الدفاع الشرعي في الحرب السيبرانية

أ. عطية أحمد عطية السويح * - كلية القانون ـ جامعة الجفرة.
tyhalswyh787@gmail.com

تاريخ الاستلام 7 / 12 / 2024م تاريخ القبول 5 / 6 / 2025م

Legitimate Defense in Cyber Warfare

*Attia A. Al-Suwaih – Lecturer at Department of International Law,
Faculty of Law, University of Al-Jufra, Libya

Abstract
With the increasing use of cyberspace as a new tool in armed conflicts, there has emerged an urgent need to examine the extent to which cyber operations are subject to international law, particularly international humanitarian law. This research explores the concept of cyber warfare and its distinguishing characteristics compared to traditional warfare. It also presents examples of prominent cyberattacks, such as the reciprocal attacks between Iran and Israel, to highlight the legal challenges posed by this emerging form of conflict.
The study focuses on analyzing the concept of self-defense in light of Article 51 of the United Nations Charter and investigates the applicability of international humanitarian law principles, despite the unique nature of cyberspace—especially the difficulty of accurately identifying actors and the overlap between civilian and military targets.
Additionally, the research discusses the reports issued by the United Nations Group of Governmental Experts (2015 and 2023), which affirmed that international law, including the UN Charter, applies to the use of information and communication technologies. The study concludes that there is growing international consensus on the necessity of subjecting cyberattacks to international legal frameworks, contributing to the achievement of peace and stability in the global digital environment.
Keywords: Cyber Warfare – Self-Defense – Cybersecurity – United Nations Charter

الملخّـــــــص:
مع تصاعد استخدام الفضاء السيبراني كأداة جديدة في النزاعات المسلحة، برزت الحاجة الملحة إلى دراسة مدى خضوع العمليات السيبرانية لأحكام القانون الدولي، وخاصة القانون الدولي الإنساني، ويتناول هذا البحث مفهوم الحرب السيبرانية، وخصائصها التي تميزها عن الحروب التقليدية، ويستعرض نماذج من أبرز الهجمات

السيبرانية، مثل الهجمات المتبادلة بين إيران وإسرائيل، بهدف إيضاح التحديات القانونية التي يفرضها هذا النوع من النزاعات الحديثة، ويركز البحث على تحليل مفهوم الدفاع الشرعي في ضوء المادة (51) من ميثاق الأمم المتحدة، واستقصاء مدى إمكانية انطباق مبادئ القانون الدولي الإنساني رغم الطبيعة الفريدة لهذا الفضاء من حيث صعوبة التحديد الدقيق للجهات الفاعلة وتداخل الأهداف المدنية والعسكرية، كما يناقش التقرير الصادر عن فريق الخبراء الحكوميين بالأمم المتحدة (2015، 2023) والذي أكد على انطباق القانون الدولي، بما في ذلك ميثاق الأمم المتحدة، على استخدام تكنولوجيا المعلومات والاتصالات. وينتهي البحث إلى أن هناك توافقًا دوليًا متزايدًا على ضرورة إخضاع الهجمات السيبرانية للضوابط القانونية الدولية، بما يسهم في تحقيق الأمن والاستقرار في البيئة الرقمية العالمية.

الكلمات المفتاحية: الحرب السيبرانية – الدفاع الشرعي – الامن السيبراني – ميثاق الامم المتحدة

تمهيد:

في ظل التطور المتسارع لثورة تكنولوجيا المعلومات والاتصالات خلال العقود الأخيرة، برز الفضاء السيبراني بوصفه ساحة جديدة وموازية لساحات الصراع التقليدي، حيث تُستخدم الوسائل الرقمية لشن هجمات إلكترونية قد تُهدّد الأمن القومي، وتستهدف البنية التحتية الحيوية للدول، وقد شكّل هذا الواقع الجديد تحديًا حقيقيًا للمنظومة القانونية الدولية، ولا سيما فيما يتعلق بإمكانية إدراج الهجمات السيبرانية ضمن مفهوم "النزاع المسلح" أو "العدوان"، كما هو منصوص عليه في المادتين (2) و(51) من ميثاق الأمم المتحدة.

وقد أسفر هذا التحوّل عن حالة من الجدل القانوني المتنامي بشأن مدى مشروعية ممارسة حق الدفاع الشرعي ردًّا على الهجمات السيبرانية، بالإضافة إلى التساؤل حول مدى انطباق مبادئ القانون الدولي الإنساني، الذي نشأ لتنظيم النزاعات المسلحة التقليدية، على هذا الشكل الحديث والمعقد من النزاعات(دراجي، العكور،2024،ص:2).

وعلى الرغم من وجود شبه إجماع قانوني على أن القانون الدولي الإنساني يمكن أن يُطبّق على العمليات السيبرانية عند وقوع نزاع مسلح، فإن طبيعة الفضاء السيبراني، بما يتسم به من صعوبة التتبع، وغموض الفاعل، وتداخل البنية المدنية والعسكرية، تمثل عوائق فعلية أمام التطبيق السليم والفعّال لقواعد هذا القانون.

وتجدر الإشارة إلى أن الهجمات السيبرانية لم تعد تقتصر على الجرائم الإلكترونية

ذات الطابع البسيط أو الأثر المحدود، بل اتّسع نطاقها لتُستخدم كأداة تهديد إستراتيجية، تتداخل مع النزاعات المسلحة سواء الدولية أو غير الدولية، وتُنفّذ أحيانًا من قبل جماعات وتنظيمات مسلحة غير حكومية، أو كجزء من عمليات عسكرية متزامنة مع الحرب التقليدية، وهو ما يزيد من تعقيد المشهد القانوني والسياسي العالمي (عبد القادر، 2025،ص:7)

في هذا السياق، برزت الحاجة الماسّة إلى إيجاد إطار قانوني دولي واضح وشامل يُنظّم العمليات السيبرانية، ويضع ضوابط لاستخدام القوة في هذا المجال المتغير، بما يُسهم في سدّ الفجوة القائمة بين التطورات التكنولوجية من جهة، والآليات القانونية المعمول بها حاليًا من جهة أخرى، سواء على المستوى الوطني أو الدولي.

ومن هذا المنطلق، تسعى هذه الدراسة إلى تسليط الضوء على الإطار القانوني للدفاع الشرعي في سياق الحرب السيبرانية، من خلال تحليل مدى مشروعية الرد على الهجمات السيبرانية وفقًا للمادة (51) من ميثاق الأمم المتحدة، واستكشاف مدى إمكانية انطباق مبادئ القانون الدولي الإنساني على هذا النوع من العمليات، خاصة في ظل ما يتميز به الفضاء السيبراني من خصائص فريدة مثل غموض الفاعل وصعوبة التمييز بين الأهداف المدنية والعسكرية. كما تهدف الدراسة إلى رصد أبرز الإشكاليات القانونية التي تطرحها هذه الهجمات، وتقييم مدى كفاية القواعد الدولية الراهنة لمواجهتها.

