تحديات القانون الدولي الإنساني في عصر التكنولوجيا"الهجمات السيبرانية"

م.م حنين فائق حسين

الجامعة المستنصرية/ كلية العلوم السياسية

haneenfaeq1205@uomustansiriyah.edu.iq

ملخص البحث:

يواجه القانون الدولي الإنساني تحديات متزايدة نتيجة للتطورات التكنولوجية الحديثة، ولا سيما مع ظهور الهجمات السيبرانية كعنصر مؤثر في النزاعات المسلحة، تعد هذه الهجمات تهديدًا جادًا للمدنيين والبنية التحتية الحيوية، مما يثير تساؤلات حول كيفية تكييف المبادئ الأساسية للقانون الدولي الإنساني لتناسب الواقع الجديد.

اذ تعيق الهجمات السيبرانية القدرة على التمييز بين الأهداف العسكرية والمدنية، مما يعقد الأمور القانونية، كذلك، تطرح مسألة المسؤولية القانونية تحديات معقدة، حيث يصبح من الصعب تحديد الجهة المسؤولة، سواء كانت دولًا أو كيانات غير حكومية، وفي غياب إطار قانوني واضح ينظم استخدام التكنولوجيا في النزاعات، تتعاظم الحاجة إلى مراجعة شاملة للقوانين الدولية.

لذلك يتطلب الوضع الراهن تطوير معايير جديدة تهدف إلى ضمان حماية المدنيين والامتثال للقوانين الدولية، لذا، يستدعي الأمر تنسيق الجهود بين الدول والمجتمع الدولي لمواجهة هذه التحديات، وضمان فعالية القوانين في ظل عصر التكنولوجيا المتقدمة.

الكلمات مفتاحية: - القانون الدولي الإنساني، المسؤولية القانونية، تكنولوجيا النزاع المسلح، الإطار التشريعي، المعايير المعاصرة.

Challenges of International Humanitarian Law in the Age of "Technology "Cyber Attacks

Mr. Hanin Faeq Hussein

Al-Mustansiriyah University / College of Political Science

Abstract :

International humanitarian law faces increasing challenges due to modern technological developments, particularly with the emergence of cyber attacks as a significant factor in armed conflicts. These attacks pose a serious threat to civilians and critical infrastructure, raising questions about how to adapt the fundamental principles of international humanitarian law to fit the new reality.

Cyber attacks hinder the ability to distinguish between military and civilian targets, complicating legal matters. Additionally, the issue of legal responsibility presents complex challenges, as it becomes difficult to determine the responsible party, whether it be states or non-state actors. In

the absence of a clear legal framework governing the use of technology in conflicts, the need for a comprehensive review of international laws becomes more pressing.

The current situation necessitates the development of new standards aimed at ensuring the protection of civilians and compliance with international laws. Therefore, it requires coordinated efforts between states and the international community to address these challenges and ensure the effectiveness of laws in an era of advanced technology.

Keyword: - International humanitarian law, Legal responsibility, Conflict technology, Legislative framework, Contemporary standards

المقدمة

تعد الحرب السيبرانية من القضايا المهمة والمتزايدة الأهمية على المستوى الدولي، في ظل التقدم التكنولوجي المستمر وتزايد الاعتماد على النظم الرقمية في القطاعات الحيوية للدول، تشكل الحرب السيبرانية جزءاً من النقاش الدولي حول شرعية استخدام أساليب الحرب الحديثة، والتي تثير جدلاً كبيراً حول مدى توافقها مع المبادئ الأساسية للقانون الدولي الإنساني، على مدى سنوات طويلة، تم ترسيخ هذه المبادئ لتصبح جزءاً من القانون الدولي العرفي، الذي يلزم الدول باتباع القواعد المتعلقة بحظر استخدام أسلحة معينة إذا ورد نص صريح بذلك.

في حال عدم وجود نص واضح، يُحكم على مشروعية استخدام أي وسيلة أو سلاح في إطار العرف الدولي، ويُلاحظ أن القانون الدولي الإنساني العرفي لا يحتوي على نصوص شاملة تحظر استخدام الحرب السيبرانية، التي تشمل البرمجيات الخبيثة والفيروسات الإلكترونية وغيرها من الأدوات السيبرانية، الاستثناء الوحيد الذي يمكن الإشارة إليه هو القاعدة التي تحظر استخدام ما يسمى بالأسلحة "العمياء"، أي الأسلحة التي لا تميز بين الأهداف المدنية والعسكرية، وهو ما يمكن تطبيقه على بعض الهجمات السيبرانية.

في الآونة الأخيرة، زاد الاهتمام الدولي بمعالجة موضوع الحروب السيبرانية والأسلحة ذات الصلة، مما أدى إلى جهود دولية لإبرام معاهدات واتفاقيات تهدف إلى تنظيم استخدام هذه الأسلحة، من أبرز المبادرات الحديثة "دليل تالين" الذي يسعى إلى تقديم تفسير لقواعد القانون الدولي وتطبيقها على النزاعات السيبرانية، كما أن الأمم المتحدة وعدد من المنظمات الدولية الأخرى تعمل على تطوير أطر قانونية لمواجهة التهديدات السيبرانية وضمان توافقها مع القوانين الإنسانية الدولية.

ومع ذلك، تبقى العديد من القضايا مفتوحة للنقاش، مثل كيفية تحديد المسؤولية عن الهجمات السيبرانية، وصعوبة تتبع الجهة الفاعلة، بالإضافة إلى التحديات المتعلقة بتطبيق مبادئ التمييز والتناسب في الفضاء السيبراني.

