University of Zawia - Faculty of Arts Journal (UZFAJ)
Volume 26, Issue 2, (2026), 339-356, ISSN: 2521-9235

Information Wars and Their Role in Threatening Political Security

Abu Harara almoalaf

Department of Sociology, Faculty of Education, University of Zawia, Zawia,

abohararaalmoalaf@gmail.com

Received 28 /04 /2026 | Accepted 03 /05 /2026 | Available online 03 / 07 /2026 | DOI: 10.26629/uzfaj.2026.30

Abstract:
The study aimed to explore information wars and their role in threatening political security through the following axes: examining the role of information wars in reshaping the nature of threats facing political security in contemporary states, investigating the extent to which misleading information and targeted digital campaigns affect the stability of political systems and citizens' trust in state institutions, identifying the main mechanisms and tools employed by information wars to infiltrate the political space and influence decision-making processes, and exploring effective strategies that states can adopt to confront information wars and mitigate their impact on political security. The researcher employed the descriptive method due to its suitability for the study objectives.
The study reached the following results:
-The study revealed that information wars have reshaped the nature of threats facing political security.
-It was found that misleading information and targeted digital campaigns have a significant impact on the stability of political systems.
-The study indicated that information wars rely on a comprehensive set of mechanisms and tools, including misleading information, cyber-attacks, and targeted digital campaigns.
-The study demonstrated that developing effective strategies to confront information wars requires a comprehensive approach that integrates cybersecurity and specialized training for human resources.

Keywords: Information Warfare, Political Security, Cybersecurity .

.

"Articles published in *Univ Zawia* Faculty Arts J are licensed under a Creative Commons Attribution-NonCommercial 4.0 International License

الحروب المعلوماتية ودورها في تهديد الأمن السياسي

أبو حرارة المؤلف

قسم علم الاجتماع، كلية التربية ناصر، جامعة الزاوية، الزاوية، ليبيا

تاريخ الاستلام 28/ 2026/04 تاريخ القبول2026/05/30 تاريخ النشر 2026/07/03

ملخص البحث

هدفت الدراسة إلى التعرف على الحروب المعلوماتية ودورها في تهديد الأمن السياسي وذلك من خلال المحاور الاتية: التعرف على دور الحروب المعلوماتية في إعادة تشكيل طبيعة التهديدات التي تواجه الأمن السياسي في الدول المعاصرة، والتعرف على مدى تأثير المعلومات المضللة والحملات الرقمية الموجهة على استقرار الأنظمة السياسية ومستوى ثقة المواطنين بمؤسسات الدولة، والتعرف على أبرز الآليات والأدوات التي توظفها الحروب المعلوماتية لاختراق الفضاء السياسي والتأثير في عملية صنع القرار، وايضاً التعرف على الاستراتيجيات الفعالة التي يمكن للدول تبنيها لمواجهة الحروب المعلوماتية والحد من انعكاساتها على أمنها السياسي، واتبع الباحث المنهج الوصفي لملائمته لأغراض الدراسة وتوصلت الدراسة إلى النتائج الاتية:

أظهرت الدراسة أن الحروب المعلوماتية أعادت تشكيل طبيعة التهديدات التي تواجه الأمن السياسي.

تبين أن المعلومات المضللة والحملات الرقمية الموجهة لها تأثير كبير على استقرار الأنظمة السياسية

كشفت الدراسة أن الحروب المعلوماتية تعتمد على مجموعة متكاملة من الآليات والأدوات تشمل المعلومات المضللة، والهجمات السيبرانية، والحملات الرقمية الموجهة.

أظهرت الدراسة أن تطوير استراتيجيات فعالة لمواجهة الحروب المعلوماتية يتطلب نهجًا شاملًا يدمج الأمن السيبراني، والتدريب المتخصص للكوادر البشرية.

الكلمات المفتاحية: الحروب المعلوماتية، الأمن السياسي. الامن السيبراني.

المقدمة

تُعدّ الحروب المعلوماتية واحدة من أبرز التحولات التي شهدها العالم المعاصر في طبيعة الصراع بين الدول والفاعلين غير الحكوميين، حيث لم يعد النزاع مقتصرًا على استخدام القوة العسكرية التقليدية، بل امتد ليشمل الفضاء الرقمي والإعلامي بوصفه ساحة جديدة للتنافس والتأثير، فقد أدى التطور المتسارع في تكنولوجيا الاتصال والمعلومات إلى خلق بيئة معقدة تتداخل فيها الأدوات الرقمية مع الأهداف السياسية، الأمر الذي جعل من المعلومات سلاحًا استراتيجيًا قادرًا على إحداث تغييرات عميقة في بنية الأمن السياسي للدول، وفي هذا السياق، برز مفهوم الحروب المعلوماتية ليعكس استخدام البيانات والإعلام والتقنيات الحديثة في التأثير على الرأي العام، وصنع القرار، وزعزعة الاستقرار الداخلي للدول، دون الحاجة إلى المواجهة المباشرة.

وإن أهمية الحروب المعلوماتية تكمن في قدرتها على تجاوز الحدود الجغرافية والسيادية، حيث يمكن لجهات خارجية أن تتدخل في الشؤون الداخلية لدولة ما عبر حملات إعلامية موجهة أو عبر نشر معلومات مضللة تستهدف التأثير على وعي المواطنين وتوجهاتهم السياسية، وقد أصبح هذا النوع من الحروب أكثر خطورة في ظل الانتشار الواسع لوسائل التواصل الاجتماعي، والتي أضحت منصة رئيسية لتداول الأخبار والمعلومات، سواء كانت صحيحة أو زائفة. هذا الانتشار الواسع للمعلومات دون رقابة كافية أتاح المجال لظهور ما يُعرف بـ"حروب السرديات"، حيث تتصارع الأطراف المختلفة لفرض رواياتها الخاصة للأحداث، بما يخدم مصالحها السياسية والاستراتيجية.

ومن ناحية أخرى يشكل الأمن السياسي أحد أهم ركائز استقرار الدولة، إذ يرتبط بقدرتها على الحفاظ على نظامها السياسي ومؤسساتها من التهديدات الداخلية والخارجية، ومع تطور الحروب المعلوماتية، بات هذا النوع من الأمن يواجه تحديات غير مسبوقة، حيث يمكن استهدافه بوسائل غير تقليدية مثل الهجمات السيبرانية، والتلاعب بالمعلومات، والتأثير على العمليات الانتخابية، وإثارة الانقسامات الاجتماعية، وإن هذه الأساليب تُمكّن الجهات الفاعلة من تحقيق أهدافها السياسية بأقل تكلفة ممكنة مقارنة بالحروب التقليدية، ما يجعلها خيارًا مغريًا للعديد من الدول والجماعات،

ولا يقتصر تأثير الحروب المعلوماتية على الجانب السياسي فحسب، بل يمتد ليشمل الجوانب الاقتصادية والاجتماعية والثقافية، ما يزيد من تعقيد عملية مواجهتها، فالتلاعب بالمعلومات يمكن أن يؤدي إلى فقدان الثقة في المؤسسات الحكومية، وإضعاف التماسك الاجتماعي، ونشر الفوضى والاضطراب داخل المجتمع، وأن استهداف البنية التحتية الرقمية للدولة قد يؤدي إلى تعطيل الخدمات الحيوية، ما ينعكس سلبًا على الاستقرار العام، ومن هنا أصبحت الحاجة ملحة لتطوير استراتيجيات فعالة لمواجهة هذا النوع

من التهديدات، ومن خلال تعزيز الوعي المجتمعي، وتطوير القدرات التقنية، ووضع أطر قانونية وتنظيمية تواكب طبيعة هذه التحديات.

