Journal of Anbar University for Law and Political Sciences
مجلة جامعة الانبار للعلوم القانونية والسياسية
P. ISSN: 2706-5804 E.ISSN: 2075-2024
Volume 16- Issue 1- March 2026 المجلد ١٦- العدد ١ – اذار ٢٠٢٦

Employing digital technology in international conflicts

[1] Dr. Alhaam Atea Awad
[1] University of Baghdad / Strategic and International Studies Center

Abstract:

This research explores the evolving role of digital technology in the context of international conflicts. With the rapid development of cyberspace, artificial intelligence, data surveillance, and digital propaganda, modern warfare and geopolitical rivalry have taken on unprecedented forms. This study analyzes how states and non-state actors are increasingly utilizing digital tools to exert influence, wage information warfare, disrupt infrastructures, and manipulate global narratives without direct military confrontation. Through a structured, inferential approach, the research investigates the theoretical foundations, practical mechanisms, and strategic consequences of digital engagement in conflict. The study also examines real-world case studies to highlight the transformative impact of digital technologies on international power dynamics, national sovereignty, and global security.

1: Email:
alham.ateaa@gmail.com
2: Email:

DOI
https://doi.org/10.37651/aujlps.2025.165299.1613

Submitted: 25/9/2025
Accepted: 9/10/2025
Published: 1/03/2026

Keywords:
Digital technology
international conflicts
cyber warfare
digital propaganda
artificial intelligence.

توظيف التكنلوجية الرقمية في الصراعات الدولية

[١] م.د. ألهام عطية عواد
[١] جامعة بغداد / مركز الدراسات الاستراتيجية والدولية

الملخص:

يشهد العالم المعاصر تحولاً جذريًا في طبيعة الصراعات الدولية نتيجة تطور التكنولوجيا الرقمية، التي أصبحت عنصرًا مركزيًا في إعادة تشكيل أدوات القوة والتأثير بين الدول. لقد تخطّت المواجهات مفاهيم الحرب التقليدية لتأخذ أبعادًا جديدة، ترتكز على الفضاء السيبراني، والذكاء الاصطناعي، وتحليل البيانات، والتضليل الرقمي، مما جعل التكنولوجيا الرقمية تلعب دورًا حاسمًا في الأمن القومي، والدبلوماسية، وميزان القوى. يستهدف هذا البحث تحليل كيفية توظيف التكنولوجيا الرقمية في الصراعات الدولية، من خلال دراسة أدواتها، واستراتيجيات توظيفها، وأبعاد تأثيرها على العلاقات الدولية، مع تسليط الضوء على أبرز النماذج والتجارب الحديثة. ويسعى البحث إلى تقديم قراءة استدلالية معمّقة لفهم التحولات الجارية، واستشراف آفاق المستقبل في ظل تسارع الابتكار الرقمي.

الكلمات المفتاحية:

التكنولوجيا الرقمية، الصراعات الدولية، الأمن السيبراني، الذكاء الاصطناعي، التضليل الرقمي.

المقدمة

منذ بداية القرن الحادي والعشرين، أخذت التكنولوجيا الرقمية تتغلغل بشكل متسارع في مفاصل الحياة السياسية والاقتصادية والعسكرية والثقافية للدول، لتتحول من أداة مساندة للأنظمة التقليدية إلى سلاح استراتيجي مستقل بحد ذاته. فقد شهد العالم تحوّلات غير مسبوقة في طبيعة الصراع الدولي، لم تعد تقتصر على المواجهات العسكرية الكلاسيكية، بل باتت تشمل صراعات سيبرانية عابرة للحدود، وحروبًا نفسية تُشن عبر منصات التواصل الاجتماعي، وهجمات معلوماتية تُصيب البُنى التحتية الحيوية، فضلًا عن استخدام الذكاء الاصطناعي والتحليل الخوارزمي في التخطيط والتأثير.

لقد أصبحت التكنولوجيا الرقمية تمثل بعدًا حاسمًا في بنية القوة العالمية، إذ يُعاد من خلالها تشكيل موازين القوى بين الدول، ويجري بناء تحالفات جديدة، وخلق تهديدات غير مرئية يصعب ردعها بالأساليب التقليدية. هذا التحول فرض واقعًا جديدًا، لا تقتصر فيه الصراعات على الدول المتقدمة، بل تشمل أيضًا الفاعلين من غير الدول، كالشركات الكبرى، والجماعات المنظمة، وحتى الأفراد المدعومين تقنيًا، مما وسّع ساحة التنافس وجعلها أكثر تشابكًا وتعقيدًا.

تنبع أهمية هذا الموضوع من أن التكنولوجيا الرقمية لم تعد تُستخدم فقط في تعزيز قدرات الردع والدفاع، بل باتت تُوظَّف في توجيه مسارات الصراعات والتأثير في نتائجها دون الحاجة إلى إطلاق رصاصة واحدة. فالهيمنة اليوم لا تقتصر على امتلاك السلاح النووي أو القوة العسكرية التقليدية، بل تمتد إلى من يملك القدرة على التحكم في المعلومات، وتوجيه السرديات، واختراق الخصوم عبر أدوات رقمية متطورة.

لذلك، يُعد تحليل توظيف التكنولوجيا الرقمية في الصراعات الدولية ضرورة ملحّة لفهم طبيعة التنافس المعاصر، واستشراف مستقبل العلاقات الدولية في ظل تعاظم هذا النمط غير التقليدي من المواجهة. وسيسعى هذا البحث إلى تقديم مقاربة تحليلية واستدلالية متكاملة، تجمع بين البعد النظري والدراسة التطبيقية، لفهم الكيفيات التي يتم من خلالها توظيف الوسائل الرقمية في إدارة النزاعات، والأثر المتولد عنها على الأمن العالمي، والسيادة الوطنية، وتوازن القوى.

أولاً: أهمية البحث

تعد التكنولوجيا الرقمية من أبرز المتغيرات التي أعادت تشكيل المشهد الدولي، إذ أصبح توظيفها في الصراعات أداة استراتيجية حاسمة تؤثر على موازين القوى والعلاقات بين الدول. مع توسع الاعتماد على الفضاء الإلكتروني والبيانات الرقمية، ظهرت أشكال جديدة من الصراعات تتجاوز الحدود التقليدية، مما يفرض تحديات أمنية وسياسية على المجتمع الدولي. لذلك، يأتي هذا البحث ليبرز أهمية فهم كيف تُستخدم التكنولوجيا الرقمية في الصراعات الدولية، ويدرس الأبعاد المختلفة لهذا التوظيف، ليسهم في تطوير آليات فعالة لمواجهتها،

وضمان استقرار النظام الدولي. كما يعزز البحث من وعي صانعي القرار والباحثين بأهمية التوازن بين الاستفادة من هذه التكنولوجيا وحماية الأمن والسلام العالميين.

ثانياً: هدف البحث

يهدف البحث إلى:

١. تحليل دور التكنولوجيا الرقمية في تطور الصراعات الدولية.

٢. دراسة الأدوات الرقمية المستخدمة في هذه الصراعات وتأثيرها على العلاقات الدولية.

٣. استكشاف التحديات الأمنية والقانونية المرتبطة باستخدام التكنولوجيا الرقمية في الصراعات.

٤. تقديم توصيات وآليات لتعزيز الأمن والاستقرار في النظام الدولي في ظل توظيف التكنولوجيا الرقمية.