أهمية البحث

نظرًا لتزايد اعتماد الدول والمنظمات غير الحكومية على الهجمات السيبرانية كأداة فعّالة في النزاعات الحديثة، باتت الحروب السيبرانية تشكل تهديداً مباشراً للأمن العالمي والبنى التحتية الحيوية، يتطلب هذا البحث التحقق من مدى قدرة القانون الدولي الإنساني الحالي على التعامل مع هذا النوع من الحروب، والذي يتسم بالغموض والسرعة وعدم إمكانية تحديد الفاعلين بسهولة، هذه الدراسة تسعى إلى فهم كيفية تكييف القوانين الحالية مع الطبيعة المتغيرة للنزاعات السيبرانية،

وتحديد ما إذا كانت المبادئ الحالية كافية لحماية المدنيين والبنى التحتية الحيوية في ظل تصاعد هذه الهجمات.

منهجية البحث:

يعتمد هذا البحث على المنهج الوصفي التحليلي والمنهج المقارن، المنهج الوصفي التحليلي يسعى إلى وصف ظاهرة الهجمات السيبرانية وتحليل تأثيرها على القانون الدولي الإنساني من خلال دراسة طبيعتها وخصائصها وكيفية تنفيذها، المنهج المقارن يهدف إلى مقارنة تطبيقات القانون الدولي الإنساني في النزاعات التقليدية والنزاعات السيبرانية، لتحديد الفجوات القانونية التي تظهر نتيجة تطور التكنولوجيا وظهور الحروب السيبرانية.

الإشكالية:

تتمثل الإشكالية الأساسية لهذه الدراسة في الكشف عن أبعاد الحروب السيبرانية من منظور القانون الدولي الإنساني، ومدى استجابة هذا الإطار القانوني لتحديات الحروب السيبرانية وتأثيرها على الأمن العالمي. وتنقسم هذه الإشكالية إلى الأسئلة التالية:

1. ما هي طبيعة الحروب السيبرانية وأساليبها والأدوات المستخدمة فيها؟
2. ما مدى قابلية تطبيق قواعد القانون الدولي الإنساني على الحروب السيبرانية، وما التحديات القانونية التي تواجه ذلك؟
3. كيف تؤثر الحرب السيبرانية على الأمن والسلم العالميين، وماهي المسؤولية الناجمه عنها؟

هيكلية البحث:

تم تقسيم البحث الى محورين فضلا عن المقدمة والخاتمة تناول المحور الاول الطبيعة القانونية للهجمات السيبرانية والمحور الثاني التحديات القانونية للهجمات السيبرانية في ظل القانون الدولي الانساني، المحور الثالث المسؤولية الدولية تجاه الهجمات السيبرانية.

المحور الأول: الطبيعة القانونية للهجمات السيبرانية

شهد القانون الدولي الإنساني تطورات عديدة استجابةً للتغيرات في طبيعة النزاعات المسلحة وظهور أسلحة جديدة، انطلق هذا القانون من قواعد عرفية لحماية المدنيين والتخفيف من ويلات الحروب، ثم توسع لاحقًا ليشمل معاهدات واتفاقيات تهدف إلى مواكبة التحولات التي أدخلتها الدول في مجال التسليح[1].

اذ مع تطور الأسلحة والتقنيات، عمل المجتمع الدولي على تعديل القانون الدولي الإنساني لضمان حماية أكبر للمدنيين، فعلى سبيل المثال تم عقد عدة اتفاقيات دولية لحمايتهم منها **اتفاقيات لاهاي (1899 و1907)**، شكلت إحدى المحاولات الأولى لتنظيم استخدام أنواع معينة من الأسلحة في النزاعات، حيث حظرت استخدام القذائف المتفجرة وأقرت قواعد تميز بين الأهداف العسكرية والمدنية.

[1] لورنس اوليفاء، امن تقنية المعلومات، المنظمة العربية للترجمة، ترجمة محمد مراياتي، بيروت، 2011، ص9

اما **اتفاقيات جنيف (1949) والبروتوكولات الإضافية (1977)** فقد جاءت هذه الاتفاقيات لتعزيز حماية المدنيين في النزاعات المسلحة ووضع معايير واضحة لاستخدام الأسلحة التي تسبب أضرارًا عشوائية وغير محددة الأهداف.

مع ظهور أسلحة جديدة أكثر فتكًا، مثل الأسلحة النووية والكيميائية والبيولوجية، تطلب القانون الدولي تعديلات إضافية، فعقب استخدام الأسلحة النووية في الحرب العالمية الثانية[1]، أبرمت معاهدة عدم انتشار الأسلحة النووية (1968)، وتبعتها معاهدات أخرى لتنظيم استخدام الأسلحة الكيميائية والبيولوجية، وذلك للحد من تأثيراتها الكارثية على البشر والبيئة.

في الوقت الحالي، ومع بروز الهجمات السيبرانية كعنصر مؤثر في النزاعات، يواجه القانون الدولي الإنساني تحديات جديدة، فالاختلاف الجوهري للهجمات السيبرانية يكمن في عدم اعتمادها على وسائل مادية ملموسة وتأثيرها الواسع على البنى التحتية الأساسية، مما قد يُعرض المدنيين لأخطار كبيرة، لذا تبرز الحاجة إلى وضع إطار قانوني قادر على تنظيم هذا النوع من الهجمات، وضمان حماية المدنيين من أضرارها المحتملة.

وتكييف القواعد والمعايير القانونية مع التغيرات التكنولوجية المتسارعة، بما يضمن حماية المدنيين وتحقيق التوازن بين استخدام التكنولوجيا الحديثة واحترام مبادئ القانون الدولي الإنساني، اذ تُعتبر الهجمات السيبرانية واحدة من أخطر التحديات التي تواجه القانون الدولي الإنساني في العصر الحديث، حيث يمكن تصنيفها ضمن أطر قانونية مختلفة مثل جرائم تقنية المعلومات، الإرهاب السيبراني، والحروب السيبرانية.