مشكلة البحث:

يشهد العالم تحوّلًا أساسياً في طبيعة النزاعات المسلحة، بأنها لم تعد مقتصرة على المواجهات التقليدية، بل امتدّت إلى ساحة جديدة وهي الفضاء السيبراني، الذي أصبح يشكّل ميدانًا فعّالًا لشنّ هجمات قد تُهدّد الأمن القومي للدول وتُلحق أضرارًا جسيمة بالبنية التحتية الحيوية.

وقد طرحت هذه التطورات إشكالات قانونية معقدة أمام القانون الدولي، وفيما يتعلق بكيفية توصيف هذه الهجمات من منظور قانوني، وتزداد المشكلة تعقيدًا مع خصوصية الهجمات السيبرانية، مثل صعوبة التحقق من الجهة الفاعلة، والطابع غير المادي للضرر، وتداخل الأهداف المدنية والعسكرية.

ومن هنا تنبع مشكلة البحث في رصد وتحليل مدى مشروعية الدفاع الشرعي ضد الهجمات السيبرانية، وفقًا لقواعد القانون الدولي، وخاصة القانون الدولي الإنساني، وتحديد ما إذا كانت هذه الهجمات تستوفي الشروط اللازمة لتفعيل هذا الحق، في ظل غياب اتفاق دولي واضح بشأن تأطير الحرب السيبرانية ضمن مفاهيم النزاع المسلح

والعدوان.

أسئلة البحث:

1- ما الإطار القانوني الذي ينظّم استخدام القوة في الفضاء السيبراني، وتحديد مدى انطباق قواعد القانون الدولي الإنساني على الهجمات السيبرانية، لا سيما في حالات النزاعات المسلحة؟

2- ما أبرز التحديات القانونية التي تعيق تطبيق مبدأ الدفاع الشرعي في الفضاء السيبراني، مثل صعوبة الإسناد والتمييز بين الأهداف المدنية والعسكري؟

3- ما أبرز النماذج الواقعية للهجمات السيبرانية، وبخاصة النزاع السيبراني بين إيران وإسرائيل، وتقييم مدى قانونية الردود التي وقعت في ضوئها ؟

4- ما المقترح في إطار قانوني متوازن يمكن أن يُسهم في سد الفجوات الحالية، ويُعزّز الحماية القانونية في ظل تنامي التهديدات السيبرانية العابرة للحدود؟

أهداف البحث:

1- تحليل الإطار القانوني الذي ينظّم استخدام القوة في الفضاء السيبراني، وتحديد مدى انطباق قواعد القانون الدولي الإنساني على الهجمات السيبرانية، لا سيما في حالات النزاعات المسلحة.

2- رصد أبرز التحديات القانونية التي تعيق تطبيق مبدأ الدفاع الشرعي في الفضاء السيبراني، مثل صعوبة الإسناد والتمييز بين الأهداف المدنية والعسكرية.

3- استعراض أبرز النماذج الواقعية للهجمات السيبرانية، وبخاصة النزاع السيبراني بين إيران وإسرائيل، وتقييم مدى قانونية الردود التي وقعت في ضوئها.

4- اقتراح إطار قانوني متوازن يمكن أن يُسهم في سد الفجوات الحالية، ويُعزّز الحماية القانونية في ظل تنامي التهديدات السيبرانية العابرة للحدود.

أهمية البحث:

تنبع أهمية هذا البحث من تناوله لقضية حديثة ومعقّدة لا تزال محل نقاش فقهي وقانوني واسع، وهي الهجمات السيبرانية، التي فرضت نفسها كواقع جديد في العلاقات الدولية والصراعات المعاصرة. ويسلط البحث الضوء على مفهوم الحرب السيبرانية باعتبارها نمطًا استثنائيًّا من أنماط العدوان، يتميز بالغموض في الفاعلين وصعوبة تتبع الأثر المباشر، وهو ما يثير تساؤلات قانونية جوهرية حول كيفية التعامل معها.

كما تكمن أهمية الدراسة في سعيها إلى تحليل مدى مشروعية الدفاع الشرعي ضد هذه

الهجمات وفقًا لما نصّت عليه المادة (51) من ميثاق الأمم المتحدة، واستجلاء حدود هذا الحق في ضوء طبيعة الهجمات السيبرانية. ويتعمق البحث كذلك في تحليل قواعد ومبادئ القانون الدولي الإنساني لاختبار قابليتها للتطبيق على هذا النوع من الأعمال العدائية، لا سيما في ظل تداخل الأهداف المدنية والعسكرية، وغموض مبدأ التناسب في السياق الرقمي.

وأخيرًا، تبرز أهمية البحث في تناوله لحالات واقعية من النزاعات السيبرانية، وعلى رأسها الهجمات المتبادلة بين إيران وإسرائيل، كمثال تطبيقي لفهم مدى توافق الممارسات الفعلية مع المبادئ القانونية الدولية، ومدى الحاجة إلى تطوير إطار قانوني شامل ومُلزم لمواكبة تحديات الحرب السيبرانية الحديثة.

مراجعة الأدبيات القانونية السابقة:

شهدت السنوات الأخيرة اهتمامًا متزايدًا من قبل الباحثين والمراكز المتخصصة في القانون الدولي بدراسة الإشكالات القانونية المرتبطة بالحرب السيبرانية، وخصوصًا مدى خضوعها لأحكام القانون الدولي الإنساني، ومشروعية الرد عليها في إطار الدفاع الشرعي.

وهناك واحدة من أبرز هذه الدراسات التي ناقشت هذه المسألة هي دراسة دارجي والعكور(2024) ، بعنوان "الهجمات السيبرانية وفقًا لأحكام القانون الدولي الإنساني"، المنشورة في مجلة دراسات: علوم الشريعة والقانون، يؤكد الباحثان على أن الهجمات السيبرانية قد تُعد بمثابة أعمال عدائية خاضعة لقواعد القانون الدولي الإنساني متى ما ارتبطت بنزاع مسلح وأدت إلى آثار تماثل تلك الناتجة عن الأسلحة التقليدية، كما شدّدا على ضرورة تطوير آليات قانونية تضمن احترام مبادئ التمييز والتناسب والضرورة.

