تطبيق مبدا التناسب في العمليات السيبرانية دراسة في ضوء مبادئ القانون الدولي الإنساني

Applying the principle of proportionality in cyber operations: A study in light of the principles of international humanitarian law

أ.م.د. أسامة صبري محمد

كلية القانون – جامعة القادسية

Osamah.sabri@qu.edu.iq

تاريخ استلام البحث: ٢٠٢٦/٦/١٥ تاريخ قبول النشر: ٢٠٢٦/٨/٣٠

الملخص:

البحث محاولة لإيجاد فهم اعمق لمفاهيم استجدت في وقتنا الحاضر، فشكلت تحديا للقواعد القانونية السائدة. الاستعانة بالأنظمة الرقمية من قبل القوات العسكرية للدول وتوظيفها في النزاعات المسلحة وما رافق ذلك الاستخدام من تحديات امام قواعد القانون الدولي الإنساني، اثار السؤال الأكبر فيما مدى قابلية تلك القواعد للاستجابة لتلك التحديات. البحث عالج اهم تحديين الا وهما التكييف القانون للعملية السيبرانية من ناحية مدى اعتبرها هجوما يتناسب مع المفهوم العام للهجوم الذي ورد في المادة ٤٩ من البروتكول الإضافي الأول، وكذلك الإشكاليات التي تواجه تطبيق مبدا التناسب في العمليات السيبرانية. حيث ان الحجج التي تساق لتبرير خروج تلك العمليات من دائرة القانون الدولي الإنساني غير مستندة الى أساس سليم، حيث ان القواعد القانونية الدولية الإنسانية متى ما عجزت عن الانطباق على المتغيرات الجديدة يمكن الاستعانة بشرط مارتنز لمعالجة أي قصور في تلك القواعد. فالبحث يحاول إيجاد المقاربات القانونية السليمة في اعتبار ان العملية السيبرانية تشكل هجوما بالاستناد الى محددات قانونية تساق من قبل الفقهاء للوصول الى فهم شامل لاعتبار تلك العمليات من قبيل الهجمات. كما ان البحث حاول إعطاء مبدا التناسب افقا أوسع في العمليات السيبرانية منتقدا من يحاول تقزيم المبدأ وحصره في دائرة العمليات العسكرية التقليدية. كل ذلك وصولا الى نتائج واقتراحات لمواجهة هذين التحديين.

الكلمات المفتاحية: مبدا التناسب، العملية السيبرانية، دليل تالين، البروتكول الإضافي الأول، الأنظمة مزدوجة الاستخدام

Abstract:

The research is an attempt to find a deeper understanding of concepts that have emerged in our current time, forming a challenge to the existing legal rules. The use of digital systems by countries' military forces and their employment in armed conflicts raised questions and challenges for the rules of international humanitarian law, especially regarding the extent to which these rules can respond to such challenges. The research addressed two main challenges: the legal classification of

cyber operations in terms of whether they are considered attacks according to the general concept of an attack, and the issues faced in applying the principle of proportionality in cyber operations as outlined in Article 49 of Additional Protocol I. The arguments used to justify taking these operations out of the scope of international humanitarian law are not well-founded, as international legal rules can rely on the Martens Clause of humanity to address any gaps whenever they fail to apply to new variables. The research tries to find proper legal approaches to consider a cyber operation as an attack based on legal determinants presented by scholars. It also aimed to give the principle of proportionality a broader understanding in cyber operations, criticizing those who try to limit the principle to traditional military operations. All of this leads to conclusions and proposals to address these two challenges.

Keywords: principle of proportionality, cyber operation, Tallinn Manual, Additional Protocol I, dual-use systems.

المقدمة

التعريف بموضوع البحث: التطور المتسارع في تقنيات الاتصالات وتكنولوجيا المعلومات احدثت ثورة في كافة المجالات التي تمس الواقع الاجتماعي والسياسي. ذلك التطور القى بضلاله على إدارة العمليات العسكرية فالجيوش لم تعد تقتصر ادارتها للعمليات الحربية على الوسائل التقليدية في القتال بل أصبحت تسخر التطور السيبراني في خدمة تلك العمليات، فلم تعد ميادين القتال تقتصر على الحروب البرية والجوية والبحرية بل تعدتها الى الفضاء السيبراني باعتباره ميدان جديد في النزاعات المسلحة. حيث ان الدول والكيانات من غير الدول بدأت تلجا لتلك الوسائل لتحقيق الأهداف العسكرية دون الحاجة لتحقيقها باللجوء الى الوسائل التقليدية في النزاعات المسلحة. هذا التحول في اللجوء لتلك الأساليب في القتال دفع الى قراءه جديدة لمفهوم الهجوم المسلح والمبادئ التي تحكمه في القانون الدولي الإنساني، لا سيما ان هذه الهجمات السيبرانية لها القدرة على احداث الاضرار المشابه وفي بعض الأحيان تفوق تلك التي تحدثها الوسائل القتالية التقليدية.

التطورات العملية في الوقت الحاضر كشفت عن عدم اقتصار الهجمات السيبرانية على التجسس الالكتروني بل امتدت بالولوج بالعمل العسكري المباشر، كما ظهر في اول تجسيد لهذا التحول في الهجوم الالكتروني المعروف بـ STUXNET ويعد واحد من اشهر الهجمات السيبرانية ذات الطابع الكلاسيكي الذي تم الاعتماد فيه على برمجيه خبيثة معقده صممت لاستهداف الأنظمة المتحكمة بالأنظمة المشغلة للصناعات وكان الهدف من هذه البرمجية هو استهداف أنظمة التحكم بأجهزة الطرد المركزي الخاصة بالمنشئات النووية الإيرانية. كما اخذت هذه الهجمات تأخذ منحى اخر عندما وجهت لاستهداف شبكات الكهرباء في أوكرانيا. افرزت تلك الهجمات واقعا جديدا في اطار قواعد القانون

الدولي الإنساني بل تحديا لتلك القواعد، حيث ان هذه الهجمات السيبرانية تؤدي الى احداث اضرار تمس المدنيين والاعيان المدنية، سواء بصورة مباشرة او غير مباشرة حيث شكلت تلك الاضرار اثرا جانبيا في النزاعات المسلحة مما اثار إشكالية قانونية في مدى خضوع تلك الاضرار الناشئة من الهجمات السيبرانية لقواعد القانون الدولي الإنساني.

انطلاقا من دور القانون الدولي الإنساني في التخفيف من ويلات النزاعات المسلحة وتقليل اثارها الإنسانية ولتفعيل ذلك الدور حدد القانون الدولي الإنساني مجموعة من المبادئ التي تساهم الى حد كبير في تخفيف بل وتقييد الوسائل القتالية التي يجب مراعاتها من اطراف النزاع عند بدء العمليات العسكرية وتتمثل تلك المبادئ بـ(مبدا التناسب، ومبدأ التمييز، ومبدأ اتخاذ الاحتياطات) حيث اثبت تلك المبادئ فعاليتها في تقييد وسائل القتال التقليدية والتقليل من الخسائر بل ساهمت في توجيه الاعمال العسكرية بما ينسجم مع فلسفة القانون الدولي الإنساني

تشرع القواعد القانونية متأثرة بالبيئة المحيطة بها، حيث ان الدول الأطراف في اتفاقيات جنيف ومن قبلها لائحة لاهاي وضعوا تلك القواعد بما ينسجم مع الوسائل القتالية التقليدية. الا ان التطور التكنلوجي وظهور الهجمات السيبرانية اثار تحديات قانونية، من الطبيعي لم تكن مثاره عند وضع القواعد المشار اليها سابقا في الاتفاقيات الدولية التي شكلت النظام القانوني المقيد للنزاعات المسلحة سواء الدولية وغير الدولية.

اهم التحديات التي واجهت القانون الدولي الإنساني تلك المتعلقة بمفهوم العملية السيبرانية، وفيما اذا تعتبر هجوما وفق مفهوم القانون الدولي الإنساني، باعتبار ان هذا القانون نطاقه الموضوعي يتمثل في وجود نزاع مسلح تظهر ملامحه بالهجوم المسلح، الذي ينطوي على الاعمال العدائية الهجومية والدفاعية، فالطبيعة المعقدة للأنظمة الرقمية، وما تسببه من اضرار دفع باتجاه بلورة رؤى حول مدى قابلية قواعد القانون الدولي الإنساني لتحكم تلك العمليات.

كما ان التعقيد في تطويع العمليات السيبرانية لم يتوقف عند مفهوم العملية السيبرانية، بل تعدى ذلك الى البحث في مدى انسجام مبادئ القانون الدولي الإنساني ومنها مبدا التناسب موضوع الدراسة مع القواعد السارية، وتكمن أهمية هذا المبدأ باعتباره يمثل جوهر القانون الدولي الإنساني في تكريس الحماية للمدنيين والاعيان المدنية. حيث انه يفرض الالتزام بعدم الاضرار بالمدنيين والاعيان المدنية لغرض تحقيق الميزة العسكرية.

سعت الجهود الدولية الى تكييف قواعد القانون الدولي الإنساني لتنسجم مع التطور السيبراني، وتميزت تلك الجهود من خلال قيام مجموعة من الباحثين في اطلاق دليل تالين ١و٢ كما ان اللجنة الدولية وانطلاقا من دورها في تطوير قواعد القانون الدولي الإنساني ساهمت في هذا المجال من خلال العديد من التفسيرات، الا ان هذه الجهود وغيرها افرزت مجموعة من المعايير التي اخذت الطابع التفسيري غير الملزم، حيث لم تتوصل الى الاطار القانوني الذي يعالج الموضوعات المرتبطة بالهجمات السيبرانية في النزاعات المسلحة ومنها تحديد مفهوم الاضرار الجانبية الناشئة من استخدام الفضاء

السيبراني ومدى مشروعيتها أي تحديد معايير المشروعية، ذلك التفاوت قاد الى إيجاد التباين في مواقف الدول مما افرز فراغا قانونيا يستدعي السعي لدراسته وتحليله.

تتزايد الأهمية في السعي لدراسة هذه الإشكالية في الاعتماد الكلي والمستمر للدول في عملياتها العسكرية على الوسائل السيبرانية لتحقيق الأهداف العسكرية كبديل عن استخدام القوة العسكرية التقليدية، الامر الذي يستدعي إعادة تقييم قواعد القانون الدولي الإنساني واليات التطبيق بما يضمن ديمومة الغرض الأساسي للقانون الدولي الإنساني منذ ان وضع هنري دونان لبنته الأولى في تكريس حماية المدنيين والاعيان المدنية من الاثار غير الضرورية الناشئة والتي لا تشكل عامل من عوامل تحقيق الميزة العسكرية في النزاعات المسلحة.

أهمية البحث: تكمن الأهمية في اختيار موضوع البحث من خلال التركيز على العملية السيبرانية وما مدى إمكانية تطويعها في اطار القانون الدولي الإنساني. كما التوسع في دراسة مبدا التناسب وقابليته للتطبيق للتقليل من الاضرار الجانبية في الفضاء السيبراني.

إشكالية البحث: تكمن المشكلة الأساسية في ان قواعد القانون الدولي الإنساني وضعت لغرض إيجاد الاطار القانوني لتقييد العلميات العسكرية التي تجري في الحروب التقليدية، حيث ان واضعي اتفاقيات جنيف والبروتكولان الملحقان، قننوا قواعد تمس الأسلحة التقليدية مما خلق وعيا لدى المؤسسات العسكرية، مكنها من التطبيق السليم لتلك القواعد. الا ان هذه التطورات التقنية فرضت واقعا قانونيا جديد، تتطلب ان تكون هناك محاولات للتصدي لتلك الثغرات القانونية.

فالدراسة تعالج اشكاليتين الأولى ما مدى اعتبار العملية السيبرانية هجوما وفق مقتضيات القانون الدولي الإنساني والاشكالية الأخرى ما مدى إمكانية التطبيق الناجع لمبدا التناسب في العمليات السيبرانية والتي ينشا عنها اضرار تلحق بالمدنيين والاعيان المدنية. بمعنى ان الإشكالية الرئيسية في هذا البحث تتمثل، فيما مدى إمكانية تطبيق قواعد القانون الدولي الإنساني المتعلقة بالنطاق الموضوعي له وبالمبادئ المقيدة للعمليات العسكرية في اطار العمليات السيبرانية ؟

منهج البحث: اعتمدت الدراسة على المنهج التحليلي للنصوص الدولية وكذلك للاجتهاد الدولي، والاحكام القضائية الدولية التي تناولت العمليات السيبرانية، كما تضمنت الدراسة العمليات السيبرانية التي وجهت للدول، وما موقف الفقه والممارسة الدولية منها

هيكلية البحث: قسم البحث الى مبحثين تناول المبحث الأول مفهوم الهجمات السيبرانية في مطلبين خصص الأول لبيان مفهوم العمليات السيبرانية بينما خصص المطلب الثاني لدراسة العمليات السيبرانية التي وجهت للدول.

اما المبحث الثاني فخصص لبيان ماهية مبدا التناسب في مطلبين خصص الأول لتحديد مفهوم مبدا التناسب في القانون الدولي الإنساني بينما خصص المطلب الثاني لبيان مدى إمكانية تطبيقه في اطار العمليات السيبرانية.

المبحث الأول: ماهية العمليات السيبرانية وتطبيقاتها

شكلت ومازالت العمليات السيبرانية في اطار النزاعات المسلحة ابرز التحديات التي تواجه المهتمين بقواعد القانون الدولي الإنساني، حيث أدى لجوء القوات المسلحة للدول للأنظمة الرقمية في القيام بالهجمات لتحقيق الميزة العسكرية، الى إعادة التفكير في قواعد القانون الدولي الإنساني التي وضعت في فترة زمنية لم تشهد هذا التطور المتسارع لهذه التقنيات. مما جعل تلك الهجمات المستندة على أساليب غير تقليدية تشكل هاجس يؤرق القائمين على تطوير قواعد القانون الدولي الإنساني. مما اثار القلق لدى المهتمين بقواعد القانون الدولي الإنساني وفي المقدمة اللجنة الدولي للصليب الأحمر للتصدي لتلك التحديات، من خلال التشجيع على الدراسات التي تعالج الثغرات التي تولدت نتيجة الاعتماد على التقنيات الرقمية في اطار النزاعات المسلحة.

المطلب الأول: مفهوم الهجمات السيبرانية

يتزامن الاهتمام بمفهوم الهجمات السيبرانية مع التوسع في الاعتماد على التكنولوجيا في كافة أوجه النشاط البشري، حتى ان هذا الاستناد امتد ليغزو الميادين العسكرية، فاصبح وسيلة فعالة في تحقيق الأهداف العسكرية في النزاعات المسلحة. على الرغم من إشاعة استخدام الهجمات السيبرانية من قبل القوات المسلحة كوسيلة لتحقيق المزايا العسكرية التي يسعى اليها في الغالب اطراف النزاع الذين وجودا ان اللجوء الى هذه التقنيات من شانه ان يحقق الإصابة الدقيقة لأهداف الخصم كما انه في ذات الوقت يقلل من الخسائر بين صفوف المقاتلين. القانون الدولي الإنساني تصدى لهذه الظاهرة من خلال البحث عن المفاهيم التي تساعد في انطباق قواعده والحيلولة دون خروج هذه العمليات السيبرانية التي تأخذ منحى العنف في النزاعات المسلحة من دائرة تطبيقه، ولتحقيق ذلك لا بد من تحديد مفهوم الهجمات السيبرانية، وهذا ما لم يتحقق عند البحث في قواعد اتفاقيات جنيف والبروتكولين الملحقين بهما، مما فتح الباب على مصراعيه امام الاجتهاد الفقهي وكذلك ممارسات الهيئات الدولية المعنية بالنزاعات المسلحة.

يعتبر Michael N.Schmitt من الفقهاء الأوائل الذين اهتموا بالهجمات السيبرانية حيث انه يناقش مفهوم الهجمات السيبرانية من خلال ما مدى المقاربة مع مصطلح الهجوم الوارد في المادة ٤٩ من البروتكول الإضافي الأول عام ١٩٧٧.[١]

يرى الفقيه Schmitt ان العملية السيبرانية لترتقي الى مستوى الهجوم وبالتالي انطباق القانون الدولي الإنساني يجب ابتدأ قراءة المادة (٤٩) من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف عام ١٩٧٧ والتي عرفت الهجمات بأنها «أعمال العنف الموجهة ضد الخصم، سواء كانت هجومية أم دفاعية.» كما ان التعليق الرسمي للجنة الدولية للصليب الأحمر على المادة (٤٩) يشير بصراحة الى هذا الفهم، إذ يوضح أن مصطلح «العملية» يجب أن يُفهم في سياقها العام، أي أنه يشير إلى ان العمليات العسكرية التي تستخدم فيها العنف. [٢]

ويستمر الفقيه في اجراء المقاربة حيث أشار الى انه بالاستناد إلى التفسير الحرفي للمادة (٤٩)، فإن العمليات غير التقليدية (Non-Kinetic Operations) – أي العمليات التي لا تستخدم القوة المادية بذاتها – لا تدخل ضمن مفهوم الهجوم. ويبدو أن هذا كان الفهم السائد عند إعداد البروتوكول الإضافي الأول. فقد أوضح بوث، وبارتش، وسولف، وهم من أبرز المشاركين في إعداد البروتوكول، أن: «مصطلح أعمال العنف يدل على استخدام القوة المادية، ولذلك فإن مفهوم الهجوم لا يشمل نشر الدعاية، أو فرض الحصار الاقتصادي، أو غير ذلك من وسائل الحرب النفسية أو الاقتصادية غير المادية.». كما يشير التعليق الرسمي للجنة الدولية للصليب الأحمر إلى أن مصطلح الهجوم يعني «العمل القتالي» (Combat Action).[٣]

يستخلص Schmitt من قراءه المادة ٥١ والمادة ٥٧ من البروتكول الإضافي الأول نتيجة أساسية، مفادها أن العبرة ليست بالعنف الكامن في الفعل ذاته، وإنما بالعنف الذي تفضي إليه نتائجه. لهذا السبب، يستنتج إن العمليات السيبرانية يمكن أن تُعد هجمات حتى وإن لم تستخدم القوة المادية مباشرة، متى كانت نتائجها مماثلة لنتائج الهجمات التقليدية. أما العملية السيبرانية التي لا ينتج عنها سوى تعطيل مؤقت أو تشويه مواقع إلكترونية أو انقطاع في الخدمات دون أضرار مادية أو إصابات بشرية، فلا ترقى – في رأيه – إلى مفهوم الهجوم في القانون الدولي الإنساني.[٤]

الاتجاه الذي تبناه Schmitt القائم على اعتبار ان العملية السيبرانية لا تُعد هجوماً إلا إذا ترتب عليها وفاة أو إصابة أو ضرر أو تدمير مادي، أو نتائج مماثلة من حيث الأثر. القى بضلاله على دليل تالين (١) ٢٠١٣ ودليل تالين (٢) ٢٠١٧.*

ويعد كلا الدليلين الذي تراس Schmitt الخبراء المعدين له المرجع الأهم في تسليط الضوء على الهجمات السيبرانية حيث حاول مجموعة من الخبراء الذين نظموا الدليل الوصول الى تعريف للهجمات السيبرانية حيث تم تعريف الهجوم السيبراني في القاعدة (٩٢) بانه (هو عملية سيبرانية، سواء كانت هجومية أو دفاعية، يُتوقع بشكل معقول أن تسبب إصابة أو وفاة للأشخاص أو أضرار أو دمار للأشياء). تحدد هذه القاعدة تعريفًا لـ'الهجوم السيبراني الذي اخذ ملامحه من ما نصت عليه المادة ٤٩(١) من البروتوكول الإضافي الأول: التي عرفت الهجمات بانها '(الهجمات تعني أعمال العنف ضد الخصم، سواء كانت هجومية أو دفاعية'). وبناءً على هذا التعريف، فإن استخدام العنف ضد هدف ما هو ما يميز الهجمات عن العمليات العسكرية الأخرى.، وبالتالي فان أي عملية سيبرانية لا تنطوي على العنف لا تعد هجوما، مثل الهجمات السيبرانية النفسية والتجسس السيبراني. [٥]

التعريف الذي تم تبنيه من الخبراء في دليل تالين ركز على طبيعة الوسيلة المستخدمة في تحقيق الميزة العسكرية، وبالتالي فان كافة الوسائل المتاحة سواء كانت دفاعية او هجومية تندرج ضمن هذا الوصف وعليه فان التعريف سلط الضوء على الوسيلة دون بيان طبيعة تلك القـــدرات.[٦]

كما اشترط الدليل الى جانب صفة العنف اشتراط ان ينتج عن ذلك الهجوم الضرر.[٧]

مما تقدم نجد ان دليل تالين عندما حاول الخبراء تكيف العملية السيبرانية بانها هجوم، والغاية من ذلك جعلها موضوعا للقانون الدولي الإنساني، استندوا الى مفهوم الهجوم في اطار المادة ٤٩ من البروتكول الإضافي الأول، فاصبح معيار العنف والضرر هما المحددين لتكيف العملية السيبرانية بانها هجوم.

الفقيه Knut Dörmann عالج موضوع الهجوم السيبراني باتجاهين الأول تعلق بتعريف الهجوم السيبراني والثاني يتعلق بمدى انطباق القانون الدولي الإنساني، حيث تعتبر اراء هذا الفقيه تعبيرا عن وجهة نظر اللجنة الدولي للصليب الأحمر.

