دور دليل تالين في تطور القانون الدولي الانساني

The role of the Tallinn Manual
In the development of international humanitarian law

م. سؤدد طه جدوع

كلية القانون–جامعة القادسية

soudad.taha@qu.edu.iq

تاريخ استلام البحث: ٢٠٢٣/٧/٥

تاريخ قبول النشر: ٢٠٢٣/١٠/٢٢

مستخلص

يشكل القانون العرفي العماد الاساس للقانون الدولي الانساني، ويتمثل بشكل رئيس بالقواعد التي ساهمت في صياغتها اللجنة الدولية للصليب الأحمر بشكل اتفاقيات دولية، كافحت من اجل الاحاطة بمعظم ظروف وتعقيدات النزاعات المسلحة، لوضع مبادئ إنسانية أكثر، تحد من وحشية الحروب، لكن هذه الوثائق الدولية وضعت منذ وقت طويل (عام ١٨٦٤ اول اتفاقية في القانون الدولي الانساني). وعلى الرغم من وجود اتفاقيات حديثة نسبياً، لكنها لم تجاري التطورات المتسارعة في التكنلوجيا وعلوم الحاسوب، والفضاء السيبراني.

تتأثر النزاعات المسلحة –مثلها مثل باقي نواحي الحياة–بالتطورات التكنلوجية التي تفاجأنا يومياً باختراعات جديدة، وتسعى الدول جاهدة من أجل تطويع هذه التقنيات في طرق ووسائل النزاعات المسلحة، ومن اكثرها استخدام الهجمات السيبرانية.

المشكلة تظهر بالإجابة على السؤال، هل من الممكن تطبيق قواعد القانون الدولي الانساني على الهجمات السيبرانية، مع إنها لم توضع لهكذا عمليات؟، نعم يوجد فيها مبادئ عامة، لكن خصوصية هذه الهجمات وما فيها من تعقيدات وتفاصيل تثير الشكوك في الاجابة على هذا السؤال. بناءً على ما تقدم قامت مجموعة من فقهاء واساتذة القانون، بتكليف من منظمة حلف شمال الأطلسي (NATO)، بوضع دليل يتضمن معالجات واجوبة، عندما يكون انطباق القانون الدولي الانساني على تلك الهجمات محل شك، سمي الدليل بـ (دليل تالين)، يلقي هذا البحث الضوء على دليل تالين، وجدواه في معالجة الهجمات السيبرانية.

الكلمات المفتاحية: القانون الدولي الإنساني، دليل تالين، العمليات العدائية السيبرانية، المسؤولية عن الهجمات السيبرانية، حماية المدنيين.

Abstract:

Ustomary law forms the basis of international humanitarian law, and is mainly represented by the rules formulated by the International Committee of the Red Cross in the form of international agreements. It struggled to cover most of the circumstances and complexities of armed conflicts, to establish more humanitarian principles that limit the brutality of wars, but these international documents were drawn up a long time ago. (1864 the first a convention in international humanitarian law).

Although there are relatively recent agreements, they have not kept pace with the rapid developments in technology, computer science, and cyberspace.

Armed conflicts - like other aspects of life - are affected by technological developments that surprise us daily with new inventions, and countries strive to adapt these technologies in the ways and means of armed conflicts, most of which are the use of cyber attacks.

The problem that arises in answering the question: Is it possible to apply the rules of international humanitarian law to cyberattacks, even though they were not designed for such operations? Yes, there are general principles in them, but the specificity of these attacks and the complexities and details they contain raise doubts in the answer to this question. Based on the above, a group of jurists and law professors, commissioned by the North Atlantic Treaty Organization (NATO), developed a guide that includes solutions and answers, when the application of international humanitarian law to these attacks is in doubt. The guide was called (the Tallinn Guide). This research presents highlighting the Tallinn Manual and its usefulness in addressing cyber-attacks.

Keywords: International humanitarian law, Tallinn Manual, cyber hostilities, liability for cyber-attacks, protection of civilians.

مقدمة

التطوير الحديث للتكنولوجيا يكون لا محالة مرتبط بتغير سلوك الحرب، مثلها مثل باقي جوانب حياة الدول، ومن الواضح أيضًا أن طرق ووسائل النزاعات المسلحة، والمشاركين فيها، يتناسون قواعد القانون الدولي الانساني بشأن استخدام القوة المسلحة، وفي الواقع، تشكل النزاعات الجديدة في بعض الحالات تحديات مستعصية على القانون الحالي، إذ يكون مدى التزام أطراف النزاع بتلك القواعد أكثر غموضاً.

وينطبق هذا بشكل خاص فيما يتعلق بالاستخدام العسكري للعمليات السيبرانية، سواء في سياق الدفاع المسلح عن النفس أو في إدارة الأعمال العدائية في وقت النزاع المسلح، حقيقة أن العمليات السيبرانية ظاهرة جديدة نسبيًا في تاريخ القانون الدولي الإنساني، تثير تلقائيًا بعض الأسئلة المهمة حول ما إذا كانت قواعد هذا القانون الحالية تنطبق عليها.

إشكالية البحث:

تتمثل إشكالية البحث في السؤال الذي يُطرح في الاعمال العدائية السيبرانية، ما إذا كان القانون الدولي الانساني يحكمها ام لا؟، وإذا كان الأمر كذلك، فما هي القواعد المحددة التي تنطبق عليها، والظروف التي تنطبق فيها، وإذا لم يكن يحكمها، فماهي القواعد التي تنطبق عليها، وهل تكفي المبادئ العامة في القانون العرفي لتغطيتها، والاحاطة بكل ما يرافقها من ظروف وتعقيدات – وهي جداً كثيرة.

أهمية البحث:

وبهدف توضيح حالة عدم اليقين بشأن القواعد المحددة ذات الصلة بالحرب السيبرانية، تم إعداد دليل تالين بشأن القانون الدولي المطبق على الحرب السيبرانية، من قبل مجموعة من علماء القانون والفقهاء المشهورين على المستوى الدولي. يقدم الدليل– او انه يحاول ان يقدم–تحليل وتفسير عن: كيف ومتى والى أي حد ينطبق القانون الدولي

الانساني على العمليات السيبرانية؟، هذا بحث يسعى الى الإجابة عن تلك الإشكالات، وتقدير قيمة ما قدمه دليل تالين من مساهمة للنهوض بالقانون الدولي الانساني، ولأجل الوقوف على ما إذا قد حقق الدليل هدفه هذا؟، ونجح في تغطية النقص في القانون الدولي الانساني فيما يتعلق بالحرب السيبرانية، كان بحثنا هذا.

منهجية البحث:

ويركز بشكل خاص على كيفية تنظيم القواعد المنصوص عليها في دليل تالين للعمليات السيبرانية بشكل عام، وما هي أبرز التحديات التي تواجه تطبيقه، ولقد انتهجنا فيه سبيل المنهج التحليلي لاهم مبادئ دليل تالين، مع المقارنة – بقدر ما تخدم المقارنة البحث – بين قواعد القانون الدولي الإنساني، ودليل تالين.

خطة البحث:

وسنتناول في هذا البحث دور دليل تالين في تطوير القانون الدولي الانساني، في مبحثين، الاول سنتناول فيه التعريف بدليل تالين، والعمليات العدائية السيبرانية، وسيكون في مطلبين يتناول كل منهما أحد هذين الموضوعين على التوالي، فيما سنناقش في المبحث الثاني معالجات دليل تالين للهجمات السيبرانية، وذلك في مطلبين ايضا، سنبحث في الاول المبادئ العامة لدليل تالين، وفي المطلب الثاني، وفي المطلب الثاني تحديات تطبيق دليل تالين.

المبحث الاول

التعريف بدليل تالين والعمليات السيبرانية

تم إبرام وثيقة قانونية عام ٢٠١٣، وهي دليل تالين الذي أعده مجموعة من خبراء القانون الدولي بدعوة من حلف الشمال الأطلسي (NATO)، قصد المدونة ابراز مدى إمكانية، اخضاع الهجمات السيبرانية لقواعد القانون الدولي الإنساني، وللوقوف على هذا الموضوع بتفصيل واف، سنتناول موضوع المبحث في مطلبين، التعريف بدليل تالين في المطلب الأول، والعمليات العسكرية السيبرانية في المطلب الثاني.