ثالثاً: إشكالية البحث

تكمن إشكالية هذا البحث في التغير السريع والمستمر الذي تحدثه التكنولوجيا الرقمية في طبيعة الصراعات الدولية، حيث أصبح من الصعب على الدول والمجتمع الدولي مجاراة هذا التطور وتنظيمه بشكل فعال. كيف تؤثر أدوات التكنولوجيا الرقمية الحديثة على ديناميكيات الصراع الدولي؟ وما هي الآليات المناسبة لمواجهة التحديات الأمنية والقانونية التي تنتج عن استخدامها؟ وما الدور الذي يمكن أن تلعبه المؤسسات الدولية في تنظيم هذا المجال وضبط استخدام هذه التكنولوجيا؟ هذه الأسئلة تشكل محور الإشكالية التي يحاول البحث الإجابة عليها.

رابعاً: فرضية البحث

تفترض هذه الدراسة أن "توظيف التكنولوجيا الرقمية في الصراعات الدولية يمثل تحوّلًا جوهريًا في طبيعة الصراع الدولي، ويزيد من تعقيد التحديات الأمنية والسياسية، مما يستدعي تطوير آليات متخصصة للتعامل معه على المستوى الدولي."

خامساً: منهجية البحث

يعتمد البحث على المنهج الوصفي التحليلي، حيث يتم جمع وتحليل المعلومات من مصادر متنوعة تشمل الدراسات الأكاديمية، التقارير الدولية، والمقالات المتخصصة في مجال

التكنولوجيا الرقمية والصراعات الدولية. كما يستخدم البحث المنهج الاستدلالي لفهم العلاقة بين تطور التكنولوجيا الرقمية وتغيرات طبيعة الصراعات، مع التركيز على تحليل الحالات العملية والدراسات الميدانية لدعم الفرضيات المطروحة

سادساً: هيكلية الدراسة:

تتألف هذه الدراسة من أربعة مباحث رئيسة مترابطة، صيغت بشكل متسلسل ومنهجي يتيح للقارئ فهم أبعاد الظاهرة قيد البحث وتحليلها على نحو متكامل، وذلك على النحو الآتي:

المبحث الأول: يتناول الإطار النظري لتوظيف التكنولوجيا الرقمية في الصراعات الدولية، من خلال تحليل المفهوم العام للصراع الرقمي، وبيان التحولات التي طرأت على طبيعة الحروب الحديثة في ظل التطور التكنولوجي، مع التركيز على الخصائص البنيوية للبيئة الرقمية وتأثيرها في بنية القوة العالمية.

المبحث الثاني: يبحث في أدوات التكنولوجيا الرقمية المستخدمة في الصراعات الدولية، كالذكاء الاصطناعي، والطائرات المسيرة، والفضاء السيبراني، والإعلام الرقمي، والخوارزميات، وغيرها من الأدوات التي أسهمت في إعادة تشكيل مفهوم القوة والنفوذ بين الدول.

المبحث الثالث: يتناول أثر التكنولوجيا الرقمية في مخرجات الصراعات الدولية، من خلال دراسة التحولات في مفاهيم الردع، والسيادة، والتفوق الاستراتيجي، وصعود الفاعلين غير الدولتيين، وما نتج عن ذلك من إعادة توزيع لأدوار القوى التقليدية.

المبحث الرابع: يسلّط الضوء على انعكاسات توظيف التكنولوجيا الرقمية على مفاهيم القانون الدولي والسيادة الوطنية، ويستعرض التحديات القانونية الناشئة عن الحروب السيبرانية، وحدود التنظيم الدولي للفضاء الرقمي، مع اقتراح أطر لإصلاح المنظومة القانونية الدولية بما يواكب المتغيرات التكنولوجية.

وتُختتم الدراسة بخاتمة تتضمن أبرز النتائج والتوصيات المستخلصة من المباحث السابقة، بما يسهم في تعزيز الوعي الأكاديمي والسياسي بأهمية ضبط استخدام التكنولوجيا الرقمية في الصراعات الدولية.

I. المبحث الأول

الإطار النظري لتوظيف التكنولوجيا الرقمية في الصراعات الدولية

تمثل التكنولوجيا الرقمية عاملًا جوهريًا في إعادة تعريف الصراعات الدولية المعاصرة، حيث أصبحت الفضاءات الإلكترونية ميدانًا للصراع مثلها مثل البر والبحر والجو، بل وتفوقت عليها أحيانًا من حيث الأهمية الاستراتيجية والسرعة والتأثير. فالتطور السريع للأدوات الرقمية، وتعدد الفاعلين القادرين على استخدامها، أدّيا إلى ظهور بيئة صراعية جديدة لا تخضع دومًا لقوانين الحرب التقليدية، ما يستدعي إطارًا نظريًا شاملاً لفهم هذه التحولات. ويتناول هذا المبحث خمس نقاط مركزية لفهم هذا التغيير البنيوي.

أولًا: مفهوم الصراع الرقمي وتحول طبيعة الحروب

يُشير مفهوم الصراع الرقمي إلى استخدام الموارد التكنولوجية، ولا سيما تقنيات الاتصال والبرمجيات والبيانات، كأدوات في صراع دولي لتحقيق مكاسب سياسية أو اقتصادية أو استراتيجية دون اللجوء إلى الصدام التقليدي. هذا النوع من الصراع يتجاوز المفاهيم التقليدية للحرب، حيث يعتمد على الاختراق، التلاعب، والتأثير دون أن يُطلق رصاصة واحدة، وهو ما يتوافق مع مفهوم "القوة الإلكترونية"[١].

لقد أنشأت الدول مؤخرًا وحدات عسكرية سيبرانية متخصصة كجزء من جيوشها التقليدية.يمكن لهذه الوحدات تنفيذ عمليات إلكترونية ضد البنية التحتية الحيوية - مثل محطات الطاقة والمنشآت النووية - مما يخلق تأثيرات استراتيجية تعادل تلك التي تنتجها الوسائل العسكرية التقليدية. لقد ظهر هذا النموذج الجديد للحرب بشكل واضح في الصراعات الحديثة، حيث تم استخدام القدرات السيبرانية بالتوازي مع القوات التقليدية [٢].

ثانيًا: خصائص التكنولوجيا الرقمية في بيئة الصراع

يتميز الصراع الرقمي بخصائص فريدة تجعله مختلفًا عن الصراع التقليدي، حيث تُعد "التكلفة المنخفضة" من أبرز هذه الخصائص، إذ يمكن لدولة صغيرة أو مجموعة غير

(١) . نايف، جوزيف س. "القوة الإلكترونية". *مركز بيلفر بجامعة هارفارد للعلوم والشؤون الدولية*، (٢٠١٠): ص. ٩

(2) Singer, P. W., & Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press. pp. 85-88

حكومية تطوير قدرات هجومية إلكترونية بتكلفة أقل بكثير من الأسلحة التقليدية. كما يتميز الصراع الرقمي بـ "صعوبة تحديد الهوية"، حيث يمكن تنفيذ الهجمات دون الكشف عن هوية الفاعل، مما يضعف استراتيجيات الردع التقليدية. بالإضافة إلى ذلك، تُظهر الهجمات السيبرانية "سرعة التنفيذ والتأثير"، حيث يمكن أن تسبب أضرارًا كبيرة في قطاعات حيوية مثل الطاقة والاتصالات خلال ثوانٍ. هذه الخصائص تجعل الصراع الرقمي أداة فعالة في يد فاعلين متنوعين، من الدول إلى الجماعات غير الحكومية[١].

