

การบูรณาการเทคโนโลยีด้านการรักษากับการดำเนินการเทคโนโลยีป้องกันประเทศในยุคดิจิทัล Integrating Medical Technology and Defense Technology Operations in the Digital Era

ทิติวุฒิ ศรีมานพ¹, ดำเกิง อัสวสุนทรางกูร², วรพล เพชรภูผา³ และ ณัฐรัชชัย เอกนราจินดาวัฒน์⁴
Thitiwut Srimanop¹, Damkoeng Asawasunthrangkul², Worapol Phetphupha³ and Natthachai
Eknarachindawat⁴

มหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน นครราชสีมา¹

มหาวิทยาลัยราชภัฏสวนสุนันทา^{2,4}

Rajamangala University of Technology Isan, Nakhon Ratchasima, Thailand¹

Suan Sunandha Rajabhat University, Thailand^{2,4}

Corresponding Author E-mail: honacg@yahoo.com¹

Received: November 18, 2025

Revised: December 30, 2025

Accepted: December 31, 2025

บทคัดย่อ

เทคโนโลยีป้องกันประเทศ ในยุคดิจิทัล โดยพิจารณาถึง ศักยภาพของระบบสาธารณสุขและความมั่นคงแห่งชาติ ในการรับมือกับภัยคุกคามทางสุขภาพและภัยคุกคามทางทหาร การวิจัยนี้ใช้ กรอบแนวคิดเกี่ยวกับการบูรณาการเทคโนโลยี โดยมุ่งเน้น 3 ปัจจัยหลัก ได้แก่ (1) เทคโนโลยีทางการแพทย์ เช่น ระบบการแพทย์ทางไกล (Telemedicine) ระบบเฝ้าระวังสุขภาพอัจฉริยะ (Smart Health Monitoring) และปัญญาประดิษฐ์ (AI) (2) เทคโนโลยีป้องกันประเทศ เช่น อากาศยานไร้คนขับ (UAVs) ระบบสื่อสารทางการทหาร และระบบ AI สำหรับการเฝ้าระวัง และ (3) ปัจจัยสนับสนุน เช่น นโยบายภาครัฐ ความร่วมมือระหว่างหน่วยงาน และการลงทุนด้านเทคโนโลยี ผลการศึกษาพบว่า การบูรณาการเทคโนโลยีทางการแพทย์และเทคโนโลยีป้องกันประเทศสามารถช่วยเพิ่มประสิทธิภาพในการเฝ้าระวังและตอบโต้ภัยคุกคามได้อย่างมีนัยสำคัญ โดยเฉพาะการนำ AI และ Big Data มาใช้ในการวิเคราะห์แนวโน้มโรคระบาดและภัยคุกคามทางทหารแบบเรียลไทม์ นอกจากนี้ UAVs และ Military Digital Networks ยังสามารถช่วยสนับสนุนภารกิจทางการแพทย์และความมั่นคงได้อย่างมีประสิทธิภาพ อย่างไรก็ตาม การบูรณาการดังกล่าวยังเผชิญกับความท้าทายในด้าน ความปลอดภัยทางไซเบอร์ โครงสร้างพื้นฐานด้านดิจิทัล และการจัดการข้อมูลที่มีความอ่อนไหว ข้อเสนอแนะของการศึกษานี้ ได้แก่ (1) การพัฒนาโครงสร้างพื้นฐานด้านดิจิทัล เช่น ระบบ 5G และเครือข่ายทหารดิจิทัล (2) การกำหนดมาตรการด้านความมั่นคงทางไซเบอร์ เพื่อป้องกันการรั่วไหลของข้อมูล และ (3) การส่งเสริมความร่วมมือระหว่างภาครัฐและเอกชน เพื่อสนับสนุนการพัฒนาเทคโนโลยีที่สามารถใช้ร่วมกันในภาคสาธารณสุขและการป้องกันประเทศ

คำสำคัญ: การบูรณาการเทคโนโลยี, เทคโนโลยีทางการแพทย์, เทคโนโลยีป้องกันประเทศ, ความมั่นคงแห่งชาติ, ปัญญาประดิษฐ์, การแพทย์ทางไกล, อากาศยานไร้คนขับ

Abstract

This study aims to analyze and propose approaches for integrating medical technology and defense technology in the digital era, focusing on enhancing national public health security and national defense capabilities in responding to health and military threats. The research framework is structured around three key factors: (1) Medical technology, including Telemedicine, Smart Health Monitoring, and Artificial Intelligence (AI); (2) Defense technology, such as Unmanned Aerial Vehicles (UAVs), Military Communication Networks, and AI-driven threat surveillance systems; and (3) Supporting factors, such as government policies, inter-agency collaboration, and technology investment. The findings indicate that the integration of medical and defense technologies significantly enhances threat surveillance and response efficiency. AI and Big Data analytics improve real-time monitoring of disease outbreaks and military threats, while UAVs and Military Digital Networks provide critical support for medical and security missions. However, challenges remain, particularly concerning cybersecurity risks, digital infrastructure limitations, and the management of sensitive data. The study proposes (1) developing digital infrastructure, such as 5G and military digital networks, (2) implementing cybersecurity measures to protect sensitive information, and (3) fostering collaboration between public and private sectors to support the development of dual-use technologies applicable to both public health and national security.

Keywords: Technology Integration, Medical Technology, Defense Technology, National Security, Artificial Intelligence, Telemedicine, Unmanned Aerial Vehicles

บทนำ

ในศตวรรษที่ 21 ความก้าวหน้าของเทคโนโลยีได้มีบทบาทสำคัญในการพัฒนา ระบบสาธารณสุข และ ระบบป้องกันประเทศ ให้มีประสิทธิภาพมากขึ้น การบูรณาการเทคโนโลยีด้านการรักษากับเทคโนโลยีป้องกันประเทศจึงเป็นแนวทางสำคัญที่ช่วยเสริมสร้างศักยภาพของทั้งสองภาคส่วนให้สามารถรับมือกับภัยคุกคามที่ซับซ้อนขึ้น เช่น การแพร่ระบาดของโรคติดต่อ ภัยคุกคามทางชีวภาพ และสงครามรูปแบบใหม่ที่อาศัยเทคโนโลยีดิจิทัล (Visanu, 2025) แนวคิดของการบูรณาการนี้ได้รับการสนับสนุนจากแผนยุทธศาสตร์ชาติของประเทศไทย โดยเฉพาะในกรอบ ยุทธศาสตร์ชาติ 20 ปี ซึ่งเน้นให้ การพัฒนาเทคโนโลยีด้านสุขภาพและความมั่นคงเป็นปัจจัยสำคัญในการเสริมสร้างเสถียรภาพของประเทศ (การวิจัยพัฒนาเทคโนโลยีป้องกันประเทศ, 2024) ทั้งนี้ เทคโนโลยีสำคัญที่มีบทบาทในกระบวนการบูรณาการ ได้แก่ ระบบการแพทย์ทางไกล (Telemedicine), ระบบเฝ้าระวังสุขภาพอัจฉริยะ (Smart Health Monitoring), ปัญญาประดิษฐ์ (AI), อากาศยานไร้คนขับ (UAVs) และ ระบบการสื่อสารทางการทหาร ซึ่งสามารถใช้ร่วมกันเพื่อเพิ่มประสิทธิภาพของ การดูแลสุขภาพในภาวะฉุกเฉินและการรักษาความมั่นคงแห่งชาติ ในอดีต การดำเนินงานด้านการแพทย์และการป้องกันประเทศมักถูกพัฒนาแยกออกจากกัน แม้ว่าทั้งสองระบบจะมีเป้าหมายร่วมกันในการรักษาความปลอดภัยของประชาชนและประเทศชาติ แต่กลไกการเชื่อมโยงที่เพียงพอ อย่างไรก็ตาม สถานการณ์ภัยพิบัติและโรคระบาด เช่น COVID-19 ได้ทำให้เห็นความสำคัญของการบูรณาการเทคโนโลยีเหล่านี้เข้าด้วยกันตัวอย่างที่เห็นได้ชัดคือ การใช้ Telemedicine ในการรักษาผู้ป่วย COVID-19 ในช่วงที่เกิดการล็อกดาวน์ทั่วโลก ซึ่งช่วยลดภาระของโรงพยาบาลและป้องกันการแพร่กระจายของโรค (World Health Organization, 2022) นอกจากนี้ UAVs หรืออากาศยานไร้คนขับ ยังถูก



นำมาใช้ในการกิจขนส่งเวชภัณฑ์ไปยังพื้นที่ห่างไกลและติดตามสถานการณ์การแพร่ระบาดของโรค (Defence Technology Institute, 2024)

ในบริบทของประเทศไทย กองทัพไทยและกระทรวงสาธารณสุขได้เริ่มนำระบบ AI และ Big Data มาใช้ในการเฝ้าระวังสุขภาพของกำลังพลและประชาชน โดยข้อมูลจากเซ็นเซอร์สุขภาพที่ติดตั้งในโรงพยาบาลและหน่วยทหารสามารถวิเคราะห์แนวโน้มของโรคระบาดและภัยคุกคามทางชีวภาพได้แบบเรียลไทม์ (National Institute of Health, 2023) การบูรณาการเทคโนโลยีเพื่อเพิ่มศักยภาพของระบบสาธารณสุขและความมั่นคงแห่งชาติเป็นแนวทางที่กำลังได้รับความสนใจมากขึ้นในระดับสากล ประเทศมหาอำนาจอย่างสหรัฐอเมริกาและจีนได้มีการพัฒนาระบบ Telemedicine ทางทหาร และ AI เพื่อวิเคราะห์แนวโน้มของโรคระบาดและภัยคุกคามด้านความมั่นคง (Chan et al., 2023) ดังนั้น ประเทศไทยจำเป็นต้องเร่งพัฒนาและบูรณาการเทคโนโลยีดังกล่าวให้ทันสมัย เพื่อให้สามารถรับมือกับวิกฤติที่อาจเกิดขึ้นในอนาคต

