

**حرب المعلومات كظاهرة استراتيجية:  
قراءة مفاهيمية في الظاهرة وأبعادها**

**Information warfare as a strategic phenomenon: a  
conceptual reading of the phenomenon and its  
dimensions**

صبرينة مزياني\*، جامعة ميله  
meziani.s@centre-univ-mila.dz

تاريخ القبول: 2025/11/21

تاريخ الاستلام: 2025/09/29

**ملخص:**

تهدف هذه الدراسة إلى تسليط الضوء على حرب المعلومات باعتبارها إحدى أبرز الظواهر الاستراتيجية التي فرضت نفسها في الآونة الأخيرة في بيئة الصراعات المعاصرة، وهذا بعد أن أصبحت المعلومة سلاحاً بالغ التأثير يفوق في كثير من الأحيان فعالية الأسلحة العسكرية التقليدية سواء من حيث القدرة على توجيه الرأي العام أو الضغط على الخصم والتحكم في مسار العلاقات.

ومن هنا، تأتي هذه الدراسة لتسليط الضوء على حرب المعلومات كأداة استراتيجية معاصرة وبيان أبعادها المختلفة، من خلال تقديم مقارنة مفاهيمية تحليلية تسعى إلى تفكيك مفهوم حرب المعلومات من خلال التركيز على تحول المعلومة إلى مورد استراتيجي أساسي يوازي في قيمته الموارد العسكرية.

\* المؤلف المراسل

**الكلمات المفتاحية:** المعلومة، حرب المعلومات، الصراعات المعاصرة، العلاقات الدولية، الظاهرة الاستراتيجية.

**Abstract:**

This study aims to shed light on information warfare as one of the most prominent strategic phenomena that has recently emerged in the context of contemporary conflicts. This is particularly true given that information has become a highly influential weapon, often surpassing the effectiveness of conventional military weapons in terms of its ability to influence public opinion, pressure opponents, and control the course of relations.

Hence, this study sheds light on information warfare as a contemporary strategic tool and demonstrates its various dimensions. It presents a conceptual and analytical approach that seeks to deconstruct the concept of information warfare by focusing on the transformation of information into a fundamental strategic resource, equivalent in value to military resources.

**Keywords:**

Information, Information Warfare, Contemporary Conflicts, International Relations , Strategic Phenomenon.

**مقدمة:**

ساهم ظهور ما يعرف بالحيز الافتراضي كفضاء معلوماتي له لغة وبروتوكولات خاصة في تعامل معه وتغيير خارطة حدود الدول و بروز مفهوم السيادة الالكترونية التي لا تستند إلى إطار جغرافي معين في بروز أنماط جديدة من الحروب كحرب المعلومات، ففي عصر الثورة الرقمية والتكنولوجية أصبحت المعلومات واحدة من أهم الأسلحة الاستراتيجية في الصراعات الدولية والإقليمية. لم تعد الحروب تقتصر على الأسلحة التقليدية مثل الدبابات والطائرات، بل امتدت لتشمل حرب المعلومات، التي تعتمد على استخدام البيانات والتكنولوجيا للتأثير على العدو أو تحقيق أهداف استراتيجية دون الحاجة إلى مواجهات عسكرية مباشرة.

فالفضاء الإلكتروني شكل مجالاً مهماً لحرب المعلومات بالإضافة إلى تغير المفاهيم التشغيلية المبتكرة والتكيف التنظيمي وزيادة هائلة في القدرة القتالية والفعالية العسكرية للقوات المسلحة، بمعنى، إجراء تغيير كبير في طبيعة الحرب في مستويات متعددة في وقت واحد من التكنولوجيا والثقافة، إلى التنظيم والاستراتيجية والتكتيكات، التدريب والعقيدة، والخدمات اللوجستية، فحرب المعلومات إذن ليست نسجاً من الخيال العلمي بل هي واقع مفروض وجزء من العمليات التي يجب التفاعل مع جانبيها الهجومي والدفاعي بغض النظر عن سياسة الدولة العسكرية.

وما يجب أن يكون واضحاً في هذه الدراسة أن موضوع حرب المعلومات هو مجال دراسة واسعة جداً بحيث لا يمكن لأي مستند واحد أن يغطي جميع جوانبه، لأن حرب المعلومات أصبحت اليوم ساحة صراع متكاملة تسعى من خلالها الأطراف المتنازعة إلى تحقيق التفوق والسيطرة الكاملة، ومن هنا تعالج هذه الدراسة الإشكالية التالية:

كيف يمكن فهم حرب المعلومات كظاهرة استراتيجية جديدة في بيئة الصراعات المعاصرة؟

وقد انبثق عن هذه الإشكالية التساؤلات الفرعية الآتية:

- كيف يمكن تحديد المقصود بحرب المعلومات في ظل التحولات التكنولوجية الراهنة؟
- ما هي أبرز التصنيفات التي اعتمدها الباحثون في دراسة ظاهرة حرب المعلومات؟
- ماهي الأنواع الأساسية التي تتضح من خلالها حرب المعلومات في البيئة الرقمية الحديثة؟

وبهدف الوصول إلى فهم دقيق للموضوع والإجابة عن التساؤلات المطروحة تم الاعتماد على ما يعرف بالمساندة المنهجية من خلال توظيف المنهج التاريخي بهدف رصد مختلف المراحل التاريخية والتطورات التي طرأت على مفهوم حرب

المعلومات، كما تم الاستعانة بالمنهج الوصفي والذي ساعدنا في وصف وتوضيح المفاهيم التي أثارها الموضوع خاصة مفهوم حرب المعلومات ووصف كل ما يتعلق به.