ثالثًا: الفاعلون الجدد في الصراع الدولي الرقمي

أدى تطور التكنولوجيا الرقمية إلى ظهور فاعلين جدد في الصراعات الدولية، حيث لم تعد الدول هي الوحيدة التي تمتلك القدرة على التأثير في الأمن الدولي. فقد برزت جماعات القرصنة والمجموعات الإلكترونية المنظمة التي تعمل بدوافع سياسية أو مالية، كما أصبحت شركات التكنولوجيا الكبرى فاعلاً مؤثرًا بسبب سيطرتها على منصات التواصل والبيانات العالمية. هذه الفاعلية الجديدة تتجاوز الحدود التقليدية للدول، حيث يمكن لهذه الجهات تنفيذ هجمات إلكترونية معقدة أو التلاعب بالرأي العام دون الحاجة إلى موارد تقليدية[٢].

رابعًا: انعكاسات الرقمنة على مفهومي السيادة والأمن

أحدثت الرقمنة تصدعًا في المفهوم التقليدي للسيادة، الذي يرتكز على السيطرة على الإقليم والموارد والسكان. فقد أضحت السيادة تتعلق بالسيطرة على البيانات، والشبكات، والبنية التحتية الرقمية. أصبح من غير الممكن الحديث عن أمن قومي دون التطرق إلى "الأمن السيبراني"، الذي يشمل حماية المؤسسات الحكومية، والبنوك، والمرافق العامة، ووسائل الإعلام من الاختراق أو التخريب أو التجسس.

وفي هذا الإطار، بات من الضروري للدول أن تؤسس "سيادة رقمية"، تُمكّنها من حماية الفضاء السيبراني الوطني، وتضمن استقلالية القرار الرقمي، وتمنع التدخل الخارجي عبر الفضاء المعلوماتي. بل إن العديد من الدول بدأت في بناء شبكات إنترنت خاصة بها (مثل

(1) Libicki, M. C. (2009). Cyberdeterrence and Cyberwar. RAND Corporation. pp. 23–27.
(2) Nye, J. S. (2011). The Future of Power. PublicAffairs. pp. 112–115.

"الإنترنت السيادي" في روسيا)، أو فرض قيود على حركة البيانات الدولية، لحماية أمنها الرقمي [١].

خامسًا: التحول في نظريات القوة في العلاقات الدولية

فرضت الثورة الرقمية إعادة تعريف لمفاهيم القوة في العلاقات الدولية. فالقوة لم تعد تُقاس فقط بعدد الجنود أو حاملات الطائرات، بل أصبحت ترتبط بمن يمتلك قدرات التحكم في المعلومات، البيانات، والخوارزميات. فالقوة الناعمة أصبحت رقمية، تستند إلى التأثير عبر الإعلام والمنصات، والقوة الصلبة أصبحت سيبرانية، تستند إلى القدرة على التدمير أو التعطيل عن بعد.

تُعيد هذه التحولات تشكيل نظريات الردع. فبدل الردع النووي مثلاً، بدأت الدول تتحدث عن "الردع السيبراني"، الذي يقوم على خلق بيئة من الغموض وعدم القدرة على التنبؤ بالرد. كما ظهرت مفاهيم مثل "التفوق السيبراني"، و"الحرب الرمادية"، وكلها تؤشر إلى أن تكنولوجيا المعلومات باتت العنصر الحاسم في الصراعات الحديثة، ومن المتوقع أن تستمر في إعادة تشكيل توازنات القوة العالمية في المستقبل.

سادسًا: الذكاء الاصطناعي كفاعل جديد في ساحة الصراعات

يُعد الذكاء الاصطناعي (AI) من أبرز الأدوات التكنولوجية التي أحدثت طفرة في كيفية إدارة الصراعات الدولية. فبفضل قدراته في تحليل كميات ضخمة من البيانات، واتخاذ قرارات شبه فورية، دخل الذكاء الاصطناعي ميادين الحرب، التجسس، والمراقبة. وقد طوّرت بعض الدول أنظمة هجومية تعتمد على الذكاء الاصطناعي لتحديد الأهداف، وتوجيه الضربات، وحتى اتخاذ قرارات عسكرية دون تدخل بشري مباشر.

ولعل الأخطر في هذا التحول هو اعتماد نظم اتخاذ القرار السياسي والعسكري على خوارزميات قد تكون غير شفافة، ما يطرح إشكاليات أخلاقية وقانونية جوهرية. كما أن استخدام الذكاء الاصطناعي في العمليات النفسية والإعلامية يضاعف القدرة على التأثير في

(1) Deibert, R. J. (2020). Reset: Reclaiming the Internet for Civil Society. House of Anansi Press. pp. 45-52.

المجتمعات، من خلال تضليل الرأي العام أو تغذية الانقسامات الداخلية، وهي أدوات باتت تُستخدم في صراعات ذات طابع هجين وغير متكافئ [١] .

سابعًا: التهديدات الرقمية للمؤسسات الديمقراطية

تشير الأدلة المتراكمة إلى أن الهجمات الرقمية لا تقتصر على البنية التحتية الحيوية، بل تستهدف أيضًا نظم الحكم والمؤسسات الديمقراطية، كالتأثير في الانتخابات، وتوجيه الرأي العام عبر وسائل التواصل الاجتماعي، واختراق بيانات الناخبين أو الأحزاب. وقد ظهرت حالات ملموسة في الولايات المتحدة وفرنسا وألمانيا، حيث وُجهت اتهامات لجهات أجنبية بالتدخل في العمليات الانتخابية من خلال حملات دعائية رقمية ضخمة أو تسريب معلومات محرجة.

وهذه الهجمات تستغل الفضاء المفتوح الذي تتيحه الديمقراطيات، مما يجعلها أكثر هشاشة أمام هذا النمط من التهديدات. وبالتالي، أصبحت الحماية الرقمية للمؤسسات السياسية تمثل جزءًا أساسيًا من الأمن القومي، حيث تعمل الدول على تطوير أطر قانونية وتقنية لضمان نزاهة العملية الديمقراطية وحمايتها من الاختراق الرقمي[٢]

II. المبحث الثاني

أدوات التكنولوجيا الرقمية في الصراعات الدولية

تمثل أدوات التكنولوجيا الرقمية عنصراً حاسماً في توجيه مسارات الصراعات الدولية الحديثة، حيث أفرز التطور التكنولوجي أنماطاً جديدة من المواجهات لم تعد تقتصر على الجغرافيا أو الأسلحة التقليدية، بل امتدت إلى الفضاءات الرقمية والذكية. في هذا المبحث، سنستعرض أبرز أدوات التكنولوجيا الرقمية التي يُعتمد عليها في إدارة أو توجيه الصراعات الدولية، مع شرح موسع لكل أداة وتحليل دورها، في سبع نقاط رئيسية.

(1) Horowitz,M. C. (2018). Artificial Intelligence, International Competition, and the Balance of Power. Texas National Security Review, 1(3), pp. 37-42.
(2) Nye,J. S. (2020). Cyber Threats to Democratic Institutions: The New Frontier. Foreign Affairs, 99(5), pp. 112-125.