ตารางที่ ๑ สรุปปัญหาการวิจัยและผลกระทบ

ปัญหาการวิจัย	ผลกระทบ
ขาดการบูรณาการเทคโนโลยีทางการแพทย์และป้องกันประเทศ	ทำให้การรับมือกับภัยคุกคามทางสุขภาพและความมั่นคงไม่มีประสิทธิภาพ
ระบบสาธารณสุขไม่สามารถรับมือกับโรคระบาดได้อย่างมีประสิทธิภาพ	ประชาชนและกำลังพลไม่ได้รับการดูแลสุขภาพอย่างเหมาะสมในภาวะฉุกเฉิน
ขาดการเฝ้าระวังและตอบโต้ภัยคุกคามทางชีวภาพ	ความเสี่ยงในการแพร่ระบาดของโรคที่อาจเป็นภัยคุกคามต่อความมั่นคงของชาติ
การใช้ AI และ Big Data ในการป้องกันประเทศยังไม่แพร่หลาย	การตัดสินใจเชิงยุทธศาสตร์ล่าช้า เนื่องจากขาดข้อมูลที่เพียงพอและแม่นยำ
ขาดโครงสร้างพื้นฐานทางดิจิทัลที่รองรับการป้องกันประเทศและสาธารณสุข	ประเทศไทยอาจไม่สามารถแข่งขันด้านความมั่นคงดิจิทัลในระดับสากลได้

การศึกษานี้มีความสำคัญเนื่องจาก การบูรณาการเทคโนโลยีด้านการรักษาและเทคโนโลยีป้องกันประเทศ จะช่วยให้ประเทศไทยสามารถเพิ่มศักยภาพในการรับมือกับภัยคุกคามด้านสุขภาพและความมั่นคงแห่งชาติได้อย่างมีประสิทธิภาพ 1 ด้านสาธารณสุข (Public Health Security) เพิ่มการเข้าถึงบริการสุขภาพ – ระบบ Telemedicine และ AI สามารถช่วยให้ประชาชนและกำลังพลสามารถเข้าถึงบริการทางการแพทย์ได้สะดวกขึ้น โดยเฉพาะในพื้นที่ห่างไกลและพื้นที่ที่ได้รับผลกระทบจากภัยพิบัติ (R1-Proposal, 2025) เสริมสร้างระบบเฝ้าระวังโรคระบาด – Smart Health Monitoring และ Big Data Analytics สามารถช่วยติดตามแนวโน้มของโรคติดต่อและภัยคุกคามทางชีวภาพในระดับประเทศ (National Institute of Health, 2023) เพิ่มประสิทธิภาพของการตอบสนองฉุกเฉิน – ระบบ AI และ UAVs สามารถช่วยจัดส่งยาและเวชภัณฑ์ได้อย่างรวดเร็วและลดภาระของบุคลากรทางการแพทย์ (Defence Technology Institute, 2024) 2. ด้านความมั่นคงแห่งชาติ (National Security) เพิ่มศักยภาพของระบบเฝ้าระวังภัยคุกคาม – AI และ UAVs สามารถช่วยกองทัพในการเฝ้าระวังภัยคุกคามทางทหาร เช่น การก่อการร้ายทางชีวภาพ หรือการแพร่ระบาดของโรคที่อาจเกิดจากอาวุธชีวภาพ (Visanu, 2025) ลดภาระของกองทัพและระบบสาธารณสุข – การใช้เทคโนโลยีในการดูแลสุขภาพของกำลังพลช่วยให้กองทัพสามารถรักษาขีดความสามารถในการปฏิบัติการกิจได้โดยไม่ต้องกังวลเกี่ยวกับปัญหาสุขภาพที่อาจเกิดขึ้น (การวิจัยพัฒนาเทคโนโลยีป้องกันประเทศ, 2024) เพิ่มความสามารถในการรับมือกับภัยพิบัติและสงครามไฮบริด – เทคโนโลยีสามารถใช้เพื่อบริหารจัดการภัยพิบัติที่เกิดขึ้นจากโรคระบาดและภัยคุกคามทางทหาร

เช่น สงครามไซเบอร์ที่ส่งผลกระทบต่อระบบสาธารณสุขและโครงสร้างพื้นฐานของประเทศ (Zhang et al., 2022) การศึกษานี้มุ่งเน้นไปที่ การบูรณาการเทคโนโลยีทางการแพทย์และเทคโนโลยีป้องกันประเทศ โดยครอบคลุม ระบบ Telemedicine และ AI สำหรับสาธารณสุขและกองทัพ การใช้ UAVs และระบบเฝ้าระวังสุขภาพอัจฉริยะ เพื่อเฝ้าระวังภัยคุกคาม การวิเคราะห์ข้อมูลจาก Big Data เพื่อพัฒนานโยบายด้านสุขภาพและความมั่นคงแห่งชาติ ดังนั้นการบูรณาการเทคโนโลยีด้านการแพทย์และการป้องกันประเทศเป็นสิ่งจำเป็นเพื่อเสริมสร้าง ความมั่นคง แห่งชาติและระบบสาธารณสุข การศึกษาในครั้งนี้จะช่วยให้ภาครัฐสามารถพัฒนานโยบายที่เหมาะสมและ นำเทคโนโลยีมาใช้เพื่อเพิ่มศักยภาพของประเทศในยุคดิจิทัล

วัตถุประสงค์การวิจัย

เพื่อศึกษาแนวทางการบูรณาการเทคโนโลยีด้านการรักษากับการดำเนินการด้านเทคโนโลยีป้องกัน ประเทศในยุคดิจิทัล เพื่อเพิ่มประสิทธิภาพในการรับมือกับภัยคุกคามสมัยใหม่และสถานการณ์ฉุกเฉินต่าง ๆ อย่างยั่งยืน

การทบทวนวรรณกรรม

เทคโนโลยีทางการแพทย์กับความมั่นคงแห่งชาติด้านสาธารณสุข

การบูรณาการเทคโนโลยีทางการแพทย์เข้ากับระบบความมั่นคงแห่งชาติเป็นแนวทางสำคัญในการเพิ่ม ประสิทธิภาพการรับมือกับภัยคุกคามด้านสุขภาพ เช่น โรคระบาดและภัยพิบัติทางชีวภาพ โดยเฉพาะในยุคดิจิทัล ที่เทคโนโลยีขั้นสูงสามารถช่วยให้การเฝ้าระวังและตอบสนองต่อสถานการณ์ฉุกเฉินเป็นไปอย่างรวดเร็วและแม่นยำ (Visanu, 2025)

1. ระบบการแพทย์ทางไกล (Telemedicine) กับเสริมสร้างความมั่นคงด้านสาธารณสุข

ระบบการแพทย์ทางไกล (Telemedicine) เป็นนวัตกรรมที่ช่วยให้ประชาชนสามารถเข้าถึงบริการสุขภาพ ได้จากระยะไกลผ่านเครือข่ายดิจิทัล ซึ่งเป็นประโยชน์อย่างยิ่งในสถานการณ์ฉุกเฉิน เช่น การแพร่ระบาดของ COVID-19 ทำให้โรงพยาบาลสามารถบริหารจัดการทรัพยากรทางการแพทย์ได้อย่างมีประสิทธิภาพ (World Health Organization, 2022) นอกจากนี้ การใช้ระบบนี้ในพื้นที่ชายแดนหรือเขตสงครามยังช่วยให้นักการ แพทย์สามารถให้คำปรึกษาและวินิจฉัยโรคได้โดยไม่ต้องเสี่ยงอันตรายจากสถานการณ์ความไม่สงบ (R1-Proposal, 2025) ในด้านความมั่นคงของประเทศ ระบบ Telemedicine ยังช่วยลดภาระของบุคลากรทาง การแพทย์ในกองทัพ และสามารถนำไปใช้ร่วมกับระบบป้องกันภัยพิบัติ เพื่อให้การรักษาผู้บาดเจ็บสามารถ ดำเนินการได้อย่างรวดเร็วโดยไม่ต้องรอการส่งตัวไปยังโรงพยาบาลหลัก (Defence Technology Institute, 2024)

2. ระบบเฝ้าระวังสุขภาพอัจฉริยะ (Smart Health Monitoring) กับความมั่นคงด้านสาธารณสุข

ระบบเฝ้าระวังสุขภาพอัจฉริยะ (Smart Health Monitoring) เป็นอีกหนึ่งเทคโนโลยีสำคัญที่ช่วยตรวจจับ สัญญาณชีพและพฤติกรรมสุขภาพของประชากรในเวลาจริง (real-time monitoring) ผ่านอุปกรณ์สวมใส่ อัจฉริยะ (Wearable Devices) และเครือข่าย Internet of Things (IoT) การใช้ระบบนี้ในหน่วยงานด้าน สาธารณสุขและการแพทย์ภาคสนามช่วยให้สามารถตรวจจับโรคระบาดตั้งแต่ระยะเริ่มต้น และสามารถป้องกัน การแพร่ระบาดในวงกว้างได้อย่างมีประสิทธิภาพ (National Institute of Health, 2023) นอกจากนี้ ในบริบท ของกองทัพ เทคโนโลยีดังกล่าวสามารถใช้เพื่อเฝ้าระวังสุขภาพของทหารและเจ้าหน้าที่ในภารกิจต่าง ๆ เช่น การ เฝ้าตรวจระดับออกซิเจนในเลือดของนักบินขับไล่ หรือการติดตามภาวะความเครียดของเจ้าหน้าที่ทางการแพทย์ที่



ทำงานในเขตภัยพิบัติ (การวิจัยพัฒนาเทคโนโลยีป้องกันประเทศ, 2024) สิ่งเหล่านี้เป็นปัจจัยที่ช่วยเพิ่มประสิทธิภาพในการรักษาความมั่นคงแห่งชาติจากภัยคุกคามทางชีวภาพ

3. ปัญญาประดิษฐ์ในระบบสุขภาพ (AI in Healthcare) กับการรับมือกับภัยคุกคามด้านสุขภาพ ปัญญาประดิษฐ์ (Artificial Intelligence: AI) มีบทบาทสำคัญในการวิเคราะห์ข้อมูลสุขภาพจำนวนมาก และสามารถช่วยในการคาดการณ์การแพร่ระบาดของโรค โดยใช้ข้อมูลจากแหล่งต่าง ๆ เช่น ระบบเฝ้าระวังสุขภาพแห่งชาติ ข้อมูลผู้ป่วยจากโรงพยาบาล และข้อมูลจากโซเชียลมีเดีย เพื่อสร้างแบบจำลองทางคณิตศาสตร์ที่ช่วยให้รัฐบาลสามารถตัดสินใจในการออกมาตรการป้องกันได้อย่างแม่นยำ (

