สงครามสารสนเทศ – เพื่อครองความเหนือกว่าทางสารสนเทศ

เทคโนโลยีสารสนเทศมีบทบาทเป็นอย่างมากในปัจจุบัน ดังจะเห็นได้จากหน่วยงานต่าง ๆ เช่น รัฐบาล ภาครัฐ ภาคเอกชน หรือแม้กระทั้ง ประชาชนทั่วไป ต่างมีแนวความคิดที่จะนำเทคโนโลยีสารสนเทศมาประยุกต์ใช่งานในกิจกรรม ต่าง ๆ เพื่อให้กิจกรรมนั้น ๆ เกิดประสิทธิภาพสูงสุด จนมีคำกล่าวว่า ปัจจุบันเป็นยุคของ “สังคมสารสนเทศ”

เมื่อสารสนเทศ ได้ถูกนำมาใช้กับกิจกรรมต่าง ๆ อย่างแพร่หลาย ย่อมเป็นสิ่งที่หลีกเลี่ยงไม่ได้ที่กิจกรรม ทางทหารจะนำสารสนเทศมาใช้งาน ทั้งทางด้านการบริหารจัดการและในสนามรบ ทำให้สารสนเทศเปรียบเสมือนทรัพยากร ที่มีความสำคัญยิ่ง ที่แต่ละฝ่ายของคู่สงครามต่างที่จะครองความเหนือกว่าทางด้านสารสนเทศ หรือที่เรียกว่า
Information Superiority

ดังนั้นกิจกรรมใด ๆ ทั้งมวลที่นำมาซึ่งความได้เปรียบทางด้านสารสนเทศของฝ่ายเราที่มีเหนือฝ่ายตรงข้าม และการป้องกันสารสนเทศของฝ่ายเราจากฝ่ายตรงข้าม เราจะเรียกว่า “สงครามสารสนเทศ” หรือ “Information Warfare” เรียกย่อ ๆ ว่า IW โดยสารสนเทศในที่นี้จะรวมถึง ข้อมูล สารสนเทศ องค์ความรู้ เทคโนโลยีสารสนเทศ ระบบสารสนเทศ และระบบเครือข่าย

“สงครามสารสนเทศ” มีบทบาทที่สำคัญยิ่งในช่วงทศวรรษที่ผ่านมาดังจะเห็นได้จาก การรบครั้งสำคัญหลายครั้งที่ผ่านมา และล่าสุด คือ ยุทธการปลดปล่อยชาวอิรัก (Operations Iraqi Freedom) ที่สหรัฐฯ และฝ่ายพันธมิตรยินยอมให้ผู้สื่อข่าวติดตามขบวนรบ เข้าไปรายงานข่าวสดจากพื้นที่การรบ ใช้เทคโนโลยีและระบบอาวุธที่ทันสมัยเลือกทำลายเป้าหมายอย่างแม่นยำ และรวมถึงการใช้ปฏิบัติการทางด้านกิจการพล

เรือน และการประชาสัมพันธ์ เพื่อครองความเหนือกว่าทางด้านสารสนเทศอย่างภาวร อันจะนำมาซึ่ง การยุติการรบอย่างรวดเร็ว เพื่อลดการสูญเสีย ของทั้งสองฝ่าย

ปัจจุบันการแบ่งประเภทของสงครามสารสนเทศนั้นมีการแบ่งประเภทที่แตกต่างกันออกไปมากมาย สำหรับที่นี้ของแบ่งตาม แนวคิดของ Martin Libiciki ที่นำเสนอในบทความชื่อ “What is Information Warfare?” เมื่อเดือน สิงหาคม พ.ศ. 2538 โดยที่ Martin ได้แบ่งสงครามสารสนเทศออกเป็น 7 ประเภท คือ

1. สงครามการควบคุมบังคับบัญชา (Command-and-Control Warfare: C2W) เป็นการปฏิบัติในระดับยุทธศาสตร์ทหารสำหรับการทำสงครามสารสนเทศที่มุ่งสู่การทำลายล้างในสนามรบ โดยการทำลายนั้นจะมุ่งไปสู่การทำลายกระบวนควบคุมบังคับบัญชาของฝ่ายข้าศึกและรวมไปถึงการป้องกันไม่ให้ฝ่ายข้าศึกทำลายกระบวนการควบคุมบังคับบัญชา แนวความคิดหลัก ๆ ของการทำสงครามควบคุมบังคับบัญชาจะมีอยู่สองแนวความคิดคือ