اولاً : الذكاء الاصطناعي والتحليل التنبؤي في التخطيط الاستراتيجي

يمثل الذكاء الاصطناعي أحد أبرز الأدوات التي توظفها الدول والقوى الفاعلة في الصراعات الدولية، من خلال استخدامه في جمع البيانات الضخمة وتحليلها للتنبؤ بسلوك الخصوم أو اتجاهات الرأي العام أو ردود الفعل الدولية. فأنظمة الذكاء الاصطناعي تُستخدم لرسم سيناريوهات متعددة لمسارات الأزمة، وتوفر للقيادة السياسية والعسكرية تصوراً استراتيجياً أكثر دقة. وتكمن قوة هذه الأداة في قدرتها على التعلم المستمر، وتحديث قراءاتها للسلوك المتغير للخصوم أو الشركاء. كما تُمكّن المؤسسات الأمنية من اكتشاف التهديدات المبكرة، ورصد مؤشرات التصعيد قبل حدوثها، مما يتيح فرصة للتدخل الوقائي أو إعادة التموضع السياسي والعسكري [١].

ثانياً : الطائرات المسيرة (الدرونز) كأداة هجومية واستطلاعية

أصبحت الطائرات المسيرة واحدة من أكثر أدوات التكنولوجيا الرقمية استخدامًا في ساحات الصراع، لمرونتها في المهام، وقدرتها على تنفيذ الضربات دون تعريض الطيارين للخطر. ويمكن توظيف الدرونز سواء في مهام الاستطلاع وجمع المعلومات أو كأدوات دقيقة للهجوم، وغالبًا ما يتم التحكم بها عن بُعد باستخدام تقنيات الذكاء الصناعي والملاحة عبر الأقمار الصناعية. وقد أثبتت الحروب المعاصرة، مثل الحرب في أوكرانيا أو النزاع في ناغورني كاراباخ، أن الدرونز غيّرت قواعد الاشتباك العسكري، بل أصبحت تلعب دورًا مركزيًا في تغيير ميزان القوى التكتيكي على الأرض [٢].

ثالثاً : الفضاء السيبراني (الهجمات السيبرانية والهجمات المضادة)

يُعد الفضاء السيبراني ساحة صراع مستقلة بذاتها، حيث تتنافس الدول على فرض الهيمنة الرقمية من خلال عمليات قرصنة واستهداف للبنى التحتية الرقمية للخصوم. الهجمات السيبرانية قد تُستخدم لتعطيل أنظمة الاتصالات، أو شبكات الكهرباء، أو لسرقة معلومات استخباراتية. كما باتت الحروب السيبرانية عنصرًا تكتيكيًا في الاستراتيجية الدفاعية

(١) خليفة، عادل. "الذكاء الاصطناعي في الأمن القومي". *مجلة شؤون أمنية*، العدد ١٨، (٢٠٢٢)، ص٩١.
(٢) معهد الدراسات العسكرية. "تكنولوجيا الدرونز وتغيير نمط الحروب". تقرير استراتيجي، ٢٠٢٣، ص ٤٤.

والهجومية للدول، يُنفذ من خلال فرق متخصصة أو عبر توظيف مرتزقة رقميين. وتمثل عمليات "الهجوم المضاد السيبراني" وجهًا جديدًا للصراع، حيث تبادر الدولة إلى الرد الفوري على الهجمات عبر استهداف مماثل في العمق الرقمي للخصم، مما يؤدي إلى تصعيد غير مرئي ولكنه شديد التأثير[١] .

رابعاً: الإعلام الرقمي والحرب النفسية عبر المنصات الاجتماعية :

باتت أدوات الإعلام الرقمي وسيلة أساسية في إدارة الصراعات، حيث تُستخدم لبث رسائل الحرب النفسية، وتوجيه الرأي العام، وإضعاف العدو داخليًا. فالحملات الإعلامية الموجّهة عبر المنصات مثل تويتر وفيسبوك ويوتيوب أصبحت تُدار بأساليب معقدة تتضمن الذكاء الاصطناعي، والحسابات الوهمية، والترويج المدفوع، مما يضفي على الرسائل طابعاً جماهيرياً واسع الانتشار. وتستخدم الدول هذه الوسائل لزرع الشك داخل الجبهات المعادية، والتشويش على الرأي العام العالمي، بل وأحيانًا لإنتاج روايات بديلة تخدم أهدافها الاستراتيجية في الصراع .

خامساً : الأقمار الصناعية والمراقبة الفضائية

وفرت الأقمار الصناعية بُعداً استراتيجياً بالغ الأهمية في إدارة الصراعات الدولية، حيث تتيح هذه التقنية مراقبة تحركات العدو، ورصد النشاط العسكري، وتحليل التضاريس. تلعب الصور الفضائية دورًا في التحقق من الانتهاكات أو في توثيق الأحداث، كما تُستخدم لتوجيه الضربات بدقة، ودعم عمليات الطيران والصواريخ الذكية. وتدخل الأقمار الصناعية أيضًا في المعركة من خلال شبكات الاتصالات المؤمنة، ما يساهم في ضمان استمرار التنسيق بين الوحدات القتالية المختلفة حتى في بيئات محجوبة أو معقدة[٢] .

سادساً: الخوارزميات الرقمية في اتخاذ القرار السياسي والعسكري

باتت الخوارزميات أدوات حيوية لدعم القرار في بيئات الصراع، حيث يمكنها تحليل عدد كبير من المتغيرات في وقت قصير، وتقديم توصيات آنية لصانع القرار. وتستخدم الدول

(١) كاظم، فاضل. "الحرب السيبرانية وتوازن الردع الرقمي". *مركز الأفق للدراسات*، (٢٠٢٢)، ص. ٥٦.
(٢) مراد، هاني. "القدرات الفضائية في زمن النزاعات". *المجلة الجيوسياسية*، العدد ٢٧، (٢٠٢٣): ص ٣٣.

المتقدمة برمجيات خوارزمية لتحليل المخاطر، وتحديد الأولويات، وتوجيه الموارد. كما يمكن للخوارزميات تقييم احتمالية ردود الفعل الدولية أو حساب كلفة التدخل العسكري بدقة متناهية، مما يعزز القدرة على اتخاذ قرارات محسوبة سياسياً واستراتيجياً. هذه الأدوات تمثل تحوّلاً من النماذج البشرية التقليدية إلى أنظمة دعم قرار ذكية [١].

سابعاً : تكنولوجيا البلوكتشين والأمن السيادي الرقمي

دخلت تكنولوجيا البلوكتشين ساحة الصراعات الرقمية كأداة لتعزيز الأمن السيادي، خصوصاً في حماية البيانات، وضمان مصداقية الاتصالات الرسمية، والتعاملات المالية للدول أثناء الأزمات. وتُستخدم هذه التكنولوجيا لضمان عدم التلاعب أو التزييف في نظم تبادل المعلومات، أو لتأمين البنى التحتية المصرفية في حالات الحرب. كما بدأت بعض الدول بتجريب هذه التقنية في أنظمة التصويت الإلكتروني في المناطق الحساسة سياسيًا، مما يعزز مناعة النظام الديمقراطي من الاختراقات الخارجية أو التشويش الإعلامي [٢].