المطلب الأول

التعريف بدليل تالين

بدأت الأسئلة المحيطة باستخدام العمليات السيبرانية وآثارها القانونية في الظهور في وقت متأخر، تحديداً نهاية عقد التسعين، في القرن المنصرم، عندما عقد في كلية حرب البحرية الامريكية، عام ١٩٩٩ مؤتمر قانوني، قدم فيه الخبراء القانونيون أوراقًا بحثية حول الجوانب المختلفة للعمليات السيبرانية، وفي وقت لاحق تم تجميعه في مجلد محرر، والذي أصبح منذ ذلك الحين مرجعًا مهمًا في الأبحاث المتعلقة بالعمليات السيبرانية[١].

يتكون الدليل من ٩٥ مادة، ساعياً فيها الى محاولة، تنحية المدنيين والاهداف المدنية، من أي عمل عسكري، ذا طبيعة سيبرانية، قام بصياغة الدليل مجموعة من خبراء القانون والخبراء العسكريين الدوليين، وساهمت فيه اللجنة الدولية للصليب الأحمر بصفتها مراقب. ويوضح السيد" لوران جيزيل" المستشار القانوني باللجنة الدولية للصليب الأحمر، أهمية الدليل كخطوة نحو التأكيد على الصلة بين القانون الدولي الإنساني أثناء النزاعات المسلحة بكافة أشكالها والهدف المنشود وهو الحد من المعاناة البشرية[٢].

يقدم" دليل تالين" رؤية مثيرة للاهتمام، فهو لم يغادر التقسيم الثنائي التقليدي للنزاعات المسلحة الدولية والنزاعات المسلحة غير الدولية، ويقر بأن العمليات الإلكترونية وحدها قد تشكل نزاعات مسلحة

– تبعاً للظروف – لا سيما الآثار المدمرة لتلك العمليات، وتكمن أهمية العمليات السيبرانية فيما بعد الهجوم، أي آثاره وما يمكن اعتباره " ضرر " في العالم الالكتروني، وبعد مناقشات طويله، اتفق أغلب الخبراء على أنه ليس الضرر المادي وحده، بل حتى توقف أحد الاهداف عن العمل قد يشكل ضرراً أيضاً، فليس من المهم كيفية حدوث ذلك سواء بوسائل حركية أو علمية إلكترونية، وهذه القضية مهمة للغاية في الممارسة العملية حيث أن أي عملية إلكترونية تستهدف تعطيل شبكة مدنية، لن يشملها الحظر الذي يفرضه القانون الدولي الإنساني على الاستهداف المباشر للأشخاص المدنيين والأعيان المدنية[٣].

وبعد سنوات من مؤتمر عام ١٩٩٩، في كلية حرب البحرية الأمريكية، ظهرت الحرب السيبرانية، وبدأ الاهتمام الدولي بالعمليات السيبرانية يتصدر الاهتمام الدولي في عام ٢٠٠٧، بعد الهجوم الضخم على شبكة الكمبيوتر في إستونيا، وخاصة تعطيل أنظمة المعلومات الحكومية والبنية التحتية التجارية للإنترنت، نشأت الهجمات السيبرانية عندما اعترض السكان الروس الساخطون على قرار الحكومة الإستونية بنقل نصب تذكاري (تمثال برونزي لجندي روسي) يقع في وسط تالين العاصمة، إلى مقبرة عسكرية خارج المدينة.

اعترض المواطنين من العرق الروسي في استونيا على نقل التمثال، وعبروا عن غضبهم بهجمات سيبرانية ضد إستونيا وتألفت هذه الهجمات من الحرمان المنظم والمنسق من الخدمات العامة، والهجمات ضد المواقع الحكومية الهامة مثل الموقع الرئاسي والوزاري للدولة وكذلك موقع البرلمان، واستهدفت الهجمات أيضًا المصالح التجارية مثل أنظمة المعلومات المصرفية والصحف[٤].

استمرت الهجمات السيبرانية ضد إستونيا، والتي بدأت في ٢٧ أبريل ٢٠٠٧، على مدى عدة أسابيع وكان لها الأثر العام المتمثل في تعطيل الخدمات الحكومية الأساسية[٥].

ووقعت حوادث سيبرانية أخرى تنطوي على عمليات سيبرانية معادية ضد الدول والكيانات التجارية بعد الهجمات الإستونية، ومن الأمثلة البارزة على ذلك العملية السيبرانية التي شنت ضد جورجيا أثناء نزاعها المسلح مع الاتحاد الروسي في عام ٢٠٠٨. في ٧ أغسطس ٢٠٠٧، وفي عام ٢٠١٠، أدت الهجمات السيبرانية الإسرائيلية، الى إبطال المبردات النووية الإيرانية التي كانت حاسمة لبرنامج التسليح. تسلط هذه الحوادث الضوء على مدى صعوبة التوصيف الدقيق للعملية السيبرانية، وبالتالي تحديد القانون الدولي الواجب التطبيق[٦].

ان الأثر الذي تخلفه العمليات الهجومية السيبرانية، تشكل تهديدًا خطيرًا للأمن القومي للدول ولسلامة الحياة البشرية والمصالح التجارية، وبناءً على ذلك، بدأت الدول تقدر أهمية صياغة مبادئ توجيهية لمعالجة التهديد الجديد المتمثل في الحرب السيبرانية.

أدت الهجمات السيبرانية ضد إستونيا، العضو في حلف شمال الأطلسي، إلى إنشاء مركز التميز للدفاع السيبراني التعاوني التابع لحلف شمال الأطلسي (CCDCOE) في استونيا، لتطوير قدرات الحلف على منع الهجمات السيبرانية واكتشافها والدفاع ضدها والتعافي منها، بما في ذلك وضع حلف الناتو خطط عملية لتحسين وتنسيق قدرات الدفاع السيبراني الوطنية للدول الاعضاء، ووضع كافة هيئات حلف شمال الأطلسي تحت الحماية السيبرانية المركزية، وتحسين

دمج الوعي والإنذار والاستجابة السيبرانية في حلف شمال الأطلسي مع الدول الأعضاء[٧].

أنشأ مركز التميز للدفاع السيبراني التعاوني التابع لحلف شمال الأطلسي(CCDCOE) فريقًا من الخبراء من الدول الأعضاء، وكلفت بصياغة دليل تالين بشأن القانون الدولي المطبق على الحرب السيبرانية[٨].

ويفترض إن استخدام القوة السيبرانية في العلاقات الدولية، سواء في سياق الدفاع عن النفس أو النزاع المسلح، يحكمه القانون الدولي العرفي، يرى بعض الفقهاء بأن القانون الدولي العرفي الحالي ينطبق على العمليات السيبرانية، ويتوافق هذا مع طابع سد الثغرات الذي يتسم به شرط مارتنز، الذي نص على " وفي الحالات التي لا يشملها هذا البروتوكول أو الاتفاقيات الدولية الأخرى، يظل المدنيون والمقاتلون تحت حماية وسلطة مبادئ القانون الدولي المستمدة من العرف الراسخ، ومن مبادئ الإنسانية، ومن ما يمليه الضمير العام" [٩].

من المهم ملاحظة بعض الظروف السيبرانية الفريدة التي ستتطلب التعديل اللازم، فالعمليات العسكرية السيبرانية، جديدة تماماً، لم يكن من الممكن لأحكام القانون الدولي الكلاسيكي أن تفكر فيها، علاوة على معالجتها.

ونرى ان تفرد حلف شمال الأطلسي بوضع دليل لتنظيم الاعمال العدائية السيبرانية، ولو بمشاركة من الصليب الأحمر بصفة مراقب، خصوصاً، أن للحلف مواقف سياسية من دول بعينها مثل روسيا والصين، قد لا يشكل عامل جذب لتطبيق دليل تالين، اذ كان من المفيد عقد اجتماعات مع الأطراف الأخرى المقابلة للمعسكر الغربي.

المطلب الثاني

العمليات العدائية السيبرانية

ظهرت الهجمات السيبرانية حديثاً، واستخدمت وسائل لم تكن مألوفة من قبل، يمكن ان يؤديها مدنيين، وفي أماكن مختلفة من العالم.

إذا أمكننا القول بأن القانون الدولي الحالي ينطبق على العمليات السيبرانية، تطبيقا لشرط مارتنز، فإن هذا القول لا يصح على اطلاقه، إذ تبقى حالات غير مغطاة بواسطة هذا المبدأ أو بواسطة اتفاق دولي آخر، والكلام هنا عن الهجمات السيبرانية، نظراً لما يصاحبها من ظروف وتعقيدات.

بناءً على ما تقدم، ومن أجل المام أكثر بالموضوع، سنتناول في نقطتين كلاً من، مفهوم الهجوم عبر الإنترنت، في النقطة الأولى، ومدى انطباق القانون العرفي التقليدي على الهجمات السيبرانية، في النقطة الثانية.

