اقتباس: محمود.احمد.م.الحياني.فتحي. م . (٢٠٢٣). تحديات تطبيق مبدأ التناسب على الهجمات السيبرانية.
مجلة دراسات إقليمية. ١٧ (٥٨).٢٢٩-٢٧٠: https://doi.org/10.33899/regs.2023.138761.1143

تحديات تطبيق مبدأ التناسب على الهجمات السيبرانية

أحمد مؤيد محمود أ.م.د. فتحي محمد فتحي الحياني
كلية الحقوق/ جامعة الموصل
ah93mad@gmail.com

الاستلام: ٢٠٢٣/٣/٥ القبول: ٢٠٢٣/٤/٥ النشر: ٢٠٢٣/١٠/١

مستخلص البحث

يهدف البحث إلى الاحاطة بموضوع مبدأ التناسب في الهجمات السيبرانية هو الإحاطة بهذا المبدأ كونه اهم المبادئ التي يقوم عليها القانون الدولي الإنساني وبيان أوجه او حالات القصور، ومحاولة إيجاد الحلول التي تجسد هذا المبدأ وتطبيقه على ارض الواقع كما يجب ان يكون وليس كما هو كائن في النزاعات المسلحة الحديثة التي تستخدم فيها الهجمات السيبرانية. وتكمن أهمية البحث في فحص مدى قدرة نصوص قانونية كتبت في فترة معينة على التعامل مع الهجمات السيبرانية، من خلال تسليط الضوء على مبدأ التناسب كونه المبدأ الاساسي الذي يوفر الحماية للسكان المدنيين والاعيان المدنية اثناء القتال. تكون البحث من مبحثين رئيسين، تناول الأول مفهوم الهجمات السيبرانية اما المبحث الثاني فتناول تطبيق مبدأ التناسب على الهجمات السيبرانية. ومن أهم الاستنتاجات التي خرج بها البحث أن الهجمات السيبرانية تفتقر الى الإطار القانوني الصارم للتعامل معها، وقواعد مبدأ التناسب في القانون الدولي وان كانت تطبق على تلك الهجمات الا انها لا تغطي جميع الحالات وتترك مساحات رمادية مليئة بالإشكاليات.

الكلمات المفتاحية: السيبرانية؛ مبدأ التناسب؛ الهجوم السيبراني.

Citation: Mahmood, A. M.ALhyyani.F.m. (2023), Challenges of Applying Proportionality to Cyber Attacks. *Regional Studies Journal*, 17 (58). 229-270:
https://doi.org/10.33899/regs.2023.138761.1143

Challenges of Applying Proportionality to Cyber Attacks

Ahmad M. Mahmood **Assist. Prof. Fathi M. F. Alhayyani**

College of Law/ University of Mosul

ah93mad@gmail.com

Received: 5/3/2023 **Accepted: 5/4/2023** **Published: 1/10/2023**

Abstract

The research aims to comprehensively tackle the subject of the principle of proportionality to cyber-attacks since it is the most important principle on which international humanitarian law is based, to indicate the aspects or cases of shortcomings, to try to find solutions that embody this principle and apply it on the ground as it should be and not as it is in modern armed conflicts in which cyber-attacks are used. The importance of the research lies in examining the ability of legal texts written in a certain period to deal with cyber-attacks by highlighting the principle of proportionality as the basic principle that protects the civilian population and civilian objects during combat. The research consisted of two main sections, the first one treated the concept of cyber-attacks and the second section addressed the application of the principle of proportionality to cyber-attacks. One of the essential conclusions of the research is that cyber-attacks lack a strict legal framework to deal with them, and the rules of the principle of proportionality in international law, although they are applied to these attacks, they do not cover all cases and leave areas that are full of problems .

Keywords: Cyber; principle of proportionality; cyber-attack.

المقدمة

التناسب مبدأ أساسي في القانون الدولي يقضي بأن شرعية عمل ما تحدد حسب احترام التوازن بين الهدف والوسيلة المستخدمة لبلوغه وبين العواقب المترتبة على هذا العمل، وهو يعني ضمنا الالتزام بتقدير السياق قبل تحديد شرعية عمل ما أو عدم شرعيته، حيث يوازن التناسب بين فكرتين متناقضتين، تتمثل الأولى بالضرورة العسكرية لإضعاف قوة العدو وتحقيق النصر، أما الفكرة الثانية فتتمثل بالاعتبارات الإنسانية وكل ما يقتضيه الضمير الانساني لحماية المدنيين والاشخاص العاجزين عن القتال والاعيان المدنية اثناء سير العمليات القتالية.

وظهر مصطلح الهجمات السيبرانية للإشارة الى وسائل واساليب القتال التي تتألف من عمليات في الفضاء الالكتروني ترقى الى مستوى النزاع المسلح او تجري في سياقه، وتتميز الهجمات السيبرانية عن الهجمات التقليدية في أن نطاق الهجمة التقليدية المجال المادي الملموس، في حين نطاق الهجمة السيبرانية المجال الرقمي غير الملموس، مما يستدعي البحث في مدى مراعاة هذا النوع من الهجمات لقواعد مبدأ التناسب.

هدف البحث: ان الهدف من وراء دراسة موضوع مبدأ التناسب في الهجمات السيبرانية هو الإحاطة بهذا المبدأ كونه اهم المبادئ التي يقوم عليها القانون الدولي الإنساني وبيان أوجه او حالات القصور، ومحاولة إيجاد الحلول التي تجسد هذا المبدأ وتطبيقه على ارض الواقع كما يجب ان يكون وليس كما هو كائن في النزاعات المسلحة الحديثة التي تستخدم فيها الهجمات السيبرانية.

أهمية البحث: تبرز أهمية البحث في ازدياد اعتماد الدول على الهجمات السيبرانية لما توفره من وقت وجهد ومال لتحقيق أهدافها وكذلك حجم الدمار الذي يمكن ان تسببه تلك الهجمات والذي قد يراه البعض يضاهي حجم الدمار الذي تسببه أسلحة الدمار الشامل، فضلا عن ان ميدان الهجمات السيبرانية هو شبكة الانترنت حيث التواجد المكثف للمدنيين مما يزيد من احتمالية انتهاك مبدأ التناسب في الهجمات السيبرانية. تكمن أهمية البحث في فحص مدى قدرة نصوص قانونية كتبت في فترة

معينة على التعامل مع الهجمات السيبرانية، من خلال تسليط الضوء على مبدأ التناسب كونه المبدأ الاساسي الذي يوفر الحماية للسكان المدنيين والاعيان المدنية اثناء القتال.

إشكالية البحث: تتجسد إشكالية البحث في محاولة الإجابة على الأسئلة الاتية:

١. هل المرونة التي جاءت في قواعد مبدأ التناسب كافية للتعامل مع الهجمات السيبرانية، مع التطور المستمر في وسائل وأساليب الحرب على خلاف قواعد القانون الدولي الإنساني الثابتة؟

٢. مدى إمكانية تحقيق الموائمة بين الهجمات السيبرانية ومبدأ التناسب في جميع الأحوال والظروف اثناء سير العمليات العدائية؟

فرضية البحث: نفترض أنه على الرغم من المرونة التي جاءت بها القواعد القانونية التي تنظم مبدأ التناسب في القانون الدولي الإنساني وقدرتها على استيعاب التغيرات التي تطرأ في المستقبل، إلا انه يوجد مساحات رمادية من الصعب امكانية استيعابها من قبل هذه القواعد التي صيغت في زمن كانت الاسلحة التقليدية هي السائدة.

منهجية البحث: سنتبع في موضوع بحثنا المنهج العلمي الاستقرائي في فهم المقصود بموضوع التناسب في الهجمات السيبرانية من خلال جمع المعلومات التي توفرها المؤلفات العلمية والدراسات والبحوث المتعلقة بهذا الشأن، وقراءتها والتعمق فيها وصولاً إلى إعطاء مفهوم شامل حول الموضوع، وأيضا سنتبع المنهج التحليلي بالرجوع الى القواعد القانونية الدولية الخاصة بمبدأ التناسب وتحليلها ومعرفة مدى ملاءمتها مع الأنماط الجديدة للهجمات.

هيكلية البحث: تكونت هيكلية البحث من مبحثين فضلا عن المقدمة والخاتمة، سنتناول في المبحث الأول مفهوم الهجمات السيبرانية من خلال التطرق الى تعريفها في المطلب الأول وتحديد أنواعها وطبيعتها في المطلب الثاني، اما المبحث الثاني سنخصصه لتطبيق مبدأ التناسب على الهجمات السيبرانية من خلال مطلبين نبين في الأول مدى خضوعها لمبدأ التناسب، ونخصص الثاني لبيان التحديات التي تواجه تطبيق التناسب على الهجمات السيبرانية.

المبحث الأول

مفهوم الهجمات السيبرانية

ادى التطور الكبير والمتسارع في تكنولوجيا المعلومات والاتصالات الى اعتماد الدول عليها بشكل كبير سياسيا واجتماعيا واقتصاديا وعسكريا، لذلك تستهدف الهجمات السيبرانية البنية التحتية التي تعتمد في عملها على شبكات الكومبيوتر والانترنت، فتتحكم وتسيطر على الحواسيب والمعلومات والشبكات الالكترونية والبنية التحتية المعلوماتية، وهي لا تقل شأناً عن الهجمات التقليدية من حيث الخطر وحجم التدمير الذي تحدثه. وعليه سنقسم المبحث الى مطلبين، نتناول في الأول تعريف الهجمات السيبرانية، ونبين في الثاني أنواع الهجمات السيبرانية وطبيعتها.

المطلب الأول

تعريف الهجمات السيبرانية

ان من التحديات التي تواجه المجتمع الدولي هي عدم وجود تعريف مشترك للهجمات السيبرانية التي أصبحت تزداد وتواكب التطور التكنولوجي الحاصل لاسيما في المجال العسكري وبشكل مستمر حتى يومنا هذا، الامر الذي يدفعنا الى تناول تعريف الهجمات السيبرانية في فرعين، نخصص الأول لبيان المعنى اللغوي لها، والثاني لبيان التعريف الاصطلاحي. كالآتي:

الفرع الأول

التعريف اللغوي للهجمات السيبرانية

بدايةً لابد لنا من الوقوف على تحديد المعنى اللغوي للهجمات السيبرانية لإمكانية الوقوف على معناها اصطلاحا كونه مصطلح جديد حديث النشأة. فمصطلح السيبرانية نجد اصوله في اللغة اليونانية في مصطلح (kybernetes) الذي ورد أولا في مؤلفات الخيال العلمي ويقصد به القيادة او التحكم عن بعد (الطائي، ٢٠١٩، ٢٩). ثم انتقل الى اللغة الإنكليزية، في كتابات عالم الرياضيات نوربرت وينر (Norbert Wiener) حيث أشار الى مصطلح (Cybernetics) في

عنوان كتابه الصادر عام ١٩٤٨، اثناء دراسته لموضوع القيادة والسيطرة والاتصال فيما يخص الحيوانات وكذلك دراسته في حقل الهندسة الميكانيكية (Wiener, 1948).

اما في اللغة العربية، وبالرجوع الى القواميس العربية نجد ان قاموس المورد الحديث ترجم كلمة (Cyber) من اللغة الإنكليزية وعرفها بأنها (بادئة معناها: أ- كومبيوتريّ <Cybertalk>. ب- عصريّ جداً، وكما ترجم كلمة (Cybernation) بأنها السَّبرنة، وتعني الضبط الاوتوماتي لعمليةٍ ما عن طريق استخدام الكومبيوترات، كما وترجم أيضا كلمة (Cybernetics) وهي أصل كلمة (Cyber) -التي استخدمها نوربرت وينر السابق ذكره- وعرفها بانها (السَّيبَرناتيّة، السِّبَرنيّة، علم الضبط)، واخيراً ترجم القاموس كلمة (Cyberspace) الى الفضاء السيبراني وعرفه بانه (الفضاء الكومبيوتريّ: عالم الاتصالات المستخدمة للكومبيوتر، وخاصةً الانترنت) (البعلبكي، د.ت، ٣٠٧).