يستند الفقيه Knut على المادة ٤٩ من البروتكول الإضافي الأول – وهو يسير بذات الاتجاه الذي سار عليه الخبراء في دليل تالين – لتحديد ملامح الهجوم السيبراني فالمادة حسب راي الفقيه ركزت على الأثر المترتب على الهجوم وليس على الوسائل التي تستخدم بالهجوم، فهو يعتبر ان التقنيات الرقمية تشكل وسائل يتم الاستعانة بها لتنفيذ عملية سيبرانية ينظر اليها فيما بعد كهجوم سيبراني من خلال الاثار التي خلفتها.[٨]

الفقيه هنا يعتبر ان الحجة القانونية في انطباق القانون الدولي الإنساني على هذه الهجمات لا تستند على المادة ٤٩ بل تستند على نص المادة ٣٦ من البروتكول الإضافي الاول والتي تنص على ((تلتزم كل دولة طرف سامٍ متعاقد، عند دراسة أو تطوير أو اقتناء أو اعتماد أي سلاح جديد، أو وسيلة أو أسلوب جديد من أساليب الحرب، بأن تتحقق مما إذا كان استخدامه محظورًا، في جميع الأحوال أو في بعضها، بموجب هذا البروتوكول أو بموجب أي قاعدة أخرى من قواعد القانون الدولي الواجبة التطبيق عليها.)).[٩]

ويخلص الفقيه الى القول ان هذه القواعد تسري بالطريقة نفسها تمامًا، سواء نُفِّذ الهجوم باستخدام الأسلحة التقليدية أو عن طريق هجمات شبكات الحاسوب، فإن الإشكالات التي قد تنشأ عند تطبيق هذه القواعد لا تُعد بالضرورة إشكالات خاصة بالعمليات السيبرانية، وإنما ترتبط أساسًا بتفسير بعض المفاهيم القانونية، مثل تحديد ما يُعد هدفًا عسكريًا، أو تقدير ما إذا كانت الأضرار العرضية (Collateral Damage) تُعد مفرطة قياسًا بالميزة العسكرية المتوقعة.[١٠]

عند تحليل كلا الرأيين نجد ان دليل تالين عندما اعتبر العملية السيبرانية هجوما بالمعنى الوارد في المادة ٤٩ من البروتكول الإضافي الأول انطلق من المعنى العام لمصطلح الهجوم التي تضمنها البروتكول، حيث وفقا للتعليقات على البروتكول الإضافي الأول اشير في الفقرة (١٨٨٠) من التعليق (ان التعريف الذي اعتمده البروتكول يتميز بنطاق أوسع، لأنه يشمل الاعمال الدفاعية الى جانب الاعمال الهجومية، وذلك لان كليهما قد يؤثر في السكان المدنيين، ولهذا السبب تم اختيار تعريف واسع للمصطلح فهو يعني عملا قتاليا). إشارة الى ذلك فان دليل تالين حافظ على منهجية تعريف الهجوم في البروتكول الإضافي الأول ولم يخرج عنه باعتبار ان المادة ٤٩ شكلت مرجعية قانونية لتكيف أي عملية عسكرية لاعتبارها هجوما. فما ذهب اليه الأستاذ Knut هو خروج عن النص وإعطاءه معنى لا ينسجم مع ما ذهب اليه واضعي البروتكول الإضافي الأول.

حاول جانب من الفقه توسيع نطاق الهجمات السيبرانية لتشمل تلك التي تستهدف الأنظمة المعلوماتية المسيطرة على انظمة القيادة والسيطرة التي غالبا ما تكون تحت تصرف القادة العسكريين والتي ترتبط بالأهداف العسكرية حيث ان تعطيل تلك الأنظمة من شانه ان يشل القدرة على توجيه القوات المسلحة مما يجعل تحقيق الأهداف العسكرية غير ناجحة.(١١)

هنا يركز هذا الجانب من الفقه على طبيعة القدرات الالكترونية من حيث التأثير على الأنظمة دون الاكتراث اذا كانت هذه العمليات تندرج ضمن العمل العسكري الهجومي او الدفاعي، كما انه يركز على الأثر أي بمعنى ان توجيه البرامج الخبيثة للأنظمة الغاية منه تعطيل تلك الأنظمة مما يفقد الخصم عنصر المناورة دون تحقيق الاضرار المادية، أي محاولة للتأخير وليس الغاية تحقيق الأهداف العسكرية وفق المنظور السائد في القانون الدولي الإنساني.

يذهب الفقيه Herbert Lin الى تعريف الهجوم السيبراني بانه (استخدام أفعال وعمليات متعمدة، الغاية منها تغيير او تعطيل او خداع او اضعاف او تدمير أنظمة وشبكات الحاسوب الخاصة بالخصم، او البيانات والبرامج الموجودة فيها او المارة عبرها، بقصد جعلها غير متاحة او غير جديرة بالثقة، وبالتالي الحد من قيمتها التشغيلية للخصم) (١٢)

يلاحظ على هذا التعريف ان الفقيه لم يركز على تحديد وسيلة بعينها بل اعتبر كل وسيلة تؤدي الى الاضرار بالأنظمة الرقمية للخصم تعد هجوما أي اخذ بالوصف الوظيفي لتلك العمليات من خلال بيان النتيجة المترتبة عليها، فكل عملية سيبرانية تؤدي الى احداث اثار مدمرة للكفاءة الرقمية تعد هجمات سيبرانية، وهذا الوصف ذي أهمية على صعيد القانون الدولي الإنساني لأنه يركز على الضرر الناشئ والمهدد للمدنيين والاعيان المدنية دون الاكتراث بالوسيلة المستخدمة أي ينظر الى النتيجة دون الوسيلة.

هناك من يميز بين الهجمات السيبرانية والجرائم السيبرانية حيث ترى Hathaway وزملاؤها قد تُعد بعض الهجمات السيبرانية في الوقت ذاته جرائم سيبرانية (Cyber-Crimes)، إلا أن ذلك لا يعني أن جميع الجرائم السيبرانية تُعد هجمات سيبرانية. فالجرائم السيبرانية قد تستهدف تحقيق منافع مالية أو أغراض شخصية أو إجرامية بحتة، دون أن يكون لها هدف سياسي أو أمني أو أن تؤثر في وظائف الأنظمة المعلوماتية على النحو الذي يميز الهجوم السيبراني. أما الحرب السيبرانية (Cyber-Warfare)، فإنها تستوفي دائمًا الشروط اللازمة لاعتبار الفعل هجومًا سيبرانيًا، غير أن العكس ليس صحيحًا؛ إذ لا يُعد كل هجوم سيبراني حربًا سيبرانية. وإنما ترتقي العملية السيبرانية إلى مستوى الهجوم السيبراني فقط إذا ترتبت عليها آثار تعادل آثار "الهجوم المسلح" (Armed Attack) بالمعنى التقليدي، أو إذا وقعت في سياق نزاع مسلح قائم. (١٣)

مما تقدم نجد ان الفقه الدولي سار في اتجاهات متعددة لتكيف العملية السيبرانية بانها هجوم، فاتجاه راعى فحوى المادة ٤٩ من البروتكول الإضافي الأول (دليل تالين). بينما ذهب اتجاه (Knut) الى تكيف الأنظمة الرقمية المستخدمة في العمليات السيبرانية من قبيل الأسلحة التي يجب ان تستوفي

متطلبات القانون الدولي الإنساني التي وردت في المادة ٣٦ من البروتكول. في حين اعتبر (Herbert) الضرر الذي يلحق بالأنظمة الرقمية هو دليل على اننا امام عملية سيبرانية شكلت (هجوم). بينما الاتجاه الأخير (Hathaway) قام بتكيف العملية السيبرانية بانها هجوم قياسا على الهجمات التقليدية من خلال النظر الى الاثار المتحققة فمتى ما كانت مشابه لتلك التي تنشا من الهجمات التقليدية نكون امام هجوم سيبراني.

والراي عندنا ان ما ذهب اليه دليل تالين هو المعول عليه لأنه لم يخرج من نطاق نص المادة ٤٩ المرجع في تكيف الهجمات في اطار القانون الدولي الإنساني.

ساهمت الدول في إيجاد تعريف للهجمات السيبرانية حيث اخذت الولايات المتحدة الامريكية بالاتجاه الضيق في تعريف تلك الهجمات والذي يركز على الهجوم، ومن امثلة التعريفات في هذا الاتجاه، ما تبنته القيادة الاستراتيجية الامريكية عام ٢٠٠٧ بشان استخدام الوسائل الالكترونية للأغراض العسكرية فقد عرفته بانه (تطويع عمليات نظام الكمبيوتر بهدف منع الخصم من الاستخدام الفعال لها، فضلا عن التسلل الى أنظمة المعلومات وشبكات الاتصال بهدف جمع البيانات التي تحتويها) [١٤].

على النقيض من الاتجاه الضيق الذي تبنته الولايات المتحدة رسميا، اعتمدت منظمة شنغهاي للتعاون نهجًا أكثر اتساعًا في تعريف الهجمات السيبرانية، يقوم على الوسيلة المستخدمة (Means-Based Approach) وليس على الآثار المترتبة عليها. فقد أعربت المنظمة عن قلقها إزاء التهديدات الناجمة عن احتمال استخدام تكنولوجيات ووسائل المعلومات والاتصالات الجديدة لأغراض لا تتوافق مع متطلبات الأمن والاستقرار الدوليين، سواء في المجال المدني أو العسكري، فهي تتبنى تصورًا واسعًا للهجمات السيبرانية، يمتد ليشمل استخدام التقنيات السيبرانية بقصد تقويض الاستقرار السياسي للدول، وليس فقط الهجمات التي تُحدث أضرارًا تقنية أو مادية بالأنظمة المعلوماتية.[١٥]

اعتمدت المملكة المتحدة تعريفا للهجمات السيبرانية كرستها في وثيقة الاستراتيجية الوطنية للأمن السيبراني الذي أورد تعريفا للهجوم السيبراني بانه (الاستغلال المتعمد لأنظمة الحاسبات، والمؤسسات المعتمدة على التقنيات الرقمية، والشبكات، بقصد احداث الضرر) [١٦]

كما استخدم المركز الوطني للأمن السيبراني البريطاني تعريفا يتسم بالتفصيل حيث أشار في تعريفه للهجوم السيبراني بانه (محاولة الحاق الضرر، او التعطيل، او الحصول على وصول غير مصرح به الى أنظمة الحاسوب او الشبكات او الأجهزة) [١٧].

ان ما يميز التعريف الإنكليزي للهجوم السيبراني اتسامه بالبساطة والسبب في ذلك ان التعريف لا ينظر الى نجاح الهجوم السيبراني في تحقيق نتائجه بل يكتفي بالمحاولة بالأضرار او الوصول غير المشروع الى الأنظمة الرقمية. ويؤخذ على هذا التعريف اتسامه بالطابع الوطني أي ذي مساس بالأمن السيبراني ولا يمكن اللجوء اليه في اطار القانون الدولي الإنساني الذي يتتبع الضرر كنتيجة لاي هجوم وليس محاولة احداث النتيجة.

نظرا لعدم وجود تعريف موحد للهجمات السيبرانية وعدم وجود اتفاقية دولية متخصصه بهذا الشأن فان الهيئات الدولية شانها شان الفقه الدولي حاولت ان تقدم تعريفات تسهم في بلورة مفهوم قانوني للهجمات السيبرانية.

اللجنة الدولية للصليب الأحمر لم تضع تعريفا مستقلا للهجوم السيبراني، بل اعتمدت على القياس في تحديد مفهومه من خلال الإشارة الى مفهوم الهجوم الذي ورد في المادة ٤٩ من البروتكول الإضافي الأول لاتفاقيات جنيف لعام ١٩٧٧ والذي نص ((الهجمات هي اعمال العنف ضد الخصم، سواء كانت هجومية ام دفاعية)). حيث ترى اللجنة ان هذا المفهوم يمكن مقاربته للهجمات السيبرانية متى ما تحقق التوقع بحدوث إصابات تتمثل بموت الأشخاص او تدمير الاعيان المدنية، كما اكدت ان المبادئ التقليدية التي تحكم سير العمليات العسكرية التقليدية يمكن وفق هذه المقاربة التي انتهجتها اللجنة الدولية للصليب الأحمر ان تطبق على الهجمات السيبرانية.[١٨]

كما ان للجنة الدولية للصليب الأحمر اتخذت موقفًا مفاده أن أي عملية تهدف لتعطيل جهاز كمبيوتر أو شبكة كمبيوتر خلال نزاع مسلح تُعتبر هجومًا كما هو معرّف في القانون الإنساني الدولي سواء تم تعطيل الهدف عن طريق التدمير أو بأي طريقة أخرى.[١٩]

اللجنة الدولية اعادت دراسة الهجمات السيبرانية في ٢٠٢٤ عندما تناولت الموضوع ضمن التحديات التي تواجه القانون الدولي الإنساني حيث اكدت ان المبادئ والقواعد الحالية للقانون الدولي الإنساني تقيد الهجمات السيبرانية في اطار النزاع المسلح، الا ان اللجنة أبدت قلقها من وتيرة التطورات التقنية واستخدام هذه الهجمات السيبرانية تفوق وتيرة المناقشات والتطورات المتعلقة بالقواعد، وعلى وجه الخصوص ترى اللجنة الدولية ان تفسيرات القانون الدولي الإنساني التي تركز على حماية الاعيان المدنية من الاضرار المادية غير المباشرة غير كافية.[٢٠]

مما تقدم نجد ان اللجنة الدولية للصليب الأحمر اعتمدت منهجا يمثل تكريسا لدورها في ضمان انطباق القانون الدولي الإنساني على أي نشاط يرتبط بالنزاعات المسلحة ومن شانه ان يلحق اضرار تتمثل في فقدان المدنيين لحياتهم او تدميرا للاعيان المدنية، بعدم الولوج في الجدل الفقهي حول التميز بين الهجمات السيبرانية والحرب الالكترونية. وهذا المنهج يستند الى الوثائق القانونية التي تشكل النظام القانوني المحدد للعمليات العسكرية. حيث الزمت المادة ٣٦ من البروتكول الأول عام ١٩٧٧ الدول المتعاقدة على ضرورة التأكد من مشروعية الأسلحة قبل إدخالها الى مجال التصنيع او الاستخدام والمشروعية هنا بان لا تكون تلك الأسلحة مما تحدث الالام غير المبررة او تكون عشوائية. واللجنة الدولية للصليب الأحمر اعتمدت الحياد التكنولوجي في مواجهة التحديات الجديدة في مجال وسائل القتال.

التحقت المنظمة العالمية الأمم المتحدة بالجهود الدولية الرامية الى إيجاد تعرف او تحديد مفهوم الهجمات السيبرانية وتكمن الأهمية في جهود منظمة الأمم المتحدة بان تبنيها لمفهوم او تعريف للهجمات السيبرانية من شانه ان يفتح الباب امام معاهدة دولية تنظم الهجمات السيبرانية وتحدد اطارا مفاهيميا لها.

ولكن للأسف لا يوجد تعريف قانوني ملزم بل اقتصر الامر على تقارير الخبراء الحكوميين للأمم المتحدة (UN GCE) والفريق العامل المفتوح (OEWG) اللذان استخدما مصطلح الهجمات او الهجمات السيبرانية دون التعريف بل التأكيد فقط على انطباق القانون الدولي وميثاق منظمة الأمم المتحدة على استخدام تكنولوجيا المعلومات والاتصالات في الفضـاء السيبراني.[٢١]

كما أشار الفريق الى ان مبادئ الإنسانية والضرورة والتناسب والتمييز قابلة للتطبيق على تلك العمليات.[٢٢]

يتضح ان المجتمع الدولي لم يتفق على تعريف موحد للهجوم السيبراني، الا ان هناك اتفاق على ان الهجوم السيبراني باعتباره تحديا يواجه المنظومة القانونية الدولية يجب ان لا يكون خارجها على أساس التبرير بعدم وجود ما يحدد مفهومه ولذلك نجد ان الأمم المتحدة حرصت على التأكيد بان هذه العمليات ليست خارج سلطة القانون الدولي وميثاقها بل اعتبرت ان الالتزام بالقانون الدولي وميثاقها أساس لمشروعية او عدم مشروعية هذه العمليات. كما ان اللجنة الدولية للصليب الأحمر التي تحرص على عدم السماح لاي متغير دولي بان يكون خارج نطاق القانون الدولي الإنساني في اطار النزاعات المسلحة وما ينتج عنه من اثار تمس المدنيين والاعيان المدنية، فقد اتجهت الى مساواة الهجمات السيبرانية بالهجوم التقليدي وبالتالي فهو مقيد بالمبادئ الرئيسية التي قيدت العمليات العسكرية كمبادئ التمييز والتناسب والاحتياطات الممكنة.

عندما تعجز الاتجاهات الفقهية وكذلك الهيئات الدولية عن الوصول الى فهم شامل لمسالة معينة تشكل تحديا قانونيا تتطلب تأطيرها قانونيا، تتجه الأنظار الى القضاء الدولي ليدلو بدلوه في معالجة القصور الذي يكتنف تحديد مفهوم الهجمات السيبرانية سواء فقهيا او على مستوى الهيئات وكذلك الدول.

محكمة العدل الدولية في قضية الأنشطة العسكرية وشبه العسكرية في نيكاراغوا ضد الولايات المتحدة الامريكية ١٩٨٦ اشارت الى معيار يمكن الركون اليه في التمييز بين استخدام القوة والهجوم المسلح حيث اعتمدت على جسامة الفعل والاثار الناشئة عنه، أي ليس على الوسيلة المستخدمة في تحقيق الأهداف. [٢٣]

اعادت المحكمة التأكيد على هذين المعيارين في قضية المنصات النفطية ٢٠٠٣ عندما اشارت الى ان ممارسة حق الدفاع عن النفس وفق المادة ٥١ من الميثاق لا يكتب له المشروعية الا اذا وقع هجوم واعادت الإشارة الى مفهوم الهجوم لحكمها السابق في قضية الأنشطة العسكرية.[٢٤]

وكررت ذات الحكم في قضية المنصات النفطية في قضية الأنشطة المسلحة على إقليم الكونغو حيث اضافت الى مشروعية الدفاع الشرعي عند وقوع الهجوم المسلح، رفضها التوسع في مفهوم الهجوم المسلح ليشمل كل صور استخدام القوة.[٢٥]

ورغم ان القضية ظهرت قبل ظهور الاهتمام الدولي بالهجمات السيبرانية، الا ان الفقه الدولي اعتبر ان معيار الحجم والاثار يمكن ان يكونا معيارين يركن اليهما لتقييم الهجمات السيبرانية، فاذا أحدثت العملية السيبرانية اثارا تماثل تلك التي تنشا عن العمليات العسكرية التقليدية، كتعطيل شبكات الكهرباء او

المستشفيات او أنظمة الدفاع الجوي وتؤدي الى خسائر جسيمة، فأنها تعد هجوما مسلحا يخضع لأحكام القانون الدولي الإنساني. وهذا ما اخذ به الخبراء عند اعداد دليل تالين فأي عملية سيبرانية استوفت معياري محكمة العدل الدولية، يمكن اعتباره هجوما مسلحا [٢٦]

لم تعتمد المحكمة الجنائية الدولية تعريفا مستقلا للهجمات السيبرانية، كما ان نظام روما الأساسي لم يتضمن نصا يمكن الرجوع اليه لتعريف تلك الهجمات، الا انه من المعروف ان منهج المحكمة في انعقاد اختصاصها قائم على طبيعة السلوك والنتائج المترتبة عليه أي يتم استبعاد الوسيلة المستخدمة في ارتكاب الفعل، وعند الحديث عن الهجوم السيبراني فانه يدخل في اختصاص المحكمة اذا أدى الى اثار استوفت اركان الجرائم الداخلة في اختصاص المحكمة بغض النظر عن الوسيلة المستخدمة، وعليه فان المحكمة لا تعرف الهجمات السيبرانية ولكنها تختص بها متى ما استوفت اركان الجرائم.

مما تقدم يتبين ان القضاء الدولي ومن خلال احكام محكمة العدل الدولية قدم فهما عميقا للعمليات السيبرانية بصورة غير مباشرة، حيث ان دراسة الهجمات السيبرانية في اطار القانون الدولي الإنساني تتطلب ابتداء تحديد وصف هذه العمليات عندما يتم اللجوء اليها في اطار نزاع مسلح أي عندما تكون وسيلة لتحقيق اهداف عسكرية، حتى يمكن إدخالها في اطار القانون الدولي الإنساني يجب ان تكون هذه العمليات بمجملها بمثابة هجوم مسلح وبغياب النص باعتبارها كذلك، استطاع الفقه الدولي الاستعانة بمعايير الهجوم المسلح الذي وضعته محكمة العدل الدولية من ناحية الحجم والاثار لتطبيقه على الهجمات السيبرانية متى ما كانت بالحجم والاثار التي تناسبت مع استنتاج القضاء الدولي عندما أشار الى (العمليات الأشد قسوة) وبالتالي يمكن ادراجها ضمن مفهوم الهجوم الذي ورد في المادة ٤٩ من البروتكول الإضافي الأول لاتفاقيات جنيف عام ١٩٧٧.

شهد العالم العديد من العمليات السيبرانية والتي تصدى لها الفقهاء بالبحث وكان التركيز حول مدى اعتبار تلك العمليات هجمات وفق مفهوم القانون الدولي الإنساني.