- ตีหัว (Antihead): แนวความคิดนี้เป็นแนวความคิดที่มุ่งกระทำต่อศูนย์การบังคับบัญชาของข้าศึกรูปแบบ ของการกระทำแบบนี้มีการปฏิบัติกันมานานตั้งแต่มีสงคราม เพราะต่างฝ่ายที่ทำการรบก็รู้ดีว่าถ้าแม่ทัพของอีกฝ่ายเสียชีวิต การบังคับบัญชาในสนามรบจะระส่ำระสาย ดังเช่น การใช้พลซุ่มยิงของฝรั่งเศสลอบสังหาร พลเรือเอก ลอร์ด เนลสัน (Admiral Lord Horatio Nelson: 1758 - 1805) แห่งสหราชอาณาจักร ในยุทธนาวีที่แหลมทราฟาลการ์ (Trafalgar) ขณะที่เขาบัญชาการรบบนเรือหลวง วิคตอร์รี่ (H.M.S. Victory) หรือ การเสียชีวิตของของพลเรือเอก อิโสโรกุ ยามาโมโต (Admiral Isoroku Yamamoto: 1884 - 1943) ที่ฝ่ายสหรัฐ ฯ สามารถถอดข้อมูลเข้ารหัสของญี่ปุ่นได้ในวันที่ 14 เมษายน พ.ศ. 2486 ว่า พลเรือเอกยามาโมโตจะบินไปตรวจภูมิประเทศที่เกาะบัวเกนวิลล์ (Bougainville Island) และบินกลับมา ที่เกาะกวนดาคานอล (Guadanal) ซึ่งอยู่บริเวณหมู่เกาะโซโลมอน ปาปัวนิวกินนี ในวันที่ 18 เมษายน พ.ศ. 2486 เวลา 0840 โดยพลเรือเอก ยามาโมโต จะโดยสารเครื่องบินทิ้งระเบิด Mitsubishi G4M Bomber หรือที่รู้จักกันในนาม Betty พร้อมด้วย เครื่องบินขับไล่ทำหน้าที่คุ้มกัน Mitsubishi A6M หรือที่รู้จักกันในนาม Zero จำนวน 6 ลำ ผลที่ตามมาคือ กองทัพสหรัฐ ฯ ส่งเครื่องบิน Lockheed P-38 Ligthing จำนวน 18 ลำ เข้าโจมตี ในวันเวลาดังกล่าว ทำให้เครื่องบินทิ้งระเบิด Betty ที่พลเรือเอกยามาโมโต โดยสารมาถูกยิงตก

อย่างไรก็ตามรูปแบบของการดำเนินสงครามได้เปลี่ยนแปลงไปในปัจจุบัน การรบนั้นมีพื้นที่ที่กว้างไกล สนามรบมีความซับซ้อนดังที่กล่าวไปในบทที่ 6 ที่เปลี่ยนมาเป็นพื้นที่การรบ ทำให้การบังคับบัญชาของแม่ทัพนายกองมีขอบข่ายที่กว้างไกล ด้วยเหตุนี้เองเทคโนโลยีต่าง ๆ ได้ถูกนำมาใช้เพื่อให้การบังคับบัญชาของแม่ทัพนายกองเป็นไปได้อย่างทั่วถึงและมีประสิทธิภาพ เมื่อนำเทคโนโลยีมาช่วยเหลือในกระบวนการบังคับบัญชา การสร้างสิ่งปลูกสร้างเพื่อกำบังและซ่อนพรางอุปกรณ์ต่าง ๆ ในการบังคับบัญชาจึงเป็นสิ่งที่สำคัญ สิ่งปลูกสร้างเหล่านี้ทางทหารจะเรียกว่า “ศูนย์ปฏิบัติการ” หรือ “ที่บังคับการ” โดยศูนย์ปฏิบัติการ หรือที่บังคับการ เหล่านี้ ปัจจุบันถือเป็นเป้าหมายที่ต้องทำลายเป็นอันดับแรก ๆ เพื่อให้การบังคับบัญชาชะงักงันเกิดความสับสนระส่ำระสายในบังคับบัญชาของหน่วยรอง ซึ่งการกระทำในรูปแบบนี้ถือได้ว่าเป็นการ ตีหัว

(antihead) ในปัจจุบัน ดังตัวอย่างเช่น การปล่อยจรวดร่อน โทมาร์ฮอร์ค (Tomahawk Cruise Missle) ของกองทัพสหรัฐ ฯ เข้าทำลายกองบัญชาการที่ต่าง ๆ ของอิรัก ในปฏิบัติการปล่อดปล่อยชาวอิรัก (Operations Iraqi Freedom) ต้นปีพ.ศ. 2546 ที่ผ่าน

- ปาดคอ (Antineck): นอกจากแนวความคิดในการตีหัวแล้ว การปาดคอ (antineck) เป็นอีกแนวทางหนึ่งในการทำสงครามการควบคุมบังคับบัญชา เพราะการสังการต่าง ๆ ของแม่ทัพนายกองนั้นมีความจำเป็นต้องอาศัยระบบการสื่อสารต่าง ๆ ดังนั้นการทำลายโครงสร้างพื้นฐานทางการสื่อสารของฝ่ายตรงข้ามจึงถือว่าเป็นการทำให้ฝ่ายตรงข้ามไม่สามารถสั่งการใด ๆ ได้จนเป็นอัมพาตในที่สุด การปาดคอ (antineck) นั้นสามารถกระได้โดยอาวุธทำลายล้าง (Lethal Weapon) อย่างเช่นระเบิด และการรบกวนระบบการสื่อสารของฝ่ายตรงข้ามด้วยสงครามอิเลคทรอนิคส์ (Electronic Warfare: EW)