كما قدمّ خليل محمد إبراهيم(2022) في دراسة بعنوان "الهجمات السيبرانية في ضوء قواعد القانون الدولي الإنساني"، يُبرز الباحث التحديات التي تعترض تطبيق قواعد النزاع المسلح على الفضاء السيبراني، وخاصة في ما يتعلق بتمييز الأهداف العسكرية عن المدنية.

وصدرت عدة تقارير ودراسات من اللجنة الدولية للصليب الأحمر (ICRC) تُقرّ بإمكانية تطبيق مبادئ القانون الدولي الإنساني على الهجمات السيبرانية خلال النزاعات المسلحة، مؤكدة أن الطابع غير المادي لا يُسقط الحقوق والضمانات الأساسية المكفولة للمدنيين.

وناقش الباحث محمد عبد المنعم (2021) في دراسته بعنوان "الحرب السيبرانية في

القانون الدولي" مدى مشروعية رد الدولة على الهجمات السيبرانية بموجب حق الدفاع الشرعي المنصوص عليه في المادة (51) من ميثاق الأمم المتحدة، وخلص إلى أن التحدي الرئيسي يتمثل في إثبات أن الهجوم السيبراني يرقى إلى مستوى "الهجوم المسلح"، وهو ما يتطلب معيارًا موضوعيًا واضحًا.

وتبرز في هذا السياق دراسة للباحثة "هومنا سوهيل" بعنوان "خطوط التصدع في تطبيق القانون الدولي الإنساني على الحرب السيبرانية"، حيث تسلط الضوء على أبرز التحديات التي تعيق تطبيق قواعد القانون الدولي الإنساني على العمليات السيبرانية، بدءًا من إشكالية تعريف "الهجوم" في الفضاء الرقمي، مرورًا بصعوبة تحديد الجهة المسؤولة عن الهجوم (الإسناد)، وصولًا إلى التباين في تفسير مفهومي "الهجوم" و"الهدف المشروع". وتشير الدراسة إلى أن غياب إجماع دولي واضح، بالإضافة إلى الافتقار لقواعد قانونية ملزمة، يُسهم في تعميق فجوة الحماية التي يوفرها القانون الإنساني في سياق النزاعات السيبرانية.

ومن هنا قدّم الباحث" رمضان عبدالله العموري" بحثا بعنوان الحروب السيبرانية: الواقع – التحديات في ضوء القانون الدولي الإنساني، حيث ناقش خطورة الحرب السيبرانية وإشكاليات مدى خضوع الحروب السيبرانية للقواعد الإنسانية الدولية ، والآثار المترتبة عليه، واستخدم في هذه الدراسة المنهج الوصفي والمنهج التحليلي، وقد توصلت الدراسة إلى عدة نتائج أهمها: أن الحروب السيبرانية تؤدي إلى أضرار كبيرة تؤثر سلباً على البُنى التحتية للدول، وكذلك بعد أن أصبحت الحروب السيبرانية عامل مهم في أمن الدول وقوتها، ومن ثم أصبحت الحروب السيبرانية في تزايد مستمر.

أما دراسة الباحث "محمد ربيع أحمد حسين محمد" بعنوان" الهجمات السيبرانية واستخدام القوة في القانون الدولي المعاصر" تناول البحث لمحة عن ماهية ونشأة الهجمات السيبرانية، والتكييف القانوني للهجمات السيبرانية في ضوء التنظيم الدولي، وتطرق إلى المسؤولية الدولية الناشئة عن الهجمات السيبرانية، وأظهرت النتائج أن المجتمع الدولي لا يزال غير متفق على مفهوم واحد للهجمات السيبرانية وطبيعتها القانونية، ولا تزال القوى المهيمنة على المجتمع الدولي، تعمد إلى عرقلة الجهود الدولية لوضع تنظيم قانوني دولي ملزم يهدف إلى تنظيم استخدام الفضاء السيبراني لمحاولة منع الهجمات السيبرانية غير المشروعة.

الإطار النظـــــــــري للبحث

اعتمدت هذه الدراسة على المنهج الوصفي التحليلي، نظرًا لما يتميز به من قدرة على تناول الموضوعات القانونية المعقدة من خلال وصف الظواهر وتحليل النصوص القانونية ذات الصلة، وهو ما يتناسب مع طبيعة البحث الذي يدور حول الدفاع الشرعي في الحرب السيبرانية، باعتباره من القضايا الحديثة التي لا تزال في طور التبلور النظري والتطبيقي.

ولغرض الإحاطة بجوانب الموضوع، قسّم الباحث الدراسة إلى أربعة مباحث رئيسية، يتناول من خلالها ما يلي:

1-توضيح مفهوم الحرب السيبرانية وخصائصها.

2-استعراض أمثلة تطبيقية للهجمات السيبرانية، وبخاصة النزاع الأخير بين إيران وإسرائيل.

3-تحليل مفهوم الدفاع الشرعي كما ورد في ميثاق الأمم المتحدة، وتحديد مدى قابليته للتطبيق في سياق الهجمات السيبرانية.

4-بيان مدى انطباق مبادئ القانون الدولي الإنساني على هذا النوع من النزاعات، في ضوء التحديات التقنية والقانونية المعاصرة.

المبحث الأول ـ مفهوم الحرب السيبرانية:

تعريف الحرب السيبرانية:

تُعد الحرب السيبرانية أحد أبرز مظاهر التحوّل في طبيعة النزاعات المعاصرة، حيث يتم استبدال السلاح التقليدي بوسائل تكنولوجية متطورة تُستخدم لاختراق الأنظمة الإلكترونية والتأثير على أمن الدول ومؤسساتها الحيوية. وعلى الرغم من أن الفقه الدولي لم يتفق بعد على تعريف قانوني موحد للحرب السيبرانية، فإن معظم التعريفات تتفق على أنها "أعمال عدائية تُمارس عبر الفضاء الإلكتروني باستخدام أدوات تقنية لإحداث ضرر أو تدمير في البنى التحتية أو الموارد الاستراتيجية لدولة ما، سواء كانت في حالة نزاع مسلح أو في وقت السلم."

