

การปฏิบัติการข่าวสาร
ภัยคุกคามที่มีผลกระทบต่อความมั่นคงปลอดภัยของกองทัพไทย

เอกสารวิจัยส่วนบุคคล



โดย

พันเอก วัชรินทร์ แก่นทอง

รองผู้อำนวยการกองปฏิบัติการเทคโนโลยีสารสนเทศ
ศูนย์เทคโนโลยีสารสนเทศทหาร กรมการสื่อสารทหาร กองบัญชาการกองทัพไทย

วิทยาลัยการทัพบก

กันยายน 2560

บทคัดย่อ

ผู้วิจัย พันเอก วัชรินทร์ แก่นทอง
เรื่อง การปฏิบัติการข่าวสารภัยคุกคามที่มีผลกระทบต่อความมั่นคงปลอดภัยของกองทัพไทย
วันที่ กันยายน 2560 **จำนวนคำ :** 5,962 **จำนวนหน้า :** 20
คำสำคัญ การปฏิบัติการข่าวสาร, Information Operations, IO
ชั้นความลับ ไม่มีชั้นความลับ

การศึกษาวิจัยเรื่อง การปฏิบัติการข่าวสารภัยคุกคามที่มีผลกระทบต่อความมั่นคงปลอดภัยของกองทัพไทย มีวัตถุประสงค์เพื่อศึกษาการปฏิบัติการข่าวสารที่มีการพัฒนาและเปลี่ยนแปลงรูปแบบซึ่งเป็นภัยคุกคามที่มีผลกระทบต่อความมั่นคงปลอดภัยของกองทัพไทย และศึกษาแนวทางการปฏิบัติกับภัยคุกคามที่เกิดจากการปฏิบัติการข่าวสาร เพื่อกำหนดกรอบในการเตรียมความพร้อมในการจัดการกับภัยคุกคามและรักษาความมั่นคงปลอดภัยสารสนเทศของกองทัพไทย

ผลการวิจัยพบว่า หน่วยงานด้านความมั่นคงและกองทัพที่มีเทคโนโลยีที่เหนือชั้นกว่าและมีระบบการจัดการข่าวสารที่ดีกว่า จะสามารถชิงความได้เปรียบในการตอบโต้ได้ดีกว่า และที่สำคัญถ้าข้อมูลข่าวสารจากพื้นที่การรบมีให้ผู้บังคับบัญชาครบรอบด้าน ก็จะทำให้ผู้บังคับบัญชาสามารถตัดสินใจได้อย่างถูกต้อง

ข้อเสนอแนะจากการวิจัย หน่วยงานด้านความมั่นคงและกองทัพจึงมีความจำเป็นที่จะต้องปรับตัวและเสริมสร้างศักยภาพขีดความสามารถในมิติไซเบอร์ (Cyberspace) ซึ่งเป็นส่วนสนับสนุนการรบที่สำคัญ โดยต้องมีความมุ่งมั่นในการวางยุทธศาสตร์ของการปฏิบัติการข่าวสาร และยุทธวิธีในการใช้และตอบโต้สงครามสารสนเทศและสื่อ เพื่อให้การปฏิบัติการข่าวสารประสบความสำเร็จอย่างเป็นรูปธรรมและมีประสิทธิผล

ABSTRACT

AUTHOR : Colonel Wacharin Kaenthong

TITLE: Information Operations threats that affect security Of Thai
Armed Forces

DATE: September 2017 **WORD COUNT:** 5,962 **PAGES:** 20

KEY TERMS: Information Operations, IO

CLASSIFICATION: Unclassified

Research study Subject Information Operations threats that affect security Of Thai Armed Forces The purpose is to study IO development and change patterns, which are a threat to the security of the Thai Armed Forces. And study the practices of IO threats. To set the framework for preparedness to deal with threats and maintain information security of the Thai Armed Forces.

The research found that Security agencies and armed forces with superior technology. Better grade and better news management system. Will be able to take advantage of the retaliation better. And most importantly, if the information from the combat area is provided to the commanding officer to complete the round. It will allow the supervisor to make the right decision.

Research recommendations Security and Army
There is a need to adapt and strengthen cyberspace, which is an important battlefield. Must be committed to the implementation of IO strategies. And tactics to use and respond to information and media warfare. To make IO successful, concrete and effective.

กิตติกรรมประกาศ

เอกสารวิจัยฉบับนี้สำเร็จได้ด้วยความอนุเคราะห์อย่างยิ่งจากอาจารย์ที่ปรึกษา พันเอก พิชชญาน พวงทอง และผู้ทรงคุณวุฒิที่ปรึกษา พลโท สุทธิศักดิ์ สลักคำ ที่กรุณาให้คำแนะนำช่วยเหลือ ตลอดจนให้ความรู้ ข้อคิดเห็น ข้อเสนอแนะต่าง ๆ และประสบการณ์ที่ดี อันเป็นประโยชน์ต่อการวิจัยอย่างต่อเนื่อง

ขอขอบคุณผู้บังคับบัญชา ที่มีส่วนในการตัดสินใจให้ผู้วิจัย มีโอกาสมาเข้ารับการศึกษาในวิทยาลัยการทัพบก สถาบันอันทรงเกียรติ ตลอดจนเพื่อนนักศึกษาที่ได้มีส่วนร่วมในการศึกษา ทำกิจกรรมร่วมกัน และเป็นกำลังใจให้กันตลอดช่วงเวลาของการทำวิจัยในช่วงเวลาของการศึกษาหลักสูตรหลักประจำ วิทยาลัยการทัพบก ชุดที่ 62

สุดท้ายนี้ ขอกราบขอบพระคุณ คณาจารย์ที่ประสิทธิ์ประสาทวิชาความรู้ แก่ผู้วิจัยสามารถทำการวิจัยได้สำเร็จลุล่วงเป็นไปตามวัตถุประสงค์ของวิทยาลัยการทัพบก ทุกประการ หากส่วนดีในการศึกษาครั้งนี้มีคุณประโยชน์อันใด ขอมอบความดีทั้งหมดให้กับทุกท่านที่ได้กล่าวถึงด้วยความเคารพ

การปฏิบัติการข่าวสาร

ภัยคุกคามที่มีผลกระทบต่อความมั่นคงปลอดภัยของกองทัพไทย

กระบวนการพัฒนาประเทศไทยภายใต้ “ประเทศไทย 4.0” เป็นอีกนโยบายหนึ่งที่เป็น การวางรากฐานการพัฒนาประเทศไทยในระยะยาว เป็นจุดเริ่มต้นในการขับเคลื่อนไปสู่ การเป็นประเทศที่มั่นคง มั่งคั่ง และยั่งยืน ตามวิสัยทัศน์รัฐบาล โดยให้ความสำคัญกับ การพัฒนาและนำเทคโนโลยีดิจิทัล มาใช้เป็นเครื่องมือสนับสนุนการพัฒนาประเทศ มุ่งเน้น ให้ประเทศไทยมีโครงสร้างพื้นฐานด้านไอซีที โดยเฉพาะอย่างยิ่งอินเทอร์เน็ตความเร็วสูง กระจายอย่างทั่วถึงเสมือนบริการสาธารณูปโภคขั้นพื้นฐานทั่วไป ประชาชน มีความรอบรู้ เข้าถึง สามารถพัฒนาและใช้ประโยชน์จากสารสนเทศโดยเท่าเทียมกัน

ความก้าวหน้าด้านสารสนเทศและการสื่อสารในโลกที่แปรเปลี่ยนไปอย่างรวดเร็ว โดย อำนาจด้านสารสนเทศและสื่อ (Information and media) ได้เปลี่ยนผ่านจากภาครัฐไปสู่ ภาคเอกชนและภาคประชาชน สารสนเทศและสื่อมีอิทธิพลต่อความคิดเห็น ความเชื่อ และ การตอบสนองของประชาชนในระดับชาติและระดับนานาชาติอย่างกว้างขวาง เนื่องจา การเชื่อมต่อข้อมูลโดยสมบูรณ์จนทำให้การกระจายตัวของข่าวสารมีความรวดเร็วแบบ Real time ปรากฏการณ์นี้ทำให้สื่อที่ผ่านทางระบบสื่อสารโทรคมนาคม โดยเฉพาะทาง อินเทอร์เน็ตมีอิทธิพลต่อการตัดสินใจในระดับชาติ จึงทำให้มิติของการรบและความมั่นคง เปลี่ยนแปลงไปอย่างมาก มิได้มีเพียงทางอากาศ ทางพื้นดิน ทางน้ำ และอวกาศ แต่ยัง รวมถึงมิติไซเบอร์ (Cyberspace)¹ ซึ่งถือเป็นส่วนสนับสนุนการรบที่สำคัญ ที่มีผลต่อปัจจัยความสำเร็จของสงครามในยุคสารสนเทศ (Information Age) ดังนั้น หน่วยงานด้านความมั่นคงและกองทัพจึงมีความจำเป็นอย่างยิ่งที่จะต้องปรับตัวและ เสริมสร้างขีดความสามารถ โดยตระหนักถึงการวางยุทธศาสตร์และยุทธวิธีในการใช้ ประโยชน์และตอบโต้การปฏิบัติการข่าวสารของฝ่ายตรงข้ามที่เป็นภัยคุกคามและ มีผลกระทบต่อความมั่นคงปลอดภัยของกองทัพไทย เพื่อการปฏิบัติได้อย่างมีประสิทธิภาพ และประสิทธิผลสูงสุด ทั้งนี้ ผู้วิจัยต้องการศึกษาในเรื่องการปฏิบัติการข่าวสารที่พัฒนา และเปลี่ยนแปลงรูปแบบในยุคสารสนเทศ, ภัยคุกคามและผลกระทบที่มีต่อกองทัพไทย และแนวทางที่จะปฏิบัติกับภัยคุกคามที่เกิดจากการปฏิบัติการข่าวสาร