2. สงครามบนบรรทัดฐานของการข่าวกรอง (Intelligence-Based Warfare: IBW) การใช้ข่าวกรองเพื่อการปฏิบัติการทางทหารในปัจจุบันได้เปลี่ยนแปลงไปอย่างมาก จากเดิมที่ผู้บังคับบัญชาเป็นผู้ใช้ข่าวกรองเพื่อประกอบในการวางแผนหรือตัดสินใจ แต่ในปัจจุบันข่าวกรองบางลักษณะถูกส่งตรงจากอุปกรณ์เซ็นเซอร์ (sensor) ไปยังอาวุธอัตโนมัติ จากนั้นอาวุธอัตโนมัติก็จะทำงานตอบสนองตามข่าวกรองที่เข้ามาทำให้การตอบสนองต่อภัยคุกคามประเภทต่าง ๆ ได้เร็วยิ่งขึ้น นอกเหนือจากการตอบสนองต่อภัยคุกคามที่เกิดแล้ว ข่าวกรองที่ได้มาในปัจจุบันยังมีความละเอียดมากกว่าข่าวกรอง ที่ได้ในอดีต ทำให้รูปแบบของวงรอบข่าวกรอง (ประกอบไปด้วย การวางแผนรวบรวมข่าวสาร (Planning) การรวบรวมข่าวสาร (Collecting) การวิเคราะห์ข่าวสาร (Analysis) และ การนำไปใช้ (Disseminate)) มีการเปลี่ยนแปลงไปตามความรูปแบบของการดำเนินสงครามในยุคสารสนเทศนี้ สำหรับการสงครามบนบรรทัดฐานของการข่าวกรองนั้นสามารถแบ่งออกได้เป็น 2 ลักษณะคือ

- การสงครามบนบรรทัดฐานของการข่าวกรองเชิงรุก (Offensive IBW): เนื่องจากความเจริญของเทคโนโลยีทำให้การพัฒนาอุปกรณ์สำหรับการตรวจจับอย่าง เซนเซอร์ (sensor) เรดาร์(RAdio Detection And Ranging: Ladar radar) อินฟาเรด (infrared) ไลดาร์ (LIght Detection And Ranging: lider) และเรดาร์ (LAser Detection And Ranging: Ladar) ให้มีประสิทธิภาพสูง สามารถนำไปติดตั้งใช้งานได้ในพื้นที่การรบ ที่แตกต่างและหลากหลายได้

การใช้อุปกรณ์ตรวจจับเหล่านี้อย่างแพร่หลายจะช่วยให้มีข้อมูล ข่าวสาร ข่าวกรอง ที่มีความละเอียด (accurate) บนเวลาจริง (real-time) และใกล้เคียงเวลาจริง (near-real-time) และเมื่อประกอบเข้ากับระบบสารสนเทศ ทางทหารแล้วจะช่วยให้ผู้บังคับบัญชาที่เป็นแม่ทัพนายกองทั้งหลายสามารถที่จะวาดภาพสนามรบ (battlefield visualization) ได้อย่างชัดเจน สำหรับแนวความคิดในการใช้อุปกรณ์ตรวจจับในพื้นที่การรบมีอยู่ 4 รูปแบบคือ (1) อุปกรณ์ตรวจจับระยะไกล (far stand-off sensors) เช่น การใช้ดาวเทียม เครื่องตรวจจับความสั่นสะเทือนแผ่นดิน เครื่องตรวจจับเสียง ฯลฯ (2) อุปกรณ์ตรวจจับระยะใกล้ (near stand-off sensors) เช่น อากาศยานไร้คนขับ (Unmanned aerial Vehicles: UAV) (3) อุปกรณ์ตรวจจับ

ภายในพื้นที่ (in-place sensors) เช่น เครื่องตรวจจับเสียง และ (4) ระบบอาวุธพร้อมอุปกรณ์ตรวจจับ (weapons sensors) เช่น เรดาร์แบบสะท้อนกลับ

เมื่อข้อมูลข่าวสารมีการไหลเข้าสู่ระบบสารสนเทศทางทหารอย่างต่อเนื่องบนเวลาจริง (real-time) การใช้ฝ่ายเสนาธิการที่เป็นมนุษย์จัดการเกี่ยวกับข้อมูลทั้งหมดอาจจะส่งผลให้เกิดการผิดพลาดได้ ทำให้ในปัจจุบันมีการนำแนวความคิดในเรื่องปัญญาประดิษฐ์ (Artificial Intelligence: AI) อย่างเช่น โครงข่ายประสาทเทียม (Neural Network) หรือ การคำนวณแบบวิวัฒนาการ (Evolutionary Computation) เข้ามาช่วยเหลือมนุษย์ในการตัดสินใจ