وقد اشتق مصطلح " السيبرانية" لغوياً من المصطلح اليوناني kybernete والذي يعني" التحكم والقيادة عن بعد دون تعامل مباشر"، كما استخدم علمياً لأول مرة في علم الرياضيات للتعبير عن التحكم والاتصالات في الحيوانات والآلات دون تلامس البشر، أو ما سمى وقتها بآليات التنظيم الذاتي (الموصلي،2021،ص8). وقد عرفها دليل تالين 2.0 بأنها: "الأعمال الإلكترونية التي يمكن أن تُسبب، في ظروف معينة،

أضرارًا مادية أو آثارًا وظيفية تعادل تلك التي تُنتجها الأسلحة التقليدية، وقد تُعتبر في بعض الحالات شكلًا من أشكال استخدام القوة أو العدوان الدولي.(Schmitt, 2017) "
في حين يُعرّفها بعض الفقهاء بأنها "استخدام متعمد للوسائل الرقمية من قبل دولة أو جهة فاعلة غير حكومية لتحقيق أهداف استراتيجية عبر التأثير في الأمن القومي، أو زعزعة استقرار الخصم، أو شل قدراته الدفاعية" (Ayalew, 2015).

وتعد الحرب السيبرانية إحدى الوسائل التي تستخدم في القتال العسكري؛ بحيث تمثل في حد ذاتها الحرب العسكرية، أو تكون جزءً من هذه الحرب، وفي كافة الأحوال فإن تأثيرها في المعارك يماثل أو يفوق تأثير الأسلحة التقليدية، إذ يتجه الهجوم السيبراني للعدوان الالكتروني على المنشآت المعادية، حيث يشمل الاختراقات والاعتداءات على النظم المعلوماتية للخصم، بحيث يؤدي هذا الاعتداء لتدمير البنية الالكترونية للعدو من خلال إصابة منشآته بالضرر والفوضى الالكترونية بحيث تعجز عن أداء وظائفها وربما تتحول قيادتها إلى الخصم (محمود،2021،ص24).

وفي الواقع أن أغلب التعريفات التي تم اقرارها بشأن الحرب السيبرانية تشترك ذات المعنى، وهو استهداف مواقع الكترونية أو نظم رقمية، أو أجهزة حاسب آلي، وذلك باستخدام وسائل اتصال رقمية، للاعتداء على سلامة وسرية المعلومات الخاصة بالخصم، إما بالحصول على هذه المعلومات أو محوها أو إتلافها، أو اعادة برمجتها بحيث تعمل بصورة عكسية في صالح الجاني وضد مصلحة الدولة مالكة النظام المعلوماتي (حيدرة،2017،ص186).

خصائص الحرب السيبرانية :

تتّسم الحرب السيبرانية بمجموعة من الخصائص التي تُميزها عن الحروب التقليدية، وتجعل التعامل القانوني معها أكثر تعقيدًا، ويمكن إبراز أهم هذه الخصائص وتحليلها على النحو التالي:

1-الطابع غير المرئي للهجوم: تُنفّذ الهجمات السيبرانية دون استخدام أدوات مادية أو عسكرية ملموسة، وغالبًا ما تكون في صورة أكواد إلكترونية أو فيروسات مبرمجة، تُرسل عن بُعد إلى شبكات الحاسوب أو البنية التحتية الرقمية. ويُصعّب عملية اكتشافه الفوري، ويجعل من الصعب على الدولة المستهدَفة إثبات وقوع اعتداء فعلي يُبرر الرد أو اتخاذ تدابير مضادة(منصور،2020،ص91).

.2-صعوبة تحديد الفاعل : من أكبر التحديات التي تطرحها الحرب السيبرانية هي القدرة على تحديد الجهة المسؤولة عن الهجوم، نظرًا لاستخدام أدوات متطورة لإخفاء الهوية، كتقنيات الانتحال الرقمي، أو حتى تنفيذ الهجوم عبر أطراف ثالثة غير

حكومية، كما أن أغلب الهجمات السيبرانية يتم اكتشافها مصادفة، وغالباً ما يكون هذا الكشف بعد انتهاء الهجمة. وهذا الغموض في الإسناد يُعقّد من إمكانية الرد القانوني، إذ أن تحديد المسؤولية هو شرط أساسي لتفعيل مبدأ الدفاع الشرعي في القانون الدولي.(منصور،2020، ص91).

3-السرعة الفائقة والانتشار اللحظي: تتميّز الهجمات السيبرانية بقدرتها على الانتشار خلال ثوانٍ معدودة، حيث يحدث الهجوم السيبراني في دقائق منتجاً أثره على النظام المعلوماتي للعدو، وقد تمتد آثارها إلى عدة دول في وقت واحد دون تقيّد بالحدود الجغرافية. فالفيروس أو البرمجية الخبيثة يمكن أن تنتقل من هدف إلى آخر بطريقة تلقائية مدمراً للبنية التحتية الالكترونية الخاصة به دون الحاجة الى التضحية بخسائر في الأرواح أو المنشآت. (منصور،2018، ص38)

4- تداخل الأهداف المدنية والعسكرية: نظرًا لاعتماد كل من المؤسسات العسكرية والمدنية على البنية التحتية ذاتها (كالإنترنت، وشبكات الكهرباء، والاتصالات) ، فإن الهجمات السيبرانية قد تطال منشآت مدنية ذات استخدام مزدوج، مثل المستشفيات أو محطات الطاقة، مما يطرح إشكالية في تطبيق مبدأ التمييز المنصوص عليه في القانون الدولي الإنساني، والذي يشترط توجيه الهجمات فقط نحو الأهداف العسكرية. (عبد الصادق،2017،ص62)

5- الطابع العابر للحدود: لا تقتصر آثار الهجوم السيبراني على الدولة المستهدفة وحدها، بل يمكن أن تمتد إلى دول أخرى مرتبطة بالأنظمة المستهدفة، أو تشترك معها في بنية تحتية رقمية، مثل الكابلات البحرية أو مزودي خدمات الإنترنت. وهذا الطابع العابر للحدود يطرح تحديًا إضافيًا أمام تحديد نطاق النزاع ومسؤوليته الدولية.

وقد أكدت الباحثة هومنا سوهيل (2022) أن هذه الخصائص مجتمعة تجعل من الصعب تكييف الهجمات السيبرانية ضمن القوالب التقليدية للنزاع المسلح المعروفة في القانون الدولي. كما أشارت إلى أن غياب اتفاق دولي ملزم بشأن تعريف "الهجوم السيبراني"، وغياب معيار واضح لقياس "الضرر" في السياق الرقمي، يُعزّزان من احتمالية تجاهل الالتزامات القانونية في سياق النزاعات السيبرانية، ويُضعفان من فعالية القانون الدولي الإنساني في تحقيق غايته الأساسية، وهي حماية المدنيين وممتلكاتهم أثناء النزاع .(سوهيل، 2022، ص3–4).