يعتبر الفقيهان Eneken Tikk and Kadri Kaska هجوم استونيا اختبارا مهما للقانون الدولي الإنساني في مدى إمكانية انطباق قواعده على الهجمات السيبرانية، حيث باشر كلاهما بدراسة هجوم استونيا لبيان مدى إمكانية اعتبار هذه العملية السيبرانية بمثابة هجوم يندرج تحت مفهوم الهجوم وفق قواعد القانون الدولي الإنساني، حيث توصل كلا الفقيهان الى عدم اعتبار العملية السيبرانية في استونيا بمثابة هجوم والسبب في ذلك حسب رايهما عدم وجود دليل على تورط دولة أجنبية في هذه العملية، لم تؤدي الوسائل المستخدم الى احداث إصابات بالمدنيين او تدمير للاعيان المدنية، حيث ان الضرر الناشئ عن العملية أدى الى افقاد الخدمات الالكترونية لوظيفتها.[٢٧]

نظرا للتزامن الزمني بين الهجمات على جورجيا وتلك التي وقعت على استونيا، اثارت جملة من التساؤلات بين الفقهاء تركزت بدرجة حول الطبيعة القانونية للهجمات السيبرانية وما هو القانون الواجب التطبيق[28]

مبررات اثارة السؤال ما مدى انطباق القانون الدولي الإنساني على هذه الهجمات نشات من الإشارات الإعلامية بان الهجمات على جورجيا ارتقت للحرب السيبرانية، وذلك لوجود قواسم مشتركة مع الهجوم على استونيا والتي كانت المراجع القانونية تشير اليها بانها الحرب السيبرانية الأولى (Cyber War 1). [٢٩]

يشير الفقيه Eneken Tikk الى مفهوم النزاع المسلح في القانون الدولي الإنساني الذي ينشا يتدخل عسكري من احدى الدول دون الحاجة للإعلان فالواقع الفعلي لبدء الاعمال العدائية هو المعيار الحاسم في انطباق القانون الدولي الإنساني، والاحداث التي وقعت بين جورجيا وروسيا تضمنت تدخلا فعليا للقوات المسلحة الروسية، وبه يعتبر نزاعا مسلحا.[٣٠]

ويسترسل الفقيه في دراسة أخرى تناولت الهجوم السيبراني ذاته بالقول ومع ذلك، فإن مجرد انطباق قانون النزاعات المسلحة (LOAC) على النزاع المسلح التقليدي بين روسيا وجورجيا لا يعني تلقائياً انطباقه على الهجمات السيبرانية التي وقعت بالتزامن مع العمليات العسكرية. فالهجمات السيبرانية، وإن حدثت في سياق نزاع مسلح، ينبغي أن تخضع لتقييم قانوني مستقل لتحديد ما إذا كانت تستوفي الشروط التي تجعلها «هجوماً مسلحاً» (Armed Attack) بالمعنى الذي يؤدي إلى تطبيق قواعد القانون الدولي الإنساني (Jus in Bello).[٣١]

كما يعتبر الفقيه أن اشتراك القوات المسلحة في النزاع يمثل أحد المؤشرات المهمة على انطباق قانون النزاعات المسلحة. إلا أن هذا المعيار يثير صعوبات عند تطبيقه على العمليات السيبرانية، لأن كثيراً من الدول لا تمتلك قوات سيبرانية مستقلة ضمن هيكلها العسكري، الأمر الذي يجعل من الصعب إثبات وجود علاقة مباشرة بين الهجوم السيبراني والقوات المسلحة للدولة.[٣٢]

ويصل الى نتيجة مفادها ان تحديد أي عملية سيبرانية بانها تشكل هجوماً يتطلب تقديراً لمدى جسامة الآثار الإنسانية التي ترتبت عليها، وليس مجرد النظر إلى الوسيلة المستخدمة في تنفيذها.[٣٣]

بخالف الاستاذ توماس ريد الراي بان العمليات السيبرانية الموجهة لجورجيا تشكل هجوم سيبراني وإنما شكلت وسيلة داعمة للعمليات العسكرية التقليدية. ولا خلاف في أن التخريب السياسي (Subversion)، والتجسس (Espionage)، والتخريب المادي أو الفني (Sabotage) – سواء نُفذت بوسائل سيبرانية أم بوسائل تقليدية – قد تصاحب العمليات العسكرية. فمنذ أقدم العصور، لجأت أطراف النزاعات المسلحة إلى هذه الوسائل لدعم عملياتها العسكرية، واستُخدمت من جانب جميع المتحاربين بوصفها أدوات مساندة للحرب.[٣٤]

وهذا ما اتفق عليه واضعي دليل تالين (٢) بان العملية السيبرانية لا تُعد هجومًا مسلحًا إلا إذا بلغت آثارها مستوى يعادل الهجوم العسكري التقليدي من حيث التدمير أو الخسائر البشرية. ولذلك فإن الهجمات على جورجيا، بالنظر إلى أنها اقتصرت أساسًا على تعطيل الخدمات الإلكترونية، لا تحقق منفردةً معيار الهجوم المسلح.[٣٥]

وصف الأستاذ الاستاذ توماس ريد هجوم Stuxnet، حتى تاريخ اكتشافه، أكثر الهجمات السيبرانية المعروفة تطورًا وتعقيدًا. فقد كان هجومًا موجَّهًا بدقة نحو أهداف محددة، يُرجَّح أنها تمثلت في برنامج تخصيب اليورانيوم الإيراني في منشأة نطنز. وقد مثَّلت البرمجية الخبيثة (Worm) عملًا تخريبيًا سيبرانيًا مستقلًا (Cyber-enabled Stand-alone Sabotage)، إذ لم يكن مرتبطًا بأي عملية عسكرية تقليدية أو مصاحبًا لها. كما صُنِّف Stuxnet ضمن ما يُعرف في صناعة الأمن السيبراني بـ التهديدات المتقدمة والمستمرة (Advanced Persistent Threats - APTs)، وهي هجمات تتميز بدرجة عالية من التخطيط والتخفي والاستمرارية.[٣٦]

أعاد الأستاذ توماس ريد التأكيد على ان هذا الهجوم لا يندرج ضمن مفهوم الهجوم السيبراني أي تحت مفهوم الحرب السيبرانية، لأنه يعتبر الضرر المتمثل بالتعطيل لا يرتقي الى العنف المشار اليه عند تحديد مفهوم الهجوم في القانون الدولي الإنساني وفق المادة ٤٩ /١ من البروتكول الإضافي الأول.[٣٧]

علق خبراء دليل تالين على هذا الهجوم بالإشارة الى ان عملية Stuxnet التي نُفذت عام ٢٠١٠ تقدم مثالًا يوضح عدم استقرار وعدم حسم معيار العتبة اللازمة لاعتبار العملية السيبرانية "هجومًا مسلحًا". ففي ضوء الأضرار التي لحقت بأجهزة الطرد المركزي الإيرانية نتيجة تلك العملية، رأى بعض أعضاء الفريق الدولي للخبراء أن الهجوم بلغ عتبة الهجوم المسلح (Armed Attack)، ما لم يكن من الممكن تبريره استنادًا إلى حق الدفاع الشرعي الاستباقي (وفقًا للقاعدة ٧٣). وفي المقابل، تبنى خبراء آخرون الرأي المعاكس، معتبرين أن العملية لم ترقَ إلى مستوى الهجوم المسلح. ومع ذلك، وكما أوضح الدليل عند مناقشة القاعدة ٦٨، فقد اتفق جميع أعضاء الفريق على أن العملية تمثل استخدامًا للقوة (Use of Force).[٣٨]

من خلال ما تقدم يمكن بيان ان هجوم Stuxnet شكل انعطاف في موضوع الحرب السيبرانية باعتبار ان البرمجيات هنا استخدمت كسلاح في المعركة، وليس كما في الهجمات السابقة كوسيلة داعمة للعمليات العسكرية.*

الراي عندنا ان العملية السيبرانية متى ما كانت في اطار نزاع مسلح، وكانت منطوية على عنف ينتج عنه اضرار تصيب المنظومات الرقمية، فان تلك العملية تعد هجوما، أي متى ما استوفت متطلبات المادة ٤٩ من البروتكول الإضافي الأول.

المطلب الثاني: تطبيقات الهجمات السيبرانية

أولا- هجوم استونيا (٢٠٠٧) [٣٩]: وفي ٢٦ نيسان/أبريل ٢٠٠٧، لوحظ التصاعد الملحوظ في حجم الهجمات السيبرانية، ويُنظر إلى هذا التاريخ على نطاق واسع بوصفه بداية الهجوم السيبراني واسع النطاق على إستونيا. وبلغت الهجمات ذروتها في ٩ أيار/مايو، وهو اليوم الذي يحيي فيه الاتحاد الروسي ذكرى الانتصار في الحرب العالمية الثانية. ومنذ ذلك التاريخ بدأ عدد العمليات العدائية في الانخفاض تدريجياً. وفي ١١ أيار/مايو توقفت أنشطة شبكات البوت المدفوعة (Paid Botnets)، بينما وقع آخر

هجوم في ٢٣ أيار/مايو، وقد استهدفت هجمات حجب الخدمة الموزعة (DDoS) بنجاح المواقع الإلكترونية لجميع الوزارات الحكومية، واثنين من أكبر المصارف في إستونيا، وعدداً من الأحزاب السياسية. كما تمكن المهاجمون من تعطيل خادم البريد الإلكتروني الخاص بالبرلمان، وأدى الهجوم إلى تعطيل خدمات بطاقات الائتمان وأجهزة الصراف الآلي [3](ATMs) وقد قدّر أحد المصارف الإستونية، الذي كان من بين ضحايا الهجمات السيبرانية، حجم خسائره بحوالي مليون دولار أمريكي.**[14] **ومع ذلك، وعند إجراء التقييم النهائي للأضرار، تبين أن الخسائر الناجمة عن الهجمات السيبرانية كانت أقل بكثير مما كان متوقعاً، وكانت غالبية العمليات عبارة عن هجمات حجب الخدمة الموزعة (DDoS)، وهي تقنية لم تكن جديدة آنذاك، إذ سبق استخدامها في العديد من الحوادث الإلكترونية السابقة.**[16] **غير أن ما ميّز الحالة الإستونية هو الجمع بين هجمات نفذها قراصنة محترفون، يُرجَّح انتماء بعضهم إلى شبكة الأعمال الروسية (Russian Business Network)، الذين استخدموا شبكات البوت (Botnets)، وبين ما يُعرف بـ«القراصنة الوطنيين» (Patriotic Hackers)، وهم أفراد، معظمهم من الشباب، اندفعوا بدافع قومي احتجاجاً على قرار سلطات تالين نقل النصب التذكاري السوفيتي.(٤٠)

يعتبر الفقيهان Eneken Tikk and Kadri Kaska هذا الهجوم اختبارا مهما للقانون الدولي الإنساني في مدى إمكانية انطباق قواعده على الهجمات السيبرانية، حيث باشر كلاهما بدراسة هجوم استونيا لبيان مدى إمكانية اعتبار هذه العملية السيبرانية بمثابة هجوم يندرج تحت مفهوم الهجوم وفق قواعد القانون الدولي الإنساني، حيث توصل كلا الفقيهان الى عدم اعتبار العملية السيبرانية في استونيا بمثابة هجوم والسبب في ذلك حسب رايهما عدم وجود دليل على تورط دولة أجنبية في هذه العملية، لم تؤدي الوسائل المستخدم الى احداث إصابات بالمدنيين او تدمير للاعيان المدنية، حيث ان الضرر الناشئ عن العملية أدى الى افقاد الخـــدمات الالكترونية لوظيفتها.(٤١)

ثانيا – الهجوم السيبراني على جورجيا: يقع النزاع السيبراني محل هذه الدراسة ضمن الإطار الزمني والسياق العام لنزاع مسلح أوسع اندلع في شهر آب/أغسطس ٢٠٠٨ بين الاتحاد الروسي وجورجيا بشأن إقليم أوسيتيا الجنوبية، وهو إقليم يتمتع بالحكم الذاتي ويُعد، من الناحية القانونية (de jure)، جزءًا منزوع السلاح من الأراضي الجورجية يقع على الحدود بين جورجيا وروسيا.

وقد أصبحت أوسيتيا الجنوبية مستقلة بحكم الأمر الواقع (de facto) عن جورجيا عقب النزاع الجورجي–الأوسيتي الذي وقع عام ١٩٩١، إلا أنها ظلت تحظى باعتراف المجتمع الدولي، بصورة عامة، بوصفها جزءًا لا يتجزأ من إقليم جورجيا. وقد استمرت غالبية الدول الأعضاء في الأمم المتحدة في الاعتراف بالسلامة الإقليمية لجورجيا حتى بعد انتهاء النزاع الروسي–الجورجي في آب/أغسطس ٢٠٠٨، وعلى الرغم من إعلان وقف إطلاق النار وإبرام العديد من الاتفاقات اللاحقة وعلى الرغم من إعلان وقف إطلاق النار وبذل العديد من الجهود السلمية منذ نزاع عام ١٩٩١، بقي التوتر في المنطقة دون حل. وللحفاظ على الاستقرار في إقليم أوسيتيا الجنوبية عقب أحداث عام ١٩٩١، شُكِّلت في عام ١٩٩٢ قوة

لحفظ السلام بموجب تفويض صادر عن منظمة الأمن والتعاون في أوروبا (OSCE)، وضمت هذه القوة وحدات عسكرية روسية وجورجية وأوسيتية جنوبية، وكانت تخضع لقيادة قائد روسي. إلا أن هذه القوات، من الناحية العملية، أخفقت في تحقيق التعاون الفعّال فيما بينها، واستمرت حدة التوتر في التصاعد تدريجيًا بين الحكومة الجورجية من جهة، والانفصاليين المدعومين في معظمهم من روسيا من جهة أخرى وبعد فترة شهدت سلسلة من الاستفزازات التي قامت بها الجماعات الانفصالية، شنت القوات الجورجية في ٧ آب/أغسطس ٢٠٠٨ هجومًا مفاجئًا على قوات الانفصاليين. وفي اليوم التالي، أي في ٨ آب/أغسطس ٢٠٠٨، ردّ الاتحاد الروسي على التحرك العسكري الجورجي، مستندًا إلى ما وصفه بالتزامه الوطني بـ**"حماية المواطنين الروس في الخارج"**، فأطلق عمليات عسكرية داخل الأراضي الجورجية.

قد امتدت العمليات العسكرية الروسية داخل الأراضي الجورجية، فبدأت أولًا في إقليم أوسيتيا الجنوبية، ثم تجاوزت لاحقًا حدود المنطقة التي كان يشملها تفويض قوات حفظ السلام. وقد اعتبرت السلطات الجورجية هذا التدخل عدوانًا عسكريًا روسيًا ضد جورجيا. وردًا على ذلك، أعلن رئيس جورجيا آنذاك، ميخائيل ساكاشفيلي، في ٨ آب/أغسطس ٢٠٠٨ أمام المجتمع الدولي بدء عملية التعبئة العامة، وفي ٩ آب/أغسطس ٢٠٠٨ أعلنت جورجيا حالة الحرب. وعلى الرغم من أن هذا الإجراء كان في المقام الأول تدبيرًا وطنيًا اتخذته جورجيا في ظل إدراكها لوجود تهديد يمس أمنها القومي وسيادتها، فإنه أرسى أيضًا الإطار القانوني الذي تعاملت الدولة في ظله مع الهجمات السيبرانية، ومن ثم فإن استحضار هذا السياق يعد أمرًا ضروريًا عند دراسة رد فعل جورجيا تجاه تلك الهجمات. وفي ٨ آب/أغسطس ٢٠٠٨، أي قبل بدء الغزو العسكري الروسي للأراضي الجورجية، كانت الهجمات السيبرانية قد بدأت بالفعل واستهدفت عددًا كبيرًا من المواقع الإلكترونية الحكومية الجورجية. وبينما انتهت العمليات العسكرية التقليدية بإبرام اتفاق لوقف إطلاق النار في ١٢ آب/أغسطس ٢٠٠٨، استمرت الهجمات السيبرانية طوال ما تبقى من ذلك الشهر، وهو ما يعكس أن العمليات الإلكترونية لم تكن مرتبطة زمنيًا فقط بالأعمال القتالية، بل امتدت آثارها إلى ما بعد توقف العمليات العسكرية التقليدية.[42]

نظرا للتزامن الزمني بين الهجمات على جورجيا وتلك التي وقعت على استونيا، اثارت جملة من التساؤلات بين الفقهاء تركزت بدرجة حول الطبيعة القانونية للهجمات السيبرانية وما هو القانون الواجب التطبيق.[٤٣]

مبررات اثارة السؤال ما مدى انطباق القانون الدولي الإنساني على هذه الهجمات نشات من الإشارات الإعلامية بان الهجمات على جورجيا ارتقت للحرب السيبرانية، وذلك لوجود قواسم مشتركة مع الهجوم على استونيا والتي كانت المراجع القانونية تشير اليها بانها الحرب السيبرانية الأولى (Cyber War 1). [٤٤]

يشير الفقيه Eneken Tikk الى مفهوم النزاع المسلح في القانون الدولي الإنساني الذي ينشا يتدخل عسكري من احدى الدول دون الحاجة للإعلان فالواقع الفعلي لبدء الاعمال العدائية هو المعيار

الحاسم في انطباق القانون الدولي الإنساني، والاحداث التي وقعت بين جورجيا وروسيا تضمنت تدخلا فعليا للقوات المسلحة الروسية، وبه يعتبر نزاعا مسلحا.(٤٥)

ويسترسل الفقيه في دراسة أخرى تناولت الهجوم السيبراني ذاته بالقول ومع ذلك، فإن مجرد انطباق قانون النزاعات المسلحة (LOAC) على النزاع المسلح التقليدي بين روسيا وجورجيا لا يعني تلقائياً انطباقه على الهجمات السيبرانية التي وقعت بالتزامن مع العمليات العسكرية. فالهجمات السيبرانية، وإن حدثت في سياق نزاع مسلح، ينبغي أن تخضع لتقييم قانوني مستقل لتحديد ما إذا كانت تستوفي الشروط التي تجعلها «هجوماً مسلحاً» (Armed Attack) بالمعنى الذي يؤدي إلى تطبيق قواعد القانون الدولي الإنساني (Jus in Bello).(٤٦)

كما يعتبر الفقيه أن اشتراك القوات المسلحة في النزاع يمثل أحد المؤشرات المهمة على انطباق قانون النزاعات المسلحة. إلا أن هذا المعيار يثير صعوبات عند تطبيقه على العمليات السيبرانية، لأن كثيراً من الدول لا تمتلك قوات سيبرانية مستقلة ضمن هيكلها العسكري، الأمر الذي يجعل من الصعب إثبات وجود علاقة مباشرة بين الهجوم السيبراني والقوات المسلحة للدولة.(٤٧)

ويصل الى نتيجة مفادها ان تحديد أي عملية سيبرانية بانها تشكل هجوماً يتطلب تقديراً لمدى جسامة الآثار الإنسانية التي ترتبت عليها، وليس مجرد النظر إلى الوسيلة المستخدمة في تنفيذها.(٤٨)

بخالف الاستاذ توماس ريد الراي بان العمليات السيبرانية الموجهة لجورجيا تشكل هجوم سيبراني وإنما شكلت وسيلة داعمة للعمليات العسكرية التقليدية. ولا خلاف في أن التخريب السياسي (Subversion)، والتجسس (Espionage)، والتخريب المادي أو الفني (Sabotage) – سواء نُفذت بوسائل سيبرانية أم بوسائل تقليدية – قد تصاحب العمليات العسكرية. فمنذ أقدم العصور، لجأت أطراف النزاعات المسلحة إلى هذه الوسائل لدعم عملياتها العسكرية، واستُخدمت من جانب جميع المتحاربين بوصفها أدوات مساندة للحرب.(٤٩)

وهذا ما اتفق عليه واضعي دليل تالين (٢) بان العملية السيبرانية لا تُعد هجومًا مسلحًا إلا إذا بلغت آثارها مستوى يعادل الهجوم العسكري التقليدي من حيث التدمير أو الخسائر البشرية. ولذلك فإن الهجمات على جورجيا، بالنظر إلى أنها اقتصرت أساسًا على تعطيل الخدمات الإلكترونية، لا تحقق منفردةً معيار الهجوم المسلح.(٥٠)

ثالثا – هجوم (Stuxnet): يُعد هجوم (Stuxnet) محطةً فارقةً في تاريخ الأمن السيبراني؛ إذ كُشف عنه لأول مرة في ١٧ حزيران/يونيو ٢٠١٠، رغم أن الأدلة تشير إلى أنه كان قيد التطوير السري منذ عام ٢٠٠٥ على الأقل. وقد صُمم(Stuxnet) بوصفه دودةً حاسوبية استهدفت على وجه التحديد تدمير برنامج إيران لتخصيب اليورانيوم، حيث وُجِّهت غالبية هجماته إلى منشأة نطنز النووية. ويُعتقد على نطاق واسع أن هذا البرنامج الخبيث المتطور قد طُوِّر بصورة مشتركة من قبل الولايات المتحدة وإسرائيل في إطار عملية سرية حملت الاسم الرمزي "الألعاب الأولمبية" (Operation Olympic Games)، رغم أن أيًا من

الدولتين لم تعترف بذلك رسميًا. وعلى خلاف البرمجيات الخبيثة التقليدية التي تهدف إلى التجسس أو سرقة البيانات، استهدف (Stuxne) إحداث أثر مادي ملموس، تمثل في تدمير أجهزة الطرد المركزي المستخدمة في عمليات تخصيب اليورانيوم.