- การสงครามบนบรรทัดฐานของการข่าวกรองเชิงรับ (Defensive IBW): การดำเนินการ IBW เชิงรับนั้น จะมุ่งเน้นไปยังการคุ้มครองป้องกันระบบตรวจจับต่าง ๆ ของฝ่ายเราให้รอดพ้นจากการโจมตีจากฝ่ายข้าศึก

3. สงครามอิเลคทรอนิคส์ (Electronic Warfare: EW) การทำสงครามอิเลคทรอนิคส์เป็นกระทำที่มุ่งเน้น ต่อการลดขีดความสามารถในการส่งผ่านข้อมูลต่าง ไม่ว่าจะเป็น เสียง ภาพ และข้อมูล โดยมีลักษณะของการปฏิบัติ 3 ประการ คือ

- โจมตีระบบเรดาร์ (Antiradar) การโจมตีต่อระบบเรดาร์นั้นเป็นรูปแบบหนึ่งของการทำสงครามอิเลคทรอนิคส์ที่มีการปฏิบัติกันมาเวลานาน ไม่ว่าจะเป็น การก่อกวน (jamming) หรือการต่อต้านการก่อกวน (counterjamming) โดยมีวัตถุประสงค์คือไม่ให้ฝ่ายตรงข้ามสามารถใช่ประโยชน์จาก เรดาร์ หรือ ป้องกันไม่ให้ฝ่ายตรงข้ามก่อกวนระบบเรดาร์ของ ฝ่ายเรา

- โจมตีระบบสื่อสาร (Communication) นอกเหนือจากการโจมตีต่อระบบเรดาร์แล้วการโจมตีต่อระบบการสื่อสารฝ่ายตรงข้ามด้วยการรบกวนสัญญาณการสื่อสาร และการป้องกันการโจมตีระบบการสื่อสารของฝ่ายเราด้วยการใช้ ระบบที่คงทนต่อการรบกวนสัญญาณ การสื่อสารมีความสำคัญมากเพราะเป็นเส้นทางการเคลื่อนย้ายข้อมูลข่าวสาร

- การเข้ารหัส (Cryptography) การเข้ารหัสและถอดรหัสเป็นอีกหนึ่งของการปฏิบัติในการทำสงครามอิเลคทรอนิกส์ การเข้ารหัสเป็นศาสตร์ที่มีมากว่าพันปี หลักฐานที่เด่นชัดคือการเข้ารหัสของ จูเลียส ซีซาร์ (Julius Caesar: 100 - 44 B.C.) จักรพรรดิ์แห่งอณาจักรโรมัน ด้วยการใช้ substitution cipher หรือเรียกอีกชื่อหนึ่งว่า Caesar cipher การเข้ารหัสเป็นการป้องกันไม่ให้ฝ่ายตรงข้ามดักรับหรือขโมยข่าวสารหรือข่าวกรอง เพื่อนำไปใช้ประโยชน์ นอกจากการเข้ารหัสแล้ว การเจาะรหัสก็เป็นสิ่งจำเป็น ในการรบหลายสมรภูมิที่ผ่านมามีความพยายามในการเจาะการเข้ารหัสฝ่ายตรงข้ามเพื่อนำข่าวสารหรือข่าวกรองเพื่อนำมาใช้ประโยชน์

4. สงครามจิตวิทยา (Psychological Warfare: PSYW): เป็นเรื่องของการโฆษณาชวนเชื่อและปฏิบัติการอื่น ๆ ที่มีจุดมุ่งหมายให้เกิดอิทธิพลต่ออารมณ์ ทัศนคติ ทีท่า ความเชื่อ พฤติกรรมของ ฝ่ายตรงข้าม

ฝ่ายเรา และฝ่ายเป็นกลาง เพื่อบรรลุวัตถุประสงค์ของชาติ รูปแบบของการทำสงครามจิตวิทยามีอยู่ 4 ลักษณะคือ

- ต่อต้านเจตจำนงแห่งชาติ (Against National Will or Counter-Will): การทำสงครามจิตวิทยาเพื่อต่อต้านเจตจำนงแห่งชาติเป็นเรื่องของกิจกรรมทางสงครามจิตวิทยาที่มุ่งกระทำแล้วส่งผลกระทบต่อเจตจำนงของชาติที่เป็นเป้าหมาย ให้เปลี่ยนไปจากเดิม ตัวอย่างที่เห็นได้ชัดสำหรับสงครามจิตวิทยาเพื่อต่อต้านเจตจำนงแห่งชาติได้แก่ การลากศพทหาร สหรัฐ ฯ ไปมาหลังจากการเข้าปฏิบัติของหน่วยเฉพาะกิจเรนเจอร์ (Task Force Ranger – จัดกำลังจาก หน่วยเดลต้ากับเรนเจอร์) ในกรุงโมกาดิสโช ประเทศโซมาเลีย (Mogadishu, Somalia) หรือที่รู้จักในชื่อ แบล็คฮอร์คดาวน์ (Blackhawk Down) เมื่อวันที่ 3 - 4 ต.ค. 36 ผลที่ตามมาคือ สหรัฐ ฯ สั่งถอนกำลังจากโซมาเลียในเวลาต่อมา หรือตัวอย่างของการสั่งถอนกำลังทหารฟิลิบปินส์จากการปฏิบัติหน้าที่ในอิรักของประธานาธิบดีแห่งฟิลิปปินส์ (อาร์โรโย) เมื่อ ก.ค. 47 ที่ผ่านมา หลังจาก ที่สำนักข่าว อัล-จาซีรา แพร่ภาพกลุ่มติดอาวุธจับคนงานฟิลิปปินส์เป็นตัวประกัน และขู่สังหารเหยื่อทิ้งหากมะนิลาไม่ถอนทหารออกจากอิรักภายใน 3 วัน