وفي ضوء ما سبق، يتضح أن الحروب المعلوماتية لم تعد مجرد مفهوم نظري، بل أصبحت واقعًا ملموسًا يفرض نفسه على الساحة الدولية، ويستدعي اهتمامًا متزايدًا من قبل الباحثين وصناع القرار على حد سواء، ففهم طبيعة هذه الحروب وآليات عملها يُعد خطوة أساسية نحو بناء منظومة أمن سياسي قادرة على التصدي للتحديات الجديدة التي يفرضها العصر الرقمي، وعليه تسعى هذه الدراسة إلى تسليط الضوء على دور الحروب المعلوماتية في تهديد الأمن السياسي، ومن خلال تحليل أدواتها وأساليبها، واستكشاف آثارها المختلفة، وبيان السبل الممكنة لمواجهتها والحد من تأثيرها، بما يسهم في تعزيز استقرار الدول وحماية سيادتها في عالم يشهد تحولات متسارعة وغير مسبوقة.

مشكلة الدراسة:

تنبع مشكلة الدراسة في موضوع الحروب المعلوماتية ودورها في تهديد الأمن السياسي من التحولات العميقة التي شهدها العالم في طبيعة مصادر التهديد وأساليب الصراع بين الدول والمجتمعات، فمع التقدم التكنولوجي المتسارع، لم تعد التهديدات الأمنية مرتبطة فقط بالقوة العسكرية التقليدية أو المواجهات المباشرة، بل أصبحت تعتمد بشكل متزايد على أدوات غير مرئية تستهدف العقول والوعي قبل استهداف الأرض والسيادة، وفي هذا الإطار، برزت الحروب المعلوماتية كأحد أخطر أشكال الصراع الحديثة، نظرًا لقدرتها على التسلل إلى البنى الداخلية للدول والتأثير على استقرارها السياسي دون الحاجة إلى استخدام القوة الصلبة، ومن هنا تبرز الإشكالية الأساسية التي تسعى هذه الدراسة إلى معالجتها، والمتمثلة في فهم الكيفية التي تسهم بها الحروب المعلوماتية في تهديد الأمن السياسي، وتحديد حدود تأثيرها وآليات اشتغالها في السياق المعاصر.

وتتجسد هذه المشكلة في التداخل المعقد بين الفضاء الرقمي والواقع السياسي، حيث أصبح من الصعب الفصل بين ما هو إعلامي وما هو أمني، وما هو داخلي وما هو خارجي، فالمعلومات التي يتم تداولها عبر الوسائط الرقمية لم تعد مجرد وسيلة لنقل الأخبار، بل تحولت إلى أداة للتأثير والتوجيه وصناعة الرأي العام، وهذا ما يثير تساؤلات جوهرية حول مدى قدرة الدول على حماية فضائها المعلوماتي من الاختراق، وحول فعالية السياسات التقليدية في مواجهة تهديدات من هذا النوع، وأن تعدد الفاعلين في هذا المجال، سواء كانوا دولًا أو جماعات منظمة أو حتى أفرادًا، يزيد من تعقيد المشكلة، حيث يصبح من الصعب تحديد مصدر التهديد أو تحميل المسؤولية بشكل دقيق.

وتزداد حدة هذه الإشكالية في ظل الانتشار الواسع لوسائل التواصل الاجتماعي، التي وفرت بيئة خصبة لانتشار المعلومات المضللة والشائعات، ما يؤدي إلى خلق حالة من الارتباك وعدم اليقين داخل المجتمع،

فالتلاعب بالمعلومات يمكن أن يُستخدم لإضعاف الثقة في المؤسسات السياسية، وتشويه صورة القيادات، وإثارة الانقسامات الداخلية، وهو ما ينعكس بشكل مباشر على استقرار النظام السياسي، وفي هذا السياق تطرح الدراسة إشكاليات فرعية تتعلق بمدى تأثير الحملات الإعلامية الموجهة على سلوك الناخبين، وقدرة الجهات الخارجية على التدخل في العمليات السياسية الداخلية، إضافة إلى دور الذكاء الاصطناعي والتقنيات الحديثة في تضخيم هذه التأثيرات.

وتكمن المشكلة في الفجوة القائمة بين سرعة تطور أدوات الحروب المعلوماتية وبين بطء استجابة الأطر القانونية والمؤسساتية لمواجهتها، فالقوانين التقليدية غالبًا ما تكون غير كافية للتعامل مع الجرائم الرقمية أو الهجمات السيبرانية، وأن المؤسسات الأمنية قد تفتقر إلى الخبرات التقنية اللازمة لرصد هذه التهديدات والتصدي لها بفعالية، وهذا يطرح تساؤلات حول مدى جاهزية الدول وخاصة النامية منها، لمواجهة هذا النوع من الحروب، وحول الحاجة إلى تطوير استراتيجيات شاملة تجمع بين البعد الأمني والتقني والإعلامي.

ومن جانب آخر تتجلى مشكلة الدراسة في صعوبة قياس تأثير الحروب المعلوماتية بشكل دقيق، نظرًا لطبيعتها غير الملموسة وتداخلها مع عوامل أخرى سياسية واجتماعية وثقافية، فالتغيرات التي تحدث في الرأي العام أو في مستوى الثقة بالمؤسسات قد تكون نتيجة لتراكمات متعددة، مما يجعل من الصعب عزل أثر الحروب المعلوماتية عن غيرها من العوامل، وهذا ما يفرض تحديات منهجية على الباحثين في هذا المجال، ويستدعي استخدام مقاربات تحليلية متعددة لفهم هذه الظاهرة بشكل أعمق.

وعليه فإن أهمية هذه المشكلة لا تقتصر على بعدها الأكاديمي، بل تمتد لتشمل أبعادًا عملية تتعلق بصياغة السياسات العامة وتعزيز الأمن الوطني، ففهم طبيعة الحروب المعلوماتية وآثارها على الأمن السياسي يُعد خطوة أساسية نحو بناء استراتيجيات فعالة للتصدي لها، وضمان استقرار الأنظمة السياسية في مواجهة تحديات العصر الرقمي، ومن هنا تأتي هذه الدراسة كمحاولة للإسهام في سد الفجوة المعرفية في هذا المجال، وتقديم تحليل علمي يساعد على فهم أعمق لهذه الظاهرة المعقدة والمتغيرة باستمرار.

تساؤلات الدراسة:

انطلاقًا من مشكلة الدراسة وأهميتها، تم صياغة عدد من التساؤلات التي تسعى إلى توجيه البحث وتحليل أبعاده المختلفة، وذلك على النحو الآتي:

1. كيف تسهم الحروب المعلوماتية في إعادة تشكيل طبيعة التهديدات التي تواجه الأمن السياسي في الدول المعاصرة؟
2. إلى أي مدى تؤثر المعلومات المضللة والحملات الرقمية الموجهة على استقرار الأنظمة السياسية وثقة المواطنين بمؤسسات الدولة؟

3.ما هي أبرز الآليات والأدوات التي تستخدمها الحروب المعلوماتية لاختراق الفضاء السياسي والتأثير في صنع القرار؟

4.كيف يمكن للدول تطوير استراتيجيات فعالة لمواجهة الحروب المعلوماتية والحد من انعكاساتها على أمنها السياسي؟

أهداف الدراسة:

بناءً على مشكلة الدراسة وتساؤلاتها يهدف هذا البحث إلى تحقيق مجموعة من الأهداف التي تُسهم في فهم أعمق لموضوعه وتسليط الضوء على أبرز العوامل المرتبطة به، وذلك من خلال ما يلي:

1.التعرف على دور الحروب المعلوماتية في إعادة تشكيل طبيعة التهديدات التي تواجه الأمن السياسي في الدول المعاصرة.