بدأ الهجوم عندما أُدخلت الدودة إلى البيئة شديدة الحماية الخاصة بالمنشأة، ويُرجح أن ذلك تم عن طريق وحدة تخزين USB مصابة. ومن هناك انتقلت بصمت إلى أجهزة الحاسوب العاملة بنظام Windows التي كانت تتحكم في أنظمة التحكم الصناعية، مستهدفةً برنامج Siemens Step المسؤول عن تشغيل وحدات التحكم المنطقية القابلة للبرمجة (Programmable Logic Controllers - PLCs). وفي شهر حزيران/يونيو ٢٠١٠، تمكن باحثون في مجال الأمن السيبراني من رصد أعطال غير اعتيادية في المعدات الصناعية، وتتبعوا مصدرها إلى برمجية (Stuxne)، الأمر الذي أثار قلق المجتمع الدولي بشأن القدرات التدميرية للأسلحة السيبرانية التي تطورها أو ترعاها الدول.(٥١)

وصف الأستاذ الاستاذ توماس ريد هجوم Stuxnet، حتى تاريخ اكتشافه، أكثر الهجمات السيبرانية المعروفة تطورًا وتعقيدًا. فقد كان هجومًا موجَّهًا بدقة نحو أهداف محددة، يُرجَّح أنها تمثلت في برنامج تخصيب اليورانيوم الإيراني في منشأة نطنز. وقد مثَّلت البرمجية الخبيثة (Worm) عملًا تخريبيًا سيبرانيًا مستقلًا (Cyber-enabled Stand-alone Sabotage)، إذ لم يكن مرتبطًا بأي عملية عسكرية تقليدية أو مصاحبًا لها. كما صُنِّف Stuxnet ضمن ما يُعرف في صناعة الأمن السيبراني بـ التهديدات المتقدمة والمستمرة (Advanced Persistent Threats - APTs)، وهي هجمات تتميز بدرجة عالية من التخطيط والتخفي والاستمرارية.(٥٢)

أعاد الأستاذ توماس ريد التأكيد على ان هذا الهجوم لا يندرج ضمن مفهوم الهجوم السيبراني أي تحت مفهوم الحرب السيبرانية، لأنه يعتبر الضرر المتمثل بالتعطيل لا يرتقي الى العنف المشار اليه عند تحديد مفهوم الهجوم في القانون الدولي الإنساني وفق المادة ٤٩ /١ من البروتكول الإضافي الأول.(٥٣)

علق خبراء دليل تالين على هذا الهجوم بالإشارة الى ان عملية Stuxnet التي نُفذت عام ٢٠١٠ تقدم مثالًا يوضح عدم استقرار وعدم حسم معيار العتبة اللازمة لاعتبار العملية السيبرانية "هجومًا مسلحًا". ففي ضوء الأضرار التي لحقت بأجهزة الطرد المركزي الإيرانية نتيجة تلك العملية، رأى بعض أعضاء الفريق الدولي للخبراء أن الهجوم بلغ عتبة الهجوم المسلح (Armed Attack)، ما لم يكن من الممكن تبريره استنادًا إلى حق الدفاع الشرعي الاستباقي (وفقًا للقاعدة ٧٣). وفي المقابل، تبنى خبراء آخرون الرأي المعاكس، معتبرين أن العملية لم ترقَ إلى مستوى الهجوم المسلح. ومع ذلك، وكما أوضح الدليل عند مناقشة القاعدة ٦٨، فقد اتفق جميع أعضاء الفريق على أن العملية تمثل استخدامًا للقوة (Use of Force).(٥٤)

من خلال ما تقدم يمكن بيان ان هجوم Stuxnet شكل انعطاف في موضوع الحرب السيبرانية باعتبار ان البرمجيات هنا استخدمت كسلاح في المعركة، وليس كما في الهجمات السابقة كوسيلة داعمة للعمليات العسكرية.*

رابعا- هجوم بيجر لبنان (٢٠٢٤) [٥٥]: مع توسع الصراع في الشرق الأوسط بعد الهجوم الأخير على لبنان، شهد العالم عصرًا جديدًا من الحروب حيث لم تعد الحرب تُخاض فقط بالجنود والدبابات، بل بأسلحة غير مرئية مثل الأسلحة السيبرانية. الحكومة اللبنانية تشك في أن الهجوم في جنوب لبنان ناتج عن هجوم سيبراني متطور ربما شنه الإسرائيليون. حيث أدى انفجار البيجرات إلى وفاة ما لا يقل عن تسعة أشخاص وإصابة أكثر من ٢٨٠٠ شخص. مثل هذه البيجرات تحولت إلى سلسلة من القنابل تستهدف كل من يحملها. حزب الله كان يستخدم أنظمة التواصل عبر البيجر منذ وقت طويل، لأنها كانت أكثر أمانًا ومحمية من تقنيات الاختراق الحديثة لتنسيق العمليات العسكرية. لم يكونوا يعلمون أن هذا النظام من التواصل سيصبح أسلحة تدميرية. يُفترض أن البيجرات التي كان يحملها مقاتلو حزب الله تم اختراقها عن بُعد، مما تسبب في تفجيرها، وهو ما أدى إلى وقوع ضحايا من المدنيين. لاحظ الخبراء تحولًا كبيرًا في الحروب في القرن الحادي والعشرين. مثل هذا الهجوم غير مرئي، لا يترك أثرًا ولا تعرف مرتكبيه.

قواعد القانون الدولي الإنساني تنطبق في هذه الحالة لأن الحرب المستمرة بين لبنان وإسرائيل لم تبدأ بتاريخ هجوم البيجر، بل بدأت كرد على الإبادة الجماعية التي ارتكبتها إسرائيل ضد المدنيين الفلسطينيين في غزة. هجوم البيجر يوضح مدى خطورة دمج الأدوات السيبرانية في الاستراتيجية العسكرية الحديثة. كما أن هجوم البيجر يعتبر دراسة حالة مهمة لأنه يقيم كيفية تطبيق القانون الدولي الإنساني على العمليات السيبرانية، بالإضافة إلى تناول التحديات المتعلقة بتطبيق القانون الدولي الإنساني، بما في ذلك التمييز بين الأهداف العسكرية والمدنية، والنسب، وصعوبة تصنيف هذه العملية كحق في الدفاع عن النفس أو استخدام للقوة.

المبحث الثاني: تطبيق مبدا التناسب في الهجمات السيبرانية

منذ كتاب تذكار سولفرينو لهنري الدونان الذي اظهر بشاعة الحروب وما تتركه من ويلات التي يكوى بنيرانها المدنيين، تلك الدعوة دفعت المجتمع الدولي للنهوض بمسؤوليته من خلال الدعوة الى إيجاد المنظومة القانونية التي تساهم في الحد من ويلات النزاعات المسلحة. فكانت اتفاقيات جنيف الأربع والبروتكولان الملحقان المظلة التي يستضل بها ضحايا النزاعات المسلحة، من خلال بلورة الالتزامات التي تقع على عاتق اطراف النزاع. ويبرز مبدا التناسب من بين المبادئ التي مست جوهر القانون الدولي الإنساني الا وهو توفير الحماية، الذي كرس اهم معادلة في القانون الدولي الإنساني الا وهي التوازن بين ما يسعى اليه اطراف النزاع من تحقيق الغلبة على الخصم وبين ان لا تكون تلك الرغبة سببا في الحاق الاضرار بالمدنيين والاعيان المدنية. انطلاقا من ذلك لابد لتلك القواعد ان تكون متوافقة مع أي متغيرات تشهدها ساحة النزاعات المسلحة.

المطلب الأول: مفهوم مبدا التناسب في القانون الدولي الانساني

التناسب هو واحد من المبادئ الأربعة المعترف بها بشكل واسع التي تحكم استخدام القوة بموجب قانون النزاع المسلح إلى جانب الضرورة والتمييز والمعاناة غير الضرورية، يوفر مبدأ التناسب قاعدة أساسية للنزاع المسلح المشروع التي يجب على العسكريين الالتزام بها إذا أرادوا التصرف بطريقة مسموحة.

مدونة ليبر لعام ١٨٦٣ هي أول محاولة لوضع قواعد القانون الدولي الإنساني الحديث للحرب البرية. تشير إلى حقيقة أن الإصابات والوفيات العرضية للمدنيين قد تكون نتيجة للأعمال العدائية. تنص المادة ١٥ على أنه "تسمح الضرورة العسكرية بكل التدمير المباشر للحياة والأعضاء للأعداء المسلحين، ولأشخاص آخرين يكون تدميرهم نتيجة حتمية غير مقصودة في النزاعات المسلحة." في المواد التالية، يتم تعريف مواطني الخصم أولاً كأعداء، وبذلك يُعتبر أنه من القانوني أن يتم "تعريضهم لصعوبات الحرب." ومع ذلك، تعترف المواد التالية بأنه "يتم الاعتراف بشكل متزايد بأن المواطن غير المسلح يجب حمايته في شخصه وممتلكاته وشرفه قدر الإمكان وفقًا لمقتضيات الحرب"، لكن هذا الحماية "كانت ولا تزال مع الشعوب غير المتحضرة، استثناءً.[٥٦]

أول اتفاقية دولية متعددة الأطراف تتعلق بطريقة تصرف الأطراف في نزاع مسلح على الأرض هي اتفاقية لاهاي لعام ١٨٩٩/١٩٠٧. بالرغم من عدم وجود قاعدة محددة حول التناسب في هذه الوثيقة، الا ان هناك عدد من الأحكام، خصوصاً المواد ٢٢-٢٨، التي تحتوي على أساس الأحكام الحالية السارية حول الاستهداف. وبالمقابل، تستند هذه الأحكام على المواد ١٢-١٨ من اعلان بروكسل ٢٧ اب ١٨٧٤ بشأن قوانين وأعراف الحرب.[٥٧]

التطور في الحروب الجوية ساهم بشكل مباشر في تطوير المبدأ حيث دفع الدول الى الاتفاق على وضع بعض القيود على الحروب الجوية، وتم دمج هذه القيود في... المادة ٢٥ من اتفاقية لاهاي لعام ١٩٠٧ بشأن الحرب البرية، من خلال إضافة عبارة "بأي وسيلة كانت" إلى النص الحالي الذي يحظر الهجوم أو القصف على المدن غير المحصنة. لذلك، لا يمكن أن يكون هناك شك في أن هذه المادة تنطبق أيضًا على الحروب الجوية.[٥٨]

بالإضافة إلى ذلك نصت المادة ٢ من الاتفاقية على أن القائد "لا يتحمل أي مسؤولية عن أي أضرار لا يمكن تجنبها قد ينجم عنها قصف" للمنشآت البحرية العسكرية والمدنية الموجودة في الموانئ والمدن غير المحمية، والتي قد تُستخدم لأغراض عسكرية. هناك إشارة مبكرة لقاعدة التناسب كما هي اليوم كذلك هذه الإشارة وردت في قواعد لاهاي للحرب الجوية لعام ١٩٢٣. حيث نصت المادة ٢٣ على: المنطقة القريبة مباشرة من عمليات القوات البرية، يكون قصف المدن والبلدات والقرى والمساكن والمباني مشروعًا، شريطة وجود افتراض معقول بأن التجمع العسكري مهم بما يكفي لتبرير القصف، مع مراعاة الخطر الذي قد يتعرض له السكان المدنيون).[٥٩]

تُذكر قاعدة القانون الإنساني الدولي المتعلقة بالتناسب في ثلاث مواد منفصلة لكنها مترابطة في البروتوكول الإضافي الأول: المواد ٥١ (٥) (ب)، و٥٧ (٢) (أ) (ثالثًا) و٥٧ (٢) (ب). بالإضافة إلى ذلك، تشير المادة ٨٥ (٣) (ب) إلى انتهاك قاعدة المادة ٥٧ (٢) (أ) (ثالثًا) كخرق جسيم إذا تم ارتكابه عن عمد وتسبب في وفاة أو إصابة خطيرة للجسم أو الصحة. خلال المؤتمر الدولي الذي أدى إلى اعتماد البروتوكول الإضافي الأول، "كان الرأي السائد على نطاق واسع أن هناك التزام إيجابي على المقاتلين بالتحقق من العلاقة بين الخسائر العرضية بين المدنيين والفائدة العسكرية المتوقعة، حيث سيؤدي ذلك الى توفير حماية متزايدة للمدنيين. [٦٠]

الفرق بين النصين هو أن قاعدة القانون الدولي الإنساني المتعلقة بالتناسب صيّغت كتحريم (في المادة ٥١ (٥) (ب) من البروتوكول الإضافي الأول) وكالتزام (في المادة ٥٧ (٢) (أ) (iii) من البروتوكول الإضافي الأول). ومع ذلك، لا يوجد فرق في المحتوى والمكونات بين القواعد الموجودة في النصين. هذا يتضح من أن صياغة المبدأ كما وردت في المادتين تم الاتفاق عليها خلال مناقشات المادة ٥٧ ومن ثم نُسخت إلى المادة ٥١. عمليًا، فإن الالتزامات الاحترازية الواردة في المادة ٥٧ تدعم الحظر العام في المادة ٥١ من خلال فرض التزامات على المهاجمين. ويمكن القول أيضًا أن المادة ٥٧ توضح عمليًا الالتزامات التي تفرضها المادة ٥١ وتحددها.

اكدت اللجنة الدولية للصليب الأحمر في دراساتها حول القواعد العرفية على تحويل مبدأ التناسب إلى قاعدة عرفية. فهو يعمل كقيد على الدول، ويشجعها على تبني أساليب ووسائل أكثر اعتدالاً، وفي بعض الحالات قد ينقذ حياة المدنيين الذين كان من الممكن أن يصبحوا «ضحايا عرضيين». علاوة على ذلك، فإن أي انتهاك لهذا المبدأ سيُعد جريمة حرب بموجب نظام روما الأساسي، الذي يوفر عقوبة المسؤولية الجنائية الفردية في حال انتهاك المبدأ.[٦١]

وجدت المحكمة الجنائية الدولية ليوغوسلافيا السابقة في قضية جاليك أنه عند تقييم التناسب، 'من الضروري فحص ما إذا كان الشخص المطلع بشكل معقول في ظروف الجاني الفعلي، وباستخدام معقول للمعلومات المتاحة له، يمكن أن يكون قد توقع وقوع خسائر مدنية مفرطة نتيجة الهجوم. في الواقع.[٦٢]

هناك فرق صغير في صياغة جريمة الحرب المتمثلة في انتهاك مبدا التناسب في القانون الإنساني الدولي كما وردت في نظام روما الأساسي للمحكمة الجنائية الدولية وبين الصياغة الموجودة في أحكام المعاهدات الأخرى. ينص الحظر في نظام روما الأساسي على أنه يُحظر خلال النزاع المسلح الدولي: "إطلاق هجوم عمدًا مع العلم أن هذا الهجوم سيسبب خسائر عرضية في الأرواح أو إصابات للمدنيين أو أضرار للأعيان المدنية... والتي ستكون واضحة الإفراط مقارنة بالمكسب العسكري المباشر المتوقع".[٦٣]

لقد دار جدل حول ما إذا كانت قاعدة القانون الدولي الإنساني المتعلقة بالتناسب كما هي منصوص عليها في البروتوكول الإضافي الأول مطابقة تمامًا لقاعدة التناسب التي يعترف بها القانون الدولي العرفي، أو ما إذا كان يجب أن تسود صياغة نظام روما الأساسي للمحكمة الجنائية الدولية. ويخلص روجرز إلى

أن صياغة المادة ٨، الفقرة ٢(ب)(رابعًا) من نظام روما الأساسي هي الصياغة الصحيحة لقاعدة القانون الدولي الإنساني المتعلقة بالتناسب، لأن هذه المادة «وُضعت مع أخذ الدول غير الأطراف في البروتوكول الأول بعين الاعتبار بشكل كبير وشاركت في المفاوضات وقد أخذ واضعي هذه المادة في الاعتبار التصريحات المختلفة الصادرة عند التصديق على البروتوكول الأول، ومن خلال اعتماد نهج وسط، حاولوا التوفيق بين متطلبات الضرورة العسكرية دون التخلي عن الإنسانية. وفقًا لدورمان، فإن الصياغة المختلفة في نظام روما الأساسي ناتجة عن شعور عام خلال مفاوضات نظام روما الأساسي بأن صياغة النص كما تم تضمينه في ذلك النظام الأساسي، كانت حالة الأمور في القانون الدولي العرفي في ذلك الوقت. ومع ذلك، يشير مكورمك ومشارو إلى أن إضافة كلمة "بوضوح" تعتبر "متطلبًا إضافيًا" لمنع الهجمات غير المتناسبة لكي تُشكل جريمة حرب بموجب نظام روما الأساسي للمحكمة الجنائية الدولية. تُناقش مسألة ما إذا كان يجب اعتبار صفة 'بوضوح' جزءًا من قاعدة التناسب في القانون الإنساني الدولي في الفصل.[٦٤]

يوجه احد الفقهاء Karen Koechانتقادا لتقنين المبدأ في القوانين التي ترسخ مبدأ التناسب، أي البروتوكول الإضافي الأول من اتفاقية جنيف ونظام روما للمحكمة الجنائية الدولية، تواجه بعض النواقص التي تؤثر على تطبيقها. أولًا، البروتوكول يحكم النزاعات المسلحة الدولية فقط، مما يخلق فجوة في تطبيق المبدأ في النزاعات المسلحة غير الدولية لأنه لا يوجد معاهدة تحكمها. ثانيًا، من المثير للاهتمام أن القوى العسكرية الكبرى في العالم ليست من الموقعين على هذه المعاهدات، وتشمل الصين والهند والولايات المتحدة وروسيا من بين آخرين. لذلك، هاتان المعاهدتان لا تغطيان نطاقًا كافيًا لضمان تنفيذ مبدأ التناسب في القانون الإنساني الدولي.

فيما يتعلق بالسؤال عن نوع التأثيرات الناتجة عن الهجوم التي يجب أخذها في الاعتبار وفقًا لمبدأ التناسب، هناك رأيان رئيسيان يمكن طرحهما: (أ) أن التناسب يقتصر فقط على التأثيرات المباشرة للهجوم؛ (ب) أن التأثيرات غير المباشرة للهجمات يجب أن تؤخذ بعين الاعتبار أيضًا، لأنه إذا كانت النية تقتصر على التأثيرات المباشرة فقط، كان من الممكن أن تتضمن القاعدة كلمة "مباشر" (كما هو الحال بالنسبة للميزة العسكرية). لذلك، فإن الرأي السائد هو أنه يجب أيضًا أخذ التأثيرات غير المباشرة في الاعتبار إلى جانب التأثيرات المباشرة. والسؤال التالي الذي يطرح نفسه نتيجة لهذا الاستنتاج هو أين وكيف يتم تحديد الحدود بين التأثيرات غير المباشرة التي تعتبر ذات صلة لأغراض مبدأ التناسب وتلك التي تعتبر بعيدة جدًا، إن وجدت.[٦٥]

حيث يجب أخذ التأثيرات المباشرة للهجوم في الاعتبار كجزء من الضرر الجانبي الذي ينبغي النظر فيه عند تحليل التناسب. على سبيل المثال، إذا تم استخدام سلاح متفجر، فإنه عادة ما يسبب انفجارًا، وتفتتًا، وتأثيرات حرارية، وحفرية واختراقية. فيما يتعلق بتأثيرات الهجوم على السكان المدنيين، يمكن التفكير في الوفاة، والإصابة الجسدية الناتجة عن موجة الانفجار، أو شظايا السلاح أو التفتت الثانوي (مثل شظايا الزجاج الناتجة عن موجة الانفجار)، أو الحروق، أو انهيار المباني وتضرر المركبات. [٦٦]

اما التأثيرات غير مباشرة على السكان المدنيين، أو ما يعرف بـ "التأثيرات المترددة" (ويشار إليها أيضًا باسم "تأثيرات متتابعة"), تم تعريفها بأنها "التأثيرات التي لا تسببها الهجوم مباشرة أو على الفور، لكنها مع ذلك تؤثر بشكل خاص على العواقب الطويلة الأمد له، على سبيل المثال، العواقب الطويلة الأمد للبنية التحتية المدنية الأساسية المتضررة. قد يشمل ذلك تأثيرات على نظام الرعاية الصحية ومستوى النظافة الذي يستطيع السكان المدنيون الحفاظ عليه خلال الأعمال العدائية وبعد انتهائها. [٦٧]

بالنسبة للنظر في التأثيرات غير المباشرة لهجوم ما لأغراض مبدأ التناسب، السؤال الرئيسي الذي قد يُطرح هو ما إذا كانت المسألة تتعلق بمدى البعد الفعلي للضرر العرضي غير المباشر (جغرافياً أو زمنياً) عن الهجوم الأصلي (الموقع)، أم أنها مسألة توقع مسبق للأحداث. وافق الأمين العام على أن قابلية التوقع هي المعيار ذي الصلة، وأنه بناءً عليه هناك التزام بأخذ جميع الأضرار غير المباشرة التي يمكن توقعها بشكل معقول من قبل شخص مطلع بشكل معقول في الاعتبار. كما ورد في قضية جاليتش لدى محكمة الجنايات الدولية ليوغوسلافيا السابقة، فإن ذلك يتطلب أيضًا أن "الشخص المطلع بشكل معقول في ظروف الجاني الفعلي، باستخدام المعطيات المتاحة له بشكل معقول، كان من الممكن أن يتوقع وقوع خسائر مدنية مفرطة نتيجة الهجوم". بالإضافة إلى ذلك، "يجب أن تأتي المعلومات اللازمة للوصول إلى تقييم لأغراض مبدأ التناسب من جميع المصادر المتاحة في الوقت ذي الصلة." من هذا يمكن الاستنتاج أن التأثيرات المترددة التي يصعب توقعها لا يلزم أخذها في الاعتبار.[٦٨]

مع ذلك، لا يوجد في القانون الدولي الإنساني أساس لفرض حد زمني معين (مطلق) على تلك التأثيرات غير المباشرة التي يجب أخذها في الاعتبار. تشير العديد من الأدلة العسكرية وبيانات الدول إلى أنه يجب أيضًا أخذ التأثيرات طويلة الأمد، أي التأثيرات غير المباشرة التي تحدث بعد وقت طويل من الهجوم الفعلي، في الاعتبار طالما كان من الممكن توقعها بشكل معقول.[٦٩]

تطبيق مبدأ التناسب في قوانين الحرب يعاني من الغموض وعدم الفاعلية، حيث لا توجد طريقة واضحة تم وضعها لأخذ المعنى الحاسم للضرر العرضي المتناسب أو 'المفرط' بعين الاعتبار. بالإضافة إلى ذلك، كما تم الإشارة أعلاه، فإن تدوين المبدأ في الصكوك الدولية غير كافٍ بالنظر إلى مركزية المبدأ في تنظيم الحروب الحديثة. لا يوجد إجابة واضحة على السؤال: 'ما الذي يعتبر متناسبًا؟' ومن المفارقات أن هذين المعاهدتين يزيدان من تعقيد هذا اللغز. هذا الوضع يمثل مأزقًا في تحديد ما إذا كان تحقيق مكسب عسكري معين يوازن مع الضرر الذي يُلحق بالسكان المدنيين أم لا. وقد اعترف أكاديميون مثل شميت بهذه الصعوبة من خلال تأكيدهم أن هذا المبدأ هو أكثر قاعدة يصعب تطبيقها بموجب قوانين النزاع المسلح.

