การปฏิบัติการข่าวสาร (Information Operation) ในยุคแห่งสงครามสารสนเทศ (Information Warfare)

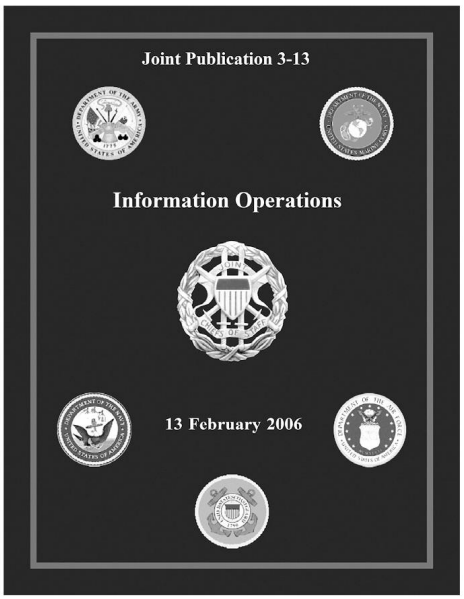
บทความพิเศษ

กองบรรณสารและเทคโนโลยีสารสนเทศ
กองบัญชาการสถาบันวิชาการป้องกันประเทศ

บทคัดย่อ

คำว่า “อินฟอร์เมชั่น โอเปอร์เรชั่น” หมายถึง **“การปฏิบัติการข่าวสาร”** ตรงกับภาษาอังกฤษว่า “Information Operations” (เรียกย่อว่า Info Ops หรือ IO) เป็นการนำเอาพันธกิจการปฏิบัติการทางทหารหลายประการมาบูรณาการเพื่อสร้างอิทธิพลหรือผลกระทบต่อการคิดและตัดสินใจของฝ่ายตรงข้าม และอาจมีชื่อเรียกเฉพาะแตกต่างกันไปทั้ง “การปฏิบัติสารสนเทศ” หรือ “การปฏิบัติการข่าวสาร” แต่ความหมายโดยนัย ก็คือ “Information Operations” เช่นเดียวกัน

“IO” เป็นส่วนหนึ่งของ “Information Warfare” หรือ “สงครามสารสนเทศ” ซึ่งบางท่านเรียกว่า “สงครามข่าวสาร”, “Cyber War” หรือ “Net War” ก็ได้ โดยคำว่า “Information Operation” หรือ “การปฏิบัติการข่าวสาร” นั้นเป็นหลักการที่ออกเป็นเอกสารอย่างเป็นทางการครั้งแรกโดยกระทรวงกลาโหมสหรัฐอเมริกาในปี ๒๐๐๓ อนุมัติหลักการโดย โดนัลด์ รัมส์เฟลด์ (Donald Rumsfeld) รัฐมนตรีกระทรวงกลาโหมสหรัฐฯ และเป็นเอกสารที่เปิดเผย (Declassified) ในปี ๒๐๐๖ ซึ่งเป็นการขยายผลจากหลักการที่เกี่ยวข้องกับสงครามสารสนเทศ (Information Warfare) ในมุมมองของกองทัพสหรัฐฯ



โดยหลักการแล้ว “IO” มีความเกี่ยวพันกับหลักการการปฏิบัติการด้านการข่าวทางทหาร ซึ่งเป็นแนวคิดจากการบูรณาการสงครามการควบคุมบังคับบัญชา (Command and Control Warfare) และสงครามสารสนเทศ (Information Warfare) ของกองทัพสหรัฐฯ โดยการนำเอาบทเรียนจากการรบกับอิรักในสงครามอ่าว (Gulf Wars) หรือที่นิยมเรียกกันว่า “CNN Effect” มาเป็นกรอบแนวคิดในการพัฒนา อาจกล่าวได้ว่า “การปฏิบัติการข่าวสาร” คือ การสนธิการปฏิบัติต่างๆ เพื่อทำให้มีอิทธิพล ทำลาย ลดประสิทธิภาพ ในการตัดสินใจและการปฏิบัติการของฝ่ายตรงข้าม รวมทั้งดำเนินการป้องกันการกระทำของฝ่ายตรงข้ามต่อฝ่ายเราในลักษณะเดียวกัน