تتمثل هذه الهجمات في أي محاولة للوصول غير المشروع إلى أجهزة الحاسوب أو الشبكات بهدف التلاعب بالبيانات، أو تعطيل الأنظمة، أو السيطرة عليها بطرق غير قانونية، تهدف هذه الهجمات إلى إحداث أضرار واسعة النطاق تتجاوز الحدود الجغرافية، وتشكل تهديداً للأمن القومي والبنية التحتية الحيوية[2].

وفقاً لتعريف وكالة إدارة الطوارئ الفيدرالية (FEMA)، يُعرف الإرهاب السيبراني بأنه هجمات غير مشروعة أو تهديدات تُمارس على الأنظمة والشبكات بهدف إرهاب أو ابتزاز الحكومات لتحقيق أهداف سياسية أو اجتماعية، هذه الهجمات قد تستهدف البنى التحتية الحساسة مثل أنظمة الطاقة، المصارف، والمستشفيات، مما يشكل تهديداً للأمن القومي، وعلى الرغم من تشابه الإرهاب التقليدي والسيبراني في أهدافهما التخريبية[3]، إلا أن وسائلهما تختلف بشكل كبير، حيث يعتمد الإرهاب السيبراني على تقنيات الحوسبة والشبكات بدلاً من الأسلحة التقليدية، تتنوع دوافع هذه الهجمات بين المكاسب المالية والتجسس وسرقة المعلومات الحساسة، مما يزيد من تعقيد التعامل معها قانونياً.

من جهة أخرى، تُعد الحروب السيبرانية بمثابة صراع بين الدول يتم فيه استخدام أدوات تقنية المعلومات لشن هجمات على الأنظمة الحيوية لدولة معادية، بهدف إحداث أضرار مادية أو

[1] عبد الوهاب الطويل، الهجمات السيبرانية، حروب المستقبل، مجلة الاقتصاد الإسلامي، المجلد43، بتك دبي الإسلامي، ص661، ص2022

[2] احمد عبيس الفتلاوي، الهجمات السيبرانية، دراسة قانونية تحليلية بشان تحديات تنظيمها المعاصر، منشورات زين الحقوقية، بيروت، لبنان، 2018، ص16

[3] Zimet .E.and C. L. Barry," Military services Overview, Cyber power and National Security", National Defense University Press Washington, DC, USA,2009,P.291

اقتصادية، يتزايد استخدام الهجمات السيبرانية في النزاعات الدولية الحديثة، حيث تتعرض الأنظمة الحكومية، والبنى التحتية، والمؤسسات المالية للهجمات، مما يثير تحديات جديدة أمام القانون الدولي الإنساني في كيفية التعامل مع هذه الأفعال وتنظيمها[1].

فالهجوم السيبراني يُعتبر هجوماً عابراً للحدود، يتميز بقدرته على التدمير عن بُعد، ما يسمح للمعتدي، سواء كان دولة أو منظمة إرهابية، بتفادي الخسائر المادية أو العسكرية أو البشرية التي تميز الحروب التقليدية أو الإرهاب التقليدي، يتم الهجوم بمجرد اكتشاف ثغرة أمنية في الأنظمة المستهدفة، والتي قد تكون على بعد آلاف الأميال، ويُنفذ خلال ثوان معدودة محققاً أهدافه، يمكن أن يصيب هذا النوع من الهجمات أهدافاً متعددة في وقت قصير أو يركز على هدف واحد بشكل متكرر، مما يمنح المعتدي ميزة هائلة في الوقت والجهد والتكاليف.

تتسم هذه الهجمات بصعوبة اكتشافها وتحديد مصدرها، في كثير من الحالات، تكون الغاية من الهجوم هي الحصول على معلومات أو أسرار حساسة من قطاعات حيوية مثل المؤسسات العسكرية أو الاستراتيجية، وقد يتم الاستيلاء على هذه المعلومات دون أن يُكتشف الهجوم أصلاً، حتى في الحالات التي يتم اكتشاف الهجوم، يكون من الصعب تحديد حجم الأضرار، أو حتى هوية المعتدي، مما يخلق بيئة غامضة تتيح للمهاجم الإفلات من المسؤولية القانونية[2].

إن هذا الغموض يعقد مسائل التحقيق في الهجمات السيبرانية ويطرح تحديات كبيرة أمام القانون الدولي الإنساني، الذي يهدف إلى تنظيم النزاعات وضمان حماية المدنيين والبنى التحتية، فعلى سبيل المثال، الهجمات التي تُنفذ لأغراض سياسية أو عسكرية تُستخدم من قبل الدول والمنظمات الإرهابية على حد سواء، لتحقيق أهداف تهدف إلى إخضاع الدولة المعتدى عليها وإرغامها على القيام بعمل معين أو الامتناع عنه، يتم ذلك عبر استهداف المرافق الحيوية أو الاستراتيجية مثل الأنظمة المالية، شبكات الطاقة، أو المنشآت الحكومية.

ومن المهم الإشارة إلى أن التكنولوجيا المستخدمة في هذه الهجمات أصبحت متاحة على نطاق واسع وبأسعار رخيصة نسبياً، مما يزيد من انتشارها ويعقد من إمكانية السيطرة عليها[3]، هذه الهجمات بدأت تبرز بشكل واضح في ثمانينيات القرن العشرين، وبالتحديد خلال فترة رئاسة الرئيس الأمريكي رونالد ريغان ، اذ كان قلق من احتمال تعرض الولايات المتحدة للهجمات السيبرانية، مما دفع إلى إنشاء وحدة السياسات القومية الخاصة بأمن نظم المعلومات والاتصالات، وهي خطوة اعتُبرت سابقةً لأوانها، تطورت هذه الفكرة خلال تسعينيات القرن الماضي، حيث اعتمد الجيش الأمريكي على تقنيات الاتصالات السيبرانية في عمليات الاستشعار عن بعد[4]، وبرزت الحاجة لهذه التقنيات بشكل أكبر خلال الحرب الأمريكية على العراق في عام 2003.