يثير مبدا التناسب عدة إشكاليات قانونية عند التطبيق، ويعزو الفقهاء السبب الى عدم وضوح المبدأ في الوثائق القانونية التي تضمنها أدى الى مثل هذه الإشكاليات.

من تلك الإشكاليات العلاقة بين مبدا التناسب والدروع البشرية، أي ما مدى إمكانية تطبيق المبدأ في مثل هذه الحالة.

مبدأ التناسب، كما مر بنا، يعتبر غامضًا بعض الشيء السؤال هنا، ما هو التأثير الفعلي للدروع البشرية على مبدأ التناسب؟ هناك ثلاث مقاربات تم اقتراحها في الأوساط الأكاديمية. النموذج التعاقدي يمنح القادة العسكريين أكبر قدر من الحرية لاستخدام تقديرهم، بحجة أن الدروع البشرية يجب تجاهلها عند النظر في التناسب. النموذج التوافقي يرى أنه رغم أنه يجب أخذ الدروع البشرية في الاعتبار عند حساب التناسب، يمكن خصم قيمتها، وبالتالي يسمح بحدوث أضرار جانبية أكبر في الحالات التي تُستخدم فيها الدروع البشرية. وأخيرًا، نموذج حقوق الإنسان هو الأقسى، حيث يدعي أن كون المدنيين دروعًا بشرية ليس له أي صلة قانونية بالنظر في التناسب ويجب احتسابهم بالكامل عند اتخاذ قرارات الاستهداف.(٧٠)

بموجب النموذج التعاقدي، يتم تجاهل الدروع البشرية من اعتبارات التناسب بالكامل. الحجة الأساسية تقول إن المدافع لا يجب أن يُسمح له بالاستفادة من انتهاكاته لقانون النزاع المسلح، وبالتالي لا يجب السماح بدور الدروع البشرية في ردع الهجمات على الأهداف العسكرية الشرعية. (٧١)

محاولات تجاهل استخدام المدنيين كدروع بشرية بشكل كامل عند النظر في التناسب ليست مقنعة. هذا النهج يتجاهل إلى حد كبير الهدف الرئيسي لقانون النزاعات المسلحة، وهو تقليل المعاناة غير الضرورية للمدنيين وحماية غير المقاتلين. وتظهر الحجج المؤيدة للنموذج التعاقدي أكثر من محاولات إنكار المزايا التي يحصل عليها الطرف الأضعف بشكل غير متكافئ من الدروع البشرية، وبطريقة ما، جعل القتال أكثر عدلاً. أي حماية طويلة الأمد قد يحصل عليها المدنيون من رفض منح ميزة عسكرية عبر الدروع البشرية هي إلى حد كبير افتراضية وقابلة للشك على أفضل تقدير، مما يجعلها مبرر قابل للجدل للغاية. ولا يمكن اعتبار الدروع البشرية الطوعية مشاركين مباشرين في الأعمال العدائية، لسبب بسيط وهو أنهم لا يقدمون أي ميزة عسكرية فعلية وحقيقية بمجرد تواجدهم كدروع. حتى لو قبلنا بالحجة بأن القيود القانونية أو التوقف الأخلاقي قبل الهجوم على أهداف محمية بالدروع ستشكل... ميزة عسكرية فعلية وحقيقية، بمجرد أن يشارك الرهائن البشريون مباشرة في الأعمال العدائية وبالتالي يفقدون وضعهم المحمي، فلن يقدموا بعد ذلك مثل هذه الميزة العسكرية.(٧٢)

العلاقة بين مبدا التناسب والدروع البشرية وفق ما اشير اليه أعلاه، الذي ميزت المناقشات بين الدروع البشرية الطوعية والدروع البشرية غير الطوعية، حيث حاولت التفسيرات في كلا الحالتين افراغ الحماية وفق المبدأ للمشاركين في هذه الدروع، وعدم الاكتراث بالأضرار التي تلحق بهم مبررين ذلك بحجج، تمثلت فيما يتعلق بالدروع البشرية غير الطوعية ان سماح الخصم بوضع الافراد كدروع بشرية هو بمثابة انتهاك للقانون الدولي الإنساني المتمثل بالتزام اطراف النزاع بأبعاد المدنيين من المواقع العسكرية او تلك التي تستخدم لأغراض عسكرية، وبالتالي فان السماح بذلك من شانه تشجيع اطراف النزاع على الانتهاك، وهنا يمكن مواجهة هذا الانتهاك. وهذا غير سليم لان القول بذلك معناه الاخذ بمبدأ التعامل بالمثل وهذا ما تجيزه اتفاقيات جنيف الاربع اذ انها لم تسمح باعتماد قاعدة المقابلة بالمثل.

اما الحجة الخاصة بالدروع البشرية الطوعية، التي تنطلق من فقدان المدنيين للحماية لمشاركتهم في العمل العدائي، حيث ان الدرع البشري الطوعي يمثل مشاركة الافراد المكونين له بعمل عدائي وهذا غير منسجم مع مفهوم المشاركة المباشرة التي تشترط ان تكون المشاركة إيجابية أي ان المدنيين الذي يشارك في العمل العدائي، ان يصدر منه عمل عدائي هجومي او دفاعي يلحق ضررا ماديا بالخصم، في حين ان وجود الدروع البشرية الطوعية يمثل نشاط سلبي وليس إيجابي وهنا يخرج من منظور المشاركة المباشرة في العمليات العدائية. وعليه فان استبعاد الدروع البشرية من نطاق مبدا التناسب، يخالف جوهر القانون الدولي الإنساني.

المطلب الثاني: تطبيق مبدا التناسب في الهجمات السيبرانية

مبدئيًا، من المهم أن نتذكر أن المدنيين لا يمكن أبدًا أن يكونوا هدفًا للهجوم، وأن مبدأ التناسب يقيّد القادة عندما يكون من المحتمل أن يتضرر المدنيون أو الأهداف المدنية نتيجة لهجوم قانوني. ولكي يكون هذا الهجوم قانونيًا، يجب على القائد أن يحدد أن الوفاة أو الإصابة أو الضرر ليست "مبالغًا فيها بالمقارنة مع الميزة العسكرية المباشرة والملموسة المتوقعة". وعلى الرغم من أن الهجمات الإلكترونية سيكون لها القدرة على قتل أو إصابة المدنيين، إلا أن الغالبية العظمى من العمليات الإلكترونية المعروفة ركّزت على أو أدت إلى الضرر، ومن هنا يتركّز الاهتمام على عنصر الضرر في المعيار القانوني.[٧٣]

في الهجمات السيبرانية، السؤال الرئيسي حول مدى نجاح مبدأ التناسب في حماية السكان المدنيين سيعتمد بشكل كبير على ما تعنيه المصطلحات المحددة داخل المبدأ وكيف يتم تطبيقها على تلك الهجمات. على سبيل المثال، مصطلح 'الهدف' لغرض تحليل التناسب له نفس معنى 'الهدف' في تحليل التمييز. وبالتالي، فإن مبدأ التناسب، مرة أخرى، يعاني من فجوة كبيرة فيما يتعلق بالبيانات. لأن 'أهمية البيانات عادة ما تتجاوز أهميتها المادية. قد يدفع القائد لاختيار هجوم إلكتروني قد يؤدي إلى أضرار جانبية تدمر تيرابايتات من البيانات بما في ذلك السجلات الطبية وقطع بيانات مدنية أخرى مهمة، افضل من توجيه ضربة تقليدية من المتوقع أن تؤدي، على سبيل المثال، إلى ثلاث حالات وفاة مدنية كأضرار جانبية. بالمثل، تحديد ما يشكل 'الضرر' في الفضاء السيبراني سيكون مفتاحاً لتحديد الحماية الكافية. على سبيل المثال، قد يؤدي الهجوم السيبراني إلى مجموعة من النتائج تتراوح من فقدان مؤقت لوظائف الأنظمة الرقمية، مما يؤدي إلى التسبب في أضرار مادية وتدمير. تحديد أي من هذه النتائج تشكل 'ضررًا' لغرض القانون الدولي الإنساني هو شرط أساسي لمعرفة ما إذا كانت الإصابة أو الأضرار مفرطة بالنسبة للميزة العسكرية المباشرة والملموسة المتوقعة. علاوة على ذلك، نظرًا لأن المبدأ 'مصاغ بلغة التوقع والاستباقية'، فإن القدرة على تقييم الأضرار الجانبية المتوقعة من المهم للغاية الحماية من الهجمات السيبرانية.[٧٤]

قلة هم من قد يجادلون بأن مبدأ التناسب لا ينطبق على الحرب السيبرانية؛ بل يتمحور الجدل حول تطبيقه على العمليات السيبرانية المحددة. هناك جانبان محددان من القاعدة يستحقان تحليلًا أكثر تفصيلاً: فهم "الضرر" ومشكلة التأثيرات غير المباشرة، يجب فهم شرط حدوث الضرر للأشياء المدنية

بشكل أوسع في الهجمات السيبرانية حيث ان الغالبية العظمى من الإنترنت، بما في ذلك الكابلات والخوادم وأجهزة التوجيه، تتكون من أشياء مدنية، وهي مملوكة أو تُدار أو تُصان بواسطة المدنيين. أي ضرر لهذه العناصر من بنية الإنترنت التحتية سيُعتبر ضررًا مدنيًا وفق مفهوم مبدا التناسب.(٧٥)

مسألة تعريف الضرر أقل جدلاً في الهجمات التقليدية. ومع ذلك، عندما يتم اللجوء للأساليب السيبرانية لشن هجوم، يصبح عندها تحديد أي من تلك الأفعال الإلكترونية تُعَدُّ ضرراً أكثر إشكالية. هناك عدة طرق لتحديد ما يُعادل الضرر في المجال الإلكتروني. أحد هذه الطرق هو المقارنة بالهجوم التقليدي من خلال القول إنه إذا كان ما يحدث من عملية إلكترونية كان سيُعتبر ضرراً إذا تم بواسطة وسائل تقليدية، فإن الهجوم يُعَدُّ ضرراً.(76)

قد يكون تقييم التأثيرات غير المباشرة في الحرب الإلكترونية أحد أصعب المواضيع عند تطبيق مبدأ التناسب. من الواضح أن القائد يجب أن يأخذ في الاعتبار التأثيرات المباشرة لهجومه السيبراني. يتم تعريف هذه التأثيرات المباشرة على أنها "العواقب الفورية من الدرجة الأولى، غير المتأثرة بالأحداث أو الآليات الوسيطة". في مجال السيبراني، يشمل هذا التأثيرات على جهاز الكمبيوتر الذي تم إيقاف تشغيله بسبب هجوم سيبراني.(٧٧)

حتى في الحالات المذكورة أعلاه، لكي يُعتبر الضرر ضمن تحليل التناسب، يجب أن يكون متوقعًا. التأثيرات غير المباشرة التي لم يكن من المتوقع أن تكون مفرطة لا تُؤخذ في التحليل. بمعنى آخر، هذا المعيار لا يتوقع أن يأتي المراجع بعد الواقعة ويقيّم مدى معقولية قرار القائد بشأن فرط التأثيرات غير المباشرة. بل يجب على أي مراجع تقييم مدى معقولية قرار القائد بناءً على ما كان القائد يتوقعه بشكل معقول من التأثيرات، بناءً على المعلومات التي كانت لديه في ذلك الوقت.(٧٨)

اثارت الأنظمة ذا الاستخدام المزدوج عدة مشكلات كما هو الحال عند تطبيق مبدا التمييز كما سبق وان بينا بانها شكلت عائقا امام التميز بين كونها هدف عسكري ام عين مدنية. فعلى الرغم من أن الأنظمة ذات الاستخدام المزدوج ليست محصنة من الهجمات السيبرانية، إلا أن أغراضها المتعددة تخلق مشكلتين مميزتين ضمن تحليل التناسبية. أولاً، الهجوم على أنظمة ذات استخدام مزدوج يزيد من احتمال أن يكون الضرر الجانبي المفترض المحسوب في اختبار التناسبية هائلاً بشكل لا يمكن تحمله عند موازنته مع الميزة العسكرية المتوقعة. ثانياً، هجوم على نظام ذو استخدام مزدوج يتطلب التعامل مع المهمة الصعبة — وغالبًا المستحيلة — في التمييز بين الأجزاء المدنية والأجزاء العسكرية في نظام ذو استخدام مزدوج.(٧٩)

وتشمل الأنظمة ذات الاستخدام المزدوج محطات الطاقة التي تزود الكهرباء لكل من المستخدمين المدنيين والعسكريين، وأنظمة مراقبة الحركة الجوية التي تخدم كل من الطائرات المدنية والعسكرية، وشبكات الاتصالات التي يعمل عليها كل من المستخدمين المدنيين والعسكريين. هذه الأنظمة شائعة نسبيًا خارج مجال الفضاء السيبراني، وأكثر شيوعًا بداخله. نظام تحديد المواقع العالمي (GPS) هو نظام تم إنشاؤه لخدمة الأغراض العسكرية، وكان في الأصل يخدم المستخدمين العسكريين فقط، على الرغم من أنه تم تطويره مؤخرًا ودمجه في الأجهزة المدنية إلى حد أن التكنولوجيا أصبحت شائعة تقريبًا في كل مكان.(٨٠)

الاستخدامات المدنية لمثل هذه الأنظمة قد تؤثر على تحليل التناسب، إلا أن الاستخدام المدني لا يمنع النظام مزدوج الاستخدام من أن يكون هدفًا قانونيًا لهجوم إلكتروني. ومع ذلك، يجب توافر شرطين قبل أن يمكن اعتبار النظام مزدوج الاستخدام هدفًا عسكريًا مشروعًا: يجب أن يساهم الهدف نفسه في العمليات العسكرية للعدو، ويجب أن يؤدي تدمير الهدف إلى تحقيق ميزة عسكرية ملموسة. علاوة على ذلك، يجب أن يمر الهجوم على نظام مزدوج الاستخدام أيضًا باختبار التناسب. ومع ذلك، على عكس حالة الأنظمة المدنية البحتة، بمجرد أن يستوفي النظام مزدوج الاستخدام هذه المتطلبات، يمكن استهدافه ومهاجمته بشكل قانوني.(٨١)

نظرًا لطبيعة انتشار الأنظمة ذات الاستخدام المزدوج في عالم التكنولوجيا السيبرانية، سيكون للهجمات السيبرانية تأثير أكبر على البنية التحتية المدنية مقارنةً بالهجمات التقليدية المماثلة. زيادة التأثير على البنية التحتية المدنية تقلل من احتمالية أن تكون الميزة العسكرية المتوقعة من مثل هذا الهجوم أكبر من الضرر الجانبي المتوقع. بكلمات أخرى، زيادة الضرر الجانبي الناتج عن انتشار الأنظمة ذات الاستخدام المزدوج تجعل من الصعب على الهجوم السيبراني المقترح اجتياز اختبار التناسب. كما أن انتشار الأنظمة ذات الاستخدام المزدوج سيعيق القدرة على التمييز بين البنية التحتية السيبرانية العسكرية والمدنية. من المحتمل أن يواجه القادة العسكريون سيناريوهات لا يستطيعون فيها تحديد الفرق بين البنية التحتية المدنية وتلك العسكرية. علاوة على ذلك، غالبًا لن يتمكن القادة من إجراء حساب كامل للتناسب بسبب عدم قدرتهم على تحديد التأثير الذي سيحدثه هجومهم على البنية التحتية المدنية.(٨٢)

علاوة على احتمال زيادة الضرر الجانبي بالقياس الى الميزة العسكرية تظهر صعوبات في التمييز بين البنية التحتية المدنية والعسكرية بسبب انتشار الأنظمة ذات الاستخدام المزدوج. هذا يؤدي إلى مشكلة من جزأين. أولاً، قد لا يتمكن القادة العسكريون من التمييز بين البنية التحتية نفسها. ثانياً، قد لا يكونون قادرين على معرفة الأثر الذي ستتركه هجماتهم على البنية التحتية المدنية ليتمكنوا من إجراء حساب متكامل للتناسب. حيث ان تمييز البنية التحتية العسكرية عن المدنية أمر بالغ الأهمية لمراجعة التناسب بشكل كامل.(٨٣)

الواضح من نصوص الأحكام ذات الصلة بالبروتوكول الإضافي الأول أنه يجب احتساب الضرر الجانبي المتوقع فقط في تقييم التناسب. أما الضرر العرضي الذي لا يُحتمل، أو قد يحدث، أو مؤكد، وبالتالي يكون مجرد احتمال فقط، فهو مستبعد من معادلة التناسب. يدعم ذلك الأعمال التحضيرية للبروتوكول الإضافي الأول، حيث تكشف مناقشات اللجنة عند النظر في إدراج عبارة "التي قد تسبب" ضررًا عرضيًا، الأمر الذي كان سيتطلب من القادة أخذ جميع الاحتمالات للضرر الجانبي الناتج في الاعتبار. ومع ذلك، فإن اعتماد عبارة "التي يُتوقع أن تسبب" في النهاية يشير إلى نية الأطراف لاستبعاد تلك الآثار الجانبية العرضية التي تكون تخمينية من تقييم التناسب.(٨٤)

ولتوضيح الفرق بين الأضرار الجانبية المتوقعة والأضرار الجانبية التي لا تتعدى كونها افتراضية، بالعودة الى المثال السابق* عن التدمير العرضي للبنية التحتية المائية الحيوية. أي ضرر مادي للبنية التحتية المائية هو تأثير مباشر للهجوم وإذا تم تصنيف البنية التحتية على أنها منشأة مدنية، فإن الضرر المتوقع سيتم أخذه في الحسابات المتعلقة بالتناسب. بغض النظر عما إذا كانت البنية التحتية المائية منشأة مدنية أو هدفًا عسكريًا، فإن التدمير الناتج يمكن أن يؤثر بشكل غير مباشر على السكان المدنيين. يجب على القائد العسكري أخذ التأثيرات غير المباشرة على سكان المدينة المدنيين الناتجة عن الهجوم في الاعتبار، أي الوفيات والإصابات بين المدنيين نتيجة انقطاع إمدادات المياه. ومع ذلك، يتم أخذ حالات الوفاة أو الإصابات المتوقعة بين المدنيين فقط بعين الاعتبار في تقييم التناسب.(٨٥)

إذا كان لدى القائد العسكري معلومات تشير إلى أن المدنيين لديهم وصول إلى إمدادات كافية من المياه المعبأة أثناء إصلاح البنية التحتية المائية، فلن يتوقع القائد أي ضرر غير مباشر للسكان المدنيين. يتم استبعاد الضرر غير المباشر من تقييم التناسب عندما يمكن توقع بشكل معقول أن يتم تجنب هذا الضرر نتيجة اتخاذ إجراءات تصحيحية. (٨٦)

أشار الخبراء الذين ساهموا في اعداد دليل تالين الى مبدا التناسب وعلاقته بالأضرار الجانبية في القاعدة ١١٣.

كما ورد في القاعدتين ٩٤ والتي تنص على (السكان المدنيون ككل، وكذلك المدنيون الفرديون، لا يجب أن يكونوا هدفًا للهجوم السيبراني.) و ٩٩والتي تنص على (لا يجب أن تكون الأهداف المدنية هدفًا للهجمات الإلكترونية. يمكن استهداف البنية التحتية السيبرانية فقط إذا كانت تُعتبر هدفًا عسكريًا) من دليل تالين، من غير القانوني جعل المدنيين أو الأشياء المدنية هدفًا للهجوم الإلكتروني. بالمقابل، تتعامل هذه القاعدة مع الحالات التي يتعرض فيها المدنيون أو الأشياء المدنية للضرر بشكل عرضي، أي أنهم ليسوا هدف الهجوم المقصود. غالبًا ما يُطلق على الوفاة العرضية للمدنيين، أو إصابتهم، أو الضرر أو تدمير الأشياء المدنية، مصطلح 'الضرر الجانبي'. وكما توضح هذه القاعدة، فإن تعرض المدنيين أو الأشياء المدنية للضرر أثناء هجوم إلكتروني على هدف عسكري قانوني لا يجعل هذا الهجوم غير قانوني بالضرورة. بدلاً من ذلك، تعتمد قانونية الهجوم الذي ينتج عنه ضرر جانبي على العلاقة بين الضرر الذي يتوقع المهاجم بشكل معقول أن يلحق بالمدنيين والأشياء المدنية والميزة العسكرية التي يتوقع المهاجم الحصول عليها نتيجة الهجوم.(٨٧)

حيث تنص هذه القاعدة (١١٣) على حالة يكون فيها الهجوم الإلكتروني على هدف عسكري ينتج عنه ضررًا للأهداف المدنية، بما في ذلك أجهزة الكمبيوتر والشبكات أو غيرها من البُنى التحتية الإلكترونية، أو للأشخاص المدنيين، والذي لا يمكن تجنبه وفقًا للقواعد ١١٤–و١٢٠وهي المتعلقة بأخذ الاحتياطات في الهجوم، ومن الجدير بالذكر في هذا الصدد أن الهجمات الإلكترونية على الأهداف العسكرية تُشن أحيانًا عبر كابلات الاتصالات المدنية أو الأقمار الصناعية أو غيرها من البُنى التحتية.