#### أولاً: السياق التاريخي والمفاهيمي لحرب المعلومات

يعد مفهوم حرب المعلومات *Information War* من المفاهيم غير المحدد بدقة والتي لا يوجد حولها تعريف جامع متفق عليه من قبل الباحثين والعسكريين، ويعود عدم الدقة في تحديد المفهوم إلى ما يسمى بثورة المعلومات التي أدت إلى التطور السريع والمستمر للفضاء السيبراني وأجهزة الكمبيوتر الصغيرة وتقنيات المعلومات المرتبطة بها، والتي انعكست بدورها على الحرب وأدت إلى تغير شكلها بسرعة مما جعلها تشكل تهديداً للعمليات العسكرية التقليدية (M. Taddeo & L. Floridi, p. 3)

وقبل تحديد المقصود من حرب المعلومات لابد من البحث في التطور التاريخي لبروز هذا المفهوم، فجدور حرب المعلومات قديمة وقد وصف سان تزو "Sun Tzu" عملية استغلال المعلومات في الحرب بقوله: "إن معرفتك لعدوك ومعرفتك لنفسك في مئات المعارك لن تجعلك تخسر أو تتعرض للخسارة، وعندما تتجاهل عدوك وتعرف نفسك فإن فرصتك في النصر أو الهزيمة متساوية، أما إذا تجاهلت نفسك وعدوك فتأكد أنك ستكون الخاسر في أية معركة"، وهذا الوصف الذي قدمه سان تزو يعبر عن أهم صفات حرب المعلومات السرية والمفاجأة (قطاي، 2017/2018، صفحة 117)

وكانت روسيا من الدول الأولى التي اهتمت بحرب المعلومات من خلال تدريس نظرية spetspropaganda "دعاية خاصة" التي اشتق منها لاحقا حرب المعلومات كموضوع منفصل لأول مرة في المعهد العسكري للغات الأجنبية سنة 1942 والذي يعرف اليوم باسم قسم المعلومات العسكرية واللغات الأجنبية بالجامعة العسكرية التابعة لوزارة الدفاع في الاتحاد الروسي، تقتصر مهمته على تدريب المتخصصين في تنظيم المعلومات الأجنبية والاتصالات العسكرية وتحليل المعلومات ومراقبة وتطوير المعلومات العسكرية، وهو الذي كان له دور كبير في تغيير نهج الحكومة الروسية تجاه موضوع حرب المعلومات (Darczewska, MAY 2014, p. 9).

أما استعمال المصطلح بهذه التسمية أول مرة كان عام 1975 بعد أن أدركت الدول المتقدمة تقنياً أهمية ذلك وسعت إلى تطبيقه في المجالات السياسية والعسكرية والاقتصادية والثقافية، ومع بداية التسعينات والتغيرات التي عرفها العالم مع نهاية الحرب الباردة وسقوط الاتحاد السوفياتي بدأ الاهتمام الفعلي بحرب المعلومات، وهو ما أكدته أندرو راثمل "*Andrew Rathmell*" عندما سمى المعلومات بأسلحة التخريب الشاملة) البداية، 2002، صفحة (114، حيث لم تعد الحرب تدار بالمال والطاقة والتواجد العسكري الفعلي للجنود كالسابق، بل أصبحت مرتبطة بالإلكترونيات والبيانات، بمعنى أن الحرب حالياً لا ترتبط بمن يمتلك أكبر عدد من الجنود والعتاد العسكري فقط بل ترتبط بمن يسيطر على المعلومات وكيف يمكن أن يوظفها بالشكل الذي يزيد من قوته.

ومن هنا ظهرت حرب المعلومات كأداة لزعزعة أمن الدول والمجتمعات بعد انتشار أنظمة الأسلحة والأجهزة العسكرية التي تعتمد فاعليتها على دقة وحداثة المعلومات المستخدمة لتشغيلها، بالإضافة إلى اعتماد أنظمة الأسلحة والأجهزة العسكرية في المستوى الوطني على أنظمة معلومات عالمية تسيطر عليها دول أخرى واستخدام العمليات المعلوماتية كسلاح ردع من قبل الدول التي تملك المعلومات التقنية وتسيطر على أنظمة المعلومات العالمية.

فضلا عن ذلك زادت خطورة هذه الحرب بعد الاعتراف بدور وسائل الإعلام كأدوات قتالية جديدة ذات فعالية كبيرة في التأثير على الأفكار مقارنة بتراجع دور الوسائل العسكرية كوسيلة وحيدة في إدارة الحروب، وقد ساعد في ذلك الانتشار الواسع لوسائل الإعلام الجديدة التي تعتمد على الفضاء الإلكتروني ما جعل العديد من الدول كروسيا والولايات المتحدة الأمريكية وبدرجة أقل كوريا الشمالية وإيران والصين تصنف حرب المعلومات ضمن استراتيجيتها لإدارة الحروب المستقبلية، هذا الذي يجعلنا نتساءل عن المقصود بحرب المعلومات *"Information War"*.