III. المبحث الثالث

تأثير التكنولوجيا الرقمية في مخرجات الصراعات الدولية: التحول في مسارات القوة والاستراتيجية

تعيش الصراعات الدولية اليوم تحوّلات عميقة بفعل الثورة الرقمية، التي لم تُغير فقط في أدوات المواجهة، بل مست جوهر العلاقات الدولية ومفاهيم القوة والنفوذ. لقد صعدت التكنولوجيا الرقمية إلى مركز الصدارة كعاملٍ حاسمٍ في تحديد نتائج النزاعات، مما أوجد واقعًا استراتيجيًا جديدًا يختلف عن النماذج التقليدية التي كانت تقوم على التفوق العسكري أو الاقتصادي وحده. وباتت الصراعات تدور في فضاءات جديدة — الفضاء السيبراني، الإعلامي، الرقمي — حيث يتم التلاعب بالعقول والبنى التحتية والمعلومات، وتُحسم المعارك دون إطلاق رصاصة واحدة. هذه البيئة الجديدة فرضت على الفاعلين الدوليين تطوير استراتيجيات معقدة تتماشى مع نمط غير متوازن من التهديدات والفرص، الأمر الذي جعل

(١) عيسى، مروان. "الخوارزميات ودورها في القرار العسكري". *مجلة الذكاء الاصطناعي والسياسة*، (٢٠٢٢): ص. ٦٢.

(٢) بشير، هالة. "البلوكتشين في الأمن السيادي". *مجلة الأمن الرقمي*، العدد ٩، (٢٠٢٣): ص٤١.

مخرجات الصراعات تتحدد ليس فقط بمن يملك السلاح الأقوى، بل بمن يملك البيانات الأدق، والسيطرة المعلوماتية الأوسع.

أولاً: إعادة تعريف مفاهيم التفوق والسيادة في ظل التكنولوجيا الرقمية

أعادت التكنولوجيا الرقمية صياغة المفاهيم الكلاسيكية للسيادة والتفوق، فلم تعد الدولة الأقوى هي تلك التي تملك أكبر جيش أو اقتصاد، بل تلك التي تمتلك البنى التحتية الرقمية الأكثر أمنًا، والسيطرة الأعلى على تدفق المعلومات وموارد البيانات. أصبحت "السيادة الرقمية" من المقاييس الجديدة لقوة الدولة، وهي تعني قدرة الدولة على حماية فضائها الرقمي من الاختراق، والتحكم بمحتوى منصاتها ومستخدميها، وضمان استقلالية نظمها المعلوماتية. على سبيل المثال، تسعى دول كالصين والولايات المتحدة إلى بناء منظومات رقمية ذات طابع سيادي مغلق أو شبه مغلق، يمنع التأثيرات الخارجية ويعزز الهيمنة على الداخل. وفي السياق نفسه، تتعامل بعض الدول مع شركات التكنولوجيا العالمية بوصفها أدوات سيادية بامتياز، لأن قدرتها على التحكم بالمعلومة توازي امتلاك أدوات الردع العسكري [١].

ثانياً: صعود الفاعلين غير الدولتيين باستخدام الأدوات الرقمية

أحد أبرز التحولات التي فرضتها البيئة الرقمية هو بروز فاعلين غير دولتيين قادرين على التأثير الفعلي في مجريات الصراع، بل وأحيانًا قلب موازينه. فالجماعات الإرهابية، والمنظمات العابرة للحدود، والهاكرز المحترفون، أصبحوا يمتلكون أدوات تمكنهم من شن هجمات على بنوك، مؤسسات إعلامية، أو منشآت استراتيجية تابعة لدول كبرى، ما كان يُعد سابقًا من المستحيلات. هؤلاء الفاعلون لا يمتلكون قواعد عسكرية أو سفارات، لكنهم يملكون المهارة والتخفي، ويعملون أحيانًا بتنسيق مع دول، وأحيانًا بشكل مستقل. هذا الانتقال من "الدولة المركزية" إلى "الفعل اللامركزي" زاد من تعقيد مشهد الصراع، وخلق تحديات غير مسبوقة للأمن القومي، لأن التهديد أصبح غير واضح المعالم، وغير مرتبط بجغرافيا أو سيادة سياسية تقليدية [٢].

(١) مرعي، خالد عبد الله. *التحول الرقمي والنزاعات الحديثة*. (دار النهضة العربية، ٢٠٢٠)، ص. ١١٥.
(٢) كنعان، نزار عبد الحميد. "التكنولوجيا كعنصر مؤثر في الأمن الدولي". *مجلة العلوم السياسية - جامعة بغداد*، العدد ٦٨، (٢٠٢٢): ص ١٤٣.

ثالثاً: تعزيز فعالية العمليات النفسية والدعائية في زمن الرقمنة

لم تعد الحرب النفسية تُمارس من خلال المنشورات أو الإذاعات فقط، بل أصبحت منصات التواصل الاجتماعي، وخوارزميات التوجيه، وصناعة المحتوى الرقمي، أدوات رئيسية للتأثير على وعي الشعوب وتوجهاتها. في الصراعات الحديثة، يتم توجيه حملات موجهة تهدف إلى خلق انقسام داخلي، أو تشويه صورة العدو، أو تقويض الثقة بالحكومة، من خلال منصات رقمية يمكن الوصول إليها بسهولة وبكلفة ضئيلة. المثال الأوضح هو ما حدث خلال الانتخابات الأمريكية ٢٠١٦، حيث استخدمت أطراف خارجية وسائل التواصل لتوجيه الرسائل وتضليل الرأي العام، وهو ما يتكرر في صراعات أخرى مثل الأزمة الأوكرانية، حيث كان الإعلام الرقمي ميدانًا متوازيًا للمعركة التقليدية. هذه الأساليب تُعد أخطر من السلاح أحيانًا، لأنها تضرب ثقة المجتمع من الداخل [١].

رابعاً: التحول من الردع التقليدي إلى الردع الرقمي

الردع في السابق كان يُبنى على قاعدة "التكلفة مقابل الرد"، ولكن في البيئة الرقمية تحولت المفاهيم، إذ أصبح بإمكان دولة صغيرة بقدرات سيبرانية عالية أن تردع قوة كبرى، ليس بالعدد والعتاد، بل بالقدرة على إحداث خلل كبير في مؤسساتها الرقمية. فالهجمات السيبرانية التي تستهدف شبكات الكهرباء، أو قواعد البيانات العسكرية، أو البورصات، قد تُحدث شللًا في الدولة الخصم دون الدخول في مواجهة عسكرية. هذه البيئة الجديدة فرضت نوعًا من "الردع الرمزي"، القائم على التهديد غير المعلن، مما يجعل الدول تعيد حساباتها، وتُدرك أن الهجوم السيبراني القادم قد يأتي من مكان غير متوقع، وفي وقت غير معلن. لذا، أصبحت الاستعدادات للردع تشمل تدريب فرق رقمية، وتطوير أدوات استخباراتية سيبرانية، والتحكم بنقاط الضعف التكنولوجي داخليًا [٢].

(1) Woolley, S. C., & Howard, P. N. (2019). Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media. Oxford University Press. pp. 45-63.

(٢) نايف، جوزيف س. مستقبل القوة. بابليك أفيرز، ٢٠١١، ص. ١٣٧.

خامساً: استراتيجيات التكيف الجديدة للدول في ظل التفوق الرقمي

تفرض الثورة الرقمية على الدول أن تُعيد صياغة استراتيجياتها الأمنية والسياسية لتشمل البيئة الرقمية، حيث لم يعد الأمن القومي يُبنى على جدران الحدود فحسب، بل على الحماية الرقمية للمؤسسات والأنظمة والشبكات. لهذا، أسست العديد من الدول مراكز متخصصة في الأمن السيبراني، ودمجت "العقيدة السيبرانية" في استراتيجيات الدفاع الوطني. كما بدأت تبني تحالفات رقمية مع دول أخرى لمواجهة التهديدات المشتركة. على سبيل المثال، حلف الناتو أطلق وحدة خاصة للردع الرقمي، وتعاونت دول الاتحاد الأوروبي لإنشاء قواعد جماعية لحماية البنية التحتية الرقمية. في المقابل، بدأت بعض الدول بفرض رقابة صارمة على الفضاء الرقمي المحلي من أجل تعزيز سيطرتها على تدفق المعلومات، ومنع التلاعب الخارجي، وهو ما يعكس عمق تحول البيئة الرقمية إلى أداة سيادية [١].