وفي اللغة العربية يواجه المختصين فيها صعوبة في الاتفاق على مصطلح معين يقابل مصطلح (Cyber) في اللغة الإنكليزية، فمن جهة نرى ان عنوان اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية (Convention on cybercrime) ترجم الى اللغة العربية (الاتفاقية المتعلقة بالجريمة الالكترونية)، ومن جهة أخرى فان الوثائق الرسمية الصادرة عن الأمم المتحدة باللغة العربية استخدمت مصطلح السيبرانية، وهو بهذا مشتق من مصطلح (Cyber) باللغة الإنكليزية (الفتلاوي، ٢٠١٦، ٦١٣).

الفرع الثاني

التعريف الاصطلاحي للهجمات السيبرانية

على الرغم من مرور مدة ليست بالقليلة على ظهور الهجمات السيبرانية، الا انه لم يتم الاتفاق على تعريف جامع مانع لها. فقد نظر البعض في تعريفه للهجمات السيبرانية من منظور ضيق يرى بانها تطال فقط الأنظمة والحواسيب والأدوات

السيبرانية، فقد عرفها مايكل شميت (Michael Schmitt) بأنها مجموعة من الإجراءات التي تتخذها الدولة للهجوم على نظم المعلومات المعادية بهدف التأثير والاضرار بها، وفي الوقت نفسه للدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة (Schmitt, 1999, 890). وفي ذات السياق ذهب كل من ريتشارد كلارك وروبرت كنيك الى تعريف الهجمات السيبرانية بانها اعمال تقوم بها دولة، تحاول من خلالها اختراق أجهزة الكومبيوتر والشبكات التابعة لدولة أخرى بهدف احداث اضرار بالغة او تعطيلها (ريتشارد و روبرت، ٢٠١٢، ٢٠).

كما أطلق عليها ماركو روسيني بالعمليات المعلوماتية التي يمكن اللجوء اليها في سياق نزاع مسلح، حيث عرف الهجمات السيبرانية بانها تطويع او الاستغلال المتكامل للإمكانيات التقنية من اجل التأثير على المواقع الالكترونية الأخرى او تعطيلها او تدميرها سواء كانت تقدم الخدمات المدنية ام العسكرية (Marco, 2010, 91).

وعرفت القيادة الاستراتيجية الامريكية في عام ٢٠٠٧ الهجمات السيبرانية بانها تطويع عمليات أنظمة الكومبيوتر لغرض منع الخصم من الاستخدام الفعَّال لها، فضلا عن التسلل الى نظم المعلومات وشبكات الاتصال بهدف الاستحواذ على البيانات التي تحتوي عليها وجمعها وتحليلها، (الفتلاوي، ٢٠١٦، ٧١٦). ويتفق هذا التعريف مع ما جاءت به المادة (٥) من اتفاقية بودابست عام ٢٠٠١ الخاصة بالجرائم الالكترونية والتي جرّمت إعاقة او عرقلة الاستخدام الشرعي لنظام المعلومات[١].

ومن جانب اخر تبنت منظمة شنغهاي للتعاون نهجاً واسعاً لتعريفها، اذ ترى ان الهجوم السيبراني جزء من الحرب، وأعربت عن مخاوفها بشأن التهديدات التي تشكلها إمكانية استخدام وسائل الاتصالات الحديثة وتقنياتها في المجال العسكري والمدني، بالإضافة الى تأثيراتها الاقتصادية والاجتماعية والثقافية والأخلاقية وغيرها،

فالهجوم السيبراني هو اعتداءات موجهة ضد نظم المعلومات والأجهزة لا سيما تلك المتصلة بالموارد الحيوية والبنية التحتية للدولة المستهدفة، (العبيدي، ٢٠٢١، ٤٥).

كما عرفها ماثيو واكسمان بانها الجهود الرامية الى تغيير او تعطيل أنظمة الحاسوب او الشبكات او تدميرها، او المعلومات والبرامج الموجودة عليها، وان الاضرار التي تسببها هذه الهجمات يمكن ان تصيب الحاسوب او البنية التحتية او حياة الأشخاص، وتتباين اضرار الهجمات السيبرانية من القرصنة الخبيثة وتشويه مواقع الانترنت الى الدمار واسع النطاق على البنية التحتية سواء العسكرية او المدنية المرتبطة بتلك الشبكات، (Waxman, 2011, 422). وفي ذات السياق عرفها جون (Johan Sigholm) بانها جزء من العمليات السيبرانية والتي تعمل على توظيف إمكانيات الفضاء السيبراني والاستخدام العدائي له من قبل الدولة والفاعلين من غير الدول في النزاعات والتي تعمل نيابة عنها، من اجل التسبب بالضرر او الدمار او سقوط الضحايا لتحقيق اهداف سياسية منها وعسكرية، (Sigholm, 2013, 6).

كما ان دليل تالين[٢] تبنى الاتجاه الواسع الذي يركز على النتائج والاثار، فعرف الهجمات السيبرانية في المادة ٣٠ منه بانها عمليات سيبرانية سواء كانت هجومية او دفاعية، والتي يهدف من خلالها بصورة معقولة التسبب بالإصابة او وفاة الأشخاص، او الاضرار او تدمير الاعيان، (Schmitt, 2013).

ومن جانبنا نذهب مع الاتجاه الواسع ونؤيد التعريف الذي أورده الخبراء في دليل تالين، اذ ان التطور الحاصل في مجال التكنولوجيا يتطلب الاخذ بالنتائج التي يمكن ان تسببها الهجمات السيبرانية سواء على أنظمة الحاسوب والشبكات والمعلومات المخزونة فيها، او ابعد من ذلك بالتسبب بوفاة الاشخاص او الاضرار بالأعيان او البنية التحتية المرتبطة بتلك الشبكات.

المطلب الثاني

أنواع الهجمات السيبرانية وطبيعتها

بعد ان عرفنا الهجمات السيبرانية نجد ان هناك أنواعاً مختلفة من هذه الهجمات كل منها تعمل بطريقة معينة ومختلفة، بالإضافة الى وجود تحدٍ اخر يواجه خبراء القانون يتعلق بطبيعة الهجمات السيبرانية، وعليه سنبين أنواعها وطبيعتها في فرعين كما يأتي:

الفرع الأول

أنواع الهجمات السيبرانية

تختلف أنواع الهجمات السيبرانية باختلاف الأدوات التي يستخدمها الطرف المهاجم وكذلك الهدف الذي يسعى الى تحقيقه من وراء الهجوم. وهذه الأنواع هي:

١- هجمات فيروسات الحاسوب: الفيروسات هي برامج مصممة خصيصا لإلحاق الضرر بالأنظمة المعلوماتية من خلال تدمير او تعطيل في برمجيات الحواسيب بصورة غير مرئية، مما يجعل امر اكتشافها او التعرف عليها صعباً للغاية، ولدى هذه الفيروسات أنواع عدة منها ما هو صعب التحديد واخر سهل ومنها ما هو سريع الانتشار ومؤذٍ ومنها ما هو بطيء يحتاج الى أيام او اشهر للانتشار واخر غير مؤذٍ يسبب الازعاج والارباك فقط، وتشكل الفيروسات الأسلحة الأساسية في الهجمات السيبرانية حيث يؤدي استخدامها الى ارسال المعلومات من الأماكن التي تغزوها، كما يمكن نشرها عبر الرسائل الالكترونية او نقل الملفات الالكترونية او تحميلها على أداة لحفظ البيانات، (فهمي، ٢٠١٧، ٢٥).

٢- هجمات ديدان الحاسوب: الديدان وهي برامج صغيرة قائمة بذاتها لا تعتمد على غيرها من البرامج، مخصصة للقيام بأعمال تدميرية او سرقة البيانات الخاصة بالمستخدمين اثناء التصفح على شبكة الانترنت، وتتميز الديدان الالكترونية بسرعة انتشارها وصعوبة التخلص منها وقدرتها الفائقة على التلون والتناسخ والمراوغة، الا انها تختلف عن الفيروسات في طريقة انتشارها وتميزها بالسرعة، فهي تقوم بنسخ

نفسها من جهاز الى اخر بواسطة شبكة الانترنت، اذ تحاول ان تصيب أكبر عدد من أجهزة الحاسب، (مواش، ٢٠١٧، ٥٠). ومن الأمثلة على ذلك دودة ميليسا التي انتشرت عام ١٩٩٩ وأدت الى خسائر قدرت بملايين الدولارات، حيث استخدم البريد الالكتروني لنشرها من خلال رسالة بريد الكتروني مزيفة تقوم فور فتحها بإرسال نفسها الى خمسين بريد الكتروني اخر، وأيضا دودة ستكسنت (Stuxnet Worm) التي انتشرت عام ٢٠١٠ عبرة أجهزة (Drives) (USB) عند وصلها بجهاز الحاسوب لتتمكن من الانتشار، حيث اصابت محطات توليد الطاقة النووية وتخصيب اليورانيوم في إيران، (عوامر، ٢٠١٨، ٢٥).

٣- حصان طروادة: هو عبارة عن جزء من برنامج صغير او شفرة مختبئ في برنامج أكبر يكون في الغالب من النوع واسع الانتشار والشهرة، وتقوم بمهمات خفية غالبا ما تكون إطلاق فيروس او دودة يعمل على اضعاف دفاعات الخصم قبل اندلاع الحرب، حيث يقوم بإرسال بيانات عن الثغرات الموجودة في النظام وسرقة المعلومات السرية للهدف، (عادل، ٢٠٠٩، صفحة ١٢١). وقد يلجأ المهاجمون الى ثغرة تسلل لها نفس فكرة حصان طروادة، وهي برامج حاسوب غير مرخصة تضاف الى برنامج ما ليسمح بالدخول الى برنامج الحاسوب، فغالبا ما يلجأ المهاجم بعد اختراق الشبكة لأول مرة الى ترك ثغرة تسلل ليتمكن من الدخول مرة أخرى في المستقبل بطريقة أسرع وأسهل، وأحيانا تسمح لهم ثغرة التسلل هذه الوصول الى الجذر فتصبح لديهم الصلاحيات التي يتمتع بها مصمم البرنامج، (جواد، ٢٠١٩، ٢٤٤).

٤- هجمات الحرمان من الخدمة: يطلق عليها هجمات حجب الخدمة (Dos)، وفي هذا النمط من الهجوم يرسل المهاجم عدد هائل من طلبات الاتصال او أوامر بروتوكولات الشبكات الى الهدف من اجل اغراقه في معالجة هذه الطلبات وتحميله اكثر من طاقته الاستيعابية ليصل أحيانا الى درجة عدم الاستجابة، وعدم قدرته على القيام بمهامه المعتادة، وثمة هناك نوع خطير من هذه الهجمات ويطلق عليه هجوم

تعطيل الخدمة الموزع (DDos)، حيث يعتمد في هجومه على توزيع البرامج المصدرة لسلسلة من طلبات الإغراق عبر عدد كبير من الأجهزة موزعة في أماكن مختلفة تعمل عن بعد، ليتم برمجة هذه الأجهزة جميعها للهجوم في وقت واحد على جهاز الخصم، ومن ثم اغراقه وتعطيله واخراجه عن الخدمة، ويعد هذا الهجوم الأخطر والاكثر ضراوة لعدم وجود حلول مباشرة له، (القحطاني، ٢٠١٥، ٦٦). ومثال على ذلك سلسلة الهجمات التي شنتها روسيا على استونيا عام ٢٠٠٧ والتي أدت الى حرمان العديد من السكان من خدمات أساسية عبر الانترنت.

٥- هجمات تعديل المعلومات او تدميرها: ويقصد بها الوصول الى المعلومات الخاصة بالخصم عبر شبكة الانترنت او الشبكات الخاصة، والقيام بعملية تعديل البيانات الهامة من دون ان يكتشف الخصم ذلك، فالبيانات تبقى موجودة لكنها مضللة قد تحدث نتائج كارثية خاصة اذا كانت هذه المعلومات تتعلق بخطط عسكرية او ما شابه، كما قد يلجأ المهاجم الى تدمير معلومات الخصم من خلال مسح وتدمير كامل للأصول والمعلومات والبيانات الموجودة على الشبكة، ويطلق عليه (تهديد سلامة المحتوى)، ويقصد بها احداث التغييرات في البيانات سواء بالحذف او التدمير من قبل اشخاص غير مخولين بذلك، (دحماني، ٢٠١٨، ٣٣). وقد يؤدي هذا الهجوم الى احداث اثار مادية كبيرة بالمنشآت الحيوية للخصم، وهذا ما حدث في هجوم ستكسنت الذي أدى الى تدمير ما يقارب ألف جهاز طرد مركزي في المفاعل النووي الإيراني.