การปฏิบัติการข่าวสาร (Information Operations) เรียกกย่อ ๆ ว่า Info Ops หรือ IO ซึ่งมาจากการให้คำจำกัดความแตกต่างกันไป ซึ่งมักจะเกิดจากความเข้าใจเอาเองของผู้ปฏิบัติ เช่น ความเข้าใจว่าหมายถึงการปฏิบัติการจิตวิทยา (Psychological Operation) การโฆษณาชวนเชื่อ (Propaganda) การวิเทศสัมพันธ์ทางสื่อมวลชน (Media Relations) หรือการลวงทางทหาร (Deception) เป็นต้น ซึ่งความเข้าใจดังกล่าวอาจจะไม่ผิด หากแต่เป็นการเลือกกล่าวถึงเครื่องมือบางประการของการปฏิบัติการข่าวสาร โดยอาจจะยังไม่เข้าใจความหมายในองค์รวม นอกจากนี้ การปฏิบัติการข่าวสารที่ใช้ในหน่วยงานที่มีภารกิจแตกต่างกัน ก็มีผลทำให้ความหมายอาจจะแตกต่างกันไปด้วย ซึ่งในที่นี้จะขอยกคำจำกัดความที่มีการใช้อีกมากกล่าวโดยสังเขป ได้แก่

คณะเสนาธิการร่วมของกองทัพสหรัฐอเมริกา ให้คำจำกัดความว่า “การปฏิบัติการที่มุ่งให้มีผลต่อข้อมูลข่าวสารของฝ่ายตรงข้าม ขณะเดียวกันก็เป็นการปฏิบัติการเพื่อป้องกันข้อมูลข่าวสารและระบบข้อมูลข่าวสารของฝ่ายสหรัฐอเมริกาเอง”²

กองทัพบกสหรัฐอเมริกา ให้คำจำกัดความว่า “การปฏิบัติการเชิงรุกและรับ โดยใช้เทคโนโลยีสารสนเทศสมัยใหม่เพื่อลดค่า ทำลาย ปฏิเสธ ลวง มีอิทธิพลเหนือหรือขยายผลต่อระบบเครือข่าย ศูนย์สั่งการ ระบบฐานข้อมูลความรู้ ความสามารถในการประมวลผล และระบบการตัดสินใจของฝ่ายตรงข้ามในสถานการณ์ที่ไม่สงบ หรือในภาวะสงคราม โดยกองทัพบกสหรัฐอเมริกาต้องป้องกันข้อมูลข่าวสาร ระบบข้อมูลข่าวสาร และระบบการตัดสินใจของฝ่ายตนให้มีความปลอดภัย”³

กองทัพอากาศสหรัฐอเมริกา ให้คำจำกัดความว่าหมายถึง “การดำเนินการให้ได้มา แสวง ประโยชน์ ป้องกัน หรือการโจมตีข้อมูลข่าวสาร ระบบข้อมูลข่าวสาร ซึ่งรวมถึงข้อมูลข่าวสารในการสงคราม (Information-in-Warfare) และสงครามข่าวสาร (Information Warfare) และการดำเนินการดังกล่าวจะคาบเกี่ยวไปในขั้นตอนของการปฏิบัติการทางทหารด้วย”⁴

นาวิกโยธินสหรัฐอเมริกา ให้คำจำกัดความว่าหมายถึง “การดำเนินการทั้งมวลที่มุ่งให้มีผลต่อข้อมูลข่าวสารหรือระบบข้อมูลข่าวสารของฝ่ายตรงข้าม ขณะเดียวกันก็เป็น การปฏิบัติการเพื่อป้องกันข้อมูลข่าวสารและระบบข้อมูลข่าวสารของฝ่ายตนเอง โดย การปฏิบัติการข่าวสารจะต้องกระทำในทุกขั้นตอนของการปฏิบัติการ ซึ่งคาบเกี่ยวเข้าไป ในขั้นตอนของการปฏิบัติการทางทหารด้วย และมีการกระทำในทุกระดับของสงคราม”⁵

กองบัญชาการกองทัพไทย ให้คำจำกัดความว่า “การสนธิการปฏิบัติต่างๆ เพื่อให้ มีอิทธิพล ทำลาย ลดประสิทธิภาพ หรือชิงการตกลงใจของฝ่ายตรงข้าม (ทั้งที่กระทำโดย มนุษย์ และระบบอัตโนมัติ) และดำเนินการเพื่อป้องกันไม่ให้ฝ่ายตรงข้ามกระทำต่อฝ่ายเรา ในลักษณะเดียวกัน”⁶

สถาบันจิตวิทยาความมั่นคง สถาบันวิชาการป้องกันประเทศ (สจว.สปท.) ให้คำจำกัดความ ว่า “การรวมหน้าที่ และขีดความสามารถต่างๆ ที่เกี่ยวข้องกับข่าวสารและระบบข้อมูล ข่าวสารไว้ด้วยกัน แนวคิดนี้คล้ายกับการปฏิบัติการร่วม (Joint Operation) อันเป็นการ รวมเอาขีดความสามารถของหน่วยต่างๆ หรือการปฏิบัติการผสม (Combined Operation) ซึ่งรวมเอากำลังของกองทัพต่างๆ ของพันธมิตรเข้าด้วยกัน ทำให้เห็นภาพ ของกิจกรรมที่มีความประสานสอดคล้อง และมีผลที่ดีกว่าการรวมตัวเฉพาะภายในหน่วย ของตน แนวคิดนี้คือรากฐานแห่งการนำเอาการปฏิบัติการข่าวสารมาใช้ให้ประสบ ความสำเร็จ ปกติการปฏิบัติการข่าวสารจะนำมาใช้ทางทหารในระดับยุทธการและยุทธวิธี ส่วนในระดับยุทธศาสตร์ การปฏิบัติการข่าวสารก็เป็นส่วนสำคัญส่วนหนึ่งของการสื่อสาร ทางยุทธศาสตร์”⁷

กองทัพบกไทย ได้มีการให้คำจำกัดความว่าหมายถึง “การปฏิบัติการที่มุ่งสร้างผลกระทบ หรือสร้างอิทธิพลต่อกระบวนการตกลงใจ ข่าวสาร ระบบสารสนเทศของฝ่ายตรงข้าม หรือ กลุ่มเป้าหมายอื่นๆ รวมไปถึงการปฏิบัติการเพื่อป้องกันข่าวสารและระบบสารสนเทศของ ฝ่ายเรา”⁸

จากคำจำกัดความดังกล่าวของกองทัพสหรัฐฯ และกองทัพไทย แม้จะมีรายละเอียด แตกต่างกันไปบ้าง แต่โดยสาระสำคัญแล้ว มีความใกล้เคียงกัน และได้แบ่งการดำเนินการ ของการปฏิบัติการข่าวสารออกเป็น 2 ด้าน คือ “เชิงรุก” กับ “เชิงรับ”

การปฏิบัติการเชิงรุก เป็นการเข้าไปใช้ประโยชน์ (ล่วงรู้ความลับ) จากข้อมูลข่าวสารของฝ่ายตรงข้าม ควบคู่ไปกับการทำลายหรือลดศักยภาพข้อมูลข่าวสารหรือระบบข้อมูลข่าวสารของฝ่ายตรงข้าม ไม่ให้เป็นภัยอันตรายต่อฝ่ายตน⁹

การปฏิบัติการเชิงรับ มุ่งเน้นไปที่การปกป้องคุ้มครองความปลอดภัยของข้อมูลข่าวสารและระบบข้อมูลข่าวสารของฝ่ายตนให้พ้นจากการที่ฝ่ายตรงข้ามจะเข้ามาใช้ประโยชน์ทำลาย หรือลดศักยภาพ โดยวัตถุประสงค์ในชั้นปลายคือการดำรงความเหนือกว่าด้านข้อมูลข่าวสาร (Information Superiority) และช่วยให้ผู้บังคับบัญชาสามารถใช้ความเหนือกว่าดังกล่าวให้เป็นประโยชน์ต่อการตัดสินใจเกี่ยวกับการทำสงคราม การรับมือกับสถานการณ์ ภัยคุกคาม หรือความเสี่ยงได้อย่างถูกต้องและทันเวลา¹⁰

หลักการสำคัญของการปฏิบัติ

การปฏิบัติการข่าวสารเป็นกระบวนการที่เกี่ยวข้องกับการดำเนินการเพื่อมุ่งให้มีผลต่อข้อมูลข่าวสาร หรือระบบข้อมูลข่าวสารของฝ่ายตรงข้าม รวมทั้งการป้องกันข้อมูลข่าวสารและระบบข้อมูลข่าวสารของฝ่ายเรา ซึ่งกระบวนการดังกล่าวจะต้องแทรกอยู่ในทุกขั้นตอนของการปฏิบัติการและทุกระดับของสงครามเพื่อให้ฝ่ายเราอยู่ในสถานะที่เหนือกว่า (superiority) ฝ่ายตรงข้าม โดยมุ่งเป้าหมายไปที่ระบบการประมวลผลของฐานข้อมูล ทั้งที่ควบคุมโดยมนุษย์และที่ปฏิบัติงานโดยอัตโนมัติ (ดังเช่นระบบเครื่องจักรกลและ software ในเครือข่ายคอมพิวเตอร์) ตั้งแต่ระดับของผู้กำหนดนโยบายหรือตัดสินใจไปจนถึงหน่วยปฏิบัติในสนามรบ รวมทั้งโครงสร้างพื้นฐานเชิงพาณิชย์ที่สามารถนำมาสนับสนุนภารกิจด้านการทหารได้ เช่น ระบบโทรคมนาคม และพลังงานไฟฟ้า เป็นต้น¹¹