وعندما يحدث هذا، قد تلحق الهجمات ضررًا بهذه البنية التحتية. بعبارة أخرى، يمكن للهجوم الإلكتروني أن يتسبب في أضرار جانبية سواء أثناء الانتقال أو بسبب الهجوم نفسه. ومن المهم أخذ كلا النوعين من الأضرار الجانبية في الاعتبار عند تطبيق هذه القاعدة.(٨٨)

في بعض الأحيان قد تتسبب العمليات الإلكترونية في الإزعاج أو الانزعاج أو التوتر أو الخوف. هذه العواقب لا تُعتبر ضررًا جانبيًا لأنها لا تُعد 'خسارة عرضية لحياة المدنيين أو إصابة المدنيين أو تلف الممتلكات المدنية' ولا يجب أخذها في الاعتبار عند تطبيق هذه القاعدة. وقد اتفق الفريق الدولي من الخبراء على أن مفهوم 'الضرر للممتلكات المدنية' قد يشمل، في ظروف معينة، الحرمان من الوظائف، وعندما يكون هذا هو الحال، يجب مراعاته في تقييم التناسب.

ويحدد الدليل الأضرار التي تُصنَّف كأضرار جانبية لأغراضه. فالتأثيرات، إذا كانت متوقعة أو كان يجب توقعها، يجب أخذها في الاعتبار عند تحليل التناسب. على النقيض من ذلك، إذا تم نقل البرمجيات الخبيثة بشكل غير متوقع أو بشكل لا يمكن توقعه عبر، على سبيل المثال، جهاز تخزين محمول إلى أنظمة مدنية، فإن العواقب الناتجة لن تُؤخذ بعين الاعتبار عند تقييم الامتثال لهذه القاعدة.(٨٩)

يتفق الخبراء ان الضرر الجانبي في الهجمات السيبرانية يأخذ نفس المفهوم في اطار الهجمات التقليدية، بمعنى ان تقييم الضرر الجانبي يقاس بمدى التناسب بين حدوث الضرر والميزة العسكرية حيث ان الخبراء يفسرون تلك الميزة بالقول (عند تحديد الميزة العسكرية الملموسة والمباشرة المتوقعة، يُعتبر من المقبول عمومًا وفقًا للقانون الدولي العرفي أن 'الميزة العسكرية المتوقعة من الهجوم يُراد بها الإشارة إلى الميزة المتوقعة من الهجوم بشكل كامل وليس فقط من أجزاء معينة أو منفصلة من الهجوم'. على سبيل المثال، قد يتم تنفيذ عملية إلكترونية بالتزامن مع شكل آخر من أشكال العمل العسكري، مثل هجوم إلكتروني على رادار دفاع جوي لمنشأة ما أثناء الغارات التقليدية على تلك المنشأة. في هذه الحالة، الميزة العسكرية الملموسة والمباشرة التي يجب النظر فيها بالنسبة للهجوم الإلكتروني ستكون تلك المتوقعة من الهجوم بأكمله، وليس فقط التأثير على الدفاعات الجوية. وبالمثل، قد يُخطط لهجوم إلكتروني واحد لإقناع العدو بأن مجموعة أهداف معينة ستكون محور الهجمات القادمة، مما يدفع العدو إلى توجيه تدابيره الدفاعية بشكل خاطئ. بينما يكون التركيز الفعلي للهجوم الرئيسي في مكان آخر. يجب تقييم أي أضرار جانبية متوقعة من الهجوم الإلكتروني الأول في ضوء الميزة العسكرية المتوقعة التي ساهمت بها العملية في الهـــجوم الرئيسي).(٩٠)

ضمن النقاشات التي جرت بين الخبراء اثر نقاش حول ما إذا كان عدم اليقين فيما يتعلق بالأضرار الجانبية يؤثر على تطبيق القاعدة وإلى أي مدى. هذه القضية لها أهمية خاصة في سياق الهجمات السيبرانية، حيث أنه في بعض الأحيان يكون من الصعب للغاية تحديد الأضرار الجانبية المحتملة بشكل موثوق مسبقًا. القلة من الخبراء اعتبر أنّه كلما انخفض احتمال حدوث أضرار جانبية، كلما قلّت الميزة العسكرية اللازمة لتبرير العملية من خلال تطبيق قاعدة التناسب. أما الغالبية منهم الخبراء فقد رفضت هذا

النهج على أساس أنه بمجرد توقع حدوث أضرار جانبية، يجب حسابها ضمن تحليل التناسب كما هي؛ ولا يكون من المناسب اعتبار درجة اليقين بالنسبة للأضرار الجانبية المحتملة. فالمهاجم إما يتوقعها بشكل معقول، أو أن احتمال حدوثها مجرد تخمين، وفي هذه الحالة لن يُؤخذ في الاعتبار عند تقييم التناسب.(٩١)

لاحظ الخبراء الذين ساهموا في دليل تالين أنه، في بعض الحالات، قد يشكل فقدان الوظائف، كما نوقش سابقًا فيما يتعلق بالهجمات، ضررًا للأشياء المدنية. على سبيل المثال، اتفق غالبية الخبراء على أن تعطّل الوظائف الذي يتطلب استبدال مكونات مادية يشكل هجومًا، وفي سياق التناسب، سيكون ضررًا جانبيا إذا وقع على شيء مدني. ومع ذلك، اختلف نفس الخبراء حول ما إذا كانت إعادة تثبيت نظام تشغيل تعد تعطّلًا كافيًا في الوظائف لتعتبر "ضررًا" عند تحديد ما إذا كانت العملية هجومًا. إدراج هذا التفسير في تحليل التناسب يوضح أنه لا يزال غير واضح ما إذا كان التعطّل الوظيفي الذي يتطلب إعادة تثبيت كبيرة للبرمجيات يعتبر "ضررًا" لغرض تقييم الضرر الجانبي. (٩٢)

مبدأ التناسب ليس محددًا بصراحة داخل المعاهدات الإنسانية الدولية كمصطلح رئيسي، بل يستفيد من التفسير القضائي النقدي. كلا اتفاقيتي جنيف وبروتوكولاتها الإضافية توفر ضمناً لمبدأ التناسب لكنها ليست بمعنى صريح. الأسباب وراء عدم توفير مثل هذا المعنى بصراحة يمكن أن تكون بشكل رئيسي لأنه لا يوجد وضوح. (٩٣)

الحدود فيما يتعلق بما ينطوي عليه المبدأ. لا يوجد إجماع دولي على معنى المبدأ أو نطاقه وتوقعاته. لكل سلطة معناها الخاص وبناءً عليه، يكون تطبيق المبدأ قضية حسب الحالة اعتمادًا على المناسبة. إن عدم تعريف مبدأ التناسب صراحةً في المعاهدات الإنسانية الدولية تسبب ببعض التحديات لكل من الأكاديميين والقادة العسكريين في شرح وتطبيق مبدأ التناسب. كان القادة العسكريون يعرفون مبدأ التناسب بما يخدم مصالحهم لتلبية رغباتهم العسكرية كما ورد في قضية مجلس قرية بيت سوريك ضد حكومة إسرائيل، حيث يجب على القائد العسكري الحفاظ على التناسب أثناء الهجوم العسكري. في هذا السياق، من المحتمل انتهاك مبدأ التناسب مما قد يؤدي إلى خسائر بين المدنيين والأعيان المدنية. أيضًا، قام بعض الأكاديميين بتفسير مبدأ التناسب وفق فهمهم الخاص، وهذا أدى إلى وجود بعض التناقضات بينهم بسبب غياب الإجماع.(٩٤)

تفسير غير واضح لمعنى أو تطبيق مبدأ التناسب يميل إلى خلق انتهاك جسيم للقانون وخصوصاً القانون الإنساني الدولي، بشكل رئيسي لأن الشخص قد يعتمد على مبدأ التناسب ليتمكن من الإفلات من المسؤولية. ونظراً لأنه يعتمد على كل حالة على حدة، حتى من يخالف القانون يمكن أن ينجو من خلال الدفاع بمبدأ التناسب.(٩٥)

على الرغم من أن القضاء حاول تفسير مبدأ التناسب، إلا أن السوابق القضائية لم تساعد كثيرًا في تفسير هذا الاختبار لمبدأ التناسب. في قضية المدعي العام ضد كوبريسكيك، قضت غرفة المحاكمة بأن مبدأ التناسب يتطلب ألا تكون الأضرار العرضية وغير المقصودة التي تلحق بالمدنيين خارج نطاق النسبة

إلى الفائدة العسكرية المباشرة الناتجة عن الهجوم العسكري. هذا يعني أنه بوجود مبدأ التناسب سيكون هناك حماية أكبر للمدنيين، لكن للأسف لم تقدم المحكمة تفسيرًا واضحًا لمبدأ التناسب.(٩٦)

قاعدة القانون الدولي الإنساني حول التناسب شهدت تطورًا تدريجيًا، لكنها تُعتبر حاليًا قاعدة من قواعد القانون الدولي الإنساني العرفية التي تنطبق بنفس الطريقة في النزاعات المسلحة الدولية كما هي في النزاعات المسلحة غير الدولية. ومن اللافت للنظر كيف أن قاعدة كانت شبه غير موجودة في عام ١٩٤٥ قد اكتسبت قبولًا واسعًا في القانون الدولي الإنساني اليوم. ومع ذلك، فإن المحتوى الدقيق لقاعدة القانون الدولي الإنساني بشأن التناسب لا يزال غير واضح تمامًا حتى اليوم. لا يزال هناك الكثير من النقاش حول المعنى الدقيق للمكونات المختلفة لقاعدة التناسب في القانون الدولي الإنساني، وكذلك حول كيفية موازنة هذه المكونات. ولعل دراسة للسلوك الفعلي في توجيه العمليات في عدد كبير من الحوادث في نزاعات مسلحة مختلفة من قِبل أنواع مختلفة من القوات المسلحة يمكن أن توفر الإثبات النهائي لوجود القاعدة، وكذلك لمحتواها الدقيق. ويبقى السؤال مفتوحًا حول مدى تأثر محتوى وتطبيق هذه القاعدة بأنواع التناسب الموجودة في مجالات أخرى من القانون الدولي التي تنظم استخدام القوة المسلحة.(٩٧)

الخاتمة

بعد الانتهاء من بحثنا الموسوم (تطبيق مبدا التناسب في العمليات السيبرانية) اصبح من اللازم ان نبين اهم النتائج التي توصل اليها الباحث والمقترحات التي يمكن تقديمها لمعالجة الثغرات التي رافقت تطبيق القانون الدولي الإنساني على العمليات السيبرانية

أولا – النتائج

١. كل عملية سيبرانية يقوم بها احد اطراف النزاع ضد الخصم وينتج عنها نتائج ملموسة مباشرة تعتبر هجوم وفق المعنى العام للمادة ٤٩ من البروتكول الإضافي الأول.

٢. تطبيق القانون الدولي الإنساني على العمليات السيبرانية التي من المتوقع ان تسبب ضررا للأشخاص والاعيان عند استهداف الأنظمة مزدوجة الاستخدام.

٣. اتجاه فقهي يشير الى ان العمليات السيبرانية لغرض تطبيق القانون الدولي الإنساني تعتبر أسلحة حديثة، وبالتالي تخضع للمادة ٣٦ من البروتكول الإضافي الأول الذي يلزم الدول عند تطوير او استخدام تلك الأسلحة مراعاة مبادئ القانون الدولي الإنساني

٤. الاتجاه القضائي في تكيف العمليات السيبرانية بانها هجمات وفق المادة ٤٩ من البروتكول الإضافي الأول يستلزم توفر شرطي جسامة الفعل والاثار الناشئة عنه.

٥. العملية السيبرانية التي تؤدي الى تعطيل الأنظمة الرقمية ويتطلب استبدال مكوناتها تعد هجوما وفق المعنى العام للمادة ٤٩

٦. اتفق الخبراء في دليل تالين بان العملية السيبرانية التي تعد هجوما وفق المعنى للمادة ٤٩ يجب ان تكون نتائجها ملموسة ومباشرة.

٧. الاخلال بمبدأ التناسب يتطلب ان تكون الاضرار الجانبية مفرطة قياسا للميزة العسكرية المتحققة من وراء العملية السيبرانية.

٨. الاضرار النفسية لاتعد اضرارا عند تحليل مبدا التناسب.

٩. التأثيرات المتوقعة او كان يجب توقعها لا تعد اضرار جانبية لغرض تحليل التناسب.

ثانيا – الاقتراحات

١. اتفاقيات جنيف والبروتكولان الاضافيان لم يتناولان صراحة العمليات السيبرانية والسبب ليس قصورا بل نتيجة الفارق الزمني وعم المعرفة بهذه التقنيات، لذلك يتطلب من المجتمع الدولي وبتشجيع من اللجنة الدولية للصليب الأحمر التحضير لمؤتمر دبلوماسي يهيئ لوضع برتوكول إضافي رابع يتناول العمليات السيبرانية بكل تفاصيلها، ليكون مرجعا قانونيا بدلا من معالجة الموضوعات المتعلقة بالعمليات السيبرانية من خلال القياس على تلك المتعلقة بالهجمات التقليدية.

٢. نظرا لكون القادة العسكريين تم توعيتهم في ظل النزاعات التقليدية، وتكون لديهم وعي عسكري تقليدي أهلهم لتقييم الاضرار عند التحليل في ضوء مبدا التناسب. يتطلب من المؤسسات العسكرية القيام بأعداد الأدلة العسكرية التي توضح العمليات السيبرانية ومدى تقيدها بقواعد القانون الدولي الإنساني وإشاعة مضامين تلك الأدلة بين القادة العسكريين

٣. غياب النصوص الصريحة لتنظيم العمليات السيبرانية وتقيدها بالقانون الدولي الإنساني ليس مبررا لعدم تقييد تلك العمليات بالقانون الدولي الإنساني. مما يتطلب من اللجنة الدولية للصليب الأحمر الدعوة الى تفعيل شرط مارتنز الذي يعد قيدا احتياطيا يمنع أي متغيرات في النزاعات المسلحة من ان تكون خارج تطبيق القانون الدولي الإنساني.

٤. قيام اللجنة الوطنية للقانون الدولي الإنساني في العراق بتنظيم دورات متقدمة للقيادات العسكرية لغرض التوعية بالعمليات السيبرانية، وتوضيح مفاهيم تلك العمليات التي تتناسب مع قواعد القانون الدولي الإنساني.

الهوامش:

(1) Michael N. Schmitt, "Cyber Operations and the Jus in Bello: Key Issues," International Law Studies 87 (2011): P.91.

(2) Ibid,PP.92-93.

(٣) غير أن شميت يرى أن الاكتفاء بالتفسير الحرفي لا يكفي، لأن قواعد تفسير المعاهدات، وفقاً لاتفاقية فيينا لقانون المعاهدات، تقضي بأن تُفسر النصوص في ضوء موضوعها وغرضها، وليس اعتماداً على ألفاظها المجردة فقط. وعندما وُضع البروتوكول الإضافي الأول عام ١٩٧٧، لم تكن العمليات السيبرانية معروفة، وكانت معظم الهجمات العسكرية تعتمد على وسائل تطلق طاقة حركية، مثل الانفجارات أو المقذوفات النارية. لذلك فإن واضعي البروتوكول لم يكونوا يقصدون التركيز على طبيعة الوسيلة المستخدمة بقدر ما كانوا يقصدون حماية السكان المدنيين من النتائج الضارة للهجمات.

ومن ثم، فإن كلمة «العنف» لم تكن هدفاً في ذاتها، وإنما كانت وسيلة لغوية مختصرة لوصف الأعمال التي تؤدي إلى إلحاق الضرر بالمدنيين. ولذلك فإن قواعد الاستهداف الواردة في البروتوكول، وإن كانت تبدو من حيث الصياغة قائمة على طبيعة الفعل، فإنها في حقيقتها قواعد قائمة على النتائج المترتبة على ذلك الفعل.

Ibid,P.93-94

(٤) ويضرب شميت مثالين توضيحيين:

فإذا استهدفت عملية سيبرانية نظام مراقبة الحركة الجوية، فإنها قد تعرض الطائرات العسكرية أو المدنية لخطر السقوط.

وإذا استهدفت نظام التحكم في أحد السدود، فقد تؤدي إلى إطلاق المياه وإغراق المناطق الواقعة أسفل السد.

وفي كلتا الحالتين، لا يكون الفعل الإلكتروني نفسه مدمراً، إلا أن نتائجه تكون عنيفة ومدمرة.

ولذلك يخلص إلى أن العملية السيبرانية تُعد هجوماً عندما تؤدي إلى:

وفاة أشخاص؛

أو إصابتهم؛

أو إحداث أضرار أو تدمير للأعيان، سواء كانت أهدافاً عسكرية أم أعياناً مدنية.

Ibid,P.94.

* ظهر مشروع دليل تالين بمبادرة من مركز الناتو التعاوني للتميز في الدفاع السيبراني (CCDCOE) في إستونيا عام ٢٠٠٩، بهدف دراسة كيفية انطباق قواعد القانون الدولي على العمليات السيبرانية، وذلك في ضوء التحديات التي كشفت عنها الهجمات السيبرانية، ولا سيما الهجمات التي تعرضت لها إستونيا عام ٢٠٠٧. وتولى رئاسة فريق الخبراء الدولي البروفيسور مايكل ن. شميث

صدر دليل تالين ١.٠ عام ٢٠١٣، وركز على تطبيق قواعد القانون الدولي على الحرب السيبرانية، ولا سيما قانون استخدام القوة والقانون الدولي الإنساني، وتضمن ٩٥ قاعدة قانونية مع شروحها.

وفي عام ٢٠١٧ صدر دليل تالين ٢.٠، الذي وسّع نطاق الدراسة ليشمل جميع العمليات السيبرانية في السلم والحرب، ولم يقتصر على النزاعات المسلحة، واشتمل على ١٥٤ قاعدة قانونية تغطي مختلف فروع القانون الدولي ذات الصلة. ويؤكد الدليلان أنهما لا ينشئان قواعد قانونية جديدة، وإنما يقدمان تفسيرًا أكاديميًا لكيفية تطبيق القانون الدولي القائم على الفضاء السيبراني

(5) Ibid,Rule.92

(6) Ibid,P.415.

(٧) نصت العديد من مواد البروتوكول الإضافي الأول، وتعليقات اللجنة الدولية للصليب الأحمر عليها، يدعم هذا الاستنتاج. على سبيل المثال، تنص المادة ٥١(١) على المبدأ العام بأن 'يجب أن يتمتع السكان المدنيون والأفراد المدنيون بالحماية العامة من المخاطر الناشئة عن العمليات العسكرية'. مواد أخرى تقدم دعمًا إضافيًا. قواعد التناسب تتحدث عن 'فقدان الأرواح المدنية، إصابة المدنيين، ضرر بالأعيان المدنية، أو مزيج منها'. تلك المتعلقة بحماية البيئة تشير إلى 'أضرار واسعة النطاق وطويلة الأجل وشديدة'، وحماية السدود والخزانات ومحطات توليد الكهرباء النووية مؤطرة بمصطلح 'خسائر جسيمة بين السكان المدنيين'. اتفق الخبراء على أن الضرر الطفيف أو الدمار البسيط

لا يفي بعتبة الضرر المطلوبة بموجب هذه القاعدة. ٥. كلمة 'تسبب' في هذه القاعدة ليست مقتصرة على تأثيرات النظام الإلكتروني المستهدف. بل تشمل أي أضرار أو دمار أو إصابات أو وفيات معقولة التوقع نتيجة لذلك. على الرغم من أن الهجمات الإلكترونية نادرًا ما تنطوي على استخدام قوة مادية مباشرة ضد النظام المستهدف، إلا أنها قد تسبب أضرارًا كبيرة للأفراد أو للأشياء. على سبيل المثال، تحرير مياه سد بواسطة التلاعب بنظام SCADA قد يسبب دمارًا واسع النطاق في مناطق أسفل السد دون إلحاق الضرر بالنظام نفسه.

Ibid,P.416.

(8) Knut Dörmann, "Applicability of the Additional Protocols to Computer Network Attacks," in Yearbook of International Humanitarian Law, Vol. ٤ (٢٠٠١),P.٤

(٩) يترتب على ذلك أن عدم وجود تنظيم قانوني صريح لنشاط عسكري معين يُعد وسيلة من وسائل الحرب، لا يعني جواز استخدامه دون قيود. وانطلاقًا من هذا الأساس، لا يوجد ما يمنع من افتراض أن الأشكال الحديثة لهجمات شبكات الحاسوب، التي لا تنطوي على استخدام الأسلحة التقليدية، تخضع للقانون الدولي الإنساني، شأنها شأن أي سلاح جديد أو نظام مستحدث لإيصال الأسلحة متى استُخدم في سياق نزاع مسلح.

Ibid,P.2.

(10) Ibid,P.5.

(11) Marco Roschini ,Cyber Operations and Use of Force in International Law ,Oxford University Press,2014,P18-29

(12) Herbert S.Lin, O offensive Cyber Operations and the Use of Force , Journal of National Security Law & Policy ,Vol.4,2010,P.63

(13) Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The Law of Cyber-Attack. California Law Review, 100(4), 837

(١٤) ا.د احمد عبيس الفتلاوي، زهراء عماد محمد، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مجلة الكوفة للعلوم القانونية والسياسية، مجلد ١٢ عدد ٤٤ الجزء الأول (٢٠٢٠)، ص٥١

(١٥) الا أن هذا المفهوم الواسع أثار انتقادات واسعة في الأوساط الفقهية؛ إذ يرى عدد من الباحثين أن هذا التعريف قد يُستخدم لتبرير فرض الرقابة على الخطاب السياسي المتداول عبر شبكة الإنترنت تحت ذريعة حماية الأمن المعلوماتي. وتكتسب هذه المخاوف أهمية خاصة في ضوء ما شهدته بعض الدول، ومنها إيران ومصر وغيرها، من إجراءات حكومية هدفت إلى الحد من التنظيم السياسي واستخدام وسائل الإعلام الجديدة في الحشد والتعبئة. ومع تزايد اعتماد الإنترنت بوصفه فضاءً لتبادل الأفكار وممارسة النشاط السياسي، فإن مثل هذه الإجراءات قد تُشكل تهديدًا مباشرًا لحقوق الإنسان، ولا سيما الحق في حرية الرأي والتعبير وحرية تداول المعلومات.