تأثرت الاستراتيجية الأمريكية للهجمات السيبرانية بالترتيبات الاستراتيجية الجديدة للصناعة العسكرية الإسرائيلية، والتي كانت تركز بشكل أساسي على استهداف المنشآت النووية الإيرانية وتطوير قدراتها السيبرانية الهجومية بشكل سري. وقد شهد مطلع التسعينيات تسارعاً ملحوظاً في اعتماد تقنيات الحوسبة لتحقيق تطورات نوعية في المجالات الأمنية والعسكرية، مما أطلق عليه البعض مصطلح "الحرب السيبرانية الباردة" أو "سباق التسلح السيبراني. اعتمدت دول مثل الولايات المتحدة، روسيا، والصين هذه التكنولوجيا لأغراض دفاعية وهجومية، لكنها متاحة أيضاً للجهات غير الحكومية مثل الجماعات الإرهابية التي تسعى إلى استخدام الهجمات السيبرانية لإثارة

[1] Lan traynor, Russia accused of unleashing cyber war to disable Estonia,guardian London,may ,2007, p17.

[2] عمر محمد أبو بكر بن يؤنس، الجرائم الناشئة عن الانترنيت، دار النهضة العربية، القاهرة ، 2004، ص158

[3] عمار ياسر محمد زهير التحديات الأمنية المعاصرة للهجمات السيبرانية، القيادة العامة لشرطة الشارقة مركز بحوث الشرطة، المجلد ٣٠ ، العدد ٢٠٢١، ١١٨ ، ص ٢٧.

[4] فرد كابلان ترجمة لؤي عبد المجيد المنطقة المعتمة التاريخ السري للحرب السيبرانية، عالم المعرفة المجلس الوطني للثقافة والفنون والاداب ، الكويت، ٢٠١٩ ، ص ٥٢ .

الذعر وإحداث الفوضى[1]، هذا التطور يجعل الحاجة ماسة إلى تعزيز الأطر القانونية الدولية وتنظيم الاستخدام المتزايد للأسلحة السيبرانية[2].

وباتت الهجمات السيبرانية أكثر تعقيداً بفضل تطور التقنيات مثل الذكاء الاصطناعي والتعلم الآلي[3]، والتي تتيح إمكانية تخطيط وتنفيذ هجمات أكثر دقة وفاعلية، هذه التقنيات تستخدم لتحليل الشبكات المستهدفة واستغلال الثغرات بشكل أوتوماتيكي، مما يزيد من صعوبة التصدي لها، كما أن تقنيات "الهجوم بدون أثر" التي لا تترك بصمات رقمية واضحة، تجعل من الصعب على فرق الأمن السيبراني اكتشاف الهجمات أو حتى تحديد كيفية حدوثها.

المحور الثاني : التحديات القانونية للهجمات السيبرانية في ظل القانون الدولي الإنساني

ان الهجمات السيبرانية تمثل تهديداً مباشراً لمبدأ أساسي في القانون الدولي، الا وهو مبدأ احترام سيادة الدولة، والذي يقتضي عدم التدخل في شؤون الدول الأخرى، وهذا ما جاء في الفقرة الرابعة من المادة الثانية في ميثاق الأمم المتحدة. فهذه الهجمات تعرض أمن الدول للخطر من خلال تسريب البيانات والمعلومات السرية الموجودة على المواقع الإلكترونية. ولا يقتصر التأثير على الدول فقط، بل يمتد إلى المدنيين، حيث تسبب الهجمات السيبرانية أضراراً مباشرة لهم عبر تعطيل الخدمات الحيوية التي يعتمدون عليها.

لايزال التكييف القانوني للهجمات السيبرانية موضع خلاف واسع بين المختصين في القانون الدولي، مما يشكل تحديًا رئيسيًا أمام المشرعين والمختصين القانونيين، فمن جهة، تتفاوت الآراء حول ما إذا كانت هذه الهجمات تدخل ضمن مبادئ القانون الدولي الإنساني، أم أن هناك فراغًا قانونيًا يتطلب استحداث قواعد جديدة للتعامل مع هذا النوع من الحروب.

ونظرًا لعدم وجود تنظيم واضح يضبط الهجمات السيبرانية، يطرح تساؤل حول القواعد القانونية التي يجب تطبيقها، فالهجمات السيبرانية تتزايد بشكل ملحوظ وتهدد السلم والأمن الدوليين، ما يستوجب قواعد قانونية تحكمها، بعض المختصين يرون أن مبادئ القانون الدولي الإنساني كافية للتعامل معها، حيث يمكن تطبيق مبادئ مثل التناسب والضرورة، في المقابل، يرى آخرون أن القانون الدولي الإنساني لم يُصمم للتعامل مع الهجمات السيبرانية، إذ يعود تقنين قواعد الحرب إلى فترات كانت وسائل وطرق القتال الإلكترونية غير موجودة[4].

وبسبب غياب الهجمات السيبرانية عند صياغة اتفاقيات لاهاي (1899-1907) واتفاقيات جنيف لعام 1949 والبروتوكولات الإضافية لعام 1977، يرى بعض المختصين ضرورة إعادة

[1] Manuel gago-areces, business strategy in the digital age, digital transformation, disruption and cyber security, cyberspace risks and benefits for society and development,published by springer, gewerbestrasse, switzerland,2017,p 80.