การปฏิบัติต่างๆ ที่ใช้ในการปฏิบัติการข่าวสาร (IOs) ซึ่งอาจเรียกว่า “ขีดความสามารถ” นั้น ได้ถูกแบ่งออกเป็น ๓ กลุ่มคือ

๑. การปฏิบัติหลัก หรือขีดความสามารถหลัก (core capabilities)

๒. การปฏิบัติสนับสนุน หรือขีดความสามารถสนับสนุน (supporting capabilities)

๓. การปฏิบัติที่เกี่ยวข้อง หรือขีดความสามารถที่เกี่ยวข้อง (related capabilities)

การปฏิบัติการหลัก : หัวใจหลักของ IO

ส่วนที่เป็นหัวใจหลักของ “IO” ที่เป็นการปฏิบัติการหลัก หรือขีดความสามารถหลัก (Core Capabilities) ประกอบด้วยการปฏิบัติ ๕ ประการ ได้แก่

๑. การปฏิบัติการจิตวิทยา (Psychological Operations หรือ “PSYOP”)

๒. การลวงทางทหาร (Military Deception หรือ “MILDEC”)

๓. การรักษาความปลอดภัยในการปฏิบัติการ (Operations Security หรือ “OPSEC”)

๔. การสงครามอิเล็กทรอนิกส์ (Electronic Warfare: EW) และ

๕. การปฏิบัติการเครือข่ายคอมพิวเตอร์ (Computer Network Operations: CNO)

โดยเมื่อเราได้ใช้การปฏิบัติหลักทั้ง ๕ ประการนี้ร่วมกับการปฏิบัติสนับสนุน (Supporting Capabilities) และการปฏิบัติที่เกี่ยวข้อง (Related Capabilities) แล้วจะกลายเป็นเครื่องมือหลักในการสร้างอิทธิพลต่อบุคคลหรือกลุ่มบุคคลเป้าหมาย (Target Audiences) โดยจะสร้างอิทธิพลในแง่ความคิด ความเชื่อ และการตัดสินใจของฝ่ายตรงข้ามให้เป็นไปตามที่ฝ่ายเราต้องการ

DOD Information Operations Core Capabilities
- Psychological Operations (PSYOP)
- Military Deception (MILDEC)
- Operational Security (OPSEC)
- Computer Network Operations (CNO)
  - Computer Network Defense (CND)
  - Computer Network Exploitation (CNE)
  - Computer Network Attack (CAN)
- Electronic Warfare (EW)
  - Domination of the Electromagnetic Spectrum
  - Electromagnetic Non-Kinetic Weapons

รูปที่ ๑ Information Operations Core Capabilities

ในส่วนของการปฏิบัติการทางด้านเครือข่ายคอมพิวเตอร์ (Computer Network Operations หรือ “CNO”) จะประกอบด้วย ๓ ส่วนหลักๆ (ดูรูปที่ ๒) ได้แก่

๑. การโจมตีเครือข่ายคอมพิวเตอร์เพื่อทำลายระบบเครือข่ายของฝ่ายตรงข้ามให้ล่มหรือใช้งานไม่ได้ (Computer Network Attack หรือ “CNA”)

๒. การป้องกันการโจมตีเครือข่ายคอมพิวเตอร์ของเราจากฝ่ายตรงข้าม (Computer Network Defence หรือ “CND”)

๓. การเจาะแอบเอาข้อมูลจากเครือข่ายคอมพิวเตอร์ของฝ่ายตรงข้าม (Computer Network Exploitation หรือ “CNE”)

