

โฉมใหม่ของสงครามยุคดิจิทัล

ร.อ.นฤพล วีระจิตต์
อาจารย์ฝ่ายศึกษา โรงเรียนนายเรือ

บทนำ

พัฒนาการด้านการทหารของโลกตั้งแต่อดีตมาจนถึงปัจจุบัน มีการเปลี่ยนแปลงอย่างรวดเร็ว เนื่องจากผู้ที่มีเทคโนโลยีเหนือกว่าจะเป็นฝ่ายชนะในสงครามในที่สุด แต่ในปัจจุบันนี้อาจไม่ใช่ เนื่องจากความเจริญก้าวหน้าดังกล่าวทำให้การผลิตอุปกรณ์ในระบบต่าง ๆ สามารถทำได้ง่ายในราคาถูก ประกอบกับความเจริญทางการสื่อสารที่ไร้พรมแดนและความสามารถในการเจาะข้อมูลด้วยแล้ว ทำให้อุปกรณ์ที่ทันสมัยต่าง ๆ ถูกผลิตลอกเลียนขึ้นอย่างรวดเร็ว

ในการทำสงครามอาจจะไม่ต้องใช้อาวุธที่ร้ายแรง ราคาแพงหรือแม่นยำ เพียงแค่ใช้ผู้ที่มีความสามารถในระบบคอมพิวเตอร์มาต่อเชื่อมระบบอินเทอร์เน็ต แล้วส่งโปรแกรมรบกวนข้อมูลทำให้ระบบปฏิบัติการ การควบคุมบังคับบัญชาของฝ่ายตรงข้ามใช้การไม่ได้ก็เพียงพอแล้ว จะเห็นว่าการปฏิบัติการดังกล่าวใช้เงินเพียงเล็กน้อย

วัตถุประสงค์ของบทความนี้จะให้ผู้อ่านได้ทราบถึง รูปแบบของสงครามที่เปลี่ยนแปลงไป และการใช้ประโยชน์จากการสื่อสารข้อมูลในระบบดิจิทัลเป็นหลัก

รูปแบบใหม่ของสงครามที่เปลี่ยนแปลงไป

จากความเจริญก้าวหน้าในโลกยุคปัจจุบันทำให้เกิดการพัฒนาทางด้าน วิทยาศาสตร์ และเทคโนโลยีใหม่ ๆ เสมอ ตั้งแต่กระบวนการผลิต การค้นพบวัสดุใหม่ และเทคนิคการประกอบ จนกระตุ้นให้เกิดนวัตกรรมขึ้น จึงเป็นผลให้การสงครามได้พัฒนาและเปลี่ยนแปลงไปจากเดิม โดยเฉพาะอย่างยิ่งการพัฒนาทางการสื่อสารข้อมูลที่มีความสำคัญยิ่งในการควบคุมบังคับบัญชา ตลอดจนการดำเนินการต่าง ๆ ทั้งระดับ ยุทธศาสตร์ ยุทธการ และยุทธวิธี และได้กำเนิดสงครามสาขาใหม่ คือสงครามข้อมูลข่าวสาร สำหรับความหมายของสงครามข้อมูลข่าวสารนั้นมิใช่ให้ความหมายมากมาย เช่น Brown Commissions ให้คำจำกัดความสงครามข้อมูลข่าวสารไว้ว่า “คือการดำเนินการใด ๆ โดยรัฐบาลกลุ่มบุคคล หรือบุคคล เพื่อควบคุมระบบข่าวสารในประเทศอื่นด้วยวิธีอิเล็กทรอนิกส์ รวมทั้งมาตรการป้องกันการกระทำดังกล่าว (activity undertaken by government, groups, or individuals to gain electronic access to information systems in other countries ...as well activities undertaken to protect against it.)”^๑

^๑ The commission on the Role and Capabilities of the U.S. Intelligence Community was charged with reviewing the efficacy and appropriateness of U.S. intelligence activities in the post-cold war global environment.