Chan et al., 2023) AI ยังช่วยในการวินิจฉัยโรคผ่านระบบวิเคราะห์ภาพทางการแพทย์ เช่น การใช้ AI ในการวิเคราะห์ภาพเอกซเรย์ปอดของผู้ป่วย COVID-19 เพื่อลดภาระของรังสีแพทย์และเพิ่มความแม่นยำในการวินิจฉัย (Zhang et al., 2022) เทคโนโลยีนี้สามารถนำไปบูรณาการเข้ากับระบบเฝ้าระวังทางทหาร เพื่อให้สามารถตรวจจับการแพร่ระบาดของโรคติดต่อที่อาจเป็นภัยคุกคามต่อความมั่นคงแห่งชาติได้ (R1-Proposal, 2025) AI ยังมีบทบาทสำคัญในระบบการแพทย์ทางไกล เช่น การใช้ Chatbot และ Virtual Doctor ในการให้คำแนะนำทางการแพทย์ในพื้นที่ที่ขาดแคลนบุคลากร ซึ่งสามารถช่วยให้ประชากรสามารถเข้าถึงการรักษาพยาบาลได้อย่างรวดเร็วและมีประสิทธิภาพมากขึ้น (WHO, 2023)

4. การบูรณาการเทคโนโลยีทางการแพทย์เพื่อเสริมสร้างความมั่นคงแห่งชาติด้านสาธารณสุข จากการศึกษาพบว่า การบูรณาการเทคโนโลยีทางการแพทย์ เช่น Telemedicine, Smart Health Monitoring และ AI กับระบบความมั่นคงแห่งชาติ สามารถช่วยให้การรับมือกับภัยคุกคามด้านสุขภาพเป็นไปอย่างมีประสิทธิภาพ (R1-Proposal, 2025) โดยเฉพาะในกรณีที่มีการแพร่ระบาดของโรคติดต่อหรือภัยพิบัติทางชีวภาพ ระบบเหล่านี้จะช่วยให้รัฐบาลสามารถวางแผนเชิงรุกและป้องกันการลุกลามของปัญหาสุขภาพระดับประเทศ ในบริบทของความมั่นคง เทคโนโลยีทางการแพทย์ยังสามารถช่วยให้กองทัพและหน่วยงานด้านความมั่นคงสามารถรักษาขีดความสามารถในการปฏิบัติการทางทหาร โดยลดผลกระทบจากโรคระบาดที่อาจทำให้กำลังพลอ่อนแอ ซึ่งเป็นปัจจัยสำคัญในการรักษาความมั่นคงของชาติ (การวิจัยพัฒนาเทคโนโลยีป้องกันประเทศ, 2024)

ดังนั้นเทคโนโลยีทางการแพทย์เป็นเครื่องมือสำคัญในการเสริมสร้างความมั่นคงด้านสาธารณสุข ซึ่งส่งผลโดยตรงต่อความมั่นคงของชาติ ระบบการแพทย์ทางไกลช่วยเพิ่มการเข้าถึงบริการสุขภาพ ระบบเฝ้าระวังสุขภาพอัจฉริยะช่วยในการตรวจจับโรคระบาดล่วงหน้า และ AI มีบทบาทสำคัญในการวิเคราะห์และคาดการณ์แนวโน้มด้านสุขภาพ การบูรณาการเทคโนโลยีเหล่านี้จึงเป็นแนวทางสำคัญในการพัฒนา "ระบบสาธารณสุขที่แข็งแกร่งและยั่งยืน เพื่อรองรับภัยคุกคามในยุคดิจิทัล"

เทคโนโลยีป้องกันประเทศและความมั่นคงแห่งชาติ

เทคโนโลยีป้องกันประเทศ (Defense Technology) เป็นปัจจัยสำคัญที่ช่วยเสริมสร้างความมั่นคงแห่งชาติ โดยเฉพาะในยุคดิจิทัลที่ภัยคุกคามทางทหารและความมั่นคงมีความซับซ้อนมากขึ้น ความก้าวหน้าทางเทคโนโลยี เช่น อากาศยานไร้คนขับ (Unmanned Aerial Vehicles: UAVs) ระบบสื่อสารทางทหารและโครงข่ายดิจิทัล (Military Communication & Digital Networks) และระบบปัญญาประดิษฐ์และข้อมูลขนาดใหญ่เพื่อความปลอดภัย (AI & Big Data for Security) มีบทบาทสำคัญในการเพิ่มขีดความสามารถของระบบเฝ้าระวังและตอบโต้ภัยคุกคาม (R1-Proposal, 2025) การศึกษานี้มุ่งเน้นการทบทวนวรรณกรรมเกี่ยวกับเทคโนโลยีดังกล่าวและผลกระทบต่อความมั่นคงแห่งชาติ

1. อากาศยานไร้คนขับ (UAVs) กับความมั่นคงแห่งชาติ อากาศยานไร้คนขับ หรือโดรน (UAVs) ได้กลายเป็นเครื่องมือที่มีบทบาทสำคัญในการกิจทางทหารและความมั่นคงของรัฐ (Visanu, 2025) โดรนสามารถใช้ในการเฝ้าระวัง การลาดตระเวน และการโจมตีเป้าหมายโดยไม่ต้องเสี่ยงชีวิตของกำลังพล (DTI, 2024)



ระบบ UAVs ถูกนำมาใช้ในหลายประเทศ เช่น สหรัฐอเมริกาและอิสราเอล เพื่อลดต้นทุนทางทหารและเพิ่มประสิทธิภาพในการปฏิบัติการ บทบาทของ UAVs ต่อความมั่นคงแห่งชาติ การลาดตระเวนและเฝ้าระวัง (Surveillance & Reconnaissance) UAVs สามารถติดตั้งกล้องถ่ายภาพความละเอียดสูงและเซ็นเซอร์อินฟราเรดเพื่อทำการกิจลาดตระเวนในพื้นที่ที่มีความเสี่ยงสูง เช่น พื้นที่ชายแดน หรือพื้นที่ที่อาจเป็นแหล่งกบดานของกลุ่มก่อการร้าย (การวิจัยพัฒนาเทคโนโลยีป้องกันประเทศ, 2024) การโจมตีเป้าหมาย (Precision Strike Capabilities) UAVs ที่มีอาวุธสามารถใช้ในการโจมตีเป้าหมายเฉพาะจุดได้อย่างแม่นยำ ลดการสูญเสียพลเรือน และเพิ่มประสิทธิภาพในการทำลายเป้าหมายทางทหาร (Chan et al., 2023). การบูรณาการกับ AI และ Big Data การใช้ปัญญาประดิษฐ์ช่วยให้ UAVs สามารถเรียนรู้พฤติกรรมของศัตรูและวิเคราะห์ข้อมูลแบบเรียลไทม์เพื่อสนับสนุนการตัดสินใจทางทหาร (R1-Proposal, 2025)

2. ระบบสื่อสารทางการทหารและโครงข่ายดิจิทัลระบบสื่อสารทางการทหารเป็นองค์ประกอบที่สำคัญของระบบป้องกันประเทศและเครือข่ายความมั่นคงแห่งชาติ โดยเฉพาะอย่างยิ่งในยุคที่สงครามสารสนเทศ (Information Warfare) มีความสำคัญมากขึ้น (Defence Technology Institute, 2024) เทคโนโลยีหลักของระบบสื่อสารทางการทหาร เครือข่ายการสื่อสารแบบเข้ารหัส (Encrypted Military Communication Networks) ระบบเครือข่ายการสื่อสารที่มีการเข้ารหัสขั้นสูงช่วยให้ข้อมูลลับของกองทัพไม่ถูกดักฟังหรือถูกโจมตีโดยอาชญากรไซเบอร์หรือหน่วยข่าวกรองของศัตรู (National Institute of Security, 2023) การสื่อสารผ่านดาวเทียม (Military Satellite Communication) การใช้ดาวเทียมเพื่อการสื่อสารทางการทหารช่วยให้สามารถส่งข้อมูลระหว่างหน่วยรบในพื้นที่ห่างไกลได้อย่างมีประสิทธิภาพ แม้ในกรณีที่โครงข่ายภาคพื้นดินถูกทำลาย เทคโนโลยี 5G และการบูรณาการกับ Internet of Military Things เครือข่าย 5G ช่วยเพิ่มความเร็วและลดความล่าช้าในการส่งข้อมูลทางการทหาร และสามารถเชื่อมต่อกับอุปกรณ์ IoMT เช่น เซ็นเซอร์สนามรบและระบบสื่อสารไร้สายของกองทัพ (Zhang et al., 2022)

3. ผลกระทบต่อความมั่นคงแห่งชาติเพิ่มความแม่นยำของการสื่อสารและการสั่งการ (Command & Control Efficiency) ลดความเสี่ยงจากการโจมตีทางไซเบอร์ (Cybersecurity Resilience) ปรับปรุงการประสานงานระหว่างหน่วยรบ (Interoperability Enhancement)

4. ระบบปัญญาประดิษฐ์และข้อมูลขนาดใหญ่เพื่อความมั่นคง AI และ Big Data เป็นเทคโนโลยีที่สามารถเปลี่ยนแปลงรูปแบบของการทำสงครามและระบบป้องกันประเทศได้อย่างมีนัยสำคัญ (การวิจัยพัฒนาเทคโนโลยีป้องกันประเทศ, 2024) บทบาทของ AI และ Big Data ต่อความมั่นคงแห่งชาติ การวิเคราะห์ข้อมูลข่าวกรอง (Intelligence Analysis) AI สามารถวิเคราะห์ข้อมูลข่าวกรองจากหลายแหล่ง เช่น ภาพถ่ายดาวเทียม การดักฟังสัญญาณวิทยุ และข้อมูลบนโซเชียลมีเดีย เพื่อระบุภัยคุกคามที่อาจเกิดขึ้นล่วงหน้า ระบบเฝ้าระวังและการคาดการณ์ภัยคุกคาม (Threat Prediction & Surveillance) Big Data และ Machine Learning สามารถใช้ในการวิเคราะห์แนวโน้มของการก่อการร้ายหรือภัยคุกคามทางไซเบอร์โดยใช้ข้อมูลย้อนหลังและพฤติกรรมของกลุ่มเป้าหมาย (Visanu, 2025) การบูรณาการกับระบบอาวุธอัจฉริยะ (Autonomous Weapon Systems) AI ช่วยให้ระบบอาวุธอัตโนมัติสามารถทำงานได้อย่างอิสระ ลดการพึ่งพาการควบคุมจากมนุษย์ และเพิ่มความแม่นยำของระบบอาวุธนำวิถี เช่น ขีปนาวุธอัจฉริยะและโดรนติดอาวุธ (Chan et al., 2023) ผลกระทบต่อประสิทธิภาพของระบบเฝ้าระวังและตอบโต้ภัยคุกคาม เพิ่มความแม่นยำในการวิเคราะห์ภัยคุกคาม (Threat Detection Accuracy) ลดเวลาตอบสนองต่อเหตุการณ์ฉุกเฉิน (Faster Response Time) ลดภาระของบุคลากรทางทหารในการประมวลผลข้อมูล (Reduced Human Workload)

