางสาวนัทธมน เพชรกล้า

หน่วยงาน คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

คณะกรรมการพิจารณาจริยธรรมการวิจัยในคน กลุ่มสหสถาบัน ชุดที่ 2 สังคมศาสตร์ มนุษยศาสตร์ และศิลปกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย พิจารณาจริยธรรมการวิจัยโดยยึดหลัก ของ Declaration of Helsinki, the Belmont report, CIOMS guidelines และ The international conference on harmonization – Good clinical practice (ICH-GCP) อนุมัติให้ดำเนินการศึกษาวิจัยเรื่องดังกล่าวได้

ลงนาม _____
(ศาสตราจารย์กิตติคุณ ดร.ธีระพันธ์ เหลืองทองคำ)
ประธานคณะกรรมการ

ลงนาม _____
(ผู้ช่วยศาสตราจารย์ ดร.หนึ่งหทัย แรงผลสืบฤทธิ์)
กรรมการและเลขานุการ

รูปแบบการพิจารณาทบทวน: แบบลดขั้นตอน

วันที่รับรอง: 7 มิถุนายน 2564 **วันหมดอายุ**: 6 มิถุนายน 2565

เอกสารที่คณะกรรมการรับรอง
1. ข้อเสนอโครงการวิจัย
2. ประวัติและผลงานของผู้วิจัย
3. เอกสารข้อมูลสำหรับกลุ่มตัวอย่าง/ผู้มีส่วนร่วมในการวิจัย
4. หนังสือยินยอมเข้าร่วมในการวิจัย
5. แนวคำถามสำหรับการสัมภาษณ์เชิงลึก

เลขที่โครงการ 073/64
วันที่รับรอง - 7 มิ.ย. 2564
วันหมดอายุ - 6 มิ.ย. 2565

เงื่อนไข

1. ผู้วิจัยรับทราบว่าเป็นการผิดจริยธรรม หากดำเนินการเก็บข้อมูลการวิจัยก่อนได้รับการอนุมัติจากคณะกรรมการพิจารณาจริยธรรมการวิจัย
2. หากใบรับรองโครงการวิจัยหมดอายุ การดำเนินการวิจัยต้องยุติ เมื่อต้องการต่ออายุต้องขออนุมัติใหม่ล่วงหน้าไม่น้อยกว่า 1 เดือน พร้อมส่งรายงานความก้าวหน้าการวิจัย
3. ต้องดำเนินการวิจัยตามที่ระบุไว้ในโครงการวิจัยอย่างเคร่งครัด
4. ใช้เอกสารข้อมูลสำหรับกลุ่มตัวอย่าง/ผู้มีส่วนร่วมในการวิจัย ใบยินยอมของกลุ่มตัวอย่างหรือผู้มีส่วนร่วมในการวิจัย และเอกสารอื่นๆที่ส่วนวิจัย เท่านั้น **เฉพาะที่ประทับตราคณะกรรมการเท่านั้น**
5. หากเกิดเหตุการณ์ไม่พึงประสงค์ร้ายแรงในสถานที่เก็บข้อมูลที่ของอนุมัติจากคณะกรรมการ ต้องรายงานคณะกรรมการภายใน 5 วันทำการ
6. หากมีการเปลี่ยนแปลงการดำเนินการวิจัย ให้ส่งคณะกรรมการพิจารณาปรับแก้ก่อนดำเนินการ
7. โครงการวิจัยไม่เกิน 1 ปี ส่งแบบรายงานสิ้นสุดโครงการวิจัย (AF 03-13) และขอต่ออายุโครงการวิจัยภายใน 30 วัน เมื่อโครงการวิจัยสิ้นสุดลง สำหรับโครงการวิจัยที่เป็นวิทยานิพนธ์ให้ส่งบทคัดย่อและการวิจัย ภายใน 30 วัน เมื่อโครงการวิจัยสิ้นสุดลง ทั้งนี้เพื่อเป็นหลักฐานในการปิดโครงการ
8. โครงการวิจัยที่ได้รับการอนุมัติโครงการโดยการพิจารณาทบทวนแบบยกเว้นการ (Exemption review) ปฏิบัติตามเงื่อนไข ข้อ 1,6 และ 7 เท่านั้น