تعد المعلومات إحدى أهم الجبهات التي تدار من خلالها الحرب في القرن الواحد والعشرين، لأن المعلومات وفق ما نصت عليه العقيدة المشتركة لعمليات المعلومات في الجيش الأمريكي هي أداة للسلطة الوطنية لديها مكونات معقدة لا يوجد بها مركز تحكم واحد، فهي تعد مورداً استراتيجياً حيوياً للأمن القومي وتسمح بتشكيل ساحة حرب المعلومات (Fowler, 2009, p. 5)، ويشار إليها على أنها استراتيجية لاستخدام المعلومات لتحقيق ميزة تنافسية، بينما هناك من يعتبرها شكلاً من أشكال الحرب السياسية، كما يعتقد البعض أنها الوسيلة التي تحقق من خلالها الدول الأهداف الاستراتيجية وتعزز أهداف السياسة الخارجية، بينما يشير إليها البعض الآخر بحملة المعلومات المضللة (LB & ML, Information Warfare Conceptual Framework, 2018, p. 26860).

ولتجنب أي جدل وبهدف البقاء في ذات سياق الذي يركز على الكيفية التي يمكن استخدام بها المعلومة بهدف تغيير ديناميكيات الحرب وتعزيز الأهداف الجيوسياسية، يمكن تعريف حرب المعلومات على النحو التالي:

يعرف ألفين توفلر *"Alvin Toffler"* وهو من أوائل المفكرين الذين تناولوا مفهوم حرب المعلومات ضمن إطار تحليله لتحولات القوة في عصر المعرفة، ويقوم تعريفه لحرب المعلومات على التركيز على فكرة التأثير على المجتمع وأفكاره وفق منطق أن الحروب الجديدة هي حروب تدور في العقل قبل ساحة المعركة،

بمعنى التركيز على حرب المعلومات المتمحورة حول الجمهور، وهو ما أكدته في مذكرة السياسة رقم 30 "التي ألقاها على رؤساء الأركان في الجيش الأمريكي عام 1993 والذي حث من خلالها الجيش على ضرورة توسيع مفهومه لحرب المعلومات ليشمل العمليات النفسية التي تهدف إلى التأثير على العواطف؛ والدوافع؛ وسلوك الآخرين بالشكل الذي يؤدي إلى تطور الحرب التقليدية (Stein, 1998, p. 154).

- تعرف الوثيقة الاستراتيجية الروسية حول أمن المعلومات الدولية لعام 2011 حرب المعلومات بأنها: "نزاع بين دولتين أو أكثر في مجال المعلومات بهدف إلحاق الضرر بنظم المعلومات، بالإضافة إلى القيام بحملات نفسية جماعية ضد سكان دولة لزعزعة استقرار المجتمع والحكومة وإجبار الدولة على اتخاذ القرارات لصالح خصومها (Catherine A, 2018, p. 9) "

في ذات السياق، تعرف الصين حرب المعلومات من خلال ربطها بمفهوم حرب الشعب، التي تعني استخدام تكنولوجيا المعلومات من قبل مئات الملايين من الناس للتأثير على صناعات السياسة للخصم واكتساب ميزة ضد تهديد غير متماثل (LB & ML, Information Warfare Conceptual Framework, p. 26863). من خلال هذا التعريف يتضح بأن حرب المعلومات هي استراتيجية تستخدم مواقع متعددة بطريقة متزامنة لزعزعة استقرار المجتمعات والتلاعب بالصلة ما بين السكان والحكومات من خلال العمل على تآكل الثقة في المؤسسات؛ والأفكار؛ والقيم؛ وإحداث اضطراب في عملية صنع القرار والخلاف في المجتمع.

- أما جوزيف س. ناي "Joseph Nye" فيرى أن حرب المعلومات تتجاوز القوة الناعمة وهي ليست بظاهرة جديدة. فالتلاعب بالأفكار له تاريخ طويل وكان كل من هتلر وستالين رائدين في هذه الحرب من خلال الهجمات الإذاعية، ويضيف ناي قائلاً أنه وعلى الرغم من أن حرب المعلومات ليست جديدة إلا أن التكنولوجيا الإلكترونية تجعلها أرخص وأسرع وأبعد مدى فضلاً عن صعوبة اكتشافها وإمكانية إنكارها بسهولة (Information Warfare) "

وحسب مانويل ويك " *WIK Manuel* " فحرب المعلومات هي " مجموع النشاطات المستعملة لبلوغ امتيازات معينة، هذه الامتيازات تستخدم لأغراض استراتيجية تكتيكية أو عملياتية لربح صراعات عسكرية أو مدنية بطريقة منسقة باستعمال تكنولوجيا الإعلام) قطاي، صفحة (121 .