แต่มีบุคคลบางกลุ่มไม่เห็นด้วยกับคำจำกัดความนี้ เนื่องจากเป็นไปได้ว่ากระทรวงกลาโหมสหรัฐอเมริกา ทั้งกระทรวงต้องทำสงครามกับเด็ก ๑๓ ขวบคนหนึ่งที่สามารถทำให้ระบบคอมพิวเตอร์ของกระทรวงกลาโหมสหรัฐอเมริกา บั่นป่วนและมีการให้ความหมายจากเอกสารของประธานคณะเสนาธิการช่วย ฯ กระทรวงกลาโหมของสหรัฐอเมริกา ค.ศ.๑๙๙๖ การสงครามข้อมูลข่าวสารไว้ว่า “สงครามข่าวสาร คือ การดำเนินการเพื่อให้เป็นฝ่ายได้เปรียบด้านข่าวสาร โดยการบ่อนทำลายข่าวสาร การดำเนินกรรมวิธีต่อข่าวสาร ระบบข่าวสาร และเครือข่ายคอมพิวเตอร์ของข้าศึก ในขณะที่เดียวกันก็ทำการป้องกันข่าวสาร การดำเนินกรรมวิธีต่อข่าวสาร ระบบข่าวสาร และเครือข่ายคอมพิวเตอร์ของตนจากการบ่อนทำลายของข้าศึก”^๒ ซึ่งในปัจจุบันการรับ-ส่ง ข้อมูลข่าวสารนั้นเป็นการส่งในระบบดิจิทัล คือ การแปลงข้อมูลต่าง ๆ เป็นฐานข้อมูลโดยใช้กลุ่มตัวเลข ๑ และ ๐ แทนที่จะส่งข้อมูลเลียนแบบข้อมูลเดิม (ระบบอนาล็อก) เครื่องส่งข้อมูลแบบดิจิทัลจะเอาข้อมูลต้นแบบมาเข้ารหัสเสียก่อน หรือ ในการปฏิบัติก็คือ คอมพิวเตอร์จะเขียนคำสั่งหรือข้อมูลนั้นในรูปตัวเลข ๐ หรือ ๑ แล้วต่อจากนั้นก็ส่งคำสั่งนั้นออกไป ซึ่งจากวิธีนี้ทำให้การส่งข้อมูลสามารถกระทำได้คราวละมาก ๆ ไม่เปลืองพลังงาน และส่งได้ในหลายสื่อกลาง เช่น ทางสายโทรศัพท์ สายใยแก้วนำแสงและทางคลื่นแม่เหล็กไฟฟ้าที่ผ่านตัวกลางทางอากาศ และในปัจจุบันนี้ตามหลักการดังกล่าว ทำให้ระบบคอมพิวเตอร์ต่าง ๆ สามารถสื่อสารกันได้ กลายเป็นระบบเครือข่าย (Network) เชื่อมโยงกันไปทั่วโลก (Internet) ประกอบกับการสื่อสารดาวเทียมที่ประเทศต่าง ๆ ส่งดาวเทียมขึ้นไปในอวกาศ และใช้คลื่นแม่เหล็กไฟฟ้าส่งข้อมูลในระบบดิจิทัลทำให้โลกในปัจจุบันเข้าสู่ยุคโลกาภิวัตน์ (Globalization) ซึ่งเป็นยุคแห่งการสื่อสารไร้พรมแดน เป็นผลให้รูปแบบของสงครามได้เปลี่ยนแปลงไป เนื่องจากการควบคุมบังคับบัญชาสามารถกระทำได้ที่จุดใดจุดหนึ่งในโลกก็ได้ ประกอบกับการกำหนดการก็ไม่จำเป็นต้องอยู่เป็นกลุ่มก้อนในที่ใดที่หนึ่ง สามารถกระจายกำลังไปได้ทั่วโลก ทำให้ในการรบต่อไปจะไม่มีแนวรบที่แน่นอน ซึ่งแต่ก่อนในการรบต่าง ๆ จะมีการวางกำลังทหารมาก ๆ บริเวณแนวรบที่จะทำสงคราม แต่ปัจจุบันนี้จะไม่มีการวางแผนนี้อีกแล้วเนื่องจากการพัฒนาทางด้านการสื่อสารข้อมูลตามที่ได้กล่าวมาข้างต้น ประกอบกับเทคโนโลยีของระบบอาวุธ และ ระบบควบคุมสั่งการที่ทันสมัยสามารถควบคุม (การสั่งยิง) ที่ใดก็ได้ ระบบอาวุธมีระยะยิงไกลและ ความสามารถในการทำลายล้างสูง ถ้ายังมีการทำสงครามในลักษณะเดิม กล่าวคือ การมีแนวรบ ที่ใช้กำลังทหารไปรวมกันมาก ๆ จะเป็นเป้าหมายใหญ่ที่จะโดนโจมตีจากฝ่ายตรงข้ามที่เราไม่ทราบ

^๒ The Joint Chiefs of Staff Instruction No. 3210.0 Information Warfare (IW). Actions taken to achieve information superiority by affecting adversary information, information-base process, information system, and computer-base networks while defending one's own information, information base processes, information systems, and computer-base network.