Office of the Research Ethics Review Committee for Research Involving Human Subjects:
The Second Allied Academic Group in Social Sciences, Humanities and Fine and Applied Arts
Chamchuri 1 Building, Room 114, Phayathai Road, Wang Mai Sub-district,
Pathum Wan District, Bangkok 10330
Telephone number 0 2218 3210-11 E-mail:curec2.ch1@chula.ac.th

COA No. 122/2564

Certificate of Research Approval

Research Project Number 073/64 GOVERNMENT SECTOR'S RESPONSE IN COUNTER-CYBER-TERRORISM IN THAILAND

Principal Researcher Miss Natthamon Petchkla

Office Faculty of Political Science, Chulalongkorn University

The Research Ethics Review Committee for Research Involving Human Subjects: The Second Allied Academic Group in Social Sciences, Humanities and Fine and Applied Arts at Chulalongkorn University, based on Declaration of Helsinki, the Belmont report, CIOMS guidelines and the Principle of the international conference on harmonization – Good clinical practice (ICH-GCP) has approved the execution of the aforementioned research project.

Signature Theraphan Luangthongkum (Emeritus Prof. Theraphan Luangthongkum, PhD.) Chairman

Signature (Asst. Prof. Nunghatai Rangpongsumrit, PhD.) Secretary

Research Project Review Categories: Expedited Review

Date of approval: 7 June 2021 **Expiry date:** 6 June 2022

Documents approved by the Committee

1. The research proposal
2. The researcher CV
3. The information sheets for research participants
4. The informed consent forms
5. The guide questions for in-depth interviews

Protocol No. 073/64
Date of Approval 7 JUN 2021
Approval Expiry Date 6 JUN 2022

Conditions

1. *The researcher has acknowledged that it is unethical if he/she collects information for the research before the application for an ethics review has been approved by the Research Ethics Review Committee.*
2. *If the certificate of the research project expires, the research execution must come to a halt. If the researcher wishes to reapply for approval, he/she has to submit an application for a new certificate at least one month in advance, together with a research progress report.*
3. *The researcher must conduct the research strictly in accordance with what is specified in the research project.*
4. *The researcher must only use documents that provide information for the research sampling population/participants, their letters of consent and the letters inviting them to take part in the research, if any that have been endorsed with the seal of the Committee.*
5. *If any seriously untoward incident happens to the place where the research information, which has requested the approval of the Committee, is kept, the researcher must report this to the Committee within five working days.*
6. *If there is any change in the research procedure, the researcher must submit the change for review by the Committee before he/she can continue with his/her research.*
7. *For a research project of less than one year the researcher must submit a report of research termination (EF 80-13) and an abstract of the research outcome within thirty days of the research being completed. For a research project which is a thesis, the researcher must submit an abstract of the research outcome within thirty days of the research being completed. This is to be used as evidence of the termination of the project.*
8. *A research project which has passed the Exemption Review, must observe only the conditions in 1, 6 and 7.*

แบบสัมภาษณ์สำหรับบุคลากรในหน่วยงานที่เกี่ยวข้องกับ

การรับมือการก่อการร้ายไซเบอร์ในประเทศไทย (ด้านนโยบาย)

วันที่..... เดือน..... พ.ศ. 2564 สถานที่.....

คำชี้แจง : แบบสัมภาษณ์ชุดนี้ประกอบไปด้วยคำถามทั้งหมด 4 ส่วน ดังนี้

ส่วนที่ 1 : ข้อมูลทั่วไปของบุคลากร

ส่วนที่ 2 : ลักษณะของการก่อการร้ายไซเบอร์

ส่วนที่ 3 : การรับมือกับการก่อการร้ายไซเบอร์

ส่วนที่ 4 : ผลกระทบจากการก่อการร้ายไซเบอร์และการพัฒนาแนวทางเพื่อรับมือ

ส่วนที่ 1: ข้อมูลทั่วไปของบุคลากร

1.1 ชื่อ.....นามสกุล.....

1.2 อายุ.....

1.3 หน่วยงานที่สังกัด.....

1.4 ตำแหน่ง.....

1.5 การศึกษา.....

1.6 ประสบการณ์ในการทำงานด้านไซเบอร์

.....