- ต่อต้านผู้บังคับบัญชาฝ่ายตรงข้าม (Against Opposing Commanders or Counter-Commander): การทำสงครามจิตวิทยาประเภทนี้เป็นการดำเนินกิจกรรมทางจิตวิทยาที่มุ่งกระทำต่อผู้นำประเทศหรือผู้นำทางทหารของประเทศเป้าหมาย ตัวอย่างของการทำสงครามจิตวิทยาประเภทนี้คือ การรณรงค์ในการทำสงครามจิตวิทยาของฝ่ายสหรัฐ ฯ ต่อประธานาธิบดีอิรัก ซัดดัม ฮุสเซ็น จนในที่สุดประธานาธิบดีซัดดัม ฯ กลายเป็นผู้ร้ายในสายตาชาวโลกในที่สุดทั้ง ๆ ที่เรา ๆ ท่าน ๆ ไม่รู้จักประธานาธิบดีซัดดัมเป็นการส่วนตัว

- ต่อต้านกองกำลังฝ่ายตรงข้าม (Against Troops or Counterforce): การทำสงครามจิตวิทยาประเภทนี้จะมุ่งกระทำต่อขวัญและกำลังใจฝ่ายตรงข้ามและเพิ่มพูนขวัญและกำลังใจให้กับกำลังฝ่ายเรา การทิ้งใบปลิว (leaflet) เพื่อให้ทหารฝ่ายตรงข้ามมีความสับสนและเสียขวัญ ดังตัวอย่างในสงครามเวียดนามที่มีการทิ้งใบปลิวให้กับทหารสหรัฐ ฯ โดยมีข้อความชี้ชวนให้ทหารสหรัฐ ฯ มีความสับสนว่า เขาเหล่านั้นจากบ้านจากเรือนมารบเพื่ออะไร ในเมื่อเวียดนามไม่ใช่แผ่นดินเกิดของเขา

- ความขัดแย้งทางวัฒนธรรม (Kulturkampf or Cultural-Conflict): (คำว่า Kulturkampf เป็นชื่อเรียกความขัดแย้งระหว่างรัฐเยอรมันกับศาสนาโรมันคาทอลิก เกี่ยวกับการควบคุมระบบการศึกษาและตำแหน่งศาสนา เกิดขึ้นระหว่างปี พ.ศ. 2416 – 2429) ความขัดแย้งทางวัฒนธรรมเป็นหนึ่งในกิจกรรมที่ถือว่าเป็นการดำเนินสงครามจิตวิทยา ความขัดแย้งทางวัฒนธรรมเป็นการทำกิจกรรมที่มุ่งสร้างความขัดแย้งให้เกิดขึ้นในสังคมใดสังคมหนึ่ง ๆ ด้วยการใช้วัฒนธรรมที่แตกต่างเข้าไปสร้างกระแสความขัดแย้งให้เกิดขึ้น โดยผลที่ตามมาหลังจากนั้นอาจจะเป็นในรูปของการครอบงำทางวัฒนธรรม ค่านิยม และแนวคิด หรือ อาจจะสร้างให้เกิดความสับสนวุ่นวายในสังคมนั้น ๆ แล้วใช้กำลังทหารเข้าแทรกแซง ตัวอย่างของการดำเนินสงครามจิตวิทยาลักษณะนี้คือ การให้ทุนการศึกษาจำนวนมากแก่ประเทศเป้าหมายเมื่อสมาชิกของประเทศนั้นมาศึกษาก็จะปลูกฝังแนวความคิดในเรื่องต่าง ๆ ทั้งทางตรงและทางอ้อม เมื่อนักศึกษาเหล่านั้นจบการศึกษากลับ

ประเทศ จะมีนักศึกษาบางส่วนที่ถูกครอบงำทาง ทัศนคติ แนวความคิด ค่านิยม ความเชื่อ ฯลฯ นำวัฒนธรรมที่ซึมซับกลับไปมีบทบาทในประเทศของตนต่อไป