سادساً: اختلال موازين الردع الإقليمي بسبب التفوق السيبراني

أحدثت القدرات الرقمية تفاوتًا كبيرًا في موازين القوى، خصوصًا في المناطق التي تشهد توترات تقليدية مثل الشرق الأوسط أو شبه الجزيرة الكورية. فبينما كانت موازين الردع تقليديًا تُبنى على الأسلحة أو التحالفات، أصبحت الدولة التي تمتلك القدرة على اختراق نظم خصومها قادرة على فرض شروطها، أو تقويض استقرارهم من الداخل. على سبيل المثال، تشير تقارير أمنية إلى أن هجمات سيبرانية ضد منشآت نفطية أو مفاعلات نووية قد تنفذها دول أو وكلاء رقميون، بهدف توجيه رسائل أو تحقيق أهداف استراتيجية دون التصعيد العسكري المباشر. هذا النوع من الصراع غير المتكافئ يجعل حتى الدول الكبرى عرضة للخطر، ويُجبرها على توسيع نطاق استراتيجياتها الأمنية [٢].

سابعاً: اندماج الذكاء الاصطناعي في القرارات الاستراتيجية العسكرية

تُحدث تقنيات الذكاء الاصطناعي (AI) تحولًا جوهريًا في كيفية اتخاذ القرارات العسكرية، إذ باتت الأنظمة الذكية قادرة على تحليل بيئات الصراع، وتحسين كفاءة العمليات

(١) ريد، توماس. *الحرب الإلكترونية لن تحدث*. (مطبعة جامعة أكسفورد، ٢٠١٣)، ص. ١٨٠.
(٢) أحمد، تالمير. "الدبلوماسية الرقمية ووساطة الصراعات". *التحليل الاستراتيجي*، المجلد ٤٥، العدد ٤، (٢٠٢١): ص٣٥٦.

من خلال أنظمة دعم القرار، والطائرات بدون طيار، والأنظمة الدفاعية الآلية. يُمكن لهذه التقنيات أن تقلل زمن الاستجابة، وتحد من الخسائر البشرية، لكنها في الوقت نفسه تفتح أبوابًا لمخاطر أخلاقية، خاصة في ما يتعلق باستقلالية الآلة في اتخاذ قرارات مميتة دون تدخل بشري. لذلك، أصبحت الرقابة على استخدام الذكاء الاصطناعي في السياق العسكري واحدة من أهم التحديات التي تواجه القانون الدولي الإنساني والاتفاقيات الأمنية، وسط غياب إجماع دولي واضح حول الحدود المقبولة لهذا الاستخدام [١].

IIII.المبحث الرابع

آثار توظيف التكنولوجيا الرقمية في الصراعات الدولية على مفاهيم السيادة والقانون الدولي

أحدثت التكنولوجيا الرقمية تحولات جذرية في بنية الصراعات الدولية، إذ لم تعد الحروب تقتصر على ساحات المعارك التقليدية، بل باتت تدور في الفضاءات السيبرانية، وتطال الأنظمة المعلوماتية والبنى التحتية الرقمية. هذا التطور فرض تحديات غير مسبوقة على مفاهيم القانون الدولي والسيادة الوطنية، إذ أصبحت الدول عرضة لاعتداءات غير مادية، قد تكون مدمّرة في آثارها أكثر من الضربات العسكرية المباشرة. وفي ظل هذا المشهد المتغيّر، برزت الحاجة إلى إعادة النظر في مدى ملاءمة القواعد القانونية الدولية القائمة، كما طُرحت تساؤلات جديدة بشأن مدى قدرة الدول على حماية نفسها في عالم تتقاطع فيه السيادة مع البرمجيات والمعطيات الافتراضية.

أولًا: تفكك المفهوم التقليدي للسيادة في ظل الهجمات السيبرانية

تواجه الدول اليوم واقعًا معقدًا يتمثل في غياب الخطوط الفاصلة بين الداخل والخارج. فالهجمات الإلكترونية، التي تُنفذ عبر الإنترنت من دون المرور بأي حدود مادية، جعلت من مفهوم "السيادة المطلقة داخل الحدود" أمرًا هشًا. إذ لم يعد بإمكان الدول السيطرة الكاملة على مجالها السيبراني، خاصة عندما تكون التهديدات ناتجة عن فاعلين غير دوليين مثل الجماعات الهاكرية أو شركات خاصة ذات طابع سياسي أو أمني. وتتمثل أبرز التحديات في:

(١) لخالدي، زينب حسن. "الصراعات الرقمية وإشكاليات السيادة الوطنية". *مجلة البحوث والدراسات السياسية*، المجلد ١٢، العدد ١، (٢٠٢٣): ص. ٩٧

١. استهداف البنية التحتية الحيوية مثل الطاقة والمياه والنقل.

٢. التلاعب بالمعلومات الداخلية أو بثّها خارجيًا بقصد زعزعة الاستقرار.

٣. صعوبة إسناد الهجمات إلى جهة معينة بشكل قانوني.

كل ذلك جعل السيادة مفهوما متحولا، يتطلب أدوات دفاعية رقمية لا تقل أهمية عن الدفاعات التقليدية [١].

ثانيًا: محدودية القانون الدولي التقليدي أمام الصراعات الرقمية

لم تعد مبادئ القانون الدولي، كما وُضعت في اتفاقيات جنيف وميثاق الأمم المتحدة، كافية لضبط السلوكيات الرقمية في زمن الصراع. فهناك إشكاليتان رئيسيتان تواجهان هذا النظام:

١. غياب التعريف الواضح للهجمات السيبرانية، وهل تُعد بمثابة "عدوان مسلح" يستوجب الدفاع عن النفس.

٢. ضعف آليات الرد والعقوبات، إذ غالبًا ما تكون الجهات الفاعلة غير قابلة للتعقب أو خارجة عن نطاق الدول.

كما أن القانون الدولي لم يطور حتى الآن نظامًا واضحًا للمسؤولية القانونية في الفضاء السيبراني، ما يخلق فراغًا قانونيًا تُستغلّه القوى الكبرى، مما يجعل القانون الحالي عاجزًا عن مجاراة الواقع الرقمي [٢].

ثالثًا: ظهور "السيادة السيبرانية" كمفهوم بديل

في محاولة لمواكبة التحولات، بدأت بعض الدول – وعلى رأسها الصين وروسيا – بالدفع نحو تبني مفهوم "السيادة السيبرانية"، الذي يقوم على:

١. السيطرة الكاملة على البيانات والمعلومات المتدفقة داخل الحدود الرقمية للدولة.

٢. فرض رقابة صارمة على منصات الإنترنت الأجنبية العاملة داخل البلاد.

٣. تطوير بنى تحتية وطنية تكنولوجية تقلل الاعتماد على الغرب.

---

(١) نايف، جوزيف س. مستقبل القوة. نيويورك: بابليك أفيرز، ٢٠١١، ص. ١٣٥.

(٢) شميت، مايكل ن. (محرر). *دليل تالين للقانون الدولي المطبق على الحرب الإلكترونية*.(مطبعة جامعة كامبريدج، ٢٠١٣)، ص٤٦.