اولاً: مفهوم الهجوم عبر الإنترنت (الاعمال العدائية السيبرانية): مفهوم " الهجوم المسلح " بموجب المادة ٥١ من ميثاق الأمم المتحدة الميثاق، يتضمن توظيف متعمد للأسلحة أو أي قوى اخرى ضد دولة عبر الحدود الدولية،وهذا يثير دائمًا التساؤل عما إذا كانت وسائل الهجوم السيبرانية تشكل أسلحة، ومع ذلك فقد تمت تسوية هذه المسألة في الرأي الصادر من محكمة العدل الدولية حول استخدام الأسلحة النووية، حيث وأوضحت أن المواد ٤٢ و ٥١ من ميثاق الأمم المتحدة فيما يتعلق بأي استخدام للقوة، بغض النظر عن الأسلحة المستخدمة، يمكن ان ينطبق الرأي المطروح بشأن الأسلحة النووية على الوسائل السيبرانية، التي يمكن أن تشكل سلاحًا بالفعل، بشرط أن يتم استخدامها في الواقع بشكل متعمد، وأن تنتج آثارًا ضارة وغير مشروعة دوليًا على نطاق واسع [١٠].

مـع ذلـك تكتنـف هـذه المقاربـة بـين الأسـلحة النووية والهجمات السيبرانية إشكالات تتعلق بالأسلحة المادية، فيما لا تنطوي الهجمات السيبرانية على أي أسلحة بالمعنى التقليدي، ومتى ستكون هذه الهجمات بمثابة هجوم مسلح يبرر اللجوء إلى تدابير الدفاع المشروعة عن النفس المنصوص عليها في المادة ٥١ من ميثاق الأمم المتحدة.

اما دليل تالين فقد ميز بين استخدام القوة، والتهديد باستخدام القوة، فاستخدام القوة عرفه " تشكل العملية السيبرانية استخداماً للقوة عندما يكون حجمها وآثارها قابلة للمقارنة مع العمليات غير السيبرانية التي تصل لمستوى استخدام القوة "[١١]، اما التهديد باستخدام القوة، فهو " التهديد بالعملية السيبرانية، يشكل تهديداً غير شرعي باستخدام القوة عندما يكون العمل المهدد به في حالة تنفيذه، سوف يعتبر استخداماً غير شرعي للقوة "[١٢].

ونرى ان اعتبار التهديد بالهجوم السيبراني بمثابة التهديد بالقوة، مسعىً محمود أذ لا تقل اهمية البنى الالكترونية للدول عن البنى الاقتصادية المادية، اذ تدير البرامج والنظم الالكترونية منشآت غاية في الخطورة والاهمية كالمفاعلات النووية، وكما منع ميثاق الامم المتحدة في الفقرة الرابعة من المادة الثانية التهديد باستخدام القوة ضد سلامة اراضي اي دولة، كذلك لا يقل عنه خطورة التهديد بعمليات عدائية سيبرانية.

ثانياً: مدى انطباق القانون العرفي التقليدي على الهجمات السيبرانية: تظهر تحديات جدية في اخضاع العمليات السيبرانية العدائية لمبادئ القانون الدولي الانساني، ومن اهم تلك المبادئ:

١. **التمييز:** يختلف مفهوم الهجوم السيبراني بموجب قانون الحرب، عن الهجوم التقليدي بموجب نفس القانون، يؤدي الهجوم التقليدي إلى فرض حظر وقيود على أساس مبدأ التمييز، الذي يتطلب من أطراف النزاع التمييز في جميع الأوقات بين السكان المدنيين والمقاتلين، وبين الأعيان المدنية والأهداف العسكرية، وبالتالي توجيه هجماتهم ضد الجيش فقط، في حالتي الهجوم او الدفاع على السواء١٣.

لكن في الهجمات السيبرانية هناك خلافات مهمة بشأن ما إذا كانت الوفاة أو الإصابة أو الدمار عناصر حاسمة في الآثار المتوقعة للهجوم السيبراني، فمثلاً هل تشكل العملية السيبرانية التي تعطل أو تتداخل أو تتلاعب بطريقة أخرى بوظيفة شيء ما دون التسبب في أي ضرر مادي هجومًا؟، هل تشكل عملا هجومياً يقوم مقام الهجوم المسلح، مثلاً، هل التدمير الدائم لملفات البيانات المصرفية وبالتالي التسبب في حالة من الذعر الشديد بين السكان المدنيين يرقى إلى مستوى " الهجوم السلح "؟، في معرض الإجابة عن الاشكالين المتقدمين – وأشباههما–، يمكن القول ان نص المادة ٤٨ من البروتوكول الإضافي الأول لعام ١٩٧٧ على مبدأ التمييز، وهو أحد المبادئ الأساسية في القانون الدولي الإنساني، وهو يتطلب التمييز في جميع الأوقات بين السكان المدنيين والمقاتلين، والأعيان والأهداف العسكرية والمدنية، وتوجيه العمليات ضد الأهداف العسكرية فقط، يحظر هذا المبدأ الهجوم المباشر ضد المدنيين أو الأهداف المدنية وكذلك الهجمات العشوائية، على الرغم من أن مبدأ التمييز قد تبدو واضحاً ومباشراً، إلا أن العديد من الأسئلة المتعلقة بالتطبيق العملي لا تزال دون حل في السياق الخاص للعمليات السيبرانية، من الأمثلة على ذلك الهجوم على البنية التحتية السيبرانية العسكرية باستخدام فيروسات كمبيوتر ضارة تنتشر لاحقًا إلى الأنظمة المدنية المتصلة، و السؤال هنا عن كون الهجمات السيبرانية قادرة على التمييز أم هي أسلحة عمياء[١٤] .

المشاركة المباشرة في الأعمال العدائية السيبرانية:
مبدأ التمييز يحمي المدنيين فقط طالما أنهم لا يشاركون بشكل مباشر في الأعمال العدائية، وهو ما يستلزم اللجوء إلى وسائل وأساليب قتل العدو أو إصابته، وبالتالي عندما يشارك المدنيون بشكل مباشر في الأعمال العدائية، فإنهم يفقدون الحماية من الهجوم المباشر وتصبح أهدافًا عسكرية مشروعة عرضة للهجوم المباشر، لكن من الجدير بالذكر أن مفهوم " المشاركة المباشرة في الأعمال العدائية " يكون أضيق من فكرة" الهجوم "، خاصة ان فكرة المباشرة تتطلب في المشاركة في الأعمال العدائية أن يستوفي السلوك المعني ثلاثة معايير:

أ. أن يتسبب في الوفاة أو الإصابة أو الدمار، أو أن يؤثر سلبًا على العمليات العسكرية أو القدرة العسكرية للطرف الخصم (حد الضرر).

ب. يجب أن يسبب الضرر المطلوب مباشرة (علاقة السببية المباشرة).

ج. يجب أن تكون مصممة لدعم أحد الطرفين على حساب الطرف الآخر[١٥].

١. تصنيف الصراع السيبراني: أحد الجوانب الأكثر إشكالية للعمليات السيبرانية بموجب قانون الحرب هو تصنيفها، أي توصيف نوع معين من الصراع مثل دولي، داخلي أو خلاف ذلك، الصعوبة تتضاعف مع تطور نزاع مسلح معين، من دولي الى داخلي او بالعكس، او تدخل قوات أخرى غير نظامية في تلك النزاعات المسلحة، فتداخل العمليات السيبرانية يزيدها تعقيداً، على عكس العمليات التقليدية التي تنطوي على أسلحة حركية، فإن العمليات السيبرانية قادرة على إحداث آثار مدمرة واسعة النطاق وطويلة الاثر على مجتمع معين أو اقتصاده، دون التسبب بالضرورة في أي ضرر مادي يرتبط في كثير من الأحيان بالعمل القتالي[١٦].

قد تختلف الجهات الفاعلة المشاركة في العمليات السيبرانية من أفراد لا يعملون تحت سيطرة طرف من أطراف النزاع، أو مجموعات غير منظمة بشكل كافٍ، أو مجموعات منظمة ولكنها موجودة بالكامل خارج إقليم ايٍ من أطراف النزاع المسلح، هذا يثير تحدٍ جديد في محاولة تحديد الانتماءات والمقاصد، مثلاً الوقوف على ما إذا كان هؤلاء الافراد –بغض النظر عن سيطرة الدولة عليهم او إدارة الدولة لنشاطهم–تابعين لدولة او مرتزقة[١٧].