[2] Tang Lan, Zhang Xin, Harry D. Raduege, Jr., Dmitry I. Grigoriev,Pavan Duggal, and Stein Schjølberg, "Global Cyber Deterrence Views from China, the U.S., Russia, India, and Norway", The EastWest
Institute, Printed in the United States, 2010, p1.

[3] سحر قدوري الرفاعي الحكومة الالكترونية وسبل تطبيقها ,مدخل استراتيجي، مجلة اقتصاديات شمال افريقيا، العدد السابع، جامعة حسيبة بو على ٢٠١٦ ، ص ٣٠٨.

[4] طلال ياسين العيسي، المسوولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي، مجلة الزرقاء للبحوث والدراسات الإنسانية، المجلد١٩، العدد ١،٢٠١٩،ص٨٨

النظر في القانون الدولي الإنساني وتطويره ليشمل تنظيم الهجمات السيبرانية، هؤلاء يرون أن طبيعة هذه الهجمات وأثرها الحركي يتطلبان إطارًا قانونيًا جديدًا يراعي تعقيداتها.

اذ تدور إشكالية تكييف الهجمات السيبرانية حول فرضيتين، الفرضية الأولى: صعوبة إثبات الأثر المادي الهجمات السيبرانية لا تترك بالضرورة أثرًا ماديًا ملموسًا كما في وسائل القتال التقليدية؛ فقد لا يتبقى بعد الهجوم آثار دمار أو جروح جسدية، هذه الطبيعة غير المادية تثير تحديات في إثبات الضرر، وهو ما يجعل التكييف القانوني معقدًا.

اما الفرضية الثانية: فتتعلق بإثبات الأثر المادي للهجمات السيبرانية ، يمكن أن تؤدي الهجمات السيبرانية إلى آثار ملموسة تؤثر في مجالات حيوية كالاقتصاد والأمن والبنية التحتية العسكرية، ما يؤكد ضرورة التعامل معها كنوع من وسائل القتال، وقد أشار القرار رقم (55/36) لعام 2000 الصادر عن الجمعية العامة للأمم المتحدة بعنوان "مكافحة إساءة استخدام تكنولوجيا المعلومات" إلى الأثر المدمر المحتمل لهذه الهجمات على الحياة البشرية، لكنه لم يوفر اتفاقية واضحة لتنظيمها أو الحد من خطورتها.

وان التأخر في تنظيم هذه الهجمات على المستوى الدولي يعزي إلى عدة أسباب، منها التكتم من قبل بعض الدول الرائدة في هذا المجال، إذ تعتبره جزءًا من أمنها القومي، ويشابه هذا الوضع ما حدث مع الأسلحة النووية حيث امتنعت الدول الكبرى عن فرض تنظيمات صارمة عليها، وتم استبدالها باتفاقيات مثل معاهدة عدم انتشار الأسلحة النووية لعام 1968 ومعاهدة الحظر الشامل للتجارب النووية لعام 1996.

وعليه فأن غياب التكييف القانوني الشامل للهجمات السيبرانية يعود بشكل أساسي إلى مصالح الدول الكبرى التي تتصدر هذا المجال، إضافة إلى طبيعة الهجمات السيبرانية التي تعتمد على برامج إلكترونية عدائية يمكن أن تتحول إلى آثار مادية ملموسة، إن تطوير إطار قانوني دولي للهجمات السيبرانية أصبح ضرورة لضمان تحقيق الأمن والسلم الدوليين وتنظيم هذا المجال الحساس.

الا انها من وجهه نظرا من المفترض ان تخضع هذه الهجمات السيبرانية أثناء النزاعات المسلحة لمبادئ القانون الدولي الإنساني، وفقاً للمادة 35 من البروتوكول الإضافي الأول لعام 1977،[1] التي تقيّد أساليب ووسائل القتال. كما أكدت محكمة العدل الدولية أن هذه المبادئ تنطبق على جميع أنواع الحروب والأسلحة، بما في ذلك الهجمات السيبرانية، رغم التحديات التي تطرحها بشأن مدى توافقها مع قواعد القانون الدولي الإنساني.

اذ تمثل الهجمات السيبرانية تحدياً كبيراً لمبادئ القانون الدولي الإنساني، خصوصاً مبدأي التناسب والضرورة العسكرية. يهدف مبدأ التناسب إلى تحقيق توازن بين الأضرار المحتملة على المدنيين والمكاسب العسكرية المتوقعة، بحيث لا تتجاوز الأضرار تلك المكاسب، وقد اكدت عده اتفاقيات على هذا المبداء منها نص المادة ٥١ الفقره الخامسة في البروتوكول الإضافي الأول لعام ١٩٧٧.[2]إلا أن الهجمات السيبرانية قد تتسبب أحياناً بأضرار جسيمة على الأعيان المدنية، مثل محطات الكهرباء أو المستشفيات، ما قد يشكل خرقاً لهذا المبدأ[3].

[1] اذ نصت الفقرة ١ من المادة ٣٥ من البروتوكول الإضافي الأول عام ١٩٧٧ علي"إن حق أطراف أي نزاع في اختيار أساليب ووسائل القتال ليس حقا لا تقيده قيود"

[2] اذ جاء في المادة ٥١/فقره٥/ب " الهجوم الذي يتوقع منه إحداث خسائر عرضية في أرواح المدنيين، إصابةالمدنيين، الإضرار بالأعيان المدنية أو مزيجا منها الذي سيكون مفرطا فيما يتعلقبالميزة العسكرية المباشرة والملموسة المرتقبة"

[3] طلال ياسين، مصدر سابق، ص٦٧

أما مبدأ الضرورة فينص على ضرورة استخدام القوة العسكرية فقط لتحقيق أهداف مشروعة وأساسية لإضعاف العدو.[1] لكن في سياق الهجمات السيبرانية، قد تُستهدف البنية التحتية المدنية بدون وجود مبرر عسكري واضح، ما يتعارض مع هذا المبدأ ويؤدي إلى حرمان المدنيين من خدمات حيوية.

