مركز البيدر للدراسات والتخطيط
Al-Baidar Center For Studies And Planning

# تسليط الضوء على الحروب الحديثة
## في مجال العلاقات الدولية مفهوماً ومضموناً

مجموعة من الباحثين

ترجمة وتحرير: مركز البيدر للدراسات والتخطيط

**الملخص**

المقال يسلط الضوء على الحروب الحديثة وما تحمله من مفهوم ومحتوى، بما في ذلك الحرب الإلكترونية والحرب المعرفية وحرب المعلومات والحرب الهجينة. في هذا الصدد ، فإنَّ السؤال الرئيس للمقال عن العناصر المشتركة في مفهوم الحروب الحديثة؟ رداً على هذا السؤال، فقد تم تقييم الفرضية القائلة بأنَّ التكنولوجيا هي العنصر المشترك الأكثر أهمية في جميع الحروب الحديثة. بعبارة أخرى إنَّ ما تسبب في نشوء حروب جديدة مثل الحرب الإلكترونية والحرب المعرفية والحرب الهجينة، أو تسبب في تطور الحروب الكلاسيكية مثل الحرب المعلوماتية (الاستخباراتية) إلى أبعاد جديدة، هو الثورة التي حصلت في مجال التكنولوجيا ولاسيما الثورة السيبرانية. في هذا الصدد، فإنَّ مستوى الاستعداد للتعامل مع مثل هذه الحروب يعتمد إلى حدٍ كبير على مستوى المعرفة والتكنولوجيا لكل دولة. بالنظر إلى ذلك، يسعى المقال بجانب تحليل المفهوم والمحتوى الخاص للحروب الجديدة، إلى مناقشة أربعة مجالات جديدة للحرب بما في ذلك المجالات السيبرانية والمعرفية والمعلوماتية والهجينة إذ يجدر الانتباه إلى الدور البارز للتكنولوجيا في أبعادها المختلفة. إنَّ آلية البحث المعتمد في هذا المقال هي الطريقة الوصفية والتحليلية التي تستند إلى مصادر المكتبات والإنترنت.

**المقدمة**

إنَّ الثورة في مجال الاتصالات والمعلومات وخاصة الثورة الإلكترونية الواسعة النطاق، أدّت إلى تغييرات جمّة في الأبعاد الاجتماعية والسياسية والاقتصادية وبالطبع العسكرية. في الواقع ، فإنَّ الثورة التكنولوجية، وخاصة الثورة الإلكترونية، مارست تأثيرها على ظاهرة الحرب والدفاع، لدرجة أنه من السهل تقييم الثورة السيبرانية باعتبارها أكبر نقطة تحول وأكثرها خصوصية في الدراسات الأمنية والاستراتيجية والحربية والدفاعية. في هذا الصدد، أدّت الثورة الإلكترونية في مجال الحرب والدفاع إلى نشوء حروب جديدة مثل الحرب الإلكترونية والحرب المعرفية والحرب الهجينة، حيث تُستخدم التكنولوجيا لتحقيق النتائج والأهداف المرجوة .

إنَّ التفوق والغلبة في هذه المعارك والحروب من نصيب الدول التي لها تفوق في مجال العلوم والتكنولوجيا، إذ إنها تتمكن من تحقيق أهدافها الاستراتيجية بسهولة أكبر بكثير وبتكلفة أقل من ذي قبل. الواقع هو أنَّ التكنولوجيا تمكنت من إعطاء أبعاد جديدة للحروب الكلاسيكية. على سبيل المثال، فقد انتشرت الحرب المعلوماتية بين الدول إنطلاقاً من المجالات العسكرية إلى مجالات أخرى مثل السياسية والاقتصادية والثقافية والاجتماعية، ومن المستوى التشغيلي والتكتيكي

إلى المستوى الاستراتيجي وذلك تحت تأثير ثورة الاتصالات والمعلومات وخاصة الثورة الإلكترونية. بناءً على ذلك فقد ساهم العلم والتقنيات الجديدة بتغير مفهوم الحرب، بحيث لا يمكن أنْ تكون مفردة الحرب لوحدها تعبيراً عن كل ما يقع في إطار الحرب. ولهذا السبب تُقيَّد مفردة الحرب بقيود أخرى مثل السيبرانية والمعرفية والمعلوماتية والهجينة لتحديد نوع وطبيعة الحرب المقصودة.

بالنظر إلى هذه القضايا، فإنَّ الهدف من هذا المقال هو شرح مفهوم ومحتوى الحروب الحديثة التي تندرج ضمن إطار ثورة الاتصالات والمعلومات وبخاصة الثورة الإلكترونية، مثل الحرب الإلكترونية والحرب المعرفية والحرب الهجينة. في هذا السياق، فإنَّ السؤال الرئيس للمقال هو عن العناصر المشتركة في مفهوم الحروب الحديثة؟

رداً على هذا السؤال، فقد تم قياس الفرضية القائلة بأنَّ التكنولوجيا هي العنصر المشترك الأكثر أهمية في جميع الحروب الحديثة. وبمعنى آخر فإنَّ ما تسبب بالتالي في نشوء حروب جديدة مثل الحرب الإلكترونية والحرب المعرفية والحرب الهجينة، أو تسبب في تطور الحروب الكلاسيكية مثل الحرب المعلوماتية إلى أبعاد جديدة، هو الثورة في مجال التكنولوجيا، ولا سيما الثورة الإلكترونية. في ضوء ذلك، يعتزم هذا المقال مناقشة أربعة مجالات جديدة للحرب، بما في ذلك المجالات السيبرانية والمعرفية والمعلوماتية والهجينة، على أنْ يضع في الاعتبار الدور البارز للتكنولوجيا في أبعادها المختلفة أثناء تحليل مفهوم الحروب الحديثة ومضامينها.

## 1. الإطار النظري

مما لاشك فيه أنَّ إحدى أهم سمات العالم المعاصر هي «ثورة المعلومات والاتصالات السيبرانية»[1]ضمن ما يشار إليه بـ «الثورة الإلكترونية»[2]. بالطبع، في الماضي وخصوصاً في النصف الثاني من القرن العشرين، كانت تقنيات الاتصالات والمعلومات موجودة على مستويات مختلفة، وخلال العقدين الماضيين فقط وبسبب الثورة التي حدثت في المجال السيبراني، تم تحقيق تلك التقنيات بالكامل ضمن ما يشار إليه باسم «القرية الكونية»[3]. في هذا السياق ، يمكننا الرجوع إلى المعلومات والإحصاءات الدولية المتاحة التي تؤكد ذلك. وَفقَ الإحصاءات الدولية، فقد تضاعف استخدام الإنترنت أكثر من أربعة أضعاف في السنوات العشر الماضية. هذا ويوجد حالياً ما يقرب من 5 مليارات مستخدم فعّال للإنترنت في جميع أنحاء العالم ( Internet Users, 2021:1) .

1. Cyber Communication Information Revolution
2. Cyber Revolution
3. Global village

ووَفقاً لأحدث الإحصاءات الدولية، فإنَّ أكثر من 40٪ من سكان العالم لديهم اتصال يومي ومستمر بالإنترنت. هذا في الوقت الذي كانت هذه النسبة في عام 1995 حوالي 1 ٪ . تُعدُّ الزيادة بنسبة 39٪ في عدد مستخدمي الإنترنت أحد المصاديق لما يسمى بالثورة الإلكترونية. كما يجب إضافة معدل انتشار الهواتف المحمولة وأجهزة التلفزيون الرقمية والذكية إلى هذه الإحصاءات. بحسب آخر الإحصاءات الدولية الصادرة عن «الاتحاد الدولي للاتصالات»[4] هناك أكثر من 7 مليارات هاتف نقال فعّال في جميع أنحاء العالم، وهو ما يمثل نفوذاً بنسبة 5/95 ٪. بمعنى آخر، فإنَّ 5/95 ٪ من سكان العالم يستخدمون الهواتف المحمولة ، ونحو 3/5 مليار من تلك الهواتف ذكية. بالإضافة إلى ذلك، فقد أحدثت الثورة الإلكترونية تغييرات جوهرية في مختلف جوانب الحياة البشرية. في الواقع فإنَّ تأثير الثورة السيبرانية على الأبعاد السياسية والاقتصادية والاجتماعية والثقافية يصل إلى حد يفوق التأثيرات التي تركتها الثورتان الصناعيتان الأولى والثانية وحتى ثورة الاتصالات والمعلومات. إنَّ مستوى وعمق تأثير الثورة السيبرانية على المجتمعات بلغ حداً يرى البعض أنه يجب أنْ يسمى القرن الحادي والعشرون بالقرن السيبراني. بالإضافة إلى ذلك، فقد تركت الأجواء السيبرانية تاثيراً على المجتمعات بطريقة أساسية لم يعد من الممكن تخيل حياة الإنسان بدونها. في الواقع، إنَّ تأثير الثورة الإلكترونية على حياة الإنسان واسعٌ جداً لدرجة أنَّ البعض يرى أنه يفوق أهمية اختراع الخط وبداية الحضارة الإنسانية. ومع ذلك، فمن الحقائق التي لا جدال فيها أنَّ الثورة الإلكترونية أحدثت ومازالت تحدث موجة تغير كبيرة في حياة الإنسان يوماً بعد آخر وتعطيه شكلاً جديداً (ترابى، طاهرى زاده، ٥١-٥٠).