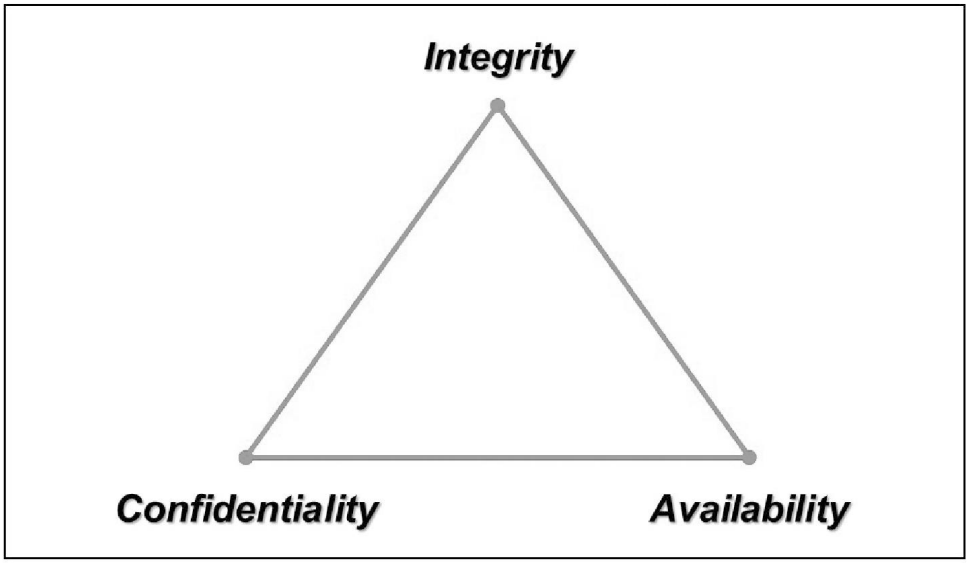
“การปฏิบัติการข่าวสาร” (Information Operation) เพียงลำพังไม่สามารถเอาชนะฝ่ายตรงข้ามได้ แต่ต้องสนธิอย่างประสานสอดคล้องและกลมกลืนเข้ากับการปฏิบัติการด้านอื่นๆ เช่น การทำลายทางกายภาพ (Physical Destruction) การต่อต้านการโฆษณาชวนเชื่อ (Counter-Propaganda) การรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Assurance) การต่อต้านข่าวกรอง (Counter-Intelligence) การต่อต้านการลวง (Counter Deception) ฯลฯ

การปฏิบัติสนับสนุน หรือขีดความสามารถในการสนับสนุน (IO Supporting Capabilities)

หัวใจหลักของการปฏิบัติการสนับสนุน ได้แก่ Information Assurance (IA), Physical Security, Physical Attack, CI และ COMCAM ซึ่งมีรายละเอียดดังนี้

Information Assurance (IA)

มีวัตถุประสงค์ในการป้องกัน (Protect) และปกป้องคุ้มครอง (Defence) สารสนเทศ (Information) และระบบสารสนเทศ (Information System) ของฝ่ายเราให้ปลอดภัย เพื่อให้แน่ใจได้ว่าเราสามารถรักษาคุณสมบัติทั้ง ๓ ประการ ด้านความมั่นคงปลอดภัยสารสนเทศ ได้แก่ การรักษาความลับ (Confidentially) การรักษาความถูกต้องสมบูรณ์ (Integrity) การรักษาความพร้อมใช้ของสารสนเทศเมื่อต้องการเข้าถึง (Availability) ซึ่งครอบคลุมถึงการพิสูจน์ตัวตน (Authentication) และการห้ามปฏิเสธความรับผิดชอบในการทำธุรกรรม (Non-Repudiation) อีกด้วย



รูปที่ ๒ องค์ประกอบของความปลอดภัยสารสนเทศ

โดย IA ใช้หลักการ Defense-In-Depth หรือ Multi-Layer Defence ในการป้องกันทั้งด้านบุคลากร (People) ด้านกระบวนการการปฏิบัติการ (Process) และด้านเทคโนโลยี (Technology) ในการเข้าถึงสารสนเทศจำเป็นต้องมีระบบควบคุมป้องกันการเข้าถึงที่ดี (Access Control)