فضلا عن ذلك يوجد مبدأ التفرقة بين المقاتلين وغير المقاتلين في القانون الدولي الإنساني اذ يلزم الأطراف المتحاربة بالتمييز بين المقاتلين والمدنيين، واستهداف العمليات العسكرية فقط نحو الأهداف العسكرية. نصت المادة ٤٨ من البرتوكول الأول الإضافي لعام ١٩٧٧ ، على هذا المبدأ: " تعمل أطراف النزاع على التمييز بين السكان المدنيين والمقاتلين وبين الأعيان المدنية والأهداف العسكرية ومن ثم توجه أعمالها ضد الأهداف العسكرية دون غيرهايحظر هذا المبدأ استهداف المدنيين أو الأعيان المدنية، أو استخدامهم كدروع بشرية. ويعد انتهاك مبدأ التفرقة جريمة حرب، ويهدف هذا المبدأ إلى حماية المدنيين من آثار النزاعات المسلحة[2].

وعليه فالهجمات السيبرانية تشكل تحدياً لمبدأ التفرقة بين المقاتلين والمدنيين، نظراً لصعوبة تحديد هوية المنفذين الذين غالباً ما يكونون بعيدين جغرافياً عن موقع الهجوم، مما يزيد من احتمال الإضرار بالأعيان المدنية.

المحور الثالث : المسؤولية الدولية تجاه الهجمات السيبرانية

تكتسب المسؤولية الدولية الناشئة عن الهجمات السيبرانية أهمية متزايدة في ظل تزايد هذه الهجمات وتطور التقنيات المستخدمة فيها، ففي السنوات الأخيرة، تصاعدت النقاشات حول كيفية تحديد المسؤولية على الدول أو الجهات الفاعلة غير الحكومية المتورطة في شن هجمات سيبرانية، ونظراً لتعقيد إثبات مسؤولية الدولة عن هذه الهجمات، تتطلب هذه القضية نظرة معمقة في القوانين الدولية العرفية والاتفاقية، وتحديد دور المحكمة الدولية وآراء كبار الفقهاء في القانون الدولي[3].

تشير المادة (1) من مشروع المسؤولية الدولية لعام 2001 إلى أن أي فعل غير مشروع تقوم به دولة ما يرتب مسؤوليتها الدولية، حتى لو لم يُسبب ضرراً مباشراً، غير أن هذا المفهوم قد يكون صعب التطبيق في حالات الهجمات السيبرانية بسبب تحديات تحديد هوية المهاجم، في النزاعات المسلحة، قد تكون الهجمات السيبرانية التي تستهدف البنية التحتية العسكرية أو المدنية مشمولة بالقانون الدولي الإنساني، الذي يفرض على الأطراف المتنازعة التمييز بين المدنيين والعسكريين، والتقيد بمبدأ الضرورة العسكرية ومبدأ التناسب، يتبين من هذا النص لم يشترط وقوع ضرر لتحريك المسؤولية الدولية، وهو ما يتناقض مع الفقه الدولي الذي اعتاد أن يشترط وجود ضرر لتحقيق هذه المسؤولية.[4]

[1] زحل محمد الأمين دور القانون الدولي الإنساني في تعزيز حماية حقوق الإنسان، دار النهضة ، ٢٠١٨ ، ص ١٩٣

[2] أبو الخير احمد عطية، حماية السكان المدنيين والأعيان المدنية إبان النزاعات المسلحة، دار النهضة العربية ١٩٩٨، ص ٥٦ ، ٥٧

[3] اماثر طالب جواد، المسؤولية الدولية عن الهجمات السيبرانية في القانون الدولي الإنساني، مجلة رسالة الحقوق، 2022، ص351

[4] زهراء عماد محمد كلنتر، المسولية الدولية الناشئة عن الهجمات السيبرانية، رسالة ماجستير ، كلية القانون، جامعة الكوفة، 2016، ص30

يعرّف الفقيه محمد حافظ غانم المسؤولية الدولية بأنها تلك التي تترتب على الدولة أو أي من أشخاص القانون الدولي نتيجة ارتكابهم أفعالاً تستوجب المؤاخذة وفقاً للمبادئ القانونية الدولية.

ولإثبات مسؤولية دولة عن تصرفات مجموعة مدعومة منها، تبنى القانون الدولي معيار "السيطرة الكاملة" أو "السيطرة الفعالة"، كما في قضايا نيكاراغوا وتادتش[1]، إذ يجب أن تُثبت الدولة المتضررة أن الهجوم تم بدعم أو توجيه مباشر من الدولة المدعى عليها، وهو ما يُعتبر عائقاً كبيراً أمام إثبات المسؤولية في الهجمات السيبرانية التي غالباً ما تكون معقدة الإسناد.

اذ تركز معظم الاتفاقيات والقواعد العرفية الدولية على تحديد المسؤولية التي تقع على عاتق الدول عند ارتكاب أفعال من قبل مؤسسات الدولة أو الأفراد المرتبطين بها، المادة (3) من اتفاقية لاهاي لعام 1907، على سبيل المثال، تشير إلى التزام الدولة بالتعويض عن الأفعال التي يقوم بها أفراد قواتها المسلحة.