إلى جانب ما تحمله الثورة السايبرية من مفهوم عميق واسع فإنها تحتوي على تطورات تكنولوجية في مختلف الفروع العلمية منها الذكاء الاصطناعي[5] ، التعلم الآلي[6] ، الحسابات الكمومية[7]وإنترنت السلوك[8] و إنترنت الأجسام [9]، إذ يكون كل منها مصدراً لتغييرات واسعة النطاق وأحياناً تغييرات جذرية في حياة الإنسان. على سبيل المثال ، يعتقد العديد من الخبراء أنَّ الذكاء الاصطناعي سيغير جميع جوانب الحياة الفردية والاجتماعية بحيث لا تكون الحياة مابعد الذكاء الاصطناعي قابلة للمقارنة مع سابقاتها (Gregory2021:1). بناءً على ذلك، يمكن اعتبار الثورة السيبرانية تفسيراً واسعاً وشاملاً للتطورات الثورية في جميع المجالات العلمية المتعلقة بالمجال السيبراني، مما يجعل

4. The International Telecommunication Union

5. Artificial Intelligence

6. Machine Learning

7. Quantum Computing

8. Interne of Behaviors

9. Internet of Bodies (IoB)

التواصل بين الناس والمجتمعات واسعاً وسهلاً للغاية، وسوف تُخضِع جميع المجالات السياسية والاقتصادية والثقافية، والمجالات الاجتماعية لتغييرات جوهرية.

**2. الحرب السيبرانية**

لا يوجد تعريف واحد للحرب السيبرانية، ولكن من خلال دراسة ومقارنة التعاريف المختلفة للحرب الإلكترونية، من الممكن تحديد عناصر مشتركة مثل تصرف الحكومة، واستخدام الفضاء الإلكتروني والتدمير نتيجة الهجوم للحصول على تعريف الحرب السيبرانية. بناءً على ذلك، فقد تم تقديم العديد من التعريفات الأكثر قبولاً من قبل المجتمع العلمي والأمني لغرض تحديد عناصرها المشتركة ومناقشة تطور مفهوم الحرب الإلكترونية. تستخدم الحرب الإلكترونية بشكل شائع لوصف الإجراءات التي تهاجم البنى التحتية الحيوية. الحرب السيبرانية هي بمثابة هجوم مسلح يتسبب عن عمد في آثار مدمرة مثل الموت أو الإصابة الجسدية أو تدمير الممتلكات. النقطة الأساسية هنا هي أنَّ الحكومات أو الأجهزة الحكومية أو الأفراد أو الجماعات التي ترعاها الحكومة لوحدها هي التي يمكنها المشاركة في الحرب الإلكترونية (Cyberwarfare, 2021: 1 ). لذلك ، فإنَّ الحرب الإلكترونية هي حرب تشنها الحكومات أو مؤسساتها ضد الحكومات الأخرى من خلال أجهزة الكمبيوتر والشبكات المتصلة بها. وعادة ما يتم تنفيذ الحرب السيبرانية من أجل تعطيل الأنظمة الإلكترونية أو الشبكات الحكومية والعسكرية للبلد أو البلدان المستهدفة أو تدميرها أو حجب استخدامها. هنا لا ينبغي الخلط بين الحرب السيبرانية والاستخدام الإرهابي للفضاء الإلكتروني أو التجسس الإلكتروني أو الجرائم الإلكترونية. فحتى لو استخدم المخربون أساليب متشابهة في الأنواع الأربعة المذكورة أعلاه، فإنَّ اعتبارها حرباً إلكترونية عار عن الصحة تماماً (SheldonL:2021:1). ينص تعريف آخر للحرب الإلكترونية على أنَّ «الحرب الإلكترونية هي نزاع من خلال الكمبيوتر أو الشبكة يتضمن هجمات ذات دوافع سياسية من قبل دولة قومية واحدة ضد دولة قومية أخرى أو أكثر» في هذا النوع من الهجوم، تحاول الجهات الفاعلة التابعة لدولة قومية واحدة أو أكثر تعطيل أنشطة الحكومات الأخرى من خلال الفضاء الإلكتروني، وخاصة لتحقيق أهداف استراتيجية أو عسكرية. على الرغم من أنَّ الحرب الإلكترونية تشير عموماً إلى الهجمات الإلكترونية التي تنفذها حكومة وطنية ضد دولة أخرى، إلا أنها يمكن أنْ تشمل أيضاً الهجمات التي تشنها الجماعات الإرهابية أو مجموعات المتسللين بالوكالة والتي تهدف إلى تعزيز الموقف لدى بعض البلدان المعينة تجاه غيرها.(Rosencrance, 2019:1 ). يمكن أنْ تتخذ الحرب السيبرانية عدة أشكال بما في ذلك:

-الفيروسات والدودة الحاسوبية والبرامج والتطبيقات الضارة التي يمكن أنْ تستهدف البنية

التحتية الحيوية والأنظمة العسكرية.

- هجمات حجب الخدمة [10] و هي أحداث أمنية إلكترونية تمنع المستخدمين من الوصول إلى أنظمة الكمبيوتر أو الأجهزة أو موارد أخرى من الخدمات عن بعد عبر الشبكة.

- القرصنة وسرقة البيانات المهمة من الوزارات والمراكز والمؤسسات والدوائر الحكومية من خلال برامج الفدية التي تأخذ أنظمة الكمبيوتر كرهائن حتى يدفع الضحايا الفدية,Rosencrance). (2019:1.

في تعريف مشابه ولكنه أكثر اكتمالاً، يعرّف «رنجر»[11] الحرب الإلكترونية على النحو التالي: «تشير الحرب الإلكترونية إلى استخدام الهجمات الرقمية مثل فيروسات الكمبيوتر والقرصنة من قبل دولة ما لتعطيل أنظمة الكمبيوتر المهمة في بلد آخر، بهدف الإضرار والموت والدمار (Cyber) Warfare 2021:1، وفي تعريف مشابه وأكمل يعرّف رنجر الحروب السيبرانية بالقول: «تستخدم الحرب السيبرانية الهجمات الرقمية مثل الفايروسات وعمليات الاختراق بهدف الإخلال والتعطيل والقضاء على المنظومات الحاسوبية الحيوية للبلاد» وبحسب ما يراه فإنَّ الحروب المستقبلية يكون القتال إضافة إلى المعارك العسكرية، القيام بعمليات الاختراق من خلال استخدام كود الكمبيوتر لمهاجمة البنى التحتية للعدو(Ranger, 2018:1).

يمكن تصنيف الأنشطة العدائية في الأجواء السيبرانية وَفقاً لأنواع الأنشطة المنجزة والأضرار الناجمة عنها كالتالي. هذا التصنيف هو تصنيف رتبته «تابانسكي»[12] بترتيب تنازلي من حيث الشدة والقوة:

1. مهاجمة أهداف مدنية تتسبب في أضرار مادية.
2. تعطيل وتدمير البنى التحتية للمعلومات الوطنية الهامة.
3. تعطيل الأهداف العسكرية في الأراضي الخاضعة لسيادة الحكومات.
4. تعطيل الأهداف العسكرية خارج الأراضي الخاضعة لسيادة للحكومات.
5. النشاط الإجرامي والتجسس الصناعي.

10. Denial-of-Service Attacks (DoS)

11. Ranger

12. Tabansky

6. جمع المعلومات والبحث عن نقاط الضعف الأمنية الشائعة واختبارات الاختراق.

7. إدارة حملة إعلامية تخريبية وإساءة استخدام المواقع الرسمية وتشويهها (Tabansky, 2011:82-83).