المبحث الثاني ـ أمثلة على الحرب السيبرانية:

خلال يومي24-25 أبريل 2020، تعرضت عدة منشآت تابعة لمصلحة المياه الاسرائيلية لهجوم الكتروني، واتُّهمت إيران بشن هجوم سيبراني على محطة المياه

الإسرائيلية في منطقة الشارون، استهدف تغيير تركيز مادة الكلور في المياه، وهو ما عُدّ تهديدًا مباشرًا للصحة العامة وتسميم الاسرائيلين عن طريق زيادة نسبة مادة الكلور في المياه (Mohajerani,2025).

وقامت إسرائيل بتاريخ18 مايو 2020م، بهجوم الكتروني استهدف ميناء "الشهيد رجائي" الإيراني المطل على مضيق هرمز، مما تسبب في تعطل شديد في حركة الملاحة عبر الممرات والطرق المؤدية إلى الميناء والشحن لأيام متتالية، وقد قال مسئول حكومي أمريكي لصحيفة" واشنطن بوست" إن الهجوم كان دقيق جداً والأضرار التي لحقت بالميناء الايراني كان أكثر خطورة مما وصفته ايران. (yant,2020)

وفي 30 يونيو 2020م، حدثت هجمات على المنشآت النووية في "نطنز" يشتبه أنها هجمات سيبرانية اسرائيلية واستهدفت سلسلة من الهجمات الغامضة لمنشآت نووية في نطنز ومواقع عسكرية في "بارشين" ويعتقد الكثير من المحللين أنها هجمات سيبرانية نفذتها اسرائيل، وإيران اقرت بأنها عملية تخريبية لتعطيل برنامج إيران النووي، وتنزيل فيروس على برنامج التشغيل الالكتروني الذي يدير عملية تخصيب اليورانيوم وتسبب في ذلك بإتلاف عدد كبير من وحدات الطرد المركزي. (الميموني، 2020،ص10)

وبعد ذلك توسع النزاع إلى الفضاء السيبراني بشكل واسع ومتحوّل إلى حرب رقمية متبادلة، تترافق مع التصعيد العسكري. وفيما يلي تفصيل لما جرى من أنشطة سيبرانية بين الطرفين: بحسب تصريحات نائب رئيس الهيئة الوطنية للأمن السيبراني الإسرائيلي "نيتسان عَمار" فقد تضاعف عدد الهجمات السيبرانية الموجهة إلى إسرائيل بمقدار ثلاث مرات منذ اندلاع الحرب مع جماعة حماس في أكتوبر 2023، بمشاركة مباشرة من فاعلين إيرانيين وحزب الله.(عمار،2025) إضافة إلى ذلك، حذّر مدير الأمن السيبراني الإسرائيلي من أن إيران هاجمت حلفاء إسرائيل دوليًا، عبر سرقة البيانات ثم استخدامها في أنشطة سيبرانية إرهابية (ورتنوي،2024)

وبعد الهجمات الصاروخية الإيرانية على إسرائيل في يونيو 2025، رُصد ارتفاع بـ700% في الحوادث السيبرانية المرتبطة بالصراع المعلوماتي، شمل عمليات تصيّد وكشف بيانات غير شرعية، واستهداف قطاعات الطاقة والاتصالات والإعلام (CybelAngel، 2025) ، استهدفت الجهات الإيرانية بنيات إسرائيلية، بينما أطلقت جهات مقربة من إسرائيل مثل "Predatory Sparrow" هجمات على البنوك الإيرانية ومحطات الطاقة باستخدام برمجيات مسح البيانات وتدميرها.(Amer,2025)

ومن أبرز الأمثلة المعاصرة للحرب السيبرانية ما بين روسيا وأوكرانيا على استخدام الفضاء السيبراني كأداة استراتيجية في النزاع، في ديسمبر 2015 استهدفت مجموعة"sandworm" ،المرتبطة بجهاز الاستخبارات الروسي GRU وشبكات توزيع الكهرباء في غرب أوكرانيا عبر برمجية BlaskEnergy مما تسبب في انقطاع التيار الكهربائي لمدة تتراوح بين ساعة وست ساعات. وتكرر الهجوم في عام 2016 باستخدام برمجية Industroyer التي صممت خصيصاً لتعطيل البنى التحتية الصناعية. (CRS، 2024)

ومع بدء الغزو الروسي في فبراير 2022، كثفت روسيا هجماتها السيبرانية بالتزامن مع العمليات العسكرية التقليدية، واستهدفت العملية الشبكات الحكومية ووسائل الإعلام والخدمات العامة بهدف خلق حالة ارتباك نفسي وشلل جزئي في البنية التحتية الرقمية، وفي المرحلة الأولى من العمليات أطلق الروس هجوم DDoS على مواقع حكومية وبنكية كبرى لتعطيل الاتصالات الأساسية (Eichensehr, 2022)

وفي ردّ مباشر على انتشار الهجمات الرقمية، أقدمت الحكومة الإيرانية في 18 يونيو 2025 على تقليص الإنترنت بشدة بنسبة تجاوزت 97% كإجراء مضاد للحد من توزيع عمليات اختراق المصدر الخارجي (Mohajerani,2025).

وبينت هذه الهجمات السيبرانية المتبادلة تصاعدًا نوعيًا في طبيعة النزاعات، مما أثار تساؤلات قانونية وأخلاقية بمدى اعتبارية هذه العمليات "أعمال عدوان" بالمعنى الوارد في ميثاق الأمم المتحدة، وما إذا كانت تبرّر حق الدفاع الشرعي وفقًا للمادة (51).

وبناء على ذلك، فإن هذه الوقائع تعزز من أهمية تطوير إطار قانوني دولي واضح وملزم لتنظيم استخدام القوة في الفضاء الالكتروني، وتطبيق قواعد القانون الدولي الإنساني عليه، بما يضمن حماية المدنيين ويحدّ من الإفلات من العقاب في هذا المجال غير المنظَّم حتى الآن.

المبحث الثالث ـ الدفاع الشرعي وفقاً لميثاق الأمم المتحدة:

لقد أدى اتساع نطاق استخدام الدول للفضاء الإلكتروني في شن الحروب السيبرانية، والاستعانة به في دعم عملياتها العسكرية أثناء النزاعات المسلحة، إلى تحفيز الجهود نحو تنظيم هذا المجال من خلال قواعد القانون الدولي. وعلى الرغم من وجود فراغ تشريعي واضح، فإنه يمكن – في ضوء قانون الحرب – الاستناد إلى المادة 36 من البروتوكول الإضافي الأول لاتفاقيات جنيف، والتي تُلزم الأطراف المتعاقدة، عند

دراستها أو تطويرها أو اقتنائها لأي سلاح جديد أو وسيلة حرب جديدة، بالتحقق مما إذا كان استخدام هذا السلاح محظورًا في بعض أو جميع الحالات، بموجب أحكام هذا البروتوكول أو وفقًا لأي من قواعد القانون الدولي.