في سياق الهجمات السيبرانية، إذا استهدف الهجوم تعطيل وسائل الاتصال العسكرية أو المدنية خلال النزاع المسلح، فإنه يندرج تحت أحكام القانون الدولي الإنساني، هناك مبادئ دولية رئيسية تتعلق بالتمييز بين المدنيين والمقاتلين، والضرر المفرط، والضرورة العسكرية[2].

عندما تُستخدم الهجمات السيبرانية في حالة السلم، مثل التجسس أو الدعم لمجموعات مسلحة غير حكومية، تقوم المسؤولية الدولية على أساس خرق مبدأ عدم التدخل في الشؤون الداخلية للدول. تُعزز مسؤولية الدولة بموجب المادة (4) من مسودة لجنة القانون الدولي حول المسؤولية عن الأفعال غير المشروعة.

كالهجوم السيبراني على شبكة الكهرباء الأوكرانية (2015)،يعد هذا الهجوم أحد الأمثلة البارزة للهجمات السيبرانية التي استهدفت البنية التحتية الحيوية، في هذا الهجوم، تعرضت شبكة الكهرباء الأوكرانية لهجمة سيبرانية شلت قدرتها على توفير الطاقة لمئات الآلاف من الأفراد، مما تسبب في انقطاع واسع للكهرباء، وقد أثار هذا الهجوم تساؤلات حول مدى قدرة القانون الدولي الإنساني على توفير الحماية اللازمة للبنى التحتية المدنية وضرورة إدخال تعديلات على القواعد القائمة لتشمل الحروب السيبرانية.

شهدت عدة دول أوروبية هجمات سيبرانية استهدفت المؤسسات الصحية والمالية، وأدت إلى تعطيل خدمات أساسية للأفراد والمجتمع، أحد أبرز الأمثلة كان الهجوم السيبراني على النظام الصحي في بريطانيا (NHS) في عام 2017، مما أسفر عن توقف عمليات عديدة في المستشفيات وتعرض حياة المرضى للخطر، هذا النوع من الهجمات يوضح التأثيرات غير المباشرة للهجمات السيبرانية، حيث يكون الضرر الواقع على المدنيين مرتفعًا رغم عدم استهدافهم مباشرة.

فضلا عن ذلك، يجب على المحاكم الدولية أن تدرس مفهوم السيطرة لتحديد مسؤولية الدول عن الأفعال المرتكبة من قبل مجموعات غير حكومية، مثال بارز على ذلك هو قضية

قضية تاديتش وهي احدى القضايا المحورية حول المسؤولية الفردية بموجب القانون الإنساني الدولي ومعايير الانتهاكات، ملفات القضية والوثائق القانونية حول الحكم موجودة ضمن أرشيف المحكمة الجنائية الدولية ليوغوسلافيا السابقة ، والتي أصبحت الآن ضمن قسم خاص في موقع الآلية الدولية لتصريف الأعمال المتبقية للمحكمتين الجنائيتين https://www.icj-cij.org/home

[2] أزهر عبد عبد الامير الفتلاوى ، العمليات العدائية طبقا لقواعد القانون الدولي الانساني ، مركز الدراسات العربية للنشر والتوزيع ، ٢٠١٨.

نيكاراغوا ضد الولايات المتحدة، حيث وجدت محكمة العدل الدولية أن معيار المسؤولية الدولية يتطلب قدرة الدولة على السيطرة على القوات شبه العسكرية.

اذ تفتقر هذه الهجمات إلى الأدلة المادية التقليدية، مما يصعب مهمة المحاكم الجنائية الدولية في تحديد المسؤولين عن الهجمات وتطبيق العقوبات، وقد أشارت محكمة العدل الدولية في قضية البوسنة عام 2007 إلى أهمية إثبات "السيطرة الفعالة" للدولة على الأفراد أو المجموعات المرتبطة بها لفرض المسؤولية، ما يشير إلى صعوبة تطبيق المعايير التقليدية في سياق الهجمات السيبرانية.

فتظل التحديات المتعلقة بالتحقيق في الهجمات السيبرانية قائمة، خاصة مع صعوبة تحديد هوية المهاجمين في الفضاء الإلكتروني، كما أن عدم وجود آليات قانونية واضحة لملاحقة المسؤولين عن هذه الجرائم يعقد الأمور، فيشير الفقهاء إلى أن عدم وجود محاكم دولية مختصة بملاحقة هذه الجرائم قد يترك العديد من الجناة بدون عقاب.

ظهرت دعوات لعقد اتفاقية دولية تجرم تقديم الدعم للهجمات السيبرانية وتحدد المسؤولية على الدول التي تتبنى أو تدعم الهجمات السيبرانية، مع التركيز على استحداث معايير جديدة تتناسب مع طبيعة الهجمات السيبرانية والتي تتجاوز حدود الدول وتختلف عن الأسلحة التقليدية في قدرتها على التخفي.

فتشير المناقشات الحالية إلى أهمية إنشاء اتفاقيات دولية تنظم استخدام الهجمات السيبرانية، حيث يمكن أن توفر هذه الاتفاقيات أساساً قانونياً لملاحقة المتورطين وتحديد المسؤولية، يتطلب ذلك التعاون بين الدول لتطوير أطر قانونية فعالة.

فضلا عن ذلك تتطلب المسؤولية الدولية الناشئة عن الهجمات السيبرانية تحليلًا دقيقًا وفهمًا عميقًا للقانون الدولي، إن تحديد مدى المسؤولية يتوقف على العديد من العوامل، بما في ذلك معايير السيطرة، والأحكام المعمول بها في القانون الدولي الإنساني، والقدرة على إثبات الأفعال في الفضاء السيبراني، إن جهود المجتمع الدولي نحو إنشاء أطر قانونية مناسبة ستكون حاسمة في تعزيز السلم والأمن الدوليين.