من الحالات المذكورة، تم تضمين حالة واحدة إلى خمس حالات فقط في تعريف الحرب الإلكترونية، لأنَّ قضية التدمير هي أحد العناصر الرئيسة للحرب الإلكترونية. بالإضافة إلى ذلك، من أجل تحديد ما إذا كان الهجوم السيبراني جزءاً من حرب إلكترونية، يجب مراعاة العديد من الخصائص الأخرى:

1 . مصدر الهجوم وأصله: هل إنَّ من يقف وراء الهجوم هو أحد البلدان أو جهات أخرى؟ إذا كان منفذ الهجوم والتدمير بلداً معيناً، فإنه يدخل ضمن الحرب الإلكترونية، وإلّا فلا يمكن تقييد الحرب بالإلكترونية.

2. هل يمكن للهجوم أنْ يتسبب في أضرار فقط أم أنه يتسبب بالفعل في أضرار وإصابات؟ إذا تسبب هجوم إلكتروني موجه من قبل حكومة ما أو جهات فاعلة فيها في إحداث ضرر أو تصميمه لإحداث ضرر، فيمكن أنْ يُعدَّ الهجوم حرباً إلكترونية، وإلّا فقد يقع ضمن التعريف الآخر مثل التجسس السيبراني.

هل تطلب الهجوم تخطيطاً معقداً وهل استخدم مصادر منسقة متاحة بشكل أساسي للحكومات؟ ( Tabansky, 2011:82-83) ومع ذلك، إذا لم تكن الإجابات عن هذه الأسئلة واضحة تماماً، فلا يمكن تسمية الهجوم السيبراني بالحرب الإلكترونية.

النقطة المهمة الأخرى حول الحرب السيبرانية هي شدة خطورتها. في كثير من الحالات، لا تكون أنظمة الكمبيوتر هي الهدف النهائي، ولكنها مستهدفة بسبب الدور الذي تلعبه في إدارة البنى التحتية في العالم الحقيقي مثل المطارات أو شبكات الطاقة. في الحرب الإلكترونية، قد يكون الهدف محدوداً، على سبيل المثال، هجوم إلكتروني على شبكة الطاقة أو محطات الطاقة النووية، لكن الحرب الإلكترونية قد تكون شاملة وواسعة النطاق وتشمل أهدافاً واسعة (Ranger, 2018:1).

**3. الحرب المعرفية:**

إنَّ أبسط تعريف للأمن المعرفي[13] هو الحفاظ على المعرفة لدى المواطنين وفهمهم ووعيهم. (Seger, Avin, and others, 2020:23-50).

13. Epistemic Security

ووَفقاً لسيجر، فإنَّ الأمن المعرفي هو الذي يضمن الوعي الحقيقي لما يراه المجتمع صحيحاً. هناك جانب آخر للأمن المعرفي وهو الذي يتضمن القدرة على التعرف على الادّعاءات الكاذبة التي لا أساس لها، وإنشاء أنظمة معلومات مقاومة للتهديدات المعرفية مثل الأخبار المزيفة[14]. من الضروري أنْ نذكر هنا أنَّ الإيبيستم أو المعرفة [15] هي مصطلح فلسفي يوناني يعني المعرفة؛ وبالتالي فإنَّ الأمن المعرفي ينطوي على ضمان أنْ يدرك المواطنون ما يعرفونه وأنَّ بإمكانهم التعرف على الادّعاءات الكاذبة التي لا أساس لها من الصحة، والتأكد من أنَّ النظم الإيكولوجية للمعلومات[16] قادرة على الصمود أمام التهديدات المعرفية مثل الأخبار المزيفة.(سيگر،١٣٩٩:١).

ووَفقاً للبحوث التي أجرتها مجموعة بحثية بقيادة إليزابيث سيجر[17]،فإنَّ العصر الحالي يشهد أربعة اتجاهات مختلفة تهدد الأمن المعرفي ، والتي يمكن أنْ تسمى تكتيكات الحرب المعرفية. الأول هو مشكلة المعلومات المكثفة وقلة الاهتمام. في هذا الصدد فإنَّ شبكة الإنترنت توفر كمية كبيرة من المعلومات غير المؤكدة للجميع إذ يعد من الصعب التمييز بين الصواب والخطأ فيها. إنَّ وفرة المعلومات وقلة الاهتمام[18] يعني أنَّ الحكومات والصحفيين وأصحاب المصالح وغيرهم يجب أنْ يتنافسوا مع بعضهم البعض في تشكيل ذهنية الجماهير، وعادة ما يكون الفائز هو الشخص الذي لديه الطريقة الأفضل، وليس بالضرورة من يقول الحقيقة. المشكلة الثانية هي فقاعات التصفية[19] والعقلانية المقيدة[20]. في الواقع، فإنَّ إحدى النتائج المقلقة لقضية عدم الانتباه بخصوص مساحة المعلومات الشاسعة هي إنشاء فقاعات التصفية. وهي عبارة عن عملية تجعل الناس يتعاملون فقط مع آرائهم الحالية ولا يعترفون أبداً بآراء المعارضة والرأي الاخر.

بشكل عام فإنَّ الناس عند تعاملهم مع الكثير من المعلومات ينتبهون إلى أولئك الذين يشبهونهم ولا يولون اهتماماً للوجوه المجهولة إلّا القليل. تؤدي النتيجة المعرفية لفقاعات التصفية هذه إلى ما يعرف بالعقلانية المحدودة. تجدر الإشارة إلى أنَّ الوصول إلى المعلومات هو أساس للتفكير الجيد واتخاذ القرار، لذا فإنَّ تقييد المعلومات الواردة من خلال التستر بهذه الفقاعات، يقلل من قوة التفكير الجيد. المشكلة الثالثة هي انتهاز العدو لتدفق المعلومات[21]. في عصر الثورة

14. Fake News
15. Episteme
16. Information Ecosystem
17. Elizabeth Seger
18. Attention Scarcity
19. Filter Bubbles
20. Bounded Rationality
21. Action by Adversaries and Blunderers

الإلكترونية، أصبح توزيع المعلومات والوصول إليها أسهل من أي وقت مضى؛ لكن الجانب السلبي لهذا التطور هو أنه يمكن استخدام نفس التقنيات لنشر معلومات خاطئة أو مضلِّلَة عن قصد أو غير قصد. عادةً ما تتلاعب جهات فاعلة مختلفة، مثل الأفراد أو المنظمات أو الحكومات، بالمعلومات عمداً لتضليل المتلقين وترسيخ المعتقدات الخاطئة.(سيگر، ١٣٩٩:١).

تجدر الإشارة إلى أنَّ الأعداء يستخدمون تقنيات مختلفة لنشر معلومات كاذبة. وعادة، يستخدم معظمهم منصات التواصل الاجتماعي المصممة للترويج للمحتوى الشائع الذي يثير المشاعر بشدة. غالباً ما تستند المعلومات المضللة إلى النماذج السلوكية ومقاطع الفيديو القصيرة التي يتم مشاركتها على نطاق واسع في تطبيقات المراسلة المغلقة[22] مثل الفيس بوك والواتساب. يمكن لناشري المعلومات المضللة إنشاء مواقع ويب مزيفة أو حسابات على وسائل التواصل الاجتماعي[23] لتلقي الرسائل، وهو تكتيك معروف اشتهر باسم الإعلانات الحاسوبية[24]. يصل هذا الاتجاه الزائف في بعض الأحيان إلى النقطة التي يتم فيها بثها أيضاً من قبل وسائل الإعلام الإخبارية السائدة والتقليدية. وفي الوقت نفسه، يستخدم أولئك الذين ينشرون المعلومات المضللة الذكاء الاصطناعي بشكل متزايد لإنشاء طرق أكثر تعقيداً، بما في ذلك إنشاء حسابات آلية وهمية ومقاطع فيديو مزيفة، والتي وصفها بعض الباحثين ومنهم «تانر»[25]، بأنها تشكل التهديد الأكثر خطورة (Tanner,2020:1-13).