- وهي كذلك الحرب القائمة على استخدام والتوجيه الخاطئ للمعلومات في الصراعات والحروب بهدف خلق فوائد للسياسة الداخلية والخارجية، وكذلك في استخدام التحريض والدعاية لتعبئة سكان (White, 2018)، لذلك، تعد شكلاً من أشكال القوة السياسية وأداة جيوسياسية مهمة تسمح بمستوى عال من التلاعب والتأثير مع احتمال ضعيف للمواجهة العسكرية، يشار إليها باسم عمليات الإقناع أو التأثير، أو حتى العمليات النفسية، هذا الذي جعل الولايات المتحدة الأمريكية تؤكد على المعلومات كعنصر من عناصر القوة القتالية وسلاح حرب لا غنى عنه لذلك عملت على دمج الدعاية والعمليات النفسية وحرب المعلومات ضمن استراتيجيتها العسكرية (Catherine A, p. 1)، نستج من خلال هذا:

- بأن حرب المعلومات تشمل مكونين أساسيين، الأول تقني مرتبط بالبنية التحتية المستخدمة لتخزين ونقل وتلقي المعلومات (وسائل الإعلام)، والثاني بشري يتعلق بالتصورات المحيطة بمحتوى المعلومات.

- وهي استراتيجية من استراتيجيات إدارة الحرب الجديدة التي تستخدم الوسائل السياسية لإضعاف خصم المتفوق عسكرياً وتحقيق الأهداف دون إطلاق رصاصة واحدة من خلال: جمع المعلومات التكتيكية، التحقق من دقة المعلومات، نشر الدعاية والتضليل لإحباط المعنويات أو التلاعب بالخصم والجمهور وتقويض جودة معلومات الخصم.

- وإذا كان دور المعلومات في الحرب هو التأثير على القرارات الاستراتيجية أو التكتيكية بهدف تجنب المنافسة العسكرية المباشرة والحرب على الأرض، فإن وسائل الإعلام تساعد على تحقيق هذا الهدف باعتبارها جزءاً لا يتجزأ من عملية جمع المعلومات ومعالجتها ونشرها عبر أدواتها المختلفة التقليدية: التلفزيون الجرائد؛ والراديو؛ والشبكات الاجتماعية: صفحات الويب؛

والحسابات والمدونات والمنشورات ؛ الشبكات الإلكترونية لتحقيق الأثر الاستراتيجي بأقل تكلفة ومع الحد الأدنى من الخطر) أبو نصر، 2010 ، صفحة 31).

وإذا كانت الدول وباقي فواعل العلاقات الدولية من خلال شن الحروب تسعى لتحقيق ميزة تفوق دون تكلفة عالية وبأقل خسائر من الناحية البشرية فحرب المعلومات هي الوسيلة الأنسب لتحقيق هذه الأهداف، نظرا لجملة الخصائص التي تتميز بها والمتمثلة في ما يلي:

- الاعتماد على التكنولوجيا والمعلومة كسلاح غير مادي لإدارة الحروب، مما يجعلها أكثر فعالية في تقليل عدد المصابين والقتلى مقارنة بالحروب بمفهومها التقليدي؛

- القدرة على الوصول إلى الأهداف المحددة والمتعددة في مناطق مختلفة؛

- حرب المعلومات هي حرب لا تعترف بالحدود الجغرافية، بحيث يمكن تنفيذ أي هجوم في أي مكان في العالم دون الحاجة إلى الوجود المادي في مكان الهجوم؛

- تتميز حرب المعلومات كذلك بالغموض بحيث يصعب تحديد الفاعل الحقيقي عن الهجمات المعلوماتية؛

- حربٌ تتميز بتكاليف منخفضة وفعالية عالية حيث لا تحتاج إلى توظيف جيوش وأسلحة ضخمة بل تكفي بوجود خبراء وتقنيات حاسوبية متقدمة.

لكن من ناحية أخرى فقد أعطت حرب المعلومات ومن خلال الخصائص التي تتمتع بها فرص للمنظمات الإجرامية أو الإرهابية بشن الحروب وزعزعة أمن الدول والأفراد، خاصة وأن المعلومة تعد سلاح ذو حدين يصعب التحكم فيه، فإذا تم استعمالها بشكل فعال وبطريقة صحيحة يؤدي هذا إلى تحقيق انتصارات تكتيكية مما يجعلها بنفس أهمية العمل العسكري، لكن حدوث سوء في إدارة هذه المعلومات يحول النجاح التكتيكي إلى فشل استراتيجي.

## ثانياً: تصنيف حرب المعلومات:

يعد تصنيف حرب المعلومات من الركائز الأساسية لفهم طبيعتها المركبة وأبعادها المتعددة، بحيث لا يمكن دراسة حرب المعلومات كظاهرة استراتيجية انتشرت بشكل كبير نتيجة التطورات المتسارعة في تكنولوجيا الاتصال والمعلومات دون التطرق إلى الجزء المتعلق بتصنيفها، خاصة وأن تصنيف حرب المعلومات لا يهدف إلى ضبط المفهوم وتوضيح مكوناته فقط بل يساهم في توضيح خطورة الظاهرة على أمن الدول والأفراد.