٦- التجسس الالكتروني: هو عبارة عن عدة طرق لاختراق المواقع الالكترونية ومن ثم الحصول على معلومات قد تكون في غاية الأهمية والخطورة كان من المفترض ان تبقى سرية، وهذا ما حدث لوزارة الدفاع الامريكية البنتاغون عندما تم اختراقها من قبل اشخاص غير تابعين للقاعدة، وكذلك اختراق وزارة الدفاع الفرنسية الذي تعرضت له لغرض سرقة معلومات عن الاستطلاعات والمناورات والنظام الصاروخي للقوات الفرنسية، فالتجسس غالبا ما يكون عمليات تجسس دولية للحصول على معلومات

سرية رسمية خاصة بحكومة دولة ما من قبل دولة أخرى، وبهذا الخصوص لابد من الإشارة الى ان هناك شبكة تجسس عالمية أمريكية أوروبية اسمها ايشيليون (Echelon) اسستها وكالة الامن القومي ناسا بالتعاون مع عدد من المؤسسات الاستخبارية العالمية بهدف التجسس على كافة الاتصالات الرقمية والسلكية واللاسلكية والاتصالات عبر الأقمار الصناعية، (مدين، ٢٠٢٠، ٣٠).

الفرع الثاني

طبيعة الهجمات السيبرانية

بعد ان عرفنا الهجمات السيبرانية نجد ان هناك تحديا اخر يواجه خبراء القانون الدولي بخصوص طبيعة الهجمات السيبرانية، فهل يمكن اعتبارها سلاحاً أي انها وسيلة قتال بحد ذاتها ام هي طريقة قتال؟ وسوف نتناول الطبيعة وفق التقسيم الاتي:

اولاً: السيبرانية وسيلة قتال

هناك من يعتبر الهجمات السيبرانية وسيلة قتال إذا ما تم استخدام الهجوم السيبراني بحد ذاته للتسلل الى الأنظمة الالكترونية المعدة لحماية او تنظيم سير عمل المنشآت الحيوية من اجل السيطرة عليها وتدميرها، كمحطات توليد الطاقة النووية او السدود او المطارات، وهذا ما حدث في الهجوم السيبراني الذي قامت به الولايات المتحدة الامريكية على محطات توليد الطاقة النووية نطنز وبوشهر في إيران، مما أدى الى الحاق اضرار جزئية في عمليات تخصيب اليورانيوم، (الفتلاوي وكلنتر، ٢٠٢٠، ٥٤).

ومن ناحية أخرى فقد اختلف الفقهاء حول طبيعة الهجمات السيبرانية وإمكانية وصفها سلاحاً بحد ذاتها ام لا، وكذلك حول إمكانية خضوعها لاتفاقية الحد

من التسلح، فيرى البعض عدم صحة وصف الهجمات السيبرانية بانها سلاحا بحد ذاتها ويبررون موقفهم بالقول ان الهجمات السيبرانية تفتقر الى الطاقة الحركية فضلا عن عدم احتوائها على مواد شديدة الانفجار، وبالتالي فهم يستبعدونها بحكم طبيعتها من طائفة الأسلحة، في حين يرى البعض الاخر انه من غير المعقول استبعاد الهجمات السيبرانية من طائفة الأسلحة، وانه يمكن اعتبارها سلاحاً بحد ذاتها، فلا يشترط فيها الطاقة الحركية كما هو الحال بطبيعة الأسلحة الكيميائية، وكذلك عدم اشتراط احتوائها على مواد شديدة الانفجار كما في الأسلحة البيولوجية، فانه يمكن استخدامها بدون الحاجة الى قنابل او صواريخ وذلك بحكم طبيعتها ومجال استخدامها، (عاشور، ٢٠٢٢، ١٣٠).

وبعيداً عن ذلك، ذهب البعض من المختصين والخبراء الى إطلاق مصطلح التعطيل الشامل (mass disruption) لوصف الهجمات السيبرانية، فهو بهذا يقابل مصطلح الدمار الشامل (mass destruction) الذي يطلق على الأسلحة النووية والكيميائية والبيولوجية، (الفتلاوي، ٢٠١٦، ٦١٨). وفي هذا الوصف تعبير عن خطورة الهجمات السيبرانية التي تستهدف نظم المعلومات للخصم وتدميرها الكلي او الجزئي سواء العسكرية منها او المدنية، وكمية الدمار الذي يمكن ان يصيب البنية التحتية المعلوماتية او المادية بحكم الاعتماد المتزايد على نظم المعلومات في تسيير المنشآت الحيوية.

وفي حال اعتبار الهجمات السيبرانية وسيلة قتال فهل تندرج تحت الأسلحة التقليدية ام الأسلحة غير التقليدية؟ تعرّف الأسلحة غير التقليدية بانها الأسلحة التي يمكن لها ان تقتل اعداد كبيرة من البشر او تسبب خسائر فادحة للمنشآت الإنسانية او الطبيعية او المنطقة المحيطة بوجه عام، وتشمل الأسلحة الذرية والبيولوجية

والكيميائية، (القطارنة، ٢٠١٤، ص ٣٤١). في حين تعرّف الأسلحة التقليدية بانها غير أسلحة الدمار الشامل، فهي الأجهزة التي تمتلك القدرة على القتل او اتلاف أي هدف عسكري بواسطة المواد شديدة الانفجار، اما الأسلحة السيبرانية فتعرّف بانها مجموعة أدوات البرمجيات الخبيثة، كما عرفت بانها أدوات برمجية ضارة يتم نشرها لألحاق الضرر بشبكات وأنظمة الخصم، (عاشور، ٢٠٢٢، ١٢٩). ويعتبر مصطلح (أسلحة الدمار الشامل) مرادفاً للأسلحة غير التقليدية، وان الأسلحة البيولوجية والكيمياوية والذرية تعتبر أسلحة دمار شامل، ووفق تعاريف جديدة تندرج الأسلحة الراديولوجية تحت هذا المصطلح بل وحتى الأسلحة التقليدية التي ينتج عن استخدامها او تتسبب في خسائر فادحة، وقد تبنى هذا النهج الواسع برنامج الدفاع المدني للولايات المتحدة الامريكية، (الإسلام والقانون الدولي الإنساني (دراسة مقارنة) *Islam And International Humanitarian Law (Comparative Study)*، ٢٠١٧، ص ١٤٣).

وعليه فان الهجمات السيبرانية لها نفس القدرة التي تتمتع بها الأسلحة غير التقليدية في احداث اضرار لا حدود لها وعلى نطاق واسع، ولكن إذا كان بالإمكان اعتبار الهجمات السيبرانية وسيلة قتال فانه من الصعب تصنيفها بانها أسلحة غير تقليدية، كون ان اثارها نسبية تختلف من هجوم لآخر حسب طبيعة استخدامها.

ثانياً: **السيبرانية طريقة قتال**

هناك من يذهب الى عد الهجمات السيبرانية أسلوب قتال إذا كان من شأنها ان تسهم في دعم القوة العسكرية التقليدية وتسهل من عملها، من خلال توجيه العمليات العسكرية كالصواريخ بعيدة المدى والطائرات بدون طيار (Drawn) لتحديد اهداف عسكرية منتخبة وتدميرها، او لتعطيل أجهزة الرادار او أجهزة الكشف المبكر

للهجمات، او كان من شأنها تعطيل عمليات الاتصال في المطارات العسكرية او المدنية، او تعطيل شبكات الانترنت والاتصالات، (الفتلاوي وكلنتر، ٢٠٢٠، ٥٥).

ففي عام ٢٠٠٨ قامت روسيا بشن هجمات سيبرانية على جورجيا، باستخدام أسلوب حجب الخدمة، ونتج عن هذه الهجمات اضراراً كبيرة في خدمات الانترنت العامة في الدولة وعطل مواقع حكومية ونظام الاتصال (IT)، مما أدى الى اضعاف الدفاعات الجوية الجورجية، ولم يتوقف الهجوم الى هذا الحد، بل كانت الهجمات السيبرانية تمهيداً لحرب برية شنتها روسيا على جورجيا، وعليه يمكن اعتبار هذه الحالة انموذجاً تكون فيه الهجمات السيبرانية مجرد وسيلة مساعدة للجهد الحربي التقليدي العام، (ملفات ساخنة، ٢٠١٣، ٥١). وفي ذات السياق فان ما سبق يتجسد أيضا في الهجوم الذي شنته إسرائيل عام ٢٠٠٧ على منشأة في دير الزور في سوريا، حيث تمكنت من اختراق منظومة الاتصالات وأجهزة الرادار وتم تعطيلها عن العمل بطريقة تجعل الرادار يبين ان السماء صافية ولا وجود لطائرات معادية، ليتبعه بعد ذلك هجوم تقليدي نفذه سلاح الجو الإسرائيلي بقصف المنشأة بزعم انها تحتوي على مفاعل نووي، (الفتلاوي، ٢٠١٦، ٦١٩). ففي هذه الهجمات لم يتم استخدام الهجمات السيبرانية لتحقيق الهدف بذاتها بل لتمهيد الطريق للقوات العسكرية لتحقيق الميزة والتفوق على الخصم، وبالتالي يمكن عدها أسلوب قتال وادراجها ضمن التخطيط والتكتيك العسكري.

وفي التمييز بين وسائل القتال واساليبه ذهب توماس رد وبيتر ماكبورني الى القول بان العنصر المعنوي او النفسي حاسم في استخدام أي سلاح، وبشكل خاص السلاح السيبراني، وان وصف أي سلاح يتوقف على عنصرين، الأول هو العنصر المعنوي او النفسي الذي يتمثل برغبة المهاجم في الحاق الضرر بالهدف العسكري،

اما الثاني فهو العنصر العملي او المادي ويتمثل بالاستخدام الفعلي للسلاح وذلك بتوجيه السلاح فعلياً الى الخصم، كما ذكروا ان هناك أسلحة او أدوات مصممة خصيصا على انها سلاح، مثل البندقية، في حين ان هنالك أدوات عادية يمكن وصفها سلاحاً عندما يرغب الشخص باستخدامها على هذا النحو، (Thomas & Peter, 2012, 7). وهذا ما نجده في الهجمات السيبرانية وفي ذلك تأكيد على أهمية البعد المعنوي او الهدف من الهجوم في تحديد طبيعتها.

ومما تقدم يتبين ان الأسلوب المتبع في تحديد طبيعة الهجمات السيبرانية بانها وسيلة ام طريقة قتال هو معيار الغرض من استخدامها والنتيجة التي يمكن ان تحدثها، وتبين انها ذات طبيعة مزدوجة فهي وسيلة قتال وأسلوب قتال في الوقت نفسه، فاذا استخدمت بذاتها لتحقيق الهدف فتعتبر وسيلة قتال، اما اذا استخدمت كجزء من خطة عسكرية فتعد أسلوب قتال. ومن جانبنا نتفق مع ما سبق بالاعتماد على الهدف من الهجوم لتحديد طبيعة الهجمات السيبرانية، الا اننا نرى ان الهجمات السيبرانية بحكم طبيعتها الخاصة والمجال الذي تحدث فيه لا يمكن إطلاق اسم السلاح عليها بشكل عام وشامل كونها ليست مخصصة فقط للعمل العسكري، وبالتالي يمكن تكييف كل حالة على حدة وفق ما ينتج عن استخدامها من اثار او اضرار، كما انه يمكن اعتبار البرمجيات الخبيثة كالفيروسات والديدان وغيرها بأنها الأسلحة السيبرانية، كما ان المادة ٣٦ من البروتوكول الإضافي الأول جاءت بعبارة (.. دراسة او تطوير او اقتناء سلاح جديد او أداة للحرب او اتباع أسلوب للحرب..)[٣]، لكي تشمل كل فعل مخالف لقواعد القتال سواء اعتبر وسيلة ام أسلوب قتال، فهي كفيلة بان تلزم الدول على توافق اعمال قواتها المسلحة مع التزاماتها الدولية.

