

القانون الدولي الإنساني والحرب السيبرانية: حدود التطبيق وإمكانياته International Humanitarian Law and Cyber Warfare: Limits of Application and Potential

♦ ولهي المختار

جامعة محمد بوضياف بالمسيلة / الجزائر
mokhtar.oualhi@univ-msila.dz

تاريخ النشر: 2025/12/25

تاريخ القبول: 2025/12/10

تاريخ الإرسال: 2025/06/16

الملخص:

تعتبر الحرب السيبرانية، من المواضيع الحديثة في القانون الدولي العام والقانون الدولي الإنساني، التي تثير العديد من المسائل القانونية باعتبارها ثورة في الوسائل والأساليب المستخدمة، في النزاعات المسلحة التقليدية، مما دفع رجال القانون والخبراء إلى مقارنة هذه الحرب مع القواعد القانونية، القابلة للتطبيق على النزاعات المسلحة في الحرب التقليدية، ومحاولة البحث في إمكانية اعتبار توجيه الأسلحة والهجوم باستخدام الحاسوب (الهجوم السيبراني)، هجوما مسلحا وفقا لقواعد القانون الدولي العام، وهل القواعد القانونية الموجودة قبل بروز هذه الحرب السيبرانية، تتسم بالوضوح بما فيه الكفاية وقادرة على مواكبة التحديات، التي يفرضها استخدام هذا النوع الجديد من الأسلحة في النزاعات المسلحة المعاصرة، التي لا يتقابل فيها جيش نظامي تقليدي تجاه جيش آخر، أو فئات أخرى منظمة.

الكلمات المفتاحية: الحرب السيبرانية، الهجوم السيبراني، القانون الدولي الإنساني

Abstract:

Cyber warfare is considered as modern topics in public international law and humanitarian law, raising numerous legal issues due to its revolutionary nature in the means and methods used in traditional armed conflicts. This has prompted legal scholars and experts to approach this form of warfare, by examining the legal rules applicable to armed conflicts in traditional warfare and attempting to explore the possibility of considering the directing of weapons, and attacks using computers (cyberattacks) as armed attacks under the rules of public international law. Furthermore, they are investigating whether the legal rules existing before

القانون الدولي الإنساني والحرب السيبرانية: حدود التطبيق وإمكاناته

the emergence of cyber warfare are sufficiently clear and capable of keeping pace with the challenges posed by the use of this new type of weapon in contemporary armed conflicts, where a traditional regular army does not necessarily face another army or other organized groups.

Keywords : Cyber Warfare, Cyber-attaque, International Humanitarian Law

مقدمة:

أدى التطور الهائل والواسع للوسائل التكنولوجية، المرتبطة بالأجهزة الإلكترونية والاتصالات ثورة شاملة في جميع نواحي الحياة، ومع هذا التطور الحاصل تزايد الاعتماد العالمي على استخدام شبكة الانترنت، مما أدى إلى تزايد التعرض لهجمات سيبرانية فيما أصبح يعرف بالجال الخامس للحرب (الفضاء السيبراني Cyber space) إلى جانب المجالات الأربع للحرب التقليدية (البر والبحر والجو والفضاء).

وأصبحت الهجمات السيبرانية هي الشغل الشاغل للمجتمع الدولي بأسره، لما لها من تداعيات خطيرة على الإنسانية بشكل واضح، حيث أصبحت آثارها تتعدى البيانات في أجهزة الحاسوب وأنظمتها، إلى العالم الحقيقي، فقد تؤدي هذه الهجمات إلى السيطرة على الملاحة الجوية، أو محطات الطاقة النووية وغيرها، ومن هنا بدأت تبرز تحديات جمة أمام المختصين في القانون الدولي، بخصوص طبيعة هذه الهجمات السيبرانية، خاصة وأن هذه الهجمات تلجأ إليها الدول لتحقيق أهداف أثناء النزاع المسلح، باستخدام التكنولوجيا الحديثة بأقل التكاليف والأضرار، حيث أصبحت الحروب المعاصرة، تتم على الفضاء السيبراني وهو ما اصطلح على تسميتها بالحرب السيبرانية.

إن الحرب السيبرانية تثير العديد من المسائل القانونية، مما دفع رجال القانون والخبراء إلى مقارنة هذه الحرب مع القواعد القانونية، القابلة للتطبيق على النزاعات المسلحة في الحرب التقليدية، ومحاولة البحث في إمكانية اعتبار توجيه الأسلحة والهجوم باستخدام الحاسوب (الهجوم السيبراني)، هجوما مسلحا وفقا لقواعد القانون الدولي العام، وهل القواعد القانونية الموجودة قبل بروز هذه الحرب السيبرانية، تنسجم بالوضوح بما فيه الكفاية وقادرة على مواكبة التحديات، التي يفرضها استخدام هذا النوع الجديد من الأسلحة في النزاعات المسلحة المعاصرة، التي لا يتقابل فيها جيش نظامي تقليدي تجاه جيش آخر، أو فئات أخرى منظمة.