٢. الاسناد: عمومًا قبلت قاعدة في القانون الدولي، أن تتحمل الدول المسؤولية القانونية الدولية عن السلوك غير المشروع الذي يعزى إليها، هذه قاعدة تنطبق بصورة مماثلة في العمليات السيبرانية، لكن عملياً وبسبب عالمية شبكة الانترنت، تبرز مشكلة معرفة هوية المهاجم أو المهاجمين، وبالتالي جعل الإسناد الدقيق عملية من الصعوبة بمكان، وتتفاقم الصعوبة العملية في إسناد الهجوم السيبراني بسبب الخصائص المتأصلة في الفضاء السيبراني، مثل عدم الكشف عن الهوية، والإجراءات متعددة المراحل، والسرعة التي يتم بها تنفيذ العميات السيبرانية[١٨].

من القواعد العامة أن يُنسب السلوك السيبراني الدولي غير المشروع لأجهزة الدولة، عندما تتصرف بصفتها الرسمية ولو كان خارج نطاق تعليماتها، ولكن هذه القاعدة تكون أقل وضوح في قضية قيام افراد، او جماعات بتلك الهجمات السيبرانية، ومن غير الواضح أيضًا ما إذا كانت العمليات السيبرانية التي تقوم بها جهة فاعلة من غير الدول، والتي لا تُنسب إلى دولة ما، يمكن أن توصف –مع ذلك–بأنها هجوم مسلح يبرر رد فعل دفاعي على مستوى استخدام القوة ضد تلك الجهة من غير الدول[١٩].

هل تشكل العملية السيبرانية التي يقوم بها أحد المتسللين الفرديين والتي تتسبب في تعطيل نظام نقل مزدوج الاستخدام أو شبكة كهربائية سببًا لفقدان الحماية، بغض النظر عن حقيقة أنها لا تؤدي إلى الوفاة أو الإصابة أو الدمار؟ وبالمثل، هل تعتبر العملية السيبرانية التي تؤدي فقط إلى تعطيل شبكة اتصالات الخصم بمثابة مشاركة مباشرة؟، والعديد من الأسئلة الأخرى التي لا يقدم القانون الدولي الإنساني أجوبة قاطعه عنها.

المبحث الثاني

معالجات دليل تالين للهجمات السيبرانية

إن العواقب السلبية المحتملة للعمليات السيبرانية التي يمكن أن تعطل وتدمر الجوانب الحيوية للمجتمعات الحديثة، تسلط الضوء على الحاجة الماسة إلى إطار قانوني متماسك يحكم استخدام التكنولوجيا السيبرانية في النزاعات المسلحة، فقواعد القانون الدولي الإنساني، وإن كانت في العديد من قواعده بمبادئ عامة، لمحاولة استيعاب الوقائع المستقبلية، لكن من يستطيع ان يتنبأ بالتطور المستقبلي بدقة، لذا ظهرت تحديات في معالجات القانون الدولي الإنساني، للعمليات العدائية السيبرانية.

يأتي دليل تالين كمحاولة ليملأ الفجوة القانونية، نظراً كون تلك العمليات بقت منطقة لم يتناولها القانون الدولي الإنساني بشكل صريح وواضح، يزيل أي لبس في تطبيق هذا القانون عليها، بناءً عليه سنتناول موضوع هذا المبحث في مطلبين، سنبحث في المطلب الأول المبادئ العامة لدليل تالين، وفي المطلب الثاني تحديات تطبيق دليل تالين.

المطلب الاول

المبادئ العامة لدليل تالين

ركز دليل تالين على الهجمات السيبرانية، وحاول تطويع القواعد العامة في القانون الدولي الانساني، لخدمة هذه الغاية، كون هذا النوع من الهجمات لم تعالج بنصوص قاطعة في القانون العرفي، واهم المبادئ الواردة في دليل تالين المتعلقة بالهجمات السيبرانية هي:

أولا: حضر استخدام القوة: يحظر دليل تالين صراحةً استخدام الفضاء الإلكتروني أو توظيف التكنولوجيا الإلكترونية في التهديد أو استخدام القوة ضد اية دولة، إذ تنص القاعدة ١٠ على أن " العملية السيبرانية التي تشكل تهديدا أو استخداما للقوة ضد السلامة الإقليمية أو الاستقلال السياسي لأي دولة، أو التي تتعارض بأي شكل آخر مع مقاصد الأمم المتحدة، تعتبر غير مشروعة"، تستند هذه القاعدة إلى القانون الدولي التعاهدي والعرفي، تتبنى القاعدة ١٠ نهجًا موسعًا يعترف بحظر التهديدات أو استخدام القوة التي تتعارض مع ميثاق الأمم المتحدة على الدول وكذلك على الجهات الفاعلة من غير الدول، إحدى القضايا المهمة التي تتناولها القاعدة ١٠ هي أن العمليات السيبرانية لا يجب أن ترقى إلى مستوى استخدام القوة، بل يكفي التهديد بها، وبالتالي فإن القاعدة ١٠ تضمن فعليًا أنه حتى في حالة وجود شك، لن يكون هناك مجال كبير لتجنب المسؤولية[٢٠].

ثانياً: المسؤولية عن الهجمات السيبرانية: تقوم مسؤولية الدولة عن العملية السيبرانية المنسوبة اليها، والتي تشكل انتهاكًا لالتزام دولي. تستند هذه القاعدة إلى القانون العرفي، ووفق المعايير الدولية لإسناد المسؤولية الدولية، هو ان هناك ثلاث فئات مختلفة من الجهات الفاعلة التي تشارك عادة في إجراء العمليات السيبرانية، فهناك "أجهزة الدولة" التي تشمل المدنيين والعسكريين وكلاء الدولة، وهناك الميليشيات المدنية التي تتكون من أفراد منظمين إلى

حد ما، لا يتمتعون بوضع عملاء الدولة بموجب القانون الداخلي للدولة المعنية، ولكن يجوز لهم التصرف تحت توجيهات تلك الدولة، واخير هناك المتسللون المواطنون المستقلون الذين يعملون بشكل مستقل أو بالتنسيق مع قراصنة آخرين[٢١].

الدليل يعترف بأن الهجمات السيبرانية يمكن أن ترتكبها أجهزة الدولة، أو أشخاص أو كيانات على الرغم من أنها ليست أجهزة تابعة لتلك الدولة، إلا أنها مخولة على وجه التحديد بموجب قانونها المحلي لممارسة هذه الهجمات حكومي سلطة. يوضح تعليق اللجنة الدولية للصليب الاحمر على القاعدة العرفية السادسة " أن الأفعال ستُنسب مسؤولية هؤلاء الأفراد أو الجماعات إلى الدولة المركزية، إذا تم بالفعل تطبيقاً لتعليمات الدولة "، ومع ذلك، فإن عتبة السيطرة التي يمكن عندها لأفعال الكيانات من غير الدول أن تترتب عليها المسؤولية الدولية للدولة أمر مثير للجدل، هناك خلاف كبير حول ما إذا كانت الدرجة المطلوبة من السيطرة ينبغي أن تكون "السيطرة الشاملة" في جميع حالات أفعال الجهات الفاعلة غير الحكومية أو ما إذا كان ينبغي أن تكون "السيطرة الفعالة" في حالة قراصنة المواطنين والمتطوعين السيبرانيين غير المنظمين[٢٢]

ومعيار السيطرة الشاملة، لا يتطلب سوى دليل على أن الدولة كان لها دور في تسهيل أو تنظيم أو تنسيق أو تخطيط أعمال كيان من غير الدول، "بغض النظر عن أي تعليمات محددة من الدولة المسيطرة فيما يتعلق بارتكاب كل من تلك الأفعال، وعلى عكس معيار السيطرة الفعالة، فإن الرقابة الشاملة لا تركز كثيرًا على السيطرة على الفعل، بل على الفاعل، وكذلك فان معيار السيطرة الشاملة ملائمة أكثر عند إسناد الأفعال الى الجماعات المنظمة، في حين أن معيار السيطرة الفعالة سيكون أكثر ملاءمة في حالة الأفراد والجماعات غير المنظمة[٢٣].

ومن المثير للدهشة أن دليل تالين لا يذكر موقفًا محددًا فيما يتعلق بمعيار الإسناد الذي يعتبر المعيار اللازم لتحديد ما إذا كانت مسؤولية الدولة متحققة ام لا، لكن نص دليل تالين على ما يلي: " إن مجرد حقيقة إطلاق عملية إلكترونية أو أنها نشأت بطريقة أخرى من البنية التحتية الإلكترونية الحكومية لا يعد دليلاً كافيًا لإسناد العملية لتلك الدولة، بل هي إشارة الى ارتباط الدولة المعنية بالعملية "[٢٤].