.....

ส่วนที่ 2 : ลักษณะของการก่อการร้ายไซเบอร์

การก่อการร้ายไซเบอร์หรือภัยคุกคามที่เกิดกับหน่วยงาน/ภาครัฐ

.....

.....

เลขที่โครงการ 073/64
วันที่รับรอง 7 มิ.ย. 64
วันหมดอายุ 6 มิ.ย. 65

2.1 ความถี่ของการก่อการร้ายหรือภัยคุกคามที่เกิดขึ้น

.....

.....

2.2 เป้าหมายของการโจมตี

.....

.....

2.3 วิธีการ/กลยุทธ์ ที่ใช้ในการโจมตี

.....

.....

.....

.....

2.4 ความเสียหายจากการโจมตี

.....

.....

.....

.....

ส่วนที่ 3 : การรับมือกับการก่อการร้ายไซเบอร์

3.1 นโยบายในการรับมือการก่อการร้ายไซเบอร์หรือภัยคุกคามทางไซเบอร์ของหน่วยงาน/ภาครัฐ

.....

.....

.....

.....

3.2 การตอบโต้กับการก่อการร้ายไซเบอร์หรือภัยคุกคาม

.....

.....

.....

3.3 ท่านคิดเห็นว่าวิธีการรับมือจากการก่อการร้ายหรือภัยคุกคามของหน่วยงาน/ภาครัฐมีประสิทธิภาพมากน้อยเพียงใด

.....

.....

3.4 ท่านคิดเห็นว่าเทคโนโลยีหรือการลงทุนทางเทคโนโลยีที่หน่วยงาน/ภาครัฐมีเพียงพอหรือไม่

.....

.....

3.5 ท่านคิดเห็นว่างบประมาณที่ใช้เพื่อพัฒนาความมั่นคงปลอดภัยไซเบอร์ที่หน่วยงาน/ภาครัฐมีเพียงพอหรือไม่

.....

.....

ส่วนที่ 4 : ผลกระทบจากการก่อการร้ายไซเบอร์และการพัฒนาแนวทางเพื่อรับมือ

4.1 ผลกระทบจากการก่อการร้ายไซเบอร์หรือภัยคุกคามทางไซเบอร์ที่มีต่อหน่วยงาน/ภาครัฐ

.....

.....

.....

.....

4.2 ความตระหนักรู้ของหน่วยงาน/ภาครัฐที่มีต่อการก่อการร้ายไซเบอร์หรือภัยคุกคามทางไซเบอร์

.....

.....

.....

.....

4.3 หน่วยงาน/ภาครัฐมีการประชาสัมพันธ์หรือช่องทางใดในการสร้างความรับรู้ต่อการก่อการร้ายไซเบอร์หรือภัยคุกคามทางไซเบอร์

.....

.....

.....

4.4 หน่วยงาน/ภาครัฐมีแนวทางในพัฒนาเครื่องมือในการรับมือการก่อการร้ายไซเบอร์หรือภัยคุกคามทางไซเบอร์อย่างไร

.....

.....

.....

.....

เลขที่โครงการ	073/64
วันที่รับรอง	7 มิ.ย. 64
วันหมดอายุ	6 มิ.ย. 65

4.5 ท่านคิดเห็นว่าผู้บริหารของหน่วยงาน/ภาครัฐให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์มากน้อยเพียงใด

.....

.....

.....

.....

หมายเหตุ: การกำหนดขอบเขตในระดับหน่วยงาน และในระดับภาครัฐนั้นเพื่อที่จะให้ผู้ถูกสัมภาษณ์สามารถถ่ายทอดประสบการณ์ได้ในภาพกว้างเพื่อนำมาวิเคราะห์ผลการวิจัยที่ได้ในภายหลังอย่างครบถ้วน

แบบสัมภาษณ์สำหรับบุคลากรในหน่วยงานที่เกี่ยวข้องกับ

การรับมือการก่อการร้ายไซเบอร์ในประเทศไทย (ด้านเทคนิค)

วันที่..... เดือน..... พ.ศ. 2564 สถานที่.....

