ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์
ในพื้นที่จังหวัดชายแดนภาคใต้

โดย

พลตรี ราชิต อรุณรังษี
รองผู้อำนวยการสำนักการข่าว
สำนักงานปฏิบัติภารกิจรักษาความมั่นคงภายในกองทัพบก

นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ ๖๐
ประจำปีการศึกษา พุทธศักราช ๒๕๖๐-๒๕๖๑

บทคัดย่อ

เรื่อง ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

ลักษณะวิชา ยุทธศาสตร์

ผู้วิจัย พลตรี ราชิต อรุณรังสี หลักสูตร วปอ. รุ่นที่ ๖๐

งานวิจัยนี้นำเสนอยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ โดยมีวัตถุประสงค์เพื่อ ๑) ศึกษารูปแบบ วิธีการ การประเมินสถานการณ์ และปัญหาผลกระทบ ๒) ศึกษาผลกระทบที่ส่งผลต่อความมั่นคงแห่งชาติ และ ๓) นำเสนอยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ การวิจัยนี้ใช้ระเบียบวิธีวิจัยเชิงคุณภาพ กลุ่มเป้าหมาย ได้แก่ ๑) หน่วยงานด้านความมั่นคงของรัฐ ๒) ผู้บริหาร/ผู้นำท้องถิ่น ๔ จังหวัด ๓) หน่วยงานภาคเอกชน ๔) หน่วยงานพลเรือน ๕) ภาคประชาชน ๖) เจ้าหน้าที่ด้านการข่าวที่เชี่ยวชาญ ๗) เจ้าหน้าที่ทหารที่รับผิดชอบ ๘) ผู้ปฏิบัติงานที่เกี่ยวข้อง ๙) ผู้ทรงคุณวุฒิจากหน่วยงานความมั่นคง และ ๑๐) ผู้เชี่ยวชาญด้านวิศวกรรมระบบไอซีทีและโลกไซเบอร์ รวมกลุ่มเป้าหมายทั้งสิ้น ๗๕ คน ได้มาจากการเลือกในลักษณะจำเพาะเจาะจง เครื่องมือที่ใช้ในการวิจัย ได้แก่ แบบสัมภาษณ์แบบไม่มีโครงสร้าง การวิเคราะห์และสังเคราะห์ข้อมูลเชิงคุณภาพโดยวิธีพรรณนาเชิงวิเคราะห์ ตรวจสอบข้อมูลโดยวิธีการสามเส้าด้านข้อมูล และยืนยันร่างยุทธศาสตร์โดยการสัมมนาอิงผู้เชี่ยวชาญ

ผลการวิจัยพบว่า ในพื้นที่จังหวัดชายแดนภาคใต้มีกระบวนการใช้โลกไซเบอร์ในการสร้างความไม่สงบสุขหลากหลายวิธี เช่น การใช้เครือข่ายสังคมออนไลน์เพื่อการบ่อนทำลายความน่าเชื่อถือ การปฏิบัติการจิตวิทยาและการโฆษณาชวนเชื่อของกลุ่มผู้ไม่หวังดี การสร้างกระแสข่าวในเชิงลบและการสร้างความขัดแย้งต่อประชาชน การก่อวินาศกรรมโดยใช้อินเตอร์เน็ตเป็นมัชฌิมโดยมีแนวโน้มจะปฏิบัติการในรูปแบบอื่นๆ มากขึ้น ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ ประกอบด้วย ๗ ยุทธศาสตร์ ได้แก่ ๑) การจัดโครงสร้างพื้นฐานของประเทศไทยสำหรับใช้ในการจัดการกับภัยคุกคามด้าน ๒) การสร้างการตระหนักรู้โลกไซเบอร์ให้กับประชาชน ๓) การพัฒนาความก้าวหน้าด้านไซเบอร์ ๔) การส่งเสริมความร่วมมือด้านไซเบอร์ระหว่างภาครัฐ ภาคเอกชน และภาคประชาชน ๕) การกำหนดใช้กฎหมายด้านไซเบอร์และการบังคับใช้กับประชาชน ๖) การใช้การบูรณาการร่วมกันเพื่อแบ่งปันข้อมูลข่าวสาร และ ๗) การรับรู้ด้านไซเบอร์เพื่อการป้องกัน การยับยั้ง และการโจมตี ประเทศไทยควรใช้ยุทธศาสตร์และมาตรการรองรับให้มีประสิทธิภาพ คุณภาพ และความเข้มแข็งอย่างต่อเนื่อง เพื่อเสริมสร้างความมั่นคงปลอดภัยด้านไซเบอร์และการนำสันติสุขกลับคืนสู่พื้นที่จังหวัดชายแดนภาคใต้ต่อไป

ABSTRACT

Title **Cyber Threats Management Strategy in Southern Border Provinces**

Field **Strategy**

Name **Major General Rachit Aroonrungsri** **Course NDC** **Class 60**

This article presents a strategy for managing cyber threats in the southern border provinces, with the following objectives: 1) study the model of the situation assessment method; 2) study the impact of cyber threats on national security in the southern border provinces; and 3) present a cyber threats management strategy in the border provinces. This research uses qualitative research methodology by study focused on specific issues leading to the establishment of cyber threat management strategies in the southern border provinces. Target groups include: 1) 10 state security agencies; 2) 8 local administrators/leaders in 4 provinces; 3) 8 private sector organizations; 4) 8 civilian organizations; 5) 8 people in southern border provinces; 6) 8 news officers threatened of cyber threats; 7) military officers threatened of cyber threats; 8) 8 people involved in internet network; 9) 4 experts from the cyber security department, Thai Army Headquarters; and 9) 5 ICT and cyber security experts. The total target groups of 75 people came from a specific selection. The research tools were unstructured interviews. Analysis and synthesis of data based on qualitative research. Analysis and synthesis of qualitative research data by means of analytical descriptive method, Validate data using data triangulation technique and confirm the strategy by using connoisseurship approach.

The research found that in the southern border provinces, there is a cybercrime process to create a variety of disturbances. Like using social networks to undermine the credibility of government officials. Including the psychological operations and propaganda of the poor. Creating negative news and creating conflicts with the people. Sabotage using the Internet is mediocre. There are likely to be other types of operations. In addition, the system uses communication through the application to avoid detection and tracking by government officials. These have made a direct impact on national security. Strategies for managing cyber threats in the southern border provinces consist of 7 strategies: 1) Thailand's infrastructure for dealing with cyber threats; 2) creating cyber awareness for the people; 3) development of cyber security; 4)

promotion of cyber-cooperation between the public, private and public sectors; 5) enforcement of cyber law and enforcement with the people; 6) use of mutual Integration to share information and 7) cyber awareness for prevention, inhibition and attack. For Thailand, strategies and measures to address cyber threats should be implemented to ensure consistency, quality and consistency. In order to strengthen cyber security and bring peace back to the southern border provinces of the country.

คำนำ

รายงานการวิจัยเรื่อง “ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้” จัดทำขึ้นเพื่อนำข้อมูลและรายงานการวิจัยดังกล่าวมาใช้ให้เป็นประโยชน์ในการกำหนดยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้สำหรับประเทศไทย โดยการศึกษาครั้งนี้ได้ดำเนินการออกแบบ วิเคราะห์ สังเคราะห์ เพื่อหาแนวทางและยุทธศาสตร์ที่เหมาะสมสำหรับการจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ที่สามารถนำไปใช้งานได้จริง เพื่อทำให้การบริหารจัดการภัยคุกคามด้านไซเบอร์ของประเทศไทยเป็นไปอย่างมีเอกภาพ มีประสิทธิภาพ และมีประสิทธิผล และสอดรับกับยุทธศาสตร์ชาติระยะ ๒๐ ปี (พ.ศ.๒๕๖๑ - ๒๕๘๐) ซึ่งอยู่ในประเด็นยุทธศาสตร์เฉพาะด้านความมั่นคงและความสัมพันธ์ระหว่างประเทศในการรักษาความมั่นคงและความสงบเรียบร้อยภายในประเทศ การนำพื้นที่จังหวัดชายแดนภาคใต้กลับสู่สันติสุขอย่างถาวร และการเตรียมรับมือกับภัยคุกคามรูปแบบใหม่ ทั้งนี้ก็เพื่อเป็นหลักประกันด้านความมั่นคงแห่งชาติด้านไซเบอร์ของประเทศไทยในอนาคต

พล.ต.
(ราชิต อรุณรังษี)
นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตร วปอ. รุ่นที่ ๖๐
ผู้วิจัย

สารบัญ

		หน้า
บทคัดย่อ		**ก**
คำนำ		**ข**
กิตติกรรมประกาศ		**ค**
สารบัญ		**ง**
สารบัญตาราง		**ฉ**
สารบัญแผนภาพ		**ช**
บทที่ ๑	**บทนำ**	**๑**
	ความเป็นมาและความสำคัญของปัญหา	๑
	วัตถุประสงค์ของการวิจัย	๕
	ขอบเขตของการวิจัย	๕
	วิธีดำเนินการวิจัย	๖
	ประโยชน์ที่ได้รับจากการวิจัย	๘
	คำจำกัดความ	๘
บทที่ ๒	**ทฤษฎีและแนวคิดเกี่ยวกับภัยคุกคาม**	**๑๐**
	แนวคิดเรื่องสงครามไซเบอร์	๑๐
	แนวคิดเรื่องความมั่นคงแห่งชาติ	๑๗
	แนวคิดเรื่องผลประโยชน์แห่งชาติ	๒๑
	ทฤษฎีความขัดแย้ง	๒๕
	ทฤษฎีการบริหารจัดการภาครัฐยุคใหม่	๓๔
	ระบบไอซีทีเพื่อการจัดการ	๔๑
	พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์(ฉบับที่ ๒) พ.ศ.๒๕๖๐	๕๔
	สถานการณ์ด้านความมั่นคงและความไม่สงบในพื้นที่จังหวัดชายแดนภาคใต้	๕๘
	การทบทวนวรรณกรรมที่เกี่ยวข้อง	๖๙
	แนวคิดของผู้ทรงคุณวุฒิ	๗๔

สารบัญ (ต่อ)

		หน้า
	กรอบความคิดของการวิจัย	๘๑
	สรุป	๘๓
บทที่ ๓	**รูปแบบภัยคุกคามด้านไซเบอร์**	**๘๔**
	รูปแบบภัยคุกคามด้านไซเบอร์ที่ปรากฏทั่วโลกในอดีตจนถึงปัจจุบัน	๘๔
	รูปแบบภัยคุกคามด้านไซเบอร์ที่ปรากฏในประเทศไทย	๙๓
	รูปแบบภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงและความไม่สงบ ในพื้นที่จังหวัดชายแดนภาคใต้ของประเทศไทย	๑๐๑
	สรุป	๑๒๐
บทที่ ๔	**วิเคราะห์ผลกระทบและกำหนดยุทธศาสตร์ในการจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้**	**๑๒๑**
	การวิเคราะห์ผลกระทบของภัยคุกคามด้านไซเบอร์	๑๒๑
	แนวทางการจัดการภัยคุกคามด้านไซเบอร์ของต่างประเทศ	๑๒๓
	การวิเคราะห์รูปแบบที่เหมาะสมของการจัดการภัยคุกคามด้านไซเบอร์ ในพื้นที่จังหวัดชายแดนภาคใต้	๑๒๙
	การวิเคราะห์ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ ในพื้นที่จังหวัดชายแดนภาคใต้	๑๔๑
	สรุป	๑๕๗
บทที่ ๕	**สรุปและข้อเสนอแนะ**	**๑๕๙**
	สรุป	๑๕๙
	ข้อเสนอแนะ	๑๘๒
บรรณานุกรม		๑๘๔
ภาคผนวก		๑๘๖
	ผนวก ก รายชื่อผู้เชี่ยวชาญ	๑๘๗
	ผนวก ข เครื่องมือที่ใช้ในการวิจัย	๑๙๐
ประวัติย่อผู้วิจัย		๒๐๓

สารบัญตาราง

ตารางที่		หน้า
๓ - ๑	ระดับของการดำเนินงานให้ประสบผลสำเร็จตามโครงสร้างหลักของกรอบการดำเนินงาน	๙๐
๓ - ๒	ระดับของการดำเนินงานให้ประสบผลสำเร็จตามโครงสร้างหลักของกรอบการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์	๙๙

สารบัญแผนภาพ

แผนภาพที่		หน้า
๒ - ๑	ภัยคุกคามด้านไซเบอร์	๑๗
๒ - ๒	ความสัมพันธ์ระหว่างองค์กรและระบบไอซีที	๔๑
๒ - ๓	โครงสร้างระบบไอซีทีภายในองค์กร	๔๒
๒ - ๔	ระบบงานไอซีทีในองค์กร	๔๓
๒ - ๕	คุณสมบัติที่สำคัญของระบบสารสนเทศเพื่อการจัดการที่ดี	๕๒
๒ - ๖	กรอบความคิดของการวิจัย	๘๒
๓ - ๑	โครงสร้างหลักของกรอบการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ตามแนวคิดของสถาบันมาตรฐานและเทคโนโลยีแห่งสหรัฐอเมริกา	๘๙
๔ - ๑	โครงสร้างหลักของกรอบการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์	๑๒๖
๔ - ๒	พันธกิจกรอบการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์	๑๒๖
๔ - ๓	องค์ประกอบหลักของการรักษาความมั่นคงปลอดภัยด้านไซเบอร์แห่งชาติ	๑๓๐
๔ - ๔	ยุทธศาสตร์ไซเบอร์เพื่อการป้องกันประเทศของกระทรวงกลาโหม พ.ศ.๒๕๕๘	๑๓๒
๔ - ๕	โครงสร้างหลักของการรักษาความมั่นคงปลอดภัยด้านไซเบอร์แห่งชาติ	๑๓๙
๔ - ๖	หน่วยบัญชาการไซเบอร์แห่งชาติ	๑๓๙
๔ - ๗	โครงสร้างพื้นฐานการจัดการภัยคุกคามด้านไซเบอร์	๑๔๐

บทที่ ๑
บทนำ

ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันระบบเทคโนโลยีสารสนเทศและการสื่อสารหรือระบบไอซีที (Information and Communication Technology : ICT) มีประโยชน์ต่อการพัฒนาประเทศให้เจริญก้าวหน้า โดยเป็นเรื่องที่เกี่ยวกับวิถีความเป็นอยู่ของสังคมสมัยใหม่ ก่อให้เกิดการเปลี่ยนแปลงวิถีชีวิตรวมถึงกลายเป็นสิ่งสำคัญและจำเป็นในการปฏิบัติงานของทุกองค์กรไม่ว่าจะเป็นการดำเนินธุรกิจอุตสาหกรรม การให้บริการโทรคมนาคม การท่องเที่ยว การทหาร และการศึกษา เป็นต้น หรือกล่าวได้ว่าโลกเข้าสู่สังคมฐานความรู้ (Knowledge-based Society) ที่มีการเชื่อมโยงข้อมูลเป็นระบบเครือข่าย โดยเฉพาะอย่างยิ่งเครือข่ายอินเตอร์เน็ตได้ถูกนำมาใช้อย่างแพร่หลายในทุกบริบทของสังคม (พงษ์ศักดิ์ ผกามาศ, ๒๕๕๓) อีกทั้งโครงสร้างพื้นฐานวิกฤต (Critical Infrastructure) ที่อยู่รอบตัวเรา เช่น ระบบไฟฟ้า น้ำประปา การคมนาคมขนส่ง ระบบธนาคาร และระบบสื่อสารโทรคมนาคม ล้วนมีการเชื่อมต่อกับเครือข่ายอินเตอร์เน็ตแทบทั้งสิ้น การแพร่หลายของเครือข่ายนี้ได้เปลี่ยนวิถีการดำรงชีวิตของมนุษย์แทบทุกด้าน เช่น การใช้เว็บไซต์ การรับส่งอีเมล์ การซื้อขายสินค้าไปจนถึงการทำธุรกรรมทางอิเล็กทรอนิกส์ เช่น ระบบ Internet Banking ระบบ GFMIS ของรัฐบาล และระบบการชำระภาษี เป็นต้น แนวโน้มในอนาคตของมนุษยชาติย่อมหลีกเลี่ยงไม่ได้กับการใช้งานระบบเครือข่ายสากล (Universal Network) ที่เพิ่มมากขึ้น ตามการเปลี่ยนแปลงทั้งทางด้านวิทยาศาตร์และเทคโนโลยี รวมถึงการเชื่อมโยงกันระหว่างประเทศในโลกยุคเศรษฐกิจดิจิทัล (Digital Economy)

พัฒนาการและการเปลี่ยนแปลงของระบบไอซีทีได้ส่งผลกระทบต่อกิจการและการดำเนินงานทางการเมือง การทหาร เศรษฐกิจ และสังคมจิตวิทยาของทุกประเทศในโลกเป็นอย่างมาก ผลจากการพัฒนาด้านวิทยาศาสตร์และเทคโนโลยีในหลายทศวรรษที่ผ่านมาทำให้เกิดการปฏิวัติสารสนเทศ (Information Revolution) ซึ่งเกี่ยวข้องกับการประมวลผลและกระจายสารสนเทศอย่างกว้างขวางจนนำมาสู่การพัฒนาในสาขาคอมพิวเตอร์และการติดต่อสื่อสารอย่างก้าวกระโดดจนก่อให้เกิดพื้นที่มิติใหม่ที่เรียกว่า “โลกไซเบอร์” (Cyberspace) ด้วยเหตุนี้ ความมั่นคงแห่งชาติ (National Security) จึงได้รับผลกระทบจากการปฏิวัติและประกฏการณ์ของโลกไซเบอร์นี้โดยตรง เห็นได้จากมีผู้กล่าวถึง “ความมั่นคงด้านไซเบอร์” (Cyber Security) ในบริบทของความมั่นคงแห่งชาติมากขึ้น อีกทั้งยังมีผู้กล่าวถึงคุณลักษณะของโลกไซเบอร์ ความล่อแหลมที่มีอยู่ภายใน

ภัยคุกคามที่เป็นไปได้ด้านไซเบอร์ รวมถึงประเด็นที่เกี่ยวข้องกับการป้องกัน (Defense) การยับยั้ง (Deterrence) และการโจมตี (Attack) ในโลกไซเบอร์มากขึ้น แม้ว่าในปัจจุบันจะยังไม่มีหลักเกณฑ์ที่แน่นอนและชัดเจนที่จะกำหนดได้ว่า “การโจมตีด้านไซเบอร์เป็นอาชญากรรม” ในขณะเดียวกันก็ยังไม่มีกลไกทางกฎหมายระหว่างประเทศใดที่จะสามารถระบุและควบคุมความสัมพันธ์ระหว่างรัฐในโลกไซเบอร์นี้ได้เลย ดังนั้นนานาอารยะประเทศรวมถึงประเทศไทยยังคงค้นหารูปแบบและวิธีการที่เหมาะสมในการจัดการกับภัยคุกคามนี้อย่างต่อเนื่องจนถึงปัจจุบัน ทั้งนี้เพื่อให้เกิดความมั่นคงในการใช้ประโยชน์จากระบบไอซีทีเพื่อการพัฒนาประเทศชาติอย่างแท้จริง

ด้วยเหตุนี้ ในโลกที่เต็มไปด้วยความขัดแย้งทางการเมือง หากคู่กรณีมุ่งที่จะบรรลุจุดมุ่งหมาย (Ends) ของตน โดยไม่สนใจว่าจะใช้เครื่องมือ (Means) อะไรด้วยแล้ว การทำสงครามไซเบอร์จึงเป็นเครื่องมือที่ง่ายและเหมาะสมมากที่สุด หากพวกเขาต้องการทำสงครามในกรอบของกฎหมายระหว่างประเทศที่มีอยู่ในปัจจุบัน อย่างไรก็ตาม การใช้อาวุธด้านไซเบอร์กับฝ่ายตรงข้ามก็ย่อมสุ่มเสี่ยงต่อการถูกโจมตีกลับเช่นเดียวกัน เพราะคงไม่มีฝ่ายใดที่จะยอมให้ฝ่ายตรงข้ามเป็นฝ่ายโจมตีได้ฝ่ายเดียว เพราะแต่ละฝ่ายต่างก็สามารถโจมตีอีกฝ่ายหนึ่งได้ทุกเมื่อ โดยอาศัยบุคลากรที่มีขีดความสามารถและระบบเครือข่ายที่มีอยู่ ทั้งนี้ก็เนื่องมาจากแต่ละฝ่ายสามารถเข้าถึงเครือข่ายจากที่ใดก็ได้ในโลกนี้ เพื่อเฝ้าติดตาม ค้นหาช่องโหว่ของระบบ โจมตีต่อระบบ การแอบฝังโปรแกรมจารกรรมข้อมูล (Spyware) แสวงประโยชน์จากการใช้ช่องโหว่ของโปรแกรมควบคุมเครือข่ายและการทำงานของระบบ (Botnet) รวมถึงแพร่ระบาดโปรแกรมไม่พึงประสงค์ (Malware) เพื่อสร้างความเสียหายต่อระบบอีกฝ่ายหนึ่งได้ตลอดเวลา ทำให้ยากที่จะป้องกัน หรือเฝ้าระวังและติดตามฝ่ายตรงข้าม (P.W. Singer and Allan Friedman, 2014) ฉะนั้นการกระทำที่เป็นอันตรายต่อระบบเครือข่ายเหล่านี้ ถือเป็นภัยคุกคามรูปแบบใหม่ที่เรียกว่า “ภัยคุกคามด้านไซเบอร์” (Cyber Threats) ซึ่งอาจเกิดจากการกระทำในระดับบุคคล องค์การ หรือรัฐก็ได้ ในระดับบุคคล การกระทำเช่นนี้ถือเป็นการก่ออาชญากรรมบนโลกไซเบอร์ (Cyber Crimes) ทั้งที่เกิดจากพวกมือสมัครเล่น พวกลองวิชา รวมไปถึงพวกไม่เพียงแต่หวังล้วงหรือขโมยข้อมูลเท่านั้น แต่อาจลามไปถึงการทำลายล้าง หรือสร้างความเสียหายต่อทรัพย์สินของเป้าหมาย หรือสร้างอันตรายและผลกระทบต่อชีวิตประชาชนทั่วไปด้วยก็ได้ อย่างไรก็ตาม กลุ่มที่กระทำโดยมีอุดมการณ์หรือวัตถุประสงค์ทางการเมือง อาจเรียกการกระทำเช่นนี้ได้ว่าเป็น “ภัยการก่อการร้ายทางโลกไซเบอร์” แน่นอนที่สุดว่า ภัยคุกคามเหล่านี้อาจมิได้กระทำโดยกลุ่มบุคคลหรือผู้ก่อการร้ายด้านไซเบอร์ตามลำพัง เพราะการกระทำของบุคคลเหล่านี้อาจมีองค์การหรือรัฐอยู่เบื้องหลังหรือให้การสนับสนุนก็ได้ ทั้งนี้ก็เพื่อบรรลุเป้าหมายทางยุทธศาสตร์ในการสร้างความเสียหายต่อโครงสร้างพื้นฐานและส่งผลกระทบต่อความมั่นคง

แห่งชาติฝ่ายตรงข้าม โดยเฉพาะในด้านผลประโยชน์ทางการเมือง เศรษฐกิจ สังคมจิตวิทยา ทรัพยากรธรรมชาติและสิ่งแวดล้อม เป็นต้น (พล.ต.ฤทธี อินทราวุธ, ๒๕๖๑)

ดังนั้น ภัยคุกคามด้านไซเบอร์จะยังคงเป็นภัยคุกคามต่อความมั่นคงตั้งแต่ระดับความมั่นคงแห่งชาติไปจนถึงระดับความมั่นคงของมนุษย์ แน่นอนที่สุดว่าโลกไซเบอร์ในอนาคตจะมีแนวโน้มขยายตัวเพิ่มขึ้นเป็นทวีคูณ เพราะโลกไซเบอร์ได้กลายเป็นสิ่งอำนวยความสะดวกต่อวิถีชีวิตมนุษย์และการทำงานประจำวันในองค์กรต่างๆ ทุกประเภท อย่างไรก็ตาม โลกไซเบอร์นี้ย่อมมีทั้งด้านที่เป็นคุณและด้านที่เป็นโทษ โดยขึ้นอยู่กับว่ามนุษย์จะใช้มันเพื่อวัตถุประสงค์ใด ด้วยเหตุนี้การที่มนุษย์ได้ประโยชน์มหาศาลจากโลกไซเบอร์ก็นำมาซึ่งความท้าทายต่อการรับมือและป้องกันความเสียหายที่เกิดจากการใช้งานดังกล่าวด้วยเช่นกัน มีคำแนะนำให้ผู้ที่เกี่ยวข้องทางด้านระบบไอซีทีให้เปลี่ยนความคิดเรื่องความปลอดภัยบนโลกไซเบอร์เสียใหม่ โดยให้พึงคิดไว้เสมอว่า “ระบบที่ตนใช้งานอยู่จะต้องถูกโจมตีแน่นอน” จะต้องทำอย่างไรจึงจะสามารถหาวิธีรับมือได้อย่างรวดเร็วและเพื่อให้เกิดผลกระทบน้อยที่สุด เนื่องจากไม่มีระบบใดในโลกที่จะสมบูรณ์ปลอดภัย ๑๐๐% การทำให้ตนเองคุ้นชินกับการถูกแฮ็คหรือถูกโจมตีจะช่วยให้สามารถรับมือกับภัยคุกคามบนโลก ไซเบอร์ได้อย่างไม่หวั่นเกรง อีกทั้งบนโลกไซเบอร์พบว่าการถูกดิสเครดิตหรือสูญเสียภาพลักษณ์ขององค์กรกลายเป็นความเสี่ยงที่ส่งผลกระทบอย่างรุนแรง เนื่องจากข่าวสารในโลกไซเบอร์สามารถแพร่กระจายอย่างรวดเร็ว และเมื่อสูญเสียความน่าเชื่อถือไปแล้วครั้งหนึ่ง การจะนำมันกลับคืนมานับว่าเป็นเรื่องยากมาก ตัวอย่างที่เห็นได้ชัดก็คือเรื่อง Single Gateway ที่ทางรัฐบาลเพียงแค่ต้องการศึกษาแนวทางเท่านั้น ยังไม่ได้วางแผนที่จะทำแต่อย่างใด แต่กลายเป็นว่าผู้คนบนโลกไซเบอร์ต่างตื่นตัวกับเรื่องดังกล่าว และมองรัฐบาลในแง่ลบจนเกิดแคมเปญ F5 ลากยาวไปถึงการตกเป็นเป้าหมายของกลุ่ม Anonymous ดังนั้นการพัฒนาศักยภาพของมนุษย์ให้รู้เท่าทันอันตรายคาดการณ์ถึงแนวโน้มในอนาคต และลงมือจัดการกับภัยคุกคามด้านไซเบอร์จะต้องอาศัยสรรพกำลังในระดับประชารัฐเพื่อการป้องกันและแก้ไขอย่างทันท่วงที โดยต้องไม่สร้างผลกระทบต่อความมั่นคงของประเทศชาติในอนาคต

สำหรับปัญหาด้านความมั่นคงในพื้นที่จังหวัดชายแดนใต้ (จชต.) ๔ จังหวัด ของประเทศไทย ที่ประกอบด้วยพื้นที่ของจังหวัดปัตตานี จังหวัดนราธิวาส และจังหวัดยะลา รวมถึง ๔ อำเภอของจังหวัดสงขลา ได้แก่ อำเภอเทพา อำเภอสะบ้าย้อย อำเภอจะนะ และอำเภอนาทวี ความรุนแรงในจังหวัดชายแดนภาคใต้ที่เกิดขึ้นมาอย่างยาวนานเป็นปัญหาที่มีพัฒนาการที่มีความซับซ้อน ละเอียดอ่อน และมีความเชื่อมโยงกันหลายมิติโดยมีใจกลางของปัญหา คือ เรื่องอัตลักษณ์ชาติพันธุ์มาลายูศาสนาอิสลาม และประวัติศาสตร์รัฐปัตตานี โดยการต่อสู้ที่ใช้ความรุนแรงเป็นผลมาจากคนกลุ่มหนึ่งที่มีอุดมการณ์ต้องการแบ่งแยกดินแดนได้นำเงื่อนไขอัตลักษณ์เฉพาะมาขยายผล

ในการใช้ความรุนแรง ทำให้เกิดบรรยากาศความกลัว ไม่ไว้วางใจระหว่างรัฐกับประชาชนและประชาชนกับประชาชนเพิ่มมากขึ้น ปัจจุบันสถานการณ์ของการก่อความไม่สงบจากภัยคุกคามด้านไซเบอร์นั้นได้มีการนำสื่อสังคมออนไลน์บนเครือข่ายอินเตอร์เน็ตมาใช้อย่างกว้างขวางในแง่การบ่อนทำลายความน่าเชื่อถือของเจ้าหน้าที่รัฐ รวมถึงการปฏิบัติการจิตวิทยาและการโฆษณาชวนเชื่อของกลุ่มผู้ไม่หวังดี นอกจากนี้การปรับเปลี่ยนรูปแบบการติดต่อสื่อสารภายในของกลุ่มก่อความไม่สงบในพื้นที่ จากเดิมใช้การติดต่อสื่อสารผ่านระบบโทรศัพท์เคลื่อนที่มาใช้ระบบการติดต่อสื่อสารผ่านแอปพลิเคชั่นที่ให้บริการผ่านเครือข่ายอินเตอร์เน็ตเพื่อหลบเลี่ยงการตรวจจับและติดตามโดยเจ้าหน้าที่รัฐ ซึ่งการเปลี่ยนแปลงดังกล่าวส่งผลกระทบในการแก้ไขปัญหาความไม่สงบในพื้นที่อย่างต่อเนื่อง และแม้ว่าในปัจจุบันเครือข่ายอินเตอร์เน็ตถูกนำมาใช้ในการสร้างผลกระทบในทางอ้อมต่อความมั่นคงในพื้นที่แต่ในอนาคตหากสถานการณ์ความรุนแรงในพื้นที่ก็ยังไม่จบลงอาจมีการนำเครือข่ายอินเตอร์เน็ตมาใช้ในการสร้างผลกระทบทางตรงต่อความมั่นคงในพื้นที่ได้อีก อาทิเช่น การก่อวินาศกรรมโดยใช้เครือข่ายอินเตอร์เน็ตเป็นมัชฌิม ซึ่งจากสถิติพบว่ามีการใช้โทรศัพท์มือถือในการจุดระเบิดมากกว่า ๗๐๐ ครั้ง ในรอบสิบปีที่ผ่านมา โดยมีแนวโน้มว่าผู้ก่อการร้ายจะปฏิบัติการในรูปแบบอื่นๆ เพิ่มมากขึ้น การสร้างกระแสข่าวในเชิงลบและการสร้างความขัดแย้งต่อประชาชนโดยใช้เครือข่ายสังคมออนไลน์ และมีการบ่อนทำลายข้อมูลสำคัญแห่งรัฐเพื่อสร้างความไม่สงบในรูปแบบต่างๆ อยู่ตลอดเวลา เป็นต้น นอกจากนั้นยังสามารถก่อผลกระทบต่อภาพลักษณ์ทางทหาร เช่น การแพร่ภาพคลิปที่ไม่เหมาะสมของทหาร ไม่ว่าจะเป็นการเลือกเผยแพร่รูปภาพเฉพาะความรุนแรง การใช้อาวุธในสถานการณ์ก่อความไม่สงบ และการแพร่คลิปการสูญเสียของทหารเพื่อลดขวัญและกำลังใจของผู้ปฏิบัติงาน ซึ่งเหตุการณ์ต่างๆ เหล่านี้ล้วนแต่ส่งผลกระทบโดยตรงต่อความมั่นคงแห่งชาติแทบทั้งสิ้น

ดังนั้นผู้วิจัยจึงเกิดแนวคิดและสนใจที่จะดำเนินการวิจัยเรื่อง “ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้” ทั้งนี้เพื่อนำข้อมูลดังกล่าวมาใช้ในการกำหนดรูปแบบ แนวทาง กลไก และมาตรการต่างๆ รวมถึงข้อเสนอแนะเชิงนโยบายในการจัดการกับภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ โดยคาดว่าผลการวิจัยสามารถนำมาใช้ให้เป็นประโยชน์กับการรับมือกับภัยคุกคามด้านไซเบอร์เพื่อเสริมสร้างความมั่นคงและระงับปัญหาความไม่สงบอย่างเป็นรูปธรรม ทั้งนี้เพื่อให้การดำรงชีวิตของประชาชนในพื้นที่เป็นไปอย่างสันติสุขทั้งในระยะสั้นและระยะยาว อีกทั้งยังใช้เป็นกรอบยุทธศาสตร์ในการพัฒนาเสริมสร้างกำลังด้านไซเบอร์ให้เป็นระบบ มีระเบียบแบบแผน มีมาตรการเชิงรับและเชิงรุกที่มีประสิทธิภาพ คุณภาพและยั่งยืน ผู้วิจัยจึงเห็นว่า “ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้” เป็นเรื่องสำคัญที่สมควรได้รับการวิจัยและผลการวิจัยนี้จะเป็นประโยชน์และสอดรับกับ

ยุทธศาสตร์ชาติระยะ ๒๐ ปี (พ.ศ.๒๕๖๑ - ๒๕๘๐) ซึ่งอยู่ในประเด็นยุทธศาสตร์เฉพาะด้านความมั่นคงและความสัมพันธ์ระหว่างประเทศในการรักษาความมั่นคงและความสงบเรียบร้อยภายในประเทศ การนำพื้นที่จังหวัดชายแดนภาคใต้กลับสู่สันติสุขอย่างถาวร และการเตรียมรับมือกับภัยคุกคามรูปแบบใหม่ เช่น การก่อการร้ายและการโจมตีทางไซเบอร์ เป็นต้น โดยสามารถนำผลการวิจัยนี้ไปใช้ในการบริหารจัดการภัยคุกคามด้านไซเบอร์ให้มีประสิทธิผลต่อไป ทั้งนี้ก็เพื่อเป็นหลักประกันด้านความมั่นคงแห่งชาติด้านไซเบอร์ของประเทศไทยในอนาคต

วัตถุประสงค์ของการวิจัย

๑. เพื่อศึกษารูปแบบ วิธีการ การประเมินสถานการณ์ และปัญหาผลกระทบของภัยคุกคามด้านไซเบอร์

๒. เพื่อศึกษาผลกระทบของภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงแห่งชาติในพื้นที่จังหวัดชายแดนภาคใต้

๓. เพื่อนำเสนอยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

ขอบเขตของการวิจัย

การศึกษาวิจัยครั้งนี้เป็นหายุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ โดยการศึกษา ค้นคว้า รวบรวม ทบทวน วิเคราะห์ และสังเคราะห์ ตามระเบียบวิธีวิจัยเชิงคุณภาพ (Qualitative Research Methodology) โดยกำหนดขอบเขตการวิจัยได้ดังนี้

๑. ขอบเขตด้านเนื้อหา เน้นการศึกษาเฉพาะประเด็นที่นำไปสู่การกำหนดยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ ได้แก่ แนวคิดเรื่องสงครามไซเบอร์ แนวคิดเรื่องความมั่นคงแห่งชาติ แนวคิดเรื่องผลประโยชน์แห่งชาติ ทฤษฎีความขัดแย้ง ทฤษฎีการบริหารจัดการภาครัฐยุคใหม่ รูปแบบภัยคุกคามด้านไซเบอร์ที่ปรากฏทั่วโลกทั้งของไทยและต่างประเทศ สถานการณ์ด้านความมั่นคงและความไม่สงบในจังหวัดชายแดนภาคใต้ที่มีสาเหตุมาจากภัยคุกคามด้านไซเบอร์ เอกสารทางวิชาการ เอกสารทางราชการของหน่วยงานที่เกี่ยวข้อง บทความวิชาการต่างๆ การสำรวจข้อมูลเชิงพื้นที่ เอกสารประกอบการบรรยายที่เกี่ยวข้อง แนวคิดของผู้ทรงคุณวุฒิ และเอกสารงานวิจัยที่เกี่ยวข้อง

๒. ขอบเขตด้านพื้นที่ ศึกษาเฉพาะพื้นที่จังหวัดชายแดนภาคใต้ประกอบด้วยพื้นที่ของจังหวัดปัตตานี จังหวัดนราธิวาส และจังหวัดยะลา รวมถึง ๔ อำเภอของจังหวัดสงขลา ได้แก่ อำเภอเทพา อำเภอสะบ้าย้อย อำเภอจะนะ และอำเภอนาทวี

๓. ขอบเขตด้านประชากร กลุ่มเป้าหมายประกอบด้วย ๑) หน่วยงานด้านความมั่นคงของรัฐ จำนวน ๑๐ คน (กองทัพภาคที่ ๔, กอ.รมน.ภาค ๔ ส่วนหน้า, ศอบต., ศชต., และ ฉก.) ๒) ผู้บริหาร/ผู้นำท้องถิ่น ๔ จังหวัด จำนวน ๘ คน ๓) หน่วยงานภาคเอกชน จำนวน ๘ คน ๔) หน่วยงานพลเรือน จำนวน ๘ คน ๕) ภาคประชาชน จำนวน ๘ คน ๖) เจ้าหน้าที่ด้านการข่าวที่เชี่ยวชาญระบบไอซีที จำนวน ๘ คน ๗) เจ้าหน้าที่ทหารที่รับผิดชอบด้านภัยคุกคามด้านไซเบอร์ จำนวน ๘ คน ๘) ผู้ปฏิบัติงานที่เกี่ยวข้องกับระบบเครือข่ายอินเตอร์เน็ต จำนวน ๘ คน ๙) ผู้ทรงคุณวุฒิจากหน่วยงานความมั่นคงด้านไซเบอร์กองทัพไทย จำนวน ๔ คน และ ๑๐) ผู้เชี่ยวชาญด้านวิศวกรรมระบบไอซีทีและโลกไซเบอร์ จำนวน ๕ คน การเลือกกลุ่มเป้าหมายที่ให้ข้อมูลเป็นไปในลักษณะจำเพาะเจาะจง (Purposive Informant) เพื่อให้ได้ข้อมูลที่มีความแม่นตรงและสามารถวิเคราะห์ได้อย่างถูกต้องเหมาะสมกับแต่ละสถานการณ์และพื้นที่

๔. ขอบเขตด้านระยะเวลา จะทำการศึกษาในช่วงระยะเวลาตั้งแต่เดือนพฤศจิกายน ๒๕๖๐ ถึงเดือนมิถุนายน ๒๕๖๑

วิธีดำเนินการวิจัย

การวิจัยนี้ใช้ระเบียบวิธีวิจัยเชิงคุณภาพ (Qualitative Research) โดยมีจุดมุ่งหมายเพื่อนำเสนอ “ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้” โดยการศึกษา ค้นคว้าและรวบรวมข้อมูลที่เกี่ยวข้องกับภัยคุกคามด้านไซเบอร์และผลกระทบด้านต่างๆ ทั้งนี้เพื่อนำข้อมูลดังกล่าวมากำหนดเป็นรูปแบบที่เหมาะสมของการจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ที่สามารถนำไปใช้ได้จริง รวมถึงร่างยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ที่สามารถป้องกันและแก้ไข เพื่อรับมือหรือยับยั้งความเสียหายที่จะเกิดขึ้นจากภัยคุกคามในอนาคตพร้อมข้อเสนอแนะเชิงนโยบาย โดยมีประเด็นการวิจัยต่อไปนี้

๑. ด้านการเก็บรวบรวมข้อมูล เก็บข้อมูลเชิงลึกตามกระบวนการวิจัยเชิงคุณภาพโดยมีข้อมูลปฐมภูมิและทุติยภูมิ ดังนี้

๑.๑ ข้อมูลปฐมภูมิ (Primary) ดำเนินการโดยการสัมภาษณ์แบบเชิงลึก (In-depth Interview) ผู้ที่มีหน้าที่เกี่ยวข้องกับความมั่นคงในพื้นที่จังหวัดชายแดนภาคใต้ ได้แก่ ๑) หน่วยงานด้านความมั่นคงของรัฐ จำนวน ๑๐ คน (กองทัพภาคที่ ๔, กอ.รมน.ภาค ๔ ส่วนหน้า, ศอบต., ศชต.,

และ ฉก.) ๒) ผู้บริหาร/ผู้นำท้องถิ่น ๔ จังหวัด จำนวน ๘ คน ๓) หน่วยงานภาคเอกชน จำนวน ๘ คน ๔) หน่วยงานพลเรือน จำนวน ๘ คน ๕) ภาคประชาชน จำนวน ๘ คน ๖) เจ้าหน้าที่ด้านการข่าวที่เชี่ยวชาญระบบไอซีที จำนวน ๘ คน ๗) เจ้าหน้าที่ทหารที่รับผิดชอบด้านภัยคุกคามด้านไซเบอร์ จำนวน ๘ คน ๘) ผู้ปฏิบัติงานที่เกี่ยวข้องกับระบบเครือข่ายอินเตอร์เน็ต จำนวน ๘ คน ๙) ผู้ทรงคุณวุฒิจากหน่วยงานความมั่นคงด้านไซเบอร์กองทัพไทย จำนวน ๔ คน และ ๑๐) ผู้เชี่ยวชาญด้านวิศวกรรมระบบไอซีทีและโลกไซเบอร์ จำนวน ๕ คน รวมกลุ่มเป้าหมายทั้งสิ้น ๗๕ คน ซึ่งกลุ่มเป้าหมายทั้งหมดได้มาจากการเลือกแบบเจาะจงโดยอาศัยความสะดวก (Convenience) ทั้งนี้ กลุ่มผู้ให้ข้อมูลหลัก (Key Informants) จะครอบคลุมผู้มีส่วนเกี่ยวข้องทั้งโดยทางตรงและทางอ้อม ทั้งหมดด้านภัยคุกคามด้านไซเบอร์และผู้ที่ปฏิบัติภารกิจในพื้นที่จังหวัดชายแดนภาคใต้

๑.๒ ข้อมูลทุติยภูมิ (Secondary) ได้จากเอกสารที่เกี่ยวข้อง อาทิ รายงานเหตุการณ์ความไม่สงบในพื้นที่ กฎหมาย ระเบียบ วารสาร บทความทางวิชาการ รายงานวิจัย และเอกสารสื่อสิ่งพิมพ์อิเล็กทรอนิกส์ทั้งในและต่างประเทศ รวมทั้งผลการสัมมนาและการทบทวนแนวทางการป้องกันและแก้ไขปัญหาภัยคุกคามด้านไซเบอร์ของหน่วยงานด้านความมั่นคงและกองทัพไทย รวมถึงฝ่ายพลเรือนในแต่ละกระทรวง

๒. ด้านการวิเคราะห์และสังเคราะห์ข้อมูล ดำเนินการวิเคราะห์และสังเคราะห์ตามหลักการวิจัยเชิงคุณภาพ และตรวจสอบข้อมูลโดยใช้เทคนิควิธีการสามเส้าด้านข้อมูล (Data Triangulation Technique) ประกอบด้วย ๑) ข้อมูลจากเอกสารและงานวิจัยที่เกี่ยวข้อง ๒) ข้อมูลที่ได้จากกลุ่มเป้าหมาย และ ๓) ข้อมูลจากระเบียบและกฎหมายที่เกี่ยวข้องกับความมั่นคงด้านไซเบอร์ รวมถึงการวิเคราะห์ SWOT เพื่อนำไปสู่การกำหนดประเด็นยุทธศาสตร์ในการจัดการกับภัยคุกคามด้านไซเบอร์อย่างเป็นระบบ

๓. ด้านการนำเสนอผลการวิจัย ตรวจสอบและยืนยัน (Confirmatory) ยุทธศาสตร์โดยการสัมมนาอิงผู้เชี่ยวชาญ (Connoisseurship) โดยอาศัยความรู้ ความเชี่ยวชาญ และประสบการณ์ของผู้วิจัย ร่วมกับความเห็นของผู้ทรงคุณวุฒิด้านวิศวกรรมระบบไอซีทีและโลกไซเบอร์ที่มีประสิทธิภาพ เพื่อแสดงความคิดเห็นและให้ข้อเสนอแนะ จากนั้นนำผลการตรวจสอบไปปรับปรุงกรอบยุทธศาสตร์ที่สมบูรณ์และนำเสนอแนวทางการปฏิบัติ แผนงาน โครงสร้างพื้นฐาน และมาตรการที่เกี่ยวข้องรวมถึงข้อเสนอแนะเชิงนโยบาย

๔. สรุปและเขียนรายงานการวิจัยฉบับสมบูรณ์

ประโยชน์ที่ได้รับจากการวิจัย

๑. ทำให้ทราบรูปแบบ วิธีการ การประเมินสถานการณ์ และปัญหาผลกระทบที่เกิดจากภัยคุกคามด้านไซเบอร์

๒. ทำให้ทราบปัญหาและผลกระทบของภัยคุกคามด้านไซเบอร์ที่ส่งผลกระทบต่อความมั่นคงในพื้นที่จังหวัดชายแดนภาคใต้รวมถึงแนวโน้มในอนาคต

๓. ทำให้ได้ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้พร้อมข้อเสนอแนะเชิงนโยบายที่สามารถใช้ในการป้องกันและแก้ไขปัญหาภัยคุกคามด้านไซเบอร์อย่างเป็นรูปธรรม

คำจำกัดความ

ภัยคุกคามด้านไซเบอร์ (Cyber Threat)	หมายถึง	สภาวการณ์หรือเหตุการณ์ใดๆ ที่อาจส่งผลกระทบอย่างร้ายแรงต่อความปลอดภัยของสารสนเทศที่อยู่ในระบบคอมพิวเตอร์หรือสังคมเครือข่ายจากการเข้าถึง (Access) การทำลาย (Destruction) การเปิดเผย (Disclosure) และการปรับเปลี่ยน (Modification) ข้อมูลโดยไม่ได้รับอนุญาต และ/หรือการปฏิเสธการทำงานของระบบคอมพิวเตอร์หรือสังคมเครือข่ายดังกล่าว โดยสามารถแบ่งออกเป็น ๒ ประเภท ได้แก่ ๑.๑ การโจมตีด้านไซเบอร์ (Cyber Attacks) หมายถึง การกระทำใดๆ อันเป็นการมุ่งทำลายทรัพย์สินของประชาชนหรือของรัฐ หรือสิ่งอันเป็นสาธารณูปโภค หรือการรบกวนขัดขวางหน่วงเหนี่ยวระบบการปฏิบัติงานใดๆ ตลอดจนการประทุษร้ายต่อบุคคลอันเป็นการก่อให้เกิดความปั่นป่วนทางการเมืองการเศรษฐกิจและสังคมแห่งชาติ โดยมุ่งหมายที่จะก่อให้เกิดความเสียหายต่อความมั่นคงของรัฐ โดยใช้เครือข่ายอินเตอร์เน็ตเป็นตัวกลางในการดำเนินการ และ ๑.๒ การจารกรรมด้านไซเบอร์ (Cyber Espionage)

		หมายถึง การล้วงความลับหรือข้อมูลจากคู่แข่งหรือศัตรูเพื่อความได้เปรียบทางการทหาร การเมือง หรือเศรษฐกิจ โดยใช้เครือข่ายอินเตอร์เน็ตเป็นตัวกลางในเข้าถึงข้อมูลที่เป็นความลับเพื่อการโจมตีระบบที่เป็นเป้าหมายต่อไป
จังหวัดชายแดนภาคใต้ (จชต.)	หมายถึง	พื้นที่ ๔ จังหวัดชายแดนภาคใต้ ได้แก่ จังหวัดปัตตานี จังหวัดนราธิวาส และจังหวัดยะลา รวมถึง ๔ อำเภอของจังหวัดสงขลา ประกอบด้วย อำเภอเทพา อำเภอสะบ้าย้อย อำเภอจะนะ และอำเภอนาทวี
ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์	หมายถึง	ยุทธศาสตร์ที่ใช้ในการจัดการกับภัยคุกคามด้านไซเบอร์เพื่อการรักษาความมั่นคงปลอดภัยให้กับระบบคอมพิวเตอร์และระบบเครือข่ายสารสนเทศ การใช้งานด้านไซเบอร์อย่างถูกวิธี ตลอดจนการป้องกันและแก้ไขปัญหาการโจมตีและการจารกรรมด้านไซเบอร์อย่างเป็นระบบ กรอบยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ประกอบด้วย การวิเคราะห์ SWOT กำหนดประเด็นที่เกี่ยวข้อง เป้าหมายยุทธศาสตร์ แนวทางหรือมาตรการ ยุทธวิธีหรือแผนการปฏิบัติ ดัชนีชี้วัดผลงาน และผลที่คาดว่าจะได้รับ เพื่อนำไปสู่การจัดการภัยคุกคามด้านไซเบอร์อย่างมีประสิทธิภาพ

บทที่ ๒
ทฤษฎีและแนวคิดเกี่ยวกับภัยคุกคาม

การวิจัยเรื่อง “ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้” โดยมีแนวคิด ทฤษฎี เอกสาร และงานวิจัยที่เกี่ยวข้องตามลำดับในประเด็นต่อไปนี้

๑. แนวคิดเรื่องสงครามไซเบอร์
๒. แนวคิดเรื่องความมั่นคงแห่งชาติ
๓. แนวคิดเรื่องผลประโยชน์แห่งชาติ
๔. ทฤษฎีความขัดแย้ง
๕. ทฤษฎีการบริหารจัดการภาครัฐยุคใหม่
๖. ระบบไอซีทีเพื่อการจัดการ
๗. พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ.๒๕๖๐
๘. สถานการณ์ด้านความมั่นคงและความไม่สงบในพื้นที่จังหวัดชายแดนภาคใต้
๙. การทบทวนวรรณกรรมที่เกี่ยวข้อง
๑๐. แนวคิดของผู้ทรงคุณวุฒิ
๑๑. กรอบความคิดของการวิจัย
๑๒. สรุป

แนวคิดเรื่องสงครามไซเบอร์

ช่วงศตวรรษที่ ๑๙๖๐ การพัฒนาของระบบเทคโนโลยีสารสนเทศและการสื่อสารหรือระบบไอซีทีโดยเฉพาะอย่างยิ่งระบบอินเตอร์เน็ตส่งผลให้เกิดการเปลี่ยนแปลงต่อเศรษฐกิจและสังคมโลกเป็นอย่างมาก เทคโนโลยีดังกล่าวช่วยลดอุปสรรคในเรื่องของเวลาและสถานที่ ช่วยทำให้เกิดการแลกเปลี่ยนข้อมูลข่าวสารและความรู้ต่างๆ ได้ง่ายขึ้น และยังมีส่วนเข้ามาช่วยในการจัดการงานด้านต่างๆ ของทุกภาคส่วนให้มีประสิทธิภาพและรวดเร็วมากยิ่งขึ้น การเปลี่ยนแปลงของระบบไอซีทีส่งผลให้โลกเปลี่ยนแปลงไปสู่สังคมโลกาภิวัตน์ที่ซึ่งเทคโนโลยีทำให้การติดต่อสื่อสารและปฏิสัมพันธ์ระหว่างบุคคลหรือองค์กรดำเนินไปโดยไม่มีอุปสรรคของเขตแดนและเวลา เมื่อเริ่มมีการนำระบบไอซีทีมาใช้อย่างแพร่หลายมากขึ้นโดยเฉพาะในประเทศผู้นำของโลก อย่างเช่น สหรัฐอเมริกาและจีน ส่งผลกระทบให้รูปแบบเศรษฐกิจและสังคมโลกมีความเปลี่ยนแปลงไปอย่าง

ชัดเจน ระบบไอซีทีที่พัฒนาไปอย่างรวดเร็วส่งผลให้เกิดแนวคิดเศรษฐกิจใหม่ (New Economy) ซึ่งมองว่างานสำคัญคืองานบริการพื้นฐานมาจากความรู้ต่างๆ ซึ่งเข้าถึงได้ด้วยระบบไอซีที พื้นฐานของเศรษฐกิจใหม่คือความสามารถทางการผลิตแบบใหม่ซึ่งอาศัยความรู้และนวัตกรรมที่ได้รับมาจากระบบไอซีที ดังนั้นการแข่งขันในระบบเศรษฐกิจใหม่จะเกิดขึ้นในสภาพแวดล้อมที่มีลักษณะเป็นโลกาภิวัตน์โดยการจัดการขององค์กรเพื่อการแข่งขันจะขึ้นอยู่กับความสามารถในการสร้างและใช้เครือข่ายต่างๆ ผ่านขีดความสามารถของระบบไอซีทีนั่นเอง หากพิจารณาในจุดแห่งความสำเร็จของบริษัท องค์กร หรือประเทศจะขึ้นอยู่กับความสามารถของพนักงานหรือพลเมืองในการประยุกต์ใช้ความรู้และข้อมูล ดังนั้นการแข่งขันระหว่างประเทศตามแนวคิดเศรษฐกิจใหม่คือการแข่งขันกันพัฒนาแรงงานและโครงสร้างพื้นฐานให้ประชาชนสามารถเข้าถึงและใช้สารสนเทศได้อย่างมีประสิทธิภาพ โดยจะนำไปสู่การลดต้นทุนในการผลิตและการตลาดอีกด้วย

ผลจากการพัฒนาด้านวิทยาศาสตร์และเทคโนโลยีในหลายทศวรรษที่ผ่านมา ทำให้ยุคสมัยปัจจุบันเกิดการปฏิวัติสารสนเทศ (Information Revolution) ซึ่งเกี่ยวข้องกับการประมวลผลและกระจายสารสนเทศอย่างกว้างขวางจนนำมาสู่การพัฒนาในสาขาคอมพิวเตอร์และการติดต่อสื่อสารอย่างก้าวกระโดดจนก่อให้เกิดพื้นที่มิติใหม่ที่เรียกว่า “โลกไซเบอร์” (Cyberspace) ด้วยเหตุนี้ ความมั่นคงแห่งชาติ (National Security) จึงได้รับผลกระทบจากการปฏิวัติสารสนเทศและประกฏการณ์ของโลกไซเบอร์นี้โดยตรง เห็นได้จากมีผู้กล่าวถึง “ความมั่นคงด้านไซเบอร์” (Cyber Security) ในบริบทของความมั่นคงแห่งชาติมากขึ้น อีกทั้งยังมีผู้กล่าวถึงคุณลักษณะของโลกไซเบอร์ ความล่อแหลมที่มีอยู่ภายในภัยคุกคามที่เป็นไปได้ด้านไซเบอร์ รวมถึงประเด็นที่เกี่ยวข้องกับการป้องกัน (Defense) การยับยั้ง (Deterrence) และการโจมตี (Attack) ในโลกไซเบอร์มากขึ้น แม้ว่าในปัจจุบันจะยังไม่มีหลักเกณฑ์ที่แน่นอนและชัดเจนที่จะกำหนดได้ว่า “การโจมตีด้านไซเบอร์เป็นอาชญากรรม” ในขณะเดียวกัน ก็ยังไม่มีกลไกทางกฎหมายระหว่างประเทศใดที่จะสามารถระบุและควบคุมความสัมพันธ์ระหว่างรัฐในโลกไซเบอร์นี้ได้เลย

ด้วยเหตุนี้ ในโลกที่เต็มไปด้วยความขัดแย้งทางการเมือง หากคู่กรณีมุ่งที่จะบรรลุจุดมุ่งหมาย (Ends) ของตน โดยไม่สนใจว่าจะใช้เครื่องมือ (Means) อะไรด้วยแล้ว การทำสงครามไซเบอร์ จึงเป็นเครื่องมือที่ง่ายและเหมาะสมมากที่สุด หากพวกเขาต้องการทำสงครามในกรอบของกฎหมายระหว่างประเทศที่มีอยู่ในปัจจุบัน อย่างไรก็ตาม การใช้อาวุธด้านไซเบอร์กับฝ่ายตรงข้ามก็ย่อมสุ่มเสี่ยงต่อการถูกโจมตีกลับเช่นเดียวกัน เพราะคงไม่มีฝ่ายใดที่จะยอมให้ฝ่ายตรงข้ามเป็นฝ่ายโจมตีได้ฝ่ายเดียว เพราะแต่ละฝ่ายต่างก็สามารถโจมตีอีกฝ่ายหนึ่งได้ทุกเมื่อ โดยอาศัยบุคลากรที่มีขีดความสามารถและระบบเครือข่ายที่มีอยู่ ทั้งนี้ก็เนื่องมาจากแต่ละฝ่ายสามารถเข้าถึงเครือข่ายจากที่ใดก็ได้ในโลกนี้ เพื่อการเฝ้าติดตาม ค้นหาช่องโหว่ของระบบ โจมตีต่อระบบ การแอบฝัง

โปรแกรมจารกรรมข้อมูล (Spyware) แสวงประโยชน์จากการใช้ช่องโหว่ของโปรแกรมควบคุมเครือข่ายและการทำงานของระบบ (Botnet) รวมถึงแพร่ระบาดโปรแกรมไม่พึงประสงค์ (Malware) เพื่อสร้างความเสียหายต่อระบบอีกฝ่ายหนึ่งได้ตลอดเวลา ทำให้ยากที่จะป้องกันหรือเฝ้าระวังและติดตามฝ่ายตรงข้าม ฉะนั้น การกระทำที่เป็นอันตรายต่อระบบเครือข่ายเหล่านี้ ถือเป็นภัยคุกคามรูปแบบใหม่ที่เรียกว่า “ภัยคุกคามด้านไซเบอร์” (Cyber Threats) (Wikipedia, 2018) ซึ่งอาจเกิดจากการกระทำในระดับบุคคล องค์การ หรือรัฐก็ได้ ในระดับบุคคล การกระทำเช่นนี้ถือเป็นการก่ออาชญากรรมบนโลกไซเบอร์ (Cyber Crimes) ทั้งที่เกิดจากพวกมือสมัครเล่น พวกลองวิชารวมไปถึงพวกไม่เพียงแต่หวังล้วงหรือขโมยข้อมูลเท่านั้น แต่อาจลามไปถึงการทำลายล้าง หรือสร้างความเสียหายต่อทรัพย์สินของเป้าหมาย หรือสร้างอันตรายและผลกระทบต่อชีวิตประชาชนทั่วไปด้วยก็ได้ อย่างไรก็ตาม กลุ่มที่กระทำโดยมีอุดมการณ์หรือวัตถุประสงค์ทางการเมือง อาจเรียกการกระทำเช่นนี้ได้ว่าเป็น “ภัยการก่อการร้ายทางโลกไซเบอร์” แน่นอนที่สุดว่า ภัยคุกคามเหล่านี้ อาจมิได้กระทำโดยกลุ่มบุคคลหรือผู้ก่อการร้ายด้านไซเบอร์ตามลำพัง เพราะการกระทำของบุคคลเหล่านี้อาจมีองค์การหรือรัฐอยู่เบื้องหลังหรือให้การสนับสนุนก็ได้ ทั้งนี้ก็เพื่อบรรลุเป้าหมายทางยุทธศาสตร์ในการสร้างความเสียหายต่อโครงสร้างพื้นฐานและส่งผลกระทบต่อความมั่นคงแห่งชาติฝ่ายตรงข้าม โดยเฉพาะในด้านผลประโยชน์ทางการเมือง เศรษฐกิจ สังคมจิตวิทยา ทรัพยากรธรรมชาติและสิ่งแวดล้อม เป็นต้น (พล.ต.ฤทธี อินทราวุธ, ๒๕๖๐)

๑. ความเป็นมาของการทำสงครามไซเบอร์

การทำสงครามไซเบอร์ถือเป็นสงครามยุคใหม่ที่ถือกำเนิดขึ้นในช่วงปลายของยุคสงครามเย็น (Cold War) เริ่มจากในปี ค.ศ. ๑๙๘๒ ได้เกิดเหตุการณ์ที่เรียกว่า “การก่อวินาศกรรมท่อส่งแก๊สธรรมชาติทรานส์-ไซบีเรีย” (Trans-Siberian Soviet Pipeline Sabotage) ของอดีตสหภาพโซเวียตรัสเซีย โดยสหรัฐอเมริกาได้หลอกให้สหภาพโซเวียตขโมยโปรแกรมควบคุมท่อส่งแก๊สธรรมชาติของตนผ่านทางบริษัทในแคนาดา โดยโปรแกรมดังกล่าวได้ถูกฝังไวรัสคอมพิวเตอร์ที่เรียกว่า “Trojan Horse” ไปด้วย เมื่อสหภาพโซเวียตนำโปรแกรมนี้ไปใช้ ไวรัสดังกล่าวได้ทำให้ท่อส่งแก๊สธรรมชาติของสหภาพโซเวียตเกิดการระเบิดขึ้นในเดือนมิถุนายน ค.ศ.๑๙๘๒ ทั้งนี้ก็เพื่อขัดขวางไม่ให้สหภาพโซเวียตมีรายได้จากการส่งขายแก๊สธรรมชาติให้กับประเทศตะวันตก และบ่อนทำลายเศรษฐกิจภายในของสหภาพโซเวียต ในปี ค.ศ.๑๙๙๔ ได้เกิดการโจมตีด้านไซเบอร์ ณ ห้องปฏิบัติการวิจัยและพัฒนาทางทหารที่ชื่อว่า “Rome Lab” โดยนักเจาะระบบคอมพิวเตอร์ (Hacker) ๒ นาย ได้เจาะเข้าสู่เครือข่ายของห้องปฏิบัติการดังกล่าวถึง ๑๕๐ ครั้ง แต่ก็ไม่สามารถสร้างความเสียหายให้กับห้องปฏิบัติการดังกล่าวได้ โดย ๑ ในนักเลงคอมพิวเตอร์จากอิสราเอลได้ถูกปล่อยตัวให้พ้นจากข้อกล่าวหาหลังถูกจับกุมตัว เนื่องจากอิสราเอลยังไม่มีกฎหมายที่สามารถ

บังคับใช้ในกรณีดังกล่าวในขณะนั้นได้ หลังจากนั้นไม่นาน ไวรัสคอมพิวเตอร์ที่เรียกว่า “Love Bug” ได้แพร่ระบาดและส่งผลกระทบต่อคอมพิวเตอร์ทั่วโลกกว่า ๖๐ ล้านเครื่อง ทำให้หลายๆ หน่วยงาน เช่น รัฐสภาอังกฤษ และบริษัทฟอร์ด มอเตอร์ จำต้องปิดระบบเสริฟเวอร์ของตนเอง ในขณะเดียวกัน นักเจาะระบบคอมพิวเตอร์ชาวฟิลิปปินส์ก็มิได้ถูกต้องข้อกล่าวหาและถูกลงโทษ เพราะตามกฎหมายของฟิลิปปินส์ถือว่า การสร้างไวรัสคอมพิวเตอร์ไม่ถือว่าเป็นอาชญากรรม

ในระหว่างสงครามโคโซโว (Kosovo War) ของกลุ่มนาโต้ (NATO) ในปี ค.ศ.๑๙๙๙ เครื่องบินขับไล่ลำหนึ่งของกลุ่มนาโต้ได้จงใจทิ้งระเบิดลงไปในสถานทูตจีนในกรุงเบลเกรด ทั้งนี้ก็เพื่อทำลายการติดต่อสื่อสารที่สถานทูตจีนพยายามให้การสนับสนุนแก่กองทัพยูโกสลาฟในขณะนั้น หลังจากนั้นเพียง ๑๒ ชั่วโมง กลุ่มนักเจาะระบบคอมพิวเตอร์ชาวจีนที่เรียกตนเองว่า “Chinese Red Hacker Alliance” ได้ร่วมกันจัดตั้ง “กลุ่มพลเรือนรักชาติชาวจีน” เพื่อร่วมกันโจมตีทางไซเบอร์ต่อประเทศต่างๆ ในกลุ่มนาโต้เพื่อเป็นการแก้แค้น ส่งผลให้เว็บไซต์หลายเว็บไซต์ของรัฐบาลสหรัฐอเมริกา เว็บไซต์ที่เป็นภาษาอังกฤษ และเว็บไซต์อื่นๆ ต้องล่มลงเป็นเวลานาน อีกเหตุการณ์หนึ่งที่น่าสนใจก็คือ เหตุการณ์ที่ระบบอินเตอร์เน็ตของเอสโตเนียล่มในปี ค.ศ.๒๐๐๗ เหตุการณ์นี้เกิดขึ้นหลังที่เอสโตเนียได้ประกาศเอกราชจากอดีตสหภาพโซเวียตในปี ค.ศ.๑๙๙๑ ซึ่งทำให้ประชาชนชาวเอสโตเนียได้มีโอกาสเปิดรับสารสนเทศและเทคโนโลยีการติดต่อสื่อสารอย่างเต็มที่ จนกระทั่งเอสโตเนียกลายเป็นชาติที่มีเครือข่ายอินเตอร์มากที่สุดชาติหนึ่งในยุโรป อย่างไรก็ตาม ภายหลังจากรัฐบาลเอสโตเนียได้รื้อถอนอนุสรณ์สถานและอนุสาวรีย์ทหารผ่านศึกของอดีตสหภาพโซเวียตที่ประกอบวีรกรรมในช่วงสงครามโลกครั้งที่ ๒ ออกไปจากสวนสาธารณะแห่งหนึ่งในเอสโตเนีย ทำให้รัฐบาลและประชาชนของสหพันธรัฐรัสเซียที่เคยเป็นใหญ่ในอดีตสหภาพโซเวียตเกิดความไม่พอใจ พวกเขาจึงร่วมมือกันทำให้ระบบอินเตอร์เน็ตของเอสโตเนียล่ม เพื่อแสดงออกถึงความไม่พอใจดังกล่าว แน่นอนที่สุดว่า รัฐบาลรัสเซียได้ปฏิเสธอย่างแข็งขันว่าไม่ได้มีส่วนเกี่ยวข้อง แต่ก็เชื่อได้ว่า นี่คือสงครามไซเบอร์ที่เกิดจากการโจมตีของต่างชาติในโลกไซเบอร์ ทำให้สังคมเครือข่ายของเอสโตเนียต่างตกเป็นเป้าหมายและได้รับผลกระทบในวงกว้างจนกระทั่งไม่สามารถให้บริการอินเตอร์เน็ตในระดับชาติได้เลยนานนับเดือน

ในปี ค.ศ.๒๐๐๘ ได้เกิดกรณีที่มีการใช้สงครามไซเบอร์ร่วมกับการใช้กำลังทางทหารในเวลาที่ใกล้เคียงกัน คือ ก่อนที่กองทัพรัสเซียจะใช้การโจมตีทางอากาศและรุกเข้าสู่จอร์เจียในเดือนสิงหาคม ค.ศ.๒๐๐๘ นั้น รัสเซียได้ทำสงครามไซเบอร์ต่อจอร์เจียโดยเริ่มโจมตีต่อเป้าหมายที่เป็นเวบไซต์ต่างๆ ของรัฐบาลจอร์เจีย สื่อ ระบบการติดต่อสื่อสาร ธนาคาร และบริษัทขนส่งต่างๆ เป็นต้น ทั้งนี้โดยอาศัยการปิดกั้นวงจรอินเตอร์เน็ตทุกช่องทางระหว่างจอร์เจียกับรัสเซีย และปิดกั้นวงจรอิเล็กทรอนิกส์ที่จะเข้าและออกจากจอร์เจียทั้งหมด ผลจากการโจมตีดังกล่าว จอร์เจียได้รับ

ผลกระทบเป็นอย่างมาก แม้ว่าผลกระทบดังกล่าวจะน้อยกว่าที่เอสโตเนียเคยได้รับในปี ค.ศ.๒๐๐๗ เนื่องจากสังคมอินเตอร์เน็ตของจอร์เจียมีความทันสมัยน้อยกว่า แต่การโจมตีดังกล่าวได้ส่งผลต่อขีดความสามารถของจอร์เจียต่อการสื่อสารกับโลกภายนอกและการสร้างการรับรู้ต่อสถานการณ์ที่แท้จริงในจอร์เจียของนานาชาติ เช่นเดียวกับกรณีของเอสโตเนีย แม้ว่ารัสเซียจะตกเป็นต้องสงสัยว่าเป็นผู้อยู่เบื้องหลังเหตุการณ์นี้มากที่สุด แต่ก็ไม่สามารถหาหลักฐานมายืนยันข้อสงสัยนี้ได้เลย อีกเหตุการณ์หนึ่งของการทำสงครามไซเบอร์ด้วยวัตถุประสงค์คล้ายกันได้เกิดขึ้นในเดือนธันวาคม ค.ศ.๒๐๐๘ ในยุทธการที่เรียกว่า “Operation Cast Lead” หรือที่รู้จักกันดีในนามของ “การสังหารหมู่ในฉนวนกาซา” (Gaza Massacre) ของทหารอิสราเอลต่อชาวปาเลสไตน์ในฉนวนกาซา โดยอิสราเอลได้ทำการโจมตีทั้งการโจมตีด้วยกำลังทหาร และไซเบอร์พร้อมกัน เพื่อทำลายการติดต่อสื่อสารของกลุ่มฮามาส (Hamas) ในฉนวนกาซา เป้าหมายของการโจมตีทั้งสองอย่างนี้ก็คือพลเรือนผู้ต้องสงสัยทั้งที่เป็นชาวปาเลสไตน์และชาวต่างชาติ ผลจากการโจมตีดังกล่าวได้ก่อให้เกิดการสูญเสียขึ้นเป็นจำนวนมากและสงครามไซเบอร์ได้ถูกตั้งคำถามในแง่ของจริยธรรมขึ้นเป็นครั้งแรกว่า “การทำสงครามไซเบอร์ควรมีข้อห้ามและข้อจำกัดอะไรบ้าง” ท้ายที่สุด ในปี ค.ศ.๒๐๐๙ ได้เกิดเหตุการณ์การโจมตีระบบเครือข่ายทางการเงินในลักษณะที่เรียกว่า “DDoS Attack” (Distributed Denial-of-Service Attack) โดยมีจุดประสงค์เพื่อให้ระบบหยุดการทำงานของเครื่องคอมพิวเตอร์เครื่องเดียวหรือทั้งระบบ เหตุการณ์นี้เกิดขึ้นเมื่อกลุ่มนักเจาะระบบคอมพิวเตอร์ไม่ทราบสัญชาติได้ถล่มเครือข่ายคอมพิวเตอร์และเว็บไซต์ของหน่วยงานรัฐบาลเกาหลีใต้ใช้งานไม่ได้นานกว่า ๔ ชั่วโมง ตราบจนถึงปัจจุบัน รัฐบาลเกาหลีใต้ก็ยังไม่ทราบว่าใครเป็นผู้กระทำ แม้ว่ารัฐบาลเกาหลีเหนือและสมาชิกองค์การอาชญากรรมในสหราชอาณาจักรจะตกเป็นผู้ต้องสงสัยมากที่สุดแต่รัฐบาลเกาหลีใต้ก็ไม่สามารถหาหลักฐานมาพิสูจน์ความจริงนี้ได้เลยตราบจนถึงปัจจุบัน

ในส่วนของผู้ให้บริการด้านความมั่นคงปลอดภัยโลกไซเบอร์อย่าง McAfee ซึ่งผู้ให้บริการโซลูชันด้านความมั่นคงปลอดภัยชื่อดัง ออกรายงาน “McAfee Labs Threats Report: November ๒๐๑๗” ประจำไตรมาสสุดท้ายของปี ๒๐๑๗ โดยใช้เครื่องมือที่เรียกว่า “Threat Intelligence Sharing” หรือการแบ่งปันข้อมูลภัยคุกคามอัจฉริยะ ซึ่งเป็นการรวบรวมข้อมูลภัยคุกคามจากแหล่งต่างๆ จากทั่วทุกมุมโลก ผ่านกระบวนการวิเคราะห์ต่างๆ เพื่อให้ทราบว่าขณะนี้องค์กรของเรากำลังเผชิญหน้ากับอะไร ผู้ที่อยู่เบื้องหลังคือใคร ต้องการทำอะไร ระบบไหนที่เป็นเป้าหมาย รวมไปถึงพฤติกรรมเชิงลึกของภัยคุกคามและผู้ที่อยู่เบื้องหลังเหล่านั้น เพื่อให้องค์กรสามารถหามาตรการควบคุมและรับมือกับภัยคุกคามไซเบอร์ต่างๆ ได้อย่างมีประสิทธิผลและทันท่วงที โดยมีการพัฒนามาอย่างต่อเนื่องเพื่อรับมือกับภัยคุกคามด้านไซเบอร์ที่นับวันจะทวีความรุนแรงยิ่งขึ้น รวมไปถึงเจาะลึกการโจมตีระดับโลกเมื่อปลายปี ๒๐๑๖ ที่ผ่านมาต่อเนื่องมาจนถึงปี

๒๐๑๗ นั่นคือ Mirai DDoS Botnet และสถิติของภัยคุกคามต่างๆ ที่ค้นพบในปี ๒๐๑๗ สรุปสถิติสำคัญของภัยคุกคามในปี ๒๐๑๗ พบว่า

(๑) มีภัยคุกคามใหม่มากกว่า ๒๐๐ รายการเกิดขึ้นทุกๆ ๑ นาที หรือเกือบ ๓ รายการทุกๆ วินาที ไตรมาสที่ ๔ ของปี ๒๐๑๗ พบเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยถูกประกาศสู่สาธารณะมากกว่า ๒๐๐ เหตุการณ์ และทั้งปี มากกว่า ๒๐๐ รวมมากกว่า ๑,๐๐๐ เหตุการณ์

(๒) จำนวนมัลแวร์ใหม่บน Mac OS เพิ่มขึ้น ๒๕% ในไตรมาสที่ ๔ และพุ่งสูงถึง ๗๕% เมื่อพิจารณาจากปี ๒๐๑๗ ทั้งปี มัลแวร์บนอุปกรณ์พกพามีปริมาณลดลง ๑๓% ในไตรมาสที่ ๔ และแต่กลับเพิ่มขึ้นถึง ๘๘% เมื่อพิจารณาทั้งปี โดยจำนวนมัลแวร์ทั้งหมดทั่วโลกเพิ่มปริมาณขึ้น ๒๕% ในปี ๒๐๑๗ คิดเป็นมากกว่า ๗๐๐ ล้านรายการ

(๓) สแปมบ็อต ๑๐ อันดับแรกก่อให้เกิดอีเมล์สแปมในไตรมาสที่ ๔ ลดน้อยกว่าปี ๒๐๑๖ ถึง ๒๒% คิดเป็น ๑๘๑ ล้านฉบับ รวมทั้งปีมากกว่า ๑,๐๐๐ ล้านฉบับ

(๔) จำนวน Ransomware ในปี ๒๐๑๗ เพิ่มขึ้นถึง ๗๒% อย่างไรก็ตาม จากการลดลงของ Locky และ CryptoWall ทำให้ปริมาณ Ransomware ใหม่ในไตรมาสที่ ๔ ลดลงถึง ๖๒%

จากการศึกษารายงานและสถิติที่ผู้เชี่ยวชาญด้านความปลอดภัยจากหน่วยงานและองค์กรที่มีชื่อเสียงและเป็นที่รู้จักในหลายประเทศทั่วโลกอย่าง Sophos, Trend Micro และ Symantec ที่ได้วิเคราะห์สถานการณ์ของภัยคุกคามทางอินเตอร์เน็ตในปี ๒๐๑๗ ที่ผ่านมาไว้ใกล้เคียงกัน ประกอบกับการติดตามรายงานและบทความที่กล่าวถึงภัยคุกคามที่ผ่านมาย้อนหลังไปในช่วง ๒-๓ ปีที่ผ่านมาแสดงให้เห็นว่า รูปแบบภัยคุกคามทางอินเตอร์เน็ตและเครือข่ายมีแนวโน้มที่กลุ่มอาชญากรไซเบอร์พยายามจะพัฒนาไปในทิศทางที่รุนแรงและซับซ้อนมากขึ้น

ดังนั้นจะเห็นได้ว่าภัยคุกคามที่เกิดขึ้นมีรูปแบบที่เปลี่ยนไปโดยถูกส่งมาในรูปของข้อมูลข่าวสาร ความรู้ และวิทยาการต่างๆ ซึ่งไหลบ่าเข้าสู่ประเทศไทยอย่างต่อเนื่องและไม่สามารถต้านทานได้อีกต่อไป องค์กรจึงไม่สามารถแก้ปัญหาด้านความมั่นคงรูปแบบใหม่ได้โดยวิธีเดิมๆ และตามลำพังได้อีกต่อไปการเผชิญภัยคุกคามรูปแบบใหม่ในยุคเศรษฐกิจฐานความรู้ องค์กรจำเป็นที่จะต้องปรับบทบาทให้มีขีดความสามารถหลากหลายมากขึ้น การพัฒนาความรู้แก่บุคลากรทุกระดับจึงเป็นปัจจัยที่สำคัญที่สุดเพื่อให้บุคลากรมีความคิดทันสมัยและทันโลก และที่สำคัญต้องพัฒนาให้บุคลากรมีความรู้ควบคู่กับปัญญา

๒. คำจำกัดความ

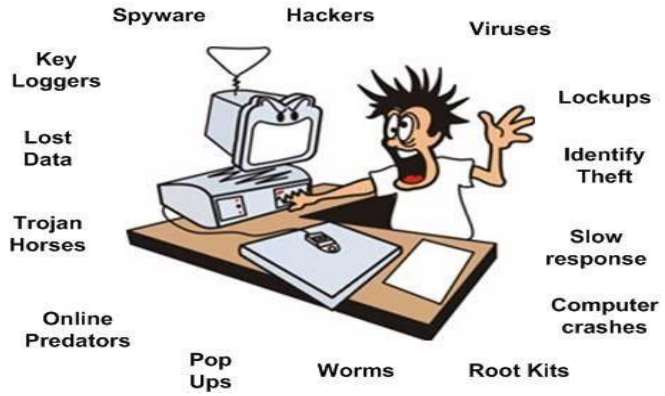
แม้คำว่า “ไซเบอร์” (Cyber) เป็นคำที่กร่อนมาจากคำว่า “ไซเบอร์เนติกส์” (Cybernetics) อันหมายถึง สิ่งที่เกี่ยวข้องกับระบบคอมพิวเตอร์และสังคมเครือข่ายสากล (เช่น ระบบอินเตอร์เน็ต (Internet)) และอาจหมายถึง สารสนเทศเสมือนจริงที่ถูกสร้างขึ้นหรือเกิดขึ้นเอง

แต่คำว่า “สงครามไซเบอร์” (Cyber War) หรือ “การทำสงครามไซเบอร์” (Cyber Warfare) กลับเป็นคำที่ให้ความหมายของคำๆ นี้ได้ยาก ความหมายของคำๆ นี้จึงขึ้นอยู่กับมุมมองของแต่ละบุคคลเป็นหลัก เช่น บางคนอาจให้ความหมายแคบๆ โดยบอกว่า “สงครามไซเบอร์” เป็นการปฏิบัติการทางทหารที่อาศัยหลักการที่เกี่ยวข้องกับสารสนเทศโดยที่ฝ่ายเราพยายามที่จะรู้ ขัดขวาง และทำลายสารสนเทศของฝ่ายตรงข้ามให้มากที่สุด ในขณะเดียวกันก็พยายามไม่ให้ฝ่ายตรงข้ามดำเนินการในลักษณะเดียวกันกับสารสนเทศของฝ่ายเรา หรือบางคนอาจให้ความหมายในวงกว้างมากขึ้นได้ว่า “สงครามไซเบอร์” ซึ่งเป็นการโจมตีโดยอาศัยการก่อวินาศกรรม (Sabotage) หรือการจารกรรม (Espionage) ต่อสารสนเทศของฝ่ายตรงข้ามผ่านทางระบบคอมพิวเตอร์หรือบนระบบสังคมเครือข่าย (Social Network) เพื่อบรรลุวัตถุประสงค์ทางการเมืองหรือธุรกรรมต่างๆ สำหรับการก่อวินาศกรรมสารสนเทศนั้นอาจเป็นกิจกรรมในลักษณะของการรบกวนด้วยการโจมตีระบบคอมพิวเตอร์หรือสังคมเครือข่ายเป้าหมายบนอินเตอร์เน็ตของกลุ่มนักเจาะระบบคอมพิวเตอร์หรืออาจเรียกว่า “อาชญากรคอมพิวเตอร์” เพื่อทำให้ระบบเป้าหมายปฏิเสธหรือหยุดการทำงานที่เรียกว่า “DoS Attack” (Denial-of-Service Attack) หรือในลักษณะของการโจมตีพร้อมๆ กันต่อระบบที่เป็นเป้าหมายเดียวกันโดยระบบที่ตกเป็นเหยื่อทั้งหมดจะสร้างข้อมูลขยะขึ้นมาแล้วส่งไปยังระบบที่เป็นเป้าหมายโดยเฉพาะอย่างยิ่งองค์กรทางความมั่นคงและธุรกิจออนไลน์ ทำให้ข้อมูลไหลเข้าสู่ระบบที่เป้าหมายด้วยปริมาณมหาศาลจนกระทั่งระบบเป้าหมายจะต้องทำงานหนักขึ้น ช้าลงเรื่อยๆ และเมื่อเกินกว่าระดับที่ระบบเป้าหมายจะรับได้ก็จะหยุดการทำงานในที่สุด เป็นต้น ในส่วนการจารกรรมข้อมูลสารสนเทศนั้นมักเกี่ยวข้องกับการค้นหาข้อมูลส่วนตัวของบุคคลที่เป็นเป้าหมาย (Doxing) การขโมยทรัพย์สินทางปัญญา และการสอดแนมระบบทางการเงินผ่านทางระบบออนไลน์ เป็นต้น โดยส่วนใหญ่การจารกรรมมักมีรูปแบบที่ไม่แน่นอนและอาจคาดเดาไม่ได้ว่าจะปรากฏอยู่ในรูปแบบใด

เนื่องจากสงครามไซเบอร์ (Cyber War) เป็นสงครามที่เกิดขึ้นในพื้นที่ที่เรียกว่า “ห้วงไซเบอร์” หรือ “โลกไซเบอร์” (Cyber Space) ซึ่งแตกต่างจากมิติของพื้นที่ทางบก ทางทะเล ทางอากาศ หรือห้วงคลื่นแม่เหล็กไฟฟ้า (Electromagnetic Spectrum) โลกไซเบอร์จึงมิได้เป็นส่วนหนึ่งของพื้นที่ตามธรรมชาติของโลก แต่เป็นพื้นที่ใดๆ ก็ได้ ที่มีเทคโนโลยีสารสนเทศอยู่ ดังนั้นความหมายของคำว่า “โลกไซเบอร์” จึงหมายถึง เครือข่ายที่มีการเชื่อมโยงกันของโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ อันประกอบด้วย อินเตอร์เน็ต (internet) เครือข่ายโทรคมนาคม (Telecommunication Networks) เครือข่ายเฉพาะภารกิจ (Mission-Specific Networks) เครือข่ายคอมพิวเตอร์ (Computers) และระบบต่างๆ ที่ฝังอยู่ในระบบคอมพิวเตอร์ (Computer Embedded Systems) ด้วยเหตุนี้ สภาพแวดล้อมของสงครามไซเบอร์จึงเป็นสภาพแวดล้อมเสมือนจริง (Virtual

Environments) อันเกิดจากข้อมูลที่ถูกจัดเก็บและข่าวสารที่ถูกประมวลผล และถูกถ่ายโอนผ่านเครือข่ายเหล่านี้ ด้วยเหตุนี้ ภัยคุกคามด้านไซเบอร์ (Cyber Threat) จึงเป็นสภาวการณ์หรือเหตุการณ์ใดๆ ที่อาจส่งผลกระทบอย่างร้ายแรงต่อความปลอดภัยของสารสนเทศที่อยู่ในระบบคอมพิวเตอร์หรือสังคมเครือข่ายจากการเข้าถึง (Access) การทำลาย (Destruction) การเปิดเผย (Disclosure) การปรับเปลี่ยน (Modification) ข้อมูลโดยไม่ได้รับอนุญาต และ/หรือการปฏิเสธการทำงานของระบบคอมพิวเตอร์หรือสังคมเครือข่ายดังกล่าว โดยทั่วไปแล้ว ภัยคุกคามด้านไซเบอร์ แบ่งออกเป็น ๒ ประเภท คือ (๑) การโจมตีด้านไซเบอร์ (Cyberattacks) ที่มุ่งเน้นในเรื่องการสร้างความเสียหาย (Damage) และการรบกวน (Disruption) ต่อระบบที่เป็นเป้าหมายเป็นหลัก และ (๒) การจารกรรมด้านไซเบอร์ (Cyber Espionage) ที่มุ่งเน้นการจัดเตรียมสารสนเทศที่จำเป็นต่อการใช้เพื่อการโจมตีระบบที่เป็นเป้าหมายต่อไป อย่างไรก็ตาม พบว่าแรงจูงใจต่อการทำสงครามไซเบอร์ (Motivations) อาจเกิดจากแรงจูงใจทางทหาร ทางพลเรือน กลุ่มนักเจาะระบบคอมพิวเตอร์ที่มีแรงจูงใจทางการเมือง ภาคเอกชน หรือกลุ่มนักวิจัยที่มิได้มุ่งหวังผลกำไรทางธุรกิจก็เป็นได้ รูปแบบทั่วไปของภัยคุกคามด้านไซเบอร์แสดงดังแผนภาพที่ ๒ - ๑

แผนภาพที่ ๒ - ๑ ภัยคุกคามด้านไซเบอร์



แนวคิดเรื่องความมั่นคงแห่งชาติ

แนวคิดเกี่ยวกับความมั่นคงแห่งชาติเป็นเรื่องที่มีความสำคัญเพราะผูกพันกับทุกสิ่งในสังคม อาร์โนล์ด วุฟเฟอร์ (Arnold Wolfers) ได้กล่าวไว้ว่าความมั่นคงแห่งชาติเป็นคำที่มีความหมายคลุมเครือ ไม่ชัด และมีผู้นิยามแนวคิดนี้ไว้ค่อนข้างหลากหลาย แนวคิดนี้นับว่าเป็นแนวคิดดั้งเดิมของประเทศทางยุโรปภายหลังการก่อตั้งประเทศเป็น“รัฐประชาชาติ” (Nation State) ระหว่างศตวรรษที่ ๑๗-๑๙ ความหมายของความมั่นคงแห่งชาติในความหมายกว้างๆ หมายถึง

ความอยู่รอดของชาติ กล่าวคือ ความสามารถของชาติหนึ่งในอันที่จะป้องกันตัวเองจากการรุกราน ด้วยกำลังทหารของชาติอื่นต่อชาติของตน (Rupert Emerson) ดังนั้นความมั่นคงจึงเกิดขึ้นเมื่อมีการใช้อำนาจของชาติ (National Power) ออกไปเพื่อให้บรรลุวัตถุประสงค์ของชาติในต่างประเทศอันเกี่ยวข้องกับการกำหนดสถานะและเงื่อนไขบางอย่างของระบบระหว่างประเทศเพื่อค้ำประกันและสนับสนุนให้ชาติมีความมั่นคงปลอดภัยในระดับที่น่าพอใจ หรือเรียกว่า “ความมั่นคงขั้นพื้นฐาน” ส่วน จอห์น เฮิร์ซ (John Herz) เห็นว่าแนวคิดเกี่ยวกับความมั่นคงแห่งชาติในช่วงแรกๆ จะจำกัดอยู่เพียงในกิจการของทหารหรือการใช้อำนาจแห่งชาติให้บรรลุผลอันสมบูรณ์ในสถานการณ์ความขัดแย้งระหว่างประเทศหรือสถานการณ์อันเร่งด่วนฉุกเฉิน อย่างไรก็ดี แนวคิดเกี่ยวกับความมั่นคงแห่งชาติก็ได้เปลี่ยนแปลงไปตามสภาพแวดล้อมกาลเวลา เมื่อมีสิ่งท้าทายทายใหม่ๆ ก้าวเข้ามามีอิทธิพลและมีผลกระทบต่อความเป็นชาติ แนวคิดเกี่ยวกับความมั่นคงแห่งชาติได้ขยายครอบคลุมถึงความสัมพันธ์ระหว่างสภาวะแวดล้อมภายในประเทศหลายๆ ด้าน คือปัจจัยทางการเมือง เศรษฐกิจ และสังคมจิตวิทยา (ฉลองขวัญ อุดทะยอด, ๒๕๔๒: ๑๓-๒๓)

ส่วนแนวความคิดและนิยามของความมั่นคงแห่งชาติในบริบทของประเทศไทยนั้น พระราชบัญญัติว่าด้วยการบริหารราชการในสถานการณ์ฉุกเฉิน พ.ศ.๒๔๘๕ ได้ให้นิยามความมั่นคงแห่งชาติเอาไว้ด้วยว่า “ความมั่นคงหรือความปลอดภัยแห่งราชอาณาจักร หมายความว่า การให้เอกราชของชาติหรือสวัสดิภาพของประชาชนอยู่ในความมั่นคงและปลอดภัย รวมตลอดถึงการให้ประเทศดำรงอยู่ในการปกครองระบอบประชาธิปไตยภายใต้รัฐธรรมนูญแห่งราชอาณาจักร” ความมั่นคงแห่งชาติ หมายถึง สภาวะที่ทำให้ประชาชนในชาติสามารถดำรงชีวิตอยู่ด้วยความมั่นใจในความปลอดภัยจากอันตราย ปราศจากการตื่นตัวและความวิตกกังวลต่างๆ และต้องมีองค์ประกอบ ๔ ประการ คือ ความมั่นคงทางด้านสังคม ความมั่นคงทางด้านเศรษฐกิจ ความมั่นคงทางด้านการเมือง และความมั่นคงทางด้านการทหาร โดยองค์ประกอบทั้ง ๔ ด้านนั้นต้องมีความมั่นคงในตัวเองประการหนึ่ง และอีกประการหนึ่งจะต้องสนับสนุนซึ่งกันและกันด้วย หากมีความขัดแย้งใดๆ เกิดขึ้น ก็สามารถทำความเข้าใจกันหรือประสานผลประโยชน์กัน เพื่อความอยู่รอดปลอดภัยของชาติ (สมชัย รักวิจิตร, ๒๕๒๑: ๑-๑๐) องค์ประกอบของความมั่นคงทั้ง ๔ ด้าน อาจแยกอธิบายได้ดังนี้ ๑) ความมั่นคงทางด้านเศรษฐกิจ โดยปกติจะพิจารณาเรื่องที่เกี่ยวกับฐานะทางเศรษฐกิจของประเทศเป็นสำคัญอันได้แก่ ความเป็นปึกแผ่นทางด้านการค้า การอุตสาหกรรม และการเงิน ตลอดจนการกินดีอยู่ดีของประชาชนในชาตินั้น เป็นต้น ๒) ความมั่นคงทางด้านสังคม–จิตวิทยา คือ การพิจารณาถึงความปลอดภัยในชีวิตและทรัพย์สินของประชาชน และการได้รับความคุ้มครองจากรัฐและเจ้าหน้าที่ของรัฐอย่างเพียงพอ สามารถดำรงชีวิตอยู่ได้ด้วยความมั่นใจในความปลอดภัยปราศจากอันตรายและปราศจากความตื่นกลัวและความวิตกกังวลต่างๆ นอกจากนี้แล้วยัง

หมายความรวมไปถึงความเป็นธรรมในสังคมด้วย (Social Justification) ซึ่งหมายถึงความเป็นธรรมที่ได้รับจากกระบวนการยุติธรรมของรัฐเป็นสำคัญ ๓) ความมั่นคงทางด้านการเมือง แบ่งออกได้เป็น ๒ ประการ คือ ความมั่นคงทางด้านการเมืองภายในประเทศและความมั่นคงด้านการเมืองระหว่างประเทศ สำหรับความมั่นคงทางด้านการเมืองภายในประเทศที่สำคัญ ได้แก่ ความศรัทธาของประชาชนส่วนใหญ่ในประเทศ ซึ่งพร้อมที่จะให้การสนับสนุนต่อระบบการปกครองและการบริหารงานของรัฐบาลที่เป็นอยู่ในขณะนั้นว่ามีมากน้อยเพียงใด ส่วนความมั่นคงทางดเนการเมืองระหว่างประเทศนั้นจะขึ้นอยู่กับนโยบายด้านการเมืองระหว่างประเทศของรัฐบาลเป็นสำคัญ กล่าวคือ จะต้องเป็นไปในลักษณะที่ช่วยให้ประเทศชาติได้รับผลประโยชน์ทั้งในด้านเศรษฐกิจ การเมือง การทหาร และสังคมจิตวิทยา โดยเสริมสร้างมิตรให้มากและหลีกเลี่ยงที่จะสร้างศัตรูโดยไม่จำเป็น อนึ่ง การดำเนินนโยบายด้านการเมืองระหว่างประเทศจะได้รับผลอย่างเต็มที่จะต้องสร้างความมั่นคงภายในประเทศให้สูงขึ้นเสียก่อน และ ๔) ความมั่นคงทางด้านการทหาร หมายถึง การที่ประเทศมีกำลังทหารอาวุธยุทโธปกรณ์ที่มีคุณภาพในการป้องกันประเทศและรักษาความสงบสุขภายในประเทศอย่างเพียงพอ และจะต้องมีอุดมการณ์ มีวินัย มีขวัญกำลังใจสูง รวมทั้งมีความเป็นอันหนึ่งอันเดียวกัน และสามารถเอาชนะการ คุกคามทั้งภายในและภายนอกประเทศได้

กล่าวโดยสรุปแล้วความมั่นคงของชาติของสังคมใดสังคมหนึ่งจะประกอบด้วยความมั่นคงในองค์ประกอบ ๔ ด้าน ได้แก่

๑. ความมั่นคงของชาติด้านเศรษฐกิจ หมายถึง สภาพการณ์ทางเศรษฐกิจที่ทำให้ประชาชนมีงานทำและยอมรับนับถือระบบเศรษฐกิจของประเทศ สามารถยกฐานะทางเศรษฐกิจทั้งส่วนตัวและส่วนรวมให้สูงขึ้นได้ในอัตราที่เหมาะสม โดยที่ฐานะทางเศรษฐกิจและสังคมไม่มีความแตกต่างเหลื่อมล้ำกันมากนัก ประเทศสามารถรักษาเสถียรภาพทางการผลิตการค้า การเงินและราคา มีระบบภาษีอากรที่เหมาะสมเป็นธรรมสามารถพัฒนาเศรษฐกิจตามแผนที่วางไว้อย่างมีประสิทธิผล มีอิสระทางเศรษฐกิจจากต่างประเทศมีความสามารถทางอุตสาหกรรม พาณิชยกรรม ตลอดจนนวิทยา และเทคโนโลยี

๒. ความมั่นคงของชาติด้านสังคม หมายถึง สถานภาพทางด้านสังคมที่ทำให้ประชาชนสามารถครองชีวิตอยู่ได้ด้วยความปกติสุข มีความปลอดภัยในชีวิตและทรัพย์สิน ได้รับความเป็นธรรมจากกระบวนการยุติธรรมและความเป็นธรรมในการดำเนินชีวิต มีความเสมอภาคและภราดรภาพ ประชาชนมีความรู้ความสามารถ มีวัฒนธรรม จริยธรรม และศีลธรรม รวมทั้งมีความรับผิดชอบต่อหน้าที่พลเมืองต่อสังคม ตลอดจนมีความสำนึกในความเป็นชาติและยึดมั่นในอุดมการณ์ของชาติ

๓. ความมั่นคงทางด้านการเมือง แบ่งออกได้เป็น ๒ ประการ คือ ความมั่นคงทางด้านการเมืองภายในประเทศและความมั่นคงด้านการเมืองระหว่างประเทศ สำหรับความมั่นคงทางด้านการเมืองภายในประเทศที่สำคัญ ได้แก่ ความศรัทธาของประชาชนส่วนใหญ่ในประเทศ ซึ่งพร้อมที่จะให้การสนับสนุนต่อระบบการปกครองและการบริหารงานของรัฐบาลที่เป็นอยู่ในขณะนั้นว่ามีมากน้อยเพียงใด ความมั่นคงทางด้านการเมืองระหว่างประเทศนั้นจะขึ้นอยู่กับนโยบายด้านการเมืองระหว่างประเทศของรัฐบาลเป็นสำคัญ กล่าวคือ จะต้องเป็นไปในลักษณะที่ช่วยให้ประเทศชาติได้รับผลประโยชน์ทั้งในด้านเศรษฐกิจ การเมือง การทหาร และสังคมจิตวิทยา โดยเสริมสร้างมิตรให้มากและหลีกเลี่ยงที่จะสร้างศัตรูโดยไม่จำเป็น อนึง การดำเนินนโยบายด้านการเมืองระหว่างประเทศจะได้รับผลอย่างเต็มที่จะต้องสร้างความมั่นคงภายในประเทศให้สูงขึ้นเสียก่อน

๔. ความมั่นคงของชาติทางด้านการทหาร หมายถึง สภาพการณ์ด้านการทหารที่แสดงให้เห็นถึงความเข้มแข็งหรือแสนยานุภาพกำลังรบของชาติ ความพร้อมรบ ความมีประสิทธิภาพของอาวุธยุทโธปกรณ์ และการใช้อาวุธ การมีวินัย มีขวัญกำลังใจ และกำลังรบอื่นๆ มีการจัดการฝึกการศึกษายุทธศาสตร์ และยุทธวิธีที่สามารถจะเอาชนะศัตรูผู้รุกรานทั้งจากภายในและภายนอกประเทศได้

ในห้วงเวลาที่ผ่านมา สถานการณ์โลกทุกๆ ด้านเปลี่ยนแปลงอย่างรวดเร็ว เนื่องมาจากผลของกระแสโลกาภิวัตน์และการสิ้นสุดของยุคสงครามเย็น สภาวการณ์ดังกล่าวมีผลกระทบโดยตรงกับความมั่นคงแห่งชาติของประเทศต่างๆ ในทุกด้าน ไม่ว่าจะเป็นด้านการเมือง เศรษฐกิจ สังคมจิตวิทยา การป้องกันประเทศ และวิทยาศาสตร์เทคโนโลยี การพลังงาน และสิ่งแวดล้อม การกำหนดและพัฒนานโยบายความมั่นคงแห่งชาติให้สอดคล้องกับสถานการณ์โลกและสภาวะแวดล้อมของประเทศทั้งภายในและภายนอก เพื่อให้ประเทศมีสมดุลในความมั่นคงแห่งชาติทุกด้านสามารถรักษาไว้ซึ่งผลประโยชน์แห่งชาติ และบรรลุวัตถุประสงค์แห่งชาติได้ จึงเป็นเรื่องท้าทายการบริหารและการจัดการของรัฐบาล สภาความมั่นคงแห่งชาติเป็นกลไกหนึ่งในการบริหารงานราชการของรัฐบาล มีหน้าที่ในการพิจารณาเสนอแนะต่อคณะรัฐมนตรีเกี่ยวกับนโยบายความมั่นคงแห่งชาติด้านต่างๆ เพื่อให้ประสานสอดคล้องเป็นไปในแนวทางเดียวกัน และเป็นผลดีต่อความมั่นคงแห่งชาติ รวมทั้งมีหน้าที่พิจารณาในเรื่องเกี่ยวกับความมั่นคงแห่งชาติตามแต่คณะรัฐมนตรีจะมอบหมาย การพิจารณากำหนดและพัฒนานโยบายความมั่นคงแห่งชาติ เป็นเรื่องที่มีความซับซ้อนและต้องมีการวิเคราะห์โดยละเอียดตามสถานการณ์และสภาวะแวดล้อมที่เป็นอยู่ นักวิชาการและนักบริหารส่วนใหญ่มีความเห็นสอดคล้องกันว่า สภาวะแวดล้อมด้านความมั่นคงระหว่างประเทศตลอดจนสภาวะแวดล้อมและสถานการณ์หรือเงื่อนไขต่างๆ ภายในประเทศได้มีการเปลี่ยนแปลง

รูปแบบและมิติไปจากที่เคยเป็นอยู่ ส่งผลให้ภัยคุกคามด้านต่างๆ เปลี่ยนแปลงตามไปด้วย การจัดการกับภัยคุกคามและปัจจัยเสี่ยงต่างๆ ซึ่งเป็นที่มาของปัญหาของชาติ จึงต้องดำเนินการในลักษณะองค์รวมแบบบูรณาการ ครอบคลุมทุกด้าน และสอดคล้องประสานกันอย่างเหมาะสม เพราะฉะนั้นบทบาทการดำเนินงานของสำนักงานสภาความมั่นคงแห่งชาติในฐานะองค์กรรับผิดชอบหลักในการกำหนดและพัฒนานโยบายความมั่นคงของชาติ จึงมีความสำคัญอย่างยิ่งที่จะต้องพิจารณาอย่างรอบคอบให้สอดคล้องกับมิติของสภาวะแวดล้อมด้านความมั่นคงทั้งภายในประเทศและต่างประเทศ

จากการศึกษาทบทวนแนวคิดเกี่ยวกับความมั่นคงแห่งชาติ สรุปได้ว่า ความมั่นคงแห่งชาติ หมายถึง สภาวะที่ทำให้ประชาชนในชาติสามารถดำรงชีวิตอยู่ด้วยความมั่นใจในความปลอดภัยจากอันตราย ปราศจากการตื่นกลัวและความวิตกกังวลต่างๆ และต้องมีองค์ประกอบ ๔ ประการ คือ ความมั่นคงทางด้านสังคม ความมั่นคงทางด้านเศรษฐกิจ ความมั่นคงทางด้านการเมือง และความมั่นคงทางด้านการทหาร โดยองค์ประกอบทั้ง ๔ ด้าน นั้นต้องมีความมั่นคงในตัวเองประการหนึ่ง และอีกประการหนึ่งจะต้องสนับสนุนซึ่งกันและกันด้วย หากมีความขัดแย้งใดๆ เกิดขึ้นก็สามารถทำความเข้าใจกันหรือประสานผลประโยชน์กัน เพื่อความอยู่รอดปลอดภัยของชาติ ส่วนภัยคุกคามต่อความมั่นคงของชาติมี ๒ ทาง คือ ภัยคุกคามจากภายใน เป็นปัญหาทางดด้านการเมืองภายในประเทศ ปัญหาเศรษฐกิจ ปัญหาพื้นที่ด้อยพัฒนา ปัญหาชายแดน ปัญหาทางด้านสังคมและจิตวิทยา และปัญหาทรัพยากรและสิ่งแวดล้อม ในขณะที่ภัยคุกคามจากภายนอก เช่น ปัญหาความขัดแย้งของสังคมโลก ปัญหากลุ่มประเทศมุสลิม และปัญหาความสัมพันธ์กับประเทศเพื่อนบ้าน เป็นต้น ซึ่งพลังอำนาจของชาติจะเป็นขีดความสามารถทำให้ประเทศชาติมีความมั่นคงผ่านพ้นจากภัยคุกคามได้

แนวคิดเรื่องผลประโยชน์แห่งชาติ

สำหรับความหมายของผลประโยชน์แห่งชาติในเชิงลึกอาจออกแบ่งได้เป็นสองความหมาย ตามนัยที่ถูกใช้ในทางการเมืองระหว่างประเทศ (Griffith, Martin., Callaghan, Terry O. and Roach, Steven C., 2008: 216-218) กล่าวคือ

ความหมายแรก ถูกใช้เป็นเครื่องมือในการวิเคราะห์เป้าหมาย (Goals) หรือวัตถุประสงค์ (Objectives) ของนโยบายต่างประเทศ ดังที่ James N. Rosenau กล่าวถึงความเป็นมาของผลประโยชน์แห่งชาติ ว่าได้ถูกใช้ไปในการวิเคราะห์การเมืองระหว่างประเทศเพื่อใช้เป็นเครื่องมือในการบรรยายและอธิบายเกี่ยวกับการดำเนินนโยบายต่างประเทศ โดยการประกาศถึงเป้าหมายของประเทศที่ได้เริ่มต้นมาตั้งแต่ศตวรรษที่ ๑๖ โดยในประเทศอิตาลีได้เน้นในเรื่องอำนาจ

อธิปไตย (Sovereignty) และความชอบธรรม (Legitimacy) อันเป็นผลสืบเนื่องมาจากกำลังอำนาจ (Power) ของประเทศในการเมืองระหว่างประเทศ ซึ่งต่อมาในศตวรรษที่ ๑๗ ในวงการเมืองประเทศอังกฤษได้กล่าวถึงผลประโยชน์แห่งชาติในเรื่องการมีเกียรติยศของประเทศ (National Honor) และผลประโยชน์สาธารณะ (Public Interest) รวมทั้งเจตนารมณ์ (General Will) ของประเทศและต่อมาก็ได้ถูกนำไปบัญญัติไว้ในรัฐธรรมนูญของสหรัฐอเมริกส (Rosenau, James N., 1980: 283-293)

ส่วนอีกความหมาย ได้ถูกนำไปใช้เป็นแนวคิดเกี่ยวกับวาทะกรรมทางการเมือง (Political Discourse) เพื่อวิเคราะห์และสนับสนุนการกำหนดนโยบายระหว่างประเทศ ดังกรณีที่ Hans J. Morgenthau ได้วิเคราะห์ระบบการเมืองระหวางประเทศในการแสดงพฤติกรรมทางการเมืองของประเทศด้วยการใช้กำลังอำนาจของประเทศ (Morgenthau, Hans J., 2005: 4-16) โดยเฉพาะในมิติทางการทหารและทางเศรษฐกิจที่สามารถครอบงำปัจจัยด้านอื่นๆ ในการกำหนดนโยบายระหว่างประเทศของผู้กำหนดนโยบายโดยคำนึงถึงผลประโยชน์แห่งชาติที่ถูกผลักดันจากเงื่อนไขที่เป็นนโยบายทางยุทธศาสตร์ (Strategic Diplomatic Milieu) และได้นำไปสู่การพึ่งพาอาศัยกันอย่างสลับซับซ้อน (Complex Interdependence) ในสังคมโลก (World Society) (Evans, Graham and Newnham, Jeffrey, 1998: 345) ซึ่งปัจจุบันสังคมโลกมีความสัมพันธ์ระหว่างประเทศในลักษณะที่เป็นเครือข่าย โดยมีการผนึกกำลังเป็นประชาคมในภูมิภาคต่างๆ รวมทั้งมีกลไกการจัดระเบียบของการเป็นสมาชิกและมีรูปแบบของการเป็นหุ้นส่วนทางยุทธศาสตร์ (Strategic Partnership) เพื่อความร่วมมือโดยมีเป้าหมายร่วมกัน (Common Goals) และยอมรับในผลประโยชน์ร่วมกัน (Martinelli, Alberto, 2005: 241-260)

ความหมายของผลประโยชน์แห่งชาติทั้งสองกรณีดังกล่าวเกี่ยวข้องกับพื้นฐานการตกลงใจในการดำเนินนโยบายของประเทศ โดยมีความสัมพันธ์กับสภาวะแวดล้อมภายนอกที่กระทบต่ออำนาจอธิปไตยของประเทศและการดำเนินนโยบายต่างประเทศรวมทั้งปัจจัยภายในประเทศจากความหลากหลายของผลประโยชน์ที่เป็นสาธารณะ อันทำให้เข้าใจถึงองค์ประกอบของผลประโยชน์แห่งชาติ ซึ่งประกอบด้วย การดำรงอยู่ของประเทศ (Self Preservation) ความมั่นคงปลอดภัย (Security) การกินดีอยู่ดีของประชาชน (Well - Being) การส่งเสริมและรักษาเกียรติภูมิ (Prestige) การเผยแพร่และรักษาอุดมการณ์ (Ideology) ตลอดจนการแสวงหาและเพิ่มพูนกำลังอำนาจของประเทศ (Lerche, Charles O. and Said, Abdul A., 1995: 28)

คำว่า “ผลประโยชน์แห่งชาติ” ในภาษาอังกฤษนั้นจะใช้คำว่า “National Interest” โดยเว็บวิกิพีเดีย ได้ให้ความหมายไว้ว่า “The national interest is a country's goals and ambitions whether economic, military, or cultural.” หรือในพจนานุกรม MSN Encarta ได้ให้ความหมายไว้ว่า

“things of benefit to nation: actions, circumstances, and decisions regarded as benefiting a particular nation”

ส่วนคำว่า “ผลประโยชน์แห่งชาติ” ในภาษาไทยนั้นเอกสาร คู่มือเรื่องการพัฒนายุทธศาสตร์ชาติ ของวิทยาลัยป้องกันราชอาณาจักร ได้ให้ความหมายไว้ว่า “ผลประโยชน์แห่งชาติ หมายถึง ความต้องการหรือความปรารถนาอันสำคัญยิ่งของประชาชนส่วนรวม ความต้องการนั้นจึงมีลักษณะกว้างและค่อนข้างถาวรและเมื่อได้พิจารณากำหนดขึ้นแล้ว ก็จะต้องมุ่งกระทำโดยต่อเนื่องเพื่อให้บรรลุผล คำว่า “ความต้องการ” มีความหมายรวมทั้งความต้องการ (Want) โดยทั่วไปและความจำเป็น (Need) ที่ขาดเสียไม่ได้ ส่วนคำว่า “ประชาชนส่วนรวม” มีความหมายว่าชาติ คือประชาชนส่วนรวมไม่ใช่บุคคลใดหรือกลุ่มบุคคลใดโดยเฉพาะ

นอกจากนี้ในเอกสารเล่มเดียวกันยังได้จำแนกผลประโยชน์แห่งชาติออกเป็น ๓ ลักษณะ คือ

๑. จำแนกตามลักษณะความสำคัญ (Degree of Primacy) ได้แก่ ผลประโยชน์แห่งชาติที่มีความสำคัญสูงสุด (Vital Interests) กับผลประโยชน์แห่งชาติระดับรอง (Secondary Interests)

๒. จำแนกตามลักษณะความยืนยง (Degree of Permanent) ได้แก่ ผลประโยชน์แห่งชาติถาวร (Permanent Interests) กับผลประโยชน์แห่งชาติไม่ถาวร (Variable Interests)

๓. จำแนกตามลักษณะความเจาะจง (Degree of Generality) ได้แก่ ผลประโยชน์แห่งชาติทั่วไป (General Interests) กับผลประโยชน์แห่งชาติเฉพาะ (Specific Interests)

สำหรับประเทศไทยการกำหนดผลประโยชน์แห่งชาตินั้นจะมีหน่วยงานที่รับผิดชอบคือ สภาความมั่นคงแห่งชาติ (สมช.) โดยกำหนดไว้ในนโยบายความมั่นคงแห่งชาติ ที่ผ่านมาในอดีตนั้น ได้กำหนดไว้ ๕ ข้อ คือ

๑. การมีเอกราช อธิปไตย และบูรณภาพแห่งอาณาเขต

๒. การดำรงอยู่อย่างมั่นคงของชาติและประชาชนจากการคุกคามทุกรูปแบบ

๓. ความปลอดภัย ความอยู่ดีมีสุข ความเป็นธรรม และการมีเกียรติ และศักดิ์ศรีของความเป็นมนุษย์

๔. การอยู่ร่วมกันอย่างสันติสุขกับประเทศเพื่อนบ้าน และ

๕. การมีเกียรติและศักดิ์ศรีในประชาคมระหว่างประเทศ

แต่ในนโยบายความมั่นคงแห่งชาติ พ.ศ.๒๕๕๐ – ๒๕๕๔ (ฉบับปัจจุบัน) ได้กำหนดผลประโยชน์แห่งชาติใหม่ครอบคลุมทั้งภัยคุกคามในรูปแบบเดิม และภัยคุกคามรูปแบบใหม่ จำนวน ๗ ประการ ได้แก่

๑. การมีเอกราช อธิปไตย และบูรณภาพแห่งเขตอำนาจรัฐการดำรงอยู่อย่างมั่นคงยั่งยืน ของสถาบันหลักของชาติ

๒. ความปรองดอง ความสามัคคีของคนในชาติ

๓. การดำรงอยู่อย่างมั่นคงของชาติและประชาชนจากการคุกคามทุกรูปแบบ

๔. ความปลอดภัย ความเป็นธรรม และความอยู่ดีมีสุขของประชาชน การมีเกียรติและศักดิ์ศรีของความเป็นมนุษย์

๕. การดำรงอยู่อย่างมั่นคงของฐานทรัพยากรธรรมชาติและสิทธิเหนือทรัพยากรชีวภาพของชาติ

๖. การอยู่ร่วมกันอย่างสันติสุขกับประเทศเพื่อนบ้าน

๗. การมีเกียรติและศักดิ์ศรีในประชาคมระหว่างประเทศ

ทุกวันนี้ถ้าคนไทยทุกคนหันไปมองทางไหนก็มักจะพบแต่ปัญหา จนกลายเป็นเรื่องที่หลายคนจะตอบได้ว่าประเทศไทยของเราจะเดินหน้าไปอย่างไรกันดี เพราะปัญหาทุกอย่างในวันนี้ล้วนแต่ต้องการทางออกจากทุกฝ่าย แต่ดูเหมือนว่าเรายังหาทางออกไม่ได้สักเรื่อง ไม่ว่าจะเป็นเรื่องของความสมัครสมานสามัคคีของคนในชาติหรือปัญหาปากท้องของประชาชน หรือจะเป็นเรื่องความไม่ลงตัวทางการเมืองจนไม่มีเสถียรภาพ ซึ่งความจริงแล้วถ้าหาผู้ที่เกี่ยวข้องและคนไทยทุกคนในชาติต่างคิดถึงผลประโยชน์แห่งชาติเป็นที่ตั้งแล้ว ทุกอย่างย่อมจะไม่เป็นอย่างที่เป็นอยู่ทุกวันนี้ และประเทศไทยเราคงเดินไปข้างหน้าอย่างที่ประเทศอื่นยากที่จะทัดเทียม การที่ประเทศไทยเราเป็นอย่างนี้นั้นส่วนหนึ่งแล้วมาจากคนไทยเราไม่เคยทราบว่าผลประโยชน์แห่งชาติไทยคืออะไร ทำให้ขาดการปลูกฝังและสร้างจิตสำนึกของคนในชาติให้ร่วมแรงร่วมใจกันทำในสิ่งที่มุ่งไปสู่สิ่งเดียวกันคือ ผลประโยชน์แห่งชาติ

จากที่กล่าวมาข้างต้น จะเห็นภาพของผลประโยชน์แห่งชาติตามหลักแนวคิดและผลประโยชน์แห่งชาติของทุกชาติโลกซึ่งก็รวมถึงประเทศไทยได้ดียิ่งขึ้น อย่างไรก็ดีจะมีคำถามที่ตามมาคือ คนไทยเราได้คำนึงผลประโยชน์แห่งชาติกันมาน้อยเพียงไร ซึ่ง ณ วันนี้สามารถตอบแทนได้อย่างเต็มปากว่า “ไม่” เพราะดูได้จากสถานการณ์ปัจจุบันที่กลุ่มการเมืองต่างฝ่ายต่างมองแต่ในส่วนของตนเอง และไม่พยายามยอมรับฟังความคิดเห็นจากคนที่มีความเห็นที่แตกต่าง เอาแต่ได้จนทำให้ต่างฝ่ายพยายามสร้างการยอมรับความคิดของตนด้วยการหาแนวร่วม ใช้มวลชน กลุ่มคนมาสนับสนุนแนวความคิดของตน และกลุ่มการเมืองเหล่านี้ก็ใช้มวลชนในการขับเคลื่อนเพื่อผลประโยชน์ที่กลุ่มตัวเองต้องการ โดยไม่คำนึงถึงผลเสียหายหรือความสูญเสียที่จะเกิดขึ้นตามมา ความจริงแล้ววันนี้ถ้าเราคนไทยทุกคนมีความอดทนอดกลั้น รู้จักยอมรับในความแตกต่าง ยอมมองข้ามในบางเรื่องแล้ว สังคมไทยน่าจะมีทิศทางไปในทางที่ดี ความเสียหายและการสูญเสียคงจะ

ไม่เป็นสิ่งที่เกิดขึ้น และยังเลยไปถึงการยุติความขัดแย้งอยู่ร่วมกันอย่างสมานฉันท์ในที่สุด เพราะฉะนั้นถ้าเราอย่างจะอยู่ร่วมกันอย่างสันติ มีความสงบสุข ประเทศไทยสามารถก้าวไปข้างหน้าได้ คำตอบเดียวในวันนี้ที่จะเป็นทางออกที่ดีที่สุดสำหรับคนไทยทุกคนคือ “มีสติและการถือเอาผลประโยชน์แห่งชาติที่เป็นตั้ง” นั่นเอง

ทฤษฎีความขัดแย้ง

๑. แนวคิดที่เกี่ยวกับความขัดแย้งด้านสังคมวิทยาและมานุษยวิทยา

หัวใจสำคัญของแนวคิดกลุ่มนี้คือ การขัดแย้งนำไปสู่การเปลี่ยนแปลงที่ดีขึ้น ความขัดแย้งเป็นปรากฏการณ์ที่มีอยู่อย่างแพร่หลายทั่วไปเราจึงไม่ควรมอง พฤติกรรมขัดแย้งว่าเป็นพฤติกรรมที่ไม่ดีหรือเป็นปรากฏการณ์ที่ผิดปกติ ทฤษฎีความขัดแย้งทางสังคม จึงมีแนวความคิดว่าสังคมนั้นตั้งอยู่บนพื้นฐานของการแบ่งแยก (Division) อันเกิดจากความไม่เท่าเทียมกันทางสังคม วิธีการสำคัญที่นักปราชญ์และนักสังคมศาสตร์ใช้วิเคราะห์ปรากฏการณ์ที่ขัดแย้งต่างๆ คือ วิธีการที่เรียกว่า “ไดอาเล็คติค” (Dialectic Method) เป็นวิธีการที่ใช้มาตั้งแต่สมัยกรีกโบราณ สมัยโซเครตีส (Socrates) ใช้เป็นวิธีถามและตอบเพื่อแสวงหาความรู้ที่แจ่มแจ้งและสมบูรณ์ทำให้เกิดการสมเหตุสมผลมากขึ้น (Logical Consistency) ต่อมานักปรัชญาชาวของโลกเยอรมันได้พัฒนา Dialectic สมัยใหม่ที่ว่าด้วยข้อเสนอเบื้องต้น (Thesis) และข้อเสนอแย้ง (Anti Thesis) และคานท์ (Kant) แสดงความเห็นว่าสาเหตุของความไม่กลมกลืนหรือไม่คล้องจองกันเป็นเพราะระบบความคิดของคนเรา ซึ่งมีอิทธิพลมากกว่าอิทธิพลทางสังคมและวัฒนธรรม ความขัดแย้งที่มีอยู่ในตัวของบุคคลเป็นสาเหตุสำคัญที่นำไปสู่ความขัดแย้งภายนอกอื่นๆ หากทำความเข้าใจเรื่องความขัดแย้งที่มีอยู่ในตัวบุคคลได้แล้วและหาทางขจัดความขัดแย้งนั้นออกไป ความขัดแย้งทางสังคมและวัฒนธรรมกอาจหายไปได้นักทฤษฎีความขัดแย้งด้านสังคมวิทยาที่สำคัญ ๓ คน ได้แก่

Marx (อ้างถึงใน เสริมศักดิ์ วิศาลาภรณ์, ๒๕๓๔: ๔๒) เป็นผู้ที่ใช้วิธีวิเคราะห์แบบ Dialectical วิเคราะห์การเปลี่ยนแปลงของทุกๆ สังคมว่า เกิดจากความสัมพันธ์ของ “อำนาจการผลิต” ซึ่งได้แก่ ที่ดิน ทุน เทคโนโลยีและการจัดการด้านแรงงานกับ “ความสัมพันธ์ทางสังคมของการผลิต” อันได้แก่ เจ้าของปัจจัยการผลิต และผู้ใช้แรงงาน ซึ่งความขัดแย้งที่เกิดขึ้นมักเกิดจากความขัดแย้งระหว่างชนชั้นเจ้าของปัจจัยการผลิตกับชนชั้นผู้ใช้แรงงาน

Sills (1968: 142) อธิบายว่า ความขัดแย้งก่อให้เกิดผลทั้งด้านลบและด้านบวก ความขัดแย้งเป็นส่วนหนึ่งของกระบวนการขัดเกลาทางสังคม ถือเป็นสภาวะหนึ่งของมนุษย์ความขัดแย้งสามารถแก้ปัญหาความแตกแยกและทำให้เกิดความสามัคคีภายในกลุ่มได้เพราะในกลุ่มหนึ่งๆ ย่อมมีทั้งความเป็นมิตรและความเป็นศัตรูอยู่ด้วยกัน ดังนั้นความขัดแย้งจึงเป็นตัวสนับสนุนให้เกิดการ

เปลี่ยนแปลงทางสังคม ได้เสนอเพิ่มเติมว่าความขัดแย้งทำให้เกิดการแบ่งกลุ่ม ลดความเป็นปรปักษ์ต่อกันอันจะพัฒนาสู่ความร่วมมือได้หรือทำให้เกิดความแปลกแยกได้

Dahrendorf (1968: 125) นักสังคมวิทยาชาวเยอรมันที่ปฏิเสธแนวคิดของมาร์กซ์ เรื่องความขัดแย้งระหว่างชนชั้น Dahrendorf อธิบายคุณลักษณะ “ความขัดแย้ง” ว่ามีลักษณะสอดคล้องกับทุกสังคมที่มีการเปลี่ยนแปลงอยู่ตลอดเวลา ดังนั้นทุกสังคมจึงเกิดความขัดแย้งได้ตลอดเวลา ซึ่งเกิดจากความไม่เท่าเทียมกันในเรื่องสิทธิอำนาจ ทำให้สังคมเกิดกลุ่มแบบไม่สมบูรณ์ขึ้น เพราะต่างฝ่ายต่างมีผลประโยชน์แอบแฝงอยู่เบื้องหลัง แต่ละฝ่ายจึงพยายามรักษาผลประโยชน์ของฝ่ายตนไว้ ทำให้ระดับของความรุนแรงจะมากหรือน้อยนั้นขึ้นอยู่กับการจัดการและการประสานผลประโยชน์ของกลุ่มที่ครอบงำกลุ่มอื่น ความขัดแย้งจึงสามารถควบคุมได้โดยการประนีประนอม และความขัดแย้งที่เกิดขึ้นในสังคมเป็นผลมาจากความกดดันจากภายนอกโดยสังคมอื่นๆ ด้วย

๒. แนวคิดทางจิตวิทยา

แนวคิดทางจิตวิทยาอธิบายความขัดแย้งว่า หมายถึง สถานการณ์ที่บุคคลถูกกระตุ้นให้เกี่ยวข้องในกิจกรรมสองอย่างหรือมากกว่า ซึ่งกิจกรรมเหล่านั้นไม่ได้เป็นไปในทิศทางเดียวกัน ทำให้การตอบสนองต่อความต้องการบรรลุวัตถุประสงค์สองอย่างพร้อมกันเป็นไปไม่ได้ จึงเกิดความขัดแย้งขึ้นได้หลายระดับ เช่น ความขัดแย้งในระดับพฤติกรรมที่ปรากฏชัด ตัวอย่างเช่น การที่คนเราพูดออกมาอย่างหนึ่งแต่ในใจคิดอีกอย่างเพราะถ้าพูดความจริงแล้วจะทำให้คนอื่นเสียใจหรือกรณีของการเกิดความขัดแย้งในตัวเอง จะเห็นว่าความขัดแย้งตามแนวคิดของจิตวิทยานั้นสามารถเกิดขึ้นได้ ตั้งแต่ภายในตัวบุคคลนั้นไปจนถึงกลุ่มหรือองค์การได้ สิ่งสำคัญที่มีอิทธิพลต่อความขัดแย้งที่เกิดขึ้นคือความคิด หรือความรู้สึกของคนเราต่อสิ่งที่มีปฏิกิริยาที่รับรู้ได้ซึ่งอาจเป็นผลมาจากความวิตกกังวล มีอคติ หรือความกลัวที่แฝงอยู่ในจิตใจมากกว่าความขัดแย้งตามแนวคิดด้านจิตวิทยาที่จะให้ความสำคัญในระดับปัจเจกบุคคล และด้านจิตวิทยาเป็นสำคัญ แนวคิดนี้ยังเชื่อว่าความขัดแย้งที่เกิดขึ้นมีผลต่ออารมณ์ของบุคคลอย่างมาก แล้วยังนำไปสู่การเปลี่ยนแปลงพฤติกรรมของคนได้ เช่น ความขัดแย้งทำให้คนเราเกิดความคับข้องใจ (Frustration) ซึ่งอาจทำให้เกิดความท้อถอย ก้าวร้าว หรือประนามผู้อื่นได้หรือในบางสถานการณ์ความขัดแย้งอาจนำมาซึ่งความล้มเหลวในการปฏิบัติงานได้ เช่น การขาดความสนใจในงาน ขาดความเชื่อมั่นตนเอง หรือกลัวความล้มเหลวจนบางครั้งกลายเป็นคนที่ชอบใส่ร้ายคนอื่นเป็นต้น

Coser (อ้างถึงใน เสริมศักดิ์ วิศาลาภรณ์, ๒๕๓๔: ๓๙) นักจิตวิทยาชาวเยอรมัน ได้จำแนกความขัดแย้งออกเป็น ๓ แบบ ได้แก่

๑. เมื่อบุคคลอยู่ระหว่างเป้าหมายที่ตนปรารถนาสองอย่างที่ต้องเลือก (Approach-Approach Conflict)

๒. เมื่อบุคคลพบกับเป้าหมายสองอย่าง ซึ่งเป็นทั้งเป้าหมายที่ตนเองชอบและไม่ชอบ (Approach-Avoidance Conflict)

๓. เมื่อบุคคลอยู่ระหว่างเป้าหมายสองอย่างที่ตนเองไม่ชอบทั้งคู่ (Avoidance-Avoidance Conflict)

นักวิชาการทางด้านมานุษยวิทยามองความขัดแย้งว่าเป็นผลมาจากความปรารถนาหรือเป้าหมายที่ไปด้วยกันไม่ได้ อาจมาจากการแข่งขันกันระหว่างกลุ่มต่างๆ ในสังคม ซึ่งเป็นผลมาจากวัฒนธรรมและเป็นแบบฉบับของพฤติกรรมการปรับตัวของมนุษย์ เช่น ความก้าวร้าว ความร่วมมือและการแข่งขันกัน เมื่อเกิดผลประโยชน์และค่านิยมที่ไปด้วยกันไม่ได้ นักวิชาการคนสำคัญที่ศึกษาเกี่ยวกับความขัดแย้งด้านนี้คือ ฟิซเซอร์ ยูรี และ แพตตัน (๒๕๔๕: ๑๑๕) ซึ่งเป็นนักมานุษยวิทยาผู้มีชื่อเสียงเห็นว่า สิ่งอันตรายที่คุกคามมวลมนุษยชาติเกิดจากนิสัยภายในตัวมนุษย์เองที่มักตกอยู่ในภาวะความขัดแย้งที่อันตรายและทำลายล้างเมื่อเกิดความแตกต่างอย่างชัดเจนขึ้นระหว่างคนสองคน กลุ่มหรือสองประเทศ

๓. แนวคิดเกี่ยวกับความขัดแย้งในคุณค่าหรือค่านิยม

แนวคิดนี้ถือว่า พฤติกรรมของบุคคลที่เบี่ยงเบนจากกฎเกณฑ์ที่กำหนดไว้นั้นเป็นเพราะสภาวการณ์นั้นไม่สอดคล้องกับคุณค่าที่กลุ่มยึดถือ จึงเห็นว่าปัญหาสังคมต่างๆ ที่เกิดขึ้นก็เพราะกลุ่มต่างๆ นำสิ่งที่ยึดถือต่างกันมาใช้แล้วขัดแย้งกัน เช่น หมอต้องการรักษาคนไข้ด้วยยาที่ทันสมัย ใช้เครื่องมือก้าวหน้า เพื่อผลการรักษาที่ดี ทำให้ค่ารักษาแพง ในขณะที่ผู้ป่วยต้องการหายจากความเจ็บป่วยและไม่ต้องเสียค่าใช้จ่ายมาก คุณค่าที่ใช้ในสภาวการณ์เดียวกันแต่ขัดแย้งกันปัญหาความไม่เข้าใจย่อมเกิด ขึ้นได้เสมอ

ทฤษฎีความขัดแย้ง (Conflict Theory) ถือได้ว่าเป็นเครื่องชี้วัดให้ประจักษ์ถึงวิวัฒนาการทางความคิดของความขัดแย้งที่มีพัฒนาการจากอดีตสู่ปัจจุบัน รากฐานของทฤษฎีความขัดแย้งพัฒนามาจากสมมติฐานที่ว่า “สังคม คือ ระบบที่มีสักษณะซับซ้อนของความไม่เท่าเทียมกัน (Inequality) และความขัดแย้ง (Conflict) จะนำไปสู่การเปลี่ยนแปลงทางสังคม” เพื่อให้เกิดความเข้าใจในทฤษฎีความขัดแย้งอย่างครอบคลุมในหลายมุมมอง ได้แก่ ด้านสังคมวิทยา ด้านจิตวิทยา ด้านมนุษยวิทยาและด้านคุณค่า (ค่านิยม) และทฤษฎีอื่นๆ ที่เกี่ยวข้อง เพื่อทำให้เห็นว่ามุมมองของนักวิชาการจากหลายสาขาวิชาต่อ “ความขัดแย้ง” นั้นมีความเหมือนและความแตกต่างกันในประเด็นสำคัญใดบ้าง ซึ่งจะเป็นประโยชน์ต่อการสร้างองค์ความรู้เพื่อการจัดการความขัดแย้งในสังคมไทยต่อไป (ฉันทนา บรรพศิริโชติ, ๒๕๔๑: ๓๗)

๔. ทฤษฎีบทบาท (Role Theory)

ทฤษฎีบทบาท (Role Theory) เป็นทฤษฎีหนึ่งที่ Moorhead and Griffin (2001: 213) ทฤษฎีนี้นำมาใช้อธิบายถึงความขัดแย้งในบทบาทของมนุษย์ในองค์การและใช้อธิบายถึงแบบแผนพฤติกรรมของบุคคลภายใต้ตำแหน่งใดตำแหน่งหนึ่ง ซึ่งมีอิทธิพลทำให้แสดงพฤติกรรมนั้นออกมาส่วนความขัดแย้งในบทบาท (Role Conflict) จะเกิดขึ้นตามประสบการณ์ของแต่ละคนที่ประสบมาหรือเกิดจากการที่พฤติกรรมของบทบาทตั้งแต่สองบทบาทขึ้นไปไม่สอดคล้องกันและความขัดแย้งเกิดจากการที่ไม่สามารถแสดงบทบาทต่างๆ ได้พร้อมกันในเวลาเดียวกัน เช่น ต้องเป็นประธานในการประชุมในฐานะครูใหญ่ หรือจะต้องออกไปรับลูกที่โรงเรียนในฐานะที่เป็นบิดา

ความขัดแย้งของบทบาท (Role Conflicts) หมายถึง เมื่อบุคคลต้องแสดงบทบาทต่างๆ หลายบทบาทในห้วงเวลาเดียวกันและบทบาทนั้นไม่สอดคล้องกัน เช่น มีบทบาทเป็นผู้บริหาร ในขณะเดียวกันก็มีบทบาทเป็นสามีที่ต้องทำหน้าที่ประเมินผลการปฏิบัติของภรรยาที่เป็นลูกน้องของตนด้วย เป็นต้น และเมื่อบทบาทนั้นไม่ชัดเจน (Role Ambiguity) ทำให้บุคคลไม่แน่ใจว่าจะปฏิบัติอย่างไร เช่น การแนะนำจากหัวหน้างานไม่ชัดเจนหรือแนวทางการร่วมปฏิบัติกับเพื่อนร่วมงานไม่ชัดเจนจะส่งผลให้บุคคลเกิดความเครียดและสับสนกับบทบาทของตัวเองที่มีอยู่กับบทบาทที่ถูกคาดหวัง และเมื่อมีมากกว่าหนึ่งบทบาทขึ้นไป จะทำให้เกิดความขัดแย้งในบทบาท (Role Conflict) ได้ซึ่งมีอยู่ ๔ แบบ ดังต่อไปนี้ (Moorhead & Griffin, 2001: 214)

๑. ความขัดแย้งภายในตัวผู้ส่งข่าวหรือผู้ที่ออกคำสั่ง (Intra-Sender Conflict) เช่น กรณีที่หัวหน้าทีม ต้องทำงานในบทบาทที่เท่าเทียมกันในทีม ในขณะเดียวกันก็มีบทบาทเป็นผู้บริหารด้วย ต้องทำหน้าที่สั่งการและบังคับบัญชาด้วยจะมีบทบาทที่เท่าเทียมกัน ในทุกบทบาทคงเป็นไปได้ยาก จึงทำให้เกิดความขัดแย้งภายในตัวเองขึ้น

๒. ความขัดแย้งระหว่างผู้ส่งข่าวหรือผู้ออกคำสั่ง (Inter-Sender Conflict) เกิดจากคนในกลุ่มมีความขัดแย้งกับคนในกลุ่มอื่นๆ ที่มีบทบาทเดียวกันทำให้ความขัดแย้งเกิดขึ้นระหว่างกลุ่ม

๓. ความขัดแย้งระหว่างบทบาท (Inter-Role Conflict) เมื่อบทบาทต่างกันทำให้บุคคลมีพฤติกรรมที่ต่างกันด้วย แต่เมื่อต้องมาทำงานร่วมกันจะพบว่ามีพฤติกรรมที่เข้ากันไม่ได้ เช่น เมื่อหัวหน้างานขอให้ช่วยทำงานล่วงเวลาเพื่อให้งานเสร็จ ในขณะเดียวกันก็กังวลกับบทบาทการเป็นแม่บ้านที่ต้องดูแลลูกหลังเลิกงาน ความขัดแย้งจึงเกิดขึ้นระหว่างเรื่องงานกับบทบาทส่วนตัวที่มีอยู่

๔. ความขัดแย้งระหว่างบุคคลกับบทบาท (Person-Role Conflict) เกิดขึ้นเมื่อเรามีบทบาทอย่างหนึ่ง แต่ไม่สามารถทำตามบทบาทที่ตนมีได้หรือการที่บุคคลมีความต้องการอย่างหนึ่ง แต่ตามบทบาทที่ถูกกำหนดไว้นั้นทำตามความต้องการของตนเองไม่ได้จะเกิดความขัดแย้งขึ้นได้

๕. ทฤษฎีความขัดแย้งแบบร่วมมือ

Leung and Tjosvold (1998: 44) เสนอว่า สิ่งสำคัญที่ทำให้การจัดการความขัดแย้งไม่ได้ผล คือการขาดแรงจูงใจที่ดี (Motivation) ดังนั้นองค์การที่ต้องการให้การจัดการความขัดแย้งได้ผลดีจึงควรมีการลงทุนเพื่อการฝึกฝนสร้างการเรียนรู้ให้บุคลากรมีสมรรถนะต่อการจัดการความขัดแย้งแบบร่วมมือ ตามทฤษฎีความขัดแย้งแบบร่วมมือ (Cooperative Conflict Theory) อันจุดเน้นที่การมีเป้าหมายเดียวกันภายใต้มิตรภาพที่ดีต่อกันและกัน “we are in this together” and “we swim or sink together” หัวใจสำคัญ คือ แนวทางปฏิบัติถูกกำหนดมาจากการบูรณาการความต้องการของทุกคนร่วมกันบนพื้นฐานของความจริงใจต่อกันเพื่อมุ่งสู่การบรรลุเป้าหมายร่วมกัน

ความขัดแย้งในทัศนะของ Barnard (1968: 145) ได้เขียนเกี่ยวกับความขัดแย้งไว้ในหนังสือ The Functions of the Executive ไว้ว่า “ความขัดแย้ง” นั้นเกิดจากการมีมาตรฐานหรือมีหลักการทำงานที่แตกต่างกัน ทำให้เกิดความเหลื่อมล้ำ เกิดการครอบงำจากการใช้อำนาจหรือใช้อิทธิพลเข้ามาต่อรองให้ฝ่ายตนอยู่เหนือกว่า จึงพบว่าความขัดแย้งในการทำงานของปัจเจกบุคคล (Conflict of Code) เป็นเรื่องที่หลีกหนีได้ยากและส่งผลสำคัญ ๓ ประการ ดังนี้

๑. การทำงานหยุดชะงัก (Paralysis of Action) เพราะเกิดความเครียดเต็มไปด้วยอารมณ์ขุ่นมัวจนทำให้คับข้องใจส่งผลให้ขาดความสามารถในการตัดสินใจและขาดความเชื่อมั่นในตนเองตามมา

๒. การมุ่งทำงานตามมาตรฐานอันหนึ่งอาจส่งผลกระทบต่อการทำงานของคนอื่นทำให้เกิดความไม่สบายใจ รู้สึกผิด ทำให้คนอื่นไม่พอใจและขาดความเชื่อมั่นตนเองได้

๓. เมื่อมีความขัดแย้งก็ต้องมีการแก้ไข เกิดการปรับปรุงระบบการทำงาน จะทำให้เปลี่ยนระบบการทำงานบ่อยๆ อาจทำให้คนสับสนจนปรับตัวไม่ทันเพราะต้องเรียนรู้ใหม่หลายครั้ง ประสบการณ์เดิมๆ ก็ใช้ไม่ได้ส่งผลต่อขวัญและกำลังใจต่อพนักงานได้ แม้แต่หลักการทำงานที่ผ่านการกลั่นกรองมาเป็นอย่างดีแล้วก็ย่อมจะพบกับปัญหาได้เสมอ เพราะคนในองค์กรมีความแตกต่างด้านความรู้ ความสามารถ ทัศนคติ การรับรู้ และที่สำคัญคือความแตกต่างด้านจริยธรรม ทำให้ความขัดแย้งกลายเป็นเรื่องที่ยากจะหลีกเลี่ยงได้ และแนวคิดของ Barnard นี้จะเห็นว่า ความขัดแย้งที่เกิดขึ้นในองค์การนั้นจะส่งผลด้านลบต่อการบริหารองค์การเป็นสำคัญ และ Barnard ก็ยอมรับว่าความขัดแย้งเป็นสิ่งที่เกิดขึ้นได้เสมอ แม้แต่จะได้เตรียมการวางแผนจัดการไว้ล่วงหน้าแล้วก็ตาม

แนวคิดความขัดแย้งของ Robbins (อ้างถึงใน สมบัติ ธำรงธัญญวงศ์, ๒๕๔๕: ๑๕-๑๖) ซึ่งเป็นนักวิชาการด้านองค์การคนสำคัญ ได้แบ่งแนวคิดเรื่องความขัดแย้งไว้ ๔ แนวคิด ดังนี้

๑. แนวคิดแบบดั้งเดิมหรือแนวคิดประเพณีนิยม (Traditional Perspective) ได้รับความนิยมในช่วง ค.ศ.๑๙๓๐-๑๙๔๘ แนวคิดนี้มองความขัดแย้งเป็นสิ่งไม่ดี และทำให้เกิดผลลบต่อ

องค์การอยู่เสมอ เช่น ทำให้คนบาดหมางกันพูดหรือสื่อสารกันไม่รู้เรื่อง จนเป็นเหตุทำลายความร่วมมือในองค์กรได้ ดังนั้นผู้บริหารควรหลีกเลี่ยงและต้องกำจัดให้หมดไปจึงจะถือว่าเป็นผู้บริหารที่มีความสามารถ

๒. แนวคิดแบบพฤติกรรมศาสตร์หรือด้านมนุษย์สัมพันธ์ (Behavioral or Human Relation Perspective) แนวคิดนี้เกิดในช่วง ค.ศ.๑๙๔๐-๑๙๗๕ แนวคิดนี้ไม่เห็นด้วยกับแบบดั้งเดิม โดยเห็นว่า ความขัดแย้งเป็นสิ่งที่เกิดขึ้นตามธรรมชาติไม่สามารถหลีกเลี่ยงได้ จึงควรยอมรับว่าความขัดแย้งเป็นส่วนหนึ่งในองค์การ ซึ่งผู้บริหารควรทำให้ความขัดแย้งกลายเป็นพลังสร้างสรรค์และเกื้อกูลการปฏิบัติงาน แม้ว่าบางครั้งความขัดแย้งจะนำมาซึ่งปัญหา แต่มันกลายเป็นตัวกระตุ้นให้เกิดความโต้แย้งในกลุ่มต่างๆ ทำให้เกิดกลยุทธ์ใหม่ๆ มาเพื่อแก้ไขความขัดแย้งแบบนั้นๆ อีกจนมีนวัตกรรมเกิดขึ้น ความขัดแย้งจะก่อประโยชน์แก่ผู้บริหารได้เพราะจะช่วยให้ทราบปัญหาต่างๆ ที่เกิดขึ้นทำให้เข้าใจสาเหตุของปัญหาทำให้วิเคราะห์ได้ตรงประเด็นมากขึ้น ในแนวคิดเชิงพฤติกรรมศาสตร์จึงเห็นว่าผู้บริหารไม่ควรหลบเลี่ยงที่จะเผชิญกับความขัดแย้ง แต่ควรหาทางลดและควบคุมให้เหมาะสมจะได้กระตุ้นพลังสร้างสรรค์ให้องค์กรเจริญและอยู่รอดได้

๓. แนวคิดแบบนักปฏิสัมพันธ์ (Inter-Artionist Perspective) แนวคิดนี้มองความขัดแย้งในเชิงสร้างสรรค์มากขึ้น และยังมองว่าเป็นสิ่งที่จำเป็นเพื่อช่วยกระตุ้นให้การทำงานมีประสิทธิภาพ เชื่อว่าจะนำมาซึ่งการเปลี่ยนแปลง ผู้บริหารจึงควรทำให้ความขัดแย้งอยู่ในระดับที่พอเหมาะ จะช่วยสนับสนุนส่งเสริมให้คนมีความกระตือรือร้น มิใช่ทำงานตามคำสั่งเหมือนหุ่นยนต์เท่านั้น ความขัดแย้งยังทำให้องค์การเกิดการพัฒนาเรียนรู้อย่างต่อเนื่อง การจัดการความขัดแย้งให้เหมาะสมจึงเป็นหน้าที่สำคัญประการหนึ่งของผู้บริหาร

๔. แนวคิดสมัยใหม่ (Emerging Perspective) แนวคิดนี้เกิดเมื่อต้นศตวรรษ ๑๙๘๐ เป็นยุคที่การบริหารงานแบบญี่ปุ่นได้แผ่อิทธิพลต่อการบริหารไปทั่วโลก โดยที่ชาวญี่ปุ่นตระหนักดีว่าความขัดแย้งเป็นสิ่งที่หลีกไม่พ้น เนื่องจากปัจจุบันบุคคลทั่วไปล้วนแล้วแต่มีข้อบกพร่อง คงไม่มีใครสมบูรณ์แบบ แต่ความสามัคคีปรองดองทำให้เกิดความสงบสุขได้ แนวคิดนี้เชื่อว่าการจัดการกับความขัดแย้งต้องคำนึงถึงความเหมาะสมและคำนึงถึงเอกภาพขององค์การ มักใช้วิธีการแก้ไขความขัดแย้งอย่างสันติ ซึ่งมีจุดแข็งกว่าแนวทางของชาวอเมริกันโดยเฉพาะในเรื่องความรัก ความสามัคคีและจงรักภักดีกลุ่ม และต่อองค์การ ทำให้สามารถสร้างทีมงานเข้มแข็งและเป็นอันหนึ่งอันเดียวกันอันจะนำไปสู่ความได้เปรียบในการแข่งขันได้

สำหรับองค์ความรู้ของความขัดแย้งในมุมมองของนักวิชาการไทยมีผู้ที่สรุปไว้หลายท่าน แต่ที่ได้รับความนิยมและเป็นนักวิชาการที่สนใจเรื่องความขัดแย้งในระดับองค์การมาตลอด

ได้แก่ เสริมศักดิ์ วิศาลาภรณ์ (๒๕๓๔: ๕๖) ได้เสนอแนวคิดความขัดแย้งของบุคคลไว้ ๒ แนวคิด ดังนี้

๑. แนวคิดเดิม

๑.๑ ความขัดแย้งควรจะถูกกำจัดให้หมดไปจากองค์การเพราะความขัดแย้ง ทำให้องค์การแตกแยก ขาดประสิทธิภาพ และอาจนำไปสู่ความเครียด ดังนั้นองค์การที่ดีที่สุดจึงต้องไม่มีความขัดแย้ง

๑.๒ ความขัดแย้งเป็นผลมาจากความผิดพลาดของการบริหารจึงพยายามหลีกเลี่ยงความขัดแย้ง

๑.๓ ผู้บริหารสามารถควบคุมและปรับพฤติกรรมของพนักงานได้ เช่น ความก้าวร้าว การแข่งขัน และควบคุม ความขัดแย้งโดยการสร้างบรรยากาศให้เหมาะสม

๒. แนวคิดใหม่

๒.๑ ความขัดแย้งเป็นส่วนหนึ่งของชีวิตในองค์การจึงไม่ควรหลีกเลี่ยงแต่ต้องรักษา ระดับความขัดแย้งให้เหมาะสม จะทำให้กระตุ้นและจูงใจให้คนปฏิบัติงานอย่างมีประสิทธิภาพได้

๒.๒ ความขัดแย้งเป็นผลมาจากความแตกต่างของรางวัลที่ได้รับเป้าหมาย ค่านิยมในองค์การและอาจเกิดจากความก้าวร้าวโดยธรรมชาติในตัวคน ดังนั้น ความขัดแย้งจะมีประโยชน์หรือโทษขึ้นกับวิธีการบริหารความขัดแย้ง

๒.๓ ผู้บริหารต้องศึกษาและทำความเข้าใจถึงปัจจัยที่ส่งผลต่อการทำงานของคนและปัจจัยที่ทำให้เกิดความขัดแย้งจะทำให้การจัดการกับความขัดแย้งมีประสิทธิภาพ

๖. ระดับความขัดแย้ง

Don Hellriegel and John W. Slocum Jr., 1970 เสนอว่าความขัดแย้งนั้นอาจจะมองในระดับต่างๆ ดังนี้ ๑) ความขัดแย้งภายในตัวบุคคล ๒) ความขัดแย้งระหว่างบุคคล ๓) ความขัดแย้งระหว่างบุคคลในกลุ่ม ๔) ความขัดแย้งระหว่างกลุ่ม และ ๕) ความขัดแย้งในองค์กร

March and Simon, 1958 ได้แบ่งระดับความขัดแย้งออกเป็น ๓ ระดับ ได้แก่ ๑) ความขัดแย้งของบุคคล ๒) ความขัดแย้งในองค์กร ซึ่งเป็นความขัดแย้งในตัวบุคคลหรือกลุ่มภายในองค์กร และ ๓) ความขัดแย้งระหว่างองค์กร ซึ่งเป็นความขัดแย้งระหว่างองค์การหรือกลุ่มต่างๆ

ระดับของความขัดแย้งที่ Don Hellriegel and John W. Slocum Jr. และ March and Simon มีความคล้ายคลึงกันมาก ซึ่งเราสามารถแบ่งความขัดแย้งนี้ได้เป็น ๒ ระดับ ได้แก่

๑. ความขัดแย้งในระดับบุคคล แบ่งเป็น

๑.๑ ความขัดแย้งภายในตัวบุคคล (Intrapersonal Conflict) หมายถึง ความขัดแย้งที่เกิดขึ้นภายในตัวของคนๆ หนึ่งไม่เกี่ยวข้องกับบุคคลอื่น หรือเรียกได้ว่า “ความขัดแย้งในตัวเอง”

๑.๒ ความขัดแย้งระหว่างบุคคล (Interpersonal Conflict) หมายถึง ความขัดแย้งที่เกิดขึ้นระหว่างบุคคลมากกว่า ๒ บุคคลขึ้นไป

๒. ความขัดแย้งระหว่างองค์กร แบ่งเป็น

๒.๑ ความขัดแย้งภายในองค์กร (Intra-Organization Conflict) หมายถึง ความขัดแย้งที่เกิดขึ้นมาโดยมีคู่กรณีขัดแย้งเป็นบุคคลหรือกลุ่มย่อยๆ ที่มีอยู่ในกลุ่มหรือที่อยู่ในองค์การหรือกลุ่มต่างๆ

๒.๒ ความขัดแย้งระหว่างองค์กร (Inter-Organization Conflict) หมายถึง ความขัดแย้งที่เกิดขึ้นมาโดยที่คู่กรณีขัดแย้งเป็นองค์กรกับองค์กร หรือกลุ่มกับกลุ่ม

๗. ผลของความขัดแย้ง

ความขัดแย้งเป็นส่วนหนึ่งของชีวิตไม่ว่าจะเป็นชีวิตในวัยเรียน ชีวิตวัยทำงาน ชีวิตครอบครัว ชีวิตภายในสังคม และเป็นเรื่องยากที่จะหลีกหนีให้พ้นจากความขัดแย้งและเนื่องจากแนวคิดปัจจุบันความขัดแย้งไม่ใช่สิ่งที่ดีทั้งหมดหรือเสียทั้งหมด ความขัดแย้งมีทั้งประโยชน์และโทษทั้งนี้ขึ้นอยู่กับประเภทของความขัดแย้งและระดับของความขัดแย้ง ซึ่งพอสรุปได้ดังนี้

๗.๑ ผลดีของความขัดแย้ง

พรนพ พุกกะพันธุ์ (๒๕๔๔: ๒๗๖) ได้กล่าวถึงผลดีของความขัดแย้งไว้ว่า ความจริงแล้วความขัดแย้งเป็นสิ่งที่หลีกเลี่ยงไม่ได้ และเมื่อเกิดขึ้นก็จะนำไปสู่ความก้าวหน้าหรือเกิดความสร้างสรรค์ได้เพราะจะเกิดแนวคิดที่สามขึ้นมา ซึ่งเหนือกว่าสองแนวคิดที่ขัดแย้งกันอยู่ ดังนั้นความขัดแย้งจึงเสมือนเป็นการบังคับให้มนุษย์แสวงหาความคิดที่ใหม่ขึ้นเสมอซึ่งจะเป็นผลดีต่อองค์การ เพราะจะเกิดความคิดสร้างสรรค์ใหม่ๆ และเปิดโอกาสให้มนุษย์ตรวจสอบความสามารถของตนเองอยู่เสมอ

วิจิตร วรุตบางกูร (๒๕๒๖: ๑๗๓-๑๗๔) โดยทั่วไปบุคคลส่วนใหญ่จะมีทัศนคติไม่ดีต่อความขัดแย้งเพราะเชื่อว่าความร่วมมือเป็นสิ่งที่ดีและความขัดแย้งเป็นสิ่งที่ไม่ดี แม้ว่าความขัดแย้งอาจก่อให้เกิดบรรยากาศที่ตึงเครียดและเป็นผลเสียต่อองค์การแต่บางครั้งความขัดแย้งอาจก่อให้เกิดผลดีได้เหมือนกัน กล่าวคือ ความขัดแย้งสามารถให้ผลในทางบวก เป็นต้นว่า

๑. ทำให้เกิดแนวปฏิบัติหรือความคิดเห็นอื่นๆ มากขึ้น

๒. ทำให้มีโอกาสเลือกแนวทางที่ดีกว่า

๓. ทำให้เกิดแรงผลักดันที่ต้องค้นหาวิธีการใหม่ๆ

๔. ทำให้เกิดความพยายามที่จะอธิบายความเห็น ความเชื่อหรือชี้แจงให้ชัดเจน จึงต้องพัฒนาความสามารถในการสื่อความหมายและให้เหตุผล

๕. ความตึงเครียดกระตุ้นให้เกิดความคิดสร้างสรรค์

๖. ทำให้เกิดความเคยชินในการแลกเปลี่ยนความเห็นและยอมรับนับถือซึ่งกันและกันมากยิ่งขึ้น

ซึ่งคล้ายกับ ทิศนา แขมมณี (๒๕๒๒: ๘๑) กล่าวว่า ความขัดแย้งไม่ใช่จะให้ผลเสียเสมอไป แท้ที่จริงแล้วความขัดแย้งมีประโยชน์ในหลายด้าน เช่น ๑) ความขัดแย้งทำให้เกิดแนวคิดใหม่ๆ ๒) ทำให้ความคิดและการทำงานไม่หยุดอยู่กับที่ และ ๓) ช่วยกระตุ้นให้บุคคลเกิดความกระตือรือร้นและแสดงความสามารถของตน อาจส่งผลให้การทำงานและผลงานของกลุ่มดีขึ้น

เสริมศักดิ์ วิศาลาภรณ์ (๒๕๔๐: ๒๒) ได้กล่าวโดยสรุปว่า ความขัดแย้งที่มีในระดับที่เหมาะสมจะก่อให้เกิดประโยชน์ต่อบุคคลและองค์การประโยชน์ที่สำคัญบางประการ ได้แก่ ๑) ป้องกันไม่ให้องค์การหยุดอยู่กับที่หรือเฉื่อยชา และ ๒) ความขัดแย้งจะทำให้เกิดการเปลี่ยนแปลง ดังนั้นผู้บริหารที่ฉลาดย่อมสามารถนำการเปลี่ยนแปลงนั้นให้เป็นประโยชน์แก่ส่วนรวม

ความขัดแย้งเป็นผลมาจากความแตกต่างของบุคคล ผู้บริหารที่ฉลาดย่อมสามารถประสานความแตกต่างมาเป็นประโยชน์ต่อองค์การทำให้เกิดความคิดริเริ่มใหม่ๆ ความขัดแย้งกระตุ้นให้เกิดการแสวงหาข้อมูลใหม่หรือข้อเท็จจริงใหม่หรือวิธีแก้ปัญหาอย่างใหม่ต่างฝ่ายก็พยายามหาข้อมูลและเหตุผลมาสนับสนุนฝ่ายตนทำให้ได้ข้อมูลหรือหลักฐานใหม่หรือต่างฝ่ายต่างก็ไม่ยอมรับวิธีของกันและกันก็จำเป็นต้องหาทางออกใหม่ ส่วนความขัดแย้งกับกลุ่มอื่นจะทำให้สมาชิกภายในกลุ่มมีความกลมเกลียวกันและรวมพลังกัน ความขัดแย้งที่เกิดจากการมีความเห็นแตกต่างกันจะช่วยทำให้มีความรอบคอบและมีปัญหา นอกจากนั้นยังช่วยเสริมการพัฒนาการทำงานอย่างมีระบบและมีประสิทธิภาพ

๗.๒ ผลเสียของความขัดแย้ง

พรนพ พุกกะพันธุ์ (๒๕๔๔: ๒๗๗) ได้กล่าวถึงผลเสียของความขัดแย้งไว้ว่า อาจจะทำให้องค์การขาดประสิทธิภาพและประสิทธิผลได้ ถ้าหากผู้บริหารไม่รู้จักแก้ไขและสาเหตุของความขัดแย้งของบุคคลภายในองค์การมีอยู่หลายประการด้วยกัน การแก้ไขจึงต้องใช้วิธีการที่แตกต่างกันด้วย ดังนั้นผู้บริหารหรือหัวหน้างานจำเป็นต้องศึกษาและทำความเข้าใจเรื่องนี้ให้ถ่องแท้ มิฉะนั้นอาจมีการแก้ไขปัญหาได้ไม่ถูกจุดและจะเกิดความเสียหายต่อผลงานขององค์การในส่วนรวมได้ เช่น อาจมีผลให้คนที่ทนไม่ได้จะต้องย้ายหนีจากหน่วยงานนั้นไป ความเป็นมิตร

ระหว่างบุคคลจะลดลง บรรยากาศของความเชื่อถือและไว้วางใจซึ่งกันและกันจะหมดไป อาจเป็นการต่อสู้ที่ใช้อารมณ์ไร้เหตุผล และมีการต่อต้านซึ่งอาจขัดต่อวัตถุประสงค์ของหน่วยงาน เป็นต้น

ทฤษฎีการบริหารจัดการภาครัฐยุคใหม่

๑. ความหมายของการบริหารงานภาครัฐแนวใหม่

การบริหารงานภาครัฐแนวใหม่ (New Public Management) คือ การปรับเปลี่ยนการบริหารจัดการภาครัฐโดยนำหลักการเพิ่มประสิทธิภาพของระบบราชการและการแสวงหาประสิทธิภาพในการปฏิบัติราชการที่มุ่งสู่ความเป็นเลิศ โดยการนำเอาแนวทางหรือวิธีการบริหารงานของภาคเอกชนมาปรับใช้กับการบริหารงานภาครัฐ เช่น การบริหารงานแบบมุ่งเน้นผลสัมฤทธิ์ การบริหารงานแบบมืออาชีพ การคำนึงถึงหลักความคุ้มค่า การจัดการโครงสร้างที่กะทัดรัดและแนวราบ การเปิดโอกาสให้เอกชนเข้ามาแข่งขันการให้บริการสาธารณะ การให้ความสำคัญต่อค่านิยม จรรยาบรรณวิชาชีพ คุณธรรมและจริยธรรม ตลอดทั้งการมุ่งเน้นการให้บริการแก่ประชาชนโดยคำนึงถึงคุณภาพเป็นสำคัญ

๒. เหตุผลที่ต้องนำแนวคิดการบริหารงานภาครัฐแนวใหม่มาใช้

๒.๑ กระแสโลกาภิวัตน์ ส่งผลให้สภาพแวดล้อมทั้งภายในและภายนอกประเทศเปลี่ยนแปลงไปอย่างรวดเร็ว จึงมีความจำเป็นอย่างยิ่งสำหรับองค์กรทั้งภาครัฐและเอกชนที่ต้องเพิ่มศักยภาพและความยืดหยุ่นในการปรับเปลี่ยนเพื่อตอบสนองต่อความต้องการของระบบที่เปลี่ยนแปลงไป

๒.๒ ระบบราชการไทยมีปัญหาที่สำคัญก็คือ ความเสื่อมถอยของระบบราชการและการขาดธรรมาภิบาล ถ้าภาครัฐไม่ปรับเปลี่ยนและพัฒนาการบริหารจัดการของภาครัฐเพื่อไปสู่องค์กรสมัยใหม่ โดยยึดหลักธรรมาภิบาล ก็จะส่งผลบั่นทอนความสามารถในการแข่งขันของประเทศ ทั้งยังเป็นอุปสรรคต่อการพัฒนาเศรษฐกิจและสังคมในอนาคตด้วย

ดังนั้นการบริหารจัดการภาครัฐแนวใหม่ (New Public Management) จึงเป็นแนวคิดพื้นฐานของการบริหารจัดการภาครัฐซึ่งจะนำไปสู่การเปลี่ยนแปลงระบบต่างๆ ของภาครัฐและยุทธศาสตร์ด้านต่างๆ ที่เป็นรูปธรรม มีแนวทางในการบริหารจัดการดังนี้

๑. การให้บริการที่มีคุณภาพแก่ประชาชน

๒. ลดการควบคุมจากส่วนกลางและเพิ่มอิสระในการบริหารให้แก่หน่วยงาน

๓. การกำหนด การวัด และการให้รางวัลแก่ผลการดำเนินงานทั้งในระดับองค์กรและระดับบุคคล

๔. การสร้างระบบสนับสนุนทั้งในด้านบุคลากร (เช่น การฝึกอบรม ระบบค่าตอบแทนและระบบคุณธรรม) เทคโนโลยีเพื่อช่วยให้หน่วยงานสามารถทำงานได้อย่างบรรลุวัตถุประสงค์

๕. การเปิดกว้างต่อแนวคิดในเรื่องของการแข่งขัน ทั้งการแข่งขันระหว่างหน่วยงานของรัฐด้วยกัน และระหว่างหน่วยงานของรัฐกับหน่วยงานของภาคเอกชน ในขณะเดียวกันภาครัฐก็หันมาทบทวนตัวเองว่าสิ่งใดควรทำเองและสิ่งใดควรปล่อยให้เอกชนทำ

๓. แนวคิดการบริหารจัดการภาครัฐแนวใหม่

หลักใหญ่ของการจัดการภาครัฐแนวใหม่ คือ การเปลี่ยนระบบราชการที่เน้นระเบียบและขั้นตอนไปสู่การบริหารแบบใหม่ซึ่งเน้นผลสำเร็จและความรับผิดชอบ รวมทั้งใช้เทคนิคและวิธีการของเอกชนมาปรับปรุงการทำงาน เรืองวิทย์ เกษสุวรรณ (๒๕๕๓) กล่าวว่าสิ่งที่เรียกว่า “การจัดการภาครัฐแนวใหม่” มีหลักสำคัญ ๗ ประการ คือ

๓.๑ จัดการโดยนักวิชาชีพที่ชำนาญการ (Hands-on professional management) หมายถึง ให้ผู้จัดการมืออาชีพได้จัดการด้วยตัวเอง ด้วยความชำนาญ โปร่งใส และมีความสามารถในการใช้ดุลพินิจ เหตุผลก็เพราะเมื่อผิดชอบต่อหน้าที่ที่ได้รับมอบหมายแล้ว ก็จะเกิดความรับผิดชอบต่อการตรวจสอบจากภายนอก

๓.๒ มีมาตรฐานและการวัดผลงานที่ชัดเจน (Explicit standards and measures of performance) ภาครัฐจึงต้องมีจุดมุ่งหมายและเป้าหมายของผลงาน และการตรวจสอบจะมีได้ก็ต้องมีจุดมุ่งหมายที่ชัดเจน

๓.๓ เน้นการควบคุมผลผลิตที่มากขึ้น (Greater emphasis on output controls) การใช้ทรัพยากรต้องเป็นไปตามผลงานที่วัดได้ เพราะเน้นผลสำเร็จมากกว่าระเบียบวิธี

๓.๔ แยกหน่วยงานภาครัฐออกเป็นหน่วยย่อยๆ (Shift to disaggregation of units in the public sector) การแยกหน่วยงานใหญ่ออกเป็นหน่วยงานย่อยๆ ตามลักษณะสินค้าและบริการที่ผลิต ให้เงินสนับสนุนแยกกัน และติดต่อกันอย่างเป็นอิสระ

๓.๕ เปลี่ยนภาครัฐให้แข่งขันกันมากขึ้น (Shift to greater competition in the public sector) เป็นการเปลี่ยนวิธีทำงานไปเป็นการจ้างเหมาและประมูล เหตุผลก็เพื่อให้ฝ่ายที่เป็นปรปักษ์กัน (rivalry) เป็นกุญแจสำคัญที่จะทำให้ต้นทุนต่ำและมาตรฐานสูงขึ้น

๓.๖ เน้นการจัดการตามแบบภาคเอกชน (Stress on private sector styles of management practice) เปลี่ยนวิธีการแบบข้าราชการไปเป็นการยืดหยุ่นในการจ้างและให้รางวัล

๓.๗ เน้นการใช้ทรัพยากรอย่างมีวินัยและประหยัด (Stress on greater discipline and parsimony in resource use) วิธีนี้อาจทำได้ เช่น การตัดค่าใช้จ่าย เพิ่มวินัยการทำงาน หยุดยั้งการ

เรียกร้องของสหภาพแรงงาน จำกัดต้นทุนการปฏิบัติ เหตุผลก็เพราะต้องการตรวจสอบความต้องการใช้ทรัพยากรของภาครัฐ และ “ทำงานมากขึ้นโดยใช้ทรัพยากรน้อยลง” (do more with less)

๔. รูปแบบการนำการบริหารจัดการภาครัฐแนวใหม่มาใช้ในระบบราชการไทย

๔.๑ พระราชบัญญัติระเบียบบริหารราชการแผ่นดิน (ฉบับที่ ๕) พ.ศ.๒๕๔๕ เหตุผลในการตราพระราชบัญญัตินี้คือ เพื่อเป็นการปรับปรุงระบบบริหารราชการเพื่อให้สามารถปฏิบัติงานตอบสนองต่อการพัฒนาประเทศและการให้บริการแก่ประชาชนได้อย่างมีประสิทธิภาพยิ่งขึ้น โดยกำหนดให้การบริหารราชการแนวทางใหม่ต้องมีการ กำหนดนโยบาย เป้าหมาย และแผนการปฏิบัติงานเพื่อให้สามารถประเมินผลการปฏิบัติราชการในแต่ละระดับได้อย่างชัดเจน มีกรอบการบริหารกิจการบ้านเมืองที่ดีเป็นแนวทางในการกำกับการกำหนดนโยบายและการปฏิบัติราชการ และเพื่อให้กระทรวงสามารถจัดการบริหารงานให้เป็นไป ตามเป้าหมายได้ จึงกำหนดให้มีรูปแบบการบริหารใหม่ โดยกระทรวงสามารถแยกส่วนราชการจัดตั้งเป็นหน่วยงานตามภาระหน้าที่ เพื่อให้เกิดความคล่องตัวและสอดคล้องกับเป้าหมายของงานที่จะต้องปฏิบัติและกำหนดให้มีกลุ่มภารกิจของส่วนราชการต่างๆ ที่มีงานสัมพันธ์กัน เพื่อที่จะสามารถกำหนดเป้าหมายการทำงานร่วมกันได้ และมีผู้รับผิดชอบกำกับการบริหารงานของกลุ่มภารกิจนั้นโดยตรง เพื่อให้งานเป็นไปอย่างมีประสิทธิภาพและรวดเร็ว รวมทั้งให้มีการประสานการปฏิบัติงาน และการใช้งบประมาณเพื่อที่จะให้การบริหารงานของทุกส่วนราชการบรรลุเป้าหมายของกระทรวงได้อย่างมีประสิทธิภาพและลดความซ้ำซ้อน มีการมอบหมายงานเพื่อลดขั้นตอนการปฏิบัติราชการ และสมควรกำหนดการบริหารราชการในต่างประเทศให้เหมาะสมกับลักษณะการปฏิบัติหน้าที่และสามารถปฏิบัติการได้อย่างรวดเร็วและมีเอกภาพ โดยมีหัวหน้าคณะผู้แทนเป็นผู้รับผิดชอบในการบริหารราชการ นอกจากนี้ สมควรให้มีคณะกรรมการพัฒนาระบบราชการเพื่อเป็นหน่วยงานที่รับผิดชอบในการดูแลการจัดส่วนราชการและการปรับปรุงระบบการทำงานของภาคราชการให้มีการจัดระบบราชการอย่างมีประสิทธิภาพต่อไป

ในมาตรา ๓/๑ ได้กำหนดให้การพัฒนาระบบราชการต้องสอดคล้องกับการเปลี่ยนแปลงทางเศรษฐกิจ การเมือง สังคม ความต้องการของประชาชนและทันต่อการบริหารราชการตามพระราชบัญญัตินี้ต้องเป็นไปเพื่อประโยชน์สุขของประชาชน เกิดผลสัมฤทธิ์ต่อภารกิจของรัฐ ความมีประสิทธิภาพ ความคุ้มค่าในเชิงภารกิจแห่งรัฐ การลดขั้นตอนการปฏิบัติงาน การลดภารกิจและยุบเลิกหน่วยงานที่ไม่จำเป็น การกระจายภารกิจและทรัพยากรให้แก่ท้องถิ่น การกระจายอำนาจตัดสินใจ การอำนวยความสะดวกและการตอบสนองความต้องการของประชาชน ทั้งนี้โดยมีผู้รับผิดชอบต่อผลของงาน

การจัดสรรงบประมาณ และการบรรจุและแต่งตั้งบุคคลเข้าดำรงตำแหน่งหรือปฏิบัติหน้าที่ต้องคำนึงถึงหลักการตามวรรคหนึ่ง

ในการปฏิบัติหน้าที่ของส่วนราชการ ต้องใช้วิธีการบริหารกิจการบ้านเมืองที่ดี โดยเฉพาะอย่างยิ่งให้คำนึงถึงความรับผิดชอบของผู้ปฏิบัติงาน การมีส่วนร่วมของประชาชน การเปิดเผยข้อมูล การติดตามตรวจสอบและประเมินผลการปฏิบัติงาน

๔.๒ พระราชกฤษฎีกาว่าด้วยหลักเกณฑ์และวิธีการบริหารกิจบ้านเมืองที่ดี พ.ศ. ๒๕๔๖ ได้กำหนด ขอบเขต แบบแผน วิธีปฏิบัติราชการ เพื่อเป็นไปตามหลักการบริหารภาครัฐแนวใหม่ ดังนี้

๑. เกิดประโยชน์สุขของประชาชน

๒. เกิดผลสัมฤทธิ์ต่อภารกิจของรัฐ

๓. มีประสิทธิภาพและเกิดความคุ้มค่าในเชิงภารกิจของรัฐ

๔. ไม่มีขั้นตอนการปฏิบัติงานเกินความจำเป็น

๕. มีการปรับปรุงภารกิจของส่วนราชการให้ทันต่อเหตุการณ์

๖. ประชาชนได้รับการอำนวยความสะดวกและได้รับการตอบสนอง

๗. มีการประเมินผลการปฏิบัติงานอย่างสม่ำเสมอ ซึ่งได้แก่ การตรวจสอบและวัดผลการปฏิบัติงาน เพื่อให้เกิดระบบการควบคุมตนเอง

๔.๓ แผนยุทธศาสตร์การพัฒนาระบบราชการ พ.ศ.๒๕๔๖-๒๕๕๐ ได้กำหนดเป้าประสงค์หลักของการพัฒนาระบบราชการไทย ๔ ประการ ได้แก่

๑. พัฒนาคุณภาพการให้บริการประชาชนที่ดีขึ้น

๒. ปรับบทบาท ภารกิจ และขนาดให้มีความเหมาะสม

๓. ยกระดับขีดความสามารถและมาตรฐานการทำงานให้อยู่ในระดับสูงเทียบเท่าเกณฑ์สากล

๔. ตอบสนองต่อการบริหารปกครองในระบอบประชาธิปไตย

โดยกำหนดยุทธศาสตร์ ๗ ด้านเพื่อให้การบริหารราชการเป็นไปอย่างมีประสิทธิภาพ ดังนี้

ยุทธศาสตร์ ๑ การปรับเปลี่ยนกระบวนการและวิธีการทำงาน ประกอบด้วย ๕ มาตรการ

ยุทธศาสตร์ ๒ การปรับปรุงโครงสร้างการบริหารราชการแผ่นดิน ประกอบด้วย ๔ มาตรการ

ยุทธศาสตร์ ๓ การรื้อปรับระบบการเงินและการงบประมาณ ประกอบด้วย ๘ มาตรการ

ยุทธศาสตร์ ๔ การสร้างระบบบริหารงานบุคคลและค่าตอบแทนใหม่ ประกอบด้วย ๗ มาตรการ

ยุทธศาสตร์ ๕ การปรับเปลี่ยนกระบวนทัศน์ วัฒนธรรม และค่านิยม ประกอบด้วย ๔ มาตราการ

ยุทธศาสตร์ ๖ การเสริมสร้างระบบราชการให้ทันสมัย ประกอบด้วย ๔ มาตรการ

ยุทธศาสตร์ ๗ การเปิดระบบราชการให้ประชาชนเข้ามามีส่วนร่วม ประกอบด้วย ๖ มาตรการ

๕. การประเมินผลการปฏิบัติราชการตามคำรับรองการปฏิบัติราชการของส่วนราชการ: KPI (Key Performance Indicators)

โดยให้มีการประเมินการปฏิบัติราชการใน ๒ องค์ประกอบ ตามหนังสือสำนักงาน ก.พ. ที่ นร ๑๐๑๒/ว ๒๐ ลงวันที่ ๓ กันยายน ๒๕๕๒ เรื่อง หลักเกณฑ์และวิธีการประเมินผลการปฏิบัติราชการของข้าราชการพลเรือนสามัญ และหนังสือสำนักงาน ก.พ. ที่ นร ๑๐๐/ว ๒๗ ลงวันที่ ๒๙ กันยายน ๒๕๕๒ เรื่อง มาตรฐานและแนวทางกำหนดความรู้ความสามารถ ทักษะ และสมรรถนะที่จำเป็นสำหรับตำแหน่งข้าราชการพลเรือนสามัญ คือ ๑) ผลสัมฤทธิ์ของการปฏิบัติราชการ และ ๒) พฤติกรรมการปฏิบัติราชการหรือสมรรถนะ

การบริหารราชการแบบบูรณาการ (CEO) ซึ่งมีลักษณะสำคัญ ได้แก่

๑. เป็นระบบบริหารจัดการในแนวราบ (Horizontal Management) ที่ใช้การบูรณาการการทำงานของทุกภาคส่วนในพื้นที่ในลักษณะ “พื้นที่ - พันธกิจ - การมีส่วนร่วม” (Area - Functional - Participation: A-F-P) ในทุกขั้นตอนของการทำงาน เพื่อสร้างความเป็นหุ้นส่วนทางการพัฒนา (Partnership) ในระดับจังหวัด ตลอดจนเพื่อสร้างการทำงานในลักษณะเครือข่าย (Networking)

๒. เป็นระบบบริหารจัดการที่มีเป้าหมายที่การตอบสนองความต้องการของประชาชนผู้ใช้บริการ (Customer Driven) ด้วยระบบงานที่มุ่งเน้นผลสัมฤทธิ์ของงาน (Result-Based) ด้วยมาตรฐานผลงานขั้นสูง (High Performance Output)

๓. เป็นระบบบริหารจัดการที่อยู่ภายใต้กรอบของบทบัญญัติและเจตนารมณ์ของรัฐธรรมนูญ และโครงสร้างการจัดระเบียบบริหารราชการแผ่นดินในปัจจุบัน รวมทั้งหลักการการบริหารกิจการบ้านเมืองและสังคมที่ดี (Good Governance) แต่ได้รับการสนับสนุนทรัพยากรทางการบริหาร ที่จำเป็นเพื่อเพิ่มประสิทธิภาพในการทำงาน

การบริหารงานภาครัฐแนวใหม่ตามแผนยุทธศาสตร์การพัฒนาระบบราชการไทย (พ.ศ.๒๕๕๖ - พ.ศ.๒๕๖๑) แผนยุทธศาสตร์การพัฒนาระบบราชการไทย (พ.ศ.๒๕๕๖ - พ.ศ. ๒๕๖๑) ได้กำหนดประเด็นยุทธศาสตร์ที่สอดคล้องกับการบริหารงานภาครัฐแนวใหม่ โดยกำหนดประเด็นยุทธศาสตร์ ๗ ยุทธศาสตร์ ดังนี้

ยุทธศาสตร์ที่ ๑ : การสร้างความเป็นเลิศในการให้บริการประชาชน

ยุทธศาสตร์นี้มีเป้าหมายเพื่อพัฒนางานบริการของส่วนราชการและหน่วยงานของรัฐสู่ความเป็นเลิศ เพื่อให้ประชาชนมีความพึงพอใจต่อคุณภาพการให้บริการ โดยออกแบบการบริการที่ยึดประชาชนเป็นศูนย์กลาง มีการนำเทคโนโลยีสารสนเทศที่เหมาะสมมาใช้เพื่อให้ประชาชนสามารถใช้บริการได้ง่ายและหลากหลายรูปแบบ เน้นการบริการเชิงรุกที่มีปฏิสัมพันธ์โดยตรงระหว่างภาครัฐและประชาชน การให้บริการแบบเบ็ดเสร็จอย่างแท้จริง พัฒนาระบบการบริหารจัดการข้อร้องเรียนให้มีประสิทธิภาพ รวมทั้งเสริมสร้างวัฒนธรรมการบริการที่เป็นเลิศ

ยุทธศาสตร์ที่ ๒ : การพัฒนาองค์การให้มีขีดสมรรถนะสูงและทันสมัย บุคลากรมีความเป็นมืออาชีพ

ยุทธศาสตร์นี้มีเป้าหมายเพื่อพัฒนาส่วนราชการและหน่วยงานของรัฐสู่องค์การแห่งความเป็นเลิศ โดยเน้นการจัดโครงสร้าง องค์การที่มีความทันสมัย กะทัดรัด มีรูปแบบเรียบง่าย (Simplicity) มีระบบการทำงานที่คล่องตัว รวดเร็ว ปรับเปลี่ยนกระบวนทัศน์ในการทำงาน เน้นการคิดริเริ่มสร้างสรรค์ (Creativity) พัฒนาขีดสมรรถนะของบุคลากรในองค์การ เน้นการทำงานที่มีประสิทธิภาพ สร้างคุณค่าในการปฏิบัติภารกิจของรัฐ ประหยัดค่าใช้จ่าย ในการดำเนินงานต่างๆ และสร้างความรับผิดชอบต่อสังคม อนุรักษ์สิ่งแวดล้อมที่ยั่งยืน

ยุทธศาสตร์ที่ ๓ : การเพิ่มประสิทธิภาพการบริหารสินทรัพย์ของภาครัฐให้เกิดประโยชน์สูงสุด

ยุทธศาสตร์นี้มีเป้าหมายเพื่อวางระบบการบริหารจัดการสินทรัพย์ของราชการอย่างครบวงจร โดยคำนึงถึงค่าใช้จ่ายที่ผูกมัด/ผูกพันติดตามมา (Ownership Cost) เพื่อให้เกิดประโยชน์สูงสุดหรือสร้างมูลค่าเพิ่ม สร้างโอกาสและสร้างความมั่นคงตามฐานะเศรษฐกิจของประเทศ ลดความสูญเสียสิ้นเปลืองและเปล่าประโยชน์ รวมทั้งวางระบบและมาตรการที่จะมุ่งเน้นการบริหารสินทรัพย์เพื่อให้เกิดผลตอบแทนคุ้มค่า สามารถลดต้นทุนค่าใช้จ่ายโดยรวม มีต้นทุนที่ต่ำลง และลดความต้องการของสินทรัพย์ใหม่ที่ไม่จำเป็น อีกทั้งส่งเสริมให้มีการใช้ระบบไอซีทีในการบริหารสินทรัพย์และบูรณาการเข้ากับระบบบริหารจัดการทรัพยากรขององค์การ (Enterprise Resource Planning : ERP) เพื่อเพิ่มประสิทธิภาพการบริหารสินทรัพย์ การบริหารจัดการองค์การโดยรวมและการลดต้นทุน โดยจัดให้มีระบบและข้อมูลเพื่อให้หน่วยราชการใช้ประกอบการวัดและ

วิเคราะห์ การใช้สินทรัพย์เพื่อให้เกิดผลิตภาพ (Asset Productivity) และเกิดประโยชน์สูงสุด (Asset Utilization) เป็นต้น

ยุทธศาสตร์ที่ ๔ : การวางระบบการบริหารงานราชการแบบบูรณาการ

ยุทธศาสตร์นี้มีเป้าหมายเพื่อส่งเสริมการทำงานร่วมกันภายในระบบราชการด้วยกันเองเพื่อแก้ปัญหาการแยกส่วนในการปฏิบัติงาน ระหว่างหน่วยงาน รวมถึงการวางระบบความสัมพันธ์และประสานความร่วมมือระหว่างราชการบริหารส่วนกลาง ส่วนภูมิภาค และส่วนท้องถิ่น ในรูปแบบของการประสานความร่วมมือที่หลากหลาย ภายใต้วัตถุประสงค์ เดียวกัน คือ นำศักยภาพเฉพาะของแต่ละหน่วยงานมาสร้างคุณค่าให้กับงานตามเป้าหมายที่กำหนด เพื่อขับเคลื่อนนโยบาย/ยุทธศาสตร์ของประเทศและการใช้ประโยชน์ทรัพยากรอย่างคุ้มค่า

ยุทธศาสตร์ที่ ๕ : การส่งเสริมระบบการบริหารกิจการบ้านเมืองแบบร่วมมือกันระหว่างภาครัฐภาคเอกชนและภาคประชาชน

ยุทธศาสตร์นี้มีเป้าหมายเพื่อส่งเสริมให้หน่วยงานราชการทบทวนบทบาทและภารกิจของตนให้มีความเหมาะสม โดยให้ ความสำคัญต่อการมีส่วนร่วมของประชาชน มุ่งเน้นการพัฒนารูปแบบความสัมพันธ์ระหว่างภาครัฐกับ ภาคส่วนอื่น การถ่ายโอนภารกิจบางอย่างที่ภาครัฐไม่จำเป็นต้องดำเนินงานเองให้ภาคส่วนอื่น รวมทั้ง การสร้างความร่วมมือหรือความเป็นภาคีหุ้นส่วน (Partnership) ระหว่างภาครัฐและภาคส่วนอื่น

ยุทธศาสตร์ที่ ๖ : การยกระดับความโปร่งใสและสร้างความเชื่อมั่นศรัทธาในการบริหารราชการแผ่นดิน

ยุทธศาสตร์นี้มีเป้าหมายเพื่อส่งเสริมและวางกลไกให้ส่วนราชการและหน่วยงานของรัฐเปิดเผยข้อมูลข่าวสารและสร้าง ความโปร่งใสในการปฏิบัติราชการ รวมทั้งส่งเสริมให้ภาคประชาชนเข้ามามีส่วนร่วมในการตรวจสอบ การทำงานของทางราชการ ตลอดจนการขับเคลื่อนยุทธศาสตร์และมาตรการในการต่อต้านการทุจริต คอร์รัปชั่นให้บรรลุผลสัมฤทธิ์อย่างเป็นรูปธรรม

ยุทธศาสตร์ที่ ๗ : การสร้างความพร้อมของระบบราชการไทยเพื่อเข้าสู่การเป็นประชาคมอาเซียน

ยุทธศาสตร์นี้มีเป้าหมายเพื่อเตรียมความพร้อมของระบบราชการไทยเพื่อรองรับการก้าวเข้าสู่ประชาคมอาเซียน รวมทั้งประสานพัฒนาเครือข่ายความร่วมมือกันในการส่งเสริมและยกระดับธรรมา ภิบาลในภาครัฐของประเทศสมาชิกอาเซียน อันจะนำไปสู่ความมั่งคั่งทางเศรษฐกิจ ความมั่นคงทางการเมือง และความเจริญผาสุกของสังคมร่วมกัน

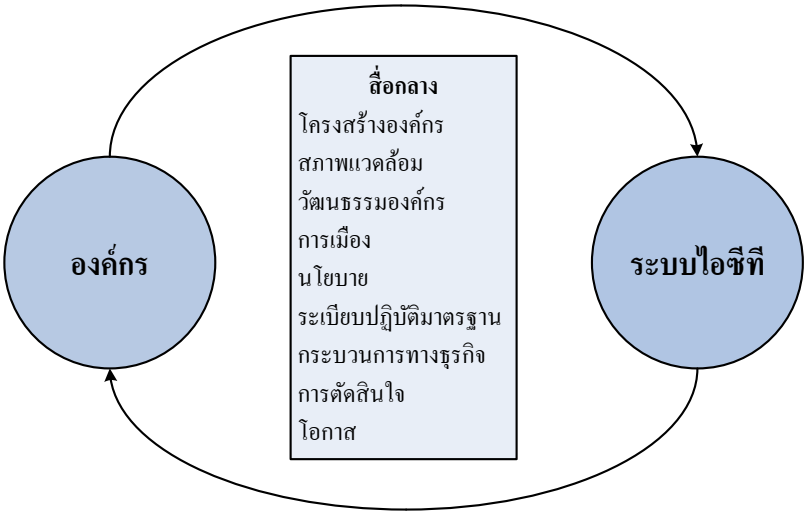
ระบบไอซีทีเพื่อการจัดการ

๑. ผลกระทบของระบบไอซีทีที่มีต่อองค์กร

องค์กรและระบบไอซีทีต่างก็มีลักษณะแห่งการปฏิสัมพันธ์กันโดยอาจจะได้รับอิทธิพลอย่างมากซึ่งมาจากองค์ประกอบที่เป็นสื่อกลางต่างๆ เช่น โครงสร้างองค์กร (Structure), สภาพแวดล้อม (Environment) วัฒนธรรมองค์กร (Organization Culture) การเมือง (Political) นโยบาย (Politic) ระเบียบปฏิบัติมาตรฐาน (Standard Procedures) กระบวนการทางธุรกิจ (Business Processes) การตัดสินใจ (Management Decisions) และโอกาส (Chance) ดังแสดงในแผนภาพที่ ๒ - ๒

องค์กรอาจมีความแตกต่างกันได้จากหลากหลายเหตุผล โดยสิ่งที่ทำให้เกิดความแตกต่างอย่างชัดเจนคือวัตถุประสงค์และความสามารถในการใช้ทรัพยากรเพื่อให้บรรลุวัตถุประสงค์ขององค์กร องค์กรอาจจะมีความแตกต่างกันที่บทบาทของความเป็นผู้นำ ได้แก่ ผู้นำแบบประชาธิปไตย (Democracy) ผู้นำแบบชอบใช้อำนาจ (Authoritarian) ผู้นำแบบตามหลักวิชา (Technocratic) ผู้นำแบบตามหลักการ (Bureaucratic) และผู้นำแบบอ่อนแอ (Laissez-faire) เป็นต้น

แผนภาพที่ ๒ - ๒ ความสัมพันธ์ระหว่างองค์กรและระบบไอซีที

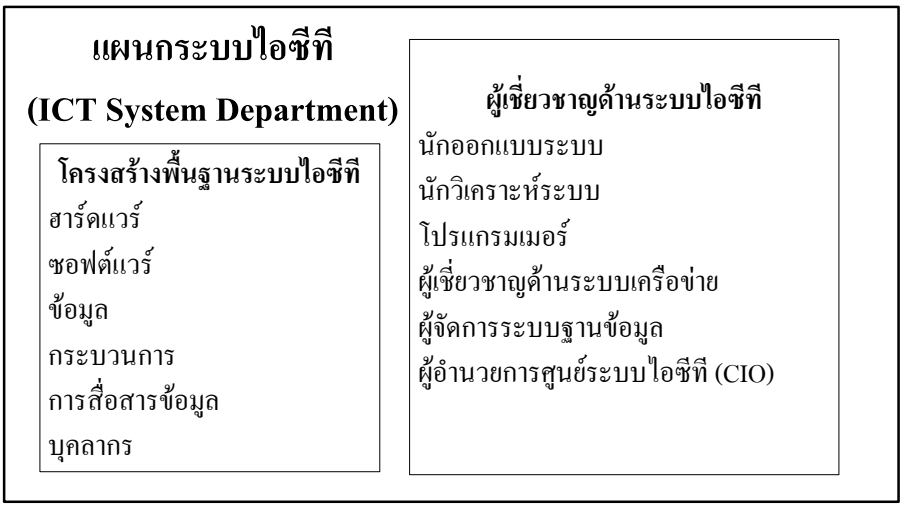


วิธีการนำเทคโนโลยีมาใช้ในการดำเนินงานขององค์กรจะมีความแตกต่างกันได้ ในบางกรณีเมื่อปรับใช้แล้วจะทำให้องค์กรมีความสามารถในการปรับแนวทางการปฏิบัติงานหรือกระบวนการทำงานที่สั้นลง ซึ่งองค์กรแบบนี้มักจะมีโครงสร้างแบบลำดับชั้นและมีระเบียบปฏิบัติ

มาตรฐาน องค์กรอีกประเภทหนึ่งอาจใช้กระบวนการตัดสินปัญหาที่สลับซับซ้อนที่ไม่สามารถเขียนเป็นหลักปฏิบัติมาตรฐานได้โดยการใช้บริษัทที่ปรึกษา ดังนั้นอาจกล่าวได้ว่าระบบไอซีทีที่นำมาประยุกต์ใช้กับการดำเนินงานขององค์กรจะก่อให้เกิดผลกระทบในหลายๆ ด้าน ในการจัดโครงสร้างระบบไอซีทีภายในองค์กรควรจะกำหนดบทบาทของระบบไอซีที ซึ่งจะเป็นการกำหนดทิศทางหรือวิธีการ เช่น การตัดสินใจในการออกแบบ การสร้าง การประยุกต์ใช้ และการบำรุงรักษา เป็นต้น

หน่วยงานที่มีหน้าที่รับผิดชอบอย่างเป็นทางการในเรื่องที่เกี่ยวกับเทคโนโลยีอาจเรียกว่าแผนกระบบไอซีที (ICT System Department) ดังแสดงในแผนภาพที่ ๒ - ๓ ซึ่งจะเป็นโครงสร้างระบบไอซีทีภายในองค์กรที่ใช้ในการกำหนดวิธีการที่จะนำเสนอการบริการไอซีทีทุกชนิดขององค์กร องค์กรสมัยใหม่ในปัจจุบันมีการกำหนดตำแหน่งหัวหน้าหรือผู้อำนวยการศูนย์ระบบไอซีที (Chief ICT System Officer : CIO) ที่จะเป็นผู้บริหารสูงสุดที่รับผิดชอบงานทางด้านระบบไอซีทีขององค์กรโดยเฉพาะ

แผนภาพที่ ๒ - ๓ โครงสร้างระบบไอซีทีภายในองค์กร



๒. บทบาทของระบบสารสนเทศเพื่อการจัดการ

ก่อนที่จะกล่าวถึงบทบาทของระบบสารสนเทศเพื่อการจัดการจะขอกล่าวถึงคำนิยามเบื้องต้นของคำต่อไปนี้

ระบบ (System) หมายถึง กลุ่มส่วนประกอบหรือระบบย่อยต่าง ๆ ที่มีการทำงานร่วมกัน เพื่อให้ประสบผลสำเร็จตามวัตถุประสงค์ที่ตั้งไว้ โดยส่วนประกอบและความสัมพันธ์

ระหว่างส่วนประกอบต่างๆ ในระบบจะเป็นตัวกำหนดว่าระบบจะสามารถทำงานได้อย่างไร เพื่อที่จะให้ผลลัพธ์ที่ได้เป็นไปตามวัตถุประสงค์ที่ต้องการ

สารสนเทศ (Information) หมายถึง กลุ่มข้อมูลที่ถูกจัดการตามกฎหรือถูกกำหนดความสัมพันธ์ให้ เพื่อให้ข้อมูลเหล่านั้นเกิดประโยชน์หรือมีความหมายเพิ่มมากขึ้น ประเภทของสารสนเทศขึ้นอยู่กับความสัมพันธ์ระหว่างข้อมูลที่มีอยู่ ตัวอย่างเช่น จำนวนยอดขายของตัวแทนจำหน่ายแต่ละคนในเดือนมกราคมจัดเป็นข้อมูล เมื่อนำมาประมวลผลรวมกันทำให้ได้ยอดขายรายเดือนของเดือนมกราคม ทำให้ผู้บริหารสามารถนำยอดขายรายเดือนมาพิจารณาว่ายอดขายเป็นไปตามวัตถุประสงค์ขององค์กรหรือไม่ได้ง่ายขึ้น ยอดขายรายเดือนนี้จึงจัดเป็นสารสนเทศ หรือตัวอย่าง เช่น ตัวเลข ๑.๑, ๑.๕, และ ๑.๖ จัดเป็นข้อมูลตัวเลข เนื่องจากเป็นค่าความจริงซึ่งยังไม่สามารถแปลความหมายใดๆ ได้แต่ข้อมูลเหล่านี้จัดเป็นสารสนเทศเมื่ออยู่ในสภาพแวดล้อมที่บ่งบอกความหมายของข้อมูลได้มากขึ้น เช่น เมื่อกล่าวว่า ตัวเลขเหล่านี้คือยอดขายประจำเดือนมกราคม กุมภาพันธ์ และมีนาคม โดยมีหน่วยเป็นหลักล้าน จะทำให้ตัวเลขทั้ง ๓ มีความหมายเกิดขึ้น หรืออาจกล่าวได้ว่ายอดขายเฉลี่ยระหว่างเดือนมกราคมถึงมีนาคมมีค่าเท่ากับ ๑.๔ ล้าน จัดเป็นสารสนเทศที่เกิดขึ้นจากข้อมูลตัวเลขทั้ง ๓ ในเนื้อความนี้อาจใช้คำว่า “ข้อมูลไอซีที” แทนคำว่า “ข้อมูลสารสนเทศ” จะเหมาะสมและให้ความหมายที่ลึกซึ้งกว่า

การจัดการ (Management) หมายถึง การบริหารอย่างมีระบบ ซึ่งประกอบด้วยการกำหนดเป้าหมายและ ทิศทางขององค์กรและการปฏิบัติเพื่อให้บรรลุเป้าหมายนั้น ซึ่งจะต้องมีการวางแผน การจัดการ การกำหนดทิศทาง และการควบคุมเพื่อให้เกิดการใช้ทรัพยากรได้อย่างเหมาะสม

กระบวนการ (Process) หมายถึง การแปลงข้อมูลให้เปลี่ยนเป็นสารสนเทศหรือกล่าวได้ว่า กระบวนการคือกลุ่มของงานที่สัมพันธ์กันเพื่อทำให้เกิดผลลัพธ์ตามที่ต้องการ

Kenneth Laudon and Jane Laudon (๒๐๑๖) กล่าวว่า ระบบสารสนเทศเพื่อการจัดการ หมายถึง ระบบสารสนเทศต่างๆ ที่มีความสัมพันธ์เพื่อการประมวลผล เก็บรักษา และกระจายสารสนเทศ เพื่อสนับสนุนการตัดสินใจ ประสานงาน และควบคุมการทำงานต่างๆ ในองค์กร

อรรถกร เก่งพล (๒๕๕๐) กล่าวว่า ระบบสารสนเทศเพื่อการจัดการ หมายถึง ระบบสารสนเทศที่ได้รับการออกแบบมาให้มีความสัมพันธ์กัน เพื่อการจัดการในด้านการประมวลผล เก็บรักษา วิเคราะห์ และกระจายสารสนเทศเหล่านั้นเพื่อการควบคุมการดำเนินงานต่างๆ

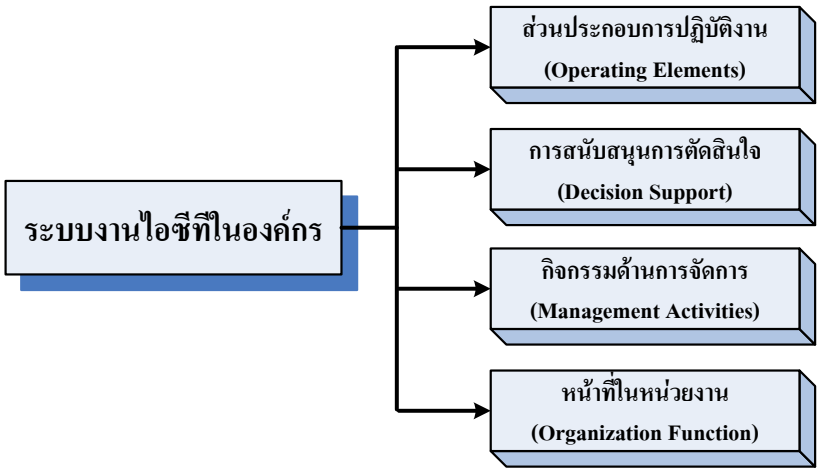
ดังนั้นสรุปได้ว่า ระบบสารสนเทศเพื่อการจัดการ หมายถึง ระบบสารสนเทศรูปแบบต่างๆ ที่ออกแบบมาให้มีความเกี่ยวเนื่องสัมพันธ์กัน เพื่อใช้ในการบริหารจัดการทั้งในด้านการ

รวบรวม ประมวลผล เก็บรักษา และเผยแพร่สารสนเทศเหล่านั้นในรูปแบบต่างๆ ที่กำหนด เพื่อการควบคุมการดำเนินงานและการสนับสนุนการตัดสินใจสำหรับองค์กร

ระบบสารสนเทศเพื่อการจัดการเป็นระบบสนับสนุนการจัดการที่มีรูปแบบธรรมดาที่ผู้ใช้จะได้รับสารสนเทศเพื่อสนับสนุนการตัดสินใจวันต่อวัน จัดเตรียมรายงาน และแสดงต่อระดับจัดการตามเนื้อหาที่ถูกกำหนดไว้ล่วงหน้าโดยดึงสารสนเทศจากฐานข้อมูล ซึ่งมีการปรับปรุงให้ทันสมัยโดยระบบจะประมวลผลรายการเปลี่ยนแปลงและข้อมูลสิ่งแวดล้อมของธุรกิจจากแหล่งภายนอก

ขอบข่ายของระบบสารสนเทศเพื่อการจัดการไม่ใช่เป็นรายการหรือสิ่งหนึ่งสิ่งใดที่แยกออกจากระบบไอซีทีอื่นๆ อย่างจริงจัง แต่เป็นเพียงการกำหนดกรอบที่ระบบไอซีทีใดๆ จะเข้าไปรวมได้อย่างเหมาะสม ดังนั้นคำว่า “ระบบสารสนเทศเพื่อการจัดการ” และ “ระบบไอซีที” จึงอาจเกิดการใช้สับเปลี่ยนได้บางครั้ง ดังนั้นสามารถอธิบายโครงสร้างของระบบงานไอซีทีในองค์กรออกได้เป็น ๔ ส่วน ได้แก่ ๑. ส่วนประกอบการปฏิบัติงาน (Operating Elements) ๒. การสนับสนุนการตัดสินใจ (Decision Support) ๓. กิจกรรมด้านการจัดการ (Management Activities) และ ๔. หน้าที่ในหน่วยงาน (Organization Function) แสดงได้ดังแผนภาพที่ ๒ - ๔ ดังต่อไปนี้

แผนภาพที่ ๒ - ๔ ระบบงานไอซีทีในองค์กร



๑. ส่วนประกอบด้านการปฏิบัติงาน (Operating Elements)

ส่วนประกอบทางกายภาพนับว่าเป็นสิ่งจำเป็นของระบบไอซีทีขององค์กรอาจแสดงในรูปของส่วนประกอบทางกายภาพ (Physical Components) โดยที่ส่วนประกอบต่างๆ เหล่านี้จะ

ทำหน้าที่ในการประมวลผลหรือออกผลรายงานหรือผลลัพธ์ของระบบ โครงสร้างของระบบจะมีดังนี้

๑.๑ ส่วนประกอบทางกายภาพ นับว่าเป็นสิ่งจำเป็นของระบบไอซีทีขององค์กร ส่วนประกอบเหล่านี้ ได้แก่ ฮาร์ดแวร์ ซอฟต์แวร์ ฐานข้อมูล ขั้นตอนการปฏิบัติงาน และพนักงาน เป็นต้น

๑.๒ หน้าที่ในการประมวลผล

๑.๓ รายงานที่ผู้ใช้ต้องการ ผู้ใช้ระบบไอซีทีต้องการรายงานผลลัพธ์ (Output) ที่ได้จากการประมวลผลข้อมูลนำเข้า (Input) รายงานที่ได้นั้นจะต้องเป็นประโยชน์ต่อการใช้งานเป็นอย่างดี กะทัดรัด ได้ใจความ เข้าใจง่าย สะดวกต่อการนำไปใช้และประการสำคัญก็คือ จะต้องให้ความสะดวกหรือง่ายต่อผู้ใช้ที่จะออกรายงานของระบบไอซีที ซึ่งสามารถจะแยกแยะได้เป็น ๕ แบบด้วยกันดังนี้

๑.๓.๑ เอกสารที่แสดงทางหน้าจอคอมพิวเตอร์

๑.๓.๒ รายงานที่ได้จัดวางไว้ล่วงหน้า

๑.๓.๓ การถาม-ตอบตามความต้องการ

๑.๓.๔ รายงานและการถาม-ตอบตามความต้องการ ในบางครั้งคราว (Ad Hoc Reports and Inquiry Responses)

๑.๓.๕ ผลลัพธ์จากการโต้ตอบระหว่างผู้ใช้กับเครื่อง

๒. ระบบไอซีทีเพื่อการจัดการที่ช่วยสนับสนุนการตัดสินใจ (Management ICT System Support for Decision Making)

การตัดสินใจในสิ่งใดๆ อาจจะมีความแตกต่างกันบ้าง ทั้งนี้จะขึ้นอยู่กับโครงสร้างของการตัดสินใจ ถ้ามีโครงสร้างไว้อย่างแน่นอนแล้วก็ย่อมจะกำหนดแผนการตัดสินใจไว้ล่วงหน้าได้ ซึ่งจะตรงกันข้ามกับการตัดสินใจแบบไม่มีโครงสร้าง

๒.๑ การตัดสินใจแบบมีโครงสร้าง (Structured, Programmable Decision) เมื่อมีการกำหนดโปรแกรมการตัดสินใจขึ้น องค์กรจะต้องเตรียมกฎเกณฑ์การตัดสินใจไว้โดยแสดงถึงขั้นตอนที่ต้องปฏิบัติซึ่งอาจจะเป็นการตัดสินใจ (Flow Chart) ตารางการตัดสินใจหรือสูตรต่างๆ ขั้นตอนการตัดสินใจนั้นต้องระบุถึงข้อมูลไอซีทีที่ต้องการ ก่อนที่จะนำไปประยุกต์ใช้กับกฎเกณฑ์การตัดสินใจ ถ้าการตัดสินใจเป็นแบบมีโครงสร้างเจ้าหน้าที่ระดับต่ำก็สามารถตัดสินใจได้ ในความเป็นจริงแล้ว การตัดสินใจแบบนี้มักจะเป็นแบบอัตโนมัติ ถึงอย่างไรก็ตามคนก็ยังเป็นทรัพยากรที่จะต้องนำมาพิจารณาด้วยเช่นกัน ดังตัวอย่างของการตัดสินใจที่มีโครงสร้างอย่างดี เช่น สูตรการหาจุดสั่งสำหรับการคงคลังสินค้า (Inventory) เป็นต้น การตัดสินใจแบบมีโครงสร้างจำเป็นต้องมี

ระบบไอซีทีอย่างเด่นชัดและมีการนำข้อมูลเข้าที่เป็นไปตามขั้นตอนอย่างแน่นอน มีขั้นตอนการตรวจสอบจนเป็นที่แน่ใจได้ว่าถูกต้อง ทั้งความสมบูรณ์ของการนำเข้าและการประมวลผลข้อมูลโดยใช้หลักการตัดสินใจทางตรรกะ (Logic) และผลลัพธ์ที่ได้จากการตัดสินใจแบบนี้จะอยู่ในรูปแบบที่เป็นประโยชน์ต่อการใช้งาน นั่นคือ จะต้องเด่นชัดในแง่ที่ว่าจะนำไปใช้ประโยชน์ได้อย่างไรและควรจะมีข้อมูลอย่างเพียงพอที่จะช่วยให้ผู้รับสามารถนำไปใช้เพื่อการตัดสินใจได้อย่างมีเหตุผล จากหลายกรณีที่เราไม่อาจจะกำหนดขั้นตอนหรือกฎเกณฑ์การตัดสินใจขึ้นมาเพื่อประยุกต์ใช้กับสถานการณ์ธรรมดาทั่วไปให้ได้มากที่สุด สำหรับสถานการณ์ที่แตกต่างออกไปและไม่สามารถที่จะนำมาประยุกต์ใช้ได้เราก็จะใช้คนเป็นผู้ตัดสินใจซึ่งจำเป็นต้องอาศัยความรู้ความสามารถเฉพาะด้าน

๒.๒ การตัดสินใจแบบไม่มีโครงสร้าง (Unstructured, Non Programmable Decision) การตัดสินใจแบบไม่มีโครงสร้างย่อมไม่สามารถจะกำหนดขั้นตอนการตัดสินใจไว้ก่อนล่วงหน้าได้ ทั้งนี้อาจเนื่องมาจากการเปลี่ยนแปลงที่มีบ่อยครั้งทำให้องค์กรต้องเสียค่าใช้จ่ายในการเตรียมขั้นตอนการตัดสินใจ (อาจจะต้องจัดเตรียมโปรแกรมบางส่วน) หรืออาจเนื่องจากความไม่เข้าใจวิธีการประมวลผลดีพอหรือมีการเปลี่ยนแปลงบ่อยครั้งเกินไปจนไม่สามารถจะกำหนดขั้นตอนการตัดสินใจที่เป็นแบบถาวรได้ สิ่งสนับสนุนการตัดสินใจแบบไม่มีโครงสร้างแบบนี้อาจได้แก่ การประมวลผลข้อมูล การวิเคราะห์ข้อมูลแบบต่างๆ และขั้นตอนการตัดสินใจที่จะประยุกต์ใช้เพื่อหาคำตอบจากปัญหา ดังนั้นข้อมูลที่ต้องการอาจจะจัดหามาก่อนล่วงหน้าได้ไม่ครบซึ่งแก้ไขโดยการดึงข้อมูลโดยอาจเกิดขึ้นเป็นบางครั้งบางคราวตามการร้องขอ ระบบไอซีทีที่สนับสนุนการตัดสินใจแบบไม่มีโครงสร้างนี้จะใช้วิธีการถาม-ตอบและการวิเคราะห์โดยทั่วไป

๓. ระบบไอซีทีเพื่อการจัดการที่กำหนดตามกิจกรรมด้านการจัดการ (Management ICT System Structured based on Management Activity)

ระบบไอซีทีเพื่อการจัดการที่สนับสนุนกิจกรรมด้านการจัดการนั้น หมายถึง การจัดแบ่งโครงสร้างระบบไอซีทีไว้เป็นลำดับ (Hierarchy) เพื่อการวางแผนด้านการจัดการ (Management Planning) และควบคุมกิจกรรม (Control Activity) ในส่วนของการควบคุมกิจกรรมด้านการจัดการ (Hierarchy of Management Activity) แอนโทนี่ได้ให้นิยามการวางแผนด้านการจัดการและการควบคุมโดยจัดแบ่งระดับไว้ ได้แก่ ๑) ระบบไอซีทีสำหรับการควบคุมด้านการปฏิบัติงาน (ICT System for Operation Control) ๒) ระบบไอซีทีสำหรับการควบคุมการจัดการ (ICT System for Management Control) และ ๓) ระบบไอซีทีสำหรับการวางแผนกลยุทธ์ (ICT System for Strategic Planning)

การจัดการกิจกรรมทั้ง ๓ ระดับนี้จะมีความแตกต่างกัน ทั้งนี้จะขึ้นอยู่กับการวางแผนของแต่ละระดับ การวางแผนกลยุทธ์เป็นการวางแผนการตัดสินใจระยะยาวที่มีจุดม่งหมายเพื่อแสวงหาทางเลือกเกี่ยวกับทิศทางของธุรกิจ กลยุทธ์ด้านการตลาด และผลิตภัณฑ์ผสม (Product Mix) เป็นต้น การควบคุมด้านการจัดการและการวางแผนยุทธวิธีเป็นการวางแผนในระยะปานกลาง ซึ่งหมายถึง การจัดหาทรัพยากร การจัดโครงสร้างการทำงานให้เป็นระบบ การจัดหาบุคลากร และการฝึกอบรม เป็นต้น สิ่งต่าง ๆ เหล่านี้จะสะท้อนถึงการจัดทำงบประมาณรายจ่ายและการวางแผนอัตรากำลังคนในช่วง ๓-๕ ปี การวางแผนด้านการปฏิบัติงานและการควบคุมเป็นการวางแผนสำหรับการตัดสินใจในระยะสั้นที่เกี่ยวข้องกับการปฏิบัติงานในปัจจุบัน เช่น การกำหนดระดับราคาและการผลิตสินค้าคงคลัง เป็นต้น สิ่งต่างๆ เหล่านี้เป็นผลที่ได้จากการวางแผนด้านการปฏิบัติงานและการควบคุมกิจกรรม ผู้จัดการคนหนึ่งอาจจะรับผิดชอบในกิจกรรมการจัดการหลายๆ อย่างได้แต่จะต้องเป็นไปตามสัดส่วนของการจัดการแต่ละระดับ ดังตัวอย่าง การจัดการในระดับล่างซึ่งหัวหน้า (Supervisor) จะใช้เวลาส่วนใหญ่เกี่ยวกับการวางแผนการปฏิบัติงานและการควบคุม ส่วนการจัดการระดับสูง เช่น รองประธานบริษัทจะใช้เวลาส่วนใหญ่ในการวางแผนกลยุทธ์และกิจกรรมต่าง ๆ และการประมวลผลข้อมูลไอซีทีของทั้ง ๓ ระดับนี้จะมีความเกี่ยวพันธ์ซึ่งกันและกัน ดังตัวอย่างเช่น การควบคุมสินค้าคงคลังในระดับการปฏิบัติงานจะขึ้นอยู่กับการประมวลผลที่ถูกต้อง ในระดับการควบคุมการจัดการ (Management Control) จะเป็นการตัดสินใจเรื่องสต๊อกเพื่อความปลอดภัย (Safety Stock) และความถี่ของการสั่งซื้อซึ่งจะขึ้นอยู่กับการสรุปผลการดำเนินงานที่ถูกต้อง ในระดับของการวางแผนกลยุทธ์จะใช้ผลจากการดำเนินงานและการควบคุมตลอดจนพฤติกรรมของคู่แข่งมากำหนดเป็นวัตถุประสงค์ การควบคุมขององค์กรมีข้อควรสังเกตประการหนึ่งก็คือ คุณลักษณะที่ต้องการของไอซีทีสำหรับการวางแผนกลยุทธ์ซึ่งจะต้องต่างจากคุณลักษณะที่ต้องการของการควบคุมด้านการปฏิบัติงาน ซึ่งความแตกต่างดังกล่าวนี้จะมีผลให้ระบบไอซีทีที่สนับสนุนการวางแผนกลยุทธ์นั้นแตกต่างจากระบบไอซีทีที่สนับสนุนด้านการควบคุมด้านการปฏิบัติงานอย่างเห็นได้ชัด โดยการตัดสินใจจะแตกต่างกันไปซึ่งจะขึ้นอยู่กับว่ากิจกรรมด้านการจัดการนั้นจะขึ้นอยู่ในระดับใด เช่น การตัดสินใจในระดับการควบคุมด้านการปฏิบัติงานซึ่งส่วนใหญ่แล้วจะเป็นแบบมีโครงสร้างหรือการตัดสินใจในระดับการวางแผน กลยุทธ์ซึ่งจะเป็นแบบไม่มีโครงสร้าง ระบบการตัดสินใจแบบมีโครงสร้างนั้นได้กำหนดหลักเกณฑ์การตัดสินใจและมีรายงานเตือนภัย (Exception Report) แต่ค่อนข้างจะมีความยืดหยุ่น (Flexible) น้อยในเรื่องของเนื้อหาหรือรายละเอียดและรูปแบบส่วนสนับสนุนการตัดสินใจ (Decision System : DSS) จะเป็นไปในทางตรงกันข้าม นั่นคือ จะมีลักษณะใช้ยืดหยุ่นต่อข้อมูล รูปแบบของผลลัพธ์ และการเก็บ