نرى ان هذه القاعدة تؤيد إمكانية اعتماد معايير الإسناد في الظروف المناسبة، لأنها لا تستبعد أن تكون العمليات السيبرانية التي يتم إطلاقها من البنية التحتية السيبرانية للدولة أساسًا لتوفر المسؤولية الدولية. ومن ثم يمكن أن تعزى العمليات السيبرانية غير القانونية إلى دولة ما إذا كانت هناك أدلة كافية تشير إلى أن الدولة تتسامح مع شن مثل هذه الهجمات من أراضيها.

ثالثاً: الدفاع الشرعي: وتنص القاعدة ١٣ من دليل تالين على ما يلي: " يجوز للدولة التي تكون هدفًا لعملية إلكترونية ترقى إلى مستوى الهجوم المسلح أن تمارس حقها الأصيل في الدفاع عن النفس. وتعتبر العملية السيبرانية هجوماً مسلحاً بالاعتماد على حجمها وآثارها "، تتشابه هذه القاعدة مع المبدأ المنصوص عليه في المادة ٥١ من ميثاق الأمم المتحدة، التي تنص على أنه " ليس في هذا الميثاق ما يضعف الحق الطبيعي في الدفاع الفردي أو الجماعي عن النفس إذا وقع هجوم مسلح ضد أحد أعضاء الأمم المتحدة، إلى أن يتخذ مجلس الأمن الإجراءات اللازمة لصون السلم والأمن الدوليين "،

يعكس هذا الحكم، الحق العرفي في الدفاع عن النفس المقرر في القانون الدولي الانساني، كما في القانون الدولي العام.

رابعاً: جسامة الهجوم السيبراني: كان هناك إجماع بين فريق الخبراء الدولي على أن بعض العمليات السيبرانية، قد تكون خطيرة بما يكفي لتشكل "هجومًا مسلحًا" بالمعنى المقصود في المادة ٥١ من ميثاق الأمم المتحدة، يجد هذا الموقف دعمًا في الرأي الاستشاري *بشأن الأسلحة النووية* حيث ذكرت محكمة العدل الدولية أن اختيار وسائل الهجوم، سواء كانت حركية، أو غير الحركية، لديها لقدرة على تحقيق النتائج المترتبة على مثل ذلك الهجوم المسلح "[٢٥].

في حين أن فكرة وجود عملية سيبرانية لديها القدرة على تشكيل هجوم مسلح تثير بالتالي الحق في الدفاع عن النفس، المشكلة في العتبة، أيّ متى توصف العملية السيبرانية بأنها بمثابة هجوم مسلح، يصر معظم الفقهاء وخبراء القانون على أنه من أجل تلبية الحد الأدنى المطلوب من الهجوم المسلح، يجب أن يكون الاستخدام المناسب للقوة على نطاق واسع نسبيًا وأن يكون له تأثير كبير. لكن هذا الرأي ليس بلا منازع، فهناك بعض فقهاء القانون، وحتى مواقف دول مثل الولايات المتحدة الامريكية، يرون أن الدفاع عن النفس يحتمل ينطبق ضد أي عمل غير قانوني يستخدم القوة، فليس هناك عتبة لاستخدام المهاجم القوة ليرتقي عمله الى حد هجوم مسلح[٢٦].

خامساً: الضرورة والتناسب: تنص القاعدة ١٤ من دليل تالين على أن " استخدام القوة الذي يشمل العمليات السيبرانية التي تقوم بها دولة ما في ممارسة حقها في الدفاع عن النفس يجب أن يكون ضرورياً ومتناسباً "، هذه القاعدة تضع شرطاً مزدوجاً لتحقيق الدفاع الشرعي عن النفس هو ان يكون ضروري ومتناسب، الضرورة تشير الى استخدام القوة كوسيلة فعالة لدفع الهجوم، ومن النقاط المهمة المتعلقة بالضرورة والتي تم تسليط الضوء عليها في التعليق على القاعدة ١٤، هي أن وجود ضرورة اللجوء إلى وسائل القوة دفاعًا عن النفس ينبغي الحكم عليه من منظور الدولة الضحية، ويجب أن يكون هذا التحديد معقولًا حسب الظروف المصاحبة، أما التناسب فيتعلق بكمية القوة، بما في ذلك القوة السيبرانية، كوسيلة للدفاع عن النفس المسموح بها بمجرد استيفاء شرط الضرورة، والتناسب كشرط في الدفاع الشرعي، هو أن حجم ونطاق ومدة القوة المستخدمة يجب ألا تكون مفرطة بالنسبة للهدف المنشود تحقيقه، أي الصد الفعال لهجوم مسلح أو هزيمة هجوم وشيك[٢٧].

سادساً: الشك في الصفة المدنية: اقر دليل تالين بحماية المدنيين، والنأي بهم عن أي هجمات سيبرانية، وأشار الى فقدان هذه الحماية إذا اشترك المدنيين بالأعمال السيبرانية العدائية[٢٨]، وتنص القاعدة ٣٣ من دليل تالين على ما يلي: " في حالة الشك فيما إذا كان شخص ما مدنيا، يعتبر ذلك الشخص مدنيا "، واضح أن هذه القاعدة تعيد صياغة القاعدة العامة للافتراض للمدني في حالات ل شك أيّ يكون مقنن في شرط ٥٠ من القانون العرفي.

المطلب الثاني

تحديات تطبيق دليل تالين

لا يخلو دليل تالين من إشكالات على المستوى النظري والتطبيق العملي، فأولاً يتعلق الامر بقيمته القانونية، فهو ليس أكثر من مدونة لمجموعة من خبراء في القانون، نظمنت تحت رعاية منظمة دولية عسكرية (حلف شمال الأطلسي)، والاشكال الآخر،

نفسه ظهر مع القانون الدولي الإنساني، هل سيستوعب الدليل كل التطورات التي سوف تحدث في المستقبل؟، مع تسارع التكنلوجيا وظهور الذكاء الصناعي، واستعماله في انتاج الأسلحة، ومن يعلم بما سيظهر من اختراعات بعد الذكاء الصناعي.

اولاً: اشكالية تطبيق دليل تالين كونه ليس مصدر من مصادر القانون الدولي العام: ان النظام الأساسي محكمة العدل الدولية حدد في المادة ٣٨ منه، مصادر القانون الدولي، وهي المعاهدات الدولية والعرف ومبادئ القانون العامة، هذان المصدران الاخيران غير التقليديان للقانون الدولي –بغض النظر عن بقية المصادر– إذ تعادل الاتفاقيات الدولية، ولكن على عكس القانون التقليدي الذي يستمد قوته القانونية من موافقة الأطراف فيه، فإن القواعد العرفية والمبادئ العامة للقانون تستمد قوتها الملزمة من ممارسة واسعة النطاق، والصكوك غير الملزمة مؤهلة أيضا كمصادر للقانون الدولي. ويمكن أن تشمل هذه الصكوك، من بين أمور أخرى، الإعلانات ومدونات قواعد السلوك والأدلة التي صاغها خبراء مستقلون، وتقارير المنظمات غير الحكومية، وتكمن فائدة هذه الصكوك في أنها تضع قواعد عامة، رغم ان الصكوك غير الملزمة، غير مدرجة في المادة ٣٨ من النظام الأساسي لمحكمة العدل الدولية، فإنها مع ذلك توضح القواعد الراسخة وغالباً ما تتم صياغتها بهدف الاستجابة بفعالية للتطورات المعاصرة. ومن ثم، يمكن اعتبار هذه الصكوك دليلاً على "الممارسة اللاحقة" بموجب المادة ٣/٣١ /ب من معاهدة فيينا بشأن المعاهدة عند تفسير معاهدة ما[٢٩].

ويكتسب هذا الأمر أهمية خاصة في حالة الصكوك المعتمدة بتوافق الآراء والتي اعتمدتها الحكومات.

وتوجد شواهد حية على أهمية الصكوك غير الملزمة، خاصة في النزاعات المسلحة، منها اعتماد القواعد غير الملزمة المنصوص عليها في دليل الحرب البحرية (دليل سان ريمو) عام ١٩٩٤، ومنذ ذلك الحين والعمليات العسكرية، للعديد من الدول تزيد من تعزيز أثرها القانوني، مما يدل على إمكانية وجود صكوك غير ملزمة، لها الاثر في هو تطور الأعراف[٣٠].