คำชี้แจง : แบบสัมภาษณ์ชุดนี้ประกอบไปด้วยคำถามทั้งหมด 4 ส่วน ดังนี้

ส่วนที่ 1 : ข้อมูลทั่วไปของบุคลากร

ส่วนที่ 2 : ลักษณะของการก่อการร้ายไซเบอร์

ส่วนที่ 3 : การรับมือกับการก่อการร้ายไซเบอร์

ส่วนที่ 4 : ผลกระทบจากการก่อการร้ายไซเบอร์และการพัฒนาแนวทางเพื่อรับมือ

ส่วนที่ 1: ข้อมูลทั่วไปของบุคลากร

1.1 ชื่อ..... นามสกุล.....

1.2 อายุ.....

1.3 หน่วยงานที่สังกัด.....

1.4 ตำแหน่ง.....

1.5 การศึกษา.....

1.6 ประสบการณ์ในการทำงานด้านไซเบอร์

.....

.....

ส่วนที่ 2 : ลักษณะของการก่อการร้ายไซเบอร์

2.1 การก่อการร้ายไซเบอร์หรือภัยคุกคามที่เกิดกับหน่วยงาน/ภาครัฐ

.....

.....

2.2 ความถี่ของการก่อการร้ายหรือภัยคุกคามที่เกิดขึ้น

.....

.....

2.3 เป้าหมายของการโจมตี

.....

.....

2.4 วิธีการ/กลยุทธ์ ที่ใช้ในการโจมตี

.....

.....

.....

.....

2.5 ความเสียหายจากการโจมตี

.....

.....

.....

.....

ส่วนที่ 3 : การรับมือกับการก่อการร้ายไซเบอร์

3.1 นโยบาย แนวทาง หรือมาตรการในการรับมือการก่อการร้ายไซเบอร์หรือภัยคุกคามทางไซเบอร์ของหน่วยงาน/ภาครัฐเป็นอย่างไร

.....

.....

เลขที่โครงการ	073/64
วันที่รับรอง	7 มิ.ย. 64
วันหมดอายุ	6 มิ.ย. 65

.....

.....

3.2 การตอบโต้กับการก่อการร้ายไซเบอร์หรือภัยคุกคาม

.....

.....

.....

3.3 ท่านคิดเห็นว่าวิธีการรับมือจากการก่อการร้ายหรือภัยคุกคามของหน่วยงาน/ภาครัฐมีประสิทธิภาพมากน้อยเพียงใด

.....

.....

3.4 ท่านคิดเห็นว่าเทคโนโลยีหรือการลงทุนทางเทคโนโลยีที่หน่วยงาน/ภาครัฐมีเพียงพอหรือไม่

.....

.....

3.5 ท่านคิดเห็นว่างบประมาณที่ใช้เพื่อพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน/ภาครัฐมีเพียงพอหรือไม่

.....

.....

ส่วนที่ 4 : ผลกระทบจากการก่อการร้ายไซเบอร์และการพัฒนาแนวทางเพื่อรับมือ

4.1 ผลกระทบจากการก่อการร้ายไซเบอร์หรือภัยคุกคามทางไซเบอร์ที่มีต่อหน่วยงาน/ภาครัฐ

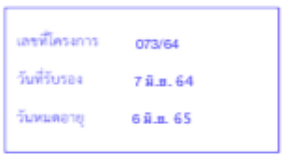
.....

.....

4.2 ความตระหนักรู้ของหน่วยงาน/ภาครัฐที่มีต่อการก่อการร้ายไซเบอร์หรือภัยคุกคามทางไซเบอร์

4.3 หน่วยงาน/ภาครัฐมีการประชาสัมพันธ์หรือช่องทางใดในการสร้างความรับรู้ในเรื่องการก่อการร้ายไซเบอร์หรือภัยคุกคามทางไซเบอร์

4.4 หน่วยงาน/ภาครัฐมีแนวทางในพัฒนาเครื่องมือในการรับมือการก่อการร้ายไซเบอร์หรือภัยคุกคามทางไซเบอร์อย่างไร



4.5 ท่านคิดเห็นว่าผู้บริหารของหน่วยงาน/ภาครัฐให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์มากน้อยเพียงใด

.....

.....

.....

.....