การปฏิบัติการข่าวสาร (IO) จำเป็นต้องมี IA เป็นตัวช่วยเสริมซึ่งกันอย่างหลีกเลี่ยงไม่ได้ จึงจำเป็นต้องพิจารณาให้ครบทั้งสองด้านทั้ง IA และ IO

Physical Security

การรักษาความปลอดภัยทางกายภาพเป็นเรื่องสำคัญที่จำเป็นในการป้องกันการโจมตีบุคลากรและทรัพย์สิน รวมถึงการป้องกันการเข้าถึงอุปกรณ์และเอกสารต่าง ๆ ของฝ่ายเราเพื่อให้รอดพ้นจากการจารกรรม, การขโมย และการทำลายล้าง การป้องกันด้านกายภาพจะเน้นไปที่การป้องกันที่ศูนย์คอมพิวเตอร์ (Physical Facilities) การป้องกันอาคารสถานที่ต่าง ๆ โดยจะไม่อนุญาตให้ผู้ที่ไม่มีส่วนเกี่ยวข้องเข้ามาในบริเวณที่ทางฝ่ายเราได้จำกัดการเข้าถึงในทางกายภาพ

Physical Attack (Physical Destruction)

เน้นไปที่การทำลายล้างเป้าหมายเชิงกายภาพของฝ่ายตรงข้ามเพื่อไม่ให้สามารถบัญชาการรบได้อย่างมีประสิทธิภาพ การทำลายและโจมตีเป้าหมายทางกายภาพนั้นสามารถปฏิบัติการร่วมกันกับ “PSYOP” หรือ “การปฏิบัติการจิตวิทยา” ได้เพื่อให้บรรลุเป้าหมายในการโจมตีให้มีประสิทธิภาพมากขึ้น

Counter Intelligence (CI)

“การต่อต้านข่าวกรอง” เป็นการรวบรวมข้อมูลข่าวสารเพื่อป้องกันการจารกรรมข้อมูลและสารสนเทศของฝ่ายเราจากแฮกเกอร์ของฝ่ายตรงข้าม ในปัจจุบันรัฐบาลหลายประเทศ ได้ว่าจ้างแฮกเกอร์ในประเทศของตนอย่างเป็นเรื่องเป็นราว เป็นหน่วยรบใต้ดินที่มีวัตถุประสงค์ในการเจาะระบบของรัฐบาลในประเทศฝ่ายตรงข้าม โดย CI สามารถปฏิบัติการร่วมกับ “OPSEC” ได้อย่างกลมกลืนและจำเป็นต้องใช้ CNO “Computer Network Operation” ในการป้องกันระบบสารสนเทศของฝ่ายเราและโจมตีฝ่ายตรงข้ามในขณะเดียวกัน

Combat Camera (COMCAM)