في هذا السياق، ولتوضيح الفكرة، يمكننا الرجوع إلى نتائج بحث نشرتها مجلة ساينس قبل فترة. فبعد القيام بتحليل ملايين التغريدات من 2006 إلى 2017 أظهر هذا البحث النتائج الآتية: «يتم نشر المعلومات والأكاذيب في جميع مجالات الحياة الاجتماعية وعلى نطاق أوسع وأسرع وأعمق» ووجد هذا البحث أيضاً أنَّ «تأثير الأخبار السياسية الكاذبة هو أكثر انتشاراً بكثير من الأخبار الكاذبة عن الإرهاب أو الكوارث الطبيعية أو العلوم أو الأساطير المحلية أو المعلومات المالية. «إنَّ هذا البحث المهم ومن خلال جمع البيانات يتطرق إلى الفكرة السائدة القائلة بأنَّ المواقع والمنصات الإلكترونية أصبحت مصدراً لنشر الأخبار غير المؤكدة والأخبار الكاذبة المثيرة للمشاعر و هو أمرٌ يدق ناقوس الخطر كون وسائل الإعلام أصبحت قوةً مهيمنة لنشر الأخبار. عموماً، تُظهر نتائج هذا التحليل أنَّ «الحقيقة تستهلك ستة أضعاف الإمكانات التي تحتاج إليها الكذبة لتصل إلى 1500 شخص «(رزنيک،) .١٣٩٧:١

22. Closed Messaging Apps
23. Fake Social Media Accounts
24. Computational Propaganda
25. Jonathan Tanner

أخيراً ، فإنَّ التهديد الأخير هو انهيار الثقة[26]. بطبيعة الحال يمكن للبشر أنْ يحددوا بأنفسهم الشخص الذي يثقون به ممن لا يثقون به. على سبيل المثال، كلما زاد عدد الأشخاص الذين يؤمنون بما يقوله الشخص، زاد احتمال ثقة الآخرين به. أيضاً، من وجهة نظر علم النفس ونظراً لوجود اهتمامات وقيم متشابهة بين الأفراد فإنَّ احتمالية ثقة الشخص بأحد أفراد مجتمعه أعلى من احتمالية ثقة الأشخاص بمن هو خارج المجتمع. بالطبع، يستخدم الناس لغة الجسد ونبرة التعبير وأسلوب الكلام من أجل قياس مستوى الصدق عند غيرهم؛ لكن الرؤية والحقائق المذكورة أعلاه يمكن أنْ تتم تخطئتها من خلال بعض التقنيات الحديثة.

على سبيل المثال، يمكن أنْ تُبرِز فقاعاتُ التصفية آراءَ الأقلية لتجعلها أكثر وضوحاً وتوحي إلى أنها آراء الأغلبية. ليس هناك شك في أنه يجب عرض بعض آراء الأقلية، لكن تطبيع الخطابات المتطرفة وجعلها تبدو محترمة أمر فيه الكثير من المشاكل. يمكن أيضاً استخدام التكنولوجيا لتضليل الرؤى اللاواعية. على سبيل المثال، يتم إنشاء مقاطع فيديو مزيفة [27]بطريقة لا تدع مجالًا لأيٍّ من علامات الشك.

أخيراً، تؤدي المشكلات الأربع المذكورة أعلاه إلى فقاعة معرفية، وهي واحدة من أسوأ الأشياء التي يمكن أنْ تحدث. في عالم الفقاعات المعرفية، يتم تدمير قدرة عامة الناس على تمييز الحقائق من الأكاذيب تماماً. المعلومات متاحة بسهولة، لكن لا يمكن للناس معرفة ما إذا كان يمكن الوثوق بما يرونه أو يقرؤونه أو يسمعونه. ومع ذلك، فإنَّ نتيجة العمليات المذكورة هي أنَّ المجتمع سيخوض في النهاية تحوّلاً في المعرفة والرؤية وسيرى القضايا كما يريده العدو ، ثم يحللها و يتخذ على وَفق ذلك الإجراءات المطلوبة (سيگر،).١٣٩٩:١

من حيث الأهداف يمكن للحرب المعرفية أنْ تسعى إلى أهداف مختلفة. عادةً ما يكون الهدف الأساس الأول للحرب المعرفية هو خلق حالة من عدم الاستقرار بين السكان المستهدفين. عدم الاستقرار هذا يعني القضاء على تماسك ووحدة السكان المستهدفين والأشخاص، مما يؤدي إلى فقدان التعاون بينهم. في هذا السياق يقوم البلد المهاجم من خلال الحرب المعرفية بطرح الأفكار والخلافات وزيادة نسبة الانقسامات في المجتمع المستهدف. ضمن المحاولات الانقسامية في الحرب المعرفية ، يُعدُّ القادةُ أفضلَ الأهداف التي يتم استهدافها لأنه يمكن تقسيم المجتمع من خلال عنصر دعم القيادة أو معارضتها.

26. Fabrication and Erosion of Trust

27. Deepfake

يمكن للدولة المهاجمة أنْ تستهدف السكان بشكل عشوائي أو في بعض الحالات تركز فقط على مجموعة معينة مثل الجيش أو الأقليات العرقية أو القومية أو مجموعات أخرى. يتم ذلك عادة من خلال بث الأخبار الكاذبة وإثارة النعرات الطائفية والمذهبية والروايات الكاذبة. تتضمن التكتيكات المستعملة في الحرب المعرفية عناصر مثل زيادة الانقسامات وبث الفرقة وإحياء الحركات المنسية ونزع الشرعية عن الحكومات والقادة وعزل الأفراد والجماعات من خلال التأكيد والمبالغة في الاختلافات وممارسة الإرباك في الأنشطة الاقتصادية الرئيسة والبنى التحتية. لذلك فإنَّ الهدف الأول للحرب المعرفية هو زعزعة استقرار الدولة والمجتمع المستهدفين وحرفهما عن المسار المؤدي إلى زيادة القوة الوطنية.

الهدف الأساسي الثاني للحرب المعرفية هو التأثير على السكان المستهدفين في قضايا محددة مثل الانتخابات أو السياسة الخارجية فيما يتعلق بملف معين. يتم تحقيق هذا الهدف من خلال التأثير والتلاعب بتفسير الناس وفهمهم لمختلف القضايا. في هذا الصدد، يمكن للمهاجمين توجيه الأفراد أو الجماعات أو المواطنين للعمل لصالحهم. وتجدر الإشارة إلى أنَّ الغرض من التأثير يختلف عن الغرض من زعزعة الاستقرار، لأنَّ الغرض من التأثير هو تشكيل عقلية أو ذهنية لدى المجتمع المستهدف، ولكن الغرض من زعزعة الاستقرار هو إثارة الشغب فيه. ومن أمثلة التأثير على المواطنين من خلال الحرب المعرفية، تأثير روسيا على نتائج الانتخابات في الدول الغربية، بما في ذلك عملية الانتخابات في الولايات المتحدة الأمريكية عام 2016، والتي أسفرت عن فوز غير متوقع لدونالد ترامب (Bernal and others, 2020:1 20).

ينبغي الإشارة إلى أنه في عالم الإنترنت اليوم، تعد الشبكات الاجتماعية إحدى أكثر أدوات الحرب المعرفية كفاءة. في هذا السياق، أجرى الناتو، بالتعاون مع جامعة جون هوبكنز[28] وإمبريال كوليدج لندن[29]، بحثاً مكثفاً حول الدور البارز للشبكات الاجتماعية في الحرب المعرفية. ينص جزء من هذا التقرير على ما يلي: «قد تُضْعِف وسائل التواصل الاجتماعي والأجهزة الذكية قدراتِنا المعرفية. يمكن أنْ يؤدي استخدام الشبكات الاجتماعية إلى زيادة التعصبات أوالتحيزات المعرفية[30] والأخطاء الجذرية[31] في اتخاذ القرار. في كتاب «التفكير السريع والبطيء»[32]، ناقش دانيال كانيمان[33]

28. Johns Hopkins University
29. Imperial College London
30. Cognitive Biases
31. Innate Decision Errors
32. Thinking, Fast and Slow
33. Daniel Kahneman

الحائز على جائزة نوبل، التحيزات المعرفية والأخطاء الجذرية في اتخاذ القرار. في هذا السياق، يشير كانيمان إلى أنَّ قنوات الأخبار ومحركات البحث تقدم نتائج أكثر انسجاماً مع رغباتنا وتفضيلاتنا. عادة ما نفسر المعلومات الجديدة ونتحقق من صحتها بطرق تتوافق مع معتقداتنا المسبقة.