2.التعرف على مدى تأثير المعلومات المضللة والحملات الرقمية الموجهة على استقرار الأنظمة السياسية ومستوى ثقة المواطنين بمؤسسات الدولة.

3.التعرف على أبرز الآليات والأدوات التي توظفها الحروب المعلوماتية لاختراق الفضاء السياسي والتأثير في عملية صنع القرار.

4.التعرف على الاستراتيجيات الفعالة التي يمكن للدول تبنيها لمواجهة الحروب المعلوماتية والحد من انعكاساتها على أمنها السياسي.

أهمية الدراسة: تتمثل أهمية الدراسة نظرياً وتطبيقياً في التالي:

الأهمية النظرية:

1- تتمثل الأهمية النظرية لهذه الدراسة في التعرف على الإطار المفاهيمي للحروب المعلوماتية وتحديد أبعادها وعلاقتها بالأمن السياسي في ظل التحولات الرقمية المعاصرة.

2- تسهم في التعرف على طبيعة التهديدات غير التقليدية وتطوير الفهم الأكاديمي لكيفية انتقال الصراع من المجال المادي إلى المجال المعلوماتي.

3- تساعد في التعرف على النماذج والنظريات المفسرة لتأثير المعلومات المضللة والحملات الرقمية في تشكيل الرأي العام وصنع القرار السياسي.

4- تعزز من التعرف على الفجوات المعرفية في الأدبيات العلمية المتعلقة بالحروب المعلوماتية، بما يفتح المجال لمزيد من الدراسات المستقبلية في هذا المجال.

الأهمية التطبيقية:

1-تتمثل الأهمية التطبيقية في التعرف على آليات عملية يمكن من خلالها تعزيز قدرة الدول على مواجهة تهديدات الحروب المعلوماتية.

2-تسهم في التعرف على سبل تطوير السياسات العامة والاستراتيجيات الأمنية لحماية الأمن السياسي من التأثيرات الرقمية السلبية.

3-تساعد صناع القرار في التعرف على أدوات رصد وتحليل المعلومات المضللة واتخاذ الإجراءات المناسبة للحد من انتشارها.

4-تعزز من التعرف على أهمية رفع الوعي المجتمعي والتثقيف الإعلامي لمواجهة الحملات الرقمية الموجهة وتقوية الثقة بالمؤسسات.

مفاهيم الدراسة:

تقتضي طبيعة هذا البحث توضيح المفاهيم الرئيسة المرتبطة بموضوعه، لضمان الدقة في الفهم والتحديد الإجرائي للمصطلحات المستخدمة.

الحروب المعلوماتية: هي نمط حديث من أنماط الصراع يعتمد على توظيف المعلومات ووسائل الاتصال الرقمية كأداة استراتيجية للتأثير على الخصم، من خلال التلاعب بالبيانات، ونشر المعلومات المضللة، والتأثير في الإدراك الجماعي وصنع القرار، بهدف تحقيق مكاسب سياسية دون استخدام القوة العسكرية التقليدية. (على الحسيني ،2020، ص45).

الأمن السياسي: هو قدرة الدولة على الحفاظ على استقرار نظامها السياسي ومؤسساتها الدستورية، وضمان شرعيتها واستمراريتها، وحمايتها من التهديدات الداخلية والخارجية التي قد تؤثر في توازنها أو تعرّضها للاضطراب أو الانهيار. (نجلاء الشافعي،2018، ص 78).

أولاً_ الحروب المعلوماتية وتحول أنماط التهديدات للأمن السياسي في الدول المعاصرة:

تُسهم الحروب المعلوماتية بشكل جوهري في إعادة تشكيل طبيعة التهديدات التي تواجه الأمن السياسي في الدول المعاصرة، ومن خلال إحداث تحول عميق في مفهوم الصراع ذاته، حيث لم يعد مقتصرًا على المواجهات العسكرية التقليدية أو الضغوط الاقتصادية المباشرة، بل أصبح يعتمد على أدوات غير مرئية تستهدف الوعي والإدراك الجمعي للمجتمعات، فالمعلومة في العصر الرقمي لم تعد مجرد وسيلة لنقل الحقيقة، بل تحولت إلى أداة استراتيجية تُستخدم في التأثير والتوجيه، الأمر الذي جعل من البيئة المعلوماتية ساحة رئيسية للصراع بين الدول والفاعلين المختلفين، وفي هذا السياق أصبحت التهديدات التي تواجه الأمن السياسي أكثر تعقيدًا وتشابكًا، نظرًا لاعتمادها على وسائل يصعب رصدها أو مواجهتها بالطرق التقليدية(سامر الزغبي،2021، ص 97).

ولقد أدت الحروب المعلوماتية إلى نقل مركز الثقل في الصراع من المجال المادي إلى المجال المعنوي، حيث يتم استهداف القيم والمعتقدات والثقة العامة بدلًا من البنى التحتية فقط، فبدلًا من تدمير المنشآت أو احتلال الأراضي، يتم العمل على زعزعة ثقة المواطنين في مؤسساتهم السياسية، وإضعاف الروابط

الاجتماعية، ونشر الشكوك حول شرعية النظام الحاكم، وهذا النوع من التهديد يُعد أكثر خطورة، لأنه يعمل بشكل تدريجي وغير مباشر، وغالبًا ما يكون تأثيره طويل الأمد، ما يجعل من الصعب اكتشافه أو احتواؤه في مراحله الأولى، وأن هذه الحروب تعتمد على استراتيجيات دقيقة تستهدف فئات محددة داخل المجتمع، مستفيدة من البيانات الضخمة والتحليل السلوكي لتوجيه الرسائل بشكل يتناسب مع ميول الأفراد واتجاهاتهم(فاطمة الكردي،2019، ص32).

ومن أبرز مظاهر إعادة تشكيل التهديدات في ظل الحروب المعلوماتية هو تزايد الاعتماد على المعلومات المضللة كأداة رئيسية للتأثير في الرأي العام، فانتشار الأخبار الزائفة والمحتوى المشوه عبر وسائل التواصل الاجتماعي يُسهم في خلق بيئة من الارتباك وعدم اليقين، حيث يصبح من الصعب على الأفراد التمييز بين الحقيقة والزيف، وهذا الوضع يُضعف من قدرة المواطنين على اتخاذ قرارات واعية، ويجعلهم أكثر عرضة للتأثر بالدعاية السياسية، ما قد يؤدي إلى نتائج خطيرة على مستوى الاستقرار السياسي، وأن تكرار هذه المعلومات المضللة بشكل مكثف قد يؤدي إلى ترسيخها في أذهان الناس، حتى وإن كانت غير صحيحة، وهو ما يُعرف بتأثير "الحقيقة الوهمية "وإضافة إلى ذلك أسهمت الحروب المعلوماتية في توسيع دائرة الفاعلين في مجال التهديدات السياسية، حيث لم تعد هذه التهديدات حكرًا على الدول، بل أصبحت تشمل جماعات منظمة، وشركات تكنولوجية، وحتى أفرادًا يمتلكون القدرة على التأثير من خلال المنصات الرقمية. هذا التعدد في مصادر التهديد يُعقّد من عملية المواجهة، وإذ يصبح من الصعب تحديد الجهة المسؤولة عن الهجوم أو التأثير، ويفتح المجال أمام استخدام أساليب غير تقليدية مثل الحسابات الوهمية والروبوتات الإلكترونية لنشر المحتوى الموجه والتأثير في النقاشات العامة(ياسر منصور،2022، ص50-52) وكما هو معروف من أن الحروب المعلوماتية أعادت تشكيل مفهوم السيادة السياسية، حيث أصبح الفضاء الرقمي مجالًا مفتوحًا للتدخل الخارجي في الشؤون الداخلية للدول، فبإمكان جهات خارجية أن تؤثر في العمليات السياسية، مثل الانتخابات أو الاستفتاءات، ومن خلال حملات رقمية موجهة تستهدف الناخبين وتعمل على تغيير توجهاتهم، وهذا النوع من التدخل لا يترك آثارًا مادية واضحة، لكنه قد يؤدي إلى تغييرات عميقة في المشهد السياسي، ويُقوّض من مبدأ الاستقلالية السياسية للدولة، وبالتالي فإن الأمن السياسي لم يعد مرتبطًا فقط بحماية الحدود الجغرافية، بل أصبح يشمل أيضًا حماية الفضاء المعلوماتي من الاختراق والتلاعب.