ثانياً: استيعاب دليل تالين لتطور وسائل وطرق النزاعات المسلحة: ورغم أن الإطار الحالي قابل للتطبيق من حيث المبدأ، فقد تكون هناك بعض الصعوبات فيما يتعلق بتطبيقه العملي. على سبيل المثال، لوحظ أن " يستخدم من الكمبيوتر والبرامج الالكترونية في الحروب يستلزم إعادة النظر في تعريف ل مصطلح سلاح، هناك نقطة أخرى توضح عدم كفاية الإطار الحالي للدليل وهي الدور الخاص الذي يلعبه الجهات الفاعلة غير الحكومية في عمليات الفضاء السيبراني، والمشكلة عندما تواجه الدولة عمليات سيبرانية من غير الدول، يكون هناك اتجاه من جانب الدول للرد بطرق تتجاوز الادوات القانونية، وهذا يسلط الضوء على الحاجة إلى معايير خاصة بالفضاء الإلكتروني لتقييد سلوك الدولة ضمن حدود قواعد القانون الدولي الراسخة[٣١].

هناك إجماع عام على أن استخدام العمليات السيبرانية في العلاقات الدولية يفترض ان يخضع لقيود دولية واضحة ومحددة، ومع ذلك، لا يوجد سوى القليل من التوجيه حول كيفية ومتى ومدى خضوع هذه العمليات للمعايير الحالية، الموجودة في دليل تالين، إن مسألة الطريقة المناسبة لحل مشكلة التنظيم القانوني غير الكافي للعمليات السيبرانية أمر مثير للجدل.

هناك مدرستان فكريتان تناولتا موضوع تنظيم العمليات السيبرانية العدائية، الاولى تدعو إلى تبني اتفاقية تحكم الحقوق والواجبات والحلول المرتبطة بإدارة العمليات السيبرانية، الثانية هناك من يرفض جدوى هكذا اتفاقية، أو قابليتها للاستمرار، ويجادلون بدلاً من ذلك، الى السماح بتطوير المعايير الخاصة بالفضاء السيبراني، من خلال الممارسة، مما يؤدي في النهاية الى تدوينها، ويحتجون بان إقحام العمليات السيبرانية في ساحات القتال ظاهرة جديدة نسبيًا، وبالتالي لم يتم بعد فهم قدرتها التخريبية والتدميرية بشكل كامل، إذ لا نزال " في البداية فقط "، إضافة الى صعوبات اخرى، تتعلق بالطابع الفريد للعمليات السيبرانية الذي يسمح للدول بتجاوز الحدود والولايات القضائية، وتحديات اثبات ان العلميات الهجومية السيبرانية قد صدرت من الدولة، او افراد او جماعات، خاضعة او غير خاضعة لها، والتمييز بين استعمال العمليات السيبرانية الهجومية في الحرب، او اعتبارها جريمة مدنية، الى غيرها من التعقيدات[٣٢].

وعلى عكس القتال التقليدي، الذي يقوم على العنصر المادي الملموس، تكون العمليات السيبرانية مكونة من عنصر مادي ملموس، يتمثل بالبنية التحتية المادية التي تنتقل من خلالها البيانات سلكيًا أو لاسلكيًا، بما في ذلك الخوادم وأجهزة التوجيه والأقمار الصناعية والكابلات والأسلاك وأجهزة الكمبيوتر، والعنصر غير المادي وهي البرامج والبيانات المستخدمة، وعلى الرغم من سهولة تحديد الدولة المستهدفة من الهجمات السيبرانية، فإن الصعوبة تكمن في التأكد من أصل الهجوم، و إسناده لدولة ما، فتجارب الحوادث السيبرانية الفعلية تشير إلى أن بعض المحاولات في معرفة المصدر، غير دقيقة، في أحسن الأحوال، ومضللة في أسوأ الأحوال، فقد يبدو ان هجوما سيبرانياً، يأتي من مكان ما، يمكن في الحقيقة تنشأ في مكان آخر، وفي حالة الهجوم من جماعات وافراد، هناك صعوبات تقنية في تحديد هوية المهاجمين السيبرانيين في الفضاء السيبراني[٣٣].

ونجد أن دليل تالين لا يتخذ موقفا واضحا فيما يتعلق بالقضايا الخلافية المحيطة الإسناد، لأن دليل تالين لم يكن المقصود منه النص على أي قواعد صارمة وسريعة في هذا الصدد، ولكن فقط لتوضيح مبادئ القانون المقبولة عمومًا، من اجل ترسيخ مبادئ الدليل وقبولها من دول العالم.

ثالثاً: مصدر دليل تالين: يناقش العديد، وبلهجة مشككة في دليل تالين، باعتباره صادر من منظمة عسكرية، وهي حلف شمال الاطلسي، والدول اعضاء هذه المنظمة، هي الدول المتقدمة تكنلوجياً واقتصاديا، وعسكرياً، وبالتالي فإنها إذ وضع الدليل من تلك المنظمة يثير الشكوك الكثيرة حوله، والحقيقة، وإن كان الدليل كتب برعاية حلف شمال الاطلسي، لكنه كُتب من خبراء واساتذة قانون، وعسكريين على مستوى عالٍ من المهنية والحرفية، وكذلك كانت توجد بالجنب لهؤلاء اللجنة الدولية للصليب الاحمر، باعتبارها مراقب في الفريق الذي وضع الدليل، ثم إن الدليل – إذا كتب له التطبيق– فسيطبق على الدول كافة، سواء التي ساهمت بوضعه أم غيرها [٣٤].

الخاتمة

يمثل استخدام الفضاء الإلكتروني كمنصة لشن الحروب تحديات عديدة للقانون الدولي الانساني الحالي، والواقع أن الاستخدام المتزايد للعمليات السيبرانية يجلب معه بعض، الصعوبات لأن ما موجود بالفعل من قواعد لا يمدنا بأحكام محددة، تستجيب

للجوانب الناشئة لهذه الأشكال الجديدة من الحروب. ومما يزيد هذا الوضع تعقيدًا أن التنظيم القانوني لجوانب معينة من استخدام القوة والصراع المسلح، لم يتم تسويته بشكل جيد، حتى في سياق الحروب التقليدية، ومن ثم فإن الغموض الناتج عن ذلك يجعل من الصعب على الأطراف في حادث سيبراني أن يحددوا على وجه اليقين ما هي القواعد المحددة التي ينبغي أن توجه سلوكهم.

وإدراكًا لأن التغيرات التكنولوجية بشكل عام، والاستخدام العدائي للعمليات السيبرانية بشكل خاص تشكل تحديًا كبيرًا للقانون الدولي الحالي، فقد تمت صياغة دليل تالين لتوفير بعض الوضوح في هذا الصدد، وعلى وجه الخصوص، إيجاد أساس لانطباق شروط ومعايير القانون العرفي على العمليات العدائية السيبرانية.

الاستنتاجات:

١) بناءً على تجربة الصكوك الأخرى غير الملزمة في القانون الدولي، فيمكن لدليلي تالين، مثل سابقاته، أن يوفر الأساس لظهور معايير ملزمة، ويمكن ان يكون معدل النجاح عندما تتطور القواعد من خلال ممارسات الدول، يكون أفضل بكثير مما يحدث عندما يتم تدوينها في شكل معاهدات دولية، فيكون أكثر مرونة في الاستجابة لحاجات الدول، وايضاً يكون قابل للتعديل بشكل أسهل من إجراءات تعديل المعاهدات الدولية.

٢) لا شك ان دليل تالين يعد اضافة ضرورية جاءت لتستجيب للحاجة الملحة لتنظيم او –على الاقل– لوضع إطار نظري، ممكن ان يشكل اساس، لأي تنظيم مستقبلي لاستخدام التكنلوجيا في الاغراض العسكرية، في الدفاع الشرعي، وحتى في الهجوم.

٣) اختلفت اراء التدوين لفريقين، ويرى الكتاب القانونيون من رافضي التدوين، أن معايير جديدة قد تتطور بشكل كاف، من خلال تنفيذ العمليات السيبرانية، أي من خلال الممارسة، فيمكن عندئذٍ تحقيق الهدف النهائي المتمثل في التدوين في شكل معاهدة بشكل مجد.

٤) تم تطوير دليل تالين من قبل مجموعة من الخبراء في القانون الدولي والأمن السيبراني والشؤون العسكرية، وهذا يمنحه مستوى عال من السلطة والمصداقية، إضافة الى اتساع الدليل وشموله ليغطي مجموعة واسعة من المواضيع، بما في ذلك استخدام القوة في الفضاء الإلكتروني، وإسناد الهجمات السيبرانية، وحماية البنية التحتية الحيوية، يتم تحديث الدليل باستمرار ليعكس التطورات الجديدة في القانون والتكنولوجيا.