المبحث الثاني

مبدأ التناسب والهجمات السيبرانية

بعد ان بينا مفهوم الهجمات السيبرانية وطبيعتها وما يمكن ان تحدثه من اضرار عرضية تصيب المدنيين والاعيان المدنية سنحاول بيان مفهوم مبدأ التناسب وبيان مدى قابلية تطبيق الفلسفة التي يحملها مبدأ التناسب بالتوفيق بين مفهومين مختلفين متعارضين على الهجمات السيبرانية، سنقسم المبحث الى مطلبين نخصص المطلب الأول لتحديد مدى خضوع الهجمات السيبرانية لمبدأ التناسب، ونخصص المطلب الثاني لبيان أبرز التحديات التي تواجه تطبيق مبدأ التناسب على الهجمات السيبرانية.

المطلب الأول

مدى خضوع الهجمات السيبرانية لمبدأ التناسب

يعتبر مبدأ التناسب جوهر القانون الدولي الإنساني الذي يحمي المدنيين ان استطعنا القول من الضرورة العسكرية التي تبيح استهدافهم، وفي ظل الهجمات السيبرانية نشأ خلاف فقهي حول خضوعها لمبدأ التناسب، وهل يمكن لآلية عمل مبدأ التناسب التقليدية ان تنطبق على هذه الهجمات؟ وهذا ما سوف نتناوله في ثلاثة فروع كما يأتي:

الفرع الأول

مفهوم مبدأ التناسب

مبدأ التناسب من المبادئ الأساسية في القانون الدولي الإنساني يهدف الى التوفيق بين مقتضيات الضرورة العسكرية والاعتبارات الإنسانية، فان لم يستطع تغليب كفة الإنسانية فانه يسعى في اضيق الحدود الى المساواة بين الكفتين. وعليه سنتناول تعريف التناسب واساسه كما يأتي:

اولاً: تعريف مبدأ التناسب

ويقصد بمبدأ التناسب، مراعاة التوازن ما بين الضرر الذي يلحق بالخصم والمزايا العسكرية التي من الممكن تحقيقها نتيجة لاستخدام القوة اثناء سير العمليات القتالية، حيث يسعى مبدأ التناسب الى اقامة التوازن بين مصلحتين مختلفتين ومتعارضتين هما: الضرورة العسكرية الحربية والاعتبارات الانسانية، فتتمثل الاولى فيما تمليه مقتضيات الضرورة الحربية او العسكرية، بينما تتمثل الثانية فيما تمليه اعتبارات الانسانية عندما لا تكون هناك حقوق او محظورات مطلقة (بشير و إبراهيم، ٢٠١٢، ١١٧).

لا يوجد نص صريح يعرف مبدأ التناسب مما دفع فقهاء القانون الدولي لمحاولة ايجاد تعريف له. فقد عرف بيترو فيري مبدأ التناسب بأنه "مبدأ يهدف الى الحد من الضرر الناجم عن العمليات العسكرية، بحيث يقضي بأن تكون آثار وسائل واساليب الحرب المستخدمة متناسبة مع الميزة العسكرية المنشودة" (فيري، ٢٠٠٦، ٨٨).

كما عرّف بأنه "مبدأ التناسب هو كيفية التعاطي مع الهدف المراد مهاجمته بعد تحديد شرعية هذا الهجوم بفضل مبدأ التمييز، ويحدد مبدأ التناسب الوسيلة ومستوى التدخل لتحقيق التوازن ما بين الضرورة العسكرية والانسانية، وان اي خلل في تطبيق هذا المبدأ انما يعرض مرتكبه لواقع انتهاك القانون تحت عنوان الاستخدام المفرط للقوة" (سليم، ٢٠١٧، ١٤).

ويعرّف ايضا مبدأ التناسب بأنه "مقياس تحديد النسبة الشرعية والقانونية بين التفوق العسكري الحاصل نتيجة استخدام الوسائل والاساليب العسكرية المختلفة، وبين كمية سقوط ضحايا ناتجة عن هذا الاستخدام"، فقواعد القانون الدولي الانساني تلزم الاطراف المتحاربين بالامتناع عن شن الهجمات العشوائية ضد الممتلكات المدنية، وباتخاذ الاحتياطات قبل تنفيذ عملياتها، وبمراعاة مبدأ التناسب اثناء القيام بعمليات عسكرية ضد الخصم (شعبان، ٢٠١٥، ١٩٨).

ووفقا للتوازن الذي يتطلبه مبدأ التناسب فإنه يعتبر قيدا على وسائل القتال واساليبه من قبل الطرف المتحارب في الهجمات التي يمكن ان توقع اضرارا جسيمة مقارنةً بما يتحقق من ميزة عسكرية، فالموت والاضرار المدنية هي نتائج حتمية في كل نزاع مسلح، ولا يمكن تجنبها بشكل نهائي، غير انه من الممكن التقليل من هذه الآثار بين المقاتلين والمدنيين الى الحد الذي يكون مقبولا مع ما تقوم به القوات المقاتلة (العرداوي، ٢٠١٦، ٣١٩).

وعليه ومما تقدم فإن التناسب يعتبر معادلة صعبة ودقيقة خاصة اثناء القتال وادارة العمليات الحربية، فتحقيق النصر على العدو هدف اساسي للقوات العسكرية، وتنفيذ الالتزام بالقيم والاخلاق العسكرية وعدم الحاق اضرار مفرطة بالخصم التزام قانوني واجب النفاذ، وعليه فالأمر يحتاج الى قائد عسكري ماهر شديد المراس يكرس جهده وعمله في سبيل تسوية ميزان هذه المعادلة، ويمكن ان يتحقق ذلك بتوافر جملة من الواجبات او الشروط التي بتوفرها يقوم مبدأ التناسب وهي (الأنور، ٢٠٠٠، ص ٣١٩): -

١) السيطرة التامة للقائد العسكري على مرؤوسيه، وعلى مصادر النيران لمنع الانتهاكات الجسيمة لقانون النزاعات المسلحة.
٢) الاقتصار على العمليات اللازمة لقهر العدو وهزيمته، فمثلا تدمير ٦٠% من قدرات العدو العسكرية يكفي للتغلب عليه.
٣) عدم جواز اصدار الامر بعدم ابقاء أحد من العدو على قيد الحياة.
٤) الامتناع عن العمليات او استخدام الاسلحة التي تسبب آلاماً لا مبرر لها والمحظور استخدامها دوليا.
٥) عدم اللجوء الى الهجمات العشوائية، التي لا توجه الى هدف عسكري محدد.
٦) عدم القيام بهجمات ردع ضد السكان المدنيين او الاعيان المدنية.
٧) الحرص التام على توجيه كل الهجمات الى الاهداف العسكرية وعدم اصابة غيرها الا عرضاً وبشكل غير مباشر.

ثانياً: الأساس القانوني لمبدأ التناسب

ان مبدا التناسب وليد قاعدة عرفية في الأصل، تم فيما بعد تقنينها في صورة الاتفاقيات والبروتوكولات الدولية. وفي الدراسات التي أجرتها اللجنة الدولية للصليب الأحمر حول القانون الدولي الإنساني العرفي، اشارت الى مبدا التناسب بشكل واضح وصريح، فقد أوردته في القاعدة الرابعة عشر، والتي مفادها انه "يُحظر الهجوم الذي قد يُتوقع منه أن يُسبب بصورة عارضة خسائر في أرواح المدنيين أو إصابات بينهم، أو أضراراً بالأعيان المدنية، أو مجموعة من هذه الخسائر والأضرار، ويكون مفرطاً في تجاوز ما يُنتظر أن يُسفر عنه من ميزة عسكرية ملموسة ومباشرة" (هنكرس و والدبك، ٢٠٠٧، ٤١).

يعد علان سان بطرسبيرغ ١٨٦٨ بشأن حظر استعمال بعض القذائف وقت الحرب أول من اقر مبدأ التناسب في شكل قاعدة والتي مفادها "ان الهدف المشروع الوحيد الذي يجب ان تسعى اليه الدول اثناء الحرب هو اضعاف قوات العدو العسكرية"، وتبعاً لذلك فان اقصاء أكبر عدد من قوات العدو يكفي لتحقيق هذا الغرض، فمثلا تدمير ٦٠% من قدرات العدو العسكرية تكفي لتحقيق النصر (السعدي، ٢٠١٤، ٧٧).

اضافةً الى ان لائحة لاهاي المتعلقة بقوانين واعراف الحرب البرية لعام ١٩٠٧ جاءت تأكيداً لما تقدم وتأكيداً لمبدأ التناسب بالقول انه ليس للمتحاربين حق مطلق في اختيار وسائل الحاق الضرر بالعدو، كما حظرت اللائحة قتل او جرح العدو الذي يعلن استسلامه او الذي أصبح عاجزاً عن القتال، وأيضا حظرت استخدام الأسلحة والقذائف والمواد التي من شأنها احداث إصابات او الآم لا مبرر لها[٤].

ومن جهته أشار البروتوكول الإضافي الأول لعام ١٩٧٧ الملحق باتفاقيات جنيف الى مبدأ التناسب في المادة ٥١ بشأن حماية السكان المدنيين، والمادة ٥٧ بشأن التدابير الوقائية اثناء الهجوم[٥]. كما اشارت المادة ٥٧ من نفس البروتوكول الى مبدأ التناسب فيما يتعلق بالاحتياطات اثناء الهجوم وذلك في الفقرة ٢/أ وكذلك ما ورد

في الفقرة ٢/ب [٦].ويتبين ان مبدأ التناسب تم النص عليه ثلاث مرات في البروتوكول الأول، مرة في المادة ٥١، ومرتين في المادة ٥٧، في حين ان البروتوكول الإضافي الثاني لعام ١٩٧٧ لا يحتوي على إشارة واضحة لمبدأ التناسب في الهجوم، ولكن تم الزعم بأن هذا المبدأ هو صلب مبدأ الإنسانية وقد تأصل في ديباجة البروتوكول، ولذلك لا يمكن تجاهل مبدأ التناسب عند تطبيق البروتوكول.

ومن جهة أخرى فان المحكمة الجنائية الدولية اشارت لمبدأ التناسب في نظامها الأساسي لعام ١٩٩٨ في المادة ٨ منه في ان تعمد شن الهجوم مع العلم بأن مثل هكذا هجوم سيسبب خسائراً عرضية في أرواح المدنيين او إصابات في صفوفهم او اضرارٍ بالأعيان المدنية يفوق الميزة العسكرية المباشرة والملموسة[٧].

الفرع الثاني

الخلاف الفقهي بشأن خضوع الهجمات السيبرانية لمبدأ التناسب

ان الحديث عن قدم قواعد القانون الدولي الإنساني وحداثة الهجمات السيبرانية يثير مسألة ما إذا كانت لهذه القواعد القدرة على استيعاب هكذا تطور، وبناءً على ذلك نشأ خلاف فقهي حول إمكانية اخضاع الهجمات السيبرانية لمبدأ التناسب واحكام القانون الدولي الإنساني. وانقسم الفقه الى اتجاهين:

الاتجاه الأول: يذهب الى عدم خضوع الهجمات السيبرانية لقواعد القانون الدولي الإنساني. ويتزعمه بعض السياسيين الأمريكيين وعلماء التقنية وثلة قليلة من فقهاء القانون، ويطلق عليه (المذهب الحر)، الذي يرفض التعامل القانوني مع الانترنت ويقولون انه لا يخضع لقانون، وحجتهم ان الفضاء السيبراني عالم جديد لا يتفق والواقع المادي التقليدي، وانه يتسم بطابع عالمي مفتوح وانه مجال مشترك بين كل الدول، ويرون انه لا يمكن اخضاعه للقانون الدولي العام التقليدي بحجة ان هذا القانون لم ينجح الى حد الان في حكم الفضاء البحري او الجوي الخارجيين (موسى وأعمر، ٢٠١٦، ٣٤٠).