ฝ่ายตรงข้ามอยู่ที่ใด การที่จะได้มาซึ่งความได้เปรียบของสงครามในรูปแบบนี้ เกิดจากหลักการ การกระจายกำลัง การซ่อนพราง และการล่องหน (หายไปจากจอร์แดร์) ถ้าไม่สามารถกระทำดังกล่าวได้ ก็ต้องฝังตัวอยู่ที่ดิน เช่น ที่รัสเซีย อิรัก เกาหลีเหนือ คิวบา ไต้หวัน ลิเบีย และสหรัฐอเมริกา (โดยการขุดหลุมลึกเพื่อหลบภัย) สำหรับตัวอย่าง การทำสงครามในลักษณะนี้ ได้แก่ “วิธีการที่ บิน ลาเต็น ลงมือจู่โจมในวันที่ ๑๑ กันยายน ด้วยการควบคุมสั่งการโดยใช้คอมพิวเตอร์ การสื่อสารผ่านดาวเทียมและระบบอินเทอร์เน็ต ซึ่งพวกอัลไกดาได้เข้าไปฝังตัวในสหรัฐอเมริกา เพื่อเตรียมลงมือก่อนปฏิบัติการเป็นเวลานานแล้ว ทั้งในสหรัฐอเมริกา และแคนาดา แล้วบิน ลาเต็น ก็ควบคุมเด็กของเขาจากที่ไหนก็ไม่รู้ ที่ห่างกันครึ่งโลกเห็นจะได้”^๓ และในที่สุดสหรัฐอเมริกาก็โดนโจมตีที่ตึกเวิร์ลเทรดและตึกเพนตากอน ซึ่งการกระทำในลักษณะนี้ยังเกิดขึ้นอย่างต่อเนื่องและเป็นปัญหาให้สหรัฐอเมริกาต้องปวดหัวจนถึงปัจจุบัน สำหรับประเทศไทยเองก็เกิดเหตุการณ์ในลักษณะนี้เหมือนกัน เช่น เหตุการณ์ความไม่สงบที่จังหวัดชายแดนภาคใต้ มีการวางระเบิดก่อวินาศกรรมจรวดจรวดจากโทรศัพท์มือถือ โดยการสั่งการทางระบบสื่อสารต่าง ๆ ซึ่งยังไม่สามารถหาผู้สั่งการได้เท่าที่ทราบอยู่ในประเทศที่สาม

จากการสื่อสารข้อมูลที่ผ่านสื่อต่าง ๆ โดยเฉพาะอย่างยิ่งในระบบเครือข่ายอินเทอร์เน็ต ทำให้เกิดสงครามอีกสาขาหนึ่งคือ สงครามเครือข่าย ซึ่งเกิดจากภายในหน่วยงานต่าง ๆ มีการใช้คอมพิวเตอร์เชื่อมต่อกันเป็นเครือข่ายและเชื่อมต่อกับระบบอินเทอร์เน็ต ทำให้ผู้ที่มีความสามารถทางด้านคอมพิวเตอร์ (แฮกเกอร์)^๔ ที่ใช้ระบบอินเทอร์เน็ตสามารถล้วงข้อมูลที่สำคัญ หรือ ส่งไวรัสคอมพิวเตอร์เข้ากระทำกับระบบเครือข่ายของหน่วยงานต่าง ๆ ได้ เช่น “แฮกเกอร์ ของจีนได้วางแผนโจมตีต่อเว็บไซต์ของสหรัฐอเมริกา และระบบเน็ตเวิร์คเป็นเวลาหลายสัปดาห์ โดย เอฟบีไอ รายงานว่า จีน ใช้ไวรัสตัวใหม่ชื่อว่า เสือโคร่งเข้าระบบอินเทอร์เน็ตในการเล่นงานสหรัฐอเมริกา”^๕ และจากการที่ “จีนได้ขโมยระบบปฏิบัติการของดาวเทียมสหรัฐอเมริกาแล้ว ด้วยการแฮกเข้าไปในแล็บหนึ่งในหลาย ๆ แล็บที่ออกแบบมันขึ้นมา ให้เหมือนกับเป็นใครก็ไม่รู้มาฉวยก๊อปปี้อันหนึ่งของซอฟต์แวร์สำหรับดาวเทียมชื่อ OS/COMET ไปจากเซิร์ฟเวอร์ของแล็บวิจัยของกองทัพเรือในเดือนธันวาคม ปี ค.ศ.๒๐๐๐ แล้วจีนยังส่งสายลับเข้าไปในสถานีสัญญาณดาวเทียมภาคพื้นดินด้วย และได้สำเนาของอัลลิงค์ ซอฟต์แวร์สำคัญ รวมทั้งโค้ดของแพ็คเกจไป ตามมาจึงดำเนินการแฮกดาวเทียมสหรัฐอเมริกา เป็นผลให้ดาวเทียมสหรัฐอเมริกาเสีย