٥) دليل تالين ليس ملزماً قانوناً، وهذا يعني أن الدول ليست ملزمة قانوناً باتباع قواعده، هذا الافتقار إلى سلطة ملزمة يمكن أن يحد من تأثيره، حيث قد تختار الدول تفسير وتطبيق القانون الدولي في الفضاء الإلكتروني بشكل مختلف.

٦) وأيضاً يرى البعض، أن دليل تالين معقد وقد يكون من الصعب فهمه، وهذا قد يجعل من الصعب على الدول تطبيق قواعدها في الممارسة العملية، صدر الدليل من مجموعة من فقهاء القانون والخبراء الغربين، ولم يوجد بينهم كتاب شرقيين، او أفارقة، ويرى البعض ان هذه ميزة حيث كتب من أكاديميين، بما يجعل الدليل أفضل من حيث الصياغة القانونية والوضوح في احكامه، مما يمكن جميع الدول من الانتفاع منه، واستخدامه لحماية فضائها السيبراني.

وعلى الرغم من هذه التحديات، فإن دليل تالين يمثل خطوة مهمة نحو تطوير إطار قانوني أكثر قوة لإدارة العمليات السيبرانية، إنه مورد قيم للحكومات والشركات في الفضاء الالكتروني، وتعتمد فائدته على اختيار الدول، والمجتمع الدولي، كيفية للتعامل مع مبادئه وتطبيقها.

التوصيات:

١) تشجيع المجتمع الدوي على التحرك نحو وضع اتفاقية دولية تعالج موضوع العمليات العدائية السيبرانية في إطار القانون الدولي يشمل كافة الجوانب المتعلقة بهذه العمليات، وباشراك أكبر عدد من دول العالم، لا أن تستأثر جهة معينة في صياغة مواثيق دولية –وأن لم تكن ملزمة–، ربما ستؤثر فيما يطرح في المستقبل في قواعد الحروب والعمليات السيبرانية.

٢) قيام منظمة الامم المتحدة بدورها على الصعيد الدولي في ادخال موضوع العمليات العدائية السيبرانية في صلب اعمال المنظمة على الصعيد الدولي؛ خصوصا في اعمال الجمعية العامة للأمم المتحدة ولجنة القانون الدولي.

٣) اشراك المنظمات الدولية غير الحكومية في هذا المجال خصوصا اللجنة الدولية للصليب الأحمر، في الجهود الدولية لوضع معاهدة لتنظيم الاعمال العدائية السيبرانية، لدورها البارز في النزاعات المسلحة الدولية وبوصفها الراعي الدولي لجهود الاغاثة الدولية اثناء هذه النزاعات.

الهوامش

(1) Jeffrey L. Caton, DISTINGUISHING ACTS OF WAR IN CYBERSPACE: ASSESSMENT CRITERIA, POLICY CONSIDERATIONS, AND RESPONSE IMPLICATIONS, Strategic Studies Institute, US Army War College, 2014, page 63. Available on URL: http://www.jstor.com/stable/resrep11175.

(2) https://www.icrc.org/ar/doc/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm .

(3) Abdulkareem Kadhim Ajeela, Kareema Lateef Abdullah, Dialectical Rules of Engagement in Cyber War, International Journal of Innovation, Creativity and Change, Volume 11, Issue 3, 2020, Page702.

(4) Joman Rabah AlKhateeb, The applicability of the rules of international humanitarian law to cyber-attacks in war, Middle east of scientific publish journal, Volume 1, Issue 5, Fourteenth Edition, 2022, page 378.

(5) Iradhati Zahra, Diajeng Wulan Christianti , The Beginning of the International Humanitarian Law Application to Cyber Attack: The Status of Rule 30 Tallinn Manual, Padjadjaran Journal of International Law, Volume 5, Number 1, January 2021, page 102.

(6) Michael N. Schmitt, Wired warfare - Protecting the civilian population during cyber operations, International Reniew of the red cross, Published by Ambridge press, 2019, page 245.

(7) Pauline Charlotte Janssens and Jan Wouters, Informal international law-making: A way around the deadlock of international humanitarian law?, International Review of the Red Cross, Published by Cambridge University Press on behalf of the ICRC. 2022, P 2116.

(8) Chih-Hsiang Chang, How Does the Tallinn Manual 2.0 Shed Light on the Threat of Cyber Attacks against Taiwan?, Institute of Interdisciplinary Legal Studies, National Taiwan University, European Conference on Cyber Warfare and Security, Published by Academic Conferences International Ltd, 2022, page651.

(٩) د. ناجي محمد أسامة، الجوانب القانونية للحرب السيبرانية–دراسة في إطار القانون الدولي الإنساني، مجلة روح القوانين، كلية الحقوق، جامعة قنا، العدد ١٣٠، الجزء الثاني، ٢٠٢٣، ١٢٧٢.

(١٠) د. احمد عبيس نعمة الفتلاوي، د. أزهر عبد الأمير الفتلاوي، المسؤولية الناشئة عن استخدام وسائل القتال الفتاكة في نشر الأوبئة (الهجمات السيبرانية في مقابل جائحة كورونا انموذجاً) ، مجلة الحقوق، الجامعة المستنصرية، كلية القانون، العدد ٤١، ٢٠٢١، ص٦٢.

(١١) القاعدة ١١ من دليل تالين.

(١٢) القعدة ١٢ من دليل تالين.

(13) (-Monica Kaminska, Fabio Cristiano, Dennis Broeders, Limiting Viral Spread: Automated Cyber Operations and the principles of Distinction and Discrimination in the Grey Zone, 3th International Conference on Cyber Confict: Going Viral Publisher: CCDCOE, 2021, Page 68.

(١٤) فيصل محمد عبد الغفار، الحروب الالكترونية، الطبعة الاولى، الجندارية للنشر والتوزيع، الاردن، ٢٠١٦، ص٣٤.

(١٥) ايلين جورج، تفكيك المشاركة المباشرة في الأعمال العدائية: العناصر التأسيسية، مجلة جامعة نيويورك للقانون الدولي والسياسة، ٢٠١٠، ص ٦٩٧.

(١٦) إم إن شميت، إتش إيه هاريسون–دينيس وتي سي وينجفيلد، "الكمبيوتر والحرب: ساحة المعركة القانونية"، ورقة خلفية لاجتماع الخبراء غير الرسمي رفيع المستوى حول التحديات الحالية للقانون الإنساني الدولي، ٢٠٠٤، ص٣.

(17) Steven Kleemann Cyber Warfare and the "Humanization" of International Humanitarian Law, International Journal of Cyber Warfare and Terrorism, Published by IGI Global 2021, page 87.

(١٨) سهيلة هادي، الحروب الالكترونية في ظل عصر المعلومات، رؤى استراتيجية، مركز الامارات للدراسات والبحوث الاستراتيجية، العدد ١٤، ٢٠١٧، ص١٣٨.

(١٩) د. هديل حربي ذاري، قوة الفضاء السيبراني: ساحة صراع جديدة بين القوى الدولية الإقليمية في القرن الحادي والعشرين، مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين، العدد ٧٢، شباط ٢٠٢٣، س ٣٤٦-٣٤٧.

(٢٠) د. سلوى يرسف الاكيابي، مدى انطباق القانون الدولي الإنساني على الهجمات السيبرانية، مجلة روح القوانين، كلية الحقوق، جامعة قنا، العدد ١٠١، ٢٠٢٣، الجزء الثاني، س١٢٨٤-١٢٨٥.

(21) Muhammad Siraj Khan and others, Approaches Towards Applicability of International Humanitarian Law on Cyber Attacks: A Critical Appraisal, Journal of Positive School Psychology, International Journal of cyber Warfare and Terrorism, Volume 6, 2021, page 890.

(22) Ido Kilovaty, ICRC, NATO and the U.S. – Direct Participation in Hacktivities – Targeting Private Contractors and Civilians in Cyberspace Under International Humanitarian Law, 2016, page 34.

(٢٣) د. كرار عباس متعب، الحرب السيبرانية، دراسة في استراتيجية الهجمات السيبرانية بين الولايات المتحدة الامريكية وإيران، مجلة حمورابي للدراسات، العدد٤٠، السنة العاشرة، ٢٠٢١، ص ٢٠١.

(٢٤) القاعدة رقم ٧ في دليل تالين.