ومن الحجج التي يستند عليها أصحاب هذا الاتجاه هي ان مفهوم الهجمات السيبرانية حديث نسبياً وان قواعد القانون الدولي الإنساني المتعلقة بوسائل وأساليب القتال قد جرى تقنينها في وقت سابق على هذا المفهوم، بالإضافة الى ان هذه الهجمات لم تكن منظمة وفقاً للقواعد العرفية، ويرون ضرورة إعادة النظر في القانون الدولي الإنساني ليستوعب التطورات الجديدة، وأيضا يقول أصحاب هذا التوجه ان مفهوم الهجمات السيبرانية لم يرد في اتفاقيات جنيف ولاهاي وكذلك ميثاق الأمم المتحدة ومعاهدة حلف شمال الاطلس، حيث استخدمت هذه المواثيق على حدٍ سواء مصطلحاتٍ من قبيل "السلامة الإقليمية" و"القوة المسلحة" و"هجوم مسلح"، وهي مصطلحات لا تنسجم مع مفهوم الهجمات السيبرانية مما يضعها خارج نطاق القانون الدولي(رمضان، ٢٠٢١، ٣٠٧٤).

كما يرى أصحاب هذا الاتجاه ان تطبيق المبادئ العامة للقانون الدولي الإنساني على الهجمات السيبرانية تبدو غير واقعية، لان الوسائل والأساليب المستخدمة غير واضحة بشكلٍ كافٍ، وانها تتم بسرية تامة بالإضافة الى صعوبة تحديد هوية المهاجم، وتحدث بدون سابق انذار وغير محددة الأهداف بخلاف الهجمات التقليدية التي تكون أهدافها ومكانها محددين (أعمر، ٢٠١٨، ١٣٧)، ويستندون بالقول ان قواعد القانون الدولي الإنساني مصممة للتعامل مع الهجمات التقليدية التي تحتوي بطبيعتها على عنصر حركي، وان الهجمات السيبرانية لا تتضمن الا القليل مما هو مادي، مما يجعلها خارج نطاقه ، فهو يطبق على النزاعات المسلحة والهجمات السيبرانية ليس لها الطابع المسلح (هاجر، ٢٠١٩، ١٦٦).

الاتجاه الثاني: ذهب الى خضوع الهجمات السيبرانية لمبادئ واحكام القانون الدولي الإنساني، وان أصحاب هذا الاتجاه يستبعدون ويفندون الاحتماليات والحجج التي جاء بها الاتجاه السابق. فبالنسبة للحجة التي تقول ان الهجمات السيبرانية يرجع تاريخها الى ما بعد تقنين مواثيق القانون الدولي الإنساني تنطوي على مغالطة صريحة، حيث ان اللجنة الدولية للصليب الأحمر اكدت بالقول ان ليس لدى اللجنة

أي شك بشأن انطباق القانون الدولي الإنساني على الهجمات السيبرانية خلال النزاعات المسلحة تماماً مثلما ينظم استخدام الوسائل والأساليب الأخرى للقتال، جديدة كانت ام قديمة، وان الدول تعتمد معاهدات القانون الدولي الإنساني لتنظيم النزاعات المسلحة الحالية والمستقبلية، وانها أدرجت في هذه المعاهدات قواعد تتوقع تطوير وسائل وأساليب جديدة للقتال، على افتراض ان هذا القانون سينطبق عليها، وفي افتراض انه لم ينطبق على وسائل واساليب القتال في المستقبل، فلن يكون من الضروري مراجعة شرعية استخدام هذه الوسائل والأساليب بموجب القانون الدولي الإنساني حسبما تقتضيه المادة ٣٦ من البروتوكول الإضافي الأول لعام ١٩٧٧ (اللجنة الدولية للصليب الأحمر، ٢٠١٩، ٣). كما يستدل أصحاب هذا الرأي بفتوى محكمة العدل الدولية بشأن مشروعية استخدام الأسلحة النووية، حيث اشارت المحكمة الى ان المبادئ والقواعد الثابتة في القانون الدولي الإنساني تنطبق على كافة اشكال الحروب وعلى كافة أنواع الأسلحة بما في ذلك ما يكون في المستقبل[٨]. وعليه فانه لا يوجد تمييز بين الأسلحة النووية والهجمات السيبرانية من حيث التوقيت فكلاهما ظهر بعد تقنين القانون الدولي الإنساني، وبالتالي تنطبق قواعده على الهجمات السيبرانية.

كما يذهب أصحاب هذا الاتجاه الى القول ان الرأي المستند الى عدم وجود نص صريح ينظم الهجمات السيبرانية يجعلها خارج نطاق القانون الدولي الإنساني هو رأي ليس له أهمية تذكر، كون ان شرط مارتنز جاء كافيا لسد الثغرات في القانون، كما ان قبول العرف الدولي كمصدر للقانون الدولي، كما جاء في نص المادة ٣٨ من النظام الأساسي لمحكمة العدل الدولية، يعتبر تأكيداً على انطباق قواعد القانون الدولي الإنساني على الهجمات السيبرانية (نجيب، ٢٠١٢، ٢٢٧). كما ان اشتراط الطبيعة الحركية في الهجمات لا يمكن الاخذ به بدليل ان الهجمات البيولوجية والكيمياوية تخضع للقانون الدولي الإنساني على الرغم من انها لا تحتوي على عنصر حركي، وكذلك الحال في الهجمات السيبرانية (هاجر، ٢٠١٩، ١٦٦).

ومما تقدم يتبين عدم وجود فراغ قانوني فيما يخص الهجمات السيبرانية، كما ان المبادئ القانونية تبقى ثابتة ولكن تطبيقها العملي او الميداني يختلف من حالة الى أخرى ومن وقت لآخر وفقاً للأحوال والظروف السائدة، وعليه فان الهجمات السيبرانية تخضع لقواعد مبدأ التناسب في القانون الدولي الإنساني، ولابد من الإشارة الى ان قبول اخضاعها لمبدأ التناسب لا يعني خلوه من الصعوبات والتحديات، وهذا ما سنبينه في المطلب التالي.

الفرع الثالث

تطبيق مبدأ التناسب على الهجمات السيبرانية

يعد التناسب مبدأً ذو طابع عملي ميداني، يتضمن فلسفة خاصة تسعى الى تحقيق التوازن بين مفهومين متعارضين، الضرورة العسكرية والاعتبارات الإنسانية، ويحول دون ان تطغى احداهما على الأخرى اثناء سير العمليات العسكرية، وفيما يخص الهجمات السيبرانية فان تساؤلاً يثور حول قدرة هذه الهجمات على الامتثال لفلسفة التناسب؟

تضمن دليل تالين قاعدة خاصة بهذا المبدأ واكد على أهمية مبدأ التناسب في الهجمات السيبرانية ووجوب الالتزام به، حيث تضمن حظر الهجوم السيبراني الذي يتوقع ان يتسبب في خسائر عرضية في أرواح المدنيين او الإصابة بهم، او الحاق اضرار بالأعيان المدنية او مزيجاً منها، والتي تكون مفرطة فيما يتعلق بالميزة العسكرية الملموسة والمباشرة المتوقعة[٩]. وهو بهذا اشتق مبدأ التناسب من المادة (٥١) الفقرة (٥)، والمادة (٥٧) من البروتوكول الإضافي الأول، كما أشار الخبراء في الدليل الى ان حقيقة تعرض المدنيين او الاعيان المدنية للأذى اثناء الهجوم السيبراني على هدف عسكري مشروع لا تجعل الهجوم غير شرعي بحد ذاته، وانما تعتمد مشروعيته على مدى تحقيق الهجوم لمبدأ التناسب بين الاضرار العرضية التي أحدثها بصفوف المدنيين او الاعيان المدنية مقارنةً مع الميزة العسكرية التي يتوقع الحصول عليها نتيجة الهجوم[١٠].

وفيما يتعلق بمبدأ الضرورة العسكرية الذي يرتبط ارتباطاً وثيقاً بمبدأ التناسب، فان الهجمات السيبرانية يجب ان تحقق ميزة عسكرية اكيدة. ويذكر دليل تالين انه في الحالات التي يكون فيها الاختيار بين عدة اهداف عسكرية ممكنا توفر جميعها نفس الميزة العسكرية، فان الهدف الذي يتم توجيه الهجمة السيبرانية ضده هو الهدف الذي يتوقع منه ان يسبب ضرراً اقل، على ان تطبيق مبدأ الضرورة العسكرية يتطلب احداث الضرر الأقل، اما في حالة تعدد الأهداف الا ان احداها تحقق ميزة عسكرية أكثر من مثيلاتها، فان من حق المهاجم توجيه الهجمة السيبرانية الى الهدف الذي يحقق الميزة الاكبر مع وجوب مراعاة الاضرار العرضية المتوقعة (سعود، ٢٠١٨، ٩٤).

وعليه فان اللجوء الى الهجمات السيبرانية يجب ان يكون ضروريا لتحقيق الهدف العسكري وان الضرر الذي يطال المنشآت المدنية بداعي الضرورة العسكرية يشكل تحديا في الهجمات السيبرانية. ويؤيد ذلك ما ذهب اليه ريكس هيوغس (Rex Hughes) مدير شبكة الابتكار السيبراني في جامعة كامبرج، في ان الهجمات السيبرانية تخلق تحديا واضحا امام تطبيق مبدأ الضرورة العسكرية، ومن اجل حل هذه المعضلة لابد من تظافر الجهود الدولية بين خبراء القانون الدولي وخبراء الهندسة الالكترونية لتحديد ما يمكن ان يوصف بهدف (Hughes, 2010, 537).

ويقترن مبدأ الإنسانية بمبدأ الضرورة العسكرية، وهذا من شأنه ان يقلص من الاعمال غير الضرورية التي لا تحقق الميزة العسكرية المرجوة قياسا بالأضرار العرضية في الظروف السائدة، وهناك اتفاق على ان التسبب بآلام لا مبرر لها هو انتهاك لمبدأ الإنسانية، وفيما يخص الهجمات السيبرانية وتطبيق مبدأ الإنسانية عليها والتي تعتبر اهم قواعده عدم التسبب بآلام لا مبرر لها، فيمكن الإشارة الى ان تطبيق هذا المبدأ عليها لا يختلف عن صور وأساليب الهجمات الأخرى من حيث عدم التسبب بأضرار عرضية تفوق قيمة الهدف والفائدة المتوخاة من استهدافه (الموسوي، ٢٠١٩، ١٧٢).

بالنظر الى طبيعة الهجمات السيبرانية وترابط الأنظمة المدنية والعسكرية فمن المرجح انتهاك مبدأ التناسب، وهذا يمثل تحديا لدى خبراء القانون الدولي. فقد ذهب شين (Shin) الى القول بإمكانية تطبيق مبدأ التناسب على الهجمات السيبرانية ولكن علينا ان نسأل إذا كان بالإمكان عد الهجمات السيبرانية هجوما مسلحا لا يختلف عن الهجوم باستخدام الصواريخ مثلا، ويضيف قائلا ان مبدأ التناسب في استخدام القوة السيبرانية لا يزال غامضاً ويحتاج الى أجوبة ومن أهمها كيفية ضمان الالتزام بمبدأ التناسب في الرد على الهجمات السيبرانية (Beomchul, 2011, 118). وفي سياق متصل يقول ريكس هيوغس (Rex Hughes) إذا تم توجيه هجوم سيبراني على منشآت او أنظمة ثنائية الاستعمال مدنية وعسكرية عن بعد، فلا يبدو ان المنفعة العسكرية ستكون واضحة، وهذا ما يجعل من تطبيق مبدأ التناسب اثناء هذه الهجمات أمراً في غاية الصعوبة (Hughes, 2010, 538).

وفي سياق اخر فهناك من يرى انه لا يمكن استبعاد ان يؤدي التطور التكنولوجي في المستقبل الى إمكانية تطوير الهجمات السيبرانية لتتسبب بأضرار عرضية اقل من الهجمات التقليدية في ظروف معينة وذلك لتحقيق الميزة العسكرية نفسها (سعيد، ٢٠١٧، ١٩١). وعليه فان عدم وجود احكام صريحة تنظم الهجمات السيبرانية يجعل تطبيق مبدأ التناسب الحالي صعباً للغاية.