ويوضح حكم المادة 36 في دراسة أو تطوير أو اقتناء سلاح جديد أو وسيلة أو طريقة جديدة للحرب، تلتزم الدولة الطرف في هذا البروتوكول بأن تحدد ما إذا كان استخدام هذا السلاح أو الوسيلة أو الطريقة محظورًا، في بعض أو جميع الأحوال، بمقتضى أحكام هذا البروتوكول أو أي قاعدة أخرى من قواعد القانون الدولي المنطبق على تلك الدولة.(صعب،2021،ص34)

ومن هنا أقرّ ميثاق الأمم المتحدة في المادة (4/2) مبدأ حظر استخدام القوة أو التهديد بها في العلاقات الدولية، باستثناء حالتين رئيسيتين، إحداهما تتمثل في حق الدفاع الشرعي المنصوص عليه في المادة (51). وقد نصت المادة بوضوح على أن: "ليس في هذا الميثاق ما يضعف أو ينتقص من الحق الطبيعي للدول في الدفاع عن أنفسهم إذا اعتدت قوة مسلحة على أحد أعضاء الأمم المتحدة".

1-إشكالية تصنيف الهجوم السيبراني كـ"عدوان مسلح": في ظل التطورات التكنولوجية الراهنة، تثير الهجمات السيبرانية تساؤلات قانونية حول ما إذا كانت ترقى إلى مستوى "العدوان المسلح" الذي يُبرر اللجوء إلى الدفاع الشرعي. فالميثاق لم يُعرّف "القوة" بشكل صريح، وقد ذهب بعض الفقهاء إلى أن الهجوم السيبراني قد يُعد عدوانًا، متى ما أسفر عن أضرار مادية جسيمة تُشبه تلك التي تُحدثها الأسلحة التقليدية، مثل تدمير البنى التحتية، أو تعطيل شبكات الكهرباء، أو التسبب في خسائر بشرية .

وقد حرص ميثاق الأمم المتحدة على إقرار هذا المبدأ بنصه في الفقرة الرابعة من مادته الثانية على أن" يمتنع أعضاء الهيئة جميعاً في علاقاتهم الدولية عن التهديد باستعمال القوة أو استخدامها ضد سلامة الاراضي أو الاستقلال السياسي لأي دولة أو على وجه آخر لا يتفق ومقاصد الأمم المتحدة" وكما اكدته العديد من الاعلانات والمواثيق الدولية العالمية منها والاقليمية وحتى في تلك الاحوال التي تجيز فيها أحكام القانون الدولي اللجوء الى القوة يكون بشروط وضوابط وفي حالات محددة، ويعد تسخير الفضاء السيبراني وخاصة في المجال العسكري تطبيقاً للاستفادة من هذه التطورات والتي مكنت من ادارة العمليات والهجمات أثناء النزاعات بوسائل وآليات تعتمد تقنيات مغايرة تماماً لوسائل الحرب التقليدية حتى اصبحت الحرب السيبرانية من سمات الحروب المعاصرة.(المقريف،2022،ص5)

وهو ما أكده "دليل تالين 2.0" في التقرير الصادر عن مركز التميز للدفاع السيبراني التابع لحلف الناتو، حيث اعتبر أن بعض الهجمات الإلكترونية قد تستوفي شروط "القوة المسلحة" بالمعنى الوارد في المادة.(51)

2-ضوابط ممارسة الدفاع الشرعي في الحرب السيبرانية: حتى إذا تم الاعتراف بالهجوم السيبراني كعدوان مسلح، فإن اللجوء إلى الدفاع يجب أن يُراعي الشروط العامة للدفاع الشرعي، وهي:

الضرورة: أن يكون الهجوم وشيكًا أو قائمًا ولا يمكن دفعه بوسائل أخرى.

التناسب: أن تكون القوة المستخدمة في الرد متناسبة مع حجم العدوان.

الإسناد: أن تكون الجهة المعتدية معروفة بوضوح، وهو ما يُعد من أبرز تحديات المجال السيبراني.

وقد أشارت الباحثة Eichensehr (2022) إلى أن الهجمات الروسية على أوكرانيا لم تستدعِ ردًا دفاعيًا سيبرانيًا واسعًا من الغرب، جزئيًا بسبب صعوبة الإسناد الدقيق، والخشية من التصعيد غير المحسوب في الفضاء الإلكتروني.

3-غياب اتفاق دولي واضح: رغم الاعتراف بحق الدفاع الشرعي، فإن المجتمع الدولي لم يتوصل بعد إلى اتفاق ملزم يُحدد متى يكون الرد على الهجمات السيبرانية مشروعًا بموجب المادة (51). وهذا يفتح الباب أمام تفسيرات مرنة، وربما استغلال سياسي لهذا الحق، خاصة في ظل غموض طبيعة التهديدات الرقمية وتعدد الفاعلين (الدول، التنظيمات، الأفراد).

ويرى بعضهم أن محكمة العدل الدولية، من خلال حكمها في قضية نيكاراغوا، قد فسّرت المادة (4/2) من ميثاق الأمم المتحدة تفسيرًا واسعًا لا يقتصر على الاستخدام التقليدي للقوة، المتمثل في تدخل القوات النظامية عبر الحدود، بل فتحت المجال لاعتبار تصرفات أخرى – غير الهجوم العسكري المباشر – ضمن الأفعال التي قد تُعد خرقًا لحظر استخدام القوة وفقًا لنص المادة المذكورة.

المبحث الرابع - مدى انطباق مبادئ القانون الدولي الانساني في الحرب السيبرانية:

كما أشرنا سابقًا، فإن أحكام القانون الدولي قد أكدت على مبدأ حظر استخدام القوة وضرورة اللجوء إلى الوسائل السلمية لتسوية النزاعات، إلا أن ذلك لا يمنع من وقوع عمليات حربية سواء كانت ضمن الاستثناءات التي تُجيز استخدام القوة، أو في الحالات التي تُمارَس فيها القوة بين الدول دون أن ترقى إلى مستوى النزاع المسلح

بين دولتين، أو حتى داخل الدولة الواحدة.