(٢٥) جون باسيت، وآخرونو، الحروب المستقبلية حرب الفضاء الالكتروني: التسليح وأساليب الدفاع الجديدة، الطبعة الأولى، مركز الامارات للدراسات والبحوث الاستراتيجية، 2014، ص 63.

(26) https://www.icrc.org/ar/doc/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm

(27) Monica Kaminska, Fabio Cristiano, Dennis Broeders, Previous source, Page 53.

(٢٨) القواعد ٢٧، ٢٩، ٣٢ من دليل تالين.

(٢٩) تنص الفقرة ب على (أي تعامل لاحق في مجال تطبيق المعاهدة يتضمن اتفاق الأطراف على تفسيرها)

(30) Diajeng Wulan Christianti, The Beginning of the International Humanitarian Law Application to Cyber Attack: The Status of Rule 30 Tallinn Manual 1.0, Padjadjaran Journal of International Law, Volume 5,Number 1, 2021, Page 102-103.

(٣١) د. احمد عبيس نعمة الفتلاوي، د. أزهر عبد الأمير الفتلاوي، المصدر السابق، ص ٣٣.

(32) Azar Abid Salih, Maiwan Bahjat Abdulrazzaq, Cyber security: performance analysis and challenges for cyber attacks detection, Indonesian Journal of Electrical Engineering and Computer Science, volume 31, Number 3, 2021, Page 768.

(33) Ido Kilovaty,؛ Previous source , Page 27.

(34) Alexia Fitz and Richard L. Wilson, Just Warfare: Is a Nuclear Attack an Appropriate Response to a Cyber Attack?, International Conference on Cyber Warfare and Security, 2023, (1) (PDF) Just Warfare: Is a Nuclear Attack an appropriate Response to a Cyber Attack? (researchgate.net)

المصادر باللغة العربية:

أولاً: المعاهدات والوثائق الدولية:

١) ميثاق الأمم المتحدة لسنة ١٩٤٥

٢) اتفاقية فينا لقانون المعاهدات الدولية ١٩٦٩.

٣) دليل تالين لسنة ٢٠١٣

ثانياً: الكتب والبحوث

١) ايلين جورج، تفكيك المشاركة المباشرة في الأعمال العدائية: العناصر التأسيسية، مجلة جامعة نيويورك للقانون الدولي والسياسة، ٢٠١٠،

٢) احمد عبيس نعمة الفتلاوي، د. أزهر عبد الأمير الفتلاوي، المسؤولية الناشئة عن استخدام وسائل القتال الفتاكة في نشر الأوبئة (الهجمات السيبرانية في مقابل جائحة كورونا انموذجاً)، مجلة الحقوق، الجامعة المستنصرية، كلية القانون، العدد ٤١، ٢٠٢١،

٣) إم إن شميت، إتش إيه هاريسون–دينيس وتي سي وينجفيلد، "الكمبيوتر والحرب: ساحة المعركة القانونية"، ورقة خلفية لاجتماع الخبراء غير الرسمي رفيع المستوى حول التحديات الحالية للقانون الإنساني الدولي، ٢٠٠٤،

٤) سلوى يوسف الاكيابي، مدى انطباق القانون الدولي الإنساني على الهجمات السيبرانية، مجلة روح القوانين، كلية الحقوق، جامعة قنا، العدد ١٠١، ٢٠٢٣، الجزء الثاني،

٥) سهيلة هادي، الحروب الالكترونية في ظل عصر المعلومات، رؤى استراتيجية، مركز الامارات للدراسات والبحوث الاستراتيجية، العدد ١٤، ٢٠١٧،

٦) فيصل محمد عبد الغفار، الحروب الالكترونية، الطبعة الاولى، الجندارية للنشر والتوزيع، الاردن، ٢٠١٦،

٧) كرار عباس متعب، الحرب السيبرانية، دراسة في استراتيجية الهجمات السيبرانية بين الولايات المتحدة الامريكية وإيران، مجلة حمورابي للدراسات، العدد٤٠، السنة العاشرة، ٢٠٢١،

٨) ناجي محمد أسامة، الجوانب القانونية للحرب السيبرانية–دراسة في إطار القانون الدولي الإنساني، مجلة روح القوانين، كلية الحقوق، جامعة قنا، العدد ١٣٠، الجزء الثاني، ٢٠٢٣،

٩) هديل حربي ذاري، قوة الفضاء السيبراني: ساحة صراع جديدة بين القوى الدولية الإقليمية في القرن الحادي والعشرين، مجلة قضايا سياسية، كلية العلوم السياسية، جامعة النهرين، العدد ٧٢، شباط ٢٠٢٣،

Reference list:

1) Abdulkareem Kadhim Ajeela, Kareema Lateef Abdullah, Dialectical Rules of Engagement in Cyber War, International Journal of Innovation, Creativity and Change, Volume 11, Issue 3, 2020, Page702.

2) Alexia Fitz and Richard L. Wilson, Just Warfare: Is a Nuclear Attack an Appropriate Response to a Cyber Attack?, International Conference on Cyber Warfare and Security, 2023, (1) (PDF) Just Warfare: Is a Nuclear Attack an appropriate Response to a Cyber Attack? www.reasearchgate.net

3) Azar Abid Salih, Maiwan Bahjat Abdulrazzaq, Cyber security: performance analysis and challenges for cyber-attacks detection, Indonesian Journal of Electrical Engineering and Computer Science, volume 31, Number 3, 2021, Page 768.

4) Chih-Hsiang Chang, How Does the Tallinn Manual 2.0 Shed Light on the Threat of Cyber Attacks against Taiwan? Institute of Interdisciplinary Legal Studies, National Taiwan University, European Conference on Cyber Warfare and Security, Published by Academic Conferences International Ltd, 2022, page651.

5) Diajeng Wulan Christianti, The Beginning of the International Humanitarian Law Application to Cyber Attack: The Status of Rule 30 Tallinn Manual 1.0, Padjadjaran Journal of International Law, Volume 5, Number 1, 2021, Page 102-103.
6) Eileen George, Deconstructing Direct Participation in Hostilities: Foundational Elements, New York University Journal of International Law and Policy, 2010, Page 697.
7) Ido Kilovaty, ICRC, NATO and the U.S. – Direct Participation in Hacktivities – Targeting Private Contractors and Civilians in Cyberspace Under International Humanitarian Law, 2016, Page 34.
8) Iradhati Zahra, Diajeng Wulan Christianti, The Beginning of the International Humanitarian Law Application to Cyber Attack: The Status of Rule 30 Tallinn Manual, Padjadjaran Journal of International Law, Volume 5, Number 1, January 2021, page 102.
9) Jeffrey L. Caton, DISTINGUISHING ACTS OF WAR IN CYBERSPACE: ASSESSMENT CRITERIA, POLICY CONSIDERATIONS, AND RESPONSE IMPLICATIONS, Strategic Studies Institute, US Army War College, 2014, page 63. Available on URL: http://www.jstor.com/stable/resrep11175.
10) John Bassett, et al., Future Wars: Cyber War: Armament and New Defense Methods, first edition, Emirates Center for Strategic Studies and Research, 2014, Page 63.
11) Joman Rabah AlKhateeb, the applicability of the rules of international humanitarian law to cyber-attacks in war, Middle east of scientific publish journal, Volume 1, Issue 5, Fourteenth Edition, 2022, page 378.
12) Michael N. Schmitt, wired warfare - Protecting the civilian population during cyber operations, International Reniew of the red cross, Published by Ambridge press, 2019, page 245.
13) Monica Kaminska, Fabio Cristiano, Dennis Broeders, Limiting Viral Spread: Automated Cyber Operations and the principles of Distinction and Discrimination in the Grey Zone, 3th International Conference on Cyber Confict: Going Viral Publisher: CCDCOE, 2021, Page 68.
14) Muhammad Siraj Khan and others, Approaches Towards Applicability of International Humanitarian Law on Cyber Attacks: A Critical Appraisal, Journal of Positive School Psychology, International Journal of cyber Warfare and Terrorism, Volume 6, 2021, Page 890.
15) Pauline Charlotte Janssens and Jan Wouters, Informal international law-making: A way around the deadlock of international humanitarian law?, International Review of the Red Cross, Published by Cambridge University Press on behalf of the ICRC. 2022, Page 2116.
16) Steven Kleemann Cyber Warfare and the "Humanization" of International Humanitarian Law, International Journal of Cyber Warfare and Terrorism, Published by IGI Global 2021, page 87.

References from the Internet:

1) https://www.icrc.org/ar/doc/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm
2) https://www.icrc.org/ar/doc/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm