# แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมกับกองทัพเรือ

โดย

พลเรือตรี วิศณุ สร้างวงศ์ใหม่
ผู้อำนวยการสำนักปฏิบัติการ กรมการสื่อสารและเทคโนโลยี
สารสนเทศทหารเรือ

นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ ๖๐
ประจำปีการศึกษา พุทธศักราช ๒๕๖๐ - ๒๕๖๑

# บทคัดย่อ

**เรื่อง แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมกับกองทัพเรือ**
**ลักษณะวิชา วิทยาศาสตร์และเทคโนโลยี**
**ผู้วิจัย พลเรือตรี วิศณุ สร้างวงศ์ใหม่ หลักสูตร วปอ. รุ่นที่ ๖๐**

วัตถุประสงค์ของการวิจัย เพื่อศึกษาแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ทิศทางการบริหารประเทศ ความท้าทายและโอกาสของประเทศ ความท้าทายจากพลวัตของเทคโนโลยีดิจิทัล และสถานภาพการพัฒนาด้วยดิจิทัลในประเทศ พร้อมทั้งเสนอแนะแนวทางในการพัฒนาการสื่อสารและเทคโนโลยีสารสนเทศ ของกองทัพเรือในส่วนขององค์วัตถุ องค์บุคคล ความรู้ หลักนิยม และปฏิบัติการทางทหาร เตรียมความพร้อมในการเชื่อมต่อเครือข่ายโทรคมนาคมกับหน่วยงานอื่น ๆ เพื่อบูรณาการการทำงาน โดยมีขอบเขตของการวิจัยในการพัฒนากองทัพเรือให้มีเครือข่ายสื่อสารและเทคโนโลยีสารสนเทศ ครอบคลุมพื้นที่ปฏิบัติการ ตอบสนองความต้องการทางยุทธวิธีในมิติความเร็ว ความปลอดภัย มีมาตรฐานตามแนวคิดการทำสงครามที่ใช้เครือข่ายเป็นศูนย์กลาง และมีวิธีดำเนินการวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ โดยได้ศึกษาแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม ที่มีความเกี่ยวข้องเชื่อมโยงกับทิศทางการพัฒนาระบบสื่อสารโทรคมนาคม โครงสร้างพื้นฐานทางดิจิทัล ซึ่งผลของการวิจัยทำให้ทราบบริบทของประเทศไทยในยุคดิจิทัล ประชาชนจะมีโอกาสสร้างรายได้จากการนำไอซีที มาเป็นเครื่องมือสนับสนุนการพัฒนาประเทศ มีอินเตอร์เน็ตความเร็วสูงกระจายอย่างทั่วถึง รวมถึงมีคุณภาพชีวิตที่ดีขึ้น การทำธุรกรรมผ่านทางออนไลน์จะมีกฎระเบียบที่ใช้ปฏิบัติได้จริง ทันต่อการเปลี่ยนแปลงทางเทคโนโลยี โดยมีเป้าหมายของการพัฒนา ๔ ระยะ ใช้เวลา ๒๐ ปี ผ่านแผนยุทธศาสตร์ ๖ แผน ได้แก่ การพัฒนาโครงสร้างพื้นฐานดิจิทัลประสิทธิภาพสูง การขับเคลื่อนเศรษฐกิจด้วยเทคโนโลยี สร้างสังคมคุณภาพที่ทั่วถึงและเท่าเทียม ปรับเปลี่ยนภาครัฐสู่การเป็นรัฐบาลดิจิทัล พัฒนากำลังคนให้พร้อมเข้าสู่ยุคเศรษฐกิจและสังคมดิจิทัล และการสร้างความเชื่อมั่นในการใช้เทคโนโลยี และยังมีข้อเสนอแนะด้านเทคโนโลยีดิจิทัลมีการเปลี่ยนแปลงอย่างรวดเร็วตลอดเวลายากต่อการคาดเดา การวางแผนจำเป็นต้องตระหนักรู้และเท่าทันการเปลี่ยนแปลงของเทคโนโลยี รวมถึงนัยของการเปลี่ยนแปลงนั้น ๆ เทคโนโลยีเหล่านี้เป็นเรื่องที่มีความสัมพันธ์กันไม่อาจมองแบบแยกส่วน การนำมาใช้ประโยชน์โดยการหลอมรวมกันอย่างเหมาะสมลงตัวจึงจะเกิดผลดีกับการพัฒนาประเทศ การติดตามการเปลี่ยนแปลงอย่างใกล้ชิดจะทำให้ไม่ตกขบวนรถไฟและไม่ถูกทอดทิ้งไว้ข้างหลัง

# ABSTRACT

**Title Digital Economy and Social Development Plan for the Navy**
**Field Science and Technology**
**Name RAdm.Wisnu Srangwongmai, RTN Course NDC Class 60**

Context of Thailand in the Digital Age People will have the opportunity to generate revenue from ICT as a tool to support the country. High speed internet is spread widely. The quality of life is improved. Online Transactions There are actually rules that apply. Keep up with technological change. With the goal of developing four phases, it takes 20 years to reach its six strategic plans, including the development of high-performance digital infrastructure. Driving the economy with technology Create a quality society that is thorough and equal. Transform the government into a digital government. Develop human resources to enter the digital economy and society. And the confidence in using technology. Mechanisms are driven by activities under institutional change. Resource allocation Follow up the progress of the plan. The threat comes with technology. It is something that should be realized. Cyber security this means the process needed to secure the technology. The concept of war began with a new concept called centrist warfare. The advancement of communication and information technology is a measure of the victory of war from the beginning. For the Navy when analyzing environmental factors. Hurdles and opportunities the navy has a telecommunications network covering land operations. Basic Information Management System and there is a tactical link to the sea. To be a maritime security agency that plays a leading role in the region and supports new threats. Need to prepare to develop a network for tactical operations in the southern border provinces. Network-centric wars need to be addressed in the development of telecommunications networks, information systems, and supervisory systems. And staff development Digital technology is constantly changing, difficult to predict. Planning needs to be aware of and be able to change the technology. These technologies are interconnected, cannot be seen separately. To be exploited by fusing together properly, it will be beneficial to the development of the country. Tracking changes closely will not leave the train and will not be left behind.

# คำนำ

แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมของรัฐบาล คสช. พล.อ.ประยุทธ์ จันทร์โอชา ซึ่งคนทั่วไปเรียกว่าไทยแลนด์ 4.0 ดิจิทัลไทยแลนด์คืออะไรเป็นคำถามที่หากไปถามชาวบ้านตามตรอกซอกซอยก็จะได้รับคำตอบที่หลากหลายเหมือนคนตาบอดคำช้าง ที่ต้องอธิบายความหมายของช้างตามที่ตนเองได้สัมผัสมาซึ่งก็คงไม่ผิดแต่ไม่ใช่ช้างทั้งตัวเหมือนกับที่คนตาดีเห็น และหากรู้แล้วว่าช้างตัวนั้นเป็นอย่างไรแล้วมันมีฤทธิ์เดชอย่างไรซึ่งหมายถึงแผนที่จะมีผลกระทบอย่างไรกับประเทศชาติและประชาชน เป็นแรงบันดาลใจให้ผู้วิจัยทำการศึกษาค้นคว้าในเรื่องนี้

เมื่อทราบแล้วว่าแผนนี้มีผลกระทบอย่างไรตามที่กล่าวแล้วนั้น แล้วกับกองทัพเรือซึ่งผู้วิจัยรับราชการอยู่จะต้องปรับตัวอย่างไรเพื่อให้ไปสู่วิสัยทัศน์หน่วยงานความมั่นคงทางทะเลที่มีบทบาทนำในภูมิภาค เป็นความท้าทายในลำดับต่อไป

อย่างไรก็ดีแผนนี้มีระยะยาวนานถึง ๒๐ ปี ขณะที่เทคโนโลยีเปลี่ยนแปลงอย่างรวดเร็วยากต่อการคาดเดา การพิจารณาแก้ไขปัญหาใด ๆ แบบแยกส่วนโดยไม่เข้าใจหรือรู้ไม่เท่าทันนัยของการเปลี่ยนแปลงนั้นอาจนำมาซึ่งความเสียหาย เนื่องจากเทคโนโลยีเหล่านี้มีความสัมพันธ์กัน การนำมาใช้ประโยชน์โดยหลอมรวมอย่างเหมาะสมลงตัวจึงจะสัมฤทธิ์ผล การติดตามการเปลี่ยนแปลงอย่างใกล้ชิดจะทำให้ไม่ถูกทอดทิ้งไว้ข้างหลังเป็นสิ่งที่ได้รับจากการวิจัย

ขอขอบคุณอาจารย์ที่ปรึกษา ผู้ทรงคุณวุฒิ เพื่อนนักศึกษา วปอ.๖๐ และผู้มีส่วนในการจัดทำเอกสารวิจัยเล่มนี้จนสำเร็จลุล่วงไปด้วยดี หวังเป็นอย่างยิ่งว่าผู้นำเอกสารเล่มนี้ไปศึกษาหรืออ้างอิงใช้ประโยชน์จะได้รับประโยชน์จากงานวิจัยนี้บ้างไม่มากก็น้อย

พล.ร.ต.
(วิศณุ สร้างวงศ์ใหม่)
นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตร วปอ. รุ่นที่ ๖๐
ผู้วิจัย

# สารบัญ

# สารบัญ (ต่อ)

# สารบัญแผนภาพ

**หน้า**

**แผนภาพที่**

# บทที่ ๑
# บทนำ

## ความเป็นมาและความสำคัญของปัญหา

แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ได้รับความเห็นชอบจาก ครม. เมื่อ ๕ เม.ย.๕๙ โดยมีผลให้ ทุกกระทรวง กรม รัฐวิสาหกิจ องค์กรปกครองส่วนท้องถิ่น หน่วยงานของรัฐ และหน่วยงานที่เกี่ยวข้อง ต้องนำแผนดังกล่าวไปพิจารณาประกอบการจัดทำแผนปฏิบัติงานและคำของบประมาณรายจ่ายประจำปีของหน่วยงาน ให้สอดคล้องกัน

วิสัยทัศน์และเป้าหมายของแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม มุ่งเน้นการพัฒนาอย่างต่อเนื่อง ในระยะยาวอย่างยั่งยืน ให้สอดคล้องกับการจัดทำยุทธศาสตร์ชาติ ๒๐ ปี กำหนดแนวทางเป็น ๔ ระยะ เพื่อให้ประเทศไทยสามารถสร้างสรรค์ และใช้ประโยชน์จากเทคโนโลยีดิจิทัลอย่างเต็มศักยภาพ ซึ่งแผนดังกล่าวประกอบด้วย ยุทธศาสตร์ที่สำคัญ ๖ ยุทธศาสตร์ ได้แก่

๑. พัฒนาโครงสร้างพื้นฐานดิจิทัลประสิทธิภาพสูงให้ครอบคลุมทั่วประเทศ

๒. ขับเคลื่อนเศรษฐกิจด้วยเทคโนโลยีดิจิทัล

๓. สร้างสังคมคุณภาพที่ทั่วถึงเท่าเทียมด้วยเทคโนโลยีดิจิทัล

๔. ปรับเปลี่ยนภาครัฐสู่การเป็นรัฐบาลดิจิทัล

๕. พัฒนากำลังพลให้พร้อมเข้าสู่ยุคเศรษฐกิจและสังคมดิจิทัล

๖. สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล

โดยในระยะที่ ๑ ใช้เวลา ๑ ปี ๖ เดือน เป็นการลงทุนสร้างรากฐานในการพัฒนาเศรษฐกิจและสังคมดิจิทัล ระยะที่ ๒ ใช้เวลา ๕ ปี ทุกภาคส่วนมีส่วนร่วมในเศรษฐกิจและสังคมดิจิทัล ระยะที ๓ ใช้เวลา ๑๐ ปี ก้าวสู่ดิจิทัลไทยแลนด์ ที่ขับเคลื่อนและใช้ประโยชน์จากนวัตกรรมอย่างเต็มศักยภาพ ระยะที่ ๔ จาก ๑๐ – ๒๐ ปี ประเทศไทยอยู่ในกลุ่มประเทศที่พัฒนาแล้ว สามารถใช้เทคโนโลยีดิจิทัลสร้างมูลค่าทางเศรษฐกิจและคุณค่าทางสังคมอย่างยั่งยืน

วิสัยทัศน์ของกองทัพเรือต่อการสื่อสารและสารสนเทศ กำหนดให้ “กองทัพเรือจะเป็นองค์กรชั้นนำด้วยการประยุกต์ใช้การสื่อสารและเทคโนโลยีสารสนเทศ ในการสนับสนุนการบริหารจัดการและการปฏิบัติภารกิจอย่างเต็มรูปแบบ” ซึ่งจากการวิเคราะห์ปัจจัยสภาวะแวดล้อมทั้งภายในและภายนอก จุดอ่อน จุดแข็ง โอกาส และอุปสรรค ในการพัฒนาด้านการสื่อสารและเทคโนโลยีสารสนเทศของกองทัพเรือ พบว่ากองทัพเรือมีโครงข่ายโทรคมนาคมครอบคลุมพื้นที่ปฏิบัติงานบนบก

มีระบบสารสนเทศพื้นฐานในการบริหารงานทั่วไป มีระบบเชื่อมโยงข้อมูลทางยุทธวิธีให้กับเรือในทะเล ซึ่งยังมีความจำเป็นต้องพัฒนาอีกมาก หากจะเป็นองค์กรชั้นนำตามที่คาดหวังไว้ ประกอบกับภารกิจที่เปลี่ยนแปลงไป ตัวอย่างเช่น การรักษาผลประโยชน์ของชาติในทะเลมีความซับซ้อนมากขึ้นจำเป็นต้องบูรณาการกับหน่วยงานทั้งภาครัฐและเอกชน ภัยคุกคามรูปแบบใหม่ การช่วยเหลือผู้ประสบภัยพิบัติในทะเล การค้ามนุษย์ การทำประมงผิดกฎหมาย และสงครามไซเบอร์

ตามที่รัฐบาลมีนโยบายที่จะพัฒนาประเทศให้เป็นประเทศในกลุ่มที่พัฒนาแล้ว หน่วยงานต่างๆ จำเป็นต้องพัฒนาโครงสร้างพื้นฐาน เครือข่ายโทรคมนาคม ให้มีความทันสมัยสามารถเชื่อมต่อใช้งานร่วมกันได้ หากกองทัพเรือสามารถใช้ประโยชน์จากโอกาสนี้ จะทำให้ประหยัดงบประมาณในการจัดหายุทโธปกรณ์ที่ซ้ำซ้อน แต่อย่างไรก็ดีเทคโนโลยีดิจิทัลมีการเปลี่ยนแปลงอย่างรวดเร็วตลอดเวลายากต่อการคาดเดา การวางแผนจำเป็นต้องตระหนักรู้และเท่าทันการเปลี่ยนแปลงของเทคโนโลยีในอนาคต รวมถึงนัยของการเปลี่ยนแปลงนั้นๆ จึงเป็นสาเหตุและความจำเป็นในการศึกษาค้นคว้าวิจัยในเรื่องนี้

## วัตถุประสงค์ของการวิจัย

๑. ศึกษาแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม ของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ทิศทางการบริหารประเทศ ความท้าทายและโอกาสของประเทศไทยในภาพรวม ความท้าทายจากพลวัตของเทคโนโลยีดิจิทัล และสถานภาพการพัฒนาด้วยดิจิทัลในประเทศไทย

๒. เสนอแนะแนวทางในการพัฒนาการสื่อสารและเทคโนโลยีสารสนเทศของกองทัพเรือในส่วนขององค์วัตถุ องค์บุคคล ความรู้ หลักนิยมและการปฏิบัติทางทหาร ตลอดจนเตรียมความพร้อมในการเชื่อมต่อเครือข่ายการสื่อสารและเทคโนโลยีสารสนเทศ กับหน่วยงานอื่นๆ เพื่อบูรณาการในงานที่มีภารกิจร่วมกัน

## ขอบเขตของการวิจัย

แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม มีเป้าหมายให้ประเทศก้าวหน้าสู่การเป็น “ดิจิทัลไทยแลนด์” ที่ขับเคลื่อนและใช้ประโยชน์จากนวัตกรรมดิจิทัลอย่างเต็มที่ ส่วนการศึกษาวิจัยครั้งนี้มีขอบเขตพัฒนากองทัพเรือให้มีโครงข่ายการสื่อสารที่ครอบคลุมพื้นที่ปฏิบัติการ ตลอดจนมีระบบสารสนเทศตอบสนองภารกิจความต้องการทางยุทธวิธี ในมิติของความเร็ว ความปลอดภัย มีมาตรฐานตามแนวคิดการทำสงครามที่ใช้เครือข่ายเป็นศูนย์กลาง

## วิธีดำเนินการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ โดยศึกษาแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม ที่มีความเกี่ยวข้องเชื่อมโยงกับทิศทางการพัฒนาระบบสื่อสารโทรคมนาคม และโครงสร้างพื้นฐานเพื่อเปลี่ยนผ่านจากระบบอนาลอกเป็นดิจิทัล รวมทั้งศึกษามติคณะรัฐมนตรี และความเห็นของหน่วยงานเกี่ยวข้องหรือมีส่วนได้เสีย

## ประโยชน์ที่ได้รับจากการวิจัย

๑. ได้รับทราบแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม และสถานภาพการพัฒนาด้วยดิจิทัลในประเทศไทย

๒. ได้ทราบแนวทางในการพัฒนาการสื่อสารและเทคโนโลยีสารสนเทศของกองทัพเรือ

๓. ได้ทราบขีดความสามารถการรองรับสงครามที่มีเครือข่ายเป็นศูนย์กลาง และการประหยัดงบประมาณในการจัดหายุทโธปกรณ์ของกองทัพเรือ

แผนภาพที่ ๑ - ๑ : What is Thailand 4.0?


ที่มา : กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

แผนภาพที่ ๑ - ๒ : What is Thailand 4.0?

ที่มา : กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

แผนภาพที่ ๑ - ๓ : Firewall ป้องกันการ login ที่ไม่ได้รับอนุญาต

ที่มา : กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

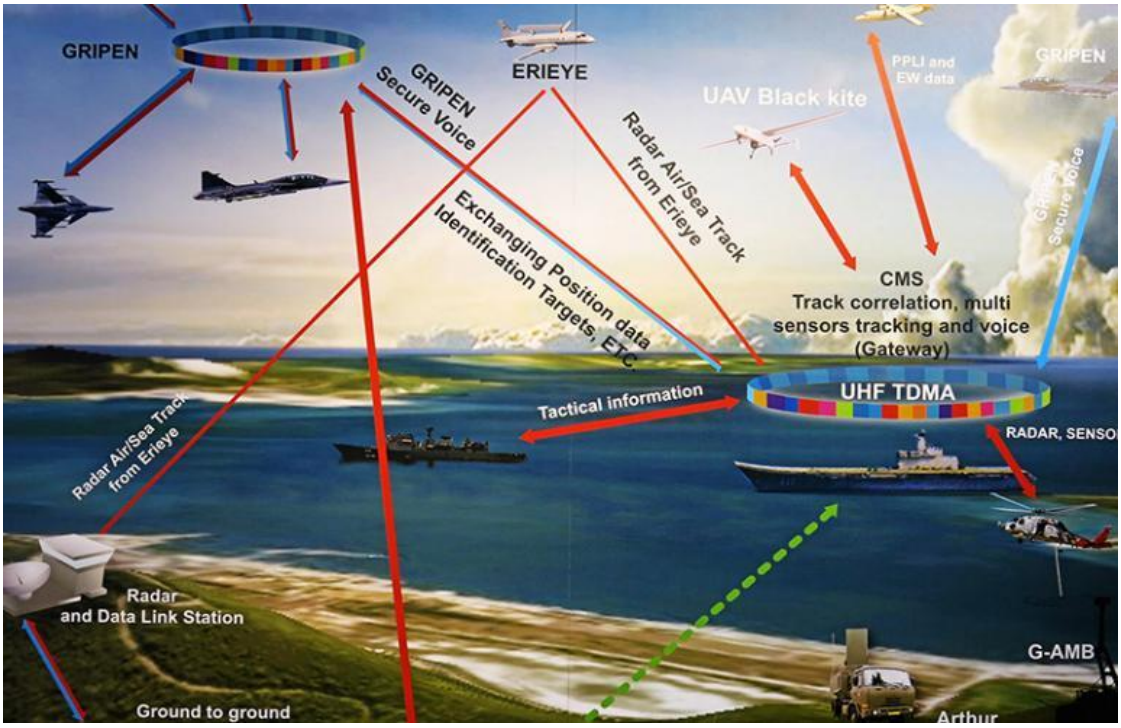
แผนภาพที่ ๑ - ๔ : Malware โปรแกรมที่ออกแบบมาเพื่อสร้างความเสียหาย
ให้กับเครื่องคอมพิวเตอร์และระบบเครือข่าย

ที่มา : กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

แผนภาพที่ ๑ - ๕ : Network Centric สงครามที่ใช้เครือข่ายเป็นศูนย์กลาง

ที่มา : กองทัพเรือ

แผนภาพที่ ๑ - ๖ : Network Centric สงครามที่ใช้เครือข่ายเป็นศูนย์กลาง




ที่มา : กองทัพเรือ

# บทที่ ๒
# แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม

โลกเริ่มเข้าสู่ยุคระบบเศรษฐกิจและสังคมดิจิทัลที่เทคโนโลยีดิจิทัลไม่ได้เป็นแค่เครื่องมือช่วยเหลือในการทำงาน แต่จะหลอมรวมเข้ากับชีวิตและเปลี่ยนโครงสร้างรูปแบบกิจกรรมทางเศรษฐกิจ การผลิต การบริการ การปฏิสัมพันธ์ระหว่างบุคคลซึ่งมีความจำเป็นที่ประเทศต้องนำเทคโนโลยีดิจิทัลมาเป็นเครื่องมือเพื่อแก้ปัญหา เพิ่มโอกาสในการพัฒนา โดย ครม.ได้เห็นชอบแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เมื่อ ๕ เม.ย.๕๙ มีผลให้ทุกกระทรวง กรม รัฐวิสาหกิจ องค์กรปกครองส่วนท้องถิ่น หน่วยงานของรัฐ และหน่วยงานที่เกี่ยวข้องต้องนำแผนดังกล่าวไปพิจารณาประกอบการจัดทำแผนปฏิบัติงาน

ดิจิทัลไทยแลนด์ มีความคาดหมายให้ประเทศไทยสามารถสร้างสรรค์และใช้ประโยชน์จากเทคโนโลยีดิจิทัลอย่างเต็มศักยภาพ มีเป้าหมาย ๔ ประการได้แก่ เพิ่มขีดความสามารถในการแข่งขัน สร้างโอกาสทางสังคมอย่างเท่าเทียม เตรียมความพร้อมบุคลากรและปฏิรูปการทำงาน การให้บริการภาครัฐ เน้นการพัฒนาระยะยาวอย่างยั่งยืน สอดคล้องกับยุทธศาสตร์ชาติ ๒๐ ปี มีเป้าหมาย ๔ ระยะคือ ระยะที่ ๑ ใช้เวลา ๑ ปี ๖ เดือน ประเทศไทยลงทุนและสร้างฐานรากในการพัฒนาเศรษฐกิจและสังคมดิจิทัล ระยะที่ ๒ ใช้เวลา ๕ ปี ทุกภาคส่วนของประเทศมีส่วนร่วมในการพัฒนาเศรษฐกิจและสังคมดิจิทัล ระยะที่ ๓ ใช้เวลา ๑๐ ปี ประเทศก้าวสู่ดิจิทัลไทยแลนด์ที่ขับเคลื่อนและใช้ประโยชน์จากนวัตกรรมดิจิทัลได้อย่างเต็มศักยภาพ และระยะที่ ๔ ประเทศไทยอยู่ในกลุ่มประเทศที่พัฒนาแล้วสามารถใช้เทคโนโลยีดิจิทัลสร้างมูลค่าทางเศรษฐกิจและคุณค่าทางสังคมอย่างยั่งยืน

## บริบทของประเทศไทยในยุคดิจิทัล

กรอบนโยบายเทคโนโลยีสารสนเทศและการสื่อสาร พ.ศ.๒๕๕๔ – ๒๕๖๓ ให้ความสำคัญกับการพัฒนาและการนำไอซีทีมาใช้เป็นเครื่องมือสนับสนุนการพัฒนาประเทศ ให้ประเทศไทยมีโครงสร้างพื้นฐาน อินเตอร์เน็ตความเร็วสูงกระจายอย่างทั่วถึง ประชาชนมีโอกาสสร้างรายได้และมีคุณภาพชีวิตที่ดี ไอซีทีมีบทบาทต่อการพัฒนาประเทศซึ่งปัจจุบันสถานภาพการพัฒนาประเทศไทย ด้านเทคโนโลยีสารสนเทศและการสื่อสารพอสรุปได้ดังนี้

**๑. ทิศทางการพัฒนาประเทศโดยภาพรวม** เป็นทั้งความท้าทายและโอกาส ได้แก่ การก้าวข้ามกับดักประเทศที่มีรายได้ปานกลางไปสู่การมีรายได้สูง ประเทศไทยยังตกอยู่ในสภาวะนี้ การเพิ่มขีดความสามารถในการแข่งขัน ยังไม่สามารถอยู่ในกลุ่มประเทศที่แข็งขันด้วยนวัตกรรม

การปรับตัวและฉกฉวยโอกาสจากการรวมกลุ่มทางเศรษฐกิจจำเป็นต้องพิจารณาผลกระทบกับกลุ่มประเทศชั้นนำของโลกด้วย การแก้ปัญหาความเหลื่อมล้ำของสังคมยังมีช่องว่างอยู่มากระหว่างผู้ใช้ประโยชน์จากเทคโนโลยีกับผู้ที่ไม่เข้าใจ ไม่เข้าถึง ไม่สามารถใช้ประโยชน์ การเข้าสู่สังคมผู้สูงวัย การพัฒนาบุคลากร และภัยคุกคามไซเบอร์เป็นการเรียนรู้ใหม่ที่ต้องมีการเตรียมการ

**๒. เทคโนโลยีดิจิทัลมีอิทธิพลต่อการใช้ชีวิตของประชาชน** การประกอบธุรกิจการเงิน ธนาคาร และภาครัฐ แต่เทคโนโลยีเปลี่ยนแปลงรวดเร็วยากต่อการคาดเดา จำเป็นต้องตระหนักรู้โดยมีตัวอย่างของการเปลี่ยนแปลงที่เห็นได้แก่

๒.๑ การเปลี่ยนแปลงทางเทคโนโลยีแบบก้าวกระโดด โดยมีเทคโนโลยีที่จะมีบทบาทนำได้แก่ การสื่อสารความเร็วสูง อุปกรณ์เคลื่อนที่เพื่อการเชื่อมต่อทุกที่ทุกเวลา การประมวลผลแบบคราวด์ การวิเคราะห์ข้อมูลขนาดใหญ่ อินเตอร์เน็ตออฟติง การพิมพ์สามมิติ เป็นต้น

๒.๒ เกิดการหลอมรวมระหว่างกิจกรรมทางเศรษฐกิจ สังคม ของโลกออนไลน์และออฟไลน์ ทำให้เส้นแบ่งระหว่างโลกไซเบอร์และโลกทางกายภาพเกือบเป็นเรื่องเดียวกัน

๒.๓ เกิดแนวโน้มการใช้เทคโนโลยีดิจิทัลเพื่อการผลิตที่มากขึ้น

๒.๔ เกิดการแข่งขันที่อยู่บนพื้นฐานของนวัตกรรมสิ้นค้าและบริการ การแข่งขันในเชิงราคาจะใช้ไม่ได้อีกต่อไป ผู้บริโภคมีความรู้มากขึ้น

๒.๕ การวิเคราะห์ข้อมูลขนาดใหญ่ที่มีจำนวมมาก เปลี่ยนแปลงอย่างรวดเร็วเป็นเรื่องจำเป็น เป็นพื้นฐานขององค์กรทั่วไป

๒.๖ ความปลอดภัยในโลกไซเบอร์ จะเป็นภัยคุกคามใหม่ที่ทำให้เกิดความเสียหายกับองค์กรหากไม่มีระบบป้องกันที่เหมาะควร จะมีความสลับซับซ้อนมากขึ้น

๒.๗ เกิดการเปลี่ยนแปลงโครงสร้างกำลังคน งานหลายประเภทถูกทดแทนด้วยเทคโนโลยีที่มีประสิทธิภาพสูงกว่า งานรูปแบบใหม่จะต้องใช้ความรู้และทักษะที่สูงขึ้น

**๓. สถานภาพการพัฒนาด้านดิจิทัลของประเทศ** มีองค์ประกอบที่ต้องนำมาพิจารณาได้แก่ โครงสร้างพื้นฐานด้านการสื่อสารและเทคโนโลยี การใช้ประโยชน์เทคโนโลยีของประชาชน ภาคธุรกิจ และภาครัฐ ทรัพยากรมนุษย์ รวมถึงกฎหมาย ระเบียบ กฎเกณฑ์ที่เกี่ยวข้อง

๓.๑ โครงสร้างพื้นฐานด้านการสื่อสารและเทคโนโลยีดิจิทัลของประเทศ ยังไม่ครอบคลุมทุกพื้นที่ หน่วยงานภาครัฐ เช่น โรงเรียน โรงพยาบาล องค์การบริหารส่วนท้องถิ่นต่างๆ หลายแห่งยังไม่สามารถเข้าถึงโครงข่ายอินเตอร์เน็ตความเร็วสูง ค่าบริการอินเตอร์เน็ตความเร็วสูงเทียบกับประเทศเพื่อนบ้านจัดว่ามีค่าบริการที่สูงมาก

๓.๒ การใช้เทคโนโลยีดิจิทัลของภาคประชาชนส่วนใหญ่เพื่อความบันเทิง สนุกสนาน เนื้อหาในรูปแบบสื่อดิจิทัลที่เหมาะสมสอดคล้องกับความต้องการของประชาชนในระดับท้องถิ่น ทั้ง

เชิงเศรษฐกิจ สังคม วัฒนธรรม และการศึกษา เพื่อนำไปประกอบอาชีพยังไม่เพียงพอ การเชื่อมต่ออินเตอร์เน็ตมีปัญหาการบริการยังไม่ทั่วถึง

๓.๓ การใช้เทคโนโลยีดิจิทัลของภาคธุรกิจยังไม่สูงมากนัก โดยเฉพาะธุรกิจ SME จำเป็นต้องส่งเสริมและกระตุ้นให้เข้าสู่ระบบการค้าดิจิทัล เพื่อเพิ่มโอกาสทางการตลาดและยกระดับเศรษฐกิจชุมชนและฐานรากให้เข้มแข็ง

๓.๔ ระบบสารสนเทศภาครัฐ ยังขาดการบูรณาการการใช้ข้อมูลร่วมกัน ข้อมูลซ้ำซ้อน ประชาชนยังต้องยื่นเอกสารหลายรายการในการติดต่อกับภาครัฐ ทำให้ใช้เวลาและมีค่าใช้จ่ายสูงไม่ก่อให้เกิดคุณค่าเพิ่มทั้งกับหน่วยงานและประชาชน อุปสรรคสำคัญของการบูรณาการระบบสารสนเทศคือเงื่อนไขและหลักเกณฑ์ ในการกำหนดรายละเอียดของข้อมูลที่แตกต่างกันเชื่อมโยงข้อมูลได้ยาก

๓.๕ ผู้ทำงานด้านไอทีในตลาดแรงงานมีแนวโน้มสูงขึ้น ส่วนใหญ่เป็นผู้ปฏิบัติงานด้านช่างเทคนิค ช่างไฟฟ้าอิเล็กทรอนิกส์ ผู้ทำงานด้านโปรแกรมเมอร์ซอฟต์แวร์ยังขาดแคลน วิชาชีพที่คาดว่าเป็นที่ต้องการของตลาดแรงงาน ได้แก่ สายงาน Cloud Computing, Big data และ Mobile application กลุ่มผู้ปฏิบัติงานที่ใช้คอมพิวเตอร์ในสถานประกอบการยังมีไม่มาก เนื่องจากสถานประกอบการไม่เห็นความสำคัญในการใช้เทคโนโลยีทำธุรกิจ การสร้างแรงจูงใจให้กับผู้บริหารระดับสูงมีความจำเป็น หากต้องการขับเคลื่อนประเทศด้วยนวัตกรรม เกิดวิชาชีพใหม่ๆ เกี่ยวกับการพัฒนาในอนาคต

๓.๖ ความเชื่อมั่นในการทำธุรกรรมผ่านทางออนไลน์มีความเสี่ยงจากการถูกฉ้อโกง ภัยคุกคามทางไซเบอร์สร้างความเสียหายให้กับบุคคลและองค์กร การถูกละเมิดการรักษาความปลอดภัยของข้อมูลคอมพิวเตอร์ ข้อมูลส่วนบุคคลเป็นสิ่งที่ต้องมีระเบียบกฎเกณฑ์ข้อบังคับที่ใช้ปฏิบัติได้จริงและทันสมัยต่อการเปลี่ยนแปลงทางเทคโนโลยี