ในการกำหนดยุทธศาสตร์ด้านการปฏิบัติการข่าวสารนั้น สิ่งจำเป็นเป็นลำดับแรกคือความจำเป็นต้องบูรณาการศักยภาพและกิจกรรมของทุกหน่วยที่เกี่ยวข้องเข้าเป็นส่วนเดียวกัน โดยเฉพาะการสนับสนุนด้านการข่าวกรองและการวางเครือข่ายโทรคมนาคมซึ่งเป็นส่วนที่มีความสำคัญมากต่อการปฏิบัติการข่าวสารทั้งเชิงรุกและเชิงรับ รวมทั้งจำเป็นต้องบูรณาการเข้ากับการปฏิบัติการอื่น ทั้งการปฏิบัติการทางอากาศหรืออวกาศ ภาคพื้นดิน ทะเล และหน่วยปฏิบัติการพิเศษ เพื่อให้สอดคล้องกับวัตถุประสงค์แห่งชาติและวัตถุประสงค์ทางทหาร

สำหรับการสนับสนุนด้านการข่าวกรองนั้น จะมีบทบาทสำคัญต่อการวางแผนการสั่งการ และการประมาณสถานการณ์ในการปฏิบัติการข่าวสาร โดยฝ่ายข่าวกรองของหน่วยงานที่ร่วมปฏิบัติการทุกหน่วยจะต้องมีการประสานงานกันอย่างใกล้ชิดและเป็นระบบเพื่อสนับสนุนการวางแผนให้เกิดความสมบูรณ์และมีประสิทธิภาพสูงสุด ประการสำคัญงานข่าวกรองต้องทันเวลา ถูกต้องแม่นยำ สามารถนำไปใช้ประโยชน์ได้ มีความสมบูรณ์ครบถ้วน และตรงกับความต้องการของผู้ใช้ข่าว

จากหลักการสำคัญดังกล่าวแล้วข้างต้น ชี้ให้เห็นได้ว่าแนวทางของการปฏิบัติการข่าวสาร จำเป็นต้องมีการบูรณาการในศักยภาพหลักของหน่วยงานที่เกี่ยวข้องเข้าด้วยกัน ประกอบด้วยสงครามอิเล็กทรอนิกส์ การปฏิบัติการเครือข่ายคอมพิวเตอร์ การปฏิบัติการจิตวิทยา การลวงทางทหาร และการรักษาความปลอดภัยในการปฏิบัติการร่วมกับการสนับสนุนพิเศษและการปฏิบัติการที่เกี่ยวข้องเพื่อให้มีอิทธิพลเหนือหรือสร้างความได้เปรียบฝ่ายตรงข้าม การทำให้ฝ่ายตรงข้ามเกิดความระส่ำระสายหรือแตกแยกทำให้เกิดความเสียหายต่อระบบการสั่งการและการตัดสินใจทั้งที่เป็นระบบสั่งการโดยมนุษย์ หรือโดยเครื่องจักร เช่น ระบบประมวลผลและสั่งการทางคอมพิวเตอร์ (automated decision - making) ขณะเดียวกัน ก็จะต้องระวังป้องกันและรักษาความปลอดภัยจากกิจกรรมทำนองเดียวกันนี้ที่กระทำโดยฝ่ายตรงข้าม

ปฏิบัติการข่าวสารเชิงรุก (Offensive Information Operations) คือ การใช้ศักยภาพและกิจกรรมที่มีการบูรณาการกันของทุกหน่วยที่เกี่ยวข้อง รวมทั้งการสนับสนุนด้านการข่าวกรองเพื่อทำให้เกิดผลเสียหายต่อผู้มีอำนาจในการตัดสินใจของฝ่ายตรงข้าม และเพื่อให้ได้มาซึ่งข้อมูลข่าวสารหรือเพื่อสนับสนุนวัตถุประสงค์พิเศษของฝ่ายเรา เช่น การให้ข้อมูลลวง หรือการขยายผลการสืบสวนในเรื่องใดเรื่องหนึ่งเกี่ยวกับฝ่ายตรงข้าม เป็นต้น โดยศักยภาพและกิจกรรมที่กล่าวถึงดังกล่าว ครอบคลุมถึงการรักษาความปลอดภัยในการปฏิบัติการ การให้ข่าวลวง การปฏิบัติการทางจิตวิทยา สงครามอิเล็กทรอนิกส์ การโจมตีหรือทำลายทางกายภาพ (หมายถึงการโจมตี/ทำลายอาคารสถานที่) การปฏิบัติการข่าวสารที่มีเป้าหมายเฉพาะ ดังเช่น เป้าหมายที่เสี่ยงจะสร้างความเสียหายต่อความมั่นคงของชาติ และอาจรวมถึงการโจมตีเครือข่ายคอมพิวเตอร์ของฝ่ายตรงข้าม

การปฏิบัติการข่าวสารเชิงรุก อาจจะต้องดำเนินการภายใต้สถานการณ์หรือสภาวะการณ์ที่มีความหลากหลาย ตั้งแต่ช่วงก่อนการปฏิบัติการทหารคาบเกี่ยวไปถึงช่วงที่ปฏิบัติการทางทหารได้เริ่มขึ้น รวมทั้งสถานการณ์ที่ล่อแหลมอย่างมากอันจะส่งผลกระทบต่อสันติภาพ หรือในห้วงเวลาที่เป็นจุดเริ่มต้นของวิกฤติ เช่นในช่วงที่ยังไม่เกิดสงครามหรือช่วงที่สงครามเพิ่งเริ่มก่อตัว การปฏิบัติการข่าวสารอาจจะต้องดำเนินการในทุกระดับของสงครามทั้งในระดับยุทธศาสตร์ ยุทธการ และยุทธวิธีที่เกิดขึ้นในทุกสนามรบเป้าหมายของการปฏิบัติการข่าวสารเชิงรุก คือ

1. ลดศักยภาพหรือขีดความสามารถในปฏิบัติการของฝ่ายตรงข้าม
2. ยับยั้งปฏิบัติการและแผนปฏิบัติการของฝ่ายตรงข้าม
3. ยับยั้งความสามารถในการออกคำสั่งด้านยุทธการทั่วไปของฝ่ายตรงข้าม
4. ลดศักยภาพในกระบวนการตัดสินใจของฝ่ายตรงข้าม
5. ชะลอปฏิบัติการของฝ่ายตรงข้าม
6. เข้าไปมีอิทธิพลเหนือการประมาณสถานการณ์ของฝ่ายตรงข้าม¹²

ปฏิบัติการข่าวสารเชิงรับ (Defensive Information Operations) คือ การบูรณาการ การประสานนโยบาย มาตรการการปฏิบัติ บุคลากร และเทคโนโลยีของทุกหน่วยที่เกี่ยวข้อง เพื่อปกป้องคุ้มครองข่าวสารและระบบข่าวสารของฝ่ายเราให้รอดพ้นจากการปฏิบัติการข่าวสารเชิงรุกโดยฝ่ายตรงข้ามโดยให้ความสำคัญทั้งในด้านการสร้างความมั่นใจต่อข้อมูลข่าวสารที่จะใช้ การรักษาความปลอดภัยในการปฏิบัติการ การรักษาความปลอดภัยทางกายภาพ การต่อต้านการให้ข่าวลวง การต่อต้านการปฏิบัติการทางจิตวิทยา การต่อต้านข่าวกรอง สงครามทางอิเล็กทรอนิกส์ และการปฏิบัติการข่าวสารที่มีเป้าหมายเฉพาะ การปฏิบัติการข่าวสารเชิงรับจะต้องได้รับการสนับสนุนข้อมูลด้านการข่าวกรองที่ทันเวลา ถูกต้องแม่นยำ สามารถนำไปใช้ประโยชน์ได้ มีความสมบูรณ์ครบถ้วน ตรงกับความต้องการของผู้ใช้ข่าวแบบเดียวกันกับการปฏิบัติการข่าวสารเชิงรุกเช่นกัน แต่สิ่งที่ต้องดำเนินการควบคู่กันคือ จะต้องสกัดกั้นไม่ให้ฝ่ายตรงข้ามสามารถเข้ามาแสวงประโยชน์ต่อข่าวสารและระบบข้อมูลข่าวสารของฝ่ายเรา รวมทั้งต้องสามารถให้การสนับสนุนการปฏิบัติการข่าวสารเชิงรุกด้วย

นอกจากนี้ การปฏิบัติการข่าวสารเชิงรับยังมีกระบวนการปฏิบัติงานที่เชื่อมโยง
เกี่ยวข้องกันอีก 4 ประการ คือ

- 1) การปกป้องคุ้มครองสภาพแวดล้อมด้านข้อมูลข่าวสารของฝ่ายเรา
- 2) การตรวจสอบความพยายามของฝ่ายตรงข้ามที่จะปฏิบัติการโจมตีฝ่ายเรา
- 3) การรักษาขีดความสามารถในการปฏิบัติการข่าวสารของฝ่ายเราให้ยังคง
สามารถปฏิบัติการได้แม้ในช่วงที่ถูกฝ่ายตรงข้ามโจมตี และ
- 4) รักษาขีดความสามารถในการปฏิบัติการตอบโต้ในช่วงที่ถูกโจมตีจากฝ่าย
ตรงกันข้าม¹³

ด้วยเหตุนี้ แม้การปฏิบัติการข่าวสารเชิงรุกและเชิงรับอาจจะเป็นภารกิจที่ดูเหมือน
แยกส่วนกัน แต่ในทางปฏิบัติแล้วทั้งสองภารกิจจำเป็นต้องมีการบูรณาการหรือ
การประสานการปฏิบัติอย่างใกล้ชิด โดยจะต้องมีการวางแผน การทดสอบการปฏิบัติ และ
การเสริมสร้างศักยภาพหรือดำเนินกิจกรรมที่ประสานสอดคล้องกันด้วยเป้าหมายของ
การปฏิบัติการข่าวสารเชิงรับ คือ