لذلك، تم الاعتماد في هذه الدراسة على مجموعة من التصنيفات التي تم وضعها من قبل المهتمين بحرب المعلومات، والمتمثلة في ما يلي:

### أ: تصنيف أندرو راثمل "Andrew Rathmell":

يصنف راثمل حرب المعلومات إلى مجموعة من المستويات والمتمثلة في ما يلي:

- المستوى الأعلى: وهو صراع الأفكار لعقل الخصم، وهذا يشمل مدى واسع من العمليات النفسية والإعلام والأساليب الدبلوماسية والعسكرية للتأثير على عقل الخصم سواء كان عسكرياً أو من السكان عامة، وعادة ما يتم التأثير ضمن هذا المستوى بما يعرف بـ "القوة تخريبية" الحرب النفسية والقائم على انتشار العمليات النفسية كقوة تخريبية المكون الرئيسي في حرب المعلومات والتي تعني: استخدام أي تدابير غير فتاكة للتأثير على معنويات ومواقف أي مجموعة من أجل تحقيق الأهداف العسكرية والتي عادة ما يشار إليها بحروب الأفكار التي تعني: الصدام بين الرؤى والمفاهيم والصور. (Catherine A, p. 9)

كما تؤدي العمليات النفسية إلى زعزعة استقرار الوضع العسكري للدولة من خلال التقارير التي تنشرها وسائل الإعلام ما يحول دون تحقيق أهدافها الوطنية، مثل ما حدث في أبريل عام 1993 عندما قدم الصحفي بريطاني مارتن بيل "Martin Bell" تقريراً إخبارياً نقل فيه مشاهدة الإبادة التي تحدث في بوسنة، كذلك خروج الولايات المتحدة الأمريكية من مقديشيو بعد مقتل 18 من جنود الجيش وسحبهم في الشوارع، بهذا تجد الجيوش نفسها أمام ضغوط الحرب الإعلامية لأن الحروب الحديثة تدمج بين معركة السلاح ومعركة

الأفكار (LB & ML, 2018) ، ليوضح هذا أن وسائل الإعلام من خلال دورها كقوة سردية وتخريبية قد جعلت من السياسة وسيلة أخرى لإدارة الحرب ، وليس كما قدمها كارل فان كلازفيتز "carl von clausewitz" على اعتبار أن الحرب هي استمرار لسياسة بوسائل أخرى (Kanwal, 2015, p. 89) .

2- المستوى الثاني: وهو يمثل مضامين إدارة خطورة ثورة المعلومات والتي تهدف إلى السيطرة على المعلومات.

3- المستوى الأدنى: ويشمل التصدي لتدفق المعلومات ونشاطاتها ويتراوح بين الهجمات الإلكترونية مثل القرصنة والتدمير المادي والتضليل.

**ب- تصنيف وين شوارتو Winn Schwartau:**

أما وين شوارتو "Winn Schwartau" في كتابه "Information warfar: *chaos on the Electronic Superhighway*" ، والذي تنبأ فيه بأن الفضاء الإلكتروني سيصبح ساحة حرب جديدة تُدار فيها الصراعات السياسية والعسكرية والاقتصادية (Winn , 1994) ، فذهب إلى أبعد من ذلك ويصنف حرب المعلومات إلى ثلاث مستويات مختلفة بناءً على طبيعة الهيئة المستهدفة من هذه الحرب:

1- حرب المعلومات الشخصية: يتم ضمن هذا المستوى من حرب المعلومات بالهجوم على خصوصية الأفراد في الفضاء المعلوماتي بالتتصت عليهم ومراقبة شؤونهم عبر البريد الإلكتروني ويتم استهداف شخصيات ذات مستوى رفيع من سياسيين وعسكريين ورجال المال والأعمال ، وتتم من خلالها سرقة البيانات المالية ونشرها عبر الشبكة الإلكترونية للمعلومات أو القيام بمراقبة البريد الإلكتروني والعبث بالسجلات الرقمية وتغيير مدخلاتها ، وتمتلك الولايات المتحدة الأمريكية أقوى البرامج في التجسس على البريد الإلكتروني وهو برنامج *carnivore* وهو البرنامج القادر على تعطيل وتدمير أنظمة المعلومات والتي قد تصل إلى تعطيل العمليات العسكرية ، فإذا استطاعت هذه البرامج التجسسية من الوصول إلى المعلومات المرتبطة بمكان وزمان الهجوم وتكتيكاته ونشرها هذا من شأنه أن يؤدي إلى خسارة استراتيجية وتكتيكية وزعزعة الاستقرار ،

لأن نجاح العمليات العسكرية مرهون بتوفر أحد أبرز مبادئ الحرب وهو السرية (Scholtz, 1998, p. 239).

- 2- حرب المعلومات بين الشركات والمؤسسات: تدور الحرب ضمن هذا المستوى في إطار المنافسة بين الشركات والمؤسسات مبدأها كل شيء مشروع في إطار تعطيل المنافس وتحقيق ميزة التفوق عليه في الأسواق، ويتم هذا من خلال:
  - اختراق النظام المعلوماتي لمنافس وتعطيله باستخدام فيروس إلكتروني.
  - تدمير البيانات الخاصة بالمنافس أو استبدالها ببيانات خاطئة.
  - رفع من الشك لدى المستثمرين والمتعاملين مع الشركة أو المؤسسة المنافسة (BAUMARD, 2002, p. 41).