รวบรวมต้นแบบการตัดสินใจ ส่วนประกอบต่างๆ นับว่าเป็นการช่วยสนับสนุนต่อกระบวนการตัดสินใจของผู้จัดการมากกว่าที่จะกำหนดให้หรือทำการตัดสินใจให้กับผู้ใช้

สำหรับหัวข้อที่จะกล่าวต่อไปนี้จะเป็นการสรุปคุณลักษณะของระบบไอซีทีที่สนับสนุนระดับการวางแผนด้านการจัดการและการควบคุมทั้ง ๓ ระดับดังนี้

๓.๑ ระบบไอซีทีสำหรับการควบคุมด้านการปฏิบัติงาน (ICT System for Operation Control) เป็นกระบวนการเพื่อต้องการจะตรวจสอบดูว่ากิจกรรมที่ได้ดำเนินไปนั้นก่อให้เกิดประสิทธิภาพและประสิทธิผลหรือไม่จากการใช้วิธีการที่กำหนดไว้ล่วงหน้า ตลอดจนหลักเกณฑ์ในการตัดสินใจขั้นตอนในการปฏิบัติงานส่วนใหญ่จะไม่ค่อยมีการเปลี่ยนแปลงการตัดสินใจและผลลัพธ์ที่เกิดขึ้นจะครอบคลุมในช่วงเวลาสั้นๆ (๑ วันหรือ ๑ สัปดาห์) รายการแต่ละรายการค่อนข้างจะมีความสำคัญดังนั้นระบบการปฏิบัติงานจึงต้องสามารถตอบสนองรายการแต่ละประเภท (Individual Transaction) และแสดงผลสรุปของทุกๆ รายการ การประมวลที่สนับสนุนการควบคุมด้านการปฏิบัติงานอาจจะประกอบด้วย ๑) การประมวลผลรายการ (Transaction Processing) ๒) การประมวลผลรายงาน (Report Processing) และ ๓) การประมวลผลการร้องขอ (Inquiry Processing) เป็นต้น

การประมวลทั้ง ๓ แบบ จะมีลักษณะของการนำมาใช้เพื่อการตัดสินใจที่แตกต่างกัน ทั้งนี้จะขึ้นอยู่กับกฎเกณฑ์การตัดสินใจที่กำหนดไว้ก่อนล่วงหน้า ดังตัวอย่างจะแสดงถึงรูปแบบที่มีขั้นตอนการตัดสินใจที่ได้กำหนดไว้สำหรับระบบการควบคุมด้านการปฏิบัติงาน ดังเช่น

๓.๑.๑ รายการเบิกวัสดุคงคลังจะผลิตเอกสารรายการ (Transaction Document) โดยผ่านโปรแกรมการประมวลผลรายการ ซึ่งจะทำการตรวจสอบจำนวนที่เหลือด้วยมือ (Balance on Hand) และทำการตัดสินใจ (โดยใช้กฎเกณฑ์ที่กำหนดไว้ก่อนล่วงหน้าถ้าวัสดุลดต่ำลงมาถึงจุดสั่งก็จะคำนวณหาปริมาณการสั่งจากสูตร “การหาปริมาณสั่งอย่างประหยัด”) ต่อจากนั้นจะเป็นการผลิตเอกสารการดำเนินการ (Action Document) ที่จะระบุถึงรายการและจำนวนที่จะสั่งซื้อผู้วิเคราะห์สินค้าคงคลังอาจจะยอมรับหรืออาจจะทำการปรับปรุงจำนวนที่จะสั่งเสียใหม่หรือไม่สนใจกับโปรแกรมการตัดสินใจ

๓.๑.๒ การสอบถามจากแฟ้มประวัติบุคลากร จะเป็นการสอบถามเพื่อดูคุณสมบัติที่เหมาะสมกับตำแหน่งงานที่ว่างอยู่โดยใช้คอมพิวเตอร์ ซึ่งโปรแกรมจะทำการค้นหา เลือก และจัดเรียงลำดับผู้มีสิทธิ์ที่จะได้รับการพิจารณา

๓.๑.๒ พนักงานปฏิบัติงานที่รับการสั่งซื้อสินค้าทางโทรศัพท์ โดยจะนำข้อมูลเข้าดูผลลัพธ์ทางจอภาพแบบออนไลน์ ในกรณีที่สินค้าขาดสต๊อกโปรแกรมการตัดสินใจที่กำหนดไว้

จะถูกนำมาใช้เพื่อหารายการทดแทนซึ่งผู้รับโทรศัพท์สามารถจะแนะนำรายการทดแทนให้กับลูกค้าได้

๓.๑.๓ โปรแกรมการตัดสินใจที่กำหนดไว้ในการประมวลผลรายงานอาจจะเป็นสาเหตุของการออกรายงานพิเศษเพื่อการจัดหาข้อมูลไอซีทีให้กับปัญหาที่กำลังประสบอยู่ดังตัวอย่างเช่น รายงานที่แสดงถึงการสั่งซื้อที่มีการจ่ายเงินล่าช้าค่อนข้างสูงภายในกำหนดเวลา ๓๐ วัน

ฐานข้อมูลสำหรับการควบคุมด้านการปฏิบัติงาน (Operation Control) และการตัดสินใจด้านการปฏิบัติงาน (Operational Decision Making) จะใช้ข้อมูลภายใน (Internal Data) ที่สร้างขึ้นจากรายการต่างๆ (Transaction) รายการข้อมูลเหล่านี้โดยปกติแล้วค่อนข้างจะเป็นปัจจุบัน (Current) สิ่งที่สำคัญอีกประการหนึ่งคือ การแปลความข้อมูลที่ถูกบันทึกไว้จากการดำเนินงานจะต้องเป็นไปอย่างรอบคอบตามขั้นตอนของกระบวนการนั้นๆ ดังตัวอย่างเมื่อได้รับสินค้าใหม่เข้าจะต้องนำไปบวกเข้ากับจำนวนสินค้าคงคลังก่อนที่จะมีการเบิกจ่าย ทั้งนี้เพื่อป้องกันการขาดสต๊อกนั่นเอง

๓.๒ ระบบไอซีทีสำหรับการควบคุมการจัดการ (ICT System for Management Control)

ผู้จัดการแผนกหรือศูนย์ควบคุมกำไรต้องการระบบไอซีทีสำหรับการควบคุมด้านการจัดการเพื่อใช้วัดประสิทธิภาพการปฏิบัติงาน (Performance) ในการตัดสินใจเกี่ยวกับการควบคุมด้านการปฏิบัติงาน เพื่อใช้กำหนดกฎเกณฑ์การตัดสินใจใหม่ๆ ให้แก่ผู้ปฏิบัติงานและใช้ในการจัดเตรียมทรัพยากร นอกจากนั้นไอซีทีสรุป (Summary ICT) ก็นับว่ามีความจำเป็นที่จะต้องจัดสร้างขึ้นเพื่อทำความเข้าใจถึงสาเหตุของการเปลี่ยนแปลงในประสิทธิภาพการปฏิบัติงาน ตลอดจนเป็นแนวทางในการแก้ปัญหา ซึ่งกระบวนการด้านการควบคุมต้องการไอซีทีแบบต่างๆ ดังต่อไปนี้

๑) ไอซีทีที่เกี่ยวกับประสิทธิภาพด้านการปฏิบัติงานที่ได้กำหนดไว้ล่วงหน้า (Planned Performance) เช่น มาตรฐานที่คาดหวังด้านงบประมาณและอื่นๆ

๒) ไอซีทีที่บอกถึงค่าความแปรปรวน (Variance) จากประสิทธิภาพการปฏิบัติงานที่ได้กำหนดไว้ล่วงหน้า (Planned Performance)

๓) ไอซีทีที่บอกถึงสาเหตุและเหตุผลของความแปรปรวน

๔) ไอซีทีที่ใช้สำหรับการวิเคราะห์เพื่อการตัดสินใจหรือเพื่อเป็นแนวทางในการปฏิบัติ

ฐานข้อมูลสำหรับการควบคุมด้านการจัดการจะประกอบด้วยส่วนประกอบหลักๆ ๒ ส่วน คือฐานข้อมูลที่เตรียมขึ้นสำหรับการปฏิบัติงานและฐานข้อมูลเพื่อจัดทำแผนงาน มาตรฐานงบประมาณและอื่นๆ ซึ่งจะเป็นการคาดคะเนความต้องการเกี่ยวกับประสิทธิภาพด้านการ

ปฏิบัติงาน นอกจากนั้นยังอาจจะต้องใช้ข้อมูลจากภายนอก (External Data) เช่น ข้อมูลตลาดทุน ดัชนีราคา และข้อมูลอื่นๆ เพื่อการเปรียบเทียบในอุตสาหกรรมประเภทเดียวกัน

กระบวนการที่มีส่วนช่วยสนับสนุนกิจกรรมด้านการควบคุมเพื่อการ บริหารจัดการที่เกี่ยวข้องมีดังต่อไปนี้

๑. ตัวแบบการวางแผนหรืองบประมาณ โดยมีส่วนช่วยผู้จัดการในการค้นหาปัญหาจัดเตรียมทบทวนและจัดทำงบประมาณ นอกจากนั้นยังจะต้องมองไปข้างหน้าถึงผลที่เกิดขึ้นจากการกระทำในปัจจุบัน (Current Actions)

๒. รายงานที่จัดทำตามหมายกำหนดการ ซึ่งเป็นรายงานที่แสดงถึงประสิทธิภาพการปฏิบัติงานและความแปรปรวน โดยเปรียบเทียบกับประสิทธิภาพการปฏิบัติงานที่กำหนดไว้หรือมาตรฐานอื่นๆ เช่น ประสิทธิภาพของคู่แข่ง เป็นต้น

๓. ตัวแบบการวิเคราะห์ (ปัญหา) สำหรับการวิเคราะห์ข้อมูลที่ใช้เป็นปัจจัยนำเข้าเพื่อการตัดสินใจ

๔. ตัวแบบการตัดสินใจ เป็นตัวแบบที่ใช้ในการวิเคราะห์สถานการณ์ของปัญหาและหาคำตอบ รวมถึงการใช้ประเมินผลด้านการบริหารจัดการ

๕. ตัวแบบการถาม-ตอบ เพื่อช่วยในการตอบคำถาม

ผลลัพธ์ที่ได้จากระบบไอซีทีสำหรับการควบคุมด้านการจัดการดังกล่าวนี้ ได้แก่ แผนงานและงบประมาณ รายงานตามกำหนดการ รายงานพิเศษ การวิเคราะห์สถานการณ์ปัญหาการตัดสินใจเพื่อให้มีการทบทวน และการตอบคำถามตามการร้องขอ (Request)

๓.๓ ระบบไอซีทีสำหรับการวางแผนกลยุทธ์ (ICT System for Strategic Planning)

จุดประสงค์ของการวางแผนกลยุทธ์ก็เพื่อที่จะพัฒนากลยุทธ์ที่ทำให้องค์กรนั้นสามารถบรรลุวัตถุประสงค์ตามความต้องการ โดยปกติแล้วการวางแผนกลยุทธ์มักจะครอบคลุมช่วงระยะเวลาที่ยาวนาน ดังนั้นจึงอาจจะมีการเปลี่ยนแปลงเกิดขึ้นในองค์กรได้ ดังตัวอย่างเช่น

๓.๓.๑ อาจมีการตัดสินใจที่จะส่งสินค้าทางเครื่องบินโดยสารตามสาขาของห้างสรรพสินค้าในต่างจังหวัด

๓.๓.๒ อาจมีการตัดสินใจขายสินค้าลดราคาตามสาขาของห้างสรรพสินค้าที่อยู่แถบชานเมืองเพื่อการขยายจุดบริการสินค้าให้ถึงผู้บริโภคโดยเร็วในสภาวะเศรษฐกิจซบเซา

๓.๓.๓ บริษัทผลิตสินค้าอุตสาหกรรมอาจจะตัดสินใจขยายธุรกิจกับการผลิตสินค้าอุปโภคบริโภคเพื่อขยายส่วนแบ่งทางการตลาด (Market Chair) ให้ครอบคลุมทุกส่วนของภาคธุรกิจ

กิจกรรมต่างๆ ในการวางแผนกลยุทธ์ไม่จำเป็นต้องเกิดขึ้นในช่วงเวลาที่แน่นอนหรือเป็นไปอย่างสม่ำเสมอเหมือนกับกิจกรรมการควบคุมด้านการจัดการ แต่อาจจะกำหนดไว้ในช่วงการวางแผนประจำปีหรือในรอบปีงบประมาณก็ได้ ข้อมูลที่ต้องการสำหรับการวางแผนกลยุทธ์โดยทั่วๆ ไปแล้วจะใช้ข้อมูลสรุปจากแหล่งต่างๆ นอกจากนั้นข้อมูลภายนอกก็นับว่ามีความจำเป็นที่จะต้องนำมาพิจารณา สำหรับตัวอย่างข้อมูลบางชนิดที่จะกล่าวถึงต่อไปนี้นับว่ามีประโยชน์และจำเป็นต่อการวางแผนกลยุทธ์ ได้แก่ สภาวะเศรษฐกิจของบริษัทในปัจจุบันและกิจกรรมต่างที่คาดหวังไว้ในอนาคต สภาวการณ์ทางการเมืองในปัจจุบันและในอนาคต ความสามารถและประสิทธิภาพเกี่ยวกับด้านการตลาดขององค์กร ในปัจจุบัน (ขึ้นอยู่กับนโยบายแต่ละขณะ) โอกาสทางอุตสาหกรรมของแต่ละประเทศ ความสามารถของคู่แข่งและส่วนแบ่งการตลาด โอกาสที่จะลงทุนในโครงการใหม่ๆ โดยพิจารณาจากการพัฒนาที่เป็นอยู่ในปัจจุบัน และที่คาดว่าจะเกิดขึ้นในอนาคต กลยุทธ์อื่นๆ และแนวโน้มความต้องการทรัพยากรสำหรับกลยุทธ์อื่นๆ

ฐานข้อมูลนี้จะบรรลุข้อมูลที่ใช้ประจำ แต่การเรียกใช้ข้อมูลในบางครั้งก็ขึ้นอยู่กับการพิจารณาการจัดเก็บข้อมูลจำนวนมากซึ่งไม่สามารถจะกระทำได้ด้วยวิธีธรรมดา และไม่สามารถจะกำหนดไว้ล่วงหน้าได้อย่างสมบูรณ์ ก็เป็นเหตุผลหนึ่งที่มีผู้โต้แย้งว่าเป็นไปไม่ได้ที่จะมีระบบไอซีทีเพื่อการจัดการสำหรับกิจกรรมการวางแผนกลยุทธ์ โดยชี้ให้เห็นถึงความไม่มีประสิทธิภาพและเกิดความยุ่งยากในการเขียนโปรแกรม การจัดเก็บ และการดึงข้อมูลต่างๆ เพื่อที่จะนำมาใช้งานด้านอุตสาหกรรม การตลาด หรือเศรษฐกิจ ถึงแม้ว่าระบบไอซีทีจะไม่สามารถสนับสนุนการวางแผนกลยุทธ์ได้อย่างสมบูรณ์เหมือนกับการควบคุมการจัดการและการปฏิบัติงาน แต่ถ้ามองในอีกแง่มุมหนึ่งแล้วระบบที่เป็นแหล่งไอซีทีที่จะช่วยในการประมวลผลเพื่อการวางแผนกลยุทธ์ ดังเช่น

๑. การประเมินผลกำลังความสามารถในปัจจุบัน โดยการใช้ข้อมูลจากภายนอกในองค์กรแล้วทำการประมวลผล แต่อาจจำเป็นต้องใช้วิธีเฉพาะหรือวิธีพิเศษเพื่อหาข้อสรุป ทั้งนี้เพื่อประโยชน์ในการวางแผนงานทางธุรกิจในโอกาสต่อไป

๒. การวางแผนกำลังความสามารถขั้นต้น ซึ่งจะได้จากการวิเคราะห์ข้อมูลในอดีตโดยฝ่ายจัดการจะยึดถือเอาประสบการณ์เป็นหลักในการพิจารณา

๓. มีการจัดเก็บข้อมูลทางด้านการตลาดและของคู่แข่งไว้ในระบบฐานข้อมูลขององค์กร

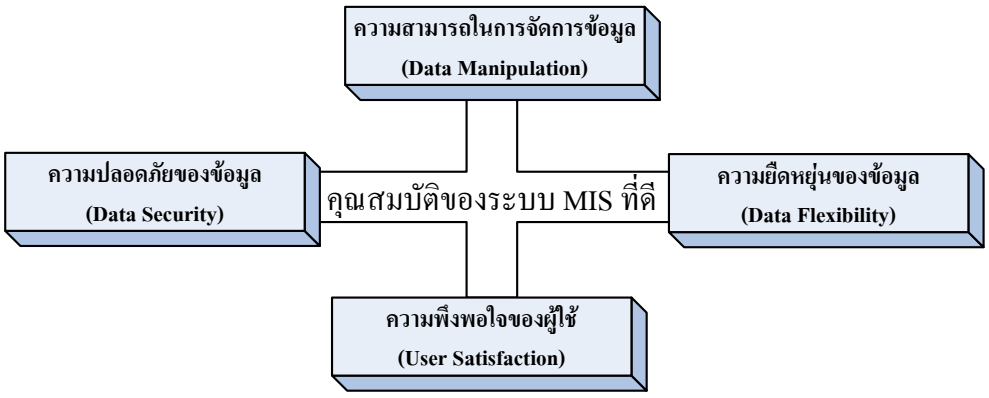
๔. มีการจัดซื้อจัดหาไอซีทีทางด้านอุตสาหกรรมและไอซีทีคู่แข่งที่อยู่ในรูปแบบที่เครื่องสามารถอ่านได้เพื่อใช้กับตัวแบบการวางแผนและตัดสินใจ

๓.๔ ระบบไอซีทีเพื่อการจัดการที่กำหนดตามหน้าที่ในองค์กร (Management ICT System Structured Based on Organizational Function)

การจัดการภายในองค์กรจะประกอบด้วยหน้าที่ต่างๆ มากมาย ซึ่งในแต่ละหน้าที่ก็ต้องการไอซีทีที่แตกต่างกันออกไป แต่โดยทั่วไปแล้วไอซีทีของระบบย่อยจะถูกออกแบบตามลักษณะการปฏิบัติงานตามหน้าที่เป็นส่วนใหญ่ เนื่องจากมีโครงสร้างการวิเคราะห์ที่ชัดเจนกว่าวิธีอื่นๆ จากที่ได้อธิบายไว้ข้างต้นแล้วว่า ระบบสารสนเทศเพื่อการจัดการเป็นระบบที่เกิดจากการรวมระบบไอซีทีหลายระบบเข้าด้วยกันโดยมีการออกแบบไว้เพื่อสนับสนุนหน้าที่ของระบบย่อยต่างๆ ในองค์กร ซึ่งอาจจะมีการเรียกใช้ฐานข้อมูล ตัวแบบ หรือโปรแกรมคอมพิวเตอร์จากส่วนกลางที่ต้องใช้ร่วม (Common) กับหน้าที่ในระบบย่อยอื่นๆ นอกจากนั้นภายในระบบย่อยแต่ละระบบก็อาจจะมีโปรแกรมประยุกต์ที่สามารถจะประมวลผลการควบคุม การปฏิบัติการควบคุม การจัดการและการวางแผนกลยุทธ์อีกด้วย

ปัจจุบันองค์กรสามารถพัฒนาระบบไอซีทีด้วยตนเองหรือให้ผู้เชี่ยวชาญจากภายนอกเข้าดำเนินการ โดยการออกแบบและพัฒนาระบบสารสนเทศเพื่อการจัดการที่สอดคล้องตามหลักการ ระบบก็จะสามารถอำนวยประโยชน์ให้กับองค์กรได้อย่างเต็มประสิทธิภาพ การพัฒนาระบบไอซีทีต้องคำนึงถึงคุณสมบัติที่สำคัญของระบบสารสนเทศเพื่อการจัดการดังต่อไปนี้ แสดงได้ดังแผนภาพที่ ๒ - ๕

แผนภาพที่ ๒ - ๕ คุณสมบัติที่สำคัญของระบบสารสนเทศเพื่อการจัดการที่ดี



๓.๔.๑ ความสามารถในการจัดการข้อมูล (Data Manipulation) ระบบไอซีทีที่ดีต้องสามารถปรับปรุงแก้ไขและจัดการกับข้อมูล ทั้งนี้เพื่อให้เป็นระบบไอซีทีที่พร้อมสำหรับนำไปใช้งานอย่างมีประสิทธิภาพ ปกติข้อมูลต่างๆ ที่เกี่ยวข้องกับการดำเนินธุรกิจจะมีการเปลี่ยนแปลงอยู่ตลอดเวลาดังนั้นข้อมูลที่ถูกป้อนเข้าสู่ระบบควรที่จะได้รับการปรับปรุงแก้ไขและพัฒนารูปแบบ ทั้งนี้เพื่อให้มีความทันสมัยและเหมาะสมกับการใช้งานอยู่เสมอ

๓.๔.๒ ความปลอดภัยของข้อมูล (Data Security) ระบบไอซีทีเป็นทรัพยากรที่สำคัญอีกอย่างขององค์กร ถ้าข้อมูลไอซีทีบางประเภทรั่วไหลออกไปสู่บุคคลภายนอกโดยเฉพาะคู่แข่งขันอาจทำให้เกิดการเสียโอกาสทางการแข่งขันหรือสร้างความเสียหายแก่ธุรกิจ ความสูญเสียที่เกิดขึ้นอาจจะเกิดจากความรู้เท่าไม่ถึงการณ์หรือการก่อการร้ายต่อระบบ ซึ่งจะมีผลโดยตรงต่อประสิทธิภาพและความเป็นอยู่ขององค์กรอย่างแน่นอน

๓.๔.๓ ความยืดหยุ่นของข้อมูล (Data Flexibility) สภาพแวดล้อมในการดำเนินธุรกิจหรือสถานการณ์การแข่งขันทางการค้าที่เปลี่ยนแปลงอย่างรวดเร็ว ส่งผลให้ระบบไอซีทีที่ดีต้องมีความสามารถในการปรับตัวเพื่อให้สอดคล้องกับการใช้งานหรือปัญหาที่เกิดขึ้น โดยที่ระบบไอซีทีที่ถูกสร้างหรือถูกพัฒนาขึ้นต้องสามารถตอบสนองต่อความต้องการของผู้บริหารได้อยู่เสมอ โดยมีอายุการใช้งาน การบำรุงรักษา และค่าใช้จ่ายที่เหมาะสมซึ่งก็คือมีความยืดหยุ่นนั่นเอง

๓.๔.๔ ความพึงพอใจของผู้ใช้ (User Satisfaction) ปกติระบบไอซีทีถูกพัฒนาขึ้นโดยมีความมุ่งหวังให้ผู้ใช้สามารถนำมาประยุกต์ในงานหรือเพิ่มประสิทธิภาพในการทำงาน ระบบไอซีทีที่ดีจะต้องกระตุ้นหรือโน้มน้าวให้ผู้ใช้หันมาใช้ระบบให้มากขึ้น โดยการพัฒนาระบบต้องทำการพัฒนาให้ตรงกับความต้องการและพยายามทำให้ผู้ใช้พอใจกับระบบ เมื่อผู้ใช้เกิดความไม่พอใจกับระบบ จะทำให้ความสำคัญของระบบลดน้อยลงไปหรืออาจจะทำให้ไม่คุ้มค่าต่อการลงทุนก็เป็นได้

ผลลัพธ์ที่ได้จากระบบไอซีทีเพื่อการจัดการคือกลุ่มของรายงานต่างๆ ซึ่งจะถูกส่งไปให้กับผู้บริหาร รายงานเหล่านี้อาจได้แก่

๑. รายงานตามตารางเวลา (Schedule Reports) เป็นรายงานที่เกิดขึ้นตามช่วงเวลาหรือตามตารางเวลา ดังเช่น รายวัน รายสัปดาห์ และรายเดือน ดังตัวอย่างของผู้จัดการฝ่ายผลิตต้องการใช้รายงานรายสัปดาห์เพื่อแสดงรายการค่าใช้จ่ายด้านค่าแรงรวม ทั้งนี้เพื่อตรวจสอบและควบคุมค่าใช้จ่ายของงานและแรงงาน รายงานตามตารางเวลาจะช่วยให้ผู้บริหารควบคุมเครดิตของลูกค้า ประสิทธิภาพของตัวแทนจำหน่าย และระดับสินค้าคงคลังได้

๒. รายงานแสดงส่วนประกอบสำคัญ (Key Indicator Reports) เป็นสรุปการปฏิบัติงานที่วิกฤติของวันก่อนหน้าและยังคงมีอยู่ในตอนต้นของแต่ละวันทำงาน รายงานเหล่านี้สามารถสรุประดับของสินค้าคงคลัง งานในการผลิต และปริมาณการขาย เป็นต้น โดยใช้สำหรับผู้จัดการและผู้บริหารระดับสูงที่ต้องการความรวดเร็วในการดำเนินธุรกิจได้อย่างถูกต้อง

๓. รายงานตามคำขอ (Demand Reports) เป็นการให้ข้อมูลตามที่ผู้จัดการร้องขอ เช่น เมื่อผู้บริหารระดับสูงต้องการทราบการผลิตของสินค้ารายการหนึ่งก็จะทำการสร้างรายงานตามความต้องการนี้ออกมา

๔. รายงานกรณียกเว้น (Exception Reports) เป็นรายงานที่ถูกผลิตออกมาอย่างอัตโนมัติเมื่อมีเหตุการณ์ที่ไม่ปกติเกิดขึ้นหรือเมื่อต้องการใช้ในการดำเนินการบริหาร

๕. รายงานแบบเจาะลึกรายละเอียด (Drill Down Reports) เป็นรายงานที่ให้รายละเอียดข้อมูลที่เกี่ยวกับสถานการณ์หนึ่งๆ

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ.๒๕๖๐

พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ.๒๕๕๐ นับเป็นกฎหมายที่กำหนดขึ้นเพื่อใช้บังคับเพิ่มเติมจากพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ โดยตรงเกี่ยวกับการรักษาความปลอดภัยแห่งชาติ แต่มีความสำคัญอย่างยิ่งในการถือปฏิบัติ และสนับสนุนให้การรักษาความมั่นคงปลอดภัยและผลประโยชน์แห่งรัฐดำรงอยู่ได้ในปัจจุบัน นอกจากนี้ ยังเป็นกฎหมายอีกฉบับที่มีการกำหนดบทลงโทษต่อผู้กระทำผิดหรือละเมิดและมีผลกับทุกภาคส่วนตั้งแต่ภาคประชาชน ภาคเอกชน ตลอดจนภาครัฐ สรุปสาระสำคัญเกี่ยวกับฐานความผิดโดยเพิ่มเติมดังมาตราสำคัญต่อไปนี้

มาตรา ๔ ให้เพิ่มความต่อไปนี้เป็นวรรคสองและวรรคสามของมาตรา ๑๑ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐

“ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นอันมีลักษณะเป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ โดยไม่เปิดโอกาสให้ผู้รับสามารถบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย ต้องระวางโทษปรับไม่เกินสองแสนบาท

ให้รัฐมนตรีออกประกาศกำหนดลักษณะและวิธีการส่ง รวมทั้งลักษณะและปริมาณของข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ ซึ่งไม่เป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับและลักษณะอันเป็นการบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย”

มาตรา ๑๒ ถ้าการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ หรือมาตรา ๑๑ เป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษา ความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงเจ็ดปี และปรับตั้งแต่ สองหมื่นบาทถึงหนึ่งแสนสี่หมื่นบาท

ถ้าการกระทำความผิดตามวรรคหนึ่งเป็นเหตุให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ดังกล่าว ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงสิบปี และปรับตั้งแต่สองหมื่นบาทถึงสองแสนบาท

ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐ เป็นการกระทำต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ตามวรรคหนึ่ง ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท ถ้าการกระทำความผิดตามวรรคหนึ่งหรือวรรคสามโดยมิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่ห้าปีถึงยี่สิบปีและปรับตั้งแต่หนึ่งแสนบาทถึงสี่แสนบาท

มาตรา ๑๔ ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(๑) โดยทุจริต หรือโดยหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือน หรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหาย แก่ประชาชน อันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา

(๒) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิด ความเสียหายต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคง ในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือก่อให้เกิด ความตื่นตระหนกแก่ประชาชน

(๓) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ อันเป็นความผิดเกี่ยวกับความมั่นคง แห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(๔) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันลามกและข้อมูล คอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(๕) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (๑) (๒) (๓) หรือ (๔)

ถ้าการกระทำความผิดตามวรรคหนึ่ง (๑) มิได้กระทำต่อประชาชน แต่เป็นการกระทำต่อบุคคลใด บุคคลหนึ่ง ผู้กระทำ ผู้เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์ดังกล่าวต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ และให้เป็นความผิดอันยอมความได้

มาตรา ๑๖ ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ

เติม หรือดัดแปลง ด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี และปรับไม่เกินสองแสนบาท

ถ้าการกระทำตามวรรคหนึ่งเป็นการกระทำต่อภาพของผู้ตาย และการกระทำนั้นน่าจะทำให้บิดา มารดา คู่สมรส หรือบุตรของผู้ตายเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง หรือได้รับความอับอาย ผู้กระทำต้องระวางโทษดังที่บัญญัติไว้ในวรรคหนึ่ง

ถ้าการกระทำตามวรรคหนึ่งหรือวรรคสอง เป็นการนำเข้าสู่ระบบคอมพิวเตอร์โดยสุจริตอันเป็น การติชมด้วยความเป็นธรรม ซึ่งบุคคลหรือสิ่งใดอันเป็นวิสัยของประชาชนย่อมกระทำ ผู้กระทำไม่มีความผิดตามวรรคหนึ่งและวรรคสองเป็นความผิดอันยอมความได้

ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งหรือวรรคสองตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรส หรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย”

มาตรา ๑๘ ภายใต้บังคับมาตรา ๑๙ เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มี เหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ หรือในกรณีที่มีการร้องขอตามวรรคสอง ให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็น หลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด

(๑) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดมาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

(๒) เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์ หรือจากบุคคลอื่นที่เกี่ยวข้อง

(๓) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา ๒๖ หรือที่อยู่ ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่หรือให้เก็บข้อมูลดังกล่าวไว้ก่อน

(๔) ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์จากระบบคอมพิวเตอร์ที่มี เหตุอันควรเชื่อได้ว่ามีการกระทำความผิด ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครอง ของพนักงานเจ้าหน้าที่

(๕) สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่

(๖) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็น

หลักฐานเกี่ยวกับ การกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้

(๗) ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับ ของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

(๘) ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิด

มาตรา ๒๐ ในกรณีที่มีการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ดังต่อไปนี้ พนักงานเจ้าหน้าที่ โดยได้รับความเห็นชอบจากรัฐมนตรีอาจยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มี คำสั่งระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์ได้

(๑) ข้อมูลคอมพิวเตอร์ที่เป็นความผิดตามพระราชบัญญัตินี้

(๒) ข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรตามที่กำหนดไว้ ในภาค ๒ ลักษณะ ๑ หรือลักษณะ ๑/๑ แห่งประมวลกฎหมายอาญา

(๓) ข้อมูลคอมพิวเตอร์ที่เป็นความผิดอาญาตามกฎหมายเกี่ยวกับทรัพย์สินทางปัญญาหรือกฎหมายอื่นซึ่งข้อมูลคอมพิวเตอร์นั้นมีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน และเจ้าหน้าที่ตามกฎหมายนั้นหรือพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญาได้ร้องขอ

ในกรณีที่มีการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่มีลักษณะขัดต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน รัฐมนตรีโดยความเห็นชอบของคณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์ จะมอบหมายให้พนักงานเจ้าหน้าที่ยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีคำสั่งระงับการทำให้แพร่หลายหรือลบซึ่งข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์ได้ ทั้งนี้ ให้นำบทบัญญัติว่าด้วยคณะกรรมการที่มีอำนาจดำเนินการพิจารณาทางปกครองตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครองมาใช้บังคับกับการประชุมของคณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์โดยอนุโลม

นอกจากนี้ เนื้อความในพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ.๒๕๖๐ ได้กำหนดรูปแบบของการสืบสวนและสอบสวนโดยเจ้าพนักงานไว้อย่างชัดเจนทุกฐานการกระทำความผิด ทั้งนี้เพื่อให้การใช้งานระบบคอมพิวเตอร์ในประเทศไทยเป็นไปด้วยความสงบเรียบร้อยและเสริมสร้างความมั่นคงแห่งชาติด้านไซเบอร์ต่อไป

เป็นที่น่าสังเกตว่าแม้บทลงโทษสำหรับผู้กระทำผิดเกี่ยวกับคอมพิวเตอร์จะค่อนข้างรุนแรงและรัดกุม แต่ทว่าในปัจจุบันยังพบการกระทำผิดในลักษณะเดิมเพิ่มมากขึ้น อีกทั้งมีการเปลี่ยนแปลงรูปแบบของความผิดไปตามกาลสมัย อย่างไรก็ตามในอนาคตก็คงต้องปรับปรุงตัวบทกฎหมายให้สอดรับกับสถานการณ์ปัจจุบันในโอกาสต่อไป

สถานการณ์ด้านความมั่นคงและความไม่สงบในพื้นที่จังหวัดชายแดนภาคใต้

สถานการณ์ความไม่สงบในชายแดนภาคใต้ของประเทศไทยหรือไฟใต้ เป็นความขัดแย้งที่กำลังดำเนินอยู่ในภาคใต้ของประเทศไทย ความขัดแย้งนี้กำเนิดในปี พ.ศ.๒๔๕๑ เริ่มจากกบฏดุซงญอเป็นการก่อกำเริบการแยกออกทางเชื้อชาติและศาสนาในภูมิภาคมลายูปัตตานี แต่ความไม่สงบดังกล่าวเริ่มบานปลายขึ้นหลังปี พ.ศ.๒๕๔๗

อดีตรัฐสุลต่านปัตตานีซึ่งมีสามจังหวัดชายแดนใต้ของไทย ได้แก่ จังหวัดปัตตานี จังหวัดยะลา จังหวัดนราธิวาส ตลอดจนบางส่วนของจังหวัดสงขลาที่อยู่ใกล้เคียง และส่วนตะวันออกเฉียงเหนือของประเทศมาเลเซียถูกราชอาณาจักรรัตนโกสินทร์พิชิตในปี พ.ศ.๒๕๓๘ และถูกไทยปกครองนับแต่นั้น ยกเว้นกะลันตัน

แม้เกิดความรุนแรงแยกตัวออกระดับต่ำในภูมิภาคมาหลายทศวรรษแล้วโดยนิยมนับตั้งแต่ปลายปี พ.ศ.๒๔๕๐ สถานการณ์ในจังหวัดชายแดนภาคใต้ร้อนระอุ เกิดเหตุการณ์เผาโรงเรียนในเขตเทศบาลเมืองปัตตานีจำนวน ๑ หลัง นอกจากนั้นมีการปล้นสะดมในท้องที่ต่างๆ รวมได้ประมาณ ๒๐๐ คดี ในวันที่ ๔ พฤศจิกายน พ.ศ.๒๔๕๖ รัฐบาลประกาศสถานการณ์ฉุกเฉินในอำเภอหาดใหญ่ จังหวัดสงขลา และจังหวัดยะลาในปี พ.ศ.๒๔๕๗ หะยีสุหลงได้หายตัวไปอย่างไร้ร่องรอยและในปี พ.ศ.๒๔๕๘ นายสมรรถ เอี่ยมวิโรจน์ อดีตสมาชิกสภาผู้แทนราษฎร จังหวัดนราธิวาสถูกลอบสังหาร

ปี พ.ศ.๒๕๒๔ มีเหตุการณ์ก่อเหตุร้ายต่างๆ เกิดขึ้นเป็นระยะๆ เช่น การจับครูเรียกค่าคุ้มครองหรือค่าไถ การกรรโชกข่มขู่นักธุรกิจพ่อค้าคนจีนโดยส่งเป็นหนังสือประทับตรากลุ่มต่างๆ ที่เคลื่อนไหวในพื้นที่และนอกพื้นที่ให้จ่ายค่าคุ้มครองดูแลความปลอดภัยของ บุคคลและกิจการธุรกิจการค้าหรือที่คนทั่วไปเรียกว่าภาษีเถื่อนนอกกฎหมาย เหตุการณ์ที่มีชื่อเสียงก็คือการลอบสังหาร กำธร ลาชโรจน์ สมาชิกสภาผู้แทนราษฎรจังหวัดปัตตานี เมื่อวันที่ ๓๐ กรกฎาคม พ.ศ.๒๕๒๔

แต่สถานการณ์บานปลายหลังปี ๒๕๔๔ และมีการระบาดใหม่ในปี ๒๕๔๗ ซึ่งบางครั้งล้นไปจังหวัดใกล้เคียง มีเหตุการณ์ที่มีการอ้างว่าผู้ก่อการกำเริบภาคใต้ เป็นผู้ลงมือเกิดในกรุงเทพมหานครและจังหวัดภูเก็ต นักสื่อสารมวลชนมักอ้างอิงเหตุการณ์ที่ ทักษิณ ชินวัตร

ตัดสินใจยุบศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ คณะกรรมการอำนวยการแก้ไขปัญหาความมั่นคงจังหวัดชายแดนภารใต้ สำนักงานคณะกรรมการอำนวยการแก้ไขปัญหาความมั่นคงจังหวัดชายแดนภาคใต้ และกองบัญชาการผสมพลเรือน ตำรวจทหารที่ ๔๓ ในวันที่ ๑ พฤษภาคม พ.ศ.๒๕๔๕ เป็นปฐมบทของความรุนแรงของความไม่สงบในชายแดนภาคใต้ของประเทศไทยที่เกิดขึ้นจนถึงปัจจุบัน ส่วนเหตุการณ์ที่นักวิชาการถือว่าเป็นปฐมบทของความรุนแรงรอบใหม่ได้แก่ เหตุการณ์ปล้นปืนครั้งใหญ่เมื่อวันที่ ๔ มกราคม ๒๕๔๗ ที่กองพันพัฒนาที่ ๔ ค่ายกรมหลวงนราธิวาสราชนครินทร์ อ.เจาะไอร้อง จ.นราธิวาส

ในวันที่ ๒๐ กรกฎาคม พ.ศ.๒๕๔๘ นายกรัฐมนตรีทักษิณ ชินวัตร ประกาศสถานการณ์ฉุกเฉิน เพื่อรับมือกับสถานการณ์ความไม่สงบภาคใต้ แต่การก่อการกำเริบยิ่งบานปลาย ในเดือนกันยายน ๒๕๔๙ คณะทหารผู้ยึดอำนาจการปกครองรัฐประหาร คณะผู้ยึดอำนาจการปกครองมีการเปลี่ยนนโยบายใหญ่ โดยแทนแนวทางก่อนหน้าของทักษิณ ชินวัตร ด้วยการรณรงค์เพื่อชนะใจของผู้ก่อการกำเริบ แม้มีความคืบหน้าเล็กน้อยในการจัดการกับความรุนแรง แต่คณะผู้ยึดอำนาจการปกครองประกาศว่าความมั่นคงกำลังดีขึ้นและสันติภาพจะคืนสู่ภูมิภาคภายในปี ๒๕๕๑ ทว่าในเดือนมีนาคม ๒๕๕๑ ยอดผู้เสียชีวิตเกิน ๓,๐๐๐ คน

ในสมัยรัฐบาลอภิสิทธิ์ เวชชาชีวะ รัฐมนตรีว่าการกระทรวงการต่างประเทศ กษิต ภิรมย์ ว่าเขามั่นใจว่าจะนำสันติภาพสู่ภูมิภาคภายใน พ.ศ.๒๕๕๓ แต่เมื่อถึงปลายปีนั้นความรุนแรงได้มีเพิ่มมากขึ้น ตรงกันข้ามกับการมองโลกในแง่ดีของรัฐบาล กรมสอบสวนคดีพิเศษจัดตั้งศูนย์ปฏิบัติการคดีพิเศษจังหวัดชายแดนภาคใต้ ในปี พ.ศ.๒๕๕๔ และในเดือนมีนาคม พ.ศ.๒๕๕๔ รัฐบาลยอมรับว่าสถานการณ์ได้เพิ่มมากขึ้นและไม่สามารถแก้ไขได้ภายในเวลาไม่กี่เดือน หลังวันที่ ๒๐ พฤษภาคม พ.ศ.๒๕๕๗ เวลา ๓.๐๐ น. คณะรักษาความสงบแห่งชาติ ประกาศใช้กฎอัยการศึกทั่วประเทศ ๑๐ เดือน ๑๑ วัน โดยยกเลิกในวันที่ ๑ เมษายน พ.ศ.๒๕๕๘

ผู้นำท้องถิ่นเรียกร้องอัตตาณัติระดับหนึ่งแก่ภูมิภาคปัตตานีจากประเทศไทยอย่างต่อเนื่องและขบวนการผู้ก่อการกำเริบแยกตัวออกบางส่วนเรียกร้องให้มีการเจรจาสันติภาพ ทว่ากลุ่มเหล่านี้ส่วนใหญ่ถูกเบี่ยงเบนความสนใจโดยกลุ่มขบวนการแนวร่วมปฏิวัติแห่งชาติมลายูปัตตานี-โคออร์ดิเนต (BRN-C) ซึ่งเป็นกลุ่มที่กำลังเป็นหัวหอกการก่อการกำเริบ กลุ่มนี้ไม่เห็นเหตุผลให้ต้องเจรจาและคัดค้านการพูดคุยกับกลุ่มก่อการกำเริบอื่น BRN-C มีเป้าหมายทันทีเพื่อทำให้ภาคใต้ของประเทศไทยปกครองไม่ได้และประสบความสำเร็จเป็นส่วนใหญ่

๑. ลักษณะของสถานการณ์

รัฐบาลได้จัดตั้งคณะกรรมการวิสามัญศึกษาปัญหาจังหวัดชายแดนภาคใต้ ครั้งแรกเมื่อ ๒๒ พฤษภาคม ปี พ.ศ.๒๕๓๓

ในวันที่ ๓ พฤษภาคม พ.ศ.๒๕๓๔ มีประกาศเลิกใช้กฎอัยการศึกในบางพื้นที่ แต่ยังคงใช้กับจังหวัดยะลาเฉพาะ อำเภอธารโต อำเภอบันนังสตา อำเภอเบตา และอำเภอยะหา จังหวัดนราธิวาสเฉพาะอำเภอจะแนะ อำเภอเจาะไอร้อง อำเภอระแงะ อำเภอแว้ง อำเภอศรีสาคร และอำเภอสุคิริน นับเป็นการใช้กฎอัยการศึกอย่างเป็นทางการในการแก้ปัญหาเป็นครั้งแรก

ในวันที่ ๑๓ พฤศจิกายน พ.ศ.๒๕๔๑ มีประกาศเลิกใช้กฎอัยการศึกในบางพื้นที่ แต่ยังคงใช้กับ จังหวัดนราธิวาสเฉพาะอำเภอจะแนะ อำเภอเจาะไอร้อง อำเภอระแงะ อำเภอแว้ง อำเภอศรีสาคร และอำเภอสุคิริน จังหวัดยะลาเฉพาะอำเภอกาบัง อำเภอธารโต อำเภอบันนังสตา อำเภอเบตา และอำเภอยะหา และประกาศเลิกใช้กฎอัยการศึกในวันที่ ๒๑ กรกฎาคม พ.ศ.๒๕๔๘

กลุ่มทหารโจรปัตตานี เริ่มต้นสร้างสถานการณ์ความไม่สงบขึ้นอีกครั้งในปี พ.ศ. ๒๕๔๔ เอกลักษณ์ของผู้ก่อการที่ต้องการผลักดันให้เกิดความขัดแย้งขึ้นนั้น ยังคงคลุมเครือเสียเป็นส่วนใหญ่ ผู้เชี่ยวชาญในระดับท้องถิ่นและภูมิภาคได้แสดงให้เห็นว่า สถานการณ์ดังกล่าวเกี่ยวข้องกับกลุ่มแบ่งแยกดินแดนดั้งเดิมในภูมิภาค อย่างเช่น พูโล บีอาร์เอ็น และจีเอ็มไอพี โดยเฉพาะอย่างยิ่ง บีอาร์เอ็น โคออดิเนต (อันเป็นสาขาหนึ่งของบีอาร์เอ็น) และกลุ่มติดอาวุธที่ถูกกล่าวหาว่ามีส่วนเกี่ยวข้องกับบีอาร์เอ็น คือ รันดา คัมปูรัน คีซิล ส่วนคนอื่นเสนอแนะว่า ความรุนแรงดังกล่าวเกิดขึ้นภายใต้อิทธิพลของกลุ่มอิสลามต่างชาติ อาทิ อัลกออิดะห์และญะมาอะห์ อิสลามียะห์ แต่ด้วยวิธีการทำงานของกองโจรในภาคใต้ ซึ่งโจมตีคลังอาวุธทหารและโรงเรียน ไม่เหมือนกับวิธีการปฏิบัติของกลุ่มอื่นซึ่งโจมตีเป้าหมายของชาติตะวันตก มุมมองที่ว่ากองโจรในภูมิภาคมีส่วนเกี่ยวข้องกับกลุ่มต่างชาตินั้นจึงอ่อน

ในตอนแรก รัฐบาลมองว่าการสร้างสถานการณ์ดังกล่าวเป็นฝีมือของโจร และอันที่จริงแล้ว ผู้สังเกตการณ์ภายนอกจำนวนมากก็เชื่อว่า กลุ่มท้องถิ่น คู่แข่งทางธุรกิจหรืออาชญากรรมมีส่วนเกี่ยวข้องกับสถานการณ์ในภูมิภาคดังกล่าว เมื่อเดือนกรกฎาคม พ.ศ.๒๕๔๕ หลังจากตำรวจเสียชีวิตไป ๑๔ นาย ในการโจมตีหลายครั้งซึ่งเกิดขึ้นในช่วงเวลานานเจ็ดเดือน นายกรัฐมนตรีทักษิณ ชินวัตร ได้ปฏิเสธถึงบทบาทของศาสนาในการโจมตีดังกล่าว เพราะตำรวจที่เสียชีวิตไปหลายคนนั้นเป็นมุสลิมด้วย

พล.อ.กิตติ รัตนฉายา ให้สัมภาษณ์ลง หนังสือพิมพ์ผู้จัดการรายวัน เมื่อวันที่ ๙ เมษายน พ.ศ.๒๕๔๕ โดยกล่าวตอนหนึ่งว่า จริงๆ แล้ว ณ วันนี้ยังไม่มีใครหาคำตอบได้ว่าสถานการณ์ที่เกิดขึ้นในภาคใต้นั้น เป็นโจรธรรมดาหรือกลุ่มขบวนการ แต่ความจริงเรื่องหนึ่งที่สังคมต้องยอมรับก็คือ ขบวนการโจรก่อการร้ายนั้นยังมีอยู่ โดยส่วนนำอยู่ที่ประเทศมาเลเซียตะวันออกกลาง และในกลุ่มประเทศยุโรป ซึ่งแนวร่วมก็คือประชาชนในพื้นที่นั่นเอง วันนี้ เราชอบพูดว่าไม่มีแล้วขบวนการ แต่จริงๆ นั้นมี และเรื่องภาคใต้วันนี้ก็เชื่อมโยงถึงขบวนการแน่นอน

รัฐบาลทักษิณ ๑ (พ.ศ.๒๕๔๔-๒๕๔๘) มีสมาชิกรัฐสภาเป็นมุสลิมหลายสิบคน สภาจังหวัดในจังหวัดชายแดนมีสมาชิกส่วนใหญ่เป็นมุสลิม และเทศบาลหลายแห่งในภาคใต้มี นายกเทศมนตรีเป็นมุสลิม มุสลิมเริ่มมีสิทธิ์มีเสียงในทางการเมืองอย่างเปิดเผยมากขึ้น และได้รับเสรีภาพในการนับถือศาสนามากยิ่งขึ้น อย่างไรก็ตาม เมื่อ ทักษิณ ชินวัตร มีคำสั่งสำนักนายกรัฐมนตรีที่ ๑๒๓/๒๕๔๕ ยุบศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ คณะกรรมการอำนวยการแก้ไขปัญหาความมั่นคงจังหวัดชายแดนภาคใต้ สำนักงานคณะกรรมการอำนวยการแก้ไขปัญหาความมั่นคงจังหวัดชายแดนภาคใต้ และกองบัญชาการผสมพลเรือน ตำรวจทหารที่ ๔๓ ในวันที่ ๑ พฤษภาคม พ.ศ.๒๕๔๕ ต่อมาในวันที่ ๑๓ พฤษภาคม พ.ศ.๒๕๔๕ มีประกาศสภาผู้แทนราษฎรเรื่องตั้งคณะกรรมมาธิการวิสามัญพิจารณาศึกษาการลอบวางระเบิดและก่อความไม่สงบเรียบร้อยในพื้นที่จังหวัดชายแดนภาคใต้

กองกำลังที่ถูกยุบถูกแทนที่ด้วยกองกำลังตำรวจที่มีเรื่องฉาวโฉ่ในด้านการคอร์รัปชั่น ซึ่งได้เริ่มการปราบปรามอย่างกว้างขวางในทันที การปรึกษาหารือกับผู้นำชุมชนท้องถิ่นก็ได้ถูกยกเลิกไปด้วย ความไม่พอใจต่อการละเมิดดังกล่าวได้นำไปสู่ความรุนแรงที่เพิ่มมากขึ้นระหว่าง พ.ศ.๒๕๔๗ และ ๒๕๔๘

ในปีเดียวกัน ทักษิณ ชินวัตร กล่าวว่า “ไม่มีการแบ่งแยกดินแดน ไม่มีผู้ก่อการร้าย อุดมการณ์ มีแต่โจรกระจอก” แต่ในปี พ.ศ.๒๕๔๗ เขาได้เปลี่ยนท่าทีและจัดว่าสถานการณ์ดังกล่าวเป็นสงครามต่อต้านการก่อการร้ายในประเทศ มีการประกาศกฎอัยการศึกในจังหวัดปัตตานี ยะลา และนราธิวาส ในเดือนมกราคม พ.ศ. ๒๕๔๗ โดยสื่อมวลชนและนักวิชาการถือว่าเหตุการณ์ปล้นปืนครั้งใหญ่เมื่อวันที่ ๔ มกราคม ๒๕๔๗ ที่กองพันพัฒนาที่ ๔ ค่ายกรมหลวงนราธิวาสราชนครินทร์ อ.เจาะไอร้อง จ.นราธิวาส เป็นจุดเริ่มต้นของความรุนแรงในพื้นที่รอบใหม่ในวันที่ ๔ ตุลาคม ๒๕๔๗ รัฐบาลจัดตั้งกองอำนวยการเสริมสร้างสันติสุขจังหวัดชายแดนภาคใต้ ตามคำสั่งสำนักนายกรัฐมนตรี ที่ ๒๖๐/๒๕๔๗ โดยยกเลิกคำสั่งเดิม

เมื่อวันที่ ๒๕ ตุลาคม พ.ศ.๒๕๔๗7 เกิดเหตุกรณีตากใบซึ่งส่งผลให้ชาวบ้านไม่ไว้ใจเจ้าหน้าที่ตำรวจทหา และหันมาเป็นศัตรูกับทหารและตำรวจมากขึ้น เนื่องจากเจ้าหน้าที่อ้างว่ากลุ่มชาวบ้านที่ประท้วงถูกจ้างและจัดตั้งขึ้นมา ในขณะที่ชาวบ้านเสียชีวิตถึง ๘๕ ราย ภายหลังจากเหตุการณ์นี้คำอธิบายจากเจ้าหน้าที่รัฐกรณีเกิดเหตุก่อการร้ายมักได้รับการอธิบายว่าเกิดจากชาวบ้านรับจ้างให้ก่อเหตุ

นายมุข สุไลมาน กล่าวสัมภาษณ์ลงหนังสือพิมพ์ผู้จัดการรายวัน เมื่อวันที่ ๑๕ พฤศจิกายน ๒๕๔๕ ตอนหนึ่งว่า “เหตุการณ์เผาโรงเรียนและวางระเบิดที่ต่างๆ ผมมั่นใจว่าไม่ใช่ขบวนการแบ่งแยกดินแดนอย่างชัดเจน แต่เกิดจากบางคนที่ชอบรับจ้างโดยอาจจะติดยาเสพติด เคย

มีคดีลักขโมยน้อย รอรับจ้างอย่างเดียว ใครจ้างก็ทำตลอด แม้ว่าจะจับคนหนึ่งก็จะมีคนหนึ่งทำต่อ เพราะคนรับจ้างมันเยอะ จะสาวไปถึงผู้ว่าจ้างมันก็ยาก ทั้งๆ ที่รู้ แต่ไม่สามารถหาของกลางได้ ซึ่งเมื่อถามผมว่า รู้ได้อย่างไร ในหลักฐานผมก็บอกไม่ได้"

ในขณะที่ นายสมชาย นีละไพจิตร ให้สัมภาษณ์ว่าหลายกรณีเจ้าหน้าที่ทหารตำรวจมักทรมานผู้ต้องสงสัยให้รับสารภาพด้วยการให้คนอื่นปัสสาวะใส่หน้า ใช้ไฟฟ้าช็อตตามร่างกายและอวัยวะเพศ นายสมชาย นีละไพจิตร หายตัวไปอย่างลึกลับแม้อัยการสั่งฟ้องเจ้าหน้าที่ตำรวจ ๕ ราย แต่ศาลยกฟ้องในที่สุด

ในวันที่ ๒๐ กรกฎาคม พ.ศ.๒๕๔๘ มีการใช้พระราชกำหนดในสถานการณ์ฉุกเฉิน พ.ศ.๒๕๔๘ ในพื้นที่จังหวัดปัตตานี จังหวัดยะลา จังหวัดนราธิวาส รัฐบาลแต่งตั้ง พลโท ขวัญชาติ กล้าหาญ แม่ทัพภาคที่ ๔ เป็นผู้อำนวยการกองอำนวยการเสริมสร้างสันติสุขจังหวัดชายแดนภาคใต้ พร้อมทั้งตั้งคณะกรรมการนโยบายเสริมสร้างสันติสุขจังหวัดชายแดนภาคใต้ โดยให้พลตำรวจเอก ชิดชัย วรรณสถิตย์ เป็นประธานกรรมการ

ในวันที่ ๕ ตุลาคม พ.ศ.๒๕๔๘ รัฐบาลแต่งตั้งคณะกรรมการบริหารจัดการในพื้นที่ตามนโยบายและยุทธศาสตร์เสริมสร้างสันติสุขจังหวัดชายแดนภาคใต้ หรือ กบชต. หลังจากรัฐประหารในปี พ.ศ.๒๕๔๙ ซึ่งทำให้ ทักษิณ ชินวัตร พ้นจากตำแหน่ง รัฐบาล สุรยุทธ์ จุลานนท์ มีการประกาศกฎอัยการศึกในพื้นที่ทั่วราชอาณาจักรในวันที่ ๑๙ กันยายน พ.ศ.๒๕๔๙ ต่อมาในวันที่ ๒๑ มกราคม พ.ศ.๒๕๕๐ รัฐบาลคงกฎอัยการศึกในจังหวัดปัตตานี จังหวัดนราธิวาส จังหวัดยะลา และจังหวัดสงขลา เฉพาะอำเภอจะนะ อำเภอเทพา อำเภอนาทวี อำเภอสะเดา และอำเภอสะบ้าย้อย ในวันที่ ๓๑ ธันวาคม พ.ศ.๒๕๕๐ รัฐบาลคงกฎอัยการศึกในจังหวัดปัตตานี จังหวัดนราธิวาส จังหวัดยะลา และจังหวัดสงขลา เฉพาะอำเภอจะนะ อำเภอเทพา อำเภอนาทวี อำเภอสะเดา และอำเภอสะบ้าย้อย นับว่ารัฐบาล สุรยุทธ์ จุลานนท์ ใช้อำนาจตามกฎหมายมากที่สุดเป็นประวัติศาสตร์ กล่าวคือ ใช้อำนาจตาม พระราชกำหนดในสถานการณ์ฉุกเฉิน พ.ศ.๒๕๔๘ ในจังหวัดปัตตานี จังหวัดนราธิวาส และจังหวัดยะลา และขยายพื้นที่กฎอัยการศึกในจังหวัดปัตตานี และจังหวัดสงขลาเฉพาะอำเภอจะนะ อำเภอเทพา อำเภอนาทวี อำเภอสะเดา และอำเภอสะบ้าย้อย

ในวันที่ ๒๘ เมษายน พ.ศ.๒๕๕๓ รัฐบาล อภิสิทธิ์ เวชชาชีวะ คงกฎอัยการศึกในจังหวัดปัตตานี จังหวัดนราธิวาส จังหวัดยะลา และจังหวัดสงขลา อำเภอสะเดา กฎอัยการศึกยังคงใช้ในพื้นที่ดังกล่าวถึงปัจจุบัน เป็นระยะเวลา ๑๐ ปี เนื่องจาก ประกาศเลิกใช้กฎอัยการศึกไม่กระทบต่อการประกาศใช้กฎอัยการศึกที่มีผลใช้บังคับก่อนวันที่ ๑๙ พฤษภาคม พ.ศ.๒๕๕๗

อย่างไรก็ตาม สถานการณ์กลับทวีความรุนแรงยิ่งขึ้น ซึ่งข้อเท็จจริงดังกล่าวน่าจะเป็นการสนับสนุนการยืนยันที่ว่า มีกลุ่มหลายกลุ่มมีส่วนเกี่ยวข้องในการสร้างสถานการณ์ และมีกลุ่ม

จำนวนน้อยที่สงบลง จากการเปลี่ยนยุทธศาสตร์ของรัฐบาลก่อนหน้านี้ ในปี พ.ศ.๒๕๓๙ ได้เกิดเหตุการณ์รุนแรงทั้งหมด ๔๒ ครั้ง และเพิ่มเป็น ๘๓ ครั้งในปี พ.ศ.๒๕๔๐ และ ๑๓๙ ครั้งในปี พ.ศ.๒๕๔๑ ส่วนในปี พ.ศ.๒๕๔๕ เกิดเหตุการณ์รุนแรงขึ้น ๘๒ ครั้ง และ ๘๔ ครั้งในปี พ.ศ.๒๕๔๖

ในปี พ.ศ.๒๕๕๑ รัฐบาลจัดตั้งกองร้อยบังคับการและบริการส่วนหน้าจังหวัดชายแดนภาคใต้ ขึ้น ตามคำสั่งกองบัญชาการกองอาสารักษาดินแดนที่ ๑๐/๒๕๕๑ ลงวันที่ ๑๕ มกราคม พ.ศ.๒๕๕๑ ตามคำสั่ง พลเอก สุรยุทธ์ จุลานนท์ ในฐานะผู้บัญชาการกองอาสารักษาดินแดน และจัดตั้งกองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร ภาค ๔ และคณะกรรมการเขตพัฒนาพิเศษเฉพาะกิจจังหวัดชายแดนภาคใต้ โดยออกระเบียบสำนักนายกรัฐมนตรีว่าด้วยระบบบริหารจัดการเพื่อเสริมสร้างสันติสุขในจังหวัดชายแดนภาคใต้ พ.ศ. ๒๕๕๑

อย่างไรก็ตามรัฐบาลไม่สามารถแก้ปัญหาได้ โดยเป็นที่รับรู้โดยทั่วไปว่าพื้นที่ในจังหวัดปัตตานี จังหวัดนราธิวาส และจังหวัดยะลา เป็นพื้นที่ที่มีธุรกิจผิดกฎหมายเติบโตขึ้นอย่างมากอาทิ ธุรกิจยาเสพติด บ่อนการพนัน การค้าประเวณี ธุรกิจน้ำมันเถื่อน และตำรวจทหารเป็นคนเก็บเงินค่าส่วยในพื้นที่เสียเอง สถานการณ์จึงยิ่งซับซ้อนขึ้นเนื่องจากทหารและตำรวจ ต้องรบกับทหารและตำรวจส่วนหนึ่งที่หันมาเป็นผู้มีอิทธิพลหรือเป็นโจรเสียเอง ปัญหาความไม่ไว้วางใจของประชาชนที่มีต่อเจ้าหน้าที่ตำรวจทหารเนื่องจากสงสัยว่าหลายกรณีมีการจับแพะและเคยมีกรณีที่ถูกเจ้าหน้าที่ทรมานผู้ต้องหา ปัญหาการไม่ให้ความร่วมมือของประชาชนในพื้นที่ ปัญหาความขัดแย้งระหว่างชาวไทยพุทธและชาวไทยมุสลิม ปัญหาความขัดแย้งผลประโยชน์นักการเมืองท้องถิ่น ปัญหาความต้องการแบ่งแยกดินแดน ปัญหาธุรกิจยาเสพติดบ่อนการพนันและค้าประเวณี ปัญหาความไม่แน่ชัดว่าศัตรูของทหาร ตำรวจ และกองอาสารักษาดินแดน นั้นคือใคร

บางปัญหาก็มีความขัดแย้งระหว่างเจ้าหน้าที่รัฐกับประชาชน อาจกล่าวสรุปได้ว่าเจ้าหน้าที่รัฐเห็นว่าประชาชนเป็นผู้ร้าย ส่วนประชาชนเห็นว่าเจ้าหน้าที่รัฐเป็นผู้ร้าย เจ้าหน้าที่รัฐยืนยันถึงสงครามระหว่างขบวนการโจรแบ่งแยกดินแดนเป็นประเด็นสำคัญซึ่ง ซัยยิดสุไลมาน ฮูซัยนี ประธานสถาบันศึกษาอัล-มะห์ดีย์ เห็นว่าเป็นประเด็นรอง เขากล่าวตอนหนึ่งว่า ส่วนตัวเองมองว่าสถานการณ์ภาคใต้มีสถานการณ์แอบแฝงอยู่ กลุ่มก่อการอาจมาจากหลายกลุ่ม กลุ่มอิทธิพลท้องถิ่น หรืออะไรก็ตาม แต่พี่น้องมุสลิมไม่สามารถทำได้เพราะเก่งกาจขนาดนี้ ไม่เคยมีประวัติศาสตร์การต่อสู้ของชาวมุสลิม กลุ่มมุสลิมไม่ใช่คนก่อเหตุ ฝ่ายเจ้าหน้าที่รัฐยืนยันถึงความเกลียดชัง ความขัดแย้งระหว่างชาวไทยพุทธและชาวไทยมุสลิม ส่วนฝ่ายประชาชนเห็นว่าความขัดแย้งระหว่างชาวไทยต่างศาสนาไม่มีในพื้นที่เลย

ในปี พ.ศ.๒๕๕๓ รัฐบาลออกกฎหมาย พระราชบัญญัติการบริหารราชการจังหวัดชายแดนภาคใต้ พ.ศ.๒๕๕๓ กำหนดให้มีคณะกรรมการยุทธศาสตร์ด้านการพัฒนาจังหวัดชายแดน

ภาคใต้ (กพต.) โดยมีนายกรัฐมนตรีเป็นประธาน ในปี พ.ศ.๒๕๕๔ กรมสอบสวนคดีพิเศษจัดตั้งศูนย์ปฏิบัติการคดีพิเศษจังหวัดชายแดนภาคใต้ขึ้น และในวันที่ ๓๑ กรกฎาคม พ.ศ.๒๕๕๕ รัฐบาลนางสาวยิ่งลักษณ์ ชินวัตร ได้จัดตั้งศูนย์ปฏิบัติการแก้ไขปัญหาจังหวัดชายแดนภาคใต้ขึ้นมาอีกครั้ง

๒. เบื้องหลังของสถานการณ์

เบื้องหลังของเหตุการณ์ความไม่สงบในชายแดนภาคใต้ของประเทศไทยอาจมีสาเหตุจากหลายกรณี ซึ่งสามารถสรุปได้ว่ามาเหตุปัจจัยดังนี้

๒.๑ ปัจจัยทางเศรษฐกิจ

มีการอ้างว่าความยากจนและปัญหาเศรษฐกิจ เป็นปัจจัยหนึ่งเบื้องหลังการก่อการกำเริบด้วยจังหวัดชายแดนยังมีรายได้เฉลี่ยต่ำสุด เมื่อเทียบกับจังหวัดภาคใต้ด้วยกัน แม้ว่าสมรรถนะของเศรษฐกิจชายแดนภาคใต้ พัฒนาขึ้นอย่างเห็นได้ชัดในช่วงทศวรรษหลังๆ ระหว่างปี ๒๕๒๖ ถึง ๒๕๔๖ รายได้ต่อหัวของจังหวัดปัตตานีเพิ่มขึ้นจาก ๙,๓๔๐ บาท เป็น ๕๗,๖๒๑ บาท ขณะที่รายได้ต่อหัวของจังหวัดยะลาและนราธิวาส ก็เพิ่มขึ้นจาก ๑๔,๙๘๗ บาท เป็น ๕๒,๗๓๗ บาท และจาก ๑๐,๓๔๐ บาท เป็น ๓๘,๕๕๓ บาท ตามลำดับ กระนั้น การขาดประสิทธิภาพการจัดการทรัพยากรเพื่อพัฒนาท้องถิ่น เป็นปัจจัยหนึ่งของความไม่สงบ เอกชนมักไม่มีส่วนร่วมในการลงทุน เพราะพื้นที่อยู่ภายใต้หน่วยงานความมั่นคงของรัฐ คณะกรรมการสมานฉันท์แห่งชาติรายงานว่า โครงสร้างการพัฒนาเศรษฐกิจของภาคใต้มีปัญหา เพราะมีประชากรยากจนสูง และมีการแย่งชิงทรัพยากร กระนั้น นักวิเคราะห์ทางสังคมกลับมองว่า ความยากจนเองมิใช่ปัญหาทั้งหมด แต่เป็นการไม่ได้รับความยุติธรรมมากกว่า และในการแก้ปัญหาความรุนแรง รัฐควรแก้ปัญหาแรงจูงใจทางการเมือง

อย่างไรก็ตาม พล.ต.ท.อุดม เจริญ อดีตผู้อำนวยการสำนักงานพระพุทธศาสนาแห่งชาติให้สัมภาษณ์หนังสือพิมพ์มติชนรายวัน ในวันที่ ๑๕ กุมภาพันธ์ พ.ศ.๒๕๔๗ โดยกล่าวว่า จากประสบการณ์ที่อยู่ใน จ.ยะลา ๑๐ กว่าปี รู้ว่าอะไรเป็นอะไร และรู้ว่ามีกลุ่มที่ก่อความไม่สงบในภาคใต้รับเงินจากต่างประเทศแล้วนำเงินมาปลูกฝังความเข้าใจผิดๆ ให้นักเรียน

๒.๒ ปัจจัยทางการศึกษา

ในระบบโรงเรียนปอเนาะ (Pondok) ของไทย พบว่ามีบางโรงเรียนที่มีเป้าหมายการแบ่งแยกดินแดนหรือการทำสงครามศักดิ์สิทธิ์เพื่อตอบโต้รัฐบาลไทย ที่ชาวมุสลิมมลายูในพื้นที่เชื่อว่ากดขี่ข่มเหงพวกเขาชัดเจน ระบบโรงเรียนดังกล่าวถูกกลุ่มแบ่งแยกดินแดนแทรกซึมแล้วเผยแพร่ลัทธิอุดมการณ์ ซึ่งหน่วยข่าวกรองกองทัพบกระบุว่า โรงเรียนสอนศาสนากลายเป็นแหล่งบ่มเพาะสมาชิกใหม่ของกลุ่มต่างๆ และหัวหน้ากลุ่มแบ่งแยกดินแดนนั้น ก็สำเร็จการศึกษาจากโรงเรียนปอเนาะ

๒.๓ ปัจจัยทางการเมือง

เป็นที่ยอมรับอย่างกว้างขวางว่ามีความขัดแย้งทางผลประโยชน์ระหว่างนักการเมืองท้องถิ่น ในวันที่ ๑๓ กุมภาพันธ์ พ.ศ.๒๕๔๔ นายมีลาภ เทพฉิม ประธานกรรมการบริหาร อบต.ปากแตระ อ.ระโนด จ.สงขลา ใช้อาวุธปืน ๑๑ มม. จ่อยิงประธานสภาและสมาชิกสภา อบต.ทีละคน เสียชีวิต ๓ ราย

พล.อ.หาญ ลีนานนท์ ให้สัมภาษณ์ลงหนังสือพิมพ์มติชนรายวัน ในวันที่ ๑ กุมภาพันธ์ ๒๕๔๗ ตอนหนึ่งว่าการเมืองท้องถิ่นนั้นแหละตัวแสบ ทำให้พื้นที่ตกอยู่ภายในอำนาจมืด คนในพื้นที่รู้ดีว่าพวกนี้ถือหางใคร เป็นหัวคะแนนใคร แก้ปัญหาที่ลูบหน้าปะจมูก จนทำให้รังสีโจรแน่น ครอบคลุมพื้นที่ไปหมด แล้วอย่างนี้ ผู้ทรงเกียรติทั้งหลาย จะไม่ทำให้สภาปั่นป่วนหรือ

ในวันที่ ๑๖ ธันวาคม พ.ศ.๒๕๕๔ เกิดเหตุคนร้ายลอบฆ่า นายมุคตาร์ กีละ อายุ ๔๗ ปี หัวหน้าพรรคประชาธรรม ในวันที่ ๔ กรฎาคม พ.ศ.๒๕๕๖ เกิดเหตุคนร้ายลอบฆ่า นายแวตูลอ แวเต๊ะ สมาชิก อบต.เนินงาม เสียชีวิต ต่อมา ในวันที่ ๑๔ สิงหาคม พ.ศ.๒๕๕๖ นายอับดุลรอฟา ปูแทน อดีต สจ.ปัตตานี เขต อ.ยะรัง ถูกคนร้ายลอบฆ่าเสียชีวิต ในวันที่ ๑๔ พฤศจิกายน พ.ศ. ๒๕๕๖ พ.อ.บรรพต พูลเพียร โฆษก กอ.รมน. กล่าวตอนหนึ่งว่า โดยทั่วไป ความขัดแย้งของการเมืองท้องถิ่น จะเชื่อมโยงกับกลุ่มผู้มีอิทธิพลในพื้นที่ ที่ต้องการรักษาผลประโยชน์ของกลุ่ม จนกลายเป็นปัญหาภัยแทรกซ้อน และ วันที่ ๑๙ ธันวาคม พ.ศ.๒๕๕๖ คนร้ายลอบยิงกำนัน ต.มะนังดาลำ นางมัสกะ มะอิง เสียชีวิต

๒.๔ ปัจจัยทางศาสนา

ภายหลังปี พ.ศ.๒๕๔๗ พบเหตุการณ์ข่มขู่คนไทยที่นับถือศาสนาพุทธเพิ่มขึ้นอาทิ มีการแจกใบปลิวไปทั่วหมู่บ้านใจความข่มขู่เอาชีวิต หากชาวไทยพุทธรายใดไม่ยอมขายสวนยางพาราในราคาถูก ในวันที่ ๑๙ สิงหาคม พ.ศ.๒๕๕๖ พบใบปลิวเขียนข้อความโจมตีเจ้าหน้าที่รัฐเกี่ยวกับเหตุการณ์สังหาร นายอับดุลรอฟา พร้อมประกาศเอาชีวิตคนไทยพุทธหากเกิดการฆ่าชาวมลายูมุสลิม นายจอห์น แบรนดอน ผอ.โครงการความสัมพันธ์ระหว่างประเทศแห่งมูลนิธิเอเชีย ในกรุงวอชิงตัน ดี.ซี.สหรัฐอเมริกา กล่าวตอนหนึ่งว่ามุสลิม ๕ ล้านคน ไม่พอใจยิ่งที่ถูกปฏิเสธไม่ยอมรับภาษา วัฒนธรรม และความเป็นมลายู

๓. เหตุการณ์สำคัญ ๓ ปี ย้อนหลัง

พ.ศ.๒๕๕๘

๑ เมษายน - พระบาทสมเด็จพระปรมินทรมหาภูมิพลอดุลยเดชมีพระบรมราชโองการโปรดเกล้าฯ ยกเลิกกฎอัยการศึกทั่วราชอาณาจักร

๓ มิถุนายน - คนร้ายยิงทหารเสียชีวิต ๔ ราย ที่ถนนในท้องที่บ้านปาลูกาปาลัส หมู่ ๗ ตำบลบาลอ อำเภอรามัน จังหวัดยะลา

๑๙ ตุลาคม - คนร้ายก่อเหตุลอบวางระเบิดมีทหารเสียชีวิต ๒ รายบาดเจ็บ ๕ ราย

๒๙ ตุลาคม - เกิดเหตุคนร้ายลอบวางระเบิด ๗ จุด ใน จังหวัดยะลา และ ๑ จุด ใน อำเภอยะรัง จังหวัดปัตตานี

๑๒ พฤศจิกายน - คนร้ายวางระเบิด บริเวณป้อมชุดรักษาความปลอดภัยหมู่บ้าน บ้านโคกขี้เหล็ก หมู่ที่ ๗ ตำบลท่าเรือ อำเภอโคกโพธิ์ จังหวัดปัตตานี มีคนเสียชีวิต ๔ ราย และบาดเจ็บสาหัส ๔ ราย

พ.ศ.๒๕๕๙

๑๓ มีนาคม - คนร้ายก่อเหตุลอบวางระเบิด ๖ จุด ที่อำเภอสุไหงปาดี ลอบวางระเบิด ๒ จุด อำเภอเจาะไอร้อง บาดเจ็บ ๙ ราย เกิดเหตุคนร้ายบุกเข้ายึดโรงพยาบาลเจาะไอร้องทำลายทรัพย์สินและพยายามเข้ายึดโรงพยาบาล มีผู้ได้รับบาดเจ็บ ๗ ราย

๑๔ มีนาคม - คนร้ายวางระเบิด อำเภอตากใบ 1 จุด อำเภอสุไหงปาดี ๑ จุด และ อำเภอเจาะไอร้อง ๑ จุด บาดเจ็บ ๓ ราย

๑๒ สิงหาคม - เกิดเหตุการณ์วางเพลิงและวางระเบิดในจังหวัดภูเก็ต จังหวัดพังงา จังหวัดสุราษฎร์ธานี จังหวัดตรัง จังหวัดนครศรีธรรมราช มีผู้เสียชีวิต ๔ ราย

๒ พฤศจิกายน - เกิดเหตุการณ์ไม่สงบ ๘ จุดในพื้นที่ จังหวัดสงขลา จังหวัดนราธิวาส และ จังหวัดปัตตานี

๒๒ พฤศจิกายน - รัฐบาลประกาศใช้ พรบ.ความมั่นคงภายในราชอาณาจักร พ.ศ. ๒๕๕๑ ถึงวันที่ ๓๐ พฤศจิกายน พ.ศ.๒๕๖๐

พ.ศ.๒๕๖๐

๑๓ มกราคม - มีคำสั่งกองอำนวยการรักษาความมั่นคงภายในราชอาณาจักรที่ ๑๔/๒๕๖๐ เรื่อง โครงสร้างการจัดและอัตรากำลังของกองอำนวยการรักษาความมั่นคงภายในภาค % ส่วนหน้า ประจำปี ๒๕๖๐ จัดเจ้าหน้าที่จำนวน ๖๑,๖๐๔ ราย

๑๔ มกราคม - มีรายงานว่า สะแปอิง บาซอ ประธานขบวนการบีอาร์เอ็น โคออดีเนต เสียชีวิต

๖ เมษายน - เกิดระเบิดจำนวน ๒๖ จุด ในพื้นที่ ๔ จังหวัดนราธิวาส จังหวัดปัตตานี จังหวัดยะลา จังหวัดสงขลา ส่งผลให้ไฟฟ้าดับสนิทเป็นบริเวณกว้าง

๑ กันยายน - ศูนย์ปฏิบัติการตำรวจจังหวัดชายแดนภาคใต้ ถูกยุบรวมกับกองบัญชาการตำรวจภูธรภาค ๙

๔ ธันวาคม - พล.อ.สุรเชษฐ์ ชัยวงศ์ รัฐมนตรีช่วยว่าการกระทรวงศึกษาธิการ ทำหน้าที่ประธานคณะกรรมการขับเคลื่อนการแก้ไขปัญหาจังหวัดชายแดนภาคใต้ ส่วนหน้า แทน พล.อ.อุดมเดช สีตบุตร

เหตุการณ์หลังรัฐประหาร พ.ศ.๒๕๕๗

หลังรัฐประหารในปี พ.ศ.๒๕๕๗ พลเอก ประยุทธ์ จันทร์โอชา ดำเนินนโยบายโดยให้มีแม่ทัพภาคที่ ๔ เป็นคนในพื้นที่เป็นครั้งแรกได้แก่ พลโท วิวรรธน์ ปฐมภาคย์ รัฐบาลจัดตั้งคณะกรรมการขับเคลื่อนการแก้ไขปัญหาจังหวัดชายแดนภาคใต้ จัดตั้งคณะกรรมการที่ปรึกษาการบริหารและการพัฒนาจังหวัดชายแดนภาคใต้ โดยให้ พลเอก กิตติ อินทสร เป็นประธานคณะกรรมการ นายบัญญัติ จันทน์เสนะ เป็นรองประธานกรรมการ พลโท เรืองศักดิ์ สุวรรณนาคะ เป็นรองประธานกรรมการ นายศุภณัฐ สิรันทวิเนติ ผู้อำนวยการศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ เป็นกรรมการและเลขานุการ นับเป็นครั้งแรกที่ผู้อำนวยการศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ เป็นกรรมการในคณะกรรมการที่รัฐบาลแต่งตั้งขึ้นโดยก่อนหน้านี้ไม่มีการแต่งตั้งผู้อำนวยการศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้เป็นกรรมการในคณะกรรมการเพื่อแก้ไขความไม่สงบในชายแดนภาคใต้ของประเทศไทย โดยมีผลในวันที่ ๑ ตุลาคม พ.ศ.๒๕๕๙ รัฐบาลได้แต่งตั้ง พลโท ปิยวัฒน์ นาควานิช น้องชาย พลเอก ธีรชัย นาควานิช อดีตเลขาธิการคณะรักษาความสงบแห่งชาติ และอดีตผู้บัญชาการทหารบก เป็นแม่ทัพภาคที่ ๔ นับเป็นครั้งแรกที่แม่ทัพภาคที่ ๔ เป็นน้องชายของอดีตผู้บัญชาการทหารบก โดยมีผลในวันที่ ๑ ตุลาคม พ.ศ.๒๕๕๙

ในปี พ.ศ.๒๕๕๘ ได้มีการแปรสภาพ ตำแหน่งจังหวัดทหารบกปัตตานีและจังหวัดทหารบกสงขลาเป็นมณฑลทหารบก มีการแต่งตั้ง พลตรี เอกรัตน์ ช้างแก้ว เป็นผู้บังคับหน่วยเฉพาะกิจนราธิวาส ในปี พ.ศ.๒๕๕๙ ได้มีการแต่งตั้งพลตรี สมพล ปานกุล เป็นผู้บังคับหน่วยเฉพาะกิจยะลา พลตรี วิรัชช์ กมลศิลป์ เป็น ผู้บัญชาการมณฑลทหารบกที่ ๔๒ และผู้บังคับหน่วยเฉพาะกิจสงขลา ในวันที่ ๑ เมษายน พ.ศ.๒๕๖๐ ได้แต่งตั้ง พันเอก จตุพร กลัมพสุต เป็น ผู้บัญชาการมณฑลทหารบกที่ ๔๖ แทน พลตรี โภชน์ นวลบุญ

พลตำรวจเอก จักรทิพย์ ชัยจินดา มอบหมายให้ พลตำรวจโท รณศิลป์ ภู่สาระ เพื่อนร่วมรุ่นนักเรียนนายร้อยตำรวจ รุ่น ๓๖ เป็นผู้อำนวยการศูนย์ปฏิบัติการตำรวจจังหวัดชายแดนภาคใต้ และให้ พลตำรวจตรี พัฒนวุธ อังคะนาวิน พลตำรวจตรี พุทธิชาต เอกฉันท์ พลตำรวจตรี มณฑล เงินวัฒนะ พลตำรวจตรี ทนงศักดิ์ วังสุภา เป็นรองผู้อำนวยการศูนย์ปฏิบัติการตำรวจจังหวัดชายแดนภาคใต้ ต่อมามีการยุบศูนย์ปฏิบัติการตำรวจจังหวัดชายแดนภาคใต้รวมกับกองบัญชาการตำรวจภูธรภาค ๙ ในวันที่ ๑ กันยายน พ.ศ.๒๕๖๐ ส่งผลให้ผู้บัญชาการสูงสุดฝ่ายตำรวจที่แก้ไขปัญหาความไม่สงบชายแดนภาคใต้เปลี่ยนตัวบุคคลเป็น พลตำรวจโท สาคร ทองมุณี

ในส่วน กองอาสารักษาดินแดน พลเอก อนุพงษ์ เผ่าจินดา ในฐานะผู้บัญชาการกองอาสารักษาดินแดน ลงนามในคำสั่งกองบัญชาการกองรักษาดินแดนที่ ๕๗/๒๕๕๙ เรื่องจัดตั้งส่วนราชการในกองบัญชาการกองรักษาดินแดน จัดตั้งกองร้อยปฏิบัติการฝึกที่ ๑ ที่ อำเภอเมืองยะลา และกองร้อยปฏิบัติการพิเศษที่ ๒ ในวันที่ ๒๙ เมษายน พ.ศ.๒๕๕๙ โดยมี นายกองตรี ปารเมศ เห้งสวัสดิ์ เป็นผู้บังคับกองร้อย ปฏิบัติการพิเศษที่ ๒ คนแรก และ นายหมวดเอก เศรษฐการ เพชรวารี เป็นรองผู้บังคับกองร้อย และในวันที่ ๑ ตุลาคม พ.ศ.๒๕๕๙ มีการแต่งตั้ง นายหมวดโท อดุลย์ หมื่นลึก เป็นผู้บังคับหมวด

พลเอก ประยุทธ์ จันทร์โอชา ประกาศพื้นที่ปรากฏเหตุการณ์อันกระทบต่อความมั่นคงภายในราชอาณาจักร ในเขตพื้นที่อำเภอแม่ลาน จังหวัดปัตตานี และอำเภอจะนะ อำเภอนาทวี อำเภอเทพา และอำเภอสะบ้าย้อย จังหวัดสงขลา โดยประกาศใช้พระราชบัญญัติความมั่นคงภายในราชอาณาจักร พ.ศ.๒๕๕๑ มีผลตั้งแต่ ระหว่างวันที่ ๑ ธันวาคม พ.ศ.๒๕๕๙ ถึงวันที่ ๓๐ พฤศจิกายน พ.ศ.๒๕๖๑ และมอบหมายให้กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร เป็นผู้รับผิดชอบดำเนินการ

๔. การแก้ปัญหาของภาครัฐ

รัฐบาลในหลายๆ รัฐบาลได้จัดตั้งหน่วยงานในลักษณะที่ส่งตำรวจทหารและเจ้าหน้าที่จากส่วนกลางหรือจากกรุงเทพมหานคร ลงไปทำงานในพื้นที่ หรือแม้แต่รัฐบาล พลเอก ประยุทธ์ จันทร์โอชา ก็แก้ปัญหาในลักษณะเดียวกัน แตกต่างตรงที่รัฐบาลแต่งตั้งบุคคลเองทั้งหมดในนาม ผู้แทนพิเศษของรัฐบาล หน่วยงานเหล่านี้ถูกแต่งตั้งขึ้นและยุบแล้วแต่งตั้งใหม่ในชื่อที่แตกต่างกันไป อาทิ ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ คณะกรรมการนโยบายเฉพาะกิจแก้ไขปัญหาและพัฒนาจังหวัดชายแดนภาคใต้ กองอำนวยการเสริมสร้างสันติสุขจังหวัดชายแดนภาคใต้ศูนย์ปฏิบัติการคดีพิเศษจังหวัดชายแดนภาคใต้ คณะกรรมการบริหารจัดการในพื้นที่ตามนโยบายและยุทธศาสตร์เสริมสร้างสันติสุขจังหวัดชายแดนภาคใต้ กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักรภาค ๔ ส่วนหน้า ศูนย์ปฏิบัติการแก้ไขปัญหาจังหวัดชายแดนภาคใต้ กองร้อยบังคับการและบริการส่วนหน้าจังหวัดชายแดนภาคใต้ คณะกรรมการขับเคลื่อนการแก้ไขปัญหาจังหวัดชายแดนภาคใต้ การแก้ปัญหามีปัญหาอย่างมากเนื่องจากมีความเห็นแตกต่างกันอย่างมากในเรื่องของอำนาจในการคุมพื้นที่โดยฝ่ายทหารต้องการคุมพื้นที่ทั้งหมด และกดดันรัฐบาล ยิ่งลักษณ์ ชินวัตร ให้ลดอำนาจศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ลง ซึ่งศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ มีอำนาจเพิ่มขึ้นในสมัยรัฐบาล อภิสิทธิ์ เวชชาชีวะ เนื่องจากมีการออก พรบ. การบริหารราชการจังหวัดชายแดนภาคใต้ พ.ศ.๒๕๕๓ การแก้ปัญหาของภาครัฐก่อให้เกิดปัญหาเสียเองเนื่องจากคนในภาครัฐแย่งอำนาจกันเองในการคุมพื้นที่ ปัจจุบันก็ยังคงเดินหน้าแก้ปัญหาไฟใต้กันต่อไปโดยไม่มีแนวโน้มว่าความสงบสุขและสันติสุขจะกลับมาเมื่อใด (ศูนย์พัฒนาหลักนิยมและยุทธศาสตร์, ๒๕๕๙)

งานวิจัยที่เกี่ยวข้อง

งานวิจัยและวรรณกรรมที่เกี่ยวข้องในการวิจัยนี้มีดังต่อไปนี้

สหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union : ITU) ได้ให้ความหมายของคำว่า “ความมั่นคงทางไซเบอร์ (Cyber Security)” ว่าคือภาพรวมของเครื่องมือ (Tools), นโยบาย (Policies), แนวคิดการรักษาความปลอดภัย (Security Concepts), การรักษาความปลอดภัย (Security Safeguards), แนวทาง (Guidelines), วิธีการบริหารความเสี่ยง (Risk Management Approaches), การปฏิบัติ (Actions), การอบรม (Training), วิธีปฏิบัติที่เป็นเลิศ (Best Practices), การรับประกัน (Assurance) และเทคโนโลยี (Technologies) ที่สามารถปกป้องสภาพแวดล้อมทางไซเบอร์ องค์กร และสินทรัพย์ผู้ใช้งาน ได้แก่ อุปกรณ์สำหรับเชื่อมต่อคอมพิวเตอร์ ข้อมูลส่วนตัว โครงสร้างพื้นฐาน แอพพลิเคชั่น บริการระบบไอซีที และภาพรวมของการส่งผ่านหรือเก็บข้อมูลในไซเบอร์

เทอดพงษ์ เปล่งศิริวัฒน์ (๒๕๕๘) ได้เขียนสรุปรายงานเรื่อง “Cyber Attack ภัยคุกคามของสถาบันการเงินไทยในยุคดิจิตอล” โดยกล่าวว่า ปัจจุบันความก้าวหน้าทางเทคโนโลยีช่วยให้เกิดการพัฒนาในหลายภาคส่วน ภาคสถาบันการเงินถือเป็นส่วนหนึ่งที่ประยุกต์เทคโนโลยีเข้ามาตอบสนองความต้องการของลูกค้าในรูปแบบ Digital Banking ช่วยให้การทำธุรกรรมการเงินและการชำระเงินเป็นไปด้วยความสะดวก รวดเร็ว มีต้นทุนถูกลง และลูกค้าสามารถเข้าถึงบริการได้ง่ายขึ้น ในทุกที่ ทุกเวลา ทุกอุปกรณ์หรือ “Anytime, Anywhere, Any Device” แต่สิ่งที่มาพร้อมกับเทคโนโลยี นั่นคือ ภัยคุกคามทางไซเบอร์ (Cyber Attack) ที่ปัจจุบันเพิ่มขึ้นอย่างรวดเร็ว ด้วยหลากหลายรูปแบบและมีความซับซ้อนมากขึ้น อาจส่งผลเสียหายต่อสถาบันการเงินและลูกค้าผู้ใช้บริการ ล่าสุดที่ประชุม World Economic Forum ปี ๒๐๑๖ ได้จัดให้ Cyber Attack เป็น ๑ ใน ๑๐ ความเสี่ยงที่มีความสำคัญของโลก ความเสียหายจาก Cyber Attack ที่เกิดขึ้นในภาคการเงินการธนาคาร มักส่งผลกระทบต่อผู้ใช้บริการในวงกว้าง เช่น ในปี ๒๕๕๖ ระบบของธนาคารเจพีมอร์แกนในสหรัฐ ถูกแฮคเกอร์เจาะเข้าไปขโมยข้อมูลลูกค้ากว่า ๘๓ ล้านบัญชี ธนาคารในเกาหลีใต้ถูกโจมตีจนระบบ ATM และ Internet/Mobile Banking ใช้บริการไม่ได้ไปหลายชั่วโมง สำหรับประเทศไทย ในปี ๒๕๕๗ พบการแจ้งเตือนว่ามี Cyber Attack สูงถึง ๖๕ ล้านรายการ เพิ่มขึ้นกว่า ๒ เท่าจากปีก่อนหน้า รูปแบบ Cyber Attack ที่พบบ่อย ได้แก่ ๑) การก่อกวนเครือข่าย (Distributed Denial of Service Attack หรือ DDoS Attack) เป็นการระดมเรียกใช้งานระบบพร้อมๆ กันในเวลาสั้นๆ จนทำให้ระบบใช้งานไม่ได้ ๒) การปลอมหน้าเว็บไซต์ (Phishing) เป็นการปลอมแปลงหรือเปลี่ยนแปลงข้อมูลบนหน้าเว็บไซต์ เพื่อให้เกิดการเข้าใจผิดหรือเกิดความเสื่อมเสีย และอาจ

เชื่อมโยงไปสู่การขโมยข้อมูลสำคัญ และ ๓) การติดตั้งโปรแกรมประสงค์ร้าย (Malware) เพื่อขโมยข้อมูลและโจรกรรมเงินในบัญชี องค์กรต่างๆ ได้ให้ความส าคัญในการรับมือกับ Cyber Attack อาทิเช่น หน่วยงาน National Institute of Standards and Technology (NIST) ของสหรัฐที่ทำหน้าที่กำหนดมาตรฐานเทคโนโลยีสารสนเทศ ได้จัดทำแนวทางการรักษาความปลอดภัยทางไซเบอร์ (Cybersecurity Framework) เพื่อให้หน่วยงานภาครัฐ เอกชน รวมถึงสถาบันการเงินต่างๆ ใช้เป็นแนวทาง ในขณะที่ธนาคารกลางของอังกฤษ สหรัฐ และสิงคโปร์ จัดให้มีการทดสอบการรับมือ Cyber Attack ในระดับประเทศมาตั้งแต่ปี ๒๕๕๔

สำหรับการรับมือกับ Cyber Attack ของสถาบันการเงินในประเทศไทย ธนาคารแห่งประเทศไทย ได้กำหนดกรอบการดูแล Cyber Security ของสถาบันการเงิน โดยให้มีการดูแลตั้งแต่ระดับนโยบาย มีกระบวนการบริหารความเสี่ยง และมีการควบคุม ติดตาม เฝ้าระวังในการปฏิบัติงานประจำวันให้สอดคล้องกับมาตรฐานสากล โดยมีหน่วยงานเฝ้าระวังและดูแล Cyber Risk ตลอด ๒๔ ชั่วโมง อีกทั้งมีหน่วยงานบริหารความเสี่ยงควบคุมดูแลอีกชั้นหนึ่ง และท้ายสุดมีหน่วยงานอิสระเข้ามาตรวจสอบ และทดสอบการเจาะระบบเป็นประจำทุกปี เพื่อให้มั่นใจในในการรับมือกับ Cyber Attack นอกจากนั้นสถาบันการเงินยังมีแนวทางพัฒนาระบบในการติดตามเฝ้าระวังอย่างต่อเนื่องเพื่อให้ทันกับภัยคุกคามใหม่ๆ และให้ความรู้แก่ลูกค้าในวิธีการใช้บริการการเงินทางอิเล็กทรอนิกส์อย่างปลอดภัยและให้มีความระมัดระวังอย่างต่อเนื่อง และเพื่อให้การรับมือกับ Cyber Attack มีประสิทธิภาพและครอบคลุมมากยิ่งขึ้น สถาบันการเงิน ผู้กำกับดูแลหน่วยงานภาครัฐและเอกชนที่เกี่ยวข้องได้หาช่องทางประสานความร่วมมืออย่างมีบูรณาการ เพื่อให้มีการแลกเปลี่ยนข้อมูลข่าวสาร การแจ้งเตือนภัย การสื่อสารที่รวดเร็วและครอบคลุม การให้ความรู้อย่างต่อเนื่อง มีระบบกลางเพื่อเป็นแหล่งรวบรวมองค์ความรู้ตลอดจนมีการซักซ้อมและพัฒนาแนวทางป้องกันและรับมือ Cyber Attack ซึ่งความร่วมมือดังกล่าวจะก่อให้เกิดประสิทธิผลต่อเนื่องในระยะยาว เพื่อให้ระบบสถาบันการเงินไทยก้าวเข้าสู่ยุค Digital Banking อย่างมั่นคง มีเสถียรภาพ และปลอดภัย ได้รับความไว้วางใจจากผู้ใช้บริการ

อรฉัตร เลียงพิบูลย์ และคณะ (๒๕๕๙) ได้เขียนสรุปรายงานเรื่อง ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) โดยกล่าวว่า การพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสารส่งผลให้เกิดการพัฒนาทั้งทางด้านเศรษฐกิจและสังคมอย่างก้าวกระโดด เนื่องจากปัจจุบันมีการพัฒนาแอพพลิเคชั่นและซอฟต์แวร์ที่มีประสิทธิภาพสูง ทำให้ผู้ใช้งานทั่วไปสามารถเข้าถึงข้อมูลได้สะดวก รวดเร็ว และประหยัดค่าใช้จ่ายได้มากขึ้น หากผู้ใช้งานนำข้อมูลไปใช้ในทางที่สร้างสรรค์ก็สามารถใช้ให้เป็นประโยชน์ต่อการพัฒนาและยกระดับเศรษฐกิจ สังคม และสิ่งแวดล้อมในมิติต่างๆ ได้ ในทางกลับกันเทคโนโลยีก็สามารถสร้างความเสียหายได้มากมาย

เช่นกัน หากผู้ประสงค์ร้ายได้พัฒนาเครื่องมืออันทันสมัยเพื่อโจมตีระบบ ขโมย ทำลาย บิดเบือนข้อมูล หรือหลอกลวง ก็จะส่งผลให้เกิดการแทรกแซงและทำลายความมั่นคงได้ในทุกระดับ ไม่ว่าจะในระดับบุคคล ระดับหน่วยงาน ระดับชาติ และระดับโลก อย่างไรก็ตาม การรักษาความมั่นคงปลอดภัยทางไซเบอร์จำเป็นจะต้องคำนึงถึงการคุ้มครองความเป็นส่วนตัวและความสะดวกสบายในการเข้าถึงระบบของแต่ละบุคคลเวยเช่นกัน การมุ่งเน้นรักษาความมั่นคงของชาติอาจเกิดการรุกล้ำความเป็นส่วนตัว ในขณะที่การมุ่งทำให้เกิดความสะดวกสบายในการเข้าถึงระบบอาจทำให้ความมั่นคงปลอดภัยทางไซเบอร์เกิดความหละหลวมเช่นกัน ดังนั้นหน่วยงานที่รับผิดชอบจำเป็นต้องรักษาสมดุลระหว่างการรักษาความมั่นคงปลอดภัยทางไซเบอร์ การคุ้มครองความเป็นส่วนตัว และการอำนวยความสะดวกในการเข้าถึงระบบให้เหมาะสม เพราะเป็นกลไกสำคัญในการสร้างความไว้วางใจและการส่งเสริมให้เกิดการใช้เทคโนโลยีดิจิทัลในการทำงานทุกภาคส่วนเพื่อการพัฒนาประเทศไทย

กล่าวโดยสรุปได้ว่า ปัญหาเรื่องภัยคุกคามทางไซเบอร์จะยังคงเติบโตอย่างต่อเนื่องตามเทคโนโลยีที่ทันสมัยมากขึ้น หน่วยงานภาครัฐจะยังคงเป็นเป้าหมายสำคัญในการโจมตีทางไซเบอร์จากผู้ไม่หวังดี ทั้งจากการโจมตีเพื่ออาศัยความน่าเชื่อถือของหน่วยงานภาครัฐมาใช้หลอกลวงประชาชนอีกต่อหนึ่ง และการโจมตีเพื่อทำลายความน่าเชื่อถือของหน่วยงานอันเกิดจากสาเหตุต่างๆ ไม่ว่าจะเป็นการต้องการแสดงพลังของกลุ่มบุคคลที่ต่อต้านนโยบายของรัฐบาล การมุ่งทำลายชื่อเสียง การก่อกวน หรือแม้กระทั่งการโจมตีเพื่อทดสอบความสามารถของตนเองเพื่อแสดงให้กลุ่มแฮคเกอร์ด้วยกันได้รับรู้ ในอนาคตการโจมตีทางไซเบอร์จะมีการปรับเปลี่ยนวิธีการหรือมีความรุนแรงมากขึ้น เนื่องจากสามารถหาเครื่องมือในการโจมตีได้ง่ายจากอินเตอร์เน็ตและเว็บไซต์ใต้ดิน ซึ่งจะทำให้มีแฮคเกอร์หน้าใหม่เกิดขึ้นได้ง่าย รัฐบาลจะต้องให้ความสำคัญเรื่องความมั่นคงปลอดภัยทางไซเบอร์อย่างเป็นรูปธรรม โดยมีการประกาศใช้พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ผ่านการทำประชาพิจารณ์เพื่อรับฟังมุมมองที่เป็นประโยชน์และการได้รับการยอมรับจากภาคเอกชนและภาคประชาชน แต่สิ่งที่สำคัญยิ่งกว่านั้น ประชาชนโดยเฉพาะอย่างยิ่งบุคลากรของหน่วยงานภาครัฐในทุกระดับจะต้องตระหนักถึงความสำคัญ การเฝ้าระวัง และการปฏิบัติให้ถูกต้องตามมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงาน เพื่อป้องกันตนเองและหน่วยงานให้ปลอดภัยจากการถูกโจมตี นอกจากนี้การติดตามสถานการณ์ความมั่นคงปลอดภัยทางไซเบอร์ก็มีความสำคัญที่จะช่วยให้สามารถพร้อมรับมือกับภัยคุกคามใหม่ๆ ที่เกิดขึ้นได้อย่างทันท่วงที

ดร.สราวุธ ปิติยาศักดิ์ อาจารย์สาขานิติศาสตร์ มสธ. ได้เขียนบทความวิชาการเรื่อง “ภัยคุกคามทางไซเบอร์กับกฎหมายไซเบอร์ไทย” โดยกล่าวว่า “ภัยคุกคามทางไซเบอร์” (Cyber

Threats) ถือเป็นภัยคุกคามใหญ่หลวงต่อผลประโยชน์ทางเศรษฐกิจ ตลอดจนความมั่นคงของประเทศ การโจมตีทางไซเบอร์มีหลายรูปแบบ เช่น การเจาะระบบคอมพิวเตอร์ (Hacking) การสอดแนมข้อมูลคอมพิวเตอร์โดยสปายแวร์ การดักรับข้อมูลคอมพิวเตอร์ (Sniffing) การโจมตีโดยชุดคำสั่งไม่พึงประสงค์ (Malicious Software : Malware) หรือการรุมสอบถามข้อมูลจนระบบล่ม (Denial of Service Attack : DOS) เป็นต้น การโจมตีแต่ละครั้งล้วนสร้างความเสียหายอย่างมหาศาลทั้งต่อความมั่นคง ความปลอดภัยของระบบสารสนเทศ และเครือข่ายคอมพิวเตอร์ ตลอดจนระบบเศรษฐกิจและความมั่นคงของประเทศ ปัจจุบันประเทศไทยได้รับการแจ้งเหตุภัยคุกคามทางไซเบอร์ในแต่ละปีเป็นจำนวนมาก โดย พ.ศ.๒๕๖๐ ประเทศไทยมีการแจ้งเหตุภัยคุกคามทางไซเบอร์รวมถึง ๖๗ ครั้ง (๑ มกราคม-๑๙ กันยายน ๒๕๖๐) รัฐบาลไทยโดย พลเอก ประยุทธ์ จันทร์โอชา นายกรัฐมนตรี จึงมีนโยบายให้บูรณาการความมั่นคงปลอดภัยทางไซเบอร์ควบคู่กับการขับเคลื่อนเศรษฐกิจดิจิทัล โดยเตรียมจัดตั้ง “คณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ” หรือ National Cybersecurity Committee ซึ่งมีนายกรัฐมนตรีหรือรองนายกรัฐมนตรีที่ได้รับมอบหมายเป็นประธาน ทั้งนี้ เป็นหนึ่งในยุทธศาสตร์การพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมของรัฐบาล ควบคู่กับการเตรียมประกาศใช้ร่าง พ.ร.บ.รักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. …

การรักษาความมั่นคงปลอดภัยไซเบอร์ คือ การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ ซึ่งจำเป็นต้องใช้มาตรการทั้งทางเทคนิคและทางกฎหมาย รวมถึงการกำกับดูแลตนเอง และการกำกับดูแลร่วมกันของบุคคล ๓ ฝ่าย ผู้อาจได้รับผลกระทบจากการโจมตีทางไซเบอร์ ได้แก่ รัฐบาล หน่วยงานภาคเอกชน และภาคประชาสังคม