หมายเหตุ: การกำหนดขอบเขตในระดับหน่วยงาน และในระดับภาครัฐนั้นเพื่อที่จะให้ผู้ถูกสัมภาษณ์สามารถถ่ายทอดประสบการณ์ได้ในภาพกว้างเพื่อนำมาวิเคราะห์ผลการวิจัยที่ได้ในภายหลังอย่างครบถ้วน

เลขที่โครงการ	073/64
วันที่รับรอง	7 มิ.ย. 64
วันหมดอายุ	6 มิ.ย. 65

แบบสัมภาษณ์สำหรับผู้เชี่ยวชาญด้านการรับมือการก่อการร้ายไซเบอร์

วันที่..... เดือน..... พ.ศ. 2564 สถานที่.....

คำชี้แจง : แบบสัมภาษณ์ชุดนี้ประกอบไปด้วยคำถามทั้งหมด 3 ส่วน ดังนี้

ส่วนที่ 1 : ข้อมูลทั่วไปของบุคลากร

ส่วนที่ 2 : ความคิดเห็นต่อการก่อการร้ายไซเบอร์

ส่วนที่ 3 : การรับมือกับการก่อการร้ายไซเบอร์

ส่วนที่ 1: ข้อมูลทั่วไปของผู้ให้สัมภาษณ์

1.1 ชื่อ.....นามสกุล.....

1.2 อายุ.....

1.3 หน่วยงานที่สังกัด.....

1.4 ตำแหน่ง.....

1.5 การศึกษา.....

1.6 ประสบการณ์ในการทำงานหรือผลงานทางวิชาการด้านไซเบอร์

.....

.....

.....

ส่วนที่ 2 : ความคิดเห็นต่อการก่อการร้ายไซเบอร์

2.1 ท่านคิดว่าการก่อการร้ายไซเบอร์แตกต่างกับการก่อการร้ายแบบดั้งเดิมหรือไม่

.....

.....

.....

.....

เลขที่โครงการ	073/64
วันที่รับรอง	~~7 มิ.ย. 64~~
วันหมดอายุ	6 มิ.ย. 65

2.2 ท่านให้นิยามคำว่า “การก่อการร้ายไซเบอร์” อย่างไร

.....

.....

.....

2.3 ท่านคิดว่าหน่วยงานที่เป็นเป้าหมายต่อการก่อการร้ายไซเบอร์คือหน่วยงานประเภทใด

.....

.....

.....

2.4 ท่านคิดว่าผลกระทบจากการก่อการร้ายไซเบอร์ในประเทศมีความรุนแรงในระดับใด

.....

.....

.....

.....

ส่วนที่ 3 : การรับมือกับการก่อการร้ายไซเบอร์

3.1 ท่านคิดว่าประเทศไทยมีความพร้อมในการรับมือการก่อการร้ายไซเบอร์หรือไม่

.....

.....

.....

.....

3.2 ท่านคิดว่าจุดอ่อนและจุดแข็งทางด้านไซเบอร์ของประเทศไทยคืออะไร

.....

.....

.....

.....

3.3 ท่านคิดว่าการกำหนดนโยบายด้านไซเบอร์และการบริหารงบประมาณในการลงทุนด้านเทคโนโลยีของประเทศไทยเหมาะสมหรือไม่

.....

.....

.....

3.4 ท่านคิดว่าหน่วยงานรักษาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทยมีประสิทธิภาพและสามารถกำหนดทิศทางนโยบายความมั่นคงทางไซเบอร์ในอนาคตได้ถูกต้องหรือไม่

.....

.....

.....

3.5 ท่านคิดว่ากฎหมายการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทยมีเพียงพอและสามารถรับมือการผู้ก่อการร้ายไซเบอร์ได้หรือไม่

.....

.....

.....

3.6 ท่านคิดว่าประเทศไทยควรมีแนวทางการรับมือการก่อการร้ายไซเบอร์ทั้งจากในประเทศและต่างประเทศอย่างไร

.....

.....

.....

3.7 ท่านคิดว่าสิ่งสำคัญที่สุดในการรับมือการก่อการร้ายไซเบอร์ประกอบไปด้วยปัจจัยอะไรบ้าง

.....

.....

.....

.....