وهنا نلاحظ وجود ما يعرف بحرب المعلومات الاقتصادية والتي يتم تطبيقها من خلال ما يلي:

- الحصار المعلوماتي: وذلك بمنع الولوج لوسائل ومنتجات المعلومة بقطع المبادلات واحتكار المعلومة الإلكترونية وهو أسهل من الحصار على السلع المادية.
- الإمبريالية التقنية للمعلومة: الاستفادة من التطورات التكنولوجية في القطاعات الاقتصادية بما في ذلك سوق العمل، الاستهلاك والثقافة) قطلا في، صفحة(137

- 3- حرب المعلومات العالمية: يدور هذا المستوى من الحرب بين الدول كما قد ينشأ بين القوى الاقتصادية العالمية ضد دول بعينها، وتعد شبكات التواصل الاجتماعي أبرز الأدوات المستخدمة ضمن هذا المستوى من الحرب كونها جعلت من الممكن استهداف الخصم مهما كانت طبيعته دولة؛ فرد؛ مؤسسة بشكل سريع وسري (Greenbery , SooHoo , & Seymour E , 1998, pp. 14-20).

#### ج: تصنيف وزارة الدفاع الفرنسية:

تصنف وزارة الدفاع الفرنسية حرب المعلومات إلى:

- 1- الحرب من أجل المعلومات، وهي حرب تهدف إلى الحصول على المعلومات عن أهداف العدو وقدراته واستراتيجياته لتمكن من الدفاع عن النفس.

2- الحرب ضد المعلومات، وتتعلق بحماية الدفاع عن المعلومات ونظمها لدينا وتدمير (الهجوم) معلومات وأنظمة العدو.

3- الحرب من خلال المعلومات وهو استخدام المعلومات كمصدر هام وحيوي للسيطرة على المعلومات الخاصة بالعدو، وتحسين الحصانة المعلوماتية والدفاعية المعلوماتية لدينا) قطاعي، الصفحات(125-126 .

### ثالثاً: أنواع حرب المعلومات:

هناك ثلاث عناصر أساسية يتم من خلالها تقسيم حرب المعلومات إلى مجموعة مختلف من الأنواع، وتتمثل هذه العناصر في ما يلي: طبيعة تفاعلات بين الهجوم والدفاع؛ وساحة تفاعلات وهي المعلومات؛ ومستوى التفاعل والذي يقصد به طبيعة الفاعل خاصة وأنه لم تعد الدول اللاعب الوحيد المتحكم في تفاعلات النظام الدولي فهناك الجماعات السياسية والعرقية والدينية والجريمة المنظمة والمنظمات الدولية وعبر الوطنية، وحتى الأفراد الذين تم تمكينهم بواسطة تكنولوجيا المعلومات وقادرون على الانخراط في هجمات المعلومات وتطوير استراتيجيات المعلومات لتحقيق غاياتهم، وبهذا تكون حرب المعلومات عبارة عن نوعين وهما حرب معلومات الهجومية وحرب معلومات الدفاعية، وفي ما يلي توضيح لهذين النوعين:

#### أ: حرب المعلومات الهجومية: *Offensive Information warfare*

تعرف حرب المعلومات الهجومية على أنها: أي إجراء يتم اتخاذه لتقويض أو تدمير البنية التحتية للمعلومات الخاصة بالعدو وأنظمتهم (Emmett, 1996, p. 82)، وبالتالي تتضمن حرب المعلومات الهجومية الهيمنة على معلومات العدو وأنظمة معلومات الكمبيوتر وأنظمة التحكم بالإضافة إلى وضع الخطط واتخاذ كافة الإجراءات لإتلاف أو سرقة أو تدمير المعلومات المسجلة أو متداولة على أنظمة الحواسيب لدى العدو ولمختلف أنواع القوات البرية؛ البحري؛ والجوية وعلى مختلف المستويات الاستراتيجية؛ التكتيكي؛ والقيادة والسيطرة، و قد تردع حرب المعلومات الهجومية الوقائية أي عدو محتمل وتوفر نفوذاً قسرياً لحل الأزمات

والصراعات (Devries, 1997, p. 3) ، ويتوقف نجاح حرب المعلومات الهجومية على:

- . المعرفة الدقيقة للبنية المعلوماتية لدى العدو.
- . أسلوب تدفق المعلومات خلال قنوات الاتصال لدى العدو .
- . المعدات المستخدمة لدى العدو والمواصفات الفنية.
- . التطبيقات والبرامج الأساسية المستخدمة في النظم الآلية لدى العدو.
- . المتابعة المستمرة الي تحديث لتلك البيانات وملاحظة تطوره.
- من خلال هذا يتضح أن أهداف حرب المعلومات تتمثل في:
- 1- منع تدفق المعلومات بين قادة الخصم ووحداتهم ، ويمكن تحقيق هذا الهدف من خلال الوسائل الآتية:
- أ . العمليات الجوية لتدمير مراكز انظمة القيادة والسيطرة .
- ب . العمليات الخاصة لقطع خطوط الاتصالات وتخريب محطات الإعادة.
- ج . التشويش الإلكتروني على اتصالات الخصم.
- 2- تشويه معلومات الخصم عن ميدان المعركة ويكون ذلك بإحدى الوسائل الآتية:
- أ. ادخال أهداف وهمية في رادارات الخصم بواسطة الخداع الإلكتروني.
- ب . تنفيذ الخداع العسكري في مسرح العمليات كتحريك بعض عناصر القوة الى مناطق بعيدة عن الاتجاه الفعلي للعملية وتطبيق اجراءات الإخفاء والتمويه.
- ج . اختراق شبكات الحاسب الآلي التابعة للخصم وحقنها بمعلومات غير دقيقة.