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. op.cit,P, 825.

(16) UK Government ,National Cyber Security Strategy 2016-2021 ,Annex 2 (Glossary),London :HM Government ,2016,P.74

(17) National Cyber Security Centre (NCSC),Cyber Attack , UK,Government,available at: https ://www.ncsc.gov/uk/section/advice-guidance/all-topics /cyber-attack

تاريخ الزيارة ٢٠٢٦/٧/١١

(١٨) وتفهم اللجنة الدولية الحرب السيبرانية بانها عمليات ضد حاسوب او نظام حاسوبي من خلال دفق بيانات عندما تستخدم كوسائل وأساليب حرب في سياق نزاع مسلح، وتثير الحرب السيبرانية مسائل تتعلق بمدى دقة انطباق احكام القانون الدولي الإنساني على هذه العمليات، وما اذا كان القانون الدولي الإنساني كافيا ام انه يستلزم المزيد من التطوير استنادا الى احكام القانون القائمة.

اللجنة الدولية للصليب الأحمر، القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة، ٢٠١٩، ص٢٦

(١٩) يوجد سببان رئيسيان يدعمان موقف اللجنة الدولية للصليب الأحمر. السبب الأول ناتج عن تفسير مفهوم الهجوم في سياقه. نظرًا لأن تعريف الأهداف العسكرية في المادة ٥٢(٢) من البروتوكول الأول يشير ليس فقط إلى التدمير أو الاستيلاء ولكن أيضًا إلى "تحييد" كاحتمال نتيجة للهجوم، ينبغي فهم مفهوم "الهجوم" بموجب المادة ٤٩ من البروتوكول الأول ليشمل العمليات المصممة للإضرار بعمل الأشياء (أي تحييدها) دون التسبب بأضرار مادية أو تدمير. في الواقع، تم الإشارة إلى أن ذكر الحياد صراحةً في المادة ٥٢(٢) سيكون زائداً عن الحاجة بخلاف ذلك. ثانيًا، فهم مفرط الصرامة لمفهوم الهجوم سيكون صعب التوافق مع هدف وغرض قواعد إجراء الأعمال العدائية، والتي تهدف إلى ضمان حماية السكان المدنيين والأعيان المدنية من آثار الأعمال العدائية. في الواقع، وفق فهم مفرط الصرامة، قد لا تغطي قواعد القانون الدولي الإنساني الأساسية التي تحمي السكان المدنيين والأعيان عملية سيبرانية تهدف إلى تعطيل شبكة مدنية (كهرباء، بنوك، اتصالات أو شبكة أخرى)، أو التي قد ينتج عنها هذا بشكل عرضي.

aurent Gisel, Tilman Rodenhäuser & Knut Dörmann, "Twenty Years On: International Humanitarian Law and the Protection of Civilians Against the Effects of Cyber Operations During Armed Conflicts," International Review of the Red Cross, Vol. 102, No. 913, 2020, pp.313-314

(٢٠) وتظل هذه العمليات خاضعة لبعض القيود بموجب القانون الدولي الإنساني فعلى وجه الخصوص، لا يجوز توجيه الهجمات السيبرانية العسكرية الى اعيان مشمولة بحماية خاصة مثل المرافق الطبية، وعند اجراء أي عملية سيبرانية عسكرية يجب الحرص على تجنيب السكان المدنيين والاعيان المدنية. وتوجيه عمليات سيبرانية تخريبية الى الاعيان المدنية بما في ذلك البيانات المدنية او تجاهل اثارها العرضية على السكان المدنيين.

اللجنة الدولية للصليب الأحمر، القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة، ٢٠٢٥، ص٥٧

(٢١) ويعد التزام الدول بالقانون الدولي، ولا سيما التزاماتها بموجب ميثاق الأمم المتحدة بمثابة اطار أساسي لتوجيه ما تقوم به من إجراءات في مجال استخدام تكنولوجيات المعلومات والاتصالات ولتعزيز بيئة مفتوحة وامنة ومستقرة وميسرة وسلمية في مجال تكنولوجيا المعلومات والاتصالات ولهذه الالتزامات أهميتها الجوهرية في بحث وتطبيق القانون الدولي على استخدام الدول لتكنولوجيات المعلومات والاتصالات.

الأمم المتحدة، الجمعية العامة، تقرير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات في سياق الامن الدولي، الوثيقة رقم ٢٢، A/٧٠/١٧٤ تموز ٢٠١٥، ص١٧، الفقرة ٢٤.

(٢٢) نفس المصدر، ص ١٨، الفقرة ٢٨، (د).

(٢٣) من المهم الإشارة الى ان عبارة جسامة الفعل واثاره ليست نصا حرفيا ورد في حكم المحكمة بل هو استخلاص لمعيار (اشد صور استخدام القوة جسامة).

قضية الأنشطة العسكرية وشبه العسكرية في نيكارغوا ضد الولايات المتحدة، حكم محكمة العدل الدولية / مجموعة احكام المحكمة لعام ١٩٨٦، ص١٤، الفقرة ١٩٥، ص١٠٣-١٠٤.

(24) Oil Platforms (Islamic Republic of Iran V.United States Of America) ,Judgment ,I.C.J.Reports , P.161,Paras.51,72,PP.186-187,196-197.

(25) Armed Activities on the Territory of the Congo (Democratic Republic of the Congo V.Uganda) , Judgment ,I.C.J,Reports 2005 , P.168,Paras.146-147,PP.222-223

(26) Michael N.Schmitt,Tallinn Manual 2,Rule 71,P.341

(27) Eneken Tikk and Kadri Kaska, "Legal Cooperation to Investigate Cyber Incidents: Estonian Case Study and Lessons," in Proceedings of the 9th European Conference on Information Warfare and Security (Reading:A cademic Publishing Limited, 2010), 288–294.

(28) Tikk, Eneken, Kadri Kaska, and Liis Vihul. International Cyber Incidents: Legal Considerations. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2010.P.66-67

(29) Ibid,P.79

(30) Ibid,PP.80-81

ولهذا، يجب تحليل مفهومي «الحرب السيبرانية» (Cyber War) و**«الهجوم السيبراني» (Cyber Attack)** وفقاً للمعايير القانونية، وليس بالاستناد إلى التوصيفات الإعلامية أو السياسية، وذلك للتحقق مما إذا كانت الهجمات السيبرانية التي تعرضت لها جورجيا تحقق عناصر الهجوم المسلح التي تستوجب تطبيق قانون النزاعات المسلحة.

(31) Eneken Tikk, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm, and Liis Vihul, Cyber Attacks Against Georgia: Legal Lessons Identified (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2010).P.20.

وفي هذا السياق، يرفض البروفيسور مايكل شميت (Michael N. Schmitt) اعتبار مشاركة القوات المسلحة المعيار الحاسم الوحيد لتوصيف الهجوم بأنه هجوم مسلح، موضحاً أن واضعي قواعد قانون النزاعات المسلحة كانوا يفترضون، في زمن صياغة تلك الاتفاقيات، أن القوات المسلحة هي الجهة الطبيعية التي تنفذ الهجمات المسلحة، وهو افتراض لم يعد يعكس الواقع في عصر الفضاء السيبراني، حيث قد تُنفذ العمليات بواسطة جهات مدنية أو مجموعات غير حكومية أو أفراد.

ويرى شميت أن المعيار الحقيقي يتمثل في طبيعة الفعل وآثاره، وبصورة خاصة النتائج التي يُحدثها، وليس في هوية الجهة المنفذة. واستناداً إلى المبادئ التي يقوم عليها تعريف الهجوم المسلح التقليدي، يقرر أن العملية السيبرانية يمكن أن تُعد هجوماً مسلحاً إذا كانت:

تهدف إلى إحداث إصابة أو وفاة أو إضرار أو تدمير، أو إذا كانت هذه النتائج متوقعة بصورة معقولة من تنفيذها.

(32) Ibid,P.20

(33) Ibid,P.20

(٣٤) ويخلص المؤلف إلى أن العمليات السيبرانية المعروفة حتى الآن تميل بدرجة أكبر إلى الجانب الإجرامي من هذا الطيف، وليس إلى جانب الحرب. ولذلك، يؤكد أنه لا توجد، حتى الآن، حالة معروفة يمكن وصفها بأنها "حرب سيبرانية" إذا استُخدم مفهوم الحرب بمعناه القانوني الدقيق.

Thomas Rid, "Cyber War Will Not Take Place," Journal of Strategic Studies 35, no. 1 (2012): P.15 https://doi.org/10.1080/01402390.2011.608939.

(https://doi.org/10.1080/01402390.2011.608939) تاريخ الزيارة ٢٠٢٦/٧/١٧

([35]) Michael N. Schmitt, Tallinn Manual 2.0, op. cit., p. 439

([36]) Thomas Rid,op.cit,P17

([٣٧]) ويخلص المؤلف إلى أن العالم لم يشهد حتى الآن حربًا سيبرانية بالمعنى القانوني الكامل؛ فالحرب السيبرانية، في نظره، يجب أن تتوافر فيها ثلاثة عناصر أساسية هي: العنف، والوسيلة الألكترونية لتحقيق غاية سياسية، وإمكانية إسناد الفعل سياسيًا إلى دولة أو جهة مسؤولة. ويرى أن أيًا من العمليات السيبرانية المعروفة حتى الآن لم يجمع هذه العناصر مجتمعة. وإنما شهد العقد الأخير تطورًا ملحوظًا في عمليات التخريب السيبراني (Sabotage) والتجسس الإلكتروني (Espionage) والتخريب السياسي أو التحريض (Subversion)، وهي أنشطة يمكن أن تدعم العمليات العسكرية، بل استُخدمت لهذا الغرض منذ قرون، إلا أنها تظل وسائل مساندة للحرب التقليدية، وليست حربًا مستقلة تُخاض بالبرمجيات بوصفها السلاح الرئيس

Ibid,P.29.

([38]) Michael N.Schmitt, Tallinn Manual 2.0, op. cit., p. 342

* تكررت الهجمات السيبرانية خلال السنوات السابقة ومن هذه الهجمات الهجوم على شبكة الكهرباء الأوكرانية (٢٠١٥-٢٠١٦) وهجوم Wannacry ٢٠١٧ وهجوم NotPetya ٢٠١٧و الهجوم على شبكة الكهرباء الأوكرانية (٢٠٢٢) وهجوم Viasat (٢٠٢٢) و هجوم) Colonial Pipeline٢٠٢١ و هجوم) SolarWinds٢٠٢٠ و الهجمات على كوستاريكا (٢٠٢٢)

([39])

([٤٠]) حظيت الهجمات السيبرانية التي تعرضت لها إستونيا عام ٢٠٠٧ بتغطية إعلامية واسعة، ووُصفت في العديد من وسائل الإعلام بأنها أول "حرب سيبرانية" في التاريخ. وقد كشفت هذه الواقعة عن الكيفية التي يمكن بها توظيف التكنولوجيا الحديثة لاستهداف دولة متقدمة تعتمد بصورة كبيرة على البنية التحتية الرقمية. وتشير الدراسة إلى أن الهجمات انطلقت من روسيا، إذ إن معظم هجمات حجب الخدمة الموزعة (DDoS) صدرت من عناوين بروتوكول الإنترنت (IP Addresses) الروسية. كما استخدم عدد كبير من المهاجمين أجهزة حاسوب موجودة داخل إستونيا، وكان معظم مستخدميها من أفراد الأقلية الروسية المقيمة فيها. ومع ذلك، لم تتمكن المفوضية الأوروبية وخبراء حلف شمال الأطلسي (الناتو) من العثور على أي دليل يثبت أن السلطات الروسية هي التي نفذت تلك الهجمات أو وجهتها، رغم أن نتائجها كانت تصب بصورة واضحة في مصلحة الكرملين.**[20] **ويبدو هذا الاحتمال أكثر ترجيحاً بعد أن اعترف أحد أعضاء منظمة الشباب الروسية "ناشي" (NASHI)، المرتبطة بالحزب الحاكم بزعامة فلاديمير بوتين، بأنه كان يقف وراء تلك الهجمات.

Andrzej Kozlowski. "Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan." In Proceedings of the International Scientific Forum (ISF 2013), vol. 3, Tirana, Albania, 12–14 December 2013, pp. 237-238.

([41]) Eneken Tikk and Kadri Kaska, "Legal Cooperation to Investigate Cyber Incidents: Estonian Case Study and Lessons," in Proceedings of the 9th European Conference on Information Warfare and Security (Reading:A cademic Publishing Limited, 2010), 288–294.

(42) Tikk, Eneken, Kadri Kaska, and Liis Vihul. International Cyber Incidents: Legal Considerations. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2010.P.66-67

(43) Ibid,P.79.

(44) Ibid,P.79

(45) Ibid,PP.80-81

ولهذا، يجب تحليل مفهومي «الحرب السيبرانية» (Cyber War) و**«الهجوم السيبراني» (Cyber Attack)** وفقاً للمعايير القانونية، وليس بالاستناد إلى التوصيفات الإعلامية أو السياسية، وذلك للتحقق مما إذا كانت الهجمات السيبرانية التي تعرضت لها جورجيا تحقق عناصر الهجوم المسلح التي تستوجب تطبيق قانون النزاعات المسلحة.

(46) Eneken Tikk, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm, and Liis Vihul, Cyber Attacks Against Georgia: Legal Lessons Identified (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2010).P.20.

وفي هذا السياق، يرفض البروفيسور مايكل شميت (Michael N. Schmitt) اعتبار مشاركة القوات المسلحة المعيار الحاسم الوحيد لتوصيف الهجوم بأنه هجوم مسلح، موضحاً أن واضعي قواعد قانون النزاعات المسلحة كانوا يفترضون، في زمن صياغة تلك الاتفاقيات، أن القوات المسلحة هي الجهة الطبيعية التي تنفذ الهجمات المسلحة، وهو افتراض لم يعد يعكس الواقع في عصر الفضاء السيبراني، حيث قد تُنفذ العمليات بواسطة جهات مدنية أو مجموعات غير حكومية أو أفراد.

ويرى شميت أن المعيار الحقيقي يتمثل في طبيعة الفعل وآثاره، وبصورة خاصة النتائج التي يُحدثها، وليس في هوية الجهة المنفذة. واستناداً إلى المبادئ التي يقوم عليها تعريف الهجوم المسلح التقليدي، يقرر أن العملية السيبرانية يمكن أن تُعد هجوماً مسلحاً إذا كانت:

تهدف إلى إحداث إصابة أو وفاة أو إضرار أو تدمير، أو إذا كانت هذه النتائج متوقعة بصورة معقولة من تنفيذها.

(47) Ibid,P.20

(48) Ibid,P.20

(٤٩) ويخلص المؤلف إلى أن العمليات السيبرانية المعروفة حتى الآن تميل بدرجة أكبر إلى الجانب الإجرامي من هذا الطيف، وليس إلى جانب الحرب. ولذلك، يؤكد أنه لا توجد، حتى الآن، حالة معروفة يمكن وصفها بأنها "حرب سيبرانية" إذا استُخدم مفهوم الحرب بمعناه القانوني الدقيق.

Thomas Rid, "Cyber War Will Not Take Place," Journal of Strategic Studies 35, no. 1 (2012): P.15 https://doi.org/10.1080/01402390.2011.608939.

(https://doi.org/10.1080/01402390.2011.608939) تاريخ الزيارة ٢٠٢٦/٧/١٧

(50) chmitt, Tallinn Manual 2.0, op. cit., p. 439

(51) Sandanu Mihisara, The Stuxnet Cyber Attack Against the Iranian Nuclear Facility, IT Security Management Report, IUFC 2024, p2

https://www.scribd.com/document/913011620/Cyber-Security-Assignment تاريخ الزيارة ٢٠٢٦/٧/١٧

وتشير الأدلة إلى أن العملية، التي يُحتمل أن مطوريها أطلقوا عليها اسم عملية "Myrtus"، كانت حملة سيبرانية استغرقت عدة سنوات، إذ يُرجَّح أن تطويرها بدأ في أواخر عام ٢٠٠٧ أو أوائل عام ٢٠٠٨. كما يُعتقد أن المرحلة الرئيسة من الهجوم نُفذت خلال الفترة الممتدة من يونيو/حزيران ٢٠٠٩ إلى يونيو/حزيران ٢٠١٠، وهي الفترة التي بدأت فيها شركات أمن تكنولوجيا المعلومات بالإعلان لأول مرة عن اكتشاف البرمجية.

وقد احتوت برمجية Stuxnet على بيانات زمنية (Timestamp) ومعلومات تقنية خاصة بالأنظمة التي أصابتها، الأمر الذي مكّن الخبراء، بعد أشهر من التحليل الهندسي الدقيق، من إعادة بناء التسلسل الزمني لانتشار البرمجية، وفهم آلية عملها، وتحليل بنيتها البرمجية، والكشف عن الغاية التي صُممت من أجلها. ومن ثم، فإن استعراض خصائص Stuxnet يبرز مستوى غير مسبوق من التعقيد التقني والتخطيط العملياتي، وهو ما جعلها نموذجًا فريدًا في تاريخ العمليات السيبرانية.

([52]) Thomas Rid,op.cit,P17

([٥٣]) ويخلص المؤلف إلى أن العالم لم يشهد حتى الآن حربًا سيبرانية بالمعنى القانوني الكامل؛ فالحرب السيبرانية، في نظره، يجب أن تتوافر فيها ثلاثة عناصر أساسية هي: العنف، والوسيلة الإلكترونية لتحقيق غاية سياسية، وإمكانية إسناد الفعل سياسيًا إلى دولة أو جهة مسؤولة. ويرى أن أيًّا من العمليات السيبرانية المعروفة حتى الآن لم يجمع هذه العناصر مجتمعة. وإنما شهد العقد الأخير تطورًا ملحوظًا في عمليات التخريب السيبراني (Sabotage) والتجسس الإلكتروني (Espionage) والتخريب السياسي أو التحريض (Subversion)، وهي أنشطة يمكن أن تدعم العمليات العسكرية، بل استُخدمت لهذا الغرض منذ قرون، إلا أنها تظل وسائل مساندة للحرب التقليدية، وليست حربًا مستقلة تُخاض بالبرمجيات بوصفها السلاح الرئيس

Ibid,P.29.

([54]) Schmitt, Tallinn Manual 2.0, op. cit., p. 342

* تكررت الهجمات السيبرانية خلال السنوات السابقة ومن هذه الهجمات الهجوم على شبكة الكهرباء الأوكرانية (٢٠١٥-٢٠١٦) وهجوم Wannacry ٢٠١٧ وهجوم NotPetya ٢٠١٧و الهجوم على شبكة الكهرباء الأوكرانية (٢٠٢٢) وهجوم Viasat (٢٠٢٢) و هجوم) Colonial Pipeline٢٠٢١ و هجوم) SolarWinds٢٠٢٠ و الهجمات على كوستاريكا (٢٠٢٢)

([55]) Al-Nabhani, Anfaal Said. "Cyber Operations as a Challenge to the Implementation of International Humanitarian Law (IHL)." Sultan Qaboos University Legal Studies Journal, vol. 4 (2025): p.1520. https://doi.org/10.61190/squlsj.1031 تاريخ الزيارة ٢٠٢٦/٧/٢٣

([56]) J. C. van den Boogaard, Proportionality in International Humanitarian Law (PhD diss., University of Amsterdam, 2019),P120

([57]) Ibid,P.120

([٥٨]) بالتزامن مع القانون المتعلق بالحرب الجوية، تطوّر القانون الخاص بالقصف من البحر. تحتوي اتفاقية ١٩٠٧ بشأن القصف البحري أيضًا على حظر لشن هجمات على الموانئ والمدن غير المحمية.

Ibid,P.121

([٥٩]) لم تدخل قواعد لاهاي للحرب الجوية حيز التنفيذ أبدًا، لكن محتواها يمكن اعتباره جزءًا من تطور قانون الاستهداف. ومع ذلك، في ذلك الوقت، تعرضت أحكامها للنقد، ووُصفت حتى بأنها "غير واقعية". يلاحظ باركس أن المقال المقترح ٢٤، الذي يتطلب العناية بالضحايا المدنيين العرضيين، كان "تغييرًا كاملًا بمقدار ١٨٠ درجة في فلسفة القصف السائدة آنذاك." يمكن العثور على إشارة أخرى لمبدأ التناسب قبل اندلاع الحرب العالمية الثانية في قرار اعتمدته جمعية عصبة الأمم بشأن الحرب الجوية عام ١٩٣٨. يحظر القرار "القصف المتعمد للمدنيين" ويكرر أن "أي هجوم على أهداف عسكرية مشروعة يجب أن ينفذ بطريقة لا يتعرض فيها السكان المدنيون في المنطقة المجاورة للقصف نتيجة الإهمال." باختصار: تعكس جهود التقنين في مؤتمرات سلام لاهاي والتطورات الأخرى قبل الحرب العالمية

الثانية قبولًا متزايدًا للتمييز. ومع ذلك، كانت قاعدة التناسب التي تزيد من حماية السكان المدنيين لا تزال بعيدة، على الرغم من ظهور وعي بضرورة مراعاة السكان المدنيين ضد آثار الأعمال العدائية.