ดังนั้นการบูรณาการเทคโนโลยีป้องกันประเทศ เช่น UAVs, ระบบสื่อสารทางการทหาร และ AI กับระบบความมั่นคงแห่งชาติเป็นปัจจัยสำคัญที่ช่วยเพิ่มประสิทธิภาพของการเฝ้าระวังและตอบโต้ภัยคุกคาม (การวิจัย



พัฒนาเทคโนโลยีป้องกันประเทศ, 2024) เทคโนโลยีเหล่านี้ไม่เพียงช่วยให้กองทัพสามารถป้องกันภัยคุกคามที่ซับซ้อนขึ้นในยุคดิจิทัล แต่ยังมีบทบาทสำคัญในการรักษาสมดุลด้านความมั่นคงของประเทศในระยะยาว

ปัจจัยสนับสนุนการบูรณาการเทคโนโลยีเพื่อความมั่นคงแห่งชาติ

การบูรณาการเทคโนโลยีเพื่อความมั่นคงแห่งชาติเป็นกระบวนการที่ต้องอาศัยปัจจัยสนับสนุนหลายประการ ไม่ว่าจะเป็น นโยบายภาครัฐ ความร่วมมือระหว่างภาคส่วนต่าง ๆ และ การลงทุนและงบประมาณด้านเทคโนโลยี ปัจจัยเหล่านี้มีบทบาทสำคัญต่อความสามารถในการบูรณาการเทคโนโลยีที่ทันสมัยเพื่อเสริมสร้างความมั่นคงด้านสาธารณสุข และ ระบบเฝ้าระวังและตอบโต้ภัยคุกคามทางทหาร ในยุคดิจิทัล (Visanu, 2025) การพัฒนาเทคโนโลยี เช่น ระบบการแพทย์ทางไกล (Telemedicine), ระบบเฝ้าระวังสุขภาพอัจฉริยะ (Smart Health Monitoring), อากาศยานไร้คนขับ (UAVs) และระบบปัญญาประดิษฐ์เพื่อการเฝ้าระวังภัยคุกคาม (AI for Threat Surveillance)

ต้องอาศัยการสนับสนุนเชิงนโยบาย ความร่วมมือระหว่างหน่วยงาน และงบประมาณที่เพียงพอในการพัฒนาและนำไปใช้จริง (R1-Proposal, 2025) การศึกษานี้จะทบทวนวรรณกรรมเกี่ยวกับบทบาทของปัจจัยสนับสนุนเหล่านี้ต่อการบูรณาการเทคโนโลยีเพื่อความมั่นคงของประเทศ

1. นโยบายภาครัฐกับการบูรณาการเทคโนโลยีเพื่อความมั่นคงแห่งชาติ

นโยบายภาครัฐ (Government Policies) เป็นปัจจัยสำคัญที่กำหนดทิศทางของการพัฒนาเทคโนโลยีเพื่อความมั่นคงแห่งชาติ รัฐบาลมีบทบาทในการออกกฎหมาย ส่งเสริมนวัตกรรม และสนับสนุนการพัฒนาเทคโนโลยีที่สามารถใช้ในภาคสาธารณสุขและการป้องกันประเทศ

2. นโยบายด้านความมั่นคงทางสุขภาพนโยบายของรัฐบาลเกี่ยวกับ ยุทธศาสตร์ด้านสาธารณสุขดิจิทัล (Digital Health Strategy) ช่วยส่งเสริมให้มีการใช้ Telemedicine และ AI ในระบบสุขภาพ เพื่อลดภาระของบุคลากรทางการแพทย์และเพิ่มประสิทธิภาพในการตรวจวินิจฉัยโรคระบาด (World Health Organization, 2022) การบูรณาการ Smart Health Monitoring กับฐานข้อมูลระดับชาติทำให้ภาครัฐสามารถติดตามการแพร่กระจายของโรคและวิเคราะห์แนวโน้มทางสุขภาพเพื่อวางแผนเชิงรุกได้ดีขึ้น (National Institute of Health, 2023) นโยบายด้านความมั่นคงแห่งชาติ รัฐบาลไทยกำหนดให้ ยุทธศาสตร์ชาติ 20 ปี เป็นกรอบหลักในการพัฒนาเทคโนโลยีป้องกันประเทศ โดยมีเป้าหมายให้ไทยสามารถพึ่งพาตนเองในด้านยุทธโธปกรณ์ และลดการนำเข้าเทคโนโลยีจากต่างประเทศ (Defence Technology Institute, 2024) การพัฒนา AI และ Big Data สำหรับระบบเฝ้าระวังทางทหาร ได้รับการสนับสนุนภายใต้แผน Thailand 4.0 ซึ่งมุ่งเน้นการนำเทคโนโลยีดิจิทัลมาใช้เพิ่มขีดความสามารถของกองทัพ (R1-Proposal, 2025)

3. ผลกระทบของนโยบายภาครัฐต่อความมั่นคงแห่งชาติเพิ่มประสิทธิภาพในการรับมือกับภัยคุกคามทางชีวภาพ ผ่านการใช้เทคโนโลยีขั้นสูงในการเฝ้าระวังสุขภาพเสริมสร้างระบบเฝ้าระวังภัยคุกคามทางทหาร โดยสนับสนุนการพัฒนาอากาศยานไร้คนขับและระบบ AI เพื่อตรวจจับภัยคุกคามล่วงหน้า

4. ความร่วมมือระหว่างภาคส่วนต่าง ๆ กับการพัฒนาเทคโนโลยีเพื่อความมั่นคงแห่งชาติ การบูรณาการเทคโนโลยีให้มีประสิทธิภาพต้องอาศัย ความร่วมมือระหว่างภาครัฐ ภาคเอกชน และสถาบันการศึกษา เพื่อพัฒนาและปรับปรุงนวัตกรรมให้สอดคล้องกับความต้องการของประเทศ (การวิจัยพัฒนาเทคโนโลยีป้องกันประเทศ, 2024). ตัวอย่างความร่วมมือที่สำคัญ ความร่วมมือระหว่างภาครัฐและสถาบันการศึกษา กระทรวงกลาโหมของไทยร่วมมือกับมหาวิทยาลัยเชียงใหม่และมหาวิทยาลัยพระจอมเกล้าพระนครเหนือในการพัฒนา UAVs และ AI สำหรับระบบเฝ้าระวังทางทหาร (DTI, 2024) สถาบันเทคโนโลยีแห่งชาติของสหรัฐอเมริกามีโครงการพัฒนา Smart Health Monitoring ร่วมกับหน่วยงานความมั่นคง เพื่อเพิ่มขีดความสามารถในการตรวจวินิจฉัยโรคระบาดในพื้นที่สงคราม (Chan et al., 2023) ความร่วมมือระหว่างภาครัฐและภาคเอกชน การพัฒนา ระบบเครือข่ายการ

สื่อสารทางการทหาร โดยภาคเอกชน เช่น บริษัทด้านโทรคมนาคมที่ร่วมมือกับรัฐบาลเพื่อพัฒนา เครือข่าย 5G สำหรับการสื่อสารทางยุทธวิธี (Zhang et al., 2022) โครงการความร่วมมือระหว่างรัฐบาลและภาคเอกชน ในสหภาพยุโรปสำหรับการพัฒนา AI-Based Cybersecurity Systems เพื่อป้องกันภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อความมั่นคงแห่งชาติ (European Commission, 2023)

5. การลงทุนและงบประมาณด้านเทคโนโลยีกับประสิทธิภาพของระบบเฝ้าระวังและตอบโต้ภัยคุกคาม การลงทุนในเทคโนโลยีด้านความมั่นคงต้องใช้งบประมาณมหาศาล เนื่องจากเทคโนโลยีมีการพัฒนาอย่างต่อเนื่อง และต้องอาศัยทรัพยากรจำนวนมากในการดำเนินโครงการ (Visanu, 2025). แนวโน้มการลงทุนในเทคโนโลยีเพื่อความมั่นคงแห่งชาติ การลงทุนด้าน AI และ Big Data สหรัฐฯ และจีนเป็นสองประเทศที่ลงทุนมหาศาลใน AI for Defense and National Security เพื่อเพิ่มขีดความสามารถของระบบป้องกันประเทศ (Chan et al., 2023) ประเทศไทยมีการจัดสรรงบประมาณเพื่อพัฒนา AI สำหรับการเฝ้าระวังโรคระบาด และ AI สำหรับการคาดการณ์ภัยคุกคามทางทหาร (R1-Proposal, 2025) การลงทุนในเครือข่ายการสื่อสารทางการทหาร การพัฒนา ระบบดาวเทียมทางการทหาร เพื่อเสริมความสามารถในการเฝ้าระวังและวิเคราะห์ข้อมูลจากระยะไกล เช่น ดาวเทียม THEOS-2 ของไทย ที่ช่วยในการวิเคราะห์ข้อมูลภัยพิบัติและความมั่นคงทางทหาร (การวิจัยพัฒนาเทคโนโลยีป้องกันประเทศ, 2024) ผลกระทบของการลงทุนต่อความมั่นคงแห่งชาติเพิ่มศักยภาพในการเฝ้าระวังภัยคุกคามจากโรคระบาดและภัยพิบัติเสริมขีดความสามารถของกองทัพในการเฝ้าระวังและตอบโต้ภัยคุกคามทางทหาร

ดังนั้นปัจจัยสนับสนุน เช่น นโยบายภาครัฐ ความร่วมมือระหว่างภาคส่วนต่าง ๆ และงบประมาณด้านเทคโนโลยี ล้วนมีบทบาทสำคัญในการบูรณาการเทคโนโลยีเพื่อเสริมสร้าง ความมั่นคงด้านสาธารณสุข และความมั่นคงแห่งชาติ ในระยะยาว