อย่างไรก็ดี แม้มาตรการทางกฎหมายอาจมีความจำเป็นในการรักษาความมั่นคงปลอดภัยไซเบอร์ อันอาจกระทบถึงความมั่นคงของชาติ แต่ความเข้มข้นของมาตรการดังกล่าวก็ต้องคำนึงถึงสิทธิเสรีภาพของประชาชน ให้ประชาชนยังคงดำรงซึ่งสิทธิเสรีภาพในโลกไซเบอร์ (โลกเสมือนจริง) เสมอกับที่มีในโลกแห่งความเป็นจริง ด้วยเหตุที่การโจมตีทางไซเบอร์อาจกระทำโดยผู้ไม่หวังดีที่มาจากทั้งภายในและภายนอกประเทศ ฉะนั้น รัฐบาล หน่วยงานภาคเอกชน และภาคประชาสังคม จำต้องมีการประสานความร่วมมือกันอย่างเป็นระบบ โดยแต่ละฝ่ายอาจมีบทบาทสำคัญ ดังนี้

๑. รัฐบาลหรือหน่วยงานของภาครัฐ ต้องมีหน้าที่หลักในการประสานความร่วมมือกับหน่วยงานภาคเอกชน และภาคประชาสังคม โดยรัฐบาลต้องกำหนดมาตรการกำกับติดตามและควบคุมการเข้าถึงและใช้งานระบบไอซีทีของหน่วยงานภาครัฐทุกหน่วย โดยเฉพาะอย่างยิ่งหน่วยงานทางความมั่นคง อีกทั้งต้องกำหนดให้หน่วยงานภาคเอกชนโดยเฉพาะอย่างยิ่งที่เกี่ยวข้องกับความมั่นคงของชาติ เช่น กิจการธนาคาร กิจการพลังงาน สายการบิน และสาธารณูปโภค เป็นต้น รวมถึงภาคประชาสังคมเพื่อให้ความร่วมมือกับภาครัฐโดยจัดให้มีการบริหารความเสี่ยงทาง

เทคนิคที่ดีและต่อเนื่อง เช่น มีระบบการตั้งค่าแบบปลอดภัย มีระบบควบคุมการเข้าถึง มีระบบป้องกันชุดคำสั่งไม่พึงประสงค์ ระบบจัดการปิดช่องโหว่คอมพิวเตอร์ และมีการแบ็กอัพข้อมูลสำคัญ เป็นต้น

๒. ภาคเอกชนต้องมีหน้าที่บริหารความเสี่ยงในการจัดการทางเทคนิคเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ เช่นไฟร์วอลล์ขอบเขต (Boundary Firewalls) เกตเวย์ อินเตอร์เน็ต ระบบการตั้งค่าแบบปลอดภัย และระบบควบคุมการเข้าถึง เป็นต้น นอกจากนี้ หน่วยงานภาคเอกชนที่เกี่ยวข้องกับกิจการสำคัญ เช่น กิจการธนาคาร สายการบิน ต้องมีหน้าที่รายงานการโจมตีทางไซเบอร์ให้หน่วยงานของภาครัฐทันที เพื่อป้องกันความเสียหายอย่างทันการณ์

๓. ภาคประชาสังคม รวมถึงประชาชนจะได้รับการคุ้มครองสิทธิเสรีภาพในโลกไซเบอร์ เสมอด้วยโลกแห่งความเป็นจริง

อย่างไรก็ตาม ภาคประชาสังคมควรมีหน้าที่เฝ้าระวังระบบและข้อมูลบนอินเตอร์เน็ตให้มีความมั่นคงปลอดภัย หากพบเว็บไซต์ที่มีเนื้อหาไม่เหมาะสมหรือพบการโจมตีทางไซเบอร์ควรรายงานต่อเจ้าหน้าที่ที่มีอำนาจในการจัดการปัญหาดังกล่าวทันทีในร่าง พ.ร.บ.รักษาความมั่นคงปลอดภัยไซเบอร์ของไทย ได้นิยามศัพท์คำว่า “ความมั่นคงปลอดภัยไซเบอร์” ว่าหมายถึง มาตรการและการดำเนินการเพื่อปกป้อง ป้องกัน ส่งเสริมเพื่อรับมือกับสถานการณ์ด้านภัยคุกคามที่จะส่งผลต่อการให้บริการด้านระบบเครือข่ายคอมพิวเตอร์ อินเตอร์เน็ต โครงข่ายโทรคมนาคม การให้บริการโดยปกติของดาวเทียม ระบบกิจการสาธารณูปโภคพื้นฐานและระบบกิจการสาธารณะที่สำคัญซึ่งเป็นเครือข่ายในระดับประเทศเพื่อมิให้เกิดผลกระทบต่อความมั่นคงของชาติ ความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ และความมั่นคงทางเศรษฐกิจ

จากนิยามศัพท์ข้างต้น จะเห็นได้ว่ากฎหมายไซเบอร์ของไทย มิได้มุ่งเฉพาะความมั่นคงปลอดภัยของระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ที่กระทบต่อเศรษฐกิจเท่านั้น แต่หมายความรวมถึงความมั่นคงทางการทหาร และความสงบเรียบร้อยภายในประเทศด้วย นอกจากนี้ กฎหมายไซเบอร์ของไทย ยังกำหนดให้มีคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรียกย่อว่า “กปช.” โดยมีหน้าที่สำคัญ คือ กำหนดแนวทางและมาตรการตอบสนองและรับมือกับภัยคุกคามไซเบอร์ และสั่งการหรือประสานความร่วมมือกับหน่วยงานภาครัฐภาคเอกชน เพื่อปฏิบัติให้เป็นไปตามนโยบายหรือแผนปฏิบัติการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือให้ดำเนินการอื่นใดที่จำเป็นต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ ทั้งในและนอกประเทศ ประการสำคัญที่สุดเพื่อประโยชน์ในการปฏิบัติหน้าที่ กฎหมายกำหนดให้พนักงานเจ้าหน้าที่ที่ได้รับมอบหมายเป็นหนังสือจากเลขาธิการ กปช. มีอำนาจเข้าถึงข้อมูลการติดต่อสื่อสาร ทั้งทางไปรษณีย์ โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือหรืออุปกรณ์ในการสื่อสาร

สื่ออิเล็กทรอนิกส์หรือสื่อทางเทคโนโลยีสารสนเทศใด หรือดำเนินการตามมาตรการที่เหมาะสม เพื่อประโยชน์ในการปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์และระงับยับยั้งความเสียหายที่จะเกิดขึ้น

ทั้งนี้ ในการปฏิบัติการของเจ้าหน้าที่ดังกล่าว ให้ยื่นคำร้องเพื่อขอคำสั่งศาลในการปฏิบัติตามอำนาจหน้าที่ แต่ในกรณีจำเป็นเร่งด่วนที่อาจจะเกิดความเสียหายอย่างร้ายแรง ให้พนักงานเจ้าหน้าที่ที่เกี่ยวข้องโดยการอนุมัติของ กปช. สามารถดำเนินการไปก่อนแล้วค่อยรายงานผลดำเนินงานและผลการปฏิบัติให้ศาลทราบโดยเร็ว

กฎหมายไซเบอร์ของไทยมุ่งรักษาความมั่นคงของรัฐจากการกระทำในโลกไซเบอร์ โดยให้อำนาจพิเศษแก่ กปช.อย่างมาก หน่วยงาน กปช.มีอำนาจอนุมัติให้เจ้าหน้าที่เข้าถึงการติดต่อสื่อสารทุกรูปแบบของประชาชน ทั้งนี้กฎหมายไซเบอร์ของไทยควรมุ่งเน้นในการสร้างความร่วมมือระหว่างหน่วยงานภาครัฐ หน่วยงานภาคเอกชน ภาคประชาสังคม ในลักษณะของการกำกับดูแลตนเองและการกำกับดูแลร่วมกัน มากกว่าการใช้ตัวบทกฎหมายที่เข้มงวดเกินไป ซึ่งอาจกระทบถึงสิทธิเสรีภาพของประชาชนในการติดต่อสื่อสารได้

แนวคิดของผู้ทรงคุณวุฒิ

แนวคิดของผู้ทรงคุณวุฒิด้านระบบไอซีทีและนักกฎหมายด้านไซเบอร์ ได้ให้นิยามและความหมายของภัยคุกคามด้านไซเบอร์ไว้ดังนี้

Richard A. Clarke (2017) อดีตที่ปรึกษาประธานาธิบดีสหรัฐอเมริกาด้านความมั่นคง ได้นำประสบการณ์ที่สหรัฐอเมริกาและประเทศต่างๆ ทั่วโลกที่ได้เผชิญปัญหาภัยคุกคามด้านไซเบอร์มาเป็นบทเรียนในการขับเคลื่อนนโยบายของสหรัฐอเมริกา โดย Clarke ได้สรุปหัวใจของแนวคิดเป็น ๔ ปัญหา และพบว่าปัญหาภัยคุกคามด้านไซเบอร์แบ่งออกได้เป็น ๔ ลักษณะ สรุปโดยย่อคือ C.H.E.W. นั่นคือ

C คือ Cybercrime เป็นปัญหาการก่ออาชญากรรมทางไซเบอร์โดยมีวัตถุประสงค์ทางการเงิน เช่นการแฮ็คบัญชีธนาคารหรือธุรกรรมออนไลน์ต่างๆ ทำให้คนส่วนหนึ่งไม่ยอมทำธุรกรรมออนไลน์ และคิดว่าตนเองก็จะไม่ได้รับผลกระทบ แต่ในมุมมองของผู้เชี่ยวชาญอาชญากรรมเหล่านี้เพิ่มต้นทุนต่อระบบ และระบบก็จะผลักต้นทุนนั้นให้ผู้บริโภคทุกคนไม่ว่าจะออฟไลน์หรือออนไลน์แบกรับในที่สุด ปัญหานี้จึงกระทบทุกคนอย่างหลีกเลี่ยงไม่ได้

H คือ Hacktivism เป็นการแฮ็คข้อมูลลับไม่ว่าจะของทางการหรือเอกชนแล้วนำมาเผยแพร่ต่อสาธารณะ เพื่อเปิดโปงเรื่องบางอย่างหรือสร้างความอับอายแก่เจ้าของข้อมูล รวมถึงการแฮ็คเว็บเพจแล้วเผยแพร่ข้อความของตนลงไปในเว็บเหล่านั้นเพื่อประกาศจุดยืนหรืออุดมการณ์

ต่างๆ แม้เราจะป้องกันตัวเองดีเพียงใด แต่หากเป็นการสื่อสารกับปลายทาง เช่น อีเมล์ เมื่อปลายทางถูกแฮ็ค ข้อมูลของเราก็รั่วไหลอยู่ดี

E คือ Espionage เป็นการจารกรรมข้อมูลเพื่อนำไปใช้ประโยชน์ต่อ เช่น การเจาะข้อมูลนวัตกรรมต่างๆ การเจาะข้อมูลทางการทหาร ซึ่งในอดีตใครที่พยายามขโมยเอกสารที่มีชั้นความลับของหน่วยงานต่างๆ เท่ากับต้องบุกรุกเข้าไปในหน่วยงาน แต่ในยุคดิจิตัล แฮ็คเกอร์อาจซ่อนตัวอยู่มุมใดมุมหนึ่งของโลก แล้วเชื่อมต่อทางออนไลน์ ต้นทุนการจารกรรมจึงต่ำมาก และความเสี่ยงในการถูกจับตัวได้ก็ลดลงมาก

W คือ War หรือ Cyberwar ซึ่งเกิดขึ้นแล้ว เช่น การทำลายฐานผลิตอาวุธนิวเคลียร์โดยไม่ต้องส่งกำลังพลหรือใช้อาวุธกายภาพแม้แต่น้อย แต่เป็นการส่งคำสั่งเข้าไปให้เครื่องยนต์ทำลายตนเอง หรือแม้แต่การที่บางประเทศโจมตีทางไซเบอร์เพื่อให้ระบบสื่อสารและแหล่งพลังงานของปฏิปักษ์ล่ม แล้วใช้กำลังพลบุกยึดครองดินแดนจริงได้อย่างง่ายดาย

ปัญหาทั้งหมดนี้ชี้ให้เห็นความจำเป็นในการพัฒนานโยบาย Cybersecurity และเพื่อการกำหนดนโยบายได้อย่างถูกต้อง ควรดำเนินการดังนี้

๑. การเลือกพัฒนาระบบโจมตี หรือจะพัฒนาระบบป้องกัน (Offense vs Defense) บางท่านคิดว่าอาวุธไซเบอร์ที่ทรงอานุภาพจะทำให้เราเป็นฝ่ายชนะ แต่แท้จริงแล้วภัยของการคุกคามทางไซเบอร์คือการถูกโจมตี ซึ่งเกิดขึ้นเวลาใดก็ได้ การขาดระบบป้องกันที่ดีกลับจะทำให้เราเป็นฝ่ายแพ้อย่างราบคาบ การพัฒนาระบบรับมือการโจมตีจึงควรเป็นสิ่งสำคัญลำดับแรก

๒. การปกป้องโครงสร้างพื้นฐานที่สำคัญ (Critical Infrastructure) ซึ่งรัฐมิได้ควบคุมด้วยตนเอง จะเลือกนโยบายเสรีให้ต่างคนต่างรับผิดชอบตนเอง หรือต้องมีนโยบายกำกับดูแล (Market forces vs Regulation) โครงสร้างพื้นฐานในยุคดิจิตัลล้วนเชื่อมต่อออนไลน์ และเสี่ยงต่อภัยคุกคาม เช่น ด้านการผลิตพลังงานหรือกระแสไฟฟ้า ด้านการขนส่งทั้งทางบก ทางน้ำ ทางอากาศ ด้านการเงินการธนาคาร ด้านโรงพยาบาลหรือบริการทางการแพทย์ ด้านการสื่อสาร หรือแม้กระทั่งตลาดหลักทรัพย์ ซึ่งล้วนแล้วแต่มีความสำคัญอย่างยิ่งยวด แต่การพัฒนาระบบรับมือภัยคุกคามต้องมีต้นทุน และในบางครั้งเอกชนก็เน้นการควบคุมหรือลดต้นทุนของตนเอง แต่ผลกระทบจากภัยคุกคามต่อสังคมนั้นมีมูลค่าสูงมากกว่าหลายเท่าตัว เช่น หากระบบไฟฟ้าของประเทศล่ม เท่ากับเศรษฐกิจดิจิทัลหยุดชะงัก จึงจำเป็นต้องมีการกำกับดูแล โดยการออก Smart Regulation ตามด้วยการตรวจสอบการปฏิบัติตามกติกา การทดสอบการโจมตีทางไซเบอร์ และการปรับปรุงพัฒนาระบบ

๓. การคุ้มครองความเป็นส่วนตัว หรือการคุ้มครองความปลอดภัย (Privacy vs Security) สังคมกังวลเกี่ยวกับการถูกละเมิดความเป็นส่วนตัวเพราะรัฐมักจะยกข้ออ้างเรื่อง Cybersecurity แต่หากไม่มี Cybersecurity ก็ไม่มีความเป็นส่วนตัว เพราะข้อมูลของเราจะถูกแฮ็คได้ตลอดเวลา ทั้งสองเรื่องจึงไม่ใช่คู่ตรงข้ามกัน แต่เป็นเรื่องที่ต้องคำนึงไปพร้อมกัน สังคมยอมรับได้หากการเปิดเผยข้อมูลเป็นไปตามคำสั่งศาลโดยชอบด้วยกฎหมาย แต่ภัยคุกคามนั้นต้องรับมือโดยเร็วให้ทันการณ์ จึงต้องมีการพัฒนาระบบการพิจารณาโดยศาลเฉพาะเรื่องนี้ให้ตอบสนองปัญหาได้เร็วที่สุด แทนระบบการออกหมายศาลแบบเดิม

๔. การลงทุนด้านซอฟต์แวร์ หรือการลงทุนพัฒนาคน (Software vs People) บริษัทพัฒนาระบบรักษาความปลอดภัยไซเบอร์มักมุ่งเน้นขายระบบให้กับหน่วยงานต่างๆ แต่การซื้อซอฟท์แวร์มาใช้งานไม่สามารถรับมือภัยคุกคามได้จริง หากบุคลากรยังมีพฤติกรรมเสี่ยง ขาดความตระหนัก หรือความรู้ความเข้าใจในเรื่องนี้ จึงต้องให้ความสำคัญกับคนมากกว่าเน้นการซื้อหรือมุ่งพัฒนาระบบแล้วคิดว่าได้เตรียมการรับมือเรียบร้อยแล้ว และเราต้องค้นหาแฮ็คเกอร์ฝีมือดีแล้วเปลี่ยนให้เป็นบุคลากรด้าน Cybersecurity ของประเทศซึ่งยังขาดแคลนเป็นอย่างมาก

๕. นวัตกรรม หรือความน่าเชื่อถือ (Innovation vs Reliability) ในยุคอินเตอร์เน็ตของสรรพสิ่ง มีอุปกรณ์เชื่อมต่อออนไลน์หลายพันล้านชิ้น และจะเพิ่มเป็นหลายหมื่นล้านชิ้นในอีกสามปีข้างหน้า ที่ผ่านมามีการแฮ็คกล้องวงจรปิดนับแสนตัวเพื่อโจมตี DDoS ไปยังระบบคอมพิวเตอร์เป้าหมาย หากอุปกรณ์หลายหมื่นล้านชิ้นเสี่ยงต่อภัยคุกคาม อนาคตของเราจะเป็นอย่างไรและความเสียหายจะมากขนาดไหน

๖. การป้องกันการบุกรุกหรือความยืดหยุ่นในการรับมือการบุกรุก (Prevention of Attack vs Resilience) การป้องกันการบุกรุกคือความพยายามไม่ให้ผู้โจมตีเข้าสู่ระบบได้ แต่ความยืดหยุ่นในการรับมือ คือเมื่อผู้บุกรุกเข้ามาในระบบ จะจำกัดขอบเขตของปฏิบัติการโจมตีได้ในระดับใด และหากเกิดผลกระทบแล้วจะฟื้นฟูระบบให้กลับสู่ปกติโดยเร็วได้อย่างไร เช่น การกู้ระบบไฟฟ้าของประเทศให้กลับคืนมาในเวลานับเป็นชั่วโมง ไม่ใช่เป็นวัน หรือเป็นสัปดาห์ หมายความว่าแต่ละระบบต้องมีข้อมูลสำรองและระบบสำรอง และต้องมีการฝึกซ้อมการกู้ระบบอย่างสม่ำเสมอ ไม่ต่างจากการซ้อมรับอัคคีภัยในอาคาร

นงรัตน์ สายเพชร (๒๕๕๖) นักวิชาการด้านความมั่นคงด้านไซเบอร์ ได้กล่าวถึงประเด็นภัยคุกคามทางไซเบอร์ว่า ผู้ก่อการเหตุทางไซเบอร์คือกลุ่มบุคคลหรือองค์กรที่มีความชำนาญในการปฏิบัติการ ภัยคุกคามไซเบอร์ซึ่งสามารถแบ่งออกเป็น ๕ กลุ่ม ได้แก่

๑. ภัยคุกคามที่เกิดจากการใช้โปรแกรมประยุกต์ โปรแกรมประยุกต์ (Application-Based Threats) ที่ถูกดาวน์โหลดมาเพื่อติดตั้งบนคอมพิวเตอร์หรืออุปกรณ์เคลื่อนที่อาจจะถูกแอบ

แฝงมาด้วยโปรแกรมที่เป็นภัยคุกคาม ภัยคุกคามประเภทนี้เรียกว่ามัลแวร์ (Malware) ซึ่งเป็นโปรแกรมที่ถูกออกแบบมาเพื่อทำอันตรายต่อข้อมูลในคอมพิวเตอร์หรืออุปกรณ์เคลื่อนที่ทำให้เกิดความขัดข้องหรือเสียหายกับระบบปฏิบัติการ นอกจากนี้โปรแกรมที่ติดมัลแวร์ยังส่งข้อความที่ไม่พึงประสงค์ออกไปยังผู้อื่นหรือขโมยข้อมูลสำคัญออกไป ตัวอย่างโปรแกรมในกลุ่มนี้ ได้แก่ Virus, Worm, Trojan, Botnet หรือ Spyware เป็นต้น

๒. ภัยคุกคามที่เกิดจากการใช้งานเว็บไซต์ ภัยคุกคามที่เกิดจากการใช้งานเว็บไซต์ (Web-Based Threats) เป็นภัยคุกคามที่เกิดจากการที่ผู้ใช้คอมพิวเตอร์หรืออุปกรณ์พกพา เปิดเว็บไซต์ขึ้นมาใช้งาน ซึ่งเว็บไซต์ที่เรียกมาใช้อาจเป็นเว็บไซต์ฟิชชิ่ง (Phishing) ซึ่งถูกออกแบบให้มีลักษณะคล้ายคลึงกับเว็บไซต์จริงเพื่อหลอกให้ผู้ใช้กรอกข้อมูลเข้าสู่ระบบของผู้ไม่หวังดี เช่น หลอกให้ผู้ใช้งานล็อกอินเข้าอีเมล์ เฟสบุ๊ค หรือเว็บไซต์ที่เกี่ยวข้องกับธุรกรรมทางการเงิน ซึ่งจะคอยดักจับรหัสล็อกอินของผู้ใช้งานนั้นๆ ทำให้ข้อมูลหรือบัญชีการใช้งานนั้นๆ มีความเสี่ยงที่จะโดนขโมยข้อมูลออก

๓. ภัยคุกคามจากการใช้งานเครือข่ายไร้สาย ปัจจุบันมีผู้ให้บริการเครือข่ายไร้สายเป็นจำนวนมาก มีทั้งที่น่าเชื่อถือและที่ไม่น่าเชื่อถือ รวมถึงผู้ที่แอบแฝงเพื่อวัตถุประสงค์อื่น ดังนั้นผู้ใช้คอมพิวเตอร์หรืออุปกรณ์เคลื่อนที่เชื่อมต่อระบบเครือข่ายไร้สายต่างๆ อาจได้รับผลกระทบโดยตรง รวมถึงยังสามารถเป็นต้นตอของผลกระทบไปยังอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์เคลื่อนที่ของผู้อื่นด้วยเช่นกัน โดยผู้ใช้เครือข่ายไร้สายอาจถูกโจมตีด้วยมัลแวร์ผ่านข้อบกพร่องของระบบปฏิบัติการ และถูกเปลี่ยนสถานะมาเป็นผู้โจมตีโดยการส่งต่อหรือแพร่กระจายมัลแวร์เหล่านี้ไปยังอุปกรณ์อื่นผ่านเครือข่ายไร้สายหรือบลูทูธ นอกจากนี้ การใช้เครือข่ายไร้สายยังเปิดโอกาสให้ผู้ไม่ประสงค์ดีดักจับข้อมูลสำคัญ หรือรหัสผ่านบนเครือข่ายไร้สายได้อีกด้วย

๔. ภัยคุกคามที่เกิดจากการถูกโจมตีแบบเจาะจงเป้าหมาย ภัยคุกคามที่เกิดการโจมตีแบบเจาะจงเป้าหมาย (Targeted Attack) ที่มาจากหลายประเทศมีมากขึ้น ผู้โจมตีหรือแฮคเกอร์ (Hackers) ในประเทศต่างๆ จะใช้การโจมตีแบบเจาะจงเป้าหมายอย่างต่อเนื่อง สร้างความเสียหายให้แก่โครงสร้างพื้นฐานวิกฤต สถาบันการเงิน และองค์กรอื่นๆ ของภาครัฐและภาคเอกชนในหลายประเทศ อาชญากรทางไซเบอร์เหล่านี้จะใช้มาตรการที่รวดเร็วและรุนแรงในการโจรกรรมข้อมูล ภัยคุกคามประเภทนี้จัดว่าเป็นภัยคุกคามที่กระทบต่อความมั่นคงของประเทศเป็นอย่างยิ่ง

พลตรี ฤทธิ อินทราวุธ (๒๕๕๘) อดีตผู้อำนวยการศูนย์ไซเบอร์กองทัพบก ได้นิยามและให้คำจำกัดความที่เกี่ยวข้องกับภัยคุกคามด้านไซเบอร์ดังนี้

คำว่า “ไซเบอร์” (Cyber) หมายถึง สิ่งที่เกี่ยวข้องกับระบบคอมพิวเตอร์และสังคมเครือข่ายสากล (เช่น ระบบอินเตอร์เน็ตและเครือข่ายต่างๆทั้งแบบมีสายและไร้สาย) และอาจ

หมายถึง สารสนเทศเสมือนจริงที่ถูกสร้างขึ้นหรือเกิดขึ้นเอง แต่คำว่า “สงครามไซเบอร์” (Cyber War) หรือ “การทำสงครามไซเบอร์” (Cyber Warfare) ความหมายของคำนี้จะขึ้นอยู่กับมุมมองของแต่ละบุคคลเป็นหลัก เช่น บางคนอาจให้ความหมายแคบๆ โดยบอกว่า “สงครามไซเบอร์” เป็นการปฏิบัติการทางทหารที่อาศัยหลักการที่เกี่ยวข้องกับสารสนเทศโดยที่ฝ่ายเราพยายามที่จะรู้ ขัดขวางและทำลายสารสนเทศของฝ่ายตรงข้ามให้มากที่สุด ในขณะเดียวกันก็พยายามไม่ให้ฝ่ายตรงข้ามดำเนินการในลักษณะเดียวกันกับสารสนเทศของฝ่ายเรา หรือบางคนอาจให้ความหมายในวงกว้างมากขึ้นได้ว่า “สงครามไซเบอร์” ซึ่งเป็นการโจมตีโดยอาศัยการก่อวินาศกรรมหรือการจารกรรมต่อสารสนเทศของฝ่ายตรงข้ามผ่านทางระบบคอมพิวเตอร์หรือสังคมเครือข่ายเพื่อบรรลุวัตถุประสงค์ที่ต้องการ ส่วนการก่อวินาศกรรมสารสนเทศนั้นอาจเป็นกิจกรรมในลักษณะของการรบกวนด้วยการโจมตีระบบคอมพิวเตอร์หรือสังคมเครือข่ายเป้าหมายบนอินเตอร์เน็ตของกลุ่มนักเจาะระบบคอมพิวเตอร์ เพื่อทำให้ระบบเป้าหมายปฏิเสธหรือหยุดการทำงานที่เรียกว่า “DoS Attack” หรือในลักษณะของการโจมตีพร้อมๆ กันต่อระบบที่เป็นเป้าหมายเดียวกัน โดยระบบที่ตกเป็นเหยื่อทั้งหมดจะสร้างข้อมูลขยะขึ้นมาแล้วส่งไปยังระบบที่เป็นเป้าหมาย ทำให้ข้อมูลไหลเข้าสู่ระบบที่เป้าหมายด้วยปริมาณมหาศาลจนกระทั่งระบบเป้าหมายต้องทำงานหนักขึ้น ช้าลงเรื่อยๆ และเมื่อเกินกว่าระดับที่ระบบเป้าหมายจะรับได้ก็จะหยุดการทำงานในที่สุด อีกทั้งมีการสร้างไวรัสรูปแบบต่างๆ เพื่อก่อกวนหรือโจมตีการทำงานของระบบคอมพิวเตอร์ ในส่วนของการจารกรรมสารสนเทศนั้นมักเกี่ยวข้องกับการค้นหาข้อมูลส่วนตัวของบุคคลที่เป็นเป้าหมาย (Doxing) การขโมยทรัพย์สินทางปัญญา และการสอดแนมระบบทางการเงินผ่านทางระบบออนไลน์ เป็นต้น

หยาดพิรุณ นาชัยสินธุ์ (๒๕๖๐) คณะรัฐศาสตร์และนิติศาสตร์ มหาวิทยาลัยบูรพา กล่าวว่า การก่อการร้ายด้านไซเบอร์เป็นรูปแบบของการก่อการร้ายโดยมีการนำระบบไอซีทีที่ทันสมัยนำมาเป็นเครื่องมือที่ช่วยให้กลุ่มก่อการร้ายสามารถดำเนินกิจกรรมต่างๆ ผู้ก่อการร้ายสามารถใช้ช่องทางไซเบอร์และผู้ใช้ระบบไอซีทีตกเป็นเป้าของการโจมตีเพื่อทำลายหรือขัดขวางการทำงานระบบเครือข่ายคอมพิวเตอร์แบบต่างๆ ไม่ว่าจะเป็นเครือข่ายการสื่อสารหรือเครือข่ายระบบคอมพิวเตอร์ที่เกี่ยวข้องกับการทำงานขององค์กรขนาดใหญ่ การควบคุมโครงสร้างพื้นฐานระบบโครงสร้างความมั่นคงทางทหาร และการล้วงข้อมูลความมั่นคงของประเทศ เป็นต้น โดยใช้วิธีการสร้างความเสียหาย ก่อให้เกิดความตื่นตระหนกต่อประชาชนและดึงดูดความสนใจของสื่อมวลชนหรือบุคคลต่างๆ ซึ่งคาดหมายว่าอนาคตจะมีการก่อการร้ายด้านไซเบอร์และเป็นยุทธวิธีในการก่อการร้ายที่มีอานุภาพร้ายแรงมาก การก่อการร้ายด้านไซเบอร์มีรูปแบบและวิธีการดังนี้ ๑) ผู้ก่อการร้ายต้องมีความรู้ด้านไซเบอร์หรือเทคโนโลยีและศึกษาข้อมูลที่เกี่ยวกับเป้าหมายที่ต้องการจะกระทำ ๒) สร้างหรือพัฒนาเครื่องมือให้ตรงกับความต้องการต่อเป้าหมาย โดยเครื่องมือ

ที่สำคัญของการก่อการร้ายทางไซเบอร์คือ อินเตอร์เน็ต ๓) ระดมคนหรือหาสมาชิกที่มีแนวความคิดแนวทางเดียวกัน ๔) ระดมเงินทุนในการสนับสนุน และ ๕) ปฏิบัติการตามวัตถุประสงค์ที่วางไว้เพื่อมุ่งเป้าหมายหลักทางการเมือง โดยสอดคล้องกับงานวิจัยของ Gobran (2015) ที่วิจัยเรื่อง ภัยคุกคามของผู้ก่อการร้ายด้านไซเบอร์ พบว่า กลุ่มผู้ก่อการร้ายเริ่มต้นการปรับให้เข้ากันและยึดเอาความได้เปรียบของเครื่องมือและความสามารถของเครื่องมือด้านไซเบอร์ การคุกคามผู้ก่อการร้ายจะกระทำเพื่อการเติบโตของกลุ่มร่วมกัน ถึงแม้ว่าผู้ก่อการร้ายจะ ไม่มีฝีมือต่อการฆ่าคนอย่างรวดเร็วโดยตรงกับการใช้เครื่องมือด้านไซเบอร์ การประทุษร้ายหรือการขัดขวางทางสังคม และการโจมตีสามารถเป็นเหตุพอดีกับวัตถุประสงค์การดำเนินการ

สราวุธ ปิติยาศักดิ์ (๒๕๖๑) อาจารย์สาขานิติศาสตร์ มสธ. ได้นิยามว่า “ภัยคุกคามทางไซเบอร์” (Cyber Threats) ถือเป็นภัยคุกคามใหญ่หลวงต่อผลประโยชน์ทางเศรษฐกิจ ตลอดจนความมั่นคงของประเทศ การโจมตีทางไซเบอร์มีหลายรูปแบบ เช่น การเจาะระบบคอมพิวเตอร์ (Hacking) การสอดแนมข้อมูลคอมพิวเตอร์โดยสปายแวร์ การดักรับข้อมูลคอมพิวเตอร์ (Sniffing) การโจมตีโดยชุดคำสั่งไม่พึงประสงค์ (Malicious Software : Malware) หรือการรุมสอบถามข้อมูลจนระบบล่ม (Denial of Service Attack : DOS) เป็นต้น การโจมตีแต่ละครั้งล้วนสร้างความเสียหายอย่างมหาศาล ทั้งต่อความมั่นคงและความปลอดภัยของระบบไอซีทีและเครือข่ายคอมพิวเตอร์ตลอดจนระบบเศรษฐกิจและความมั่นคงของประเทศ

ปริญญา หอมเอนก (๒๕๖๑) ประธานและผู้ก่อตั้ง บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด กล่าวถึงสถานการณ์ภัยคุกคามทางไซเบอร์ในปัจจุบันว่า ในต่างประเทศกำลังเปลี่ยนจากการลงทุนทางด้านไซเบอร์ซิเคียวริตี้ (Cyber Security) หรือการเตรียมความพร้อมก่อนเกิดการโจมตีที่ปัจจุบันกลายเป็นพื้นฐานของระบบรักษาความปลอดภัย เข้าสู่ยุคของ ไซเบอร์ริซีเลียนซ์ (Cyber Resilience) ในการเตรียมแผนว่าถ้าโดนโจมตีแล้วองค์กรต้องทำอย่างไร

“Cyber Resilience ถือเป็นอีกระดับของการรักษาความปลอดภัยในโลกไซเบอร์ ที่ทราบกันดีว่าการโจมตีทางออนไลน์จะเกิดขึ้นจากใครก็ได้ ดังนั้นองค์กรควรมีแผนในการรับมือภัยคุกคามที่เกิดขึ้นว่าเมื่อเกิดขึ้นแล้วต้องทำอย่างไร เพื่อให้ธุรกิจเดินหน้าต่อไป หรือให้บริการลูกค้าต่อไปได้โดยไม่กระทบจากภัยคุกคาม”

ขณะเดียวกัน ยังได้มีการเสนอแผนการยกระดับความปลอดภัยนี้เข้าไปในร่าง พรบ. ความมั่นคงทางไซเบอร์ เพื่อให้ประเทศสามารถเตรียมความพร้อมในการรับมือกับการโจมตีทางไซเบอร์บนแนวคิดที่ทันสมัยขึ้น ไม่ใช่การยกร่างจากแนวคิดในอดีตที่ไม่เพียงพอต่อการป้องกันภัยคุกคามแล้ว “ตอนนี้ทุกฝ่ายที่เกี่ยวข้องต้องเปลี่ยนแนวคิด ที่ว่าทำอย่างไรธุรกิจจะรอดจากการโจมตีมาเป็นการเตรียมความพร้อมว่า เมื่อมีการโจมตีทางไซเบอร์แล้วจะป้องกันและแก้ไขอย่างไร ซึ่งใน

ต่างประเทศก็เริ่มพูดเรื่องนี้มา ๒-๓ ปีแล้ว และคิดว่าถึงเวลาที่ประเทศไทยต้องเตรียมความพร้อมในเรื่องนี้”

สำหรับในประเทศไทยเริ่มมีหน่วยงานที่เริ่มขยับแล้วเกี่ยวกับการทำ Cyber Resilience คือธนาคารแห่งประเทศไทย ในการกำหนดกรอบประเมินความพร้อมด้าน Cyber Resilience สำหรับสถาบันการเงินที่อยู่ภายใต้การกำกับดูแลของธปท. ที่ธนาคารหรือหน่วยงานที่เกี่ยวข้องจะต้องมีการเตรียมความพร้อมทั้งในแง่ของการเฝ้าระวัง (Security Operation Center) การซ้อมรับการโจมตี (Cyber Drill) และมีแผนรองรับในกรณีเกิดเหตุการณ์ไม่คาดคิด (Incident Response)

นอกจากนี้ ยังชี้ให้เห็นถึง ๑๐ แนวโน้มการป้องกันภัยที่จะเกิดขึ้นในช่วงปี พ.ศ.๒๕๖๑ ประกอบไปด้วย

๑. ระบบการรักษาความปลอดภัยแบบยืนยันตัวตน ๒ ขั้นตอน จะกลายเป็นมาตรฐานของการใช้งานคลาวด์ เนื่องจากมีคุณลักษณะในการป้องกันการจารกรรมข้อมูลได้ดีกว่ารูปแบบในปัจจุบัน

๒. ระบบเศรษฐกิจข้อมูลจะเข้ามาแทนที่ระบบเศรษฐกิจดิจิทัล ทำให้จะเกิดการโจมตีทางด้านข้อมูลในระดับชาติเพิ่มมากขึ้น จากการที่ปัจจุบันข้อมูลออนไลน์ต่างๆ ถูกนำไปเก็บไว้ในต่างประเทศ

๓. เกิดภัยคุกคามจากข้อมูลส่วนบุคคลที่อยู่ในโซเชียลมีเดีย สมาร์ทโฟน และคลาวด์โดยไม่สามารถระงับยับยั้งได้อย่างสมบูรณ์

๔. การเก็บข้อมูลบนคลาวด์สาธารณะจะไม่ปลอดภัยอีกต่อไป เมื่อผู้ให้บริการสามารถวิเคราะห์ข้อมูลที่ถูกส่งขึ้นไปเก็บได้ จนก่อให้เกิดการรั่วไหลของข้อมูล ดังนั้นองค์กรควรเลือกใช้คลาวด์สำหรับองค์กรธุรกิจ หรือควรทำการป้องกันข้อมูลบนคลาวด์ให้เหมาะสม

๕. จะมีการนำระบบ Artificial Intelligence หรือ AI และ Machine Learning มาใช้ในการวิเคราะห์และนำเสนอข้อมูลแก่ผู้ใช้งานอินเตอร์เน็ต จนเกิดการโน้มน้าวผู้บริโภคเพื่อทำให้เลือกซื้อสินค้าและบริการจากข้อมูลที่ถูกปั้นเข้ามาแบบเฉพาะตัว

๖. การลงทุนทางด้าน ICO และ Smart Contract จะกลายเป็นเรื่องที่ทุกฝ่ายให้ความสนใจ ซึ่งหน่วยงานกำกับดูแลควรออกมาควบคุมให้เหมาะสม

๗. เรื่องถิ่นที่อยู่ของข้อมูล (Data Residency) และการกำกับดูแล OTT ยังเป็นประเด็นสำคัญที่ควรมีหน่วยงานมากำกับดูแล เนื่องจากปัจจุบันข้อมูลการใช้งานออนไลน์ของผู้บริโภคในไทยถูกนำไปเก็บไว้ในต่างประเทศทั้งหมด จากผู้ให้บริการข้ามชาติ ดังนั้นข้อมูลเหล่านี้จึงถือเป็นความเสี่ยงที่อาจเกิดการนำข้อมูลไปใช้ในทางที่ไม่ถูกต้องได้

๘. สมาร์ทโฟนจะกลายเป็นช่องทางในการโจมตีด้วยฟิชชิ่ง และอีเมล์หลอกลวงยังคงเป็นช่องทางหลักในการโจมตีของแฮกเกอร์ ทำให้องค์กรต้องมีการอบรมให้ความรู้ความเข้าใจกับพนักงาน ควบคู่ไปกับการทดลองโจมตีเพื่อให้เกิดการตระหนักถึงภัยคุกคามดังกล่าวและรู้ทันสถานการณ์ที่จะเกิดขึ้น

๙. การโจมตีอุปกรณ์ IoT (Internet of Things) ที่มีการตั้งค่าด้วยรหัสพื้นฐานจะเกิดขึ้นอย่างต่อเนื่องเนื่องจากมีลักษณะการเชื่อมต่อกับระบบอินเตอร์เน็ต และจะลามไปถึงการโจมตีโครงสร้างพื้นฐานต่อไปถ้าไม่มีระบบการป้องกันที่ทันสมัยกว่า สุดท้าย

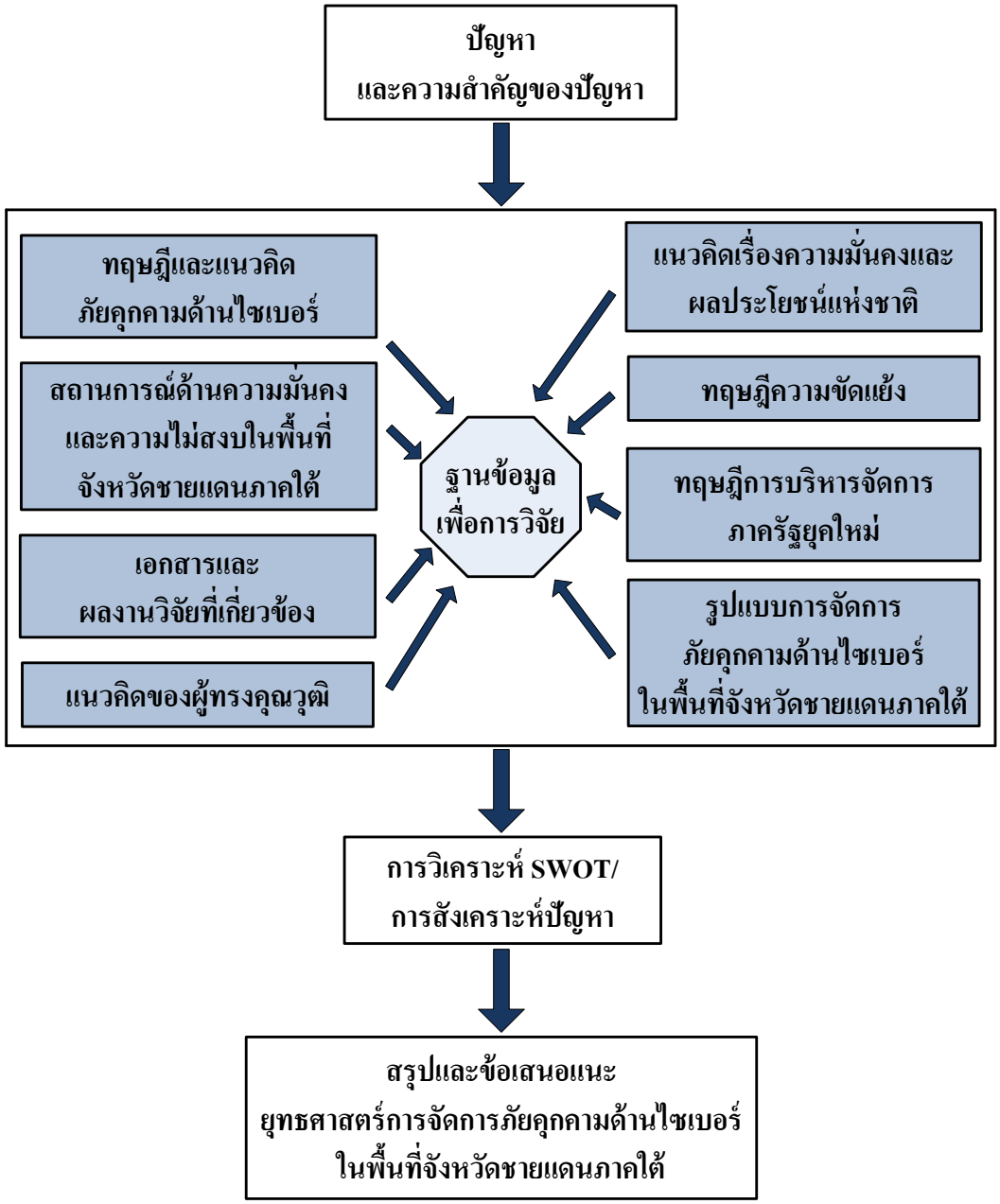
๑๐. เรื่องของ Cyber Resilience และการบังคับใช้กฎหมายการปกป้องข้อมูลทั่วไป (General Data Protection Regulation : GDPR) จะกลายเป็นพื้นฐานของการป้องกันภัยคุกคามด้านไซเบอร์ได้ในอนาคต เนื่องจากจะเป็นระบบที่ยังทรงสมรรถนะในการป้องกันภัยคุกคามด้านไซเบอร์ได้เป็นอย่างดี

จากแนวคิดของผู้ทรงคุณวุฒิด้านระบบไอซีทีและนักกฎหมายด้านไซเบอร์ที่กล่าวมาทั้งหมดทำให้ทราบถึงคุณลักษณะของโลกไซเบอร์ที่ชัดเจนมากขึ้น อีกทั้งยังเป็นประเด็นที่สนับสนุนว่าในการบริหารจัดการย่อมต้องใช้รูปแบบและมาตรการที่เหมาะสมที่สุดจึงจะสามารถรับมือกับภัยคุกคามประเภทนี้ได้อย่างมีประสิทธิภาพ

กรอบความคิดของการวิจัย

จากข้อมูลที่กล่าวมาข้างต้นสามารถยืนยันได้ว่าควรมีการศึกษาวิจัยเกี่ยวกับยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ ทั้งนี้เพื่อนำข้อมูลการวิจัยไปใช้เป็นข้อมูลสำคัญกับการรับมือกับภัยคุกคามด้านไซเบอร์เพื่อเสริมสร้างความมั่นคงและระงับปัญหาความไม่สงบอย่างเป็นรูปธรรม รวมถึงเพื่อสร้างความมั่นคงให้กับกองทัพไทยและหน่วยงานทางด้านความมั่นคงอื่นๆ ดังนั้นเพื่อให้สามารถนำเสนอประเด็นยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้อย่างมีประสิทธิภาพและมีประสิทธิผล ผู้วิจัยจึงได้กำหนดกรอบความคิดของการวิจัย (Conceptual Framework) ดังแผนภาพที่ ๒ - ๖

แผนภาพที่ ๒ - ๖ กรอบความคิดของการวิจัย



สรุป

การวิจัยเพื่อหายุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ โดยมีเอกสารและงานวิจัยที่เกี่ยวข้อง ได้แก่ รูปแบบภัยคุกคามด้านไซเบอร์ที่ปรากฏทั่วโลกในอดีตจนถึงปัจจุบัน สถานการณ์และรูปแบบภัยคุกคามด้านไซเบอร์ในประเทศไทย รูปแบบภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงและความไม่สงบในพื้นที่จังหวัดชายแดนภาคใต้ของประเทศไทย งานวิจัยและวรรณกรรมที่เกี่ยวข้องเพื่อนำไปสร้างกรอบความคิดของการวิจัย

บทนี้นำเสนอข้อมูลเบื้องต้นรวมถึงบทวิเคราะห์จากการศึกษาและค้นคว้าเอกสารเกี่ยวกับ แนวคิดเรื่องสงครามไซเบอร์ แนวคิดเรื่องความมั่นคงแห่งชาติ แนวคิดเรื่องผลประโยชน์แห่งชาติ ทฤษฎีความขัดแย้ง ทฤษฎีการบริหารจัดการภาครัฐยุคใหม่ ระบบไอซีทีเพื่อการจัดการ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ.๒๕๖๐ สถานการณ์ด้านความมั่นคงและความไม่สงบในพื้นที่จังหวัดชายแดนภาคใต้ งานวิจัยและวรรณกรรมที่เกี่ยวข้องเอกสารทางวิชาการ เอกสารทางราชการของหน่วยงานที่เกี่ยวข้อง บทความวิชาการต่างๆ การสำรวจข้อมูลเชิงพื้นที่ แนวคิดของผู้ทรงคุณวุฒิ รวมทั้งเอกสารประกอบการบรรยายที่เกี่ยวข้องเพื่อรวบรวมข้อมูลที่มีความหลากหลายเพื่อนำมาประกอบการดำเนินการวิจัยเชิงคุณภาพเพื่อหายุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ต่อไป บทต่อไปจะนำเสนอเกี่ยวกับรูปแบบภัยคุกคามด้านไซเบอร์ที่ปรากฏทั่วโลกในอดีตจนถึงปัจจุบัน สถานการณ์และรูปแบบภัยคุกคามด้านไซเบอร์ในประเทศไทย รูปแบบภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงและความไม่สงบในพื้นที่จังหวัดชายแดนภาคใต้ของประเทศไทย โดยจะนำเสนอตามลำดับต่อไป

บทที่ ๓
รูปแบบภัยคุกคามด้านไซเบอร์

การศึกษาในบทที่ ๓ จะเป็นการศึกษาเพื่อตอบวัตถุประสงค์ข้อที่ ๑ และ ๒ โดยศึกษาข้อมูลที่เกี่ยวข้องเพื่อนำไปสู่การสร้างยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ บทนี้นำเสนอผลการวิเคราะห์และสังเคราะห์ในประเด็นที่เกี่ยวข้องกับรูปแบบภัยคุกคามด้านไซเบอร์ตามลำดับดังต่อไปนี้

๑. รูปแบบภัยคุกคามด้านไซเบอร์ที่ปรากฏทั่วโลกในอดีตจนถึงปัจจุบัน

๒. รูปแบบภัยคุกคามด้านไซเบอร์ที่ปรากฏในประเทศไทย

๓. รูปแบบภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงและความไม่สงบในพื้นที่จังหวัดชายแดนภาคใต้

๔. สรุป

รูปแบบภัยคุกคามด้านไซเบอร์ที่ปรากฏทั่วโลกในอดีตจนถึงปัจจุบัน

ในปัจจุบัน กว่า ๖๐ ประเทศในโลกมีหรือกำลังพัฒนาบุคลากรและเครื่องมือเพื่อใช้สำหรับการจารกรรมและการโจมตีต่อระบบคอมพิวเตอร์แล้ว ในขณะที่มี ๒๙ ประเทศที่มีหน่วยงานที่จัดตั้งขึ้นอย่างเป็นทางการ ทั้งที่เป็นหน่วยงานทางทหารและหน่วยงานข่าวกรอง เพื่อใช้สำหรับการทำสงครามไซเบอร์เชิงรุก ในขณะเดียวกันก็มี ๔๙ ประเทศ ที่สามารถซื้อขายโปรแกรมเจาะระบบคอมพิวเตอร์ได้ตามท้องตลาดทั่วไป และมีอีก ๖๓ ประเทศที่ใช้เครื่องมือทางไซเบอร์เพื่อใช้เฝ้าติดตามความเคลื่อนไหวออนไลน์ ทั้งที่เกิดขึ้นภายในและภายนอกประเทศ (P.W. Singer and Allan Friedman, 2014) ด้วยเหตุนี้ หลายประเทศในโลกจึงเป็นที่รับรู้กันดีหรือตกเป็นผู้ต้องสงสัยอยู่เสมอว่าเป็นผู้พัฒนาเครื่องมือด้านไซเบอร์เพื่อการใช้งานเชิงรุก ไม่ว่าจะเป็นการเฝ้าติดตาม การสร้างความเสียหาย หรือการบ่อนทำลาย โดยอาจใช้หน่วยงานทางทหารหรือหน่วยงานข่าวกรองเพื่อมุ่งใช้งานด้านการทำสงครามไซเบอร์แต่เพียงอย่างเดียวหรืออาจจัดตั้งหรือใช้หน่วยงานเอกชนทั้งที่มีส่วนเกี่ยวข้องหรือมิได้มีส่วนเกี่ยวข้องกับหน่วยงานของรัฐเลยก็ได้ (National Institute of Standards and Technology, 2014) ตัวอย่างของประเทศที่มีขีดความสามารถและมีบทบาททางด้านการทำสงครามไซเบอร์ของโลกในปัจจุบันสรุปโดยย่อมีดังนี้

๑. สหรัฐอเมริกา

ชาวอเมริกันมีการใช้อินเตอร์เน็ตมากกว่า ๗๐% ของประชากรทั้งหมด โลกไซเบอร์มีบทบาทสำคัญต่อการควบคุมโครงสร้างพื้นฐานที่สำคัญ รวมถึงกระบวนการต่างๆ ในการผลิต สิ่งอำนวยความสะดวก กิจการธนาคาร การติดต่อสื่อสาร และระบบต่างๆ ทางทหารอีกด้วย ด้วยเหตุนี้ สหรัฐอเมริกาจึงตระหนักรู้ถึงความล่อแหลมของระบบเหล่านี้เป็นอย่างดี โดยสหรัฐอเมริกาถือว่า การบริการในโลกไซเบอร์ มีความสำคัญยิ่งต่อผลประโยชน์แห่งชาติของสหรัฐอเมริกา นอกจากนี้แล้ว จากคำจำกัดความของวิทยาลัยการทัพบกสหรัฐอเมริกาที่ว่า “ภัยคุกคามด้านไซเบอร์ถือเป็นภัยคุกคามที่อาจส่งผลกระทบต่อ ๓ ใน ๔ ผลประโยชน์แห่งชาติหลักของสหรัฐอเมริกา ได้แก่ ความมั่นคงภายใน (Security of the Homeland) สภาพความเป็นอยู่ทางเศรษฐกิจของประชาชน (Economic Well-Being) และความเป็นระเบียบโลกที่ยั่งยืน (A Stable International Order)”

สหรัฐอเมริกาได้เริ่มเข้าสู่การทำสงครามไซเบอร์อย่างจริงจังในปี ค.ศ.๒๐๑๐ เมื่อหน่วยบัญชาการไซเบอร์ของสหรัฐอเมริกา (U.S. Cyber Command) ได้รวมขีดความสามารถด้านไซเบอร์ของกองทัพบก กองทัพเรือ กองทัพอากาศ และนาวิกโยธินเข้าไว้ด้วยกันและอยู่ภายใต้หน่วยงานเดียวกัน โดยสหรัฐอเมริกาได้ทุ่มเงินลงไปหลายพันล้านดอลลาร์เพื่อใช้สำหรับโครงการนี้ ในขณะเดียวกัน เพนตากอนก็ได้ขยายขีดความสามารถด้านไซเบอร์อย่างขนานใหญ่ เห็นได้จากในปี ค.ศ.๒๐๑๔ มีการเพิ่มเจ้าหน้าที่ด้านไซเบอร์ถึง ๑,๘๐๐ นาย และในปี ค.ศ.๒๐๑๖ ได้เพิ่มขึ้นอีกเป็น ๖,๐๐๐ นาย นอกจากนี้แล้ว การทำสงครามไซเบอร์ยังเป็นส่วนหนึ่งของยุทธศาสตร์ทหารแห่งชาติของสหรัฐอเมริกาที่เรียกว่า “การป้องกันเชิงรุกด้านไซเบอร์” (Proactive Cyber Defence) และการใช้สงครามไซเบอร์เป็นส่วนหนึ่งของการโจมตีทางทหาร ดังนั้น ในปี ค.ศ.๒๐๑๓ สงครามไซเบอร์จึงได้รับการพิจารณาโดยเจ้าหน้าที่ข่าวกรองของสหรัฐอเมริกาเป็นครั้งแรกว่าเป็นภัยคุกคามที่ร้ายแรงกว่าอัลเคด้าหรือการก่อการร้าย และเพนตากอนเริ่มยอมรับอย่างเป็นทางการว่าโลกไซเบอร์ คือ ขอบเขตของการทำสงครามรูปแบบใหม่ และกลายเป็นการปฏิบัติการที่สำคัญยิ่งเช่นเดียวกับการปฏิบัติการทางทหารทางบก ในทะเล บนอากาศ และในอวกาศ อีกทั้ง ในปี ค.ศ.๒๐๐๙ ประธานาธิบดีบารัค โอบามา ก็ได้ประกาศแล้วว่า โครงสร้างพื้นฐานด้านดิจิทัลของสหรัฐอเมริกาได้กลายเป็นเครื่องมือของชาติในระดับยุทธศาสตร์ไปเรียบร้อยแล้ว และในปี ค.ศ.๒๐๑๐ เพนตากอนก็ได้จัดตั้งหน่วยงานใหม่ที่เรียกว่า “หน่วยบัญชาการไซเบอร์ของสหรัฐอเมริกา” (U.S. Cyber Command : USCYBERCOM) เพื่อใช้ป้องกันเครือข่ายทางทหารของสหรัฐอเมริกาและใช้โจมตีระบบเครือข่ายของชาติอื่น ทำให้เห็นได้ว่าสหรัฐอเมริกาได้ตระหนักดีถึงความเสี่ยงจากภัยคุกคามด้านไซเบอร์ต่อทั้งระบบคอมพิวเตอร์และสังคมเครือข่ายทั้งที่เป็นของภาครัฐและภาคเอกชน กิจการธนาคารและการเงิน การขนส่ง กระบวนการผลิตสินค้า การแพทย์ และการศึกษา

เป็นต้น ซึ่งทั้งหมดนี้ต่างขึ้นอยู่กับระบบคอมพิวเตอร์และสังคมเครือข่ายที่ใช้อยู่เป็นประจำในปัจจุบันแทบทั้งสิ้น ต่อเนื่องมาถึงรัฐบาลของประธานาธิบดีโดนัล ทรัมส์ ก็ยังคงเพิ่มมาตรการเชิงรุกในการจัดการกับปัญหาที่เกิดขึ้นโดยการเพิ่มขีดความสามารถในการทำสงครามไซเบอร์อย่างไม่รู้จบ

ในแง่ของการป้องกัน สหรัฐอเมริกาได้กำหนดให้การรักษาความมั่นคงปลอดภัยด้านไซเบอร์เป็นหนึ่งในลำดับเร่งด่วนด้านความมั่นคงแห่งชาติ โดยสำนักงานสอบสวนกลาง (Federal Bureau of Investigation : FBI) ได้กำหนดให้ภัยคุกคามด้านไซเบอร์ว่ามีศักยภาพที่จะเป็นภัยคุกคามต่อความมั่นคงของสหรัฐอเมริกาในระนาบเดียวกันหรืออาจจะมากกว่าภัยคุกคามจากการก่อการร้ายในอนาคตอันใกล้ ในปัจจุบันกระทรวงความมั่นคงแห่งมาตุภูมิ (The Department of Homeland Security) เป็นผู้รับผิดชอบหลักเกี่ยวกับการดำเนินงานเชิงรับกับระบบเครือข่ายของรัฐบาล โดยอาจมีการประสานความร่วมมือเพื่อปกป้องและป้องกันโครงสร้างพื้นฐานที่สำคัญของชาติ รวมถึงโครงสร้างพื้นฐานด้านไซเบอร์ โดยทำงานร่วมกับหน่วยงานเฉพาะภายใต้สายการบริหารงานของศูนย์รักษาความมั่นคงปลอดภัยด้านไซเบอร์แห่งชาติ (National Cyber Security Center) ยิ่งไปกว่านั้น สหรัฐอเมริกายังได้สถาปนาความร่วมมือกับหุ้นส่วนภาคเอกชนในเรื่องการรักษาความมั่นคงปลอดภัยด้านไซเบอร์เป็นจำนวนมาก อีกทั้งกระทรวงกลาโหมและกระทรวงความมั่นคงแห่งมาตุภูมิ ต่างมีความสัมพันธ์กับหุ้นส่วนภาคเอกชนในลักษณะเดียวกัน โดยเฉพาะในงานเกี่ยวกับการสืบสวนสอบสวนและการข่าวกรอง ในปี ค.ศ.๒๐๐๘ รัฐบาลประธานาธิบดีจอร์จ บุช ได้ออกคำสั่งให้หน่วยเฉพาะกิจร่วมด้านการสืบสวนสอบสวนด้านไซเบอร์แห่งชาติ (National Cyber Investigative Joint Task Force) เป็นศูนย์รวมของการประสานงาน การบูรณาการ และการแบ่งปันสารสนเทศที่เกี่ยวข้องกับการสืบสวนสอบสวนภัยคุกคามด้านไซเบอร์ภายในประเทศให้กับหน่วยงานภาครัฐทั้งหมด โดยสำนักงานสอบสวนกลาง เป็นผู้รับผิดชอบในการจัดตั้งและสนับสนุนหน่วยเฉพาะกิจนี้ ซึ่งอาจมีหน่วยงานข่าวกรองและหน่วยงานบังคับใช้กฎหมายของสหรัฐอเมริการวมกันมากกว่า ๒๐ หน่วยงาน (Frank J. Cilluffo, 2013)

สิ่งที่เห็นได้อย่างชัดเจนก็คือ ทิศทางทางยุทธศาสตร์ทั่วไป (Overall Strategic Direction) เกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ของสหรัฐอเมริกา ได้แสดงรายละเอียดในบททบทวนนโยบายเกี่ยวกับโลกไซเบอร์ของฝ่ายบริหารในปี ค.ศ.๒๐๑๒ (The administration’s 2012 Cyberspace Policy Review) โดยได้กำหนดตารางการปฏิบัติของระบบการป้องกันด้านไซเบอร์เอาไว้แล้ว อย่างไรก็ตาม ตราบจนถึงปัจจุบัน วุฒิสภาก็ยังไม่ได้ให้ความเห็นชอบเกี่ยวกับการดำเนินการดังกล่าว แม้ว่าฝ่ายบริหารได้จัดตั้งคณะกรรมการนโยบายเพื่อบูรณาการโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการติดต่อสื่อสาร (Information and Communications Infrastructure Interagency Policy Committee) แล้วก็ตาม โดยคณะกรรมการ

ดังกล่าว มีผู้แทนทั้งจากสภาความมั่นคงแห่งชาติ (National Security Council) และสภาความมั่นคงแห่งมาตุภูมิเข้าร่วมด้วย ทั้งนี้ก็เพื่อใช้เป็นองค์กรประสานนโยบายหลักที่เกี่ยวกับการดำเนินงานเพื่อให้ได้มาซึ่งความเชื่อมั่น ความไว้วางใจ ความปลอดภัย และความอยู่รอดสารสนเทศและโครงสร้างพื้นฐานด้านการติดต่อสื่อสารของโลก และการพัฒนาขีดความสามารถต่างๆ ที่เกี่ยวข้อง บททบทวนนโยบายโลกไซเบอร์นี้ยังอาจเป็นการกำหนดนโยบายอย่างเป็นทางการด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ของฝ่ายบริหารอีกด้วย หากมีการรายงานบททบทวนนี้ไปยังสภาความมั่นคงแห่งชาติเพื่อประสานนโยบายและกิจกรรมต่างๆ ที่เกี่ยวข้องกับการรักษาความความมั่นคงปลอดภัยด้านไซเบอร์ของสหรัฐอเมริกา

ในขณะเดียวกัน ในปี ค.ศ.๒๐๑๔ สถาบันมาตรฐานและเทคโนโลยีแห่งสหรัฐอเมริกา (National Institute of Standards and Technology : NIST) ซึ่งเป็นหน่วยงานอิสระที่อยู่ภายใต้กระทรวงพาณิชย์ของสหรัฐอเมริกา ที่มีภารกิจในการส่งเสริมนวัตกรรมและความสามารถในการแข่งขันทางอุตสาหกรรมของสหรัฐอเมริกา โดยการสร้างมาตรการเพื่อความก้าวหน้าทางวิทยาศาสตร์ มาตรฐาน และเทคโนโลยี ในวิถีทางที่จะเพิ่มพูนความมั่นคงทางเศรษฐกิจของชาติและพัฒนาคุณภาพชีวิตของประชาชนของสหรัฐอเมริกา ได้ออกกรอบการดำเนินงานล่าสุดเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ (Cybersecurity) โดยเนื้อหาหลักประกอบด้วยองค์ประกอบหลัก ๓ องค์ประกอบ คือ (๑) โครงสร้างหลักของกรอบการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ (Framework Core) (๒) ระดับของการดำเนินงานให้ประสบผลสำเร็จตามโครงสร้างหลักของกรอบการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ (Framework implementation Tiers) และ (๓) โครงร่างของโครงสร้างหลักของกรอบการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์" (Framework Profiles) เพื่อกำหนดแนวปฏิบัติที่ดีให้นำไปใช้ใน การจัดการระบบของหน่วยงานในอุตสาหกรรมที่เกี่ยวกับโครงสร้างพื้นฐานสำคัญ ครอบคลุม ๑๖ กลุ่มโครงสร้างพื้นฐานสำคัญ ได้แก่ ๑) กลุ่มอุตสาหกรรมเคมี (Chemical Sector) ๒) กลุ่มโรงงานเพื่อการพาณิชย์ (Commercial Facilities Sector) ๓) กลุ่มการติดต่อสื่อสาร (Communications Sector) ๔) กลุ่มอุตสาหกรรมการผลิตที่สำคัญ (Critical Manufacturing Sector) ๕) กลุ่มเขื่อนกั้นน้ำ (Dams Sector) ๖) กลุ่มฐานอุตสาหกรรมกลาโหม (Defense Industrial Base Sector) ๗) กลุ่มบริการฉุกเฉิน (Emergency Services Sector) ๘) กลุ่มพลังงาน (Energy Sector) ๙) กลุ่มบริการทางการเงิน (Financial Services Sector) ๑๐) กลุ่มอาหารและเกษตรกรรม (Food and Agriculture Sector) ๑๑) กลุ่มหน่วยงานราชการของรัฐบาล (Government Facilities Sector) ๑๒) กลุ่มบริการทางการแพทย์และสาธารณสุข (Healthcare and Public Health Sector) ๑๓) กลุ่มเทคโนโลยีสารสนเทศ (Information Technology Sector) ๑๔) กลุ่มเครื่องปฏิกรณ์นิวเคลียร์ วัสดุ

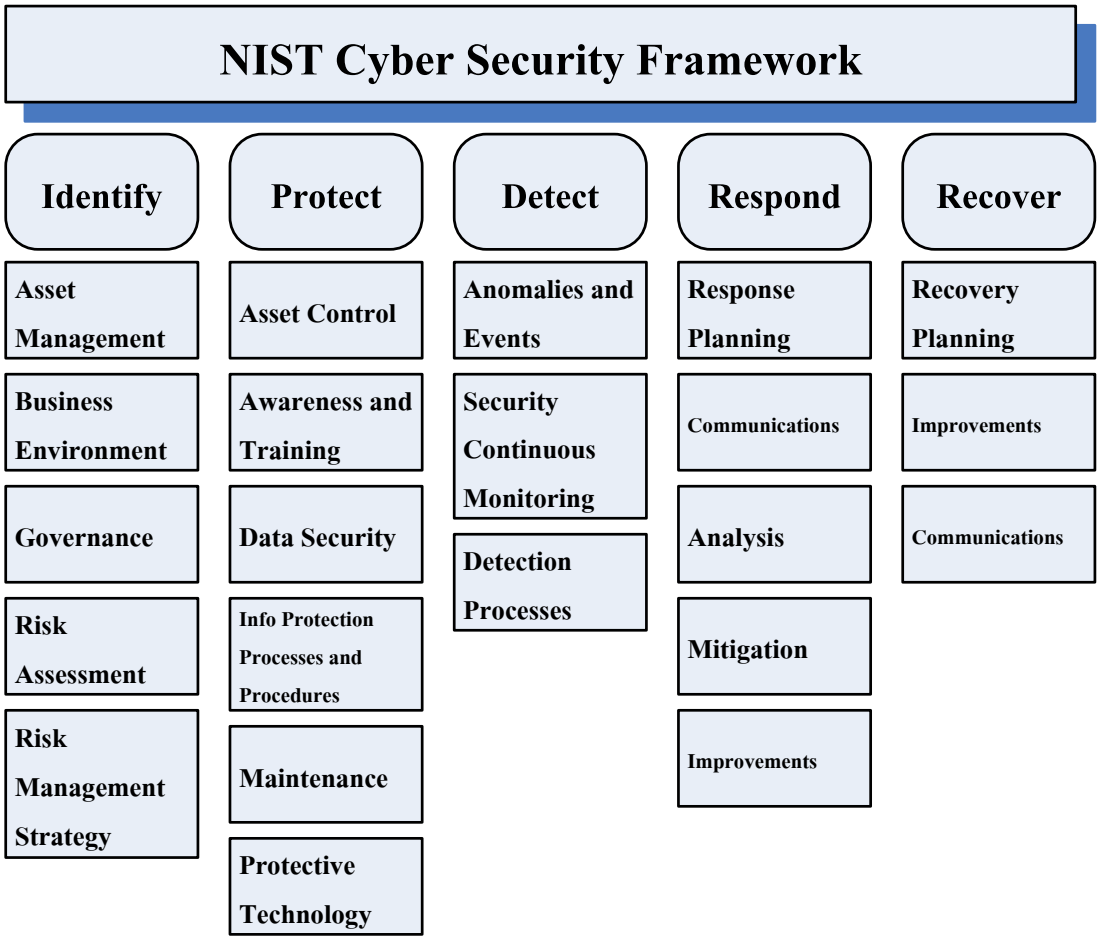
นิวเคลียร์ และกากเชื้อเพลิงนิวเคลียร์ (Nuclear Reactors, Materials, and Waste Sector) ๑๕) กลุ่มระบบขนส่ง (Transportation Systems Sector) และ ๑๖) กลุ่มระบบน้ำและน้ำเสีย (Water and Wastewater Systems Sector)

โครงสร้างหลักของกรอบการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ (Framework Core) ตามแนวคิดของสถาบันมาตรฐานและเทคโนโลยีแห่งสหรัฐอเมริกา ประกอบด้วย (๑) พันธกิจ (Functions) ซึ่งเป็นการจัดกิจกรรมพื้นฐานด้านความมั่นคงปลอดภัยด้านไซเบอร์ในระดับใหญ่สุด โดยแบ่งออกเป็น ๕ พันธกิจ ได้แก่ ๑) พิสูจน์ทราบ (Identify) ๒) ป้องกัน (Protect) ๓) ตรวจจับ (Detect) ๔) ตอบสนอง (Respond) และ ๕) คืนสภาพ (Recover) การจัดเป็นพันธกิจเช่นนี้จะช่วยให้องค์การสามารถกำหนดมาตรการการจัดการความเสี่ยงเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ โดยอาศัยการจัดระเบียบสารสนเทศ การตกลงใจเกี่ยวกับการจัดการความเสี่ยง การกำหนดภัยคุกคาม และปรับปรุง การดำเนินงานขององค์การ โดยอาศัยการเรียนรู้จากกิจกรรมที่ได้ดำเนินการในอดีตที่ผ่านมา (๒) กลุ่มงาน (Categories) ซึ่งเป็นการแบ่งพันธกิจออกเป็นกลุ่มงานตามผลลัพธ์ด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ และจะเชื่อมโยงกับความต้องการตามโครงการและกิจกรรมต่างๆ ที่กำหนดไว้แล้ว เช่น กลุ่มบริหารจัดการทรัพย์สิน กลุ่มควบคุมการเข้าถึง และกลุ่มกระบวนการตรวจจับ เป็นต้น (๓) กลุ่มงานย่อย (Subcategories) ซึ่งเป็นการแบ่งกลุ่มงานออกเป็นกลุ่มงานย่อยโดยจำแนกตามผลลัพธ์เฉพาะในเชิงเทคนิค และ/หรือตามกิจกรรมการบริหารจัดการขององค์การ ทั้งนี้ก็เพื่อช่วยให้บรรลุผลลัพธ์ในแต่ละกลุ่มย่อยได้มากยิ่งขึ้น เช่น ระบบสารสนเทศภายนอกได้ถูกบันทึกลงในบัญชีข้อมูลพร้อมใช้งานได้รับการปกป้อง และการแจ้งเตือนจากระบบตรวจจับได้รับการตรวจสอบ เป็นต้น และ (๔) ข้อมูลอ้างอิง (Informative References) ซึ่งเป็นส่วนของการกำหนดมาตรฐาน แนวทาง และแนวปฏิบัติ ที่ใช้ในกลุ่มโครงสร้างพื้นฐานสำคัญแต่ละกลุ่ม โดยจะแสดงวิธีการที่จะบรรลุผลลัพธ์ที่เกี่ยวข้องกับกลุ่มงานย่อยแต่ละกลุ่ม กรอบการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์และมาตรการต่างๆ แสดงดังแผนภาพที่ ๓ - ๑ และตารางที่ ๓ - ๑ ตามลำดับ

ระดับของการดำเนินงานให้ประสบผลสำเร็จตามโครงสร้างหลักกรอบการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ (The Framework Implementation Tiers) เป็นการกำหนดบริบทเกี่ยวกับวิธีการต่างๆ เพื่อให้องค์การสามารถมองความเสี่ยงและกระบวนการเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านไซเบอร์เพื่อนำไปสู่การจัดการกับความเสี่ยงเหล่านั้น ระดับของการดำเนินงานให้ประสบผลสำเร็จ จะเริ่มจากระดับที่มีความเข้มงวดน้อยสุด (Tier I) ไปจนถึงระดับที่มีความเข้มงวดสูงสุด (Tier IV) และรายละเอียดในแนวปฏิบัติของการจัดการความเสี่ยงข้อพิจารณาเกี่ยวกับการจัดการความเสี่ยงนี้จะประกอบไปด้วยมุมมองที่หลากหลายของการรักษา

ความมั่นคงปลอดภัยด้านไซเบอร์ รวมถึงข้อพิจารณาเกี่ยวระดับความลับและความมีอิสระในการจัดการความเสี่ยงรวมถึงการตอบสนองต่อความเสี่ยงที่เป็นไปได้ต่อการรักษาความมั่นคงปลอดภัยด้านไซเบอร์

แผนภาพที่ ๓ - ๑ โครงสร้างหลักของกรอบการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ตามแนวคิดของสถาบันมาตรฐานและเทคโนโลยีแห่งสหรัฐอเมริกา



ที่มา: The Department of Defense, United States of America, Cyber Strategy, 2016.

โครงร่างของโครงสร้างหลักของกรอบการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ (Framework Profiles) เป็นการจัดเรียงพันธกิจ (Functions) กลุ่มงาน (Categories) และกลุ่มงานย่อย (Subcategories) ให้ตรงกับความต้องการของภาคธุรกิจต่างๆ ระดับความเสี่ยงที่ยอมรับได้ และทรัพยากรขององค์กร ด้วยเหตุนี้ โครงร่างของโครงสร้างหลักนี้จะช่วยให้องค์กรจัดทำแผนกลยุทธ์ (Roadmap) เพื่อลดระดับความเสี่ยงต่อการรักษาความมั่นคงปลอดภัย

ด้านไซเบอร์ให้เป็นตามเป้าประสงค์ขององค์กร ระเบียบ/ข้อกำหนดตามกฎหมาย วิธีการปฏิบัติที่เป็นเลิศทางอุตสาหกรรม และลำดับความเร่งด่วนในการจัดการความเสี่ยง ในกรณีที่องค์กรมีขนาดใหญ่และมีการจัดที่ซับซ้อน ผู้นำองค์กรอาจเลือกใช้โครงร่างที่หลากหลาย สอดคล้องกับองค์ประกอบเฉพาะ และตอบสนองต่อความต้องการของบุคลากรขององค์กรก็ได้ ดังนั้นการประสานการดำเนินงานตามโครงสร้างหลักให้ประสบผลสำเร็จ จึงจำเป็นต้องอาศัยความร่วมมือร่วมใจกันระหว่างบุคลากรในองค์กร ๓ ระดับ ได้แก่ ๑) ระดับผู้บริหาร (Executive Level), ๒) ระดับกระบวนการ (Business/Process Level) และ ๓) ระดับปฏิบัติการ(Implementation/Operations Level)

ตารางที่ ๓ - ๑ ระดับของการดำเนินงานให้ประสบผลสำเร็จตามโครงสร้างหลักของกรอบการดำเนินงาน

	Risk Management Process	**Integrated Risk Management Program**	**External Participation**
Partial	•Not formalized •Reactive	•Limited Awareness •Irregular risk management •Private information	No external collaboration
Risk Informed	•Approved Practices •Not widely use as poligy	•More awareness •Risk-informed, processes & Procedures •Adequate resources •Internal sharing	Not formalized to interact & share information
Repeatable	•Approved as Policy •Update rewularly	•Organization approach •Risk-informed, processes & procesures defined & implemented as intended, and reviewed •Knowledge & skills	•Collaborate •Receive information
Adaptive	Continuous improvement	•Rish-informed, processes & procesures for potential events •Continuous awareness •Actively	Actively shares information

ที่มา: The Department of Defense, United States of America, Cyber Strategy, 2016.

๒. จีน

ในช่วงปี ค.ศ.๑๙๙๕-๒๐๐๘ รัฐบาลจีนได้ถูกกล่าวหาว่ามีส่วนเกี่ยวข้องกับการจารกรรมข้อมูลที่เป็นความลับผ่านทางเครือข่ายอิสระของนักศึกษา นักธุรกิจ นักวิทยาศาสตร์ นักการทูต และวิศวกรชาวจีนโพ้นทะเลเป็นจำนวนมาก อีกทั้งจีนยังจัดส่งสายลับหลายร้อยนายแทรกซึมเข้าไปอยู่ในวงการอุตสาหกรรมต่างๆ ทั่วทั้งทวีปยุโรป ในปี ค.ศ.๒๐๐๗ ผู้บริหารระดับสูงคนหนึ่งของรัสเซียได้ถูกศาลตัดสินลงโทษจำคุกเป็นเวลา ๑๑ ปี เนื่องจากได้ขายความลับเกี่ยวกับหน่วยงานด้านเทคโนโลยีและอวกาศให้กับจีน อย่างไรก็ตาม เป้าหมายส่วนใหญ่ของจีนมักอยู่ที่สหรัฐอเมริกา โดยเฉพาะสารสนเทศที่เกี่ยวกับโครงการวิศวกรรมอวกาศ การออกแบบกระสวยอวกาศ ข้อมูลเกี่ยวกับระบบ C4ISR ระบบคอมพิวเตอร์สมรรถนะสูง การออกแบบอาวุธนิวเคลียร์ ข้อมูลเกี่ยวกับจรวดร่อน สารกึ่งตัวนำ การออกแบบแผงวงจรรวม และรายละเอียดเกี่ยวกับการขายอาวุธของสหรัฐอเมริกาให้กับไต้หวัน ในขณะเดียวกัน จีนได้ถูกตั้งข้อสงสัยว่าเป็นผู้อยู่เบื้องหลังในการโจมตีด้านไซเบอร์ต่อสถาบันทั้งภาครัฐและภาคเอกชนจำนวนมากทั้งในสหรัฐอเมริกา อินเดีย รัสเซีย แคนาดา และฝรั่งเศส แม้ว่ารัฐบาลจีนจะปฏิเสธว่าไม่ได้มีส่วนร่วมต่อการล้วงความลับด้านไซเบอร์เหล่านั้นเลยก็ตาม และยังกล่าวอ้างด้วยว่าจีนไม่ใช่เป็นภัยคุกคาม แต่จีนได้ตกเป็นเหยื่อหรือเป้าหมายของการโจมตีด้านไซเบอร์เป็นจำนวนมาก (Li Zhang, 2012)

เมื่อเร็วๆ นี้ แหล่งข่าวตะวันตก (CNN และ BBC) ได้เปิดโปงว่าประเทศจีนได้จัดตั้งศูนย์บัญชาการไซเบอร์ขึ้นอย่างลับๆ กลางสลัมในเซี่ยงไฮ้ ถึงแม้ว่าจะมีหลักฐานอย่างชัดเจนโดยนักข่าว CNN ได้พยายามบุกเข้าไปในศูนย์บัญชาการนี้จนกระทั่งถูกทหารที่อยู่หน้าศูนย์บัญชาการดังกล่าวจับกุมตัว แต่จีนก็ปฏิเสธอย่างแข็งขันว่าไม่เคยมีหน่วยงานนี้จริง นอกจากนี้แล้ว จีนค่อนข้างมีนโยบายด้านการป้องกันภัยคุกคามด้านไซเบอร์ค่อนข้างดี โดยจีนมีการจัดแบ่งพื้นที่รับผิดชอบเป็นมณฑลในแต่ละภูมิภาค ในแต่ละมณฑลจะมีเจ้าหน้าที่ที่รับผิดชอบด้านไซเบอร์ประมาณ ๓๐,๐๐๐ คน เมื่อรวมกับประชาชนที่เป็นอาสาสมัคร ทำให้จีนมีบุคลากรถึงประมาณ ๑ ล้านคนที่สามารถทำงานด้านไซเบอร์ ในขณะเดียวกัน จีนก็พยายามที่จะแสวงหาความร่วมมือด้านการทำสงครามไซเบอร์กับชาติอื่นที่เป็นพันธมิตรใกล้ชิดอีกด้วย เห็นได้จากจีนได้พยายามขอความร่วมมือกับประเทศไทย โดยการประสานงานและขอนำเครื่องมือบางอย่างเข้ามาใช้ในประเทศไทยเพื่อเฝ้าติดตามสารสนเทศที่จีนสนใจ แต่จีนมีนโยบายอย่างหนึ่ง ก็คือ จะไม่ส่งวิศวกรเข้ามาประจำอยู่ในประเทศไทยและข้อมูลจะต้องส่งกลับสำนักงานใหญ่ที่ตั้งอยู่ในจีน และจีนจะพยายามตั้งสำนักงานย่อยในประเทศไทยให้น้อยที่สุด ในปัจจุบันเป็นที่เชื่อได้ว่าจีนด้พยายามขยายขีดความสามารถด้านไซเบอร์และเทคโนโลยีทางทหารของตนโดยอาศัยเทคโนโลยีทางทหารของต่างชาติ โดยเฉพาะระบบการเฝ้าตรวจและระบบการรวบรวมข่าวกรองจากฐานที่อยู่ในอวกาศแบบ

ใหม่ อาวุธต่อต้านดาวเทียม ระบบต่อต้านเรดาร์ ระบบการลวงด้วยอินฟราเรด และเครื่องสร้างเป้าหมายลวง เป็นต้น เพื่อบรรลุซึ่งวัตถุประสงค์นี้ รัฐบาลจีนจึงสนับสนุนให้มีกระบวนการพัฒนาระบบสารสนเทศ (Informationization) ในทางการทหาร โดยการเพิ่มพูนความรู้ด้านการทำสงครามไซเบอร์ให้กับทหารของตน การปรับปรุงเครือข่ายสารสนเทศเพื่อใช้สำหรับการฝึกทางทหาร การสร้างห้องปฏิบัติการเสมือนจริง ห้องสมุดดิจิตอล และวิทยาลัยเขตดิจิตอลมากยิ่งขึ้น ทั้งนี้ก็เพื่อจัดเตรียมกองทัพปลดปล่อยประชาชนจีนให้สามารถเผชิญหน้ากับรูปแบบภัยคุกคามที่หลากหลายของการทำสงครามและศัตรูที่มีขีดความสามารถทางเทคโนโลยีที่เหนือกว่าในสงครามยุคใหม่ที่จีนเรียกว่า “สงครามเย็นด้านไซเบอร์” (Cyber Cold War)

๓. รัสเซีย

รัสเซียเป็นอีกประเทศหนึ่งที่ถูกกล่าวหาบ่อยครั้งว่าเป็นผู้ใช้สงครามไซเบอร์ในการโจมตีชาติอื่น โดยเฉพาะการโจมตีแบบ DoS การโจมตีโดยอาศัยนักเจาะระบบคอมพิวเตอร์ (Hacker Attacks) การแพร่กระจายข่าวสารลวงผ่านระบบอินเตอร์เน็ต สนับสนุนกลุ่มผู้แสดงความเห็นผ่านเว็บไซต์ทางการเมือง การค้นหาและเฝ้าติดตามทางอินเตอร์เน็ตด้วยการใช้เทคโนโลยีที่เรียกว่า “SORM” และการก่อกวนกลุ่มผู้ที่ไม่เห็นด้วยกับรัฐบาลด้านไซเบอร์ สาเหตุที่นำมาซึ่งข้อสงสัยเหล่านี้เกิดจากกิจกรรมบางอย่างเหล่านี้ต่างสอดคล้องกับการดำเนินงานของหน่วยงานข่าวกรองสัญญาณของรัสเซียซึ่งเป็นหน่วยงานหนึ่งของหน่วยงานด้านความมั่นคงของรัสเซีย (Federal Security Service: FSB) ซึ่งในอดีตเคยเป็นส่วนหนึ่งของแผนกที่ ๑๖ ของหน่วยเคจีบี (KGB) ในขณะที่หน่วยงานอื่นๆ อยู่ภายใต้การควบคุมของกระทรวงมหาดไทยและกิจการทางทหารของรัสเซีย ในกรณีของเหตุการณ์การโจมตีด้านไซเบอร์ต่อจอร์เจียนั้น สถาบันวิจัยอิสระที่ตั้งอยู่ในสหรัฐอเมริกาเชื่อว่า การโจมตีดังกล่าวแทบไม่มีส่วนเกี่ยวข้องกับหน่วยงานทางทหารหรือหน่วยงานภาครัฐของรัสเซียเลย เนื่องจากการโจมตีดังกล่าวเกิดจากผู้ใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลที่หลากหลายที่อยู่ในรัสเซีย ยูเครน และลัตเวีย โดยกลุ่มบุคคลเหล่านี้ต่างเต็มใจและสนับสนุนรัฐบาลรัสเซียอยู่แล้ว อีกทั้งยังเคยให้การสนับสนุนรัสเซียในช่วงสงครามออสเซเตียใต้ (South Ossetia War) ในปี ค.ศ.๒๐๐๘ มาแล้วด้วย นอกจากนี้ การโจมตีบางครั้งก็มีการใช้ Botnets หรือกองทัพซอมบี้ (Zombie Army) อีกด้วย อย่างไรก็ตาม การโจมตีโดยอาศัย นักเจาะระบบคอมพิวเตอร์ต่างถูกควบคุมโดยหน่วยงานลับหลายหน่วยงาน โดยเฉพาะในช่วงวิกฤตกาลจับตัวประกันในโรงหนังกลางกรุงมอสโคว์ ในปี ค.ศ.๒๐๐๒ ในเดือนมีนาคม ค.ศ.๒๐๑๔ แหล่งข่าวหลายแหล่งต่างรายงานว่า รัสเซียได้ใช้อาวุธไซเบอร์ที่เรียกว่า “Snake” หรือ “Ouroboros” เพื่อสร้างความเสียหายต่อระบบเครือข่ายของรัฐบาลยูเครนในเดือนตุลาคม ค.ศ.๒๐๑๔ นักเจาะระบบคอมพิวเตอร์ของรัสเซียได้แสวงประโยชน์จากข้อบกพร่อง (Bug) ในโปรแกรม Microsoft

Windows และโปรแกรมอื่นๆ เพื่อล้วงความลับของเครื่องคอมพิวเตอร์ต่างๆ ที่ใช้งานอยู่ในองค์การนาโต้ (NATO) สหภาพยุโรป (European Union) ยูเครน และบริษัทต่างๆ ที่อยู่ในสายพลังงานและโทรคมนาคม ทำให้เชื่อได้ว่าเหตุการณ์ไฟฟ้าดับในยูเครน น่าจะเกิดจากการโจมตีด้านไซเบอร์ของรัสเซีย โดยเฉพาะจากกลุ่มนักเจาะระบบคอมพิวเตอร์ที่ชื่อว่า “Sandworm” หรือจากกลุ่มที่มีรัฐบาลรัสเซียอยู่เบื้องหลัง โดยใช้การโจมตีด้วยการฝังโปรแกรมที่ไม่พึงประสงค์ (Malware) เข้าทำลายเครือข่ายระบบไฟฟ้าของยูเครนในเดือนธันวาคม ค.ศ.๒๐๑๕

จากข้อมูลที่ปรากฏเกี่ยวกับภัยคุกคามด้านไซเบอร์เป็นที่ประจักษ์ชัดแล้วว่าทุกประเทศทั่วโลกต่างก็ให้ความสำคัญและถือว่าเป็นภัยคุกคามแห่งชาติที่สำคัญยิ่ง โดยอาจมองได้อีกว่าเป็นภัยคุกคามที่สามารถควบคุม ป้องกัน และระงับยับยั้งได้โดยต้องมียุทธศาตร์ที่ชัดเจนทั้งในระดับชาติและระดับโลก

รูปแบบภัยคุกคามด้านไซเบอร์ที่ปรากฏในประเทศไทย

สำหรับประเทศไทย สงครามไซเบอร์ไม่ใช่เรื่องที่ไกลตัวอีกต่อไป เหตุการณ์ที่เห็นได้ชัดที่สุดก็คือ “ปรากฏการณ์ F5” ที่ต่อต้านนโยบาย Single Gateway ของประเทศไทยจากกลุ่มต่อต้านที่เรียกตัวเองว่า “Anonymous” ที่เริ่มขึ้นมาตั้งแต่ต้นปี พ.ศ.๒๕๕๘ เนื่องจากพวกเขาเข้าใจว่า รัฐบาลไทยมีความพยายามที่จะเชื่อมต่อโลกอินเตอร์เน็ตระหว่างประเทศไทยกับต่างประเทศผ่านช่องทางเดียวแล้วมี Firewall มาครอบไว้เหมือนกับจีนหรือสิงคโปร์ เพื่อควบคุมเนื้อหาที่เป็นประเด็นอ่อนไหวของรัฐบาล แม้ว่าในแง่ดี Single Gateway ทำให้การดูแลการเข้าถึงอินเตอร์เน็ต การตรวจสอบข้อมูล และการดักจับข้อมูล เป็นต้น สามารถทำได้ง่ายกว่าปกติมาก และจุดประสงค์หลักที่รัฐบาลต้องการใช้ระบบนี้ก็เนื่องมาจากรัฐบาลต้องการควบคุมการใช้งานและเข้าถึงสารสนเทศที่ไม่เหมาะสมจากโลกภายนอกนั่นเอง แต่กลุ่มที่คัดค้านนโยบายนี้กลับมองในแง่ร้ายที่ไม่อยากอยู่ภายใต้การตรวจสอบของรัฐบาล องค์การหรือบุคคลอื่นใด โดยพวกเขามักยกตัวอย่างภาพของการใช้งานสื่อสังคมออนไลน์ในประเทศจีน ที่รัฐบาลจีนได้ใช้ระบบนี้ในการตรวจสอบสกัดกั้น และติดตามการใช้งานด้านอินเตอร์เน็ตของประชาชน จนทำให้ประชาชนไม่สามารถใช้งานเว็บไซต์หลายๆ เว็บไซต์ได้ ไม่ว่าจะเป็น Facebook, Youtube หรือเว็บไซต์ที่กำลังได้รับความนิยมในประเทศอื่นๆ อีกทั้งการใช้ระบบนี้ทำให้การเชื่อมต่ออินเตอร์เน็ตมากระจุกตัวอยู่ในช่องทางเดียว ทำให้มีโอกาสที่อินเตอร์เน็ตจะช้า ล่ม หรือใช้การไม่ได้มากยิ่งขึ้น ด้วยเหตุนี้ ภายหลังมีกระแสข่าวลือว่ารัฐบาลไทยมีนโยบายจะนำ Single Gateway มาใช้ในประเทศไทย บรรดาชาวเน็ตหรืออาจเรียกว่า “นักรบไซเบอร์” จำนวนหนึ่งก็ได้ร่วมกันประท้วง โดยเริ่มจากเว็บไซต์ Change.org ได้ออกแคมเปญรณรงค์ต่อต้านการใช้ Single Gateway และมีการล่ารายชื่อเสนอต่อรัฐบาล จากนั้นได้มีการ

รวมตัวกันเข้าไปป่วนการใช้งานเว็บไซต์ของหน่วยงานรัฐด้วยวิธีการ “DDoS” หรือการกด F5 รัวๆ ในหน้าเว็บไซต์ เพื่อทำให้เว็บไซต์เหล่านั้น “ล่ม” เช่น เว็บไซต์ของกระทรวงไอซีที บริษัท กสท. โทรคมนาคม จำกัด (มหาชน) กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร (กอ.รมน.) ทำเนียบรัฐบาล และบริษัท ทีโอที จำกัด(มหาชน) เป็นต้น ทั้งนี้ก็เพื่อเป็นการแสดงออกเชิงสัญลักษณ์ถึงการต่อต้านนโยบายดังกล่าว (พล.ต.ฤทธี อินทราวุธ, ๒๕๖๐)

คำว่า “Single Gateway” หมายถึง ประตูหรือช่องทางเดียวที่เชื่อมต่อระหว่างเครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่ง และเป็นตัวเชื่อมต่อโครงข่ายของแต่ละประเทศเข้าไว้ด้วยกัน โดยทั่วไปแล้ว ทั่วโลกนิยมที่จะมีผู้ให้บริการเครือข่าย (Gateway) หลายๆ ช่องทาง เพื่อให้การเชื่อมต่อกับเครือข่ายต่างๆ เป็นไปอย่างสะดวกและรวดเร็ว ฉะนั้นการใช้ “Single Gateway” จึงอาจเปรียบได้ว่าเป็นการเชื่อมต่อระบบอินเตอร์เน็ตด้วยประตูหรือช่องทางเดียว ซึ่งเท่ากับว่ามีผู้ให้บริการเครือข่ายเพียงเจ้าเดียว ทำให้สามารถควบคุมและดักจับข้อมูลเมื่อมีผู้ใช้อินเตอร์เน็ตผ่านประตูบานนี้ไปยังเว็บไซต์ต่างๆ ได้อย่างง่ายดาย ปัจจุบันนี้มีประเทศที่ใช้ “Single Gateway” คือ ลาว จีน เกาหลีเหนือ และประเทศในแถบตะวันออกกลาง ซึ่งต่างล้วนเห็นว่า การใช้อินเตอร์เน็ตผ่านสื่อสังคมออนไลน์หากปล่อยให้มีการดำเนินการโดยเสรีย่อมจะส่งผลกระทบต่อความมั่นคงแห่งชาติทั้งด้านการเมือง เศรษฐกิจ และสังคมจิตวิทยาของประเทศ ด้วยเหตุนี้ รัฐบาลของประเทศเหล่านี้โดยเฉพาะรัฐบาลจีนจึงต้องการควบคุมไม่ให้ประชาชนในประเทศเล่นสื่อสังคมออนไลน์อย่าง Facebook และ Twitter รวมถึงห้ามใช้ Line และ Google ด้วย ด้วยเหตุนี้ ทันทีที่มีข่าวว่าคณะรักษาความสงบแห่งชาติมีนโยบายเตรียมผลักดันการจัดตั้ง Single Gateway โดยมอบหมายให้กระทรวงไอซีทีเป็นผู้รับผิดชอบในการตรวจสอบข้อมูลที่ไม่เหมาะสม หรือบล็อกข้อมูลที่ก่อให้เกิดความวุ่นวาย รวมทั้งเพื่อป้องกันการโจมตีด้านไซเบอร์ด้วยการก่อการร้าย โดยมีการสั่งงานของรัฐบาลเป็นระยะตั้งแต่กลางปี พ.ศ.๒๕๕๘ โดยมีการมอบหมายให้กระทรวงไอซีทีร่วมกับหน่วยงานที่เกี่ยวข้อง เช่น กระทรวงยุติธรรมและสำนักงานตำรวจแห่งชาติดำเนินการจัดตั้ง Single Gateway เพื่อใช้เป็นเครื่องมือควบคุมเว็บไซต์ที่ไม่เหมาะสมและการไหลเข้าของข้อมูลข่าวสารจากต่างประเทศผ่านทางระบบอินเตอร์เน็ต รวมถึงมีมติคณะรัฐมนตรีเมื่อวันที่ ๓๐ มิถุนายน ๒๕๕๘ ให้กระทรวงไอซีทีและหน่วยงานที่เกี่ยวข้องเร่งรัดการจัดตั้ง Single Gateway โดยด่วน และให้ทุกส่วนราชการสร้างการรับรู้เกี่ยวกับการดำเนินการทุกอย่างของรัฐบาลให้แก่ประชาชนตั้งแต่เริ่มแรก การดำเนินการดังกล่าวของรัฐบาลได้ก่อให้เกิดกระแสคัดค้านนโยบายดังกล่าวอย่างรุนแรงในสื่อสังคมออนไลน์ทั้งในประเทศและต่างประเทศ เนื่องจากพวกเขาต่างมองว่ารัฐบาลต้องการเป็นผู้ควบคุมการเข้าถึงอินเตอร์เน็ตของคนในประเทศ ทำให้ผู้ใช้อินเตอร์เน็ตทั่วไปถูกจำกัดการใช้เครือข่ายกับต่างประเทศและต้องระวังการเข้าถึงเนื้อหาที่ไม่เหมาะสมโดยไม่รู้ตัว อีกทั้งรัฐบาลอาจปิดกั้นการเข้าถึงข้อมูลที่

ประชาชนค้นหาได้อย่างรวดเร็วเต็มประสิทธิภาพด้วยป้องกันการเข้าถึงเว็บไซต์ที่รัฐบาลไม่ต้องการ อินเตอร์เน็ตอาจช้าลงเนื่องจากมี Gateway เดียว และหาก Gateway นี้ล่มก็จะล่มกันหมดทั้งประเทศ เพราะจะไม่มี Gateway ตัวอื่นรองรับ รวมถึงมีค่าใช้จ่ายสูง เนื่องจากต้องสร้าง Gateway ที่มีขนาดใหญ่รองรับปริมาณการใช้งานทั้งประเทศ และต้องใหญ่พอที่จะรองรับปริมาณที่เพิ่มมากขึ้นในอนาคต ในขณะเดียวกัน บริษัทข้ามชาติอาจลังเลที่จะเข้ามาลงทุนในประเทศไทย เนื่องจากอาจไม่มั่นใจด้านความมั่นคงและรู้สึกไม่ปลอดภัยในการให้บริการอินเตอร์เน็ต กังวลถึงข้อมูลทางการค้าที่ถูกล้วงความลับได้ง่าย และประเทศไทยขาดโอกาสการเป็นศูนย์กลาง (Hub) ทางเศรษฐกิจดิจิทัลของอาเซียน

อย่างไรก็ตาม รัฐบาลได้พยายามออกมาปฏิเสธว่ายังไม่เคยคิดที่จะนำ “Single Gateway” มาใช้ การดำเนินการที่ผ่านมาของรัฐบาล เป็นเพียงขั้นตอนการศึกษาความเป็นไปได้เท่านั้น แต่ทว่ากลุ่มคัดค้านที่รวมตัวกันเรียกว่า “กลุ่มพลเมืองต่อต้าน Single Gateway” ได้ออกประกาศผ่าน Facebook เพื่อทำสงครามไซเบอร์ครั้งใหม่กับรัฐบาลไทย เนื่องจากพวกเขายังคงเชื่อว่า รัฐบาลมีแนวคิดที่นำนโยบาย Single Gateway ไปไว้ในกฎหมายดิจิตอล และ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับปรับปรุงใหม่) ดังนั้นกลุ่มพลเมืองต่อต้าน Single Gateway จึงเรียกร้องให้รัฐบาลยกเลิกโครงการนี้ ด้วยการออกมติคณะรัฐมนตรีมายกเลิกมติคณะรัฐมนตรีเดิม เมื่อรัฐบาลยังมีท่าทีแบ่งรับแบ่งสู้ อีกทั้งยังมีการจัดตั้ง “กองสงครามไซเบอร์” ขึ้นมาอีกด้วย ทำให้พวกเขามองว่ารัฐบาลพยายามถ่วงเวลาและดำเนินการอย่างไม่ลดละเพื่อตอบโต้พวกเขา พวกเขาจึงได้จัดตั้ง “เครือข่ายประชาชนไทยผู้ใช้อินเตอร์เน็ต” และประกาศสงครามไซเบอร์กับรัฐบาลไทยนับตั้งแต่นั้น โดยทางเครือข่ายได้ประกาศว่า พวกเขาจะมีกิจกรรมการใช้ F5 ขึ้นทุกสัปดาห์ในเวลาราชการ โดยเน้นเป้าหมายไปที่หน่วยงานราชการของรัฐ แต่ก็จะหลีกเลี่ยงการสร้างความเสียหายให้แก่ภาคเอกชนและประชาชน โดยเริ่มดำเนินการครั้งแรกเมื่อวันที่ ๒๒ ตุลาคม พ.ศ.๒๕๕๘ เวลา ๑๐.๐๐ น. เป็นต้นไป และจะจัดให้มีกิจกรรมเช่นนี้จนกว่าพวกเขาจะเห็นว่าเสรีภาพได้กลับคืนสู่ประชาชนไทยแล้วอย่างเป็นรูปธรรม

ผลจากความไม่พร้อมและกระแสข่าวลือในโลกไซเบอร์ได้สร้างความกังวลให้กับประชาชนจำนวนไม่น้อย โดยเห็นได้จากการเกิดกระแสปฏิเสธนโยบายของรัฐบาลที่จะให้บริการ “พร้อมเพย์” (PromptPay) แก่ประชาชน ซึ่งเป็นการให้บริการรับ-โอนเงินระหว่างกันแบบใหม่โดยไม่ต้องใช้เลขที่บัญชีธนาคาร โดยใช้เพียงแค่หมายเลขโทรศัพท์มือถือหรือเลขประจำตัวประชาชนผ่านช่องทางต่างๆ เช่น Internet Banking, Mobile Banking และ ATM เป็นต้น ทำให้การโอนเงินผ่านบริการพร้อมเพย์มีความสะดวกสบายและปลอดภัย ทั้งนี้รัฐบาลหมายมั่นปั้นมือที่จะเปิดลงทะเบียนอย่างเป็นทางการตั้งแต่วันที่ ๑๕ กรกฎาคม พ.ศ.๒๕๕๙ นี้ แต่สิ่งที่ประชนกังวลก็เกิดมา

จากกระแสข่าวลือที่ว่า เมื่อมีการนำหมายเลขโทรศัพท์และเลขบัตรประชาชนมาผูกกับบัญชีธนาคารแล้วจะทำให้ถูกเจาะข้อมูลได้ง่าย ไม่ปลอดภัย มิหนำซ้ำยังอาจมีปัญหาด้านกฎหมาย เนื่องจากการนำเลขบัตรประชาชนไปซึ่งมีข้อมูลส่วนตัวไปผูกกับเลขบัญชีธนาคารตามระบบพร้อมเพย์เป็นความเสี่ยงต่อความปลอดภัยในเรื่องของข้อมูลส่วนบุคคล แม้ว่าธนาคารแห่งประเทศไทยได้ออกมาชี้แจงในเรื่องดังกล่าวแล้วว่า ระบบพร้อมเพย์เป็นระบบที่เปิดให้ประชาชนผู้ใช้บริการสมัครใจเข้ามาลงทะเบียนโดยไม่ได้บังคับ อีกทั้งตาม พ.ร.บ.ธุรกิจธนาคาร มาตรา ๑๕๔ ได้ห้ามธนาคารนำข้อมูลความลับของลูกค้าไปเปิดเผย หากเกิดความเสียหายขึ้นธนาคารจะต้องเป็นผู้รับผิดชอบ แต่ตามรายงานยอดผู้ที่สมัครเข้าลงทะเบียนพร้อมเพย์ตั้งแต่วันที่ ๑ กรกฎาคม พ.ศ. ๒๕๕๙ มีจำนวนทั้งสิ้นเพียง ๙.๗ ล้านราย โดยแบ่งเป็นการลงทะเบียนผูกบัญชีกับเบอร์โทรศัพท์ ๑.๖ ล้านราย และผูกบัญชีกับเลขบัตรประชาชน ๘.๑ ล้านราย ส่วนในปี พ.ศ.๒๕๖๐ ก็มีแนวโน้มการลงทะเบียนเพิ่มมากขึ้นกว่า ๑๐ ล้านราย

นอกจากนี้ จากรายงานการใช้งานสื่อสังคมออนไลน์ เมื่อปลายปี พ.ศ.๒๕๖๐ ยังพบว่าประเทศไทยมีการใช้งานแอพพลิเคชั่นนี้มากกว่า ๔๗ ล้านคน หรือมีบัญชี Facebook User มากกว่า ๔๗ ล้านผู้ใช้ หรือคิดเป็น ๒ เปอร์เซ็นต์ของประชากรโลก ส่วนแอพพลิเคชั่น Instagram มีผู้ใช้มากกว่า ๑๑ ล้านคน และแอพพลิเคชั่น Twitter มีผู้ใช้มากกว่า ๙ ล้านคน ตามลำดับ โดยมีอัตราการเติบโตเพิ่มขึ้น ๒๐ เปอร์เซ็นต์ในแต่ละปี อีกทั้งยังมีแอพพลิเคชั่นอื่นๆ ที่รวมความสามารถทางด้านการสื่อสารออนไลน์ได้อย่างรวดเร็วและสามารถใช้งานเป็นกลุ่มเฉพาะกิจ เช่น YouTube, WhatsApp, Facebook Messenger, WeChat, Skype, LinkedIn, Snapchat, Viber, Line และอื่นๆ จากรายงานนี้สรุปได้ว่า กระแสความตื่นตัวทางระบบไอซีที ความจำเป็นในการติดต่อสื่อสารทางธุรกิจและความนิยมในการใช้ไซเบอร์อย่างมากมายส่งผลให้เกิดการเปลี่ยนแปลงทางสังคม เศรษฐกิจและการเมืองอย่างรวดเร็ว ถึงแม้ว่าไซเบอร์จะทำให้เกิดประโยชน์อย่างมหาศาลแต่หากมนุษย์ใช้โลกไซเบอร์ในทางที่ไม่ถูกต้องนำไปเป็นเครื่องมือเพื่อวัตถุประสงค์บางประเภท เช่น การนำไปปลุกระดมมวลชน การชักจูงหรือเผยแพร่ข่าวสาร การจารกรรมข้อมูล การปล่อยไวรัส และจะนำไปสู่ก่อการร้ายได้อันส่งผลให้เกิดความเสียหายอย่างมากแก่มนุษย์ อีกทั้งการใช้ไซเบอร์เพื่อเป็นเครื่องมือที่สำคัญต่อการก่อการร้ายและสร้างความเสียหายและสูญเสียเป็นจำนวนมากในอดีตที่ผ่านมา