وقد بُذلت العديد من الجهود الدولية من أجل الحد من مخاطر النزاعات المسلحة، والسعي إلى تنظيمها وتقليل آثارها السلبية، لا سيما أن التجارب أثبتت أن مثل هذه النزاعات غالبًا ما تتسبب في آثار إنسانية كارثية، خصوصًا عند استخدام وسائل غير تقليدية كالهجمات السيبرانية ، وأفضت تلك الجهود إلى إقرار مجموعة من القواعد القانونية المعروفة باسم قواعد القانون الدولي الإنساني، والتي تهدف إلى تنظيم سير العمليات الحربية، وهي قواعد مُلزمة التطبيق على جميع الأطراف المنخرطة في النزاع المسلح، بغض النظر عن طبيعة الوسائل أو الأدوات المستخدمة. (أعمر،2019،ص136)

وتُعد اتفاقيات جنيف الأربع المبرمة عام 1949، والبروتوكولان الإضافيان لها الصادران عام 1977، المصدر الأساسي لقواعد القانون الدولي الإنساني، وهي قواعد واجبة التطبيق على جميع الأنشطة التي تقوم بها الأطراف أثناء النزاع المسلح، سواء على الأرض أو خارجه، بهدف تنظيمها والحد من آثارها، لا سيما على المدنيين.

ونظرًا لما شهده الواقع من تغيّر في صور الحروب عن تلك التي كانت سائدة وقت إبرام هذه الاتفاقيات، وما رافقها من تطور في الأسلحة وامتداد ميادين النزاع، والذي كان نتيجة طبيعية للتطور العلمي الكبير الذي حققته الدول، خصوصًا في تطوير قدراتها الحربية؛ فقد بات هناك سعي دائم لمواكبة هذه المستجدات، إذ لم تعد التطورات الحربية محصورة في الوسائل التقليدية، بل شملت مجالات متعددة مثل الفضاء السيبراني الذي أصبح يُوظف في العمليات العسكرية، ويُنظر إليه كساحة جديدة للنزاع.(سمودي،2018،ص384)

وقد أدى استخدام الفضاء السيبراني في المجال العسكري إلى بروز نوع جديد من التهديدات، يقوم على مناورات معلوماتية بدلًا من الأسلحة التقليدية، كناتج مباشر للتطورات التكنولوجية المتسارعة، حتى صارت هذه التقنيات تُستخدم في قيادة الجيوش، وتوجيه الذخائر بدقة عالية، والتحكم في منظومات الإمداد والتموين، مما زاد من تعقيد النزاعات المسلحة وحدّة آثارها، وفاقم التحديات أمام القانون الدولي الإنساني.

لكن، قبل الخوض في مدى خضوع العمليات السيبرانية لمبادئ القانون الدولي الإنساني، تجدر الإشارة إلى أن هذا القانون لا يُطبق إلا في حال قيام نزاع مسلح، وذلك استنادًا إلى المادة الثانية المشتركة من اتفاقيات جنيف لعام 1949، وهو ما يثير

التساؤل بشأن ما إذا كانت العمليات السيبرانية، بمفردها، تُعد من النزاعات المسلحة التي تخضع لقواعد القانون الدولي الإنساني. (لين،2012،ص518)

ويذهب البعض إلى اعتبار بعض الهجمات السيبرانية خاضعة لهذا القانون، حتى وإن لم يُصاحبها استخدامٌ فعلي للقوات المسلحة التقليدية، انطلاقًا من طبيعة الهجمات ذاتها، وما قد تُسببه من أضرار جسيمة. ويرى هؤلاء أن خضوع الهجمات السيبرانية للقانون الدولي الإنساني يتوقف على تقييم نتائجها؛ فإذا نتج عنها آثار مدمرة تُقارن بتلك الناتجة عن استخدام القوة المسلحة التقليدية، من حيث تسببها في الوفاة أو الأذى أو الدمار، فإن القانون الإنساني يكون واجب التطبيق.

في المقابل، يرى فريق آخر أن الهجمات السيبرانية لا ترقى إلى مستوى النزاع المسلح الذي تُطبق عليه قواعد القانون الدولي الإنساني، لعدم وجود نص قانوني صريح ضمن وثائق هذا القانون يُشير إلى مثل هذا النوع من الهجمات. (الرشيدي،2024)

وفي الختام، يمكن القول إن هناك اتجاهًا متزايدًا بين العديد من الدول، والمنظمات الدولية، وخبراء القانون الدولي، يؤيد إخضاع العمليات السيبرانية لأحكام القانون الدولي الإنساني. وقد أكّد على هذا التوجه تقرير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي، التابع للأمم المتحدة، في دورتيه لعامي 2015 و2023؛ حيث نص التقرير على أن أحكام القانون الدولي، وبخاصة ميثاق الأمم المتحدة، تنطبق على استخدام تكنولوجيا المعلومات والاتصالات، باعتبار ذلك شرطًا أساسيًا لحفظ السلم والأمن الدوليين، ولبناء بيئة مستقرة وآمنة لاستخدام هذه التكنولوجيا.

الخاتمة:

وفي ضوء التحليل القانوني المتعمق، والاستعراض النظري لميثاق الأمم المتحدة، والوقائع الميدانية الموثقة من أمثلة الهجمات السيبرانية يكمن القول:

ـ الهجمات السيبرانية هي استهداف مواقع الكترونية أو نظم رقمية، أو أجهزة حاسب آلي، وذلك بتدمير هذه النظم أو محو وسرقة البيانات، والهجمات السيبرانية ذات طابع غير مرئي، وصعوبة تحديد الجهة الفعالة، والسرعة الفائقة للانتشار، وتداخل الأهداف المدنية والعسكرية.

ـ من الصعب تكييف الهجمات السيبرانية ضمن القوالب التقليدية للنزاع المسلح المعروفة في القانون الدولي.

ـ استخدام الهجمات السيبرانية في أغلب الحروب المعاصرة حرب إسرائيل مع ايران2025، وحرب روسيا وأوكرنيا2020.

ـ أن الهجمات السيبرانية يمكن أن تشكل خطرا على السلم والأمن الدوليين، كما في الحروب التقليدية، وتعدو مخالفة لمبدأ عدم استخدام القوة في النزاعات المسلحة.

التوصيات:

ضرورة تطوير قواعد القانون الدولي وإبرام اتفاقية في إطار الأمم المتحدة للهجمات السيبرانية من خلال تعريفها وتحديد صورها وخصائصها والأليات القانونية لمعاقبة مرتكبها.

المراجـــــــــع:

- إبراهيم، خليل محمد. (2022). الهجمات السيبرانية في ضوء قواعد القانون الدولي الإنساني. مجلة كلية القانون للعلوم القانونية والسياسية، 11.(2)
- أعمر، عمر محمود.(2019). الحرب الالكترونية في القانون الدولي الانساني، دراسات علوم الشريعة والقانون، المجلد46،العدد3.
- حيدرة، صبري. (2017). مواجهة الهجمات السيبرانية في القانون الدولي. مجلة حقوق الإنسان والحريات العامة، (4). جامعة عبد الحميد بن باديس، مستغانم، الجزائر.
- دارجي، محمد حسن سعيد، والعكور، عمر صالح. (2024). الهجمات السيبرانية وفقًا لأحكام القانون الدولي الإنساني. مجلة دراسات: علوم الشريعة والقانون، 51.(1)
- عمّار، نيتسان. (2025، 24 يوليو). الهجمات السيبرانية ضد إسرائيل تضاعفت ثلاث مرات منذ السابع من أكتوبر. تايمز أوف إسرائيل. تم الاسترداد من
- https://www.timesofisrael.com/cyberattacks-by-iran-hezbollah-have-tripled-during-the-war-says-israel-cyber-cza
- الرشيدي، هالة أحمد.(2021). هل من حرب سيبرانية بين الولايات المتحدة وروسيا، منشور بجريدة الأهرام، العدد48972، متاح على الرابطhttp://gate.aharm.org.eg/daily/News
- سمودي، رزق أحمد.(2018). حق الدفاع عن النفس نتيجة الهجمات الالكترونية في ضوء قواعد القانون الدولي العام. مجلة جامعة الشارقة للعلوم القانونية، المجلد15، العدد2.
- سوهيل، هومنا. (2022). خطوط التصدع في تطبيق القانون الدولي الإنساني على الحرب السيبرانية. مجلة علم التحقيقات الرقمية وأمن المعلومات والقانون، 17(1)، مقال رقم 8. متاح عبر: https://commons.erau.edu/jdfsl/vol17/iss1/8

- شميت، مايكل. (2017). دليل تالين حول القانون الدولي المنطبق على العمليات السيبرانية، مركز دراسات الدفاع في الناتو، جامعة كمبريدج.
- صعب، ريماس.(2021). المواجهة القانونية للأسلحة غير التقليدية في القانون الدولي، منشورات زين الحقوقية، بيروت.
- عبد الصادق، عادل.(2017). الارهاب الالكتروني كشكل جديد للصراع الدولي، مركز الدراسات السياسية والاستراتيجية، القاهرة.
- عبد القادر، دحماني.(2025). الحروب السيبرانية في ظل القانون الدولي الإنساني. المجلة الجزائرية للحقوق والعلوم السياسية، المجلد 10، العدد 1.
- عبد المنعم، محمد. (2021). الحرب السيبرانية في القانون الدولي. مجلة القانون والسياسة الدولية، 5(3).
- اللجنة الدولية للصليب الأحمر. (2022). القانون الدولي الإنساني والعمليات السيبرانية أثناء النزاعات المسلحة2022-https://www.icrc.org/ar/document/cyber-ihl .
- لين، هربرت.(2012). النزاع السيبراني والقانوني الدولي الانساني. مختارات من المجلة الدولية للصليب الاحمر، مجلد 94.
- محمد، محمد ربيع أحمد حسين.(2023). الهجمات السيبرانية واستخدام القوة في القانون الدولي المعاصر، مجلة العلوم القانونية والاقتصادية،مج65،ع1.
- محمود، عبد الكريم.(2021). تحديات السيادة السيبرانية في القانون الدولي، المركز العربي لأبحاث الفضاء الالكتروني، القاهرة.
- المقريف، نورية الساعدي.(2022). الحرب السيبرانية في ضوء أحكام القانون الدولي. مجلة أبحاث قانونية،مج7ع2.
- منصور، أشرف سعد.(2018). التنظيم الدولي للقوة الالكترونية، المركز القومي للإصدارات القانونية، القاهرة.
- منصور، شادي عبد الوهاب.(2020). حروب الجيل الخامس- أساليب التفجير من الداخل على الساحة الدولية، دار العربي للنشر والتوزيع، القاهرة.
- الموصلي، نور أمير. (2021). الهجمات السيبرانية في ضوء القانون الإنساني (بحث مقدم لاستكمال متطلبات نيل درجة ماجستير التأهيل والتخصص في القانون الدولي الإنساني). الجامعة الافتراضية السورية، دمشق.متاح عبرhttps://svuonline.org :
- الميموني، أحمد بن علي.(2020). الجبهة النشطة: تداعيات المواجهة السيبرانية بين ايران واسرائيل. مجلة الدراسات الإيرانية، مج14،ع12.
- ورتنوي، يوف. (2024، 21 مارس). مسؤولون إسرائيليون: إيران وحزب الله شنّوا هجمات إلكترونية خارج حدود إسرائيل. تايمز أوف إسرائيل. تم الاسترداد من https://www.timesofisrael.com/cyber-officials-say-iranian-hezbollah-attacks-against-israel-tripled-since-oct-

المراجع الاجنبية:

- Ayalew, Yohannes Eneyew. (2015). Cyber Warfare: A New Hullaballoo under International Humanitarian Law. Beijing Law Review, 6(4).
- Amar, N. (2025, July 24). Cyberattacks by Iran, Hezbollah have tripled during the war, says Israel cyber czar. The Times of Israel. Retrieved from

https://www.timesofisrael.com/cyberattacks-by-iran-hezbollah-have-tripled-during-the-war-says-israel-cyber-cza

- CybelAngel. (2025, June 17). Iran-Israel Cyber Conflict Flash Report. CybelAngel. Retrieved from https://cybelangel.com/israel-iran-cyber-conflict-flash-report
- CRS. (2024). Attacks on Ukraine's Electric Grid: Insights for U.S. Policy. https://www.scirp.org/html/1-3300369_60300.htm
- Eichensehr, K. E. (2022). Ukraine, Cyberattacks, and the Lessons for InternationalLaw. American Journal of International Law, 116(3), 512–518. Cambridge University ،Press. https://doi.org/10.1017/ajil.2022.36
- Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0 on the International Law Cambridge University Press. https://bit.ly/2Zexpya
- Mohajerani, M. (2025, June 19). Iran restricts internet access to 97% amid major cyberattacks. The Hacker News. Retrieved from
- https://thehackernews.com/2025/06/iran-restricts-internet-access-to.html
- yant,Iran tried to poison Israelis by increasing chlorine in water, (June 10 2020), Accessed on:26 july,2025.
متاح على موقع المجلس القومي للبحوث الأمريكية:
https://sgp.fas.org/crs/row/R48067.pdf?utm_source=chatgpt.com