وَفقاً لذلك، تقوم برامج التواصل الاجتماعي بتحديث معلومات المستخدمين بسرعة من خلال تزويدهم بمعلومات جديدة لتخلق بينهم الإنتماء والتحيز، مما يجعل الناس يبالغون في تقدير أهمية الأحداث الأخيرة مقارنة بالماضي. بالإضافة إلى ذلك، فإنَّ مواقع التواصل الاجتماعي تمارس التأثير الاجتماعي المعلوماتي[34] بحيث توحي أنها تحظى بقبول المجتمع. وعلى إثرِ وجود عنصر التأثير الاجتماعي يقوم الناس، بمطابقة أفعال ومعتقدات الآخرين مع مجموعاتهم في تلك المواقع الاجتماعية، والتي تتحول إلى غرف الدردشة والتفكير الجماعي. المشكلة الأخرى التي توجد في هذا المجال هي السرعة العالية لنشر الأخبار وإعادة النشر والرد عليها. في هذا الصدد، فإنَّ السرعة العالية في إرسال الرسائل ونشر الأخبار والشعور بالحاجة إلى الاستجابة السريعة لها، يشجع على التفكير الانعكاسي والعاطفي السريع[35]، وهو عكس التفكير الهادئ والمنطقي. واليومَ فإنَّ المنافذ الإخبارية ذات السمعة الطيبة هي الأخرى تستخدم العناوين العاطفية المثيرة لمشاعر المتلقين لتشجيع الإقبال السريع على المواد الإخبارية والتحليلية التي تقدمها. إنَّ المشكلة الأخيرة هي عدم الدقة وتخصيص الوقت المطلوب لقراءة الأخبار ونشرها. الحقيقة هي أنَّ الناس يقضون وقتاً أقل في قراءة المحتوى، حتى لو شاركوه كثيراً. لقد تم تحسين أنظمة المراسلة الاجتماعية لتوزيع المقتطفات القصيرة التي غالباً ما تتجاهل السياقات والاختلافات المهمة. هذا يمكن أنْ يُسهِّل وينشر التفسير السيئ المتعمد وغير المتعمد للمعلومات[36]والروايات المقلوبة[37].

في هذا الصدد، قد يؤدي قصر منشورات وسائل التواصل الاجتماعي، بجانب الصور المرئية الرائعة، إلى منع القراء من فهم دوافع الآخرين وقيمهم. (Johns Hopkins University & Imperial College London, 2021 1-5.).

على الصعيد الدفاعي فإنه يجب على الحكومات أنْ تدرك على الأقل أنَّ هناك محاولاتٍ حربيةً جاريةً. يمكن أنْ توفر الحلول التقنية الأدوات اللازمة للإجابة على بعض الأسئلة الرئيسة في هذا السياق: هل شُنَّت الحملة؟ ما مصدرها؟ من يديرها؟ ماذا يمكن أنْ تكون أهداف المهاجمين؟

34. Social Proofing

35. Reflexively and Emotionally Thinking Fast

36. Intentionally and Unintentionally Misinterpreted Information

37. Slanted Narratives

تظهر أبحاث الناتو أنَّ هناك أنماطاً متكررة يمكن تصنيفها. قد يقدمون أيضاً توقيعاتٍ خاصةٍ لبعض الجهات الفاعلة التي يمكن أنْ تساعد في التعرف على المهاجمين. الحل الخاص في هذا المجال هو استخدام نظام المراقبة والإنذار في الحرب المعرفية[38]. يمكن لمثل هذا النظام أنْ يساعد في التعرف على الحروب المعرفية وحدوثها ومتابعتها. يمكن أنْ يشمل ذلك لوحة معلومات تدمج البيانات المكونة من مجموعة واسعة من وسائل التواصل الاجتماعي ووسائل الإعلام الإخبارية والرسائل الاجتماعية ومواقع الشبكات الاجتماعية. يمكن أنْ تكشف لوحة المعلومات عن الاتصالات والأنماط المتكررة من خلال تحديد المواقع الجغرافية والافتراضية التي تنشأ منها منشورات الوسائط الاجتماعية والرسائل والأخبار، وكذلك من خلال الموضوعات محل الخلاف والمشاعر ودلالات لغوية وعوامل أخرى. بالإضافة إلى ذلك، يمكن أنْ يساعد استخدام خوارزميات التعلم الآلي[39] والتعرف على النماذج الموجودة وبشكل سريع في تحديد الحملات الناشئة وتصنيفها دون الحاجة إلى تدخل بشري. سيوفر مثلُ هذا النظام المراقبةَ والإنذارَ في الوقت المناسب لصانعي القرار، ومساعدتهم على الاستعداد والمواجهة المطلوبة مع ظهور الحرب المعرفية وتطورها (Johns Hopkins University & Imperial College London, 2021:1-5).

**4. حرب المعلومات**

من وجهة النظر الدلالية، فإنَّ حرب المعلومات هي صراع على عمليات المعلومات والاتصالات، وهي حرب يتم تنفيذها بتخطيط من خلال تطبيق القوة المدمرة على نطاق واسع ضد أصول وأنظمة المعلومات، أي ضد أجهزة الكمبيوتر والشبكات التي تدعم البنية الأساسية (Brian, 2021:1). يعرّف الناتو «حرب المعلومات» على النحو التالي: «حرب المعلومات هي عملية يتم تنفيذها من أجل الحصول على تفوق معلوماتي على الخصم». تتضمن هذه الحرب التحكم في مساحة المعلومات، وحماية الوصول إلى المعلومات الشخصية، أثناء محاولة الحصول على المعلومات واستخدامها، وتدمير أجهزة المعلومات والإرباك في منظومة معلومات العدو. حرب المعلومات ليست ظاهرة جديدة، لكنها تتضمن عناصر ابتكارية نتيجة للتطورات التكنولوجية التي تؤدي إلى نشر أسرع للمعلومات على نطاق أوسع (Information Warfare,2005:1).

تُعرِّف وزارة الدفاع الأمريكية حرب المعلومات على أنها: «الإجراءات المتخذة لتحقيق التفوق المعلوماتي على الخصم من خلال التأثير على معلومات العدو والعمليات القائمة على المعلومات وأنظمة المعلومات والشبكات المستندة إلى حواسيب العدو، وإلى جانبها الحفاظ على معلوماتنا

38. Cognitive Warfare Monitoring and Alert System

39. Machine Learning and Pattern Recognition Algorithms

الشخصية وعملياتنا القائمة على أساس المعلومات، والحفاظ على أنظمة المعلومات والشبكات التابعة لنا المستندة إلى الحواسيب. تؤكد وزارة الدفاع الأمريكية في التعريف التكميلي أنَّ حرب المعلومات هي» القدرة على جمع ومعالجة ونشر التدفق المستمر للمعلومات لتحقيق أو تعزيز الأهداف ضد عدو معين إلى جانب منع العدو من الوصول إلى هذه القدرات:(Ramlee,2005).

(2-1 بمعنى آخر، فإنَّ حرب المعلومات هي كل ما يتعلق بخداع العدو. إذ تشمل هذه الحرب المعلومات نفسها ، معالجة المعلومات وتحليلها، البنية التحتية للمعلومات والأشخاص والقادة. من ناحية أخرى، فإنَّ حرب المعلومات هي أيضاً محاولة لتوفير معلومات دقيقة يحتاجها القادة وفي الوقت المناسب لمساعدتهم في عمليات صنع القرار.(Ramlee,2005:3) تُعرِّف البحرية الأمريكية حرب المعلومات على النحو التالي: «حرب المعلومات» مصطلح محل نقاش وغالباً ما يفتقر إلى تعريف مقبول؛ لكنْ بالنسبة للقوات الجوية الأمريكية، فإنَّ حرب المعلومات هي أنشطة تنسق عناصر الاستخبارات والمراقبة والاستطلاع، وعمليات الفضاء الإلكتروني، والحرب الكهرومغناطيسية لتحقيق نتائج تخص فترة حرب المعلومات وفترة السلم. اليوم يصف سلاح الجو الأمريكي حرب المعلومات على أنها استخدام للقدرات والإمكانيات العسكرية في بيئة المعلومات للتأثير عمداً على سلوك قوات العدو وما يمتلكه من نظام المعلومات (Gagnon, 2020:5) يقول الجنرال تيموثي هوغ[40] ، قائد الحرب المعلوماتية في سلاح الجو الأمريكي[41] بهذا الشأن: «أحد الأمثلة البارزة التي تُظهر كيف يريد الجيش هزيمة الأعداء باستخدام حرب المعلومات، هو الجهد المبذول لفهم أهداف العدو ومدى قدراته لتحقيق تلك الأهداف. وعليه يمكن أنْ تكون حرب المعلومات مجرد حرب نفسية غير ملموسة، وهي حرب تجتمع فيها مزيج عناصر الفضاء السيبراني، أو المعلومات، أو الحرب الإلكترونية، أو العمليات الاستخباراتية، أو العمليات النفسية، أو الخداع العسكري. الهدف النهائي من هذه التدابير هو التأثير على بيئة المعلومات أو تغيير عقلية العدو (Mark, 2020:1).