^๓ เบอร์โควิทซ์, บรูซ.: *The New Face of War*

^๔ การปฏิบัติการของสงครามแฮกเกอร์มีด้วยกันหลายระดับ ซึ่งกระทำกับคอมพิวเตอร์ ทั้งที่อยู่ในที่ตั้งและนอกที่ตั้ง มุ่งระดับความเสียหายตั้งแต่ให้ระบบคอมพิวเตอร์เป็นอัมพาต เปิดๆ ปิดๆ เป็นระยะ หรือข้อมูลผิดพลาด ข้อมูลถูกขโมย เป็นต้น เพื่อให้ผู้ปฏิบัติการทำการควบคุมได้ ตลอดจนพยายามบ่อนทำลายชื่อเสียงสถาบันหรือประเทศ ตลอดจนตัวผู้นำบุคคลสำคัญผ่านระบบอินเทอร์เน็ต อีกทั้งเพื่อมุ่งผลให้เกิดความเสียหาย หรือเข้าใจผิดได้ หรือระดับพื้นฐาน คือ ขโมยใช้บริการ ลักลอบใช้โทรศัพท์หรือเปลี่ยนตัวเลข

^๕ เบอร์โควิทซ์, บรูซ.: *The New Face of War*

การควบคุมไประยะหนึ่ง”^๖

จะเห็นว่าการบันทึกข้อมูลในระบบดิจิทัลนั้นมีจุดอ่อนในเรื่องการรักษาความปลอดภัย ที่จะต้องมีให้ข้อมูลรั่วไหลไปยังฝ่ายตรงข้าม มิเช่นนั้นข้าศึกจะล่วงรู้ข้อมูลสำคัญต่าง ๆ ได้ เช่น “คัลลิสัน” นักข่าวของสหรัฐอเมริกา อีริกได้เข้าไปทำข่าวแล้วคอมพิวเตอร์โน้ตบุ๊กเสีย จึงไปหาซื้อคอมพิวเตอร์เครื่องใหม่จากร้านขายคอมพิวเตอร์ในอิรัก ปรากฏว่าเจอบคอมพิวเตอร์มือสองของพวก อัลไคด้า จึงซื้อมา และได้ทำการแกะข้อมูลเดิมที่อยู่ในเครื่อง ปรากฏว่าได้พบข้อมูลโดยละเอียดของการปฏิบัติการก่อการร้าย ที่เก็บเอาไว้เป็นเวลานานสี่ปี ขององค์การก่อการร้าย ทั้งในอัฟกานิสถาน และในประเทศอื่น ๆ”^๗

การใช้เทคโนโลยีใหม่ ๆ มาใช้ประโยชน์ในการสงคราม

ระบบการบังคับบัญชา ควบคุม สื่อสาร ในประเทศสหรัฐอเมริกา ได้พัฒนาระบบ C4ISR (Command Control Communication Computers Intelligence Surveillance and Reconnaissance) ในการบังคับบัญชา การควบคุม สื่อสาร บวกกับความรวดเร็วแม่นยำในการรวบรวมข้อมูล ตำแหน่งที่ตั้ง และการเคลื่อนไหวของข้าศึก ซึ่งการสื่อสารจะเป็นในระบบคอมพิวเตอร์ไร้สาย และสามารถทำงานได้อย่างต่อเนื่องตลอดเวลา มีความคล่องตัวสูง โดยใช้เทคโนโลยี ๗ ด้าน คือ การจัดตั้งเครือข่ายเคลื่อนที่และยานความถี่ การเชื่อมโยงระบบเครือข่ายเซนเซอร์ ขีดความสามารถในการรับ-ส่งข้อมูล ระหว่างดาวเทียม เครื่องบินสอดแนมไร้คนบิน และศูนย์บัญชาการ ระบบสายรับ-ส่งสัญญาณศักยภาพสูง ระบบปกป้องข้อมูลเครือข่าย และสุดท้ายระบบเครือข่ายประสานการยิงจรวดขีปนาวุธและอาวุธหนักต่าง ๆ