1. เสริมสร้างมาตรการป้องกันเพื่อลดศักยภาพการปฏิบัติการของฝ่ายตรงข้ามต่อ
ระบบการบัญชาการและควบคุมของฝ่ายเรา
2. ป้องกันระบบการบัญชาการและควบคุมของฝ่ายเราไม่ให้เกิดความผิดพลาด
จากการปฏิบัติการแทรกแซงกันเอง¹⁴

ในการปฏิบัติการข่าวสารจำเป็นต้องมีการจัดตั้งหน่วยงานเฉพาะ หรือหน่วยงานกลาง
ที่รับผิดชอบด้านการปฏิบัติการข่าวสารขึ้น ซึ่งมีหน้าที่กำหนดแผนและแนวทางปฏิบัติด้าน
การปฏิบัติการข่าวสาร เพื่อแจกจ่ายแผนและแนวทางปฏิบัติให้แก่หน่วยงานที่เกี่ยวข้อง
นำไปปรับให้สอดคล้องกับภารกิจของแต่ละหน่วย หน่วยงานดังกล่าวจะครอบคลุม
ทุกหน่วยที่มีความเกี่ยวข้องกับการปฏิบัติการข่าวสารทั้งเชิงรุกและเชิงรับ ซึ่งได้แก่
หน่วยงานของแต่ละเหล่าทัพ และหน่วยงานในภาคเอกชนที่มีความเกี่ยวข้องโดยตรง
เพื่อให้สามารถบูรณาการ ประสานความร่วมมือ และร่วมกันหาทางระงับยับยั้งผลกระทบ
ที่อาจเกิดขึ้นในช่วงที่ดำเนินการปฏิบัติการข่าวสารสำหรับการวางแผนนั้น ควรจะ
ประกอบด้วยแผนหลักและแผนฉุกเฉิน (ในภาวะวิกฤติ) ซึ่งครอบคลุมแนวทางการปฏิบัติ

ทุกขั้นตอน ตั้งแต่การจัดหาบุคลากร การฝึกอบรมและทดสอบการปฏิบัติงานของบุคลากร การจัดหาวัสดุอุปกรณ์และการทดสอบระบบเครื่องมืออุปกรณ์ที่จำเป็นต้องใช้ การจัดตั้ง และการแบ่งมอบหน้าที่ต่อผู้ปฏิบัติหรือหน่วยงานต่างๆ ที่มีส่วนร่วมในการปฏิบัติการ ตลอดจนการกำหนดแนวทางการปฏิบัติการต่างๆ ทุกขั้นตอน นับตั้งแต่ช่วงเริ่มต้นของการปฏิบัติการข่าวสารไปจนเสร็จสิ้นภารกิจ รวมทั้งการวิเคราะห์โอกาสและปัจจัยเสี่ยงที่จะส่งผลกระทบต่อการทำงานของปฏิบัติการข่าวสารด้วย

อย่างไรก็ตาม สิ่งสำคัญที่สุดสำหรับประเทศที่ยังไม่มีการวางระบบการปฏิบัติการข่าวสารมาก่อน จำเป็นต้องเริ่มต้นที่การกำหนดหลักนิยม (doctrine) หลักการ (principles) และกรอบความคิด (concept) เพื่อให้ทุกหน่วยของเหล่าทัพ (รวมทั้งหน่วยงานที่จะต้องมีส่วนเกี่ยวข้องกับปฏิบัติการข่าวสาร) ถือปฏิบัติไปในแนวทางเดียวกัน

ดังนั้นหากกล่าวโดยสรุป การปฏิบัติการข่าวสาร จึงเป็นการดำเนินกิจกรรมที่เกี่ยวข้องกับภารกิจต่างๆ ดังนี้

ปฏิบัติการข่าวสารเชิงรุก ประกอบด้วย

1. การทำสงครามอิเล็กทรอนิกส์
2. การโจมตีเครือข่ายคอมพิวเตอร์
3. การโจมตี/ทำลายทางกายภาพ (อาคาร/สถานที่)
4. การทำสงครามจิตวิทยา
5. การลวงทางทหาร
6. การทำสงครามข่าวสาร
7. การรักษาความปลอดภัยการปฏิบัติการ¹⁵

ปฏิบัติการข่าวสารเชิงรับ ประกอบด้วย

1. การรักษาความปลอดภัยทางกายภาพ
2. การรักษาความปลอดภัยการปฏิบัติการ
3. การต่อต้านทางจิตวิทยา

4. การต่อต้านการลวงทางทหาร
5. การสร้างความถูกต้องด้านข่าวสาร
6. การปกป้องคุ้มครองทางอิเล็กทรอนิกส์
7. การต่อต้านข่าวกรอง
8. การป้องกันเครือข่ายคอมพิวเตอร์¹⁶

การปฏิวัติของระบบข้อมูลข่าวสาร (Information Revolution) คือ การกำหนดคุณสมบัติจากความรวดเร็วของการแผ่ขยายข่าวสารนั่นเอง ข้อมูลข่าวสารนั้น เคลื่อนไหวอย่างกว้างขวาง ทุกหนทุกแห่ง เร็วมากทั้งการเข้ามาและจากไป (ทันสมัยและกลายเป็นล้าสมัย ในเวลาอันรวดเร็ว) เนื่องจากข้อมูลข่าวสาร (Information) มีช่วงอายุ (Life Span) สั้น มันจึงมีคุณค่าเอนกอนันต์ เมื่อแรกพบ แต่ก็จจะดูไร้ค่าเมื่อเวลาผ่านไปไม่นาน จึงไม่ควรที่จะเก็บซ่อนข้อมูลไว้ (Hiding Information) ฉะนั้นใครหรือองค์กรใดที่ประสบความสำเร็จ ต้องสามารถใช้ประโยชน์จากข้อมูลข่าวสารได้เร็วกว่าผู้อื่น

การปฏิบัติการข่าวสาร ในอดีตจะมุ่งเน้นที่สภาวะสงคราม แต่ในปัจจุบันจะมุ่งเน้นการปฏิบัติการในสภาวะปกติ และวิกฤติการณ์ เพื่อการเสริมความมั่นคงมากกว่า¹⁷

หลักการ IO มีความเกี่ยวพันกับ หลักการการปฏิบัติการด้านการข่าวทางทหาร เป็นแนวคิดจากการบูรณาการ สงครามบังคับบัญชาและควบคุม (Command and Control Warfare, C2W) และ สงครามสารสนเทศ (Information Warfare) ของกองทัพสหรัฐฯ เป็นการนำเอาบทเรียนจากการรบกับอิรักใน สงครามอ่าว (Gulf Wars) หรือ ที่นิยมเรียกกันว่า CNN Effect มาเป็นกรอบแนวคิดในการพัฒนา กล่าวได้ว่า การปฏิบัติการสารสนเทศ คือ การสนธิการปฏิบัติต่างๆ เพื่อให้มีอิทธิพล ทำลาย ลดประสิทธิภาพในการตัดสินใจและการปฏิบัติการของฝ่ายตรงข้าม รวมทั้งดำเนินการป้องกันการกระทำของฝ่ายตรงข้ามต่อฝ่ายเราในลักษณะเดียวกัน

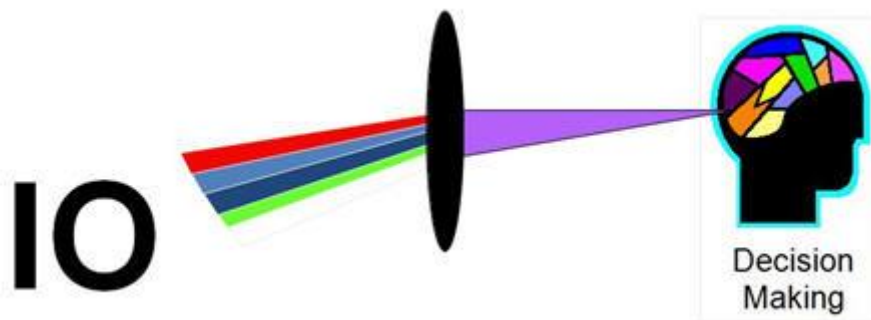
ในการปฏิบัติการทางทหาร การปฏิบัติการข่าวสาร (Information Operations) เป็นหลักการเพื่อใช้ในการบูรณาการสารสนเทศในทุกๆด้าน เพื่อปกป้อง สนับสนุนและเพื่อการเพิ่มอำนาจกำลังรบ โดยมีเป้าหมายเพื่อให้มีอำนาจในการควบคุมสนามรบในเวลาและสถานที่ที่ต้องการ ด้วยอาวุธ รวมทั้งทรัพยากรที่เหมาะสม ด้วยการปฏิบัติการอย่างต่อเนื่องในการรวบรวม นำเข้ากระบวนการแยกแยะและวิเคราะห์ และนำไปสู่ภาคการปฏิบัติ ข้อมูลข่าวสาร เพื่อนำไปสู่การได้เปรียบในการปฏิบัติการทางทหาร

การปฏิบัติการข่าวสาร (Information Operations) หรือเรียกว่า IO นั้น เป็นหลักการที่ออกเป็นเอกสารอย่างเป็นทางการครั้งแรกโดยกระทรวงกลาโหมสหรัฐอเมริกาในปี 2003 อนุมัติหลักการโดย นายโดนัลด์ รัมเฟลด์ (Donald Rumsfeld) รัฐมนตรีกระทรวงกลาโหมสหรัฐฯและเป็นเอกสารที่เปิดเผย (Declassified) ในเดือนมกราคม 2006 ซึ่งเป็นการขยายผลจากหลักการที่เกี่ยวข้องกับสงครามข้อมูลข่าวสาร (Information Warfare) ในมุมมองของกองทัพสหรัฐฯ อย่างไรก็ตามหลักการที่แสดงในเอกสารดังกล่าวเป็นศาสตร์ในด้าน IO แต่ความสำเร็จในการปฏิบัตินั้น ต้องใช้ยุทธศิลป์และประสบการณ์เข้าไปผสมผสานด้วย