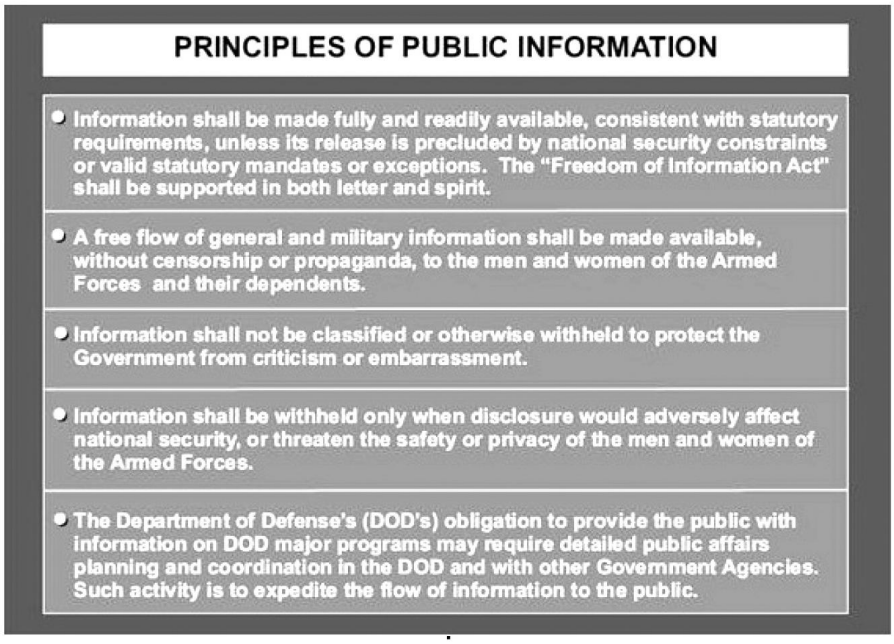
กล้องถ่ายภาพการรบเป็นส่วนสนับสนุนที่มีความสำคัญในการปฏิบัติการสารสนเทศเช่นกันกล่าวคือ ภาพถ่ายจากกล้องสามารถนำไปสนับสนุนการทำ “PSYOP” และ “MILDEC” ได้ด้วย เพราะถ้าหากถูกฝ่ายตรงข้ามเจาะข้อมูลภาพถ่ายก็จะตกเป็นฝ่ายเสียเปรียบทันที

การปฏิบัติที่เกี่ยวข้อง หรือขีดความสามารถที่เกี่ยวข้อง (IO Related Capabilities)

การปฏิบัติที่เกี่ยวข้อง ประกอบไปด้วย ๓ เรื่อง ได้แก่

Public Affairs (PA)

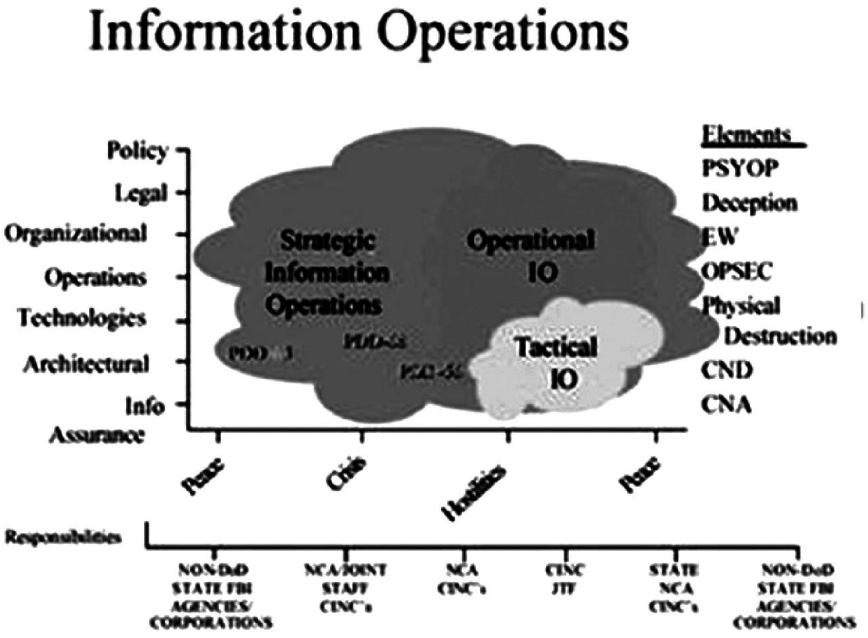
เป็นการประชาสัมพันธ์ทั้งในประเทศและต่างประเทศ เพื่อให้เกิดความรู้สึกที่ดีต่อภาพลักษณ์ของฝ่ายเรา ตามหลักการ “Principle of Public Information”



รูปที่ ๓ Principles of Public Information

Civil Military Operations (CMO)

เป็นการทำงานร่วมกันระหว่างทหารและพลเรือน สามารถทำได้ในช่วงเวลาสงบที่ไม่มีสงคราม (Peace) ทั้งก่อน และหลังสงคราม (ดูรูปที่ ๒) เป็นการสนับสนุน ทั้ง PSYOP, CNO และ CI เพื่อสร้างความเชื่อมั่น ปรองดอง สมานฉันท์ พึ่งพาอาศัยกัน เพื่อให้มีเอกภาพในการอยู่ร่วมกัน และสร้างแนวคิดให้สนับสนุน การปฏิบัติการสารสนเทศในระยะยาว



รูปที่ ๔ Big Picture of IO

DSPD (Defence Support to Public Diplomacy)

เป็นการสนับสนุนในการทำ “PSYOP” ต่อรัฐบาลในประเทศต่าง ๆ ทางด้านการทูต โดยทางกระทรวงกลาโหมต้องปฏิบัติการร่วมกับกระทรวงการต่างประเทศ เพื่อเสริมสร้างภาพลักษณ์ที่ดีและการได้รับการสนับสนุนจากนานาประเทศ

กรณีศึกษา นปช. และ ศอฉ.ในประเด็นการปฏิบัติการสารสนเทศ

จากตัวอย่างสงครามระหว่างอิรัก และสหรัฐอเมริกา จากผลของ “CNN effect” จะเห็นได้ว่า การใช้สื่อมีความสำคัญเปรียบเทียบเท่าการใช้อาวุธในการโจมตีฝ่ายตรงข้าม อาจกล่าวได้ว่า “การปฏิบัติการข่าวสารเป็นอาวุธร้ายที่เราไม่ควรมองข้าม” และข่าวสารเปรียบเสมือนกระสุนที่พุ่งออกจากปืนของสื่อเข้าไปเจาะทะลวงจิตใจ และความคิดของผู้รับข่าวสารนั้น ๆ มีผลกระทบต่อกระบวนการในการตัดสินใจของผู้รับข่าวสาร เพื่อให้เป็นไปตามความต้องการที่แอบแฝงของแต่ละฝ่าย

สำหรับในประเทศไทย ผู้เขียนขอยกกรณีตัวอย่างจากเหตุการณ์ความไม่สงบทางการเมืองในประเทศไทย เมื่อปี พ.ศ. ๒๕๕๓ ระหว่าง นปช. และ ศอฉ. เพื่อประกอบการศึกษา และทำความเข้าใจเกี่ยวกับ “IO” โดยในช่วงเวลาดังกล่าว พบว่า ทั้ง นปช. และ ศอฉ. ล้วนใช้ “IO” ในการโจมตีฝ่ายตรงข้าม เพื่อให้มวลชนคล้อยตามฝั่งของตนตามหลักการ “IO” ทางรัฐบาลเน้นว่ามีผู้ก่อการร้ายอยู่ในกลุ่มผู้ชุมนุมและออกมาสังหารทหารเมื่อวันที่ ๑๐ เมษายน ๒๕๕๓ ขณะเดียวกัน ทาง นปช. ก็กล่าวว่าทหารทำร้าย-สังหารประชาชน เช่น ปัญหาผู้เสียชีวิตในวัดปทุมวนารามที่สื่อนำรูปทหารยิงปืนหันไปทางวัดมาขึ้นปกนิตยสารในหลายฉบับ เป็นตัวอย่างของการปฏิบัติการจิตวิทยา (PSYOP) ซึ่งเป็นส่วนหลักของ “IO”

ในส่วนของการลวงทางทหาร (MILDEC) ยกตัวอย่างเรื่องการปล่อยข่าวบนเวที นปช. ว่าจะปิดถนนสีลมในวันรุ่งขึ้น ทางฝ่ายรัฐบาลก็ส่งทหารเข้ามาปิดบริเวณสีลมในทันทีที่ทราบข่าว ซึ่งสีลมเลยกลายเป็นบริเวณที่ถูกปิดโดยรัฐบาลไม่ใช่ฝ่าย นปช. การที่ฝ่าย นปช. สามารถเคลื่อนกำลังเข้ายึดแยกราชประสงค์อย่างที่รัฐไม่ทันตั้งตัวนั้นถือได้ว่าเป็นการปฏิบัติการที่สามารถรักษาความปลอดภัยของฝั่งตนไว้ได้เข้ากรณีของ “OPSEC” ซึ่งการรักษาความปลอดภัยในการปฏิบัติการนั้นเป็นเรื่องที่สำคัญเพื่อไม่ให้ข่าวรั่วก่อนการปฏิบัติการ ซึ่งในช่วงหลัง ศอฉ. ก็มีความรัดกุมในการปฏิบัติการมากขึ้น

สำหรับตัวอย่างของสงครามอิเล็กทรอนิกส์ (EW) ก็คือ การปิดสัญญาณดาวเทียมของ People Channel ไม่ให้สามารถถ่ายทอดผ่านดาวเทียมได้ แต่ก็ยังมีหลุดรอดผ่านวิทยุชุมชน และผ่านทางสถานีส่งคลื่นความถี่ต่ำในบริเวณกรุงเทพมหานครเพื่อการถ่ายทอดสดจากเวทีของ นปช. ที่แยกราชประสงค์

สงครามข่าวสารที่รัฐบาลต้องกลับมาทบทวนผลการปฏิบัติงานก็คือ “การปฏิบัติการของระบบเครือข่ายคอมพิวเตอร์” หรือ “CNO” ซึ่งเป็นสงครามไซเบอร์ หรือสงครามบนระบบเครือข่ายอินเทอร์เน็ตอย่างเต็มรูปแบบ ซึ่งทาง นปช. ถือว่าทำได้สำเร็จผลในระดับหนึ่ง มีการใช้เทคโนโลยีใหม่ ๆ ทางอินเทอร์เน็ตอย่างเต็มรูปแบบ เช่น Media Streaming (Flash Media Server) และ Cloud Computing ของ Google และ Microsoft (Google Appspot/App Engine และ Microsoft Horizon) และการถ่ายทอดสดผ่านทาง Peer-To-Peer Broadcasting Software จะเห็นว่าการปิดกั้นเว็บไซต์ของกระทรวง ICT นั้นได้ผลเพียงระดับหนึ่งไม่สามารถปิดกั้นข่าวสารของทาง นปช. ได้ทั้งหมด ๑๐๐%

จากองค์ความรู้ดังกล่าวจะเห็นว่าเรื่อง “สงครามสารสนเทศ” โดยการใช้หลัก “การปฏิบัติการข่าวสาร” นั้น เป็นเรื่องที่มีความสำคัญต่อความมั่นคงของชาติ ในระดับที่นายกรัฐมนตรีและรัฐมนตรีที่เกี่ยวข้องต้องให้ความสำคัญและจัดตั้งหน่วยงานด้าน “National Cyber Security” ขึ้นอย่างเป็นทางการ เพื่อการกำหนดยุทธศาสตร์ นโยบายและกิจกรรมต่าง ๆ ที่เกี่ยวข้องกับ

การรักษาไว้ซึ่งความมั่นคงของชาติในยุคที่สมรภูมิรบไม่ได้อยู่เฉพาะบนบก, ในน้ำหรือบนอากาศอีกต่อไป แต่สมรภูมิรบนั้นอยู่ใน “Cyberspace” หรือ “Cyber Domain” ที่ผู้นำแต่ละประเทศจะมองข้ามเรื่องนี้ไม่ได้เป็นอันขาด หากไม่เน้นจะส่งผลกระทบต่อความมั่นคงของชาติในระยะยาวอย่างหลีกเลี่ยงไม่ได้เรื่อง “IO” เป็นศาสตร์และศิลป์ (Science and Art) ที่จำเป็นต้องศึกษาและเรียนรู้อย่างเป็นระบบตามหลักวิชาการเพื่อเป็นพื้นฐานในการพัฒนา “Nation Cyber Security” ของประเทศไทยในอนาคต