ระบบระบุตำแหน่งบนพื้นโลก หรือ Global Positioning System (GPS) อันเป็นเทคโนโลยีการบอกตำแหน่งด้วยดาวเทียม เครื่องรับสัญญาณ GPS สามารถบอกคุณได้ว่าอยู่ตรงไหนได้ในหน่วยของเมตร ด้วยการตีค่าสัญญาณที่ถูกส่งมาจากกลุ่มดาวเทียม ระบบนี้จะทำงานด้วยวิธีการสามเหลี่ยม (Triangulation) เหมือนเดิม ด้วยหลักการเดิมไม่ผิดเพี้ยน ด้วยการคำนวณหาตำแหน่งแห่งที่ คุณเอาจุดที่ทราบตำแหน่งแล้วทั้งสามจุด และใช้คำนวณทางเรขาคณิต โดยครั้งแรกกระทรวงกลาโหมสหรัฐอเมริกา เป็นผู้จัดส่งดาวเทียมชุดแรก โดยมีวัตถุประสงค์เบื้องต้นเพื่อสร้างระบบนำร่องและนำวิถีที่มีความแม่นยำสูง ใช้กับการกิจการทางทหารทุกด้านได้ตลอด ๒๔ ชั่วโมง และทุกสภาพอากาศ ในเวลาต่อมาจึงขยายระบบสู่ภาคเอกชน ปัจจุบันระบบจีพีเอสมีดาวเทียมในระบบ ๒๙ ดวง ซึ่งจะบอกตำแหน่ง และแสดงบนแผนที่ดิจิทัลอย่างแม่นยำแน่นอน แล้วยังสามารถบอกความสูง (๓ มิติ) ได้อีกด้วย

^๖ เบอร์โควิทซ์, บรูซ.: *The New Face of War*

^๗ เบอร์โควิทซ์, บรูซ.: *The New Face of War*

จรวดความแม่นยำสูง ระบบอาวุธแบบ Joint Direct Attack Munition (JDAM) จรวดแบบนี้ประกอบด้วยเครื่องรับสัญญาณระบบจีพีเอส หน่วยวัดแรงเฉื่อยขนาดเล็ก และครีบบังคับทิศทางอีกหนึ่งชุด ไปติดบนระเบิดก็จะได้จรวดฉลาด (สมาร์ทบอมบ์) ในราคายอมเยา (ลูกละ ๑๖,๐๐๐ เหรียญ)^๘

เครื่อง Jam ระบบ GPS ในปี ค.ศ.๑๙๙๙ บริษัท Aviaconversia ของรัสเซียได้นำเอาอุปกรณ์รบกวนสัญญาณ GPS ออกจำหน่าย “ราคาเครื่องละประมาณ ๔,๐๐๐ ดอลลาร์”^๙ ซึ่งสามารถสกัดสัญญาณ GPS ได้ในรัศมี ๑๕๐ – ๒๐๐ กิโลเมตร ด้วยกำลังส่งเพียง ๔-๘ วัตต์ ทำให้ยากในการตรวจพบและทำลาย หลังจากนั้นได้มีการเสนอขายชิ้นส่วนอุปกรณ์ดังกล่าวในระบบอินเทอร์เน็ต “ในราคาเพียง ๔๐ ดอลลาร์”^{๑๐} ส่วนกระทรวงกลาโหมสหรัฐอเมริกา ได้เร่งสร้างเครื่องตรวจจับระบบรบกวนสัญญาณ GPS ซึ่งสามารถระบุแหล่งที่มาได้อย่างชัดเจน ทางด้านออสเตรเลียก็กำลังจะพัฒนาวิธีป้องกันระบบสัญญาณ GPS แบบใหม่ วิธีการหนึ่งที่ชักกัอยู่ในขณะนี้คือการเปลี่ยนย่านความถี่ของสัญญาณ แต่วิธีนี้ทำได้เฉพาะผู้ที่ควบคุมดาวเทียม GPS เท่านั้น ในช่วงต้นสงครามอิรักครั้งที่ ๒ สหรัฐอเมริกาได้โจมตีบริษัทเอกชนของรัสเซีย ว่าเป็นผู้ขายอุปกรณ์รบกวนสัญญาณ GPS ให้กับอิรัก แต่บริษัทดังกล่าวได้ออกมาปฏิเสธว่าไม่มีส่วนเกี่ยวข้อง

ระบบต่อต้านขีปนาวุธ รัฐบาลสหรัฐอเมริกา ได้พัฒนาระบบป้องกันขีปนาวุธ โดยประกาศถอนตัวจากสนธิสัญญา ABM ในสมัยประธานาธิบดี บุช ในช่วงกลางปี ค.ศ.๒๐๐๒ และเดินหน้าโครงการ National Missile Defense (NMD) เต็มตัวถึงแม้จะมีเสียงคัดค้านจากหลายฝ่ายก็ตาม ระบบป้องกันขีปนาวุธแห่งชาติ (NMD) มีวัตถุประสงค์หลักเพื่อปกป้องดินแดนทั้ง ๕๐ รัฐของสหรัฐอเมริกา จากการโจมตีด้วยของฝ่ายศัตรู นอกจากนี้ยังสามารถป้องกันประเทศพันธมิตรและกองกำลังของสหรัฐอเมริกา ที่ประจำการอยู่ในต่างประเทศอีกด้วย ส่วนประกอบของระบบประกอบด้วยส่วนสำคัญ ๕ ส่วน ได้แก่

๑. Upgraded Early-warning Radar (UEWR) เป็นระบบตรวจจับขีปนาวุธและหัวรบที่พุ่งมายังสหรัฐอเมริกา ในช่วงกลางเส้นทาง ก่อนหน้าเรดาร์ XBR

๒. X-band/Ground-based Radar (XBR) เป็นระบบเรดาร์อเนกประสงค์ใช้สัญญาณเรดาร์ความถี่สูง ทำหน้าที่ตรวจจับและติดตามความเคลื่อนไหวของขีปนาวุธและหัวรบที่พุ่งเข้าใกล้ดินแดน

^๘ เบอร์โควิทซ์, บรูซ.: *The New Face of War*

^๙ รอฮัม ปรามาส : *FUTUREWAR & FIGHTING MACHINE สงครามอนาคต และนวัตกรรมทางทหาร*

^{๑๐} รอฮัม ปรามาส : *FUTUREWAR & FIGHTING MACHINE สงครามอนาคต และนวัตกรรมทางทหาร*

สหรัฐอเมริกา สามารถแยกแยะเป้าหมายได้ว่าเป็นหัวรบปลอมหรือหัวรบจริง และยังทำหน้าที่สนับสนุนกิจการของกระสวยอวกาศ และตรวจจับอวกาศที่พุ่งมายังโลก

๓. Space-based Infrared System (SBIRS) เป็นระบบที่ใช้ดาวเทียมทั้งหมด ๒๔ ดวง แบ่งเป็น ๓ กลุ่มที่มีระดับวงโคจรเท่ากัน ดาวเทียม SBIRS จะสามารถตรวจจับขีปนาวุธได้ตลอดเส้นทางตั้งแต่ช่วงต้น ๆ ทำให้สามารถยิงอาวุธสกัดกั้นได้ก่อนหน้าที่ขีปนาวุธจะเดินทางเข้าถึงระยะทำงานของ XBR

๔. Ground-Based Interceptor (GBI) เป็นระบบอาวุธของ NMD ทำหน้าที่สกัดกั้นหัวรบของขีปนาวุธที่นอกชั้นบรรยากาศโลก

๕. Battle Management/Command , Control and Communication (BM/C3) เป็นเหมือนสมองของระบบ NMD ที่ควบคุมบัญชาการ ประสานการปฏิบัติต่าง ๆ ในระบบ สามารถสั่งการยิงสกัดกั้นขีปนาวุธได้ภายในเวลา ๒๐ นาที