อย่างไรก็ตามการนำหลักการการปฏิบัติการข่าวสาร (Information Operations) ของกองทัพสหรัฐอเมริกาซึ่งเป็นผู้คิดค้นต้นแบบมาใช้กับกองทัพในประเทศต่างๆ โดยตรงนั้น อาจจะไม่เหมาะสม ทั้งนี้เนื่องจากโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสาร วัฒนธรรมองค์กร ความพร้อมของบุคลากรและกระบวนการปฏิบัติงาน มีความแตกต่างกันอย่างมาก ซึ่งการนำมาใช้โดยไม่มี การเตรียมการและประยุกต์ใช้ให้เหมาะสมกับกองทัพในประเทศต่างๆก็อาจทำให้ไม่เกิดประสิทธิผล อีกทั้งอาจก่อให้เกิดปัญหายุ่งยากต่อกองทัพของประเทศนั้น ๆ ได้ ดังนั้นจึงควรมีการพัฒนาปรับปรุงให้เหมาะสมกับวัฒนธรรมของกองทัพของประเทศที่นำหลักการ IO ของกองทัพสหรัฐอเมริกาไปใช้ ในการที่จะเพิ่มศักยภาพและพลังอำนาจให้แก่กองทัพที่เหนือกว่าฝ่ายตรงข้าม ด้วยการที่กองทัพสามารถ รู้ก่อน (see first) ตัดสินใจก่อน (decide first) ปฏิบัติก่อน (act first) และปฏิบัติอย่างมีประสิทธิภาพกว่า (act more effectively)

สมมติฐานที่สำคัญที่เกี่ยวข้องกับการปฏิบัติการข่าวสารสารสนเทศ (Information) มีความสำคัญอย่างยิ่งต่อการสงคราม และในปัจจุบันถือว่าเป็นปัจจัยวิกฤตต่อความสำเร็จของการปฏิบัติการทางทหาร และจะยิ่งทวีความสำคัญอย่างไม่สามารถประเมินได้ในอนาคต โดยมีสมมติฐานที่เกี่ยวข้องดังนี้

1. IO ถือว่าเป็นหนึ่งในขีดความสามารถหลัก (Core competency) ของหน่วยงานด้านความมั่นคงและกองทัพ ดังนั้นจึงมีความจำเป็นที่จะต้องกำหนดเส้นทางสู่การปฏิบัติการข่าวสาร (IO Roadmap) เพื่อให้หน่วยงานด้านความมั่นคงและกองทัพสามารถสร้างขีดความสามารถหลักด้าน IO ได้อย่างเป็นรูปธรรม
2. ขีดความสามารถในการสื่อสารที่มีประสิทธิภาพของหน่วยงานภาครัฐมีความสำคัญยิ่งต่อการวางแผนเพื่อทำการยุทธกับฝ่ายตรงข้าม โดยที่ขีดความสามารถดังกล่าวหมายถึงขีดความสามารถที่สามารถจัดการกับข่าวสารเพื่อทำให้เป้าหมาย (ผู้รับข่าวสาร) เกิดความเชื่อตามที่ฝ่ายเราต้องการ จนส่งอิทธิพลโดยตรงต่อการตัดสินใจของเป้าหมาย (ผู้รับข่าวสาร) ให้ตัดสินใจกระทำในสิ่งที่ฝ่ายเราต้องการ รวมทั้งส่งผลต่อกลุ่มผู้นำต่างๆและประชาชนไม่สนับสนุนพลังอำนาจการยุทธ์ทุกด้านให้แก่ฝ่ายตรงข้าม
3. ระบบสารสนเทศและการสื่อสารเพื่อการปฏิบัติการข่าวสาร เป็นโครงสร้างพื้นฐานที่สำคัญในการปฏิรูปการปฏิบัติการข่าวสารของหน่วยงาน ด้านความมั่นคง ซึ่งจะทำให้เกิดการสั่งการบังคับบัญชาในสถานการณ์ต่างๆได้อย่างมีประสิทธิภาพ เกิดความรวดเร็วและเกิดความแม่นยำในการตัดสินใจ
4. ระบบ C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) เป็นโครงสร้างพื้นฐานที่สำคัญในการปฏิรูปกระทรวงกลาโหมและกองทัพ ซึ่งจะทำให้เกิดการสั่งการบังคับบัญชาสามารถเห็นภาพในทุกมิติ (Transparent battle space) เกิดความรวดเร็วและเกิดประสิทธิภาพในการตัดสินใจ
5. ระบบ C4ISR จะมีประสิทธิภาพได้ก็ขึ้นอยู่กับระบบการตัดสินใจและระบบสนับสนุนที่เป็นแบบอัตโนมัติ (Automated decision making and support) รวมไปถึงขีดความสามารถในการปฏิบัติด้านคลื่นแม่เหล็กไฟฟ้า (Electromagnetic capability)¹⁹



รูปที่ 1 แสดงถึงความหมายของ IO คือการกระทำต่อความคิดของผู้มีอำนาจ เพื่อให้ตัดสินใจตามที่ฝ่ายเราต้องการ และเป้าหมายที่แท้จริงมีใช่เอาชนะกำลังทหาร ฝ่ายตรงข้าม แต่เป็นการเอาชนะความเชื่อและการตัดสินใจของผู้นำ¹⁹

ปัญหาพื้นฐานที่พบในการปฏิบัติการข่าวสารในทุกประเทศ องค์กรที่เกี่ยวข้องกับความมั่นคงของรัฐส่วนใหญ่จะมีการเชื่อมโยงกันแบบหลวมๆระหว่างหน่วยงานต่างๆ ในระดับผู้กำหนดนโยบายและผู้ปฏิบัติ ผลก็คือทำให้การจัดงบประมาณเพื่อการดำเนินการด้านการปฏิบัติการข่าวสารไม่สามารถสนับสนุนยุทธศาสตร์และกลยุทธ์ด้านการปฏิบัติการข่าวสารได้อย่างชัดเจน ทำให้ผู้บังคับบัญชาระดับสูงไม่สามารถมองเห็นและบอกได้ว่าองค์กรได้อะไรจากการจัดงบประมาณ ด้านการปฏิบัติการข่าวสารบ้าง และหน่วยงานที่ทำงานด้านการปฏิบัติการข่าวสารก็ไม่สามารถสื่อสารกับผู้บังคับบัญชาระดับสูงได้ว่า การปฏิบัติการข่าวสารมีความสำคัญอย่างไร และมีไว้เพื่ออะไร ซึ่งปัญหาการขาดช่องในการเชื่อมโยง (Disconnects) ดังกล่าว จำเป็นต้องถูกแก้ไขเพื่อทำให้นโยบายและยุทธศาสตร์ด้านการปฏิบัติการ ข่าวสารสามารถนำมาสู่ภาคการปฏิบัติได้อย่างแท้จริง

นอกจากปัญหาการเชื่อมโยงของกระบวนการบริหารดังกล่าว ยังคงมีปัญหาต่างๆ อีกมาก ที่พบซึ่งสามารถสรุปได้ดังนี้

1. นโยบายและแผนระดับยุทธศาสตร์ไม่เกื้อหนุนหรือขัดเคลื่อนการปฏิบัติการข่าวสาร
2. นโยบายและแผนระดับยุทธศาสตร์มุ่งเน้นแต่ด้านเทคโนโลยีมากกว่าจะเข้าถึง กลยุทธ์ทางการปฏิบัติการข่าวสารโดยตรง

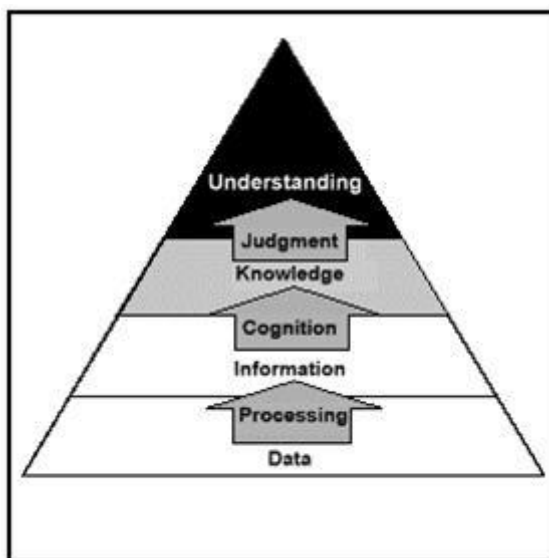
3. ผู้บังคับบัญชาในระดับสูงไม่มีความเชื่อและเห็นว่าการปฏิบัติการข่าวสารจะเป็นสิ่งที่สามารถขับเคลื่อนยุทธศาสตร์ด้านความมั่นคงของรัฐได้จริง
4. งบประมาณของหน่วยงานความมั่นคงไม่สะท้อนถึงผลของการวางแผนด้านการปฏิบัติการข่าวสาร
5. การดำเนินการด้านการปฏิบัติการข่าวสารไม่ได้มุ่งเน้นต่อระบบการตัดสินใจ ของฝ่ายตรงข้ามอย่างแท้จริงจึงไม่เกิดผลกระทบต่อชัยชนะอย่างชัดเจน
6. การขาดปฏิสัมพันธ์ระหว่างหน่วยงานซึ่งมีพื้นฐานมาจากมุมมองที่ต่างกัน (Different views) ระหว่างผู้บังคับบัญชาในระดับสูงและหน่วยปฏิบัติเกี่ยวกับบทบาทหน้าที่ของการปฏิบัติการข่าวสาร คุณค่าประโยชน์ที่การปฏิบัติการข่าวสารจะเป็นกุญแจแห่งความสำเร็จของการรักษาความมั่นคง และกระบวนการบริหารจัดการที่สามารถนำการปฏิบัติการข่าวสารเข้ามามีบทบาทต่อ กลยุทธ์อย่างมีประสิทธิภาพ ซึ่งมุมมองที่ต่างกัันนี้มีผลมาจากความล้มเหลวในการวางแผน การจัดอันดับความสำคัญ และการวัดผลงานของการปฏิบัติการข่าวสารให้มีความสอดคล้องกับยุทธศาสตร์และยุทธวิธี และความล้มเหลวนี้มีผลมาจาก วัฒนธรรมในการบังคับบัญชาและการบริหารจัดการทรัพยากรที่ไม่ประสานสอดคล้องกัน