#### ب: حرب المعلومات الدفاعية: defensive information warfare

يستخدم مصطلح "حرب المعلومات الدفاعية" للإشارة إلى جميع الوسائل الوقائية المتوفرة للحد من أعمال التخريب التي قد تتعرض لها نظم المعلومات والإجراءات المتخذة للدفاع ضد الهجمات المعلوماتية ، أي الهجمات على صانعي القرار والمعلومات والعمليات القائمة على المعلومات التي يعتمدون عليها خاصة وأن هذه الهجمات يمكن أن يتم إطلاقها خلال أوقات السلم على أهداف غير

عسكرية من قبل مجموعات غير عسكرية أجنبية ومحلية على حد سواء (ALBERTS, 1996, p. 2)، ليشير بذلك الدفاع هنا إلى منع الهجمات وصد الهجمات والسيطرة على الضرر الناجم عن الهجمات.

وتتم العملية الدفاعية من خلال مجموعة من الخطوات المتمثلة في ما يلي:

- التحذير والتنبيه: وتعتبر هذه أول خطوة في إطار حرب المعلومات الدفاعية، لأنه دوما ما يسعى الطرف المستهدف لتوقع حدوث الهجوم قبل وقوعه في مراحله الأولى لتجنب الكثير من الأضرار المحتمل حدوثها خاصة إذا ما كان الطرف المستهدف على درجة عالية من الأهمية سواء السياسية أو العسكرية أو الاقتصادية أو الأمنية...إلخ.

- المنع والوقاية: يتم فيها منع حدوث المخاطر من البداية، وذلك بحماية نظم المعلومات من وصول المهاجمين إليها كاتخاذ إجراءات اخفاء المعلومات "Hiding Information" وتشفيرها "Coding"، بالإضافة إلى اتباع إجراءات التحكم في الدخول إلى نظم المعلومات "Control A".

- كشف الاختراقات وكيفية التعامل معها: ويشمل هذا على استخدام وسائل تقليدية كاميرات مراقبة نظم المعلومات للكشف عن الدخول غير المصرح به للمبنى الذي يضم نظم معلومات المطلوب حمايته، إلى جانب وسائل تقنية جاسوسية تتمثل في برامج وأجهزة تقوم بمراقبة العمليات التي تنفذها نظم المعلومات لكشف عن العمليات غير المصرح بها) عبد الصادق، صفحة(6).

من خلال ما سبق ذكره يمكننا تحديد وسائل حرب المعلومات

الدفاعية كالآتي:

أ. الحماية الإلكترونية: وهذه الوسيلة بدورها ذات شقين الأول هو إجراءات حماية الكترونية وقائية تطبق في السلم والحرب لحرمان الخصم من التقاط البث الصادر من أجهزة الاتصالات والرادارات التابعة للدفاع، أما الشق الثاني فهو إجراءات الحماية الإلكترونية العلاجية طبق في حال تعرض الأجهزة التي للهجوم الإلكتروني لتجاوز أثاره أو تقليله.

ب. الإجراءات الأمنية "Information Security": وتشمل هذه أمن المعلومات الذي يعد بمثابة تدابير لحماية سرية وسلامة المعلومات من مجمل الأخطار المتوقعة الداخلية والخارجية، وبالتالي فهي تهدف إلى منع وصول الخصم إلى معلومات المدافع وأنظمتها المعلوماتية، ويتم هذا من خلال تطبيق النظام المتعلق بالتعريف بالشخص المستخدم لتحديد الهوية والمصادقة عليه *identification and authentication*، أو من خلال مراقبة الاستخدام وتتبع سجلات الأداء بهدف مراقبة العاملين وتحديد هوية القائم بالعمل والوقت) عرب، الصفحات (48-50).

ت. العمليات النفسية المضادة *Psyops – Counter* : الغرض منها هو اكتشاف مثل تلك العمليات التي يمارسها المهاجم والعمل على مواجهتها باستخدام الوسائل المختلفة المتاحة والعمل على رفع المعلومات ومقاومة الإشاعات. ث. الخداع العسكري *Deception Military* : تشتمل على عمليات الإخفاء والتمويه وتحريك بعض الوحدات في اتجاهات واقعية ولكنها بعيدة عن الاتجاه الفعلي للهجوم، بالإضافة إلى قيام القادة السياسيين والعسكريين بالتصريح والادلاء بمعلومات غير صحيحة عن الوضع العسكري.