5. สงครามแฮกเกอร์ (Hacker Warfare): การการโจมตีต่อระบบคอมพิวเตอร์ของฝ่ายพลเรือน มีลักษณะของการดำเนินการอยู่ 3 ลักษณะคือ (1) การโจมตีทางกายภาพ (physical) (2) การโจมตีทางไวยกรณ์ (syntactic) และ (3) การโจมตีทางความหมาย (semantic) โดยที่การโจมตีทางไวยกรณ์จะเป็นการดำเนินการหลักของสงครามแฮกเกอร์นี้ ส่วนการโจมตีทางกายภาพเป็นสิ่งที่เกิดขึ้นน้อยในการทำสงครามแฮกเกอร์ส่วนใหญ่แล้วจะเกิดขึ้นในสงครามการควบคุมบังคับบัญชา (C2 warfare) มากกว่า และการโจมตีทางความหมายจะเป็นเรื่องของสงครามไซเบอร์ (cyber war) การโจมตีทางไวยกรณ์ มีลักษณะเป็นการลักลอบเข้าไปเปลี่ยนแปลงขั้นตอนหรือกระบวนการทำงานหลักของระบบสารสนเทศนั้น ๆ เพื่อให้ระบบสารสนเทศนั้นทำงานไม่ถูกต้อง ยกตัวอย่างเช่น หลังจากที่เครื่องบินสอดแนม EP-3E (Airborne Reconnaissance Integrated Electronic System II, ARIES II) บินเข้าไปในน่านน้ำของจีน และถูกบังคับให้ลงจอดฉุกเฉินที่เกาะไหหลำ (Hainan) ในวันที่ 1 เม.ย.2544 หลังจากนั้นในวันที่ 1 – 8 พ.ค.2544 จีนได้เปิดสงครามแฮกเกอร์กับสหรัฐ ฯ ด้วยการใช้แฮกเกอร์เข้าไปแก้ไขเวบไซต์หน่วยงานราชการสหรัฐ ฯ ด้วยการแสดงธงชาติจีนที่เวบไซต์นั้น และสหรัฐ ฯ ตอบโต้กลับที่เช่นเดียวกันกับเวบไซต์ของจีน หรือ ในช่วงเดือน เม.ย. พ.ศ.2543 เวบไซต์ที่มีชื่อเสียงอย่าง Yahoo, Amazon, CNN.com, ZDNet ฯลฯ ถูกแฮกเกอร์ โจมตีด้วยรูปแบบที่เรียกว่า การยุติการให้บริการ (denial-of-service (DoS) attacks) ทำให้เวบไซต์เหล่านั้นไม่สามารถให้บริการใด ๆ กับลูกค้า ได้ส่งผลให้เกิดความเสียหายทางเศรษฐกิจอย่างใหญ่หลวง

6. สงครามสารสนเทศทางเศรษฐศาสตร์ (Economic Information Warfare: EIW): เศรษฐศาสตร์ถือเป็นพลังอำนาจของชาติที่ใช้ขับเคลื่อนรัฐ ดังนั้นการกระทำใด ๆ ที่ส่งผลกระทบต่อเศรษฐกิจของกลุ่มเป้าหมาย เช่น ประเทศ หรือ กลุ่มที่อยู่ตรงข้าม ย่อมสงผลกระทบโดยรวมต่อเป้าหมายนั้น ๆ สำหรับปัจจุบันการดำเนินสงครามสารสนเทศทางเศรษฐศาสตร์ มีอยู่ 2 ลักษณะคือ

- การปิดกั้นทางสารสนเทศ (Information Blockade): การดำเนินสงครามสารสนเทศลักษณะนี้คือ การกระทำทุกวิถีทางที่จะไม่ให้สารสนเทศต่าง ๆ ไหลออกและเข้าไปยังประเทศหรือกลุ่ม ที่เป็นเป้าหมาย เพราะในปัจจุบันสารสนเทศถือเป็นสิ่งที่สำคัญยิ่งต่อการดำเนินการทุกอย่าง เช่น ทางด้านเศรษฐกิจข่าวสารเรื่องของการปรับลดค่าเงินบาทส่งผลให้มีการซื้อเงินต่างชาติจำนวนมากเพื่อแสวงกำไรจากการ ปรับลดค่าเงินบาท หรือทางทหารข่าวสารของการปรับโครงสร้างกองทัพของกองทัพประเทศคู่ขัดแย้งส่งผลให้กองทัพของฝ่ายเราต้องปรับยุทธศาตร์ และแผนการป้องกันประเทศ ทำให้ต้องใช่งบประมาณมากขึ้น เป็นต้น

การปิดกั้นสารสนเทศนั้นทำให้ประเทศที่ถูกปิดกั้นตั้งอยู่บนความมืดมิดเปรียบเสมือนกับการปิดอ่าวในยุคล่าอณานิคม ที่ไม่สามมารถขนถ่ายสินค้าได้ การปิดกั้นสารสนเทศมีความจำเป็นต้องทำการปิดกั้นทั้งทางกายภาพ (physical) และการปิดกั้นการไหลเวียนของสารสนเทศ (information flow) โดยการปิดกั้นทางกายภาพเป็นเรื่องของการกระทำต่อระบบโทรคมนาคม สื่อสารมวลชน วิทยุ โทรทัศน์ ไม่ให้สามารถรับหรือส่ง