ปี พ.ศ.๒๕๖๑ ภาครัฐบาลโดย ดร.พิเชฐ ดุรงคเวโรจน์ รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ดีอี) ได้มีการหารือกับรัฐมนตรีว่าการกระทรวงการค้าต่างประเทศแห่งสหราชอาณาจักรและอุปทูตจากสถานเอกอัครราชทูตสหราชอาณาจักรประจำประเทศไทย และผู้แทนจากฝ่าย สหราชอาณาจักรที่เกี่ยวข้อง โดยทั้งสองฝ่ายเห็นควรผลักดันให้เกิดความร่วมมือในด้านการพัฒนาทรัพยากรมนุษย์ด้านดิจิทัลและความปลอดภัยด้านไซเบอร์เป็นโครงการเริ่มต้น

สำหรับด้านวิชาการจะมีการส่งเสริมให้มหาวิทยาลัยของสหราชอาณาจักรที่มีศักยภาพในสาขาที่เป็นที่ต้องการของไทยเข้ามาสร้างความร่วมมือในโครงการพัฒนาระเบียงเศรษฐกิจพิเศษภาคตะวันออก (EEC) เพื่อสนับสนุนการวิจัยและพัฒนานวัตกรรมของเอกชน รวมทั้งสร้างบุคลากรที่มีทักษะสอดคล้องกับความต้องการของภาคเอกชน ในส่วนของความปลอดภัยด้านไซเบอร์ จะมีการผลักดันให้หน่วยงานภาครัฐและเอกชนของสหราชอาณาจักร เข้ามามีส่วนร่วมในศูนย์ ASEAN-Japan Capacity Building Center ซึ่งประเทศไทยได้รับการคัดเลือกจากอาเซียนให้จัดตั้งศูนย์ดังกล่าวเพื่อพัฒนาบุคลากรด้านความปลอดภัยไซเบอร์ของอาเซียน ทั้งนี้จะมีการจัดทำบันทึกความเข้าใจว่าด้วยความร่วมมือด้านดิจิทัลระหว่างไทยและสหราชอาณาจักร เพื่อเป็นกรอบความร่วมมือที่เป็นรูปธรรมระหว่างสองประเทศในอนาคตต่อไป

สถานการณ์ไซเบอร์ภายในประเทศไทยนับว่ายังไม่มีความรุนแรงมากนักเนื่องจากการโจมตีในลักษณะที่เป็นการทำสงครามไซเบอร์ระดับประเทศนั้นยังไม่ปรากฏเหตุการณ์ที่ชัดเจน มีเพียงแต่เหตุการณ์ที่เว็บไซต์ของหน่วยงานต่างๆ ถูกโจมตีด้วยการเปลี่ยนหน้าเว็บไซต์จากบุคคลเฉพาะกลุ่ม เช่น กลุ่มพลเมืองต่อต้าน Single Gateway กลุ่มพลเมือง ต่อต้าน พ.ร.บ.คอมพิวเตอร์โดยผู้กระทำผิดหรือแฮกเกอร์ กลุ่มดังกล่าวต้องการต่อต้านอำนาจของรัฐ หรือทำให้รัฐ เกิดความวุ่นวายและเสียหาย นอกจากนี้ยังมีการโจมตีอีกรูปแบบหนึ่งที่เกิดขึ้น คือ การปฏิบัติการข่าวสาร (Information Operations : IO) กล่าวคือ เป็นการเปลี่ยนแปลงข่าวสารการรับรู้ต่างๆ ของประชาชน เช่น การแฮกเข้าไปบนเว็บไซต์เพื่อทิ้งข้อความบางอย่างไว้ การที่หน่วยงานภาครัฐทำ IO ผลงานนายกรัฐมนตรีเป็น infografic เผยแพร่ออกไป แต่กลุ่มดังกล่าวก็ทำการเปลี่ยนแปลงด้วยการตัดต่อเป็นรูปตลกขบขัน ซึ่งถือเป็นสงคราม IO ที่เกิดขึ้นเพื่อต้องการดึงประชาชนรวมถึงสื่อต่างประเทศที่เลือกฝั่งชัดเจนและไม่เลือกฝั่งชัดเจนเข้ามาในสนามนี้ด้วย จากสถิติการแจ้งเหตุภัยคุกคามด้านไซเบอร์ที่เกิดขึ้นในประเทศไทยประจำปี พ.ศ.๒๕๕๙ โดยจำแนก ประเภทภัยคุกคามออกเป็น ๙ ประเภท ตามที่กำหนด โดย The European Computer Security Incident Response Team: eCSIRT พบการแจ้งเหตุภัยคุกคาม ทั้งสิ้น ๓,๗๙๗ เรื่อง โดยสามารถจัดลำดับตามจำนวนเหตุภัยคุกคามที่ได้รับแจ้งออกเป็นประเภทใหญ่ๆ ได้โดยภัยคุกคามส่วนใหญ่ประมาณร้อยละ ๒๖.๙ (จำนวน ๑,๐๒๐ เรื่อง) เป็นภัยคุกคามที่เกิดจากโปรแกรมหรือซอฟต์แวร์ที่ถูกพัฒนาขึ้นเพื่อส่งให้เกิดผลลัพธ์ที่ไม่พึงประสงค์กับผู้ใช้งานหรือระบบ (Malicious Code) และประมาณร้อยละ ๒๖.๙ (จำนวน ๑,๐๒๐ เรื่อง) เป็นภัยคุกคามที่เกิดกับระบบที่ถูกบุกรุก/เจาะเข้าระบบได้สำเร็จและระบบถูกครอบครองโดยผู้ที่ไม่ได้รับอนุญาต (Intrusions) ในส่วนภัยคุกคามที่รองลงมาประมาณร้อยละ ๒๖.๔ (จำนวน ๑,๐๐๒ เรื่อง) เป็นภัยคุกคามภัยที่เกิดจากการฉ้อฉลฉ้อโกงหรือการหลอกลวงเพื่อ

ผลประโยชน์ (Fraud) และลำดับสุดท้ายประมาณร้อยละ ๑๘.๖ (จำนวน ๗๐๖ เรื่อง) เป็นภัยคุกคามที่เกิดจากความพยายามจะบุกรุก/เจาะเข้าระบบ (Intrusion Attempts) ข้อมูลแสดงดังตารางที่ ๓ - ๒

จะเห็นได้ว่าสถานการณ์ความรุนแรงของสงครามไซเบอร์ในปัจจุบันมีความเปลี่ยนแปลงไปจากเดิมที่เน้นโจมตีระบบไอซีทีเป็นหลัก เช่น สมาร์ทโฟนและเครื่องคอมพิวเตอร์ไม่ว่าจะเป็นส่วนบุคคลหรือเครือข่ายคอมพิวเตอร์ในองค์กร โดยเป็นการเข้าถึงโดยไม่ได้รับอนุญาต การรบกวนการทำงานของคอมพิวเตอร์ การใช้คอมพิวเตอร์เพื่อการหลอกลวงและทำลายข้อมูล รวมถึงการสอดแนมข้อมูลทางการเมืองและการทหาร และการโจมตีที่ส่งผลกระทบร้ายแรงต่อนานาประเทศคงหนีไม่พ้นการโจมตีเทคโนโลยีปฏิบัติการ (Operational Technology) อันครอบคลุมถึงเทคโนโลยีที่ดูแลระบบพลังงานไฟฟ้า เขื่อน ตลอดจนพลังงานนิวเคลียร์ซึ่งหากกระทำการได้สำเร็จก็จะสร้างความเสียหายที่ร้ายแรงกว่าในอดีต ซึ่งกลุ่มแฮกเกอร์ที่มีประสิทธิภาพกระทำการในลักษณะนี้ได้มักเป็นกลุ่มแฮกเกอร์ที่ได้รับการสนับสนุนจากประเทศมหาอำนาจหรือประเทศใดประเทศหนึ่ง จากความรุนแรงของภัยคุกคามด้านไซเบอร์ประเทศในประชาคมโลกต่างก็แสวงหาแนวทางและวิธีการรับมือที่แตกต่างกันไป สำหรับประเทศไทยในเวทีความร่วมมืออาเซียน นายกรัฐมนตรีได้เข้าร่วมประชุมสุดยอดอาเซียน ครั้งที่ ๒๗ ณ กรุงกัวลาลัมเปอร์ ประเทศมาเลเซีย ซึ่งการประชุมดังกล่าวนายกรัฐมนตรีไทยมีข้อเสนอให้มีการจัดตั้งศูนย์ไซเบอร์อาเซียนขึ้นเพื่อรับมือกับผลกระทบทางลบจากความเชื่อมโยงและความท้าทายจากความมั่นคงรูปแบบใหม่ โดยเฉพาะอาชญากรรมไซเบอร์ (กระทรวงการต่างประเทศ, ๒๕๕๘: ๑-๔) ในระดับประเทศ ซึ่งขณะนี้สำนักงานสภาความมั่นคงแห่งชาติกำลังดำเนินการจัดทำนโยบายรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเพื่อใช้เป็นกรอบกำหนดทิศทางการรักษาความปลอดภัยของประเทศ อันจะนำไปสู่การออก พรบ. และกฎหมายอื่นๆ ที่เกี่ยวข้องตามมา นอกจากนั้นรองนายกรัฐมนตรีฝ่ายความมั่นคง และรัฐมนตรีว่าการกระทรวงกลาโหมมีนโยบายต่อภัยคุกคามด้านไซเบอร์ โดยให้เสริมสร้างขีดความสามารถการปฏิบัติการด้านไซเบอร์กระทรวงกลาโหมทั้งในด้านโครงสร้าง การจัดหน่วยระดับนโยบาย และระดับปฏิบัติการสรรหาและการพัฒนาความรู้ให้กับบุคลากรที่จะบรรจุในอัตราของหน่วยที่เกี่ยวข้องกับการปฏิบัติงานไซเบอร์ การพัฒนาหลักนิยมและหลักการสำหรับการปฏิบัติการด้านไซเบอร์ทั้งเชิงรุกและเชิงรับ รวมทั้งการสร้างความตระหนักรู้เกี่ยวกับภัยคุกคามด้านไซเบอร์ให้กับกำลังพลโดยทั่วไป เพื่อให้เห็นถึงความสำคัญและมีความตื่นตัวในการปฏิบัติตามมาตรการรักษาความปลอดภัยด้านไซเบอร์ (กระทรวงกลาโหม, ๒๕๖๐: ๑) เช่นเดียวกับกองบัญชาการกองทัพไทยโดยผู้บัญชาการทหารสูงสุดก็ได้มีนโยบายให้จัดตั้งและบูรณาการหน่วยงานรับผิดชอบหลักงานด้านไซเบอร์ให้มีขีดความสามารถทั้งเชิงรุกและเชิงรับ และการ

พัฒนาขีดความสามารถด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ทั้งด้านความมีเอกภาพ หลักนิยม กำลังพล และยุทโธปกรณ์ (กองทัพไทย, ๒๕๖๐: ๒๒)

ตารางที่ ๓ - ๒ ระดับของการดำเนินงานให้ประสบผลสำเร็จตามโครงสร้างหลักของกรอบการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์

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	○	○	○	○	○	○	○	○	○	○	○	○	○
Availability	○	○	○	○	○	○	○	○	○	○	○	๒๕	๒๕
Froud	๕๘	๕๕	๖๖	๗๓	๑๖๔	๑๒๕	๑๐๔	๕๒	๕๗	๕๕	๔๓	๗๐	๑,๐๐๒
Information gathering	○	○	○	○	○	○	○	○	○	○	○	○	○
Information security	○	○	○	○	○	○	○	○	○	○	๒	๑๘	๒๐
Intrusion attemts	๓๕	๓๕	๓๖	๖๒	๖๕	๗๐	๕๕	๘๒	๔๒	๓๕	๖๖	๑๑๑	๗๐๖
Intrusions	๑๗๕	๕๑	๑๒๒	๕๖	๕๓	๔๔	๑๕๘	๖๐	๕๕	๓๗	๔๐	๘๕	๑,๐๒๐
Malicious code	๕๗	๑๒๓	๘๐	๑๐๔	๑๖๘	๑๖๗	๔๕	๑๔	๗๘	๓๐	๘๕	๒๑	๑,๐๒๐
Other	○	○	○	○	○	○	○	○	○	○	○	○	○
รวม	๔๐๕	๓๐๘	๓๐๔	๓๓๕	๔๕๔	๔๐๖	๓๗๐	๒๐๘	๒๗๒	๑๕๗	๒๔๐	๓๓๘	๓,๗๕๗

ที่มา: ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT), ๒๕๕๕

ผลจากความเสียหายที่เกิดจากภัยคุกคามด้านไซเบอร์ที่ผ่านมา ทำให้ประเทศไทยโดยหน่วยงานความมั่นคงได้ตระหนักดีถึงผลกระทบทั้งในแง่ที่เป็นประโยชน์และโทษจากสงครามไซเบอร์ ทำให้ทุกฝ่ายต่างก็พยายามพัฒนาขีดความสามารถด้านไซเบอร์ทั้งในเชิงรุกและการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ เพื่อใช้เป็นมาตรการทั้งเชิงรุกและเชิงรับจากการโจมตีด้านไซเบอร์ของฝ่ายตรงข้าม (สราวุธ ปิติยาศักดิ์, ๒๕๖๐) ดังจะเห็นได้จากประเด็นสำคัญของยุทธศาสตร์และมาตรการด้านไซเบอร์ของประเทศไทยที่สำคัญ ดังนี้

๑. ศูนย์ไซเบอร์ กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม กระทรวงกลาโหม (ศซบ.ทสอ.กห.) เพื่อให้ เป็นหน่วยงานหลักประสานงานด้านไซเบอร์ในภาพรวมของกระทรวงกลาโหม เชื่อมโยงนโยบายด้านไซเบอร์กับระดับรัฐบาล และนำไปสู่การดำเนินการของหน่วยไซเบอร์ระดับปฏิบัติ รวมทั้งดำเนินการความร่วมมือด้านไซเบอร์กับหน่วยงานภาครัฐและภาคเอกชนที่เกี่ยวข้องทั้งในและต่างประเทศ

๒. กองปฏิบัติการสงครามเครือข่าย สำนักปฏิบัติ การกรมยุทธการทหาร (กสค.สปก.ยก.ทหาร) มีความรับผิดชอบหลักในการจัดการและบูรณาการการปฏิบัติทางไซเบอร์ในระดับกองทัพไทย เช่น จัดทำยุทธศาสตร์การปฏิบัติการไซเบอร์ของกองทัพไทย และมีหน้าที่รับผิดชอบในฐานะเป็นองค์ประกอบหนึ่งของศูนย์ประสานการรักษาความปลอดภัยระบบคอมพิวเตอร์กระทรวงกลาโหม (MODCERT)

๓. กองรักษาความปลอดภัยสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร มีพันธกิจใน การดำเนินการตรวจสอบวิเคราะห์ป้องกันกู้คืนและประเมิน ผลการดำเนินงานด้านการรักษาความมั่นคงปลอดภัย สารสนเทศ จัดทำแนวทาง หลักการ ระเบียบมาตรการ และแผนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของ บก.ทท. รวมทั้งพิจารณาเสนอแนะการดำเนินการต่อภัยคุกคามที่มีผลกระทบต่อระบบสารสนเทศของ บก.ทท.และมีหน้าที่รับผิดชอบในฐานะเป็นองค์ประกอบ หนึ่งของศูนย์ประสานการรักษาความปลอดภัยระบบคอมพิวเตอร์กระทรวงกลาโหม

๔. การจัดตั้งศูนย์ไซเบอร์ทหาร จากข้อมูลข้างต้นจะเห็นได้ว่าปัจจุบันกองบัญชาการกองทัพไทยมีหน่วยงานหลักที่รับผิดชอบด้านความมั่นคงปลอดภัยทางไซเบอร์อยู่ ๒ หน่วยงาน คือ กสค.สปก.ยก.ทหาร และ กรส.ศทศ. สส.ทหาร ซึ่งทั้ง ๒ หน่วยงานมีภารกิจทางด้านไซเบอร์ที่ต้องรับผิดชอบเหมือนกัน แต่มีสายการบังคับบัญชาที่แยกกันอยู่ เมื่อผู้บังคับบัญชาได้เล็งเห็นถึงความเชื่อมโยงระหว่าง ๒ หน่วยงานนี้จึงมีนโยบายให้มีการแปรสภาพ ๒ หน่วยงานดังกล่าวให้เป็น “ศูนย์ไซเบอร์ทหาร” และขึ้นตรงกับสำนักผู้บัญชาการทหารสูงสุด

จากข้อมูลที่กล่าวมาทั้งหมดสามารถสรุปได้ว่า รูปแบบภัยคุกคามด้านไซเบอร์ที่ปรากฏในประเทศไทยและกระบวนการแก้ไขปัญหาค่อนข้างไม่มีรูปแบบตายตัว ส่วนใหญ่จะพิจารณาเพื่อแก้ไขปัญหาเฉพาะหน้ามากกว่า อีกทั้งการปรับรูปแบบการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ยังอยู่ในระหว่างการค้นหาวิธีการที่เหมาะสมในการดำเนินการ ภาครัฐควรหันมาสนใจเรื่องนี้เป็นการเฉพาะอาจจะช่วยให้การแก้ไขปัญหารวดเร็วขึ้นได้

รูปแบบภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงและความไม่สงบในพื้นที่จังหวัดชายแดนภาคใต้ของประเทศไทย

ผลการศึกษาพบว่ารูปแบบภัยคุกคามด้านไซเบอร์ที่เกิดขึ้นในจังหวัดชายแดนภาคใต้ปรากฏผลดังประเด็นต่อไปนี้

๑. รูปแบบของภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

๑.๑ รูปแบบของภัยคุกคามด้านไซเบอร์ที่พบในพื้นที่จังหวัดชายแดนภาคใต้ในความคิดเห็นของหน่วยงานด้านความมั่นคงของรัฐ (กองทัพภาคที่ ๔, กอ.รมน.ภาค ๔ ส่วนหน้า, ศอบต., ศชต., และ ฉก.) ผู้บริหาร/ผู้นำท้องถิ่น ๔ จังหวัด สามารถสรุปได้ว่ามีรูปแบบที่ปรากฏดังนี้

๑.๑.๑ รูปแบบของการสร้างข้อมูล การสร้างข้อมูลเป็นรูปแบบปกติของการนำเสนอข้อมูลข่าวสารในยุคปัจจุบัน จะสังเกตุได้ว่ามีการนำระบบไซเบอร์และเครือข่ายสังคมออนไลน์มาใช้สร้างและเผยแพร่ข้อมูลข่าวสารมากขึ้นเรื่อยๆ โดยอาจจะมากกว่าการใช้กำลังเสียอีก ทั้งมีการแฮกหรือการเจาะข้อมูลของส่วนงานราชการและหน่วยงานทางความมั่นคง ซึ่งยังไม่มีการตรวจพบอย่างเด่นชัดจากเจ้าหน้าที่ผู้เชี่ยวชาญ แต่พบว่ามีการพบการโจมตีทางไซเบอร์ด้วยความพยายามในการเจาะและกระทำการบุกรุกฐานข้อมูลของ กอ.รมน. เช่น เมื่อทำการบุกรุกได้ก็จะมีการเปลี่ยนหน้าตาโฮมเพจและอ้างว่าสามารถที่จะเจาะข้อมูลของหน่วยงานราชการได้สำเร็จและแจ้งให้กับแนวร่วมว่าได้ทำตามเป้าหมายเรียบร้อยผ่านทางเครือข่ายออนไลน์วิธีใดวิธีหนึ่ง เป็นต้น จากการวิเคราะห์ของผู้รับผิดชอบด้านความมั่นคงพบว่าอาจเป็นการเชื่อมโยงกับการเมืองหรือการก่อกวนให้เกิดความหวาดระแวงระหว่างเจ้าหน้าที่รัฐและประชาชนนั่นเอง

๑.๑.๒ รูปแบบของการบิดเบือนข้อมูล ในพื้นที่สังคมเมืองมีการเข้าถึงอินเตอร์เน็ตได้ดี แต่ในส่วนพื้นที่นอกเมืองมีการใช้งานน้อยกว่า คนอายุ ๔๐ ขึ้นไป มักจะยังใช้งานอินเตอร์เน็ตเป็นสื่อในการติดต่อสื่อสารประจำวันรวมถึงการบริโภคข่าวสารบ้านเมืองต่างๆ แต่มีการใช้การบอกเล่าข่าวลือเพื่อให้คนที่เข้าถึงอินเตอร์เน็ตไม่ได้ได้รับข่าวบิดเบือนจากความเป็นจริงบ้าง โดยมีการตรวจพบโฆษณาชวนเชื่อและมีการโจมตีในประเด็นการเผยแพร่ข่าวสารโดยมีการนำสื่อสังคมออนไลน์ เช่น Facebook, Line, Twitter และ Blog อื่นๆ มาใช้ในการหาแนวร่วมซึ่งมีการขยายช่องทางการสื่อสารตลอดเวลา โดยเมื่อทางการตรวจสอบได้ก็จะมีการเปลี่ยนรูปแบบของสื่อออนไลน์ไปได้ใช้ช่องทางอื่นไม่มีที่สิ้นสุด มีการใช้จิตวิทยาโดยเน้นการสร้างความเข้าใจผิดๆ ให้ประชาชนเพื่อให้เข้าใจผิดหรือเกิดความรู้สึกขัดแย้งกับการทำงานของรัฐบาลตลอดจนหน่วยงานทางความมั่นคงอื่นๆ เช่น หากเจ้าหน้าที่จับผู้ต้องสงสัยในพฤติกรรมบางกลุ่มก็จะมีการเผยแพร่ข้อมูลผ่านทางช่องทางต่างๆ ว่าจับผิดตัว มีการกล่าวหาใส่ร้ายป้ายสีรวมถึงการสร้างความขัดแย้งกัน

ระหว่างกลุ่มประชาสังคม ตลอดจนการนำประเด็นทางการเมืองมาเชื่อมโยงและขยายผลให้ไปสู่การสร้างสถานการณ์แห่งความรุนแรงดังเหตุการณ์ที่เกิดขึ้นในหลายๆ ครั้งในพื้นที่ชายแดนภาคใต้

๑.๑.๓ รูปแบบของการชักชวน พื้นฐานของประชาชนในพื้นที่ชายแดนภาคใต้ถูกสอนให้ติดดินซึ่งทำให้ผู้คนสูงอายุไม่ได้สนใจสื่อสังคมสมัยใหม่หรือไม่สนใจรับรู้ข่าวสารจากภาครัฐ โดยส่วนใหญ่จะมีความเชื่อในตัวผู้นำหมู่บ้านหรือโต๊ะอิหม่ามมากกว่าการเชื่อถือหน่วยงานภาครัฐหรือข่าวสารจากที่อื่นๆ รูปแบบของการชักชวนจะปรากฏให้เห็นผ่านสื่อสังคมออนไลน์ประเภทต่างๆ โดยเฉพาะอย่างยิ่งกลุ่มของ IS ที่มีการเผยแพร่แนวคิดและความรุนแรงโดยการหาแนวร่วมเพื่อเชิญชวนให้ไปร่วมรบในประเทศซีเรียหรือบริเวณต่างๆ ที่เกิดความรุนแรงบนโลก โดยมีการตรวจพบจากเจ้าหน้าที่ด้านความมั่นคงว่าการชักชวนและโจมตีในประเด็นการเผยแพร่ข่าวสารเกี่ยวกับประเด็นการชักชวนนี้เสมอมาตั้งแต่อดีตจนถึงปัจจุบัน

ปัจจุบันจะเห็นว่ากลุ่มผู้บริโภคข้อมูลข่าวสารโดยใช้ระบบอินเตอร์เน็ตและเครือข่ายสังคมออนไลน์มีด้วยกันทั้งสิ้น ๖ กลุ่ม ได้แก่ กลุ่มขบวนการก่อการร้าย กลุ่มภาคประชาสังคม กลุ่มสื่อสารมวลชน กลุ่มสื่อทางเลือก กลุ่มสื่อสารสังคมออนไลน์ และกลุ่มภาคประชาชน จากการติดตามพฤติกรรมการใช้งานสื่อสังคมออนไลน์ เช่น Facebook, Twitter และ Line ของทุกกลุ่มพบว่ามีการสร้างข้อมูลและบิดเบือนข้อมูลอยู่ตลอดเวลา โดยเมื่อเจ้าหน้าที่ฝ่ายความมั่นคงตรวจพบมากขึ้นก็จะมีการปรับมาใช้ Telegram Messenger แทนในบางโอกาส รวมถึงมีการขยายผลหากมีการจับได้โดยการใช้การติดตามย้อนหลังจากอุปกรณ์ที่ยึดมาได้เพื่อนำไปสู่การจับกุมขบวนการก่อการร้ายต่อไป ผลการวิจัยสอดคล้องกับ หยาดพิรุณ นาชัยสินธุ์ (๒๕๖๐) ที่กล่าวว่าเครื่องมือที่สำคัญของการก่อการร้ายทางไซเบอร์ก็คือ อินเตอร์เน็ตและเครือข่ายสังคมออนไลน์นั่นเอง

๑.๒ รูปแบบของภัยคุกคามด้านไซเบอร์ที่พบในพื้นที่จังหวัดชายแดนภาคใต้ในความคิดเห็นของเจ้าหน้าที่ระดับปฏิบัติการด้านความมั่นคงรวมถึงเจ้าหน้าที่ทหารที่รับผิดชอบด้านภัยคุกคามของสำนักปฏิบัติการข่าวสาร สามารถสรุปได้ว่ามีรูปแบบที่ปรากฏดังนี้

๑.๒.๑ รูปแบบที่ ๑ จะเป็นลักษณะการโจมตีโดยเน้นการโจมตีโดยมีรูปแบบเป็นกลุ่มขบวนการก่อการร้ายที่หวังผลทำให้เกิดความเสียหายต่อหน่วยงานของภาครัฐ ปฏิบัติการด้วยการสร้างระบบข้อมูลข่าวสารอันเป็นเท็จและขยายผลผ่านเครือข่ายสังคมออนไลน์รูปแบบต่างๆ

๑.๒.๒ รูปแบบที่ ๒ ช่วงปี พ.ศ.๒๕๕๐-๒๕๕๑ ได้มีบุคคลภายนอกเข้ามาเจาะข้อมูลโดยพยายามเข้ามาผ่านระบบ File Wall แต่ทางเจ้าหน้าที่ของรัฐยังไม่ทราบว่าได้นำข้อมูลใดออกไปได้มากน้อยเพียงใด หลังจากนั้นก็ได้มีการสร้างระบบการป้องกันมากยิ่งขึ้น ดังนั้นจึงกล่าวได้ว่าเป็นรูปแบบที่ใช้บุคคลภายนอกผู้เชี่ยวชาญด้านระบบไอซีทีเป็นคนดำเนินการ

๑.๒.๓ รูปแบบที่ ๓ เป็นรูปแบบสายลับจากภายนอกเข้ามาขโมยข้อมูลโดยเข้ามารับราชการหรือบรรจุเข้าปฏิบัติราชการและอาจเข้ากลุ่มเครือข่ายสังคมออนไลน์ของเจ้าหน้าที่รัฐเพื่อนำข้อมูลภายในออกไปสู่กลุ่มเป้าหมายหรือขบวนการก่อการร้าย จากการตรวจสอบของเจ้าหน้าที่ว่าทราบเรื่องเนื่องจากเคยเกิดเหตุการณ์ปะทะกันและเข้าตรวจค้นพื้นที่จึงพบฮาร์ดดิสก์เป็นข้อมูลภายใน ๓๕๑ ที่สามารถหลุดออกไปได้

๑.๒.๔ รูปแบบที่ ๔ เป็นรูปแบบจากบุคคลภายในองค์กรนำข้อมูลข่าวสารออกไปโดยทั้งตั้งใจและความรู้เท่าไม่ถึงการณ์หรือคนภายในออกไปเผยแพร่ข้อมูลเองในเครือข่ายสังคมออนไลน์โดยมิได้คำนึงถึงผลกระทบที่จะตามมาในอนาคต

๑.๓ รูปแบบของภัยคุกคามด้านไซเบอร์ที่พบในพื้นที่จังหวัดชายแดนภาคใต้ในความคิดเห็นของนักวิชาการและผู้เชี่ยวชาญด้านระบบไอซีทีซึ่งเป็นเจ้าหน้าที่ด้านความมั่นคงสามารถสรุปได้ว่ามีรูปแบบที่ปรากฏดังนี้

๑.๓.๑ รูปแบบของภัยคุกคามส่วนมากเป็นการใช้สื่อในการกระจายข่าว การสร้างเพจเพื่อบิดเบือนข่าวสารข้อมูล ปลุกปั่นและสร้างกระแสทั้งทางที่ดีและไม่ดี การสร้างเครือข่ายสังคมเฉพาะกลุ่ม และการนำแนวคิดกระจายลงสู่พื้นที่ให้ประชาชนในพื้นที่มากที่สุดโดยผ่านสื่อต่างๆ รวมถึงเครือข่ายสังคมออนไลน์

๑.๓.๒ รูปแบบของภัยคุกคามที่ปรากฏมี ๓ รูปแบบ คือ ๑) การสร้างข่าวขึ้นใหม่รายวัน ๒) ข่าวจริงแต่บิดเบือนข่าวปัจจุบัน และ ๓) นำข่าวเก่ามานำเสนอซ้ำ เพื่อนำเสนอข่าวออกไปในทางลบโดยผ่านสื่อต่างๆ รวมถึงเครือข่ายสังคมออนไลน์ การสร้างความขัดแย้งระหว่างกลุ่มการเมืองและผลประโยชน์ และการสร้างความเกลียดชังให้ประชาชนไม่ไว้วางใจเจ้าหน้าที่ของรัฐ ยกตัวอย่างกรณีของเรือเหาะกองทัพบก เป็นต้น ในส่วนของสถานที่ราชการและสถานที่สำคัญของจังหวัด เช่น มหาวิทยาลัย มัสยิดกลาง และศาลาประชาคม มีการพบข่าวสารบิดเบือนที่แพร่กระจายผ่านสื่อออนไลน์ค่อนข้างมาก โดยมีการตอบโต้โดยการพูดคุยทำความเข้าใจกับประชาชน มีการประชุมแลกเปลี่ยนกันเป็นประจำ และมีการกำหนดรูปแบบการพูดคุยการให้ข่าวสารจากหน่วยเหนืออีกด้วย

๑.๓.๓ รูปแบบการเข้าเจาะข้อมูลโดยเป็นการดึงข้อมูลออกไป หลังจากนั้นมีการเปลี่ยนภาพในโฮมเพจหรือในเว็บไซต์ให้เป็นภาพการ์ตูน บางครั้งจัดว่าเป็นการโจมตีแต่ไม่พบเป็นการจารกรรมข้อมูลโดยตรง แต่เพื่อการเข้ามาตรวจสอบดูการเคลื่อนไหวของหน่วยงานของรัฐเท่านั้น จากข้อมูลเชิงลึกของสำนักข่าวกรองพบว่ามีการ จารกรรมข้อมูลออกไปครั้งหนึ่งปี พ.ศ. ๒๕๕๘ โดยเว็บไซต์ของสำนักข่าวกรองที่ใช้ในการรายงานข่าวไม่สามารถตรวจสอบได้ว่ามีการนำข้อมูลออกไปได้มากน้อยเพียงใด

๑.๓.๔ รูปแบบเฉพาะกิจ เช่น การพยายามจารกรรมและเจาะเข้าระบบฐานข้อมูลขบวนการก่อการร้าย ซึ่งระบบดังกล่าวจะเป็นการเก็บข้อมูลรายงานข่าวการเคลื่อนไหวของขบวนการ โดยเปรียบเหมือนการลองของโดยไม่ได้เน้นโจมตี อีกทั้งมีการใช้สายลับโดยให้บุคคลมาสมัครรับราชการในหน่วยงานด้านความมั่นคงและเมื่อเข้ามาได้ก็จะหาวิธีการรายงานข้อมูลให้ขบวนการได้ทราบความเคลื่อนไหวและมีการนำข้อมูลออกไปสู่ภายนอก ดังตัวอย่างเหตุการณ์ปะทะต้นหมีที่มีผู้เสียชีวิตสามศพแล้วค้นพบฮาร์ดดิสก์ในที่เกิดเหตุ ซึ่งเมื่อตรวจสอบพบข้อมูลภายในที่มาจากหน่วยทหาร ทำให้ทราบได้ว่ามีการจารกรรมข้อมูล จากนั้นมีการสอบสวนทำให้ทราบผู้รับผิดชอบ

๑.๔ รูปแบบของภัยคุกคามด้านไซเบอร์ที่พบในพื้นที่จังหวัดชายแดนภาคใต้ในความคิดเห็นของหน่วยงานภาคเอกชน หน่วยงานพลเรือน และภาคประชาชน สามารถสรุปได้ว่ามีรูปแบบที่ปรากฏดังนี้

๑.๔.๑ พบการเผยแพร่หรือแชร์ข้อมูลข่าวสารในลักษณะการบิดเบือนทางสื่อสังคมออนไลน์ชนิดต่างๆ โดยไม่รู้ที่มาและแชร์กันไปทั่ว ซึ่งทำให้เกิดการแชร์ต่อโดยไม่มีคัดกรองและข้อมูลข่าวสารเหล่านั้นย่อมแพร่กระจายได้อย่างรวดเร็ว

๑.๔.๒ หากมีการได้รับข่าวสารใดๆ จะมีการแจ้งต่อกันในหมู่เพื่อน แต่จะมีการวิเคราะห์ดูความเป็นมาและพิจารณาก่อนเพื่อการป้องกันข่าวลวง และมักจะมีคำกล่าวที่ว่า “เหตุการณ์ที่จริงมักจะไม่ค่อยมีการแชร์กัน”

๑.๔.๓ ในการเผยแพร่ข้อมูลข่าวสารบางอย่าง ถ้ารู้จักกันเป็นการส่วนตัวมักจะมีการเตือนกันว่าให้พิจารณาข้อมูลก่อนเผยแพร่ เพราะอาจเป็นการโฆษณาชวนเชื่อหรือการสร้างข่าวเท็จในน่าเชื่อถือก็เป็นได้

๑.๔.๕ หน่วยงานภาคเอกชน หน่วยงานพลเรือน และภาคประชาชน ยังไม่เคยเห็นมาตรการทางกฎหมายว่าสามารถดำเนินการกับผู้บิดเบือนข่าวสารผ่านสื่อสังคมออนไลน์ได้อย่างไร ระดับการใช้งานที่เหมาะสมเป็นอย่างไร อะไรคือข้อพิจารณาในการเผยแพร่ข้อมูลข่าวสารที่ถูกต้องในการดำรงชีวิตของประชาชน

๒. วิธีการของภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

๒.๑ วิธีการของภัยคุกคามด้านไซเบอร์ที่พบในพื้นที่จังหวัดชายแดนภาคใต้ในความคิดเห็นของหน่วยงานด้านความมั่นคงของรัฐ (กองทัพภาคที่ ๔, กอ.รมน.ภาค ๔ ส่วนหน้า, ศอบต., ศชต., และ ฉก.) ผู้บริหาร/ผู้นำท้องถิ่น ๔ จังหวัด สามารถสรุปได้ว่ามีวิธีการที่ปรากฏดังนี้

๒.๑.๑ วิธีการโจมตียังไม่ปรากฏเด่นชัดเนื่องจากยังไม่มีหน่วยงานใดออกมายืนยันว่าภัยคุกคามนี้มีขั้นตอนกระบวนการทางวิชาการอย่างไร ปรากฏเพียงแค่การสร้างข่าวสาร

การแพร่กระจาย และการโต้ตอบกันผ่านสื่อสังคมออนไลน์รูปแบบต่างๆ ครั้งหนึ่งเว็บไซต์ของหน่วยงานหลักทางความมั่นคงในพื้นที่เคยถูกจารกรรมข้อมูลทำเนียบกำลังรบเนื่องจากอยู่ในช่วงปรับปรุงข้อมูลและส่วนเชื่อมโยง โดยมีการทำซ้ำหน้าทำเนียบกำลังรบไปเผยแพร่หรืออาจแจ้งต่อกลุ่มผู้ก่อการร้ายให้ทราบความเคลื่อนไหวของเจ้าหน้าที่ทางการ แต่ปัจจุบันได้รับการแก้ไขแล้ว

๒.๑.๒ เจ้าหน้าที่ใช้สมาร์ทโฟนและแอพพลิเคชั่นต่างๆ อย่างแพร่หลาย มีความรู้เท่าไม่ถึงการณ์ของเจ้าหน้าที่บางคนซึ่งมีการนำเอกสารชั้นความลับไปเผยแพร่บนเว็บ โดยอาจเป็นละเมิดการรักษาความปลอดภัยข้อมูลทางราชการและรวมถึงสิทธิส่วนบุคคล ทำให้บุคคลที่ไม่มีหน้าที่ได้รับทราบข่าวสารนั้นไปด้วย (ปริญญา หอมเอนก, ๒๕๖๐) เหตุการณ์นี้อาจเป็นการคาดไม่ถึงหรือมองไม่รอบด้านของฝ่ายความมั่นคงซึ่งโดยปกติแต่ละหน่วยมีมาตรการทั้งระดับบุคคลและระดับหน่วยที่กำกับดูแลการให้ข้อมูลข่าวสารอยู่แล้ว

๒.๒ วิธีการของภัยคุกคามด้านไซเบอร์ที่พบในพื้นที่จังหวัดชายแดนภาคใต้ในความคิดเห็นของเจ้าหน้าที่ระดับปฏิบัติการด้านความมั่นคงรวมถึงเจ้าหน้าที่ทหารที่รับผิดชอบด้านภัยคุกคามของสำนักปฏิบัติการข่าวสาร สามารถสรุปได้ว่ามีวิธีการที่ปรากฏดังนี้

๒.๒.๑ ยังไม่พบการเจาะข้อมูลแต่พบการแฝงตัวว่าเป็นเจ้าหน้าที่รัฐแล้วเข้ากลุ่ม Line และ Facebook ที่ประกอบด้วยชาวบ้านและเจ้าหน้าที่รัฐหรือเข้ามาดำเนินการขโมยข้อมูลโดยติดตามว่าใครเป็นเจ้าหน้าที่บ้าง เมื่อเจ้าหน้าที่พิสูจน์ทราบก็มีการรายงานไปยัง Line และ Facebook เพื่อให้สลายกลุ่มหรือปิด

๒.๒.๒ มีการนำข้อมูลสารสนเทศทั้งในส่วนราชการและภาคเอกชนไปใช้ในการใส่ร้ายป้ายสี ยั่วยุปลุกปั่น และสร้างความขัดแย้งทางศาสนา โดยการเผยแพร่และสร้างภาพให้เจ้าหน้าที่รัฐเกิดความเสียหายและกระทำผิดต่อประชาชน

๒.๒.๓ ยังไม่มีการเชื่อมโยงกับศูนย์ไซเบอร์ทั้งในระดับชุมชนและระดับหน่วยงานโดยเฉพาะอย่างยิ่งหน่วยงานทางความมั่นคง โดยยังไม่มีเจ้าภาพรับผิดชอบหรือไม่มีตัวกลางด้านไซเบอร์และด้าน IO

๒.๒.๔ มีการตรวจพบว่าผู้ประกอบวิชาชีพอาจารย์และประชาชนหลากหลายสาขาอาชีพได้นำข้อมูลข่าวสารไปบิดเบือนหลายๆ ครั้ง โดยเจ้าหน้าที่มีการประชุมติดตามและมีการตรวจสอบติดตามผ่านทางสื่อสังคมออนไลน์เช่นกัน อีกทั้งผู้ประสานงานสายข่าวได้มีการสร้างบัญชีปลอมขึ้นเพื่อการตรวจหาข่าวโดยมีสถานะอำพลางตัวตนเพื่อให้เข้าถึงแหล่งข่าว และในที่สุดจะนำไปสู่การค้นหาแหล่งที่มาของขบวนการก่อการร้ายต่อไป

๒.๒.๕ มีการส่งข่าวสารบิดเบือนผ่านทางอีเมล์ในลักษณะลูกโซ่ นั่นคือ เมื่อผู้ใดได้รับข้อมูลข่าวสารแล้วก็จะดำเนินการส่งต่อให้ผู้เป็นสมาชิกและไม่เป็นสมาชิกของกลุ่มก่อ

การร้ายในทันทีโดยไม่ได้ปรึกษาหารือกับหน่วยงานราชการก่อนว่าข้อมูลข่าวสารนี้มีที่มาที่ไปอย่างไร น่าเชื่อถือหรือไม่ และมีเป้าประสงค์ใด

๒.๒.๖ หากมีสื่อสังคมออนไลน์ที่บิดเบือนจาก YouTube จะทำการสรุปหาการเชื่อมโยงและรายงานไปยังหน่วยงานระดับสูงกว่าเพื่อดำเนินการต่อไป โดยในส่วนการสั่งปิดจะต้องส่งไปยังกระทรวงไอซีที แต่ถ้าเป็น Facebook จะทำการเฝ้าระวังโดยการแฝงตัวแทนเพื่อการติดตามข้อมูลและพฤติกรรมอย่างใกล้ชิดและรายงานผลให้ผู้บังคับบัญชาทราบตามลำดับต่อไป

๒.๓ วิธีการของภัยคุกคามด้านไซเบอร์ที่พบในพื้นที่จังหวัดชายแดนภาคใต้ในความคิดเห็นของนักวิชาการและผู้เชี่ยวชาญด้านระบบไอซีทีซึ่งเป็นเจ้าหน้าที่ด้านความมั่นคง สามารถสรุปได้ว่ามีวิธีการที่ปรากฏดังนี้

๒.๓.๑ ภัยคุกคามทางออนไลน์นับว่ามีความรุนแรงและเพิ่มขึ้น เนื่องจากเยาวชนไม่รู้เท่าทันสื่อและข้อมูลข่าวสาร ทำให้เป็นช่องทางในการชักชวนเข้าสู่ส่วนหนึ่งของกระบวนการก่อการร้ายได้

๒.๓.๒ การแจ้งข่าวสารหรือการโต้ตอบข่าวสารของทางภาครัฐค่อนข้างล่าช้าทำให้ไม่ทันการณ์หรือเป็นสถานะผู้ตามอยู่เสมอ

๒.๓.๔ การใช้สื่อสังคมออนไลน์ในการบิดเบือนข่าวสาร โดยมีทั้งข่าวที่เป็นความจริงและความจริงที่บิดเบือนเพื่อประโยชน์บางอย่าง เนื่องจากสื่อสังคมออนไลน์ไม่มีการควบคุมหรือควบคุมยาก วิธีการแก้ไขจากทางการก็คือทางการจะต้องใช้ความจริงที่จริงกว่า

๒.๓.๕ แต่เดิมสื่อถูกควบคุมโดยภาครัฐ แต่ปัจจุบันการเผยแพร่ข้อมูลเปลี่ยนไปโดยเทคโนโลยีและไม่มีการควบคุมกลั่นกรอง ทำให้การบิดเบือนกระจายข้อมูลข่าวสารไปได้ในวงกว้างอย่างง่ายขึ้นและยากต่อการควบคุมอีกต่อไป

๒.๔ วิธีการของภัยคุกคามด้านไซเบอร์ที่พบในพื้นที่จังหวัดชายแดนภาคใต้ในความคิดเห็นของหน่วยงานภาคเอกชน หน่วยงานพลเรือน และภาคประชาชน สามารถสรุปได้ว่ามีวิธีการที่ปรากฏดังนี้

๒.๔.๑ มีการใช้เทคโลยีในการก่อการร้ายมากยิ่งขึ้นเช่นแต่ก่อนใช้กดระเบิดแต่ปัจจุบันใช้สมาร์ทโฟน และในอนาคตอาจเกิดการใช้เทคโนโลยีอื่นๆ มาร่วมด้วยมากขึ้น ส่งผลให้สถานการณ์อันตรายมากขึ้นเนื่องจากการก่อเหตุมีความแม่นยำมากยิ่งขึ้น

๒.๔.๒ มีสมาชิก NGO หลายคนไม่สนับสนุนการทำงานของภาครัฐและนำข้อมูลข่าวสารไปบิดเบือนจนสร้างความเสียหายให้กับประเทศชาติ โดยควรมีการนำ พรบ. คอมพิวเตอร์ฯ มาใช้เป็นเครื่องอย่างจริงจังที่อาจส่งผลให้ความเสียหายให้กับประเทศชาติลดลง

๓. การประเมินสถานการณ์ภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

๓.๑ การประเมินสถานการณ์ภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ในความคิดเห็นของหน่วยงานด้านความมั่นคงของรัฐ (กองทัพภาคที่ ๔, กอ.รมน.ภาค ๔ ส่วนหน้า, ศอบต., ศชต., และ ฉก.) ผู้บริหาร/ผู้นำท้องถิ่น ๔ จังหวัด สามารถสรุปได้ว่ามีกระบวนการประเมินที่ปรากฏดังนี้

๓.๑.๑ มีการตรวจจับและติดตามผู้โพสข้อความและข้อมูลข่าวสาร วิเคราะห์ รวบรวม บันทึกจับกุมจากทีมข่าวเปิด และรายงานผลซึ่งกระทำโดยคนเป็นหลัก มีการเปลี่ยนรูปแบบเสมอถ้ามีการจับได้ แต่ทางการมีการนำอุปกรณ์มาใช้ในการตรวจจับมากขึ้นโดยเฉพาะฮาร์ดแวร์พิเศษ โดยยังไม่มีการใช้ Sniffer แต่มีการตรวจสอบจากเครื่องมือสื่อสารที่ยึดได้และมีการสร้างการวิเคราะห์เชื่อมโยง (Link Analyze)

๓.๑.๒ การประเมินสถานการณ์ยังไม่มีรูปแบบแน่นอนตายตัว สืบเนื่องมาจากส่วนงานที่รับผิดชอบด้านไซเบอร์ระดับประเทศยังมีลักษณะไม่เป็นรูปธรรม หน่วยงานที่รับผิดชอบในพื้นที่ก็พยายามเรียนรู้และพัฒนาขีดความสามารถของการตรวจจับเพิ่มขึ้นเรื่อยๆ มีการประชุมร่วมกันแบ่งปันข้อมูลข่าวสารระหว่างหน่วยงานต่างๆ ของจังหวัดชายแดนภาคใต้อยู่เสมอ หากไม่มีมาตรการที่เหมาะสมก็จะดำเนินการเชิงรับต่อไป

๓.๑.๓ จากการประเมินสถานการณ์ในส่วนผู้ก่อเหตุรุนแรงพบว่ามักมีรูปแบบการแบ่งทีมกันทำงานอย่างเป็นระบบ โดยมีการจัดตั้งกลุ่ม เช่น ทีมวางระบบ ทีมคอมพิวเตอร์ ทีมสร้างข่าว กลุ่มสนับสนุน NGO,CSO และกลุ่มภาคประชาสังคม เป็นต้น ซึ่งเมื่อรวมกันพบว่ามีองค์กรประมาณ ๕๒๑ องค์กร โดยจัดตั้งเป็น ๔ กลุ่ม ได้แก่ ๑) กลุ่มเคลื่อนไหวลงประชามติการแบ่งแยกดินแดนประมาณ ๓๐ กว่าองค์กร ๒) กลุ่มดำเนินการสร้างสภาพแวดล้อม ๓) กลุ่มโจมตี การปฏิบัติหน้าที่ของรัฐและกลุ่มทนายความ และ ๔) กลุ่มดำเนินงานเพื่อเอื้อประโยชน์ให้แก่ฝ่ายรัฐ

๓.๒ การประเมินสถานการณ์ภัยคุกคามด้านไซเบอร์ที่พบในพื้นที่จังหวัดชายแดนภาคใต้ในความคิดเห็นของเจ้าหน้าที่ระดับปฏิบัติการด้านความมั่นคงรวมถึงเจ้าหน้าที่ทหารที่รับผิดชอบด้านภัยคุกคามของสำนักปฏิบัติการข่าวสาร สามารถสรุปได้ว่ามีกระบวนการประเมินที่ปรากฏดังนี้

๓.๒.๑ เจ้าหน้าที่ประเมินว่าทีมข่าวเปิดเปรียบเสมือนการลาดตระเวนทางไซเบอร์ ดังนั้นจะต้องดำเนินการด้วยมาตรการเชิงรุกอย่างต่อเนื่องเพื่อให้รู้เท่าทันขบวนการก่อการร้ายที่มาอย่างไร้รูปแบบชัดเจน ประกอบกับการสนับสนุนจากหน่วยงานภาครัฐอย่างเป็นระบบจะช่วยให้การทำงานมีประสิทธิภาพมากขึ้น

๓.๒.๒ มีการคุกคามและสร้างความเสียหายมากขึ้นเรื่อยๆ จากการใช้งานไซเบอร์รูปแบบต่างๆ เจ้าหน้าที่ต้องตระหนักว่าสื่อสังคมออนไลน์ต่างๆ ล้วนไม่มีความปลอดภัย ดังนั้นต้องมีกระบวนการสร้างความตระหนักด้านความปลอดภัยไซเบอร์ให้มากขึ้นโดยการสร้างความรับรู้ด้านต่างๆ ที่เกี่ยวข้องทุกมิติ การมีส่วนร่วมในการจัดการภัยคุกคามด้านไซเบอร์ มีการใช้มาตรการทางกฎหมายหากมีการตรวจพบ ดังสถานการณ์ตัวอย่างที่สร้างความเสียหาย อาทิ การถูกบล็อกเพจของหน่วยงานด้านความมั่นคง หากมีการตรวจพบการใช้งานสื่อสังคมออนไลน์ที่หน้าสงสัยจะต้องมีการตรวจสอบหาความเชื่อมโยง จดสถิติ และมีการจัดตั้งทีมรายงานเพื่อรายงานไปยังเจ้าของแอพพลิเคชั่นที่รับผิดชอบเพื่อดำเนินการอย่างหนึ่งอย่างดกับผู้บุกรุกเพื่อปิดเพจนั้นทันทีก่อนที่จะกระจายไปไม่รู้จบ แต่บางครั้งก็ไม่ได้รับการตอบรับจากเจ้าของแอพพลิเคชั่นก็คงต้องมีมาตรการส่งต่อไปยังหน่วยงานที่กำกับดูแลในระดับสูงต่อไป

๓.๒.๓ ปัจจุบันฝ่ายทหารและหน่วยงานด้านความมั่นคงอื่นก็มีการใช้งานสื่อสังคมออนไลน์ เช่น Facebook, Line, Twitter และ Blogger ในการทำลายฝ่ายตรงข้ามเช่นกัน เรียกได้ว่าเป็นการใช้ข้อมูลข่าวสารเพื่อประโยชน์ในงานด้านการข่าวและการตรวจจับหรือเฝ้าระวังผู้บุกรุกผ่านระบบไอซีที ดังนั้นจึงอยากให้มีเครื่องมือจับ IP address ของเครื่องที่บิดเบือนข่าวสารจะก่อให้เกิดความสะดวกในการทำงานมากขึ้น

๓.๒.๔ เนื่องจากในฝ่ายทหารและตำรวจรวมถึงหน่วยงานที่เกี่ยวข้องด้านความมั่นคงยังไม่มีศูนย์ทางไซเบอร์ที่ทันสมัย โดยเฉพาะอย่างยิ่งในสามจังหวัดชายแดนภาคใต้มีความต้องการใช้มากเนื่องจากมีการนำสื่อสังคมออนไลน์มาบิดเบือนเป็นประจำ ควรมีการนำกสทช. มาช่วยและบูรณาการในเรื่องการตัดสินใจอย่างเป็นรูปธรรม การขาดบุคลากรในการดำเนินการเพราะรัฐจ่ายค่าตอบแทนในอัตราที่ต่ำ ดังนั้นบุคลากรด้านนี้จึงไม่มีการเติบโตและทำงานเท่าเดิม

๓.๒.๕ ปัจจุบันประเทศไทยยังไม่มีกฎหมายควบคุมอุปกรณ์อิเล็กทรอนิกส์โดยเฉพาะเจ้าหน้าที่นโยบายความปลอดภัยทางกายภาพ ไม่มีกฎหมายการจัดการส่งข้อมูลผ่านสื่ออิเล็กทรอนิกส์ ซึ่งยังไม่มีการเข้ารหัส มีการปลุกปั่นและสื่อให้เห็นว่าเป็นการแบ่งแยกดินแดนเป็นรัฐปัตตานี มีความพยายามกำหนดให้การแบ่งแยกดินแดนเป็นรัฐปัตตานีเป็นหน้าที่ของคนอิสลามทุกคน โดยประชาชนได้รับข่าวสารแต่เพียงด้านเดียว ดังนั้นสื่อสังคมออนไลน์สามารถทำให้เข้าถึงประชาชนเป้าหมายได้มากขึ้นและสามารถนำสื่อกลับมาใช้ใหม่ได้ ทำให้เกิดการกระจายข่าวสารที่ผิดพลาดได้อย่างต่อเนื่องซึ่งไม่ส่งผลดีต่อการสร้างความสงบสุขให้กับประชาชน

๓.๒.๖ มีการสร้างแนวคิดที่บิดเบือนเพื่อครอบงำประชาชนในพื้นที่ ได้แก่ ๑) รัฐชาติมาลายู ๒) ศาสนาอิสลาม และ ๓) มาตุภูมิ ฉะนั้นต้องปรับเปลี่ยนทัศนคติ โดยเรื่องเหล่านี้

ปรากฏอยู่บนสื่อสังคมออนไลน์อย่างต่อเนื่องโดยแทบจะไม่มีหน่วยงานใดเข้าไปดำเนินการอย่างเป็นรูปธรรมได้ รูปแบบการประเมินสถานการณ์นั้นต้องประเมินการเคลื่อนไหวใน ๗ กลุ่ม ที่สร้างความเสียหาย ได้แก่ กลุ่มที่ ๑ BRN, กลุ่มที่ ๒ พูโล ๑ ดาว, กลุ่มที่ ๓ พูโล ๔ ดาว, กลุ่มที่ ๔ พูโล ๕ ดาว, กลุ่มที่ ๕ GMP, กลุ่มที่ ๖ BIPP และกลุ่มที่ ๗ GMIP โดยจะต้องมีหน่วยงานที่เชี่ยวชาญด้านระบบไอซีทีและไซเบอร์คอยติดตามความเคลื่อนไหวในกลุ่มต่างๆ เหล่านี้อย่างใกล้ชิดและต่อเนื่องที่สุด

๓.๓ การประเมินสถานการณ์ภัยคุกคามด้านไซเบอร์ที่พบในพื้นที่จังหวัดชายแดนภาคใต้ในความคิดเห็นของนักวิชาการและผู้เชี่ยวชาญด้านระบบไอซีทีซึ่งเป็นเจ้าหน้าที่ด้านความมั่นคง สามารถสรุปได้ว่ามีกระบวนการประเมินที่ปรากฏดังนี้

๓.๓.๑ รูปแบบของสถานการณ์ที่เกิดขึ้นพบว่าชาวบ้านจะเชื่อผู้นำทางศาสนามากกว่า ฝ่ายปกครอง ดังนั้นจึงปรากฏภาพที่ไม่เหมาะสมและมีโอกาสกระจายผ่านออนไลน์ได้ง่ายและเร็ว เนื่องจากหากเกิดเหตุแล้วประชาชนหรือมูลนิธิอาจไปถึงก่อนทำให้ภาพแห่งความรุนแรงหลุดไปก่อน

๓.๓.๒ มีหน่วยงานติดตามข้อมูลข่าวสารทางสื่อสังคมออนไลน์และมีการประชุมกลั่นกรองเพื่อส่งต่อไปกระทรวงไอซีทีเพื่อปิดเว็บ และขั้นต่อไปจะต้องส่งฟ้องศาล แต่หากเป็นเว็บต่างประเทศต้องติดต่อผ่านกระทรวงต่างประเทศ

๓.๓.๓ มีทีมทำ IO ที่จัดตั้งมาสำหรับการตอบโต้ข่าวบิดเบือนผ่านสื่อสังคมออนไลน์ดังเช่นเหตุการณ์จับคนขับรถโรงเรียน ข่าวออกไปว่าตำรวจไปล้อมจับรถตู้ นักเรียนที่อยู่ในรถได้รับความเดือนร้อน ร้องไห้ตกใจ และทำเกินกว่าเหตุ แต่ในความเป็นจริงคนขับมีหมายจับและขับมาเจอด่านจึงมีการเชิญตัวไปและรับส่งนักเรียนอย่างเรียบร้อยโดยไม่มีการกระทำเกินกว่าเหตุ ผลที่ปรากฏทำให้ภาพลักษณ์ของเจ้าหน้าที่รัฐเสียหายมากในสายตาประชาชนและยังสามารถเป็นชนวนให้เกิดความขัดแย้งได้เพิ่มขึ้นอีก

๓.๔ การประเมินสถานการณ์ภัยคุกคามด้านไซเบอร์ที่พบในพื้นที่จังหวัดชายแดนภาคใต้ในความคิดเห็นของหน่วยงานภาคเอกชน หน่วยงานพลเรือน และภาคประชาชน สามารถสรุปได้ว่ามีกระบวนการประเมินที่ปรากฏดังนี้

๓.๔.๑ ภัยคุกคามด้านไซเบอร์นับเป็นภัยคุกคามที่อันตรายร้ายแรง จะต้องมีการประชาสัมพันธ์ให้ทุกภาคส่วนรับรู้และเรียนรู้อย่างต่อเนื่องทั้งทางสื่อสังคมออนไลน์เองและการลงพื้นที่ทำความเข้าใจกับประชาชน

๓.๔.๒ เจ้าหน้าที่รัฐจะจัดการกับปัญหาสื่อสังคมออนไลน์ที่มีลักษณะสร้างความรุนแรงเหล่านี้ได้ยากขึ้น เพราะบางส่วนอาจคิดว่าเป็นเครื่องมือของเจ้าหน้าที่รัฐ

๓.๔.๓ มีการประเมินสถานการณ์ตลอด แต่หากมีเหตุการณ์ใหญ่ก็จะมีการออกหนังสือชี้แจงและหากเล็กน้อยก็จะไม่ตอบโต้ ประชาชนส่วนใหญ่มีการคิดวิเคราะห์ก่อนเมื่อได้รับข้อมูลข่าวสารที่ไม่ชัดเจนและจะไม่เผยแพร่ต่อถ้ายังไม่มั่นใจ

๔. ปัญหาผลกระทบของภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

๔.๑ ปัญหาผลกระทบของภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ในความคิดเห็นของหน่วยงานด้านความมั่นคงของรัฐ (กองทัพภาคที่ ๔, กอ.รมน.ภาค ๔ ส่วนหน้า, ศอบต., ศชต., และ ฉก.) ผู้บริหาร/ผู้นำท้องถิ่น ๔ จังหวัด สามารถสรุปได้ว่ามีปัญหาผลกระทบที่ปรากฏดังนี้

๔.๑.๑ เป็นการพัฒนาขีดความสามารถของผู้ก่อการร้ายในการเข้าถึงและทำลาย ซึ่งการก่อการร้ายระดับโลกก็มีตัวอย่างให้เห็นแล้วว่าพัฒนาการของผู้ก่อการร้ายมีมาอย่างต่อเนื่อง โดยหากเกิดผลเสียหายต่อประเทศชาติทางตรงก็ต้องมีการแถลงข่าวตอบโต้ทันที

๔.๑.๒ ในขบวนการก่อการร้ายมีการอบรมการสร้างมีเดียหรือคอนเท็นในการนำเสนอโฆษณาชวนเชื่อทางอ้อมซึ่งสามารถสร้างความสับสน ปั่นป่วน และความขัดแย้งให้กับประชาชน โดยมีลักษณะ ได้แก่ การนำรูปภาพมาบิดเบือน การนำคำพูดบิดเบือน และการสร้างสถานการณ์บิดเบือน เป็นต้น ผู้ก่อการร้ายอาจมีหลากหลายทีม เช่น ทีมการเมือง ทีมครู ทีมศาสนา และทีมผู้รู้ไอซีที เป็นต้น

๔.๑.๓ ผลกระทบของภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้จัดได้ว่าเป็นปัญหาใหญ่ระดับชาติที่คอยขัดขวางและกีดกันการสร้างความสงบสุขให้พี่น้องประชาชน ดังนั้นรัฐบาลควรตระหนักและใช้มาตรการที่เข้มข้นในทุกมิติเพื่อขจัดปัญหาเหล่านี้ก่อนที่จะเกิดเหตุบานปลายในโอกาสต่อไป

๔.๑.๔ มีการบิดเบือนข้อมูลข่าวสารอย่างมากและยากต่อการแก้ไขสถานการณ์ซึ่งย่อมส่งผลเสียต่อภาพลักษณ์ของทางภาครัฐ ทำให้การแก้ไขปัญหาความไม่สงบในจังหวัดชายแดนภาคใต้ยากมากยิ่งขึ้น

๔.๒ ปัญหาผลกระทบของภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ในความคิดเห็นของเจ้าหน้าที่ระดับปฏิบัติการด้านความมั่นคงรวมถึงเจ้าหน้าที่ทหารที่รับผิดชอบด้านภัยคุกคามของสำนักปฏิบัติการข่าวสาร สามารถสรุปได้ว่ามีปัญหาผลกระทบที่ปรากฏดังนี้

๔.๒.๑ หากเกิดเหตุการณ์ เช่น ทหารพรานอิสลามไปยิงผู้ก่อการร้าย ทางผู้ก่อการร้ายจะบิดเบือนข่าวและส่งข้อมูลผ่านสื่อสังคมออนไลน์ได้อย่างรวดเร็ว แต่ฝ่ายทหารต้องผ่านผู้บังคับบัญชาหลายชั้นทำให้การแถลงข่าวล่าช้าไปมากทำให้ไม่ทันการณ์และส่งผลให้ประชาชนเข้าใจผิดว่าเป็นการกระทำของเจ้าหน้าที่รัฐ

๔.๒.๒ ไม่มีใครสามารถควบคุมสื่อได้เพราะข้อมูลข่าวสารที่บิดเบือนสามารถเผยแพร่ออกไปทุกวันทั้งในรูปแบบปิด (เฉพาะกลุ่ม) และแบบสาธารณะ โดยเจ้าหน้าที่รัฐต้องตามแก้ไขในลักษณะรายวัน

๔.๒.๓ ปัจจุบันกลุ่มสื่อสังคมออนไลน์สามารถสร้าง รวบรวม และชักจูงคนเข้าร่วมได้ง่ายมาก โดยอาจเป็นฝ่ายสนับสนุน เช่น การดูต้นทางหรือสำรวจเส้นทางให้ผู้ก่อการร้ายปฏิบัติการได้อย่างสะดวก เป็นต้น เนื่องจากผู้ก่อการร้ายมักมีการทำงานเป็นทีม ดังนั้นความคิดของชาวบ้านที่ได้รับข้อมูลข่าวสารผิดๆ มา เนื่องจากบางคนมีอคติกับเจ้าหน้าที่รัฐและเมื่อเชื่อมากๆ ก็จะกลายเป็นแนวร่วมกับผู้ก่อการร้ายหรือสนับสนุนในที่สุด

๔.๒.๔ โดยปกติของชาวบ้านจะเชื่อบุคคลสนิทมากกว่านำข้อมูลที่ได้ไปวิเคราะห์ เช่น มีการแปลคัมภีร์ทางศาสนาบิดเบือนโดยโต๊ะอีหม่ามหรือผู้นำศาสนาแล้วนำไปใช้สอนในโรงเรียนสอนศาสนาบางแห่ง ทำให้เยาวชนหลงเชื่อและปฏิบัติตามแนวคิดได้ง่าย และในที่สุดเยาวชนเหล่านี้ก็จะเติบโตมาพร้อมกับอุดมการณ์แห่งความรุนแรงที่ปรากฏในประเทศไทยต่อไป

๔.๓ ปัญหาผลกระทบของภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ในความคิดเห็นของนักวิชาการและผู้เชี่ยวชาญด้านระบบไอซีทีซึ่งเป็นเจ้าหน้าที่ด้านความมั่นคงสามารถสรุปได้ว่ามีปัญหาผลกระทบที่ปรากฏดังนี้

๔.๓.๑ มีผลกระทบที่รุนแรงมากในระยะยาว แต่อาจใช้เวลามากในการแย่งชิงมวลชนโดยอาจจะเป็นกลุ่มระดับกลางและกลุ่มผู้มีการศึกษา โดยเป็นเป้าหมายเพื่อให้เข้าร่วมกับผู้ก่อการร้าย ดังเช่น วันที่ ๓ กุมภาพันธ์ ของทุกปีจะเป็นวันทหารผ่านศึก แต่ผู้ก่อการร้ายตั้งให้เป็นวันมนุษยธรรมแห่งปัตตานี ทั้งนี้เพื่อชูประเด็นให้เข้ากฎหมายขององค์การสหประชาชาติเพื่อให้มีการแทรกแซงในประเด็นการจับกุมซ้อมทรมานและการผิดหลักหลักสิทธิมนุษยชน เป็นต้น

๔.๓.๒ การเผยแพร่แนวคิดสุดโต้งรุนแรงอาจมีการเชื่อมโยงกับกลุ่มก่อการร้ายจากต่างประเทศ ซึ่งผู้ก่อการร้ายติดต่อกับขบวนการต่างประเทศได้ง่ายขึ้นผ่านสื่อสังคมออนไลน์ เนื่องจากใช้ภาษามาลายูหรืออาหรับได้

๔.๓.๓ มีการบิดเบือนข่าวสารผ่านโลกออนไลน์ได้รวดเร็วและเป็นวงกว้าง แต่ในขณะที่ทางภาครัฐจะออกข่าวแก้ไขได้ต้องผ่านกระบวนการตามขั้นตอนซึ่งต้องใช้เวลาพอสมควร ทำให้การแก้ข่าวและการทำความเข้าใจไม่ทันต่อทุกสถานการณ์

๔.๓.๔ ทัศนคติของประชาชนในการมีส่วนร่วมกับเจ้าหน้าที่ต่ำมาก เพราะเหตุแห่งความหวาดระแวงและมีความเกลียดชังต่อเจ้าหน้าที่รัฐอย่างต่อเนื่อง ดังนั้นควรให้เจ้าหน้าที่รัฐทำงานอย่างจริงจังโดยมีหลักเกณฑ์สากลในการจัดการและการบังคับใช้กฎหมาย ดังเช่น เมื่อเกิด

เพจที่ไม่ดีหรือมีการเผยแพร่ข่าวสารบิดเบือนผ่านสื่อสังคมออนไลน์อยู่ทั้งที่สื่อนี้เปิดมานานมาก เจ้าหน้าที่มักจะแถลงข่าวไม่ทันท่วงทีและบางครั้งเจ้าหน้าที่รัฐตอบสนองต่อการแจ้งปัญหาทางไซเบอร์ช้ามาก เป็นต้น

๔.๔ ปัญหาผลกระทบของภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ในความคิดเห็นของหน่วยงานภาคเอกชน หน่วยงานพลเรือน และภาคประชาชน สามารถสรุปได้ว่ามีปัญหาผลกระทบที่ปรากฏดังนี้

๔.๔.๑ หากเกิดเหตุการณ์ความวุ่นวายในพื้นที่ ชาวบ้านก็ไม่กล้าออกมานอกบ้านเนื่องจากหวาดกลัวเรื่องความไม่ปลอดภัย ซึ่งจะส่งผลต่อการดำเนินธุรกิจและทุกภาคส่วนจะได้รับผลกระทบตามมาอย่างหลักเลี่ยงไม่ได้

๔.๔.๒ ผลกระทบของภัยคุกคามด้านไซเบอร์สามารถเป็นชนวนสร้างความเกลียดชังขึ้นในสังคม ก่อให้เกิดความหวาดระแวงต่อกัน รวมถึงการเสียชีวิตและทรัพย์สินของพี่น้องประชาชนคนไทย ซึ่งเป็นปัญหาที่ถ้าปล่อยเอาไว้ก็จะก่อให้เกิดปัญหาใหญ่ตามมาได้อีกมากมายนับไม่ถ้วน

๕. ผลกระทบของภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงแห่งชาติรวมถึงแนวโน้มในอนาคต

๕.๑ ผลกระทบของภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงแห่งชาติรวมถึงแนวโน้มในอนาคตในความคิดเห็นของหน่วยงานด้านความมั่นคงของรัฐ (กองทัพภาคที่ ๔, กอ.รมน.ภาค ๔ ส่วนหน้า, ศอบต., ศชต., และ ฉก.) ผู้บริหาร/ผู้นำท้องถิ่น ๔ จังหวัด สามารถสรุปได้ว่ามีผลกระทบที่ปรากฏดังนี้

๕.๑.๑ การสร้างทัศนคติเชิงลบต่อรัฐให้กับประชาชนส่งผลต่อความมั่นคงแห่งชาติเป็นอย่างยิ่ง โดยหากประชาชนจะไปรับข้อมูลข่าวสารอื่นที่ถูกบิดเบือนผ่านสื่อสังคมออนไลน์อย่างต่อเนื่อง ทำให้ต่อไปประชาชนอาจจะไม่เชื่อหรือไม่รับข้อมูลใดจากฝ่ายรัฐอีก และในที่สุดจะนำไปสู่ความเกลียดชังต่อเจ้าหน้าที่ของรัฐและยากที่จะปรับทัศนคติให้กลับคืนมาได้

๕.๑.๒ ผลกระทบต่อความมั่นคงแห่งชาติจะทำให้เกิดความแตกแยกของผู้คนทั้งทางด้านเชื้อชาติและศาสนา โดยเป็นการทำลายสังคมพหุวัฒนธรรมของพื้นที่นี้จนอาจนำไปสู่การแยกตัวไปเป็นเอกเทศในอนาคตการยังไม่ได้รับการแก้ไข

๕.๑.๓ แนวโน้มในอนาคตของภัยคุกคามด้านไซเบอร์จะยังคงเป็นปัญหาหลักที่รัฐบาลต้องดำเนินการอย่างเป็นระบบ ก่อนที่จะเกิดเหตุการณ์บานปลายจนกระทั่งรัฐบาลอาจไม่อยู่ในสถานะควบคุมได้ต่อไป นั่นคือ รัฐไม่มีเสถียรภาพและรัฐไม่มีความน่าเชื่อถือในการดำเนินการเรื่องความปลอดภัย

๕.๑.๔ ปัญหาเรื่องภัยคุกคามด้านไซเบอร์อาจก่อให้เกิดปัญหาระหว่างประเทศได้ถ้าไม่มีกระบวนการแก้ไขโดยความเห็นชอบสากล

๕.๒ ผลกระทบของภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงแห่งชาติรวมถึงแนวโน้มในอนาคตในความคิดเห็นของเจ้าหน้าที่ระดับปฏิบัติการด้านความมั่นคงรวมถึงเจ้าหน้าที่ทหารที่รับผิดชอบด้านภัยคุกคามของสำนักปฏิบัติการข่าวสาร สามารถสรุปได้ว่ามีผลกระทบที่ปรากฏดังนี้

๕.๒.๑ ในโลกไซเบอร์มีการนำประเด็นชาติพันธุ์และศาสนาเข้ามาเป็นประเด็นเพื่อการสร้างข่าวบิดเบือนและเผยแพร่สู่เครือข่ายสังคมออนไลน์ ซึ่งจะส่งผลให้เกิดความเกลียดชังขึ้นในสังคมทุกระดับชั้นโดยทำให้สังคมนั้นอยู่ร่วมกันโดยไม่มีความสงบสุข

๕.๒.๒ ในโลกไซเบอร์และเครือข่ายสังคมออนไลน์มีการนำประเด็นในอดีตทั้งประวัติศาสตร์ที่จริงและบิดเบือนมาใช้เป็นเงื่อนไขสร้างสถานการณ์รุนแรง การสร้างความคิดความเชื่อให้เยาวชนซึ่งจะส่งผลต่ออนาคตของชาติในระยะยาว

๕.๒.๓ ในความเป็นจริงพบว่า ชาวบ้านต้องการความสงบแต่ไม่กล้าบอกเจ้าหน้าที่เนื่องจากไม่แน่ใจว่าเจ้าหน้าที่จะคุ้มครองได้ตลอดชีวิตหรือไม่ ดังนั้นต้องหาวิถีทางคุ้มครองความปลอดภัยของชีวิตและทรัพย์สินให้ดีขึ้นโดยอาจต้องปรับกฎหมายด้านการคุ้มครองให้เห็นเป็นประจักษ์และถูกต้องตามหลักสากล

๕.๒.๔ หากมีปัจจัยหรือสถานการณ์ที่น่าจะมีแนวโน้มรุนแรงมากขึ้น ภาครัฐต้องระวังไม่ให้เกิดเหตุเพื่อให้ผู้ก่อการร้ายนำไปขยายผลไปสู่ความรุนแรงอื่นๆ ได้

๕.๓ ผลกระทบของภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงแห่งชาติรวมถึงแนวโน้มในอนาคตในความคิดเห็นของนักวิชาการและผู้เชี่ยวชาญด้านระบบไอซีทีซึ่งเป็นเจ้าหน้าที่ด้านความมั่นคง สามารถสรุปได้ว่ามีผลกระทบที่ปรากฏดังนี้

๕.๓.๑ ในอนาคตถ้าไม่เกี่ยวข้องกับภัยคุกคามด้านไซเบอร์น่าจะมีการเกิดเหตุการณ์รุนแรงน้อยลง เนื่องจากฝ่ายผู้ก่อการร้ายอาจจะมีงบประมาณหรือผู้สนับสนุนน้อยลง

๕.๓.๒ เหตุการณ์ความไม่สงบมักเกิดจากผลประโยชน์ของคนบางกลุ่มและเจ้าเมืองเก่า โดยมีการปลูกฝังเยาวชนรุ่นใหม่ให้เข้าใจผิดและเกลียดชังต่อรัฐบาล อย่างไรก็ตามมีคนอิสลามรุ่นใหม่ที่มีใจยอมรับได้มากขึ้น

๕.๓.๓ มีแนวโน้มเกิดเหตุการณ์การสร้างข่าวสารบิดเบือนผ่านสื่อสังคมออนไลน์จะทวีความรุนแรงมากยิ่งขึ้นเนื่องจากมีการใช้ไซเบอร์มากขึ้น มีการดึงต่างประเทศเข้ามาร่วมเพื่อให้มีผู้สนับสนุนให้แยกประเทศโดยทำให้ประเทศไทยมีปัญหาในเวทีโลก

๕.๓.๔ ปัจจุบันยังมีกระบวนการละเมิดสถาบันพระมหากษัตริย์ผ่านเครือข่ายสังคมออนไลน์อย่างต่อเนื่อง ซึ่งถือว่าเป็นภัยคุกคามด้านความมั่นคงแห่งชาติต่อสถาบันหลักของประเทศ

๕.๔ ผลกระทบของภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงแห่งชาติรวมถึงแนวโน้มในอนาคตในความคิดเห็นของหน่วยงานภาคเอกชน หน่วยงานพลเรือน และภาคประชาชน สามารถสรุปได้ว่ามีผลกระทบที่ปรากฏดังนี้

๕.๔.๑ มาตรการป้องกันและแก้ไขของเจ้าหน้าที่รัฐยังไม่เหมาะสม ดังเช่นเมื่อผู้ต้องหาส่วนมากที่เป็นผู้ปลุกปั่นและบิดเบือนข่าวสารในสังคมออนไลน์ แต่เจ้าหน้าที่ไม่มีเครื่องมือในการหาหลักฐานอย่างเช่นการตรวจ IP Address เป็นต้น

๕.๔.๒ ปัญหานี้ส่งผลกระทบต่อจิตใจของประชาชนอย่างหลีกเลี่ยงไม่ได้เนื่องจากภัยคุกคามด้านไซเบอร์จะสามารถนำไปสู่ชนวนแห่งการสร้างสถานการณ์รุนแรงได้อยู่เสมอ ดังนั้นควรใช้ยุทธศาสตร์ชาติในการแก้ไขปัญหาอย่างเป็นระบบ

๕.๒ แนวโน้มในอนาคตของภัยคุกคามด้านไซเบอร์ มีประเด็นดังต่อไปนี้

๕.๒.๑ แนวโน้มในอนาคตของภัยคุกคามด้านไซเบอร์ทั้งด้านทักษะและทรัพยากร คือองค์ประกอบ ๒ อย่างที่ผู้โจมตีใช้สร้างอาวุธ แต่ผู้โจมตีจะไม่มีวันเจาะผ่านระบบความปลอดภัยหรือทำการโจมตีที่ซับซ้อนได้หากไม่ค้นพบจุดอ่อนในระบบตั้งแต่แรก การโจมตีด้วยมัลแวร์จำนวนมาก กลโกงทางอีเมล์ การเจาะระบบอุปกรณ์ และการสร้างความเสียหายให้กับบริการ ทั้งหมดนี้ล้วนอาศัยช่องโหว่ของเครือข่าย ไม่ว่าจะเป็นจากเทคโนโลยีหรือบุคลากร เพื่อให้บรรลุภารกิจดังกล่าวมีหลายตัวอย่างที่ทราบกันดี เช่น การเชื่อมต่อและการมีปฏิสัมพันธ์ที่เพิ่มมากขึ้นในเครือข่ายที่ไม่ปลอดภัย แต่โชคร้ายที่การนำเทคโนโลยีที่ไม่สมบูรณ์ไปใช้ยิ่งเพิ่มโอกาสของการเกิดภัยคุกคามเพิ่มมากขึ้น การป้องกันในจุดที่จำเป็นและในเวลาที่จำเป็นจึงกลายเป็นเสาหลักของการรักษาความปลอดภัยในโลกที่ภัยคุกคามมีการเปลี่ยนแปลงอยู่ตลอดเวลา ในปี พ.ศ.๒๕๖๑ การขู่กรรโชกทางดิจิทัลจะเป็นโมเดลธุรกิจหลักของอาชญากรคอมพิวเตอร์ส่วนใหญ่ และเป็นแรงผลักดันให้เกิดอุบายอื่นๆ ที่จะหลอกลวงเหยื่อกระเป๋าหนักตามมา ขณะที่ช่องโหว่ในอุปกรณ์ IoT จะเริ่มขยายพื้นที่ของการโจมตีอย่างเห็นได้ชัด เนื่องจากอุปกรณ์เหล่านี้จะเชื่อมต่อถึงกันมากยิ่งขึ้นจนเป็นสภาพแวดล้อมแบบอัจฉริยะในทุกแห่งหน อุบายหลอกลวงทางอีเมล์ธุรกิจจะดักเหยื่อที่เป็นองค์กรมากขึ้นเพื่อหลอกเอาเงิน ยุคสมัยของข่าวปลอมและการโฆษณาชวนเชื่อทางอินเทอร์เน็ต จะยังคงดำเนินต่อไปด้วยลูกไม้เก่าๆ ของอาชญากรคอมพิวเตอร์

๕.๒.๒ การเรียนรู้ของเครื่องจักร (Machine Learning) และแอพพลิเคชั่นด้านบล็อกเชนจะให้ทั้งความหวังและเป็นหลุมพรางอันตราย บริษัทต่างๆ จะต้องเผชิญกับความท้าทาย

ในการปรับตัวให้ทันกับการบังคับใช้กฎหมายการปกป้องข้อมูลทั่วไป (GDPR) ไม่เพียงแต่องค์กรจะเต็มไปด้วยจุดอ่อนเท่านั้น แต่ช่องโหว่ในกระบวนการภายในจะถูกใช้เป็นเครื่องมือเพื่อบ่อนทำลายการผลิตด้วยเช่นกัน สิ่งเหล่านี้คือภัยคุกคามที่เข้ามามีบทบาทในปีนี้ และภัยคุกคามเหล่านี้จะเป็นข้อพิสูจน์ว่าโซลูชั่นความปลอดภัยแบบเดิมๆ ล้าสมัยเกินกว่าที่จะระบุและตรวจจับภัยคุกคามได้เมื่อสภาพแวดล้อมเริ่มเชื่อมต่อถึงกันมากขึ้นและซับซ้อนยิ่งขึ้น มุมมองของเราที่มีต่อภัยคุกคามจึงเปลี่ยนรูปแบบไปจากเดิมอย่างมาก โมเดลธุรกิจของซอฟต์แวร์เรียกค่าไถ่หรือแรนซัมแวร์ยังคงเป็นอาชญากรรมทางคอมพิวเตอร์ที่พบ ขณะที่การขู่กรรโชกทางดิจิทัลในรูปแบบอื่นๆ จะบรรลุผลสำเร็จมากยิ่งขึ้น

๕.๒.๓ เมื่อปี พ.ศ.๒๕๖๐ อาชญากรคอมพิวเตอร์จะพัฒนาซอฟต์แวร์เรียกค่าไถ่ไปสู่การโจมตีแบบอื่นๆ ซึ่งก็เกิดขึ้นจริง เพราะปีดังกล่าวเริ่มด้วยเหตุการณ์การโจมตีของ WannaCry และ Petya ซึ่งแพร่กระจายในเครือข่ายอย่างรวดเร็ว ตามด้วยสแปม Locky และ FakeGlobe จากนั้นก็เป็น Bad Rabbit ซึ่งเปิดฉากการโจมตีประเทศในยุโรปตะวันออก โดยคาดว่าภัยคุกคามของซอฟต์แวร์เรียกค่าไถ่จะไม่จางหายไปในเร็ววัน แต่ในทางตรงกันข้ามคาดกันว่าภัยดังกล่าวจะกลับมาอีกครั้งในไม่ช้า แม้ว่าจะเริ่มตรวจพบการขู่กรรโชกทางดิจิทัลในรูปแบบอื่นๆ มากขึ้นก็ตาม อาชญากรคอมพิวเตอร์จะพยายามทำทุกวิถีทางเพื่อใช้ข้อมูลสำคัญเป็นอาวุธในการบีบบังคับให้เหยื่อยอมจ่ายเงิน ด้วยการเสนอซอฟต์แวร์เรียกค่าไถ่ในฐานะบริการ (RaaS) ตามฟอรัมสนทนาใต้ดินโดยใช้บิตคอยน์ซึ่งปลอดภัยในการเก็บค่าไถ่ ซึ่งส่งผลให้อาชญากรคอมพิวเตอร์จะเริ่มเข้าสู่โมเดลธุรกิจมากยิ่งขึ้น

๕.๒.๔ หากพัฒนาการทางกลยุทธ์ของอาชญากรคอมพิวเตอร์ตลอดหลายปีที่ผ่านมาคือตัวบ่งชี้ ก็คงสรุปได้ว่าอาชญากรคอมพิวเตอร์กำลังพุ่งเป้าโดยตรงไปที่ “เงิน” แทนที่จะเป็นการลวงผู้ใช้เพื่อเอาข้อมูลประจำตัว ซึ่งภัยคุกคามทางออนไลน์ในยุคแรกๆ จะเน้นไปที่ซอฟต์แวร์ขโมยข้อมูลและมัลแวร์ที่เข้าควบคุมธุรกรรมของธนาคารเพื่อขโมยข้อมูลส่วนตัว และในเวลาต่อมาภัยคุกคามประเภทนี้ได้เปลี่ยนไปเป็นโซลูชั่นหลอกลวงที่แสร้งว่าเป็นโปรแกรมต้านมัลแวร์ (FAKEAV) เพื่อลวงผู้ใช้ในดาวน์โหลดซอฟต์แวร์ดังกล่าวและต้องยอมจ่ายเงิน เพื่อให้สามารถเข้าถึงคอมพิวเตอร์ที่ตกเป็นเหยื่อได้อีกครั้ง นับแต่บัดนั้นซอฟต์แวร์เรียกค่าไถ่ก็ได้ยึดหัวหาดนี้ต่อด้วยการเลียนแบบพฤติกรรมของ FAKEAV ความสำเร็จของการรุกรานโดยซอฟต์แวร์เรียกค่าไถ่ในปัจจุบัน โดยเฉพาะเรื่องการขู่กรรโชกได้จุดประกายให้อาชญากรคอมพิวเตอร์มองหาช่องทางทำกำไรจากเป้าหมายที่กระหายผลตอบแทนสูงสุด ผู้โจมตียังคงอาศัยการหลอกลวงด้วยวิธีฟิชชิงที่ส่งอีเมลแฝงซอฟต์แวร์เรียกค่าไถ่ให้คนจำนวนมาก เพื่อให้แน่ใจว่าจะมีคนบางส่วนที่โดนหลอก ในขณะเดียวกันผู้โจมตียังหวังลาภก้อนใหญ่โดยพุ่งเป้าไปที่เหยื่อระดับองค์กร ซึ่งอาจใช้

อุปกรณ์ที่เชื่อมต่ออินเตอร์เน็ตระดับอุตสาหกรรม (Industrial Internet of Things - IIoT) เพราะการโจมตีด้วยซอฟต์แวร์เรียกค่าไถ่จะทำให้การปฏิบัติงานหยุดชะงัก และส่งผลต่อสายการผลิต เราได้เห็นความเสียหายนี้แล้วจากการแพร่ระบาดของ WannaCry และ Petya และอีกไม่ช้าการโจมตีนั้นจะกลายเป็นเจตนาหลักของภัยคุกคาม การขู่กรรโชกจะเริ่มมีบทบาทมากขึ้นเมื่อ GDPR ประกาศใช้ อาชญากรคอมพิวเตอร์อาจพุ่งเข้าไปที่ข้อมูลส่วนบุคคลที่คุ้มครองโดยกฎหมาย และกรรโชกทรัพย์จากบริษัทเพื่อแลกกับการที่บริษัทต้องเสี่ยงถูกปรับตามกฎหมายสูงถึง ๔ เปอร์เซ็นต์ของรายได้ประจำปี ซึ่งอาชญากรคอมพิวเตอร์สามารถกำหนดราคาค่าไถ่ได้ โดยดูจากข้อมูลทางการเงินของบริษัทที่เปิดเผยต่อสาธารณะแล้วคำนวณค่าปรับ GDPR สูงสุดเท่าที่บริษัทเหล่านั้นต้องโดน ข้อมูลนี้จะยิ่งผลักดันให้เกิดความพยายามเจาะระบบและเรียกร้องค่าไถ่มากขึ้น ยิ่งไปกว่านั้นคาดการณ์ว่า GDPR จะถูกใช้เป็นกลยุทธ์ในการหลอกลวงในแบบเดียวกับที่การละเมิดลิขสิทธิ์และใบสั่งของเจ้าหน้าที่ตำรวจถูกใช้เพื่อเผยแพร่ FAKEAV และซอฟต์แวร์เรียกค่าไถ่ ผู้ใช้และองค์กรสามารถรับมือกับการขู่กรรโชกทางดิจิทัลเหล่านี้ได้โดยใช้โซลูชั่นเกตเวย์สำหรับเว็บและอีเมล์เพื่อเป็นปราการป้องกันด่านแรก โซลูชั่นที่อาศัยการเรียนรู้ของเครื่องจักรที่แม่นยำสูง การติดตามพฤติกรรมและการอุดช่องโหว่จะช่วยป้องกันไม่ให้ภัยคุกคามบรรลุเป้าหมาย ความสามารถเหล่านี้เป็นประโยชน์อย่างยิ่งโดยเฉพาะในกรณีของซอฟต์แวร์เรียกค่าไถ่สายพันธุ์ต่างๆ ที่เริ่มหันไปส่งแบบไม่มีไฟล์ ซึ่งทำให้ไม่มีเนื้อหาอันตรายหรือไม่มีไฟล์ไบนารีให้โซลูชั่นแบบเดิมๆ ตรวจพบได้

๕.๒.๕ อาชญากรคอมพิวเตอร์จะสำรวจวิธีใหม่ๆ เพื่อใช้อุปกรณ์ IoT สร้างประโยชน์ให้กับตนเอง การโจมตีที่ใช้เทคนิคของ DoS ในแบบกระจาย (Distributed Denial of Service : DDoS) จำนวนมากโดย Mirai และ Persirai ซึ่งเข้าไปควบคุมอุปกรณ์ IoT เช่น เครื่องบันทึกวิดีโอแบบดิจิทัล (DVR) กล้อง IP และเราเตอร์ ได้ยกระดับของถกเถียงไปสู่ประเด็นที่ว่าอุปกรณ์ที่เชื่อมต่อกันเหล่านี้มีช่องโหว่และสร้างความเสียหายได้อย่างไรบ้าง เมื่อเร็วๆ นี้มีการค้นพบบ็อทเน็ตบน IoT ชื่อ Reaper ซึ่งอาศัยรหัสของ Mirai ซึ่งนิยมใช้เพื่อเจาะเว็บของอุปกรณ์ ซึ่งทำได้แม้กระทั่งจากอุปกรณ์ต่างผู้ผลิตกัน โดยคาดว่านอกจากทำเพื่อโจมตี DDoS แล้ว อาชญากรคอมพิวเตอร์จะหันไปใช้อุปกรณ์ IoT เพื่อสร้างพร็อกซีสำหรับอำพรางตำแหน่งที่อยู่และการรับส่งข้อมูลของเว็บ โดยมองว่าหน่วยงานที่บังคับใช้กฎหมายมักอ้างอิงที่อยู่ IP และบันทึกกิจกรรม เพื่อสืบสวนอาชญากรรม และวิเคราะห์ทางนิติเวชหลังถูกโจมตี การรวบรวมเครือข่ายของอุปกรณ์ที่ไม่ระบุชื่อ (ซึ่งทำงานด้วยข้อมูลประจำตัวตามค่าเริ่มต้นและแทบไม่มีการเก็บบันทึกกิจกรรมเลย) สามารถใช้เป็นจุดหลบหนีสำหรับอาชญากรคอมพิวเตอร์ที่ทำงานอย่างลับๆ ในเครือข่ายที่มีช่องโหว่ และเรายังคาดด้วยว่าจะมีช่องโหว่ของ IoT เพิ่มมากขึ้นเนื่องจากมีผู้ผลิตจำนวนมากกำลังวางตลาดอุปกรณ์ที่ไม่ได้ออกแบบมาเพื่อความปลอดภัยตั้งแต่แรก ความเสี่ยงนี้จะยิ่งทวีเพิ่มขึ้นด้วย

ข้อเท็จจริงที่ว่าการแก้ไขระบบในอุปกรณ์ IoT ไม่ได้ง่ายเหมือนในคอมพิวเตอร์ส่วนบุคคล เพราะแค่อุปกรณ์ที่ไม่ปลอดภัยเพียงตัวเดียวที่ยังไม่มีโปรแกรมแก้ไข หรือยังไม่ได้อัพเดตเป็นเวอร์ชันล่าสุด ก็สามารถเป็นช่องทางเข้าสู่เครือข่ายส่วนกลางได้แล้ว การโจมตีด้วย KRACK ได้พิสูจน์แล้วว่าแม้แต่ในการเชื่อมต่อแบบไร้สายเองก็เกิดปัญหาด้านความปลอดภัยได้ ช่องโหว่นี้กระทบกับอุปกรณ์ส่วนใหญ่ที่เชื่อมต่อด้วยโปรโตคอล WPA2 ซึ่งทำให้เกิดคำถามต่อความปลอดภัยของเทคโนโลยี 5G ที่คาดว่าจะครอบคลุมระบบทั้งหมดที่มีการเชื่อมต่อ

๕.๒.๖ อุปกรณ์ที่เป็นเป้าหมายของการทำลายล้างและอาชญากรรมคอมพิวเตอร์ด้วยโดรนนับแสนเครื่องที่เข้าสู่น่านฟ้าของสหรัฐอเมริกา การควบคุมดูแลพาหนะทางอากาศจึงเป็นเรื่องน่ากังวลยิ่ง โดยราคาดว่าการรายงานอุบัติเหตุเกี่ยวกับโดรนหรือการชนกันจะเป็นแค่จุดเริ่มต้น เมื่อแฮกเกอร์พบวิธีเข้าถึงคอมพิวเตอร์ ขโมยข้อมูลสำคัญ และเข้ายึดการขนส่งสินค้าผ่านโดรน ในอุปกรณ์ตามบ้านก็เช่นเดียวกัน ไม่ว่าจะเป็นลำโพงไร้สายหรือผู้ช่วยแบบสั่งด้วยเสียงก็อาจทำให้แฮกเกอร์รู้ตำแหน่งที่อยู่ของบ้านเพื่อจัดแจะได้

๕.๒.๗ คาดการณ์ว่าในปี พ.ศ.๒๕๖๑ จะเกิดคดีเกี่ยวกับการจารกรรมข้อมูลชีวภาพผ่านทางอุปกรณ์สวมใส่และอุปกรณ์ทางการเพทย์ อุปกรณ์บันทึกชีวมาตร เช่น เครื่องติดตามการเต้นของหัวใจและสายรัดบันทึกการออกกำลังกาย อาจถูกดักจับข้อมูลเกี่ยวกับผู้ใช้ แม้แต่อุปกรณ์ช่วยชีวิตอย่างเครื่องกระตุ้นหัวใจก็ยังพบว่ามีช่องโหว่ที่อาจถูกใช้เพื่อทำร้ายถึงชีวิต สิ่งที่ผู้ใช้เทคโนโลยีและผู้ออกกฎระเบียบควรรับทราบในปัจจุบันก็คือ อุปกรณ์ IoT ทั้งหลายไม่ได้มีสร้างมาพร้อมกับระบบรักษาความปลอดภัย เรื่องความปลอดภัยที่แข็งแกร่งยิ่งไม่ต้องพูดถึง อุปกรณ์เหล่านี้เปิดช่องให้ถูกโจมตี เว้นแต่ผู้ผลิตจะประเมินความเสี่ยงและหมั่นตรวจสอบความปลอดภัยอยู่เป็นนิจ ผู้ใช้ยังต้องรับผิดชอบต่อการตั้งค่าอุปกรณ์ของตนเองเพื่อความปลอดภัย ซึ่งอาจทำได้ง่ายๆ เพียงแค่เปลี่ยนรหัสผ่านเริ่มต้นและอัพเดตเฟิร์มแวร์อยู่เสมอ

๕.๒.๘ ในการปฏิบัติงานและแพลตฟอร์มต่างๆ ขององค์กรเสี่ยงจะได้รับการก่อกวนและเกิดช่องโหว่ จากสภาพการณ์ทุกวันนี้ที่อุตสาหกรรม ๔.๐ ทำให้ระบบกายภาพไซเบอร์และกระบวนการผลิตเชื่อมต่อถึงกันและทำงานเองได้ด้วยซอฟต์แวร์มากขึ้น แต่ความเสี่ยงต่างๆ กลับเริ่มต้นจากบางสิ่งบางอย่างภายในระบบเอง แนวคิดการมี “ฝาแฝดดิจิทัล” ซึ่งก็คือสิ่งจำลองเสมือนหรือการจำลองการผลิตหรือกระบวนการในโลกแห่งความเป็นจริง ได้เปิดช่องให้องค์กรต่างๆ แก้ปัญหาการดำเนินงานที่อาจเกิดขึ้นกับสินทรัพย์ที่จับต้องได้ แต่เราเชื่อว่า แม้ควรมีการปฏิรูปการดำเนินงานต่างๆ ผู้คุกคามที่ต้องการก่อกวนระบบ หยุด และความเสียหายให้การดำเนินงานก็อาจแทรกซึมเข้ามายังเครือข่ายการผลิตเช่นกัน และด้วยการก่อกวนฝาแฝดดิจิทัลนี้เองทำให้ผู้คุกคามเหล่านี้สามารถสร้างกระบวนการผลิตที่ดูเหมือนปกติทั้งๆ ที่ปรับแต่งแล้ว

นอกจากนี้ ข้อมูลการผลิตที่มีการส่งผ่านระบบปฏิบัติการการผลิต (MES) โดยตรง (หรือโดยอ้อม) ไปยัง SAP หรือระบบการวางแผนทรัพยากรองค์กร (ERP) อื่นๆ ก็ตกอยู่ในอันตรายจากการโจมตีระบบ หากข้อมูลส่วนใดที่ถูกปลอมแปลงหรือมีคำสั่งที่ไม่ถูกต้องถูกส่งไปยังระบบ ERP แล้ว เครื่องจักรอาจก่อกระบวนการสร้างความเสียหายจากการตัดสินใจที่ผิดพลาด เช่น การขนส่งสินค้าไปยังปลายทางด้วยจำนวนที่ไม่ถูกต้อง โอนเงินโดยไม่ได้ตั้งใจ หรือแม้แต่ทำให้ระบบทำงานหนักเกิน ระบบต่างๆ ขององค์กรไม่ได้เป็นระบบเดียวที่ตกเป็นเป้าหมายโจมตี และในปีนี้คาดว่าจะยังคงเห็นข้อบกพร่องด้านความปลอดภัยในแพลตฟอร์มของ Adobe และ Microsoft แต่สิ่งที่น่าสนใจเป็นอย่างยิ่ง คือการหันมาเน้นช่องโหว่ที่เกิดขึ้นจากเบราว์เซอร์และในฝั่งเซิร์ฟเวอร์อีกครั้ง ทั้งนี้นับว่าเป็นเวลานานหลายปีแล้วที่ช่องโหว่ของโปรแกรมเสริมชื่อดังในเบราว์เซอร์ เช่น Adobe Flash Player, Microsoft Java และ Silverlight กลายเป็นเป้าการโจมตี แต่คาดว่าในปีนี้ความอ่อนแอในกลไกต่างๆ ที่เป็นประเภทจาวาสคริปต์จะส่งผลเสียต่อเบราว์เซอร์รุ่นใหม่เป็นหลัก เริ่มตั้งแต่ปัญหาการหยุดทำงานเองของกลไกจาวาสคริปต์แบบโอเพ่นซอร์ส ชื่อ V8 ของ Google Chrome ไปจนถึง Open Sources ชื่อ Chakra ของ Microsoft Edge โดยช่องโหว่ในเบราว์เซอร์ที่มีจาวาสคริปต์เป็นพื้นฐานจะยิ่งเห็นได้ชัดเจนขึ้นจากการใช้สคริปต์เหล่านี้อย่างแพร่หลายในเว็บไซต์

๕.๒.๔ ผู้โจมตีจะเน้นการใช้ช่องโหว่ที่เกิดขึ้นในฝั่งเซิร์ฟเวอร์อีกครั้งเพื่อส่งข้อมูลไปยังคอมพิวเตอร์เป็นปริมาณมากจนก่อให้เกิดอันตราย โดยคาดว่าจะมีการโจมตีโดยใช้ช่องโหว่จาก Server Message Block (SMB) และ Samba เพื่อแพร่กระจายซอฟต์แวร์เรียกค่าไถ่มากขึ้น โดยช่องโหว่ของ SMB สามารถถูกโจมตีได้โดยไม่ต้องการการปฏิสัมพันธ์จากผู้ใช้งาน ที่จริงแล้วมีการใช้ประโยชน์จากช่องโหว่ของ SMB ระหว่างการโจมตี EternalBlue ที่ทำลายเครือข่ายจำนวนมากซึ่งทำงานบนระบบปฏิบัติการ Windows ระหว่างการโจมตีด้วยซอฟต์แวร์เรียกค่าไถ่ WannaCry และ Petya และที่ใหม่กว่านั้นก็คือในการโจมตี Bad Rabbit ที่ใช้ประโยชน์จาก EternalRomance เช่นเดียวกัน ขณะที่ Samba (โอเพ่นซอร์ส) บนระบบปฏิบัติการ Linux ก็อาจนำมาหาประโยชน์จากช่องโหว่ที่อยู่ในโปรโตคอล SMB ได้ การโจมตีกระบวนการผลิตผ่าน SAP และ ERP เท่ากับว่าองค์กรจำเป็นต้องถือความปลอดภัยของการปฏิบัติงานที่เกี่ยวข้องเป็นสิ่งสำคัญอันดับต้น การเข้าถึงการปฏิบัติงานนี้ได้จำเป็นต้องได้รับการจัดการและตรวจตราเสมอเพื่อเลี่ยงการเข้าถึงที่ไม่ได้รับอนุญาต โดยปกติแล้วผู้ใช้งานและองค์กรได้รับคำแนะนำให้ตรวจสอบการปรับปรุงซอฟต์แวร์เป็นประจำ และนำซอฟต์แวร์อัพเดตมาใช้เมื่อมีให้ปรับปรุง แต่เนื่องจากผู้ดูแลระบบอาจไม่ได้ปรับปรุงระบบให้ทันสมัยอย่างทันท่วงที เราจึงแนะนำให้นำระบบปกป้องช่องโหว่มาใช้งานเข้ากับระบบต่างๆ เพื่อให้แพลตฟอร์มเหล่านั้นได้รับการป้องกันจากช่องโหว่ที่ยังไม่ได้อุดหรือที่ยังหาไม่พบ โซลูชั่นเครือข่ายเองก็ควรปกป้องอุปกรณ์ที่เชื่อมต่อกับเครือข่ายจากการบุกรุก

เข้ามายังระบบที่อาจเกิดขึ้น ผ่านการอุดช่องโหว่เสมือนและการตรวจตราเชิงรุกต่อการเคลื่อนที่ของข้อมูลในเว็บไซต์

๕.๒ การจัดการความปลอดภัยปี พ.ศ.๒๕๖๑

ภัยคุกคามที่มีอยู่มากมายหลายชนิดทำให้สภาพในปัจจุบันมีความเสี่ยงและคาดว่าจะเผชิญต่อภัยร้ายในปี พ.ศ.๒๕๖๑ ตั้งแต่ช่องโหว่ของระบบ ซอฟต์แวร์เรียกค่าไถ่ และการโจมตีที่เป้าหมายเฉพาะ สิ่งที่ทั้งองค์กรและผู้ใช้งานทำได้มากที่สุด คือการลดความเสี่ยงไม่ให้ความปลอดภัยลดลงในทุกชั้นของระบบ การมองเห็นภัยคุกคามที่ดีขึ้นและการรักษาความปลอดภัยแบบหลายชั้นสำหรับองค์กร การต่อสู้กับภัยที่มีจำนวนมากขึ้นในทุกวันนี้และการป้องกันภัยดังกล่าวที่ยังมาไม่ถึงนั้น องค์กรต่างๆ ควรนำโซลูชั่นด้านความปลอดภัยที่สามารถมองเห็นภัยคุกคามได้ทั่วเครือข่าย และสามารถให้การป้องกันและปกป้องช่องโหว่และการโจมตีในแบบเรียลไทม์ ทั้งยังต้องเลี่ยงไม่ให้เกิดการบุกรุกใดๆ ในอนาคตและการละเลยปกป้องข้อมูลหรือสินทรัพย์โดยใช้วิธีรักษาปลอดภัยที่เปลี่ยนแปลงตามกาลเวลาอยู่เสมอ ซึ่งวิธีการเหล่านี้จะต้องรองรับการรักษาความปลอดภัยทั้งในรูปแบบเดิม และแบบใหม่ได้เพื่อให้เหมาะกับภัยคุกคามที่มีอยู่อย่างหลากหลาย สำหรับเทคโนโลยีรักษาความปลอดภัยดังกล่าว มีดังนี้

(๑) การสแกนแบบเรียลไทม์ การสแกนที่ทำงานอัตโนมัติตลอดเวลาจะช่วยให้สามารถตรวจพบมัลแวร์ที่มีฤทธิ์รุนแรงและเพิ่มประสิทธิภาพการทำงานของอุปกรณ์ให้ดียิ่งขึ้นได้