ومن ناحية أخرى أدت الحروب المعلوماتية إلى تسريع وتيرة الأزمات السياسية، حيث يمكن لمعلومة مضللة أو خبر كاذب أن ينتشر بسرعة كبيرة ويُحدث ردود فعل فورية داخل المجتمع، مما قد يؤدي إلى تصعيد الأوضاع بشكل مفاجئ، وهذا ما يجعل من إدارة الأزمات أكثر صعوبة، إذ يتعين على صناع القرار التعامل مع تدفقات هائلة من المعلومات في وقت قصير، مع ضرورة التحقق من صحتها واتخاذ

قرارات مناسبة بناءً عليها، وأن هذه السرعة في انتشار المعلومات تُقلل من فعالية الردود الرسمية، التي غالبًا ما تكون أبطأ من الحملات الرقمية، مما يمنح الجهات المهاجمة أفضلية في التأثير.

ولا يمكن إغفال الدور الذي تلعبه التقنيات الحديثة، مثل الذكاء الاصطناعي، في تعزيز فعالية الحروب المعلوماتية، حيث أصبح بالإمكان إنتاج محتوى مزيف عالي الجودة، مثل الفيديوهات المفبركة أو الأصوات المقلدة، ما يزيد من صعوبة اكتشاف التلاعب ويُعزز من تأثيره على المتلقين، وهذه التطورات التقنية تُضيف بُعدًا جديدًا للتهديدات، وتجعل من الضروري تطوير أدوات متقدمة لرصدها والتعامل معها (هند العبيدي،2020، ص 56،57).

وفي ضوء ما سبق يتضح أن الحروب المعلوماتية لم تُضف فقط نوعًا جديدًا من التهديدات إلى الأمن السياسي، بل أعادت تشكيل طبيعة هذه التهديدات بشكل جذري، من حيث أدواتها وفاعليها وآليات تأثيرها. فهي تهديدات غير متماثلة، عابرة للحدود، تعتمد على التأثير النفسي والإدراكي أكثر من القوة المادية، وتستهدف بنية النظام السياسي من الداخل، وهذا التحول يفرض على الدول إعادة النظر في استراتيجياتها الأمنية، وتبني مقاربات شاملة تأخذ في الاعتبار الأبعاد التقنية والإعلامية والاجتماعية، وبما يضمن حماية الأمن السياسي في عصر تتداخل فيه الحقيقة مع التضليل، وتصبح فيه المعلومة سلاحًا لا يقل خطورة عن أي سلاح تقليدي.

ثانياً- تأثير المعلومات المضللة والحملات الرقمية الموجهة على استقرار الأنظمة السياسية وثقة المواطنين بمؤسسات الدولة:

يُعدّ التحول في طبيعة التهديدات التي تواجه الأمن السياسي في الدول المعاصرة من أبرز ملامح العصر الرقمي، حيث لم تعد هذه التهديدات محصورة في الأطر التقليدية المرتبطة بالقوة العسكرية أو الضغوط الجيوسياسية المباشرة، بل أصبحت تتخذ أشكالًا أكثر تعقيدًا ومرونة بفعل بروز الحروب المعلوماتية كأداة مركزية في إدارة الصراع. لقد أفرز التقدم الهائل في تكنولوجيا المعلومات والاتصال بيئة جديدة تتسم بالسيولة والتداخل، حيث تتشابك فيها الأبعاد السياسية والإعلامية والتقنية، ما أدى إلى إعادة تعريف مفهوم الأمن السياسي ذاته، وفي هذا السياق لم يعد الحفاظ على استقرار النظام السياسي مرهونًا فقط بحماية الحدود أو ردع التهديدات الخارجية، بل أصبح مرتبطًا بقدرة الدولة على التحكم في فضائها المعلوماتي، وصون وعي مواطنيها من التأثيرات الخارجية والداخلية التي تستهدف إعادة تشكيل إدراكهم للواقع. (محمود العطار،2019، 23-88)

وإن الحروب المعلوماتية بوصفها نمطًا مستحدثًا من أنماط الصراع، تقوم على استغلال المعلومات كأداة للتأثير الاستراتيجي، حيث يتم توظيفها ليس فقط لنقل الحقائق، بل لإعادة صياغتها بما يخدم أهدافًا سياسية محددة، ومن هنا يتجلى أحد أهم أوجه التحول في طبيعة التهديدات، والمتمثل في الانتقال من

التهديدات المادية المباشرة إلى التهديدات غير الملموسة التي تستهدف البنية الذهنية والمعرفية للمجتمع، فبدلًا من تدمير البنية التحتية أو إسقاط الأنظمة بالقوة، يتم العمل على تقويض أسس الشرعية السياسية من خلال نشر الشكوك، وزعزعة الثقة، وإثارة الانقسامات الداخلية، وهذا النوع من التهديد يُعد أكثر خطورة، لأنه يتسلل إلى داخل المجتمع بشكل تدريجي، ويعمل على تفكيك تماسكه من الداخل دون أن يترك آثارًا واضحة يمكن التعامل معها بالوسائل التقليدية.

فالحروب المعلوماتية أعادت تشكيل طبيعة الفاعلين في مجال التهديدات السياسية، حيث لم تعد الدولة هي الفاعل الوحيد أو حتى الرئيسي في بعض الأحيان، بل ظهرت إلى جانبها أطراف متعددة تشمل جماعات منظمة، وشبكات إعلامية، وشركات تكنولوجية، بل وحتى أفراد يمتلكون القدرة على التأثير عبر المنصات الرقمية، وهذا التعدد في الفاعلين يُنتج بيئة معقدة يصعب فيها تحديد مصدر التهديد بدقة، ويُضعف من فعالية الردود التقليدية التي تقوم على مبدأ المواجهة المباشرة بين أطراف محددة، ونتيجة لذلك أصبح الأمن السياسي يواجه تهديدات موزعة وغير متماثلة، تتسم بالمرونة والقدرة على التكيف مع مختلف السياقات.(سليم البدر،2021، ص11-14).

وفي إطار هذا التحول برزت المعلومات المضللة كأحد أخطر أدوات الحروب المعلوماتية، حيث يتم استخدامها بشكل ممنهج لإعادة تشكيل وعي الأفراد والتأثير في مواقفهم السياسية، وإن انتشار الأخبار الزائفة والمحتوى المشوه عبر وسائل التواصل الاجتماعي يُسهم في خلق حالة من الفوضى المعرفية، حيث تتداخل الحقائق مع الأكاذيب، ويصبح من الصعب على الأفراد التمييز بينهما، وهذه الحالة لا تؤثر فقط على مستوى الوعي الفردي، بل تمتد لتشمل البنية الكلية للنظام السياسي، ومن خلال إضعاف الثقة في المؤسسات، وتقويض مصداقية الخطاب الرسمي، وفتح المجال أمام انتشار نظريات المؤامرة والخطابات الشعبوية، ومن ثم فإن التهديد لم يعد يقتصر على الفعل الخارجي، بل أصبح يتجسد في تفاعلات داخلية يغديها تدفق المعلومات غير المنضبط.

ومن جهة أخرى أسهمت الحروب المعلوماتية في إعادة تعريف مفهوم السيادة السياسية، حيث لم تعد الحدود الجغرافية تمثل حاجزًا حقيقيًا أمام التدخل الخارجي، فالفضاء الرقمي أتاح إمكانية الوصول المباشر إلى المجتمعات، والتأثير في توجهاتها دون الحاجة إلى وجود مادي على الأرض، وهذا ما يجعل من الأمن السياسي عرضة لاختراقات مستمرة، قد تأتي من جهات غير مرئية أو يصعب تتبعها، وأن هذا النوع من التهديد يُقوّض من قدرة الدولة على التحكم في المجال العام، حيث تصبح السرديات المتداولة خارج نطاق السيطرة، وتتنافس فيها أطراف متعددة على فرض رؤاها وتفسيراتها للأحداث.(احمد المطيري،2018،ص 44-88).

ولا يقتصر تأثير الحروب المعلوماتية على المستوى الداخلي فقط، بل يمتد ليشمل العلاقات الدولية، حيث تُستخدم كأداة لتحقيق مكاسب استراتيجية دون الدخول في مواجهات مباشرة، فالدول قد تلجأ إلى استخدام الحملات المعلوماتية للتأثير في استقرار دول أخرى، أو لإضعاف خصومها سياسيًا، أو حتى لإعادة تشكيل موازين القوة على الساحة الدولية، وهذا ما يجعل من الحروب المعلوماتية عنصرًا أساسيًا في معادلة القوة الحديثة، حيث لم يعد التفوق العسكري وحده كافيًا لضمان الأمن، بل أصبح التفوق المعلوماتي لا يقل أهمية، إن لم يكن أكثر تأثيرًا.

وأن التطور التكنولوجي وخاصة في مجال الذكاء الاصطناعي وتحليل البيانات، قد أضفى بُعدًا جديدًا على طبيعة هذه التهديدات، حيث أصبح بالإمكان تصميم حملات معلوماتية دقيقة تستهدف فئات محددة من المجتمع بناءً على خصائصها النفسية والسلوكية، وهذا المستوى من التخصيص يزيد من فعالية التأثير، ويجعل من الصعب مقاومته، خاصة في ظل غياب الوعي الكافي لدى الأفراد، ومن ثم فإن التهديد لم يعد عامًا أو عشوائيًا، بل أصبح موجهًا بدقة، ويستند إلى فهم عميق لطبيعة المجتمعات المستهدفة.

وفي ضوء هذه التحولات يتضح أن الحروب المعلوماتية قد أسهمت في إعادة تشكيل طبيعة التهديدات التي تواجه الأمن السياسي بشكل جذري، من حيث أدواتها، وفاعليها، وآليات تأثيرها، فهي تهديدات تتسم بالخفاء، والسرعة، والقدرة على التكيف، وتعتمد على التأثير النفسي والمعرفي أكثر من الاعتماد على القوة المادية، وهذا ما يفرض على الدول ضرورة إعادة النظر في مفاهيمها التقليدية للأمن، وتبني مقاربات جديدة تأخذ في الاعتبار الأبعاد الرقمية والإعلامية، وتعزز من قدرتها على حماية فضائها المعلوماتي، وصون استقرارها السياسي في عالم باتت فيه المعلومة أداة صراع لا تقل خطورة عن أي سلاح تقليدي.

ثالثاً– أبرز الآليات والأدوات التي تستخدمها الحروب المعلوماتية لاختراق الفضاء السياسي والتأثير في صنع القرار:

تُعَدّ الحروب المعلوماتية من أبرز التحولات في طبيعة الصراع السياسي الحديث، إذ لم يعد التهديد السياسي محصورًا في القوة العسكرية أو الضغوط الاقتصادية التقليدية، بل امتد ليشمل الفضاء الرقمي والمعلوماتي، حيث تُستخدم مجموعة معقدة من الأدوات والآليات لاستهداف الوعي العام وصنع القرار السياسي، وتشكل هذه الحروب تهديدًا متعدد الأبعاد، إذ تدمج بين التأثير النفسي والإعلامي والتقني بطريقة تجعل من الصعب التعرف على مصادرها أو مواجهتها بالأساليب التقليدية، ويمكن القول إن جوهر هذه الحروب يكمن في القدرة على استخدام المعلومات كسلاح استراتيجي لإعادة تشكيل التصورات المجتمعية، وزعزعة الثقة في المؤسسات السياسية، وإحداث تغييرات ملموسة في الأولويات السياسية للدولة المستهدفة.(ريم الشامي،2022، ص 76،77).

وأحد أبرز الآليات المستخدمة في الحروب المعلوماتية يتمثل في المعلومات المضللة، وهي أدوات رقمية تستخدم لنشر الأخبار الكاذبة أو المشوهة بغرض التأثير على وعي الأفراد والجماعات. وتنتشر هذه المعلومات بشكل واسع عبر وسائل التواصل الاجتماعي والمواقع الإلكترونية المدفوعة، حيث تصل إلى جمهور واسع بسرعة تفوق قدرة المؤسسات الرسمية على الرد عليها وتصحيحها، وتكمن خطورة هذه الآلية في قدرتها على التأثير النفسي بشكل مباشر، إذ تعمل على تشكيل إدراك الأفراد للواقع السياسي بما يخدم أهداف الجهات المهاجمة، وتخلق حالة من عدم اليقين والفوضى المعرفية، وهو ما يضعف قدرة الدولة على الحفاظ على استقرارها الداخلي ويزيد من هشاشة النظام السياسي.

وإلى جانب المعلومات المضللة، تلعب الحملات الرقمية الموجهة دورًا رئيسيًا في التأثير على صنع القرار السياسي، حيث تعتمد هذه الحملات على تحليل البيانات الضخمة وفهم السلوكيات النفسية والاجتماعية للمستهدفين، ويتم تصميم الرسائل بعناية لتناسب خصائص الجمهور المستهدف، سواء من خلال الترويج لروايات معينة أو تشويه صورة الخصوم السياسيين أو تحفيز الانقسامات المجتمعية، وغالبًا ما تُستخدم في هذه الحملات الروبوتات الإلكترونية والحسابات الوهمية لتضخيم انتشار الرسائل، ما يزيد من تأثيرها ويخلق وهم الشعبية أو الرأي العام المساند لها، وبفضل هذه الأدوات تستطيع الجهات الفاعلة توجيه النقاش العام بطريقة دقيقة ومؤثرة، بحيث تصبح القدرة على اتخاذ قرارات واعية لدى الأفراد والجماعات محدودة للغاية(خالد الهاشمي،2021، ص 93،94).

وتُستثمر الهجمات السيبرانية ضمن مجموعة الآليات الأساسية للحروب المعلوماتية، حيث يتم استهداف البنى التحتية الرقمية للدولة مثل قواعد البيانات الحكومية، والأنظمة الانتخابية، والمنصات الإعلامية الرسمية. وتهدف هذه الهجمات إلى سرقة المعلومات، أو تعطيل الخدمات الحيوية، أو نشر الفوضى التنظيمية التي تعيق قدرة الدولة على اتخاذ قراراتها بشكل سليم، ويكمن التحدي في صعوبة تحديد مصدر هذه الهجمات بدقة، ما يمنح الجهات المهاجمة أفضلية استراتيجية ويجعل الأمن السياسي عرضة لاختراقات غير مرئية لكنها ذات تأثير بالغ على الاستقرار الداخلي.

وتشكل أدوات التلاعب النفسي والإعلامي جزءًا محوريًا من استراتيجيات الحروب المعلوماتية، حيث يتم تصميم محتوى رقمي مؤثر باستخدام تقنيات الذكاء الاصطناعي لإنشاء فيديوهات مزيفة أو تسجيلات صوتية مفبركة، وتستهدف هذه الآلية إعادة صياغة التصورات العامة لدى المجتمع، بحيث تُقدم الحقائق والمعلومات بشكل مشوه يجعلها قابلة للتأثير على سلوكيات الأفراد واتجاهاتهم السياسية، ويؤدي ذلك إلى تغييرات تدريجية في مواقف المواطنين تجاه النظام السياسي، ويقلل من مصداقية المؤسسات الرسمية، وهو ما ينعكس على استقرار الدولة وقدرتها على مواجهة الأزمات(منى ياسين،2020، ص 66-102).

وتتضمن الآليات أيضًا استهداف الرأي العام بشكل مباشر، من خلال مراقبة الاتجاهات العامة وتحليلها باستخدام أدوات التحليل الرقمي، ومن ثم توجيه الرسائل الرقمية وفقًا للنتائج المكتشفة، وتتيح هذه الآلية فرض سرديات محددة على المجتمع، والتحكم في النقاشات العامة بحيث تخدم مصالح الجهة المهاجمة، ويُعد هذا النوع من التأثير غير المرئي أحد أخطر أساليب الحروب المعلوماتية، لأنه يعمل على إعادة تشكيل الإدراك الجمعي بشكل تدريجي، ويجعل من الصعب على الأفراد والقيادات السياسية مقاومة هذه التوجهات أو مواجهتها بفعالية.

وكما تُستخدم شبكة العلاقات الرقمية كأداة مساعدة لتعزيز تأثير الحروب المعلوماتية، حيث يتم بناء تحالفات بين وسائل الإعلام الإلكترونية، والمنصات الرقمية، والمراكز البحثية، بهدف زيادة انتشار الرسائل الموجهة وإخفاء مصادرها الحقيقية، وتُستثمر هذه الشبكات لتضخيم محتوى محدد، ولخلق بيئة يسودها التأثير المتبادل بين وسائل الإعلام والمجتمع، ما يزيد من صعوبة السيطرة على تدفق المعلومات المضللة. (حسين البغدادي،2019، ص114،115). ويترتب على هذه الأدوات والآليات أن الحروب المعلوماتية لم تعد مجرد تهديد تكتيكي أو مؤقت، بل أصبحت تشكل تهديدًا استراتيجيًا طويل الأمد للأمن السياسي، إذ تعمل على تفكيك أسس الشرعية السياسية، وزعزعة الثقة في المؤسسات، وإعادة تشكيل مواقف المواطنين تجاه الدولة وسياستها، ولذلك فإن مواجهة هذه التهديدات تتطلب تطوير استراتيجيات شاملة تأخذ بعين الاعتبار الأبعاد التقنية والنفسية والإعلامية، وتعزز القدرة على رصد المعلومات المضللة، وحماية الفضاء الرقمي، ورفع وعي المجتمع حول كيفية التعامل مع الحملات الرقمية الموجهة.

وإن فهم هذه الآليات والأدوات يمثل خطوة أساسية لصياغة سياسات أمنية فاعلة، فهو يتيح للدولة ليس فقط رصد التهديدات واستجابتها في الوقت المناسب، بل يمكّنها من الحد من تأثير الحروب المعلوماتية على صنع القرار السياسي واستقرار النظام العام. كما أن دراسة هذه الأدوات تُساعد في تعزيز قدرات الأمن السيبراني وبناء مقاومة جماعية ضد التلاعب بالمعلومات، بما يضمن استمرار شرعية المؤسسات السياسية وثقة المواطنين بها في مواجهة التحديات الرقمية المتسارعة والمعقدة. (سامي الكيلاني،2018، ص 53،54).

رابعاً- تطوير استراتيجيات فعالة لمواجهة الحروب المعلوماتية والحد من انعكاساتها على الأمن السياسي: مع تزايد المخاطر الناتجة عن الحروب المعلوماتية وتعقيد تهديداتها للأمن السياسي، باتت الحاجة ماسة للدول لتبني استراتيجيات فعالة قادرة على مواجهة هذا النوع الحديث من الصراعات، والحد من انعكاساته السلبية على استقرار الأنظمة السياسية، ويترتب على الفشل في تطوير هذه الاستراتيجيات تعرض الدولة لهزات سياسية، وفقدان الثقة في مؤسساتها، وتراجع قدرتها على اتخاذ القرارات الصائبة في

الأزمات، وهو ما يجعل تطوير إطار متكامل لمواجهة الحروب المعلوماتية أولوية استراتيجية تتطلب الجمع بين البعد الأمني، والتقني، والإعلامي، والاجتماعي في آن واحد.

وتبدأ عملية تطوير الاستراتيجيات بضرورة إدراك طبيعة الحروب المعلوماتية والآليات التي تستخدمها، وفهم أن هذه الحروب تعتمد على استهداف الوعي الجمعي وصنع القرار أكثر من استهداف البنية المادية للدولة، وأن أي استراتيجية فعالة يجب أن تكون شاملة، تدمج بين الوقاية والرصد والاستجابة السريعة والتصحيح المستمر للأضرار التي يمكن أن تسببها المعلومات المضللة، وفي هذا السياق يُعد تعزيز الأمن السيبراني وتطوير قدرات الرصد الرقمي أحد الأسس الحيوية لهذه الاستراتيجية، حيث يسمح للجهات الرسمية بالكشف المبكر عن الحملات الرقمية الموجهة والهجمات الإلكترونية قبل أن تتسبب في إحداث أضرار كبيرة، ويُمكّن الدولة من حماية بياناتها الحساسة والبنية التحتية الرقمية من الاختراق، بما يعزز من قدرتها على الحفاظ على سيادتها الرقمية والسياسية(هناء الزهراني،2021، ص 81-85).

وإضافة إلى ذلك لا تقل أهمية تطوير القدرات البشرية والتدريب المتخصص عن الجانب التقني، إذ يشكل العنصر البشري حجر الزاوية في أي استراتيجية فعالة، فبناء فرق متخصصة في تحليل البيانات الرقمية، وفهم السلوكيات النفسية والاجتماعية للمجتمع، ومتابعة السرديات الإعلامية المتغيرة باستمرار يُمكّن الدولة من تصميم ردود فعّالة وسريعة على التهديدات، ويتيح صقل السياسات العامة بحيث تكون أكثر مرونة واستجابة للمتغيرات الرقمية، ويشمل ذلك تدريب المسؤولين وصناع القرار على التعرف على الحملات الرقمية المضللة، ورفع مستوى الوعي لديهم حول تأثيرها على الرأي العام وصنع القرار السياسي، ما يُحسّن من قدرتهم على اتخاذ مواقف حاسمة تجاه أي تهديد يظهر في الفضاء الرقمي.

وتلعب آليات التثقيف الإعلامي والوعي المجتمعي دورًا محوريًا في الحد من تأثير الحروب المعلوماتية، وإذ يمكن من خلال برامج توعية منهجية تعليم المواطنين كيفية التحقق من المعلومات، وتمكينهم من التمييز بين الأخبار الصحيحة والمضللة، وهو ما يقلل من قدرة الجهات المهاجمة على خلق انقسامات داخل المجتمع أو التأثير على الاتجاهات السياسية، ويتيح هذا البعد الشعبي تعزيز الثقة بالمؤسسات الرسمية، وتقوية الروابط بين الدولة والمجتمع، بحيث تصبح قوة المجتمع الرقمي جزءًا من منظومة الدفاع ضد التلاعب بالمعلومات والحملات الرقمية الموجهة.

ومن الناحية المؤسسية يحتاج تطوير الاستراتيجيات إلى وضع أطر قانونية وتنظيمية واضحة تتوافق مع طبيعة العصر الرقمي، بحيث تضمن حماية المعلومات الشخصية والبيانات الحكومية، وتضع معايير للتعامل مع الأخبار المضللة والحملات الرقمية التي تهدد الأمن السياسي، وتشمل هذه الأطر وضع قوانين لمكافحة الهجمات السيبرانية، وتنظيم عمل وسائل الإعلام الرقمية، وضمان الشفافية في العمليات الانتخابية والسياسية، بما يحد من قدرة الجهات الفاعلة على استغلال الفضاء الرقمي لإضعاف الدولة،

ويؤدي وجود هذه القوانين إلى خلق بيئة مستقرة تسمح بالتعامل مع الأزمات الرقمية بطريقة منظمة وفعالة، ويعزز من مصداقية الدولة أمام مواطنيها والمجتمع الدولي على حد سواء(لطيفة الشريف،2020، ص 102-146).

وينبغي للدول أن تستثمر التكنولوجيا الحديثة في تطوير استراتيجياتها، لا سيما الذكاء الاصطناعي والتحليل الرقمي، بحيث يتمكن صانع القرار من تتبع الحملات الرقمية بدقة، وفهم طبيعة التأثيرات على المجتمع، والتنبؤ بالاتجاهات المستقبلية، وبالتالي التفاعل معها قبل أن تتفاقم آثارها، ويتيح استخدام هذه الأدوات إمكانية إنتاج حلول مبتكرة لمواجهة التهديدات الرقمية بشكل فوري، بما يضمن استمرارية صنع القرار السياسي دون تعطيل أو انحراف عن الأهداف الاستراتيجية للدولة.

ولا يمكن إغفال البعد الدولي في تطوير هذه الاستراتيجيات، إذ إن الحروب المعلوماتية غالبًا ما تكون عابرة للحدود، ويشارك فيها فاعلون خارجيون يسعون للتأثير في سياسات الدولة من دون مواجهة مباشرة، ولذا فإن التعاون الدولي وتبادل الخبرات والمعلومات بين الدول أصبح جزءًا أساسيًا من أي استراتيجية ناجحة، وحيث يمكن من خلاله تعزيز القدرات الدفاعية، وتنسيق الجهود لرصد التهديدات العابرة للحدود، ومواجهة الحملات الرقمية المشتركة التي قد تستهدف أكثر من دولة في الوقت نفسه، ويؤدي هذا التعاون إلى خلق منظومة دفاعية رقمية أكثر تكاملًا، تضمن حماية الأمن السياسي على مستوى الإقليمي والدولي (أحمد يوسف،2018، ص78)

وفي النهاية يظهر أن تطوير استراتيجيات فعالة لمواجهة الحروب المعلوماتية يتطلب رؤية شاملة تدمج بين الأبعاد التقنية والبشرية والقانونية والمجتمعية والدولية، بحيث تكون الدولة قادرة على حماية فضائها المعلوماتي، وتعزيز الثقة بمؤسساتها، وضمان استقرارها السياسي في مواجهة تهديدات العصر الرقمي، فنجاح هذه الاستراتيجيات لا يعتمد فقط على الإجراءات التقنية أو القانونية، بل على قدرة الدولة على تفعيل قدراتها المؤسسية، ورفع مستوى وعي مجتمعها، واستثمار التكنولوجيا الحديثة بشكل مستدام، ما يضمن قدرتها على مواجهة التحديات المتغيرة للحروب المعلوماتية والحفاظ على استقرار النظام السياسي في ظل عالم رقمي متسارع التغيرات.

الدراسات السابقة:

تُعد الدراسات السابقة ركيزة أساسية في البحث العلمي، إذ تسهم في بناء الإطار المعرفي للموضوع وتحديد الاتجاهات البحثية ذات الصلة به، وقد تناولت العديد من الدراسات المحلية قضايا التهديدات السيبرانية والحروب الرقمية وانعكاساتها على الأمن القومي والأمن السياسي، في ظل التطورات التكنولوجية المتسارعة التي يشهدها العالم المعاصر، وتكتسب هذه الدراسات أهمية خاصة لكونها تسلط الضوء على طبيعة المخاطر الرقمية التي تواجه الدولة الليبية وتأثيرها في استقرار مؤسساتها وقدرتها على

حماية فضائها المعلوماتي، وفيما يلي عرض لأبرز الدراسات السابقة ذات العلاقة بموضوع الحروب المعلوماتية ودورها في تهديد الأمن السياسي.

دراسة سليمة مصباح حامد، بعنوان: "التهديدات السيبرانية وانعكاساتها على الأمن القومي الليبي: التأسيس وآليات التحصين المعرفي"، بحث منشور في المؤتمر العلمي الدولي الرابع لكلية الاقتصاد والتجارة، جامعة الأسمرية الإسلامية، ليبيا، (2023).

هدفت الدراسة إلى التعرف على طبيعة التهديدات السيبرانية وانعكاساتها على الأمن القومي الليبي، وبيان أهم الآليات والاستراتيجيات اللازمة لمواجهتها وتعزيز التحصين المعرفي للمجتمع والدولة، واعتمدت الباحثة المنهج الوصفي التحليلي في تحليل الظاهرة السيبرانية وأبعادها الأمنية.

وتوصلت الدراسة إلى النتائج الآتية:

أكدت النتائج أن التهديدات السيبرانية أصبحت من أبرز التحديات التي تواجه الأمن القومي الليبي.

بينت الدراسة أن اختراق الأنظمة والمعلومات الحكومية ينعكس بصورة مباشرة على الاستقرار السياسي والأمني.

أوصت الدراسة بضرورة تطوير استراتيجيات وطنية للأمن السيبراني وتعزيز الوعي المجتمعي بمخاطر التهديدات الرقمية.

دراسة الوليد عبد المجيد عصمان، بعنوان: "أثر التهديدات السيبرانية على الأمن القومي في ليبيا"، بحث منشور في مجلة جامعة درنة للعلوم الإنسانية والاجتماعية، ليبيا، (2025).

هدفت الدراسة إلى تحليل تأثير التهديدات والهجمات السيبرانية على مؤسسات الدولة الليبية، وبيان انعكاساتها على الأمن القومي والاستقرار السياسي، واعتمد الباحث المنهج الوصفي التحليلي لدراسة أبعاد الأمن السيبراني والتهديدات المرتبطة به.

وتوصلت الدراسة إلى النتائج الآتية: أظهرت النتائج أن الهجمات السيبرانية تمثل تهديداً مباشراً للمؤسسات الحيوية في الدولة الليبية. وبينت الدراسة أن استهداف البنية التحتية الرقمية يؤدي إلى إضعاف كفاءة المؤسسات الحكومية ويؤثر في عملية صنع القرار.

كما أكدت النتائج أهمية إنشاء مراكز وهيئات متخصصة في الأمن السيبراني وتعزيز الثقافة الأمنية الرقمية لدى المواطنين.

دراسة ياسين محمد أحمد بونه، بعنوان: "الهجمات السيبرانية: الحرب الرقمية التي تجاوزت الحدود الجغرافية"، بحث منشور في مجلة شمال إفريقيا للنشر العلمي، ليبيا، (2023).

هدفت الدراسة إلى تسليط الضوء على مفهوم الحروب السيبرانية والهجمات الرقمية وعلاقتها بالأمن القومي والسيادة الوطنية، مع بيان أبرز المخاطر والتحديات التي تفرضها البيئة الرقمية الحديثة، واعتمد الباحث المنهج الوصفي التحليلي في معالجة موضوع الدراسة.

وتوصلت الدراسة إلى التالي :أوضحت النتائج أن الهجمات السيبرانية أصبحت أحد أهم أدوات الصراع الحديثة بين الدول والفاعلين غير الحكوميين. وبينت الدراسة أن الحروب الرقمية تؤثر بصورة متزايدة في مفهوم السيادة الوطنية والأمن السياسي. كما أكدت النتائج ضرورة تطوير البنية التشريعية والتقنية لمواجهة التهديدات السيبرانية وتعزيز قدرة الدولة على حماية فضائها الرقمي.

النتائج:

– أظهرت الدراسة أن الحروب المعلوماتية أعادت تشكيل طبيعة التهديدات التي تواجه الأمن السياسي، حيث تحولت التهديدات من كونها مادية مباشرة إلى تهديدات نفسية ومعرفية تستهدف وعي المواطنين وصنع القرار السياسي، ما يضعف استقرار الأنظمة أكثر هشاشة أمام التدخلات الرقمية. وخلق انقسامات داخل المجتمع، وتغيير مواقف المواطنين تجاه السياسات العامة، وهو ما يضعف قدرة الدولة على إدارة شؤونها الداخلية والخارجية بشكل فعال.

– كشفت الدراسة أن الحروب المعلوماتية تعتمد على مجموعة متكاملة من الآليات والأدوات تشمل المعلومات المضللة، والهجمات السيبرانية، والحملات الرقمية الموجهة، والتلاعب النفسي والإعلامي، والاستغلال المتقدم للبيانات، ما يجعلها أكثر تعقيدًا وصعوبة في الرصد والمواجهة مقارنة بالتهديدات التقليدية. ذلك أن تطوير استراتيجيات فعالة لمواجهة الحروب المعلوماتية يتطلب نهجًا شاملًا يدمج الأمن السيبراني، والتدريب المتخصص للكوادر البشرية، والتوعية المجتمعية، والأطر القانونية والتنظيمية، والتعاون الدولي، بحيث تضمن حماية الفضاء المعلوماتي وتعزيز الثقة بالمؤسسات السياسية، والحد من انعكاسات هذه الحروب على الأمن السياسي للدولة.

التوصيات:

– تعزيز قدرات الدول في الأمن السيبراني لحماية البنى التحتية الرقمية والأنظمة المعلوماتية الحيوية من الاختراقات والهجمات المعلوماتية. من خلال إنشاء فرق متخصصة لرصد المعلومات المضللة والحملات الرقمية الموجهة وتحليلها بشكل مستمر للكشف المبكر عن أي تهديدات تستهدف الأمن السياسي.

– تطوير برامج توعية وتثقيف إعلامي للمواطنين لتعزيز قدرتهم على التمييز بين المعلومات الصحيحة والمضللة، والحد من التأثير النفسي والإدراكي للحروب المعلوماتية. والعمل علي اعتماد تشريعات قانونية وتنظيمية متقدمة تتعلق بحماية البيانات، ومكافحة الهجمات السيبرانية، ومراقبة المحتوى الرقمي الذي يهدد الأمن السياسي.

- توظيف التقنيات الحديثة مثل الذكاء الاصطناعي وتحليل البيانات الضخمة لرصد الحملات الموجهة، والتنبؤ بالاتجاهات الرقمية، وتصميم استراتيجيات فعالة للتعامل معها. ودمج التدريب المتخصص للكادر البشري وصناع القرار بحيث يمتلكون القدرة على التعرف على الحملات الرقمية المضللة وفهم تأثيرها على الرأي العام وصنع القرار السياسي
- تعزيز التعاون الدولي والإقليمي لتبادل المعلومات والخبرات، ومواجهة الهجمات العابرة للحدود، وتنسيق الجهود ضد الجهات الفاعلة في الحروب المعلوماتية.
- تطوير آليات استجابة سريعة ومرنة لمواجهة التهديدات المعلوماتية فور ظهورها، بما يضمن الحد من تأثيرها السلبي على مؤسسات الدولة واستقرار النظام السياسي. وهذا يتطلب العمل على الاستثمار في بحوث ودراسات مستمرة حول الحروب المعلوماتية لتحديث الاستراتيجيات الأمنية وتكييفها مع التطورات التقنية والأساليب الجديدة التي يستخدمها الفاعلون في تهديد الأمن السياسي
- تعزيز الوعي المؤسسي في المؤسسات الحكومية والسياسية حول أهمية الفضاء الرقمي وتأثيره على السياسات الداخلية والخارجية، لضمان اتخاذ قرارات مستنيرة وصائبة.

قائمة المصادر والمراجع:

المطيري، أحمد.(2018) تأثير الأخبار الزائفة على الثقة بالمؤسسات (ط1). الكويت: دار الربيع للنشر.

البغدادي، حسين .(2019) الفضاء السيبراني وأمن الدول (ط1). بغداد: دار النهضة العلمية.

البدر، سليم (2021) السياسة الرقمية وعولمة الإعلام (ط2). بيروت: دار الفكر العربي.

الشامي، ريم . (2022) الحملات الرقمية الموجهة وأمن الانتخابات (ط1). عمّان: دار الفكر المعاصر.

الشافعي، نجلاء (2018) .الإعلام الرقمي وأثره في الرأي العام (ط1). الرياض: المركز العربي للأبحاث.

الشريف، لطيفة .(2020) .منظومات الرصد الإعلامي وأمن المعلومات (ط1). القاهرة: دار النهضة.

العبيدي، هند.(2020) . منصات التواصل الاجتماعي ودورها في تشكيل الوعي (ط1). تونس: دار الإبداع.

العطار، محمود .(2019) القانون في مواجهة الجرائم المعلوماتية (ط1). القاهرة: دار الثقافة للنشر.

الزعبي، سامر.(2021) الاستقرار السياسي في ظل تهديدات العصر الرقمي (ط3) عمّان: دار الفكر الحديث.

الزهراني، هناء .(2021) التهديدات غير التقليدية في السياسة الحديثة (ط1). الرياض: دار اليمامة.

الحسيني، على .(2020) الحروب المعاصرة وأمن المعلومات (ط2). بيروت: دار النهضة العربية.

الكردي، فاطمة .(2019) تقنية المعلومات والأمن السيبراني (ط1). القاهرة: دار الفكر الجامعي.

الكيلاني، سامي .(2018) الثقافة الرقمية والمجتمع (ط1). دمشق: دار الفكر العربي.

الهاشمي، خالد .(2021) الذكاء الاصطناعي في الفضاء الإعلامي (ط1). القاهرة: دار المعرفة.

منصور، ياسر (2022) تحليل البيانات الرقمية وأثرها في صناعة القرار (ط2). دبي: دار الشروق.

ياسين، منى .(2020) سياسات مكافحة المعلومات المضللة (ط2). الرباط: دار الكتاب الأكاديمي.