หัวใจหลักของ Information Operations

IO เป็นการบูรณาการสารสนเทศในทุกๆด้าน เพื่อปกป้อง สนับสนุนและเพื่อการเพิ่มอำนาจกำลังรบ โดยมีเป้าหมายเพื่อมีอำนาจในการควบคุมสนามรบในเวลาและสถานที่ที่ต้องการ และด้วยอาวุธ รวมทั้งทรัพยากรที่เหมาะสม ด้วยการปฏิบัติการอย่างต่อเนื่องในการรวบรวม นำเข้ากระบวนการแยกแยะและวิเคราะห์ และนำไปสู่ภาคการปฏิบัติข้อมูลข่าวสาร เพื่อนำไปสู่การได้เปรียบในการปฏิบัติการทางทหาร

ผู้บังคับบัญชาและฝ่ายเสนาธิการต้องตระหนักไว้เสมอว่า การตัดสินใจบนพื้นฐานของความเชื่อ นั้นมีความเสี่ยงสูงยิ่งเมื่อเปรียบเทียบกับ การตัดสินใจบนพื้นฐานของความรู้ ซึ่งมันก็คือปรัชญาของ IO นั่นเอง

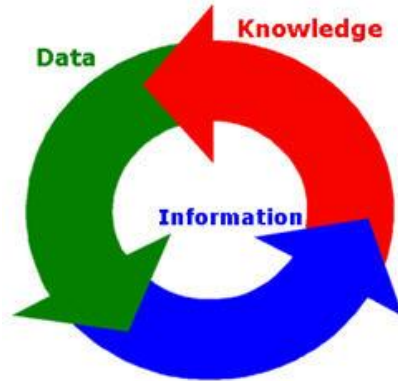
โดยปกติแล้วข้อมูล (Data) ข่าวสาร/สารสนเทศ (Information) และความรู้ (Knowledge) มีความสัมพันธ์กันอย่างมาก ดังนี้คือ ข้อมูล (Data) หมายถึงเนื้อหา และตัวเลข และข้อเท็จจริงที่ได้เก็บรวบรวมไว้โดยไม่ได้คำนึงถึงสาระที่เกิดจากข้อมูล เหล่านั้น แต่หลังจากผ่านกระบวนการ (Processing) แยกแยะ ตีความ ประมวลผล แยกส่วนที่ผิดพลาดออกและวิเคราะห์แล้ว ข้อมูลดังกล่าวก็จะถูกยกระดับเป็นข่าวสารหรือสารสนเทศ (Information) และเมื่อข่าวสารหรือสารสนเทศ (Information) ผ่านการหาความสัมพันธ์เชิงลึกของข่าวสารบวกกับประสบการณ์ ความคิด และความเชี่ยวชาญ/การเรียนรู้ (Cognition) ของแต่ละบุคคลแล้ว ก็จะกลายเป็นความรู้ (Knowledge) ในที่สุด (ดังแสดงในรูป)



รูปที่ 2 แสดงความสัมพันธ์ระหว่างข้อมูล ข่าวสาร/สารสนเทศ และความรู้²⁰

กระบวนการการวิเคราะห์และสังเคราะห์ข้อมูลทำให้เราสามารถแปลงจากข้อมูลดิบ (Data) ที่ยังไม่มีประโยชน์มาก จนกลายมาเป็นข่าวสาร/สารสนเทศ (Information) ซึ่งเริ่มทำให้เห็นถึงความสัมพันธ์ต่างๆในสารสนเทศนั้น และถ้ามีการเก็บข้อมูล วิเคราะห์และสังเคราะห์ข้อมูลเป็นเวลานานนับปี ก็อาจทำให้เราเห็นถึงความสัมพันธ์ที่ลึกซึ้ง จนอาจทำให้เราสามารถคาดการณ์หรือพยากรณ์อนาคตได้แม่นยำมากขึ้น นั่นคือเรากำลังสร้าง

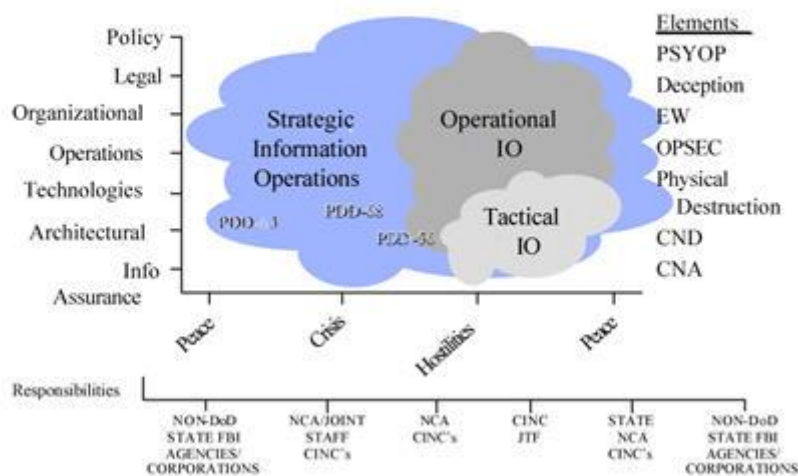
การเรียนรู้ให้กับการปฏิบัติการข่าวสารได้ในระดับเป็นองค์ความรู้ (Knowledge) นั้นเอง ซึ่งกระบวนการนี้จะเป็นวงจร (Cycle) ไม่มีวันจบสิ้นดังแสดงในรูป



รูปที่ 3 วงจรข้อมูล (Data) ข่าวสาร/สารสนเทศ (Information) และความรู้ (Knowledge)²¹

IO นั้นครอบคลุมทั้งในการปฏิบัติการในยามสงบ (Peace) ยามวิกฤต (Crisis) และในยามสงคราม (Hostilities) และยังเกี่ยวข้องกับการปฏิบัติการในทุกระดับ ตั้งแต่ในระดับยุทธศาสตร์ ยุทธการ และยุทธวิธี

Information Operations



รูปที่ 4 ระบบการปฏิบัติการข่าวสาร (Information Operations)²²

อีกทั้ง IO ครอบคลุมไม่เพียงแต่เฉพาะในความรับผิดชอบของกระทรวงกลาโหมเท่านั้น แต่ยังเกี่ยวข้องกับการประสานความร่วมมือกับหน่วยงานความมั่นคงอื่นๆอีกด้วย โดยมีมิติการปฏิบัติการทุกๆด้าน ไม่ว่าจะเป็นในด้านนโยบาย กฎหมาย การดำเนินการขององค์กร เทคโนโลยี ข้อมูลข่าวสาร และตามที่ได้กล่าวไปแล้วในตอนต้นแล้วว่า IO นั้นใช้หลักการของสงครามการควบคุมบังคับบัญชา (Command and Control Warfare) เป็นส่วนที่เป็นหัวใจของ IO ซึ่งประกอบด้วย การปฏิบัติการจิตวิทยา (Psychology Operation, PSYOP) การลวง (Deception) สงครามอิเล็กทรอนิกส์ (Electronic Warfare, EW) การใช้การรักษาความปลอดภัยในการปฏิบัติการ (Operations Security, OPSEC) และการทำลายขีดความสามารถของระบบควบคุมบังคับบัญชาทางกายภาพ (Physical Destruction) ทั้ง 5 องค์ประกอบนี้เองเป็นองค์ประกอบหลักของ IO หรือเรียกว่า การปฏิบัติหลัก หรือขีดความสามารถหลัก (core capabilities) โดยจะกล่าวต่อไปในหัวข้อการปฏิบัติหลัก

การปฏิบัติต่างๆ ที่ใช้ในการปฏิบัติการข่าวสาร (IO) ซึ่งอาจเรียกว่า “ขีดความสามารถ” นั้น ได้ถูกแบ่งออกเป็น 3 กลุ่มคือ การปฏิบัติหลัก หรือขีดความสามารถหลัก (core capabilities) การปฏิบัติสนับสนุน หรือขีดความสามารถสนับสนุน (supporting capabilities) และการปฏิบัติที่เกี่ยวข้อง หรือขีดความสามารถที่เกี่ยวข้อง (related capabilities)

การปฏิบัติหลัก ประกอบด้วยการปฏิบัติ ๕ ประการคือ

1. การปฏิบัติการจิตวิทยา (Psychological Operation, PSYOP)
2. การลวงทางทหาร (Military Deception, MILDEC)
3. การรักษาความปลอดภัยในการปฏิบัติการ (Operation Security, OPSEC)
4. สงครามอิเล็กทรอนิกส์ (Electronic Warfare, EW)
5. การปฏิบัติการเครือข่ายคอมพิวเตอร์ (Computer Network Operations, CNO)

การประสานการใช้องค์ประกอบทั้ง 5 ของสงครามการควบคุมบังคับบัญชา (OPSEC, PSYOP, MILITARY DECEPTION, EW, PHYSICAL DESTRUCTION) ทำให้เกิดศักยภาพ