هذا التوجه يعكس مخاوف الدول من فقدان السيطرة الرقمية لصالح الشركات متعددة الجنسيات أو القوى الغربية، وهو ما أطلق نقاشًا عالميًا حول التوازن بين الأمن الرقمي وحرية الإنترنت [١].

رابعًا: تفكك مفاهيم الحياد الرقمي وتحدياته في أوقات الحرب

كانت المفاهيم التقليدية كالحياد في النزاعات المسلحة مرتبطة بالدول، لكن في الفضاء الرقمي، أصبح الحياد أكثر تعقيدًا. فعلى سبيل المثال:

١. شركات التكنولوجيا مثل "مايكروسوفت" أو "ستارلينك" أصبحت أطرافًا مؤثرة في الحروب، كما حدث في أوكرانيا.
٢. شبكات التواصل الاجتماعي تُستغل لنشر الدعاية أو التضليل أو حتى للتنسيق العسكري.

كل ذلك يُفرغ مبدأ الحياد من مضمونه ويجعل من الفضاء السيبراني ساحة تداخل بين مصالح سياسية، اقتصادية، وعسكرية، ما يفرض إعادة نظر في المفهوم القانوني للحياد وأطراف النزاع [٢].

خامسًا: الحاجة لإصلاح شامل في بنية القانون الدولي السيبراني

أمام هذه التحديات المتزايدة، بات من الضروري تطوير نظام قانوني دولي خاص بالصراعات الرقمية، يتضمن:

١. تعريفًا دقيقًا للهجوم السيبراني وشروط الرد المشروع عليه.
٢. آليات تحقق تقنية وقانونية لإسناد الهجمات.
٣. إطارًا تعاونيًا عالميًا لتقاسم المعلومات والدفاع السيبراني الجماعي.

وقد برزت محاولات في هذا السياق، مثل "مبادئ تالين" التي حاولت تقديم تفسير قانوني للصراعات السيبرانية، لكنها لا تزال غير ملزمة قانونيًا، ما يبرز الحاجة إلى معاهدة دولية شاملة [٣].

---

(١) كريمرس، روجير. "الصين الإلكترونية: ترقية الدعاية، الرأي العام، وإدارة المجتمع للقرن الواحد والعشرين". *مجلة الصين المعاصرة*، المجلد ٢٦، العدد ١٠٣، (٢٠١٧): ص ٩٠.

(٢) تاديو، ماريا روساريا. "حدود الحياد في الفضاء الإلكتروني". *أخلاقيات وتقنية المعلومات*، المجلد ١٩، العدد ١، (٢٠١٧): ص. ١٢.

(٣) هاثاواي، أونا أ.، وآخرون. "قانون الهجوم الإلكتروني". *مجلة كاليفورنيا للقانون*، المجلد ١٠٠، العدد ٤، (٢٠١٢): ص٨٥٢.

الخاتمة

في الختام، يمكن القول أن توظيف التكنولوجيا الرقمية في الصراعات الدولية قد أصبح عنصرًا أساسيًا في تطور الحروب الحديثة. إن هذه التكنولوجيا لم تقتصر فقط على مجال الحرب التقليدية، بل توسعت لتشمل الفضاء السيبراني ووسائل الإعلام الرقمية، ما أتاح للدول والجماعات المسلحة استراتيجيات جديدة وأكثر تطورًا للتأثير على الأحداث الدولية. هذا التطور يشكل تحديات كبيرة للأمن الوطني والدولي على حد سواء، حيث ظهرت الحاجة الملحة لتطوير نظم قانونية دولية تتعامل مع هذه الظواهر بشكل فعال.

لقد أظهرت الدراسة أن التكنولوجيا الرقمية تسهم بشكل كبير في إدارة الحروب الحديثة، من خلال تعزيز القدرات العسكرية والاستخباراتية، وإعادة تشكيل مفاهيم الحرب النفسية، فضلاً عن تسهيل وتيرة الهجمات الإلكترونية ضد البنية التحتية الحساسة. ومع تزايد استخدام وسائل التواصل الاجتماعي وتكنولوجيا المعلومات في الصراعات الدولية، تصبح التهديدات السيبرانية أكثر تعقيدًا وتراكمًا، ما يتطلب استجابة سريعة ومتجددة من قبل الدول والمجتمع الدولي.

ومع ذلك، يبقى هناك تحدي كبير في توظيف هذه التكنولوجيا بشكل آمن وأخلاقي، لتجنب تبعات غير متوقعة قد تؤدي إلى تصعيد الأزمات أو انتهاك حقوق الإنسان. في هذا السياق، يبقى من الضروري أن تتعاون الدول والهيئات الدولية في وضع استراتيجيات متكاملة للتصدي لهذه التحديات، بما في ذلك تعزيز الدفاعات السيبرانية، وتطوير سياسات قانونية تحكم استخدام التكنولوجيا في النزاعات.

في النهاية، فإن الحاجة إلى توازن دقيق بين الاستخدام المسؤول للتكنولوجيا الرقمية وتعزيز الأمن الدولي تبقى أمرًا حاسمًا في تحقيق الاستقرار والسلام في العالم المعاصر. ومن المهم أن تبقى الجهود البحثية والسياسية مستمرة في هذا المجال، مع التركيز على تقديم حلول قانونية وتكنولوجية مبتكرة، لضمان حماية السيادة الوطنية وضمان السلامة الرقمية للأجيال القادمة.

أولاً: النتائج

١. التكنولوجيا الرقمية أصبحت عنصراً فاعلاً في بنية الصراعات الدولية المعاصرة

أظهرت الدراسة أن التكنولوجيا الرقمية لم تعد مجرد أداة مساندة في الصراع، بل أصبحت في قلب العمليات الاستراتيجية، مؤثرة في صنع القرار السياسي والعسكري، وتحديد مسارات النزاع في أبعاده السيبرانية والميدانية.

٢. التحول في مفهوم السيادة والأمن القومي

أدى التوسع في استخدام الأدوات الرقمية إلى إعادة تشكيل مفهوم السيادة، حيث باتت التهديدات غير تقليدية وعابرة للحدود، ما فرض على الدول إعادة النظر في أدواتها الدفاعية ومصادر قوتها الوطنية.

٣. تنامي استخدام الذكاء الاصطناعي والخوارزميات في إدارة الحروب

دلّت المباحث على أن الذكاء الاصطناعي لم يعد مجرد وسيلة لتحليل البيانات، بل أصبح لاعباً رئيساً في توجيه الطائرات دون طيار، وتحليل أنماط الخصم، وتنسيق العمليات العسكرية بفعالية غير مسبوقة.

٤. الدور المحوري لوسائل التواصل الاجتماعي في الحروب النفسية والمعلوماتية

أصبحت المنصات الرقمية ساحة مواجهة مركزية، إذ تُستخدم بشكل منظم في التأثير على الرأي العام، وتزييف الحقائق، وتوجيه الحملات الدعائية، ما عزز من تأثير الحرب النفسية في بنية النزاعات الحديثة.

٥. غياب إطار قانوني دولي واضح ينظم استخدام التكنولوجيا الرقمية في الصراعات

أوضحت الدراسة وجود فراغ قانوني كبير فيما يتعلق بتأطير استخدام الفضاء السيبراني وأدوات التكنولوجيا الحديثة في النزاعات المسلحة، وهو ما قد يؤدي إلى تصاعد غير منضبط في استخدام هذه الوسائل دون رادع دولي ملزم.