บทสรุป

จะพบว่าในการทำสงครามในขณะนี้ รูปแบบได้เปลี่ยนแปลงไปจากเดิม จะไม่มีการรบซึ่งหน้า ไม่มีแนวรบ กำลังรบต่าง ๆ กระจุกกระจายกันอยู่ ชัยชนะในสงครามไม่ชัดเจน เนื่องจากไม่สามารถทำลายเครือข่ายการสื่อสาร การบังคับบัญชา และกำลังรบทั้งหมดของฝ่ายตรงข้ามให้หมดสิ้นได้ จากการพัฒนาระบบอาวุธของประเทศมหาอำนาจที่มีทุนในการดำเนินการ ทำให้เทคโนโลยีทางการทหาร และระบบอาวุธมีศักยภาพสูง ใช้กำลังพลน้อย สามารถทำลายฝ่ายตรงข้ามได้โดยไม่ต้องเคลื่อนพล

เมื่อพิจารณาจากรูปแบบของสงครามที่เปลี่ยนแปลงไป และระบบอาวุธที่ทันสมัยของประเทศมหาอำนาจแล้วนั้น วิธีที่ประเทศเล็ก ๆ จะสามารถต่อสู้กับประเทศมหาอำนาจในอนาคตได้ ก็คงจะมีแต่การรบแบบแอบซุ่มโจมตี ซึ่งการรบในรูปแบบนี้ จะไปสนับสนุนในการทำสงครามที่เรียกว่า สงครามก่อการร้าย ที่ใช้อาวุธและเทคโนโลยีในราคาถูก แต่การต่อสู้กับมันอาจต้องใช้งบประมาณมหาศาล ซึ่งในความคิดของผู้เขียนแล้วการที่จะได้มาซึ่งชัยชนะในสงครามแบบนี้ ไม่ใช่ว่าการใช้กำลังทางทหารเข้าทำลายฝ่ายตรงข้ามแต่เพียงอย่างเดียว เพราะเมื่อศัตรูถูกล้มมีกำลังอีกจะต่อสู้กลับอย่างแน่นอน ดังนั้นเราต้องเอาชนะจิตใจและจิตใจสำนึกของเขาด้วย แล้วเราจะได้มาซึ่งชัยชนะอย่างสมบูรณ์

บรรณานุกรม

รอฮีม ปรามาส : สงครามอนาคต และนวัตกรรมทางการทหาร ๑. กรุงเทพฯ : มติชน ๒๕๔๗.

รอฮีม ปรามาส : **FUTUR & FIGHTING MACHINE WAR** สงครามอนาคต และนวัตกรรมทาง
การทหาร. กรุงเทพฯ : สำนักพิมพ์มติชน ๒๕๔๗

BERKOWITZ, BRUCE : **THE NEW FACE OF WAR** โฉมใหม่ของสงครามยุคดิจิทัล แปลโดย
สรศักดิ์ สุปงกช กรุงเทพฯ : สำนักพิมพ์ อนิเมท กรุ๊ป ๒๕๔๗.

<http://www.iwar.org.uk/iwar/resources/belvoir-iw-course/infocfront.htm>, November 24, 2004.

<http://www.fas.org/irp/wwwinfo.html>, November 24, 2004.

<http://www.au.af.mil/au/awc/awcgate/barnett/b5toc>, November 24, 2004.

<http://www.rand.org/publications/reviews.html>, December 2, 2004.

ประวัติย่อของผู้เขียน

ชื่อ ร.อ.นฤพล วีระจิตต์

วันเดือนปีเกิด ๔ พฤศจิกายน ๒๕๑๗

การศึกษา มัธยมศึกษาตอนปลาย รร.สาธิต มหาวิทยาลัยบูรพา
นักเรียนเตรียมทหาร รุ่นที่ ๓๔
นักเรียนนายเรือ รุ่นที่ ๙๑
โรงเรียนนายทหารพรคนาวิน รุ่นที่ ๔๙

หลักสูตรการศึกษาที่สำคัญ นายทหารสื่อสาร ระยะเวลา ๑๐ สัปดาห์ สส.ทร
ต้นปืน กฝร.กร.
หลักสูตรการตรวจเรือชั้นต้น และชั้นสูง จัสแมคไทย

ประวัติการทำงาน ประจำแผนกข่าว กยพ.กร.
นสส.ร.ล.ปิ่นเกล้า
ตท.ร.ล.ล่องลม
นกว.ร.ล.ล่องลม
ตร.ร.ล.ล่องลม
ผบ.เรือ.ต.๑๓

ประวัติเกี่ยวกับการศึกษา เรื่อง Information Warfare

- หลักสูตรนายทหารสื่อสาร สส.ทร.