البعض الاخر يَعدُّ حرب المعلومات في الأساس المعلومات العسكرية نفسها، والتي تعني في إطار أضيق حرب المعلومات بين جيوش الدول المتحاربة وهي تشمل جمع وتحليل المعلومات العسكرية حول جميع التخصصات والفروع ونشرها للوحدات العسكرية وصناع القرار. تنقسم المعلومات العسكرية إلى معلومات بشرية [42] ومعلومات تقنية ، والتي تشمل المعلومات

40. Gen. Timothy Haugh

41. Information Warfare Organization

42. Human Intelligence

التصويرية[43] والمعلومات الإلكترونية[44] . يتم تنفيذ أنشطة الاستخبارات على جميع المستويات التكتيكية والتنفيذية والاستراتيجية، سواء في وقت السلم أو في زمن الحرب(Military intelligence training, 2021)، وقد جاء في تعريف آخر أنَّ المعلومات العسكرية هي تخصص عسكري يساعد القادة في اتخاذ القرارات عبر استخدام أساليب جمع المعلومات وتحليلها. يتم تحقيق هذا الهدف من خلال عرض البيانات وتحليلها اعتماداً على مجموعة واسعة من المصادر والتي تغني حاجة القادة ومهمتهم القيادية أو للإجابة على الأسئلة كجزء من التخطيط العملياتي. وعادة، من أجل القيام بتحليل البيانات والمعلومات يتم تحديد احتياجات القائد بالنسبة إلى المعلومات أولاً ، ثم يتم إعطاء الأولوية لجمع المعلومات وتحليلها ونشرها.

قد تشمل مجالات الدراسة، بيئة العمليات والقوات المعادية والصديقة والمحايدة، والسكان المدنيين في إحدى مناطق العمليات القتالية، وغيرها من مجالات الاهتمام. يتم تنفيذ الأنشطة الاستخباراتية أو المعلوماتية على جميع المستويات، من التكتيكية إلى الاستراتيجية، في وقت السلم والانتقال إلى الحرب وأثناء الحرب. تتعلق المعلومات الاستراتيجية بموضوعات واسعة مثل الاقتصاد والتحليل السياسي والقدرات العسكرية وأهداف الدول الأجنبية، وبشكل متزايد، الجهات الفاعلة غير الحكومية مثل الإرهابيين. قد تكون هذه المعلومات علمية أو تقنية أو تكتيكية أو دبلوماسية أو اجتماعية.

تُعَرَّف المعلومات الاستراتيجية رسمياً بأنها المعلومات المطلوبة لتحديد السياسات والخطط العسكرية على المستويين الوطني والدولي بحيث تتوافق مع المستوى الاستراتيجي للحرب(Rolington, 2013).

يقسمُ خبراءٌ آخرون حرب المعلومات إلى ثلاث مجموعات. الأولى: حرب المعلومات، أي الحصول على معلومات عن أدوات العدو وقدراته واستراتيجياته. الثانية: الحرب على المعلومات، أي حماية أنظمة المعلومات و في الوقت نفسه الإخلال أو تعطيل مصادر تخزين معلومات العدو. والثالثة: هي الحرب من خلال المعلومات، أي إنتاج معلومات غير واقعية أو خادعة بطريقة تؤدي إلى الهيمنة المعلوماتية والإعلامية.

لعل أحدث تعريف لحرب المعلومات هو الذي اقترحته الحكومة الروسية، والذي يُعدُّ واحداً من أكثر التعريفات نجاحاً في هذا المجال. تُعرِّفُ الحكومةُ الروسيةُ حرب المعلومات على النحو التالي:

43. Technical Intelligence – Mainly Imagery Intelligence

44. Electronic Intelligence

«صراعٌ بين حكومتين أو أكثر في مجال المعلومات بهدف إتلاف ما لدى الطرف الآخر من الأنظمة والعمليات ومصادر المعلومات والهياكل الحيوية وغيرها؛ التأثير على النظم السياسية والاقتصادية والاجتماعية؛ خلق حملات نفسية واسعة النطاق ضد شعب لإضعاف استقرار المجتمع والحكومة والضغط على الحكومة لاتخاذ قرارات تتناسب مع مصالح المعتدي (Blagovest,2019:129-133).

وعلى وَفق ما يشير إليه هذا التعريف فإنَّ الحكومة الروسية ترى أنَّ حرب المعلومات تتجاوز المجال العسكري وتتجاوز الجهد المبذول لتدمير أنظمة معلومات العدو، فهي تستهدف جميع مجالات وأبعاد دولة العدو. لقد أشرنا سابقاً إلى أنَّ روسيا تُعدُّ من الدول الرائدة في مجال حرب المعلومات وتوسيع معناها ومفهومها بالطبع. جاء في تقرير عن حرب المعلومات في روسيا أنَّ : «روسيا ليست مجرد تهديد للمعلومات لأوروبا والولايات المتحدة فحسب، بل إنَّ لدى روسيا استراتيجية عالمية تؤثر على كل منطقة من مناطق العالم بنهج مختلف وبدرجات مختلفة.» نهج روسيا في حرب المعلومات شامل ويتضمن الهجمات الإلكترونية والعمليات الاستخباراتية كعناصر متماسكة تعمل معاً لتحقيق أهداف السياسة الخارجية الروسية .(Cunningham, 2020:1) بالإضافة إلى ذلك، لا تسعى روسيا في حربها المعلوماتية فقط إلى إضعاف القوات المسلحة للعدو بل إنها تسعى إلى التأثير على تصور السكان المستهدفين بطريقة تخدم مصالحها. بالطبع على عكس العمليات السايبرية ، فإنَّ العمليات الاستخباراتية قديمة جداً، وقد استخدمها الكرملين لفترة طويلة لتحقيق أهدافه. في هذا الصدد، سرعان ما أدرك القادة السوفييت قيمة المعلومات وكيفية استخدامها للتأثير على الجماهير في الداخل والخارج. بعد ذلك، تمكن الاتحاد الروسي من زيادة فعاليتها في حرب المعلومات بتكلفة منخفضة عبر استخدام الإنترنت.(Arampatzis and Cobaugh, 2018).

في هذا الصدد، أصبحت وسائل الإعلام المدعومة حكومياً والترول[45] (المتصيدون) والروبوتات أحد العناصر الرئيسة في حرب المعلومات الروسية. لقد عملت روسيا بعد الحرب الباردة على إضعاف النظام الدولي الذي كان مُهيمَناً عليه من قبل الغرب ومؤسساته الديمقراطية العالمية، لتقوم بنشر نسخة من الأحداث العالمية تتماشى مع أهداف سياستها الخارجية. لقد ساعدت روسيا الجناحين السياسيين -اليسار واليمين- في الغرب لكي يفرطا في نشاطاتهما وهما بالتالي قدّما من خلال طرق هادفة مساعدة كبرى لتنفيذ السياسات الخارجية لروسيا(Troianovski, Warrick,2018:1).

45. Internet Trolls

الترول هم أشخاص يساهمون بتعليقات أو كلام مثير للجدل لا علاقة له بالموضوع المشارك فيه داخل غرف الدردشة يهدف به الهدم والخروج عن الموضوع، وإثارة الجدل والمشاكل بين المشاركين .

و على وَفق ما جاء في التعاريف المذكورة، يمكن القول إنَّ حرب المعلومات قد شهدت قيوداً أو توسعاً مفاهيمياً تحت تأثير ثورة الاتصالات والمعلومات، وتحت تأثير الثورة السيبرانية بطريقة خاصة. وبذلك فقد أدت ثورات الاتصالات والمعلومات والثورة الإلكترونية إلى توسيع نطاق حرب المعلومات من المجال العملياتي والتكتيكي العسكري إلى المجالات الاستراتيجية. وكما مرّت الإشارة فلا يقتصر اليوم دورُ حربِ المعلومات على المجال العسكري فحسب، بل تجعل الحكومات جميع المجالات العسكرية والسياسية والاقتصادية والثقافية والاجتماعية وحتى المجالات المعرفية والمعلوماتية هدفاً لحرب المعلومات؛ لذلك، فقد اكتسبت حرب المعلومات بُعداً استراتيجياً وأهدافاً مختلفة. هذا أولاً و ثانياً فإنَّ ارتباط واستخدام حرب المعلومات مع أنواع أخرى من الحروب الحديثة، مثل الحرب الإلكترونية والحرب الهجينة، يزيد تنفيذها المتزامن من قوة الدولة المهاجمة ويجعل الدولة العدوة أكثر عرضة للخطر(Mumford, 2020:3).

**5. الحرب الهجينة**

لأول مرة قام فرانك هافمن[46] عام 2007 بتوسيع مفهوم الحرب الهجينة (2020:2Green) بحسب رأي هافمن فإنَّ الحرب الهجينة هي انفصال بين ما هو جزء من الساحة وما هو ليس منها، بتعبير آخر هي الحرب التي تزيل التمايز بين فترتي الحرب والصلح من خلال استخدام جميع الآليات السياسية والعسكرية والاقتصادية والاجتماعية والاستخباراتية والسايبرية وما يتعلق بالبنى التحتية. الحرب الهجينة متعددة الأوجه وتستخدم على مستويات متعددة في نفس الوقت. أدّى هذا النوع من الحرب إلى تكديس المستويات التقليدية للحرب، بما في ذلك التكتيكات والعمليات الاستراتيجية، وبالتالي زيادة السرعة على المستويين الاستراتيجي والتشغيلي بما يتجاوز قدرة الفاعل التقليدي.

في الحرب الهجينة، ترتبط المساحات المادية التقليدية مثل الأرض والبحر والجو والفضاء بشكل متزايد بالمساحات الاجتماعية والمشيدة مثل المساحات السياسية والاقتصادية والثقافية والمعلوماتية والإلكترونية، والأهم من ذلك، المساحات المعرفية والنفسية؛ ونتيجة لذلك، فإنه يقلل من الحاجة إلى استخدام القوة العسكرية الثقيلة. في هذا الصدد وبدلاً من إجبار العدو على الاستسلام من خلال تدمير قدراته العسكرية وكسر مقاومته، فإنَّ ساحة المعركة الرئيسة هي في الفضاءات المعرفية للديمغرافية المحلية والدولية الرئيستين وحدود العمل لدى السياسيين وبالتالي إجبار العدو على الاستسلام أو تقديم تنازلات .(Mumford, 2020:3) وفي الوقت نفسه، تلعب التقنيات الجديدة وخاصة التقنيات الإلكترونية دوراً مهماً في الحرب الهجينة. في الواقع، توفر

46. Frank Hoffman

التقنيات الجديدة وخاصة الذكاء الاصطناعي وسيلة لتحقيق أهداف سياسية في المنطقة الرمادية بين الحرب والسلام. على الجانب الدفاعي ، تقدم التطورات التكنولوجية الجديدة خيارات لاكتشاف أفضل وفهم أعمق ودفاع أكثر فعالية ضد الحروب الهجينة. لذا فإنه من المهم بالنسبة إلى القادة السياسيين والعسكريين وصناع القرار أنْ يكون لديهم فهمٌ شاملٌ لآثار التقنيات الجديدة في الحرب الهجينة . (Thiele,2020:6) بناءً على ذلك ، فإنَّ مصطلح الحرب الهجينة يُستخدم لتحديد مجموعة فرعية خاصة من الإجراءات التي تتضمن التطبيق الاستراتيجي لاستخدام طاقة الغموض[47] لكسب الأراضي أو تحقيق أهداف استراتيجية أخرى. تشكل الحرب الهجينة، على عكس الأنواع الأخرى من الأعمال المشتركة، مثل إجراءات التدخل وعمليات التسلل[48]، أنشطة قسرية واضحة. في هذا الصدد، لا يحتاج الفاعلون في الحرب الهجينة إلى إنكار أفعالهم، لأنَّ قضية مسؤولية استخدام القوة منفصلة عن قضية الغموض. في هذا الصدد، فإنَّ النقطة الأساسية والمهمة للغاية هي أنَّ الغرض من الغموض ليس بالضرورة إخفاء الفاعل الحقيقي وراء الأنشطة، بل إنه يتمثل في عدم إعطاء جواب مقنع وبالتالي التهرب من المسؤولية .على سبيل المثال، يمكن ذكر حرب القرم كمثال على حرب هجينة ناجحة في مجال الغموض للتهرب من تحمل المسؤولية. في حرب القرم، على الرغم من حقيقة معرفة الدول الغربية بأنَّ روسيا كانت السبب الرئيس وراء حرب القرم وأزمتها ، إلا أنَّ الدور والتدخل الروسي كان غامضاً لدى الدول الغربية لدرجة أنَّ روسيا تمكنت إلى حد كبير من الهروب من تحمل المسؤولية وعواقبها. بعبارة أخرى، تصرفت روسيا دون مستوى تحريك الطرف الآخر نحو الانتقام المشروع[49] في حرب القرم (Mumford, 2020:3).

وتجدر الإشارة إلى أنَّ مفهوم الغموض في الدراسات الإستراتيجية الغربية يقع تاريخياً في أدبيات الإستراتيجية النووية[50]، حيث يرتبط بفكرة الردع. إذ قدَّم جون بايليس[51] في دراسته للاستراتيجية النووية البريطانية[52] مدرستين فكريتين بخصوص هذه المسألة وميز بين الاستراتيجيين الذين يفضلون الغموض المتعمد[53] في مجال إمكانية استخدام الأسلحة النووية أصحاب الغموض غير المقصود [54]. تستند الحرب الهجينة بقوة على ما يسميه بايليس الغموض المحسوب. في هذا

47. The Force of Ambiguity
48. Interference and Influence Operations
49. Legitimate Retaliation
50. Nuclear Strategy
51. John Baylis
52. British Nuclear Strategy
53. Deliberate Ambiguity
54. Unintentional Ambiguity

السياق، يشير مؤسس الفكر الاستراتيجي الحديث، كارل فون كلاوزفيتز[55]، في أطروحته الأصلية بعنوان «في الحرب»[56] إلى ما أطلق عليه الآخرون فيما بعد بـــ «غبار الحرب»[57] لتحديد ما يحتاج إليه القادة من المعلومات في الحرب. في هذا الصدد، يعد تكوين صورة ذكية لنوايا العدو وهيكلية القوة والقدرات التسليحية لديه وما إلى ذلك جزءاً مهماً من أي استراتيجية. تمثل الحرب الهجينة أكثر أشكال الحرب غموضاً بسبب التعمد في إخفاء هوية الدولة المهاجمة. و على أيِّ حال فإنَّ عدم معرفة البلد المهاجم المعتدي يمثل بالضبط تحدياً أساسياً لصياغة الاستراتيجية وتحديد معالمها. (Mumford 2020:5).

**الاستنتاج**

الحقيقة هي وجود نوع من الارتباك في المجال النظري والعملي في تعريف وتشخيص الحروب الجديدة مثل حرب المعلومات والحرب الإلكترونية والحرب الهجينة والحرب المعرفية. إنَّ هذه المجموعة الواسعة من أسماء الحروب الحديثة، إلى جانب أوجه التشابه المفاهيمية الواسعة والأمثلة الموجودة فيها، هي مؤشر على الوضع المربك في تعريف وتشخيص الحروب الحديثة.

لهذا السبب، يحاول البعض استخدام تعبير الحرب الهجينة لجميع أنواع الحروب الحديثة، وهو ما لا يتوافق مع الحقائق القائمة وتنوع الحروب الحديثة من حيث المفاهيم والأمثلة. وكمثال على ذلك، فإنَّ العملية الإلكترونية التخريبية هي في النهاية حرب إلكترونية واضحة، ولا يمكن تصنيفها تحت عنوان آخر مثل الحرب الهجينة. على هذا الأساس، يمكن القول إنَّ العالم اليوم شاء أو أبى قد أصبح تحت تأثير الثورة التكنولوجية، وخاصة ثورة المعلومات والاتصالات، والأهم منهما الثورة الإلكترونية، إذ واجه إمكانات يؤدي استخدامها إلى تشكيل أنواع جديدة من الحروب الحديثة وأنماط حديثة من الحروب الكلاسيكية التي يصعب التجهيز لمواجهتها. بالطبع فإنَّ هناك سمة مشتركة تماماً في جميع الحروب الحديثة، والتي يمكن اعتبارها مفتاح الفهم الإدراكي والنموذجي، فضلاً عن التحضير للتفوق في شنها ومواجهتها. في هذا الصدد، فإنَّ السمة المشتركة لجميع الحروب الحديثة هي الدور البارز للتكنولوجيا، بما في ذلك المعلومات والاتصالات والتكنولوجيا السيبرانية، وباختصار، العلم والمعرفة في تكوينها أو تطورها. في الواقع، أدَّت التقنيات الجديدة إلى بروز حروب جديدة مثل الحرب الإلكترونية التي جعلت الحروب السابقة مثل حرب المعلومات تواجه أبعاداً مختلفة مع تغييرات في الشكل والمحتوى. من الضروري الإشارة إلى أنَّ التأثيرات الأساسية للعلم

55. Carl von Clausewitz

56. On War

57. Fog of War

والمعرفة على الحروب العسكرية والحديثة تفوق مستوى الحديث عن الثورة في الشؤون العسكرية بسبب التكنولوجيا، ويكاد العلم الحديث ، مثل العلوم السيبرانية وخاصة الذكاء الاصطناعي، يعمل على تغيير مفهوم الصراع والعداوة في العلاقات الدولية بشكل أساسي. بناءً على ذلك، فإنَّ الطريقة الوحيدة للاستعداد للحروب الحديثة هي الزيادة في العلم والمعرفة.