(๒) การตรวจสอบความน่าเชื่อถือของเว็บไซต์และไฟล์ การตรวจจับมัลแวร์และการป้องกันผ่านการตรวจสอบความน่าเชื่อถือของเว็บไซต์ เทคนิคการต่อต้านสแปม และการควบคุมแอพพลิเคชั่น ช่วยปกป้องผู้ใช้งานจากการโจมตีด้วยซอฟต์แวร์เรียกค่าไถ่และการหาประโยชน์ในทางที่ผิดได้

(๓) การวิเคราะห์พฤติกรรม ต้องมีการตรวจจับและกีดกันมัลแวร์และเทคนิคต่างๆ ที่ทันสมัยที่สามารถเอาชนะการรักษาความปลอดภัยแบบเดิมได้

(๔) แมชีนเลิร์นนิ่งที่มีความเที่ยงตรงสูง การป้อนข้อมูลเข้าสู่ระบบด้วยมนุษย์พร้อมการเพิ่มข้อมูลด้านการเรียน รู้ต่อภัยคุกคาม เปิดทางให้มีการตรวจจับที่รวดเร็วและรักษาความปลอดภัยที่แม่นยำต่อภัยทั้งที่เรารู้จักและยังไม่รู้จัก

(๕) การรักษาความปลอดภัยที่อุปกรณ์ปลายทาง คือการรักษาความปลอดภัยที่นำคุณสมบัติแซนด์บ็อกซิ่ง การตรวจหาช่องโหว่ และความสามารถต่างๆ จากเซ็นเซอร์ที่อุปกรณ์ปลายทางมาใช้ จะช่วยตรวจจับกิจกรรมที่น่าสงสัยและป้องกันการโจมตี การเคลื่อนไหวแบบลับๆ ภายในเครือข่ายได้

กล่าวโดยสรุป การศึกษาวิจัยเพื่อหายุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ตามข้อมูลที่ปรากฏสามารถนำไปวิเคราะห์และสังเคราะห์เพื่อกำหนดรูปแบบการจัดการกับภัยคุกคามด้านไซเบอร์ ข้อมูลที่กล่าวมาทั้งหมดสามารถยืนยันได้ว่าภัยคุกคามด้านไซเบอร์เป็นภัยที่ก่อให้เกิดความเสียหายร้ายแรงกับประเทศชาติ โดยถือเป็นภัยคุกคามใหญ่หลวงต่อผลประโยชน์ทางเศรษฐกิจ สังคม ตลอดจนความมั่นคงของชาติ (สราวุธ ปิติยาศักดิ์, ๒๕๖๐) ดังนั้นการศึกษาให้เห็นถึงคุณลักษณะของภัยคุกคามนี้อย่างถ่องแท่ย่อมเป็นผลดีต่อการพัฒนายุทธศาสตร์ในการบริหารจัดการให้มีประสิทธิภาพ รวมถึงเกิดประโยชน์ต่อประเทศชาติในการรักษาผลประโยชน์และความมั่นคงแห่งชาติในภาพรวมอีกด้วย

สรุป

การวิจัยเพื่อหายุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ โดยมีเอกสาร งานวิจัยที่เกี่ยวข้อง และผลจากการศึกษาเบื้องต้น ได้แก่ รูปแบบภัยคุกคามด้านไซเบอร์ที่ปรากฏทั่วโลกในอดีตจนถึงปัจจุบัน สถานการณ์และรูปแบบภัยคุกคามด้านไซเบอร์ในประเทศไทย และรูปแบบภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงและความไม่สงบในพื้นที่จังหวัดชายแดนภาคใต้ของประเทศไทย ตามลำดับ

บทนี้นำเสนอข้อมูลรวมถึงบทวิเคราะห์จากการศึกษาและค้นคว้าเอกสารเกี่ยวกับรูปแบบภัยคุกคามด้านไซเบอร์ที่ปรากฏทั่วโลกในอดีตจนถึงปัจจุบัน รูปแบบภัยคุกคามด้านไซเบอร์ที่ปรากฏในประเทศไทย และรูปแบบภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงและความไม่สงบในพื้นที่จังหวัดชายแดนภาคใต้ ซึ่งสามารถสรุปได้ว่า สถานการณ์และการเปลี่ยนแปลงของโลกอย่างรวดเร็วในปัจจุบันส่งผลต่อความมั่นคงของนานาประเทศในหลายมิติรวมทั้งประเทศไทย มีสิ่งบ่งชี้ว่าความมั่นคงของชาติได้รับผลกระทบจากไซเบอร์ในหลายระดับตั้งแต่รูปแบบที่มีผลกระทบต่อการใช้ชีวิตประจำวันของประชาชน ความน่าเชื่อถือทางเศรษฐกิจสังคมการเมือง การละเมิดสถาบัน รวมไปถึงสภาวะแวดล้อมรอบตัว คุณลักษณะสำคัญประการหนึ่งของไซเบอร์ก็คือสามารถแพร่กระจายอย่างรวดเร็วและไร้ซึ่งพรมแดน จึงนับเป็นภัยที่สามารถเกิดขึ้นได้ในทุกภูมิภาคทั่วโลก ประเทศไทยจึงต้องเตรียมการและใช้ศักยภาพด้านไซเบอร์ให้เป็นไปอย่างสอดคล้องกับสถานการณ์ระดับประเทศ ระดับภูมิภาค และในระดับโลกเพื่อให้ภัยคุกคามนี้ส่งผลต่อการดำเนินงานของหน่วยงานและองค์กรต่างๆ รวมถึงความเป็นอยู่ของประชาชนคนไทยให้น้อยที่สุด บทนี้นำเสนอรูปแบบและวิธีการภัยคุกคามด้านไซเบอร์ทั้งในและต่างประเทศ โดยเฉพาะอย่างยิ่งในพื้นที่จังหวัดชายแดนภาคใต้ที่มีรูปแบบการใช้งานด้านไซเบอร์ที่ส่งผลกระทบต่อความมั่นคงของชาติอย่างแท้จริง ส่วนการกำหนดประเด็นยุทธศาสตร์ในการจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้จะกล่าวถึงในบทที่ ๔ ต่อไป

บทที่ ๔
วิเคราะห์ผลกระทบและกำหนดยุทธศาสตร์ในการจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

การวิจัยเรื่อง “ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้” บทนี้เป็นการวิเคราะห์และสังเคราะห์เพื่อตอบวัตถุประสงค์ข้อที่ ๓ เพื่อกำหนดยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้โดยมีลำดับการศึกษาวิจัยดังนี้

๑. การวิเคราะห์ผลกระทบของภัยคุกคามด้านไซเบอร์

๒. แนวทางการจัดการภัยคุกคามด้านไซเบอร์ของต่างประเทศ

๓. การวิเคราะห์รูปแบบที่เหมาะสมของการจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

๔. การวิเคราะห์ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

๕. สรุป

การวิเคราะห์ผลกระทบของภัยคุกคามด้านไซเบอร์

ผลกระทบของภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงแห่งชาติรวมถึงแนวโน้มในอนาคตดังที่กล่าวมาแล้วในบทที่ ๓ สามารถนำมาศึกษาวิเคราะห์ได้ดังนี้

๑. ผลกระทบของภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงแห่งชาติรวมถึงแนวโน้มในอนาคตจากความคิดเห็นของหน่วยงานด้านความมั่นคงของรัฐ สามารถวิเคราะห์ได้ดังนี้

๑.๑ การสร้างทัศนคติเชิงลบต่อรัฐให้กับประชาชนส่งผลต่อความมั่นคงแห่งชาติและถือเป็นภัยคุกคามสำคัญที่อาจจะสร้างสถานการณ์ให้บานปลายได้ ถ้ารัฐบาลไม่มีการกำหนดยุทธศาสตร์หรือวิธีการแก้ไขในระดับปฏิบัติการอย่างจริงจัง

๑.๒ ผลกระทบต่อความมั่นคงแห่งชาติจะทำให้เกิดความแตกแยกของผู้คนทั้งทางด้านเชื้อชาติและศาสนา เพราะปัจจุบันโลกไซเบอร์มีอานุภาพในการเข้าถึงสังคมพหุวัฒนธรรมในพื้นที่จังหวัดชายแดนภาคใต้ได้อย่างรวดเร็วและไม่มีข้อกำหนด

๑.๓ แนวโน้มในอนาคตของภัยคุกคามด้านไซเบอร์จะยังคงเป็นปัญหาหลักที่รัฐบาลต้องดำเนินการอย่างเป็นระบบ ดังนั้นการกำหนดนโยบายแห่งชาติถือเป็นเรื่องสำคัญประการหลักที่มีต่ออนาคตของภัยคุกคามนี้

๑.๔ ปัญหาเรื่องภัยคุกคามด้านไซเบอร์ในประเทศไทยอาจกลายเป็นชนวนที่ก่อให้เกิดปัญหาระหว่างประเทศในอนาคตได้ ถ้าไม่มีกระบวนการแก้ไขอย่างเป็นรูปธรรมโดยความเห็นชอบสากล

๒. ผลกระทบของภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงแห่งชาติรวมถึงแนวโน้มในอนาคตจากความคิดเห็นของเจ้าหน้าที่ระดับปฏิบัติการด้านความมั่นคงรวมถึงเจ้าหน้าที่ทหารที่รับผิดชอบด้านภัยคุกคามของสำนักปฏิบัติการข่าวสาร สามารถวิเคราะห์ได้ดังนี้

๒.๑ การนำประเด็นชาติพันธุ์และศาสนาเข้ามาเพื่อการสร้างข่าวบิดเบือนและเผยแพร่สู่เครือข่ายสังคมออนไลน์ อาจส่งผลให้เกิดความแตกแยกขึ้นในสังคมทุกระดับชั้นโดยจะทำให้สังคมนั้นอยู่ร่วมกันโดยไม่มีความสงบสุขได้เลย

๒.๒ ในโลกไซเบอร์และเครือข่ายสังคมออนไลน์มีการนำประเด็นในอดีตทั้งประวัติศาสตร์ที่จริงและบิดเบือนมาใช้เป็นเงื่อนไขสร้างสถานการณ์ให้ทวีความรุนแรงขึ้น การอาศัยรูปแบบและวิธีการดังกล่าวเท่ากับเป็นการสร้างความคิดความเชื่อให้เยาวชนใหม่ ซึ่งจะส่งผลต่ออนาคตของชาติในระยะยาว

๒.๓ ในการใช้งานเครือข่ายสังคมออนไลน์ ถ้าหากมีปัจจัยหรือสถานการณ์ที่น่าจะมีแนวโน้มรุนแรงมากขึ้น ภาครัฐต้องระวังควบคุมการใช้งานอย่างทันท่วงทีเพื่อไม่ให้ผู้ก่อการร้ายนำไปขยายผลไปสู่ความรุนแรงอื่นๆ ได้

๓. ผลกระทบของภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงแห่งชาติรวมถึงแนวโน้มในอนาคตจากความคิดเห็นของนักวิชาการและผู้เชี่ยวชาญด้านระบบไอซีทีซึ่งเป็นเจ้าหน้าที่ด้านความมั่นคง สามารถวิเคราะห์ได้ดังนี้

๓.๑ ในอนาคตถ้าไม่เกี่ยวข้องกับภัยคุกคามด้านไซเบอร์น่าจะมีการเกิดเหตุการณ์รุนแรงน้อยลง เนื่องจากฝ่ายผู้ก่อการร้ายอาจจะมีงบประมาณหรือผู้สนับสนุนน้อยลง อีกทั้งการใช้เครื่องมือและเทคโนโลยีสมัยใหม่เพื่อควบคุมอาจช่วยลดปฏิบัติการของผู้ก่อการได้มากขึ้น

๓.๒ เหตุการณ์ความไม่สงบในพื้นที่มักเกิดจากผลประโยชน์ของคนบางกลุ่มและเจ้าเมืองเก่า โดยมีการปลูกฝังเยาวชนรุ่นใหม่ให้เข้าใจผิดและเกลียดชังต่อรัฐบาลซึ่งอาศัยเครือข่ายสังคมออนไลน์อย่างเป็นด้านหลัก ดังนั้นการออกแบบระบบเพื่อควบคุมการใช้งานก็เป็นเหตุผลประกอบที่รัฐบาลควรดำเนินการในเรื่องนี้ด้วย

๓.๓ มีแนวโน้มเกิดเหตุการณ์การสร้างข่าวสารบิดเบือนผ่านสื่อสังคมออนไลน์จะทวีความรุนแรงมากยิ่งขึ้นเนื่องจากมีการใช้งานโลกไซเบอร์มากขึ้น อีกทั้งมีการดึงต่างประเทศเข้ามาร่วมเพื่อให้มีผู้สนับสนุนให้แยกประเทศโดยทำให้ประเทศไทยมีปัญหาในเวทีโลก ดังนั้นจึงเป็นปัจจัยที่นำมาใช้ในการออกแบบระบบที่มีความปลอดภัยสูงสุด

๓.๔ ปัจจุบันยังมีกระบวนการละเมิดสถาบันพระมหากษัตริย์ผ่านเครือข่ายสังคมออนไลน์อย่างต่อเนื่อง ซึ่งถือว่าเป็นภัยคุกคามด้านความมั่นคงแห่งชาติต่อสถาบันหลักของประเทศ ดังนั้นรัฐบาลควรเร่งปฏิรูปและออกนโยบายต่อการจัดการภัยคุกคามด้านไซเบอร์โดยเร่งด่วนที่สุด

๔. ผลกระทบของภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงแห่งชาติรวมถึงแนวโน้มในอนาคตจากความคิดเห็นของหน่วยงานภาคเอกชน หน่วยงานพลเรือน และภาคประชาชน สามารถวิเคราะห์ได้ดังนี้

๔.๑ มาตรการป้องกันและแก้ไขของเจ้าหน้าที่รัฐยังไม่เหมาะสม ดังนั้นควรออกแบบเครื่องมือและวิธีการที่ทันสมัยเพื่อช่วยในการกำกับและควบคุมการใช้งานเครือข่ายสังคมออนไลน์ในพื้นที่จังหวัดชายแดนภาคใต้เป็นกรณีพิเศษ

๔.๒ เนื่องจากปัญหาภัยคุกคามด้านไซเบอร์จะสามารถนำไปสู่ชนวนแห่งการสร้างสถานการณ์รุนแรงอื่นได้อยู่เสมอ ดังนั้นควรใช้ยุทธศาสตร์ชาติในการแก้ไขปัญหาอย่างเป็นระบบจะสามารถยืนยันถึงการรักษาความสงบสุขในพื้นที่ได้

แนวทางการจัดการภัยคุกคามด้านไซเบอร์ของต่างประเทศ

ดังที่กล่าวมาแล้วในบทที่ ๓ เกี่ยวกับประเด็นของภัยคุกคามด้านไซเบอร์ทั้งรูปแบบภัยคุกคามด้านไซเบอร์ที่ปรากฏทั่วโลกในอดีตจนถึงปัจจุบัน รูปแบบภัยคุกคามด้านไซเบอร์ที่ปรากฏในประเทศไทย และรูปแบบภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงและความไม่สงบในพื้นที่จังหวัดชายแดนภาคใต้ เมื่อนำผลการวิเคราะห์รูปแบบของภัยคุกคามด้านไซเบอร์มาพิจารณาสามารถสรุปเป็นแนวทางการจัดการภัยคุกคามด้านไซเบอร์ของต่างประเทศได้ดังนี้

๑. สหรัฐอเมริกา

โลกไซเบอร์สำหรับชาวอเมริกันต่อชีวิตประจำวันเป็นอย่างมาดังที่ได้กล่าวมาแล้วในบทที่ ๓ สหรัฐอเมริกาถือว่าการบริการในโลกไซเบอร์มีความสำคัญยิ่งต่อผลประโยชน์แห่งชาติของสหรัฐอเมริกา ซึ่งเริ่มเข้าสู่การทำสงครามไซเบอร์อย่างจริงจังในปี ค.ศ.๒๐๑๐ เมื่อจัดตั้งหน่วยบัญชาการไซเบอร์โดยได้รวมขีดความสามารถด้านไซเบอร์ของกองทัพบก กองทัพเรือ กองทัพอากาศ และนาวิกโยธินเข้าไว้ด้วยกันและอยู่ภายใต้หน่วยงานเดียวกัน โดยได้ทุ่มงบประมาณลงไปหลายพันล้านดอลลาร์เพื่อใช้สำหรับโครงการนี้ ในขณะเดียวกัน เพนตากอนก็ได้

ขยายขีดความสามารถด้านไซเบอร์อย่างขนานใหญ่ดังจะเห็นได้จากในปี ค.ศ.๒๐๑๔-๒๐๑๗ ที่มีการเพิ่มเจ้าหน้าที่ด้านไซเบอร์ถึงมากกว่า ๖,๐๐๐ นาย นอกจากนี้ การทำสงครามไซเบอร์ยังเป็นส่วนหนึ่งของยุทธศาสตร์ทหารแห่งชาติอีกด้วย อีกทั้งหน่วยงานใหม่ที่เรียกว่า “หน่วยบัญชาการไซเบอร์ของสหรัฐอเมริกา” จะใช้เพื่อป้องกันเครือข่ายทางทหารของสหรัฐอเมริกาและใช้โจมตีระบบเครือข่ายของชาติอื่น (Richard A. Clarke, 2017) ต่อเนื่องมาถึงรัฐบาลของประธานาธิบดีโดนัล ทรัมส์ ก็ยังคงเพิ่มมาตรการเชิงรุกในการจัดการกับภัยคุกคามด้านไซเบอร์โดยการเพิ่มขีดความสามารถด้านบุคลากรและสมรรถนะของเครื่องมือไอซีทีอย่างเป็นด้านหลักเพื่อการเฝ้าระวังโดยไม่ให้ก่อปัญหาในระดับชาติและระดับโลก เป็นที่ทราบกันว่าในแง่ของการป้องกันนั้น สหรัฐอเมริกาได้ดำเนินการในการบริหารจัดการภัยคุกคามด้านไซเบอร์โดยลำดับดังนี้

๑.๑ การกำหนดให้การรักษาความมั่นคงปลอดภัยด้านไซเบอร์เป็นหนึ่งในลำดับเร่งด่วนด้านความมั่นคงแห่งชาติ โดยกระทรวงความมั่นคงแห่งมาตุภูมิเป็นผู้รับผิดชอบหลักเกี่ยวกับการดำเนินงานเชิงรับกับระบบเครือข่ายของรัฐบาล และมีการประสานความร่วมมือเพื่อปกป้องและป้องกันโครงสร้างพื้นฐานที่สำคัญของชาติ รวมถึงโครงสร้างพื้นฐานด้านไซเบอร์โดยทำงานร่วมกับหน่วยงานเฉพาะภายใต้สายการบริหารงานของศูนย์รักษาความมั่นคงปลอดภัยด้านไซเบอร์แห่งชาติ

๑.๒ การสถาปนาความร่วมมือกับหุ้นส่วนภาคเอกชนในเรื่องการรักษาความมั่นคงปลอดภัยด้านไซเบอร์เป็นจำนวนมาก อีกทั้งกระทรวงกลาโหมและกระทรวงความมั่นคงแห่งมาตุภูมิ ต่างมีความสัมพันธ์กับหุ้นส่วนภาคเอกชนในลักษณะเดียวกัน โดยเฉพาะในงานเกี่ยวกับการสืบสวนสอบสวนและการข่าวกรอง

๑.๓ หน่วยเฉพาะกิจร่วมด้านการสืบสวนสอบสวนด้านไซเบอร์แห่งชาติใช้เป็นศูนย์รวมของการประสานงาน การบูรณาการ และการแบ่งปันสารสนเทศที่เกี่ยวข้องกับการสืบสวนสอบสวนภัยคุกคามด้านไซเบอร์ภายในประเทศให้กับหน่วยงานภาครัฐทั้งหมด โดยสำนักงานสอบสวนกลางเป็นผู้รับผิดชอบในการจัดตั้งและสนับสนุนหน่วยเฉพาะกิจนี้ ซึ่งอาจมีหน่วยงานข่าวกรองและหน่วยงานบังคับใช้กฎหมายของสหรัฐอเมริการวมกันมากกว่า ๒๐ หน่วยงาน

๑.๔ รัฐบาลได้กำหนดกรอบทิศทางยุทธศาสตร์ทั่วไปเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านไซเบอร์แห่งชาติ โดยได้กำหนดตารางการปฏิบัติของระบบการป้องกันด้านไซเบอร์ซึ่งมี โดยมีคณะกรรมการนโยบายเพื่อบูรณาการโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการติดต่อสื่อสารที่มีผู้แทนทั้งจากสภาความมั่นคงแห่งชาติและสภาความมั่นคงแห่งมาตุภูมิเข้าร่วมด้วย ทั้งนี้ก็เพื่อใช้เป็นองค์กรประสานนโยบายหลักที่เกี่ยวกับการดำเนินงานเพื่อให้ได้มาซึ่ง

ความเชื่อมั่น ความไว้วางใจ ความปลอดภัย และความอยู่รอดสารสนเทศและโครงสร้างพื้นฐานด้านการติดต่อสื่อสารของโลก และการพัฒนาขีดความสามารถต่างๆ ที่เกี่ยวข้อง

๑.๕ สถาบันมาตรฐานและเทคโนโลยีแห่งสหรัฐอเมริกา ได้ออกกรอบการดำเนินงานล่าสุดเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ เพื่อกำหนดแนวปฏิบัติที่ดีให้นำไปใช้ใน การจัดการระบบของหน่วยงานในอุตสาหกรรมที่เกี่ยวกับโครงสร้างพื้นฐานสำคัญ ครอบคลุม ๑๖ กลุ่มโครงสร้างพื้นฐานสำคัญของสหรัฐอเมริกา โดยเนื้อหาหลักประกอบด้วยองค์ประกอบหลัก ๓ องค์ประกอบ ได้แก่

๑.๕.๑ โครงสร้างหลักของกรอบการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์

๑.๕.๒ ระดับของการดำเนินงานให้ประสบผลสำเร็จตามโครงสร้างหลักของกรอบการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์

๑.๕.๓ โครงร่างของโครงสร้างหลักของกรอบการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์”

๑.๖ โครงสร้างหลักของกรอบการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ของสหรัฐอเมริกา ประกอบด้วย

(๑) พันธกิจ (Functions) โดยแบ่งออกเป็น ๕ พันธกิจ ได้แก่ ๑) พิสูจน์ทราบ (Identify) ๒) ป้องกัน (Protect) ๓) ตรวจจับ (Detect) ๔) ตอบสนอง (Respond) และ ๕) คืนสภาพ (Recover) แสดงดังแผนภาพที่ ๔ - ๑ และ แผนภาพที่ ๔ - ๒ ตามลำดับ

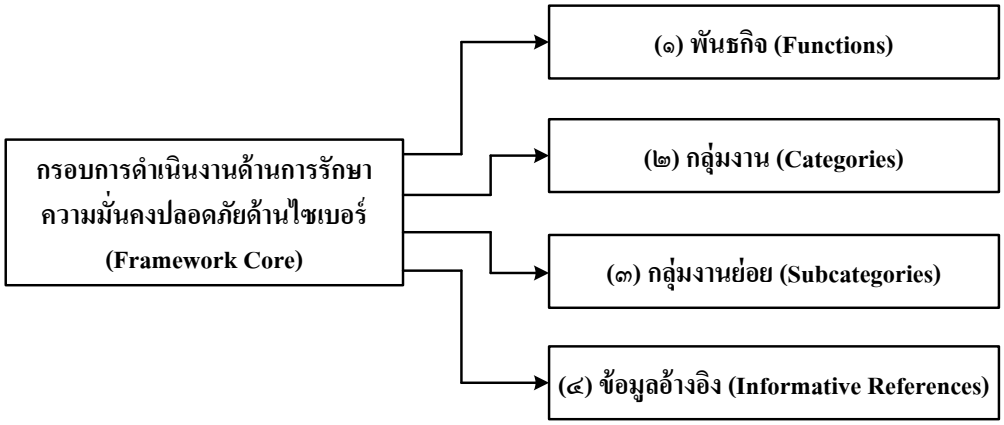
(๒) กลุ่มงาน (Categories)

(๓) กลุ่มงานย่อย (Subcategories) และ

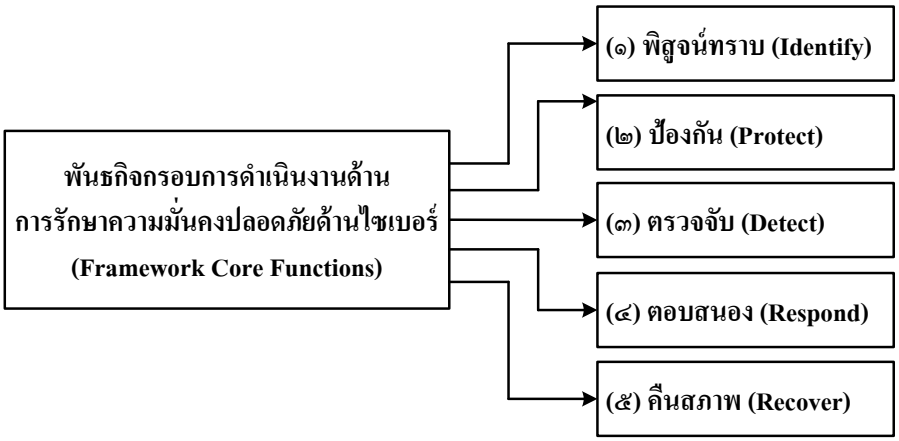
(๔) ข้อมูลอ้างอิง (Informative References)

๑.๗ โครงร่างของโครงสร้างหลักของกรอบการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ดังแสดงในแผนภาพที่ ๓ - ๑ เป็นการจัดเรียงพันธกิจ กลุ่มงาน และกลุ่มงานย่อย ให้ตรงกับความต้องการของภาคธุรกิจ ระดับความเสี่ยงที่ยอมรับได้ และทรัพยากรขององค์การ ดังนั้นการประสานการดำเนินงานตามโครงสร้างหลักให้ประสบผลสำเร็จ จึงจำเป็นต้องอาศัยความร่วมมือร่วมใจกันระหว่างบุคลากรในองค์การ ๓ ระดับ คือ (๑) ระดับผู้บริหาร (Executive Level) (๒) ระดับกระบวนการ (Business/Process Level) และ (๓) ระดับปฏิบัติการ (Implementation/Operations Level) ดังที่ได้กล่าวมาแล้วในบทที่ ๓

แผนภาพที่ ๔ - ๑ โครงสร้างหลักของกรอบการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์



แผนภาพที่ ๔ - ๒ พันธกิจกรอบการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์



๒. จีน

รัฐบาลจีนได้จัดตั้งศูนย์บัญชาการไซเบอร์ขึ้นอย่างลับๆ กลางสลัมในเซี่ยงไฮ้เพื่อใช้เป็นศูนย์บัญชาการกลางด้านไซเบอร์ จีนค่อนข้างมีนโยบายด้านการป้องกันภัยคุกคามด้านไซเบอร์ค่อนข้างดีโดยมีการจัดแบ่งพื้นที่รับผิดชอบเป็นมณฑลในแต่ละภูมิภาคซึ่งทำให้จีนมีบุคลากรด้านไซเบอร์ถึงประมาณ ๑ ล้านคนในปัจจุบัน ในขณะเดียวกันจีนก็พยายามที่จะแสวงหาความร่วมมือด้านการทำสงครามไซเบอร์กับชาติอื่นที่เป็นพันธมิตรใกล้ชิดรวมทั้งประเทศไทยอีกด้วย ปัจจุบันเป็นที่เชื่อได้ว่าจีนได้พยายามขยายขีดความสามารถและสมรรถนะด้านไซเบอร์และเทคโนโลยีทางทหารของตนโดยอาศัยเทคโนโลยีทางทหารของต่างชาติ รัฐบาลจีนจึงสนับสนุนให้มี

กระบวนการพัฒนาสารสนเทศทางการทหารอยู่เสมอ ทั้งนี้ก็เพื่อจัดเตรียมกองทัพปลดปล่อยประชาชนจีนให้สามารถเผชิญหน้ากับรูปแบบภัยคุกคามที่หลากหลายในอนาคตนั่นเอง (Li Zhang, 2012)

๓. รัสเซีย

รัสเซียได้ชื่อว่าเป็นประเทศที่มีความเชี่ยวชาญด้านการโจมตีทางไซเบอร์โดยมักถูกกล่าวหาบ่อยครั้งว่าเป็นผู้ใช้สงครามไซเบอร์ในการโจมตีชาติอื่น รูปแบบการโจมตีจะอาศัยนักเจาะระบบคอมพิวเตอร์ การแพร่กระจายข่าวสารลวงผ่านระบบอินเตอร์เน็ต การสนับสนุนกลุ่มผู้แสดงความเห็นผ่านเว็บไซต์ทางการเมือง การค้นหาและเฝ้าติดตามทางอินเตอร์เน็ตด้วยการใช้เทคโนโลยีต่างๆ และการก่อกวนกลุ่มผู้ที่ไม่เห็นด้วยกับรัฐบาลด้านไซเบอร์ ส่วนการใช้มาตรการดำเนินงานด้านไซเบอร์ของรัฐเซียนั้นยังไม่ปรากฏออกมาเด่นชัดมากนัก (Frank J. Cilluffo, 2013)

ผลจากความเสียหายที่เกิดจากภัยคุกคามด้านไซเบอร์ที่ผ่านมา ทำให้ทุกประเทศทั่วโลกต่างก็ตระหนักดีถึงผลกระทบทั้งในแง่ที่เป็นประโยชน์และโทษจากการทำสงครามไซเบอร์ ทำให้ทุกประเทศต่างก็พยายามพัฒนาขีดความสามารถด้านการทำสงครามไซเบอร์ทั้งในเชิงรุกและการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ เพื่อใช้เป็นมาตรการทั้งเชิงรุกและเชิงรับจากการโจมตีด้านไซเบอร์ของฝ่ายตรงข้าม เห็นได้จากประเด็นสำคัญของยุทธศาสตร์และมาตรการด้านการทำสงครามไซเบอร์ของประเทศต่างๆ ที่สำคัญ ดังนี้

๑. สหรัฐอเมริกา

ประเทศสหรัฐอเมริกาได้กำหนดกรอบยุทธศาสตร์ในการจัดการกับภัยคุกคามด้านไซเบอร์โดยมีแนวคิดและมาตรการต่อไปนี้ (The Department of Defense, 2016)

๑.๑ สหรัฐอเมริกามองว่าโลกในปัจจุบันถูกเชื่อมโยงเป็นเครือข่ายและล่อแหลมต่อการถูกโจมตีผ่านทางเครือข่าย ด้วยเหตุนี้ ยุทธศาสตร์ด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ของสหรัฐอเมริกาจะต้องรับประกันในเรื่องการรักษาความลับ (Confidentiality) ความพร้อมใช้งาน (Availability) และความสมบูรณ์ของข้อมูล (Integrity of Data)

๑.๒ สหรัฐอเมริกาขอสงวนสิทธิที่จะใช้เครื่องมือใดๆ ที่เห็นว่าจำเป็น (เช่น การทูต สารสนเทศ การทหาร และเศรษฐกิจ เป็นต้น) เพื่อตอบโต้กับภัยคุกคามอย่างเหมาะสมและสอดคล้องกับกฎหมายที่มีอยู่ หากใช้เครื่องมือดังกล่าวแล้วไม่เป็นผล สหรัฐอเมริกาก็พร้อมที่จะใช้กำลังทหารเมื่อใดก็ได้ที่ต้องการ

๑.๓ การใช้การโจมตีด้านไซเบอร์เป็นเครื่องมือทางการเมือง ได้สะท้อนให้เห็นถึงแนวโน้มที่เป็นอันตรายต่อความสัมพันธ์ระหว่างประเทศ ดังนั้นการทำสงครามไซเบอร์กับฝ่ายตรงข้ามอาจยกระดับไปสู่สงครามที่มีการใช้กำลังทหารอย่างแท้จริงก็ได้

๒. สหราชอาณาจักร

ประเทศอังกฤษได้กำหนดแนวทางในการจัดการภัยคุกคามด้านไซเบอร์โดยมีแนวคิดและมาตรการต่อไปนี้ (The UK Cyber Security Strategy, 2015)

๒.๑ สหราชอาณาจักรจะจัดการกับอาชญากรรมด้านไซเบอร์และจะดำเนินการทุกวิถีทางเพื่อให้สหราชอาณาจักรเป็นประเทศที่มีความปลอดภัยมากที่สุดประเทศหนึ่งในโลกสำหรับการทำธุรกิจในโลกไซเบอร์

๒.๒ สหราชอาณาจักรจะรับมือกับการโจมตีด้านไซเบอร์ที่ยืดหยุ่นมากขึ้นและจะปกป้องผลประโยชน์ต่างๆ ของสหราชอาณาจักรในโลกไซเบอร์ให้ดียิ่งขึ้น

๒.๓ สหราชอาณาจักรจะช่วยปรับสภาพโลกไซเบอร์ให้เปิดกว้าง มีเสถียรภาพและมีชีวิตชีวา เพื่อให้ประชาชนของสหราชอาณาจักรสามารถใช้โลกไซเบอร์ได้อย่างปลอดภัยและสนับสนุนสังคมที่เปิดกว้าง

๒.๔ ประชาชนของสหราชอาณาจักรจะต้องมีความรู้ ทักษะ และขีดความสามารถที่หลากหลายและจำเป็นต่อการบรรลุจุดมุ่งหมายของการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ของประเทศ

๓. จีน

ประเทศจีนได้กำหนดแนวทางในการจัดการภัยคุกคามด้านไซเบอร์โดยมีแนวคิดและมาตรการเบื้องต้นดังต่อไปนี้

๓.๑ จีนเชื่อว่ากฎหมายระหว่างประเทศที่มีอยู่จะต้องได้รับการแก้ไข ให้ความชัดเจนหรือสร้างหลักเกณฑ์ขึ้นมาใหม่ให้สอดคล้องกับโลกไซเบอร์ในปัจจุบัน โดยเฉพาะในเรื่องสิ่งบ่งชี้ของการโจมตีด้านไซเบอร์ที่เป็นการก่ออาชญากรรมด้านไซเบอร์ และการกำหนดว่า ความเสียหายที่เกิดขึ้นจากการป้องกันตนเองอย่างไร จึงจะถือว่า เป็นการป้องกันตนเองอย่างเหมาะสมและถูกต้องตามกฎหมายระหว่างประเทศ

๓.๒ จีนตระหนักดีว่า สหรัฐอเมริกาและประเทศตะวันตกอื่นๆ ได้ใช้ให้บริษัทคู่สัญญาด้านกลาโหม เช่น Lockheed Martin, Boeing, Northrop Grumman, และ Raytheon เพื่อพัฒนาและใช้อาวุธด้านไซเบอร์ (Cyber-Weapon) กับทุกประเทศที่เป็นปรปักษ์

๓.๓ รัฐบาลจีนยังคงยึดถือหลักการพื้นฐานเกี่ยวกับโลกไซเบอร์ ๔ ประการ ได้แก่ ๑) หลักการว่าด้วยการเคารพต่อสิทธิและเสรีภาพในโลกไซเบอร์ โดยเน้นย้ำในเรื่องการเคารพต่อกฎหมายภายในของแต่ละประเทศเพื่อให้ได้มาซึ่งสิทธิในการได้มาและเผยแพร่สารสนเทศ สิทธิมนุษยชน และเสรีภาพพื้นฐานของมนุษย์ ๒) หลักการว่าด้วยความสมดุล โดยถือว่า เทคโนโลยีจะเป็นคุณหรือโทษก็ขึ้นอยู่กับผู้ใช้ ดังนั้นจีนจึงให้ความสำคัญกับความสมดุลระหว่าง “เสรีภาพ” กับ

“การควบคุม” “สิทธิ” กับ “ความรับผิดชอบ” และ “ความมั่นคง” กับ “การพัฒนา” ๓) หลักการว่าด้วยการใช้โลกไซเบอร์อย่างสันติ หลักการนี้จะเกี่ยวข้องกับการปกป้องเทคโนโลยีสารสนเทศของโลก โครงสร้างพื้นฐาน และระบบสารสนเทศทางพลเรือน มิให้ตกเป็นเป้าหมายจากภัยคุกคามหรืออาวุธทางไซเบอร์ และ ๔) หลักการว่าด้วยการพัฒนาอย่างเสมอภาค หลักการนี้จะกล่าวถึงการแบ่งแยกทางดิจิตอล การคุ้มครองสิทธิและผลประโยชน์ของประเทศที่ด้อยกว่า และคัดค้านต่อการแสวงประโยชน์ในโลกไซเบอร์ของประเทศที่เหนือกว่าทางเทคโนโลยี เพื่อทำให้ประเทศที่ด้อยกว่าไม่สามารถควบคุมเทคโนโลยีสารสนเทศและการบริการของตนได้อย่างอิสระ รวมถึงใช้คุกคามต่อเสถียรภาพทางการเมือง เศรษฐกิจ และสังคมของประเทศอื่น

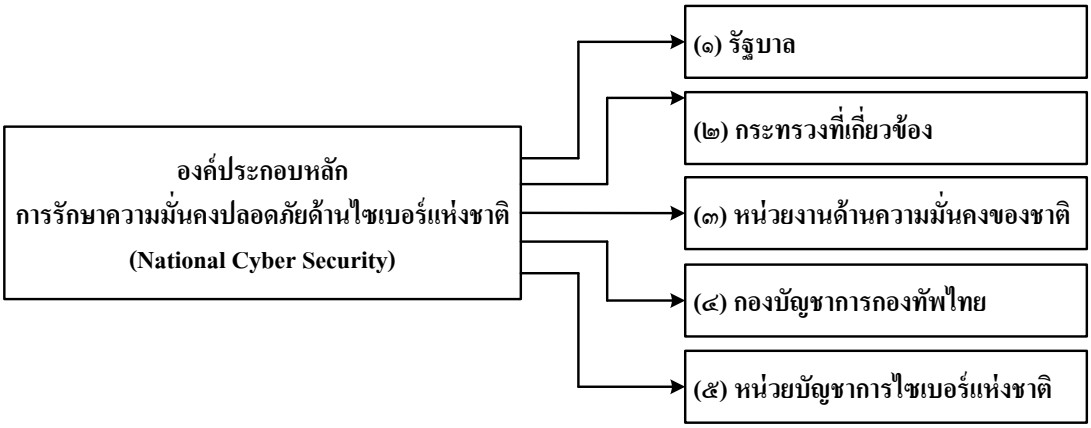
จากข้อมูลที่ปรากฏเกี่ยวกับภัยคุกคามด้านไซเบอร์เป็นที่ประจักษ์ชัดแล้วว่าประเทศมหาอำนาจทุกประเทศต่างก็มีการระบุแนวคิด ยุทธศาสตร์ และมาตรการในการจัดการกับภัยคุกคามด้านไซเบอร์ โดยกำหนดกรอบการทำงานอย่างชัดเจนเพราะมองว่าเป็นภัยคุกคามที่สามารถควบคุม ป้องกัน และระงับยับยั้งได้โดยต้องมีกระบวนการชัดเจน อีกทั้งต้องมีการเฝ้าระวังโดยไม่ประมาทต่ออาชญากรด้านไซเบอร์ที่สามารถบุกรุกโจมตีได้ตลอดเวลาโดยไม่มีเงื่อนไข

การวิเคราะห์รูปแบบที่เหมาะสมของการจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

สถานการณ์ รูปแบบ และแนวทางการจัดการกับภัยคุกคามด้านไซเบอร์ทั้งในประเทศไทยและต่างประเทศ ดังที่ได้กล่าวมาแล้วในบทที่ ๓ สามารถแสดงให้เห็นพัฒนาการของภัยคุกคามนี้ได้เป็นอย่างดี อย่างไรก็ตามสามารถกล่าวได้ว่ารูปแบบหรือแนวทางการจัดการกับภัยคุกคามด้านไซเบอร์ที่มีประสิทธิภาพนั้นยังไม่มีข้อกำหนดหรือรูปแบบที่แน่นอนว่าควรดำเนินการในประเด็นใด ทุกประเทศต่างก็มีมาตรการเป็นของตนเองในการดำเนินการในเรื่องนี้และบางยุทธวิธีก็ยังอยู่ในขั้นตอนที่เป็นความลับ ดังนั้นแต่ละประเทศต่างก็แสวงหาหนทางในการจัดการอย่างเป็นระบบเช่นเดียวกับประเทศไทยและกลุ่มประเทศอาซียน สำหรับประเทศไทยนั้นการกำหนดนโยบายและยุทธศาสตร์ในการจัดการภัยคุกคามด้านไซเบอร์มักเกิดขึ้นจากภาครัฐเป็นส่วนใหญ่ โดยอาศัยหน่วยงานทางความมั่นคงและกระทรวงที่เกี่ยวข้องในการกำหนดนโยบายตามที่ปรากฏในยุทธศาสตร์ชาติระยะ ๒๐ ปี พ.ศ.๒๕๖๐-๒๕๗๘ โดยไม่มีประเด็นที่เกี่ยวกับรูปแบบการดำเนินงาน แผนงาน และมาตรการที่เกี่ยวข้อง ซึ่งยังไม่ปรากฏเด่นชัดจากการที่ไม่ได้กำหนดเจ้าภาพรับผิดชอบโดยตรง จากการศึกษาข้อมูลเอกสาร รายงาน และการวิจัยที่เกี่ยวข้องสามารถนำมาวิเคราะห์เพื่อหารูปแบบที่เหมาะสมของการจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดน

ภาคใต้ โดยกำหนดเป็นประเด็นที่เกี่ยวกับผู้รับผิดชอบโดยตรงด้านไซเบอร์ในระดับชาติก่อน เพื่อให้เห็นภาพรวมของการทำสงครามไซเบอร์ ซึ่งสามารถกำหนดองค์ประกอบหลักของการรักษาความมั่นคงปลอดภัยด้านไซเบอร์แห่งชาติแสดงดังแผนภาพที่ ๔ - ๓

แผนภาพที่ ๔ - ๓ องค์ประกอบหลักของการรักษาความมั่นคงปลอดภัยด้านไซเบอร์แห่งชาติ



องค์ประกอบหลักของการรักษาความมั่นคงปลอดภัยด้านไซเบอร์แห่งชาติดังแสดงในแผนภาพที่ ๔ - ๓ สามารถกำหนดบทบาทของแต่ละส่วนดังนี้

๑. รัฐบาล

รัฐบาลไทยได้กำหนดยุทธ์ศาสตร์ชาติระยะ ๒๐ ปี (พ.ศ.๒๕๖๑ - ๒๕๘๐) ซึ่งอยู่ในประเด็นยุทธศาสตร์ที่ ๑ เฉพาะด้านความมั่นคงและความสัมพันธ์ระหว่างประเทศในการรักษาความมั่นคงและความสงบเรียบร้อยภายในประเทศ นั่นคือ ๑) การเสริมสร้างความมั่นคงของสถาบันหลักภายใต้การปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทางเป็นประมุข ๒) การรักษาความมั่นคงแลความสงบเรียบร้อยภายในประเทศ ๓) การนำพื้นที่จังหวัดชายแดนภาคใต้กลับสู่สันติสุขอย่างถาวร ๔) การดูแลพื้นที่แนวชายแดน ฝั่งทะเลอาณาเขต และเขตเศรษฐกิจจำเพาะ ๕) การเสริมสร้างความมั่นคงของโลก (Global Security) และความมั่นคงในภูมิภาค (Regional Security) ๖) การเสริมสร้างศักยภาพในการป้องปรามฝ่ายตรงข้ามและความเข้มแข็งของกองทัพในการป้องกันประเทศ ๗) การผนึกกำลังและระดมสรรพกำลังจากทุกภาคส่วนในการป้องกันประเทศ และ ๘) การเตรียมรับมือกับภัยคุกคามรูปแบบใหม่ (Non-conventional Security Threats) ซึ่งได้แก่ การก่อการร้ายและการโจมตีทางไซเบอร์และการบริหารจัดการวิกฤตการณ์ระดับชาติ (National Crisis Management) ดังนั้นในส่วนของภัยคุกคามด้านไซเบอร์ก็ย่อมต้องมียุทธศาสตร์ระดับชาติในการสร้างนโยบายและวิธีการบริหารจัดการที่มีกลไกที่ชัดเจนเพื่อที่จะให้ส่วนงานต่างๆ ของประเทศ

ดำเนินการไปตามนโยบายของภาครัฐอย่างมีประสิทธิภาพ เนื่องจากภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้มีลักษณะเป็นยุทธศาสตร์ตามพื้นที่เป้าหมาย (Area) หรือยุทธศาสตร์ตามประเด็นเฉพาะ (Agenda) ดังนั้นเพื่อให้มีการขับเคลื่อนแผนงานและโครงการในระดับปฏิบัติที่มีประสิทธิภาพจะต้องมีการกำกับดูแลอย่างใกล้ชิดเพื่อให้เกิดความสัมพันธ์ที่เชื่อมโยงกับยุทธศาสตร์ชาติมากที่สุด

๒. กระทรวงที่เกี่ยวข้อง

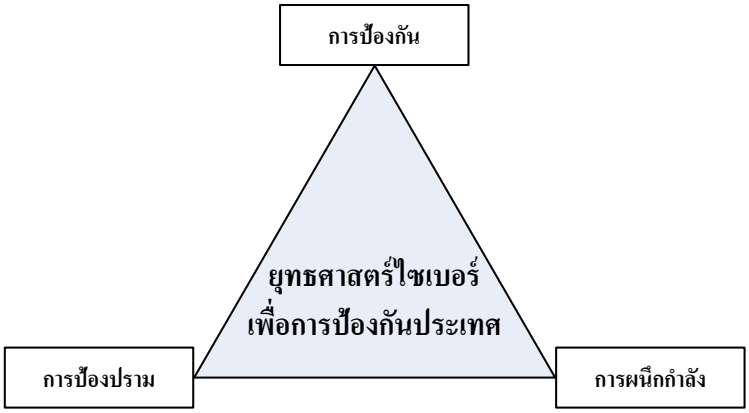
กล่าวได้ว่าการบริหารจัดการเกี่ยวกับภัยคุกคามด้านไซเบอร์มีส่วนเกี่ยวข้องกับทุกกระทรวง เนื่องจากในปัจจุบันเป็นยุคของระบบไอซีที โดยเป็นเรื่องที่เกี่ยวกับวิถีความเป็นอยู่ของสังคมสมัยใหม่ซึ่งก่อให้เกิดการเปลี่ยนแปลงวิถีชีวิตรวมถึงกลายเป็นสิ่งสำคัญและจำเป็นในการปฏิบัติงานของทุกองค์กร ไม่ว่าจะเป็นการทำธุรกิจ อุตสาหกรรม การให้บริการโทรคมนาคม การท่องเที่ยว การทหาร และการศึกษา เป็นต้น อีกทั้งโครงสร้างพื้นฐานวิกฤต (Critical Infrastructure) ที่อยู่รอบตัว เช่น ระบบไฟฟ้า น้ำประปา การคมนาคมขนส่ง ระบบธนาคาร และระบบโทรคมนาคม ล้วนมีการเชื่อมต่อกับเครือข่ายอินเตอร์เน็ตแทบทั้งสิ้น การแพร่หลายของเครือข่ายนี้ได้เปลี่ยนวิถีการดำรงชีวิตของมนุษย์แทบทุกด้าน โดยส่งผลให้ทุกกระทรวงมีส่วนเกี่ยวข้องกับการใช้บริการและการดำเนินงานอย่างหลีกเลี่ยงไม่ได้ ดังนั้นทุกกระทรวงจะต้องมีผู้เชี่ยวชาญในระบบไอซีทีและไซเบอร์ เพื่อให้สามารถรู้เท่าทันการเปลี่ยนแปลงและสามารถรับมือได้หากเกิดเหตุการณ์โจมตีระบบฐานข้อมูลของกระทรวงใดกระทรวงหนึ่ง

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมนับได้ว่าเป็นกระทรวงหลักหรืออาจเป็นเจ้าภาพหลักในการรับผิดชอบเรื่องกรอบนโยบายการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ของประเทศไทย เนื่องจากเป็นกระทรวงที่กำกับดูแลด้านการใช้งานและการบริการข้อมูลข่าวสารดิจิทัล โดยในปี พ.ศ.๒๕๖๑ จากการที่ ดร.พิเชฐ ดุรงคเวโรจน์ รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (ดีอี) ได้มีการหารือกับรัฐมนตรีว่าการกระทรวงการค้าต่างประเทศแห่งสหราชอาณาจักร ที่ทั้งสองฝ่ายเห็นควรผลักดันให้เกิดความร่วมมือในด้านการพัฒนาทรัพยากรมนุษย์ด้านดิจิทัลและความปลอดภัยด้านไซเบอร์เป็นโครงการเริ่มต้น ในส่วนของความปลอดภัยด้านไซเบอร์จะมีการผลักดันให้หน่วยงานภาครัฐและเอกชนของสหราชอาณาจักรเข้ามามีส่วนร่วมในศูนย์ ASEAN-Japan Capacity Building Center ซึ่งประเทศไทยได้จัดตั้งศูนย์ดังกล่าวเพื่อพัฒนาบุคลากรด้านความปลอดภัยไซเบอร์ของอาเซียน ทั้งนี้ถือได้ว่าเป็นจุดเริ่มต้นของการทำสงครามไซเบอร์ของประเทศไทยก็ว่าได้

๓. หน่วยงานด้านความมั่นคงของชาติ

เมื่อวันที่ ๒๙ กุมภาพันธ์ ๒๕๕๙ สภากลาโหมได้ให้ความเห็นชอบร่างยุทธศาสตร์ไซเบอร์เพื่อการป้องกันประเทศของกระทรวงกลาโหม พ.ศ.๒๕๕๘ โดยกระทรวงกลาโหม มีความจำเป็นที่จะต้องมียุทธศาสตร์ไซเบอร์แสดงดังแผนภาพที่ ๔ - ๔ เนื่องจากตระหนักดีว่า ภัยคุกคามด้านไซเบอร์ในปัจจุบันมีผลกระทบต่อความมั่นคงแห่งชาติและอาจถูกใช้เป็นเครื่องมือทางทหารของหลายประเทศเพื่อชิงความได้เปรียบและถูกใช้เป็นเครื่องมือในการสร้างความไม่สงบขึ้นได้ ฉะนั้นกระทรวงกลาโหมจึงจำเป็นต้องเตรียมการรับมือกับภัยคุกคามด้านไซเบอร์อย่างเป็นระบบ มีเอกภาพ และมีประสิทธิภาพ โดยกระทรวงกลาโหมได้จัดทำร่างยุทธศาสตร์ดังกล่าวขึ้นเพื่อใช้ในการป้องกันประเทศและเสริมสร้างศักยภาพด้านไซเบอร์ให้เป็นเครื่องมือด้านการปฏิบัติการทางทหารและเพิ่มมิติด้านการปฏิบัติภารกิจทางทหารของกระทรวงกลาโหม วัตถุประสงค์ของการร่างยุทธศาสตร์ดังกล่าวนี้ก็คือ เพื่อใช้ป้องกันประเทศและทำให้ฝ่ายเรามีเสรีจากการใช้ประโยชน์จากโลกไซเบอร์ จำกัดเสรีของฝ่ายตรงข้ามที่จะแทรกแซงและสนับสนุนการใช้ไซเบอร์ระดับชาติ โดยมียุทธศาสตร์ที่สำคัญ ๓ ประเด็น ดังนี้

แผนภาพที่ ๔ - ๔ ยุทธศาสตร์ไซเบอร์เพื่อการป้องกันประเทศของกระทรวงกลาโหม พ.ศ.๒๕๕๘



๓.๑ ด้านการป้องกัน

โดยกำหนดให้มีหน่วยงานกลางทำหน้าที่ประสานงานเชื่อมต่อระหว่างการปฏิบัติงานร่วมกันในระดับนโยบายความมั่นคงที่ดูแลความปลอดภัยระดับชาติไปสู่กระทรวงกลาโหม รวมถึงพัฒนาความร่วมมือกับมิตรประเทศ วัตถุประสงค์ของการป้องกัน ก็คือการดำเนินการทุกวิถีทางเพื่อไม่ให้ฝ่ายเราถูกโจมตีจากฝ่ายตรงข้าม โดยดำเนินการต่อกลุ่มสารสนเทศของหน่วยงานหรือขององค์กร โดยเฉพาะกระทรวงกลาโหมและกองทัพเฉพาะด้าน

ความมั่นคง โดยให้น้ำหนักไปในเรื่องของมาตรการป้องกันเป็นหลัก ฉะนั้น “การป้องกัน” จะป้องกันในระดับที่เป็นตัวระบบ กล่าวคือ เป็นการดำเนินการเพื่อไม่ให้เข้าถึงตัวระบบ ซึ่งในตัวระบบป้องกันนี้ หลายหน่วยงานจะมีรูปแบบภาพการป้องกันของหน่วยงานที่เป็นมาตรฐานอยู่แล้ว ตัวอย่างเช่น ระบบการป้องกันของกองบัญชาการกองทัพบก ด่านแรกที่บุคคลหนึ่งบุคคลใดจะเข้าไปในอาณาบริเวณของกองบัญชาการกองทัพบกได้จะต้องผ่านประตูที่เรียกได้ว่าเป็น “Gateway” ที่มีเจ้าหน้าที่รักษาความปลอดภัยยืนเฝ้าประตูอยู่เสียก่อน หากเจ้าหน้าที่รักษาความปลอดภัยพิจารณาแล้วว่า บุคคลดังกล่าวอาจเป็นภัยคุกคามก็สามารถผลักบุคคลดังกล่าวออกไปได้ แน่นอนที่สุด ทั้งบุคคลและยานพาหนะที่จะเข้าไปอาจมีรูปลักษณ์ หรือตราสัญลักษณ์ที่อนุญาตให้ผ่านไปได้ แต่ถ้ารูปลักษณ์หรือตราสัญลักษณ์ดังกล่าวดูแล้วน่าสงสัยว่าจะเป็นภัยคุกคาม เจ้าหน้าที่ก็สามารถกักบุคคลหรือยานพาหนะดังกล่าวไว้เพื่อตรวจสอบก่อนได้ กรณีตัวอย่างของการปฏิบัติหน้าที่ของเจ้าหน้าที่รักษาความปลอดภัยนี้ ก็มีลักษณะการทำงานเดียวกับการทำงานของระบบการป้องกันการลุกล้ำเข้ามาสู่ระบบที่เรียกว่า “HIPS” (Host Intrusion Prevention System) ที่จะไม่ยอมให้บุคคลหรือยานพาหนะใดๆ ไปมาพรวดพราดเข้ามาในกองบัญชาการกองทัพบกโดยไม่ได้ถูกตรวจสอบ ในขณะที่การแลกบัตร ณ กองรักษาการณ์ ก็มีลักษณะการทำงานเช่นเดียวกับการทำงานระบบ Firewall ที่มีหน้าที่คัดกรองบุคคลว่า สมควรอนุญาตให้เข้ามาในสถานที่ได้หรือไม่ หรือให้ไปติดต่อใคร ต้องแลกบัตรหรือไม่ หรือเอาบัตรไปตรวจสอบก่อนหรือไม่ หากตรวจสอบแล้วว่าเป็นบุคคลไม่พึงประสงค์ก็จะไม่ให้เข้า นอกจากนี้แล้วการใช้บัตรอนุญาตผ่าน หรือใบผ่านชั่วคราวก็มีลักษณะการทำงานเช่นเดียวกับระบบ CA (Certificate Authority) ตรวจสอบบุคคลว่าเป็นตัวจริงเสียงจริงไหมเพื่อเข้าไป ก่อนที่จะผ่านเข้าไปตรงนั้น จะมีการบันทึกเวลาเข้าออกว่าบุคคลผู้นั้นเป็นใครมาจากไหน เป็นการเก็บข้อมูลเข้าออก เพื่อตรวจสอบว่า บุคคลผู้นี้เข้าออกบ่อย มีความต้องการอะไร เป็นต้น อย่างไรก็ตาม ในแง่ของการป้องกันระบบคอมพิวเตอร์หรือระบบเครือข่ายของฝ่ายเราจากการโจมตีของฝ่ายตรงข้าม ไม่ว่าฝ่ายเราจะมีระบบป้องกัน HIPS ระบบ Firewall หรือระบบ CA ที่ดีมากแค่ไหน ฝ่ายตรงข้ามก็ยังคงสามารถลัดเลาะหาช่องโหว่และลุกล้ำเข้ามาในระบบของฝ่ายเราจนได้ ดังนั้น ระบบเหล่านี้ จึงทำหน้าที่คล้ายระบบเฝ้าระวัง (Monitor) ที่ช่วยให้ฝ่ายเราสามารถป้องกันไม่ให้ฝ่ายตรงข้ามโจมตีต่อระบบจนกระทั่งสร้างความเสียหายทั้งระบบเท่านั้น ทั้งนี้ก็โดยอาศัยสิ่งที่บอกเหตุที่ฝ่ายเราตรวจพบจากการเฝ้าระวังด้วยระบบหรือมาตรการป้องกันต่างๆ ของฝ่ายเรานั่นเอง

๓.๒ ด้านการป้องปราม

เมื่อร่างยุทธศาสตร์นี้มีผลบังคับใช้จะมีการจัดตั้งศูนย์เฝ้าระวังภัยคุกคามจากไซเบอร์ที่พร้อมจะดำเนินการเชิงรุกต่อฝ่ายที่เข้าแทรกแซง ในอดีตที่ผ่านมา การดำเนินการของทุก

ส่วนราชการไม่ว่าจะเป็นกระทรวงกลาโหมหรือกองทัพไทย ในฐานะหน่วยงานด้านความมั่นคงของรัฐ ต่างก็มีมาตรการในการเฝ้าระวังและป้องกันไม่ให้เกิดความเสียหายต่อระบบ และเกิดภาพลักษณ์ในเชิงลบต่อส่วนราชการของตนเองทั้งสิ้น อย่างไรก็ตาม ภาพของการโจมตีที่ผ่านมาอาจถือได้ว่าความรุนแรงยังไม่ถึงกับขั้นวิกฤตที่จำเป็นต้องใช้เครื่องมือหรือเทคโนโลยีขั้นสูงมากนัก แต่ภัยคุกคามด้านไซเบอร์ในปัจจุบันทุกหน่วยงานอาจตกเป็นเป้าหมายของการโจมตีด้านไซเบอร์ได้ทั้งสิ้น ฉะนั้นสิ่งที่สำคัญก็คือการเตรียมความพร้อมในการรับมือทุกรูปแบบไม่ว่าจะเป็นด้านการป้องกันและการป้องปรามตามนโยบายของกระทรวงกลาโหมที่ได้กำหนดยุทธศาสตร์ไว้ หากเทียบกับการป้องปรามของการปฏิบัติการทางทหาร “การป้องปราม” ก็คือ การฝึก การตรวจสอบ การซักซ้อม การแสดงกำลัง หรือการแสดงแสนยานุภาพให้ฝ่ายตรงข้ามได้เห็น เพื่อให้ฝ่ายตรงข้ามเกิดความยับยั้งชั่งใจจนไม่คิดที่จะเข้ารุกรานด้านการทหารต่อฝ่ายเรา ในขณะที่การป้องปรามด้านไซเบอร์ การแจ้งสารสนเทศ และการเฝ้าระวังที่บ่งบอกถึงการเตรียมความพร้อมของหน่วยงานต่างๆ ที่พร้อมจะรับมือกับภัยคุกคามด้านไซเบอร์ รวมทั้งการจัดตั้งศูนย์ไซเบอร์ของกองทัพบกและหน่วยงานอื่นๆ ต่างล้วนเป็นมาตรการป้องปรามด้านไซเบอร์ทั้งสิ้น

๓.๓ ด้านการผนึกกำลัง

การผนึกกำลังด้านไซเบอร์ คือ การเพิ่มมาตรการและขีดความสามารถของการทำงานร่วมกันของทุกหน่วยงานที่เกี่ยวข้องกับไซเบอร์ของชาติ โดยจะประสานความร่วมมือกับหน่วยงานต่างๆ ทั้งกระทรวงกลาโหม กองทัพไทย และกองบัญชาการเหล่าทัพ เป็นเครือข่ายและจัดตั้งให้เป็นประชาคมไซเบอร์ของกระทรวงกลาโหม ฉะนั้นในส่วนของกองทัพไทยจึงควรมีการหมุนเวียนจัดให้มีการประชุม เสวนา และแลกเปลี่ยนความรู้เกี่ยวกับสงครามไซเบอร์ระหว่างกัน โดยอาจเปิดกว้างให้กับพลเรือน หน่วยงานพลเรือน รัฐวิสาหกิจ และภาคประชาชนเข้ามามีส่วนร่วมด้วย เนื่องจากภัยคุกคามด้านไซเบอร์ไม่ใช่ภัยคุกคามต่อตัวบุคคลหรือเฉพาะหน่วยงานใดหน่วยงานหนึ่งอีกแล้ว แต่เป็นภัยคุกคามที่เกี่ยวข้องกับทุกคนและทุกองค์การ อีกทั้งความเสียหายที่เกิดขึ้นอาจส่งผลกระทบในวงกว้างจนถึงขนาดทำให้โครงสร้างพื้นฐานสำคัญของชาติต้องหยุดชะงักลงก็เป็นได้

๔. กองบัญชาการกองทัพไทย

ภัยคุกคามด้านไซเบอร์มีความเป็นไปได้สูงในอนาคต นั่นคือ การโจมตีจากฝ่ายตรงข้ามด้วยวัตถุประสงค์ต่างๆ ประเทศไทยควรเสริมขีดความสามารถด้านสงครามไซเบอร์และความมั่นคงปลอดภัยของข้อมูลข่าวสารในทุกภาคส่วน ภาครัฐควรกำหนดยุทธศาสตร์เฉพาะและแผนรองรับ ควรวางโครงสร้างพื้นฐานด้านระบบไอซีทีทั้งภาครัฐและภาคเอกชนให้มีความมั่นคงปลอดภัย ควรสร้างความตระหนักรู้และความรู้ความเข้าใจที่ถูกต้องกับประชาชนทั่วไปในการใช้

เทคโนโลยีและการสื่อสาร แต่ละองค์กรโดยเฉพาะหน่วยงานทางความมั่นคงและองค์กรภาคธุรกิจควรจัดเตรียมบุคลากรด้านความปลอดภัยของระบบสื่อสารและสารสนเทศ จัดหาเทคโนโลยีจัดการฝึกอบรม กำหนดมาตรการป้องกัน และตรวจสอบเครือข่ายของตนเองให้มีความพร้อมในการป้องกันและปกป้องข้อมูลข่าวสารขององค์กร ในส่วนของกองทัพไทยทุกเหล่าทัพควรมีขีดความสามารถและสมรรถนะที่พร้อมทั้งเชิงรุกและเชิงรับ ทั้งนี้เพื่อให้สามารถป้องปรามหรือตอบโต้ฝ่ายตรงข้ามได้อย่างทันท่วงทีและเพื่อมิให้ตกเป็นฝ่ายถูกโจมตีขัดขวางหรือถูกจารกรรมข้อมูลข่าวสารด้านความมั่นคงทางทหาร การดำเนินการของแต่ละเหล่าทัพเกี่ยวกับภัยคุกคามด้านไซเบอร์ปรากฏผลดังนี้

๔.๑ กองทัพอากาศ

ในส่วนของกองทัพอากาศได้เริ่มพัฒนามาตั้งแต่ปี พ.ศ.๒๕๔๓ จนถึงปัจจุบัน เพื่อสนับสนุนระบบสารสนเทศด้านงานยุทธการและระบบสารสนเทศสนับสนุนการรบ เพื่อให้ระบบสารสนเทศของกองทัพอากาศยังคงขีดความสามารถการรักษาความลับ มีความปลอดภัย และสามารถใช้งานได้ต่อเนื่อง ปัจจุบันเพื่อรองรับภัยคุกคามด้านไซเบอร์ที่มีความซับซ้อน และทวีความรุนแรงมากขึ้น กองทัพอากาศจึงมีการพัฒนางานด้านสงครามไซเบอร์ ทั้งเชิงรุกและเชิงรับ บนแนวคิดที่จะเสริมสร้างความมั่นคงปลอดภัยด้านไซเบอร์ การป้องปราม และการรับมือทางไซเบอร์ (Cyber Resilience) ในทุกรูปแบบ โดยการปฏิบัติการเชิงรุกจะมุ่งเน้นไปที่การสร้างทีมตรวจสอบความมั่นคงปลอดภัย นขต.ทอ. (ICT Security Audit) เพื่อหาจุดอ่อนหรือช่องโหว่ของระบบต่างๆ เพื่อเสนอแนวทางแก้ไขก่อนที่จะเกิดความเสียหายขึ้นจริงและการปฏิบัติการเชิงรับ จะมุ่งเน้นที่การบริหารความเสี่ยงเพื่อปรับปรุงกระบวนการป้องกันที่สมดุล เสริมเทคโนโลยีให้ทันสมัย และที่สำคัญก็คือการพัฒนาบุคลากรเพื่อให้ไม่เป็นจุดอ่อนด้านความมั่นคงปลอดภัยด้านไซเบอร์ แต่เป็นองค์ประกอบที่สำคัญยิ่งในการร่วมกันระวังป้องกันภัยด้วยการสร้างวัฒนธรรมความมั่นคงปลอดภัยด้านไซเบอร์ “Cyber Security Culture” ในกองทัพอากาศด้วย

กองทัพอากาศมีแผนงานเตรียมความพร้อมในการรับมือกับภัยคุกคามด้านไซเบอร์และได้ดำเนินการมาอย่างต่อเนื่อง โดยในปี พ.ศ.๒๕๖๐ กองทัพอากาศมุ่งเน้นการนำมาตรฐาน ISO 27001 มาปรับใช้ทั้งกองทัพฯ จัดหาระบบป้องกันเพื่อให้สามารถเฝ้าระวังภัยด้านไซเบอร์ พร้อมรายงานการบุกรุกเครือข่ายได้อย่างรวดเร็ว และที่สำคัญมุ่งให้ผู้ใช้ระบบสารสนเทศทุกคนต้องไม่ใช่ผู้ที่จะสร้างปัญหาด้านความปลอดภัยด้านไซเบอร์ แต่ต้องเป็นส่วนหนึ่งของเครือข่ายระวังป้องกันภัยด้านไซเบอร์ด้วยการสร้างจิตสำนึกหรือวิจารณญาณ และวัฒนธรรมความมั่นคงปลอดภัยด้านไซเบอร์ในด้านการป้องปรามอีกด้วย

ปัจจุบันกองทัพอากาศได้พัฒนาชุดปฏิบัติการด้านไซเบอร์อย่างต่อเนื่องเพื่อตรวจสอบและประเมินระบบรักษาความมั่นคงปลอดภัยสารสนเทศของหน่วย โดยขึ้นตรงกองทัพอากาศและหน่วยงานภายนอกสนับสนุน อีกทั้งมีการให้ความร่วมมือในการปฏิบัติการกับเหล่าทัพอื่นหากได้รับการร้องขอ สามารถผนึกกำลังในการสนับสนุนปฏิบัติการด้านสงครามไซเบอร์ให้กับกองทัพไทย รวมทั้งหน่วยงานภาครัฐและเอกชน โดยยกระดับความสำคัญของระบบเครือข่ายภายในระหว่างกองบัญชาการกองทัพไทยและเหล่าทัพอื่น เพื่อให้สามารถแลกเปลี่ยนข้อมูลได้อย่างเสรีโดยไม่พึ่งพาระบบอินเตอร์เน็ตและเพื่อลดปัญหาความเสี่ยงจากผู้ไม่ประสงค์ดี อันจะส่งผลให้ประสิทธิภาพการทำงานของภาครัฐได้รับการยกระดับ ประชาชนมีความมั่นใจในความปลอดภัยในการใช้งาน ตลอดจนเสริมสร้างความมั่นคงด้านไซเบอร์ต่อประเทศไทยอีกด้วย

๔.๒ กองทัพเรือ

ในส่วนของกองทัพเรือได้เล็งเห็นความสำคัญของภัยคุกคามด้านไซเบอร์มาตั้งแต่ปี พ.ศ.๒๕๔๕ จนถึงปัจจุบัน โดยมีการพัฒนาสมรรถนะของระบบไอซีทีด้านงานยุทธการและประยุกต์ใช้เพื่อสนับสนุนการรบในรูปแบบการเดินเรือทะเล อีกทั้งยังคงขีดความสามารถในการใช้งานได้ต่อเนื่อง ปัจจุบันสามารถกล่าวได้ว่าระบบไอซีทีเพื่อรองรับภัยคุกคามด้านไซเบอร์ที่มีความซับซ้อนและทวีความรุนแรงมากยิ่งขึ้น กองทัพเรือจึงมีการพัฒนางานด้านการทำสงครามไซเบอร์มาจนถึงปัจจุบัน

ในปี พ.ศ.๒๕๖๑ นาวาเอก ปัทพงษ์ ดุรงค์ฤทธิชัย ผู้อำนวยการกองไซเบอร์ สำนักปฏิบัติการกรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ กล่าวว่า กองทัพมีการเตรียมความพร้อม ทั้งในเรื่องการพัฒนาบุคลากรทางการทหารให้มีความเชี่ยวชาญการปฏิบัติการด้านไซเบอร์เชิงรับ (Defensive) และการปฏิบัติการด้านไซเบอร์เชิงรุก (Offensive) โดยหลายปีที่ผ่านมา มีการนำร่องการอบรมและเพิ่มทักษะให้กับกำลังพลของกองทัพเรือเพื่อฝึกฝนความรู้ทางด้านไซเบอร์ให้บุคลากรนายทหารระดับสูงจนถึงระดับล่างมาดูแลเรื่องความมั่นคงและปลอดภัยทางด้านไซเบอร์ที่ชัดเจนและรัดกุมต่อไป

๔.๓ กองทัพบก

ในส่วนของกองทัพบกได้อนุมัติหลักการให้จัดตั้งศูนย์ไซเบอร์กองทัพบก (Army Cyber Center) เพื่อปฏิบัติงานเพื่อพลาง และเริ่มทดลองงานตั้งแต่วันที่ ๑ ตุลาคม พ.ศ.๒๕๕๗ เพื่อใช้เป็นหน่วยงานรับผิดชอบงานด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ และมีขีดความสามารถในการปฏิบัติการไซเบอร์เชิงรุก โดยได้ดำเนินการภายใต้หลักการบริหารงานเชิงกลยุทธ์ ๔ ประการ คือ การวางแผนงาน (Planning) การจัดการองค์กร (Organizing) การนำไปสู่การปฏิบัติ (Leading) และการประเมินผล (Evaluating) ทั้งนี้ได้เริ่มทดลองปฏิบัติงานขั้นต้นเป็นการ

ภายในมาตั้งแต่เดือนกันยายน พ.ศ.๒๕๕๗ เช่น การสำรวจตรวจสอบทรัพย์สินที่เกี่ยวข้องกับไซเบอร์ การตรวจสอบสภาพแวดล้อมภัยคุกคามไซเบอร์ การตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่งคงปลอดภัยไซเบอร์ การประเมินช่องโหว่ของระบบสารสนเทศ การปลูกฝังสร้างเสริมความสำนึก ความตระหนัก และการฝึกอบรม การสร้างภาคีประชาคมเครือข่ายไซเบอร์กองทัพบก การเฝ้าระวัง ตรวจสอบ วิเคราะห์ไซเบอร์ และข้อมูลข่าวสารที่เป็นภัยต่อความมั่นคง รวมถึงการปรับปรุงห้องปฏิบัติการความมั่นคงปลอดภัยไซเบอร์ เป็นต้น โดยอาศัยเครื่องมืออุปกรณ์ที่มีอยู่เดิม ซอฟต์แวร์เปิด และแสวงหาความร่วมมือจากหน่วยงานภายนอกทั้งจากภาครัฐเอกชน และสถาบันการศึกษา สำหรับแผนการดำเนินงานในขั้นทดลองปฏิบัติงานของศูนย์ไซเบอร์กองทัพบกนั้น จะมีความพร้อม ความน่าสนใจ และความเข้มข้นเพิ่มขึ้นตามลำดับ โดยเฉพาะอย่างยิ่งด้านการพัฒนาบุคลากรด้านไซเบอร์ เพื่อรองรับภารกิจที่ท้าทายความรู้ ความสามารถของกำลังพลในกองทัพบก และเพื่อเป็นการรับมือกับภัยคุกคามด้านไซเบอร์ที่กำลังเป็นภัยคุกคามไปทั่วทุกมุมโลก กองทัพบกก็จะเปิดกว้างให้กับประชาชน และองค์กรทุกภาคส่วนเข้ามามีส่วนร่วมในด้านการพัฒนาความพร้อมด้านไซเบอร์ร่วมกัน เพื่อเสริมสร้างให้ประเทศไทยมีศักยภาพและมีความแข็งแกร่งในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในภูมิภาคอาเซียน

นอกจากนี้กองบัญชาการกองทัพไทยควรเร่งดำเนินการเพื่อการรับมือกับภัยคุกคามด้านไซเบอร์ในประเด็นต่อไปนี้

(๑) การพัฒนากำลังพลของกองทัพให้มีความรู้ความสามารถเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ เพื่อให้กำลังพลของกองทัพมีความรู้ที่ทันต่อสถานการณ์ที่เปลี่ยนแปลงไปอย่างความต่อเนื่องและมีทักษะที่จำเป็นต่อการรับมือกับภัยคุกคามที่หลากหลายรูปแบบ ในขณะเดียวกัน ก็ควรกองทัพในเรื่องการบริหารจัดการ เครื่องมือ และบุคลากรให้สอดรับกับแนวทางการปฏิบัติ นโยบาย และยุทธศาสตร์ที่รัฐบาลได้กำหนดขึ้น ทั้งนี้โดยอาศัยการประสานงานและบูรณาการระหว่างเหล่าทัพ รวมถึงภาครัฐและเอกชนที่เกี่ยวข้อง เพื่อผนึกกำลังกันสร้างพลังอำนาจที่ไม่มีตัวตนเพื่อรับมือกับการโจมตีดังกล่าว

(๒) การให้ความรู้และสร้างความตระหนักรู้ถึงภัยคุกคามด้านไซเบอร์ให้กับกำลังพล บุคคลในครอบครัว ญาติพี่น้อง หรือบุคคลในสถานศึกษาต่างๆ เพื่อให้ช่วยกันเฝ้าระวังและตระหนักในเรื่องของการใช้เทคโนโลยีไม่ให้พวกเขาตกเป็นเหยื่อหรือเป็นเป้าหมายของการโจมตีด้านไซเบอร์ได้ง่าย

๕. หน่วยบัญชาการไซเบอร์แห่งชาติ

การจัดตั้งหน่วยบัญชาการไซเบอร์แห่งชาติ (National Cyber Department) อาจเป็นการยกระดับความสำคัญของภัยคุกคามด้านไซเบอร์ และเล็งเห็นความสำคัญว่าควรมีการสร้าง

ยุทธศาสตร์ในระดับชาติรวมถึงความร่วมมือในระดับโลกในการพัฒนาขีดความสามารถเพื่อการป้องกันและระงับยับยั้งไม่ให้ภัยคุกคามนี้ก่อปัญหากับประเทศไทย ประเด็นสำคัญของแนวทางด้านการทำสงครามไซเบอร์ของประเทศไทย ในส่วนหน่วยบัญชาการไซเบอร์แห่งชาติรับไปดำเนินการมีดังนี้

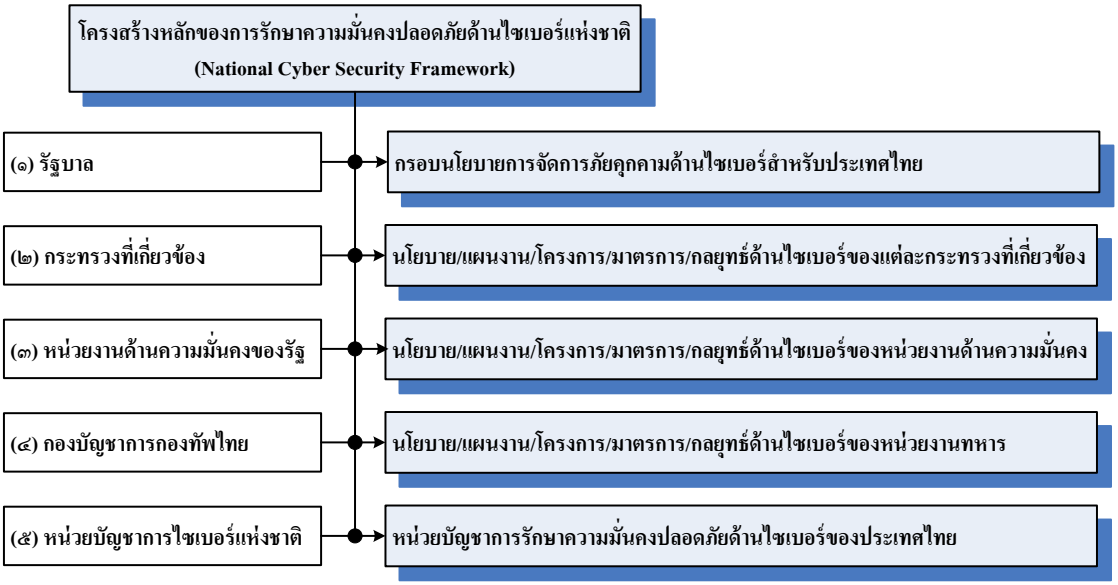
๕.๑ การพัฒนายุทธศาสตร์ นโยบาย และแนวทางการปฏิบัติ เพื่อใช้รับมือกับภัยคุกคามด้านไซเบอร์ทุกรูปแบบ โดยอาศัยความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้องเพื่อที่จะเสริมขีดความสามารถ ผนึกกำลัง และเสริมสร้างกำลังอำนาจที่ไม่มีตัวตนในโลกไซเบอร์ของฝ่ายเรา

๕.๒ การนำกรอบยุทธศาสตร์ด้านไซเบอร์ทั้ง ๓ ด้าน ไม่ว่าจะเป็นด้านการป้องกัน การป้องปราม และการผนึกกำลัง ไปดำเนินการเพื่อให้บรรลุผลสำเร็จตามยุทธศาสตร์ดังกล่าวอย่างเป็นรูปธรรม

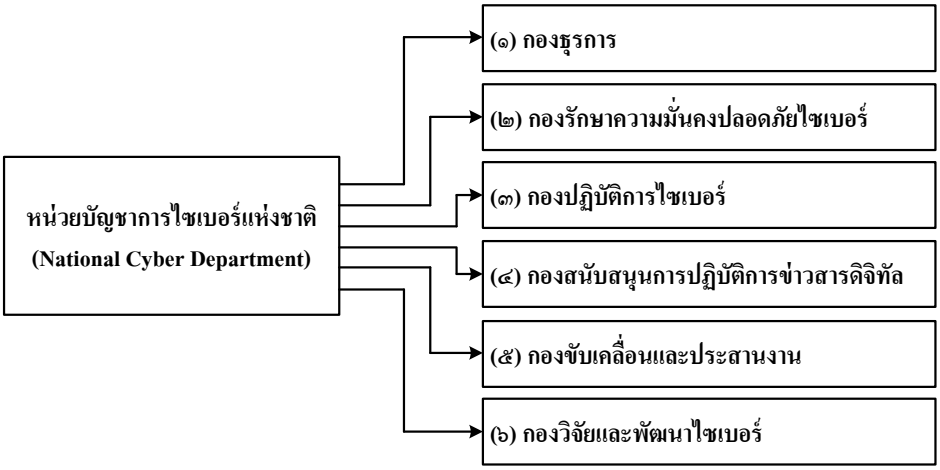
๕.๓ เตรียมการรับมือกับภัยคุกคามด้านไซเบอร์ โดยอาศัยกรอบการดำเนินงาน ๕ ขั้นตอน เช่นเดียวกับพันธกิจ ๕ อย่าง ที่สถาบันมาตรฐานและเทคโนโลยีแห่งสหรัฐอเมริกาใช้ (Identify, Protect, Detect, Response และ Recovery) ซึ่งขั้นตอนเหล่านี้เป็นพื้นฐานของการรับมือกับการโจมตีด้านไซเบอร์ที่ทั่วโลกยอมรับ กล่าวคือ (๑) ขั้นที่ ๑ การพิสูจน์ทราบภัยคุกคาม (Identify) เพื่อระบุภัยคุกคามหรือผลกระทบที่จะเกิดขึ้นว่า เป็นภัยคุกคามอะไรและมีผลกระทบอย่างไร (๒) การป้องกันภัยคุกคาม (Protect) เพื่อป้องกันระบบไม่ให้เกิดความเสียหาย (๓) การตรวจจับภัยคุกคาม (Detect) เพื่อตรวจค้น สืบค้น และค้นพบให้ได้ว่าเกิดการโจมตีที่ไหน ด้วยเครื่องมืออะไร และมีเป้าหมายอยู่ที่ไหน (๔) การตอบสนอง (Respond) เพื่อแก้ปัญหาที่เกิดขึ้นจากการโจมตีดังกล่าว และ (๕) การคืนสภาพระบบ (Recover) เพื่อให้ระบบกลับมาใช้งานต่อไปได้ตามปกติ จากขั้นตอนดังกล่าวทำให้เห็นได้ว่าทุกหน่วยงานที่มีการใช้ระบบไอซีทีเป็นหน้าที่ของบุคลากรภายในหน่วยที่จะเป็นผู้ดำเนินการโดยอาศัยเครื่องมือที่มีอยู่ของหน่วยเป็นหลัก ส่วนหลักการที่สำคัญต่อการดำเนินการตามขั้นตอนเพื่อรับมือกับภัยคุกคามด้านไซเบอร์ที่มีประสิทธิภาพใน ๕ ขั้นตอน ก็คือ “ตรวจพบให้เร็ว” “ป้องกันไว้ก่อน” “ค้นหาให้เจอ” “ตอบสนองให้ไว” และ “กู้คืนให้ได้”

จากบทบาทที่กำหนดสามารถนำมาเขียนแผนภาพความสัมพันธ์โครงสร้างหลักของการรักษาความมั่นคงปลอดภัยด้านไซเบอร์แห่งชาติ ดังแผนภาพที่ ๔ - ๕ ส่วนแผนภาพที่ ๔ - ๖ และแผนภาพที่ ๔ - ๗ แสดงถึงรูปแบบการจัดองค์กรของหน่วยบัญชาการไซเบอร์แห่งชาติและโครงสร้างพื้นฐานการจัดการภัยคุกคามด้านไซเบอร์ ตามลำดับ

แผนภาพที่ ๔ - ๕ โครงสร้างหลักของการรักษาความมั่นคงปลอดภัยด้านไซเบอร์แห่งชาติ



แผนภาพที่ ๔ - ๖ หน่วยบัญชาการไซเบอร์แห่งชาติ



จากนั้นเมื่อนำข้อมูลทุกด้านมาตรวจสอบด้วยวิธีการสามเส้าด้านข้อมูลพบว่า ข้อมูลที่ได้มาจากการศึกษาเอกสารและรายงานการวิจัยที่เกี่ยวข้อง การสัมภาษณ์ และข้อเท็จจริงที่เกิดขึ้น สามารถกล่าวได้ว่าภัยคุกคามด้านไซเบอร์เป็นภัยที่ร้ายแรงสำหรับประเทศไทย ดังนั้นจึงควรมีนโยบาย มาตรการ แผนงาน และกิจกรรมที่ต้องสอดคล้องกับนโยบายแห่งรัฐเพื่อการจัดการภัยคุกคามให้มีประสิทธิภาพต่อไป

แผนภาพที่ ๔ - ๗ โครงสร้างพื้นฐานการจัดการภัยคุกคามด้านไซเบอร์

เมื่อวิเคราะห์มาถึงหัวข้อนี้สามารถกล่าวได้ว่า ประเด็นสำคัญของแนวทางด้านการทำสงครามไซเบอร์ของประเทศไทยในการแก้ปัญหาความไม่สงบสุขในพื้นที่จังหวัดชายแดนภาคใต้ควรใช้นโยบายระดับชาติก่อนในเบื้องต้น โดยการกำหนดโครงสร้างพื้นฐานให้สมบูรณ์พร้อมทั้งภารกิจหน้าที่ จากนั้นก็ต้องกำหนดแผนงานและมาตรการที่เกี่ยวข้องทั้งด้านการสื่อสารข้อมูลและอำนาจตามกฎหมายที่พร้อมจะให้กลุ่มงานดำเนินการได้ และในที่สุดจึงจะสามารถนำนโยบายมาใช้ในการแก้ปัญหาในจังหวัดชายแดนภาคใต้ได้ตามเป้าหมาย ดังรายละเอียดที่กล่าวมาย่อมแสดงถึงรูปแบบที่เหมาะสมของการจัดตั้งองค์กรจึงจำเป็นต้องอาศัยความร่วมมือร่วมใจกันระหว่างบุคลากรในองค์กร ๓ ระดับ ได้แก่ (๑) ระดับผู้บริหาร (๒) ระดับกระบวนการ และ (๓) ระดับปฏิบัติการ โดยมีภารกิจหน้าที่หลัก ๓ ประการ ได้แก่ การป้องกัน (Defense) การยับยั้ง (Deterrence) และการโจมตี (Attack) ส่วนร่างยุทธศาสตร์ในการจัดการกับภัยคุกคามด้านไซเบอร์จะกล่าวถึงในหัวข้อต่อไป

การวิเคราะห์ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

จากผลการศึกษาทั้งในบทที่ ๓ และหัวข้อที่ผ่านมาสามารถนำมากำหนดร่างยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ได้ดังนี้

๑. การวิเคราะห์สภาพแวดล้อมภายในและภายนอก

๑.๑ การวิเคราะห์สภาพแวดล้อมภายใน (Internal Environment)

สถานการณ์ในปัจจุบันและแนวโน้มการเปลี่ยนแปลงของสภาพแวดล้อมภายในที่เกี่ยวกับประเด็นด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พบว่าในช่วงหลายปีที่ผ่านมา รัฐบาลไทยตระหนักและให้ความสำคัญกับการป้องกันและแก้ไขปัญหาไซเบอร์อย่างจริงจัง เนื่องจากความแพร่หลายของการให้และใช้บริการข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ เครือข่ายคอมพิวเตอร์ อินเตอร์เน็ต และโครงข่ายสื่อสารโทรคมนาคม เป็นต้น ที่ครอบคลุมเกือบทุกพื้นที่ทั้งภายในประเทศและทั่วโลก ซึ่งการเชื่อมโยงถึงกันดังกล่าว หากพิจารณาจากมุมมองของผู้ที่ปฏิบัติหน้าที่รักษาความมั่นคงปลอดภัยของประเทศ ก็อาจถือเป็นปัจจัยเชิงลบที่คุกคามและส่งผลกระทบอย่างรวดเร็วและรุนแรงต่อประชาชน เศรษฐกิจ และความมั่นคงของประเทศ หากภาครัฐและหน่วยงานที่เกี่ยวข้องยังขาดความพร้อมและไม่มีมาตรการป้องกันแก้ไขที่ชัดเจนและมีประสิทธิภาพเพียงพอแล้ว ความเสียหายที่เกิดขึ้นต่อทุกภาคส่วนของสังคมนั้นก็จะมีมูลค่ามหาศาลและยากที่จะประเมินได้

๑.๒ การวิเคราะห์สภาพแวดล้อมภายนอก (External Environment)

สถานการณ์ในปัจจุบันและแนวโน้มการเปลี่ยนแปลงของสภาพแวดล้อมภายนอกที่เกี่ยวกับประเด็นด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พบว่ารัฐบาลไทยมีบทบาทสำคัญต่อการรักษาความมั่นคงปลอดภัยในระดับอาเซียน ดังจะเห็นได้จากการพัฒนาความร่วมมือด้านการต่อต้านการก่อการร้ายด้านไซเบอร์และความพยายามในการตั้งศูนย์ไซเบอร์กลางของอาเซียนที่ประเทศไทย จากผลการศึกษาปัญหาอาชญากรรมไซเบอร์รูปแบบต่างๆ ได้แผ่ขยายไปทั่วโลกพบว่าเกิดผลกระทบต่อบุคคล องค์กร และประเทศ ทั้งในมิติเศรษฐกิจ สังคม และความมั่นคงของชาติ ดังเช่น สหรัฐอเมริกาพบปัญหาการค้าคลิปลามกอนาจารบนอินเตอร์เน็ต ปัญหาการล่อลวงเด็กและเยาวชนผ่านการสื่อสารทางอินเตอร์เน็ต รวมถึงปัญหาการโจรกรรมข้อมูลบัตรเครดิต เช่น บัตรวีซ่าและมาสเตอร์การ์ดของลูกค้าอย่างต่อเนื่อง ในทวีปเอเชีย มีการพบปัญหาการก่อกวนระบบเครือข่ายตลาดหลักทรัพย์ฮ่องกงจนทำให้เกิดผลกระทบอย่างมหาศาลต่อระบบการเงิน บุคคล และบริษัทหลายร้อยราย เนื่องจากการซื้อขายหุ้นในตลาดหลักทรัพย์ฮ่องกงหยุดชะงัก ในขณะที่ประเทศญี่ปุ่น

เกิดกรณีแฮกเกอร์โจมตีเว็บไซต์ของกระทรวงการคลัง ศาลฎีกา และศาลทรัพย์สินทางปัญญา โดยมีจุดประสงค์เพื่อต่อต้านการออกกฎหมายป้องกันการดาวน์โหลดสินค้าลิขสิทธิ์ซึ่งส่งผลให้เว็บไซต์ดังกล่าวต้องปิดตัวลงชั่วคราว ทั้งหมดที่กล่าวมาสามารถยืนยันได้ว่าการถูกโจมตีทางไซเบอร์มีโอกาสเกิดขึ้นได้อยู่เสมอโดยไม่มีรูปแบบและเวลาตายตัว แต่จะส่งผลกระทบต่อกิจการงานอย่างไม่มีเงื่อนไข

๒. การวิเคราะห์ SWOT

๒.๑ จุดแข็ง (Strengths)

๒.๑.๑ ความก้าวหน้าด้านไซเบอร์ คือ เทคโนโลยีที่มีอินเตอร์เน็ตเพื่อเชื่อมโยงการสื่อสารได้ทุกที่ทุกเวลาไม่ว่าจะอยู่ที่ใดบนโลก มีความสะดวกรวดเร็ว โลกไซเบอร์มีความสำคัญอย่างมากต่อการดำรงชีวิตของมนุษย์ในปัจจุบัน โดยมีเครื่องมือที่ใช้ในการติดต่อสื่อสาร ประกอบด้วย คอมพิวเตอร์ สมาร์ทโฟน แท็บเล็ต และเครื่องมืออื่นๆ ความก้าวหน้าด้านไซเบอร์ต้องมีกระบวนการสื่อสารความเร็วสูง มีระบบรักษาความปลอดภัยของข้อมูล มีระบบปฏิบัติการที่ดีและมีประสิทธิภาพจึงจะสามารถเข้าถึงได้ง่าย

๒.๑.๒ วิธีการก่อการร้ายด้านไซเบอร์ มีวิธีการดังนี้ ๑) ผู้ก่อการร้ายหรืออาชญากรไซเบอร์ต้องมีความรู้ด้านไซเบอร์หรือเทคโนโลยี มีการศึกษาข้อมูลที่เกี่ยวกับเป้าหมายที่ต้องการจะกระทำ ๒) สร้างหรือพัฒนาเครื่องมือให้ตรงกับความต้องการต่อเป้าหมาย โดยเครื่องมือที่สำคัญของการก่อการร้ายด้านไซเบอร์ก็คือ ระบบอินเตอร์เน็ต ระบบเครือข่าย และสื่อสังคมออนไลน์ ๓) ระดมคนหรือหาสมาชิกที่มีแนวความคิดหรือแนวทางเดียวกัน ๔) ระดมเงินทุนในการสนับสนุน และ ๕) ปฏิบัติการตามวัตถุประสงค์ที่วางไว้เพื่อมุ่งสู่เป้าหมายตามอุดมการณ์

๒.๒ จุดอ่อน (Weakness)

๒.๒.๑ ประเทศไทยแม้ไม่ใช่เป้าหมายโดยตรงของกลุ่มผู้ก่อการร้ายแต่อาจตกเป็นเป้าหมายสำหรับการปฏิบัติการของกลุ่มผู้ก่อการร้าย เนื่องจากประเทศไทยมีผลประโยชน์เกี่ยวข้องกับประเทศต่างๆ โดยเฉพาะประเทศตะวันตกซึ่งเป็นเป้าหมายของกลุ่มผู้ก่อการร้ายจำนวนมาก โดยกลุ่มผู้ก่อการร้ายส่วนใหญ่ที่เข้ามาเคลื่อนไหวและปฏิบัติการในประเทศไทยจะใช้ประเทศไทยเป็นแหล่งที่หลบภัยและผลิตยุทโธปกรณ์ของกลุ่มผู้ก่อการร้าย อีกทั้งยังแสวงหาผลประโยชน์จากทางการเงิน การธนาคาร ประเทศไทยมีมาตรการที่ไม่รัดกุมซึ่งเป็นช่องทางสนับสนุนทางการเงินของกลุ่มผู้ก่อการร้าย นอกจากนี้การก่อการร้ายเชื่อมโยงกับการก่ออาชญากรรมประเภทอื่นด้วย เช่น การลักลอบค้ายาเสพติด การค้าอาวุธ การฟอกเงิน การปลอมแปลงเอกสารเดินทาง และบัตรประจำตัวประชาชนหรือเอกสารทางราชการ เป็นต้น ผู้ก่อการร้ายผลิตและลักลอบค้ายาเสพติดสามารถสร้างเงินและรายได้จำนวนมหาศาล และนำเงินที่ได้มาซื้ออาวุธหรือสร้างฐานกำลังเพื่อ

ดำเนินการก่อการร้ายกับประเทศที่เป็นเป้าหมาย โดยมีวัตถุประสงค์หลักในการใช้ประเทศไทยเป็นฐาน เป็นศูนย์กลางในการจัดส่งอาวุธ และเป็นทางผ่านไปยังประเทศเป้าหมาย

๒.๒.๒ ปัจจัยที่เกี่ยวข้องกับแรงจูงใจในการก่อการร้ายด้านไซเบอร์ ด้วยประเทศไทยเป็นประเทศเปิดเสรีรับนักท่องเที่ยวและมีนโยบายส่งเสริมให้เกิดการท่องเที่ยวในทุกที่โดยไม่มีข้อจำกัด ดังนั้นจึงเป็นเหมือนสวรรค์ของผู้ก่อการร้าย อีกทั้งการส่งเสริมการเปิดใช้อินเตอร์เน็ตในทุกที่ทำให้ประชาชนขาดการตระหนักรู้ในเรื่องของการใช้งานไซเบอร์ กระบวนการก่อการร้ายด้านไซเบอร์นั้นผู้ก่อการร้ายจะใช้เครื่องมือทางไซเบอร์ที่หาง่ายและใช้เครื่องมือได้ทุกที่ เช่น สมาร์ทโฟน แท็บเล็ต และคอมพิวเตอร์ที่สามารถเชื่อมต่ออินเตอร์เน็ตได้ทำให้คนเข้าถึงได้ง่ายและเชื่อง่ายขึ้น แรงจูงใจที่นำไซเบอร์มาก่อการร้าย ผู้เชี่ยวชาญมองว่าเรื่องเงินเป็นสำคัญ รองมาเป็นเรื่องของแนวคิดและอุดมการณ์ทางการเมืองหรือทางศาสนา และแม้แต่ความไม่พอใจต่อหน่วยงานหรือองค์กร แต่ปัจจัยที่สำคัญที่ผู้เชี่ยวชาญมองต่างกันคือ แรงจูงใจที่สำคัญต่อการกระทำที่เป็นการก่อการร้ายจะต้องเป็นการกระทำที่มาจากแรงจูงใจทางเมืองเป็นสำคัญ จึงเห็นได้ว่าความเข้าใจในความหมายของการก่อการร้ายที่แตกต่างกัน นำไปสู่การอธิบายแรงจูงใจของการก่อการร้ายที่ต่างกันด้วย การอธิบายแรงจูงใจต่อการก่อการร้ายด้านไซเบอร์จึงไม่ได้มีการให้คำจำกัดความที่ชัดเจนเช่นเดียวกัน

๒.๒.๓ ผู้ก่อการร้ายแสวงหาโอกาสจากประเทศไทยในหลายด้านเพื่อก่อการร้าย ประเด็นสำคัญที่พบคือ ประเทศไทยเป็นประเทศที่เปิดเสรีและประชาชนมีการต้อนรับชาวต่างประเทศ มีการยิ้มแย้มแจ่มใสและต้อนรับผู้อื่นอย่างเป็นมิตรจึงเหมือนกับเป็นสวรรค์ของผู้ก่อการร้าย ส่วนใหญ่ผู้ก่อการร้ายจะใช้ประเทศไทยเป็นฐานในการเตรียมการก่อการร้ายไปยังประเทศที่สาม หรือประเทศที่เป็นเป้าหมายมากกว่า และประเทศไทยไม่มีมาตรการในการป้องกันความปลอดภัยด้านไซเบอร์ ประชาชนยังไม่มีการตระหนักรู้ต่อภัยคุกคามด้านไซเบอร์จึงทำให้มีการใช้งานอย่างระมัดระวัง

๒.๓ โอกาส (Opportunities)

ประเทศไทยมีโอกาสในการพัฒนาความก้าวหน้าด้านไซเบอร์ได้อีกมาก ด้วยบริบทของประเทศไทยยังคงเป็นประเทศที่ไม่ได้มีการใช้งานไซเบอร์ทั้งระบบในโครงสร้างพื้นฐานและมีโอกาสในการพัฒนาทางไซเบอร์ด้วยปัจจัยหลายด้าน เช่น ความสามารถของคนรุ่นใหม่ที่มีความสนใจด้านไซเบอร์ ความตื่นตัวต่อการเรียนรู้ด้านไซเบอร์ การพัฒนาโครงสร้างพื้นฐานให้มีความพร้อมโดยสามารถที่จะพัฒนาควบคู่ไปกับการใช้งานไซเบอร์ในวิถีปัจจุบัน และมีวิธีการป้องกันที่ดีต่อการก่อการร้าย เป็นต้น

๒.๔ ภัยคุกคาม (Threats)

ประเทศไทยกล่าวได้ว่าแม้ไม่ใช่เป้าหมายโดยตรงของกลุ่มผู้ก่อการร้ายแต่อาจตกเป็นเป้าหมายสำหรับการปฏิบัติการของกลุ่มผู้ก่อการร้าย เนื่องจากประเทศไทยมีผลประโยชน์เกี่ยวข้องกับประเทศต่างๆ โดยเฉพาะประเทศตะวันตกซึ่งเป็นเป้าหมายของกลุ่มผู้ก่อการร้ายจำนวนมาก โดยกลุ่มผู้ก่อการร้ายส่วนใหญ่ที่เข้ามาเคลื่อนไหวและปฏิบัติการในประเทศไทยจะใช้ประเทศไทยเป็นแหล่งที่หลบภัยและผลิตยุทโธปกรณ์ของกลุ่มผู้ก่อการร้าย อีกทั้งยังแสวงหาผลประโยชน์จากทางการเงิน การธนาคาร ประเทศไทยมีมาตรการที่ไม่รัดกุมเป็นช่องทางสนับสนุนทางการเงินของกลุ่มผู้ก่อการร้าย นอกจากนี้การก่อการร้ายเชื่อมโยงกับการก่ออาชญากรรมประเภทอื่นด้วย เช่น การลักลอบค้ายาเสพติด การค้าอาวุธ การฟอกเงิน การปลอมแปลงเอกสารเดินทาง บัตรประจำตัวประชาชนหรือเอกสารราชการ เป็นต้น ผู้ก่อการร้ายผลิตและลักลอบค้ายาเสพติดสามารถสร้างเงินและรายได้จำนวนมหาศาลให้กับผู้ก่อการร้าย และนำเงินที่ได้มาซื้ออาวุธหรือสร้างฐานกำลังเพื่อดำเนินการก่อการร้ายกับประเทศที่เป็นเป้าหมาย โดยมีวัตถุประสงค์ในการใช้ประเทศไทยเป็นฐานหรือศูนย์กลางในการจัดส่งอาวุธหรือเป็นทางผ่านไปยังประเทศเป้าหมาย ประเด็นที่กล่าวมาถือเป็นภัยคุกคามหรืออุปสรรคต่อการป้องกันเป็นอย่างยิ่ง

ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ สามารถกำหนดรูปแบบได้ดังนี้

วิสัยทัศน์ (Vision) : ประเทศไทยมีศักยภาพในการจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

พันธกิจ (Mission) : การพัฒนารูปแบบการจัดการภัยคุกคามด้านไซเบอร์โดยมุ่งสร้างฐานความรู้ให้กับประชาชนทุกระดับ เพื่อความมั่นคงปลอดภัยและความสงบสุขในพื้นที่จังหวัดชายแดนภาคใต้ของประเทศไทย

วัตถุประสงค์ (Objective) :

๑. เพื่อใช้เป็นยุทธศาสตร์ที่มีประสิทธิภาพในการจัดการกับภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ของประเทศไทย

๒. เพื่อพัฒนาขีดความสามารถในการจัดการกับภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ของประเทศไทย

๓. เพื่อเสริมสร้างความมั่นคงปลอดภัยด้านไซเบอร์และก่อให้เกิดความสงบสุขในพื้นที่จังหวัดชายแดนภาคใต้ของประเทศไทย

ยุทธศาสตร์ (Strategy) : ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ ประกอบด้วย IADCLIP โดยมีโครงสร้างประกอบด้วย

เป้าหมายยุทธศาสตร์ (Corperate Goal) : ……

แนวทางหรือมาตรการ (Guideline) : ……

ยุทธวิธีหรือแผนปฏิบัติการ (Action Plan) : ……

ดัชนีชี้วัดผลงาน (Key Performance Indicators, KPIs) : ……

ผลที่คาดว่าจะได้รับ (Outcome) : ……

ยุทธศาสตร์ที่ ๑ : ยุทธศาสตร์การจัดโครงสร้างพื้นฐานของประเทศไทยสำหรับใช้ในการจัดการกับภัยคุกคามด้านไซเบอร์ (Infrastructure)

เป้าหมายยุทธศาสตร์ : เพื่อการจัดโครงสร้างพื้นฐานของประเทศไทยสำหรับการจัดการกับภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

แนวทางหรือมาตรการ มีดังต่อไปนี้

๑. การจัดโครงสร้างพื้นฐานของประเทศไทยสำหรับใช้ในการจัดการกับภัยคุกคามด้านไซเบอร์ประกอบด้วย ๑) หน่วยบัญชาการไซเบอร์แห่งชาติ (National Cyber Department), ๒) เทคโนโลยีฮาร์ดแวร์ (Hardware Technology), ๓) เทคโนโลยีซอฟต์แวร์ (Software Technology), ๔) เทคโนโลยีเครือข่ายความเร็วสูง (Hi-Speed Network Technology), ๕) นักปฏิบัติการด้านไซเบอร์ (Cyber Operators) และ ๖) รูปแบบการจัดการภัยคุกคามด้านไซเบอร์ (Cyber Treats Management Format)

๒. การกำหนดรูปแบบการจัดการภัยคุกคามด้านไซเบอร์ที่เหมาะสมและมีประสิทธิภาพโดยคำนึงถึงความมั่นคงปลอดภัยและความสงบสุขของประชาชนอย่างเป็นด้านหลัก

ยุทธวิธีหรือแผนปฏิบัติการ มีดังต่อไปนี้

๑. การนำโครงสร้างพื้นฐานไปใช้จัดตั้งเพื่อกำหนดให้เป็นโครงสร้างหลักในการจัดการภัยคุกคามด้านไซเบอร์

๒. นำรูปแบบของระบบไอซีทีเพื่อการบริหารจัดการองค์กรเพื่อความมั่นคงปลอดภัยโดยเน้นการรักษาความมั่นคงปลอดภัยตามมาตรฐานสากล

ดัชนีชี้วัดผลงาน : ระบบป้องกันภัยคุกคามด้านไซเบอร์และสถิติการบุกรุกเพื่อจารกรรมข้อมูลข่าวสาร

ผลที่คาดว่าจะได้รับตามยุทธศาสตร์ที่ ๑ : ประเทศไทยมีโครงสร้างพื้นฐานสำหรับการจัดการกับภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

ยุทธศาสตร์ที่ ๒ : ยุทธศาสตร์การสร้างการตระหนักรู้โลกไซเบอร์ให้กับประชาชน (Awareness)

เป้าหมายยุทธศาสตร์ : เพื่อการสร้างการตระหนักรู้โลกไซเบอร์ให้กับประชาชนในพื้นที่จังหวัดชายแดนภาคใต้

แนวทางหรือมาตรการ มีดังต่อไปนี้

๑. การสนับสนุนให้ประชาชนมีการสร้างความรู้ความเข้าใจที่ดีต่อการใช้งานด้านไซเบอร์และมีการถ่ายทอดความรู้ความเข้าใจที่ดีต่อการใช้ไซเบอร์เพื่อประโยชน์ส่วนตนรวมถึงประเทศชาติ รวมทั้งมีการถ่ายทอดความรู้ความเข้าใจจากรุ่นไปสู่รุ่น

๒. การเผยแพร่ความรู้และประชาสัมพันธ์ให้ประชาชนมีการใช้งานด้านไซเบอร์อย่างถูกวิธีรวมทั้งตระหนักถึงผลกระทบต่อการใช้งานไซเบอร์ที่ไม่ถูกต้อง เพื่อป้องกันการนำมาใช้เป็นเครื่องมือในการก่อการร้ายในประเทศไทย

ยุทธวิธีหรือแผนปฏิบัติการ มีดังต่อไปนี้

๑. สร้างรูปแบบและวิธีการในการให้ความรู้ความเข้าใจโดยอาจใช้วิธีการฝึกอบรมภายในหน่วยงานหรือการถ่ายทอดความรู้โดยใช้สื่อสารมวลชน

๒. ใช้สถาบันการศึกษาในการถ่ายทอดความรู้ความเข้าใจให้กับเยาวชนโดยอาจบรรจุไว้ในหลักสูตรหรือกิจกรรมเสริมหลักสูตร

๓. กำหนดหลักสูตรที่เกี่ยวกับไซเบอร์ในทุกระดับเพื่อให้เยาวชนได้มีรากฐานของการศึกษาและเข้าใจต่อการใช้งานไซเบอร์อย่างถูกต้อง

๔. พัฒนาหลักสูตรในระดับอุดมศึกษาเพื่อพัฒนาองค์ความรู้ทางไซเบอร์ให้สามารถนำความรู้ไปใช้อย่างครอบคลุมและมีประสิทธิภาพในทุกมิติ

ดัชนีชี้วัดผลงาน : ความรู้ความเข้าใจต่อภัยคุกคามด้านไซเบอร์และรูปแบบการใช้งานด้านไซเบอร์ที่สร้างสรรค์ต่อสังคมโดยไม่ใช่การก่ออาชญากรรม

ผลที่คาดว่าจะได้รับตามยุทธศาสตร์ที่ ๒ : ประชาชนในพื้นที่จังหวัดชายแดนภาคใต้มีความตระหนักรู้ต่อภัยคุกคามด้านไซเบอร์และมีรูปแบบการใช้งานที่ไม่เป็นภัยต่อผลประโยชน์และความมั่นคงของชาติ

ยุทธศาสตร์ที่ ๓ : ยุทธศาสตร์การพัฒนาความก้าวหน้าด้านไซเบอร์ (Development)

เป้าหมายยุทธศาสตร์ : เพื่อการพัฒนาความก้าวหน้าด้านไซเบอร์ของประเทศไทยให้เข้าสู่มาตรฐานสากล

แนวทางหรือมาตรการ มีดังต่อไปนี้

๑. การจัดตั้งหน่วยงานการพัฒนาด้านไซเบอร์เพื่อพัฒนาระบบไอซีทีและการรักษาความปลอดภัยด้านไซเบอร์ข้อมูลข่าวสาร

๒. จัดฝึกอบรมให้ความรู้ สนับสนุนการจัดสอบเพื่อให้บุคลากรผ่านเกณฑ์มาตรฐานสากลรวมทั้งการวิจัยสร้างองค์ความรู้ใหม่ด้านไซเบอร์

๓. การพัฒนาบุคลากรให้มีความเชี่ยวชาญในการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ รวมทั้งสร้างแรงจูงใจในการจงรักภักดีและทำงานเพื่อประเทศชาติเพื่อป้องกันสมองไหลไปยังต่างประเทศ

ยุทธวิธีหรือแผนปฏิบัติการ มีดังต่อไปนี้

๑. การสร้างหน่วยงานด้านความมั่นคงปลอดภัยด้านไซเบอร์ที่มีเครื่องมือและอุปกรณ์ที่ทันสมัย และพร้อมรับมือกับการป้องกัน การโจมตี และการโต้ตอบ

๒. การสร้างชุดกิจกรรมฝึกอบรมกับประชาชนทุกระดับให้ทราบถึงความหมายและการรักษาความปลอดภัยทั้งข้อมูลส่วนตัวและข้อมูลส่วนรวม

๓. จัดโครงการพัฒนาบุคลากรในหน่วยงานด้านความมั่นคงของชาติให้เป็นผู้เชี่ยวชาญด้านไซเบอร์ที่มีศักยภาพสูงและพร้อมปฏิบัติการทุกรูปแบบ

๔. การวิจัยและพัฒนาด้านไซเบอร์ที่เป็นประโยชน์ต่อการพัฒนาประเทศไทยและต่อต้านการก่อการร้ายด้านไซเบอร์

ดัชนีชี้วัดผลงาน : ทุกองค์กรในหน่วยงานด้านความมั่นคงของชาติรวมถึงภาคธุรกิจเอกชนมีผู้เชี่ยวชาญด้านไซเบอร์ที่มีศักยภาพสูงและงานวิจัยที่มีคุณภาพ

ผลที่คาดว่าจะได้รับตามยุทธศาสตร์ที่ ๓ : ประเทศไทยมีความก้าวหน้าด้านไซเบอร์และมีรูปแบบการบริหารจัดการเทียบเท่ามาตรฐานสากล ทำให้เป็นจุดเริ่มต้นของการสร้างความสงบสุขในพื้นที่จังหวัดชายแดนภาคใต้

ยุทธศาสตร์ที่ ๔ : ยุทธศาสตร์การส่งเสริมความร่วมมือด้านไซเบอร์ระหว่างภาครัฐ ภาคเอกชน และภาคประชาชน (Coordinate)

เป้าหมายยุทธศาสตร์ : เพื่อการสร้างความร่วมมือด้านไซเบอร์ระหว่างภาครัฐ ภาคเอกชน และภาคประชาชน

แนวทางหรือมาตรการ มีดังต่อไปนี้

๑. มีการเสริมสร้างความเข้าใจร่วมกันในการกำหนด นิยาม ความหมายของภัยคุกคามและการก่อการร้ายด้านไซเบอร์

๒. มีการกำหนดนโยบาย แนวทาง และแผนปฏิบัติการที่ชัดเจนเพื่อให้เกิดการแปลงแผนไปสู่กลยุทธ์และไปสู่การปฏิบัติตามวิสัยทัศน์ พันธกิจ และเป้าประสงค์ที่กำหนดไว้อย่างมีประสิทธิภาพ

๓. กำหนดกลไกในการทบทวน ติดตาม และประเมินความเสี่ยงต่อการนำแผนงานไปปรับใช้เพื่อปรับแนวทางให้มีความเหมาะสมตามสถานการณ์ใหม่หรือสถานการณ์ที่แตกต่าง

ยุทธวิธีหรือแผนปฏิบัติการ มีดังต่อไปนี้

๑. การใช้หน่วยบัญชาการไซเบอร์แห่งชาติเป็นศูนย์กลางเพื่อร่วมกันกำหนด นิยามความหมายของภัยคุกคามด้านไซเบอร์ การก่อการร้าย และการก่อการร้ายทางไซเบอร์

๒. การกำหนดนโยบาย แนวทาง และแผนปฏิบัติการที่ชัดเจนเพื่อนำไปสู่การปฏิบัติตามวิสัยทัศน์ พันธกิจ และเป้าประสงค์ที่กำหนดของทุกภาคส่วนอย่างมีประสิทธิภาพและประสิทธิผล

๓. การสร้างกลไกเฉพาะในการทบทวน ติดตาม และประเมินความเสี่ยงของภัยคุกคามด้านไซเบอร์ต่อการนำแผนงานไปปรับใช้อย่างมีประสิทธิภาพและประสิทธิผล

ดัชนีชี้วัดผลงาน : รูปแบบการใช้งานด้านไซเบอร์ที่มีประสิทธิภาพและประสิทธิผลทั้งในระดับองค์กรและระดับบุคคล

ผลที่คาดว่าจะได้รับตามยุทธศาสตร์ที่ ๔ : ทุกภาคส่วนของประเทศไทยมีความร่วมมือในการต่อต้านการก่อการร้ายด้านไซเบอร์โดยเฉพาะอย่างยิ่งในพื้นที่จังหวัดชายแดนภาคใต้

ยุทธศาสตร์ที่ ๕ : ยุทธศาสตร์การกำหนดใช้กฎหมายด้านไซเบอร์และการบังคับใช้กับประชาชน (Law and Enforcement)

เป้าหมายยุทธศาสตร์ : เพื่อการผลักดันการใช้กฎหมายสำหรับอาชญากรไซเบอร์ที่สร้างความรุนแรงในพื้นที่จังหวัดชายแดนภาคใต้

แนวทางหรือมาตรการ มีดังต่อไปนี้

๑. กำหนดกฎหมาย กฎระเบียบ ขั้นตอน และแนวปฏิบัติที่เกี่ยวข้องกับการใช้ด้านไซเบอร์ ความมั่นคงปลอดภัยด้านไซเบอร์ และการต่อต้านการก่อการร้ายด้านไซเบอร์อย่างครอบคลุม

๒. กำหนดแนวทางที่ชัดเจนและเหมาะสมต่อการบังคับใช้กฎหมาย พร้อมทั้งมาตรการและบทลงโทษต่อการกระทำอันเกี่ยวข้องกับก่อการร้ายด้านไซเบอร์

ยุทธวิธีหรือแผนปฏิบัติการ มีดังต่อไปนี้

๑. การใช้หน่วยงานทางกฎหมายร่วมกันกำหนดกฎหมาย กฎระเบียบ ขั้นตอน และแนวปฏิบัติที่เกี่ยวข้องกับการใช้งานด้านไซเบอร์ ความมั่นคงปลอดภัยด้านไซเบอร์ และรูปแบบการต่อต้านการก่อการร้ายด้านไซเบอร์

๒. การใช้หน่วยงานทางกฎหมายร่วมกันกำหนดแนวทางที่ชัดเจนและเหมาะสมต่อการบังคับใช้กฎหมาย พร้อมทั้งมาตรการและบทลงโทษต่อการกระทำอันเกี่ยวข้องกับก่อการร้ายด้านไซเบอร์

ดัชนีชี้วัดผลงาน : กฎหมาย กฎระเบียบ ขั้นตอน และแนวปฏิบัติที่เกี่ยวข้องกับการใช้ด้านไซเบอร์ที่มีประสิทธิภาพและประสิทธิผลทั้งในระดับองค์กรและระดับบุคคล

ผลที่คาดว่าจะได้รับตามยุทธศาสตร์ที่ ๕ : ประเทศไทยมีกฎหมาย กฎระเบียบ ขั้นตอน และแนวปฏิบัติที่เกี่ยวข้องกับการใช้ด้านไซเบอร์ในการต่อต้านการก่อการร้ายและการสร้างความไม่สงบสุขในพื้นที่จังหวัดชายแดนภาคใต้

ยุทธศาสตร์ที่ ๖ : ยุทธศาสตร์การใช้การบูรณาการร่วมกันเพื่อแบ่งปันข้อมูลข่าวสาร (Integration)

เป้าหมายยุทธศาสตร์ : เพื่อการใช้การบูรณาการร่วมกันเพื่อแบ่งปันข้อมูลข่าวสารในพื้นที่จังหวัดชายแดนภาคใต้อย่างถูกวิธีและไม่ส่งผลกระทบต่อความมั่นคงแห่งชาติ

แนวทางหรือมาตรการ มีดังต่อไปนี้

๑. การใช้หน่วยบัญชาการไซเบอร์แห่งชาติที่มีหน้าที่ในการกำกับดูแลและดำเนินการด้านไซเบอร์ มีการแบ่งปันข้อมูลร่วมกันเพื่อประโยชน์ของประชาชน รวมทั้งมีการบูรณาการการทำงานร่วมกัน อีกทั้งระบุโอกาส และความท้าทายในการเพิ่มขีดความสามารถของกลไกการตอบสนองต่อการก่อการร้ายรูปแบบต่างๆ

๒. การสร้างฐานข้อมูลกลางเพื่อรวบรวมข้อมูลสำคัญจากทุกภาคส่วน รวมทั้งมีการควบคุมดูแลเพื่อไม่ให้ข้อมูลถูกเผยแพร่ ตลอดจนเปิดโอกาสให้ทุกหน่วยงานที่เกี่ยวข้องกับไซเบอร์สามารถดึงข้อมูลไปใช้ในทางที่ถูกต้องและเป็นประโยชน์ต่อชาติบ้านเมือง

๓. จัดตั้งสำนักข่าวกรองด้านไซเบอร์ เพื่อทำงานด้านการข่าวด้านไซเบอร์ แบ่งปันข้อมูลข่าวสาร และประสานงานความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้อง

ยุทธวิธีหรือแผนปฏิบัติการ มีดังต่อไปนี้

๑. การกำหนดภารกิจและบทบาทของหน่วยบัญชาการไซเบอร์แห่งชาติในด้านการกำกับดูแลและดำเนินการด้านไซเบอร์เพื่อต่อต้านการก่อการร้ายด้านไซเบอร์

๒. การสร้างฐานข้อมูลกลางโดยระดมผู้เชี่ยวชาญด้านการออกแบบและพัฒนาระบบไอซีทีที่มีศักยภาพในการสร้างฐานข้อมูลที่มีความมั่นคงปลอดภัยในระดับสูงสุด

๓. การกำหนดภารกิจและบทบาทของสำนักข่าวกรองด้านไซเบอร์เพื่องานด้านการข่าวที่เกิดจากการประสานความร่วมมือกันของทุกภาคส่วน

ดัชนีชี้วัดผลงาน : หน่วยบัญชาการไซเบอร์แห่งชาติและสำนักข่าวกรองด้านไซเบอร์มีรูปแบบภารกิจที่สนับสนุนงานด้านไซเบอร์ที่ได้มาตรฐาน

ผลที่คาดว่าจะได้รับตามยุทธศาสตร์ที่ ๖ : ประเทศไทยมีการใช้การบูรณาการร่วมกันเพื่อแบ่งปันข้อมูลข่าวสารที่เป็นประโยชน์เพื่อรักษาผลประโยชน์ของชาติและต่อต้านการก่อการร้ายด้านไซเบอร์

ยุทธศาสตร์ที่ ๗ : ยุทธศาสตร์การรับรู้ด้านไซเบอร์เพื่อการป้องกัน การยับยั้ง และการโจมตี (Perception)

เป้าหมายยุทธศาสตร์ : เพื่อให้เกิดการรับรู้ด้านไซเบอร์ทั้งการป้องกัน การยับยั้ง และการโจมตีด้านไซเบอร์

แนวทางหรือมาตรการ มีดังต่อไปนี้

๑. การปลูกฝังทัศนคติและแนวทางการใช้งานไซเบอร์ที่เป็นรูปธรรมเพื่อให้ประชาชนมีการรับรู้ต่อการใช้งานไซเบอร์ในทางที่ถูกต้องและไม่เป็นภัยต่อความมั่นคงของชาติ

๒. การสร้างรูปแบบการมีส่วนร่วมของทุกภาคส่วน รวมทั้งวิธีการในการตระเตรียมตนเองเพื่อให้เกิดการปฏิบัติอย่างรู้เท่าทัน

ยุทธวิธีหรือแผนปฏิบัติการ มีดังต่อไปนี้

๑. การกำหนดรูปแบบการปลูกฝังทัศนคติและแนวทางการใช้งานไซเบอร์ที่เป็นรูปธรรมเพื่อให้ประชาชนมีการรับรู้ต่อการใช้งานไซเบอร์ในทางที่ถูกต้องและไม่ส่งผลกระทบต่อความมั่นคงแห่งชาติ

๒. การสร้างรูปแบบการมีส่วนร่วมของทุกภาคส่วน รวมทั้งวิธีการในการตระเตรียมตนเองและใช้มาตรการต่างๆ เพื่อให้เกิดการปฏิบัติอย่างรู้เท่าทัน

ดัชนีชี้วัดผลงาน : ทัศนคติในการใช้งานไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้มีประโยชน์ต่อการพัฒนาประเทศทุกมิติ

ผลที่คาดว่าจะได้รับตามยุทธศาสตร์ที่ ๗ : ทุกภาคส่วนมีการรับรู้ด้านไซเบอร์เพื่อการป้องกัน การยับยั้ง และการโจมตี

ผลที่คาดว่าจะได้รับ (Outcomes) :

๑. ภาครัฐมียุทธศาสตร์ที่มีประสิทธิภาพในการจัดการกับภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

๒. ขีดความสามารถในการจัดการกับภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ของประเทศไทยเพิ่มขึ้น

๓. ทำให้เกิดความมั่นคงปลอดภัยด้านไซเบอร์และก่อให้เกิดความสงบสุขในพื้นที่จังหวัดชายแดนภาคใต้ของประเทศไทย

ผลจากความเสียหายที่เกิดจากภัยคุกคามด้านไซเบอร์ที่ผ่านมา ทำให้รัฐบาลไทยตระหนักดีถึงผลกระทบทั้งในแง่ที่เป็นประโยชน์และโทษจากการทำสงครามไซเบอร์ โดยพยายามพัฒนาขีดความสามารถด้านการทำสงครามไซเบอร์ทั้งในเชิงรุกและการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ เพื่อใช้เป็นมาตรการทั้งเชิงรุกและเชิงรับจากการโจมตีด้านไซเบอร์ของฝ่ายตรงข้าม (สราวุธ ปิติยาศักดิ์, ๒๕๖๑) ประเด็นสำคัญของนโยบายด้านการทำสงครามไซเบอร์ของประเทศไทย ในส่วนรัฐบาลและหน่วยงานด้านความมั่นคงที่เกี่ยวข้อง มีดังนี้

(๑) ก่อนที่จะนำนโยบายหรือกฎหมายฉบับใดที่เกี่ยวข้องกับโลกไซเบอร์มาประกาศใช้ รัฐบาลต้องประชาสัมพันธ์ให้ประชาชนมีความเข้าใจอย่างแท้จริง เกี่ยวกับวัตถุประสงค์ ประโยชน์ที่ประชาชนจะพึงได้รับ และผลกระทบที่จะตามมา เพื่อป้องกันการเกิดข่าวลือที่ไม่พึงประสงค์ และกระแสต่อต้านของประชาชนในสื่อสังคมออนไลน์

(๒) องค์กรและหน่วยงานทั่วไปที่มีการใช้งานในโลกไซเบอร์ ควรมีมาตรการการรักษาปลอดภัยด้านไซเบอร์ (Cyber Security Measures) สำหรับหน่วยงานของตน

(๓) ในระดับประเทศ ควรมีหน่วยงานไซเบอร์เป็นการเฉพาะที่ให้การรักษาความมั่นคงปลอดภัยด้านไซเบอร์และการบริการประชาชนในการเฝ้าระวัง แจ้งเตือนภัย และการแก้ไขปัญหา เพื่อสร้างความเชื่อมั่นและความมั่นใจในการใช้งานในโลกไซเบอร์

(๔) ควรมีกลไกในการตัดสินใจภายใต้ประเมินความเสี่ยงเพื่อให้สามารถตอบสนองต่อการโจมตีด้านไซเบอร์ของฝ่ายตรงข้ามได้อย่างเหมาะสม และ พิจารณาถึงผลกระทบที่จะตามมา รวมถึงอาศัยภาวะผู้นำของผู้บริหารในการตัดสินใจที่ไม่ใช่มุ่งเน้นในเรื่อง “การป้องกัน” มากเกินไปจนละเลยหรือเพิกเฉยต่อ “การตอบโต้” กับการโจมตีดังกล่าว

(๕) ควรกำหนดทิศทางแก้ไขปัญหาและมาตรการตอบโต้การโจมตีด้านไซเบอร์ที่เหมาะสม โดยแต่ละหน่วยงานภาครัฐจะต้องตรวจสอบดูว่า นโยบายที่กำหนดขึ้นเพื่อการป้องกันและตอบโต้ต่อการโจมตีด้านไซเบอร์ของตนสามารถปฏิบัติได้จริง มีช่องโหว่ หรือปัญหาอะไรหรือไม่ โดยนโยบายดังกล่าวจะต้องเป็นนโยบายที่สามารถดำเนินการได้ในสภาพความเป็นจริงด้วย

(๖) ควรเสริมสร้างความรู้ความเข้าใจโลกไซเบอร์แก่เจ้าหน้าที่ภาครัฐและประชาชนทั่วไป โดยมุ่งเน้นในเรื่องมาตรการป้องกันมากกว่าการบังคับใช้กฎหมายหรือระเบียบที่เข้มงวดซึ่งเป็นการแก้ไขปัญหานี้ที่ปลายเหตุ เพราะยิ่งมีกฎหมายหรือระเบียบที่เข้มงวดมากขึ้นเท่าใด คนก็จะ

พยายามหลีกเลี่ยงมากขึ้นเท่านั้น ดังนั้น การดำเนินนโยบายหรือการหาช่องทางในการปิดกั้นหรือตัดขาดการรับรู้ของประชาชนจากโลกไซเบอร์ในสภาพแวดล้อมของโลกในปัจจุบันจึงเป็นสิ่งที่ทำไม่ได้อีกแล้ว หรือหากกระทำได้ก็จะเป็นการฝืนมติมหาชนอย่างรุนแรง ด้วยเหตุนี้ แนวทางที่ดีที่สุดต่อการดำเนินการด้านไซเบอร์ของรัฐบาลและหน่วยงานที่เกี่ยวข้อง ก็คือ “การสร้างความเข้าใจให้กับประชาชน” เพื่อให้ประชาชนไว้เนื้อเชื่อใจต่อการดำเนินงานของรัฐบาล ไม่ใช่การออกกฎหมายเพื่อใช้บังคับกับประชาชนเพียงอย่างเดียว

(๗) ควรมีกฎหมายด้านไซเบอร์เป็นการเฉพาะ เพื่อกำหนดกฎกติกาทางสังคมของโลกไซเบอร์และมาตรการป้องปรามป้องกันการละเมิดกฎหมาย โดยกฎหมายจะเป็นเครื่องมือที่สำคัญอย่างมากสำหรับการสร้างโลกไซเบอร์ที่ปลอดภัย รวมถึงการมีหน่วยงานที่สามารถบังคับใช้กฎหมายด้านไซเบอร์อย่างจริงจัง

โดยในส่วนกำลังพลของกองทัพและประชาชนทั่วไป มีดังนี้

ในฐานะปัจเจกชน โลกไซเบอร์ย่อมถือได้ว่าอาจเป็นคุณอย่างมหาศาลหรืออาจเป็นโทษอย่างอนันต์ก็ได้ อย่างไรก็ตาม ภัยคุกคามที่มาพร้อมกับประโยชน์ที่ได้จากโลกไซเบอร์นี้อาจเกิดขึ้นได้ตลอดเวลาและมีความเสี่ยงสูงที่ผู้ใช้งานด้านต่างๆ ในโลกไซเบอร์จะต้องประสบกับปัญหาจากภัยคุกคามในโลกไซเบอร์ดังกล่าว ดังนั้น กำลังพลของกองทัพหรือประชาชนทั่วไปที่มีส่วนเกี่ยวข้องกับการแสวงประโยชน์จากโลกไซเบอร์พึงต้องตระหนักถึงภัยคุกคามและผลกระทบที่จะเกิดขึ้นตามมา รวมถึงให้ความสำคัญกับการรักษาความปลอดภัยในโลกไซเบอร์อย่างเคร่งครัดในเบื้องต้น ดังนี้

(๑) ไม่ควรระบุข้อมูลส่วนตัวในการลงทะเบียนสมาชิก (Registration) ที่เกินความจำเป็น และเผยแพร่สู่สาธารณะ เช่น ชื่อ/นามสกุลจริง วันเดือนปีเกิด สถานที่เกิด ภูมิลำเนา สถานที่ทำงาน หมายเลขโทรศัพท์ และอีเมล์ เป็นต้น เพราะอาจจะถูกใช้เป็นข้อมูลอ้างอิงให้กับผู้ประสงค์ร้าย และคาดเดารหัสผ่าน (Password) ที่ใช้อยู่ได้

(๒) ควรกำหนดรหัสผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยปฏิบัติตามกฎการรักษาความปลอดภัยด้านสารสนเทศ ควรเปลี่ยนแปลงรหัสผ่านด้วยตนเองในภายหลังตามที่ระบบกำหนด หรือเปลี่ยนตามห้วงระยะเวลา และควรหลีกเลี่ยงการกำหนดรหัสที่เป็นชื่อ วันเดือนปีเกิด หรือรหัสอื่นๆ ที่นักเจาะระบบสามารถเดาสุ่มได้ ไม่ควรเปิดเผยรหัสผ่านให้ผู้อื่นทราบโดยเฉพาะการให้ผู้อื่นนำรหัสผ่านของตนมาเข้าใช้งานแทน เพราะอาจมีการนำไปใช้งานในทางที่มิชอบ และไม่ควรจดบันทึกรหัสผ่านลงในบัตรอิเล็กทรอนิกส์ บัตรเครดิต และกระดาษบันทึก หรือบันทึกลงในโทรศัพท์มือถือ เป็นต้น เพราะมีโอกาสสูญหายและรั่วไหลไปยังบุคคลอื่นได้

(๓) ไม่ควรนำข้อมูลแผนการต่างๆ อย่างละเอียดเผยแพร่บนสื่อสาธารณะ เช่น แผนการเดินทางส่วนตัว ข้อมูลแผนที่เกี่ยวกับที่อยู่อาศัย และระบุชื่อบุคคลในรูปภาพ (ติด Tag) เพราะจะเป็นข้อมูลให้กับเหล่ามิจฉาชีพ อาจถูกนำไปใช้ในทางมิชอบ หรือส่งผลกระทบต่อกองทัพ

(๔) ไม่ควรปล่อยให้เด็กใช้งานระบบคอมพิวเตอร์หรือระบบเครือข่ายโดยอิสระ โดยขาดการตรวจสอบ ควบคุม กำกับดูแลของผู้ใหญ่ เพราะเด็กอาจจะนำข้อมูลที่ไม่เหมาะสมไปเผยแพร่ด้วยความคึกคะนอง ไม่ตั้งใจ ไม่ทันคิด หรืออาจจะถูกล่อลวงไปในทางมิชอบ

(๕) หลีกเลี่ยงการนำเสนอข้อมูลพฤติกรรมส่วนตัวที่ส่งผลกระทบต่อความสงบเรียบร้อยทางสังคม เช่น ภาพการดื่มสุรา สูบบุหรี่ การกระทำที่ก้าวร้าวรุนแรง และการทารุณกรรม เป็นต้น เพราะอาจจะถูกนำไปใช้เป็นเครื่องมือในทางมิชอบ หรือนำไปสู่การเลียนแบบพฤติกรรมที่ไม่ดี

(๖) ไม่ใช้บริการเครือข่ายสังคมออนไลน์ที่ไม่แน่ใจในเรื่องของความปลอดภัย แต่ให้เลือกใช้งานเฉพาะกลุ่มและสมาชิกที่มีความรู้จักมักคุ้น มีความเชื่อถือไว้ใจได้ มีความปลอดภัย และมีพฤติกรรมที่เหมาะสม ทั้งนี้เพื่อป้องกันข้อมูลข่าวสารของกลุ่มและสมาชิกในกลุ่มไม่ให้ถูกเผยแพร่ไปสู่ที่อื่น

(๗) ระบบงานที่มีความสำคัญยิ่ง ควรใช้อุปกรณ์ทางชีวภาพ (Biometric Device) เช่น การสแกนลายนิ้วมือ (Finger Scan) การสแกนฝ่ามือ (Palm Scan) และการสแกนม่านตา (Eye Scan) เป็นต้น เพื่อใช้เป็นอุปกรณ์ตรวจสอบลักษณะส่วนบุคคลทางชีวภาพ และเป็นการยืนยันตัวบุคคล (Authentic) ประกอบกับการใช้รหัสผ่านเพื่ออนุญาตการเข้าใช้งานโปรแกรม ระบบงาน หรือการเข้าใช้ห้องระบบคอมพิวเตอร์

(๘) การใช้งานเครือข่ายอินเตอร์เน็ตสาธารณะแบบไร้สาย (Public WiFi) หรือเครือข่ายอินเตอร์เน็ตไร้สายฟรี (Free WiFi) ผู้ใช้พึงต้องระมัดระวัง รอบคอบ และมั่นใจว่าได้ในเรื่องความปลอดภัย ไม่ควรติดตั้งระบบอินเตอร์เน็ตไร้สายฟรี เพราะจะเป็นช่องทางให้นักเจาะระบบหรือผู้ไม่ประสงค์ดีเข้ามาใช้งานในทางมิชอบและเจาะระบบเข้าถึงข้อมูลในองค์กรได้อย่างง่ายดาย รวมถึงส่งผลต่อการทำงานและก่อปัญหาให้กับองค์กรในภาพรวมได้อีกด้วย

จากผลการศึกษาสามารถนำมาสร้างแนวทางการป้องกันภัยคุกคามทางอินเตอร์เน็ตเพื่อการรักษาความมั่นคงปลอดภัยของข้อมูลข่าวสารดังนี้ (ปริญญา หอมเอนก, ๒๕๖๑)

๑. การป้องกันภัยคุกคามทางอินเตอร์เน็ตสำหรับหน่วยงาน

๑.๑ ตรวจสอบและยืนยันสิทธิการเข้าระบบที่สำคัญของบัญชีผู้ใช้ให้สอดคล้องกับความจำเป็นเข้าถึงระบบและข้อมูล

๑.๒ เพิ่มมาตรการป้องกันเว็บไซต์สำคัญด้วยระบบการป้องกันการโจมตี เช่น Web Application Firewall หรือ DDoS

๑.๓ แจ้งเจ้าหน้าที่ของหน่วยงานและพนักงานให้เพิ่มความระมัดระวังในการใช้อินเตอร์เน็ตโดยหลีกเลี่ยงการเข้าเว็บไซต์ที่ไม่เหมาะสม ไม่คลิกไฟล์แนบจากผู้อื่นกรณีที่ไม่ได้ตกลงกันก่อนหรือไม่รับเมล์แนบจากคนที่ไม่รู้จัก ระมัดระวังความเสี่ยงจากการเปิดไฟล์ผ่านโปรแกรมสนทนาต่างๆ หรือช่องทางเครือข่ายออนไลน์ทุกชนิด ทั้งนี้เพื่อหลีกเลี่ยงการติดมัลแวร์

๑.๔ หากพบพิรุธว่าระบบถูกโจมตี เช่น ไม่สามารถเข้าใช้งานระบบ/เว็บไซต์ได้ หรือมีความล่าช้ากว่าปกติ ควรตรวจสอบข้อมูลการเข้าถึงระบบที่สำคัญ เช่น ข้อมูล Log ย้อนหลัง ๓๐ วัน เพื่อตรวจหาความผิดปกติในการเข้าถึงข้อมูล

๑.๕ การตั้งค่าระบบงานที่สำคัญให้บันทึกเหตุการณ์ (Log) การเข้าใช้งานระบบไม่ต่ำกว่า ๙๐ วัน หรือตามที่กฎหมายกำหนด

๑.๖ หากเป็นไปได้ ให้หน่วยงานส่งรายชื่อผู้ติดต่อ (Contact Point) กรณีเกิดเหตุภัยคุกคามด้านไซเบอร์มายังศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย : ThaiCERT (ไทยเซิร์ต) เพื่อการตรวจสอบที่ถูกต้อง

๒. การป้องกันภัยคุกคามทางอินเตอร์เน็ตสำหรับประชาชนทั่วไป

๒.๑ เพิ่มความระมัดระวังในการใช้อินเตอร์เน็ต โดยหลีกเลี่ยงการเข้าเว็บไซต์ที่ไม่เหมาะสม เว็บผิดกฎหมาย ไม่คลิกไฟล์แนบจากผู้อื่นกรณีที่ไม่ได้ตกลงกันหรือไม่รู้จักกันมาก่อน ระมัดระวังความเสี่ยง จากการเปิดไฟล์ผ่านโปรแกรมแชตต่างๆ หรือช่องทาง Social Media เพื่อหลีกเลี่ยงการติดมัลแวร์ ซึ่งนับวันมัลแวร์จะมาจากพวกไฟล์แนบทางเครือข่ายสังคมออนไลน์เพิ่มมากขึ้น

๒.๒ การใช้บริการอินเตอร์เน็ต อย่าตั้งรหัสผ่านเหมือนกันทุกระบบ เพราะหากคุณโดนแฮกเกอร์เจาะระบบสำเร็จแล้ว ระบบอื่นๆ ก็อาจถูกเจาะระบบด้วยหากใช้รหัสผ่านเดียวกัน

๒.๓ ติดตามข้อมูลข่าวสารเกี่ยวกับความมั่นคงปลอดภัยด้านไซเบอร์ และอ่านพิจารณาข้อมูลก่อนการแชร์ข้อมูลทุกครั้ง ตลอดจนไม่ส่งต่อข้อมูลที่ไม่ได้รับการยืนยันจากผู้ที่เกี่ยวข้อง

ข้อเสนอแนะเชิงนโยบาย

๑. การบริหารจัดการภาครัฐและการบูรณาการยุทธศาสตร์

๑.๑ ภาครัฐควรปรับปรุงระบบบริหารจัดการภัยคุกคามด้านไซเบอร์ให้เป็นระบบที่มีความชัดเจนสมบูรณ์ครบถ้วนเพียงระบบเดียว (Comprehensive System) ทั้งนี้เพื่อเพิ่มประสิทธิภาพของหน่วยงานภาครัฐในการขับเคลื่อนยุทธศาสตร์เชิงบูรณาการ และเอื้ออำนวยต่อ

การบริหารจัดการยุทธศาสตร์ขององค์กร รวมทั้งขจัดข้อจำกัดหรือก้าวข้ามกับดักในการพัฒนาระบบบริหารจัดการเพื่อนำไปสู่ความเป็นรัฐบาลดิจิทัลอย่างแท้จริง

๑.๒ ภาครัฐควรจัดตั้งศูนย์อำนวยการขับเคลื่อนยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ที่มีหน้าที่วางแผนเชิงบูรณาการ อำนวยการ ประสานงาน เฝ้าติดตามและรายงานความก้าวหน้าในการขับเคลื่อนยุทธศาสตร์ จัดทำฐานข้อมูลร่วม เสนอแนะแนวทางแก้ปัญหาในเชิงบูรณาการ สรุปผลการปฏิบัติในภาพรวมในห้วงระยะเวลาที่เหมาะสม และสร้างความรู้ความเข้าใจที่ถูกต้องให้ทุกภาคส่วนและประชาชน

๑.๓ ภาครัฐเร่งรีบในการทบทวนภารกิจหน้าที่ของหน่วยงานภาครัฐให้เป็นไปตามยุทธศาสตร์ที่กำหนด นำทฤษฎีการจัดองค์กรภาครัฐแนวใหม่มาวิเคราะห์และปรับโครงสร้างของหน่วยงานให้เหมาะสมและมีประสิทธิภาพ รวมทั้งปรับปรุงกระบวนการให้กระชับรวดเร็วและทันต่อสถานการณ์แห่งภัยคุกคามด้านไซเบอร์

๑.๔ ภาครัฐดำเนินการปรับเปลี่ยนบทบาทเป็นผู้อำนวยความสะดวกและกำหนดกติกาให้เกิดความเป็นธรรมโดยให้ภาควิชาการและเอกชนเป็นกลไกหลักในการขับเคลื่อนยุทธศาสตร์ด้านไซเบอร์

๑.๕ ภาครัฐดำเนินการปรับแนวคิดให้หน่วยงานในกำกับมีความรับผิดชอบอย่างแท้จริง กล่าวคือ มีทั้ง Responsibility และ Accountability ในการปฏิบัติงาน และการปรับเปลี่ยนวัฒนธรรมองค์กรเพื่อให้การปฏิบัติงานอย่างต่อเนื่อง มุ่งมั่นและจริงจัง เพื่อตอบสนองต่อการพัฒนาประเทศให้ยั่งยืน

๑.๖ ภาครัฐเสริมสร้างความพร้อมในการปฏิบัติงานของหน่วยงานที่เกี่ยวข้องทั้งในด้านบุคลากร งบประมาณ หรือทรัพยากรอื่นๆ เพื่อให้สามารถปฏิบัติงานตามยุทธศาสตร์ให้มีประสิทธิภาพและประสิทธิผล

๑.๗ ภาครัฐส่งเสริมให้กฎหมายและระเบียบปฏิบัติต่างๆ ที่เกี่ยวข้องเป็นเครื่องมือในการขับเคลื่อนยุทธศาสตร์ด้านไซเบอร์และกำหนดวงรอบให้หน่วยงานเปิดรับฟังความคิดเห็นเพื่อทบทวนปรับปรุงแก้ไขกฎหมายให้ทันสมัยและมีประสิทธิภาพอยู่ตลอดเวลา โดยสอดคล้องและเอื้ออำนวยต่อการปฏิบัติงานของหน่วยงานที่เกี่ยวข้อง

๒. การแปลงยุทธศาสตร์เป็นการปฏิบัติ

๒.๑ ภาครัฐควรกำหนดแนวทางในการแปลงยุทธศาสตร์ชาติด้านไซเบอร์ให้เป็นยุทธศาสตร์รองลงมา และถ่ายทอดลงมาเป็นแผนงานและโครงการ นโยบายหรือมาตรการหรือการปฏิบัติในลักษณะอื่นอย่างเป็นระบบ

๒.๒ ภาครัฐควรกำหนดให้ศูนย์ตรวจสอบประเมินผลยุทธศาสตร์ซึ่งเป็นหน่วยงานกลางที่เป็นอิสระ โดยตรวจสอบว่าสอดคล้องกับเป้าประสงค์และเจตนารมณ์ที่แท้จริงของยุทธศาสตร์หลักหรือไม่

๓. การพัฒนาและบริหารจัดการบุคลากรด้านไซเบอร์

๓.๑ ภาครัฐควรเสริมสร้างความรู้ความเข้าใจที่ถูกต้องเกี่ยวกับยุทธศาสตร์ด้านไซเบอร์ให้กับบุคลากรภาครัฐ เสริมสร้างทักษะในการทำงานเป็นทีม รวมทั้งการเตรียมความพร้อมของบุคลากรในการร่วมจัดทำยุทธศาสตร์ที่รองรับขององค์กร

๓.๒ ภาครัฐควรปลูกฝังจิตสำนึกและอุดมการณ์ในการทำงานเพื่อส่วนรวมและองค์กรให้กับบุคลากรอย่างต่อเนื่อง รวมทั้งส่งเสริมให้เป็นผู้เชี่ยวชาญด้านไซเบอร์ในระดับนานาชาติตลอดการรับราชการ

๓.๓ ภาครัฐจัดทำแผนงานพัฒนาบุคลากรและระบบบริหารจัดการที่สอดคล้องกับการดำเนินยุทธศาสตร์ โดยเริ่มศึกษาวิเคราะห์ระบบพัฒนาผู้เชี่ยวชาญด้านไซเบอร์ระดับสูง รวมถึงการพิจารณาคัดเลือกนักวิชาการและเยาวชนที่มีศักยภาพสูง (High Potential) อย่างเป็นระบบ

๓.๔ ภาครัฐมุ่งมั่นปลุกฝังจิตสำนึกในการบริการ กระตุ้นให้เกิดความกระตือรือร้น ความเอาใจใส่ จริงจังในการปฏิบัติงาน รวมทั้งปรับปรุงอุปนิสัยและบุคลิกภาพให้กับบุคลากรด้านไซเบอร์ของประเทศไทย

๔. การมีส่วนร่วมของทุกภาคส่วนและการสื่อสารทางยุทธศาสตร์

๔.๑ ภาครัฐเสริมสร้างความเชื่อมั่นให้กับสังคมไทยเรื่องความมั่นคงปลอดภัยด้านไซเบอร์ และสร้างความเชื่อมั่นให้กับประชาคมโลกในความมุ่งมั่นจริงจังของทุกฝ่ายที่จะดำเนินการตามยุทธศาสตร์ชาติด้านไซเบอร์

๔.๒ ภาครัฐส่งเสริมการมีส่วนร่วมของทุกภาคส่วนเพื่อให้ยุทธศาสตร์ได้รับการยอมรับและได้รับการสนับสนุนจากทุกฝ่าย รวมทั้งชี้แจงถึงผลประโยชน์ชาติและประโยชน์ที่ทุกภาคส่วนจะได้รับจากการปฏิบัติตามยุทธศาสตร์

๔.๓ ภาครัฐนำแนวคิดในการสื่อสารยุทธศาสตร์ด้านไซเบอร์มาใช้ในการสร้างความรู้ความเข้าใจที่ถูกต้องให้กับประชาชนทั่วไปและผู้มีส่วนได้ส่วนเสียโดยใช้การประชาสัมพันธ์เชิงรุกเป็นเครื่องมือหลัก

๕. การตรวจสอบประเมินผลยุทธศาสตร์

๕.๑ ภาครัฐควรรีบเร่งปรับปรุงการประเมินผลยุทธศาสตร์ให้เป็นไปด้วยความจริงจังและเที่ยงตรง

๕.๒ ภาครัฐส่งเสริมเพิ่มเติมการทบทวนปรับปรุงแก้ไขยุทธศาสตร์ด้านไซเบอร์ในห้วงระยะเวลาที่เหมาะสมหรือเมื่อมีความจำเป็นเข้าไปในกระบวนการ

๕.๓ ภาครัฐควรจัดตั้งศูนย์ตรวจสอบประเมินผลยุทธศาสตร์โดยเป็นหน่วยงานอิสระที่ขึ้นตรงต่อนายกรัฐมนตรี โดยมีหน้าที่ตรวจสอบความก้าวหน้าและการประเมินผลโดยบุคลากรที่เป็นตัวแทนของทุกภาคส่วนที่มีความรู้ความสามารถและสมรรถนะที่เมหาะสมและได้รับการยอมรับจากทุกฝ่าย

๕.๔ ภาครัฐจัดให้มีการตรวจสอบตัวชี้วัดของหน่วยงานด้านไซเบอร์ให้ได้มาตรฐาน ตรงประเด็นเหมาะสมกับบริบทหรือสภาพความเป็นจริง โดยสามารถชี้วัดความสำเร็จของยุทธศาสตร์ชาติด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างแท้จริง

สรุป

การศึกษาในบทที่ ๔ มีความมุ่งหมายเพื่อกำหนดยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ ซึ่งเป็นการศึกษาเพื่อตอบวัตถุประสงค์ข้อที่ ๓ ผลการศึกษาสามารถสรุปได้ดังนี้

บทนี้นำเสนอข้อมูลการวิเคราะห์ผลกระทบของภัยคุกคามด้านไซเบอร์ แนวทางการจัดการภัยคุกคามด้านไซเบอร์ของต่างประเทศ การวิเคราะห์รูปแบบที่เหมาะสมของการจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ และการวิเคราะห์ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ ซึ่งข้อมูลสรุปมีดังนี้

แนวทางการจัดการภัยคุกคามด้านไซเบอร์ของต่างประเทศนั้นมีรูปแบบและแนวทางที่ต่างกัน เนื่องจากรูปแบบการโจมตีของอาชญากรไซเบอร์ต่างก็มีรูปแบบและวิธีการที่แตกต่างกันออกไป ดังนั้นรูปแบบที่เหมาะสมของการจัดการย่อมขึ้นอยู่กับสถานการณ์ วิธีการ และลักษณะของการโจมตี ส่วนกระบวนการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ต่างขึ้นอยู่กับประสิทธิภาพการพัฒนาโครงสร้างพื้นฐานและการจัดหน่วยบังคับบัญชาเพื่อการจัดการกับภัยคุกคามนี้ในรูปแบบเฉพาะ

การวิเคราะห์รูปแบบที่เหมาะสมของการจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้พบว่า ประเด็นสำคัญของแนวทางด้านการทำสงครามไซเบอร์ของประเทศไทยในการแก้ปัญหาความไม่สงบสุขในพื้นที่จังหวัดชายแดนภาคใต้ ควรใช้นโยบายระดับชาติก่อนในเบื้องต้นโดยการกำหนดโครงสร้างพื้นฐานให้สมบูรณ์พร้อมทั้งภารกิจหน้าที่ จากนั้นก็ต้องกำหนดแผนงานและมาตรการที่เกี่ยวข้องทั้งด้านการสื่อสารข้อมูลและอำนาจตามกฎหมายที่พร้อมจะให้กลุ่มงานดำเนินการได้ และในที่สุดจึงจะสามารถนำนโยบายมาใช้ในการแก้ปัญหาในจังหวัดชายแดนภาคใต้ได้ตามเป้าหมาย

ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ ประกอบด้วย ๗ ยุทธศาสตร์ ได้แก่

ยุทธศาสตร์ที่ ๑ : ยุทธศาสตร์การจัดโครงสร้างพื้นฐานของประเทศไทยสำหรับใช้ในการจัดการกับภัยคุกคามด้านไซเบอร์

ยุทธศาสตร์ที่ ๒ : ยุทธศาสตร์การสร้างการตระหนักรู้โลกไซเบอร์ให้กับประชาชน

ยุทธศาสตร์ที่ ๓ : ยุทธศาสตร์การพัฒนาความก้าวหน้าด้านไซเบอร์

ยุทธศาสตร์ที่ ๔ : ยุทธศาสตร์การส่งเสริมความร่วมมือด้านไซเบอร์ระหว่างภาครัฐ ภาคเอกชน และภาคประชาชน

ยุทธศาสตร์ที่ ๕ : ยุทธศาสตร์การกำหนดใช้กฎหมายด้านไซเบอร์และการบังคับใช้กับประชาชน

ยุทธศาสตร์ที่ ๖ : ยุทธศาสตร์การใช้การบูรณาการร่วมกันเพื่อแบ่งปันข้อมูลข่าวสาร

ยุทธศาสตร์ที่ ๗ : ยุทธศาสตร์การรับรู้ด้านไซเบอร์เพื่อการป้องกัน การยับยั้ง และการโจมตี

ปัญหาเรื่องภัยคุกคามด้านไซเบอร์จะยังคงเติบโตอย่างต่อเนื่องตามเทคโนโลยีที่ทันสมัยมากยิ่งขึ้น หน่วยงานภาครัฐจะยังคงเป็นเป้าหมายสำคัญในการโจมตีด้านไซเบอร์จากผู้ไม่หวังดีหรืออาชญากรไซเบอร์ ทั้งจากการโจมตีเพื่ออาศัยความน่าเชื่อถือของหน่วยงานภาครัฐมาใช้หลอกหลงประชาชนอีกต่อหนึ่ง และการโจมตีเพื่อทำลายความน่าเชื่อถือของหน่วยงานอันเกิดจากสาเหตุต่างๆ ไม่ว่าจะเป็นการแสดงพลังของกลุ่มบุคคลที่ต่อต้านนโยบายรัฐบาล การมุ่งทำลายชื่อเสียง การก่อกวน หรือแม้กระทั่งการโจมตีเพื่อทดสอบความสามารถของตนเองเพื่อแสดงให้กลุ่มอาชญากรไซเบอร์ด้วยกันได้รับรู้ ในอนาคตการโจมตีด้านไซเบอร์จะมีการเปลี่ยนรูปแบบหรือวิธีการให้มีความรุนแรงมากยิ่งขึ้น เนื่องจากสามารถหาเครื่องมือในการโจมตีได้ง่ายจากอินเตอร์เน็ตและเว็บไซต์ใต้ดิน ซึ่งจะทำให้อาชญากรไซเบอร์หน้าใหม่เกิดขึ้นได้ง่ายอีกด้วย ดังนั้นรัฐบาลต้องให้ความสำคัญอย่างยิ่งยวดต่อเรื่องความมั่นคงปลอดภัยด้านไซเบอร์อย่างเป็นรูปธรรม การนำยุทธศาสตร์ที่นำเสนอมาใช้งานอย่างเร่งด่วน การออกพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ที่ผ่านการทำประชาพิจารณ์เพื่อรับฟังมุมมองที่เป็นประโยชน์และได้รับการยอมรับจากภาคเอกชนและภาคประชาชน แต่สิ่งที่สำคัญยิ่งกว่านั้นก็คือ “ประชาชน” โดยเฉพาะอย่างยิ่งบุคลากรหน่วยงานภาครัฐในทุกระดับจะต้องตระหนักถึงความสำคัญในการเฝ้าระวังและการปฏิบัติให้ถูกต้องตามมาตรการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ของหน่วยงาน เพื่อป้องกันตนเองและหน่วยงานให้ปลอดภัยจากการถูกโจมตี นอกจากนี้การติดตามสถานการณ์ด้านความมั่นคงปลอดภัยด้านไซเบอร์ก็มีความสำคัญที่จะช่วยให้สามารถพร้อมรับมือกับภัยคุกคามใหม่ๆ ที่อาจเกิดขึ้นได้อย่างทันท่วงที

บทที่ ๕
สรุปและข้อเสนอแนะ

การศึกษาเรื่อง ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้โดยมีวัตถุประสงค์การวิจัยเพื่อ ๑) ศึกษารูปแบบ วิธีการ การประเมินสถานการณ์ และปัญหาผลกระทบของภัยคุกคามด้านไซเบอร์ ๒) ศึกษาผลกระทบของภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงแห่งชาติในพื้นที่จังหวัดชายแดนภาคใต้และ ๓) นำเสนอยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้การวิจัยนี้ใช้ระเบียบวิธีวิจัยเชิงคุณภาพโดยเน้นการศึกษาเฉพาะประเด็นที่นำไปสู่การกำหนดยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้กลุ่มเป้าหมาย ได้แก่๑) หน่วยงานด้านความมั่นคงของรัฐ จำนวน ๑๐ คน (กองทัพภาคที่ ๔, กอ.รมน.ภาค ๔ ส่วนหน้า, ศอบต., ศชต., และ ฉก.) ๒) ผู้บริหาร/ผู้นำท้องถิ่น ๔ จังหวัด จำนวน ๘ คน ๓) หน่วยงานภาคเอกชน จำนวน ๘ คน ๔) หน่วยงานพลเรือน จำนวน ๘ คน ๕) ภาคประชาชน จำนวน ๘ คน ๖) เจ้าหน้าที่ด้านการข่าวที่เชี่ยวชาญระบบไอซีที จำนวน ๘ คน ๗) เจ้าหน้าที่ทหารที่รับผิดชอบด้านภัยคุกคามด้านไซเบอร์ จำนวน ๘ คน ๘) ผู้ปฏิบัติงานที่เกี่ยวข้องกับระบบเครือข่ายอินเตอร์เน็ต จำนวน ๘ คน ๙) ผู้ทรงคุณวุฒิจากหน่วยงานความมั่นคงด้านไซเบอร์กองทัพไทย จำนวน ๔ คนและ ๑๐) ผู้เชี่ยวชาญด้านวิศวกรรมระบบไอซีทีและโลกไซเบอร์ จำนวน ๕ คนรวมกลุ่มเป้าหมายทั้งสิ้น ๗๕ คนได้มาจากการเลือกในลักษณะจำเพาะเจาะจง เครื่องมือที่ใช้ในการวิจัย ได้แก่ แบบสัมภาษณ์แบบไม่มีโครงสร้าง การวิเคราะห์และสังเคราะห์ข้อมูลตามหลักการวิจัยเชิงคุณภาพโดยวิธีพรรณนาเชิงวิเคราะห์ตรวจสอบข้อมูลโดยใช้วิธีการสามเส้าด้านข้อมูล และยืนยันร่างยุทธศาสตร์โดยใช้การสัมมนาอิงผู้เชี่ยวชาญ โดยมีผลการศึกษาวิจัยและข้อเสนอแนะดังนี้

สรุป

ผลการศึกษาวิจัยโดยภาพรวมพบว่า ในพื้นที่จังหวัดชายแดนภาคใต้มีกระบวนการใช้โลกไซเบอร์ในการสร้างความไม่สงบสุขหลากหลายวิธี เช่น การใช้เครือข่ายสังคมออนไลน์เพื่อการบ่อนทำลายความน่าเชื่อถือของเจ้าหน้าที่รัฐ รวมถึงการปฏิบัติการจิตวิทยาและการโฆษณาชวนเชื่อของกลุ่มผู้ไม่หวังดี การสร้างกระแสข่าวในเชิงลบและการสร้างความขัดแย้งต่อประชาชนการก่อวินาศกรรมโดยใช้เครือข่ายอินเตอร์เน็ตเป็นมัชฌิมโดยมีแนวโน้มจะปฏิบัติการในรูปแบบอื่นๆ

เพิ่มมากขึ้น นอกจากนี้ใช้ระบบการติดต่อสื่อสารผ่านแอปพลิเคชั่นเพื่อหลบเลี่ยงการตรวจจับและติดตามโดยเจ้าหน้าที่รัฐเหล่านี้ล้วนสร้างผลกระทบโดยตรงต่อความมั่นคงแห่งชาติแทบทั้งสิ้น ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ ประกอบด้วย ๗ ยุทธศาสตร์ ได้แก่ ๑) การจัดโครงสร้างพื้นฐานของประเทศไทยสำหรับใช้ในการจัดการกับภัยคุกคามด้านไซเบอร์๒) การสร้างการตระหนักรู้โลกไซเบอร์ให้กับประชาชน ๓) การพัฒนาความก้าวหน้าด้านไซเบอร์๔) การส่งเสริมความร่วมมือด้านไซเบอร์ระหว่างภาครัฐ ภาคเอกชน และภาคประชาชน ๕) การกำหนดใช้กฎหมายด้านไซเบอร์และการบังคับใช้กับประชาชน ๖) การใช้การบูรณาการร่วมกันเพื่อแบ่งปันข้อมูลข่าวสาร และ ๗) การรับรู้ด้านไซเบอร์เพื่อการป้องกันการยับยั้ง และการโจมตีสำหรับประเทศไทยควรใช้ยุทธศาสตร์และมาตรการรองรับการจัดการกับภัยคุกคามในโลกไซเบอร์ให้มีประสิทธิภาพ คุณภาพ และความเข้มแข็งอย่างต่อเนื่อง เพื่อเสริมสร้างความมั่นคงปลอดภัยด้านไซเบอร์และการนำสันติสุขกลับคืนสู่พื้นที่จังหวัดชายแดนภาคใต้ของประเทศต่อไป

ผลการศึกษาตอบวัตถุประสงค์ข้อที่ ๑ สรุปได้ว่ารูปแบบภัยคุกคามด้านไซเบอร์ที่เกิดขึ้นในจังหวัดชายแดนภาคใต้ปรากฏผลดังประเด็นต่อไปนี้

๑. รูปแบบของภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

๑.๑ รูปแบบของภัยคุกคามด้านไซเบอร์ที่พบในพื้นที่จังหวัดชายแดนภาคใต้จากความคิดเห็นของหน่วยงานด้านความมั่นคงของรัฐ (กองทัพภาคที่ ๔, กอ.รมน.ภาค ๔ ส่วนหน้า, ศอบต., ศชต., และ ฉก.) ผู้บริหาร/ผู้นำท้องถิ่น ๔ จังหวัด สรุปได้ดังนี้

๑.๑.๑ รูปแบบของการสร้างข้อมูล การสร้างข้อมูลเป็นรูปแบบปกติของการนำเสนอข้อมูลข่าวสารในยุคปัจจุบัน มีการนำระบบไซเบอร์และเครือข่ายสังคมออนไลน์มาใช้สร้างและเผยแพร่ข้อมูลข่าวสารมากขึ้นเรื่อยๆ โดยอาจจะมากกว่าการใช้กำลังเสียอีกทั้งมีการแฮกหรือการเจาะข้อมูลของส่วนงานราชการและหน่วยงานทางความมั่นคง (พ.อ.ดร.เศรษฐพงค์ มะลิสุวรรณ , ๒๕๕๙) ซึ่งยังไม่มีการตรวจพบอย่างเด่นชัดจากเจ้าหน้าที่ผู้เชี่ยวชาญ แต่พบว่ามีการพบการโจมตีทางไซเบอร์ด้วยความพยายามในการเจาะและกระทำการบุกรุกฐานข้อมูลของ กอ.รมน. จากการวิเคราะห์ของผู้รับผิดชอบด้านความมั่นคงพบว่าอาจเป็นการเชื่อมโยงกับการเมืองหรือการก่อกวนให้เกิดความหวาดระแวงระหว่างเจ้าหน้าที่รัฐและประชาชนนั่นเอง (นงรัตน์ สายเพชร, ๒๕๕๖)

๑.๑.๒ รูปแบบของการบิดเบือนข้อมูล ในพื้นที่สังคมเมืองมีการเข้าถึงอินเตอร์เน็ตได้ดี แต่ในส่วนพื้นที่นอกเมืองมีการใช้งานน้อยกว่า คนอายุ ๔๐ ขึ้นไป มักจะยังใช้งานอินเตอร์เน็ตเป็นสื่อในการติดต่อสื่อสารประจำวันรวมถึงการบริโภคข่าวสารบ้านเมืองต่างๆ แต่มีการใช้การบอกเล่าข่าวลือเพื่อให้คนที่เข้าถึงอินเตอร์เน็ตไม่ได้ได้รับข่าวบิดเบือนจากความเป็นจริง

บ้าง โดยมีการตรวจพบโฆษณาชวนเชื่อและมีการโจมตีในประเด็นการเผยแพร่ข่าวสารโดยมีการนำสื่อสังคมออนไลน์ มาใช้ในการหาแนวร่วมซึ่งมีการขยายช่องทางการสื่อสารตลอดเวลา โดยเมื่อทางการตรวจสอบได้ก็จะมีการเปลี่ยนรูปแบบของสื่อออนไลน์ไปได้ใช้ช่องทางอื่นไม่มีที่สิ้นสุด มีการใช้จิตวิทยาโดยเน้นการสร้างความเข้าใจผิดๆ ให้ประชาชนเพื่อให้เข้าใจผิดหรือเกิดความรู้สึกขัดแย้งกับการทำงานของรัฐบาลตลอดจนหน่วยงานทางความมั่นคงอื่นๆ มีการกล่าวหาใส่ร้ายป้ายสี รวมถึงการสร้างความขัดแย้งกันระหว่างกลุ่มประชาสังคม ตลอดจนการนำประเด็นทางการเมืองมาเชื่อมโยงและขยายผลให้ไปสู่การสร้างสถานการณ์แห่งความรุนแรงดังเหตุการณ์ที่เกิดขึ้นในหลายๆ ครั้งในพื้นที่จังหวัดชายแดนภาคใต้ ซึ่งสอดคล้องกับหลักการของ อาจารย์ ดร.สราวุธ ปิติยาศักดิ์ (๒๕๕๒) ได้เขียนบทความวิชาการเรื่อง “ภัยคุกคามทางไซเบอร์กับกฎหมายไซเบอร์ไทย” โดยกล่าวว่า “ภัยคุกคามทางไซเบอร์” ถือเป็นภัยคุกคามใหญ่หลวงต่อผลประโยชน์ทางเศรษฐกิจตลอดจนความมั่นคงของประเทศ การโจมตีทางไซเบอร์มีหลายรูปแบบ เช่น การเจาะระบบคอมพิวเตอร์ (Hacking) การสอดแนมข้อมูลคอมพิวเตอร์โดยสปายแวร์ การดักรับข้อมูลคอมพิวเตอร์ (Sniffing) การโจมตีโดยชุดคำสั่งไม่พึงประสงค์ (Malicious Software : Malware) หรือการรุมสอบถามข้อมูลจนระบบล่ม (Denial of Service Attack : DOS)

๑.๑.๓ รูปแบบของการชักชวน รูปแบบของการชักชวนจะปรากฏให้เห็นผ่านสื่อสังคมออนไลน์ประเภทต่างๆ โดยเฉพาะอย่างยิ่งกลุ่มของ IS ที่มีการเผยแพร่แนวคิดและความรุนแรงโดยการหาแนวร่วมเพื่อเชิญชวนให้ไปร่วมรบในประเทศซีเรียหรือบริเวณต่างๆ ที่เกิดความรุนแรงบนโลก โดยมีการตรวจพบจากเจ้าหน้าที่ด้านความมั่นคงว่าการชักชวนและโจมตีในประเด็นการเผยแพร่ข่าวสารเกี่ยวกับประเด็นการชักชวนนี้เสมอมาตั้งแต่อดีตจนถึงปัจจุบัน

ปัจจุบันจะเห็นว่ากลุ่มผู้บริโภคข้อมูลข่าวสารโดยใช้ระบบอินเตอร์เน็ตและเครือข่ายสังคมออนไลน์มีด้วยกันทั้งสิ้น ๖ กลุ่ม ได้แก่ กลุ่มขบวนการก่อการร้าย กลุ่มภาคประชาสังคม กลุ่มสื่อสารมวลชน กลุ่มสื่อทางเลือก กลุ่มสื่อสารสังคมออนไลน์ และกลุ่มภาคประชาชน ผลการวิจัยสอดคล้องกับ หยาดพิรุณ นาชัยสินธุ์ (๒๕๖๐) ที่กล่าวว่าเครื่องมือที่สำคัญของการก่อการร้ายทางไซเบอร์ก็คือ อินเตอร์เน็ตและเครือข่ายสังคมออนไลน์นั่นเอง

๑.๒ รูปแบบของภัยคุกคามด้านไซเบอร์ที่พบในพื้นที่จังหวัดชายแดนภาคใต้จากความคิดเห็นของเจ้าหน้าที่ระดับปฏิบัติการด้านความมั่นคงรวมถึงเจ้าหน้าที่ทหารที่รับผิดชอบด้านภัยคุกคามของสำนักปฏิบัติการข่าวสาร สรุปได้ดังนี้

๑.๒.๑ จะเป็นลักษณะการโจมตีโดยเน้นการโจมตีโดยมีรูปแบบเป็นกลุ่มขบวนการก่อการร้ายที่หวังผลทำให้เกิดความเสียหายต่อหน่วยงานของภาครัฐ ปฏิบัติการด้วยการสร้างระบบข้อมูลข่าวสารอันเป็นเท็จและขยายผลผ่านเครือข่ายสังคมออนไลน์รูปแบบต่างๆ

๑.๒.๒ ช่วงปี พ.ศ.๒๕๕๐-๒๕๕๑ ได้มีบุคคลภายนอกเข้ามาเจาะข้อมูลโดยพยายามเข้ามาผ่านระบบ File Wall แต่ทางเจ้าหน้าที่ของรัฐยังไม่ทราบว่าได้นำข้อมูลใดออกไปได้มากน้อยเพียงใด หลังจากนั้นก็ได้มีการสร้างระบบการป้องกันมากยิ่งขึ้น ดังนั้นจึงกล่าวได้ว่าเป็นรูปแบบที่ใช้บุคคลภายนอกผู้เชี่ยวชาญด้านระบบไอซีทีเป็นคนดำเนินการ

๑.๒.๓ เป็นรูปแบบสายลับจากภายนอกเข้ามาขโมยข้อมูลโดยเข้ามารับราชการหรือบรรจุเข้าปฏิบัติราชการ และอาจเข้ากลุ่มเครือข่ายสังคมออนไลน์ของเจ้าหน้าที่รัฐเพื่อนำข้อมูลภายในออกไปสู่กลุ่มเป้าหมายหรือขบวนการก่อการร้าย จากการตรวจสอบของเจ้าหน้าที่ว่าทราบเรื่องเนื่องจากเคยเกิดเหตุการณ์ปะทะกันและเข้าตรวจค้นพื้นที่จึงพบฮาร์ดดิสก์เป็นข้อมูลภายใน ๓๕๑ ที่สามารถหลุดออกไปได้

๑.๒.๔ เป็นรูปแบบจากบุคคลภายในองค์กรนำข้อมูลข่าวสารออกไปโดยทั้งตั้งใจและความรู้เท่าไม่ถึงการณ์หรือคนภายในออกไปเผยแพร่ข้อมูลเองในเครือข่ายสังคมออนไลน์โดยมิได้คำนึงถึงผลกระทบที่จะตามมาในอนาคต

๑.๓ รูปแบบของภัยคุกคามด้านไซเบอร์ที่พบในพื้นที่จังหวัดชายแดนภาคใต้ในความคิดเห็นของนักวิชาการและผู้เชี่ยวชาญด้านระบบไอซีทีซึ่งเป็นเจ้าหน้าที่ด้านความมั่นคงสามารถสรุปได้ว่ามีรูปแบบที่ปรากฏดังนี้

๑.๓.๑ รูปแบบของภัยคุกคามส่วนมากเป็นการใช้สื่อในการกระจายข่าว การสร้างเพจเพื่อบิดเบือนข่าวสารข้อมูล ปลุกปั่นและสร้างกระแสทั้งทางที่ดีและไม่ดี การสร้างเครือข่ายสังคมเฉพาะกลุ่ม และการนำแนวคิดกระจายลงสู่พื้นที่ให้ประชาชนในพื้นที่มากที่สุดโดยผ่านสื่อต่างๆ รวมถึงเครือข่ายสังคมออนไลน์

๑.๓.๒ รูปแบบของภัยคุกคามที่ปรากฏมี ๓ รูปแบบ คือ ๑) การสร้างข่าวขึ้นใหม่รายวัน ๒) ข่าวจริงแต่บิดเบือนข่าวปัจจุบัน และ ๓) นำข่าวเก่ามานำเสนอซ้ำ เพื่อนำเสนอข่าวออกไปในทางลบโดยผ่านสื่อต่างๆ รวมถึงเครือข่ายสังคมออนไลน์ การสร้างความขัดแย้งระหว่างกลุ่มการเมืองและผลประโยชน์ และการสร้างความเกลียดชังให้ประชาชนไม่ไว้วางใจเจ้าหน้าที่ของรัฐ ในส่วนของสถานที่ราชการและสถานที่สำคัญของจังหวัด เช่น มหาวิทยาลัย มัสยิดกลาง และศาลาประชาคม มีการพบข่าวสารบิดเบือนที่แพร่กระจายผ่านสื่อออนไลน์ค่อนข้างมาก โดยมีการตอบโต้โดยการพูดคุยทำความเข้าใจกับประชาชน มีการประชุมแลกเปลี่ยนกันเป็นประจำ และมีการกำหนดรูปแบบการพูดคุยการให้ข่าวสารจากหน่วยเหนืออีกด้วย

๑.๓.๓ รูปแบบการเข้าเจาะข้อมูลโดยเป็นการดึงข้อมูลออกไป หลังจากนั้นมีการเปลี่ยนภาพในโฮมเพจหรือในเว็บไซต์ให้เป็นภาพการ์ตูน บางครั้งจัดว่าเป็นการโจมตีแต่ไม่พบเป็นการจารกรรมข้อมูลโดยตรง แต่เพื่อการเข้ามาตรวจสอบดูการเคลื่อนไหวของหน่วยงานของรัฐ

เท่านั้น จากข้อมูลเชิงลึกของสำนักข่าวกรองพบว่ามีการ จารกรรมข้อมูลออกไปครั้งหนึ่งปี พ.ศ. ๒๕๕๘ โดยเว็บไซต์ของสำนักข่าวกรองที่ใช้ในการรายงานข่าวไม่สามารถตรวจสอบได้ว่ามีการนำข้อมูลออกไปได้มากน้อยเพียงใด

๑.๓.๔ รูปแบบเฉพาะกิจ เช่น การพยายามจารกรรมและเจาะเข้าระบบฐานข้อมูลขบวนการก่อการร้าย ซึ่งระบบดังกล่าวจะเป็นการเก็บข้อมูลรายงานข่าวการเคลื่อนไหวของขบวนการ โดยเปรียบเหมือนการลองของโดยไม่ได้เน้นโจมตี อีกทั้งมีการใช้สายลับโดยให้บุคคลมาสมัครรับราชการในหน่วยงานด้านความมั่นคงและเมื่อเข้ามาได้ก็จะหาวิธีการรายงานข้อมูลให้ขบวนการได้ทราบความเคลื่อนไหวและมีการนำข้อมูลออกไปสู่ภายนอก

๑.๔ รูปแบบของภัยคุกคามด้านไซเบอร์ที่พบในพื้นที่จังหวัดชายแดนภาคใต้จากความคิดเห็นของหน่วยงานภาคเอกชน หน่วยงานพลเรือน และภาคประชาชน สรุปได้ดังนี้

๑.๔.๑ พบการเผยแพร่หรือแชร์ข้อมูลข่าวสารในลักษณะการบิดเบือนทางสื่อสังคมออนไลน์ชนิดต่างๆ โดยไม่รู้ที่มาและแชร์กันไปทั่ว ซึ่งทำให้เกิดการแชร์ต่อโดยไม่มีคัดกรองและข้อมูลข่าวสารเหล่านั้นย่อมแพร่กระจายได้อย่างรวดเร็ว

๑.๔.๒ หากมีการได้รับข่าวสารใดๆ จะมีการแจ้งต่อกันในหมู่เพื่อน แต่จะมีการวิเคราะห์ดูความเป็นมาและพิจารณาก่อนเพื่อการป้องกันข่าวลวง และมักจะมีคำกล่าวที่ว่า “เหตุการณ์ที่จริงมักจะไม่ค่อยมีการแชร์กัน”

๑.๔.๓ ในการเผยแพร่ข้อมูลข่าวสารบางอย่าง ถ้ารู้จักกันเป็นการส่วนตัวมักจะมีการเตือนกันว่าให้พิจารณาข้อมูลก่อนเผยแพร่ เพราะอาจเป็นการโฆษณาชวนเชื่อหรือการสร้างข่าวเท็จในน่าเชื่อถือก้เป็นได้

๑.๔.๕ หน่วยงานภาคเอกชน หน่วยงานพลเรือน และภาคประชาชน ยังไม่เคยเห็นมาตรการทางกฎหมายว่าสมารถดำเนินการกับผู้บิดเบือนข่าวสารผ่านสื่อสังคมออนไลน์ได้อย่างไร ระดับการใช้งานที่เหมาะสมเป็นอย่างไร อะไรคือข้อพิจารณาในการเผยแพร่ข้อมูลข่าวสารที่ถูกต้องในการดำรงชีวิตของประชาชน

๒. วิธีการของภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

๒.๑ วิธีการของภัยคุกคามด้านไซเบอร์ที่พบในพื้นที่จังหวัดชายแดนภาคใต้จากความคิดเห็นของหน่วยงานด้านความมั่นคงของรัฐ (กองทัพภาคที่ ๔, กอ.รมน.ภาค ๔ ส่วนหน้า, ศอบต., ศชต., และ ฉก.) ผู้บริหาร/ผู้นำท้องถิ่น ๔ จังหวัด สรุปได้ดังนี้

๒.๑.๑ วิธีการโจมตียังไม่ปรากฏเด่นชัดเนื่องจากยังไม่มีหน่วยงานใดออกมายืนยันว่าภัยคุกคามนี้มีขั้นตอนกระบวนการทางวิชาการอย่างไร ปรากฏเพียงแค่การสร้างข่าวสาร การแพร่กระจาย และการโต้ตอบกันผ่านสื่อสังคมออนไลน์รูปแบบต่างๆ

๒.๑.๒ เจ้าหน้าที่ใช้สมาร์ทโฟนและแอพพลิเคชั่นต่างๆ อย่างแพร่หลาย มีความรู้เท่าไม่ถึงการณ์ของเจ้าหน้าที่บางคนซึ่งมีการนำเอกสารชั้นความลับไปเผยแพร่บนเว็บ โดยอาจเป็นละเมิดการรักษาความปลอดภัยข้อมูลทางราชการและรวมถึงสิทธิส่วนบุคคล ทำให้บุคคลที่ไม่มีหน้าที่ได้รับทราบข่าวสารนั้นไปด้วย (ปริญญา หอมเอนก, ๒๕๖๐) เหตุการณ์นี้อาจเป็นการคาดไม่ถึงหรือมองไม่รอบด้านของฝ่ายความมั่นคงซึ่งโดยปกติแต่ละหน่วยมีมาตรการทั้งระดับบุคคลและระดับหน่วยที่กำกับดูแลการให้ข้อมูลข่าวสารอยู่แล้ว

๒.๒ วิธีการของภัยคุกคามด้านไซเบอร์ที่พบในพื้นที่จังหวัดชายแดนภาคใต้จากความคิดเห็นของเจ้าหน้าที่ระดับปฏิบัติการด้านความมั่นคงรวมถึงเจ้าหน้าที่ทหารที่รับผิดชอบด้านภัยคุกคามของสำนักปฏิบัติการข่าวสาร สรุปได้ดังนี้

๒.๒.๑ ยังไม่พบการเจาะข้อมูลแต่พบการแฝงตัวว่าเป็นเจ้าหน้าที่รัฐแล้วเข้ากลุ่ม Line และ Facebook ที่ประกอบด้วยชาวบ้านและเจ้าหน้าที่รัฐหรือเข้ามาดำเนินการขโมยข้อมูลโดยติดตามว่าใครเป็นเจ้าหน้าที่บ้าง เมื่อเจ้าหน้าที่พิสูจน์ทราบก็มีการรายงานไปยัง Line และ Facebook เพื่อให้สลายกลุ่มหรือปิด

๒.๒.๒ มีการนำข้อมูลสารสนเทศทั้งในส่วนราชการและภาคเอกชนไปใช้ในการใส่ร้ายป้ายสี ยั่วยุปลุกปั่น และสร้างความขัดแย้งทางศาสนา โดยการเผยแพร่และสร้างภาพให้เจ้าหน้าที่รัฐเกิดความเสียหายและกระทำผิดต่อประชาชน

๒.๒.๒ ยังไม่มีการเชื่อมโยงกับศูนย์ไซเบอร์ทั้งในระดับชุมชนและระดับหน่วยงานโดยเฉพาะอย่างยิ่งหน่วยงานทางความมั่นคง โดยยังไม่มีเจ้าภาพรับผิดชอบหรือไม่มีตัวกลางด้านไซเบอร์และด้าน IO

๒.๒.๓ มีการตรวจพบว่าผู้ประกอบวิชาชีพอาจารย์และประชาชนหลากหลายสาขาอาชีพได้นำข้อมูลข่าวสารไปบิดเบือนหลายๆ ครั้ง โดยเจ้าหน้าที่มีการประชุมติดตามและมีการตรวจสอบติดตามผ่านทางสื่อสังคมออนไลน์เช่นกัน อีกทั้งผู้ประสานงานสายข่าวได้มีการสร้างบัญชีปลอมขึ้นเพื่อการตรวจหาข่าวโดยมีสถานะอำพลางตัวตนเพื่อให้เข้าถึงแหล่งข่าว และในที่สุดจะนำไปสู่การค้นหาแหล่งที่มาของขบวนการก่อการร้ายต่อไป

๒.๒.๔ มีการส่งข่าวสารบิดเบือนผ่านทางอีเมล์ในลักษณะลูกโซ่ นั่นคือ เมื่อผู้ใดได้รับข้อมูลข่าวสารแล้วก็จะดำเนินการส่งต่อให้ผู้เป็นสมาชิกและไม่เป็นสมาชิกของกลุ่มก่อการร้ายในทันทีโดยไม่ได้ปรึกษาหารือกับหน่วยงานราชการก่อนว่าข้อมูลข่าวสารนี้มีที่มาที่ไปอย่างไร น่าเชื่อถือหรือไม่ และมีเป้าประสงค์ใด

๒.๒.๕ หากมีสื่อสังคมออนไลน์ที่บิดเบือนจาก YouTube จะทำการสรุปหาการเชื่อมโยงและรายงานไปยังหน่วยงานระดับสูงกว่าเพื่อดำเนินการต่อไป โดยในส่วนการสั่งปิด

จะต้องส่งไปยังกระทรวงไอซีที แต่ถ้าเป็น Facebook จะทำการเฝ้าระวังโดยการแฝงตัวแทนเพื่อการติดตามข้อมูลและพฤติกรรมอย่างใกล้ชิดและรายงานผลให้ผู้บังคับบัญชาทราบตามลำดับต่อไป

๒.๓ วิธีการของภัยคุกคามด้านไซเบอร์ที่พบในพื้นที่จังหวัดชายแดนภาคใต้จากความคิดเห็นของนักวิชาการและผู้เชี่ยวชาญด้านระบบไอซีทีซึ่งเป็นเจ้าหน้าที่ด้านความมั่นคง สรุปได้ดังนี้

๒.๓.๑ ภัยคุกคามทางออนไลน์นับว่ามีความรุนแรงและเพิ่มขึ้น เนื่องจากเยาวชนไม่รู้เท่าทันสื่อและข้อมูลข่าวสาร ทำให้เป็นช่องทางในการชักชวนเข้าสู่ส่วนหนึ่งของกระบวนการก่อการร้ายได้

๒.๓.๒ การแจ้งข่าวสารหรือการโต้ตอบข่าวสารของทางภาครัฐค่อนข้างล่าช้าทำให้ไม่ทันการณ์หรือเป็นสถานะผู้ตามอยู่เสมอ

๒.๓.๔ การใช้สื่อสังคมออนไลน์ในการบิดเบือนข่าวสาร โดยมีทั้งข่าวที่เป็นความจริงและความจริงที่บิดเบือนเพื่อประโยชน์บางอย่าง เนื่องจากสื่อสังคมออนไลน์ไม่มีการควบคุมหรือควบคุมยาก วิธีการแก้ไขจากทางการก็คือทางการจะต้องใช้ความจริงที่จริงกว่า

๒.๓.๕ แต่เดิมสื่อถูกควบคุมโดยภาครัฐ แต่ปัจจุบันการเผยแพร่ข้อมูลเปลี่ยนไปโดยเทคโนโลยีและไม่มีการควบคุมกลั่นกรอง ทำให้การบิดเบือนกระจายข้อมูลข่าวสารไปได้ในวงกว้างอย่างง่ายขึ้นและยากต่อการควบคุมอีกต่อไป

๒.๔ วิธีการของภัยคุกคามด้านไซเบอร์ที่พบในพื้นที่จังหวัดชายแดนภาคใต้ในความคิดเห็นของหน่วยงานภาคเอกชน หน่วยงานพลเรือน และภาคประชาชน สามารถสรุปได้ว่ามีวิธีการที่ปรากฏดังนี้

๒.๔.๑ มีการใช้เทคโลยีในการก่อการร้ายมากยิ่งขึ้นเช่นแต่ก่อนใช้กดระเบิดแต่ปัจจุบันใช้สมาร์ทโฟน และในอนาคตอาจเกิดการใช้เทคโนโลยีอื่นๆ มาร่วมด้วยมากขึ้น ส่งผลให้สถานการณ์อันตรายมากขึ้นเนื่องจากการก่อเหตุมีความแม่นยำมากยิ่งขึ้น

๒.๔.๒ มีสมาชิก NGO หลายคนไม่สนับสนุนการทำงานของภาครัฐและนำข้อมูลข่าวสารไปบิดเบือนจนสร้างความเสียหายให้กับประเทศชาติ โดยควรมีการนำ พรบ. คอมพิวเตอร์ฯ มาใช้เป็นเครื่องอย่างจริงจังที่อาจส่งผลให้ความเสียหายให้กับประเทศชาติลดลง

๓. การประเมินสถานการณ์ภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

๓.๑ การประเมินสถานการณ์ภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้จากความคิดเห็นของหน่วยงานด้านความมั่นคงของรัฐ (กองทัพภาคที่ ๔, กอ.รมน.ภาค ๔ ส่วนหน้า, ศอบต., ศชต., และ ฉก.) ผู้บริหาร/ผู้นำท้องถิ่น ๔ จังหวัด สรุปได้ดังนี้

๓.๑.๑ มีการตรวจจับและติดตามผู้โพสข้อความและข้อมูลข่าวสาร วิเคราะห์ รวบรวม บันทึกจับคุมจากทีมข่าวเปิด และรายงานผล โดยมีการทำโดยคนเป็นหลัก มีการเปลี่ยนรูปแบบเสมอถ้ามีการจับได้ แต่ทางการก์มีการนำอุปกรณ์มาใช้ในการตรวจจับมากขึ้นโดยเฉพาะฮาร์ดแวร์พิเศษ โดยยังไม่มีการใช้ Sniffer แต่มีการตรวจสอบจากเครื่องมือสื่อสารที่ยึดได้และมีการสร้างการวิเคราะห์เชื่อมโยง (Link Analyze)

๓.๑.๒ การประเมินสถานการณ์ยังไม่มีรูปแบบแน่นอนตายตัว สืบเนื่องมาจากส่วนงานที่รับผิดชอบด้านไซเบอร์ระดับประเทศยังมีลักษณะไม่เป็นรูปธรรม หน่วยงานที่รับผิดชอบในพื้นที่ก็พยายามเรียนรู้และพัฒนาขีดความสามารถของการตรวจจับเพิ่มขึ้นเรื่อยๆ มีการประชุมร่วมกันแบ่งปันข้อมูลข่าวสารระหว่างหน่วยงานต่างๆ ของจังหวัดชายแดนภาคใต้อยู่เสมอ หากไม่มีมาตรการที่เหมาะสมก็จะดำเนินการเชิงรับต่อไป

๓.๑.๓ จากการประเมินสถานการณ์ในส่วนผู้ก่อเหตุรุนแรงพบว่ามักมีรูปแบบการแบ่งทีมกันทำงานอย่างเป็นระบบ โดยมีการจัดตั้งกลุ่ม เช่น ทีมวางระบบ ทีมคอมพิวเตอร์ ทีมสร้างข่าว กลุ่มสนับสนุน NGO,CSO และกลุ่มภาคประชาสังคม เป็นต้น ซึ่งเมื่อรวมกันพบว่ามีองค์กรประมาณ ๕๒๑ องค์กร โดยจัดตั้งเป็น ๔ กลุ่ม ได้แก่ ๑) กลุ่มเคลื่อนไหวลงประชามติการแบ่งแยกดินแดนประมาณ ๓๐ กว่าองค์กร ๒) กลุ่มดำเนินการสร้างสภาพแวดล้อม ๓) กลุ่มโจมตี การปฏิบัติหน้าที่ของรัฐและกลุ่มทนายความ และ ๔) กลุ่มดำเนินงานเพื่อเอื้อประโยชน์ให้แก่ฝ่ายรัฐ

๓.๒ การประเมินสถานการณ์ภัยคุกคามด้านไซเบอร์ที่พบในพื้นที่จังหวัดชายแดนภาคใต้จากความคิดเห็นของเจ้าหน้าที่ระดับปฏิบัติการด้านความมั่นคงรวมถึงเจ้าหน้าที่ทหารที่รับผิดชอบด้านภัยคุกคามของสำนักปฏิบัติการข่าวสาร สรุปได้ดังนี้

๓.๒.๑ เจ้าหน้าที่ประเมินว่าทีมข่าวเปิดเปรียบเสมือนการลาดตระเวนทางไซเบอร์ ดังนั้นจะต้องดำเนินการด้วยมาตรการเชิงรุกอย่างต่อเนื่องเพื่อให้รู้เท่าทันขบวนการก่อการร้ายที่มาอย่างไร้รูปแบบชัดเจน ประกอบกับการสนับสนุนจากหน่วยงานภาครัฐอย่างเป็นระบบจะช่วยให้การทำงานมีประสิทธิภาพมากขึ้น

๓.๒.๒ มีการคุกคามและสร้างความเสียหายมากขึ้นเรื่อยๆ จากการใช้งานไซเบอร์รูปแบบต่างๆ เจ้าหน้าที่ต้องตระหนักว่าสื่อสังคมออนไลน์ต่างๆ ล้วนไม่มีความปลอดภัย ดังนั้นต้องมีกระบวนการสร้างความตระหนักด้านความปลอดภัยไซเบอร์ให้มากขึ้นโดยการสร้างความรับรู้ด้านต่างๆ ที่เกี่ยวข้องทุกมิติ การมีส่วนร่วมในการจัดการภัยคุกคามด้านไซเบอร์ มีการใช้มาตรการทางกฎหมายหากมีการตรวจพบอย่างจริงจัง

๓.๒.๓ ปัจจุบันฝ่ายทหารและหน่วยงานทางความมั่นคงอื่นก็มีการใช้งานสื่อสังคมออนไลน์ เช่น Facebook, Line, Twitter และ Blogger ในการทำลายฝ่ายตรงข้ามเช่นกัน เรียกได้ว่าเป็นการใช้ข้อมูลข่าวสารเพื่อประโยชน์ในงานด้านการข่าวและการตรวจจับหรือเฝ้าระวังผู้บุกรุกผ่านระบบไอซีที ดังนั้นจึงอยากให้มีเครื่องมือจับ IP address ของเครื่องที่บิดเบือนข่าวสารจะก่อให้เกิดความสะดวกในการทำงานมากขึ้น

๓.๒.๔ เนื่องจากในฝ่ายทหารและตำรวจรวมถึงหน่วยงานที่เกี่ยวข้องด้านความมั่นคงยังไม่มีศูนย์ทางไซเบอร์ที่ทันสมัย โดยเฉพาะอย่างยิ่งในสามจังหวัดชายแดนภาคใต้มีความต้องการใช้มากเนื่องจากมีการนำสื่อสังคมออนไลน์มาบิดเบือนเป็นประจำ ควรมีการนำ กสทช. มาช่วยและบูรณาการในเรื่องการตัดสินใจอย่างเป็นรูปธรรม การขาดบุคลากรในการดำเนินการเพราะรัฐจ่ายค่าตอบแทนในอัตราที่ต่ำ ดังนั้นบุคลากรด้านนี้จึงไม่มีการเติบโตและทำงานเท่าเดิม

๓.๒.๕ ประเทศไทยยังไม่มีกฎหมายควบคุมอุปกรณ์อิเล็กทรอนิกส์โดยเฉพาะเจ้าหน้าที่นโยบายความปลอดภัยทางกายภาพ ไม่มีกฎหมายการจัดการส่งข้อมูลผ่านสื่ออิเล็กทรอนิกส์ ซึ่งยังไม่มีการเข้ารหัส มีการปลุกปั่นและสื่อให้เห็นว่าเป็นการแบ่งแยกดินแดนเป็นรัฐปัตตานี มีความพยายามกำหนดให้การแบ่งแยกดินแดนเป็นรัฐปัตตานีเป็นหน้าที่ของคนอิสลามทุกคน โดยประชาชนได้รับข่าวสารแต่เพียงด้านเดียว ดังนั้นสื่อสังคมออนไลน์สามารถทำให้เข้าถึงประชาชนเป้าหมายได้มากขึ้นและสามารถนำสื่อกลับมาใช้ใหม่ได้ ทำให้เกิดการกระจายข่าวสารที่ผิดพลาดได้อย่างต่อเนื่องซึ่งไม่ส่งผลดีต่อการสร้างความสงบสุขให้กับประชาชน

๓.๒.๖ มีการสร้างแนวคิดที่บิดเบือนเพื่อครอบงำประชาชนในพื้นที่ ได้แก่ ๑) รัฐชาติมาลายู ๒) ศาสนาอิสลาม และ ๓) มาตุภูมิ ฉะนั้นต้องปรับเปลี่ยนทัศนคติ โดยเรื่องเหล่านี้ปรากฏอยู่บนสื่อสังคมออนไลน์อย่างต่อเนื่องโดยแทบจะไม่มีหน่วยงานใดเข้าไปดำเนินการอย่างเป็นรูปธรรมได้ รูปแบบการประเมินสถานการณ์นั้นต้องประเมินการเคลื่อนไหวใน ๗ กลุ่ม ที่สร้างความเสียหาย ได้แก่ กลุ่มที่ ๑ BRN, กลุ่มที่ ๒ พูโล ๑ ดาว, กลุ่มที่ ๓ พูโล ๔ ดาว, กลุ่มที่ ๔ พูโล ๕ ดาว, กลุ่มที่ ๕ GMP, กลุ่มที่ ๖ BIPP และกลุ่มที่ ๗ GMIP โดยจะต้องมีหน่วยงานที่เชี่ยวชาญด้านระบบไอซีทีและไซเบอร์คอยติดตามความเคลื่อนไหวในกลุ่มต่างๆ เหล่านี้อย่างใกล้ชิดและต่อเนื่องที่สุด

๓.๓ การประเมินสถานการณ์ภัยคุกคามด้านไซเบอร์ที่พบในพื้นที่จังหวัดชายแดนภาคใต้จากความคิดเห็นของนักวิชาการและผู้เชี่ยวชาญด้านระบบไอซีทีซึ่งเป็นเจ้าหน้าที่ด้านความมั่นคง สรุปได้ดังนี้

๓.๓.๑ รูปแบบของสถานการณ์ที่เกิดขึ้นพบว่าชาวบ้านจะเชื่อผู้นำทางศาสนามากกว่า ฝ่ายปกครอง ดังนั้นจึงปรากฏภาพที่ไม่เหมาะสมและมีโอกาสกระจายผ่านออนไลน์ได้ง่ายและเร็ว เนื่องจากหากเกิดเหตุแล้วประชาชนหรือมูลนิธิอาจไปถึงก่อนทำให้ภาพแห่งความรุนแรงหลุดไปก่อน

๓.๓.๒ มีหน่วยงานติดตามข้อมูลข่าวสารทางสื่อสังคมออนไลน์และมีการประชุมกลั่นกรองเพื่อส่งต่อไปกระทรวงไอซีทีเพื่อปิดเว็บ และขั้นต่อไปจะต้องส่งฟ้องศาล แต่หากเป็นเว็บต่างประเทศต้องติดต่อผ่านกระทรวงต่างประเทศ

๓.๓.๓ มีทีมทำ IO ที่จัดตั้งมาสำหรับการตอบโต้ข่าวบิดเบือนผ่านสื่อสังคมออนไลน์ดังเช่นเหตุการณ์จับคนขับรถโรงเรียน ข่าวออกไปว่าตำรวจไปล้อมจับรถตู้ นักเรียนที่อยู่ในรถได้รับความเดือนร้อน ร้องไห้ตกใจ และทำเกินกว่าเหตุ แต่ในความเป็นจริงคนขับมีหมายจับและขับมาเจอด่านจึงมีการเชิญตัวไปและรับส่งนักเรียนอย่างเรียบร้อยโดยไม่มีการกระทำเกินกว่าเหตุ ผลที่ปรากฏทำให้ภาพลักษณ์ของเจ้าหน้าที่รัฐเสียหายมากในสานตาประชาชนและยังสามารถเป็นชนวนให้เกิดความขัดแย้งได้เพิ่มขึ้นอีก

๓.๔ การประเมินสถานการณ์ภัยคุกคามด้านไซเบอร์ที่พบในพื้นที่จังหวัดชายแดนภาคใต้จากความคิดเห็นของหน่วยงานภาคเอกชน หน่วยงานพลเรือน และภาคประชาชน สรุปได้ดังนี้

๓.๔.๑ ภัยคุกคามด้านไซเบอร์นับเป็นภัยคุกคามที่อันตรายร้ายแรง จะต้องมีการประชาสัมพันธ์ให้ทุกภาคส่วนรับรู้และเรียนรู้อย่างต่อเนื่องทั้งทางสื่อสังคมออนไลน์เองและการลงพื้นที่ทำความเข้าใจกับประชาชน

๓.๔.๒ เจ้าหน้าที่รัฐจะจัดการกับปัญหาสื่อสังคมออนไลน์ที่มีลักษณะสร้างความรุนแรงเหล่านี้ได้ยากขึ้น เพราะบางส่วนอาจคิดว่าเป็นเครื่องมือของเจ้าหน้าที่รัฐ

๓.๔.๓ มีการประเมินสถานการณ์ตลอด แต่หากมีเหตุการณ์ใหญ่ก็จะมีการออกหนังสือชี้แจงและหากเล็กน้อยก็จะไม่ตอบโต้ ประชาชนส่วนใหญ่มีการคิดวิเคราะห์ก่อนเมื่อได้รับข้อมูลข่าวสารที่ไม่ชัดเจนและจะไม่เผยแพร่ต่อถ้ายังไม่มั่นใจ

ผลการศึกษาตอบวัตถุประสงค์ข้อที่ ๒ สรุปได้ว่า ผลกระทบของภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงแห่งชาติรวมถึงแนวโน้มในอนาคต ปรากฏผลดังประเด็นต่อไปนี้

๑. ผลกระทบของภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงแห่งชาติรวมถึงแนวโน้มในอนาคตจากความคิดเห็นของหน่วยงานด้านความมั่นคงของรัฐ (กองทัพภาคที่ ๔, กอ.รมน.ภาค ๔ ส่วนหน้า, ศอบต., ศชต., และ ฉก.) ผู้บริหาร/ผู้นำท้องถิ่น ๔ จังหวัด สรุปได้ดังนี้

๑.๑ การสร้างทัศนคติเชิงลบต่อรัฐให้กับประชาชนส่งผลต่อความมั่นคงแห่งชาติเป็นอย่างยิ่ง โดยหากประชาชนจะไปรับข้อมูลข่าวสารอื่นที่ถูกบิดเบือนผ่านสื่อสังคมออนไลน์อย่างต่อเนื่อง ทำให้ต่อไปประชาชนอาจจะไม่เชื่อหรือไม่รับข้อมูลใดจากฝ่ายรัฐอีก และในที่สุดจะนำไปสู่ความเกลียดชังต่อเจ้าหน้าที่ของรัฐและยากที่จะปรับทัศนคติให้กลับคืนมาได้

๑.๒ ผลกระทบต่อความมั่นคงแห่งชาติจะทำให้เกิดความแตกแยกของผู้คนทั้งทางด้านเชื้อชาติและศาสนา โดยเป็นการทำลายสังคมพหุวัฒนธรรมของพื้นที่นี้จนอาจนำไปสู่การแยกตัวไปเป็นเอกเทศในอนาคตการยังไม่ได้รับการแก้ไข

๑.๓ แนวโน้มในอนาคตของภัยคุกคามด้านไซเบอร์จะยังคงเป็นปัญหาหลักที่รัฐบาลต้องดำเนินการอย่างเป็นระบบ ก่อนที่จะเกิดเหตุการณ์บานปลายจนกระทั่งรัฐบาลอาจไม่อยู่ในสถานะควบคุมได้ต่อไป นั่นคือ รัฐไม่มีเสถียรภาพและรัฐไม่มีความน่าเชื่อถือในการดำเนินการเรื่องความปลอดภัย

๑.๔ ปัญหาเรื่องภัยคุกคามด้านไซเบอร์อาจก่อให้เกิดปัญหาระหว่างประเทศได้ถ้าไม่มีกระบวนการแก้ไขโดยความเห็นชอบสากล

๒. ผลกระทบของภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงแห่งชาติรวมถึงแนวโน้มในอนาคตจากความคิดเห็นของเจ้าหน้าที่ระดับปฏิบัติการด้านความมั่นคงรวมถึงเจ้าหน้าที่ทหารที่รับผิดชอบด้านภัยคุกคามของสำนักปฏิบัติการข่าวสาร สรุปได้ดังนี้

๒.๑ ในโลกไซเบอร์มีการนำประเด็นชาติพันธ์และศาสนา เข้ามาเป็นประเด็นเพื่อการสร้างข่าวบิดเบือนและเผยแพร่สู่เครือข่ายสังคมออนไลน์ ซึ่งจะส่งผลให้เกิดความเกลียดชังขึ้นในสังคมทุกระดับชั้นโดยทำให้สังคมนั้นอยู่ร่วมกันโดยไม่มีความสงบสุข

๒.๒ ในโลกไซเบอร์และเครือข่ายสังคมออนไลน์มีการนำประเด็นในอดีตทั้งประวัติศาสตร์ที่จริงและบิดเบือนมาใช้เป็นเงื่อนไขสร้างสถานการณ์รุนแรง การสร้างความคิดความเชื่อให้เยาวชนซึ่งจะส่งผลต่ออนาคตของชาติในระยะยาว

๒.๓ ในความเป็นจริงพบว่า ชาวบ้านต้องการความสงบแต่ไม่กล้าบอกเจ้าหน้าที่เนื่องจากไม่แน่ใจว่าเจ้าหน้าที่จะคุ้มครองได้ตลอดชีวิตหรือไม่ ดังนั้นต้องหาวิถีทางคุ้มครองความปลอดภัยของชีวิตและทรัพย์สินให้ดีขึ้นโดยอาจต้องปรับกฎหมายด้านการคุ้มครองให้เห็นเป็นประจักษ์และถูกต้องตามหลักสากล

๒.๔ หากมีปัจจัยหรือสถานการณ์ที่น่าจะมีแนวโน้มรุนแรงมากขึ้น ภาครัฐต้องระวังไม่ให้เกิดเหตุเพื่อให้ผู้ก่อการร้ายนำไปขยายผลไปสู่ความรุนแรงอื่นๆ ได้

๓. ผลกระทบของภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงแห่งชาติรวมถึงแนวโน้มในอนาคตจากความคิดเห็นของนักวิชาการและผู้เชี่ยวชาญด้านระบบไอซีทีซึ่งเป็นเจ้าหน้าที่ด้านความมั่นคง สรุปได้ดังนี้

๓.๑ ในอนาคตถ้าไม่เกี่ยวข้องกับภัยคุกคามด้านไซเบอร์น่าจะมีการเกิดเหตุการณ์รุนแรงน้อยลง เนื่องจากฝ่ายผู้ก่อการร้ายอาจจะมีงบประมาณหรือผู้สนับสนุนน้อยลง

๓.๒ เหตุการณ์ความไม่สงบมักเกิดจากผลประโยชน์ของคนบางกลุ่มและเจ้าเมืองเก่า โดยมีการปลูกฝังเยาวชนรุ่นใหม่ให้เข้าใจผิดและเกลียดชังต่อรัฐบาล อย่างไรก็ตามมีคนอิสลามรุ่นใหม่ที่มีใจยอมรับได้มากขึ้น

๓.๓ มีแนวโน้มเกิดเหตุการณ์การสร้างข่าวสารบิดเบือนผ่านสื่อสังคมออนไลน์จะทวีความรุนแรงมากยิ่งขึ้นเนื่องจากมีการใช้ไซเบอร์มากขึ้น มีการดึงต่างประเทศเข้ามาร่วมเพื่อให้มีผู้สนับสนุนให้แยกประเทศโดยทำให้ประเทศไทยมีปัญหาในเวทีโลก

๓.๔ ปัจจุบันยังมีกระบวนการละเมิดสถาบันพระมหากษัตริย์ผ่านเครือข่ายสังคมออนไลน์อย่างต่อเนื่อง ซึ่งถือว่าเป็นภัยคุกคามด้านความมั่นคงแห่งชาติต่อสถาบันหลักของประเทศ

๔. ผลกระทบของภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงแห่งชาติรวมถึงแนวโน้มในอนาคตจากความคิดเห็นของหน่วยงานภาคเอกชน หน่วยงานพลเรือน และภาคประชาชน สรุปได้ดังนี้

๔.๑ มาตรการป้องกันและแก้ไขของเจ้าหน้าที่รัฐยังไม่เหมาะสม ดังเช่น เมื่อผู้ต้องหาส่วนมากที่เป็นผู้ปลุกปั่นและบิดเบือนข่าวสารในสังคมออนไลน์ แต่เจ้าหน้าที่ไม่มีเครื่องมือในการหาหลักฐานอย่างเช่นการตรวจ IP Address เป็นต้น

๔.๒ ส่งผลกระทบต่อจิตใจของประชาชนอย่างหลีกเลี่ยงไม่ได้ เนื่องจากภัยคุกคามด้านไซเบอร์จะสามารถนำไปสู่ชนวนแห่งการสร้างสถานการณ์รุนแรงได้อยู่เสมอ ดังนั้นควรใช้ยุทธศาสตร์ชาติในการแก้ไขปัญหาอย่างเป็นระบบ

ส่วนรูปแบบที่เหมาะสมสำหรับการจัดการภัยคุกคามด้านไซเบอร์สำหรับประเทศไทย สรุปได้ดังนี้ ประเทศไทยนั้นการกำหนดนโยบายและยุทธศาสตร์ในการจัดการภัยคุกคามด้านไซเบอร์มักเกิดขึ้นจากภาครัฐเป็นส่วนใหญ่ โดยอาศัยหน่วยงานด้านความมั่นคงและกระทรวงที่เกี่ยวข้องในการกำหนดนโยบายตามที่ปรากฏในยุทธศาสตร์ชาติระยะ ๒๐ ปี พ.ศ.๒๕๖๐-๒๕๗๘ โดยไม่มีประเด็นที่เกี่ยวกับรูปแบบการดำเนินงาน แผนงาน และมาตรการที่เกี่ยวข้อง ซึ่งยังไม่ปรากฏเด่นชัดจากการที่ไม่ได้กำหนดเจ้าภาพรับผิดชอบโดยตรง จากการศึกษาข้อมูลเอกสารรายงาน และการวิจัยที่เกี่ยวข้องสามารถนำมาวิเคราะห์เพื่อหารูปแบบที่เหมาะสมของการจัดการภัย

คุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ โดยกำหนดเป็นประเด็นที่เกี่ยวกับผู้รับผิดชอบโดยตรงด้านไซเบอร์ในระดับชาติก่อนเพื่อให้เห็นภาพรวมของการทำสงครามไซเบอร์ ซึ่งสามารถกำหนดองค์ประกอบหลักของการรักษาความมั่นคงปลอดภัยด้านไซเบอร์แห่งชาติ ประกอบด้วย ๑) รัฐบาล ๒) กระทรวงที่เกี่ยวข้อง ๓) หน่วยงานด้านความมั่นคงของชาติ ๔) กองบัญชาการกองทัพไทย และ ๕) หน่วยบัญชาการไซเบอร์แห่งชาติ ส่วนโครงสร้างของหน่วยบัญชาการไซเบอร์แห่งชาติและโครงสร้างพื้นฐานการจัดการภัยคุกคามด้านไซเบอร์ประกอบด้วย ๑) หน่วยบัญชาการไซเบอร์แห่งชาติ (National Cyber Department), ๒) เทคโนโลยีฮาร์ดแวร์ (Hardware Technology), ๓) เทคโนโลยีซอฟต์แวร์ (Software Technology), ๔) เทคโนโลยีเครือข่ายความเร็วสูง (Hi-Speed Network Technology), ๕) นักปฏิบัติการด้านไซเบอร์ (Cyber Operators) และ ๖) รูปแบบการจัดการภัยคุกคามด้านไซเบอร์ (Cyber Treats Management Format)

ผลจากความเสียหายที่เกิดจากภัยคุกคามด้านไซเบอร์ที่ผ่านมา ทำให้รัฐบาลไทยตระหนักดีถึงผลกระทบทั้งในแง่ที่เป็นประโยชน์และโทษจากการทำสงครามไซเบอร์ โดยพยายามพัฒนาขีดความสามารถด้านการทำสงครามไซเบอร์ทั้งในเชิงรุกและการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ เพื่อใช้เป็นมาตรการทั้งเชิงรุกและเชิงรับจากการโจมตีด้านไซเบอร์ของฝ่ายตรงข้าม (สราวุธ ปิติยาศักดิ์, ๒๕๖๑) ประเด็นสำคัญของนโยบายและแนวทางด้านการทำสงครามไซเบอร์ของประเทศไทย ในส่วนกระทรวงกลาโหม กองทัพไทย และกองทัพบก มีดังนี้

(๑) ควรพัฒนายุทธศาสตร์ นโยบาย และแนวทางการปฏิบัติ เพื่อใช้รับมือกับภัยคุกคามด้านไซเบอร์ทุกรูปแบบ โดยอาศัยความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้องเพื่อที่จะเสริมขีดความสามารถ ผนึกกำลัง และเสริมสร้างกำลังอำนาจที่ไม่มีตัวตนในโลกไซเบอร์ของฝ่ายเรา

(๒) ควรนำกรอบยุทธศาสตร์ด้านไซเบอร์ทั้ง ๓ ด้าน ไม่ว่าจะเป็นด้านการป้องกัน การป้องปราม และการผนึกกำลัง ไปดำเนินการเพื่อให้บรรลุผลสำเร็จตามยุทธศาสตร์ดังกล่าวอย่างเป็นรูปธรรม

(๓) ควรเตรียมการรับมือกับภัยคุกคามด้านไซเบอร์ โดยอาศัยกรอบการดำเนินงาน ๕ ขั้นตอน ดังเช่นเดียวกับพันธกิจ ๕ อย่าง ที่สถาบันมาตรฐานและเทคโนโลยีแห่งสหรัฐอเมริกาใช้ ซึ่งขั้นตอนเหล่านี้เป็นพื้นฐานของการรับมือกับการโจมตีด้านไซเบอร์ที่ทั่วโลกยอมรับ เพื่อให้ระบบกลับมาใช้งานต่อไปได้ตามปกติ จากขั้นตอนดังกล่าวทำให้เห็นได้ว่าทุกหน่วยงานที่มีการใช้ระบบด้านสารสนเทศเป็นหน้าที่ของบุคลากรภายในหน่วยที่จะเป็นผู้ดำเนินการโดยอาศัยเครื่องมือที่มีอยู่ของหน่วย หลักการที่สำคัญต่อการดำเนินการตามขั้นตอนเพื่อรับมือกับภัยคุกคามด้านไซเบอร์ ก็คือ “ตรวจพบให้เร็ว” “ป้องกันไว้ก่อน” “ค้นหาให้เจอ” “ตอบสนองให้ไว” และ “กู้คืนให้ได้” (Richard A. Clarke, 2017)

(๔) ควรพัฒนากำลังพลของกองทัพให้มีความรู้ความสามารถเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ เพื่อให้กำลังพลของกองทัพมีความรู้ที่ทันต่อสถานการณ์ที่เปลี่ยนแปลงไปอย่างความต่อเนื่องและมีทักษะที่จำเป็นต่อการรับมือกับภัยคุกคามที่หลากหลายรูปแบบในขณะเดียวกัน ก็ควรกองทัพในเรื่องการบริหารจัดการ เครื่องมือ และบุคลากรให้สอดรับกับแนวทางการปฏิบัติ นโยบาย และยุทธศาสตร์ที่รัฐบาลได้กำหนดขึ้น ทั้งนี้โดยอาศัยการประสานงานและบูรณาการระหว่างเหล่าทัพ รวมถึงภาครัฐและเอกชนที่เกี่ยวข้อง เพื่อผนึกกำลังกันสร้างพลังอำนาจที่ไม่มีตัวตนเพื่อรับมือกับการโจมตีดังกล่าว

(๕) ควรให้ความรู้และสร้างความตระหนักรู้ถึงภัยคุกคามด้านไซเบอร์ให้กับกำลังพล บุคคลในครอบครัว ญาติพี่น้อง หรือบุคคลในสถานศึกษาต่างๆ เพื่อให้ช่วยกันเฝ้าระวัง ติดตาม และตระหนักในเรื่องของการใช้เทคโนโลยีไม่ให้พวกเขาตกเป็นเหยื่อหรือเป็นเป้าหมายของการโจมตีด้านไซเบอร์ได้ง่าย

ในฐานะปัจเจกชน โลกไซเบอร์ย่อมถือได้ว่าอาจเป็นคุณอย่างมหาศาลหรืออาจเป็นโทษอย่างอนันต์ก็ได้ อย่างไรก็ตาม ภัยคุกคามที่มาพร้อมกับประโยชน์ที่ได้จากโลกไซเบอร์นี้อาจเกิดขึ้นได้ตลอดเวลาและมีความเสี่ยงสูงที่ผู้ใช้งานด้านต่างๆ ในโลกไซเบอร์จะต้องประสบกับปัญหาจากภัยคุกคามในโลกไซเบอร์ดังกล่าว ดังนั้น กำลังพลของกองทัพหรือประชาชนทั่วไปที่มีส่วนเกี่ยวข้องกับการแสวงประโยชน์จากโลกไซเบอร์พึงต้องตระหนักถึงภัยคุกคามและผลกระทบที่จะเกิดขึ้นตามมา รวมถึงให้ความสำคัญกับการรักษาความปลอดภัยในโลกไซเบอร์อย่างเคร่งครัดในเบื้องต้น (สราวุธ ปิติยาศักดิ์, ๒๕๖๐) ดังนี้

(๑) ไม่ควรระบุข้อมูลส่วนตัวในการลงทะเบียนสมาชิก (Registration) ที่เกินความจำเป็น และเผยแพร่สู่สาธารณะ เช่น ชื่อ/นามสกุลจริง วันเดือนปีเกิด สถานที่เกิด ภูมิลำเนา สถานที่ทำงาน หมายเลขโทรศัพท์ และอีเมล์ เป็นต้น เพราะอาจจะถูกใช้เป็นข้อมูลอ้างอิงให้กับผู้ประสงค์ร้าย และคาดเดารหัสผ่าน (Password) ที่ใช้อยู่ได้

(๒) ควรกำหนดรหัสผู้ใช้งาน (Username) และรหัสผ่านโดยปฏิบัติตามกฎการรักษาความปลอดภัยด้านสารสนเทศ ควรเปลี่ยนแปลงรหัสผ่านด้วยตนเองในภายหลังตามที่ระบบกำหนดหรือเปลี่ยนตามห้วงระยะเวลา และควรหลีกเลี่ยงการกำหนดรหัสที่เป็นชื่อ วันเดือนปีเกิด หรือรหัสอื่นๆ ที่นักเจาะระบบสามารถเดาสุ่มได้ ไม่ควรเปิดเผยรหัสผ่านให้ผู้อื่นทราบ โดยเฉพาะการให้ผู้อื่นนำรหัสผ่านของตนมาเข้าใช้งานแทน เพราะอาจมีการนำไปใช้งานในทางที่มิชอบ และไม่ควรจดบันทึกรหัสผ่านลงในบัตรอิเล็กทรอนิกส์ บัตรเครดิต และกระดาษบันทึก หรือบันทึกลงในโทรศัพท์มือถือ เป็นต้น เพราะมีโอกาสสูญหายและรั่วไหลไปยังบุคคลอื่นได้

(๓) ไม่ควรนำข้อมูลแผนการต่างๆ อย่างละเอียดเผยแพร่บนสื่อสาธารณะ เช่น แผนการเดินทางส่วนตัว ข้อมูลแผนที่เกี่ยวกับที่อยู่อาศัย และระบุชื่อบุคคลในรูปภาพ (ติด Tag) เพราะจะเป็นข้อมูลให้กับเหล่ามิจฉาชีพ อาจถูกนำไปใช้ในทางมิชอบ หรือส่งผลกระทบต่อกองทัพ

(๔) ไม่ควรปล่อยให้เด็กใช้งานระบบคอมพิวเตอร์หรือระบบเครือข่ายโดยอิสระ โดยขาดการตรวจสอบ ควบคุม กำกับดูแลของผู้ใหญ่ เพราะเด็กอาจจะนำข้อมูลที่ไม่เหมาะสมไปเผยแพร่ด้วยความคึกคะนอง ไม่ตั้งใจ ไม่ทันคิด หรืออาจจะถูกล่อลวงไปในทางมิชอบ

(๕) หลีกเลี่ยงการนำเสนอข้อมูลพฤติกรรมส่วนตัวที่ส่งผลกระทบต่อความสงบเรียบร้อยทางสังคมทุกรูปแบบ เพราะอาจจะถูกนำไปใช้เป็นเครื่องมือในทางมิชอบ หรือนำไปสู่การเลียนแบบพฤติกรรมที่ไม่ดี

(๖) ไม่ใช้บริการเครือข่ายสังคมออนไลน์ที่ไม่แน่ใจในเรื่องของความปลอดภัย แต่ให้เลือกใช้งานเฉพาะกลุ่มและสมาชิกที่มีความรู้จักมักคุ้น มีความเชื่อถือไว้ใจได้ มีความปลอดภัย และมีพฤติกรรมที่เหมาะสม เพื่อป้องกันข้อมูลข่าวสารในกลุ่มไม่ให้ถูกเผยแพร่ออกไป

(๗) ระบบงานที่มีความสำคัญยิ่ง ควรใช้อุปกรณ์ทางชีวภาพ (Biometric Device) เช่น การสแกนลายนิ้วมือ (Finger Scan) การสแกนฝ่ามือ (Palm Scan) หรือการสแกนม่านตา (Eye Scan) เป็นต้น เพื่อใช้เป็นอุปกรณ์ตรวจสอบลักษณะส่วนบุคคลทางชีวภาพ และเป็นการยืนยันตัวบุคคล (Authentic) ประกอบกับการใช้รหัสผ่านเพื่ออนุญาตการเข้าใช้งานโปรแกรม ระบบงาน หรือการเข้าใช้ห้องระบบคอมพิวเตอร์

(๘) การใช้งานเครือข่ายอินเตอร์เน็ตสาธารณะแบบไร้สาย (Public WiFi) หรือเครือข่ายอินเตอร์เน็ตไร้สายฟรี (Free WiFi) ผู้ใช้พึงต้องระมัดระวัง รอบคอบ และมั่นใจว่าได้ในเรื่องความปลอดภัย ไม่ควรติดตั้งระบบอินเตอร์เน็ตไร้สายฟรี เพราะจะเป็นช่องทางให้นักเจาะระบบ หรือผู้ไม่ประสงค์ดีเข้ามาใช้งานในทางมิชอบและเจาะระบบเข้าถึงข้อมูลในองค์กรได้อย่างง่ายดาย รวมถึงส่งผลต่อการทำงานและก่อปัญหาให้กับองค์กรในภาพรวมได้อีกด้วย

จากผลการศึกษาสามารถนำมาสร้างมาตรการป้องกันภัยคุกคามทางอินเตอร์เน็ตเพื่อการรักษาความมั่นคงปลอดภัยของข้อมูลข่าวสารดังนี้ (ปริญญา หอมเอนก, ๒๕๖๑)

๑. มาตรการป้องกันภัยคุกคามทางอินเตอร์เน็ตสำหรับหน่วยงาน

๑.๑ ตรวจสอบและยืนยันสิทธิการเข้าระบบที่สำคัญของบัญชีผู้ใช้ให้สอดคล้องกับความจำเป็นเข้าถึงระบบและข้อมูล

๑.๒ เพิ่มมาตรการป้องกันเว็บไซต์สำคัญด้วยระบบการป้องกันการโจมตี เช่น Web Application Firewall หรือ DDoS

๑.๓ แจ้งเจ้าหน้าที่ของหน่วยงานและพนักงานให้เพิ่มความระมัดระวังในการใช้อินเตอร์เน็ตโดยหลีกเลี่ยงการเข้าเว็บไซต์ที่ไม่เหมาะสม ไม่คลิกไฟล์แนบจากผู้อื่นกรณีที่ไม่ได้ตกลงกันก่อนหรือไม่รับเมล์แนบจากคนที่ไม่รู้จัก ระมัดระวังความเสี่ยงจากการเปิดไฟล์ผ่านโปรแกรมสนทนาต่างๆ หรือช่องทางเครือข่ายออนไลน์ทุกชนิด ทั้งนี้เพื่อหลีกเลี่ยงการติดมัลแวร์

๑.๔ หากพบพิรุธว่าระบบถูกโจมตี เช่น ไม่สามารถเข้าใช้งานระบบ/เว็บไซต์ได้ หรือมีความล่าช้ากว่าปกติ ควรตรวจสอบข้อมูลการเข้าถึงระบบที่สำคัญ เช่น ข้อมูล Log ย้อนหลัง ๓๐ วัน เพื่อตรวจหาความผิดปกติในการเข้าถึงข้อมูล

๑.๕ การตั้งค่าระบบงานที่สำคัญให้บันทึกเหตุการณ์ (Log) การเข้าใช้งานระบบไม่ต่ำกว่า ๙๐ วัน หรือตามที่กฎหมายกำหนด

๑.๖ หากเป็นไปได้ ให้หน่วยงานส่งรายชื่อผู้ติดต่อ (Contact Point) กรณีเกิดเหตุภัยคุกคามด้านไซเบอร์มายังศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย : ThaiCERT (ไทยเซิร์ต) เพื่อการตรวจสอบที่ถูกต้อง

๒. มาตรการป้องกันภัยคุกคามทางอินเตอร์เน็ตสำหรับประชาชนทั่วไป

๒.๑ เพิ่มความระมัดระวังในการใช้อินเตอร์เน็ต โดยหลีกเลี่ยงการเข้าเว็บไซต์ที่ไม่เหมาะสม เว็บผิดกฎหมาย ไม่คลิกไฟล์แนบจากผู้อื่นกรณีที่ไม่ได้ตกลงกันหรือไม่รู้จักกันมาก่อน ระมัดระวังความเสี่ยง จากการเปิดไฟล์ผ่านโปรแกรมสนทนาต่างๆ หรือช่องทางสื่อสังคมออนไลน์ เพื่อหลีกเลี่ยงการติดมัลแวร์ ซึ่งนับวันมัลแวร์จะมาจากพวกไฟล์แนบทางเครือข่ายสังคมออนไลน์เพิ่มมากขึ้น

๒.๒ การใช้บริการอินเตอร์เน็ต อย่าตั้งรหัสผ่านเหมือนกันทุกระบบ เพราะหากคุณโดนแฮกเกอร์เจาะระบบสำเร็จแล้ว ระบบอื่นๆ ก็อาจถูกเจาะระบบด้วยหากใช้รหัสผ่านเดียวกัน

๒.๓ ติดตามข้อมูลข่าวสารเกี่ยวกับความมั่นคงปลอดภัยด้านไซเบอร์ และอ่านพิจารณาข้อมูลก่อนการแชร์ข้อมูลทุกครั้ง ตลอดจนไม่ส่งต่อข้อมูลที่ไม่ได้รับการยืนยันจากผู้ที่เกี่ยวข้อง

เมื่อนำข้อมูลทุกด้านมาตรวจสอบด้วยวิธีการสามเส้าด้านข้อมูลพบว่า ข้อมูลที่ได้มาจากการศึกษาเอกสารและรายงานการวิจัยที่เกี่ยวข้อ การสัมภาษณ์ และข้อเท็จจริงที่เกิดขึ้น สามารถกล่าวได้ว่าภัยคุกคามด้านไซเบอร์เป็นภัยที่ร้ายแรงสำหรับประเทศไทย ดังนั้นจึงควรมีนโยบาย มาตรการ แผนงาน และกิจกรรมที่ต้องสอดคล้องกับนโยบายแห่งรัฐเพื่อการจัดการภัยคุกคามให้มีประสิทธิภาพต่อไป

จากผลการศึกษาวิจัยสามารถนำข้อมูลทั้งหมดมาวิเคราะห์ SWOT และกำหนดร่างยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้เพื่อตอบวัตถุประสงค์

ข้อที่ ๓ สรุปได้ว่ายุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ประกอบด้วย

วิสัยทัศน์ (Vision) : ประเทศไทยมีศักยภาพในการจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ของประเทศไทย

พันธกิจ (Mission) : การพัฒนารูปแบบการจัดการภัยคุกคามด้านไซเบอร์โดยมุ่งสร้างฐานความรู้ให้กับประชาชนทุกระดับ เพื่อความมั่นคงปลอดภัยและความสงบสุขในพื้นที่จังหวัดชายแดนภาคใต้ของประเทศไทย

วัตถุประสงค์ (Objective) :

๑. เพื่อใช้เป็นยุทธศาสตร์ที่มีประสิทธิภาพในการจัดการกับภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ของประเทศไทย

๒. เพื่อพัฒนาขีดความสามารถในการจัดการกับภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ของประเทศไทย

๓. เพื่อเสริมสร้างความมั่นคงปลอดภัยด้านไซเบอร์และก่อให้เกิดความสงบสุขในพื้นที่จังหวัดชายแดนภาคใต้ของประเทศไทย

ยุทธศาสตร์ (Strategy) : ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ ประกอบด้วย IADCLIP โดยมีโครงสร้างประกอบด้วย

ยุทธศาสตร์ที่ ๑ : ยุทธศาสตร์การจัดโครงสร้างพื้นฐานของประเทศไทยสำหรับใช้ในการจัดการกับภัยคุกคามด้าน ไซเบอร์ (Infrastructure)

เป้าหมายยุทธศาสตร์ : เพื่อการจัดโครงสร้างพื้นฐานของประเทศไทยสำหรับการจัดการกับภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

แนวทางหรือมาตรการ มีดังต่อไปนี้

๑. การจัดโครงสร้างพื้นฐานของประเทศไทยสำหรับใช้ในการจัดการกับภัยคุกคามด้านไซเบอร์ประกอบด้วย ๑) หน่วยบัญชาการไซเบอร์แห่งชาติ (National Cyber Department), ๒) เทคโนโลยีฮาร์ดแวร์ (Hardware Technology), ๓) เทคโนโลยีซอฟต์แวร์ (Software Technology), ๔) เทคโนโลยีเครือข่ายความเร็วสูง (Hi-Speed Network Technology), ๕) นักปฏิบัติการด้านไซเบอร์ (Cyber Operators) และ ๖) รูปแบบการจัดการภัยคุกคามด้านไซเบอร์ (Cyber Treats Management Format)

๒. การกำหนดรูปแบบการจัดการภัยคุกคามด้านไซเบอร์ที่เหมาะสมและมีประสิทธิภาพโดยคำนึงถึงความมั่นคงปลอดภัยและความสงบสุขของประชาชนอย่างเป็นด้านหลัก

ยุทธวิธีหรือแผนปฏิบัติการ มีดังต่อไปนี้

๑. การนำโครงสร้างพื้นฐานไปใช้จัดตั้งเพื่อกำหนดให้เป็นโครงสร้างหลักในการจัดการภัยคุกคามด้านไซเบอร์

๒. นำรูปแบบของระบบไอซีทีเพื่อการบริหารจัดการองค์กรเพื่อความมั่นคงปลอดภัย โดยเน้นการรักษาความมั่นคงปลอดภัยตามมาตรฐานสากล

ดัชนีชี้วัดผลงาน : ระบบป้องกันภัยคุกคามด้านไซเบอร์และสถิติการบุกรุกเพื่อจารกรรมข้อมูลข่าวสาร

ผลที่คาดว่าจะได้รับตามยุทธศาสตร์ที่ ๑ : ประเทศไทยมีโครงสร้างพื้นฐานสำหรับการจัดการกับภัยคุกคามด้าน ไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

ยุทธศาสตร์ที่ ๒ : ยุทธศาสตร์การสร้างการตระหนักรู้โลกไซเบอร์ให้กับประชาชน (Awareness)

เป้าหมายยุทธศาสตร์ : เพื่อการสร้างการตระหนักรู้โลกไซเบอร์ให้กับประชาชนในพื้นที่จังหวัดชายแดนภาคใต้

แนวทางหรือมาตรการ มีดังต่อไปนี้

๑. การสนับสนุนให้ประชาชนมีการสร้างความรู้ความเข้าใจที่ดีต่อการใช้งานด้านไซเบอร์และมีการถ่ายทอดความรู้ความเข้าใจที่ดีต่อการใช้ไซเบอร์เพื่อประโยชน์ส่วนตนรวมถึงประเทศชาติ รวมทั้งมีการถ่ายทอดความรู้ความเข้าใจจากรุ่นไปสู่รุ่น

๒. การเผยแพร่ความรู้และประชาสัมพันธ์ให้ประชาชนมีการใช้งานด้านไซเบอร์อย่างถูกวิธีรวมทั้งตระหนักถึงผลกระทบต่อการใช้งานไซเบอร์ที่ไม่ถูกต้อง เพื่อป้องกันการนำมาใช้เป็นเครื่องมือในการก่อการร้ายในประเทศไทย

ยุทธวิธีหรือแผนปฏิบัติการ มีดังต่อไปนี้

๑. สร้างรูปแบบและวิธีการในการให้ความรู้ความเข้าใจโดยอาจใช้วิธีการฝึกอบรมภายในหน่วยงานหรือการถ่ายทอดความรู้โดยใช้สื่อสารมวลชน

๒. ใช้สถาบันการศึกษาในการถ่ายทอดความรู้ความเข้าใจให้กับเยาวชนโดยอาจบรรจุไว้ในหลักสูตรหรือกิจกรรมเสริมหลักสูตร

๓. กำหนดหลักสูตรที่เกี่ยวกับไซเบอร์ในทุกระดับเพื่อให้เยาวชนได้มีรากฐานของการศึกษาและเข้าใจต่อการใช้ไซเบอร์อย่างถูกต้อง

๔. พัฒนาหลักสูตรในระดับอุดมศึกษาเพื่อพัฒนาองค์ความรู้ทางไซเบอร์ให้สามารถนำความรู้ไปใช้อย่างครอบคลุมและมีประสิทธิภาพในทุกมิติ

ดัชนีชี้วัดผลงาน : ความรู้ความเข้าใจต่อภัยคุกคามด้านไซเบอร์และรูปแบบการใช้งานด้านไซเบอร์ที่สร้างสรรค์ต่อสังคมโดยไม่ใช่การก่ออาชญากรรม

ผลที่คาดว่าจะได้รับตามยุทธศาสตร์ที่ ๒ : ประชาชนในพื้นที่จังหวัดชายแดนภาคใต้มีความตระหนักรู้ต่อภัยคุกคามด้านไซเบอร์และมีรูปแบบการใช้งานที่ไม่เป็นภัยต่อผลประโยชน์และความมั่นคงของชาติ

ยุทธศาสตร์ที่ ๓ : ยุทธศาสตร์การพัฒนาความก้าวหน้าด้านไซเบอร์ (Development)

เป้าหมายยุทธศาสตร์ : เพื่อการพัฒนาความก้าวหน้าด้านไซเบอร์ของประเทศไทยให้เข้าสู่มาตรฐานสากล

แนวทางหรือมาตรการ มีดังต่อไปนี้

๑. การจัดตั้งหน่วยงานการพัฒนาด้านไซเบอร์เพื่อพัฒนาระบบไอซีทีและการรักษาความปลอดภัยทางไซเบอร์ข้อมูลข่าวสาร

๒. จัดฝึกอบรมให้ความรู้ สนับสนุนการจัดสอบเพื่อให้บุคลากรผ่านเกณฑ์มาตรฐานสากลรวมทั้งการวิจัยสร้างองค์ความรู้ใหม่ทางด้านไซเบอร์

๓. การพัฒนาบุคลากรให้มีความเชี่ยวชาญในการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ รวมทั้งสร้างแรงจูงใจในการจงรักภักดีและทำงานเพื่อประเทศชาติเพื่อป้องกันสมองไหลไปยังต่างประเทศ

ยุทธวิธีหรือแผนปฏิบัติการ มีดังต่อไปนี้

๑. การสร้างหน่วยงานด้านความมั่นคงปลอดภัยด้านไซเบอร์ที่มีเครื่องมือและอุปกรณ์ที่ทันสมัย และพร้อมรับมือกับการป้องกัน การโจมตี และการโต้ตอบ

๒. การสร้างชุดกิจกรรมฝึกอบรมกับประชาชนทุกระดับให้ทราบถึงความหมายและการรักษาความปลอดภัยทั้งข้อมูลส่วนตัวและข้อมูลส่วนรวม

๓. จัดโครงการพัฒนาบุคลากรในหน่วยงานด้านความมั่นคงของชาติให้เป็นผู้เชี่ยวชาญด้านไซเบอร์ที่มีศักยภาพสูงและพร้อมปฏิบัติการทุกรูปแบบ

๔. การวิจัยและพัฒนาด้านไซเบอร์ที่เป็นประโยชน์ต่อการพัฒนาประเทศไทยและต่อต้านการก่อการร้ายด้านไซเบอร์

ดัชนีชี้วัดผลงาน : ทุกองค์กรในหน่วยงานด้านความมั่นคงของชาติรวมถึงภาคธุรกิจเอกชนมีผู้เชี่ยวชาญด้านไซเบอร์ที่มีศักยภาพสูงและงานวิจัยที่มีคุณภาพ

ผลที่คาดว่าจะได้รับตามยุทธศาสตร์ที่ ๓ : ประเทศไทยมีความก้าวหน้าด้านไซเบอร์และมีรูปแบบการบริหารจัดการเทียบเท่ามาตรฐานสากล ทำให้เป็นจุดเริ่มต้นของการสร้างความสงบสุขในพื้นที่จังหวัดชายแดนภาคใต้

ยุทธศาสตร์ที่ ๔ : ยุทธศาสตร์การส่งเสริมความร่วมมือด้านไซเบอร์ระหว่างภาครัฐ ภาคเอกชน และภาคประชาชน (Coordinate)

เป้าหมายยุทธศาสตร์ : เพื่อการสร้างความร่วมมือด้านไซเบอร์ระหว่างภาครัฐ ภาคเอกชน และภาคประชาชน

แนวทางหรือมาตรการ มีดังต่อไปนี้

๑. มีการเสริมสร้างความเข้าใจร่วมกันในการกำหนด นิยาม ความหมายของภัยคุกคามด้านไซเบอร์ การก่อการร้าย และการก่อการร้ายทางไซเบอร์

๒. มีการกำหนดนโยบาย แนวทาง และแผนปฏิบัติการที่ชัดเจนเพื่อให้เกิดการแปลงแผนไปสู่กลยุทธ์และไปสู่การปฏิบัติตามวิสัยทัศน์ พันธกิจ และเป้าประสงค์ที่กำหนดไว้อย่างมีประสิทธิภาพ

๓. กำหนดกลไกในการทบทวน ติดตาม และประเมินความเสี่ยงต่อการนำแผนงานไปปรับใช้เพื่อปรับแนวทางให้มีความเหมาะสมตามสถานการณ์ใหม่หรือสถานการณ์ที่แตกต่าง

ยุทธวิธีหรือแผนปฏิบัติการ มีดังต่อไปนี้

๑. การใช้หน่วยบัญชาการไซเบอร์แห่งชาติเป็นศูนย์กลางเพื่อร่วมกันกำหนด นิยาม ความหมายของภัยคุกคามด้านไซเบอร์ การก่อการร้าย และการก่อการร้ายทางไซเบอร์

๒. การกำหนดนโยบาย แนวทาง และแผนปฏิบัติการที่ชัดเจนเพื่อนำไปสู่การปฏิบัติตามวิสัยทัศน์ พันธกิจ และเป้าประสงค์ที่กำหนดของทุกภาคส่วนอย่างมีประสิทธิภาพและประสิทธิผล

๓. การสร้างกลไกเฉพาะในการทบทวน ติดตาม และประเมินความเสี่ยงของภัยคุกคามด้านไซเบอร์ต่อการนำแผนงานไปปรับใช้อย่างมีประสิทธิภาพและประสิทธิผล

ดัชนีชี้วัดผลงาน : รูปแบบการใช้งานด้านไซเบอร์ที่มีประสิทธิภาพและประสิทธิผลทั้งในระดับองค์กรและระดับบุคคล

ผลที่คาดว่าจะได้รับตามยุทธศาสตร์ที่ ๔ : ทุกภาคส่วนของประเทศไทยมีความร่วมมือในการต่อต้านการก่อการร้ายด้านไซเบอร์โดยเฉพาะอย่างยิ่งในพื้นที่จังหวัดชายแดนภาคใต้

ยุทธศาสตร์ที่ ๕ : ยุทธศาสตร์การกำหนดใช้กฎหมายด้านไซเบอร์และการบังคับใช้กับประชาชน (Law and Enforcement)

เป้าหมายยุทธศาสตร์ : เพื่อการผลักดันการใช้กฎหมายสำหรับอาชญากรไซเบอร์ที่สร้างความรุนแรงในพื้นที่จังหวัดชายแดนภาคใต้

แนวทางหรือมาตรการ มีดังต่อไปนี้

๑. กำหนดกฎหมาย กฎระเบียบ ขั้นตอน และแนวปฏิบัติที่เกี่ยวข้องกับการใช้ด้านไซเบอร์ ความมั่นคงปลอดภัยด้านไซเบอร์ และการต่อต้านการก่อการร้ายด้านไซเบอร์อย่างครอบคลุม

๒. กำหนดแนวทางที่ชัดเจนและเหมาะสมต่อการบังคับใช้กฎหมาย พร้อมทั้งมาตรการและบทลงโทษต่อการกระทำอันเกี่ยวข้องกับก่อการร้ายด้านไซเบอร์

ยุทธวิธีหรือแผนปฏิบัติการ มีดังต่อไปนี้

๑. การใช้หน่วยงานทางกฎหมายร่วมกันกำหนดกฎหมาย กฎระเบียบ ขั้นตอนและแนวปฏิบัติที่เกี่ยวข้องกับการใช้งานด้านไซเบอร์ ความมั่นคงปลอดภัยด้านไซเบอร์ และรูปแบบการต่อต้านการก่อการร้ายด้านไซเบอร์

๒. การใช้หน่วยงานทางกฎหมายร่วมกันกำหนดแนวทางที่ชัดเจนและเหมาะสมต่อการบังคับใช้กฎหมาย พร้อมทั้งมาตรการและบทลงโทษต่อการกระทำอันเกี่ยวข้องกับก่อการร้ายด้านไซเบอร์

ดัชนีชี้วัดผลงาน : กฎหมาย กฎระเบียบ ขั้นตอน และแนวปฏิบัติที่เกี่ยวข้องกับการใช้ด้านไซเบอร์ที่มีประสิทธิภาพและประสิทธิผลทั้งในระดับองค์กรและระดับบุคคล

ผลที่คาดว่าจะได้รับตามยุทธศาสตร์ที่ ๕ : ประเทศไทยมีกฎหมาย กฎระเบียบ ขั้นตอน และแนวปฏิบัติที่เกี่ยวข้องกับการใช้ด้านไซเบอร์ในการต่อต้านการก่อการร้ายและการสร้างความไม่สงบสุขในพื้นที่จังหวัดชายแดนภาคใต้

ยุทธศาสตร์ที่ ๖ : ยุทธศาสตร์การใช้การบูรณาการร่วมกันเพื่อแบ่งปันข้อมูลข่าวสาร (Integration)

เป้าหมายยุทธศาสตร์ : เพื่อการใช้การบูรณาการร่วมกันเพื่อแบ่งปันข้อมูลข่าวสารในพื้นที่จังหวัดชายแดนภาคใต้อย่างถูกวิธีและไม่ส่งผลกระทบต่อความมั่นคงแห่งชาติ

แนวทางหรือมาตรการ มีดังต่อไปนี้

๑. การใช้หน่วยบัญชาการไซเบอร์แห่งชาติที่มีหน้าที่ในการกำกับดูแลและดำเนินการด้านไซเบอร์ มีการแบ่งปันข้อมูลร่วมกันเพื่อประโยชน์ของประชาชน รวมทั้งมีการบูรณาการการทำงานร่วมกัน อีกทั้งระบุโอกาส และความท้าทายในการเพิ่มขีดความสามารถของกลไกการตอบสนองต่อการก่อการร้ายรูปแบบต่างๆ

๒. การสร้างฐานข้อมูลกลางเพื่อรวบรวมข้อมูลสำคัญจากทุกภาคส่วน รวมทั้งมีการควบคุมดูแลเพื่อไม่ให้ข้อมูลถูกเผยแพร่ ตลอดจนเปิดโอกาสให้ทุกหน่วยงานที่เกี่ยวข้องกับไซเบอร์สามารถดึงข้อมูลไปใช้ในทางที่ถูกต้องและเป็นประโยชน์ต่อชาติบ้านเมือง

๓. จัดตั้งสำนักข่าวกรองด้านไซเบอร์ เพื่อทำงานด้านการข่าวด้านไซเบอร์ แบ่งปันข้อมูลข่าวสาร และประสานงานความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้อง

ยุทธวิธีหรือแผนปฏิบัติการ มีดังต่อไปนี้

๑. การกำหนดภารกิจและบทบาทของหน่วยบัญชาการไซเบอร์แห่งชาติในด้านการกำกับดูแลและดำเนินการด้านไซเบอร์เพื่อต่อต้านการก่อการร้ายด้านไซเบอร์

๒. การสร้างฐานข้อมูลกลางโดยระดมผู้เชี่ยวชาญด้านการออกแบบและพัฒนาระบบไอซีทีที่มีศักยภาพในการสร้างฐานข้อมูลที่มีความมั่นคงปลอดภัยในระดับสูงสุด

๓. การกำหนดภารกิจและบทบาทของสำนักข่าวกรองด้านไซเบอร์เพื่องานด้านการข่าวที่เกิดจากการประสานความร่วมมือกันของทุกภาคส่วน

ดัชนีชี้วัดผลงาน : หน่วยบัญชาการไซเบอร์แห่งชาติและสำนักข่าวกรองด้านไซเบอร์มีรูปแบบภารกิจที่สนับสนุนงานด้านไซเบอร์ที่ได้มาตรฐาน

ผลที่คาดว่าจะได้รับตามยุทธศาสตร์ที่ ๖ : ประเทศไทยมีการใช้การบูรณาการร่วมกันเพื่อแบ่งปันข้อมูลข่าวสารที่เป็นประโยชน์เพื่อรักษาผลประโยชน์ของชาติและต่อต้านการก่อการร้ายด้านไซเบอร์

ยุทธศาสตร์ที่ ๗ : ยุทธศาสตร์การรับรู้ด้านไซเบอร์เพื่อการป้องกัน การยับยั้ง และการโจมตี (Perception)

เป้าหมายยุทธศาสตร์ : เพื่อให้เกิดการรับรู้ด้านไซเบอร์ทั้งการป้องกัน การยับยั้ง และการโจมตีด้านไซเบอร์

แนวทางหรือมาตรการ มีดังต่อไปนี้

๑. การปลูกฝังทัศนคติและแนวทางการใช้งานไซเบอร์ที่เป็นรูปธรรมเพื่อให้ประชาชนมีการรับรู้ต่อการใช้งานไซเบอร์ในทางที่ถูกต้องและไม่เป็นภัยต่อความมั่นคงของชาติ

๒. การสร้างรูปแบบการมีส่วนร่วมของทุกภาคส่วน รวมทั้งวิธีการในการตระเตรียมตนเองเพื่อให้เกิดการปฏิบัติอย่างรู้เท่าทัน

ยุทธวิธีหรือแผนปฏิบัติการ มีดังต่อไปนี้

๑. การกำหนดรูปแบบการปลูกฝังทัศนคติและแนวทางการใช้งานไซเบอร์ที่เป็นรูปธรรมเพื่อให้ประชาชนมีการรับรู้ต่อการใช้งานไซเบอร์ในทางที่ถูกต้องและไม่ส่งผลกระทบต่อความมั่นคงแห่งชาติ

๒. การสร้างรูปแบบการมีส่วนร่วมของทุกภาคส่วน รวมทั้งวิธีการในการตระเตรียมตนเองและใช้มาตรการต่างๆ เพื่อให้เกิดการปฏิบัติอย่างรู้เท่าทัน

ดัชนีชี้วัดผลงาน : ทัศนคติในการใช้งานไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้มีประโยชน์ต่อการพัฒนาประเทศทุกมิติ

ผลที่คาดว่าจะได้รับตามยุทธศาสตร์ที่ ๗ : ทุกภาคส่วนมีการรับรู้ด้านไซเบอร์เพื่อการป้องกัน การยับยั้ง และการโจมตี

ผลที่คาดว่าจะได้รับ (Outcomes) :

๑. ภาครัฐมียุทธศาสตร์ที่มีประสิทธิภาพในการจัดการกับภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

๒. ขีดความสามารถในการจัดการกับภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ของประเทศไทยเพิ่มขึ้น

๓. ทำให้เกิดความมั่นคงปลอดภัยด้านไซเบอร์และก่อให้เกิดความสงบสุขในพื้นที่จังหวัดชายแดนภาคใต้ของประเทศไทย

กล่าวโดยสรุปได้ว่า ภัยคุกคามด้านไซเบอร์จะยังคงเป็นภัยคุกคามต่อความมั่นคงตั้งแต่ระดับความมั่นคงแห่งชาติลงไปจนถึงระดับความมั่นคงของมนุษย์ แน่นอนที่สุดว่าโลกไซเบอร์ในอนาคตจะมีแนวโน้มขยายตัวเพิ่มขึ้นเป็นทวีคูณ เพราะโลกไซเบอร์ได้กลายเป็นสิ่งอำนวยความสะดวกต่อวิถีชีวิตมนุษย์และการทำงานประจำวันในองค์การต่างๆ ทุกประเภท อย่างไรก็ตาม โลกไซเบอร์นี้ย่อมมีทั้งด้านที่เป็นคุณและด้านที่เป็นโทษ โดยขึ้นกับมนุษย์ว่าจะใช้มันเพื่อวัตถุประสงค์ใดและได้ประโยชน์ด้านใด ด้วยเหตุนี้ การที่มนุษย์ได้ประโยชน์อย่างมหาศาลจากโลกไซเบอร์ ก็นำมาซึ่งความท้าทายต่อการป้องกันความเสียหายที่เกิดจากการใช้งานดังกล่าวด้วยเช่นกัน ดังนั้น การพัฒนาศักยภาพของมนุษย์ให้รู้เท่าทันกับอันตราย คาดการณ์ถึงแนวโน้มในอนาคต และลงมือจัดการกับภัยคุกคามในโลกไซเบอร์ จะต้องอาศัยการแลกเปลี่ยนข้อมูลระหว่างกัน เทคโนโลยีคลาวด์ (Cloud Computing Technology) และการสร้างสมรรถนะและความคล่องตัวทั้งในแง่ของระบบและบุคลากร ในรูปแบบที่ทัดเทียมกับเหล่าอาชญากรด้านไซเบอร์ โดยต้องรู้เท่าทันต่อการรบกวนและโจมตีในรูปแบบต่างๆ พร้อมจะรับมือได้ทั้งในระดับนโยบาย องค์กร และปัจเจกบุคคล ด้วยเหตุนี้ เราจะเอาชนะสงครามไซเบอร์ทั้งในปัจจุบันและในอนาคตได้ก็ต่อเมื่อรัฐบาล หน่วยงานด้านความมั่นคงของรัฐ กระทรวงกลาโหม กองทัพไทย และเหล่าทัพ รวมถึงองค์การอื่นๆ ที่เกี่ยวข้อง ต่างมองเห็นสถานการณ์นี้ได้อย่างชัดเจน มีการบูรณาการข้อมูลอย่างเป็นระบบ เรียนรู้ข้อมูลระหว่างกัน ตรวจจับเหตุผิดปกติ ตอบสนองได้อย่างรวดเร็ว ใช้เครื่องมือและทรัพยากรที่มีอยู่ได้อย่างคุ้มค่าและมีประสิทธิภาพสูงสุด ในส่วนของกองทัพไทยทั้งสามเหล่าทัพก็ควรเตรียมความพร้อมทั้งทางด้านบุคลากร การจัดหน่วย ผู้เชี่ยวชาญ นักวิเคราะห์ระบบ และเครื่องมือที่ทันสมัย เพื่อการรับมือกับภัยคุกคามด้านไซเบอร์ที่มีความรุนแรง ความเสียหายอย่างใหญ่หลวง และส่งผลกระทบต่อความมั่นคงของประเทศ อีกทั้งควรพัฒนาเสริมสร้างกำลังด้านไซเบอร์อย่างเป็นระบบ มีระเบียบแบบแผน ทั้งมาตรการเชิงรับและเชิงรุก ให้มีประสิทธิภาพ คุณภาพ และความเข้มแข็งอย่างต่อเนื่องและยั่งยืน เพื่อเป็นหลักประกันด้านความมั่งคงปลอดภัยด้านไซเบอร์ของประเทศต่อไป

ข้อเสนอแนะ

ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้และในประเทศไทย ถือว่าเป็นเรื่องสำคัญที่ต้องดำเนินการโดยเร็วที่สุด ทั้งนี้ก็เพื่อการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ทุกหน่วยงานราชการ ภาคเอกชน และภาคประชาชนให้มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้ตามปกติ ตลอดจนการระงับยับยั้งการก่อการร้ายด้านไซเบอร์ไม่ให้เกิดขึ้นในประเทศไทย ผู้วิจัยมีข้อเสนอแนะดังนี้

๑. ข้อเสนอแนะเชิงนโยบาย

๑.๑ ก่อนที่จะนำนโยบายหรือกฎหมายฉบับใดที่เกี่ยวข้องกับโลกไซเบอร์มาประกาศใช้ รัฐบาลต้องประชาสัมพันธ์ให้ประชาชนมีความเข้าใจอย่างแท้จริง เกี่ยวกับวัตถุประสงค์ ประโยชน์ที่ประชาชนจะพึงได้รับ และผลกระทบที่จะตามมา เพื่อป้องกันการเกิดข่าวลือที่ไม่พึงประสงค์ และกระแสต่อต้านของประชาชนในสื่อสังคมออนไลน์

๑.๒ องค์กรและหน่วยงานทั่วไปที่มีการใช้งานในโลกไซเบอร์ ควรมีมาตรการการรักษาปลอดภัยด้านไซเบอร์ (Cyber Security Measures) สำหรับหน่วยงานของตน

๑.๓ ในระดับประเทศ ควรมีหน่วยงานไซเบอร์เป็นการเฉพาะที่ให้การรักษาความมั่นคงปลอดภัยด้านไซเบอร์และการบริการประชาชนในการเฝ้าระวัง แจ้งเตือนภัย และการแก้ไขปัญหา เพื่อสร้างความเชื่อมั่นและความมั่นใจในการใช้งานในโลกไซเบอร์

๑.๔ ควรมีกลไกในการตัดสินใจภายใต้ประเมินความเสี่ยงเพื่อให้สามารถตอบสนองต่อการโจมตีด้านไซเบอร์ของฝ่ายตรงข้ามได้อย่างเหมาะสม และ พิจารณาถึงผลกระทบที่จะตามมา รวมถึงอาศัยภาวะผู้นำของผู้บริหารในการตัดสินใจที่ไม่ใช่มุ่งเน้นในเรื่อง “การป้องกัน” มากเกินไป จนละเลยหรือเพิกเฉยต่อ “การตอบโต้” กับการโจมตีดังกล่าว

๑.๕ ควรกำหนดทิศทางแก้ไขปัญหาและมาตรการตอบโต้การโจมตีด้านไซเบอร์ที่เหมาะสม โดยแต่ละหน่วยงานภาครัฐจะต้องตรวจสอบดูว่า นโยบายที่กำหนดขึ้นเพื่อการป้องกันและตอบโต้ต่อการโจมตีด้านไซเบอร์ของตนสามารถปฏิบัติได้จริง มีช่องโหว่ หรือปัญหาอะไรหรือไม่ โดยนโยบายดังกล่าวจะต้องเป็นนโยบายที่สามารถดำเนินการได้ในสภาพความเป็นจริงด้วย

๑.๖ ควรมีกฎหมายด้านไซเบอร์เป็นการเฉพาะ เพื่อกำหนดกฎกติกาทางสังคมของโลกไซเบอร์และมาตรการป้องปรามป้องกันการละเมิดกฎหมาย โดยกฎหมายจะเป็นเครื่องมือที่สำคัญอย่างมากสำหรับการสร้างโลกไซเบอร์ที่ปลอดภัย รวมถึงการมีหน่วยงานที่สามารถบังคับใช้กฎหมายด้านไซเบอร์อย่างจริงจัง

๒. ข้อเสนอแนะระดับปฏิบัติการ

๒.๑ ภาครัฐควรกำหนดแนวทางในการแปลงยุทธศาสตร์ชาติด้านไซเบอร์ให้เป็นยุทธศาสตร์รองลงมา และถ่ายทอดลงมาเป็นแผนงานและโครงการ นโยบายหรือมาตรการหรือการปฏิบัติในลักษณะอื่นอย่างเป็นระบบ

๒.๒ ภาครัฐควรกำหนดให้ศูนย์ตรวจสอบประเมินผลยุทธศาสตร์ซึ่งเป็นหน่วยงานกลางที่เป็นอิสระ โดยตรวจสอบว่าสอดคล้องกับเป้าประสงค์และเจตนารมณ์ที่แท้จริงของยุทธศาสตร์หลักหรือไม่

๒.๓ ควรเสริมสร้างความรู้ความเข้าใจโลกไซเบอร์แก่เจ้าหน้าที่รัฐและประชาชนทั่วไป โดยมุ่งเน้นเรื่องมาตรการป้องกันมากกว่าการบังคับใช้กฎหมายหรือระเบียบที่เข้มงวด ดังนั้นการดำเนินนโยบายหรือหาช่องทางในการปิดกั้นการรับรู้ของประชาชนจากโลกไซเบอร์ในสภาพแวดล้อมของโลกในปัจจุบันจึงเป็นสิ่งที่ทำไม่ได้อีกแล้ว หรือหากกระทำได้ก็จะเป็นการฝืนมติมหาชนอย่างรุนแรง ด้วยเหตุนี้ แนวทางที่ดีที่สุดต่อการดำเนินการด้านไซเบอร์ของรัฐบาลและหน่วยงานที่เกี่ยวข้อง ก็คือ “การสร้างความเข้าใจให้กับประชาชน” เพื่อให้ประชาชนไว้เนื้อเชื่อใจต่อการดำเนินงานของรัฐบาล ไม่ใช่การออกกฎหมายเพื่อใช้บังคับกับประชาชนเพียงอย่างเดียว

๓. ข้อเสนอแนะในการวิจัยครั้งต่อไป

๓.๑ ควรมีการศึกษาวิจัยการออกแบบและพัฒนาระบบรักษาความปลอดภัยด้านไซเบอร์ที่เหมาะสมกับหน่วยงานทางความมั่นคงหรือกองทัพอื่น เพื่อให้เกิดความหลากหลายและเกิดประโยชน์ในการพัฒนางานวิจัยมากยิ่งขึ้น

๓.๒ ควรมีการศึกษาวิจัยการพัฒนาขีดความสามารถทางด้านการรักษาความปลอดภัยด้านไซเบอร์เพื่อให้ทัดเทียมกับมาตรฐานการรักษาความปลอดภัยด้านไซเบอร์สากล และเกิดประโยชน์ในการนำไปใช้แก้ปัญหาด้านความมั่นคงของชาติต่อไป

๓.๓ ควรมีการศึกษาวิจัยเชิงลึกยุทธศาสตร์การสร้างระบบรักษาความปลอดภัยด้านไซเบอร์ที่เชื่อมโยงกับมาตรฐานสากล

๓.๔ ควรมีการศึกษาวิจัยเชิงลึกถึงแผนงานและมาตรการในการพัฒนาระบบรักษาความปลอดภัยด้านไซเบอร์ที่เกี่ยวข้องกับนวัตกรรมและเทคโนโลยีสมัยใหม่ เพื่อให้ได้รูปแบบระบบรักษาความปลอดภัยด้านไซเบอร์ของกองทัพไทยและหน่วยงานทางความมั่นคงที่ทันสมัย

๓.๕ ควรมีการศึกษาวิจัยและพัฒนามาตรฐานด้านการรักษาความปลอดภัยด้านไซเบอร์ที่สามารถเชื่อมโยงนโยบายแห่งรัฐกับหน่วยงานทางความมั่นคง องค์กรต่อต้านการก่อการร้าย ภาคเอกชน ภาคประชาสังคม และภาคประชาชน เพื่อให้ได้รูปแบบของระบบรักษาความปลอดภัยด้านไซเบอร์ที่มีประสิทธิภาพภายใต้มาตรฐานเดียวกัน

บรรณานุกรม

ภาษาไทย

กลาโหม, กระทรวง. “นโยบายเร่งด่วนของรัฐมนตรีว่าการกระทรวงกลาโหม ประจำปีงบประมาณ พ.ศ. ๒๕๖๐” ๑ ต.ค.๕๙ – ๓๐ ก.ย.๖๐, ๒๕๖๐.

กองทัพไทย. “นโยบาย ผบ.ทสส./ผบ.ศบท. ปร(๒๕๖๑). ประจำปีงบประมาณ ๒๕๖๐”, ไทยพับลิก้า. ๒๕๕๖. เอ็ดเวิร์ด สโนว์เดน กับการเปิดโปง “พริซึมเกต”. (ออนไลน์). เข้าถึงได้จาก : http:// thaipublica.org/2013/06/edward-snowden-prism/, ๒๕๖๑.

การต่างประเทศ, กระทรวง. “ผลการประชุมสุดยอดอาเซียนครั้งที่ ๒๗ และการประชุมสุดยอดอื่นๆ ที่เกี่ยวข้อง”. ๒๕๕๘.

ฤทธี อินทราวุธ, พลตรี. “การรักษาความมั่นคงปลอดภัยด้านไซเบอร์ : ความท้าทายของกองทัพบก (Cyber Security : A Challenge of Army)”, รองผู้อำนวยการศูนย์เทคโนโลยีทางทหาร.
(ออนไลน์). เข้าถึงได้จาก : http://rittee1834.blogspot.com/2014/08/cyber-security-challenge-of-army.html, ๒๕๕๗.

ทิพาวดี เมฆสวรรค์, “การปฏิรูปภาคราชการสู่สภาพที่พึงปรารถนา : ทำอย่างไร ใครรับผิดชอบ”. วารสารข้าราชการ, ปีที่ ๔๒ (ฉบับที่ ๒), ๒๕๔๐. หน้า ๒๔-๔๓.

นงรัตน์ สายเพชร. “ความมั่นคงไซเบอร์ของสหรัฐอเมริกา American Cyber Security”. จุลสารความมั่นคงศึกษา. (ฉบับที่ ๑๒๙-๑๓๐). กันยายน พ.ศ.๒๕๕๖.

บวร เทศารินทร์. “ประเทศไทย ๔.๐ โมเดลเศรษฐกิจใหม่”, (ออนไลน์). เข้าถึงได้จาก : http://www.drborworn.com/articledetail.asp?id=16223, ๒๕๕๙.

บีบีซีไทย. “ฝรั่งเศสสกัดแผนโจมตีทางไซเบอร์ได้ ๒๔,๐๐๐ ครั้ง”. (ออนไลน์). เข้าถึงได้จาก : http://www.bbc.com/thai/international-38547157, ๒๕๖๐.

ปริญญา หอมเอนก. “Cyber Security”, (ออนไลน์). เข้าถึงได้จาก : https://www.acisonline.net/?page_id=797, ๒๕๖๑.

พงษ์ศักดิ์ ผกามาศ. ระบบไอซีทีและการจัดการยุคใหม่. กรุงเทพ: สำนักพิมพ์ Witty, ๒๕๕๓.

เรืองวิทย์ เกษสุวรรณ. ความรู้เบื้องต้นเกี่ยวกับรัฐประศาสนศาสตร์. กรุงเทพมหานคร : บพิธการพิมพ์. หน้า ๒๓๘-๒๓๙, ๒๕๕๓.

ศูนย์พัฒนาหลักนิยมและยุทธศาสตร์. “ กองทัพบกกับภัยคุกคามด้านไซเบอร์”. จุลสารยุทธศาสตร์ด้านความมั่นคง กรมยุทธศึกษาทหารบก, ๒๕๕๙.

ศูนย์พัฒนาหลักนิยมและยุทธศาสตร์. “๑๐ ปี บทเรียนจากการป้องกันและปราบปรามการก่อความไม่สงบในพื้นที่จังหวัดชายแดนภาคใต้”. จุลสารยุทธศาสตร์ด้านความมั่นคง กรมยุทธศึกษาทหารบก, ๒๕๕๙.

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT). “สถิติภัยคุกคาม”. (ออนไลน์). เข้าถึงได้จาก : https://www.thaicert.or.th/statistics/statistics.html, ๒๕๖๑.

เศรษฐพงค์ มะลิสุวรรณ. “เปิดแนวคิด “เศรษฐพงค์” ยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์”, (ออนไลน์). เข้าถึงได้จาก : http://www.manager.co.th/game/viewnews.aspx?NewsID=9590000070219,๒๕๕๙.

สราวุธ ปิติยาศักดิ์. “ความมั่นคงด้านไซเบอร์” (ออนไลน์). เข้าถึงได้จาก : https://thainetizen.org/2015/10/digital-economy-laws-update-sarawut-kittisak/,๒๕๖๑.

ส่วนนโนบายรัฐบาลอิเล็กทรอนิกส์. “ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)”. สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน). จัดทำเมื่อวันที่ ๑๐ กันยายน ๒๕๕๙.

ภาษาต่างประเทศ

Frank J. Cilluffo. Cyber Threats from China, Russia and Iran: Protecting American Critical Infrastructure. Cyber Center for National and Economic Security, The George Washington University, 2013.

Li Zhang. A Chinese perspective on cyber war. International Review of the Red Cross, 94 (886), 2012.

National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cyber security., Version 1.0, February 12, 2014.

P.W. Singer and Allan Friedman. Cyber security and Cyber war: What Everyone Needs to Know® 1st Edition, Oxford University Press, New York, 2014.

Richard A. Clarke. US Cyber Security. https://en.wikipedia.org/wiki/Richard_A._Clarke, Retrieved 5 May 2018.

The Department of Defense. United States of America, Cyber Strategy. January 2016.

The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world. November 2015.

ภาคผนวก

ผนวก ก
รายชื่อผู้เชี่ยวชาญ

ผู้ทรงคุณวุฒิด้านความมั่นคงแห่งชาติ

๑. พลเอก ฤทธิ อินทราวุธ อดีตผู้อำนวยการศูนย์เทคโนโลยีทางทหาร ที่ปรึกษาปลัดกระทรวงกลาโหม

๒. พลเอก พิศาล วัฒนวงศ์คีรี อดีตแม่ทัพภาคที่ ๔

๓. พลตรี ชาติชาย ชัยเกษม ผู้อำนวยการศูนย์ไซเบอร์กองบัญชาการกองทัพไทย

๔. พลตรี ธานินทร์ สนิทชน เสนาธิการกองทัพน้อยที่ ๒

๕. พลตรี วาสิฏฐ์ มณีโชติ ผู้ทรงคุณวุฒิกองทัพบก

ผู้เชี่ยวชาญด้านวิศวกรรมระบบไอซีทีและโลกไซเบอร์

๑. รศ.ดร.ครรชิต มาลัยวงศ์ อดีตผู้อำนวยการศูนย์สารสนเทศทางเทคโนโลยี สวทช./ราชบัณฑิตสาขาวิทยาการคอมพิวเตอร์ บุรี

๒. รศ.ดร.วิสุทธิ์ สุนทรกนกพงศ์ คณะครุศาสตร์อุตสาหกรรม มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธน

๓. ผศ.ดร.พงษ์ศักดิ์ ผกามาศ สำนักงานวิจัยและพัฒนาการทางทหารกองทัพบก

๔. ผศ.ดร.เศรษฐชัย ชัยสนิท คณบดี วิทยาเขตชลบุรี คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี

๕. ดร. ธ ธง พวงสุวรรณ ที่ปรึกษาด้านนวัตกรรมและเทคโนโลยี มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี

ผู้เชี่ยวชาญด้านภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

๑. พันเอก ภูวนัย ไตรภูวนาถ ผอ.กสข.สขว.กอ.รมน.ภาค ๔ สน.

๒. พันเอก พงษ์สันติ์ จันทร์สอน รอง ผอ.กสข.สขว.กอ.รมน.ภาค ๔ สน.

๓. พันเอก คมกฤช รัตนฉายา ผบ.กกล.ทพ.จชต.

๔. พันเอก สาโรช บุญญาพิชิตเดโช กอ.รมน.ภาค ๔ สน.

๕. พันเอก คุณากร พันธุ์ดี กอ.รมน.ภาค ๔ สน.

๖. พันเอก ชาติชาย ชัยเกษม กอ.รมน.ภาค ๔ สน.

๗. พันเอก สุภกิจ รู้หลัก รองผู้อำนวยการสำนักข่าวกรอง กอ.รมน.ภาค ๔ สน.

๘. พันเอก ชวลิต ชูคำ อดีตผู้บัญชาการสำนักข่าวกรอง จังหวัดชายแดนภาคใต้ ที่ปรึกษา ผอ.กอ.รมน.ภาค ๔ สน.

๙. พันโท ศรายุทธ พัฒนชัย กอ.รมน.ภาค ๔ สน.

๑๐. พันโท คณิต คหบดีกนกกุล กอ.รมน.ภาค ๔ สน.

๑๑. พันโท จตุรงค์ ป้องเพชร กอ.รมน.ภาค ๔ สน.

๑๒. พันโท สราวุธ ทึมหาญ สำนักปฏิบัติการข่าวสาร กอ.รมน.ภาค ๔ สน.

๑๓. ร้อยเอก สุวิทย์ ชูแก้ว สำนักปฏิบัติการข่าวสาร กอ.รมน.ภาค ๔ สน.

๑๔. ร้อยเอก ยงยุทธ์ สำเร หน.ชุดงานข่าวการเมืองและภาคประชาสังคม รศ.ขกท.สน.จชต.

ผู้เชี่ยวชาญตรวจสอบเครื่องมือที่ใช้ในการวิจัย

๑. ผศ.ดร.ชัยวัฒน์ ประสงค์สร้าง คณะศิลปศาสตร์ มหาวิทยาลัยเทคโลยีราชมงคลรัตนโกสินทร์

๒. ผศ.ดร.รัชฎาวรรณ นิ่มนวล ผู้ช่วยคณบดีฝ่ายวิชาการและประกันคุณภาพ คณะสถาปัตยกรรมศาสตร์และการออกแบบ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี

๓. ผศ.ดร.สรายุทธ์ เศรษฐขจร รองอธิการบดี มหาวิทยาลัยปทุมธานี

๔. พันเอกหญิง ดร.นพมาศสิริ วงศ์บา สำนักงานวิจัยและพัฒนาการทางทหารกองทัพบก

๕. ดร.สุรีวัลย์ ลิ้มพิพัฒนกุล นักวิชาการศึกษาชำนาญการพิเศษ สำนักงานการศึกษานอกโรงเรียน กระทรวงศึกษาธิการ

การสัมมนาอิงผู้เชี่ยวชาญ (Connoisseurship)

๑. พลตรี มานพ สัมมาขันธ์ ผู้อำนวยการศูนย์ไซเบอร์กองทัพบก

๒. พลตรี ธานินทร์ สนิทชน เสนาธิการกองทัพน้อยที่ ๒

๓. พลตรี ชัยรัตน์ จ่างแก้ว รองเจ้ากรมข่าวทหารบก

๔. พันเอก เดชา พลสุวรรณ รองผู้บัญชาการโรงเรียนทหารสื่อสาร กรมการทหารสื่อสาร

๕. พันเอก ชูเกียรติ ช่วยเพชร รองผู้อำนวยการสำนักงานวิจัยและพัฒนาการทางทหารกองทัพบก

๖. ผศ.ดร.พงษ์ศักดิ์ ผกามาศ สำนักงานวิจัยและพัฒนาการทางทหารกองทัพบก

๗. ผศ.ดร.เศรษฐชัย ชัยสนิท คณบดี วิทยาเขตชลบุรี คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี

๘. ผศ.ดร.ชัยวัฒน์ ประสงค์สร้าง คณะศิลปศาสตร์ มหาวิทยาลัยเทคโลยีราชมงคลรัตนโกสินทร์

๙. ดร.มูนีเร๊าะ ผดุง ประธานหลักสูตรคอมพิวเตอร์ศึกษา มหาวิทยาลัยราชภัฏยะลา

ผนวก ข
เครื่องมือที่ใช้ในการวิจัย

วิทยาลัยป้องกันราชอาณาจักร

แบบสัมภาษณ์ (Interview Guide)

เรื่อง ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

Title Cyber Threat Management Strategy in Southern Border Provinces.

กลุ่มเป้าหมาย ๑. หน่วยงานด้านความมั่นคงของรัฐ (กองทัพภาคที่ ๔, กอ.รมน.ภาค ๔ ส่วนหน้า, ศอบต., ศชต., และ ฉก.)

๒. ผู้บริหาร/ผู้นำท้องถิ่น ๔ จังหวัด

๓. หน่วยงานภาคเอกชน

๔. หน่วยงานพลเรือน

๕. ภาคประชาชน

<u>คำชี้แจง</u>

วัตถุประสงค์ของแบบสัมภาษณ์นี้เพื่อนำไปใช้สร้าง “ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้” โดยแบบสัมภาษณ์นี้จะมีประเด็นหลัก ๗ ประเด็น ได้แก่

๑. รูปแบบของภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

๒. วิธีการของภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

๓. การประเมินสถานการณ์ภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

๔. ปัญหาผลกระทบของภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

๕. ผลกระทบของภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงแห่งชาติรวมถึงแนวโน้มในอนาคต

๖. ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

๗. ข้อเสนอแนะ

ข้อมูลส่วนบุคคล เช่น ชื่อ-สกุล อายุ การศึกษา อาชีพ และระยะเวลาที่อาศัยอยู่

ข้อ ๑. รูปแบบของภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

๑.๑ บทบาทและความสำคัญ

๑.๒ รูปแบบการใช้งานระบบอินเตอร์เน็ตและเครือข่าย

๑.๓ รูปแบบ (การโจมตี/การจารกรรม)

๑.๔ ระดับ (การโจมตี/การจารกรรม)

๑.๕ เหตุการณ์สำคัญ

ข้อ ๒. วิธีการของภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

๒.๑ บทบาทและความสำคัญ

๒.๒ วิธีการใช้งานระบบอินเตอร์เน็ตและเครือข่าย

๒.๓ วิธีการ (การโจมตี/การจารกรรม)

๒.๔ ระดับ (การโจมตี/การจารกรรม)

๒.๕ เหตุการณ์สำคัญ

ข้อ ๓. การประเมินสถานการณ์ภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

๓.๑ สถานการณ์ที่เกิดขึ้น

๓.๒ รูปแบบการประเมินสถานการณ์

๓.๓ การจัดการ/การรับมือ

๓.๔ แนวทางการป้องกันและแก้ไข

๓.๕ กระบวนการรับมือในอนาคต

ข้อ ๔. ปัญหาผลกระทบของภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

๔.๑ รูปแบบและวิธีการของปัญหา

๔.๒ ผลกระทบทางตรง

๔.๓ ผลกระทบทางอ้อม

๔.๔ ระดับความรุนแรง

๔.๕ กระบวนการแก้ไขปัญหา

ข้อ ๕. ผลกระทบของภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงแห่งชาติรวมถึงแนวโน้มในอนาคต

๕.๑ รูปแบบและวิธีการที่ส่งผลต่อความมั่นคงแห่งชาติ

๕.๒ ผลกระทบทางตรงที่ส่งผลต่อความมั่นคงแห่งชาติ

๕.๓ ผลกระทบทางอ้อมที่ส่งผลต่อความมั่นคงแห่งชาติ

๕.๔ การจัดการ/การรับมือ

๕.๕ แนวโน้มผลกระทบของภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงแห่งชาติในอนาคต

ข้อ ๖. ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

๖.๑ รูปแบบและวิธีการบริหารจัดการ

(การวางแผนงาน/การจัดการองค์กร/การนำไปสู่การปฏิบัติ/การประเมินผล)

๖.๒ นโยบาย/กรอบการดำเนินงาน (การป้องกัน/การป้องปราม/การผนึกกำลัง)

๖.๓ โครงสร้างพื้นฐานของการรักษาความมั่นคงปลอดภัยด้านไซเบอร์

๖.๔ มาตรการ/แนวทาง/แนวปฏิบัติ

๖.๕ แผนงาน/โครงการ/กิจกรรม/ทรัพยากร/งบประมาณ/กรอบเวลา

๖.๖ กระบวนการจัดการภัยคุกคามด้านไซเบอร์ในอนาคต

ข้อ ๗. ข้อเสนอแนะ

๗.๑ ข้อเสนอแนะทั่วไป

.....

.....

.....

๗.๒ ข้อเสนอแนะเชิงนโยบาย

.....

.....

.....

วิทยาลัยป้องกันราชอาณาจักร

แบบสัมภาษณ์ (Interview Guide)

เรื่อง ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

Title Cyber Threat Management Strategy in Southern Border Provinces.

กลุ่มเป้าหมาย ๑. เจ้าหน้าที่ด้านการข่าวที่เชี่ยวชาญระบบไอซีที
๒. เจ้าหน้าที่ทหารที่รับผิดชอบด้านภัยคุกคาม
๓. ผู้ปฏิบัติงานที่เกี่ยวข้องกับระบบเครือข่ายอินเตอร์เน็ต
๔. ผู้เชี่ยวชาญด้านวิศวกรรมระบบไอซีทีและโลกไซเบอร์

<u>คำชี้แจง</u>

วัตถุประสงค์ของแบบสัมภาษณ์นี้เพื่อนำไปใช้สร้าง “ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้” โดยแบบสัมภาษณ์นี้จะมีประเด็นหลัก ๗ ประเด็น ได้แก่

๑. รูปแบบของภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้
๒. วิธีการของภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้
๓. การประเมินสถานการณ์ภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้
๔. ปัญหาผลกระทบของภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้
๕. ผลกระทบของภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงแห่งชาติรวมถึงแนวโน้มในอนาคต
๖. ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้
๗. ข้อเสนอแนะ

ข้อมูลส่วนบุคคล เช่น ชื่อ-สกุล อายุ การศึกษา อาชีพ และระยะเวลาที่อาศัยอยู่

ข้อ ๑. รูปแบบของภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

๑.๑ บทบาทและความสำคัญ

๑.๒ รูปแบบการใช้งานระบบอินเตอร์เน็ตและเครือข่าย

๑.๓ รูปแบบ (การโจมตี/การจารกรรม)

๑.๔ ระดับ (การโจมตี/การจารกรรม)

๑.๕ เหตุการณ์สำคัญ

ข้อ ๒. วิธีการของภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

๒.๑ บทบาทและความสำคัญ

๒.๒ วิธีการใช้งานระบบอินเตอร์เน็ตและเครือข่าย

๒.๓ วิธีการ (การโจมตี/การจารกรรม)

๒.๔ ระดับ (การโจมตี/การจารกรรม)

๒.๕ เหตุการณ์สำคัญ

ข้อ ๓. การประเมินสถานการณ์ภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

๓.๑ รายงานการประเมินสถานการณ์

๓.๒ รูปแบบการประเมินสถานการณ์

๓.๓ การจัดการ/การรับมือ

๓.๔ แนวทางการป้องกันและแก้ไข

๓.๕ กระบวนการที่เหมาะสมในการประเมินสถานการณ์ในอนาคต

ข้อ ๔. ปัญหาผลกระทบของภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

๔.๑ รายงานปัญหาผลกระทบ

๔.๒ ผลกระทบทางตรง

๔.๓ ผลกระทบทางอ้อม

๔.๔ ระดับความรุนแรง

๔.๕ กระบวนการที่เหมาะสมในการแก้ไขปัญหาผลกระทบ

ข้อ ๕. ผลกระทบของภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงแห่งชาติรวมถึงแนวโน้มในอนาคต

๕.๑ รายงานผลกระทบที่ส่งผลต่อความมั่นคงแห่งชาติ

๕.๒ ผลกระทบทางตรงที่ส่งผลต่อความมั่นคงแห่งชาติ

๕.๓ ผลกระทบทางอ้อมที่ส่งผลต่อความมั่นคงแห่งชาติ

๕.๔ การจัดการ/การรับมือ

๕.๕ แนวโน้มของภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงแห่งชาติในอนาคต

ข้อ ๖. ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

๖.๑ รูปแบบและวิธีการบริหารจัดการที่เหมาะสม
(การวางแผนงาน/การจัดการองค์กร/การนำไปสู่การปฏิบัติ/การประเมินผล)

๖.๒ นโยบาย/กรอบการดำเนินงาน (การป้องกัน/การป้องปราม/การผนึกกำลัง)

๖.๓ โครงสร้างพื้นฐานของการรักษาความมั่นคงปลอดภัยด้านไซเบอร์

๖.๔ มาตรการ/แนวทาง/แนวปฏิบัติ

๖.๕ แผนงาน/โครงการ/กิจกรรม/ทรัพยากร/งบประมาณ/กรอบเวลา

๖.๖ ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ที่เหมาะสมในอนาคต

ข้อ ๗. ข้อเสนอแนะ

๗.๑ ข้อเสนอแนะทั่วไป

.....

.....

.....

๗.๒ ข้อเสนอแนะเชิงนโยบาย

.....

.....

.....

วิทยาลัยป้องกันราชอาณาจักร

แบบยืนยัน (Confirm Guide)

เรื่อง ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

Title Cyber Threat Management Strategy in Southern Border Provinces.

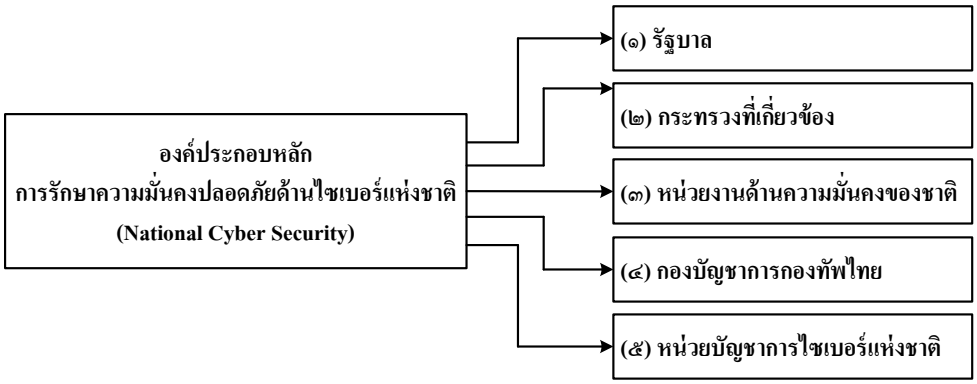
กลุ่มเป้าหมาย ๑. ผู้ทรงคุณวุฒิจากหน่วยงานความมั่นคงด้านไซเบอร์ของกองทัพไทย
๒. ผู้เชี่ยวชาญด้านระบบไอซีทีและโลกไซเบอร์

<u>คำชี้แจง</u>

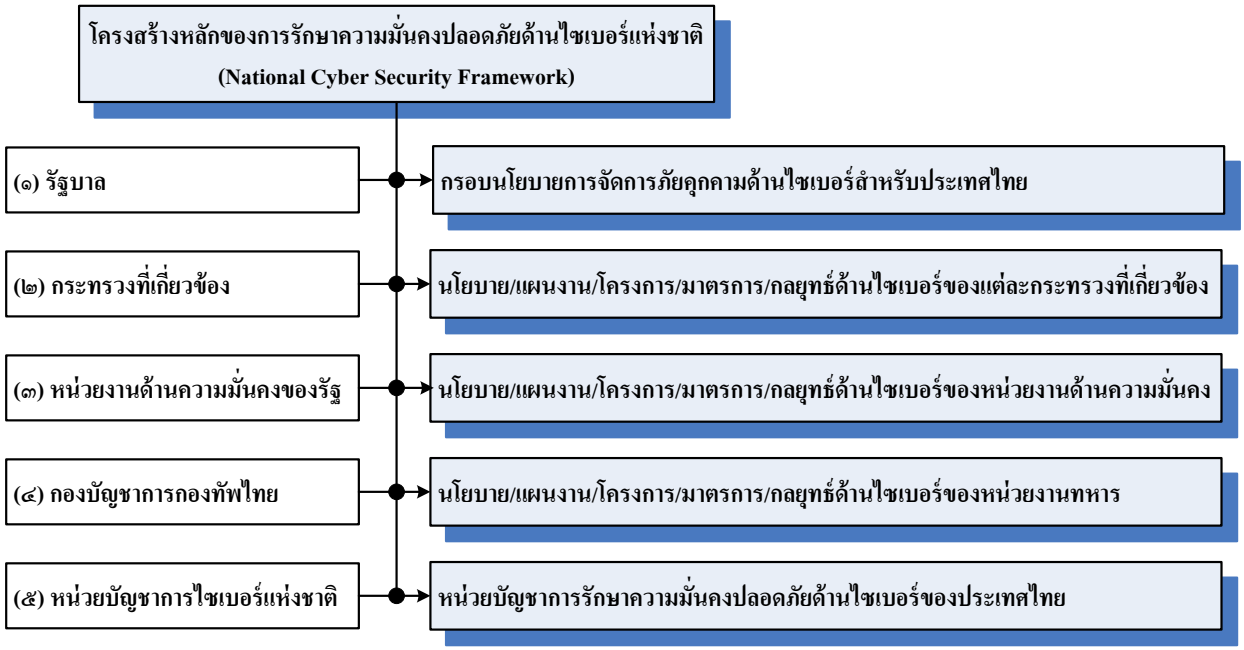
วัตถุประสงค์ของแบบยืนยันนี้เพื่อสนับสนุนร่าง “ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้” โดยจะมีการดำเนินการดังนี้

๑. ให้ผู้ทรงคุณวุฒิและผู้เชี่ยวชาญพิจารณาองค์ประกอบหลักของการรักษาความมั่นคงปลอดภัยด้านไซเบอร์แห่งชาติ ขอความคิดเห็นและข้อเสนอแนะ
๒. ให้ผู้ทรงคุณวุฒิและผู้เชี่ยวชาญพิจารณาโครงสร้างหลักของการรักษาความมั่นคงปลอดภัยด้านไซเบอร์แห่งชาติ ขอความคิดเห็นและข้อเสนอแนะ
๓. ให้ผู้ทรงคุณวุฒิและผู้เชี่ยวชาญพิจารณาหน่วยบัญชาการไซเบอร์แห่งชาติ ขอความคิดเห็นและข้อเสนอแนะ
๔. ให้ผู้ทรงคุณวุฒิและผู้เชี่ยวชาญพิจารณาโครงสร้างพื้นฐานการจัดการภัยคุกคามด้านไซเบอร์ ขอความคิดเห็นและข้อเสนอแนะ
๕. ให้ผู้ทรงคุณวุฒิและผู้เชี่ยวชาญพิจารณายุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ ขอความคิดเห็นและข้อเสนอแนะ

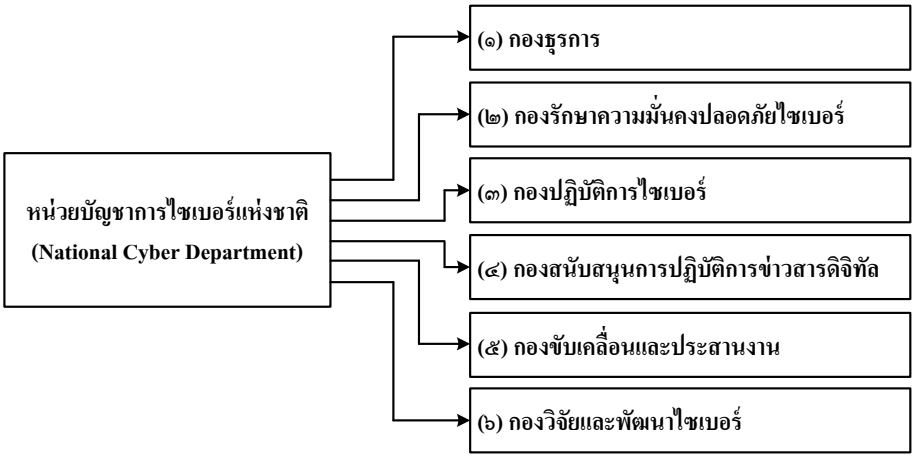
ข้อ ๑. องค์ประกอบหลักของการรักษาความมั่นคงปลอดภัยด้านไซเบอร์แห่งชาติ



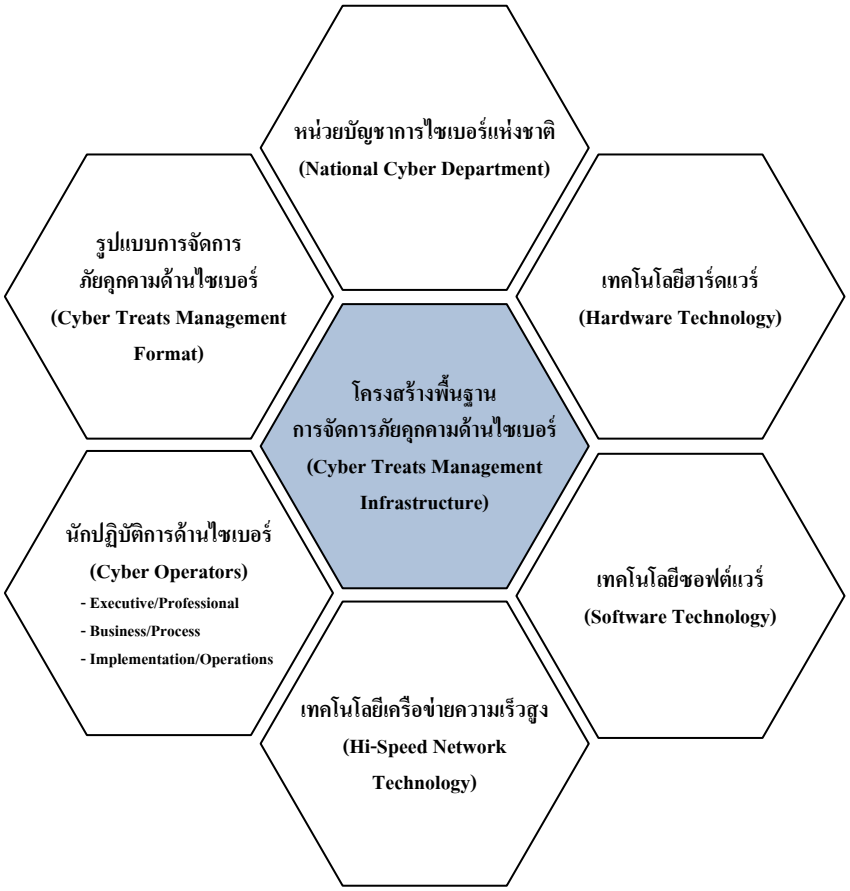
ข้อ ๒. โครงสร้างหลักของการรักษาความมั่นคงปลอดภัยด้านไซเบอร์แห่งชาติ



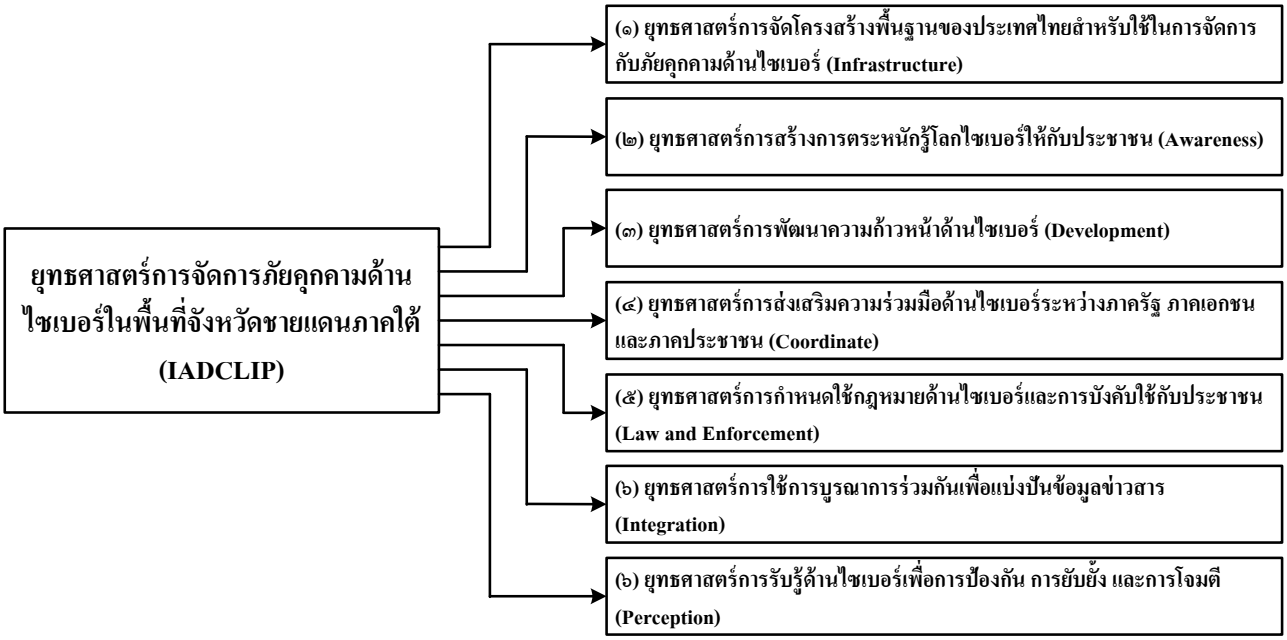
ข้อ ๓. หน่วยบัญชาการไซเบอร์แห่งชาติ



ข้อ ๔. โครงสร้างพื้นฐานการจัดการภัยคุกคามด้านไซเบอร์



ข้อ ๕. ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้



ข้อ ๖. ข้อเสนอแนะ

๖.๑ ข้อเสนอแนะทั่วไป

……

……

……

……

๖.๒ ข้อเสนอแนะเชิงนโยบาย

……

……

……

……

วิทยาลัยป้องกันราชอาณาจักร

การสัมมนาอิงผู้เชี่ยวชาญ (Connoisseurship)

เรื่อง ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

Title Cyber Threat Management Strategy in Southern Border Provinces.

กลุ่มเป้าหมาย ผู้ทรงคุณวุฒิด้านวิศวกรรมระบบไอซีทีและโลกไซเบอร์

<u>คำชี้แจง</u>

วัตถุประสงค์ของการสัมมนาอิงผู้เชี่ยวชาญนี้เพื่อพิจารณายืนยันร่าง “ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้” โดยหัวข้อการสัมมนาจะเกี่ยวข้องกับประเด็นหลัก ๕ ประเด็น ได้แก่

๑. รูปแบบและสถานการณ์ของภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้
๒. ปัญหาและผลกระทบที่เกิดจากภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้
๓. รูปแบบที่เหมาะสมของการบริหารจัดการภัยคุกคามด้านไซเบอร์รวมถึงแนวโน้มในอนาคต
๔. ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้
๕. ข้อเสนอแนะ

ข้อ ๑. รูปแบบและสถานการณ์ของภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

ให้ผู้ทรงคุณวุฒิพิจารณารูปแบบและสถานการณ์ของภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ ขอความคิดเห็นและข้อเสนอแนะ

ข้อ ๒. ปัญหาและผลกระทบที่เกิดจากภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

ให้ผู้ทรงคุณวุฒิพิจารณาปัญหาและผลกระทบที่เกิดจากภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ ขอความคิดเห็นและข้อเสนอแนะ

ข้อ ๓. รูปแบบที่เหมาะสมของการบริหารจัดการภัยคุกคามด้านไซเบอร์รวมถึงแนวโน้มในอนาคต

ให้ผู้ทรงคุณวุฒิพิจารณารูปแบบที่เหมาะสมของการบริหารจัดการภัยคุกคามด้านไซเบอร์รวมถึงแนวโน้มในอนาคต ขอความคิดเห็นและข้อเสนอแนะ

ข้อ ๔. ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

ให้ผู้ทรงคุณวุฒิพิจารณายุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ ขอความคิดเห็นและข้อเสนอแนะ

ข้อ ๕. ข้อเสนอแนะ

๕.๑ ข้อเสนอแนะทั่วไป

……

……

……

……

๕.๒ ข้อเสนอแนะเชิงนโยบาย

……

……

……

……

๕.๓ ข้อเสนอแนะระดับปฏิบัติการ

……

……

……

……

ประวัติย่อผู้วิจัย

ชื่อ พล.ต. ราชิต อรุณรังษี

วัน เดือน ปี เกิด ๒ มกราคม ๒๕๐๕

การศึกษา **หลักสูตรทางทหาร**

- นักเรียนเตรียมทหาร รุ่นที่ ๒๐
- นักเรียนนายร้อย จปร. รุ่นที่ ๓๑
- หลักสูตรชั้นนายร้อยเหล่า ร. รุ่นที่ ๗๖
- หลักสูตรชั้นนายพันเหล่า ร. รุ่นที่ ๕๔
- หลักสูตรประจำ รร.สธ.ทบ. ชุดที่ ๗๒
- หลักสูตรรวบรวมพิเศษ รุ่นที่ ๒๐
- หลักสูตรบริหารจัดการความมั่นคง

ประวัติการทำงาน **ณ ที่ตั้งหน่วย**

- ผบ.มว.ปล.ร้อย อวบ.ร.๔. พัน ๕
- ผบ.ร้อย อวบ.ร.๔. พัน ๕
- ผบ.ร้อย บก.ร.๑. รอ.
- น.ส่งกำลัง ร.๑. รอ.
- ผช.ผอ.ฝขว. พล.๑ รอ.
- หน.ขว.ทบ.
- ฝขว. ประจำ ขว.ทบ.
- ผบ.หน่วย ขกท./นสศ
- เสธ.ขกท.
- รอง ผบ.ขกท.

ตำแหน่งปัจจุบัน รองผู้อำนวยการสำนักการข่าว สำนักงานปฏิบัติภารกิจรักษาความมั่นคงภายในกองทัพบก

สรุปย่อ

ลักษณะวิชา ยุทธศาสตร์

เรื่อง ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

ผู้วิจัย พล.ต. ราชิต อรุณรังษี หลักสูตร วปอ. รุ่นที่ ๖๐

ตำแหน่ง รองผู้อำนวยการสำนักการข่าว กอ.รมน.

ความเป็นมาและความสำคัญของปัญหา

ภัยคุกคามด้านไซเบอร์เป็นภัยคุกคามต่อความมั่นคงตั้งแต่ระดับความมั่นคงแห่งชาติไปจนถึงระดับความมั่นคงของมนุษย์ ในอนาคตมีแนวโน้มขยายตัวเพิ่มขึ้นเป็นทวีคูณ เพราะโลกไซเบอร์ได้กลายเป็นสิ่งอำนวยความสะดวกต่อวิถีชีวิตมนุษย์และการทำงานประจำวันในองค์กรต่างๆ อย่างไรก็ตาม โลกไซเบอร์นี้ย่อมมีทั้งด้านที่เป็นคุณและด้านที่เป็นโทษ โดยขึ้นอยู่กับว่ามนุษย์จะใช้มันเพื่อวัตถุประสงค์ใด ด้วยเหตุนี้ การที่มนุษย์ได้ประโยชน์มหาศาลจากโลกไซเบอร์ก็นำมาซึ่งความท้าทายต่อการรับมือและป้องกันความเสียหายที่เกิดจากการใช้งานดังกล่าวด้วยเช่นกัน

สำหรับปัญหาด้านความมั่นคงในพื้นที่จังหวัดชายแดนใต้ (จชต.) ๔ จังหวัด ของประเทศไทย ที่ประกอบด้วยพื้นที่ของจังหวัดปัตตานี จังหวัดนราธิวาส และจังหวัดยะลา รวมถึง ๔ อำเภอของจังหวัดสงขลา ความรุนแรงในจังหวัดชายแดนภาคใต้ที่เกิดขึ้นมาอย่างยาวนานเป็นปัญหาที่มีพัฒนาการที่มีความซับซ้อน ละเอียดอ่อน และมีความเชื่อมโยงกันหลายมิติ ปัจจุบันสถานการณ์ของการก่อความไม่สงบจากภัยคุกคามด้านไซเบอร์นั้นได้มีการนำสื่อสังคมออนไลน์บนเครือข่ายอินเตอร์เน็ตมาใช้อย่างกว้างขวางในแง่การบ่อนทำลายความน่าเชื่อถือของเจ้าหน้าที่รัฐ การปฏิบัติการจิตวิทยาและการโฆษณาชวนเชื่อของกลุ่มผู้ไม่หวังดี โดยมีแนวโน้มจะปฏิบัติการในรูปแบบอื่นๆ เพิ่มมากขึ้น การสร้างกระแสข่าวในเชิงลบและการสร้างความขัดแย้งต่อประชาชนโดยใช้เครือข่ายสังคมออนไลน์ และมีการบ่อนทำลายข้อมูลสำคัญแห่งรัฐเพื่อสร้างความไม่สงบในรูปแบบต่างๆ อยู่ตลอดเวลา นอกจากนั้นยังสามารถก่อผลกระทบต่อภาพลักษณ์ทางทหาร เช่น การแพร่ภาพคลิปที่ไม่เหมาะสมของทหาร ไม่ว่าจะเป็นการเลือกเผยแพร่รูปภาพเฉพาะความรุนแรง การใช้อาวุธในสถานการณ์ก่อความไม่สงบ และการแพร่คลิปการสูญเสียของทหารเพื่อลดขวัญและกำลังใจของผู้ปฏิบัติงาน ซึ่งเหตุการณ์ต่างๆ เหล่านี้ล้วนแต่ส่งผลกระทบโดยตรงต่อความมั่นคงแห่งชาติแทบทั้งสิ้น

ดังนั้นผู้วิจัยจึงเกิดแนวคิดที่จะดำเนินการวิจัยเรื่อง “ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้” ทั้งนี้เพื่อนำข้อมูลดังกล่าวมาใช้ในการกำหนดรูปแบบ แนวทาง กลไก และมาตรการต่างๆ รวมถึงข้อเสนอแนะเชิงนโยบายในการจัดการ โดยคาดว่าผลการวิจัยสามารถนำมาใช้ให้เป็นประโยชน์กับการรับมือกับภัยคุกคามนี้เพื่อเสริมสร้างความมั่นคงและระงับปัญหาความไม่สงบอย่างเป็นรูปธรรม ทั้งนี้เพื่อให้การดำรงชีวิตของประชาชนในพื้นที่เป็นไปอย่างสันติสุขทั้งในระยะสั้นและระยะยาว อีกทั้งยังใช้เป็นกรอบยุทธศาสตร์ในการพัฒนาเสริมสร้างกำลังด้านไซเบอร์ให้เป็นระบบ มีระเบียบแบบแผน มีมาตรการเชิงรับและเชิงรุกที่มีประสิทธิภาพ ทั้งนี้ก็เพื่อเป็นหลักประกันด้านความมั่นคงแห่งชาติด้านไซเบอร์ของประเทศไทยในอนาคต

วัตถุประสงค์ของการวิจัย

๑. เพื่อศึกษารูปแบบ วิธีการ การประเมินสถานการณ์ และปัญหาผลกระทบของภัยคุกคามด้านไซเบอร์

๒. เพื่อศึกษาผลกระทบของภัยคุกคามด้านไซเบอร์ที่ส่งผลต่อความมั่นคงแห่งชาติในพื้นที่จังหวัดชายแดนภาคใต้

๓. เพื่อนำเสนอยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้

ขอบเขตของการวิจัย

การศึกษาวิจัยตามระเบียบวิธีวิจัยเชิงคุณภาพ (Qualitative Research Methodology) โดยกำหนดขอบเขตการวิจัยได้ดังนี้

๑. ขอบเขตด้านเนื้อหา เน้นการศึกษาเฉพาะประเด็นที่นำไปสู่การกำหนดยุทธศาสตร์ ได้แก่ แนวคิดเรื่องสงครามไซเบอร์ ความมั่นคงแห่งชาติ ผลประโยชน์แห่งชาติ ทฤษฎีความขัดแย้ง ทฤษฎีการบริหารจัดการภาครัฐยุคใหม่ รูปแบบภัยคุกคามด้านไซเบอร์ที่ปรากฏทั่วโลก สถานการณ์ด้านความมั่นคงและความไม่สงบในพื้นที่ที่มีสาเหตุมาจากภัยคุกคามด้านไซเบอร์ เอกสารทางวิชาการ เอกสารทางราชการของหน่วยงานที่เกี่ยวข้อง บทความวิชาการต่างๆ การสำรวจข้อมูลเชิงพื้นที่ เอกสารประกอบการบรรยายที่เกี่ยวข้อง แนวคิดของผู้ทรงคุณวุฒิ และเอกสารงานวิจัยที่เกี่ยวข้อง

๒. ขอบเขตด้านพื้นที่ ศึกษาเฉพาะพื้นที่จังหวัดชายแดนภาคใต้ประกอบด้วยพื้นที่ของจังหวัดปัตตานี จังหวัดนราธิวาส และจังหวัดยะลา รวมถึง ๔ อำเภอของจังหวัดสงขลา ได้แก่ อำเภอเทพา อำเภอสะบ้าย้อย อำเภอจะนะ และอำเภอนาทวี

๓. ขอบเขตด้านประชากร กลุ่มเป้าหมายประกอบด้วย ๑) หน่วยงานด้านความมั่นคงของรัฐ ๒) ผู้บริหาร/ผู้นำท้องถิ่น ๔ จังหวัด ๓) หน่วยงานภาคเอกชน ๔) หน่วยงานพลเรือน ๕) ภาคประชาชน ๖) เจ้าหน้าที่ด้านการข่าวที่เชี่ยวชาญระบบไอซีที ๗) เจ้าหน้าที่ทหารที่รับผิดชอบด้านภัยคุกคามด้านไซเบอร์ ๘) ผู้ปฏิบัติงานที่เกี่ยวข้องกับระบบเครือข่ายอินเตอร์เน็ต ๙) ผู้ทรงคุณวุฒิจากหน่วยงานความมั่นคงด้านไซเบอร์กองทัพไทย และ ๑๐) ผู้เชี่ยวชาญด้านวิศวกรรมระบบไอซีทีและโลกไซเบอร์ การเลือกกลุ่มเป้าหมายที่ให้ข้อมูลเป็นไปในลักษณะจำเพาะเจาะจง เพื่อให้ได้ข้อมูลที่มีความแม่นตรงและสามารถวิเคราะห์ได้อย่างถูกต้องเหมาะสมกับแต่ละสถานการณ์และพื้นที่

๔. ขอบเขตด้านระยะเวลา จะทำการศึกษาในช่วงระยะเวลาตั้งแต่เดือนพฤศจิกายน ๒๕๖๐ ถึงเดือนมิถุนายน ๒๕๖๑

วิธีดำเนินการวิจัย

การวิจัยนี้ใช้ระเบียบวิธีวิจัยเชิงคุณภาพ (Qualitative Research) โดยมีการดำเนินการตามขั้นตอนต่อไปนี้

๑. ด้านการเก็บรวบรวมข้อมูล เก็บข้อมูลเชิงลึกตามกระบวนการวิจัยเชิงคุณภาพโดยมีข้อมูลปฐมภูมิและทุติยภูมิ ดังนี้

๑.๑ ข้อมูลปฐมภูมิ (Primary) ดำเนินการโดยการสัมภาษณ์แบบเชิงลึกผู้ที่มีหน้าที่เกี่ยวข้องกับความมั่นคงในพื้นที่จังหวัดชายแดนภาคใต้ ได้แก่ ๑) หน่วยงานด้านความมั่นคงของรัฐ ๒) ผู้บริหาร/ผู้นำท้องถิ่น ๔ จังหวัด ๓) หน่วยงานภาคเอกชน ๔) หน่วยงานพลเรือน ๕) ภาคประชาชน ๖) เจ้าหน้าที่ด้านการข่าวที่เชี่ยวชาญระบบไอซีที ๗) เจ้าหน้าที่ทหารที่รับผิดชอบด้านภัยคุกคามด้านไซเบอร์ ๘) ผู้ปฏิบัติงานที่เกี่ยวข้องกับระบบเครือข่ายอินเตอร์เน็ต ๙) ผู้ทรงคุณวุฒิจากหน่วยงานความมั่นคงด้านไซเบอร์กองทัพไทย และ ๑๐) ผู้เชี่ยวชาญด้านวิศวกรรมระบบไอซีทีและโลกไซเบอร์ รวมกลุ่มเป้าหมายทั้งสิ้น ๗๕ คน ซึ่งกลุ่มเป้าหมายทั้งหมดได้มาจากการเลือกแบบเจาะจงโดยอาศัยความสะดวก ทั้งนี้กลุ่มผู้ให้ข้อมูลหลัก (Key Informants) จะครอบคลุมผู้มีส่วนเกี่ยวข้องทั้งโดยทางตรงและทางอ้อมทั้งหมดด้านภัยคุกคามด้านไซเบอร์และผู้ที่ปฏิบัติภารกิจในพื้นที่จังหวัดชายแดนภาคใต้

๑.๒ ข้อมูลทุติยภูมิ (Secondary) ได้จากเอกสารที่เกี่ยวข้อง อาทิ รายงานเหตุการณ์ความไม่สงบในพื้นที่ กฎหมาย ระเบียบ วารสาร บทความทางวิชาการ รายงานวิจัย และเอกสารสื่อสิ่งพิมพ์อิเล็กทรอนิกส์ทั้งในและต่างประเทศ รวมทั้งผลการสัมมนาและการทบทวนแนวทางการ

ป้องกันและแก้ไขปัญหาภัยคุกคามด้านไซเบอร์ของหน่วยงานด้านความมั่นคงและกองทัพไทย รวมถึงฝ่ายพลเรือนในแต่ละกระทรวง

๒. ด้านการวิเคราะห์และสังเคราะห์ข้อมูล ดำเนินการวิเคราะห์และสังเคราะห์ตามหลักการวิจัยเชิงคุณภาพ และตรวจสอบข้อมูลโดยใช้เทคนิควิธีการสามเส้าด้านข้อมูล ประกอบด้วย ๑) ข้อมูลจากเอกสารและงานวิจัยที่เกี่ยวข้อง ๒) ข้อมูลที่ได้จากกลุ่มเป้าหมาย และ ๓) ข้อมูลจากระเบียบและกฎหมายที่เกี่ยวข้องกับความมั่นคงด้านไซเบอร์ รวมถึงการวิเคราะห์ SWOT เพื่อนำไปสู่การกำหนดประเด็นยุทธศาสตร์ในการจัดการกับภัยคุกคามด้านไซเบอร์อย่างเป็นระบบ

๓. ด้านการนำเสนอผลการวิจัย ตรวจสอบและยืนยันยุทธศาสตร์โดยการสัมมนาอิงผู้เชี่ยวชาญ โดยอาศัยความรู้ ความเชี่ยวชาญ และประสบการณ์ของผู้วิจัย ร่วมกับความเห็นของผู้ทรงคุณวุฒิ เพื่อแสดงความคิดเห็นและให้ข้อเสนอแนะ จากนั้นนำผลการตรวจสอบไปปรับปรุงกรอบยุทธศาสตร์ที่สมบูรณ์และนำเสนอแนวทางการปฏิบัติ แผนงาน โครงสร้างพื้นฐาน และมาตรการที่เกี่ยวข้องรวมถึงข้อเสนอแนะเชิงนโยบาย

๔. สรุปและเขียนรายงานการวิจัยฉบับสมบูรณ์

ผลการวิจัย

จากผลการศึกษาวิจัยสามารถนำข้อมูลทั้งหมดมาวิเคราะห์ SWOT และกำหนดร่างยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้ประกอบด้วย IADCLIP โดยมีโครงสร้างดังนี้

ยุทธศาสตร์ที่ ๑ : ยุทธศาสตร์การจัดโครงสร้างพื้นฐานของประเทศไทยสำหรับใช้ในการจัดการกับภัยคุกคามด้าน ไซเบอร์ (Infrastructure)

ยุทธศาสตร์ที่ ๒ : ยุทธศาสตร์การสร้างการตระหนักรู้โลกไซเบอร์ให้กับประชาชน (Awareness)

ยุทธศาสตร์ที่ ๓ : ยุทธศาสตร์การพัฒนาความก้าวหน้าด้านไซเบอร์ (Development)

ยุทธศาสตร์ที่ ๔ : ยุทธศาสตร์การส่งเสริมความร่วมมือด้านไซเบอร์ระหว่างภาครัฐ ภาคเอกชน และภาคประชาชน (Coordinate)

ยุทธศาสตร์ที่ ๕ : ยุทธศาสตร์การกำหนดใช้กฎหมายด้านไซเบอร์และการบังคับใช้กับประชาชน (Law and Enforcement)

ยุทธศาสตร์ที่ ๖ : ยุทธศาสตร์การใช้การบูรณาการร่วมกันเพื่อแบ่งปันข้อมูลข่าวสาร (Integration)

ยุทธศาสตร์ที่ ๗ : ยุทธศาสตร์การรับรู้ด้านไซเบอร์เพื่อการป้องกัน การยับยั้ง และการโจมตี (Perception)

ยุทธศาสตร์การจัดการภัยคุกคามด้านไซเบอร์ในพื้นที่จังหวัดชายแดนภาคใต้และในประเทศไทย ถือว่าเป็นเรื่องสำคัญที่ต้องดำเนินการโดยเร็วที่สุด ทั้งนี้ก็เพื่อการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ทุกหน่วยงานราชการ ภาคเอกชน และภาคประชาชนให้มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้ตามปกติ ตลอดจนการระงับยับยั้งการก่อการร้ายด้านไซเบอร์ไม่ให้เกิดขึ้นในประเทศไทย

ข้อเสนอแนะ

ข้อเสนอแนะเชิงนโยบายที่ได้จากการวิจัยมีดังนี้

๑. ก่อนที่จะนำนโยบายหรือกฎหมายฉบับใดที่เกี่ยวข้องกับโลกไซเบอร์มาประกาศใช้ รัฐบาลต้องประชาสัมพันธ์ให้ประชาชนมีความเข้าใจอย่างแท้จริง เพื่อป้องกันการเกิดข่าวลือที่ไม่พึงประสงค์และกระแสต่อต้านของประชาชนในสื่อสังคมออนไลน์

๒. องค์กรและหน่วยงานทั่วไปที่มีการใช้งานในโลกไซเบอร์ ควรมีมาตรการการรักษาปลอดภัยด้านไซเบอร์ (Cyber Security Measures) สำหรับหน่วยงานของตน

๓. ในระดับประเทศ ควรมีหน่วยงานไซเบอร์เป็นการเฉพาะที่ให้การรักษาความมั่นคงปลอดภัยด้านไซเบอร์และการบริการประชาชนในการเฝ้าระวัง แจ้งเตือนภัย และการแก้ไขปัญหาเพื่อสร้างความเชื่อมั่นและความมั่นใจในการใช้งานในโลกไซเบอร์

๔. ควรมีกลไกในการตัดสินใจภายใต้ประเมินความเสี่ยงเพื่อให้สามารถตอบสนองต่อการโจมตีด้านไซเบอร์ของฝ่ายตรงข้ามได้อย่างเหมาะสม รวมถึงอาศัยภาวะผู้นำของผู้บริหารในการตัดสินใจที่ไม่ใช่มุ่งเน้นในเรื่อง “การป้องกัน” มากเกินไป จนละเลยหรือเพิกเฉยต่อ “การตอบโต้”

๕. ควรกำหนดทิศทางแก้ไขปัญหาและมาตรการตอบโต้การโจมตีด้านไซเบอร์ที่เหมาะสม โดยนโยบายดังกล่าวจะต้องเป็นนโยบายที่สามารถดำเนินการได้ในสภาพความเป็นจริงด้วย

๖. ควรเสริมสร้างความรู้ความเข้าใจโลกไซเบอร์แก่เจ้าหน้าที่ภาครัฐและประชาชนทั่วไป โดยมุ่งเน้นในเรื่องมาตรการป้องกันมากกว่าการบังคับใช้กฎหมายหรือระเบียบที่เข้มงวด แนวทางที่ดีที่สุดต่อการดำเนินการด้านไซเบอร์ของรัฐบาลและหน่วยงานที่เกี่ยวข้อง ก็คือ “การสร้างความเข้าใจให้กับประชาชน” เพื่อให้ประชาชนไว้เนื้อเชื่อใจต่อการดำเนินงานของรัฐบาล

๗. ควรออกกฎหมายด้านไซเบอร์เป็นการเฉพาะ เพื่อกำหนดกฎกติกาทางสังคมของโลกไซเบอร์และมาตรการป้องปรามการละเมิดกฎหมาย รวมถึงการมีหน่วยงานที่สามารถบังคับใช้กฎหมายด้านไซเบอร์อย่างจริงจัง