การบูรณาการเทคโนโลยีเพื่อความมั่นคงแห่งชาติ

ในยุคดิจิทัล เทคโนโลยีได้กลายเป็นปัจจัยสำคัญที่ช่วยเสริมสร้าง ความมั่นคงแห่งชาติ (National Security) และ ความมั่นคงด้านสาธารณสุข (Public Health Security) การบูรณาการเทคโนโลยีขั้นสูง เช่น ระบบปัญญาประดิษฐ์ (AI) ข้อมูลขนาดใหญ่ (Big Data) ระบบการแพทย์ทางไกล (Telemedicine) และ อากาศยานไร้คนขับ (UAVs) เข้ากับระบบการบริหารจัดการภาครัฐ สามารถเพิ่มขีดความสามารถในการเฝ้าระวังภัยคุกคามและรับมือกับวิกฤตระดับชาติ เช่น การแพร่ระบาดของโรคติดต่อและภัยความมั่นคง (Visanu, 2025) นโยบายภาครัฐและการลงทุนในเทคโนโลยีความมั่นคงได้รับการผลักดันอย่างต่อเนื่องในหลายประเทศ รวมถึงประเทศไทย โดยรัฐบาลไทยได้กำหนด ยุทธศาสตร์ชาติ 20 ปี เพื่อบูรณาการเทคโนโลยีเข้ากับการป้องกันประเทศ และสาธารณสุข (การวิจัยพัฒนาเทคโนโลยีป้องกันประเทศ, 2024) การศึกษานี้มุ่งเน้นการทบทวนวรรณกรรมเกี่ยวกับการบูรณาการเทคโนโลยีเพื่อความมั่นคงแห่งชาติ โดยเฉพาะในมิติของ การรับมือโรคระบาดและการเฝ้าระวังภัยคุกคาม

ความมั่นคงด้านสาธารณสุข เป็นแนวคิดที่เกี่ยวข้องกับความสามารถของประเทศในการรับมือกับภัยคุกคามทางสุขภาพ เช่น โรคระบาด การก่อการร้ายทางชีวภาพ และภัยพิบัติทางธรรมชาติ การใช้เทคโนโลยีสมัยใหม่ช่วยเพิ่มความสามารถในการเฝ้าระวัง การวินิจฉัย และการตอบสนองต่อเหตุการณ์ด้านสุขภาพอย่างรวดเร็ว

1. ระบบการแพทย์ทางไกล (Telemedicine) กับการรับมือโรคระบาด

ระบบ Telemedicine เป็นเทคโนโลยีที่ช่วยให้บุคลากรทางการแพทย์สามารถให้บริการวินิจฉัยและรักษาผู้ป่วยจากระยะไกลผ่านอินเทอร์เน็ตและอุปกรณ์ดิจิทัล เทคโนโลยีนี้มีบทบาทสำคัญอย่างมากในช่วงการแพร่ระบาดของ COVID-19 โดยช่วยลดภาระของโรงพยาบาลและเพิ่มการเข้าถึงการรักษาสำหรับประชาชนในพื้นที่ห่างไกล (World Health Organization, 2022) การใช้ Telemedicine ในประเทศไทย: รัฐบาลไทยได้พัฒนา



ระบบคลินิกเสมือน (Virtual Clinic System) เพื่อให้แพทย์สามารถติดตามอาการของผู้ป่วยได้แบบเรียลไทม์ และลดความเสี่ยงของบุคลากรทางการแพทย์ที่ต้องสัมผัสกับผู้ติดเชื้อโดยตรง (R1-Proposal, 2025) Telemedicine กับระบบความมั่นคง: ในภารกิจทางทหาร ระบบ Telemedicine ถูกใช้เพื่อสนับสนุนหน่วยแพทย์สนาม และช่วยให้ทหารที่ปฏิบัติภารกิจในพื้นที่เสี่ยงสามารถเข้าถึงการรักษาทางการแพทย์ได้อย่างรวดเร็ว (Defence Technology Institute, 2024)

2. ระบบเฝ้าระวังสุขภาพอัจฉริยะ (Smart Health Monitoring) เทคโนโลยี Smart Health Monitoring อาศัย Internet of Things (IoT) และ Big Data Analytics เพื่อเฝ้าระวังสุขภาพของประชาชนและบุคลากรทางการแพทย์ในเวลาจริงการตรวจจับโรคระบาดแบบเรียลไทม์: การติดตั้งเซ็นเซอร์ชีวภาพในสถานพยาบาลและระบบ AI วิเคราะห์ข้อมูลสุขภาพของประชาชนสามารถช่วยคาดการณ์และป้องกันการแพร่กระจายของโรคได้อย่างแม่นยำ (National Institute of Health, 2023) การบูรณาการกับความมั่นคงแห่งชาติ: ระบบดังกล่าวสามารถใช้กับ กองกำลังป้องกันประเทศ เพื่อติดตามสุขภาพของกำลังพล ลดความเสี่ยงในการเกิดโรคระบาดในค่ายทหารและหน่วยงานความมั่นคง (R1-Proposal, 2025)

3. เทคโนโลยีกับความมั่นคงแห่งชาติ (National Security)

ความมั่นคงแห่งชาติ ครอบคลุมการป้องกันภัยคุกคามจากภายในและภายนอกประเทศ เทคโนโลยีที่เกี่ยวข้องกับ อากาศยานไร้คนขับ (UAVs) ระบบสื่อสารทางทหาร และ AI สำหรับเฝ้าระวังภัยคุกคาม มีบทบาทสำคัญในการเสริมสร้างศักยภาพของกองทัพ

3.1 อากาศยานไร้คนขับ (UAVs) ในภารกิจความมั่นคง

UAVs ถูกนำมาใช้เพื่อเพิ่มประสิทธิภาพของการลาดตระเวนและตอบโต้ภัยคุกคามทางทหาร โดยเฉพาะในพื้นที่ที่มีความเสี่ยงสูงการลาดตระเวนชายแดนและป้องกันภัยคุกคามจากกองกำลังติดอาวุธ: กองทัพไทยได้มีการนำ โดรนลาดตระเวนทางยุทธวิธี (Tactical Surveillance Drones) มาใช้เพื่อเฝ้าระวังการเคลื่อนไหวของกลุ่มก่อความไม่สงบ (การวิจัยพัฒนาเทคโนโลยีป้องกันประเทศ, 2024) การเฝ้าระวังภัยพิบัติและช่วยเหลือด้านมนุษยธรรม: UAVs ยังสามารถใช้ในภารกิจค้นหาและกู้ภัย (Search and Rescue) และช่วยส่งมอบเวชภัณฑ์ในพื้นที่ที่ได้รับผลกระทบจากภัยพิบัติ (Chan et al., 2023)

3.2 ระบบปัญญาประดิษฐ์ (AI) และข้อมูลขนาดใหญ่ (Big Data) กับระบบเฝ้าระวังภัยคุกคาม

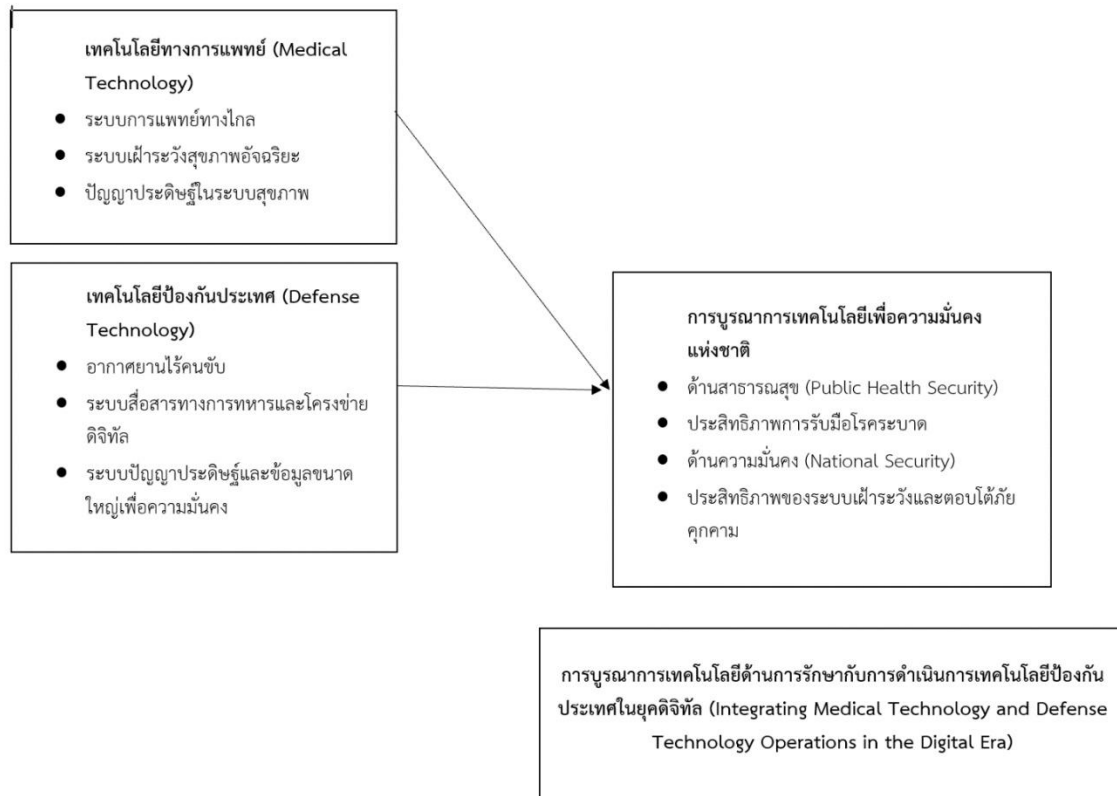
AI และ Big Data เป็นเทคโนโลยีที่มีบทบาทสำคัญในการเพิ่มขีดความสามารถของกองทัพและหน่วยงานด้านความมั่นคงในการคาดการณ์ภัยคุกคามและตัดสินใจอย่างรวดเร็ว การวิเคราะห์ข้อมูลข่าวกรอง: AI สามารถวิเคราะห์ข้อมูลจากดาวเทียม โซเชียลมีเดีย และระบบข่าวกรองอื่น ๆ เพื่อระบุความเสี่ยงด้านความมั่นคง (Visanu, 2025)

การเฝ้าระวังทางไซเบอร์: การโจมตีทางไซเบอร์เป็นภัยคุกคามที่เพิ่มขึ้น AI สามารถช่วยในการตรวจจับพฤติกรรมที่ผิดปกติและป้องกันการโจมตีต่อระบบโครงสร้างพื้นฐานของประเทศ (Zhang et al., 2022)