สารสนเทศได้ เช่นการให้แฮกเกอร์ใช้เทคนิคการยุติการให้บริการ (denial-of-service (DoS) attacks) ทำให้เวบไซต์ของตลาดหลักทรัพย์ของประเทศเป้าหมายไม่สามารถให้บริการข้อมูลการซื้อขายหุ้นได้

ส่วนการปิดกั้นการไหลเวียนของสารสนเทศนั้นเป็นการกระทำที่ไม่ต้องการให้สารสนเทศไหลเข้าและออกจากประเทศหรือกลุ่มเป้าหมาย เช่นการจำกัดสิทธิในการเข้าไปดูเว็บไซต์ การรับข้อมูลจากการกระจายเสียง การห้ามจำหน่ายหนังสือหรือสื่อสิ่งพิมพ์ต่าง ๆ ส่วนใหญ่แล้วการปิดกั้นเฉพาะการไหลเวียนสารสนเทศเป็นการกระทำยาก เพราะเป็นการยาก ที่จะปิดช่องทางการไหลของสารสนเทศทั้งหมด โดยเฉพาะอย่างยิ่งในปัจจุบันมีอินเตอร์เน็ต ดังนั้นการปิดกั้นทางสารสนเทศ ที่ได้ผลคือ การกระทำควบคู่ไปทั้งทางกายภาพและการไหลเวียนของสารสนเทศ

- การแผ่อิทธิพลทางสารสนเทศ (Information Imperialism): การดำเนินการสงครามสารสนเทศทางเศรษฐศาสตร์เป็นสิ่งที่มีบทบาทเป็นอย่างมาในปัจจุบัน โดยเฉพาะอย่างยิ่งการเกิดขึ้นของอินเตอร์เน็ตที่ช่วยให้การเข้าถึงข้อมูลเป็นไปได้อย่างแพร่หลาย การแผ่อิทธิผลทางสารสนเทศในปัจจุบันเป็นการกระทำร่วมกับการดำเนินสงครามจิตวิทยาด้วยการสร้าง ความขัดแย้งทางวัฒนธรรม (Kulturkampf or Cultural-Conflict) ด้วยการให้กลุ่มเป้าหมายถูกครอบงำโดยสารสนเทศ ตัวอย่างเช่น การสร้างภาพยนต์ของฮอลลิวูด (Hollywood) ของสหรัฐ ฯ แล้วส่งขายยังต่างประเทศ โดยที่เนื้อหาในภาพยนต์ที่สร้าง ใส่แนวคิดต่าง ๆ ลงไป พร้อมกับสร้างด้วยเทคนิคที่ทันสมัยทำให้ไม่มีออุตสาหกรรมทางภาพยนต์ของประเทศอื่น ๆ เข้ามามีส่วนร่วมในส่วนแบ่งตลาดนี้ได้ หรือ รูปแบบการดำเนินธุรกิจของบรรษัทข้ามชาติอย่างไมโครซอฟร์ (Microsoft) ที่พัฒนาระบบปฏิบัติการ (operating system: OS) อย่าง ไมโครซอฟร์วินโดว์ (Microsoft Windows) ให้มีความใช้งานง่าย เอื้ออำนวยความสะดวกต่าง ๆ รวมทั้งการเชื่อมต่อกับอินเตอร์เน็ต และระบบเครือข่ายต่าง ๆ ที่ทำให้ผู้ใช้งาน ๆ จนติด และในที่สุดคนจำนวนมากต้องใช้ ระบบปฏิบัติการวินโดว์จนติดไม่สามารถใชระบบปฏิบัติการอื่นได้ โดยในที่สุดประเทศอื่น ๆ ก็ต้องเป็นลูกค้าของไมโครซอฟร์ไปโดยปริยาย

7. สงครามไซเบอร์ (Cyber Warfare): คำว่าไซเบอร์หมายถึงอะไรก็ตามที่เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ ดังนั้นการดำเนินการสงครามไซเบอร์จึงเป็นเรื่องที่มีแนวทางในการดำเนินที่แตกต่างและหลากหลาย ซึ่งได้แก่

- การก่อการร้ายทางสารสนเทศ (Information Terrorism): เป็บลักษณะของการก่อความรุนแรง ความเสียหาย หรือก่อควมไม่สงบบนระบบเครือข่ายที่เชื่อมต่อกัน ตัวอย่างของการดำเนินการสงครามในลักษณนี้ได้แก่การใช้แฮกเกอร์เข้าไปเจาะระบบสารสนเทศของฝ่ายตรงข้ามแล้วทำให้ฝ่ายตรงข้ามสามารถทำงานหรือใช้สารสนเทศนั้นได้