## المصادر

### أ . المصادر الفارسية

ترابی، قاسم و طاهری‌زاده، محمدناصر (١٤٠٠). »انقلاب سایبری و تحول مفهوم جنگ اطلاعاتی در عرصه روابط بین‌الملل«، فصلنامه مطالعات بین‌المللی، سال ١٧، شماره ٤(٦٨)، بهار.

رزنیک، برایان (١٣٩٧). »انتشار اخبار جعلی توییتر کار کیست«، قابل‌دسترس در :http://www taadolnewspaper.ir

سیگر، الیزابت (١٣٩٩). »بزرگترین تهدید امنیتی در عصر پساحقیقت؛ چرا رساندن اطلاعات دقیق به مردم روزبه‌روز سخت‌تر می‌شود؟«، قابل‌دسترس در/https://www.bbc.com/persian : magazine-56112997

### ب. المصادر الإنجليزية

Bernal, Alonso and Others(2020), Cognitive Warfare on Attack Truth Thought, at:https:// www.innovationhub-act.org/sites/default/files/202103/Cognitive%20

Warfare.pdf Russia's Information Warfare Exploring the Cognitive ,(٢٠١٩Blagovest, Tashev( Dimension, at: https://www.usmcu.edu/Portals/218/CAOCL/files/RussiasInformationWarfare

_MCUJ_Fall2019.pdf?ver=2019-11-19-093543-040 Brian, Lewis (2021), Information Warfare, at:

https://fas.org/irp/eprint/snyder/infowarfare.htm Brigadier General Gagnon (2020), Information Warfare, Cyberspace Objectives, and the US Air Force, at:

https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-34_Issue-3/SLP-Gagnon. pdf

Cunningham, Conor (2020), A Russian Federation Information Warfare Primer, at: https:// jsis.washington.edu/news/a-russian-federation-information-warfare-

primer/#_ftnref5 Cyber Warfare (2021), at: https://www.rand.org/topics/cyber-warfare.html

Cyberwarfare (2021), at: https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/ cyberwarfare.html

Green. Kieran (2020), Does War Ever Change? A Clausewitzian Critique of Hybrid Warfare, at: https://www.e-ir.info/pdf/87895

Information Warfare (2005), at: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-

deepportal4-information-warfare.pdf

Lewis Internet Users, (2021), at: https://www.internetlivestats.com/internet-users/ Johns Hopkins University & Imperial College London (2021), Countering cognitive warfare: awareness and resilience, at: https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-

warfare-awareness-and-resilience/index.html

Gregory, Jennifer (2021), Quantum Security and AI: Building a Future Together, at:https://securityintelligence.com/articles/quantum-security-artificial-intelligence-future-together/

Military intelligence training (2021), at: https://www.groupedci.com/offers/military-intelligence-training/

Mumford,Andrew (2020), Ambiguity in hybrid warfare, at: Https://www.hybridcoe.fi/wp-content/uploads/2020/09/202009_Strategic-Analysis24-1.pdf

Pomerleau, Mark (2020) The New Ways the Military is Fighting Against Information Warfare Tactics, at: https://www.c4isrnet.com/information-warfare/2020/07/20/the-new-ways-the-military-is-fighting-against-information-warfare-tactics/aaa

Ramlee Sulaiman (2005), information warfare, at: https://www.giac.org/paper/gsec/1870/information-warfare/103284

Ranger, Steve (2018), what is Cyberwar? Everything you Need to Know About the Frightening future of Digital Conflict, at; https://www.zdnet.com/article/cyberwar-a-guide-to-the-frightening-future-of-online-conflict/

Rolington, Alfred (2013), Strategic Intelligence for the 21st Century: The Mosaic

Method. Oxford University Press.

Rosencrance,Linda(2019),Cyberwarfare, at:

https://searchsecurity.techtarget.com/definition/cyberwarfare

Seger, Elizabeth, Avin, Shahar and others (2020), Tackling Threats to Informed Decision-Making in Democratic Societies, Promoting Epistemic Security in a

Technologically-AdvancedWorld, at:

https://www.turing.ac.uk/sites/default/files/2020-10/epistemic-security-report_final.pdf

Sheldon, John (2021), Cyberwar, at:

https://searchsecurity.techtarget.com/definition/cyberwarfare

Sherman, J. Arampatzis, A. & Cobaugh, P, (2018), An Assessment of

InformationWarfare as aCybersecurityIssue, at:

https://www.realcleardefense.com/articles/2018/06/18/an_assessment_of_infor mation_ warfare_as_a_cybersecurity_issue_113541.html

Tabansky, Lior (2011), Basic Concepts in Cyber Warfare, at: http://book.itep.ru/depository/cyberwar/1308129610.pdf.

Tanner, Jonathan (2020), 10 Things to Know About Misinformation and Disinformation, at: https://www.odi.org/sites/odi.org.uk/files/resource-documents/10_things_to_know_about_misinformation_and_disinformation.pdf Thiele, Ralph (2020), Artificial Intelligence -A Key Enabler of Hybrid Warfare.at:https://www.hybridcoe.fi/wp-content/uploads/2020/07/WP-6_2020_rgb-1.pdf Troianovski, A. & Warrick, J. (2018), How a Powerful Russian Propaganda Machine Chips Away at Western Notions of Truth, at:

https://www.washingtonpost.com/graphics/2018/world/national-security/russian-propaganda-skripal-salisbury/

## هوية البحث

**أسماء الباحثين:**

1. علي رضا رضائي - أستاذ مشارك في العلاقات الدولية،جامعة آزاد الإسلامية.

2. قاسم ترابي - أستاذ مشارك في العلاقات الدولية، جامعة آزاد الإسلامية.

**عنوان البحث:** تسليط الضوء على الحروب الحديثة في مجال العلاقات الدولية مفهوماً ومضموناً

**تأريخ النشر:** أيلول 2022

**رابط البحث:** http://www.rahbordsyasi.ir/article_153192.html

**ملاحظة:**

الآراء الواردة في هذا البحث لا تعبر بالضرورة عن وجهة نظر المركز، إنما تعبر فقط عن وجهة نظر كاتبها

## عن المركز

مركز البيدر للدراسات والتخطيط منظمة عراقية غير حكوميّة، وغير ربحّية، تأسس سنة 2015م، ومُسجل لدى دائرة المنظمات غير الحكومية في الأمانة العامة لمجلس الوزراء.

ويسعى المركز للمساهمة في بناء الدولة، عن طريق طرح الرؤى والحلول العملية للمشاكل والتحديات الرئيسة التي تواجهها الدولة، وتطوير آليات إدارة القطاع العام، ورسم السياسات العامة ووضع الخطط الاستراتيجية، وذلك عن طريق الدراسات الرصينة المستندة على البيانات والمعلومات الموثقة، وعن طريق اللقاءات الدورية مع الجهات المعنية في الدولة والمنظمات الدولية ذات العلاقة. ويسعى المركز لدعم الإصلاحات الاقتصادية والتنمية المستدامة وتقديم المساعدة الفنية للقطاعين العام والخاص، كما يسعى المركز لدعم وتطوير القطاع الخاص، والنهوض به لتوفير فرص عمل للمواطنين عن طريق التدريب والتأهيل لعدد من الشباب، بما يقلل من اعتمادهم على المؤسسة الحكومية، ويساهم في دعم اقتصاد البلد والارتقاء به.

ويحرص أيضاً للمساهمة في بناء الانسان، باعتباره ثروة هذا الوطن، عن طريق تنظيم برامج لإعداد وتطوير الشباب الواعد، وعقد دورات لصناعة قيادات قادرة على طرح وتبني وتطبيق رؤى وخطط مستقبلية، تنهض بالفرد والمجتمع وتحافظ على هوية المجتمع العراقي المتميزة ومنظومته القيمية، القائمة على الالتزام بمكارم الاخلاق، والتحلي بالصفات الحميدة، ونبذ الفساد بأنواعه كافة، إدارية ومالية وفكرية وأخلاقية وغيرها.



**www.baidarcenter.org**

**info@baidarcenter.org**