หมายเหตุ: การกำหนดขอบเขตในระดับหน่วยงาน และในระดับภาครัฐนั้นเพื่อที่จะให้ผู้ถูกสัมภาษณ์สามารถถ่ายทอดประสบการณ์ได้ในภาพกว้างเพื่อนำมาวิเคราะห์ผลการวิจัยที่ได้ในภายหลังอย่างครบถ้วน

เลขที่โครงการ	073/64
วันที่รับรอง	7 มิ.ย. 64
วันหมดอายุ	6 มิ.ย. 65

แบบสัมภาษณ์สำหรับผู้เชี่ยวชาญด้านการก่อการร้ายและสงคราม

วันที่..... เดือน..... พ.ศ. 2564 สถานที่.....

คำชี้แจง : แบบสัมภาษณ์ชุดนี้ประกอบไปด้วยคำถามทั้งหมด 2 ส่วน ดังนี้

ส่วนที่ 1 : ข้อมูลทั่วไปของบุคลากร

ส่วนที่ 2 : ความคิดเห็นต่อการก่อการร้ายดั้งเดิมและการก่อการร้ายไซเบอร์

ส่วนที่ 1: ข้อมูลทั่วไปของผู้ให้สัมภาษณ์

1.1 ชื่อ.....นามสกุล.....

1.2 อายุ.....

1.3 หน่วยงานที่สังกัด.....

1.4 ตำแหน่ง.....

1.5 การศึกษา.....

1.6 ประสบการณ์ในการทำงานหรือผลงานวิชาการด้านการก่อการร้าย

.....

.....

.....

ส่วนที่ 2 : ความคิดเห็นต่อการก่อการร้ายดั้งเดิมและการก่อการร้ายไซเบอร์

2.1 ท่านนิยาม “การก่อการร้าย” อย่างไร

.....

.....

2.2 ท่านคิดเห็นว่า “การก่อการร้าย” สามารถมาในรูปแบบไซเบอร์ได้หรือไม่

.....

.....

2.3 ท่านคิดเห็นว่า การก่อการร้ายแบบดั้งเดิม และ การก่อการร้ายไซเบอร์ มีเป้าประสงค์เดียวกันหรือไม่

.....

.....

2.4 ท่านคิดเห็นว่ากลยุทธ์ที่ใช้ใน การก่อการร้ายแบบดั้งเดิม และ การก่อการร้ายไซเบอร์ มีความเหมือนและต่างกันอย่างไร

.....

.....

.....

.....

2.5 ท่านคิดเห็นว่าการรับมือ การก่อการร้ายแบบดั้งเดิม และ การก่อการร้ายไซเบอร์ มีความเหมือนและต่างกันหรือไม่ อย่างไร

.....

.....

.....

.....

หมายเหตุ: การกำหนดขอบเขตในระดับหน่วยงาน และในระดับภาครัฐนั้นเพื่อที่จะให้ผู้ถูกสัมภาษณ์สามารถถ่ายทอดประสบการณ์ได้ในภาพกว้างเพื่อนำมาวิเคราะห์ผลการวิจัยที่ได้ในภายหลังอย่างครบถ้วน

เลขที่โครงการ	073/64
วันที่รับรอง	7 มิ.ย. 64
วันหมดอายุ	6 มิ.ย. 65

แบบสัมภาษณ์สำหรับผู้บริหารที่มีส่วนเกี่ยวข้องกับการรับมือการก่อการร้ายไซเบอร์ในประเทศไทย

วันที่..... เดือน..... พ.ศ. 2564 สถานที่.....

คำชี้แจง : แบบสัมภาษณ์ชุดนี้ประกอบไปด้วยคำถามทั้งหมด 4 ส่วน ดังนี้

ส่วนที่ 1 : ข้อมูลทั่วไปของบุคลากร

ส่วนที่ 2 : ความคิดเห็นต่อการก่อการร้ายไซเบอร์

ส่วนที่ 3 : การรับมือกับการก่อการร้ายไซเบอร์

ส่วนที่ 4 : ผลกระทบจากการก่อการร้ายไซเบอร์และการพัฒนาแนวทางเพื่อรับมือ

ส่วนที่ 1: ข้อมูลทั่วไปของผู้ให้สัมภาษณ์

1.1 ชื่อ.....นามสกุล.....

1.2 อายุ.....

1.3 หน่วยงานที่สังกัด.....

1.4 ตำแหน่ง.....

1.5 การศึกษา.....

ประสบการณ์ในการทำงานที่เกี่ยวข้องกับด้านไซเบอร์

.....

.....

.....

ส่วนที่ 2 : ความคิดเห็นต่อการก่อการร้ายไซเบอร์

2.1 ท่านนิยาม “การก่อการร้ายไซเบอร์” อย่างไร

.....

.....

2.2 ท่านเคยมีประสบการณ์ในการรับมือการก่อการร้ายไซเบอร์หรือไม่

.....

.....

2.3 ท่านคิดเห็นว่าหน่วยงาน/ภาครัฐ มีความเสี่ยงต่อการก่อการร้ายไซเบอร์หรือไม่

.....

.....

2.4 ในการกำหนดนโยบายของหน่วยงาน/ภาครัฐ ให้ความสำคัญกับนโยบายความมั่นคงปลอดภัยทางไซเบอร์มากน้อยเพียงใด

.....

.....

.....

.....

ส่วนที่ 3 : การรับมือกับการก่อการร้ายไซเบอร์

3.1 ท่านมีนโยบาย แนวทาง หรือมาตรการ ในการรับมือการก่อการร้ายไซเบอร์หรือไม่ อย่างไร

.....

.....

.....

.....

3.2 ท่านมีการประเมิน นโยบาย แนวทาง หรือมาตรการ ในการรับมือการก่อการร้ายไซเบอร์ดังกล่าวหรือไม่

3.3 อุปสรรคหรือข้อจำกัดที่เกิดขึ้นกับการรับมือการก่อการร้ายคืออะไร

- ด้านกฎหมาย

- ด้านงบประมาณ

- ด้านเทคโนโลยี

- ด้านบุคลากร

3.4 หากเกิดเหตุคุกคามทางไซเบอร์แบบเร่งด่วน ท่านมีการรับมืออย่างไร

.....

.....

.....

3.5 หน่วยงาน/ภาครัฐ มีช่องทางประชาสัมพันธ์หรือการสร้างความตระหนักรู้แก่บุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์หรือไม่ อย่างไร

.....

.....

.....

3.6 ความสำเร็จในด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์คืออะไร

.....

.....

.....

ส่วนที่ 4 : ผลกระทบจากการก่อการร้ายไซเบอร์และการพัฒนาแนวทางเพื่อรับมือ

4.1 ผลกระทบจากการก่อการร้ายไซเบอร์หรือภัยคุกคามทางไซเบอร์

.....

.....

.....

.....

4.2 ความตระหนักรู้ของบุคลากรของหน่วยงาน/ภาครัฐ ที่มีต่อการก่อการร้ายไซเบอร์หรือภัยคุกคามทางไซเบอร์

.....

.....

.....

.....

4.3 ท่านคิดว่าควรมีการประชาสัมพันธ์หรือช่องทางใดในการสร้างความรับรู้ต่อการก่อการร้ายไซเบอร์หรือภัยคุกคามทางไซเบอร์

.....

.....

.....

4.3 ท่านมีแนวทางในพัฒนาเครื่องมือในการรับมือการก่อการร้ายไซเบอร์หรือภัยคุกคามทางไซเบอร์อย่างไร

.....

.....

.....

.....

ประวัติผู้เขียน

ชื่อ-สกุล	นัทธมน เพชรกล้า
วัน เดือน ปี เกิด	12 สิงหาคม 2534
สถานที่เกิด	จังหวัดยะลา
วุฒิการศึกษา	จุฬาลงกรณ์มหาวิทยาลัย มหาวิทยาลัยคิงส์คอเลจ ลอนดอน
ที่อยู่ปัจจุบัน	23 ซอยสวัสดี 1 ถนนผังเมือง 5 ตำบลสะเตง อำเภอเมืองยะลา จังหวัดยะลา
รางวัลที่ได้รับ	รัฐศาสตรบัณฑิต เกียรตินิยมอันดับ 1 จุฬาลงกรณ์มหาวิทยาลัย MA. War Studies King's College London