- การโจมตีทางความหมาย (Semantic Attack): เป็นการใช้เทคนิคและความสามารถในการเป็นแฮกเกอร์แอบเข้าไปยังระบบสารสนเทศของฝ่ายตรงข้าม เพื่อเปลี่ยนความหมายที่แท้จริงของสารสนเทศที่นำไปใช้งาน เช่น การใช้แฮกเกอร์เจาะระบบตรวจจับของฝ่ายตรงข้ามแล้วทำการแก้ไขโปรแกรมให้ทำงานผิดผลาด โดยตรวจจับเครื่องบินฝ่ายเราได้แล้วแสดงเป็นเครื่องบินฝ่ายเดียวกันกับเครื่องบินฝ่ายตรงข้าม ทำให้ฝ่าย

ตรงข้ามไม่สามารถตรวจจับเครื่องบินของฝ่ายเราได้ เพราะนึกว่าเป็นเครื่องบินฝ่ายเดียวกัน หรือการใช้แฮกเกอร์เจาะระบบสารสนเทศทางทหารของฝ่ายตรงข้ามแล้วเข้าไปแก้ไขข้อมูลต่าง ๆ ที่ใช้ประกอบในการตัดสินใจ ทำให้มีการตัดสินใจที่ผิดพลาด เป็นต้น

- สงครามจำลอง (Simula Warfare): ในปัจจุบันความเจริญก้าวหน้าของเทคโนโลยีต่าง ๆ โดยเฉพาะอย่างยิ่ง เทคโนโลยีสารสนเทศที่มีการพัฒนาไปอย่างมากจนสามารถจำลองสถานการณ์ต่าง ๆ ได้มีความเหมือนจริง การทำการจำลองนี้จะสามารถช่วยในการวางแผนสำหรับการปฏิบัติการทางทหารได้อย่างมีประสิทธิภาพ ทำให้ผู้ที่มีหน้าที่ในการตกลงใจ (เป็นภาษาทหารทางพลเรือนจะใช้คำว่าตัดสินใจ) มองเห็นภาพของสนามรบ (battle visualization) อย่างมีความชัดเจนมากขึ้น ตัวอย่างของสงครามจำลองได้แก่ การฝึกบินเครื่องบินรบในเครื่องจำลองการฝึกบิน (flight simulator) การฝึกพลประจำรถถังในเครื่องจำลองการฝึกที่มีการจำลองการรบ เป็นต้น

- สงครามกิ๊บสันน์ (Gibson Warfare): ในสงครามกิ๊บสันเป็นแนวความคิดของ Martin Libiciki หลังจากได้ดูภาพยนต์เรื่อง ทรอน (TRON) ซึ่งเป็นเรื่องที่นำเค้าโครงมาจากหนังสือเรื่อง Neuromancer ในปี พ.ศ.2527 (1984) เขียนโดย William Gibson ที่เป็นเรื่องของการเปลี่ยนแปลงลักษณะของคนเข้าไปอยู่ในระบบคอมพิวเตอร์จากนั้นทำการสู้กัน แนวความคิดนี้สามารถพัฒนาไปสู่การนำลักษณะของคนเข้าไปอยู่ในคอมพิวเตอร์แล้วทำการสู้รบกันแทนที่จะทำการ
รบกันจริง

จากรูปแบบของสงครามสารสนเทศของ Martin Libiciki นั้นทำให้เราทราบถึงทิศทาง แนวคิด และความเป็นไปได้ที่จะมีการดำเนินสงครามสารสนเทศตามลักษณะดังกล่าว ถึงแม้แนวความคิดในบางเรื่องอาจจะต้องใช้เวลาในการพัฒนาถึงจะเป็นไปได้ หรือบางเรื่องอาจจะเป็นไปไม่ได้เลย แต่อย่างน้อยก็เป็นการบ่งชี้ได้ว่าสารสนเทศมีบทบาทที่สำคัญต่อการดำเนินสงครามในปัจจุบัน

อย่างไรก็ตามถึงแม้กองทัพไทยจะยังไม่ศักยภาพเพียงพอที่จะนำสงครามสารสนเทศมาใช้อย่างเต็มรูปแบบ แต่การเรียนรู้เป็นสิ่งที่จำเป็นและมีความสำคัญต่อการเตรียมการในการพัฒนากองทัพ ไม่ว่าจะเป็นทางด้านโครงสร้าง หรือกำลังพล เพราะเรื่องของความมั่นคงของชาติและการรักษาผลประโยชน์ของชาติในปัจจุบัน มีความซับซ้อนมากจนไม่สามารถใช้แนวความคิดแบบเดิม ๆ ที่กระทำมาตั้งแต่ในอดีตทำให้บรรลุวัตถุประสงค์ได้ ในปัจจุบันและในอนาคตอันใกล้นี้ การบูรณาการความรู้ ทฤษฎี แนวคิด และ หลักนิยม ต่าง ๆ เข้าด้วยกันถือเป็นสิ่งที่สำคัญที่สามารถช่วยให้กองทัพยังคงสามารถปฏิบัติหน้าที่เพื่อความมั่นคงและผลประโยชน์ของชาติไว้ให้ลูกให้หลานในอนาคตไว้ได้