## เป้าหมายของการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมไทย

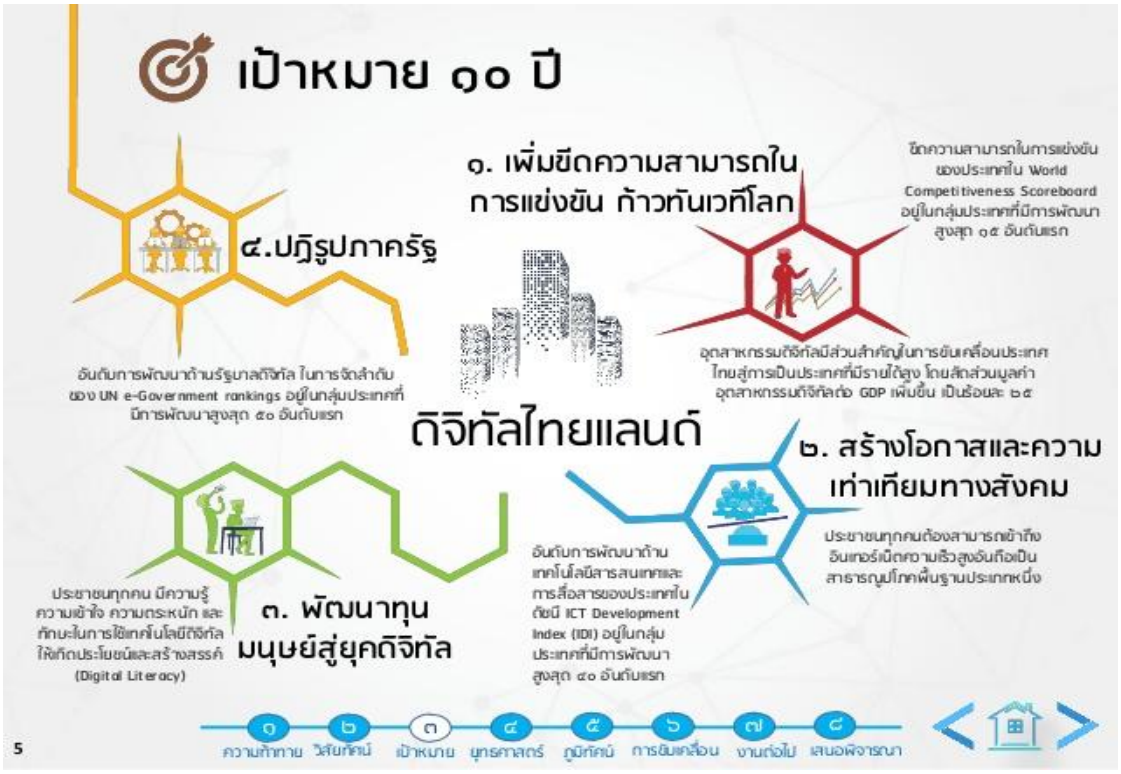
ดิจิทัลไทยแลนด์ หมายถึงประเทศไทยสามารถใช้ประโยชน์และสร้างสรรค์นวัตกรรมจากการใช้เทคโนโลยีดิจิทัลอย่างเต็มศักยภาพ โดยมีเป้าหมายในระยะ ๑๐ ปี ได้แก่ การเพิ่มขีดความสามารถในการแข่งขันให้ก้าวทันเวทีโลกด้วยการใช้นวัตกรรมและเทคโนโลยีดิจิทัลเป็นเครื่องมือสร้างโอกาสทางสังคมอย่างเท่าเทียมด้วยข้อมูลข่าวสารและบริการผ่านสื่อดิจิทัล ยกระดับคุณภาพชีวิตประชาชน พัฒนาทุนมนุษย์สู่ยุคดิจิทัล ด้วยการเตรียมความพร้อมให้บุคลากรมีความรู้และทักษะเหมาะสมกับการดำเนินชีวิต และปฏิรูปกระบวนทัศน์การทำงานและการให้บริการภาครัฐที่มีประสิทธิภาพโปร่งใสตรวจสอบได้ ในการนี้แบ่งการทำงานออกเป็น ๓ ระยะได้แก่

**๑. ระยะที่ ๑ ใช้เวลา ๑ ปี ๖ เดือน** ประเทศไทยลงทุนและสร้างฐานรากในการพัฒนาเศรษฐกิจและสังคมดิจิทัล โดยการลงทุนโครงสร้างพื้นฐานเครือข่ายโทรคมนาคมความเร็วสูง

ส่งเสริมธุรกิจที่ใช้เทคโนโลยีเป็นฐานโดยเฉพาะกลุ่ม SME และวิสาหกิจชุมชน สถาบันการศึกษาและหน่วยงานที่ให้บริการสาธารณะทุกพื้นที่ มีการใช้งานเทคโนโลยีดิจิทัลเชื่อมต่ออินเตอร์เน็ตความเร็วสูง การบริหารงานงานภาครัฐเปลี่ยนเป็นระบบดิจิทัลอย่างเป็นระบบ คนในประเทศได้รับการส่งเสริมทักษะด้านดิจิทัลที่มีมาตรฐานสากล กฎระเบียบต่างๆ ต้องปรับแก้ให้เอื้อต่อเศรษฐกิจและสังคมดิจิทัล

**๒. ระยะที่ ๒ ใช้เวลา ๕ ปี** ทุกภาคส่วนของประเทศมีส่วนร่วมในการพัฒนาเศรษฐกิจและสังคม ประเทศไทยมีโครงข่ายความเร็วสูงแบบใช้สายและไร้สายเข้าถึงทุกหมู่บ้านครอบคลุมทั่วประเทศ การแพร่ภาพและกระจายเสียงทางวิทยุและโทรทัศน์จะเปลี่ยนผ่านจากระบบอนาล็อกมาเป็นดิจิทัลอย่างเต็มรูปแบบ ภาคการเกษตร ภาคอุตสาหกรรม และภาคบริการ เติบโตด้วยการใช้ประโยชน์จากเทคโนโลยีพัฒนาไปสู่การทำธุรกิจด้วยระบบอัตโนมัติ ประชาชนเข้าถึงโครงข่ายความเร็วสูงและบริการสาธารณะพื้นฐาน โดยเฉพาะการเรียนรู้ การใช้ดิจิทัลเป็นเครื่องมือพัฒนาบุคลากร ส่งเสริมดูแลสุขภาพของคนในเมืองและชนบทห่างไกล ภาครัฐสามารถบูรณาการข้ามหน่วยงานโดยสมบูรณ์ ผู้บริหารเข้าถึงข้อมูลได้ในทุกระดับ ประชาชนเข้าถึงข้อมูลที่มีความมั่นคงปลอดภัย รักษาความเป็นส่วนตัว ตรวจสอบได้ นำไปสู่การดำเนินงานที่โปร่งใส รูปแบบการจ้างงานและวัฒนธรรมการทำงานจะเปลี่ยนแปลงไป ผู้เชี่ยวชาญด้านดิจิทัลจะมีจำนวนมากขึ้น กฎหมายที่สนับสนุนและจำเป็นต่อนโยบาย Digital Economy มีการบังคับใช้ไม่เลือกการปฏิบัติ

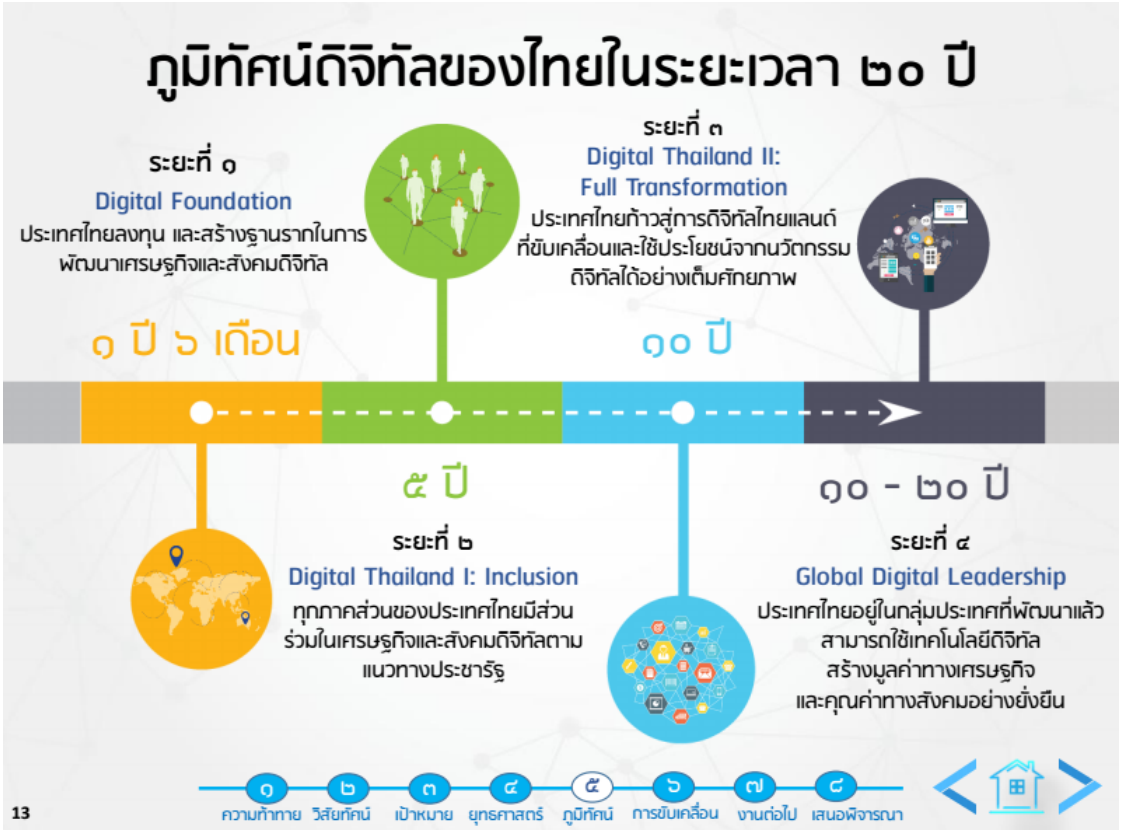
แผนภาพที่ ๒ - ๑ : เป้าหมาย ๑๐ ปี




ที่มา : กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

**๓. ระยะที่ ๓ ใช้เวลา ๑๐ ปี** ประเทศไทยก้าวสู่การเป็นดิจิทัลไทยแลนด์ที่ขับเคลื่อนและใช้ประโยชน์จากนวัตกรรมดิจิทัลได้อย่างเต็มที่ มีโครงสร้างพื้นฐานดิจิทัลที่ทันสมัยทัดเทียมประเทศพัฒนาแล้ว อินเตอร์เน็ตความเร็วสูงเป็นสาธารณูปโภคขั้นพื้นฐานเช่นเดียวกับถนน ไฟฟ้า น้ำประปา ข้อมูลการใช้บริการอินเตอร์เน็ตจะถูกเก็บใส่ในดาต้าเซ็นเตอร์ สามารถเข้าถึงและใช้ประโยชน์ได้ตลอดเวลา ประเทศไทยเป็นศูนย์กลางการค้าและการลงทุนดิจิทัล ภาคอุตสาหกรรมสามารถนำเทคโนโลยีมาใช้ปรับปรุงประสิทธิภาพการทำงาน ภาคเกษตรกรรมปรับเปลี่ยนรูปแบบสู่การทำเกษตรแบบอัจฉริยะ ประชาชนทุกกลุ่มโดยเฉพาะผู้ด้อยโอกาส ผู้สูงอายุ คนพิการ เข้าถึงบริการของรัฐได้ทุกที่ทุกเวลาผ่านเทคโนโลยีดิจิทัล รัฐบาลมีกระบวนการทำงานเป็นระบบดิจิทัลโดยสมบูรณ์ การทำงานบูรณาการเหมือนเป็นองค์กรเดียวกัน โครงสร้างกำลังคนรุ่นใหม่มีทักษะดิจิทัลระดับสูง กฎระเบียบที่เป็นอุปสรรคต่อการค้าการลงทุนดิจิทัลได้รับการทบทวนปรับปรุงแก้ไขอย่างต่อเนื่อง

แผนภาพที่ ๒ - ๒ : ภูมิทัศน์ดิจิทัลของไทยในระยะเวลา ๒๐ ปี




ที่มา : กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

**๔. ระยะที่ ๔ ใช้ระยะเวลา ๒๐ ปี** เป็นบทสรุปจากการดำเนินการที่ผ่านมา แต่เนื่องจากเทคโนโลยีเปลี่ยนแปลงอย่างรวดเร็วตลอดเวลายากต่อการคาดเดาแต่อาจกล่าวได้ว่าประเทศไทยอยู่ในกลุ่มประเทศที่พัฒนาแล้ว สามารถใช้เทคโนโลยีดิจิทัลสร้างมูลค่าทางเศรษฐกิจและคุณค่า

ทางสังคมอย่างยั่งยืน เทคโนโลยีดิจิทัลจะไม่ใช่สิ่งแปลกใหม่ในสังคมเป็นเสมือนปัจจัยที่ ๕ ในการใช้ชีวิตประจำวัน ประเทศไทยก้าวข้ามกับดักรายได้ปานกลางไปสู่ประเทศที่มีรายได้สูงทัดเทียมประเทศพัฒนาแล้ว การพัฒนาประเทศจะขับเคลื่อนจากชนบทเข้าสู่ศูนย์กลาง รัฐจะไม่เป็นผู้สร้างบริการสาธารณะอีกต่อไป แต่จะเป็นผู้อำนวยความสะดวกในการให้บริการ ผู้เชี่ยวชาญด้านดิจิทัลของประเทศไทยทำงานให้กับบริษัทที่อยู่ต่างประเทศเพิ่มมากขึ้น

## ยุทธศาสตร์การพัฒนา

แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมได้กำหนดยุทธศาสตร์การพัฒนาแผนทั้ง ๔ ระยะไว้ ๖ ยุทธศาสตร์ ได้แก่ การพัฒนาโครงสร้างพื้นฐานดิจิทัลประสิทธิภาพสูงให้ครอบคลุมทั่วประเทศ การขับเคลื่อนเศรษรกิจด้วยเทคโนโลยีดิจิทัลสร้างสังคมคุณภาพที่เท่าเทียมและทั่วถึง ปรับเปลี่ยนภาครัฐสู่การเป็นรัฐบาลดิจิทัล พัฒนากำลังพลและสร้างความเชื่อมั่นในการใช้เทคโนโลยี ดังนี้

**๑. การพัฒนาโครงสร้างพื้นฐานดิจิทัลประสิทธิภาพสูง**ให้ครอบคลุมทั่วประเทศ โครงสร้างพื้นฐานดิจิทัลประสิทธิภาพสูงที่สำคัญประกอบด้วยโครงสร้างเทคโนโลยีสารสนเทศโทรคมนาคม การแพร่ภาพกระจายเสียงที่มีความทันสมัย มีคุณภาพ รองรับการแลกเปลี่ยนข้อมูลด้านเศรษฐกิจการบริการภาครัฐ ค่าบริการที่ประชาชนจ่ายจะไม่เป็นอุปสรรคในการให้บริการ

**๒. ขับเคลื่อนเศรษฐกิจด้วยเทคโนโลยีดิจิทัล** การพัฒนาเศรษฐกิจของประเทศโดยอาศัยเทคโนโลยีดิจิทัลเพื่อให้ภาคธุรกิจสามารถลดต้นทุนการผลิต เพิ่มประสิทธิภาพ เชื่อมโยงท้องถิ่นกับตลาดโลก สร้างมูลค่าสินค้าชุมชน ส่งเสริมการใช้เทคโนโลยี วิเคราะห์และประเมินผลข้อมูลขนาดใหญ่ เพิ่มช่องทางประชาสัมพันธ์ บริการชุมชน เช่น การท่องเที่ยว ธุรกิจแพทย์ทางเลือก บริหารจัดการพื้นที่เพาะปลูก ระบบน้ำ การผลิต

**๓. สร้างสังคมคุณภาพที่ทั่วถึงเท่าเทียมด้วยเทคโนโลยีดิจิทัล** ประชาชนทุกกลุ่มโดยเฉพาะกลุ่มเกษตรกรผู้ที่อยู่ห่างไกล ผู้สูงอายุ ผู้ด้อยโอกาส คนพิการ สามารถเข้าถึงและใช้ประโยชน์จากบริการของรัฐผ่านเทคโนโลยีดิจิทัล ประชาชนมีความรู้เท่าทันข้อมูลข่าวสารและมีทักษะในการใช้ประโยชน์จากเทคโนโลยีอย่างมีความรับผิดชอบต่อสังคม เป็นการสร้างสังคมที่มีคุณภาพลดความเหลื่อมล้ำทางโอกาส ยกระดับคุณภาพชีวิตของทุกกลุ่มผ่านบริการดิจิทัลของรัฐ

**๔. ปรับเปลี่ยนภาครัฐสู่การเป็นรัฐบาลดิจิทัล** นำเทคโนโลยีดิจิทัลมาใช้ในการปรับปรุงประสิทธิภาพการบริหารจัดการภาครัฐ พัฒนาสู่การเป็นรัฐบาลดิจิทัล หลอมรวมการทำงานภาครัฐเสมือนเป็นองค์กรเดียวกัน ประชาชนมีส่วนร่วมในการกำหนดแนวทางการพัฒนาประเทศ บริการภาครัฐมีธรรมาภิบาล สามารถบริการประชาชนแบบเบ็ดเสร็จ ณ จุดเดียว ผ่านระบบเชื่อมโยง

ข้อมูลอัตโนมัติ การเปิดเผยข้อมูลภาครัฐไม่กระทบต่อสิทธิส่วนบุคคล ให้ความสำคัญกับการรักษาความปลอดภัยไซเบอร์

**๕. พัฒนากำลังคนให้พร้อมเข้าสู่ยุคเศรษฐกิจและสังคมดิจิทัล** สร้างและพัฒนาบุคลากรผู้ทำงานให้มีความสามารถในการสร้างสรรค์และใช้เทคโนโลยีอย่างชาญฉลาดในการประกอบอาชีพ สร้างให้เกิดการจ้างงานที่มีคุณค่าสูงรองรับการพัฒนาประเทศ เกิดการจ้างงานแบบใหม่จากการพัฒนาเทคโนโลยี ผู้บริหารระดับสูงสามารถวางแผนยุทธศาสตร์นำเทคโนโลยีไปใช้ในการพัฒนาองค์กร

**๖. สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล** กฎหมาย ระเบียบ กติกาต่างๆ มีประสิทธิภาพทันสมัยสอดคล้องกับหลักสากล สร้างความปลอดภัยในข้อมูลข่าวสาร คุ้มครองสิทธิให้กับผู้ใช้งานเพื่อให้เกิดความสะดวก ลดอุปสรรคในการประกอบกิจกรรมที่เกี่ยวข้องการกับใช้เอกสารอิเล็กทรอนิกส์ ไม่ต้องยื่นแบบฟอร์มกระดาษในการทำธุรกรรมต่างๆ เกิดความมั่นคงปลอดภัยเพียงพอต่อการค้าและการลงทุน

## กลไกการขับเคลื่อน

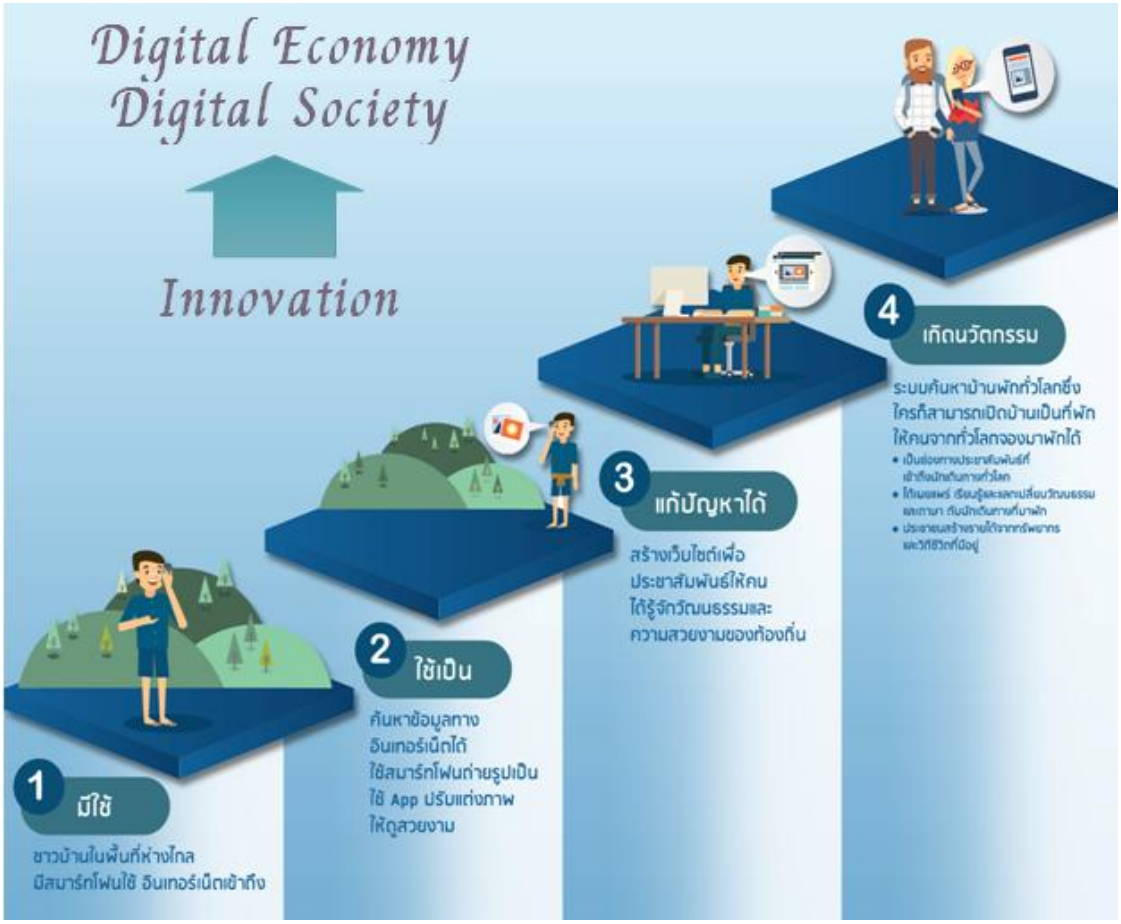
เพื่อเป็นการวางรากฐานให้พร้อมรับการเปลี่ยนแปลงที่เกิดจากการนำเทคโนโลยีดิจิทัลมาประยุกต์ใช้ภายใต้นโยบายการขับเคลื่อนประเทศไทย จะมีกลไกในการทำงานและติดตามผล ได้แก่ การขับเคลื่อนด้วยกิจกรรม การขับเคลื่อนภายใต้การเปลี่ยนแปลงโครงสร้างเชิงสถาบัน การบูรณาการและการจัดสรรงบประมาณ และการติดตามความก้าวหน้าซึ่งมีรายละเอียด ได้แก่

**๑ การขับเคลื่อนด้วยกิจกรรมด้านโครงสร้างพื้นฐาน**เป็นการขยายเครือข่ายอินเตอร์เน็ตความเร็วสูงให้ครอบคลุมทุกหมู่บ้านทั่วประเทศ ยกระดับโครงสร้างพื้นฐานให้มีเครือข่ายเชื่อมต่อโดยตรงกับศูนย์กลางการแลกเปลี่ยนข้อมูลอินเตอร์เน็ตของโลกให้มีเสถียรภาพและความจุเพียงพอ ลดต้นทุนการเชื่อมต่อระหว่างประเทศเพื่อให้สามารถลดต้นทุนเพิ่มประสิทธิภาพในการแข่งขัน มีกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เป็นผู้รับผิดชอบดูแล

ด้านเศรษฐกิจดิจิทัลเป็นการสร้างความเข็มแข็งให้กับเศรษฐกิจฐานราก โดยการเพิ่มโอกาสการสร้างรายได้ให้กับชุมชน ยกระดับการประกอบอาชีพด้วยการส่งเสริมให้ประชาชนในชุมชนมีโอกาสเรียนรู้วิธีการค้าขายผ่านพาณิชย์อิเล็กทรอนิกส์ การเพิ่มขีดความสามารถในการแข่งขันให้กับภาคธุรกิจไทยด้วยการพัฒนาปรับปรุงกระบวนการดำเนินธุรกิจในระดับองค์กร สร้างกลไกและยกระดับความเชื่อมั่นให้กับสินค้าไทย สนับสนุนอุตสาหกรรมเทคโนโลยีและสื่อสร้างสรรค์ ผลักดันการพัฒนาคลัสเตอร์ดิจิทัลตามนโยบายส่งเสริม เขตเศรษฐกิจพิเศษ เพื่อให้เป็นฐานการแลกเปลี่ยนองค์ความรู้และการถ่ายทอดเทคโนโลยีระหว่างภาครัฐ ภาคเอกชน และสถาบันการศึกษา พัฒนากำลังคน

ทางด้านดิจิทัลในธุรกิจเทคโนโลยีดิจิทัล เพื่อให้มีทักษะ ความเชี่ยวชาญในการต่อยอดนวัตกรรม และสร้างสินค้าและบริการรูปแบบใหม่ มีกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงวัฒนธรรม กระทรวงมหาดไทย และกระทรวงวิทยาศาสตร์และเทคโนโลยีเป็นผู้รับผิดชอบดูแล

แผนภาพที่ ๒ - ๓ Digital Economy Digital Society




ที่มา : กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ด้านสังคมดิจิทัลเป็นการพัฒนาเครือข่ายดิจิทัลชุมชน มีการจัดกิจกรรมเชิงเศรษฐกิจอย่างต่อเนื่อง เช่น การเปิดร้านค้าออนไลน์ การปรับปรุงสินค้าและบริการควบคู่กับการจัดสภาพแวดล้อมการเรียนรู้ตลอดชีวิตที่เอื้อต่อการเรียนรู้ทุกที่ทุกเวลา เพื่อให้ประชาชนมีความรู้เท่าทันและใช้ประโยชน์จากเทคโนโลยีเป็นฐานรากของการพัฒนาที่ยั่งยืน ส่งเสริมให้ประชาชนทุกกลุ่มมีช่องทางในการเรียนรู้ตลอดชีวิต พื้นที่ชายขอบของประเทศซึ่งห่างไกลไม่มีไฟฟ้า สัญญาณอินเตอร์เน็ต สัญญาณโทรศัพท์มือถือ ต้องได้รับโอกาสเข้าถึงข้อมูลความรู้มากยิ่งขึ้น ส่งเสริมการใช้ดิจิทัลอย่างสร้างสรรค์รับผิดชอบต่อสังคม รณรงค์และส่งเสริมทักษะดิจิทัลให้ประชาชนเข้าถึง เรียนรู้และใช้ประโยชน์จากการใช้เทคโนโลยีอย่างปลอดภัย สร้างสรรค์ มีจริยธรรม ตระหนักถึงผลกระทบต่อสังคม สร้างเมืองปลอดภัยน่าอยู่ด้วยการเชื่อมโยง CCTV ป้องกันอาชญากรรมเชิงรุก รายงานสภาพจราจรแบบ

Realtime มีกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงมหาดไทย กระทรวงศึกษาธิการ เป็นผู้ดูแลรับผิดชอบ

ด้านบริการภาครัฐเป็นการยกระดับคุณภาพงานปรับกระบวนการดำเนินการภาครัฐโดยนำเทคโนโลยีดิจิทัลมาใช้ในการพัฒนาระบบสนับสนุนงานบริการประชาชน บูรณาการข้อมูลและระบบงาน สนับสนุนมาตรการและนโยบายผ่านอุปกรณ์สื่อสารแบบเคลื่อนที่ ลดเอกสารสำเนาที่ซ้ำซ้อน ผลักดันชุดกฎหมายที่เกี่ยวกับการส่งเสริมและพัฒนาเศรษฐกิจและสังคมดิจิทัล หน่วยงานภาครัฐทุกหน่วยต้องมีส่วนรับผิดชอบ

**๒. กลไกการขับเคลื่อนภายใต้การเปลี่ยนโครงสร้างเชิงสถาบัน** เป็นการปรับปรุงรูปแบบและวิธีการทำงานของรัฐที่จะต้องเปลี่ยนแปลงจากรูปแบบเดิมที่มีโครงสร้างขนาดใหญ่ ยึดกฎระเบียบขั้นตอนการทำงานที่มีความชัดเจน ผูกขาดการให้บริการสาธารณะ เป็นการยกระดับประสิทธิภาพ ประสิทธิผล การให้บริการสาธารณะที่รวดเร็วโปร่งใสมีคุณภาพใช้ได้หลายช่องทางไม่จำกัดด้วยสถานที่ เวลา กระจายอำนาจ ลดกระบวนการขั้นตอนการทำงาน ซึ่งต้องมีหน่วยงานกลางเพื่อทำหน้าที่กำหนดนโยบายขับเคลื่อนให้การพัฒนาเป็นเอกภาพ หน่วยงานใหม่ควรมีเท่าที่จำเป็นมีโครงสร้างที่ยืดหยุ่นเน้นเป้าหมายมากกว่ากระบวนการ ไม่ยึดติดกับกฎระเบียบ มีอิสระและอำนาจการตัดสินใจภายใต้กรอบการดูแลและตรวจสอบ เพื่อการส่งมอบงานที่มีประสิทธิภาพ คุณภาพ รวดเร็ว

**๓. กลไกการบูรณาการและการจัดสรรทรัพยากร** ภาครัฐจำเป็นต้องบูรณาการการทำงานร่วมกันในลักษณะที่เป็นองค์รวมแทนการทำงานแบบแยกส่วน เพื่อให้กลไกต่างๆ ทำงานอย่างมีประสิทธิภาพ เชื่อมโยงกันเพื่อการใช้ทรัพยากรร่วมกัน ลดต้นทุน รวมถึงการนำระบบเทคโนโลยีสารสนเทศมาใช้เพื่อให้บริการสาธารณะแก่ประชาชน การขับเคลื่อนจำเป็นต้องรวดเร็วสอดคล้องกับพลวัตของเทคโนโลยี มีกองทุนสนับสนุนการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม

**๔. กลไกลติดตามความก้าวหน้าของแผนงาน** เพื่อให้การขับเคลื่อนแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมเกิดประสิทธิภาพตามเป้าหมายจำต้องมีการติดตาม ตรวจสอบ ประเมินผล เมื่อพบปัญหาอุปสรรคข้อขัดข้องต้องมีกลไกช่วยเหลือจัดสรรทรัพยากรตามความจำเป็นอย่างทันเวลา เปิดโอกาสให้ทุกภาคส่วนมีส่วนร่วม

## มติคณะรัฐมนตรีและความเห็นจากผู้มีส่วนได้เสีย

ด้วยคณะรัฐมนตรีมุ่งเน้นนโยบายการเพิ่มศักยภาพทางเศรษฐกิจของประเทศ โดยให้มีการส่งเสริมภาคเศรษฐกิจดิจิทัล และวางรากฐานของเศรษฐกิจดิจิทัลให้เริ่มขับเคลื่อนได้อย่างจริงจัง

ซึ่งจะทำให้เศรษฐกิจก้าวหน้าไปได้ทันประเทศต่างๆ สามารถแข่งขันในโลกสมัยใหม่ได้ เทคโนโลยีดิจิทัลสามารถตอบปัญหาความท้าทายเหล่านี้ โดยการเพิ่มขีดความสามารถในการแข่งขันบนเวทีโลก

กรอบยุทธศาสตร์ชาติ ระยะ ๒๐ ปี (พ.ศ.๒๕๕๘ – ๒๕๗๗) กำหนดวิสัยทัศน์ประเทศไทยมีความมั่นคง มั่งคั่ง ยั่งยืน เป็นประเทศพัฒนาแล้วด้วยการพัฒนาตามหลักปรัชญาเศรษฐกิจพอเพียง ทิศทางของแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติฉบับที่ ๑๒ (พ.ศ.๒๕๖๐ – ๒๕๖๔) ได้กำหนดแนวทางการพัฒนาเพื่อยกระดับศักยภาพการแข่งขันและการหลุดพ้นกับดักรายได้ปานกลางสู่รายได้สูง โดยมีแนวทางการพัฒนาเพื่อปรับปรุงระบบโทรคมนาคมของประเทศ ยกระดับและพัฒนาสมรรถนะแรงงานไทยด้วยเทคโนโลยี เร่งรัดให้แรงงานทั้งระบบมีการเรียนรู้ขั้นพื้นฐาน เพื่อแข่งขันในตลาดแรงงาน พัฒนาผู้ประกอบการให้มีความยืดหยุ่นสามารถปรับตัวและดำเนินธุรกิจท่ามกลางการดำเนินนโยบายและมาตรการกีดกันทางการค้าในรูปแบบต่างๆ พัฒนาต่อยอดอุตสาหกรรมและบริการเพื่อเข้าสู่การเป็นศูนย์กลางการผลิต บริการและอุตสาหกรรมดิจิทัล ซึ่งผลกระทบของแผนดิจิทัลเพื่อเศรษฐกิจและสังคมกับประเทศไทยที่จะเกิดขึ้นในระยะ ๒๐ ปี สามารถจำแนกออกเป็นสองประการ ได้แก่ ผลกระทบด้านเศรษฐกิจ และผลกระทบด้านสังคม

ผลกระทบด้านเศรษฐกิจ การวางรากฐานของประเทศด้วยการขับเคลื่อนนโยบายเศรษฐกิจดิจิทัลภายใต้แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม นับเป็นพื้นฐานสำคัญในการส่งเสริมศักยภาพในการแข่งขันของประเทศ เพิ่มขีดความสามารถในการแข่งขันของผู้ประกอบการ เสริมสร้างความเข็มแข็งแก่วิสาหกิจขนาดกลางและขนาดย่อย พัฒนาความสามารถในการผลิตและการแข่งขันในตลาดโลก การดำเนินการตามร่างแผนงานจะช่วยประหยัดงบประมาณของประเทศด้านสื่อสารและเทคโนโลยีสารสนเทศ

ผลกระทบด้านสังคม การดำเนินการตามแผนจะมีการกระจายโครงสร้างพื้นฐานสารสนเทศอย่างทั่วถึงและเท่าเทียมกัน การใช้เทคโนโลยีสร้างโอกาสด้านต่างๆ ให้กับประชาชน เพื่อลดความเหลื่อมล้ำทางสังคม เช่นการบูรณาการระบบสารสนเทศเพื่อการศึกษา การเรียนรู้ และพัฒนาศูนย์ดิจิทัลชุมชน การสร้างโอกาสในการเรียนรู้ตลอดชีวิต การได้รับบริการสาธารณะต่างๆ ของภาครัฐผ่านโครงสร้างพื้นฐานดิจิทัลดังกล่าว จะช่วยยกระดับคุณภาพชีวิต และทำให้การติดต่อสื่อสารระหว่างประชาชนกับประชาชน และประชาชนกับภาครัฐสะดวกรวดเร็วยิ่งขึ้น เพิ่มโอกาสให้ประชาชนที่มีส่วนร่วมในการกำหนดและสะท้อนความต้องการต่อการบริการภาครัฐ

คณะรัฐมนตรีได้ประชุมปรึกษากันในเรื่องแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม ตามที่กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เมื่อวันที่ ๕ เม.ย.๕๙ เห็นชอบให้

๑. กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เป็นหน่วยงานหลักในการขับเคลื่อนแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม รวมทั้งจัดทำแผนปฏิบัติการเพื่อขับเคลื่อนการพัฒนายุทธศาสตร์ร่วมกับหน่วยงานที่เกี่ยวข้อง

๒. ให้ทุกกระทรวง กรม รัฐวิสาหกิจ องค์กรปกครองท้องถิ่น หน่วยงานของรัฐ ไปพิจารณาจัดทำแผนปฏิบัติราชการ และคำของบประมาณรายจ่ายประจำปีของหน่วยงานให้สอดคล้องกับแผนดังกล่าวและสอดคล้องกัน

๓. ให้ทุกกระทรวง กรม รัฐวิสาหกิจ องค์กรปกครองท้องถิ่น หน่วยงานของรัฐ จัดทำแผนปฏิบัติการดิจิทัล ระยะ ๓ ปี ของหน่วยงานแทนการจัดทำแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารเดิม ยกเลิกมติ ครม. ๙ มิ.ย.๔๑ แผนแม่บทเทคโนโลยีสารสนเทศ

๔. มอบหมายให้สำนักงบประมาณ สำนักงานคณะกรรมการข้าราชการพลเรือน สำนักงานคณะกรรมการพัฒนาระบบราชการ และหน่วยงานที่เกี่ยวข้องให้การสนับสนุนงบประมาณ บุคลากร การทบทวนโครงสร้างของส่วนราชการ การปรับปรุงระเบียบ กำหนดตัวชี้วัด ติดตามประเมินผลหน่วยงานภาครัฐ เพื่อให้เกิดประสิทธิภาพตามที่กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเสนอ

นอกจากคณะรัฐมนตรีได้เห็นชอบแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมแล้ว ยังให้กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารรับความเห็นของกระทรวงกลาโหม กระทรวงการคลัง กระทรวงการท่องเที่ยวและกีฬา กระทรวงคมนาคม กระทรวงยุติธรรม กระทรวงแรงงาน กระทรวงวิทยาศาสตร์และเทคโนโลยี กระทรวงสาธารณสุข สำนักงบประมาณ สำนักงานคณะกรรมการกฤษฎีกา สำงานงาน ก.พ. สำนักงาน ก.พ.ร. สำนักงานคณะกรรมการกิจการกระจายเสียงกิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ ธนาคารแห่งประเทศไทย ไปพิจารณาดำเนินการในส่วนที่เกี่ยวข้องด้วย ดังนี้

**๑. กระทรวงกลาโหม** ควรพิจารณาเรื่องการลดภาษีด้านเทคโนโลยีสารสนเทศ เพื่อเป็นการส่งเสริมและเพิ่มประสิทธิภาพในการดำเนินธุรกิจ ตลอดจนพัฒนาไปสู่การแข่งขันธุรกิจในระยะยาว ซึ่งจะส่งผลให้หน่วยราชการสามารถปรับลดการใช้จ่ายงบประมาณด้านการจัดหาอุปกรณ์ที่จำเป็นต่อการดำเนินการได้ ยุทธศาสตร์การยกระดับความมั่นคง และเพิ่มความปลอดภัยของประชาชน ควรมีหน่วยงานที่รับผิดชอบด้านการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ในระดับประเทศ ควรส่งเสริมให้มีการพัฒนาระบบปฏิบัติการโปรแกรมด้านงานเอกสารที่พัฒนาโดยประเทศไทย ส่งเสริมให้เกิดอุตสาหกรรมซอฟต์แวร์

**๒. กระทรวงการคลัง** หากสามารถดำเนินการตามแผนฯ ได้จะเป็นการเพิ่มขีดความสามารถการแข่งขันของประเทศในด้านต่างๆ เพิ่มประสิทธิภาพการทำงานของรัฐ กระทรวงการคลังจะเป็นปัจจัยสนับสนุนการขยายฐานภาษีและการจัดเก็บภาษีให้มีประสิทธิภาพเพิ่มขึ้น การดำเนินการจำเป็นต้องบูรณาการการทำงานของหน่วยงานจำนวนมาก การจัดทำแผนงาน วิธีการดำเนินการ ระยะเวลาและกรอบวงเงินงบประมาณ จะต้องมีความชัดเจนและไม่ทับซ้อนกับงานของส่วนราชการที่กำลังดำเนินการอยู่

**๓. กระทรวงการท่องเที่ยวและกีฬา** มีการดำเนินงานตามบทบาทภารกิจของกระทรวง ภายใต้ยุทธศาสตร์การท่องเที่ยวไทย พ.ศ.๒๕๕๙ – ๒๕๖๐ ที่ให้ความสำคัญกับการพัฒนาเศรษฐกิจดิจิทัล ได้แก่การพัฒนาช่องทางบริการของหน่วยงานภายในผ่านระบบดิจิทัล (e-Service Postal) และการพัฒนาฐานข้อมูลภาครัฐที่มีมาตรฐาน รวมถึงพัฒนาการดำเนินงานของภาครัฐให้มีประสิทธิภาพ โดยอาศัยเทคโนโลยีร่วมกัน โดยกระทรวงการท่องเที่ยว และกีฬา มีการพัฒนาระบบ Tourism Gateway ระบบ Tourism Intelligence Centre ซึ่งสอดคล้องกับแนวทาง การกำหนดนโยบายผลักดันเศรษฐกิจดิจิทัล ตลอดจนการสร้างความร่วมมือในการพัฒนาธุรกิจดิจิทัล ระหว่างรัฐและเอกชน การขับเคลื่อนเศรษฐกิจด้วยเทคโนโลยีดิจิทัล การปรับเปลี่ยนภาครัฐสู่การเป็นรัฐบาลดิจิทัล และการสร้างความเชื่อมั่นในการใช้เทคโนโลยี เพื่อส่งเสริมเศรษฐกิจดิจิทัลในอุตสาหกรรมการท่องเที่ยวให้เกิดผลอย่างเป็นรูปธรรม

**๔. กระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม** เห็นด้วยกับแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม เนื่องจากเป็นการเพิ่มศักยภาพทางเศรษฐกิจของประเทศ ให้การขับเคลื่อนนโยบายเศรษฐกิจดิจิทัลโดยภาครัฐ ภาคเอกชน และภาคประชาชน เป็นไปในทิศทางเดียวกันอย่างมีเอกภาพ

**๕. กระทรวงพลังงาน** เห็นด้วยกับแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม เนื่องจากเห็นว่าสามารถใช้ประโยชน์จากเทคโนโลยีดิจิทัลอย่างเต็มศักยภาพ เพื่อขับเคลื่อนการพัฒนาเศรษฐกิจและสังคมของประเทศสู่ความมั่นคง มั่งคั่ง และยั่งยืน ยกระดับภาครัฐสู่การเป็นรัฐบาลดิจิทัลที่มีการบูรณาการระหว่างหน่วยงานมีประชาชนเป็นศูนย์กลาง

**๖. กระทรวงมหาดไทย** เห็นด้วยตามที่กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเสนอ

**๗. กระทรวงยุติธรรม** เห็นด้วยและเห็นควรเร่งพัฒนาปรับปรุงกฎหมายที่เกี่ยวข้องโดยเร่งด่วน เพื่อไม่ให้เกิดอุปสรรคในการนำไปปฏิบัติ และมีข้อเสนอเพิ่มเติม ได้แก่

๗.๑ การที่จะทำให้ข้อมูลของหน่วยงานรัฐมีการเชื่อมโยงและสามารถแลกเปลี่ยนข้อมูลระหว่างกันได้ จำเป็นต้องพัฒนาและจัดเก็บข้อมูลในรูปแบบอิเล็กทรอนิกส์ ทั้งข้อมูลที่ใช้ในการปฏิบัติงานประจำและข้อมูลการให้บริการประชาชน

๗.๒ หน่วยงานภาครัฐควรเร่งพัฒนาและปรับปรุงการทำงานของตนเอง โดยการพิจารณาลดขั้นตอนการทำงานที่ซ้ำซ้อน นำเทคโนโลยีมาใช้ในการปฏิบัติงาน ทั้ง Back office และ Front office เพื่อเพิ่มประสิทธิภาพการทำงานลดการใช้ทรัพยากร

๗.๓ ควรมีการปรับปรุงกฎหมาย กฎ ระเบียบ ที่ล้าสมัย เป็นอุปสรรคต่อการนำเทคโนโลยีมาใช้ในการปฏิบัติงานและบริการประชาชน

๗.๔ ควรให้ความรู้แก่แประชาชน นักเรียน นักศึกษา ให้มีความรู้เท่าทัน ตระหนักถึงความปลอดภัยในเครือข่ายสังคมออนไลน์

๗.๕ การพัฒนาระบบฐานข้อมูลกลางภาครัฐ ควรมีหน่วยงานกลางจัดลำดับความสำคัญเร่งด่วนกำหนดหลักเกณฑ์มาตรฐานและเทคโนโลยีที่ใช้ ประสานงานความร่วมมือระหว่างหน่วยงาน

**๘. กระทรวงแรงงาน** เห็นด้วยเนื่องจากมีการกำหนดเป้าหมาย และมีทิศทางดำเนินการที่ชัดเจนที่จะตอบสนองต่อนโยบายรัฐบาล ยกระดับและพัฒนาขีดความสามารถในการแข่งขันของภาคธุรกิจและความเป็นอยู่ที่ดีของประชาชน และมีความเห็นเพิ่มเติมได้แก่

๘.๑ ด้านข้อมูล หน่วยงานภาครัฐควรบูรณาการเชื่อมโยงข้อมูลอย่างจริงจังโดยผ่านระบบเชื่อมโยงข้อมูลกลาง มีนโยบายและกฎหมายรองรับ ปรับปรุงกฎระเบียบให้ยืดหยุ่นเพื่อรองรับเทคโนโลยีดิจิทัล และควรแก้ไขกฎหมายที่เป็นอุปสรรคของรัฐในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน

๘.๒ ด้านโครงสร้างส่วนราชการและบุคลากร ควรปรับปรุงโครงสร้างส่วนราชการให้สอดคล้องกับภารกิจงานที่เปลี่ยนแปลงไป พร้อมทั้งจัดสรรบุคลากรที่เหมาะสมให้เพียงพอ และมีแผนพัฒนาศักยภาพบุคลากรอย่างต่อเนื่องให้สามารถรองรับกับภารกิจที่เพิ่มขึ้นได้

๘.๓ ด้านระบบเครือข่ายสื่อสารข้อมูล หน่วยงานภาครัฐควรใช้เครือข่ายสื่อสารข้อมูลของรัฐไม่ควรแยกหน่วยงานดำเนินการ ซึ่งจะทำให้สิ้นเปลืองงบประมาณมาก และต้องจัดหาให้รองรับการใช้งานที่เหมาะสมตามความจำเป็นของแต่ละหน่วยงาน

๘.๔ ด้านการให้บริการความช่วยเหลือแบบบูรณาการเชิงรุก เห็นควรเพิ่มในส่วนของงานประกันสังคม ซึ่งสามารถบูรณาการงานบริการให้กับกลุ่มเป้าหมายที่เป็นผู้ประกันตน ทั้งในและนอกระบบด้วย เพื่อให้งานบริการภาครัฐมีความครอบคลุมทั่วถึงครบวงจร

๘.๕ ด้านการบูรณาการตลาดแรงงานแบบครบวงจร เห็นว่ามีขอบเขตการดำเนินงานค่อนข้างจำกัด ซึ่งในความเป็นจริงการให้บริการของกระทรวงแรงงานมีขอบเขตที่กว้างและหลากหลาย จึงเห็นควรปรับเปลี่ยนเป็นการบูรณาการการให้บริการด้านแรงงานแบบครบวงจร เพื่อให้ครอบคลุมในทุกมิติด้านแรงงาน

**๙. กระทรวงวัฒนธรรม** เห็นชอบด้วยโดยไม่มีความเห็นเพิ่มเติม

**๑๐. กระทรวงวิทยาศาสตร์และเทคโนโลยี** เห็นด้วยในหลักการต่อแผนดังกล่าว เนื่องจากเป็นการกำหนดกรอบและทิศทางในการผลักดันให้เทคโนโลยีดิจิทัล เป็นเครื่องมือและกลไกสำคัญในการพัฒนาเศรษฐกิจและสังคมของประเทศ รวมทั้งมีข้อคิดเห็น ข้อสังเกต เพิ่มเติมดังนี้

๑๐.๑ กลไกการขับเคลื่อนควรมีความชัดเจน โดยเฉพาะหน่วยงานที่จะต้องมีส่วนร่วม รวมถึงการมี Template หรือวิธีการในการจัดทำแผนปฏิบัติการของหน่วยงาน

๑๐.๒ ควรปรับแผนระยะ ๓ ปี ในประเด็นต่างๆ เช่น

๑๐.๒.๑ ความสอดคล้องของยุทธศาสตร์การเปลี่ยนภาครัฐสู่การเป็นรัฐบาลดิจิทัล

๑๐.๒.๒ เป้าหมายยุทธศาสตร์และตัวชี้วัดควรมีความชัดเจน

๑๐.๒.๓ ความเชื่อมโยงของยุทธศาสตร์ มาตรการต่างๆ ที่จะทำให้ไม่เกิดปัญหาการบูรณาการทรัพยากร และการใช้ข้อมูลข้ามหน่วยงาน

๑๐.๒.๔ ความปลอดภัยของระบบเครือข่าย

**๑๑. กระทรวงสาธารณสุข** ระบบบริการสุขภาพของประเทศไทยโดยสำนักงานปลัดกระทรวงสาธารณสุข มีสถานพยาบาลในสังกัดมากกว่า ๑,๑๐๐ แห่ง ครอบคลุมพื้นที่ทุกตำบลของประเทศไทย ดูแลสุขภาพของประชาชนในการรักษาส่งเสริมและป้องกันสุขภาพ ซึ่งทุกสถานพยาบาลใช้เทคโนโลยีสารสนเทศในการให้บริการประชาชนอยู่แล้ว จึงขอให้เพิ่มเติมในประเด็นของตำแหน่งงานด้านเทคโนโลยีสารสนเทศรองรับในหน่วยบริการสาธารณสุข มีแผนการกระจายบุคลากร และกำหนดค่าตอบแทนเพื่อเป็นแรงจูงใจกับผู้ทำงานภาครัฐ

**๑๒. กระทรวงอุตสาหกรรม** เห็นด้วยเนื่องจากมีการวางแผนการพัฒนาที่ครอบคลุมทุกด้าน ทั้งการพัฒนาโครงสร้างพื้นฐาน การพัฒนาโปรแกรม และการพัฒนาบุคลากร ซึ่งสามารถรองรับการเปลี่ยนแปลงด้านเทคโนโลยีดิจิทัลอย่างมีศักยภาพ

**๑๓. สำนักงบประมาณ** เห็นว่าค่าใช้จ่ายที่จะเกิดขึ้นเพื่อสนับสนุนการดำเนินการตามแผนควรให้หน่วยงานแปลงแผนไปสู่การปฏิบัติที่ชัดเจน ทำงบประมาณในลักษณะบูรณาการเชิงยุทธศาสตร์และสอดคล้องกับภารกิจของหน่วยงานตามความจำเป็น

**๑๔. สำนักงาน กสทช.** มีประเด็นที่ต้องพิจารณา ๔ ข้อ ได้แก่

๑๔.๑ ประเด็นความทับซ้อนกับจำนวนหน้าที่ขององค์กรกำกับดูแลตามกฎหมาย ร่างแผนดังกล่าวมีหลายประเด็นที่ทับซ้อนกับจำนวนหน้าที่ของ กสทช.โดยเนื้อหาบางส่วน ในการพัฒนาโครงสร้างพื้นฐานดิจิทัลประสิทธิภาพสูงให้ครอบคลุมทั่วประเทศ

๑๔.๑.๑ การจัดให้มีนโยบายและแผนพัฒนาการบริหารจัดการโครงสร้างพื้นฐาน คลื่นความถี่ และการหลอมรวมของเทคโนโลยีในอนาคต กับการกำหนดนโยบายด้านโครงสร้างพื้นฐาน และการใช้คลื่นความถี่ให้เหมาะสมเพียงพอกับภารกิจเชิงพาณิชย์ การบริการสาธารณะด้านความมั่นคง และการบริหารจัดการภาวะวิกฤติ เนื่องจากในการเรียกคืนคลื่นความถี่เพื่อนำมาจัดสรรใหม่ ยังมีข้อจำกัดจากหน่วยงานที่ถือครองโดยไม่ได้ใช้ประโยชน์

๑๔.๑.๒ การปรับปรุงกฎหมายที่เกี่ยวข้อง เช่นกฎหมายในเรื่องการกำกับดูแลเพื่อให้เกิดเครือข่ายที่เป็นกลาง และรองรับการหลอมรวมของเทคโนโลยีและบริการ ให้สอดคล้องกับมาตรฐานสากลและทันต่อการเปลี่ยนแปลงของเทคโนโลยี เหล่านี้ กสทช. ได้กำหนดหลักเกณฑ์ไว้แล้ว เช่น เรื่องการใช้โครงสร้างพื้นฐานโทรคมนาคมร่วมกันสำหรับโครงข่ายโทรศัพท์เคลื่อนที่ เรื่อง

แผนการจัดให้มีบริการโทรคมนาคมพื้นฐานโดยทั่วถึงและบริการเพื่อสังคม เรื่องหลักเกณฑ์และวิธีการเกี่ยวกับการใช้สิทธิในการปักหรือตั้งเสา หรือเดินสาย วางท่อ หรือติดตั้งอุปกรณ์ประกอบในการให้บริการโทรคมนาคม

๑๔.๒ ประเด็นการขาดความสอดคล้องกับร่างแผนพัฒนาดิจิทัลฯ เป้าหมายตัวชี้วัด ยุทธศาสตร์ และแนวทางการขับเคลื่อนในแผนงานปฏิรูปรัฐวิสาหกิจโทรคมนาคม ควรมีการระบุปัจจัยแห่งความสำเร็จ ตัวชี้วัดที่ประเมินแล้วไม่สามารถวัดผลได้ สร้างเป็นรูปธรรม เช่น ประชาชนทุกคนต้องสามารถเข้าถึงอินเตอร์เน็ตความเร็วสูง ประชาชนทุกคนมีความตระหนัก ความรู้ เข้าใจ ทักษะการใช้เทคโนโลยีดิจิทัลให้เกิดประโยชน์และสร้างสรรค์

๑๔.๓ ประเด็นการกำหนดเจ้าภาพเพื่อดำเนินการ หมายถึงผู้รับผิดชอบต่อความสำเร็จของแผน โดยเฉพาะนโยบายและแผนบริหารจัดการโครงสร้างพื้นฐาน เพื่อรองรับการขยายตัวของอุปกรณ์เชื่อมโยง และการหลอมรวมของเทคโนโลยีปัจจุบันกับอนาคต นโยบายการบริหารกิจการดาวเทียมของประเทศ ซึ่งครอบคลุมถึงการใช้วงโคจรดาวเทียมและการบริการข้อมูลผ่านดาวเทียม เพื่อให้มีการแข่งขันในการเข้าถึงวงโคจรดาวเทียมค้างฟ้า และพัฒนากิจการบริการข้อมูลผ่านดาวเทียมที่ถูกกฎหมาย

๑๔.๔ การกำหนดผู้ดำเนินการหลัก ซึ่ง กสทช. เห็นว่า ด้านโครงสร้างพื้นฐานดิจิทัล กสทช. มีบทบาทในการส่งเสริมการพัฒนา และขยายโครงข่ายอินเตอร์เน็ตความเร็วสูง ทั้งในระดับประเทศและระหว่างประเทศ ไม่ว่าจะเป็นการกำหนดเงื่อนไขแนบท้ายใบอนุญาตประกอบกิจการโทรคมนาคม การกำหนดอัตราค่าใช้หรือค่าเชื่อมต่อโครงข่ายในการประกอบกิจการ

**๑๕. ธนาคารแห่งประเทศไทย** เห็นว่าหลักการของแผนจะมีส่วนช่วยยกระดับคุณภาพชีวิตประชาชน เพิ่มประสิทธิภาพ ภาครัฐและธุรกิจ เพิ่มขีดความสามารถในการแข่งขันของประเทศไทย และมีความเห็นเพิ่มเติมได้แก่

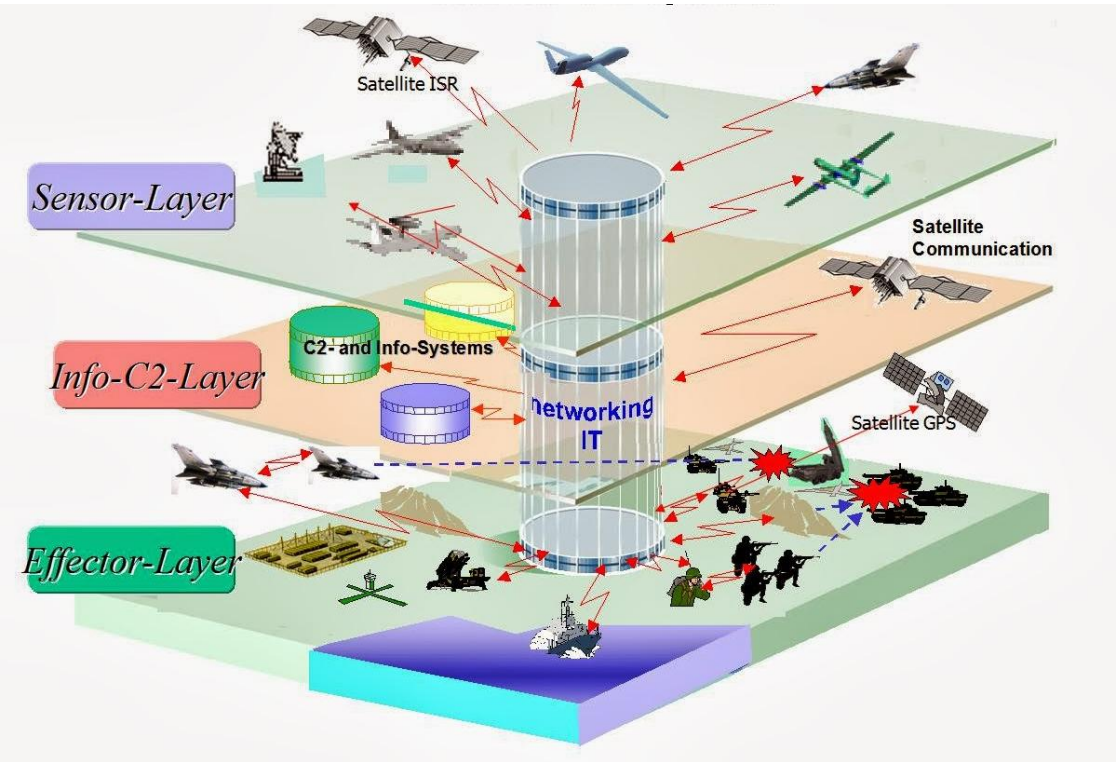
๑๕.๑ การรักษาความปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ เป็นความท้าทายในยุค Digital Economy และเพื่อให้การดูแลครอบคลุมทุกภาคส่วน ภาครัฐอาจพิจารณาขอบเขตการดูแลให้มีความเชื่อมโยงกันของภาครัฐกับเอกชน ให้เป็นไปตามมาตรฐานสากล เพื่อป้องกันและแก้ปัญหาอย่างมีประสิทธิภาพ

๑๕.๒ การจัดตั้งหน่วยงานบริหารจัดการข้อมูลทางการเงินอย่างบูรณาการ มีฐานข้อมูลกลาง(Public Credit Registry) ซึ่งครอบคลุมข้อมูลทางการเงินที่ยังกระจัดกระจายอยู่ เช่น การชำระค่าสาธารณูปโภคพื้นฐาน ข้อมูลสหกรณ์ ประกันภัย ระบบบำเหน็จบำนาญของกองทุนต่างๆ เพื่อการวิเคราะห์เชิงลึก สามารถให้ความช่วยเหลือแก่ประชาชนและภาคธุรกิจอย่างตรงกลุ่มเป้าหมาย สนับสนุนการเข้าถึงแหล่งเงินทุน SME

**๑๖. กระทรวงพาณิชย์** มีความเห็นเกี่ยวกับการยืนยันตนผ่านบัญชีผู้ใช้อิเล็กทรอนิกส์กลาง ควรมีหน่วยงานเพื่อความมีมาตรฐานความปลอดภัยในการทำธุรกรรม

## กรอบแนวคิดของการวิจัย

แผนภาพที่ ๒ - ๔ : Network Centric




ที่มา : The Center for Digital Intelligence

การวิจัยครั้งนี้ มีกรอบแนวคิดการวิจัยในเรื่องของสงครามที่ใช้เครือข่ายเป็นศูนย์กลาง ซึ่งมีพื้นฐานการใช้เครือข่ายคอมพิวเตอร์เริ่มด้วยการพัฒนาโครงข่ายสารสนเทศ ที่เชื่อมต่อข้อมูลทุกภาคส่วนเข้าด้วยกัน ได้แก่ การข่าว การรบ ภารกิจที่จะต้องปฏิบัติเป็นประจำ เซนเซอร์ภาคพื้นดินหรือดาวเทียมที่เชื่อมต่อกันผ่านระบบเครือข่ายเพื่อให้การประเมินผล และตัดสินใจ รวมถึงการมอบหมายหน้าที่ หรือสั่งการ โดยใช้ทรัพยากรที่มีเพื่อตอบโต้ และจากความก้าวหน้าของเทคโนโลยีที่เกิดขึ้น จะส่งผลกระทบกับการปฏิบัติการทางทหาร ทั้งในยามปกติ และยามสงคราม ในการปฏิบัติการทางทหาร ปัจจัยของความสำเร็จคือกระบวนการตัดสินใจของผู้บังคับบัญชา ซึ่งมีพื้นฐานจากข้อมูลข่าวสารการรบที่รวดเร็ว ถูกต้อง เชื่อถือได้ เหมาะสมกับสถานการณ์ฝ่ายที่สามารถใช้ผลประโยชน์จากความได้เปรียบนี้จะประสพความสำเร็จ จนกล่าวได้ว่าความได้เปรียบนี้ เป็นหัวใจหลักในการปฏิบัติการทางทหาร เป็นตัวชี้วัดผลแพ้ชนะของสงครามปัจจุบัน

# สรุป

บริบทของประเทศไทยในยุคดิจิทัล ประชาชนจะมีโอกาสสร้างรายได้จากการนำไอซีทีมาเป็นเครื่องมือสนับสนุนการพัฒนาประเทศ มีอินเตอร์เน็ตความเร็วสูงกระจายอย่างทั่วถึง รวมถึงมีคุณภาพชีวิตที่ดีขึ้น การทำธุรกรรมผ่านทางออนไลน์ จะมีกฎระเบียบที่ใช้ปฏิบัติได้จริง ทันต่อการเปลี่ยนแปลงทางเทคโนโลยี โดยมีเป้าหมายของการพัฒนา ๔ ระยะ ใช้เวลา ๒๐ ปี ผ่านแผนยุทธศาสตร์ ๖ แผน ได้แก่ การพัฒนาโครงสร้างพื้นฐานดิจิทัลประสิทธิภาพสูง การขับเคลื่อนเศรษฐกิจด้วยเทคโนโลยี สร้างสังคมคุณภาพที่ทั่วถึงและเท่าเทียม ปรับเปลี่ยนภาครัฐสู่การเป็นรัฐบาลดิจิทัล พัฒนากำลังคนให้พร้อมเข้าสู่ยุคเศรษฐกิจและสังคมดิจิทัล และการสร้างความเชื่อมั่นในการใช้เทคโนโลยี มีกลไกขับเคลื่อนด้วยกิจกรรมภายใต้การเปลี่ยนแปลงโครงสร้างเชิงสถาบันบูรณาการการจัดสรรทรัพยากร และติดตามความก้าวหน้าของแผนงาน นอกจากนี้คณะรัฐมนตรี และผู้มีส่วนได้เสียต่างก็มีความเห็นสอดคล้องไปในแนวทางเดียวกัน เห็นด้วยกับแผนดังกล่าว ผู้มีส่วนได้เสียบางหน่วยงาน เช่น สำนักงาน กสทช. เห็นว่ามีหลายประเด็นที่ทับซ้อนกับอำนาจหน้าที่ของ กสทช. และหลายหน่วยงานมีความเป็นห่วงในเรื่องของความปลอดภัยไซเบอร์

# บทที่ ๓
# เทคโนโลยีในยุคดิจิทัลไทยแลนด์

คอลัมน์ลึกแต่ไม่ลับหนังสือพิมพ์มติชนสุดสัปดาห์ ประจำเดือนพฤศจิกายน ๒๕๖๐ ความว่า “โครงการเน็ตประชารัฐ รัฐบาลบิ๊กตู่วางเป้าให้ประชาชนไกลปืนเที่ยง มีโอกาสใช้ระบบสื่อสารโทรคมนาคม ทั้งโทรมือถือ อินเตอร์เน็ต เหมือนคนในเมืองตามโมเดลใหม่ “ประเทศไทย 4.0” รองรับแผนยุทธศาสตร์ ๒๐ ปี วันนี้ “เน็ตประชารัฐ” มูลค่า ๔ หมื่นล้านรัฐบาลแบ่งให้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กับ กสทช. ไปจัดทำในพื้นที่ห่างไกลทั่วประเทศ เริ่มเห็นเป็นรูปร่างจับต้องได้แล้ว กระทรวงดีอีสั่งงานให้ทีโอทีไปติดตั้งระบบอินเตอร์เน็ต ๒๔,๗๐๑ หมู่บ้านเกือบเสร็จเต็มที่ ส่วน กสทช. ทำใน ๒ เฟส เฟสแรกเป็นเน็ตชายขอบ ๕ พื้นที่ครอบคลุม ๓,๙๒๐ หมู่บ้านทั่วประเทศ มูลค่า ๑๓,๖๑๔.๖๒ ล้านบาท

การประกวดราคาผ่านราบรื่นสะดวกโยธิน บริษัทแข่งกันเสนอเนื้องานต่ำกว่าราคากลางที่ กสทช. ตั้งไว้ ช่วยประหยัดเงินรัฐอีกกว่า ๖๐๐ ล้านบาท

ส่วนเฟส ๒ วงเงินลงทุนเบื้องต้น ๑๓,๐๐๐ ล้านบาท ในจำนวน ๑๕,๗๓๒ หมู่บ้านเตรียมเปิดให้เอกชนยื่นซองประกวดราคาในเดือนพฤศจิกายนปีนี้

“ฐากร ตัณฑสิทธิ์” เลขาธิการ กสทช. กล่าวว่ามีแผนเตรียมรองรับเน็ตชายขอบไว้ ๕ ปี แต่ละหมู่บ้าน มีจุดบริการไวไฟฟรีทั้งในโรงเรียน สถานีอนามัย ให้ประชาชนเปิดโลกทัศน์ใหม่ๆ ผ่านโครงข่ายโทรคมนาคม ยุคใหม่ เช่น การเรียนการสอนผ่านทางอินเตอร์เน็ตเชื่อมระหว่างโรงเรียนในหมู่บ้านกับสถาบันการศึกษาชั้นนำ การรักษาทางการแพทย์เชื่อมระหว่างสถานีอนามัยในหมู่บ้านชายขอบกับแพทย์ผู้เชี่ยวชาญประจำโรงพยาบาลในกรุงเทพมหานคร ช่วยลดเวลาและค่าใช้จ่ายของผู้ป่วย

การวางเครือข่ายอินเตอร์เน็ตและโทรศัพท์มือถือเคลื่อนที่ในหมู่บ้านชายขอบ ทำให้เกิดธุรกรรมการเงินใหม่ๆ ขึ้น ในแต่ละหมู่บ้านจะมีผู้คิดค้นริเริ่มธุรกิจการค้าใหม่ๆ หรือสตาร์ตอัพผ่านระบบออนไลน์เชื่อมกันทั่วโลก เช่น ท่องเที่ยวเชิงนิเวศน์ โฮมสเตย์ สินค้าโอท็อป ฯลฯ ปลายเดือนธันวาคมปีนี้ เน็ตชายขอบจำนวน ๑๕ เปอร์เซ็นต์ของโครงการทั้งหมดหรือ ๕๘๘ หมู่บ้าน จะเปิดใช้บริการได้ฟรีกลางๆ ปี ๒๕๖๑ คาดว่าโครงการเสร็จสมบูรณ์ ๑๐๐ เปอร์เซ็นต์

กสทช. ประเมินว่าประชาชนใน ๓,๙๒๐ หมูบ้าน จำนวน ๗ แสนครัวเรือน จะร่วมกันใช้เครื่องมือไฮเทคเหมือนๆ กับคนในเมือง แต่ละครัวเรือนคิดสร้างสรรค์หารายได้เพิ่มขึ้นเฉลี่ยแค่

เดือนละ ๑ พันบาท จะเกิดเงินหมุนเวียนในพื้นที่ชายขอบปีละ ๘,๔๐๐ ล้านบาท ๕ ปี เงินสะพัดสูงถึง ๔๒,๐๐๐ ล้านบาท และคุณภาพชีวิตของผู้คนเหล่านี้ดีขึ้นอย่างแน่นอน

“ฐากร” ปิดท้ายว่า การสื่อสารโทรคมนาคมของไทยหยุดชะงักมากว่า ๑๐ปี “คสช.เข้ามาบริหารประเทศจึงเกิดพัฒนาอย่างรวดเร็วชนิดก้าวกระโดด ถ้าไทยเปลี่ยนผ่านเข้าสู่ยุค ๕ จี ผนวกเน็ตประชารัฐ ๔ หมื่นหมู่บ้าน เอกชนอีก ๓๖,๐๑๓ หมู่บ้าน จะเห็นภาพการเชื่อมโยงโครงข่ายสื่อสารโทรคมนาคมทั้งระบบที่ใหญ่มหึมาพร้อมขับเคลื่อนประเทศอย่างมีพลัง”

จากข่าวข้างต้นทำให้พอประเมินได้ว่า เป้าหมายระยะที่ ๑ ใช้ระยะเวลา ๑ ปี ๖ เดือน ของแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม เริ่มเห็นเป็นรูปร่างแล้ว ข้อสังเกตในเรื่องของการซ้ำซ้อนในอำนาจหน้าที่ ได้รับการจัดสรรอย่างลงตัวจนผู้เกี่ยวข้องยอมรับ ซึ่งต่อไปจะกล่าวถึงเทคโนโลยีที่จะเกิดขึ้นในยุคดิจิทัลไทยแลนด์ เทคโนโลยีดังกล่าวไม่ใช่ของใหม่ที่ผู้วิจัยคิดขึ้นเอง แต่เป็นสิ่งที่เกิดขึ้นแล้วในประเทศพัฒนาเป็นไปตามแผนระยะที่ ๔ ที่ต้องการให้ประเทศไทยอยู่ในกลุ่มประเทศพัฒนาแล้ว

## กล่าวโดยทั่วไป

สหภาพโทรคมนาคมระหว่างประเทศ (ITU) คาดการณ์ไว้ว่าภายในสิ้นปี ๒๕๕๘ จำนวนผู้ใช้อุปกรณ์สื่อสารเคลื่อนที่จะมีมากกว่า ๗,๐๐๐ ล้านราย เครือข่ายอินเตอร์เน็ตความเร็วสูงในระบบเคลื่อนที่จะกลายเป็นเซกเมนต์หนึ่งที่มีพลวัตมากที่สุด อัตราการเข้าถึงอินเตอร์เน็ตความเร็วสูงในระบบเคลื่อนที่ทั่วโลกเพิ่มเป็น ๔๗ % ในปี ๒๕๕๘ โดยเพิ่มเป็น ๒ เท่า นับจากปี ๒๕๔๐ ซึ่งอย่างไรก็ตามนอกจากเทคโนโลยีสื่อสารเคลื่อนที่และอุปกรณ์อัจฉริยะแล้ว เทคโนโลยีอื่นๆ ที่มีบทบาทสำคัญจนสามารถเปลี่ยนแปลงวิถีชีวิต การดำเนินธุรกิจ แนวนโยบายของรัฐต่อประชาชน ยังรวมถึงสังคมออนไลน์ แอปพลิเคชั่นต่างๆ เทคโนโลยีการประมวลผลแบบ Cloud Computing เทคโนโลยีจัดการข้อมูลขนาดใหญ่ Big data

โดยทั่วไปการประมวลผลแบบ Cloud Computing หมายถึงวิธีการประมวลผลที่อิงกับความต้องการของผู้ใช้ โดยผู้ใช้สามารถระบุความต้องการไปยังซอฟต์แวร์ของระบบ จากนั้นซอฟต์แวร์จะร้องขอให้ระบบจัดสรรทรัพยากรและบริการให้ตรงกับความต้องการผู้ใช้ ทั้งนี้ระบบสามารถเพิ่มและลดจำนวนของทรัพยากร รวมถึงเสนอบริการให้พอเหมาะกับความต้องการของผู้ใช้ได้ตลอดเวลา ประโยชน์ของ Cloud Computing มีหลายประการ ตั้งแต่ลดต้นทุนในการจัดซื้อซอฟต์แวร์ หรือการบำรุงรักษา เริ่มใช้งานได้เร็วไม่มีขั้นตอนยุ่งยาก มีความยืดหยุ่นในการลดหรือเพิ่มทรัพยากรตามความต้องการ เสียค่าใช้จ่ายตามปริมาณการใช้ ทำให้การใช้ทรัพยากรมีความคุ้มค่า ซึ่งการเปลี่ยนแปลงตามที่กล่าวมาได้เกิดขึ้นแล้ว และกำลังสร้างความเปลี่ยนแปลงอย่างต่อเนื่องในอีก ๕ – ๑๐ ปีข้างหน้า เทคโนโลยีเหล่านี้มีความสัมพันธ์กัน ไม่อาจมองแบบแยกส่วนได้

แนวโน้มที่น่าสนใจเนื่องจากได้ก่อตัวขึ้นแล้วในมหานครและเมืองใหญ่บางแห่งที่มีการเจริญเติบโตและพัฒนาขึ้นมาอย่างรวดเร็ว เป็นแบบอย่างของความก้าวหน้าในอนาคต เช่น กรุงโซล เกาหลีใต้ กรุงบรัสเซลส์ เบลเยี่ยม กรุงบูดาเปสต์ ฮังการี ได้แก่นวัตกรรมและเทคโนโลยีอัจฉริยะ รถอัจฉริยะ สมาร์ทโฟนรุ่นใหม่ๆ การแพทย์อัจฉริยะ โครงข่ายพลังงานอัจฉริยะ และเมืองอัจฉริยะ แนวโน้มสำคัญนี้จะสร้างการเปลี่ยนแปลงทางเทคโนโลยีหลายๆ ด้าน ตั้งแต่ Cloud computing สงครามข้อมูลข่าวสาร เทคโนโลยีหุ่นยนต์ ซึ่งจะฉลาดมากขึ้น กลายเป็นมาตรฐานของระบบคอมพิวเตอร์สำหรับธุรกิจและสังคมทั่วไป การมีดาวเทียมสื่อสารมากกว่า ๑๐๐ ดวงในปี ๒๕๖๓ จะเป็นการเปลี่ยนแปลงครั้งใหญ่ทั้งในการดำเนินธุรกิจ การใช้ชีวิตประจำวันและการทหาร

วาระแห่งชาติที่เกิดขึ้นในหลายประเทศคือเศรษฐกิจดิจิทัล เช่น ในสหภาพยุโรป กำหนด Digital Agenda เป็นหนึ่งในวาระที่มีเป้าหมายเพื่อพลิกฟื้นเศรษฐกิจยุโรปไปสู่ความแข็งแกร่งและยั่งยืน หรือ รัฐบาลมาเลเซียกำหนด Digital lifestyle Malaysia เป็นแผนที่กระตุ้นการเติบโต และปรับปรุงคุณภาพชีวิตของคนในประเทศ

โดยสรุปจากกระแสต่างๆ ที่เกิดขึ้นคาดว่าภายในปี ๒๕๖๓ ทุกๆ ครัวเรือนในโลกจะมีอุปกรณ์ที่เชื่อมต่ออินเตอร์เน็ตอย่างน้อย ๑๐ เครื่อง และในปีเดียวกันจะมีผู้ใช้อินเตอร์เน็ตมากกว่า ๕,๐๐๐ ล้านราย และครึ่งหนึ่งเป็นการเชื่อมต่อผ่านทางอุปกรณ์แบบพกพา การเชื่อมโยงดังกล่าวจะแทรกซึมเข่าสู่ชีวิตประจำวัน ทั้งในบ้าน ที่ทำงาน สิ่งแวดล้อมอื่นๆ จนกลายเป็น Connected living ซึ่งหมายถึงทุกจังหวะชีวิต ทุกที่ ทุกเวลา จะมีเทคโนโลยีดิจิทัลเข้ามาเกี่ยวข้อง

## ภัยคุกคามที่มาพร้อมกับเทคโนโลยี

การที่อินเตอร์เน็ตได้รับความนิยมมากขึ้นจากการใช้อุปกรณ์แท็บเล็ตและสมาร์ทโฟน การใช้เครือข่ายสังคมออนไลน์ การทำธุรกรรมทางการเงินผ่าน application ทำให้ไม่รู้สึกว่าคอมพิวเตอร์อยู่ไกลตัว แต่ปัจจุบันแท็บเล็ตและสมาร์ทโฟนคือคอมพิวเตอร์ที่มีความสามารถสูง เข้าถึงได้ง่ายกว่าคอมพิวเตอร์พีซีหรือโน้ตบุ๊ก เป็นสาเหตุที่ภัยอันตรายจากการใช้งานอินเตอร์เน็ตเข้ามาใกล้ตัวอย่างเงียบๆ พฤติกรรมของประชาชนก็เปลี่ยนแปลงไป เช่นคนบางกลุ่มใช้เวลาในโลกไซเบอร์วันละไม่ต่ำกว่า ๔ ช.ม. การใช้งานอินเตอร์เน็ตความเร็วสูงโดยขาดสติ มีโอกาสพลาดได้ง่ายเนื่องจากลักษณะการใช้งานที่รวดเร็วทันใจ เมื่อโพสต์ข้อความใดๆ ไปก็จะไม่สามารถลบข้อมูลนั้นได้เนื่องจากข้อมูลนั้นแพร่กระจายไปเก็บไว้ในส่วนต่างๆ บนเครือข่าย ไม่สามารถลบข้อมูลทุกที่ได้ ข้อมูลที่จัดเก็บไว้ในโลกไซเบอร์ปัจจุบันมีจำนวนมหาศาลรวมเรียกว่า Big data ระบบ Search Engine สมัยใหม่ เช่น Google , Yahoo สามารถนำข้อมูลเหล่านี้ไปวิเคราะห์ด้านการตลาดจนเราอาจเสียความเป็นส่วนตัวได้ ในบางโอกาส การวิเคราะห์ตำแหน่งทางภูมิศาสตร์ (GPS Tracking) เป็นอีกหนึ่งตัวอย่างที่จะทำให้เรา

สูญเสียความเป็นส่วนตัวไป ภัยคุกคามที่มาพร้อมกับเทคโนโลยีที่มีแนวโน้มจะเป็นอันตราย จนต้องระมัดระวังเป็นพิเศษได้แก่

**๑. มัลแวร์ (Malware)** หรือบางทีเรียกว่า มัลลิเชียสโค้ด (Malicious Code) เป็นโปรแกรมประสงค์ร้ายที่ออกแบบมาเพื่อเจาะเข้าทำลาย หรือสร้างความเสียหายให้แก่ระบบคอมพิวเตอร์ เช่น ไวรัส โทรจันฮอร์ส ลอจิกบอมป์ และบอตเน็ต

ไวรัส หมายถึงโปรแกรมที่ทำลายระบบคอมพิวเตอร์ โดยแพร่กระจายไปยังไฟล์อื่นๆ ที่อยู่ในคอมพิวเตอร์ สามารถทำลายไฟล์ทั้งหมดที่อยู่ในเครื่องให้เสียหาย รบกวนให้เกิดความรำคาญ ไวรัสไม่สามารถแพร่กระจายไปยังเครื่องอื่นได้ด้วยตัวเอง จำเป็นต้องอาศัยโปรแกรมอื่นๆ หรือมนุษย์ช่วยเหลือในการทำงาน

เวิร์ม หมายถึงโปรแกรมที่เป็นอันตรายต่อระบบคอมพิวเตอร์ แพร่กระจายได้ด้วยตัวเองไปยังคอมพิวเตอร์อื่นๆ ในเครือข่าย ใช้ประโยชน์จากแอพพลิเคชั่นที่รับส่งไฟล์โดยอัตโนมัติ ไม่ต้องอาศัยคนเพื่อเปิดปิดไฟล์ เวิร์มมีส่วนของโปรแกรมที่สามารถรันตัวเองเพื่อสร้างความเสียหายได้ บางทีอาจอาศัยอีเมลในการแพร่กระจายตัวเองเช่นเดียวกับไวรัส

โทรจันฮอร์สเป็นคำที่มาจากสงครามเมืองทรอยที่ชาวกรีกสร้างม้าไม้ตัวใหญ่บรรจุคนอยู่ภายในทิ้งไว้ก่อนที่จะถอยทัพกลับ ทหารเมืองทรอยคิดว่าเป็นของขวัญชาวกรีก จึงนำเข้าไปในเมือง พอตกดึกทหารกรีกออกมาจากม้าเปิดประตูเมืองให้ทหารกรีกเข้ามาได้ ส่วนความหมายในทางคอมพิวเตอร์ โทรจันคือโปรแกรมที่แฝงมากับโปรแกรมอื่นเช่น เกมส์ เมื่อผู้ใช้ดาวน์โหลดขึ้นมาติดตั้งแล้วรันโปรแกรมโทรจันจะทำลายระบบให้เสียหาย เช่น ลบไฟล์ ทำให้เครื่องประมวลผลช้าลง

จากคำจำกัดความข้างต้น ไวรัส เวิร์ม และโทรจัน อาจมีความหมายคล้ายกัน โปรแกรมบางชนิดอาจมีคุณลักษณะทั้งสามอย่างได้ อย่างไรก็ตามโปรแกรมทั้งสามมีวัตถุประสงค์ในการทำลายระบบของคอมพิวเตอร์ทั้งสิ้น

**๒. บอตเน็ต (Botnet)** หมายถึงเครื่องที่แฮกเกอร์สามารถควบคุมได้ในระยะไกล หรือ Robot Network เป็นเครือข่ายของแฮกเกอร์เพื่อใช้ในการประกอบธุรกรรมผิดกฎหมาย เช่น ส่งสแปมเมล หรือเป็นฐานในการโจมตีเป้าหมายโดยวิธี DoS เป็นต้น มีรายงานว่าเครื่องคอมพิวเตอร์ที่กลายเป็น Botnet ทั่วโลกมากกว่าสี่ล้านเครื่อง และมีแนวโน้มที่จะสูงขึ้นเรื่อยๆ สาเหตุที่ทำให้ตกเป็นเหยื่อของ Botnet ก็คือ การที่ไม่ติดตั้งระบบป้องกัน เช่นไฟร์วอลล์ โดยปกติแล้ววินโดว์จะมีโปรแกรมไฟร์วอลล์มาให้สามารถเปิดใช้งานได้ทันทีแต่ก็แก้ปัญหาได้ในระดับหนึ่ง อีกปัญหาคือผู้ใช้มักไม่ค่อยติดตั้ง Patch ให้กับระบบปฏิบัติการทำให้เกิดช่องโหว่ (Vulnerability) ที่แฮกเกอร์ใช้เป็นช่องทางในการเจาะระบบ การติดตั้ง Patch ระบบและการอัพเดทซอฟแวร์ เป็นสิ่งที่ควรทำอย่างสม่ำเสมอ สามารถดาวน์โหลดและติดตั้งอัพเดทโดยอัตโนมัติได้เวลาที่เปิดเครื่อง แต่อาจทำให้เสียเวลาไปบ้าง นอกจากนี้การใช้วินโดว์ซึ่งละเมิดลิขสิทธิ์จะไม่มีการอัพเดทอัตโนมัติ ทำให้ตกเป็นเหยื่อได้เช่นกัน

**๓. Advanced Persistent Threat (APT)** เป็นประเภทหนึ่งของอาชญากรรมทางคอมพิวเตอร์ มีเป้าหมายโจมตีหน่วยงานที่มีความสำคัญ เช่นหน่วยงานความมั่นคงทางทหาร หรือองค์กรธุรกิจขนาดใหญ่ รูปแบบการโจมตีมักจะเป็นกลุ่มบุคคล ซึ่งอาจเป็นไปได้ว่ามีองค์กรหรือรัฐบาลของประเทศใดคอยให้การสนับสนุนอยู่เบื้องหลัง การโจมตีมีเป้าหมายแน่ชัด ผู้โจมตีมักแฝงอยู่ในระบบเป้าหมายเป็นเวลานานและใช้ทุกวิถีทางเพื่อให้บรรลุความสำเร็จ มีทรัพยากรจำนวนมากวิธีการจะใช้เครื่องมือและเทคนิคชั้นสูงเพื่อเจาะระบบ อาศัยจิตวิทยาหลอกล่อให้ได้มาซึ่งข้อมูลสำคัญ Advanced Persistent คือการโจมตีอย่างค่อยเป็นไปสม่ำเสมอ เนื่องจากต้องแฝงตัวเข้าไปในระบบไม่ให้เป้าหมายรู้ตัว ส่วน Threat หมายถึงภัยคุกคามที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งเมื่อเอาความหมายทั้งสามมารวมกันจึงเป็นคำว่า APT

ตัวอย่างของการใช้ APT ในการโจมตีได้แก่ Operation Aurora เป็นการโจมตีกูเกิลเมื่อวันที่ ๑๒ ม.ค.๒๕๕๓ โดยกูเกิลประกาศว่าถูกโจมตีตั้งแต่กลางปี ๒๕๕๒ ถึง ธ.ค.๒๕๕๒ จากแหล่งที่มาจากประเทศจีน สาเหตุคาดว่าเกิดจากผู้โจมตีไม่พอใจกูเกิลที่ไม่ยอมรับเงื่อนไขของรัฐบาลจีนในการเซนเซอร์การสืบค้นข้อมูลทางเว็บไซต์กูเกิลประเทศจีน เป็นผลให้กูเกิลตัดสินใจย้ายสำนักงานใหญ่ออกจากประเทศจีน

**๔. ฟิชชิ่ง (Phishing)** คือการโจมตีที่ใช้ในการปลอมแปลงอีเมลหรือเว็บไซต์เพื่อต้องการข้อมูลสำคัญของผู้ใช้ เช่น Username, Password, หมายเลขบัตรเครดิต ส่วนมากจะแสร้งว่าเป็นบริษัทที่มีความน่าเชื่อถือ หรือจากแหล่งที่เหยื่อเป็นสมาชิก เช่น E Bay , Pay Pal ฟิชชิ่งมีการค้นพบครั้งแรกเมื่อปี 1987 โดยชื่อแผลงมาจากคำว่า Fishing ใช้ Ph แทน F เหมือนกับการตกปลาที่ต้องใส่เหยื่อและรอให้ปลามาติดเบ็ด

กรรมวิธีที่ใช้ จะมีการส่งข้อมูลข่าวสารไปหาเหยื่อแจ้งว่าเซิร์ฟเวอร์ของบริษัทได้รับความเสียหาย ลูกค้าต้องกรอกข้อมูลใหม่ให้กับบริษัท ส่วนใหญ่จะใช้อีเมลที่ลิงค์ไปหาเว็บไซต์ปลอมเพื่อกรอกข้อมูลโดยเว็บไซต์ปลอมจะเหมือนจริงทุกประการ

หน้าเว็บไซต์ปลอมบางหน้าจะใช้วิธีแยบยลโดยการฝังโทรจันที่สามารถขโมยข้อมูลที่ต้องการ เช่น ทำหน้าที่เป็น Key-logger คอยติดตามว่าผู้เสียหายพิมพ์คีย์บอร์ดอะไรบ้าง เมื่อผู้เสียหายกดลิงค์มาที่หน้าเว็บไซต์ปลอมจะติดโทรจันโดยอัตโนมัติ

นอกจาก Phishing แล้วเทคนิคอื่นๆ ที่คล้ายกัน เช่น Vishing และ Smishing พฤติกรรมของแก๊งคอลเซ็นเตอร์ที่หลอกลวงให้ได้มาซึ่งข้อมูลส่วนบุคคลผ่านทางโทรศัพท์ หรือการใช้ SMS

**๕. แฮกเกอร์ (Hacker)** หรือการเจาะระบบหมายถึงการใช้ประโยชน์จากช่องโหว่ (Vulnerability) ของระบบคอมพิวเตอร์ มีหลายประเภทเช่น แฮกเกอร์หมวกขาว มีความหมายเหมือนกับคำว่าแฮกเกอร์ที่มีจริยธรรม หรือนักทดลองเจาะระบบ ซึ่งจะตรงข้ามกับแฮกเกอร์หมวกดำหรือ Cracker หรือ Malicious Attacker อย่างไรก็ตามไม่ว่าจะเป็นฝ่ายดีหรือร้าย จะมีขั้นตอนการ

แผนภาพที่ ๓ - ๑ : Hacker

ที่มา : www.itgenius.co.th

แผนภาพที่ ๓ - ๒ : Hacker


ที่มา : www.itgenius.co.th

เจาะระบบเหมือนกันหรือใช้เครื่องมือเดียวกันในการเจาะระบบ โดยหลักการแล้วเพื่อให้หน้าที่ของแฮกเกอร์หมวกขาวสมบูรณ์แบบ แฮกเกอร์หมวกขาวควรคิดและทำเหมือนแฮกเกอร์หมวกดำเพื่อที่จะได้รู้ว่าระบบนั้นๆ มีช่องโหว่และแก้ไขได้ทันก่อนที่จะถูกเจาะระบบ

นักเจาะระบบหรือ Hacker มีหลายประเภทขึ้นอยู่กับความชำนาญและแรงจูงใจที่กระทำ Hacker แต่ละประเภทใช้เครื่องมือที่หลากหลายตั้งแต่เครื่องมือพื้นฐานเครื่องมือที่ซับซ้อนเครื่องมือที่มีอำนาจการทำลายสูง ซึ่งสามารถแบ่งประเภทของ Hacker ได้ดังนี้

| นักโจมตี | ระดับความชำนาญ | แรงจูงใจ |
|---|---|---|
| แฮกเกอร์ | สูง | เพื่อปรับปรุงการรักษาความปลอดภัยระบบ |
| แคร็คเกอร์ | สูง | เพื่อทำลายระบบ |
| สคริปต์คิดดี้ส์ | ต่ำ | เพื่อให้ได้รับการยอมรับ |
| สายลับ | สูง | เพื่อผลประโยชน์ |
| พนักงาน | หลากหลาย | หลากหลาย |
| ผู้ก่อการร้าย | สูง | เพื่ออุดมการณ์ทางการเมือง |

โดยที่ Hacker มี ๒ ความหมาย เมื่อพูดถึงจะเข้าใจว่าบุคคลที่พยายามเจาะระบบโดยไม่ได้รับอนุญาต และความหมายเดิมคือผู้ใช้ความรู้ความชำนาญเกี่ยวกับคอมพิวเตอร์ แต่ไม่มีจุดประสงค์ทำลายหรือด้านลบ ดังนั้นในความหมายที่สองนี้จะเป็นผู้ที่ใช้ความรู้ในทางบวก เช่น การสำรวจเครือข่ายเพื่อค้นหาสิ่งแปลกปลอม อย่างไรก็ตามการเจาะเข้าระบบของผู้อื่นเป็นสิ่งผิดกฎหมาย แต่ในมุมมองของ Hacker ถือว่าเป็นเรื่องถูกจริยธรรม ถ้าไม่มีการขโมยข้อมูลความลับ หรือทำลายระบบแรงจูงใจนั้นก็เพื่อพัฒนาระบบให้มีความปลอดภัยซึ่งเป็นความรับผิดชอบของพวกเราที่ต้องหาช่องโหว่หรือจุดอ่อนของระบบ และแก้ไขหรือปิดช่องโหว่นั้นก่อนที่จะเกิดเหตุการณ์ไม่พึงประสงค์ ซึ่งความจริงก็คือโดยส่วนใหญ่ช่องโหว่หรือปัญหาของซอฟต์แวร์จะถูกค้นพบก่อนโดยแฮกเกอร์ที่ไม่ใช่นักพัฒนาระบบแฮกเกอร์ที่มีจรรยาบรรณจะประกาศให้กับผู้เกี่ยวข้องแก้ไขปัญหานั้นเสียก่อน

**๖. แคร็คเกอร์ (Cracker)** คือบุคคลที่พยายามจะทำลายระบบและมีแรงจูงใจที่จะทำ เช่น ปฏิเสธการให้บริการกับผู้ใช้งานที่ได้รับอนุญาต ทำให้เกิดปัญหาต่างๆ ในระบบเครือข่าย แคร็คเกอร์จะมีความสุขใจหากสามารถเจาะระบบและสร้างความเสียหายได้มาก ในขณะเดียวกันจะรู้สึกแย่หากมีคนอื่นสามารถทำลายล้างได้มากกว่า แคร็คเกอร์อาจแบ่งได้เป็นกลุ่มที่มีความรู้อยู่บ้าง ความรู้ปานกลาง และขั้นมืออาชีพ กลุ่มที่มีความรู้อยู่บ้างเรียกว่าสคริปต์คิดดี้ส์ มีประมาณ 95 % ของนักโจมตีระบบส่วนใหญ่เป็นเด็กที่มีเวลาว่างมากๆ เจาะระบบของผู้อื่นเพียงเพื่อทดลองขีดความสามารถของซอฟต์แวร์เป็นแรงบันดาลใจในการทำงาน แต่สร้างปัญหาให้กับคนที่ใช้คอมพิวเตอร์ได้มาก กลุ่มที่มีความรู้ปานกลางอาจมีความเข้าใจระบบปฏิบัติการลีนุกซ์ และวินโดว์ ความรู้เกี่ยวกับเครือข่าย โปรโตคอลและเซอร์วิสมีขีดความสามารถในการโจมตีสูงกว่าสคริปต์คิดดี้ส์ ส่วนใหญ่เขียนโปรแกรมเองไม่ได้ ยังไม่รู้จุดอ่อน

ของซอฟต์แวร์ และจะเป็นผู้ตามมากกว่าผู้นำ กลุ่มมืออาชีพอาจเรียนรู้ด้วยตัวเองหรือได้รับการฝึกอบรมจนชำนาญ ดาวน์โหลดโปรแกรมแล้วทดสอบเพื่อหาจุดอ่อนระบบ ใช้ประโยชน์จากจุดอ่อนส่งต่อให้ผู้อื่นหรือแชร์บนออนไลน์ ซึ่งบางครั้งก็เป็นคนดีที่ต้องการพัฒนาระบบหรือซอฟต์แวร์ ปัจจุบันแฮกเกอร์แบ่งออกเป็นสองกลุ่มได้แก่ Anonymous และ Lulzsec มีผลงานเจาะระบบของบริษัทใหญ่ๆ ทั่วโลกโดยวิธี APT เพื่อล้วงความลับขององค์กร ตัวอย่างเช่นเหตุการณ์ “Wiki leaks” โดยที่ปัจจุบันเครือข่ายคอมพิวเตอร์จำนวนมากทั่วโลกได้รับการติดตั้งโปรแกรมโทรจันของกลุ่มแฮกเกอร์นี้โดยไม่รู้ตัว โปรแกรมเหล่านี้จะสอดแนมส่งข้อมูลกลับไปให้แฮกเกอร์อยู่ตลอดเวลา ทำให้เราขาดความเป็นส่วนตัว องค์กรอาจมีปัญหาเมื่อความลับรั่วไหลออกไป

**๗. อาชญากรรมไซเบอร์ (Cybercrime)** จากนักพัฒนาระบบได้กลายเป็นนักเจาะระบบหรือแฮกเกอร์ที่มีเป้าหมายเพื่อเงิน ดังนั้นลูกค้าของธนาคารที่ใช้บริการออนไลน์ กลายเป็นเป้าหมายของแฮกเกอร์ ลูกค้าบัตรเครดิตต่างๆ เมื่อแฮกเกอร์สามารถเจาะการเข้ารหัสได้สำเร็จยังพัฒนานำไปขายกับแฮกเกอร์มือสมัครเล่นได้อีกทอดหนึ่ง ดังนั้นการเข้ารหัสที่ธนาคารใช้อยู่ปัจจุบันยังไม่เพียงพอกับขีดความสามารถของแฮกเกอร์แล้ว ธนาคารจำเป็นต้องมีการตรวจสอบตัวตนแบบ Two Factor Authentication หรือการส่ง OTP ผ่านทาง SMS เข้ามือถือของผู้ใช้ และแน่นอนว่านักพัฒนาระบบปัจจุบันก็มีวิธีคิดใหม่ๆ เช่น สร้างมัลแวร์ในรูปแบบม้าโทรจัน ฝังเข้าสู่ระบบเป้าหมาย มีรายงานว่าสถานทูตหลายแห่งทั่วโลกถูกเจาะระบบด้วยวิธีนี้ และผู้ให้บริการยังไม่สามารถแก้ไขได้สร้างปัญหาให้กับสถานทูตจนปัจจุบันนี้

## การรักษาความปลอดภัยไซเบอร์

การรักษาความปลอดภัยไซเบอร์ (Cyber security) หมายถึงการใช้เทคโนโลยีและกระบวนการหรือการกระทำทั้งหมดที่จำเป็น เพื่อให้องค์กรปราศจากความเสี่ยงและความเสียหายที่มีผลต่อความปลอดภัยของข้อมูลข่าวสารในทุกรูปแบบ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ ความปลอดภัยของระบบเครือข่ายที่ใช้ในการเก็บ เข้าถึง ประมวลผล การกระจายข้อมูล การป้องกันต่ออาชญากรรม การโจมตี การบ่อนทำลาย การจารกรรม อุบัติเหตุ และความผิดพลาดองค์บุคคล

ไซเบอร์ (Cyber) หรือ Cybernetics หมายถึงระบบเครือข่าย เช่น ระบบอินเตอร์เน็ต หมายถึงการควบคุมการพูดและกระบวนการในการทำงานของสมอง ซึ่งนำไปใช้ในเรื่องเกี่ยวกับคอมพิวเตอร์และอิเล็กทรอนิกส์ในการทำงานของระบบควบคุมระยะไกล โดยรวมแล้วไซเบอร์เป็นความหมายเชิงนามธรรมหมายถึงขอบเขตที่เกี่ยวข้องกับการใช้งานของระบบเครือข่ายคอมพิวเตอร์หรือระบบอิเล็กทรอนิกส์ ซึ่งครอบคลุมมากกว่าคอมพิวเตอร์ที่เป็นรูปธรรมของอุปกรณ์คอมพิวเตอร์ทั่วไป แต่หากเปรียบเทียบกับระบบข้อมูลข่าวสาร (Information System) สามารถกำหนดให้ไซเบอร์เป็นส่วนหนึ่งหรือ Subset ของระบบข้อมูลข่าวสารได้ และในทางปฏิบัติเพื่อรักษาความปลอดภัยของ

ระบบข้อมูลข่าวสาร ไซเบอร์สเปซและเครือข่ายคอมพิวเตอร์ไม่สามารถแยกออกจากกันได้ รูปแบบของการรักษาความปลอดภัยของข้อมูลข่าวสารและทรัพย์สินอื่นๆ มีวิวัฒนาการเหมือนกับสังคมโดยรวมและเทคโนโลยีต่างๆ การเรียนรู้และเข้าใจปัจจุบันจะช่วยเหลือและเป็นบทเรียนไม่ให้มีข้อผิดพลาดเหมือนในอดีตอีก โดยต่อไปจะได้กล่าวถึงการรักษาความปลอดภัยในแง่มุมต่างๆ ที่เกี่ยวข้อง ได้แก่ ในด้านกายภาพ ด้านการสื่อสาร ด้านการแผ่รังสี ด้านคอมพิวเตอร์ เครือข่ายและข้อมูล

**๑. การรักษาความปลอดภัยด้านกายภาพ (Physical Security)** เมื่อสมัยก่อนทรัพย์สินจะเป็นวัตถุที่จับต้องได้ ข้อมูลสำคัญก็อยู่ในรูปแบบของวัตถุ บันทึกอยู่บนแผ่นหิน แผ่นหนัง หรือกระดาษ ถ้าต้องการส่งข้อมูลไปที่อื่นก็จะใช้พลนำสารมีผู้คุ้มกัน ทรัพย์สิน เช่น เงิน ทอง หรือข้อมูลสำคัญ จะถูกขโมยหรือแย่งชิงไป ต้องได้มาจากเจ้าของหรือผู้ควบคุมดูแลทรัพย์สินนั้นๆ ซึ่งเป็นความหมายในเชิงกายภาพ

**๒. การรักษาความปลอดภัยด้านการสื่อสาร (Communication Security)** เมื่อการรักษาความปลอดภัยด้านกายภาพมีจุดอ่อน ข้อบกพร่อง เช่น ถ้าเอกสารถูกขโมยระหว่างการรับ - ส่ง ฝ่ายตรงข้ามก็อาจนำข้อมูลไปใช้ประโยชน์ ในยุคศตวรรษที่ ๒ จึงมีความคิดในการซ่อนข้อมูลหรือการเข้ารหัส (Encryption) ที่หากข้อมูลตกหล่นสูญหายก็จะไม่มีใครรู้ข้อความนั้นๆ ในสมัยสงครามโลกครั้งที่ ๒ เยอรมันใช้เครื่องมือที่เรียกว่า Enigma เข้ารหัสข้อมูล ทำให้ได้เปรียบในช่วงต้นสงครามและต้องพ่ายแพ้ในที่สุดเมือ Enigma ถูกถอดรหัสได้ และหลังสงครามโลกครั้งที่ ๒ โซเวียตใช้ Onetime Pad เพื่อเข้ารหัสข้อมูลที่ รับ-ส่ง โดยสายลับ เข้ารหัสโดยการส่งข้อความเป็นปึกกระดาษแต่ละหน้าประกอบด้วยตัวเลขที่เป็น Random ใช้แทนหนึ่งข้อความไม่สามารถถอดรหัสได้ถ้าใช้อย่างถูกต้อง คือใช้หนึ่งคีย์ต่อการเข้ารหัสหนึ่งข้อความ

**๓. การรักษาความปลอดภัยการแผ่รังสี (Emission Security)** การถอดรหัสเป็นสิ่งที่ยากต้องใช้เทคโนโลยีชั้นสูง หรือเสียเวลามากจนทำให้ข้อความนั้นๆ ถูกเปิดเผยจนไม่เป็นความลับอีกแล้ว มีความพยายามที่จะใช้เทคนิคต่างๆ เพื่ออ่านข้อมูลเข้ารหัส เช่น ในปี 1950 ได้ค้นพบว่าข้อมูลที่ รับ-ส่ง สามารถดักจับได้จากสัญญาณไฟฟ้าที่ส่งผ่านสายโทรศัพท์ เนื่องจากอุปกรณ์อิเล็กทรอนิกส์ทุกประเภทจะมีการแผ่รังสี รวมถึงเครื่องโทรสารและเครื่องเข้ารหัสข้อมูล ซึ่งทำให้ข้อมูลเดิมที่ยังไม่ถูกเข้ารหัส จะสามารถกู้คืนมาได้โดยใช้เครื่องมืออ่านสัญญาณไฟฟ้าที่ดี ซึ่งเป็นเหตุให้สหรัฐกำหนดมาตรฐาน TEMPEST ในการควบคุมการแผ่รังสีของอุปกรณ์คอมพิวเตอร์ของระบบที่มีความสำคัญเพื่อลดการแผ่รังสีของอุปกรณ์ที่จะสามารถกู้คืนข้อมูลได้

**๔. การรักษาความปลอดภัยคอมพิวเตอร์ (Computer Security)** การเข้ารหัสและการควบคุมการแผ่รังสีนั้นเพียงพอสำหรับการรักษาความปลอดภัยข้อมูล หากการส่งข้อมูลเป็นเพียงการส่งโทรสาร แต่เมื่อมีการนำคอมพิวเตอร์มาใช้งานแทนเครื่องโทรสารข้อมูลส่วนใหญ่เป็นดิจิตอล และเครื่องคอมพิวเตอร์มีขีดความสามารถสูงขึ้น ปัญหาความปลอดภัยในการจัดเก็บข้อมูลเป็น

แผนภาพที่ ๓ - ๓ : เครื่องถอดรหัส Enigma


ที่มา : www.scimath.org

แผนภาพที่ ๓ - ๔ : เครื่องถอดรหัส Enigma

ที่มา : www.scimath.org

เรื่องสำคัญที่ตามมา จนในปี 1970 มีแนวคิดในการจัดระดับความปลอดภัยของข้อมูลเป็น ๔ ระดับ คือ ปกติ ลับ ลับมาก และลับที่สุด และจัดระดับผู้ที่สามารถเข้าถึงข้อมูลนี้ออกเป็น ๔ ระดับเช่นกัน ผู้ที่มีสิทธิน้อยไม่สามารถเข้าถึงชั้นความลับสูงได้ โดยแนวคิดนี้เป็นที่รู้จักทั่วไปว่า Orange Book และแน่นอนว่ามีปัญหามากมายในการรับประกันความเชื่อถือได้ของระบบ จนทำให้ระบบนี้ล้าสมัยไป ในเวลาไม่นานมีมาตรฐานใหม่มาแทนเพื่อแก้ไขข้อบกพร่องต่างๆ เพื่อรับรองว่าคอมพิวเตอร์นั้นมีความปลอดภัยระดับไหน และเนื่องจากวิวัฒนาการของระบบปฏิบัติการรวมถึงฮาร์ดแวร์ใหม่ๆ ถูกพัฒนาขึ้นแทนของเก่าอย่างรวดเร็ว ทำให้กระบวนการตรวจสอบความปลอดภัยของระบบเป็นไปได้ยากหรือแทบเป็นไปไม่ได้เลยที่จะพิสูจน์ว่าระบบใดปลอดภัยหรือไม่

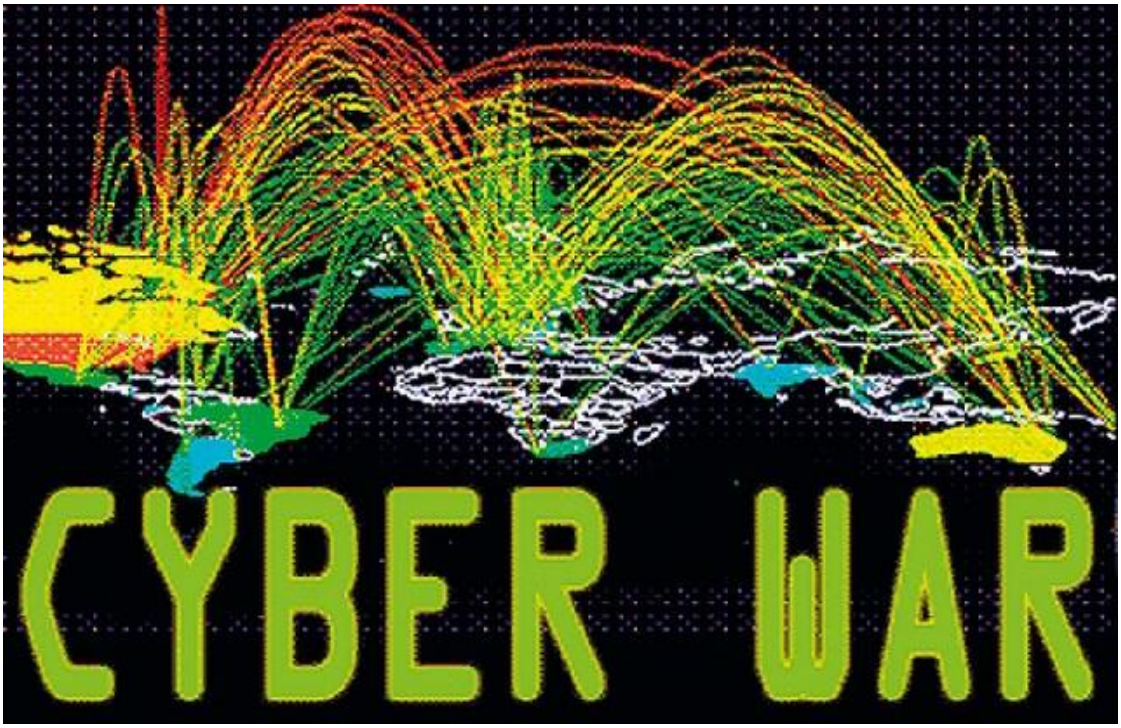
**๕. การรักษาความปลอดภัยเครือข่าย (Network Security)** เมื่อคอมพิวเตอร์เชื่อมต่อกับระบบเครือข่าย ปัญหาใหม่ก็เกิดขึ้นขณะที่ปัญหาเก่าก็ยังเป็นปัญหาอยู่ การเข้ารหัสโดยใช้เครื่องเดี่ยว ๆ อาจไม่ได้ผล การแผ่รังสีจากสายทองแดงที่ใช้สูงมากจนสามารถ login ได้จากหลาย ๆ ที่ทั่วห้อง ทั่วอาคาร การเชื่อมต่อคอมพิวเตอร์กับเครือข่ายทำให้ใบรับรองเกี่ยวกับความปลอดภัยไม่มีประโยชน์ ข้อกำหนดเกี่ยวกับฟังก์ชั่นต่างๆ และการรับประกันใช้เวลามากในการตรวจสอบทดลอง ทำให้เสียเวลาและค่าใช้จ่ายสูงเพื่อรับรองความปลอดภัยระบบจนไม่มีการใช้เชิงพาณิชย์

**๖. การรักษาความปลอดภัยข้อมูล (Information Security)** จากที่กล่าวมาทั้งหมดสรุปได้ว่าไม่มีวิธีการใดแก้ปัญหาเรื่องการรักษาความปลอดภัยได้ทั้งหมด จึงจำเป็นต้องใช้ทุกๆ วิธีการร่วมกันในการป้องกันคุณสมบัติของข้อมูล ๓ ด้านได้แก่ ความลับ ความถูกต้อง และความพร้อมใช้งาน หมายถึงการอนุญาตเฉพาะผู้ที่มีสิทธิที่จะเข้าถึงข้อมูล เฉพาะผู้มีสิทธิจึงจะแก้ไขข้อมูลได้ และผู้ที่จะเข้าถึงข้อมูลได้เมื่อต้องการ เนื่องจากข้อมูลปัจจุบันอยู่ในรูปแบบดิจิตอล และอาจถูกจัดเก็บไว้ในมีเดียฮาร์ดดิสก์ หรืออยู่ระหว่างประมวลผลส่งผ่านในระบบเครือข่าย ไม่ว่าจะอยู่แห่งใดมาตรการรักษาความปลอดภัยทั้งหมดที่กล่าวมามีความจำเป็นทั้งสิ้น

## สงครามไซเบอร์ (Cyber Warfare)

เมื่อคอมพิวเตอร์และเทคโนโลยีสารสนเทศได้รับการพัฒนาอย่างต่อเนื่อง ประชาชนเข้าถึงอินเตอร์เน็ตได้ทุกสถานที่ทุกเวลา มีการใช้เทคโนโลยีอำนวยความสะดวกในทุกวงการไม่ยกเว้นการทหาร ที่นำเอาเทคโนโลยีมาใช้เป็นองค์ประกอบสำคัญของระบบอาวุธ เช่น ระบบบัญชาการรบ เรดาร์ โซนาร์ ระบบต่าง ๆ เหล่านี้เชื่อมต่อถึงกันแบบอัตโนมัติผ่านระบบเครือข่ายคอมพิวเตอร์ ภัยคุกคามด้านไซเบอร์มีให้รับรู้รับทราบบ่อยครั้งขึ้นทุกวัน ผู้ไม่หวังดีอาจใช้ประโยชน์ในการก่อวินาศกรรมมุ่งเป้าทำลายสาธารณูปโภคที่มีผลกระทบในวงกว้าง เช่น ระบบเครือข่าย กระแสไฟฟ้า รถไฟฟ้าใต้ดิน ระบบโทรคมนาคม การเงิน การธนาคาร หรือปฏิบัติการทางไซเบอร์ทำพร้อมกับปฏิบัติการทางทหารตามรูปแบบ

แผนภาพที่ ๓ - ๕ : สงครามไซเบอร์




ที่มา : www.prachachat.net

แผนภาพที่ ๓ - ๖ : สงครามไซเบอร์

ที่มา : www.prachachat.net

อย่างไรก็ดีภัยคุกคามทางไซเบอร์อาจไม่เกิดขึ้นเลยถ้ามีการป้องกันที่ดี หรือมีการเตรียมรับเหตุการณ์ไว้แล้ว เมื่อมีภัยคุกคาม ความเสียหายอาจจะลดระดับลงได้ โดยภัยคุกคามอาจเกิดขึ้นในรูปแบบต่าง ๆ ได้แก่ ภัยคุกคามที่เป็นการเปิดเผย (Disclosure) มีลักษณะเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต ภัยคุกคามที่เป็นการแก้ไข (Modification) เป็นการเข้าไปแก้ไขข้อมูลโดยไม่ได้รับอนุญาต และภัยคุกคามที่เป็นการปฏิเสธการให้บริการ (Denial of Service) มีลักษณะขัดขวางหน่วงเวลาไม่ให้เข้าถึงข้อมูลโดยที่มีรูปแบบของการโจมตีได้แก่

**๑. การสอดแนม (Sniffing)** หรือ Snooping หมายถึงการดักเพื่อแอบดูข้อมูล จัดเป็นภัยคุกคามแบบเปิดเผย เป็นการโจมตีแบบ Passive ไม่มีการเปลี่ยนแปลงแก้ไขข้อมูล ตัวอย่างเช่นการดักรับข้อมูลที่ส่งผ่านเครือข่าย ย้ายไฟล์ที่จัดเก็บอยู่ในระบบ แท็ปสายสัญญาณเพื่อเฝ้าดูข้อมูลที่วิ่งผ่านเครือข่าย การเข้ารหัสข้อมูล (Encryption) สามารถป้องกันภัยคุกคามรูปแบบนี้ได้

แพ็กเก็ตสนิฟเฟอร์ (Packet Sniffer) ข้อมูลที่ส่งผ่านระบบเครือข่าย จะถูกแบ่งแยกเป็นชุดเล็กๆ เรียกว่า packet และ Network Protocol จะกำหนดให้ packet นั้น ๆ ส่งไปที่ใด ปัจจุบันนี้โปรแกรม Packet Sniffer มีให้ดาวน์โหลดบนเครือข่ายจำนวนมาก ผู้ใช้งานไม่จำเป็นต้องมีความรู้ทางคอมพิวเตอร์ก็สามารถใช้ซอฟแวร์เหล่านี้ได้ เช่น การตรวจจับข้อมูลผู้ใช้และรหัสผ่าน หากแฮกเกอร์นำข้อมูลและรหัสผ่านที่ตรวจจับได้ไปบุกรุกหรือโจมตีเครือข่ายอื่น ๆ จะเป็นสิ่งที่น่ากลัวมาก ความเสียหายที่เกิดขึ้นเกินกว่าจะทำนายได้

**๒. การแก้ไขข้อมูล (Modification)** หมายถึงการเข้าไปแก้ไขเนื้อหาของข้อมูลโดยไม่ได้รับอนุญาต ฝ่ายรับข้อมูลไม่รู้ว่าข้อมูลที่ได้รับถูกแก้ไขอะไรไปบ้าง จัดเป็นการโจมตีแบบ Active ผู้รับและผู้ส่งไม่ทราบว่าบุคคลที่สามเข้ามาแก้ไขข้อมูลเมื่อใด การรักษาความถูกต้องของข้อมูล (Integrity) เป็นวิธีการป้องกันการโจมตีลักษณะนี้ โดยการเข้ารหัสข้อมูล

**๓. การปลอมตัว (Spoofing)** หมายถึงการทำให้อีกฝ่ายหนึ่งเข้าใจผิดว่าเป็นบุคคลอื่นหลอกให้คู่สนทนาเชื่อว่ากำลังสนทนาอยู่กับบุคคลนั้น ๆ จริง อาจเป็นการโจมตีแบบ Passive ที่ไม่มีการเปลี่ยนแปลงข้อมูลและสามารถเป็นการโจมตีแบบ Active ที่เปลี่ยนแปลงข้อมูลก็ทำได้ การรักษาความถูกต้องโดยการแสดงตัวตน (Authentication) เป็นวิธีการป้องกันการโจมตีในรูปแบบนี้

การหลอกลวงแบบมาคัวสเรตดิ้ง (Masquerading) เป็นอีกวิธีหนึ่งในการปลอมตัว หมายถึงการมอบอำนาจให้ผู้อื่นทำหน้าที่แทนตน ซึ่งแตกต่างจากการปลอมตัว คือไม่สามารถล่วงรู้ว่าผู้ปลอมตัวเป็นใคร ในมาตรการเกี่ยวกับการรักษาความปลอดภัยนั้น การมอบอำนาจสามารถกระทำได้ ส่วนการปลอมตัวถือว่าผิดกฎหมาย

ไอพีสนู๊ฟฟิง (IP Snooping) เป็นการใช้ IP Address เหมือนกับผู้ใช้ในเครือข่าย แต่เป็นบุคคลอื่นนำมาใช้ทำให้สามารถใช้ทรัพยากรในเครือข่ายนั้นได้ ส่วนใหญ่แล้วการโจมตีลักษณะนี้ร้อยละ 90 เกิดจากคนในองค์กรเองทั้งนั้น

**๔. การปฏิเสธการให้บริการ (Denial Service : Dos)** หมายถึงการขัดขวางไม่ให้เข้าถึงการบริการหรือข้อมูล ส่วนใหญ่เกิดขึ้นที่เครื่องเซิร์ฟเวอร์ ทำให้เซิร์ฟเวอร์ขัดข้องหรือขัดขวางช่องทางการสื่อสารของเครื่อง การรักษาความพร้อมใช้งาน (Availability) เป็นวิธีป้องกันการโจมตีแบบนี้ การทำให้เซิร์ฟเวอร์ใช้ทรัพยากรจนหมดหรือเกินขีดความสามารถของ Memory Hard disk , Bandwidth เป็นต้น เป็นการโจมตีที่จุดอ่อนของระบบมากกว่าที่จะโจมตีจุดบกพร่อง (Bug) หรือช่องโหว่ จะทำให้ประสิทธิภาพเครือข่ายลดลง เช่นการส่ง Email ขยะจำนวนมาก ๆ จากหลาย ๆ ที่พร้อมกัน ใช้กับคอมพิวเตอร์ที่ไม่มีระบบรักษาความปลอดภัย ให้ผลทันที ผู้โจมตีได้รับความพอใจเนื่องจากเซิร์ฟเวอร์ล่มแต่ไม่ได้รับประโยชน์อะไรมากนัก

**๕. การปฏิเสธแหล่งที่มา (Repudiation of Origin)** เป็นการไม่ยอมรับข้อมูลที่ส่งให้ผู้รับ เช่น บริษัทเปิดบริการขายสินค้าออนไลน์แล้วมีลูกค้าสั่งซื้อสินค้า แต่เมื่อมีการส่งสินค้าไปถึงลูกค้ากลับถูกปฏิเสธว่าไม่ใช่ผู้สั่งซื้อ หากบริษัทไม่สามารถพิสูจน์ได้ว่าการสั่งซื้อมาจากลูกค้าแน่นอนถือว่าการโจมตีนี้สำเร็จ

**๖. การปฏิเสธการได้รับ (Repudiation of Receipt)** หมายถึงการที่ได้รับข้อมูลแล้วแต่ปฏิเสธ ตัวอย่างเช่น ลูกค้าสั่งซื้อสินค้าราคาแพงและจ่ายเงินไปก่อน แต่เมื่อได้รับสินค้าแล้วกลับปฏิเสธว่าไม่ได้รับ และยืนยันให้ส่งสินค้าใหม่ หากบริษัทพิสูจน์ไม่ได้ว่าลูกค้าได้รับสินค้า ก็จะเกิดความเสียหายการโจมตีในลักษณะนี้สามารถป้องกันได้ด้วยการรักษาความถูกต้อง (Integrity) และความพร้อมใช้ (Availability) ของข้อมูล

**๗. การหน่วงเวลา (Delay)** หมายถึงการยับยั้งไม่ให้ข้อมูลส่งถึงตามเวลาที่ควรจะเป็นโดยผู้บุกรุกสามารถควบคุมระบบบางส่วนไว้ได้ เช่น ไฟล์เซิร์ฟเวอร์ หรือเครือข่าย การรักษาความพร้อมใช้งานเป็นวิธีที่ใช้ในการป้องกันการโจมตีแบบนี้

**๘. วิศวกรรมสังคม (Social Engineering)** เป็นวิธีการที่ง่ายที่สุดเนื่องจากผู้บุกรุกไม่จำเป็นต้องมีความรู้เกี่ยวกับคอมพิวเตอร์หรือเครือข่าย แต่อาศัยการหลอกลวงให้หลงกล เช่น หลอกให้ได้มาซึ่งข้อมูลสำคัญ รหัสผ่าน Password เป็นจุดอ่อนที่ป้องกันได้ยากเพราะเกี่ยวข้องกับคน หรือค้นหาข้อมูลจากถังขยะ เอกสารที่ทิ้งอาจมีคู่มือการใช้รหัสผ่าน เขียนใส่ไว้ในกระดาษ หรือการส่งอีเมลเพื่อหลอกลวงว่าส่งมาจากบุคคลที่น่าเชื่อถือ หลอกให้คลิกเข้าไปในเว็ปไซต์ปลอมแล้วถามข้อมูลบัตรเครดิต การป้องกันโดยการอบรมพนักงานให้เข้มงวดการใช้รหัสผ่าน ปฏิบัติตามนโยบายการรักษาความปลอดภัยระบบเป็นการแก้ปัญหานี้

**๙. การถอดรหัสข้อมูล (Cryptanalysis)** มีรากศัพท์มาจากภาษากรีก คำว่า Crypto หมายถึงการซ่อน และ Graph หมายถึงการเขียน เป็นศาสตร์ในการแปลงข้อมูลให้ปลอดภัยเมื่อมีการสื่อสารหรือจัดเก็บข้อมูลที่ใดที่หนึ่ง ไม่ใช่การปกปิดความมีอยู่ของข้อมูลแต่เป็นการย่อยให้ละเอียดแล้วคนเพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้าถึง ส่วนรหัสผ่าน (Password) หมายถึงกลุ่มอักษรและ

ตัวเลข ที่ใช้ในการพิสูจน์ตัวตนของผู้ใช้เป็นความลับที่ผู้ใช้เท่านั้นจะล่วงรู้ได้ ใช้คู่กับ Username เพื่อล็อกอินเข้าสู่ระบบ Username เป็นส่วนที่เปิดเผยได้ บางครั้ง Password และ Username เองก็เป็นจุดอ่อน เนื่องจากผู้ใช้แต่ละคนอาจมีรหัสผ่านถึง 10 คู่ ที่ต้องใช้เข้าสู่ระบบต่าง ๆ เช่น คอมพิวเตอร์ที่บ้าน ที่ทำงาน บัญชีธนาคาร ร้านค้าออนไลน์ อีเมลต่าง ๆ เป็นการยากที่จะจำข้อมูลได้ทั้งหมด และบางครั้งรหัสผ่านอาจมีอายุการใช้งานแค่ 30 วัน ต้องเปลี่ยนรหัสใหม่ ผู้ใช้หลายคนจึงเลือกจะมีรหัสผ่านที่ง่ายต่อการจดจำหรือใช้รหัสผ่านเดียวกันทุก ๆ ล็อกอิน ผู้โจมตีจะใช้ประโยชน์จากจุดอ่อนนี้ในการเดารหัสผ่าน

**๑๐. การโจมตีแบบคนกลาง (Men in the middle attack)** แบ่งออกเป็นการโจมตีแบบ Active และ Passive เป็นการดักรับข้อมูลที่คอมพิวเตอร์สื่อสารกัน การโจมตีแบบ Active จะแก้ไขข้อมูลก่อนส่งผ่านให้ผู้รับ ส่วนแบบ Passive ผู้รับจะได้รับข้อความที่ถูกต้องแต่ไม่เป็นความลับอีกต่อไปเนื่องจากถูกล่วงรู้โดยคนกลาง

**๑๑. การเจาะระบบ (Hacking)** คือการใช้ประโยชน์จากช่องโหว่ (Vulnerability) ของระบบไม่ว่าจะเป็นช่องโหว่ที่เกิดจากอุปกรณ์ฮาร์ดแวร์ ซอฟแวร์ หรือพิเพิลแวร์ การเจาะระบบส่วนใหญ่ถือเป็นสิ่งที่ผิดกฎหมาย เนื่องจากไม่ได้รับอนุญาตจากเจ้าของระบบ แต่หากได้รับอนุญาตก็จะไม่ผิดกฎหมาย เรียกว่าการทดลอง มีจุดประสงค์เพื่อหาช่องโหว่และปิดช่องโหว่นั้นทำให้ระบบมีความปลอดภัยมากยิ่งขึ้น เป็นการพิสูจน์ให้เห็นว่าช่องโหว่นั้นสามารถถูกแฮกเกอร์ไม่ประสงค์ดีเจาะระบบเข้ามาได้ เป็นกระบวนการที่จะทำให้ระบบเครือข่ายปลอดภัยจากการถูกโจมตี

## สงครามที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Warfare)

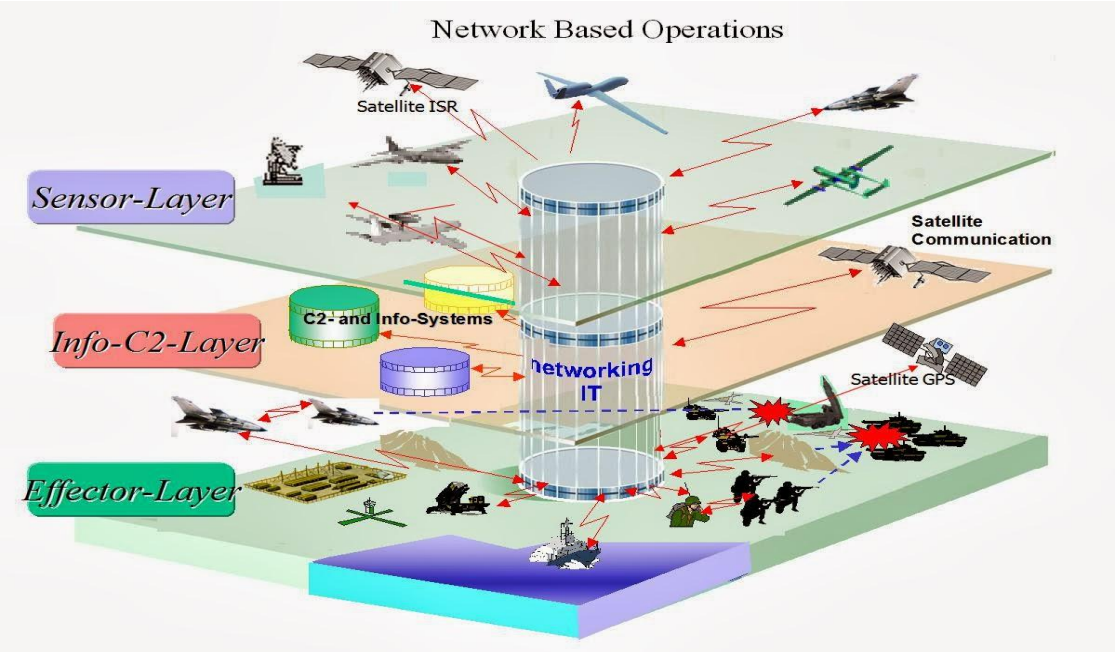
จากแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม ทำให้เทคโนโลยีการสื่อสารและสารสนเทศมีความก้าวหน้า ทุกภาคส่วนมีบทบาทก่อให้เกิดการเปลี่ยนแปลงทางเศรษฐกิจและสังคม รวมถึงกองทัพที่รูปแบบของการทำสงครามได้เปลี่ยนแปลงด้วย การแพ้ชนะในสงครามอนาคตมีเวลาเป็นตัวชี้วัด ผู้ที่ได้รับข้อมูลที่รวดเร็วทันเวลาจะเป็นฝ่ายที่ได้เปรียบ

สงครามที่ใช้เครือข่ายเป็นศูนย์กลางเป็นแนวคิดที่กองทัพหลายประเทศโดยเฉพาะประเทศที่พัฒนาแล้วให้ความสนใจในการวิจัยและพัฒนา เพื่อให้ระบบควบคุมบังคับบัญชามีเครือข่ายรวมศูนย์เชื่อมต่อกันด้วยสัญญาณดิจิทัลทำให้รับรู้สถานการณ์ได้อย่างรวดเร็ว ทันเวลา บางครั้งอาจมีลักษณะเป็น Real time ซึ่งเป็นการเพิ่มประสิทธิภาพ ลดเวลาการตัดสินใจ ซึ่งองค์ประกอบของแนวคิดขึ้นอยู่กับการประมวลผลของระบบคอมพิวเตอร์และเครือข่าย ระบบเรดาร์ ระบบอาวุธ เครือข่ายและสารสนเทศเพื่อการบริหาร ดังนี้

### ๑. ระบบควบคุมบังคับบัญชา (Command Control and Communication)

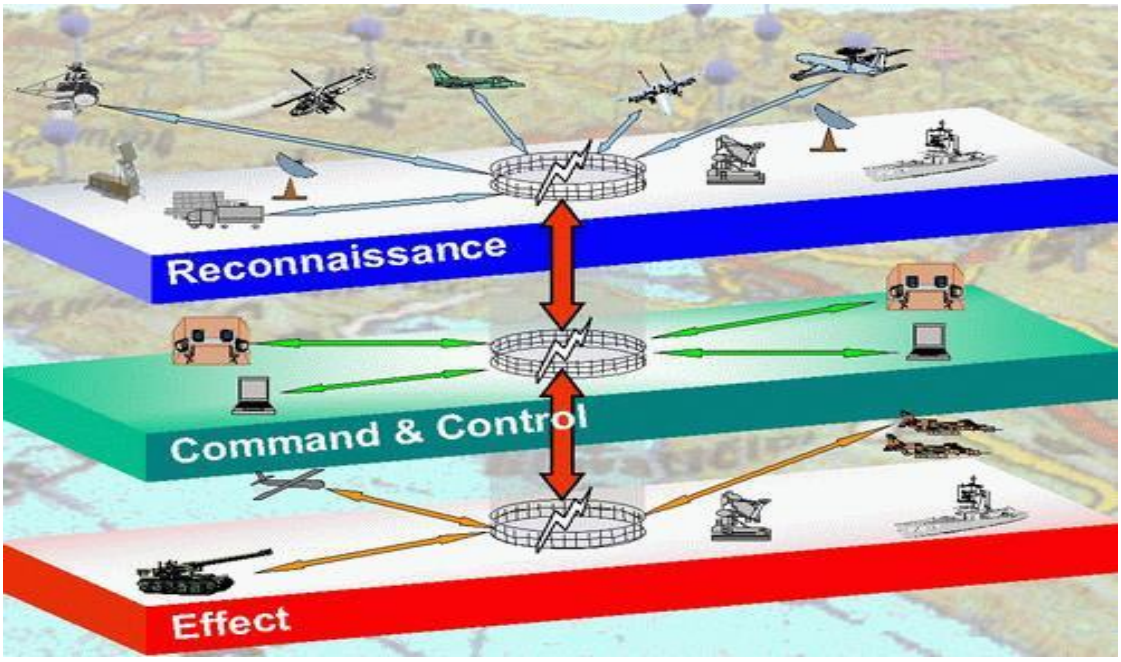
หรือเรียกอีกอย่างว่าระบบบัญชาการรบ คือระบบที่สามารถบูรณาการและเชื่อมโยงข้อมูลที่จำเป็น

แผนภาพที่ ๓ - ๗ : Network Centric




ที่มา : The Center for Digital Intelligence

แผนภาพที่ ๓ - ๗ : Network Centric




ที่มา : The Center for Digital Intelligence

เช่น ข้อมูลเป้า ความเร็ว ระยะทาง การพิสูจน์ฝ่าย เป็นเครื่องมือในการตัดสินใจใช้อาวุธ ควบคุมปฏิบัติการทางทหาร บางครั้งอาจเรียกว่าระบบ $C^3$, $C^3I$

**๒. ระบบเรดาร์ (Radar System)** เป็นระบบที่ใช้คลื่นแม่เหล็กไฟฟ้าส่งสัญญาณออกไปกระทบวัตถุแล้วรับสัญญาณกลับมาแปลเป็นค่าระยะทาง ความสูงและทิศทาง เป็นเทคโนโลยีสำคัญที่ใช้ในทางทหาร แต่ปัจจุบันนำมาใช้ในชีวิตประจำวัน ได้แก่ เรดาร์เดินเรือ เดินอากาศ ระบบเตือนภัยดาวเทียมเพื่อสร้างภาพถ่ายทางอากาศ ฯลฯ ส่วนใหญ่เรดาร์จะเป็นระบบปิดไม่เชื่อมต่อกับระบบอื่น ๆ จึงไม่มีการรักษาความปลอดภัยที่ดี เป็นเป้าหมายแรก ๆ ของการโจมตีทางไซเบอร์

**๓. ระบบอาวุธ (Weapon System)** ในปัจจุบันใช้เทคโนโลยีดิจิทัลเพื่อให้มีความแม่นยำปฏิบัติการได้ในระยะไกลเกินกว่าระยะขอบฟ้า เชื่อมโยงข้อมูลกับส่วนต่าง ๆ เป็นส่วนสำคัญของการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง

**๔. ระบบเครือข่ายโทรคมนาคม (Network of Telecommunication)** จะเชื่อมโยงเครือข่ายหลักของกองทัพ ได้แก่ ระบบบัญชาการรบ ระบบสนับสนุน ให้มีความรวดเร็ว ปลอดภัย เชื่อถือได้ คลอบคลุมพื้นที่ปฏิบัติการ สามารถเชื่อมโยงข้อมูลทางยุทธวิธีที่มีมาตรฐานกับอุปกรณ์ยุทโธปกรณ์ของกองทัพ

**๕. ระบบสารสนเทศเพื่อการบริหาร** หน่วยกำลังรบและสนับสนุนมีขีดความสามารถบูรณาการและประสานสอดคล้องในการปฏิบัติการได้อย่างมีประสิทธิภาพ โดยมีโครงสร้างและระบบงานที่เป็นมาตรฐานสากล เอื้อต่อการแลกเปลี่ยนเรียนรู้ร่วมกัน เชื่อมโยงระหว่างเหล่าทัพ ซึ่งระบบที่ใช้ในทางทหารกับองค์กรทั่วไปใช้ระบบเดียวกัน เช่น Website อีเมล บัญชี บุคลากร เป็นเป้าหมายการโจมตีสำหรับสงครามในอนาคต ปัจจุบันกองบัญชาการกองทัพไทย กองทัพบก กองทัพเรือ และกองทัพอากาศ ต่างมีแผนพัฒนากองทัพให้มีขีดความสามารถในการป้องกันประเทศและการทำสงครามโดยใช้เครือข่ายเป็นศูนย์กลาง ซึ่งแน่นอนการพัฒนาขีดความสามารถดังกล่าวต้องอาศัยเวลาทั้งในด้านการพัฒนาองค์วัตถุ เครือข่ายโทรคมนาคม การสื่อสารเทคโนโลยีสารสนเทศ และที่ขาดไม่ได้คือการพัฒนาบุคลากรให้มีขีดความสามารถในการทำงานร่วมกับเทคโนโลยีสารสนเทศและการสื่อสารที่ทันสมัย ในความเป็นจริงแล้วเมื่อพิจารณาแนวทางการพัฒนากองทัพให้มีขีดความสามารถในการสงครามที่ใช้เครือข่ายเป็นศูนย์กลาง คือความพยายามของหน่วยงานด้านความมั่นคงต่าง ๆ ที่จะปรับตัว และแนวทางการทำงานโดยมุ่งเน้นการนำเทคโนโลยีสารสนเทศและการสื่อสารมาประยุกต์ใช้ในการปฏิบัติงานให้กองทัพมีขีดความสามารถสูงสุดในการปฏิบัติการต่าง ๆ ท่ามกลางความเปลี่ยนแปลงที่เกิดขึ้นอย่างมากมายในยุคพลวัตรแห่งข้อมูลข่าวสาร สภาพแวดล้อม และภัยคุกคามที่เปลี่ยนแปลงรูปแบบออกไปจากเดิม ซึ่งแน่นอนว่านอกจากภารกิจทางการทหารแล้ว กองทัพที่มีโครงสร้างกำลังและการควบคุมบังคับบัญชาที่ดี ย่อมมีความพร้อมสำหรับการปฏิบัติภารกิจอื่นใดนอกเหนือจากการปฏิบัติทางการทหารต่าง ๆ เป็นอย่างดี ไม่ว่าจะเป็นภารกิจการต่อต้านการก่อการร้าย

ภารกิจการปฏิบัติการเพื่อสันติภาพ ภารกิจการปราบโจรสลัด และงานรักษากฎหมาย รวมทั้งการช่วยเหลือผู้ประสบภัยดังเช่นภัยจากน้ำท่วม หรือแผ่นดินไหว

## เหตุการณ์สำคัญจากภัยคุกคามทางไซเบอร์

การศึกษาและติดตามสถานการณ์ทางไซเบอร์ ให้ทราบถึงพัฒนาการของภัยคุกคามและนำข้อมูลมาวิเคราะห์เพื่อแก้ไขในอนาคตมีตัวอย่างดังต่อไปนี้

**๑. การโจมตีทางไซเบอร์ในเอสโทเนีย** เมื่อปี ๒๕๕๐ เว็บไซต์ของหน่วยงานสำคัญได้แก่ รัฐสภา ธนาคาร กระทรวงต่าง ๆ และสถานีโทรทัศน์ การให้บริการทางออนไลน์ต้องสะดุดหยุดลง เกิดผลกระทบทางด้านเศรษฐกิจเป็นวงกว้างโดยแนวทางการโจมตีที่เรียกว่า DDoS ทางรัฐบาลรัสเซียได้ออกมาปฏิเสธปฏิบัติการดังกล่าว แต่จากการสอบสวนมีหลักฐานบ่งชี้ว่าการโจมตีมีจุดเริ่มต้นจากรัสเซีย

**๒. ปฏิบัติการ Orchard** เป็นการโจมตีซีเรียโดยกองทัพอิสราเอลด้วยเครื่องบิน F 15I จำนวน ๑๐ ลำ เข้าไปทิ้งระเบิดยังอาคารหลังหนึ่งในประเทศซีเรียเมื่อ ๖ กันยายน พ.ศ.๒๕๕๐ ซึ่งทางการอิสราเอลให้เหตุผลว่าอาคารหลังนี้ใช้เป็นสถานที่ในการผลิตอาวุธนิวเคลียร์ ซึ่งหากพิจารณาในเบื้องต้นแทบจะไม่พบความเกี่ยวเนื่องกับสงครามไซเบอร์ใด ๆ แต่เมื่อพิจารณาข้อเท็จจริงที่ว่าเครื่องบินรบของอิสราเอลสามารถบินเข้าทำลายเป้าหมายโดยไม่ถูกตรวจพบจากเรดาร์ตรวจการณ์ทางอากาศ และกองบัญชาการควบคุมภาคพื้นดินของซีเรีย โดยที่เครื่องบินรบที่ปฏิบัติภารกิจในครั้งนี้ไม่มีเครื่องบินลำใดที่เป็นเครื่องบินล่องหน (Stealth Aircraft) และจากการตรวจสอบของซีเรียไม่พบความบกพร่องในการปฏิบัติหน้าที่ของเจ้าหน้าที่ที่เกี่ยวข้องกับเรดาร์ตรวจการณ์ทางอากาศแต่อย่างใด ตามข้อสันนิษฐานพบว่าการที่เครื่องบินรบของอิสราเอลสามารถหลุดรอดการตรวจพบของเรดาร์ตรวจการณ์ไปได้ ย่อมหมายถึงการที่ระบบรักษาความมั่นคงปลอดภัยทางสารสนเทศที่แน่นหนาของซีเรียถูกเจาะ และมีแนวทางที่เป็นไปได้คือการส่งซอฟท์แวร์จำพวกมัลแวร์เข้าไปรบกวนการทำงานของเรดาร์ตรวจการณ์ซีเรีย รวมถึงสร้างเป้าลวงบนหน้าจอเรดาร์เพื่อไม่ให้เจ้าหน้าที่ของซีเรียเกิดความสงสัย หรืออิสราเอลส่งสายลับเข้าไปยังซีเรียเพื่อติดตั้งซอฟท์แวร์ประเภท Trapdoor หรือ Backdoor ลงในซอฟท์แวร์ควบคุมระบบของซีเรีย เพื่อไปรบกวนหรือทำลายระบบของซีเรีย หรือเพื่อเปิดช่องให้แฮกเกอร์ของอิสราเอลเข้ามาปฏิบัติภารกิจทางไซเบอร์ก่อนที่เครื่องบินจะโจมตีเพียงเล็กน้อย และมีการส่งสายลับเพื่อลักลอบตัดสายไฟเบอร์ออพติก ที่ใช้ในการเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ของกองทัพซีเรียแล้วพ่วงสายไฟเบอร์ออพติกดังกล่าวกับระบบเครือข่ายของแฮกเกอร์อิสราเอล และเมื่อถึงเวลา จะมีการส่งซอฟท์แวร์ทำลายระบบควบคุมอากาศยานของซีเรียผ่านเครือข่ายไฟเบอร์ออฟติกดังกล่าว

**๓. การโจมตีโรงงานผลิตอาวุธนิวเคลียร์ของประเทศอิหร่านด้วยมัลแวร์ Stuxnet** ถูกตรวจพบในปี ๒๕๕๓ เป้าหมายคือเครื่องหมุนเหวี่ยงสำหรับสกัดสารกัมมันตภาพรังสีใช้ในอาวุธนิวเคลียร์ที่ตั้งในโรงงานผลิตอาวุธนิวเคลียร์ประเทศอิหร่าน ทำให้ขีดความสามารถ ร้อยละ ๒๐ ของเครื่องมือไม่สามารถใช้งานได้ Stuxnet ใช้ซอฟท์แวร์ควบคุมการทำงานของเครื่องหมุนเหวี่ยงที่ผลิตโดย Siemens ซึ่งเป็นการโจมตีในระดับที่ลึกกว่าการโจมตีด้วยไวรัสบนเครื่องคอมพิวเตอร์ทั่วไป ถือว่าเป็นการโจมตีทางไซเบอร์ครั้งแรก ๆ ที่สร้างความเสียหายโดยตรงต่ออุปกรณ์หรือเครื่องมือที่เกี่ยวข้องกับการทหาร เป้าหมายในการพัฒนา Stuxnet นอกจากจะเป็นเรื่องของการโจมตีโรงงานผลิตอาวุธนิวเคลียร์แล้ว มีการคาดการณ์กันว่า Stuxnet ถูกพัฒนาขึ้นมาเพื่อโจมตีอุปกรณ์อิเล็กทรอนิกส์ที่ใช้ในการควบคุมการทำงานอื่น ๆ เช่นการผลิตไฟฟ้า น้ำประปา รวมไปถึงอุปกรณ์อิเล็กทรอนิกส์ที่ใช้ในโรงงานอุตสาหกรรม มีข้อสันนิษฐานว่า Stuxnet เป็นโครงการที่เกิดขึ้นด้วยความร่วมมือของผู้เชี่ยวชาญจากสหรัฐอเมริกา สหราชอาณาจักร อิสราเอล และเยอรมนี

**๔. การโจมตีทางไซเบอร์ในประเทศเกาหลีใต้ ใน พ.ศ.๒๕๕๒** เว็บไซต์ของหน่วยงานราชการ ธนาคาร และบริษัททางการเงินของเกาหลีใต้ ได้ถูกโจมตีด้วยวิธี DDoS จากเครื่องคอมพิวเตอร์ที่เป็น Zombies มีปริมาณระหว่าง ๒๐,๐๐๐ ถึง ๑๖๖,๐๐๐ เครื่อง เป็นระลอกใหญ่ ๆ รวม ๓ ระลอก โดยคาดการณ์กันว่าผู้ที่อยู่เบื้องหลังการโจมตีครั้งนี้คือเกาหลีเหนือ หลังจากนั้นถูกโจมตีอีกในเดือนมีนาคม พ.ศ.๒๕๕๔ ด้วยวิธีการที่คล้ายคลึงกัน เป้าหมายเป็นเว็บไซต์ของหน่วยงานรัฐบาลและบริษัทขนาดใหญ่ และเช่นเดียวกัน เกาหลีเหนือถูกกล่าวหาว่าอยู่เบื้องหลังในการโจมตี ต่อมาปี พ.ศ.๒๕๕๖ เกาหลีใต้ถูกโจมตีทางไซเบอร์อีกครั้ง ในครั้งนี้แตกต่างจากการถูกโจมตีในสองครั้งที่ผ่านมา โดยเป้าหมายเปลี่ยนจากการโจมตีเว็บไซต์มาเป็นการโจมตีระบบเครือข่าย และเครื่องคอมพิวเตอร์ของสถานีโทรทัศน์หลายช่อง รวมถึงธนาคารจำนวนหนึ่งได้ถูกโจมตีทางไซเบอร์จนไม่สามารถให้บริการได้ ซึ่งเกาหลีเหนือถูกตกเป็นจำเลยอีกครั้งในฐานะผู้อยู่เบื้องหลังการโจมตี แม้ว่าหมายเลขไอพีของผู้โจมตีจะเป็นหมายเลขไอพีของประเทศจีนก็ตาม แต่ก็มีการสันนิษฐานว่าหน่วยงานด้านสงครามไซเบอร์ของเกาหลีเหนือได้ใช้ไอพีที่ตรวจพบเป็นข้อมูลอำพรางตัวตนที่แท้จริงของผู้โจมตี

**๕. การหลุดของข้อมูลโทรเลขจากสถานทูตสหรัฐ** เหตุการณ์ที่ได้รับความสนใจจากรัฐบาลหลายประเทศ ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยทางสารสนเทศ รวมถึงแฮกเกอร์จากทั่วทุกมุมโลกเป็นอย่างมากเหตุการณ์หนึ่ง คือการหลุดของข้อมูลโทรเลขจากสถานทูตสหรัฐฯ ประจำประเทศต่าง ๆ และข้อมูลที่หลุดออกมาได้ถูกนำเผยแพร่ในเว็บไซต์ Wikileaks แม้โดยตัวต้นเหตุการณ์จะไม่ถือว่าเป็นเหตุการณ์ที่เป็นสงครามไซเบอร์โดยตรง แต่มีความเกี่ยวโยงกับสงครามไซเบอร์ย่อย ๆ อีกหลายเหตุการณ์เกี่ยวโยงกับความมั่นคงของหลายประเทศ รวมถึงความสัมพันธ์ระหว่างประเทศ และเป็นเหตุการณ์ที่ทำให้รัฐ หน่วยงานความมั่นคง รวมถึงนักวิชาการด้านรัฐศาสตร์ ต้องหันมา

ทบทวนในประเด็นที่ว่าด้วยบทบาทของรัฐที่ควรมีต่อประชาชน ความสัมพันธ์ระหว่างรัฐกับประชาชน และรัฐกับรัฐ การเผยแพร่ข้อมูลโทรเลขผ่าน Wikileaks ภายใต้นามเรียกขาน “Cablegate” ได้เริ่มขึ้นตั้งแต่ ๒๘ พฤศจิกายน พ.ศ.๒๕๕๓ โดย Wikileaks ทยอยเปิดเผยข้อมูลที่มีจนกระทั่งปัจจุบัน ข้อมูลที่เปิดเผยเป็นโทรเลขภายในของหน่วยงานภาครัฐของสหรัฐฯ ตั้งแต่ปี พ.ศ.๒๕๓๙ - ๒๕๕๓ จำนวนรวมทั้งสิ้น ๒๕๑,๒๘๗ ฉบับ โดยเป็นโทรเลขชั้นความลับ ๑๕,๖๕๒ ฉบับ และเป็นโทรเลขชั้นปกปิด จำนวน ๑๐๑,๗๘๔ ฉบับ มีการสืบทราบในภายหลังว่าโทรเลขดังกล่าวได้ถูกลักลอบออกจากสถานทูตโดย พลทหาร Bradley Manning ในขณะที่เขาประจำการที่ประเทศอิรัก และต่อมาเขาได้ถูกพิพากษาจำคุก ๓๕ ปี จากการกระทำดังกล่าว โดยเนื้อหาในโทรเลขแบ่งออกเป็นหัวข้อต่าง ๆ ตามที่ทางกระทรวงการต่างประเทศสหรัฐฯ กำหนด แต่หัวข้อที่ได้รับความสนใจและส่งผลกระทบมากที่สุดเป็นเรื่องเกี่ยวกับข้อมูลสถานการณ์ทางการเมืองภายในประเทศ การรายงานและการวิเคราะห์ประเมินพฤติกรรมของนักการเมืองของประเทศนั้น ๆ รวมถึงข้อมูลเชิงลึกที่ได้จากการพบปะพูดคุยระหว่างเจ้าหน้าที่จากสถานทูตสหรัฐฯ กับนักการเมือง และบุคลากรที่เกี่ยวข้อง ซึ่งข้อมูลที่ถูกเปิดเผยมีข้อมูลที่เกี่ยวข้องกับประเทศไทยรวมอยู่ด้วย ผลจากการเผยแพร่ข้อมูลของ Wikileaks ทำให้รัฐบาลของหลายประเทศโดยเฉพาะอย่างยิ่งสหรัฐฯ ต้องการนำผู้รับผิดชอบ และผู้ดูแลระบบของ Wikileaks มาดำเนินคดีในประเทศของตนเอง บุคคลผู้ที่ได้รับความสนใจที่สุดในบรรดาผู้ที่เกี่ยวข้องกับ Wikileaks คือ Julian Assange แฮกเกอร์และนักเคลื่อนไหวชาวออสเตรเลียผู้ก่อตั้งและผู้ดูแลด้านความปลอดภัยให้กับ Wikileaks

**๖. กลุ่มแฮกเกอร์ Anonymous ออกแถลงการณ์ถึงรัฐบาลไทยแสดงเจตนารมณ์ต่อต้านโครงการ Single Gateway** ของรัฐบาล โดยมองว่าตั้งขึ้นมาเพื่อจะควบคุม ยับยั้ง และจับกุมใครก็ตามที่ไม่เชื่อฟังคำสั่งของคณะรักษาความสงบแห่งชาติ อีกทั้งถือเป็นเรื่องยอมรับไม่ได้ที่มีการแต่งตั้งทหารมาควบคุมดูแลองค์กรสารสนเทศที่ใหญ่ที่สุด คือ บริษัท กสท โทรคมนาคม จำกัด (มหาชน) พร้อมระบุหน่วยงานหรือบุคคลใด ๆ ที่มีส่วนช่วยดำเนินการโครงการ Single Gateway จะตกเป็นเป้าโจมตีทางอิเล็กทรอนิกส์ทุกทาง และอ้างว่าจะประกาศเปิดโปงเรื่องคอร์รัปชั่น ผลประโยชนทับซ้อนต่าง ๆ และจะร่วมกันต่อต้านความยุติธรรมของรัฐบาลที่ปิดกั้นเสรีภาพขั้นพื้นฐานของประชาชนในการแสดงความคิดเห็น ต่อมาเมื่อ ๒๔ ตุลาคม พ.ศ.๒๕๕๘ รัฐบาลโดยกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารได้ให้ข้อมูลต่อสื่อมวลชลว่า ได้รับทราบและติดตามสถานการณ์มาตลอด มีการประสานงานเพื่อดำเนินมาตรการป้องกัน และอยู่เลยขั้นการแสดงความคิดเห็นคัดค้านโครงการ Single Gateway รวมทั้งรัฐบาลได้ยืนยันแล้วว่าไม่ได้ดำเนินการโครงการ Single Gateway แล้ว จากกรณีดังกล่าวแสดงให้เห็นว่าเป็นการกระทำที่ไม่ชอบด้วยเหตุผล และชักชวนกลุ่มคนทั้งในและต่างประเทศเข้ามาทำลายระบบคอมพิวเตอร์ของประเทศ ซึ่งผลกระทบไม่ได้

เกิดขึ้นกับภาครัฐฝ่ายเดียว แต่มีผลกระทบต่อระบบความมั่นคงทางไซเบอร์ของประเทศ และสิทธิส่วนบุคคลของประชาชนด้วย ดังนั้น

## สรุป

เทคโนโลยีในยุคดิจิทัลไทยแลนด์ เริ่มเห็นเป็นรูปธรรมบ้างแล้วโดยการเน็ตประชารัฐ มูลค่าสี่หมื่นล้านบาท ประชาชนที่อยู่ห่างไกลจะมีโอกาสใช้ระบบสื่อสารโทรคมนาคม ทั้งโทรศัพท์มือถือ อินเตอร์เน็ต เหมือนคนในเมือง และเชื่อว่าในปี ๒๕๖๓ ทุกครัวเรือนในโลกจะมีอุปกรณ์เชื่อมต่ออินเตอร์เน็ตอย่างน้อย ๑๐ เครื่อง มีผู้ใช้อินเตอร์เน็ตมากกว่า ๕,๐๐๐ ล้านราย ครึ่งหนึ่งเป็นการเชื่อมต่อผ่านทางอุปกรณ์แบบพกพา การเชื่อมโยงดังกล่าวแทรกซึมเข้าสู่ชีวิตประจำวันทั้งในบ้าน ที่ทำงาน สิ่งแวดล้อมต่าง ๆ ทุกที่ทุกเวลา จะมีเทคโนโลยีเข้ามาเกี่ยวข้องและภัยคุกคามที่มากับเทคโนโลยี ได้แก่ มัลแวร์ ไวรัส เวิร์ม อาชญากรรมไซเบอร์ เป็นสิ่งที่ควรจะตระหนักรู้ การรักษาความปลอดภัยไซเบอร์ ซึ่งหมายถึงกระบวนการที่จำเป็นเพื่อให้เกิดความปลอดภัยจากการใช้เทคโนโลยี มีความจำเป็นสำหรับองค์กรขนาดใหญ่เนื่องจากเป็นยุคที่ข้อมูลมีความสำคัญหากได้รับความเสียหายจะมีผลกระทบที่ประเมินค่าไม่ได้ สงครามไซเบอร์เป็นสิ่งที่เกิดขึ้นแล้วแต่สามารถป้องกันหรือลดความเสียหายได้ หากมีการเตรียมการที่ดี รูปแบบของการทำสงครามเริ่มมีแนวคิดใหม่เรียกว่าสงครามที่มีเครือข่ายเป็นศูนย์กลาง ซึ่งอาศัยความก้าวหน้าของเทคโนโลยีการสื่อสารและสารสนเทศเป็นตัวชี้วัดชัยชนะของสงครามตั้งแต่เริ่มต้น กองบัญชาการกองทัพไทย กองทัพบก กองทัพเรือ และกองทัพอากาศ ต่างมีแผนพัฒนาขีดความสามารถด้านนี้ แต่เนื่องจากเทคโนโลยีเปลี่ยนแปลงเร็วมาก การพัฒนาจำเป็นต้องอาศัยเวลาและทรัพยากรจำนวนมาก การที่ภาครัฐมีนโยบายส่งเสริมให้ทุกภาคส่วนเข้าถึงเทคโนโลยีด้วยการพัฒนาโครงสร้างพื้นฐานดิจิทัลประสิทธิภาพสูง หากองค์กรใดสามารถใช้ประโยชน์จากโอกาสนี้จะทำให้ประหยัดงบประมาณในการจัดหาสิ่งอุปกรณ์ต่าง ๆ ที่ซ้ำซ้อนไม่ต้องลงทุนเพิ่มเติมในสิ่งที่มีอยู่แล้ว สำหรับกองทัพเรือจะได้กล่าวถึงในบทต่อไป หน่วยงานความมั่นคงทางทะเลที่มีบทบาทนำในภูมิภาค

# บทที่ ๔
# หน่วยงานความมั่นคงทางทะเลที่มีบทบาทนำในภูมิภาค

หน่วยงานความมั่นคงทางทะเลที่มีบทบาทนำในภูมิภาคและเป็นเลิศในการบริหารจัดการ เป็นวิสัยทัศน์ของกองทัพเรือในปี ๒๕๕๗ โดยมุ่งเน้นการพัฒนากองทัพให้มีประสิทธิภาพเป็นที่เชื่อมั่นและไว้วางใจจากประชาชน โดยปฏิบัติการทางทหารเพื่อให้เกิดความได้เปรียบในการรักษาสิทธิและอำนาจอธิปไตยทางทะเล รักษาความมั่นคงและผลประโยชน์ของชาติ ปฏิบัติภารกิจตามที่รับมอบตั้งแต่ภาวะปกติเป็นความภูมิใจของคนในชาติ เสริมสร้างความมั่นคงทางทะเลในระดับนานาชาติเป็นเกียรติและศักดิ์ศรีในเวทีระหว่างประเทศ ให้ความสำคัญกับการพึ่งพาตนเอง ไม่มุ่นเน้นการแข่งขันเพื่อเสริมสร้างกำลังรบจนเกินความจำเป็น มีการกำกับดูแลองค์กรที่มีธรรมาภิบาล บริหารจัดการอย่างมาตรฐานมุ่งสู่ความเป็นเลิศ รับผิดชอบต่อสังคมเป็นสิ่งที่ยอมรับเชื่อถือในความโปร่งใสสุจริตมีคุณธรรมใช้เงินงบประมาณที่เป็นภาษีของประชาชนอย่างคุ้มค่าเป็นแบบอย่างที่ดีด้านการบริหารจัดการ และเป็นองค์กรแห่งการเรียนรู้มีประโยชน์ต่อสังคมโดยรวม

การที่โลกเริ่มเข้าสู่ยุคระบบเศรษฐกิจและสังคมที่เทคโนโลยีดิจิทัลไม่ได้เป็นเพียงเครื่องมือสนับสนุนการทำงานเช่นที่ผ่านมาอีกต่อไป แต่จะหลอมรวมเข้ากับชีวิตและเปลี่ยนโครงสร้างรูปแบบกิจกรรมทางสังคม การปฏิสัมพันธ์ระหว่างบุคคล โดยที่แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมของรัฐบาลปัจจุบัน มีเป้าหมายปฏิรูปประเทศสู่ดิจิทัลไทยแลนด์ อันหมายถึงประเทศไทยสามารถสร้างสรรค์และใช้ประโยชน์จากเทคโนโลยีอย่างเต็มศักยภาพ ก้าวข้ามกับดักประเทศที่มีรายได้ปานกลางอยู่ในกลุ่มประเทศที่พัฒนาแล้ว สร้างมูลค่าทางเศรษฐกิจและคุณค่างทางสังคมอย่างยั่งยืน ซึ่งก็ตรงกับวิสัยทัศน์ของกองทัพเรือต่อการสื่อสารและสารสนเทศ ที่จะเป็นองค์กรชั้นนำด้วยการประยุกต์ใช้การสื่อสารและเทคโนโลยีสารสนเทศในการบริหารจัดการและการปฏิบัติภารกิจอย่างเต็มรูปแบบ ในการนี้กองทัพเรือควรมีการปรับตัวและฉกฉวยโอกาสอย่างไรเพื่อให้ไปสู่จุดหมาย โดยสามารถใช้ทรัพยากรร่วมกับหน่วยงานอื่น ๆ ที่มีการพัฒนาตามแนวนโยบายรัฐบาล ซึ่งจะทำให้มิติงบประมาณด้านการจัดหายุทโธปกรณ์ต่ำลง เป็นประโยชน์ที่คาดว่าจะได้รับจากการวิจัยครั้งนี้และจะทำให้การสื่อสารและเทคโนโลยีสารสนเทศของกองทัพเรือ มีความสามารถรองรับสงครามที่มีเครือข่ายเป็นศูนย์กลาง

เพื่อให้รองรับการปฏิบัติการทางทหารในรูปแบบต่าง ๆ เตรียมความพร้อมในการเชื่อมต่อเครือข่ายการสื่อสารและเทคโนโลยีสารสนเทศด้านความมั่นคงกับหน่วยงานความมั่นคงภายในกระทรวงกลาโหม กองทัพเรือนานาชาติ กองทัพเรือได้วิเคราะห์ปัจจัยสภาวะแวดล้อม อุปสรรคและโอกาส พบว่ากองทัพเรือมีเครือข่ายการโทรคมนาคมที่ครอบคลุมพื้นที่ปฏิบัติการทางบก มีระบบสารสนเทศพื้นฐานในการบริหารงานและมีการพัฒนาระบบเชื่อมโยงข้อมูลทางยุทธวิธีให้กับเรือรองรับการติดต่อสื่อสารข้อมูลในพื้นที่ปฏิบัติการทางทะเล และด้วยภัยคุกคามรูปแบบใหม่ภารกิจที่เปลี่ยนแปลงไป ทำให้มีความจำเป็นต้องเตรียมความพร้อมในการพัฒนาโครงข่ายการสื่อสารสำหรับสนับสนุนการปฏิบัติงานในระดับยุทธวิธีในพื้นที่สำคัญทางบกเพิ่มเติม เช่น สามจังหวัดชายแดนภาคใต้ การแก้ไขปัญหาการทำประมงผิดกฎหมาย การบูรณาการกับศูนย์ประสานการปฏิบัติในการรักษาผลประโยชน์แห่งชาติในทะเล สงครามไซเบอร์ ในกรณีนี้ควรจะพิจารณาในเรื่องการพัฒนาโครงข่ายสื่อสารโทรคมนาคมให้เชื่อถือได้ รวดเร็ว ปลอดภัย เป็นมาตรฐาน ครอบคลุมพื้นที่ปฏิบัติการ การพัฒนาระบบสื่อสารและสารสนเทศ การพัฒนาระบบควบคุมบังคับบัญชา และการพัฒนาองค์บุคคล

**๑. เครือข่ายการสื่อสารโทรคมนาคม** ปัจจุบันกองทัพเรือมีเครือข่ายการสื่อสารโทรคมนาคม ครอบคลุมพื้นที่ปฏิบัติการได้แก่

๑.๑ การสื่อสารบนบก ระหว่างหน่วยขึ้นตรงและหน่วยเฉพาะกิจ การสื่อสารทางเสียงและข้อมูล ผ่านระบบโทรคมนาคมภาคพื้น วิทยุเชื่อมโยง สายสัญญาณความเร็วสูง เป็นข่ายหลัก ระบบการสื่อสารผ่านดาวเทียมเป็นข่ายรอง แบ่งออกเป็น ข่ายวิทยุเชื่อมโยง ทร. และข่ายการสื่อสารจาก บก.ทท. กับคู่สายสัญญาณความเร็วสูงจากเอกชน ซึ่งมีช่องสัญญาณจำกัด การพัฒนาระบบสงครามที่ใช้เครือข่ายเป็นศูนย์กลาง การแก้ไขปัญหาประมงผิดกฎหมาย การบูรณาการภาครัฐ และภารกิจที่เพิ่มเติมจำเป็นต้องเพิ่มช่องสัญญาณอีกจำนวนหนึ่ง

๑.๒ การสื่อสารกับเรือในทะเล มีทั้งทางเสียงและข้อมูล ด้วยความถี่ HF เป็นข่ายหลัก การสื่อสารผ่านดาวเทียมเป็นข่ายรอง การสื่อสารข้อมูลผ่านวิทยุ HF และระบบดาวเทียม C Band ใช้กับเรือที่มีคุณค่าทางยุทธการสูง

๑.๓ การสื่อสารระหว่างเรือในทะเล ทั้งทางยุทธการและทางยุทธวิธี ใช้การสื่อสารทางวิทยุเป็นข่ายหลัก ด้วย HF/SSB ในระยะไกล และ UHF ในระยะใกล้ ส่วนทางธุรการใช้ HF/SSB ในระยะไกล VHF ในระยะใกล้ การสื่อสารข้อมูลยังอยู่ระหว่างการทดลองใช้และต้องปรับปรุงอีกมากให้มีความเชื่อถือได้

๑.๔ การสื่อสารระหว่างเรือกับอากาศยาน ใช้วิธีการเดียวกับเรือในทะเลด้วยวิทยุ UHF และ VHF ส่วน HF/SSB ติดตั้งเฉพาะอากาศยานบางประเภท เมื่อเดินทางไปต่างประเทศ

๑.๕ การรักษาความปลอดภัยทางการสื่อสาร ระหว่างหน่วยบกใช้อุปกรณ์เข้ารหัสเชื่อมต่อกับโทรศัพท์และคอมพิวเตอร์ ระหว่างหน่วยเรือและหน่วยเรือกับฝั่งใช้ Frequency Hopping และอุปกรณ์เข้ารหัส

๑.๖ การสื่อสารระหว่างเหล่าทัพ และการสื่อสารกับต่างประเทศ เป็นการสื่อสารทางเสียงยังมีความต้องการการสื่อสารด้วยข้อมูลดิจิทัล

**๒. ระบบสื่อสารและสารสนเทศ** กองทัพเรือมีระบบประมวลผลกลาง และระบบเครือข่ายสารสนเทศที่เป็นมาตรฐานสากล สามารถใช้ได้กับเครือข่ายภายในและภายนอกกองทัพเรือผ่าน Proxy Server เพื่อเผยแพร่ข้อมูลและเพื่อการบริหาร โดยเป็นการพัฒนาระบบที่หน่วยงานต่าง ๆ สร้างขึ้น จึงยังไม่สามารถแลกเปลี่ยนข้อมูลกันได้ ในส่วนของการรักษาความปลอดภัยไซเบอร์มีห้องปฏิบัติการเครือข่าย ร่วมกับมาตรการรักษาความปลอดภัยที่ได้รับการับรองมาตรฐาน ISO มีขีดความสามารถในเชิงป้องกันและตรวจสอบช่องโหว่ต่าง ๆ ที่อาจเป็นช่องทางให้ถูกโจมตีทางไซเบอร์

**๓. ระบบควบคุมบังคับบัญชา** กองทัพเรือมีระบบควบคุมบังคับบัญชา จำนวน ๕ พื้นที่ ได้แก่ กรุงเทพฯ สัตหีบ ภาคตะวันออก อ่าวไทยตอนล่าง และทะเลอันดามัน เชื่อมต่อกับกองบัญชาการกองทัพไทย และหน่วยงานอื่น ๆ ผ่านเครือข่ายซึ่งมีขีดความสามารถในการแสดงภาพสถานการณ์ ประชุมผ่านทางไกล สนับสนุนการตัดสินใจของผู้บังคับบัญชา แต่ยังขาดการวิเคราะห์และกระจายข้อมูลไปยังหน่วยกำลังในพื้นที่ปฏิบัติการ การเชื่อมโยงข้อมูลทางยุทธวิธีสำหรับการปฏิบัติการร่วม ทร. ทอ. ใช้กับเรือที่มีคุณค่าทางยุทธการสูง ข้อมูลทางยุทธวิธีในการปฏิบัติการทางบก ใช้ระบบ Blue Force Tracking ติดตามตำบลที่ฝ่ายเดียวกันในพื้นที่จังหวัดชายแดนใต้

**๔. บุคลากร** กำลังพลของกองทัพเรือในระดับผู้บริหารยังขาดความเข้าใจในเทคโนโลยีที่เปลี่ยนแปลง ทำให้ขาดขีดความสามารถในการบริหารจัดการ แต่อย่างไรก็ดีมีการจ้างผู้เชี่ยวชาญจากภายนอกมาให้คำปรึกษาซึ่งมีค่าใช้จ่ายอยู่บ้าง ระดับผู้ใช้งานสามารถใช้อุปกรณ์ต่าง ๆ ได้ดี แต่ยังขาดความตระหนักรู้ในเรื่องการรักษาความปลอดภัย ระดับเจ้าหน้าที่เทคนิคมีความรู้ความเชี่ยวชาญสามารถแก้ปัญหาเฉพาะหน้าได้ แต่มีภาระงานมาก บุคลากรไม่เพียงเพียงพอ การซ่อมบำรุงอุปกรณ์มีขีดจำกัด หลายระบบต้องให้เอกชนดำเนินการ มีภาระในเรื่องซ่อมบำรุง

## การพัฒนาเครือข่ายโทรคมนาคม

แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม มีแผนในการพัฒนาโครงสร้างพื้นฐานดิจิทัลประสิทธิภาพสูงให้ครอบคลุมทั่วประเทศมีความทันสมัยมีเสถียรภาพตอบสนองความต้องการใช้งานด้วยราคาที่เหมาะสม เพื่อสร้างโอกาสการเข้าถึงเทคโนโลยีได้อย่างเท่าเทียม มีบริการอินเตอร์เน็ตความเร็วสูงเข้าถึงพื้นที่ทั่วประเทศ โครงข่ายสามารถเชื่อมต่อกันได้ในลักษณะแบบเปิด มีนโยบายบริหารกิจการดาวเทียมเพื่อให้มีการแข่งขันในการเข้าถึงวงโคจรดาวเทียมค้างฟ้า มีคลื่นความถี่ที่

เหมาะสมเพียงพอด้านความมั่นคงและบริหารจัดการภาวะวิกฤติ แผนดังกล่าวกองทัพเรือสามารถใช้ประโยชน์ในการพัฒนาเครือข่ายโทรคมนาคมให้เชื่อถือได้ รวดเร็ว ปลอดภัย เป็นมาตรฐาน และครอบคลุมพื้นที่ปฏิบัติการ รวมทั้งสามารถใช้ทรัพยากรร่วมกับหน่วยงานอื่น ๆ รองรับภารกิจเพิ่มขึ้นใหม่ เช่น การป้องกันการทำประมงผิดกฎหมาย การปฏิบัติการทางทหารนอกเหนือจากสงคราม ได้แก่

๑. พัฒนาและปรับปรุงระบบการบริหารจัดการเครือข่าย เพื่อดำรงความพร้อมของข่ายการสื่อสาร ลดปริมาณข้อมูลที่เกินความจำเป็น ควบคุมการใช้งานทางยุทธการ ทางธุรการ ให้มีลำดับความสำคัญเร่งด่วน ลดการใช้งานที่ไม่จำเป็นเนื่องจากมีช่องทางที่เหมาะสมปลอดภัยกว่า เครือข่ายมีความอ่อนตัว

๒. การขยายเครือข่ายดิจิทัลตั้งแต่ Back Bone จนถึง Last Mile กองทัพเรือมีแนวคิดที่จะใช้วิทยุเชื่อมโยงร่วมกับสายใยแก้วนำแสง โดยระยะแรกเพื่อเสริมขนาดช่องสัญญาณรองรับการขยายตัวในพื้นที่สัตหีบเป็นระบบฐานข้อมูลสำรอง และในระยะสุดท้ายสามารถใช้เครือข่ายของรัฐที่ครอบคลุมทั่วประเทศ เชื่อมโยงกับหน่วยงานความมั่นคงอื่น ๆ ตามนโยบาย นอกจากนี้ยังสามารถรองรับการขยายตัวของระบบ Logistic พื้นที่ภาคตะวันออกที่อยู่ระหว่างดำเนินได้ โดยสายใยแก้วนำแสงจะใช้ทดแทนระบบวิทยุเชื่อมโยง เส้นทางหลักในเขตเมืองส่วนเส้นทางรองใช้บริการของเอกชน เพื่อลดภาระงบประมาณการลงทุน ในกรณีนี้สถานีตรวจการณ์ต้องมีขนาดช่องสัญญาณเพื่อรองรับภาพสถานการณ์ ภาพเคลื่อนไหวจากกล้องตรวจการณ์และเชื่อมต่อสัญญาณกับระบบ Network Centric ได้

ห้องปฏิบัติการเครือข่าย (Network Captions Center) จัดให้มีการรักษาความปลอดภัย วิเคราะห์ Lag analysis เพื่อสืบค้นร่องรอยของผู้บุกรุกหรือผู้ไม่ประสงค์ดี

ระบบสื่อสารดาวเทียมเป็นการดำรงสภาพในปัจจุบัน เพื่อทดสอบ ทดลองระบบ ตามโครงการพัฒนาขีดความสามารถสำหรับสงครามที่ใช้เครือข่ายเป็นศูนย์กลาง โดยดำรงสภาพการใช้งาน C-Band บนบกและในทะเล เพื่อรองรับการใช้งานความถี่ X –Band ของกระทรวงกลาโหมเมื่อมี ความพร้อมและเนื่องจากนโยบายกิจการดาวเทียม เพื่อให้มีการแข่งขันในการเข้าถึงวงโคจรดาวเทียมค้างฟ้า ซึ่งคาดว่าจะมีคลื่นความถี่ที่เหมาะสมเพียงพอไม่เป็นภาระในด้านงบประมาณมากนัก ในกรณีนี้กองทัพเรือเคยใช้ดาวเทียม MVSAT สื่อสารข้อมูลความเร็วสูงรองรับการประชุมทางไกลผ่าน VDO Conference กับหมู่เรือปราบปรามโจรสลัดและชาติอื่น ๆ ที่มาปฏิบัติการร่วมกันที่โซมาเลีย ซึ่งสามารถติดต่อสื่อสารได้ทั้งทางโทรศัพท์ โทรสาร และข้อมูล ได้ทุกที่ ทุกเวลา แม้ว่าในทะเลจะมีคลื่นลม มีค่าใช้จ่ายอยู่บ้างแต่เป็นเครื่องพิสูจน์ว่าระบบสงครามที่ใช้เครือข่ายเป็นศูนย์กลางจำเป็นต้องพัฒนาต่อไป

การขยายการใช้งานระบบสื่อสารดาวเทียมของเอกชน เป็นอีกโครงการหนึ่งที่กองทัพเรือจะได้ประโยชน์ซึ่งขณะนี้กองทัพเรือใช้เมื่อมีความจำเป็นเนื่องจากมีค่าใช้จ่ายสูงและระบบการสื่อสารที่

มีอยู่ไม่สามารถรองรับได้ ดาวเทียมทางทหารยังไม่มีแนวทางที่ชัดเจนโดยเฉพาะการใช้งานบนเรือขนาดเล็ก หน่วยกำลังในพื้นที่ในย่านความถี่ X /Ku /L-Band

๓. ระบบสถานีวิทยุชายฝั่ง (HF) เป็นการสนับสนุนการควบคุมบังคับบัญชาระยะไกล ให้มีมาตรการรักษาความปลอดภัยข้อมูล รองรับปฏิบัติการทางเรือ การฝึกร่วมผสมระหว่างเหล่าทัพและนานาชาติ

๔. เครือข่ายโทรศัพท์พื้นฐาน นำเทคโนโลยีดิจิทัล Voice Over IP มาใช้แทนของเดิม เป็นการเปลี่ยนผ่านจากอนาล็อกเป็นดิจิทัลตามนโยบายดิจิทัลไทยแลนด์

๕. เครือข่ายวิทยุ (VHF /UHF) รวมถึงอุปกรณ์ทวนสัญญาณ การใช้งานระดับยุทธวิธี เปลี่ยนผ่านเป็นระบบดิจิทัลมีการเข้ารหัสเพื่อความปลอดภัยทางการสื่อสาร

การพัฒนาเครือข่ายโทรคมนาคมตามที่กล่าวนี้เพื่อเสริมสร้างรองรับสงครามที่ใช้เครือข่าย เป็นศูนย์กลาง ตามโครงการตั้งแต่ ๒๕๕๙ – ๒๕๖๘ โดยกำหนดขีดความสามารถที่ต้องการคือ มีอุปกรณ์ตรวจจับ สนับสนุนการตรวจการณ์ การเฝ้าตรวจ และการลาดตระเวนในระดับยุทธการและยุทธวิธี ในพื้นที่ปฏิบัติการเพื่อการแลกเปลี่ยนข้อมูลระหว่างหน่อยกำลังในทะเล บนบก กับศูนย์ปฏิบัติการกองทัพเรือ มีระบบควบคุมบังคับบัญชาระดับยุทธศาสตร์ ยุทธการ และยุทธวิธี ทีมีขีดความสามารถประเมินภาพสถานการณ์สนับสนุนผู้บังคับบัญชาในการควบคุมบังคับบัญชา การใช้อาวุธกับภัยคุกคาม ช่วยเหลือผู้ประสพภัยในทะเล เนื่องจากเป็นโครงการที่ใช้ระยะเวลาหลายปีเทคโนโลยีเปลี่ยนผ่านอย่างรวดเร็ว การวางแผนตัดสินใจลงทุนมีความจำเป็นต้องรู้เท่าทันเทคโนโลยี อีกทั้งหากมีการลดภาษีด้านเทคโนโลยีสารสนเทศเพื่อเป็นการส่งเสริมและเพิ่มประสิทธิภาพในการดำเนินธุรกิจพัฒนาไปสู่การแข่งขันระยะยาวจะส่งผลให้กองทัพปรับลดค่าใช้จ่ายในการจัดหาอุปกรณ์ที่จำเป็นต่อการดำเนินการได้

## การพัฒนาการสื่อสารและสารสนเทศ

ยุทธศาสตร์การพัฒนาโดยการปรับเปลี่ยนภาครัฐสู่การเป็นรัฐบาลดิจิทัล โดยการนำเทคโนโลยีมาใช้ปรับปรุงประสิทธิภาพการบริหารจัดการภาครัฐ หลอมรวมการทำงานภาครัฐเหมือนเป็นองค์กรเดียวกัน บริการภาครัฐมีธรรมาภิบาล สามารถบริการประชาชนแบบเบ็ดเสร็จ ณ จุดเดียว ผ่านระบบข้อมูลอัตโนมัติ การเปิดเผยข้อมูลภาครัฐไม่กระทบต่อสิทธิส่วนบุคคล และให้ความสำคัญกับการรักษาความปลอดภัยไซเบอร์ สร้างความเชื่อมั่นในการใช้เทคโนโลยี ลดอุปสรรคการประกอบกิจกรรมที่เกี่ยวข้องกับการใช้เอกสารอิเล็กทรอนิกส์ ไม่ต้องยื่นแบบฟอร์มกระดาษในการทำธุรกรรมกับภาครัฐ ยุทธศาสตร์นี้เป็นแรงผลักดันเสริมให้กองทัพจำเป็นต้องปรับตัวและนำแผนดังกล่าวไปพิจารณาประกอบการจัดทำแผนปฏิบัติงาน ในกรณีนี้กองทัพเรือมีระบบสื่อสารและสารสนเทศแบ่งเป็น ระบบสนับสนุนปฏิบัติการทางทหาร ระบบการบริหารงานทั่วไป และระบบภายในหน่วยงาน

ทั้งสามระบบนี้สามารถเชื่อมต่อกันได้ มีความต้องการฐานข้อมูลสำรอง และการรักษาความปลอดภัย ความเชื่อถือได้ ลดการใช้กระดาษ รวมถึงการปรับโครงสร้างหน่วยรองรับการจัดตั้งศูนย์บัญชาการไซเบอร์แห่งชาติ

๑. การรักษาความปลอดภัยด้านกายภาพ Physical and Environmental Security เป็นการป้องกันระบบไอทีจากภัยธรรมชาติ และการกระทำของคน เช่น การขโมย การลักลอบเข้าไปในพื้นที่หวงห้าม หรือ Data Center ซึ่งเป็นห้องคอร์สวิตซ์ของเน็ตเวิร์ค และไฟร์เซิร์ฟเวอร์ โดยมีสิ่งที่ต้องพิจารณาคือระบบไฟฟ้า ระบบปรับอากาศ การป้องกันอัคคีภัย วัสดุในอาคาร และมาตรการควบคุมการเข้าออก เนื่องจากปัจจุบันมี พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ซึ่งสามารถใช้หลักฐานทางดิจิทัลประกอบสำนวนนำไปร้องต่อศาลได้ ทำให้ผู้บริการระบบไอทีจำเป็นต้องเก็บล็อก (ประวัติการใช้ระบบไอที) อย่างน้อย ๓๐ วัน เพื่อใช้ตรวจพิสูจน์การกระทำของผู้ใช้งานระบบไอที ความสำคัญในการป้องกันระบบไอทีจึงมีความจำเป็นสำหรับผู้ให้บริการ

กองทัพเรือมี Data Center เป็นที่ใช้จัดวางระบบประมวลผลระบบเครือข่ายและล็อกสำหรับงานสารบัญอิเล็กทรอนิกส์ ผู้ใช้สามารถเชื่อมต่อผ่านเครือข่ายได้ทั้งภายในและภายนอกกองทัพเรือ ผ่าน Proxy Server ที่ออกแบบโดยใช้มาตรฐานสากล ควบคุมการเข้าออกโดยระบบสแกนลายนิ้วมือ มีเวรยามปฏิบัติงานตลอดทั้งวันไม่มีวันหยุดและอยู่ระหว่างการพัฒนา Recovery Site เป็นฐานข้อมูลสำรองเมื่อ Data Center ขัดข้อง

๒. การป้องกันการโจมตีจากมัลแวร์หรือแฮกเกอร์จากภายนอก ไฟร์วอลล์ (Firewall) หมายถึงกำแพงที่สร้างขึ้นเพื่อป้องกันไม่ให้ไฟไหม้ลามผ่านกำแพงมาได้ ทำให้พื้นที่ที่อยู่ข้างหลังปลอดภัยจากการถูกไฟไหม้ ไฟร์วอลล์ในรถยนต์เป็นแผ่นโลหะแยกส่วนของเครื่องยนต์และที่นั่งผู้โดยสารออกจากกัน ไฟร์วอลล์ในระบบไอที เป็นอุปกรณ์รักษาความปลอดภัยใช้สำหรับป้องกันไฟจากเครือข่ายอินเตอร์เน็ต เช่น มัลแวร์ แฮกเกอร์ลามเข้ามาในระบบเครือข่าย ป้องกันผู้ใช้ระบบไม่ให้ออกไปถูกไฟจากเครือข่ายภายนอก การที่องค์กรเชื่อมต่อโดยตรงกับอินเตอร์เน็ตโดยไม่ผ่านไฟร์วอลล์เป็นการเปิดช่องโหว่ให้ถูกโจมตีหรือบุกรุกได้อย่างง่ายดาย

กองทัพเรือป้องกันการบุกรุกจากภายนอกผ่านไฟร์วอลล์ที่มีมาตรฐานพร้อมโปรแกรมตรวจจับผู้บุกรุก Intrusion Detection System (IDS) และ Intrusion Prevention System (IPS) รองรับการทำสงครามไซเบอร์ และการใช้งานระบบสารสนเทศปกติ มีระบบการจำกัดสิทธิการเข้าใช้การยืนยันตัวบุคคล ซึ่งอยู่ระหว่างการพัฒนาระบบ SSO (Single Sign ON) มาใช้ยืนยันตัวบุคคลเป็นบัญชีผู้ใช้รายเดียวเช่นเดียวกับ Email

๓. ศูนย์สงครามไซเบอร์ (Cyber Warfare Center) เป็นแนวคิดที่อยู่ระหว่างดำเนินการเพื่อรองรับศูนย์บัญชาการไซเบอร์แห่งชาติกระทรวงกลาโหม ปัจจุบันกองทัพเรือมีหน่วยงานที่เกี่ยวข้องชื่อว่ากองสงครามไซเบอร์ เป็นหน่วยงานระดับกองขึ้นการบังคับบัญชากับสำนักปฏิบัติการ

กรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ มีหน้าที่วางแผน อำนวยการ กำกับการเกี่ยวกับการปฏิบัติสงครามไซเบอร์ พัฒนาขีดความสามารถองค์บุคคลเชิงรุกและเชิงรับ มีขอบเขตความรับผิดชอบในการกำหนดแนวทางมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ค้นหาจุดอ่อน ตรวจสอบและทดลองทดสอบระบบ เก็บข้อมูลและวิเคราะห์สถิติ ประเมินผล ติดตามรวบรวมข่าวสารด้านการรักษาความปลอดภัย มีหน่วยขึ้นตรงสามแผนกได้แก่ แผนกข้อมูลสงครามไซเบอร์ แผนกปฏิบัติการและแผนกรักษาความมั่นคงไซเบอร์

โครงสร้างดังกล่าวยังไม่เพียงพอกับสถานการณ์ไซเบอร์ปัจจุบัน ที่ภัยคุกคามเริ่มใกล้ตัวและทวีความรุนแรงมากขึ้น โครงสร้างใหม่นี้จะมีระดับนายพลเรือตรีเป็นหัวหน้าศูนย์ การพัฒนาศักยภาพในการปฏิบัติการจะเริ่มจากการพัฒนาในส่วนของการป้องกันเครือข่ายคอมพิวเตอร์ ป้องกันการถูกโจมตีผ่านทางไซเบอร์สเปซต่อระบบต่าง ๆ ในปฏิบัติการสงครามที่ใช้เครือข่ายเป็นศูนย์กลาง จากนั้นจึงพัฒนาการใช้ประโยชน์จากเครือข่ายในด้านการข่าวก่อนจะพัฒนาไปสู่การโจมตีที่ใช้กับฝ่ายตรงข้าม ซึ่งเทคนิคและวิธีการในการโจมตีนี้ก็เป็นประโยชน์ในการป้องกันฝ่ายตรงข้ามได้ด้วย แนวทางการดำเนินการต้องเตรียมความพร้อมสำคัญ ๓ ด้านคือ บุคลากร การบริหารจัดการ และเทคโนโลยี หรือ PPT (People , Process , Technology) เริ่มจากการฝึกอบรม จัดลำดับทำทำเนียบนักรบไซเบอร์ ประเมินผลรวม ทั้งให้สวัสดิการพิเศษ ป้องกันการถูกซื้อตัวจากองค์กรอื่น ๆ

## การพัฒนาระบบควบคุมบังคับบัญชา

เป็นแนวคิดตามการปรับโครงสร้างกองทัพเป็น Area Command Concept ระบบจะเชื่อมต่อกับเรดาร์ตรวจการณ์และส่วนใช้กำลังโดยอัตโนมัติ บูรณาการข่าวสารเพื่อสนับสนุนการแลกเปลี่ยนสถานการณ์กับหน่วยนอกกองทัพเรืออย่างปลอดภัย การเชื่อมโยงข้อมูลทางยุทธวิธีสนับสนุนการแสดงภาพสถานการณ์ สามารถควบคุมบังคับบัญชาได้ในลักษณะ Real Time ซึ่งจะต้องมีแนวทางดำเนินการได้แก่

๑. กำหนดมาตรฐานหลักนิยมการปฏิบัติตามห้วงเวลาที่เหมาะสมกับเทคโนโลยี โดยเฉพาะการบูรณาการกับหน่วยงานภายนอก เช่น กรมเจ้าท่า กรมประมง หน่วยงาน ศรชล. ตามภารกิจที่ได้รับมอบหมายเพิ่มเติม เช่นการแก้ปัญหาการทำประมงผิดกฎหมาย การค้ามนุษย์ และการป้องกันภัยพิบัติ

๒. การเชื่อมโยงข้อมูลทางยุทธวิธี สนับสนุนการควบคุมบังคับบัญชาระยะไกล เพื่อให้ได้ภาพสถานการณ์ครอบคลุมพื้นที่ปฏิบัติการ ซึ่งอาจใช้ทรัพยากรจากนโยบายไทยแลนด์ 4.0 เพื่อประหยัดงบประมาณในการลงทุน เช่นในพื้นที่จังหวัดชายแดนใต้ สามารถใช้เน็ตประชารัฐได้โดยกองทัพเรือไม่ต้องลงทุนเพิ่ม

๓. ด้านสงครามอิเล็กทรอนิกส์ มีการจัดตั้ง Electronic Warfare Support Center พัฒนาขีดความสามารถบุคลากรด้านสงครามอิเล็กทรอนิกส์

๔. ด้านสงครามไซเบอร์ จัดตั้งศูนย์สงครามไซเบอร์รองรับการปฏิบัติงานศูนย์ไซเบอร์แห่งชาติ ซึ่งจะต้องบูรณาการกับส่วนราชการทั้งภายนอกและในกระทรวงกลาโหม มีการฝึกอบรม สร้างเครือข่าย และแก้ไขร่างระเบียบปฏิบัติที่เปลี่ยนแปลงตามเทคโนโลยี

## การพัฒนาบุคลากร

หมายรวมถึงการพัฒนาองค์ความรู้ การจัดการความรู้เพื่อให้สามารถทำงานอย่างมีประสิทธิภาพ วัตถุประสงค์เพื่อพัฒนากำลังพลระดับต่าง ๆ ได้แก่ระดับผู้บริหาร ระดับเจ้าหน้าที่เทคนิค และผู้ใช้งานทั่วไป ให้มีความรู้ความชำนาญความรับผิดชอบ รองรับการเปลี่ยนแปลงที่จะเกิดขึ้น มีการกำหนดมาตรฐานตามสากล และจัดเก็บองค์ความรู้ทั้งในตัวบุคคลและในระบบ ให้สามารถปฏิบัติงานได้อย่างต่อเนื่อง สามารถทดแทนงานกันได้ในระดับที่ใกล้เคียงกัน โดย

๑. ศึกษาทิศทางการพัฒนาของเทคโนโลยี เพื่อนำมาใช้ในการกำหนดมาตรฐานของระบบสื่อสารและสารสนเทศที่ตอบสนองความต้องการสำหรับการจัดทำแผนพัฒนาระบบ กำหนดคุณลักษณะเฉพาะให้สามารถนำมาใช้งานได้จริง

๒. จัดทำและปรับปรุงระเบียบปฏิบัติ นโยบาย ให้สอดคล้องเท่าทันเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็ว

๓. กำหนดขีดสมรรถนะที่ต้องการ รวมถึงหลักสูตรการฝึกอบรมให้ครอบคลุมบุคลากรทุกระดับ บุคลากรมีตำแหน่งเลื่อนไหลตามขีดความสามารถและมีค่าตอบแทนที่เหมาะสมเป็นแรงจูงใจในการปฏิบัติงาน

## กองทัพไซเบอร์

การพัฒนาศักยภาพในการปฏิบัติการไซเบอร์ ประกอบด้วยองค์ประกอบ ๓ ส่วน ได้แก่ บุคลากร กระบวนการ และเทคโนโลยี ซึ่งในส่วนของเทคโนโลยีจะหมายถึงเครื่องมือหรืออาวุธไซเบอร์ ส่วนกระบวนการคือรูปแบบหรือขั้นตอนในการทำสงครามซึ่งก็คือ CNO

CNO (Computer Network Operation) เป็นขีดความสามารถสุดท้ายที่เพิ่มเข้าไปในขีดความสามารถหลักของปฏิบัติการข่าวสาร (IC) สาเหตุหลักเนื่องมาจากมีการใช้เครือข่ายคอมพิวเตอร์และเทคโนโลยีสารสนเทศในทางทหารอย่างแพร่หลาย CNO จะใช้ร่วมกับ EW (Electronics Warfare) เพื่อการโจมตี ลดประสิทธิภาพ การลวง การกวน ขัดขวางและใช้ประโยชน์

ในอีกความหมายของ CNO คือ การใช้ประโยชน์จากเครือข่ายคอมพิวเตอร์ การโจมตีเครือข่าย และการป้องกันเครือข่าย

ส่วนบุคลากร คือ นักรบไซเบอร์ ที่ต้องมีการฝึกให้พร้อมปฏิบัติหน้าที่ อาจกล่าวได้ว่าอาวุธจะไม่มีประโยชน์ถ้าคนไม่รู้จักวิธีใช้ นักเจาะระบบหรือแฮกเกอร์คือผู้ที่จะใช้อาวุธหรือเครื่องมือเพื่อที่จะโจมตีในรูปแบบต่าง ๆ แฮกเกอร์มีหลายประเภทตามที่ได้กล่าวไว้แล้ว ส่วนนักรบไซเบอร์หมายถึงคนที่จะทำหน้าที่ปฏิบัติการเครือข่ายคอมพิวเตอร์ตามภารกิจที่ได้รับมอบหมาย เพื่อบรรลุวัตถุประสงค์ในทางทหาร ซึ่งอาจจะเป็นการใช้ประโยชน์จากเครือข่ายคอมพิวเตอร์ การโจมตีหรือการปกป้องเครือข่าย ดังนั้นความสามารถของนักรบจะขึ้นอยู่กับภารกิจที่ได้รับมอบและความรับผิดชอบส่วนบุคคล ทั้งนี้ต้องมีการฝึกและทดสอบอย่างต่อเนื่อง

คุณสมบัติที่สำคัญของนักรับ คือ ความรู้ ความชำนาญเฉพาะด้าน เนื่องจากวิทยาการด้านการรักษาความปลอดภัยข้อมูลนั้นเป็นวิทยาการใหม่เมื่อเทียบกับวิทยาการด้านอื่น ๆ จึงอาจไม่มีรูปแบบการฝึกที่เป็นมาตรฐานตายตัว และจำเป็นต้องมีความรู้พื้นฐานด้านอื่น ๆ มาก่อน ความรู้เกิดจากการศึกษาอาจหมายถึงคุณวุฒิที่ได้รับก่อนมาทำหน้าที่ในสายวิทยาการรักษาความปลอดภัย ส่วนใหญ่แล้วนักรบไซเบอร์ควรจบการศึกษาระดับปริญญาตรีมีจำนวนมากที่จบปริญญาโท คนที่จบสายเทคนิคไม่ว่าจะเป็นวิทยาการคอมพิวเตอร์ วิศวกรรมคอมพิวเตอร์ เทคโนโลยีสารสนเทศ หรือสาขาอื่นที่ใกล้เคียง เป็นสาขาที่จบแล้วสามารถปฏิบัติงานได้ทันที

การฝึกอบรมนักรบไซเบอร์ที่ได้มาตรฐานและใบรับรองที่ได้รับการยอมรับมากที่สุดคือ CISSP (Certified Information System Security Professional) ออกให้โดยสถาบันนานาชาติ ISC (International Information System Security Certification Consortium)

การบรรจุนักรบไซเบอร์เข้ารับราชการ อาจแบ่งเป็น ๒ สายคือ สายเทคนิค และสายบริการ แต่ละสายแบ่งความชำนาญออกเป็น ๓ ระดับได้แก่

ระดับที่ ๑ มีความชำนาญและประสบการณ์ต่ำสุดมีความรู้เบื้องต้นเกี่ยวกับไอทีทั่ว ๆ ไป

ระดับที่ ๒ มีความชำนาญและประสบการณ์ระดับกลาง มีความรู้ด้านเครือข่ายเป็นสำคัญ

ระดับ ๓ มีความชำนาญและประสบการณ์สูงสุด จะได้รับมอบหมายให้ทำงานที่มีชั้นความลับ

ในขั้นต้นอาจมีความยากลำบากที่จะจัดระดับทั้ง ๓ นี้ แต่เมื่อได้ทำงานแล้วระยะหนึ่งควรมีการปรับระดับตามตำแหน่งงานนี้เพื่อให้เกิดความเลื่อนไหลของการปฏิบัติราชการ

## สรุป

หน่วยงานความมั่นคงทางทะเลที่มีบทบาทนำในภูมิภาคและเป็นเลิศในการจัดการ เป็นวิสัยทัศน์ของกองทัพเรือในปี ๒๕๕๗ ซึ่งสอดคล้องกับเป้าหมายของรัฐบาลที่จะให้ประเทศไทยก้าวข้ามกับดักประเทศที่มีรายได้ปานกลาง ไปอยู่ในกลุ่มประเทศที่พัฒนาโดยใช้แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นเครื่องมือ และเพื่อให้รองรับปฏิบัติการทางทหารกองทัพเรือจำเป็นต้องพัฒนาขีดความสามารถของเครือข่ายการสื่อสารโทรคมนาคม ระบบสื่อสารและสารสนเทศ ระบบควบคุมบังคับบัญชา พร้อม ๆ กับการพัฒนาบุคลากร

การพัฒนาเครือข่ายโทรคมนาคม ส่วนหนึ่งสามารถบูรณาการร่วมกับหน่วยงานอื่นได้ เนื่องจากรัฐบาลมีโครงสร้างพื้นฐานดิจิทัลประสิทธิภาพสูง การพัฒนาการสื่อสารและสารสนเทศจะต้องเพิ่มการรักษาความปลอดภัยด้านกายภาพ การป้องกันการโจมตีจากมัลแวร์หรือแฮกเกอร์จากภายนอก และจัดตั้งศูนย์สงครามไซเบอร์ ระบบควบคุมบังคับบัญชาสามารถแสดงภาพสถานการณ์ได้ในลักษณะ Real Time และการพัฒนาบุคลากรจำเป็นต้องมีมาตรฐานที่เป็นสากล จนมีขีดความสามารถเป็นกองทัพไซเบอร์ ตามแนวความคิดการทำสงครามที่ใช้เครือข่ายเป็นศูนย์กลางได้

# บทที่ ๕
# สรุปและข้อเสนอแนะ

## สรุป

ผู้วิจัยได้ศึกษาแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม ทิศทางการบริหารประเทศ ความท้าทายและโอกาส จากพลวัตของเทคโนโลยีดิจิทัล และต้องการเสนอแนวทางในการพัฒนากองทัพ โดยคาดหวังว่าประโยชน์ที่ได้รับ จะทำให้กองทัพเรือมีขีดความสามารถรองรับสงครามที่มีเครือข่ายเป็นศูนย์กลาง โดยความเป็นมาและความสำคัญของปัญหาอยู่ที่แผนดังกล่าว มีผลให้ทุกกระทรวง กรม รัฐวิสาหกิจ หน่วยงานของรัฐ ต้องนำแผนไปประกอบการจัดทำแผนปฏิบัติงานและคำของบประมาณรายจ่ายประจำปี

บริบทของประเทศไทยในยุคดิจิทัล ประชาชนจะมีโอกาสสร้างรายได้จากการนำไอซีทีมาเป็นเครื่องมือสนับสนุนการพัฒนาประเทศ มีอินเตอร์เน็ตความเร็วสูงกระจายอย่างทั่วถึง รวมถึงมีคุณภาพชีวิตที่ดีขึ้น การทำธุรกรรมผ่านทางออนไลน์ จะมีกฎระเบียบที่ใช้ปฏิบัติได้จริง ทันต่อการเปลี่ยนแปลงทางเทคโนโลยี โดยมีเป้าหมายของการพัฒนา ๔ ระยะ ใช้เวลา ๒๐ ปี ผ่านแผนยุทธศาสตร์ ๖ แผน ได้แก่ การพัฒนาโครงสร้างพื้นฐานดิจิทัลประสิทธิภาพสูง การขับเคลื่อนเศรษฐกิจด้วยเทคโนโลยี สร้างสังคมคุณภาพที่ทั่วถึงและเท่าเทียม ปรับเปลี่ยนภาครัฐสู่การเป็นรัฐบาลดิจิทัล พัฒนากำลังคนให้พร้อมเข้าสู่ยุคเศรษฐกิจและสังคมดิจิทัล และการสร้างความเชื่อมั่นในการใช้เทคโนโลยี มีกลไกขับเคลื่อนด้วยกิจกรรมภายใต้การเปลี่ยนแปลงโครงสร้างเชิงสถาบันบูรณาการการจัดสรรทรัพยากร และติดตามความก้าวหน้าของแผนงาน นอกจากนี้คณะรัฐมนตรี และผู้มีส่วนได้เสียต่างก็มีความเห็นสอดคล้องไปในแนวทางเดียวกัน เห็นด้วยกับแผนดังกล่าว ผู้มีส่วนได้เสียบางหน่วยงาน เช่น สำนักงาน กสทช. เห็นว่ามีหลายประเด็นที่ทับซ้อนกับอำนาจหน้าที่ของ กสทช. และหลายหน่วยงานมีความเป็นห่วงในเรื่องของความปลอดภัยไซเบอร์

เทคโนโลยีในยุคดิจิทัลไทยแลนด์ เริ่มเห็นเป็นรูปธรรมบ้างแล้วโดยโครงการเน็ตประชารัฐมูลค่าสี่หมื่นล้านบาท ประชาชนที่อยู่ห่างไกลจะมีโอกาสใช้ระบบสื่อสารโทรคมนาคม ทั้งโทรศัพท์มือถือ อินเตอร์เน็ต เหมือนคนในเมือง และเชื่อว่าในปี ๒๕๖๓ ทุกครัวเรือนในโลกจะมีอุปกรณ์เชื่อมต่ออินเตอร์เน็ตอย่างน้อย ๑๐ เครื่อง มีผู้ใช้อินเตอร์เน็ตมากกว่า ๕,๐๐๐ ล้านรายครึ่งหนึ่งเป็นการเชื่อมต่อผ่านทางอุปกรณ์แบบพกพา การเชื่อมโยงดังกล่าวแทรกซึมเข้าสู่ชีวิตประจำวันทั้งในบ้าน ที่ทำงาน สิ่งแวดล้อมต่าง ๆ ทุกที่ทุกเวลา จะมีเทคโนโลยีเข้ามาเกี่ยวข้อง

และภัยคุกคามที่มากับเทคโนโลยี ได้แก่ มัลแวร์ ไวรัส เวิร์ม อาชญากรรมไซเบอร์ เป็นสิ่งที่ควรจะตระหนักรู้ การรักษาความปลอดภัยไซเบอร์ ซึ่งหมายถึงกระบวนการที่จำเป็นเพื่อให้เกิดความปลอดภัยจากการใช้เทคโนโลยี มีความจำเป็นสำหรับองค์กรขนาดใหญ่เนื่องจากเป็นยุคที่ข้อมูลมีความสำคัญหากได้รับความเสียหายจะมีผลกระทบที่ประเมินค่าไม่ได้ รูปแบบของการทำสงครามเริ่มมีแนวคิดใหม่เรียกว่าสงครามที่มีเครือข่ายเป็นศูนย์กลาง ซึ่งอาศัยความก้าวหน้าของเทคโนโลยีการสื่อสาร และสารสนเทศเป็นตัวชี้วัดชัยชนะของสงครามตั้งแต่เริ่มต้น กองบัญชาการกองทัพไทย กองทัพบก กองทัพเรือ และกองทัพอากาศ ต่างมีแผนพัฒนาขีดความสามารถด้านนี้ แต่เนื่องจากเทคโนโลยีเปลี่ยนแปลงเร็วมาก การพัฒนาจำเป็นต้องอาศัยเวลาและทรัพยากรจำนวนมาก การที่ภาครัฐมีนโยบายส่งเสริมให้ทุกภาคส่วนเข้าถึงเทคโนโลยีด้วยการพัฒนาโครงสร้างพื้นฐานดิจิทัลประสิทธิภาพสูง หากองค์กรใดสามารถใช้ประโยชน์จากโอกาสนี้จะทำให้ประหยัดงบประมาณในการจัดหาสิ่งอุปกรณ์ต่าง ๆ ที่ซ้ำซ้อนไม่ต้องลงทุนเพิ่มเติมในสิ่งที่มีอยู่แล้ว

หน่วยงานความมั่นคงทางทะเลที่มีบทบาทนำในภูมิภาคและเป็นเลิศในการจัดการ เป็นวิสัยทัศน์ของกองทัพเรือในปี ๒๕๕๗ ซึ่งสอดคล้องกับเป้าหมายของรัฐบาลที่จะให้ประเทศไทยก้าวข้ามกับดักประเทศที่มีรายได้ปานกลาง ไปอยู่ในกลุ่มประเทศที่พัฒนาโดยใช้แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นเครื่องมือ สำหรับกองทัพเรือเมื่อวิเคราะห์ปัจจัยสภาวะแวดล้อม อุปสรรค์และโอกาส พบว่ากองทัพเรือมีเครือข่ายโทรคมนาคมที่ครอบคลุมพื้นที่ปฏิบัติการทางบก มีระบบสารสนเทศพื้นฐานในการบริหารงานทั่วไป และมีระบบเชื่อมโยงข้อมูลทางยุทธวิธีกับเรือในทะเล การที่จะเป็นหน่วยงานความมั่นคงทางทะเลที่มีบทบาทนำในภูมิภาคและรองรับภัยคุกคามในรูปแบบใหม่จำเป็นต้องเตรียมความพร้อมในการพัฒนาเครือข่ายสำหรับการปฏิบัติงานทางยุทธวิธีในจังหวัดชายแดนใต้ สงครามที่ใช้เครือข่ายเป็นศูนย์กลางจำเป็นต้องดำเนินการในเรื่องการพัฒนาเครือข่ายโทรคมนาคม ระบบสารสนเทศ ระบบควบคุมบังคับบัญชา และพัฒนาบุคลากร

การพัฒนาเครือข่ายโทรคมนาคมด้วยการปรับปรุงระบบบริหารเครือข่าย ขยายเครือข่ายดิจิทัลให้เชื่อมโยงกับเครือข่ายของรัฐบาล โดยเฉพาะในพื้นที่ภาคตะวันออกที่อยู่ระหว่างดำเนินการดำรงสภาพการสื่อสารดาวเทียม C - Band เพื่อรองรับการใช้ความถี่ X - Band เมื่อมีความพร้อม ระบบวิทยุชายฝั่ง (HF) มีการรักษาความปลอดภัยข้อมูลรองรับการปฏิบัติการทางทะเล โทรศัพท์พื้นฐานเปลี่ยนเป็นเทคโนโลยีดิจิทัล Voice over IP ทดแทนของเดิม รวมถึงวิทยุ VHF/UHF เปลี่ยนไปใช้เป็นระบบดิจิทัลที่มีการเข้ารหัส

ระบบสารสนเทศปรับปรุงด้านการรักษาความปลอดภัยทางกายภาพ เป็นการป้องกันระบบไอทีจากภัยธรรมชาติ การกระทำของคน เช่นการขโมย การลักลอบเข้าพื้นที่หวงห้าม การป้องกันการโจมตีจากมัลแวร์หรือแฮกเกอร์จากภายนอกด้วยไฟร์วอลล์ที่มีมาตรฐาน มีโปรแกรมตรวจจับผู้บุกรุกรองรับปฏิบัติการสงครามไซเบอร์

ระบบควบคุมบังคับบัญชา $C^3I$ สามารถเชื่อมโยงข้อมูลทางยุทธวิธีสนับสนุนการแสดงภาพสถานการณ์ได้ในลักษณะ Real Time มีหลักนิยมเชื่อมต่อหน่วยงาน เช่น กรมเจ้าท่า กระประมง กรมศุลกากร ศรชล. โดยอาจใช้นโยบายไทยแลนด์ 4.0 ดำเนินการ เพื่อไม่ให้เกิดการลงทุนที่ซ้ำซ้อน

การพัฒนาบุคลากรเพื่อให้ผู้บริหาร เจ้าหน้าที่เทคนิค และผู้ใช้งานทั่วไป มีความรู้ ความชำนาญ และความรับผิดชอบ รองรับการเปลี่ยนแปลงโดยศึกษาทิศทางการพัฒนาเทคโนโลยี ปรับปรุงกฎระเบียบ และกำหนดขีดสมรรถนะ

สงครามไซเบอร์เป็นสิ่งที่เกิดขึ้นแล้ว เช่น การโจมตีโรงงานผลิตอาวุธนิวเคลียร์ของอิหร่านด้วยมัลแวร์ Stuxnet การโจมตีทางไซเบอร์ในเอสโทเนีย ปฏิบัติการ Orchard ที่อิสราเอลใช้เครื่องบินเข้าไปทิ้งระเบิดอาคารผลิตอาวุธนิวเคลียร์ของซีเรีย โดยที่เรดาร์ตรวจการณ์ของซีเรียไม่สามารถตรวจจับอะไรได้เลย นอกจากนี้มีแนวโน้มที่หลายชาติเริ่มเตรียมการเพื่อทำสงครามโดยการเจาะเข้าสู่เครือข่ายคอมพิวเตอร์และโครงสร้างสาธารณูปโภคซึ่งกันและกัน พร้อมกับจัดวางแทรปดอร์หรือลอจิกบอมบ์ ซึ่งเป็นอาวุธในทางไซเบอร์ เมื่อวันเวลาที่รอคอยมาถึง เครือข่ายคอมพิวเตอร์เหล่านั้นจะถูกควบคุมให้ทำสิ่งแปลก ๆ ออกมา เช่น โอนเงินจำนวนมาก ปล่อยน้ำมันให้รั่วไหลทิ้ง ปิดวาล์วปล่อยก๊าซ ทำให้รถไฟตกราง สิ่งต่าง ๆ เหล่านี้สามารถป้องกันหรือลดความเสียหายได้หากมีการเตรียมการที่ดี กองทัพไซเบอร์จึงเป็นขีดความสามารถที่พึงมีเพื่อป้องกันเหตุร้ายดังกล่าวในเวลาปกติ โดยมีองค์ประกอบ ๓ ส่วน ได้แก่ บุคลากร กระบวนการ และเทคโนโลยี แต่เนื่องจากวิทยาการด้านการรักษาความปลอดภัยไซเบอร์เป็นเรื่องใหม่ไม่มีรูปแบบที่ตายตัว การฝึกอบรมที่ได้มาตรฐานจึงมีความจำเป็นเพื่อให้สอดคล้องกับกระบวนการและเทคโนโลยีของกองทัพเรือต่อไป

## ข้อเสนอแนะ

เทคโนโลยีดิจิทัลมีการเปลี่ยนแปลงอย่างรวดเร็วตลอดเวลายากต่อการคาดเดา การวางแผนจำเป็นต้องตระหนักรู้และเท่าทันการเปลี่ยนแปลงของเทคโนโลยี รวมถึงนัยของการเปลี่ยนแปลงนั้น ๆ เทคโนโลยีเหล่านี้เป็นเรื่องที่มีความสัมพันธ์กันไม่อาจมองแบบแยกส่วน การนำมาใช้ประโยชน์โดยการหลอมรวมกันอย่างเหมาะสมลงตัวจึงจะเกิดผลดีกับการพัฒนาประเทศ การติดตามการเปลี่ยนแปลงอย่างใกล้ชิดจะทำให้ไม่ตกขบวนรถไฟและไม่ถูกทอดทิ้งไว้ข้างหลัง

การพัฒนาเครือข่ายโทรคมนาคม ส่วนหนึ่งสามารถบูรณาการร่วมกับหน่วยงานอื่นได้ เนื่องจากรัฐบาลมีโครงสร้างพื้นฐานดิจิทัลประสิทธิภาพสูง การพัฒนาการสื่อสารและสารสนเทศจะต้องเพิ่มการรักษาความปลอดภัยด้านกายภาพ การป้องกันการโจมตีจากมัลแวร์หรือแฮกเกอร์จากภายนอก และจัดตั้งศูนย์สงครามไซเบอร์ ระบบควบคุมบังคับบัญชาสามารถแสดงภาพสถานการณ์ได้ในลักษณะ Real Time และการพัฒนาบุคลากรจำเป็นต้องมีมาตรฐานที่เป็นสากล จนมีขีดความสามารถเป็นกองทัพไซเบอร์ ตามแนวความคิดการทำสงครามที่ใช้เครือข่ายเป็นศูนย์กลางได้

# บรรณานุกรม

## ภาษาไทย

### หนังสือ

ธเรศ ปุณศรี,พลอากาศเอก. ชุมชนดิจิทัลไทยแลนด์ 2020. สำนักงานคณะกรรมการกิจการกระจายเสียงและกิจการโทรคมนาคมแห่งชาติ.

คลาร์ก ริชาร์ด เอ. สงครามไซเบอร์-Cyber War. กรุงเทพมหานคร : มติชน, ๒๕๕๕. ๔๑๖ หน้า.

เทคโนโลยีสารสนเทศและการสื่อสาร,กระทรวง. แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม. :กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, พฤษภาคม ๒๕๕๙.

# ประวัติย่อผู้วิจัย

**ชื่อ** พลเรือตรี วิศณุ สร้างวงศ์ใหม่

**วัน เดือน ปีเกิด** เกิดเมื่อวันที่ ๑๕ ก.พ.๒๕๐๕

**การศึกษา** ระดับมัธยมศึกษา โรงเรียนเทพศิรินทร์ พ.ศ.๒๕๒๐

ระดับอุดมศึกษา ปริญญาตรีวิทยาศาสตร์บัณฑิต โรงเรียนนายเรือ พ.ศ.๒๕๒๖

หลักสูตรเสนาธิการทหารเรือ รุ่นที่ ๕๔

หลักสูตรวิทยาลัยการทัพเรือ รุ่นที่ ๓๙

**ประวัติการทำงานโดยย่อ**

ผู้อำนวยการกองจัดการขนส่ง กรมการขนส่งทหารเรือ

ผู้อำนวยการกองการสงเคราะห์ กรมสวัสดิการทหารเรือ

ผู้อำนวยการกองตรวจทั่วไป กรมจเรทหารเรือ

เสนาธิการ กองเรือฟริเกตที่ ๒ กองเรือยุทธการ

รองเสนาธิการ ทัพเรือภาคที่ ๒

**ตำแหน่งปัจจุบัน** ผู้อำนวยการสำนักปฏิบัติการ กรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ

# สรุปย่อ

**ลักษณะวิชา วิทยาศาสตร์และเทคโนโลยี**

**เรื่อง แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมกับกองทัพเรือ**

**ผู้วิจัย พล.ร.ต.วิศณุ สร้างวงศ์ใหม่ หลักสูตร วปอ. รุ่นที่ ๖๐**

**ตำแหน่ง ผู้อำนวยการสำนักปฏิบัติการ กรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ**

## ความเป็นมาและความสำคัญของปัญหา

แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ได้รับความเห็นชอบจาก ครม. เมื่อ ๕ เม.ย.๕๙ มีผลให้ทุกกระทรวง รัฐวิสาหกิจ หน่วยงานของรัฐ ต้องนำแผนดังกล่าวไปประกอบการจัดทำแผนปฏิบัติงาน และคำของบประมาณประจำปี

โดยแผนดังกล่าวมีวิสัยทัศน์และเป้าหมายในการพัฒนาอย่างต่อเนื่อง ระยะยาว สอดคล้องกับยุทธศาสตร์ชาติ ๒๐ ปี มีแนวทางแบ่งออกเป็น ๔ ระยะ ได้แก่

ระยะที่ ๑ ใช้เวลา ๑ ปี ๖ เดือน เป็นการลงทุนสร้างรากฐานในการพัฒนาเศรษฐกิจและสังคมดิจิทัล

ระยะที่ ๒ ใช้เวลา ๕ ปี ทุกภาคส่วนมีส่วนร่วม

ระยะที่ ๓ ใช้เวลา ๑๐ ปี ก้าวสู่ดิจิทัลไทยแลนด์ ประเทศไทยขับเคลื่อนและใช้ประโยชน์จากนวัตกรรมอย่างเต็มศักยภาพ

ระยะที่ ๔ จาก ๑๐ - ๒๐ ปี ประเทศไทยอยู่ในกลุ่มประเทศที่พัฒนาแล้ว สามารถใช้เทคโนโลยีสร้างมูลค่าทางเศรษฐกิจอย่างยั่งยืน

ในส่วนของกองทัพเรือมีวิสัยทัศน์ที่จะเป็นหน่วยงานความมั่นคงทางทะเลที่มีบทบาทนำในภูมิภาค ซึ่งก็เป็นเป้าหมายเดียวกันกับยุทธศาสตร์ชาติ ที่ต้องการเป็นประเทศในกลุ่มพัฒนาแล้ว ในระยะ ๒๐ ปี การที่รัฐบาลมีการพัฒนาโครงสร้างพื้นฐานดิจิทัลประสิทธิภาพสูงให้ครอบคลุมทั่วประเทศ เป็นโอกาสของกองทัพที่จะใช้โครงสร้างนี้พัฒนาร่วมกับเครือข่ายโทรคมนาคมเดิมของกองทัพ ซึ่งจะทำให้ประหยัดงบประมาณในการจัดหายุทโธปกรณ์ที่ซ้ำซ้อน และเนื่องจากเทคโนโลยีมีการเปลี่ยนแปลงอย่างรวดเร็วตลอดเวลาอยากต่อการคาดเดา การวางแผนจำเป็นต้องตระหนักรู้และเท่าทันการเปลี่ยนแปลงของเทคโนโลยีในอนาคต รวมถึงนัยของการเปลี่ยนแปลงนั้น ๆ ซึ่งเป็นความสำคัญของปัญหาที่จะดำเนินการวิจัย

## วัตถุประสงค์ของการวิจัย

๑. ศึกษาแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ทิศทางการบริหารประเทศ ความท้าทายและโอกาสของประเทศ ความท้าทายจากพลวัตของเทคโนโลยีดิจิทัล และสถานภาพการพัฒนาด้วยดิจิทัลในประเทศ

๒. เสนอแนะแนวทางในการพัฒนาการสื่อสารและเทคโนโลยีสารสนเทศ ของกองทัพเรือในส่วนขององค์วัตถุ องค์บุคคล ความรู้ หลักนิยม และปฏิบัติการทางทหาร เตรียมความพร้อมในการเชื่อมต่อเครือข่ายโทรคมนาคมกับหน่วยงานอื่น ๆ เพื่อบูรณาการการทำงาน

## ขอบเขตของการวิจัย

การวิจัยนี้มีขอบเขตพัฒนากองทัพเรือให้มีเครือข่ายสื่อสารและเทคโนโลยีสารสนเทศครอบคลุมพื้นที่ปฏิบัติการ ตอบสนองความต้องการทางยุทธวิธีในมิติความเร็ว ความปลอดภัย มีมาตรฐานตามแนวคิดการทำสงครามที่ใช้เครือข่ายเป็นศูนย์กลาง

## วิธีดำเนินการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ โดยได้ศึกษาแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม ที่มีความเกี่ยวข้องเชื่อมโยงกับทิศทางการพัฒนาระบบสื่อสารโทรคมนาคม โครงสร้างพื้นฐานทางดิจิทัล ศึกษามติคณะรัฐมนตรีและความเห็นของหน่วยงานที่มีส่วนได้เสีย

## ผลของการวิจัย

บริบทของประเทศไทยในยุคดิจิทัล ประชาชนจะมีโอกาสสร้างรายได้จากการนำไอซีทีมาเป็นเครื่องมือสนับสนุนการพัฒนาประเทศ มีอินเตอร์เน็ตความเร็วสูงกระจายอย่างทั่วถึง รวมถึงมีคุณภาพชีวิตที่ดีขึ้น การทำธุรกรรมผ่านทางออนไลน์จะมีกฎระเบียบที่ใช้ปฏิบัติได้จริง ทันต่อการเปลี่ยนแปลงทางเทคโนโลยี โดยมีเป้าหมายของการพัฒนา ๔ ระยะ ใช้เวลา ๒๐ ปี ผ่านแผนยุทธศาสตร์ ๖ แผน ได้แก่ การพัฒนาโครงสร้างพื้นฐานดิจิทัลประสิทธิภาพสูง การขับเคลื่อนเศรษฐกิจด้วยเทคโนโลยี สร้างสังคมคุณภาพที่ทั่วถึงและเท่าเทียม ปรับเปลี่ยนภาครัฐสู่การเป็นรัฐบาลดิจิทัล พัฒนากำลังคนให้พร้อมเข้าสู่ยุคเศรษฐกิจและสังคมดิจิทัล และการสร้างความเชื่อมั่นในการใช้เทคโนโลยี มีกลไกขับเคลื่อนด้วยกิจกรรมภายใต้การเปลี่ยนแปลงโครงสร้างเชิงสถาบันบูรณาการการจัดสรรทรัพยากร และติดตามความก้าวหน้าของแผนงาน นอกจากนี้คณะรัฐมนตรี และผู้มีส่วนได้เสียต่างก็มีความเห็นสอดคล้องไปในแนวทางเดียวกัน เห็นด้วยกับแผนดังกล่าว ผู้มีส่วนได้เสียบาง

หน่วยงาน เช่น สำนักงาน กสทช. เห็นว่ามีหลายประเด็นที่ทับซ้อนกับอำนาจหน้าที่ของ กสทช. และหลายหน่วยงานมีความเป็นห่วงในเรื่องของความปลอดภัยไซเบอร์

เทคโนโลยีในยุคดิจิทัลไทยแลนด์ เริ่มเห็นเป็นรูปธรรมบ้างแล้วโดยโครงการเน็ตประชารัฐมูลค่าสี่หมื่นล้านบาท ประชาชนที่อยู่ห่างไกลจะมีโอกาสใช้ระบบสื่อสารโทรคมนาคม ทั้งโทรศัพท์มือถือ อินเตอร์เน็ต เหมือนคนในเมือง และเชื่อว่าในปี ๒๕๖๓ ทุกครัวเรือนในโลกจะมีอุปกรณ์เชื่อมต่ออินเตอร์เน็ตอย่างน้อย ๑๐ เครื่อง มีผู้ใช้อินเตอร์เน็ตมากกว่า ๕,๐๐๐ ล้านราย ครึ่งหนึ่งเป็นการเชื่อมต่อผ่านทางอุปกรณ์แบบพกพา การเชื่อมโยงดังกล่าวแทรกซึมเข้าสู่ชีวิตประจำวันทั้งในบ้าน ที่ทำงาน สิ่งแวดล้อมต่าง ๆ ทุกที่ทุกเวลา จะมีเทคโนโลยีเข้ามาเกี่ยวข้องและภัยคุกคามที่มากับเทคโนโลยี ได้แก่ มัลแวร์ ไวรัส เวิร์ม อาชญากรรมไซเบอร์ เป็นสิ่งที่ควรจะตระหนักรู้ การรักษาความปลอดภัยไซเบอร์ ซึ่งหมายถึงกระบวนการที่จำเป็นเพื่อให้เกิดความปลอดภัยจากการใช้เทคโนโลยี มีความจำเป็นสำหรับองค์กรขนาดใหญ่เนื่องจากเป็นยุคที่ข้อมูลมีความสำคัญหากได้รับความเสียหายจะมีผลกระทบที่ประเมินค่าไม่ได้ สงครามไซเบอร์เป็นสิ่งที่เกิดขึ้นแล้วแต่สามารถป้องกันหรือลดความเสียหายได้ หากมีการเตรียมการที่ดี รูปแบบของการทำสงครามเริ่มมีแนวคิดใหม่เรียกว่าสงครามที่มีเครือข่ายเป็นศูนย์กลาง ซึ่งอาศัยความก้าวหน้าของเทคโนโลยีการสื่อสารและสารสนเทศเป็นตัวชี้วัดชัยชนะของสงครามตั้งแต่เริ่มต้น กองบัญชาการกองทัพไทย กองทัพบก กองทัพเรือ และกองทัพอากาศ ต่างมีแผนพัฒนาขีดความสามารถด้านนี้ แต่เนื่องจากเทคโนโลยีเปลี่ยนแปลงเร็วมาก การพัฒนาจำเป็นต้องอาศัยเวลาและทรัพยากรจำนวนมาก การที่ภาครัฐมีนโยบายส่งเสริมให้ทุกภาคส่วนเข้าถึงเทคโนโลยีด้วยการพัฒนาโครงสร้างพื้นฐานดิจิทัลประสิทธิภาพสูง หากองค์กรใดสามารถใช้ประโยชน์จากโอกาสนี้จะทำให้ประหยัดงบประมาณในการจัดหาสิ่งอุปกรณ์ต่าง ๆ ที่ซ้ำซ้อนไม่ต้องลงทุนเพิ่มเติมในสิ่งที่มีอยู่แล้ว สำหรับกองทัพเรือจะได้กล่าวถึงในบทต่อไป หน่วยงานความมั่นคงทางทะเลที่มีบทบาทนำในภูมิภาค

หน่วยงานความมั่นคงทางทะเลที่มีบทบาทนำในภูมิภาคและเป็นเลิศในการจัดการเป็นวิสัยทัศน์ของกองทัพเรือในปี ๒๕๕๗ ซึ่งสอดคล้องกับเป้าหมายของรัฐบาลที่จะให้ประเทศไทยก้าวข้ามกับดักประเทศที่มีรายได้ปานกลาง ไปอยู่ในกลุ่มประเทศที่พัฒนาโดยใช้แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นเครื่องมือ สำหรับกองทัพเรือเมื่อวิเคราะห์ปัจจัยสภาวะแวดล้อม อุปสรรค์และโอกาส พบว่ากองทัพเรือมีเครือข่ายโทรคมนาคมที่ครอบคลุมพื้นที่ปฏิบัติการทางบก มีระบบสารสนเทศพื้นฐานในการบริหารงานทั่วไป และมีระบบเชื่อมโยงข้อมูลทางยุทธวิธีกับเรือในทะเล การที่จะเป็นหน่วยงานความมั่นคงทางทะเลที่มีบทบาทนำในภูมิภาคและรองรับภัยคุกคามในรูปแบบใหม่จำเป็นต้องเตรียมความพร้อมในการพัฒนาเครือข่ายสำหรับการปฏิบัติงานทางยุทธวิธีในจังหวัดชายแดนใต้ สงครามที่ใช้เครือข่ายเป็นศูนย์กลางจำเป็นต้องดำเนินการในเรื่องการพัฒนาเครือข่ายโทรคมนาคม ระบบสารสนเทศ ระบบควบคุมบังคับบัญชา และพัฒนาบุคลากร

การพัฒนาเครือข่ายโทรคมนาคมด้วยการปรับปรุงระบบบริหารเครือข่าย ขยายเครือข่ายดิจิทัลให้เชื่อมโยงกับเครือข่ายของรัฐบาล โดยเฉพาะในพื้นที่ภาคตะวันออกที่อยู่ระหว่างดำเนินการดำรงสภาพการสื่อสารดาวเทียม C - Band เพื่อรองรับการใช้ความถี่ X - Band เมื่อมีความพร้อม ระบบวิทยุชายฝั่ง (HF) มีการรักษาความปลอดภัยข้อมูลรองรับการปฏิบัติการทางทะเล โทรศัพท์พื้นฐานเปลี่ยนเป็นเทคโนโลยีดิจิทัล Voice over IP ทดแทนของเดิม รวมถึงวิทยุ VHF/UHF เปลี่ยนไปใช้เป็นระบบดิจิทัลที่มีการเข้ารหัส

ระบบสารสนเทศปรับปรุงด้านการรักษาความปลอดภัยทางกายภาพ เป็นการป้องกันระบบไอทีจากภัยธรรมชาติ การกระทำของคน เช่นการขโมย การลักลอบเข้าพื้นที่หวงห้าม การป้องกันการโจมตีจากมัลแวร์หรือแฮกเกอร์จากภายนอกด้วยไฟร์วอลล์ที่มีมาตรฐาน มีโปรแกรมตรวจจับผู้บุกรุก รองรับปฏิบัติการสงครามไซเบอร์

ระบบควบคุมบังคับบัญชา $C^3I$ สามารถเชื่อมโยงข้อมูลทางยุทธวิธีสนับสนุนการแสดงภาพสถานการณ์ได้ในลักษณะ Real Time มีหลักนิยมเชื่อมต่อหน่วยงาน เช่น กรมเจ้าท่า กระประมง กรมศุลกากร ศรชล. โดยอาจใช้นโยบายไทยแลนด์ 4.0 ดำเนินการ เพื่อไม่ให้เกิดการลงทุนที่ซ้ำซ้อน

การพัฒนาบุคลากรเพื่อให้ผู้บริหาร เจ้าหน้าที่เทคนิค และผู้ใช้งานทั่วไป มีความรู้ ความชำนาญและความรับผิดชอบ รองรับการเปลี่ยนแปลงโดยศึกษาทิศทางการพัฒนาเทคโนโลยี ปรับปรุงกฎระเบียบ และกำหนดขีดสมรรถนะ

สงครามไซเบอร์เป็นสิ่งที่เกิดขึ้นแล้ว เช่น การโจมตีโรงงานผลิตอาวุธนิวเคลียร์ของอิหร่านด้วยมัลแวร์ Stuxnet การโจมตีทางไซเบอร์ในเอสโทเนีย ปฏิบัติการ Orchard ที่อิสราเอลใช้เครื่องบินเข้าไปทิ้งระเบิดอาคารผลิตอาวุธนิวเคลียร์ของซีเรีย โดยที่เรดาร์ตรวจการณ์ของซีเรียไม่สามารถตรวจจับอะไรได้เลย นอกจากนี้มีแนวโน้มที่หลายชาติเริ่มเตรียมการเพื่อทำสงครามโดยการเจาะเข้าสู่เครือข่ายคอมพิวเตอร์และโครงสร้างสาธารณูปโภคซึ่งกันและกัน พร้อมกับจัดวางแทรปดอร์หรือลอจิกบอมบ์ ซึ่งเป็นอาวุธในทางไซเบอร์ เมื่อวันเวลาที่รอคอยมาถึง เครือข่ายคอมพิวเตอร์เหล่านั้นจะถูกควบคุมให้ทำสิ่งแปลก ๆ ออกมา เช่น โอนเงินจำนวนมาก ปล่อยน้ำมันให้รั่วไหลทิ้ง ปิดวาล์วปล่อยก๊าซ ทำให้รถไฟตกราง สิ่งต่าง ๆ เหล่านี้สามารถป้องกันหรือลดความเสียหายได้หากมีการเตรียมการที่ดี กองทัพไซเบอร์จึงเป็นขีดความสามารถที่พึงมีเพื่อป้องกันเหตุร้ายดังกล่าวในเวลาปกติ โดยมีองค์ประกอบ ๓ ส่วน ได้แก่ บุคลากร กระบวนการ และเทคโนโลยี แต่เนื่องจากวิทยาการด้านการรักษาความปลอดภัยไซเบอร์เป็นเรื่องใหม่ไม่มีรูปแบบที่ตายตัว การฝึกอบรมที่ได้มาตรฐานจึงมีความจำเป็นเพื่อให้สอดคล้องกับกระบวนการและเทคโนโลยีของกองทัพเรือต่อไป

## ข้อเสนอแนะ

เทคโนโลยีดิจิทัลมีการเปลี่ยนแปลงอย่างรวดเร็วตลอดเวลายากต่อการคาดเดา การวางแผนจำเป็นต้องตระหนักรู้และเท่าทันการเปลี่ยนแปลงของเทคโนโลยี รวมถึงนัยของการเปลี่ยนแปลงนั้น ๆ เทคโนโลยีเหล่านี้เป็นเรื่องที่มีความสัมพันธ์กันไม่อาจมองแบบแยกส่วน การนำมาใช้ประโยชน์โดยการหลอมรวมกันอย่างเหมาะสมลงตัวจึงจะเกิดผลดีกับการพัฒนาประเทศ การติดตามการเปลี่ยนแปลงอย่างใกล้ชิดจะทำให้ไม่ตกขบวนรถไฟและไม่ถูกทอดทิ้งไว้ข้างหลัง