ในการทำลายฝ่ายตรงข้าม ซึ่งถือว่าเป็นผลการทวีกำลัง (Synergistic Effects) โดยเมื่อผู้บังคับบัญชาใช้การปฏิบัติหลักทั้ง 5 ประการนี้ร่วมกับการปฏิบัติสนับสนุน และการปฏิบัติที่เกี่ยวข้องแล้ว จะเป็นเครื่องมือหลักในการสร้างอิทธิพลต่อบุคคลหรือกลุ่มบุคคลเป้าหมาย (Target Audiences: TAs) ในฝ่ายตรงข้าม อันจะทำให้กำลังรบมีเสรีในการปฏิบัติในสภาวะแวดล้อมของข่าวสาร

การปฏิบัติที่สนับสนุนการปฏิบัติการข่าวสาร ประกอบด้วย การประกันข่าวสาร (Information Assurance: IA) การรักษาความปลอดภัยทางวัตถุ (Physical Security) การโจมตีทางวัตถุ (Physical Attack) การต่อต้านข่าวกรอง (Counterintelligence, CI) และภาพถ่ายการรบ (Combat Camera, COMCAM) การปฏิบัติเหล่านี้จะรวมอยู่ในสภาวะแวดล้อมของข่าวสารไม่ว่าจะเป็นทางตรง หรือทางอ้อม เป็นการปฏิบัติที่ช่วยให้การปฏิบัติการข่าวสารมีประสิทธิภาพ การปฏิบัติเหล่านี้ควรปฏิบัติโดยการสนธิและประสานกับการปฏิบัติหลัก และนอกจากจะใช้การปฏิบัติเหล่านี้สนับสนุนการปฏิบัติการข่าวสารแล้ว ยังสามารถใช้สำหรับจุดประสงค์อื่นๆ ที่กว้างกว่านี้ได้อีกด้วย

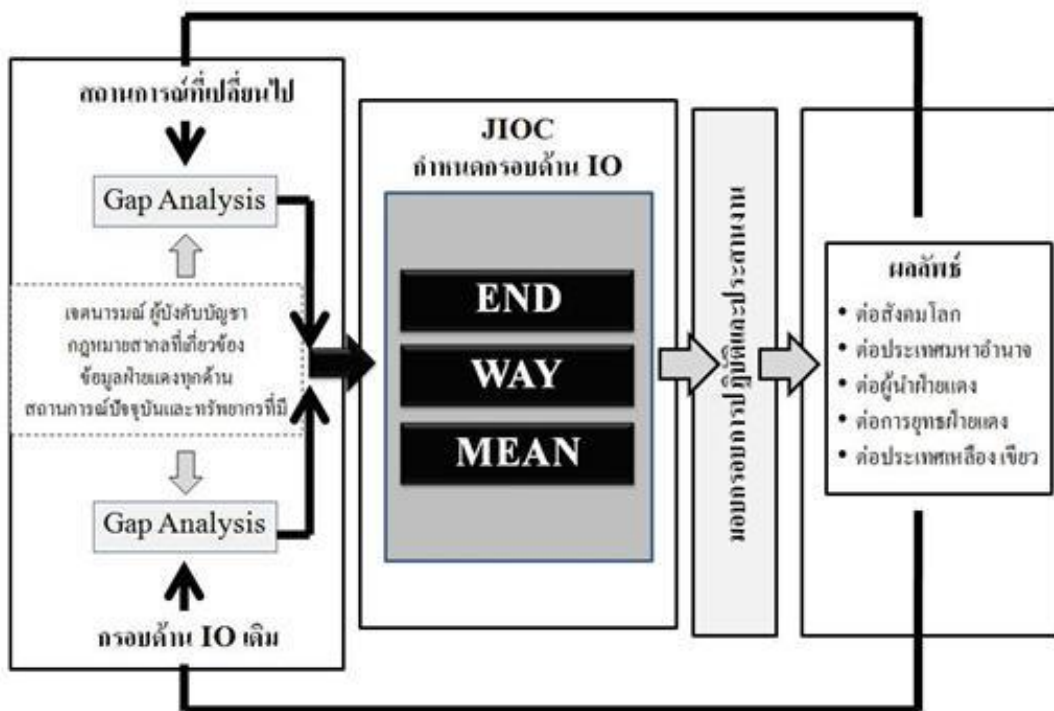
การปฏิบัติที่เกี่ยวข้องสำหรับการปฏิบัติการข่าวสาร กำหนดขึ้นด้วยหน้าที่ทางทหาร 3 ประการ คือ การประชาสัมพันธ์ (Public Affairs, PA) การปฏิบัติการระหว่างพลเรือนกับทหาร (Civil-Military Operations, CMO) และกลาโหมสนับสนุนต่อการทูตสาธารณะ (Defense Support to Public Diplomacy, DSPD) การปฏิบัติเหล่านี้มีส่วนสำคัญในการปฏิบัติการข่าวสาร และต้องปฏิบัติโดยประสานและสนธิกับการปฏิบัติหลัก และการปฏิบัติสนับสนุน ในการปฏิบัติการข่าวสารเสมอ อย่างไรก็ตาม จุดประสงค์หลัก และกฎต่างๆ ที่เป็นกรอบของการปฏิบัติเหล่านี้ จะต้องไม่ถูกผูกมัด หรือได้รับผลเสียหายจากการปฏิบัติการข่าวสาร ซึ่งเป็นสิ่งที่ต้องพึงเล็งและเป็นข้อพิจารณาเพิ่มเติมในการวางแผนและการปฏิบัติ ในการปฏิบัติการข่าวสาร ด้วยเหตุนี้ เจ้าหน้าที่ในการประชาสัมพันธ์ (PA) และการปฏิบัติการระหว่างพลเรือนกับทหาร (CMO) จึงต้องทำงานโดยการประสานงานอย่างใกล้ชิดเป็นการเฉพาะกับฝ่ายเสนาธิการที่วางแผนในการปฏิบัติการข่าวสารกระบวนการ การปฏิบัติการข่าวสาร

แนวความคิดในการปฏิบัติ

1. สนับสนุนการปฏิบัติทุกหนทางปฏิบัติ เพื่อให้ฝ่ายเรามีความเหนือกว่าทางข้อมูลข่าวสาร เพิ่มโอกาสในการบรรลุภารกิจ สามารถเข้าถึงข้อมูลข่าวสารที่จำเป็นเพื่อการตัดสินใจได้ ในเวลาที่ต้องการ และสามารถนำการตัดสินใจไปสู่การปฏิบัติได้อย่างทันเวลา
2. สร้างผลกระทบต่อการเรียนรู้ข้อมูลข่าวสารของกลุ่มเป้าหมาย และผู้ที่มีอำนาจการตัดสินใจที่จะกระทำหรือไม่กระทำ ต้องดำเนินการไปในทิศทางที่ฝ่ายเราต้องการ

กระบวนการในการปฏิบัติ

1. การปฏิบัติข่าวสารเป็นการปฏิบัติที่เป็นวงรอบโดยไม่มีที่สิ้นสุดดัง แสดงในรูป



รูปที่ 5 กระบวนการการปฏิบัติข่าวสาร²³

จากรูปเห็นได้ว่าการปฏิบัติข่าวสารเริ่มต้นจากการพิจารณาข้อมูลหลายมิติ เช่น การสื่อสารเชิงยุทธศาสตร์ชาติ สื่อสารเชิงยุทธศาสตร์ทางทหาร เจตนาธรรมผู้บังคับบัญชา กฎหมายสากลที่เกี่ยวข้อง การข่าวและข่าวสารที่เกี่ยวกับข้าศึก และทรัพยากรของฝ่ายเรา โดยมีกระบวนการเป็นขั้นตอน ดังต่อไปนี้

1. กำหนดกรอบแนวคิดเชิงยุทธศาสตร์และยุทธการด้านการปฏิบัติข่าวสารทางทหาร โดยต้องมีการกำหนดผลลัพธ์สุดท้าย (End) วิธีการดำเนินการและปฏิบัติการ (Way) และทรัพยากรที่ต้องใช้ (Mean) เพื่อเป็นแนวทางให้แก่หน่วยในระดับยุทธวิธีในการดำเนินกลยุทธ์

2. มอบแนวทางในการปฏิบัติต่อหน่วยที่เกี่ยวข้อง และทำการประสานการปฏิบัติอย่างต่อเนื่อง
3. ตรวจสอบและประเมินผลการปฏิบัติอย่างต่อเนื่อง โดยตรวจสอบผลลัพธ์ที่ได้ตรงตามเป้าหมายที่วางไว้หรือไม่
4. นำผลการประเมินมาวิเคราะห์เพื่อปรับแผนให้เป็นไปตามสถานการณ์ปัจจุบัน โดยกระบวนการตั้งแต่ ขั้นตอนที่ 1 ถึงขั้นตอนที่ 4 จะเป็นการปฏิบัติเป็นวงรอบไม่มีที่สิ้นสุด

ปัจจัยที่สำคัญต่อความสำเร็จในการปฏิบัติการข่าวสาร คือ การที่ผู้บังคับบัญชา ต้องมีความเชื่อและศรัทธาอย่างแท้จริงก่อนว่า การปฏิบัติการข่าวสารต้องเป็นขีดความสามารถหลัก (Core competency) ของกองทัพและผู้บังคับบัญชาจะต้องทำให้ผู้ใต้บังคับบัญชา มีความเข้าใจการปฏิบัติการข่าวสารไปในทิศทางเดียวกัน และจะต้องมีความเชื่อร่วมกันว่า การปฏิบัติการข่าวสาร เป็นขีดความสามารถหลักหนึ่งของหน่วยงานด้านความมั่นคงและกองทัพ (Core Competency)²⁴

การปฏิบัติการข่าวสารมีการพัฒนาและเปลี่ยนรูปแบบจากเดิม เช่น การโฆษณา, ประชาสัมพันธ์, ชวนเชื่อ, ปลุกปั่น, ยุยง, ปลุกกระดม และปลุกฝังแนวความคิด บนสื่อภาพยนตร์, แผ่นป้ายโฆษณา, แผ่นพับ, หนังสือ, ตำรา, หนังสือพิมพ์, รายการวิทยุ, รายการโทรทัศน์ ฯลฯ ปัจจุบันในยุคสารสนเทศ (Information Age) การปฏิบัติการข่าวสารได้พัฒนารูปแบบมาผ่านทางระบบสื่อสารโทรคมนาคม โดยเฉพาะอย่างยิ่งบนสื่อออนไลน์ทางอินเทอร์เน็ต ซึ่งทำให้การกระจายตัวของข่าวสารมีความรวดเร็วแบบ Real time

การปฏิบัติการข่าวสารผ่านสื่อออนไลน์ เช่น

1. เว็บไซต์หมิ่นสถาบันพระมหากษัตริย์
2. กลุ่มต่อต้านคณะรักษาความสงบแห่งชาติ และรัฐบาล
3. สงครามข่าวสารแย่งชิงมวลชนภาคใต้
4. ต่อด้านนโยบายรัฐบาลกรณี Single Gateway

ซึ่งนับเป็นเครื่องมือสำคัญทางการเมือง เศรษฐกิจ สังคมจิตวิทยา และการทหาร ที่สามารถสร้างกระแส ความได้เปรียบต่อฝ่ายตรงข้าม และนำไปสู่ความสำเร็จ โดยแทบไม่ต้องใช้กำลังรบและยุทธโภภณในการต่อสู้ ซึ่งมีผลกระทบต่อความมั่นคงปลอดภัยของกองทัพไทย ใน 2 ลักษณะ คือ

1. ความมั่นคงภายในประเทศ ได้แก่ บ่อนทำลายสถาบันหลัก, สงครามการเมือง และการก่อความไม่สงบ
2. ความมั่นคงระหว่างประเทศ ได้แก่ การแทรกแซงรัฐหรือประเทศอื่น และการก่อการร้าย

แนวทางที่จะปฏิบัติกับภัยคุกคามที่เกิดขึ้นจากการปฏิบัติการข่าวสาร ต้องมีการเฝ้าระวัง สืบค้น ติดตามและตรวจสอบ แหล่งที่มาของข้อมูลข่าวสาร ที่เป็นภัยต่อความมั่นคงของกองทัพไทย อย่างต่อเนื่องและตลอดเวลา ทั้งภายในและภายนอกประเทศอย่างใกล้ชิด รวมถึงการปฏิบัติการเชิงรุกบางโอกาสภายใต้กรอบกฎหมายที่มีอยู่ ในฐานะหน่วยงานด้านความมั่นคงของประเทศ เตรียมความพร้อมโดยการพัฒนาบุคลากร พัฒนาองค์ความรู้ให้ทันต่อเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว และรู้เท่าทันภัยคุกคามรูปแบบใหม่ สร้างความตระหนักรู้ในเรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศ รวมถึงพัฒนาความสัมพันธ์และความร่วมมือผืนนี้กำลังระหว่างหน่วยงานด้านความมั่นคงในการปฏิบัติงานร่วมกันเป็นประชาคมไซเบอร์ (Cyber Community)

อำนาจด้านสารสนเทศและสื่อได้เปลี่ยนผ่านจากภาครัฐไปสู่ภาคเอกชนและมีแนวโน้มเปลี่ยนผ่านไปสู่ภาคประชาชนซึ่งมีอิทธิพลต่อความคิดเห็น ความเชื่อและการตอบสนองของประชาชนในระดับชาติและระดับนานาชาติ การปฏิบัติการข่าวสารในยุคสารสนเทศ หน่วยงานด้านความมั่นคงและกองทัพ จึงมีความจำเป็นที่จะต้องปรับตัวและเสริมสร้างศักยภาพขีดความสามารถในมิติไซเบอร์ (Cyberspace) ซึ่งเป็นส่วนสนับสนุนการรบที่สำคัญ โดยต้องมีความมุ่งมั่นในการวางยุทธศาสตร์ของการปฏิบัติการข่าวสาร และยุทธวิธีในการใช้และตอบโต้สงครามสารสนเทศและสื่อ เพื่อให้การปฏิบัติการข่าวสารประสบความสำเร็จอย่างเป็นรูปธรรมและมีประสิทธิผล

เอกสารอ้างอิง

¹ ปรัชญา เถลิมวัฒน์, พันเอก. หลักนียมการรบในมิติไซเบอร์., กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม. [อินเทอร์เน็ต]. [เข้าถึงเมื่อ 31 มกราคม 2560]. เข้าถึงได้จาก: <https://drive.google.com/file/d/0Bww6glmbUKPhRE0tcULRdkNXUEU/view>

² มนวัติ ตั้งตรงหลุทัย. เอกสารศึกษาเฉพาะกรณี การสื่อสารทางยุทธศาสตร์ (Strategic Communication : SC) และการปฏิบัติการข่าวสาร (Information Operations : IO) ของกองทัพไทย. กรุงเทพฯ: ศูนย์ศึกษายุทธศาสตร์ สถาบันวิชาการป้องกันประเทศ; 2559. หน้า 1-2.

³ เรื่องเดียวกัน; หน้า 7.

⁴ เรื่องเดียวกัน; หน้า 8.

⁵ เรื่องเดียวกัน; หน้า 8.

⁶ เรื่องเดียวกัน; หน้า 8.

⁷ เรื่องเดียวกัน; หน้า 8.

⁸ เรื่องเดียวกัน; หน้า 9.

⁹ สุรชาติ บำรุงสุข. ปฏิบัติการข่าวสาร (Information Operations). จุลสารความมั่นคงศึกษา ฉบับที่ 78. กรุงเทพฯ: สถาบันข่าวกรอง สำนักข่าวกรองแห่งชาติ; 2553. หน้า 6.

¹⁰ เรื่องเดียวกัน; หน้า 6.

¹¹ เรื่องเดียวกัน; หน้า 6.

¹² เรื่องเดียวกัน; หน้า 8.

¹³ เรื่องเดียวกัน; หน้า 9.

¹⁴ เรื่องเดียวกัน; หน้า 9.

¹⁵ เรื่องเดียวกัน; หน้า 10.

¹⁶ เรื่องเดียวกัน; หน้า 11.

¹⁷ โรงเรียนเสนาธิการทหารบก. คู่มือการปฏิบัติการข่าวสาร. กรุงเทพฯ: ศูนย์พัฒนาหลักนียมและยุทธศาสตร์. กรมยุทธศึกษาทหารบก. 2557. หน้า 8.

¹⁸ เศรษฐพงศ์ มะลิสุวรรณ. การปฏิบัติการข่าวสาร (Information Operations). [อินเทอร์เน็ต]. 2554. [เข้าถึงเมื่อ 31 มกราคม 2560]. เข้าถึงได้จาก:
<http://www.vcharkarn.com/varticle/42857>

²⁰ เรื่องเดียวกัน;

²¹ เรื่องเดียวกัน;

²² เรื่องเดียวกัน;

²³ เรื่องเดียวกัน;

²⁴ วุฒิชัย สายเสถียร. งาน IO (Information Operations) กับกองทัพเรือ. [อินเทอร์เน็ต]. 2556. [เข้าถึงเมื่อ 31 มกราคม 2560]. เข้าถึงได้จาก:
<http://www.rtni.org/th/library/wp-content/uploads/2014/04/นาวิกศาสตร์-พค-2556-งาน-IO-Information-Operations-กับกองทัพเรือ.pdf>

ประวัติย่อผู้วิจัย

ยศ ชื่อ

พันเอก วัชรินทร์ แก่นทอง

วัน เดือน ปี เกิด

14 มกราคม 2514

ประวัติสำเร็จการศึกษา

- พ.ศ.2536 วิทยาศาสตรบัณฑิต (วิทยาการคอมพิวเตอร์)
สถาบันราชภัฏบ้านสมเด็จเจ้าพระยา
- พ.ศ.2545 หลักสูตรชั้นนายร้อย เหล่าสารบรรณ โรงเรียนทหารสารบรรณ
กรมสารบรรณทหารบก
- พ.ศ.2549 หลักสูตรชั้นนายพัน เหล่าสารบรรณ โรงเรียนทหารสารบรรณ
กรมสารบรรณทหารบก
- พ.ศ.2550 วิทยาศาสตรมหาบัณฑิต (เทคโนโลยีอินเทอร์เน็ตและสารสนเทศ)
มหาวิทยาลัยนเรศวร
- พ.ศ.2553 หลักสูตรนายทหารบกอาวุโส โรงเรียนเสนาธิการทหารบก

ประวัติการทำงาน

- พ.ศ.2537 – 2543 นายทหารควบคุมข้อมูล กองกลาง กรมยุทธการทหาร
กองบัญชาการทหารสูงสุด
- พ.ศ.2543 – 2545 นายทหารโปรแกรม กองสารสนเทศทางทหาร
กรมการสนเทศทหาร กองบัญชาการทหารสูงสุด
- พ.ศ.2545 – 2546 ประจำแผนกโครงการ กองนโยบายและแผน
กรมการสนเทศทหาร กองบัญชาการทหารสูงสุด
- พ.ศ.2546 – 2547 นายทหารบริหารเครือข่ายคอมพิวเตอร์
กองกำลังเฉพาะกิจปฏิบัติการเพื่อนมนุษย์ธรรม 976 ไทย/อิรัก