### خاتمة

من خلال ما تم عرضه في سياق هذه الدراسة، تبين أن حرب المعلومات تمثل اليوم أحد أبرز مظاهر الحروب الحديثة، حيث ساهم التطور التكنولوجي والمعلوماتي في توفير أدوات فعالة كان لها الدور البارز في انتشارها كظاهرة العصر الحالي وساحة معركة جديدة توظف فيها الجهات الفاعلة كل إمكانياتها الرقمية والاستخباراتية من أجل تحقيق ميزة تفوق على الخصم، وهذا ما جعل حرب المعلومات تتحول إلى تهديد أمني خطير يهدد أمن الدول خاصة مع تمكن التنظيمات الإرهابية من استغلال هذا التطور لتوسيع مجال نشاطها، وعليه فإن مواجهة هذا النوع من الحروب تستدعي تعزيز التعاون الدولي وتطوير استراتيجيات وقائية وأمنية قادرة على الحد من مخاطرها وحماية المجتمعات من تداعياتها المتنامية.

- وبناءً على ذلك، تقدم هذه الدراسة مجموعة من التوصيات المتمثلة في ما يلي:
- وضع قواعد ومعايير دولية تنظم استخدام المعلومات والتكنولوجيا في الحروب.
  - وضع استراتيجيات وطنية للأمن السيبراني تركز على تعزيز الحماية.
  - تطوير القدرات التقنية والبشرية في مجال الأمن الرقمي.
  - تطوير سياسات وقائية لحماية البنى التحتية من الهجمات المعلوماتية.
  - وضع آليات دقيقة لتعقب الأنشطة الرقمية للتنظيمات الإرهابية وتجهيف مصادر تمويلها الإلكتروني.
  - تدريب الكوادر الوطنية في مجال الأمن السيبراني والذكاء الاصطناعي.
  - تشجيع الدراسات الأكاديمية حول حرب المعلومات وأهميتها تأثيرها في مسار الحروب والصراعات.

#### قائمة المراجع:

- *Information Warfare*. (n.d.). Retrieved 9 15, 2025, from ECPS: European Center for Populism Studies: <https://www.populismstudies.org/Vocabulary/information-warfare/>
- حكيم قطافي. (2017/2018). إدارة حرب المعلومات : دراسة لحرب لبنان 2006 عبر نات " دراسة وصفية تحليلية . أطروحة دكتوراه علوم في علوم الاعلام والاتصال، ص. 117 الجزائر : جامعة الجزائر 3 ، كلية علوم الاعلام والاتصال.
- ذياب البداينة. (2002). *الأمن وحرب المعلومات*. دار الشروق للنشر والتوزيع.
- يونس عرب. *بلا تاريخ .(أمن المعلومات : ماهيتها وعناصرها واستراتيجيتها*.
- ALBERTS, D. (1996). *Defensive Information Warfare*. National Defense University, NDU Press Book,.
- BAUMARD, P. (2002). les limites d'une économie de la guerre cognitive. Dans Lavauzelle, *la guerre cognitive l'arme de la connaissance* (p. 41). Paris.
- Catherine A. (2018). *Theohary, Information Warfare: Issues for Congress*. Congressional Research Service Report.
- Darczewska, J. ( MAY 2014). *The anatomy of Russian information warfare the Crimean operation, a case study* . Centre for Eastern Studies.

- Devries, A. D. (1997). *Information Warfare and Its Impact on National Security*. Naval war college.
- Emmett, E. D. (1996). *Attacking the infrastructure: exploring potential uses of offensive information warfare*. California: Naval Postgraduate School,.
- Fowler, J. (2009). *New Media Warfare: Tweeting From the Front Lines*. The New School.
- Greenberg , L., SooHoo , K., & Seymour E . (1998). *Information Warfare and International Law*. National Defence University Press.
- Kanwal, G. (2015). Cyber Security: Avoiding a 2020 Pearl Harbour. *CLAWS Journal*, p. p89.
- LB , M., & ML, K. (2018, May). Information Warfare Conceptual Framework. *International Journal of Recent Scientific Research*, Vol. 9(Issue5), p. 26860.
- LB , M., & ML, K. (2018, May). Information Warfare Conceptual Framework. *International Journal of Recent Scientific Research*, Issue5.
- M. Taddeo, & L. Floridi. (n.d.). *The Ethics of Information Warfare – An Overview*. University of Warwick, University of Oxford.
- Scholtz, L. (1998). The media and the military: Allies or adversaries? *South African Journal of Military Studies*,, No 2, p. 239.
- Stein, G. (1998). Information War - Cyber war – Netwar . In B. Schneider , & L. Grinter, *Battefield of the Future 21st Century - Warfare Issues* (p. p154). Alabam: Maxwell Air Force Base, Air University Press.
- White, S. (2018, November 12). *Information Warfare in the Digital Age: A Study of #SyriaHoax*. Retrieved september 15, 2025, from techscience: <https://techscience.org/a/2018111302/>
- سامية أبو نصر .(2010). الإعلام والعمليات النفسية في ظل الحروب المعاصرة واستراتيجية المواجهة) المجلد .(1 القاهرة: دار النشر للجامعات.
- عادل عبد الصادق). بلا تاريخ .(القوة الإلكترونية أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني مجلة السياسة الدولية ، صفحة.6