Ibid,P.123

(٦٠) بعض الوفود في المؤتمر الدولي الذي أدى إلى اعتماد البروتوكول الإضافي الأول كانت لديها بعض الشكوك حول تضمين قاعدة القانون الإنساني الدولي المتعلقة بالتناسب في المعاهدة. كانوا يخشون أن يؤدي ذلك إلى إساءة استخدام القاعدة وأن يطمس المبدأ الواضح والصريح للتمييز. ومع ذلك، نظرًا لحقيقة أن سير الأعمال العدائية سيسبب حتماً ضرراً وخسائر في الأرواح وأضرار للمدنيين والأعيان المدنية، «سادت وجهة النظر القائلة إنه من الأفضل أن يعكس القانون هذه الحقيقة وأن يُستخدم لفرض ضبط النفس، بدلاً من الصمت حيال الأمر وتركه تمامًا لممارسات المتحاربين.»

Ibid,P.127

(61) Elliot Winter, "Autonomous Weapons in Humanitarian Law: Understanding the Technology, Its Compliance with the Principle of Proportionality and the Role of Utilitarianism," Groningen Journal of International Law 6, no. 1 (2018),P.192

(62) Ibid,P.193

(63) J. C. van den Boogaard,OP.cit,P.131

(64) Ibid,p.132

(65) nternational Law Association Study Group on the Conduct of Hostilities in the 21st Century, The Conduct of Hostilities and International Humanitarian Law: Challenges of 21st Century Warfare, International Law Studies 93 (2017) (Newport, RI: Stockton Center for the Study of International Law, 2017),P.352

(66) Ibid,P.352

(٦٧) وفقًا لمستشار طبي خبير من اللجنة الدولية للصليب الأحمر قد تتأثر مرافق الرعاية الصحية مباشرة بتأثيرات الانفجار أو شظايا الأسلحة المتفجرة؛ قد تُقطع إمدادات الكهرباء والمياه؛ قد يُقتل أو يُصاب طاقم الرعاية الصحية أو يصبح غير قادر على الوصول إلى العمل؛ وقد تنخفض مخزونات الدم لأن المتبرعين المنتظمين لا يستطيعون الوصول إلى مرافق الرعاية الصحية. غالبًا ما يعني أحد هذه العوامل أو مجموعة منها أن قدرة مرافق الرعاية الصحية تكون ضعيفة في الوقت الذي تكون فيه الحاجة إليها أكبر – أي بعد الهجوم عندما تواجه المستشفيات العديد من المرضى، غالبًا بإصابات متعددة.

Ibid,P.353

(68) Ibid,P.353

(٦٩) لذلك، عند النظر في التأثيرات غير المباشرة، يجب ألا يكون التركيز بالدرجة الأولى على الإطار الزمني الذي ستظهر فيه هذه التأثيرات، بل على إمكانية توقعها. من المهم الإشارة إلى أن التأثيرات غير المباشرة يمكن أن تكون شديدة مثل التأثيرات المباشرة للهجوم أو حتى أكثر شدة. على سبيل المثال، قد يكون للتأثيرات المتتابعة على الأشياء الضرورية لنظام الرعاية الصحية تأثير متوقع وعميق من حيث فقدان حياة المدنيين وإصابة المدنيين الناتج عن هجوم مخطط له. هذا لا يعني أن القانون يمنع مجرد الإزعاج للسكان المدنيين الناجم عن الأعمال العدائية – إذ أن مجرد الإزعاج عادة لا يكون مفرطا مقارنة بالمصلحة العسكرية المباشرة والملموسة المتوقعة – لكنه يعني أن القادة بحاجة إلى موازنة المصلحة العسكرية المباشرة والملموسة التي يسعون لتحقيقها مع أكثر من مجرد الضرر العرضي المباشر الذي

يتوقعونه من هجومهم المخطط له. يمكن ويجب على أطراف النزاع المسلح تعزيز قدرتهم على توقع التأثيرات المتتابعة المتوقعة لهجوم مخطط له، على سبيل المثال من خلال التدريب العسكري للقادة وضباط الأجهزة، وأخذ التجارب السابقة في المعارك بعين الاعتبار، وبرامج المحاكاة الحاسوبية.

Ibid,P.354

([70]) Tuomas Heikkinen and Martin Faix, "The Use of Human Shields and the Principle of Proportionality under Law of Armed Conflict," Czech Yearbook of International Law 7 (2016,P.248

([٧١]) علاوة على ذلك، بينما يختلف بعض الأكاديميين مع هذا الرأي، إلا أنهم يجادلون أيضًا بأنه، بينما يجب أن يستمر الدروع البشرية غير الطوعية في التمتع بحمايتهم المدنية بموجب القانون الإنساني الدولي، فإن الدروع البشرية الطوعية تعتبر حالة مختلفة. الدروع البشرية الطوعية ستُعتبر على أنها "مشاركة مباشرة في الأعمال العدائية" وبالتالي ستفقد وضعها المحمي بموجب القانون. ومع ذلك، من الناحية الجدلية، ليس من الواضح دائمًا ما إذا كانت الدروع البشرية طوعية أم غير طوعية. التمييز بين الدروع البشرية الطوعية وغير الطوعية يمكن أن يكون إشكاليًا. في الواقع.

Ibid,248

([72]) Ibid,P.252

([٧٣]) بالإضافة إلى ذلك، يجب فهم شرط حصول الضرر للأشياء المدنية بشكل واسع. الغالبية العظمى من الإنترنت، بما في ذلك الكابلات والخوادم والراوترات، تتألف من أشياء مدنية، والتي يمتلكها ويديرها ويصونها المدنيون. أي ضرر لهذه العناصر من بنية الإنترنت التحتية سيُعتبر ضرراً مدنياً لأغراض تحليل التناسب.

Eric Talbot Jensen, "Cyber Attacks: Proportionality and Precautions in Attack," International Law Studies,VOI , 89 (2013):P.205

([74]) Peter Pascucci ,OP.cit,P.446

([٧٥]) على الرغم من أن واضعي البروتوكول الإضافي الأول لعام ١٩٧٧ لم يتوقعوا بالتأكيد الحرب السيبرانية، إلا أنهم أدركوا أن التقدمات الإلكترونية في التكنولوجيا ستؤثر على طريقة خوض الحروب وعلى تأثيراتها المحتملة على المدنيين. في التعليق التفسيري، تشير اللجنة الدولية للصليب الأحمر إلى أنه "تم أيضًا الإشارة إلى أن الوسائل الإلكترونية الحديثة جعلت من الممكن تحديد الأهداف العسكرية، لكنها لم توفر معلومات عن وجود عناصر مدنية داخل هذه الأهداف أو في محيطها." وعلى الرغم من أن هذا قد لا يكون صحيحًا تمامًا في الحرب السيبرانية، إلا أن هذه الفكرة تؤثر بالتأكيد على تطبيق مبدأ التناسب في الهجمات السيبرانية.

Eric Talbot Jensen,OP,cit,P.205

([76]) الميزة في هذا النهج هي أنه يضع القادة في موقف مريح لتطبيق العوامل المعروفة. لقد كان القادة يطبقون تحليل التناسب على الهجمات التقليدية طوال حياتهم المهنية ومن المرجح أن يشعروا بالراحة الشديدة مع هذا التحليل. كما يبدو أن النهج الوظيفي هو أفضل تطبيق لقاعدة التناسب في المجال السيبراني، لأنه يأخذ في الاعتبار الجوانب الفريدة للعمليات السيبرانية، دون أن يجعل تحليل التناسب صعب التطبيق للقادة.

Ibid,P.206

([77]) Ibid,p.207

([78]) Ibid,p.208

(79) Hensey A. Fenton III, "Proportionality and Its Applicability in the Realm of Cyber-Attacks," Duke Journal of Comparative & International Law 29, no. 2 (2019):PP.349-350

(80) Eric Boylan, "Applying the Law of Proportionality to Cyber Conflict: Suggestions for Practitioners," Vanderbilt Journal of Transnational Law 50, no. 1 (2017):P.231

(81) Hensey A. Fenton III,OP.cit,P.349

(82) Ibid,P.349

(٨٣) قد يكون مثال واحد هو نظام الأقمار الصناعية الذي يُستخدم لتوجيه نظام تحديد المواقع GPS. إذا كانت هناك معرفة بأن نظام الأقمار الصناعية يُستخدم لأغراض مدنية وعسكرية معًا، فقد يكون من الصعب على القائد العسكري تحديد مدى استخدام النظام لكل غرض. ونظرًا للطبيعة الغامضة والسريعة للعمليات العسكرية، قد يكون لدى القائد فقط معلومات استخباراتية تشير إلى أن القمر الصناعي يوفر توجيهًا لنظام عسكري، وربما لا يعرف ما هي الوظائف الأخرى التي يؤديها. هذا يجعل من الصعب إجراء تحليل للتناسب. إذا لم يعرف القائد الاستخدام المدني للنظام، فسوف يكون من الصعب أو المستحيل تقدير تأثيرات الهجوم. على عكس الأنظمة التقليدية، التي يمكن للقائد فهمها بسهولة من النظرة الأولى، غالبًا ما تكون الأنظمة السيبرانية أصعب في الاستيعاب.

(84) an Henderson and Kate Reece,OP.cit,P.852

* هجوم على مقر القيادة، من المحتمل أن يتسبب نفس السلاح المتفجر العالي أيضًا في إتلاف البنية التحتية للمياه الحيوية الموجودة في الأرض تحت المقر، والتي من المتوقع أن تعطل إمدادات المياه النظيفة للشرب والصرف الصحي للمدينة. افترض أن نقص المياه النظيفة من المرجح أن يزيد بشكل كبير من خطر مختلف الأمراض مثل الكوليرا والإسهال والدوسنتاريا والتهاب الكبد A وحمى التيفوئيد وشلل الأطفال. بينما سيكون تدمير البنية التحتية للمياه تأثيرًا مباشرًا (أوليًا) للهجوم، وفقدان الوصول إلى المياه النظيفة نتيجة لذلك تأثيرًا غير مباشر (ثانويًا)، هل يتطلب قانون النزاعات المسلحة من القائد العسكري المعقول أن يأخذ في اعتباره، كجزء من حسابه للأضرار الجانبية المتوقعة، التأثيرات غير المباشرة (الثالثة والرابعة) أي زيادة خطر الأمراض والنتائج الصحية السيئة والوفيات على السكان المدنيين نتيجة انقطاع إمدادات المياه؟

(85) Ibid,P.853

(٨٦) ومع ذلك، لدى القائد معلومات إضافية تشير إلى أن هذه المياه المعبأة لا يمكن توزيعها بنجاح على حوالي ١٠ في المئة من سكان المدينة المدنيين. بدون وجود مصدر للمياه، من المحتمل أن يموت بعض هؤلاء المدنيين عطشًا في الأسابيع المقبلة. هناك الآن مجال لوجهتي نظر محتملتين. إحدى وجهات النظر يمكن أن تكون أن هذه الوفيات نتيجة متوقعة للهجوم، بغض النظر عن الإطار الزمني المتوقع لحدوث هذه الوفيات. وبناءً عليه، سيتم احتساب عدد الضحايا المتوقع ضمن أي تقييم للتناسب. وجهة النظر الأخرى يمكن أن تكون أن هذا مجرد تكهن. ربما ينتقل المدنيون إلى مكان آخر. ربما يتم تقديم المساعدة الإنسانية. ربما ينتهي النزاع المسلح. ربما يكون موسم الأمطار ويمكن جمع مياه الأمطار. لذلك، بينما من الممكن أن يموت المدنيون عطشًا في الأسابيع المقبلة، إلا أن ذلك ليس بالضرورة حتميًا. وأكثر من ذلك، لا يمكن التنبؤ به بثقة. علاوة على ذلك، قد يمكن تجنبه من خلال اتخاذ إجراءات علاجية محتملة. وفقًا للوجهة الثانية، أي خطر لوقوع إصابات بين المدنيين سيكون بعيدًا جدًا ليُعتبر بشكل معقول ناتجًا عن الهجوم. لذلك، لن تُعتبر هذه الوفيات ضررًا غير مباشر متوقعًا نتيجة للهجوم ولن يتم احتسابها في ومع ذلك، لدى القائد معلومات إضافية تشير إلى أن هذه المياه المعبأة لا يمكن توزيعها بنجاح على حوالي ١٠ في المئة من سكان المدينة المدنيين. بدون وجود مصدر للمياه، من المحتمل أن

يموت بعض هؤلاء المدنيين عطشًا في الأسابيع المقبلة. هناك الآن مجال لوجهتي نظر محتملتين. إحدى وجهات النظر يمكن أن تكون أن هذه الوفيات نتيجة متوقعة للهجوم، بغض النظر عن الإطار الزمني المتوقع لحدوث هذه الوفيات. وبناءً عليه، سيتم احتساب عدد الضحايا المتوقع ضمن أي تقييم للتناسب. وجهة النظر الأخرى يمكن أن تكون أن هذا مجرد تكهن. ربما ينتقل المدنيون إلى مكان آخر. ربما يتم تقديم المساعدة الإنسانية. ربما ينتهي النزاع المسلح. ربما يكون موسم الأمطار ويمكن جمع مياه الأمطار. لذلك، بينما من الممكن أن يموت المدنيون عطشًا في الأسابيع المقبلة، إلا أن ذلك ليس بالضرورة حتميًا. وأكثر من ذلك، لا يمكن التنبؤ به بثقة. علاوة على ذلك، قد يمكن تجنبه من خلال اتخاذ إجراءات علاجية محتملة. وفقًا للوجهة الثانية، أي خطر لوقوع إصابات بين المدنيين سيكون بعيدًا جدًا ليُعتبر بشكل معقول ناتجًا عن الهجوم. لذلك، لن تُعتبر هذه الوفيات ضررًا غير مباشر متوقعًا نتيجة للهجوم ولن يتم احتسابها في القانون الدولي العرفي

Ibid,P.854

([87]) Michael N.Schmitt, Tallinn Manual 2.0, op. cit., p. 471

([88]) Ibid,P.471

([٨٩]) لا يُسمح إلا بالضرر العرضي الذي يكون مفرطًا بالنسبة للميزة العسكرية الملموسة والمباشرة المتوقعة. مصطلح 'مفرط' غير محدد في القانون الدولي. ومع ذلك، كما هو مذكور في دليل الأسلحة التقليدية، فإن المبالغة "ليست مسألة عدّ الإصابات المدنية ومقارنتها بعدد مقاتلي العدو الذين تم إخراجهم من الخدمة". المقياس الأساسي ليس مقدار الضرر الذي يلحق بالمدنيين وممتلكاتهم بشكل مجرد. بدلاً من ذلك، السؤال هو ما إذا كان الضرر المتوقع مفرطًا بالمقارنة مع الميزة العسكرية المتوقعة في ظل الظروف السائدة في ذلك الوقت. وعلى الرغم من وجود تأكيد معاكس في تعليق البروتوكولات الإضافية للصليب الأحمر ١٩٨٧، اتخذ غالبية مجموعة الخبراء الدولية موقفًا مفاده أن الضرر العرضي الواسع قد يكون قانونيًا إذا كانت الميزة العسكرية الملموسة والمباشرة المتوقعة كبيرة بما فيه الكفاية. وعلى النقيض، حتى الضرر الطفيف قد يكون غير قانوني إذا كانت الميزة العسكرية المتوقعة ضئيلة.

Ibid,P.473

([٩٠]) من المهم ملاحظة أن المعيار لهذه القاعدة مستقبلي. استخدام كلمتي 'متوقع' و'مرجو' يشير إلى أن تطبيقها يتطلب تقييم مدى معقولية القرار في الوقت الذي تم فيه التخطيط للهجوم المعني، أو الموافقة عليه، أو تنفيذه. عند اتخاذ مثل هذه القرارات، ويجب النظر في كل ما يبدو موثوقًا فالتوقع والترقب لا يتطلبان اليقين المطلق بحدوث الأمر. وبالمثل، فإن مجرد احتمال حدوثه لا يكفي لنسب التوقع أو الترقب إلى من يخططون أو يوافقون أو ينفذون هجومًا إلكترونيًا. مصطلحي 'متوقع' و'مترقب' يتيحان 'هوامش تقدير واسعة إلى حد ما'.

Ibid,P.474

([91]) Ibid,p.474

([92]) Peter Pascucci ,OP.cit,P.447

([93]) Reuben Ramases, Legal Challenges on the Proportionality Principle under International Humanitarian Treaties (Bachelor's Research Paper, University of Dodoma, Tanzania, 2021),P.43

([94]) Ibid,P.44

([95]) Ibid,P.45

([96]) Ibid,P.45

([97]) J. C. van den Boogaard,OP.cit,P.149

المصادر

أولا- الكتب الاجنبية

1) Dörmann, Knut. Applicability of the Additional Protocols to Computer Network Attacks. In Yearbook of International Humanitarian Law, Vol. 4. The Hague: T.M.C. Asser Press, 2001.
2) Roschini, Marco. Cyber Operations and the Use of Force in International Law. Oxford: Oxford University Press, 2014.
3) Schmitt, Michael N., ed. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. 2nd ed. Cambridge: Cambridge University Press, 2017.
4) Tikk, Eneken, Kadri Kaska, and Liis Vihul. International Cyber Incidents: Legal Considerations. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2010.
5) Tikk, Eneken, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm, and Liis Vihul. Cyber Attacks Against Georgia: Legal Lessons Identified. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2010.
6) van den Boogaard, J. C. Proportionality in International Humanitarian Law. PhD diss., University of Amsterdam, 2019.
7) Ramases, Reuben. Legal Challenges on the Proportionality Principle under International Humanitarian Treaties. Bachelor's
8) Research Paper, University of Dodoma, Tanzania, 2021.

ثانياً: المقالات العلمية

1) Al-Nabhani, Anfaal Said. "Cyber Operations as a Challenge to the Implementation of International Humanitarian Law (IHL)." Sultan Qaboos University Legal Studies Journal 4 (2025).
2) Boylan, Eric. "Applying the Law of Proportionality to Cyber Conflict: Suggestions for Practitioners." Vanderbilt Journal of Transnational Law 50, no. 1 (2017).
3) Dörmann, Knut. "Applicability of the Additional Protocols to Computer Network Attacks." Yearbook of International Humanitarian Law 4 (2001): 139–153.
4) Fenton III, Hensey A. "Proportionality and Its Applicability in the Realm of Cyber-Attacks." Duke Journal of Comparative & International Law 29, no. 2 (2019): 321–357.
5) Gisel, Laurent, Tilman Rodenhäuser, and Knut Dörmann. "Twenty Years On: International Humanitarian Law and the Protection of Civilians Against the Effects of Cyber Operations During Armed Conflicts." International Review of the Red Cross 102, no. 913 (2020): 287–334.

6) Hathaway, Oona A., Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegel. "The Law of Cyber-Attack." California Law Review 100, no. 4 (2012): 817–885.
7) Heikkinen, Tuomas, and Martin Faix. "The Use of Human Shields and the Principle of Proportionality under the Law of Armed Conflict." Czech Yearbook of International Law 7 (2016).
8) Jensen, Eric Talbot. "Cyber Attacks: Proportionality and Precautions in Attack." International Law Studies 89 (2013): 183–220.
9) Lin, Herbert S. "Offensive Cyber Operations and the Use of Force." Journal of National Security Law & Policy 4 (2010): 63–86.
10) Rid, Thomas. "Cyber War Will Not Take Place." Journal of Strategic Studies 35, no. 1 (2012): 5–32.
11) Schmitt, Michael N. "Cyber Operations and the Jus in Bello: Key Issues." International Law Studies 87 (2011): 89–110.
12) Winter, Elliot. "Autonomous Weapons in Humanitarian Law: Understanding the Technology, Its Compliance with the Principle of Proportionality and the Role of Utilitarianism." Groningen Journal of International Law 6, no. 1 (2018).
13) Kozlowski, Andrzej. "Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan." In Proceedings of the International Scientific Forum (ISF 2013), vol. 3, 2013.

ثالثاً: وثائق وتقارير المنظمات الدولية

اللجنة الدولية للصليب الأحمر (ICRC)

1) International Committee of the Red Cross (ICRC). International Humanitarian Law and the Challenges of Contemporary Armed Conflicts. Geneva: ICRC, 2019.
2) International Committee of the Red Cross (ICRC). International Humanitarian Law and the Challenges of Contemporary Armed Conflicts. Geneva: ICRC, 2025.

الأمم المتحدة

1) United Nations General Assembly. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/70/174. New York: United Nations, 22 July 2015.

رابعاً: أحكام محكمة العدل الدولية

1) Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Judgment. I.C.J. Reports 1986.
2) Oil Platforms (Islamic Republic of Iran v. United States of America). Judgment. I.C.J. Reports 2003.
3) Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda). Judgment. I.C.J. Reports 2005.

خامساً: المراجع العربية

١) أحمد عبيس الفتلاوي، وزهراء عماد محمد. "تكييف الهجمات السيبرانية في ضوء القانون الدولي." مجلة الكوفة للعلوم القانونية والسياسية، المجلد ١٢، العدد ٤٤، الجزء الأول (٢٠٢٠): ٥١–٧٨.

٢) اللجنة الدولية للصليب الأحمر. القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة. جنيف: اللجنة الدولية للصليب الأحمر، ٢٠١٩.

٣) اللجنة الدولية للصليب الأحمر. القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة. جنيف: اللجنة الدولية للصليب الأحمر، ٢٠٢٥.

٤) الأمم المتحدة، الجمعية العامة. تقرير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي. الوثيقة A/٧٠/١٧٤، ٢٢ تموز/يوليو ٢٠١٥.

سادساً: المواقع الإلكترونية

1) National Cyber Security Centre. **"Cyber Attack."** Accessed July 11, 2026.

2) Thomas Rid. **"Cyber War Will Not Take Place."** DOI:10.1080/01402390.2011.608939.

3) Al-Nabhani, Anfaal Said. "Cyber Operations as a Challenge to the Implementation of International Humanitarian Law (IHL)." DOI: 10.61190/squlsj.1031.