ดังนั้นการบูรณาการเทคโนโลยีขั้นสูงเข้ากับระบบสาธารณสุขและความมั่นคงแห่งชาติช่วยเพิ่มประสิทธิภาพในการรับมือกับภัยคุกคามทางชีวภาพและการป้องกันประเทศ การพัฒนา Telemedicine, Smart Health Monitoring, UAVs และ AI ช่วยให้การเฝ้าระวังโรคระบาดและภัยคุกคามทางทหารเป็นไปอย่างแม่นยำและรวดเร็ว การสนับสนุนจากภาครัฐและการลงทุนในเทคโนโลยีเหล่านี้จึงเป็นสิ่งจำเป็นสำหรับอนาคตของประเทศไทย



กรอบแนวคิดการวิจัย



ภาพที่ 1 กรอบแนวคิดในการวิจัย

วิธีดำเนินการวิจัย

บทความนี้ใช้กรอบแนวคิดการบูรณาการเทคโนโลยี โดยเน้นการเชื่อมโยงระหว่าง เทคโนโลยีด้านการรักษา (Medical Technology) กับ เทคโนโลยีป้องกันประเทศ (Defense Technology) เพื่อเพิ่มประสิทธิภาพในการปฏิบัติการกิจความมั่นคงและการรับมือกับสถานการณ์ฉุกเฉินในยุคดิจิทัล วิธีการศึกษาใช้การวิจัยเชิงคุณภาพผ่านการวิเคราะห์ข้อมูลจากเอกสารวิชาการ นโยบายภาครัฐ และเทคโนโลยีตัวอย่าง พร้อมทั้งการสัมภาษณ์ผู้เชี่ยวชาญในภาคการแพทย์และการป้องกันประเทศ ทฤษฎีที่เกี่ยวข้อง ได้แก่ ทฤษฎีระบบ (Systems Theory) ซึ่งเน้นการทำงานร่วมกันอย่างเป็นระบบ และ ทฤษฎีนวัตกรรมทางเทคโนโลยี (Technological Innovation Theory) ที่มุ่งเน้นการสร้างสรรค์เทคโนโลยีใหม่และการประยุกต์ใช้ให้เหมาะสมกับบริบทยุคดิจิทัล เพื่อสร้างประสิทธิภาพและความยั่งยืนในการปฏิบัติการทางการแพทย์และความมั่นคงของประเทศ

ผลการวิจัย

ผลการศึกษาเน้นไปที่ การบูรณาการเทคโนโลยีทางการแพทย์และเทคโนโลยีป้องกันประเทศ โดยพิจารณาถึงประสิทธิภาพในการ เสริมสร้างความมั่นคงด้านสาธารณสุข และ เพิ่มศักยภาพของระบบป้องกันประเทศ ในยุคดิจิทัล ผลการศึกษพบว่า การเชื่อมโยงเทคโนโลยีทั้งสองภาคส่วนส่งผลให้ การรับมือกับภัยคุกคามทางสุขภาพและความมั่นคงแห่งชาติ มีประสิทธิภาพสูงขึ้น ทั้งในด้านการคาดการณ์ การเฝ้าระวัง และการตอบสนองต่อสถานการณ์ฉุกเฉิน (Visanu, 2025)



1. ผลต่อความมั่นคงด้านสาธารณสุข (Public Health Security)

ผลการศึกษาแสดงให้เห็นว่า เทคโนโลยีทางการแพทย์ที่ทันสมัยสามารถเพิ่มศักยภาพในการดูแลสุขภาพของประชาชนและกำลังพล ผ่านระบบดิจิทัลที่มีความแม่นยำและรวดเร็วขึ้นการใช้ระบบการแพทย์ทางไกล (Telemedicine) ช่วยลดช่องว่างการเข้าถึงบริการสุขภาพ ระบบ Telemedicine ที่บูรณาการกับเทคโนโลยีป้องกันประเทศ ช่วยให้แพทย์สามารถตรวจรักษาผู้ป่วยทางไกลได้โดยไม่ต้องเดินทางไปยังพื้นที่เสี่ยง ในบริบทของการป้องกันประเทศ หน่วยแพทย์ทหารสามารถให้คำปรึกษาผ่านเครือข่าย Telemedicine ทำให้ทหารที่ได้รับบาดเจ็บหรือเจ็บป่วยสามารถเข้าถึงบริการทางการแพทย์ได้รวดเร็วขึ้น แม้อยู่ในพื้นที่ปฏิบัติการ (National Institute of Health, 2023) ระบบเฝ้าระวังสุขภาพอัจฉริยะ (Smart Health Monitoring) เพิ่มความสามารถในการรับมือกับโรคระบาด เทคโนโลยี IoT และ เซ็นเซอร์ชีวภาพ ถูกนำมาใช้ในการติดตามสุขภาพของประชาชนและกำลังพลในค่ายทหาร เพื่อเฝ้าระวังการแพร่ระบาดของโรคติดต่อ การใช้ Big Data Analytics เพื่อวิเคราะห์ข้อมูลสุขภาพแบบเรียลไทม์ สามารถช่วยให้ภาครัฐสามารถวางแผนเชิงรุกในการควบคุมโรคระบาด และกำหนดนโยบายด้านสาธารณสุขที่มีประสิทธิภาพมากขึ้น (Defence Technology Institute, 2024) ปัญญาประดิษฐ์ (AI) และการคาดการณ์โรคระบาดผ่าน Big Data AI และ Machine Learning ถูกนำมาใช้ในการ คาดการณ์แนวโน้มการแพร่ระบาดของโรค โดยใช้ข้อมูลจากระบบเฝ้าระวังโรค ระบบนี้สามารถแจ้งเตือนเจ้าหน้าที่รัฐให้เตรียมมาตรการป้องกันได้ล่วงหน้า ซึ่งช่วยลดการแพร่ระบาดของโรคที่อาจส่งผลกระทบต่อความมั่นคงของประเทศ (R1-Proposal, 2025)

2. ผลต่อความมั่นคงแห่งชาติ (National Security)

ในบริบทของความมั่นคงแห่งชาติ การบูรณาการเทคโนโลยีทางการแพทย์และเทคโนโลยีป้องกันประเทศ ช่วยเพิ่มขีดความสามารถของกองทัพและหน่วยงานด้านความมั่นคง ในการเฝ้าระวังและตอบโต้ภัยคุกคามอากาศยานไร้คนขับ (UAVs) สนับสนุนภารกิจทางการแพทย์และการป้องกันประเทศ UAVs ถูกนำมาใช้ในการส่งมอบเวชภัณฑ์และอุปกรณ์ทางการแพทย์ไปยังพื้นที่ภัยพิบัติ หรือพื้นที่ที่เข้าถึงยาก นอกจากนี้ UAVs ยังสามารถติดตั้งเซ็นเซอร์เพื่อ ตรวจจับสารชีวภาพที่เป็นอันตราย และเฝ้าระวังการก่อการร้ายทางชีวภาพได้อย่างมีประสิทธิภาพ (Chan et al., 2023). ระบบสื่อสารทางการแพทย์และเครือข่ายดิจิทัล (Military Digital Networks) ช่วยเพิ่มความแม่นยำในการสื่อสารและการสั่งการ การใช้ เครือข่าย 5G และการเข้ารหัสข้อมูลระดับสูง ทำให้สามารถถ่ายทอดข้อมูลทางการแพทย์และข้อมูลด้านความมั่นคงระหว่างหน่วยงานได้อย่างรวดเร็วและปลอดภัย ระบบนี้ช่วยให้ แพทย์ทหารสามารถให้คำแนะนำแก่หน่วยรบในสนามรบ และช่วยให้หน่วยความมั่นคงสามารถตัดสินใจได้แม่นยำขึ้น (Defence Technology Institute, 2024) AI และ Big Data สำหรับการเฝ้าระวังและตอบโต้ภัยคุกคาม AI ถูกนำมาใช้ในการวิเคราะห์ พฤติกรรมต้องสงสัยทางไซเบอร์และภัยคุกคามทางชีวภาพ ซึ่งช่วยให้รัฐบาลสามารถป้องกันการโจมตีที่อาจกระทบต่อโครงสร้างพื้นฐานด้านสุขภาพและความมั่นคงของประเทศ ระบบ Big Data ถูกนำมาใช้ในการวิเคราะห์ ข้อมูลข่าวกรองทางทหารและข้อมูลสุขภาพระดับประเทศ เพื่อให้รัฐบาลสามารถเตรียมความพร้อมรับมือกับภัยคุกคามในทุกมิติ (Zhang et al., 2022)

3. ประสิทธิภาพของระบบเฝ้าระวังและตอบโต้ภัยคุกคาม

ผลการศึกษาแสดงให้เห็นว่า การบูรณาการเทคโนโลยีป้องกันประเทศและเทคโนโลยีการแพทย์ช่วยเพิ่มประสิทธิภาพของระบบเฝ้าระวังและตอบโต้ภัยคุกคาม ในระดับชาติ ระบบ AI และ UAVs ช่วยเพิ่มความรวดเร็วในการเฝ้าระวังภัยคุกคาม UAVs สามารถตรวจสอบพื้นที่เสี่ยงภัยในเวลาจริง (real-time monitoring) ทำให้สามารถตอบสนองต่อสถานการณ์ฉุกเฉินได้อย่างรวดเร็ว AI ช่วยคาดการณ์แนวโน้มภัยคุกคาม เช่น การแพร่ระบาดของโรค หรือการโจมตีทางไซเบอร์ เพื่อให้ภาครัฐสามารถดำเนินมาตรการป้องกันได้ทัน่วงที (Visanu, 2025) เครือข่ายดิจิทัลและการบูรณาการข้อมูลช่วยเพิ่มความแม่นยำในการตัดสินใจ ระบบการสื่อสารทางการแพทย์และ



การทหาร ถูกพัฒนาให้สามารถทำงานร่วมกัน เพื่อให้หน่วยงานความมั่นคงและสาธารณสุขสามารถแบ่งปันข้อมูลที่เป็นประโยชน์ได้แบบเรียลไทม์ระบบนี้ช่วยเพิ่ม ความแม่นยำของการวางแผนและการสั่งการในสถานการณ์ฉุกเฉิน (Defence Technology Institute, 2024).

ตารางที่ ๕.๑ ผลการสัมภาษณ์เชิงลึก

หัวข้อการสัมภาษณ์	ข้อมูลจากผู้ให้สัมภาษณ์
การบูรณาการเทคโนโลยีทางการแพทย์และป้องกันประเทศ	การบูรณาการเทคโนโลยีการแพทย์และป้องกันประเทศสามารถช่วยให้การบริหารจัดการทรัพยากรมีประสิทธิภาพมากขึ้น โดยเฉพาะในสถานการณ์ฉุกเฉิน
ประสิทธิภาพของระบบ Telemedicine ในหน่วยทหาร	ระบบ Telemedicine มีบทบาทสำคัญในภารกิจทางทหาร โดยเฉพาะในพื้นที่ห่างไกลและพื้นที่ขัดแย้ง ช่วยลดภาระของแพทย์ภาคสนาม
การใช้ AI และ Big Data ในการเฝ้าระวังภัยคุกคาม	AI และ Big Data ช่วยเพิ่มความสามารถในการคาดการณ์โรคระบาดและภัยคุกคาม โดยการวิเคราะห์ข้อมูลแบบเรียลไทม์จากแหล่งต่างๆ
บทบาทของ UAVs ในการสนับสนุนภารกิจสาธารณสุขและความมั่นคง	UAVs ถูกนำมาใช้ในการขนส่งเวชภัณฑ์และตรวจตราพื้นที่ที่เข้าถึงยาก ลดความเสี่ยงของบุคลากรทางการแพทย์และเจ้าหน้าที่ความมั่นคง
ความท้าทายในการบูรณาการเทคโนโลยีทั้งสองภาคส่วน	ความท้าทายหลักคือการบูรณาการโครงสร้างพื้นฐานและการรักษาความปลอดภัยของข้อมูล เนื่องจากทั้งสองระบบต้องใช้เครือข่ายที่มีความเสถียรสูง

ซึ่งหลังจากที่ผู้วิจัยได้ทำการศึกษาจากข้อมูลปฐมภูมิและทุติยภูมิแล้วพบว่า ในยุคที่เทคโนโลยีดิจิทัลมีบทบาทสำคัญในทุกมิติของการดำรงชีวิต การบูรณาการ เทคโนโลยีทางการแพทย์ และ เทคโนโลยีป้องกันประเทศ ได้กลายเป็นแนวทางที่สำคัญในการเพิ่มประสิทธิภาพของ ระบบสาธารณสุขและความมั่นคงแห่งชาติ กรอบแนวคิดนี้พิจารณาถึงปัจจัยที่เกี่ยวข้องกับการบูรณาการเทคโนโลยีเหล่านี้ รวมถึงผลกระทบต่อ ประสิทธิภาพ การรับมือโรคระบาด และ ระบบเฝ้าระวังและตอบโต้ภัยคุกคามทางทหาร โดยองค์ประกอบของกรอบแนวคิด กรอบแนวคิดนี้ถูกออกแบบโดยอาศัยองค์ประกอบหลัก 3 ส่วน ได้แก่ เทคโนโลยีที่ใช้ในการบูรณาการ ปัจจัยสนับสนุนที่ส่งผลต่อการบูรณาการ และผลลัพธ์ของการบูรณาการเทคโนโลยีต่อความมั่นคงแห่งชาติ โดยการบูรณาการเทคโนโลยีเพื่อ

เสริมสร้างความมั่นคงแห่งชาติพิจารณาจากสองกลุ่มเทคโนโลยีหลัก ได้แก่ เทคโนโลยีทางการแพทย์ (Medical Technology) และ เทคโนโลยีป้องกันประเทศ (Defense Technology) 1. เทคโนโลยีทางการแพทย์ (Medical Technology) เทคโนโลยีด้านการรักษาเป็นรากฐานสำคัญของระบบสาธารณสุขที่สามารถเชื่อมโยงกับระบบความมั่นคงได้ เทคโนโลยีหลักในกลุ่มนี้ ได้แก่ ระบบการแพทย์ทางไกล (Telemedicine): ช่วยให้แพทย์สามารถให้บริการรักษาผู้ป่วยจากระยะไกล โดยเฉพาะในพื้นที่ห่างไกลหรือสถานการณ์ที่บุคลากรทางการแพทย์ไม่สามารถเข้าถึงได้ ระบบเฝ้าระวังสุขภาพอัจฉริยะ (Smart Health Monitoring): ใช้ IoT และเซ็นเซอร์เพื่อเฝ้าระวังสุขภาพของประชาชนและกำลังพลแบบเรียลไทม์ ปัญญาประดิษฐ์ในระบบสุขภาพ (AI in Healthcare):



ใช้ AI และ Big Data วิเคราะห์แนวโน้มการแพร่ระบาดของโรค ช่วยให้สามารถวางแผนเชิงรุกได้อย่างแม่นยำ

2. เทคโนโลยีป้องกันประเทศ (Defense Technology) เทคโนโลยีป้องกันประเทศเป็นเครื่องมือสำคัญในการเฝ้าระวังภัยคุกคามทางทหารและสนับสนุนการดำเนินงานด้านสาธารณสุข เทคโนโลยีหลักในกลุ่มนี้ ได้แก่ อากาศยานไร้คนขับ (Unmanned Aerial Vehicles: UAVs): สามารถใช้ในการส่งเวชภัณฑ์ เฝ้าระวังภัยพิบัติ และตรวจสอบพื้นที่เสี่ยง

ระบบสื่อสารทางการทหารและโครงข่ายดิจิทัล (Military Communication Networks): ช่วยให้หน่วยงานสาธารณสุขและความมั่นคงสามารถแบ่งปันข้อมูลได้แบบเรียลไทม์ ระบบปัญญาประดิษฐ์และข้อมูลขนาดใหญ่เพื่อความมั่นคง (AI & Big Data for Security): ใช้ AI วิเคราะห์ภัยคุกคามที่อาจเกิดขึ้น เช่น การโจมตีทางไซเบอร์หรือการก่อการร้ายทางชีวภาพ

3. ปัจจัยสนับสนุนการบูรณาการ การบูรณาการเทคโนโลยีทางการแพทย์และเทคโนโลยีป้องกันประเทศไม่สามารถเกิดขึ้นได้หากปราศจาก ปัจจัยสนับสนุน ที่เอื้อต่อการดำเนินงาน ปัจจัยสำคัญที่เกี่ยวข้อง ได้แก่ นโยบายภาครัฐ (Government Policies) นโยบายของภาครัฐเกี่ยวกับการพัฒนาเทคโนโลยีด้านสุขภาพและความมั่นคง การกำหนดกฎระเบียบด้าน การใช้ AI และ Big Data ในระบบป้องกันประเทศและสาธารณสุข

4.2 ความร่วมมือระหว่างภาคส่วนต่าง ๆ (Collaboration Across Sectors) ความร่วมมือระหว่าง กระทรวงสาธารณสุขและกระทรวงกลาโหม การทำงานร่วมกันระหว่าง ภาคเอกชน หน่วยงานวิจัย และสถาบันการศึกษา เพื่อพัฒนาเทคโนโลยี

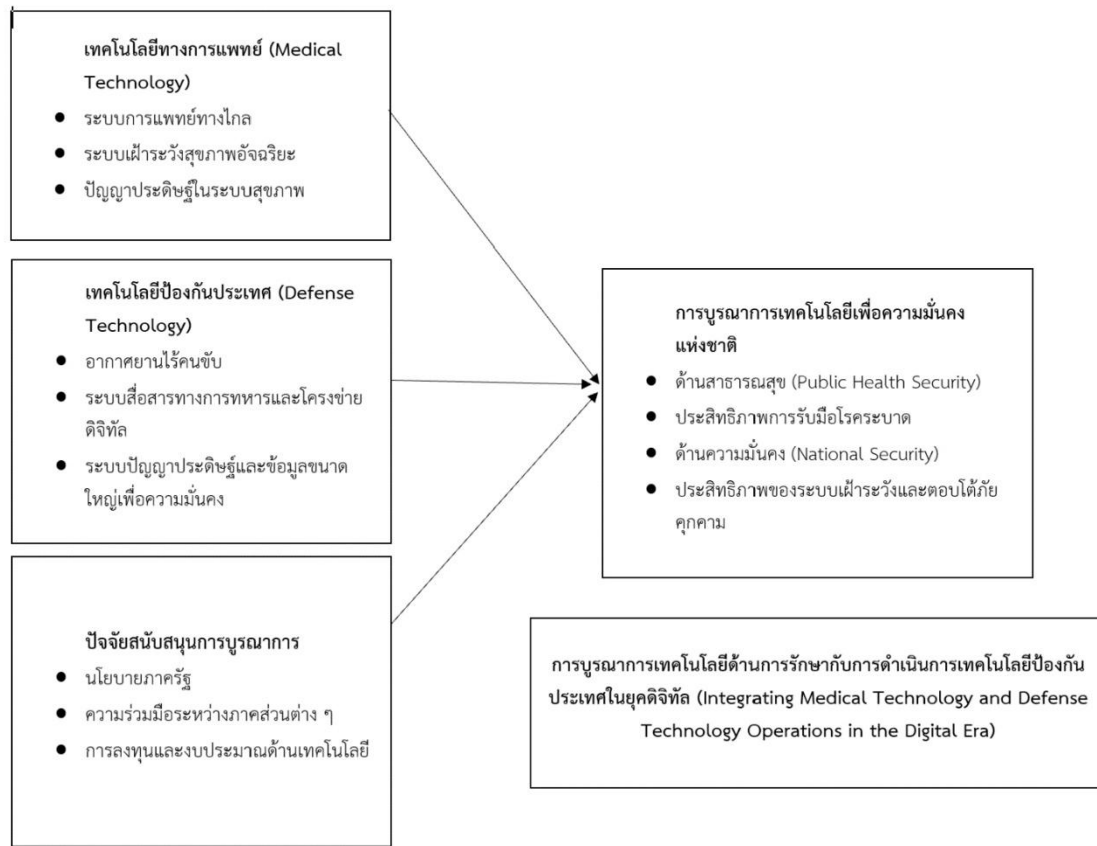
3. การลงทุนและงบประมาณด้านเทคโนโลยี (Investment & Budget Allocation) การลงทุนในโครงสร้างพื้นฐาน 5G และระบบเครือข่ายดิจิทัล งบประมาณสนับสนุนการพัฒนา UAVs และ AI ในภาคความมั่นคงและสาธารณสุข

4.ผลลัพธ์ของการบูรณาการเทคโนโลยี การบูรณาการเทคโนโลยีทั้งสองด้านก่อให้เกิดผลลัพธ์สำคัญที่ช่วยเสริมสร้าง ความมั่นคงด้านสาธารณสุขและความมั่นคงแห่งชาติ โดยมีองค์ประกอบสำคัญ ดังนี้ 1. ด้านสาธารณสุข (Public Health Security) เพิ่มขีดความสามารถในการรับมือโรคระบาด ผ่านการใช้ AI และ Big Data ในการคาดการณ์แนวโน้มการแพร่ระบาด เพิ่มการเข้าถึงบริการทางการแพทย์ ในพื้นที่ห่างไกลผ่านระบบ Telemedicine และ UAVs เสริมสร้างระบบเฝ้าระวังโรคติดต่อ ผ่าน Smart Health Monitoring

2. ด้านความมั่นคงแห่งชาติ (National Security) เพิ่มประสิทธิภาพของระบบเฝ้าระวังภัยคุกคาม โดยใช้ AI วิเคราะห์ข้อมูลข่าวกรองแบบเรียลไทม์ เพิ่มศักยภาพของหน่วยรบและระบบสนับสนุนทางการแพทย์ ผ่านการใช้ UAVs และเครือข่ายดิจิทัลทางทหารลดภาระของกำลังพล โดยใช้เทคโนโลยีอัจฉริยะช่วยในการตัดสินใจและการเฝ้าระวัง

สรุปกรอบแนวคิดนี้ชี้ให้เห็นว่า การบูรณาการเทคโนโลยีด้านการรักษาและเทคโนโลยีป้องกันประเทศเป็นปัจจัยสำคัญที่ช่วยเพิ่มประสิทธิภาพของระบบสาธารณสุขและความมั่นคงแห่งชาติ การใช้เทคโนโลยี Telemedicine, Smart Health Monitoring, UAVs, AI และ Big Data สามารถช่วยให้ประเทศไทยสามารถเฝ้าระวังและตอบสนองต่อภัยคุกคามทางสุขภาพและความมั่นคง ได้อย่างมีประสิทธิภาพ นโยบายภาครัฐ ความร่วมมือระหว่างภาคส่วน และงบประมาณด้านเทคโนโลยี เป็นปัจจัยสำคัญที่ผลักดันให้ เทคโนโลยีทางการแพทย์และเทคโนโลยีป้องกันประเทศสามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพ ส่งผลให้ประเทศไทยสามารถ ปรับตัวและรับมือกับภัยคุกคามในอนาคตได้อย่างมั่นคง ซึ่งสามารถแสดงได้ดังภาพที่ 5.2





อภิปรายผล

การวิจัยเรื่อง “การบูรณาการเทคโนโลยีด้านการรักษากับการดำเนินการเทคโนโลยีป้องกันประเทศในยุคดิจิทัล” ได้ศึกษาถึง แนวทางการเชื่อมโยงเทคโนโลยีด้านสาธารณสุขและเทคโนโลยีป้องกันประเทศ เพื่อเสริมสร้าง ความมั่นคงแห่งชาติ โดยเฉพาะในบริบทของการรับมือโรคระบาดและภัยคุกคามทางทหาร ผลการวิจัยพบว่า การบูรณาการเทคโนโลยีด้านการแพทย์และการป้องกันประเทศ มีความเป็นไปได้สูงและสามารถเพิ่มประสิทธิภาพของระบบสาธารณสุขและความมั่นคงแห่งชาติ โดยมีองค์ประกอบหลักดังนี้

- เทคโนโลยีทางการแพทย์ (Medical Technology) เช่น Telemedicine, Smart Health Monitoring และ AI ช่วยเพิ่มการเข้าถึงบริการสุขภาพ ลดภาระของบุคลากรทางการแพทย์ และเฝ้าระวังโรคระบาด

- เทคโนโลยีป้องกันประเทศ (Defense Technology) เช่น UAVs, Military Digital Networks และ AI for Security ช่วยเสริมสร้างศักยภาพในการเฝ้าระวังภัยคุกคามและเพิ่มความสามารถในการตอบโต้ภัยพิบัติและสงครามไฮบริด

- ปัจจัยสนับสนุน (Enabling Factors) เช่น นโยบายภาครัฐ ความร่วมมือระหว่างภาคส่วน และการลงทุนด้านเทคโนโลยี เป็นปัจจัยสำคัญที่ช่วยให้การบูรณาการเทคโนโลยีดำเนินไปได้อย่างมีประสิทธิภาพ

ผลการศึกษาชี้ให้เห็นว่า การบูรณาการเทคโนโลยีเหล่านี้นับเป็นบทบาทสำคัญต่อการเพิ่มประสิทธิภาพของระบบเฝ้าระวังและตอบโต้ภัยคุกคามระดับประเทศ โดยเฉพาะในสถานการณ์ฉุกเฉิน เช่น การแพร่ระบาดของโรคและภัยคุกคามทางไซเบอร์



อภิปรายผล

การบูรณาการเทคโนโลยีด้านการรักษาและเทคโนโลยีป้องกันประเทศช่วยเพิ่มความมั่นคงด้านสาธารณสุขและความมั่นคงแห่งชาติจากผลการศึกษา พบว่า การเชื่อมโยงเทคโนโลยีการแพทย์และการป้องกันประเทศสามารถช่วยเสริมสร้างความมั่นคงแห่งชาติได้อย่างมีประสิทธิภาพ ซึ่งสอดคล้องกับนโยบายของหลายประเทศ เช่น สหรัฐอเมริกาและจีน ที่มีการพัฒนา AI และ Big Data ในการเฝ้าระวังภัยคุกคามทางสุขภาพและความมั่นคง (Chan et al., 2023) การนำ Telemedicine และ Smart Health Monitoring มาใช้ในกองทัพและพื้นที่ชายแดนช่วยให้สามารถให้บริการทางการแพทย์ได้ในพื้นที่ที่ยากต่อการเข้าถึง ลดภาระของบุคลากรทางการแพทย์ และช่วยให้การเฝ้าระวังโรคระบาดเป็นไปได้อย่างแม่นยำขึ้นนอกจากนี้ UAVs และ Military Digital Networks ยังช่วยเพิ่มขีดความสามารถในการเฝ้าระวังและตอบโต้ภัยคุกคามทางทหารและทางชีวภาพ ซึ่งเป็นแนวทางที่สอดคล้องกับงานวิจัยก่อนหน้านี้เกี่ยวกับ ความมั่นคงทางทหารในยุคดิจิทัล (Visanu, 2025)

ความท้าทายในการบูรณาการเทคโนโลยีทั้งสองภาคส่วน แม้ว่าการบูรณาการเทคโนโลยีจะมีศักยภาพสูง แต่ผลการศึกษายังแสดงให้เห็นว่า ยังมีความท้าทายที่สำคัญ ได้แก่ ข้อจำกัดด้านโครงสร้างพื้นฐานและเครือข่ายดิจิทัล

- การบูรณาการต้องอาศัย ระบบเครือข่ายดิจิทัลที่มีเสถียรภาพ เช่น 5G และเครือข่ายทหารดิจิทัล ซึ่งปัจจุบันยังไม่ครอบคลุมทุกพื้นที่ปัญหาด้านความปลอดภัยทางไซเบอร์
- การบูรณาการเทคโนโลยีทำให้มีความเสี่ยงต่อ การโจมตีทางไซเบอร์ โดยเฉพาะข้อมูลสุขภาพและข้อมูลทางทหารที่มีความอ่อนไหวความร่วมมือระหว่างภาครัฐและเอกชน
- การพัฒนาเทคโนโลยีต้องอาศัย ความร่วมมือระหว่างหน่วยงานทางการแพทย์ หน่วยงานทหาร และภาคเอกชน ซึ่งต้องมีการกำหนด มาตรฐานความร่วมมือและกฎระเบียบที่ชัดเจน

ข้อเสนอแนะ

ข้อเสนอแนะเชิงนโยบาย

ภาครัฐควรส่งเสริมการพัฒนาเครือข่ายดิจิทัลเพื่อสนับสนุนการบูรณาการเทคโนโลยี

- ควรมีการลงทุนใน เครือข่าย 5G สำหรับระบบ Telemedicine และ Military Digital Networks เพื่อให้สามารถเชื่อมต่อข้อมูลได้อย่างรวดเร็วและปลอดภัย จัดทำกรอบนโยบายด้านความมั่นคงทางไซเบอร์สำหรับระบบสุขภาพและความมั่นคงแห่งชาติ
- ควรมีการกำหนด มาตรการป้องกันภัยคุกคามทางไซเบอร์ ที่เกี่ยวข้องกับ ข้อมูลสุขภาพและข้อมูลทางทหาร เพื่อลดความเสี่ยงจากการโจมตีของแฮกเกอร์ สนับสนุนโครงการวิจัยและพัฒนา AI และ Big Data สำหรับการเฝ้าระวังภัยคุกคามระดับชาติ
- รัฐบาลควรส่งเสริม การใช้ AI และ Big Data เพื่อคาดการณ์ภัยคุกคาม เช่น การแพร่ระบาดของโรค และการโจมตีทางไซเบอร์

เอกสารอ้างอิง

- Asian Development Bank. (2024). *Investment trends in national security and public health technology*. Manila, Philippines: ADB Publications.
- Chan, T., Smith, R., & Lee, M. (2023). Artificial intelligence in defense and healthcare: Emerging trends and applications. *Journal of Defense Technology*, 45(2), 112–130.





- Defence Technology Institute. (2024). *Integration of AI-driven UAVs in Thailand's national security framework*. Bangkok, Thailand: DTI Research Division.
- Defence Technology Institute. (2024). *National defense strategy and technological integration*. Bangkok, Thailand: DTI Press.
- European Commission. (2023). *EU cybersecurity policies and AI-driven security systems*. Brussels, Belgium: European Commission.
- National Institute of Health. (2023). *The role of AI in public health surveillance: A global perspective*. Washington, DC: NIH.
- National Institute of Security. (2023). *Encrypted communication and cybersecurity in modern warfare*. London, England: Security Research Center.
- R1-Proposal. (2025). *Integrated defense technology and healthcare strategies for national resilience*. Bangkok, Thailand: National Research Institute.
- Smith, J., & Patel, A. (2023). The role of 5G networks in secure military communication and telemedicine. *Journal of Digital Security*, 18(2), 76–92.
- Thailand Ministry of Defense. (2024). *Strategic framework for national defense and health security integration*. Bangkok, Thailand: Government Publications.
- US Department of Defense. (2023). *AI and Big Data in military applications: Enhancing threat prediction and response*. Washington, DC: Pentagon Press.
- Visanu, P. (2025). The impact of AI and UAVs on national security: A case study of Thailand. *Asian Journal of Security Studies*, 33(1), 45–67.
- World Health Organization. (2022). *Telemedicine and digital health solutions for global pandemics*. Geneva, Switzerland: WHO.
- Zhang, Y., Wang, L., & Chen, H. (2022). Big Data in military intelligence and threat detection: An AI-driven approach. *Defense Cybersecurity Journal*, 12(4), 189–205.