المطلب الثاني

التحديات التي تواجه تطبيق مبدأ التناسب على الهجمات السيبرانية

بعد ان بينا مفهوم كل من الهجمات السيبرانية ومبدأ التناسب وموقف الفقه من خضوعها لهذا المبدأ، فان هناك اشكالية تتعلق باعتبار الهجوم السيبراني هجوما بالمعنى الحقيقي، بالإضافة الى تحديات عملية تواجه تطبيق المبدأ في ظل طبيعة الهجمات السيبرانية وما يمكن ان تحدثه من اضار عرضية بالمدنيين، وعليه سنبين هذه التحديات في فرعين كما يأتي:

الفرع الأول

اعتبار الهجمات السيبرانية هجمات مسلحة

هنالك تساؤل حول مدى اعتبار الهجمات السيبرانية هجوما مسلحاً يحتوي على اعمال عنف تستوجب تطبيق القانون الدولي الإنساني؟ وما هو المعيار المعتمد لوصفها بأنها هجوم مسلح؟

تخضع الهجمات السيبرانية المنفذة في سياق نزاع مسلح للقانون الدولي الإنساني كما ينطبق على أي عمليات أخرى يتم الاضطلاع بها في سياق النزاع المسلح، وعلى الرغم من حداثة مفهوم الهجمات السيبرانية وعدم وجود قواعد محددة تتعامل معها الا ان فريق الخبراء الدولي اتفق بالإجماع على ان القانون الدولي الإنساني ينطبق على مثل هذه الهجمات في كل من النزاعات الدولية وغير الدولية[١١].

كما ان مبادئ التناسب والتمييز والاحتياط التي تحمي المدنيين والاعيان المدنية تنطبق فقط على العمليات العسكرية التي تشكل "هجمات" على النحو المحدد في القانون الدولي الإنساني، وتعرف المادة (٤٩) من البروتوكول الإضافي الأول الهجمات بأنها "اعمال العنف الهجومية والدفاعية ضد الخصم"[١٢]، على الرغم من ان هذا التعريف يعد واسعاً لأنه يشمل الاعمال الهجومية والدفاعية الا انه في المقابل يؤخذ عليه اشارته الى "العنف" وهي بهذا المعنى تشير الى القوة الفيزيائية الحركية فقط، بحيث لا تشمل أنواعا أخرى من الحروب لأنها لا تتضمن المعنى الفيزيائي الحركي للقوة مثل المقاطعة او الحرب الإعلامية وغيرها، لكن في المقابل تشمل كل وسيلة تحمل في مضمونها معنى الاكراه المادي الفيزيائي، وهذا ما حدث في حرب فيتنام عندما استخدمت القوات الامريكية زراعة الغيوم لزيادة نسبة الامطار من اجل إعاقة حركة العدو، فقد يبدو من غير المنطقي ان يعد المطر هجمات الا انه في هذه الحالة يمكن ان يحقق الإعاقة المادية الفيزيائية بالفعل ومن ثم ينطبق عليه تعريف الهجمة (الحياني، ٢٠٢٢، ١٢٢).

وبالتالي فان مدى تفسير مفهوم الهجوم على نطاق واسع او ضيق فيما يتعلق بالهجمات السيبرانية امر ضروري لانطباق هذه القواعد، ومن المتفق عليه ان الهجمات السيبرانية التي تتسبب بوفاة او إصابة او اضرار مادية تشكل هجوما مسلحا بموجب القانون الدولي الإنساني، سواء كانت الاضرار مباشرة ام غير مباشرة، مثل وفاة المرضى في وحدات العناية المركزة نتيجة لعملية سيبرانية ضد شبكة الكهرباء، كما ان من وجهة نظر اللجنة الدولية للصليب الأحمر فان الهجمات التي تعطل الخدمات الأساسية بشكل كبير دون ان تتسبب في الحاق اضرار مادية تصنف على انها هجوم مسلح، لان تضييق مفهوم الهجوم قد يجعلها خارج نطاق القانون الدولي الإنساني (اللجنة الدولية للصليب الأحمر، ٢٠١٩، ٧).

اما بشأن الهجمات السيبرانية المنفردة دون وجود نزاع مسلح. فقد ذهب مايكل شميت (Michael Schmitt) الى القول بأن تفسير اتفاقيات جنيف وبروتوكوليها الاضافيين لمفهوم النزاع المسلح بانه أي خلاف بين دولتين يؤدي الى تدخل القوات المسلحة، لا يعتمد عليه اذ لا يمكن ان يكون تدخل القوات العسكرية هو المعيار الوحيد، لانها قد تستخدم دون ان ينتج عنها نزاع مسلح، كعمليات الاستطلاع والمراقبة، كما من المقبول ان الحوادث المتفرقة مثل المناوشات الحدودية لا تصل الى مستوى النزاع المسلح (Schmitt, 2002, 372). في حين يشترط البعض لتطبيق مبادئ القانون الدولي الإنساني على الهجمات السيبرانية، ان تعزى الى دولة معينة وان تكون أكثر من حوادث متفرقة أي انها ممنهجة ومخطط لها فضلاً عن تحقيق الهدف من الهجوم بإحداث الاضرار (المالكي ونجيب، ٢٠١٦، ٤٦). ومن وجهة نظر الخبراء في دليل تالين فان بعض العمليات السيبرانية كالتي تؤثر على إيصال المساعدات الإنسانية تخضع للقانون الدولي الإنساني حتى عندما لا ترقى تلك العمليات الى مستوى الهجوم[١٣].

ومن الجدير بالذكر حول مفهوم الهجمة في سياق مبدأ التناسب، ان مفهوم الهجمة الوارد في المادة ٥١ والمادة ٥٧ يعد اضيق من مفهومها بموجب المادة ٤٩

من البروتوكول الأول والذي يشمل كل فعل ضد الخصم سواء أكان دفاعيا ام هجومياً، فقيام جندي بطلاق النار بشكل منفرد يعتبر هجمة بموجب المادة ٤٩ ولا يعتبر كذلك بموجب المواد ٥١ و٥٧ لانها حددت الأشخاص الذين يقومون بجمع المعلومات ويحددوا طبيعة الهدف، فمفهوم الهجمة في ظل هذه المواد يعتبر اكثر تعقيداً لانه يعتمد على سلسلة من الإجراءات التي يجب القيام بها قبل الشروع بالهجوم (الحياني، ٢٠٢٢، ١٢٨).

من وجهة نظر اللجنة الدولية للصليب الأحمر إذا تعطل أحد الاعيان عن العمل ليس مهماً كيفية حدوث ذلك، سواء بوسائل حركية ام بهجمات سيبرانية، ومما تقدم يتبين ان تطور وسائل وأساليب القتال لا سيما الهجمات السيبرانية يتطلب لتطبيق قواعد مبدأ التناسب في القانون الدولي الإنساني الاعتماد على معيار الأثر او النتائج التي تحدثها هذه الهجمات.

الفرع الثاني

التحديات العملية لتطبيق مبدأ التناسب

نظراً لطبيعة الهجمات السيبرانية والأهداف التي تصيبها والمتمثلة بأنظمة الاتصالات والشبكات ما يجعل الاضرار الجانبية بالمدنيين امراً محتملاً في كل هجمةٍ، مما يزيد عبء مبدأ التناسب للحكم على شرعية الهجمات السيبرانية، والذي لا يخلو من الصعوبات التي تواجهه عند تطبيقه على الهجمات السيبرانية. ويمكن لنا ان نبين أبرز هذه التحديات فيما يلي:

أولا:- الاستخدام المزدوج للأنظمة

وفق الفهم التقليدي للأعيان ذات الاستخدام المزدوج فان العين المدنية متى ما استخدمت لأغراض مدنية وعسكرية على حدٍ سواء، تصبح هدفا عسكريا مشروعاً، وهذا الهدف يجب ان يستوفي معيارين، الأول ان يسهم مساهمة فعالة في العمل العسكري، والثاني ان يحقق تدميره الكلي او الجزئي ميزة عسكرية اكيدة (ميلزر، ٢٠١٦، ٨٩). اما الفضاء السيبراني فان كثيرا من الاعيان التي تشكل بنيته الأساسية

ذات استخدام مزدوج يجعل منها اهدافاً عسكرية جذابة. وقد تناول دليل تالين مفهوم الاستخدام المزدوج وبيَّن ان الاعيان والأنظمة المستخدمة للأغراض المدنية والعسكرية بما فيها البنية التحتية السيبرانية، وان أي استخدام حتى وان كان مستقبلي يسهم في عمل عسكري يجعل من الاعيان هدفا عسكريا مشروعا، ويضيف أيضا ان أي هجوم سيبراني على هدف عسكري يستخدم أيضا جزئيا لأغراض مدنية يخضع لمبدأ التناسب والاحتياطات في الهجوم(١٤).

وتشكل الهجمات السيبرانية تحديات فريدة بشأن الشبكة التي تستخدم لأغراض عسكرية ومدنية على حدٍ سواء، فقد يكون من المستحيل تحديد أي جزء من الشبكة تتم عبره الارسالات العسكرية وايها للاستخدام المدني، ففي مثل هذه الحالات تكون الشبكة بأكملها هدفا عسكريا (الموصلي، ٢٠٢١، ٣٩). كما ان تعرض شبكة الانترنت او أجزاء كبيرة منها لهجوم سيبراني يترك إشكالية حول إمكانية استهدافها بالكامل او اجزاء منها عند استخدامها لأغراض عسكرية وكان تدميرها يوفر ميزة عسكرية اكيدة، وهذا التحدي مرهون أيضا بمبدأ التناسب (ب. ت. موسى، ٢٠٢٠، ٢١٠). فان الهجوم على شبكة الانترنت، من وجهة نظر الدليل او على أجزاء كبيرة منه قد يتعارض مع مبدأ التناسب، حيث يتم استخدام الانترنت بكثافة في الاستجابة للطوارئ المدنية، والدفاع المدني، والإغاثة، كما يتم استخدامه للتشخيص الطبي والوصول الى السجلات الطبية وطلب الادوية وغيرها(١٥).

وما يثير قلق اللجنة الدولية للصليب الأحمر ان يؤدي الاستخدام العسكري للفضاء السيبراني الى اعتبار العديد من الاعيان التي تشكل جزءا منه لم تعد محمية بصفتها اعيانا مدنية، وقد يؤدي ذلك الى تعطيل واسع النطاق للاستخدام المدني للفضاء السيبراني، وبذلك اذا انتفت الحماية على أجزاء معينة من البنية التحتية للفضاء السيبراني بوصفها اعيانا مدنية فان أي هجوم عليها سيبقى محكوماً بقواعد مبدأ التناسب (اللجنة الدولية للصليب الأحمر، ٢٠١٩، ٦). وعليه فان الاستخدام المزدوج للأعيان والشبكات يصعِّب من مهمة مبدأ التناسب في الهجمات السيبرانية مع

التوسع في حالات اللجوء الى الضرورة العسكرية والتوسع في مفهوم الأهداف العسكرية ليشمل المزدوجة الاستخدام منها.

ثانيا:- عدم القدرة على تحديد نتائج او آثار الهجوم

يتطلب تقييم مبدأ التناسب في النزاع المسلح توقع النتائج المحتملة لهجوم معين، ولكن عدم اليقين الإضافي سيجعل هذا التقييم اكثر صعوبة في سياق الهجمات السيبرانية، ونتيجة لذلك قد تغير هذه الهجمات التقييم المعطى للاثار المباشرة، وقد تجبر القادة العسكريين على مواجهة حالة عدم اليقين اكثر مما تواجهه في اتخاذ القرارات بشأن شرعية الهجمات المخطط لها، لذلك يشكل تقييم التناسب في الهجمات السيبرانية تحديا للمهاجم السيبراني، فقد يكون من الصعب تقييم ما اذا كان الهجوم سيكون متناسبا فيما يتعلق بالخسائر في أرواح المدنيين او الإصابات او الاضرار التي لحقت بالأعيان المدنية او مزيجا من ذلك مقابل الميزة العسكرية الاكيدة، فكيف ينبغي تقييم العجز المؤقت للأنظمة الحيوية المهمة، فقد يتسبب ذلك في عدم قدرة المستشفيات على توصيل المعلومات الحيوية مما يؤدي الى خسائر كبيرة بالأرواح، وبالتالي فان تقييم مبدأ التناسب المسبق لهجوم الحرمان من الخدمة قد يحمل درجة من عدم اليقين اكبر من أي هجوم تقليدي (Hathaway & Crootof, 2012, 851).

كما ان توقع نتيجة او أثر الهجوم السيبراني يتطلب قدرا كبيرا من المعلومات الاستخبارية حول الأنظمة المستهدفة، وانه حتى مع وجود هذه المعلومات فان عدد العوامل الخارجة عن سيطرة المهاجم يمكن ان تؤدي الى انتشار الهجوم عن غير قصد الى ما وراء الهدف المقصود، فالهجمات السيبرانية التي تستخدم فيروسا او دودة، على سبيل المثال، يمكن ان تخرج عن نطاق السيطرة بسرعة وتتسلل الى الأنظمة المدنية وتتسبب بالحاق اضرار تتجاوز نية المهاجم السيبراني (Gervais, 2012, 570).

ومما يزيد من تعقيد مبدأ التناسب مسألة الاثار غير المباشرة أي تلك التي لا تحدث بشكل وفوري نتيجة الهجوم، والمثال الأكثر استشهاداً هو الهجوم على شبكة الكهرباء العراقية في حرب الخليج ١٩٩١، على الرغم من انه نجح في تعطيل القيادة والسيطرة العراقية الا انه حرم السكان المدنيين من الكهرباء، مما اثر على المستشفيات والاستجابة للطوارئ، وكذلك قيام حلف الناتو باستهداف شبكة الكهرباء في يوغسلافيا السابقة، فرغم تعطيل منظومات الدفاع الجوي الا انه أدى الى اغلاق محطات ضخ مياه الشرب كأثر غير مباشر للهجوم السيبراني، وبالتالي فان مسألة الاثار غير المباشرة تؤثر على تطبيق التناسب لذلك يجب اخذها بالاعتبار عند التقييم .(Schmitt, 2002, 392)

وفي الحرب الدائرة حاليا بين روسيا وأوكرانيا أدى هجوم سيبراني في ٢٤ فبراير ٢٠٢٢ استهدف خدمة الانترنت عبر الأقمار الصناعية (KA-SAT) الى تعطيل الاتصالات العسكرية الأوكرانية، وهذا الهجوم الذي نسبه مسؤولون امريكيون الى وكالة التجسس العسكرية الروسية تجاوز الحدود الأوكرانية، حيث أدى الى قطع الانترنت عن عشرات الالاف من الناس في جميع انحاء أوروبا وأكثرها فرنسا، كما ظلت الشبكة مقطوعة عن حوالي (٢٠٠٠) عنفة هوائية في المانيا بعد مرور شهر على الهجوم (بوركهالتر، ٢٠٢٢). فعدم القدرة على توقع النتائج يعقد تطبيق مبدأ التناسب.

ثالثا:- التفاوت في إمكانيات تكنولوجيا المعلومات بين الدول

ينطوي تقييم تناسب الهجمات السيبرانية على صعوبة بالغة وذلك لان تكنولوجيا المعلومات والاتصالات غير متساوية في الدول، ومن ثم قد تكون الدولة التي تتعرض لهجوم سيبراني غير متطورة من ناحية مواجهة هكذا هجوم وصد الهجمات السيبرانية الموجهة ضدها (الفتلاوي وكلنتر، ٢٠٢٠، ٦٣). كما ان التفاوت في درجة الاعتماد على تكنولوجيا المعلومات في إدارة الدولة او بنيتها التحتية بين الدول قد يؤثر على تطبيق مبدأ التناسب من حيث حجم الاضرار العرضية التي تطال

المدنيين او الاعيان المدنية، والمثال على ذلك ما تعرضت له كل من استونيا وجورجيا، فالهجمات التي استهدفت شبكات الاتصال والانترنت كان لها اثر اكبر على استونيا من جورجيا نتيجة اعتمادها المتقدم على الفضاء السيبراني وتكنولوجيا المعلومات في إدارة الدولة، في حين لم تكن النتائج فادحة على جورجيا نتيجة للانخفاض النسبي في اعتماد جورجيا على تكنولوجيا المعلومات والاتصالات (محمد.، ٢٠٢١، ١٧٧). ومما تقدم فان كل هذه الصعوبات تطرأ عند تطبيق مبدأ التناسب اثناء الهجوم السيبراني مما يصعب مهمة أصحاب القرار عند تقدير النتائج المتوقع حدوثها من هجماتهم.

الخاتمة

تثير الهجمات السيبرانية العديد من الإشكاليات والتحديات وأبرزها ما يتعلق بتطبيق مبدأ التناسب في القانون الدولي الإنساني، نظراً للطبيعة التقنية للفضاء السيبراني الذي تحدث فيه والذي أصبح يشكل الميدان الجديد للنزاعات المسلحة، وانتشار تلك الهجمات في الفضاء المتشابك بين الاستخدامات العسكرية والمدنية يدفع الى التفكير في تطوير قواعد مبدأ التناسب لمعالجة الإشكاليات التي تثيرها الهجمات السيبرانية. وقد أسفر بحثنا عن عدة نتائج وتوصيات يمكن لنا ان نوردها كما يأتي:

اولاً:- الاستنتاجات:

١. وجود خلاف فقهي حول خضوع الهجمات السيبرانية لمبدأ التناسب وقواعد القانون الدولي الإنساني التي وضعت في وقت سابق على تلك الهجمات الامر الذي يزيد من صعوبة إيجاد إطار قانوني خاص يحكمها.

٢. ان الهجمات السيبرانية تفتقر الى الإطار القانوني الصارم للتعامل معها، وقواعد مبدأ التناسب في القانون الدولي وان كانت تطبق على تلك الهجمات الا انها لا تغطي جميع الحالات وتترك مساحات رمادية مليئة بالإشكاليات.

٣. ان معيار الأثر هو المعيار المتبع لاعتبار الهجمات السيبرانية هجمات مسلحة بالمعنى الحقيقي وان تطبيق مبدأ التناسب يتطلب الاخذ بهذا المعيار، فعند وقوع اضرار كبيرة فانه ليس مهما كيفية حدوثها.

٤. يواجه مبدأ التناسب مجموعة من التحديات منها ما يتعلق باعتبار الهجوم السيبراني هجوماً مسلحاً، وأخرى تحديات عملية تفرضها طبيعة الهجمات والفضاء الذي تحدث فيه، وأبرزها الاستخدام المزدوج للفضاء السيبراني للأغراض العسكرية والمدنية وصعوبة الفصل بينهما.

ثانياً:- التوصيات:

١. دعوة المجتمع الدولي الى انشاء اتفاقية خاصة بالهجمات السيبرانية تحدد تعريفها وتضع عناصره والتعامل معها بجدية أكثر، فتركها لقواعد ومبادئ القانون الدولي الإنساني العامة يفسح المجال امام الدول لاستخدامها دون مراعاة العواقب.

٢. ضرورة الاعتراف بالفضاء السيبراني ميداناً للحرب لا يقل أهمية عن بقية الميادين البرية والبحرية والجوية، وتحديد طبيعة الهجمات السيبرانية على انها اسلوب او طريقة قتال، واعتبار البرمجيات الخبيثة المتمثلة بالفيروسات والديدان والقنابل المنطقية وغيرها بانها أسلحة قتال سيبرانية.

٣. الحاجة الى تطوير قواعد القانون الدولي الإنساني الخاصة بالتناسب لتتماشى مع التطورات التقنية والتكنولوجية في وسائل الاتصال لاحتواء التحديات الجديدة التي تطرأ على الساحة الدولية.

الهوامش

(١) تنص المادة (٥) من اتفاقية بودابست على: (تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الأفعال التالية في قانونها الوطني، اذا ما ارتكبت عمداً وبغير حق: الإعاقة الخطيرة لاشتغال نظام الكومبيوتر عن طريق ادخال بيانات حاسوبية، ارسالها، اتلافها، حذفها، افسادها، تغييرها او تدميرها). للمزيد ينظر: مجلس اوروبا، مجموعة المعاهدات الاوربية، الاتفاقية المتعلقة بالجريمة الالكترونية، بودابست، ٢٠٠١.

(٢) دليل تالين :هو كتاب خاص بشأن القانون الدولي المطبق على الحروب السيبرانية أعدته مجموعة من الخبراء في القانون الدولي بين عامي 2013 بدعم من مركز التميز للدفاع الالكتروني التعاوني المرتبط بحلف الناتو ومقره العاصمة الاستونية) تالين (التي سمي الدليل باسمها، حيث يتكون الدليل من 154 قاعدة، تتضمن اراء الخبراء وتعليقاتهم على كل قاعدة منه.

(٣) نصت المادة ٣٦ من البروتوكول الإضافي الأول لعام ١٩٧٧ على "يلتزم أي طرف سام متعاقد، عند دراسة أو تطوير أو اقتناء سلاح جديد أو أداة للحرب أو اتباع أسلوب للحرب، بأن يتحقق مما إذا كان ذلك محظوراً في جميع الأحوال أو في بعضها بمقتضى هذا الملحق أو أية قاعدة أخرى من قواعد القانون الدولي التي يلتزم بها الطرف السامي المتعاقد.

(٤) ينظر: المادة ٢٢ والمادة ٢٣/الفقرة (ج) والفقرة (هـ) من لائحة لاهاي المتعلقة بقوانين وأعراف الحرب البرية.

(٥) نصت المادة ٥١ الفقرة (٥/ب) من البروتوكول الإضافي الأول لعام ١٩٧٧ الملحق باتفاقيات جنيف على "تعتبر الأنواع التالية من الهجمات، من بين هجمات أخرى، بمثابة هجمات عشوائية: ... ب- والهجوم الذي يمكن ان يتوقع منه ان يسبب خسارة في أرواح المدنيين او إصابة بهم او اضراراً بالأعيان المدنية، او ان يحدث خلطاً من هذه الخسائر والاضرار، يفرط في تجاوز ما ينتظر ان يسفر عنه ذلك الهجوم من ميزة عسكرية ملموسة ومباشرة

(٦) نصت المادة ٥٧ الفقرة ٢/أ من البروتوكول الإضافي الأول ١٩٧٧ على "يجب على من يخطط لهجوم او يتخذ قراراً بشأنه: ...ثانياً- ان يتخذ جميع الاحتياطات المستطاعة عند تخير وسائل وأساليب الهجوم من اجل تجنب احداث خسائر في أرواح المدنيين، او الحاق الإصابة بهم او الاضرار بالأعيان المدنية، وذلك بصفة عرضية، وعلى أي الأحوال حصر ذلك في اضيق نطاق.

ثالثا– ان يمتنع عن اتخاذ قرار بشن أي هجوم قد يتوقع منه، بصفة عرضية، ان يحدث خسائر في أرواح المدنيين او الحاق الإصابة بهم، او الاضرار بالأعيان المدنية، او ان يحدث خلطاً من هذه الخسائر والاضرار، مما يفرط في تجاوز ما ينتظر ان يسفر عنه ذلك الهجوم من ميزة عسكرية ملموسة ومباشرة". ونصت الفقرة ٢/ب من نفس المادة على "يلغى او يعلق أي هجوم إذا تبين ان الهدف ليس هدفاً عسكريا او انه مشمول بحماية خاصة او ان الهجوم قد يتوقع منه ان يحدث خسائر في أرواح المدنيين او الحاق الإصابة بهم، او الاضرار بالأعيان المدنية، او ان يحدث خلطاً من هذه الخسائر والاضرار، وذلك بصفة عرضية، تفرط في تجاوز ما ينتظر ان يسفر عنه ذلك الهجوم من ميزة عسكرية ملموسة ومباشرة".

(٧) ينظر: المادة ٨ الفقرة ب/٤ من النظام الأساسي للمحكمة الجنائية الدولية عام ١٩٩٨.

(٨) فتوى محكمة العدل الدولية بشأن مشروعية التهديد بالأسلحة النووية او استخدامها، ١٩٩٦، الفقرة ٨٦.

(٩) القاعدة ٥١ من دليل تالين.