الخاتمة:

للقانون الدولي الإنساني دورًا حيويًا في حماية المدنيين والبنية التحتية في النزاعات، إلا أن التقدم التكنولوجي والهجمات السيبرانية يشكلان تحديات جديدة تهدد هذه الحماية، إن العمل على تطوير الأطر القانونية وتكييفها مع هذه التحديات يعد أمرًا حاسمًا لضمان فعالية القانون في العصر الرقمي.

الاستنتاجات:

1. أدت الهجمات السيبرانية إلى ظهور نوع جديد من النزاعات المسلحة، لا يعتمد على الأسلحة التقليدية بل على التكنولوجيا، مما زاد من تعقيد النزاعات وأظهر محدودية قواعد القانون الدولي الإنساني الحالية في التصدي لهذا النوع من التهديدات.
2. غياب الأدلة القاطعة وصعوبة تتبع مصدر الهجمات السيبرانية يجعل من الصعب تحديد المسؤولية عن هذه الهجمات، وهو ما يقوّض مبدأ المحاسبة في القانون الدولي الإنساني.
3. اظهرت الهجمات السيبرانية أن مبادئ القانون الدولي الإنساني التقليدية، مثل التفرقة بين المدنيين والمقاتلين، بحاجة إلى مراجعة وتكييف كي تكون قادرة على مواكبة التهديدات السيبرانية وضمان حماية المدنيين بشكل فعّال.

التوصيات:

1- تعزيز التعاون الدولي لإعداد إطار قانوني جديد يتعامل مع تحديات الهجمات السيبرانية ويتوافق مع مبادئ القانون الدولي الإنساني.
2- العمل على تطوير قواعد جديدة لتحديد المسؤولية القانونية للهجمات السيبرانية، خاصة في ظل صعوبة إثبات الأضرار.
3- إطلاق برامج تدريبية دولية لدعم القدرات الوطنية في مجال الأمن السيبراني، بهدف حماية البنية التحتية الحيوية من الهجمات.
4- دعم الجهود الدولية لتطوير معاهدات واتفاقيات خاصة بالحروب السيبرانية، مع ضمان احترام القوانين الإنسانية.

المصادر:

- **المصادر العربية:**

1. أحمد عبيس الفتلاوي، *الهجمات السيبرانية: دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر*، منشورات زين الحقوقية، بيروت، لبنان، 2018.
2. أزهر عبد عبد الأمير الفتلاوي، *العمليات العدائية طبقاً لقواعد القانون الدولي الإنساني*، مركز الدراسات العربية للنشر والتوزيع، 2018.
3. أبو الخير أحمد عطية، *حماية السكان المدنيين والأعيان المدنية إبان النزاعات المسلحة*، دار النهضة العربية، 1998.
4. أماثر طالب جواد، *المسؤولية الدولية عن الهجمات السيبرانية في القانون الدولي الإنساني*، مجلة رسالة الحقوق، 2022.
5. عبد الوهاب الطويل، *الهجمات السيبرانية: حروب المستقبل*، مجلة الاقتصاد الإسلامي، المجلد 43، بيتك دبي الإسلامي، 2022.
6. عمر محمد أبو بكر بن يونس، *الجرائم الناشئة عن الإنترنت*، دار النهضة العربية، القاهرة، 2004.
7. فرد كابلان، ترجمة لؤي عبد المجيد، *المنطقة المعتمة: التاريخ السري للحرب السيبرانية*، عالم المعرفة، المجلس الوطني للثقافة والفنون والآداب، الكويت، 2019.
8. قدوري الرفاعي، سحر، *الحكومة الإلكترونية وسبل تطبيقها: مدخل استراتيجي*، مجلة اقتصاديات شمال أفريقيا، العدد السابع، جامعة حسيبة بو علي، 2016.
9. لورنس أوليفاء، ترجمة محمد مراياتي، *أمن تقنية المعلومات*، المنظمة العربية للترجمة، بيروت، 2011.
10. طلال ياسين العيسي، *المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي*، مجلة الزرقاء للبحوث والدراسات الإنسانية، المجلد 19، العدد 1، 2019، ص 88.
11. عمار ياسر محمد زهير، *التحديات الأمنية المعاصرة للهجمات السيبرانية*، القيادة العامة لشرطة الشارقة، مركز بحوث الشرطة، المجلد 30، العدد 2021
12. زهراء عماد محمد كلنتر، *المسؤولية الدولية الناشئة عن الهجمات السيبرانية*، رسالة ماجستير، كلية القانون، جامعة الكوفة، 2016، .
13. زحل محمد الأمين، *دور القانون الدولي الإنساني في تعزيز حماية حقوق الإنسان*، دار النهضة، 2018.

- **المصادر الإنكليزية:**

1. Gago-Areces, Manuel. Business Strategy in the Digital Age, Digital Transformation, Disruption and Cyber Security, Cyberspace Risks and Benefits for Society and Development. Published by Springer, Gewerbestrasse, Switzerland, 2017
2. .Lan, Tang, Zhang Xin, Raduege, Harry D. Jr., Grigoriev, Dmitry I., Duggal, Pavan, and Schjølberg, Stein. "Global Cyber Deterrence Views from China, the U.S., Russia, India, and Norway," The EastWest Institute, Printed in the United States, 2010
3. .Traynor, Lan. "Russia Accused of Unleashing Cyber War to Disable Estonia," The Guardian, London, May 2007
4. Zimet, E., and C. L. Barry. "Military Services Overview, Cyber Power and National Security," National Defense University Press, Washington, DC, USA, 2009.