٦. ضعف التعاون الدولي في مجال الأمن السيبراني

تبيّن أن هناك تبايناً في استجابات الدول لمخاطر التكنولوجيا الرقمية، وغياب آليات شاملة للتنسيق بين الفاعلين الدوليين، ما يجعل من الأمن السيبراني مجالاً هشًّا وسهل الاختراق في بعض السياقات.

ثانياً: التوصيات

١. ضرورة وضع إطار قانوني دولي شامل ينظم استخدام التكنولوجيا الرقمية في النزاعات

توصي الدراسة بضرورة تحرك المجتمع الدولي، من خلال الأمم المتحدة والمنظمات الإقليمية، نحو صياغة اتفاقية دولية مُلزمة تُنظم استخدام الفضاء السيبراني في أوقات السلم والحرب، وتضع تعريفًا دقيقًا للهجمات السيبرانية ومعايير الرد المشروع عليها.

٢. تعزيز قدرات الدول في الأمن السيبراني من خلال الاستثمار في البنى التحتية الرقمية

ينبغي للدول، ولا سيما النامية، أن تضع الأمن الرقمي في صلب استراتيجياتها الدفاعية عبر بناء أنظمة متقدمة للحماية من الهجمات السيبرانية، وتدريب كوادر مختصة، وتطوير مراكز للإنذار المبكر والاستخبارات الرقمية.

٣. إعادة تعريف السيادة الوطنية في ضوء التهديدات الرقمية العابرة للحدود

توصي الدراسة بأن تتبنى الدول مفهوماً حديثاً للسيادة يأخذ في الاعتبار التحديات الناتجة عن الأدوات الرقمية، بحيث لا تُفهم السيادة فقط بالحدود الجغرافية، بل تشمل الفضاءات المعلوماتية والبيانات الوطنية.

٤. تعزيز الشفافية والمساءلة في استخدام تقنيات الذكاء الاصطناعي في المجالات العسكرية

يجب أن تخضع استخدامات الذكاء الاصطناعي في الحروب لرقابة مدنية وقانونية تضمن عدم استخدامها في انتهاك حقوق الإنسان أو استهداف المدنيين، من خلال بناء قواعد بيانات موحدة ومعايير أخلاقية واضحة.

٥. تنمية الوعي المجتمعي بمخاطر الحرب الرقمية وأدوات التأثير المعلوماتي

توصي الدراسة بتكثيف برامج التثقيف الإعلامي في المجتمعات، وتعزيز المهارات الرقمية لدى المواطنين، لمواجهة التلاعب بالمعلومات، والكشف عن حملات التضليل السيبراني، بما يسهم في بناء جبهة داخلية صلبة ضد الاختراقات.

٦. تشجيع التعاون الدولي في مجال البحث والتطوير التكنولوجي الدفاعي

على الدول تبنّي سياسات للتعاون في مجال الابتكار الرقمي المرتبط بالأمن، وتبادل الخبرات والتجارب الناجحة، خاصة في مجالات الحوسبة الكمومية، التشفير المتقدم، وأنظمة الدفاع الإلكتروني التنبؤية.

المصادر

أولاً: الكتب:

١- ريد، توماس. *الحرب الإلكترونية لن تحدث*. مطبعة جامعة أكسفورد، ٢٠١٣.

٢- شميت، مايكل ن. (محرر). *دليل تالين للقانون الدولي المطبق على الحرب الإلكترونية*. مطبعة جامعة كامبريدج، ٢٠١٣.

٣- كاظم، فاضل. *الحرب السيبرانية وتوازن الردع الرقمي*. مركز الأفق للدراسات، ٢٠٢٢.

٤- مرعي، خالد عبد الله. *التحول الرقمي والنزاعات الحديثة*. دار النهضة العربية، ٢٠٢٠.

ثانياً: المجلات العلمية:

١- أحمد، تالمير. "الدبلوماسية الرقمية ووساطة الصراعات". *التحليل الاستراتيجي*، المجلد ٤٥، العدد ٤، (٢٠٢١): ص. ٣٥٦.

٢- بشير، هالة. "البلوكتشين في الأمن السيادي". *مجلة الأمن الرقمي*، العدد ٩، (٢٠٢٣): ص. ٤١.

٣- تاديو، ماريا روساريا. "حدود الحياد في الفضاء الإلكتروني". *أخلاقيات وتقنية المعلومات*، المجلد ١٩، العدد ١، (٢٠١٧): ص. ١٢.

٤- الخالدي، زينب حسن. "الصراعات الرقمية وإشكاليات السيادة الوطنية". *مجلة البحوث والدراسات السياسية*، المجلد ١٢، العدد ١، (٢٠٢٣): ص. ٩٧.

٥- خليفة، عادل. "الذكاء الاصطناعي في الأمن القومي". *مجلة شؤون أمنية*، العدد ١٨، (٢٠٢٢): ص. ٩١.

٦- عيسى، مروان. "الخوارزميات ودورها في القرار العسكري". *مجلة الذكاء الاصطناعي والسياسة*، (٢٠٢٢): ص. ٦٢.

٧- كريمرس، روجير. "الصين الإلكترونية: ترقية الدعاية، الرأي العام، وإدارة المجتمع للقرن الواحد والعشرين". *مجلة الصين المعاصرة*، المجلد ٢٦، العدد ١٠٣، (٢٠١٧): ص. ٩٠.

٨- كنعان، نزار عبد الحميد. "التكنولوجيا كعنصر مؤثر في الأمن الدولي". *مجلة العلوم السياسية - جامعة بغداد*، العدد ٦٨، (٢٠٢٢): ص. ١٤٣.

٩- مراد، هاني. "القدرات الفضائية في زمن النزاعات". *المجلة الجيوسياسية*، العدد ٢٧، (٢٠٢٣): ص. ٣٣.

١٠-معهد الدراسات العسكرية. "تكنولوجيا الدرونز وتغيير نمط الحروب". تقرير استراتيجي، ٢٠٢٣، ص. ٤٤.

١١-نايف، جوزيف س. "القوة الإلكترونية". *مركز بيلفر بجامعة هارفارد للعلوم والشؤون الدولية*، (٢٠١٠): ص. ٩–١٣.

١٢-نايف، جوزيف س. "مستقبل القوة. بابليك أفيرز"، (٢٠١١): ص. ١٣٧.

١٣- هاثاواي، أونا أ.، وآخرون. "قانون الهجوم الإلكتروني". *مجلة كاليفورنيا للقانون*، المجلد ١٠٠، العدد ٤، (٢٠١٢): ص. ٨٥٢.

ثالثاً: المصادر باللغة الانكليزية

1- Deibert, R. J. (2020). Reset: Reclaiming the Internet for Civil Society. House of Anansi Press. pp. 45-52.

2- Horowitz,M. C. (2018). Artificial Intelligence, International Competition, and the Balance of Power. Texas National Security Review, 1(3), pp. 37-42.

3- Libicki, M. C. (2009). Cyberdeterrence and Cyberwar. RAND Corporation. pp. 23–27.

4- Nye, J. S. (2011). The Future of Power. PublicAffairs. pp. 112–115.

5- Nye,J. S. (2020). Cyber Threats to Democratic Institutions: The New Frontier. Foreign Affairs, 99(5), pp. 112-125.

6- Singer, P. W., & Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press. pp. 85-88

7- Woolley, S. C., & Howard, P. N. (2019). Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media. Oxford University Press. pp. 45-63.