(١٠) ينظر: التعليق رقم ٢ على القاعدة ٥١ من دليل تالين.

(١١) ينظر التعليق رقم ١ على القاعدة ٢٠ من دليل تالين التي نصت على "تخضع العمليات السيبرانية المنفذة في سياق نزاع مسلح لقانون النزاع المسلح".

(١٢) المادة ٤٩ من البروتوكول الإضافي الأول لعام ١٩٧٧.

(١٣) ينظر: التعليق رقم ٤ على القاعدة ٢٠ من دليل تالين.

(١٤) القاعدة ٣٩ من دليل تالين.

(١٥) ينظر: التعليق رقم ٦ على القاعدة ٣٩ من دليل تالين.

المصادر

المصادر العربية:

الإسلام والقانون الدولي الإنساني (دراسة مقارنة) Islam And International Humanitarian Law (Comparative Study). (٢٠١٧). (ط ٣). مركز الحضارة لتنمية الفكر الإسلامي.

أعمر، ع. م. (٢٠١٨). الحرب الإلكترونية في القانون الدولي الإنساني Electronic Warfare in the International Humanitarian Law. دراسات علوم الشريعة والقانون، ٤٦(٢).

الأنور، أ. (٢٠٠٠). قواعد وسلوك القتال Fighting Rules and Conduct. في دراسات في القانون الدولي الإنساني. اللجنة الدولية للصليب الأحمر.

بشير، هـ.، و إبراهيم، إ. ع. ر. (٢٠١٢). المدخل لدراسة القانون الدولي الإنساني Introduction To the Study of International Humanitarian Law. المركز القومي للإصدارات القانونية.

البعلبكي، م. (د.ت). المورد الحديث (قاموس إنكليزي – عربي) Al-Mawred Al-Hadith (English-Arabic Dictionary). دار العلم للملايين.

بوركهالتر، د. (٢٠٢٢, يونيو ١٠). متى يعد الهجوم الإلكتروني جريمة حرب؟ When Is a Cyber Attack A War Crime? https://www.swissinfo.ch.

جواد، أ. م. (٢٠١٩). الحرب في السياسة الخارجية الأمريكية بعد الحرب الباردة War In American Foreign Policy After the Cold War. الأكاديميون للنشر والتوزيع.

الحياني، ف. م. ف. (٢٠٢٢). القانون الدولي الإنساني وتطبيقاته على النزاعات المسلحة في العراق The International Humanitarian Law and Its Applications to Armed Conflicts in Iraq. جمعية الامل العراقية.

دحماني، س. (٢٠١٨). أثر التهديدات السيبرانية على الأمن القومي (الولايات المتحدة الأمريكية أنموذجاً (2001-2017) The Impact of Cyber Threats on National Security (The United States of America A Model (2001-2017))، رسالة ماجستير غير منشورة. جامعة محمد بوضياف.

رمضان، ش. ع. ا. ح. (٢٠٢١). الحرب السيبرانية ومدى ملاءمتها مع القانون الدولي الإنساني Cyber Warfare and Its Relevance with the International Humanitarian

Law. مجلة كلية الشريعة والقانون بتهفا، ٢٣(٤).

ريتشارد، ك.، وروبرت، ك. (٢٠١٢). حرب الفضاء الإلكتروني: الخطر القادم على الأمن القومي وسبل مواجهته Cyberwar: The Coming Threat to National Security and Ways to Confront It. مركز الامارات للبحوث والدراسات الاستراتيجية.

السعدي، و. ن. إ. (٢٠١٤). القانون الدولي الإنساني وجهود المجتمع الدولي في تطويره The International Humanitarian Law and The Efforts of The International Community in Its Development. دار الفكر الجامعي، الاسكندرية.

سعود، ي. ي. (٢٠١٨). الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني Cyber Warfare in Light of The Rules of the International Humanitarian Law. المجلة القانونية، ٤.

سعيد، د. (٢٠١٧). الحروب السيبرانية وأثرها على حقوق الإنسان (دراسة في ضوء أحكام دليل تالين) Cyberspace Warfare And Its Impact on Human Rights (A Study in The Light of The Provisions of The Tallinn Manual). المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية، ٥٤(٥).

سليم، ب. ش. (٢٠١٧). مبدأ التناسب في القانون الدولي The Proportionality Principle in The International Law، رسالة ماجستير غير منشورة. جامعة محمد الصديق بن يحيى جيجل.

شعبان، أ. خ. (٢٠١٥). الحماية الدولية والشرعية لضحايا النزاعات المسلحة القانون الدولي الإنساني (دراسة مقارنة) International And Legal Protection for Victims of Armed Conflicts, International Humanitarian Law (A Comparative Study). منشورات الحلبي الحقوقية.

الطائي، ح. أ. (٢٠١٩). المشاركة المباشرة للهبة الجماعية في الهجمات السيبرانية Direct Participation of The Collective Giveaway in Cyber Attacks. مجلة كلية الحقوق جامعة النهرين. ٢١(٢).

عاشور، أ. ح. (٢٠٢٢). فاعلية قواعد القانون الدولي الإنساني في تنظيم الهجمات السيبرانية The International Humanitarian Law Rules Effectiveness in Organizing Cyber Attacks. جامعة الموصل.

العبيدي، ع. ع. (٢٠٢١). مكافحة الجرائم السيبرانية كآلية لتعزيز الأمن السيبراني Combating Cybercrime as a Mechanism to Enhance Cybersecurity. مركز

الدراسات العربية.

العرداوي، م. ع. ن. (٢٠١٦). تقييد وسائل وأساليب القتال إعمالاً لمبادئ القانون الدولي الإنساني Restricting The Means and Methods of Fighting in Implementation of The Principles of the International Humanitarian Law, A Master's Thesis، رسالة ماجستير غير منشورة. جامعة بابل.

عوامر، ف. (٢٠١٨). تأثير القوة السيبرانية على الاستراتيجيات الأمنية للدول الكبرى (دراسة حالة الصين) The Cyber Power Impact on The Security Strategies of Major Countries (China Case Study). جامعة قاصدي مرباح.

الفتلاوي، أ. ع. (٢٠١٦). الهجمات السيبرانية (مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر) Cyber-Attacks (Their Concept and The International Responsibility Arising from Them in Light of The Contemporary International Organization). مجلة المحقق الحلي للعلوم القانونية والسياسية ٨(٤).

الفتلاوي، أ. ع.، وكلنتر، ز. ع. (٢٠٢٠). تكييف الهجمات السيبرانية في ضوء القانون الدولي Adapting Cyber Attacks in Light of International Law. مجلة الكوفة للعلوم القانونية والسياسية ١(٤٤).

فهمي، م. (٢٠١٧). البعد المعلوماتي في الحروب اللاتماثلية دراسة التنظيمات الإرهابية (داعش أنموذجاً) The Informational Dimension in Asymmetric Wars: Studying Terrorist Organizations (ISIS As a Model)، رسالة ماجستير غير منشورة. جامعة زيان عاشور.

فيري، ب. (٢٠٠٦). قاموس القانون الدولي للنزاعات المسلحة The International Law Dictionary of Armed Conflict.في ش. عتلم (محرر)، & م. وفاء (مترجم)، القانون الدولي الإنساني (دليل الأوساط الأكاديمية) International Humanitarian Law (A Handbook for Academia). اللجنة الدولية للصليب الاحمر.

القحطاني، ذ. ب. ع. (٢٠١٥). أمن المعلومات Information Security . مدينة الملك عبد العزيز للعلوم والتقنية.

القطارنة، ز. ح. (٢٠١٤). إدارة الكوارث Disaster Management. الأكاديميون للنشر والتوزيع.

اللجنة الدولية للصليب الأحمر. (٢٠١٩). القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة The International Humanitarian Law and Cyber Operations During Armed Conflicts.

المالكي، هـ. ن.، و نجيب، م. س. ع. (٢٠١٦). النطاق المكاني للعمليات الحربية في النزاعات المسلحة الدولية Spatial Scope of Military Operations in International Armed Conflicts. مجلة العلوم القانونية، ٣١(٤).

محمد.، أ. ع. (٢٠٢١). استخدام روسيا للقوة السيبرانية في إدارة تفاعلاتها الدولية Russia's Use of Cyber Power in Managing Its International Interactions. مجلة كلية الاقتصاد والعلوم السياسية،، ٢٢(٤).

مدين، م. (٢٠٢٠). فن التحقيق والإثبات في الجرائم الإلكترونية The Investigation and Evidence Art in Electronic Crimes. المصرية للطباعة والنشر.

ملفات ساخنة. (٢٠١٣). حرب التحكم الآلي (سلاح الحرب الخامس) War Automation (The 5th Weapon War). دار الجليل للنشر والتوزيع.

مواش، ض. ج. آ. (٢٠١٧). جريمة التجسس المعلوماتي (دراسة مقارنة) Information Espionage Crime (Comparative Study). المركز العربي للنشر والتوزيع.

الموسوي، ع. م. ك. (٢٠١٩). المشاركة المباشرة في الهجمات السيبرانية Direct Participation in Cyber Attacks. المؤسسة الحديثة للكتاب.

موسى، ب. ت. (٢٠٢٠). الحرب السيبرانية والقانون الدولي الإنساني Cyber Warfare and International Humanitarian Law. مجلة الاجتهاد القضائي، ١٢(٢٢).

موسى، ط. ح.، و أعمر، ع. م. (٢٠١٦). الإنترنت قانوناً Internet Legally. مجلة الشريعة والقانون، ٦٧.

الموصلي، ن. ا. (٢٠٢١). الهجمات السيبرانية في ضوء القانون الدولي الإنساني Cyber Attacks in Light of the International Humanitarian Law، رسالة ماجستير غير منشورة. الجامعة الافتراضية السورية.

ميلزر، ن. (٢٠١٦). القانون الدولي الإنساني (مقدمة شاملة) The International Humanitarian Law (A Comprehensive Introduction). اللجنة الدولية للصليب الأحمر.

نجيب، ن. (٢٠١٢). الحرب السيبرانية من منظور القانون الدولي الإنساني Cyber Warfare

from the International Humanitarian Law Vision. المجلة النقدية للقانون والعلوم السياسية، ١٦ (4).

هاجر، خ. (٢٠١٩). الوضع القانوني للحرب السيبرانية على ضوء قواعد القانون الدولي The Legal Status of Cyber Warfare in Light of The Rules of the International Law. مجلة التواصل في الاقتصاد والإدارة والقانون، ٢٥ (٣).

هنكرس، ج. م.، و والدبك، ل. د. (٢٠٠٧). القانون الدولي الإنساني العرفي Customary International Humanitarian Law. اللجنة الدولية للصليب الأحمر، جنيف.

المصادر الأجنبية:

Beomchul, S. (2011). The Cyber warfare and the right of self-defense: Legal perspectives and the case of the United States. *IFANS, 19*(1) Gervais, M. (2012). Cyber attack and the law of war. *Berekeley Journal of International Law, 30*(2).

Hathaway, O., & Crootof, R. (2012). *The law of cyber attack*. Yale Law School Legal Scholarship Repostory.

Hughes, R. (2010). A treaty for cyberspace. *International Affairs Journal, 86*(2).

Marco, R. (2010). Worldwide Warfare Jus Ad Bellum and The Use of Cyber Force. *Max Planck UNYB 14*.

Schmitt, M. N. (1999). computer network attach and the use of force in international law: thoughts on a normative framework. *Columbia journal of transnational law 37*.

Schmitt, M. N. (2002). Wired warfare: computer network attack and jus in bello. *IRRC, 84*(846).

Schmitt, M. N. (2013). *Tallin Manual, on the international law applicable to cyber warfare*. Cambridge university.

Sigholm, J. (2013). Non-State Actors in Cyberspace Operations. *Finland and Finish Society of Military Sciences 4(1)*.

Thomas, R., & Peter, M. (2012). Cyber Weapons Routledge Publisher. *The RUSI Journal 157(1)*.

Waxman, M. C. (2011). Cyber-Attacks and the Use of Force: Back to

the Future of Article 2(4). ***Yale Journal of International Law 36*****.**

Wiener, N. (1948). ***Cybernetics or control communication in the machine*****. Cambridge, Massachusetts.**