وعليه تهدف هذه الورقة البحثية، إلى بيان مدى إمكانية تطبيق قواعد ومبادئ القانون الدولي الإنساني على الحرب السيبرانية، وهذا من خلال محورين: الأول منه يعالج الحرب السيبرانية وقانون الجوّاء إلى الحرب، أما المحور الثاني فيُخصّص إلى موقف القانون الدولي الإنساني من الحرب السيبرانية.

1: مدى مشروعية الحرب السيبرانية في القانون الدولي

إن احتمال شن عمليات عدائية في الفضاء السيبراني وغيره، أصبحت من المسائل ذات الأهمية البالغة في السنوات الأخيرة، حيث أصبحت العمليات السيبرانية حقيقة واقعة في النزاعات المسلحة المعاصرة، ولعل

ولهي المختار

موضوع الأمن الإلكتروني، أو السيبراني يحتل أعلى الدرجات في سلم التهديدات، التي تواجه الدول، خاصة الدول الكبرى في ظل محاولاتها المتنامية للتدخل في مناطق النزاعات المسلحة، فقد أصبح الفضاء السيبراني ميدانا جديدا للقتال، وساحة جديدة للحرب، تُضاف إلى الساحات التقليدية المعروفة في النزاعات المسلحة المتمثلة في الأرض والجو والبحر والفضاء الخارجي.

وعليه تتعرض بالدراسة، إلى الإطار المفاهيمي للحرب والنزاعات الدولية في الفضاء السيبراني (المطلب الأول)، بالإضافة إلى الحرب السيبرانية، واستخدام القوة وفقا لميثاق الأمم المتحدة (المطلب الثاني).

1.1: الإطار المفاهيمي للحرب والنزاعات الدولية في الفضاء السيبراني

بداية نشير إلى ان الفضاء السيبراني (Cyber space) مصطلح حديث، برز نتيجة الثورة الهائلة لتكنولوجيا المعلومات، ويشمل جميع الحواسيب والمعلومات التي بداخلها والأنظمة والبرامج، والشبكات المفتوحة لاستعمال الجمهور العام، المصممة للاستعمال من طرف فئة معينة من المستخدمين، منفصلة عن شبكة الانترنت العامة¹، وبما أن الحرب السيبرانية تقع في هذا الفضاء، وجب التعرض لمفهوم الحرب السيبرانية (الفرع الأول)، ثم النزاعات الدولية في الفضاء السيبراني (الفرع الثاني).

1.1.1: مفهوم الحرب السيبرانية

الحرب السيبرانية أو الهجمات السيبرانية مصطلح حديث نسبيا، لذلك حاول العديد من المهتمين والخبراء وضع تعريف محدد له.

فقد عرّف (Schmith) الحرب السيبرانية بأنها: "مجموعة من الإجراءات، التي تتخذها الدولة للهجوم على نظم المعلومات المعادية، بهدف التأثير والإضرار بها، وفي الوقت نفسه الدفاع عن نظم المعلومات، الخاصة بالدولة المهاجمة"².

وعلى نفس النهج، عرّف الخبراء القانونيون في دليل تالين الهجمات السيبرانية بأنها: "عمليات سيبرانية، سواء هجومية، أو دفاعية، يهدف من خلالها التسبب بالإصابة، أو الوفاة لأشخاص، أو الإضرار وتدمير الأهداف (الأعيان)"³.

ويُعرّفها البعض بأنها: "امتداد للحرب السياسية، من خلال الإجراءات المتخذة في الفضاء السيبراني، من قبل دول، أو فاعلين غير دوليين، حيث تُشكل تهديدا خطيرا للأمن القومي"¹.

¹ محمود محارب، إسرائيل والحرب السيبرانية - قراءة في كتاب حرب في الفضاء الإلكتروني: اتجاهات وتأثيرات على إسرائيل، - مراجعة كتب صادرة عن المركز العربي للأبحاث ودراسة السياسات، 2011، ص 01.

² أحمد عيسى نعمة الفتلاوي، الهجمات السيبرانية (دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر)، ط 01، منشورات زين الحقوقية، بيروت، 2018، ص 16.

³ سعيد درويش، الحروب السيبرانية وأثرها على حقوق الانسان: دراسة على ضوء أحكام دليل تالين، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية، المجلد 54، العدد 5، 2017، ص 181.

القانون الدولي الإنساني والحرب السيبرانية: حدود التطبيق وإمكاناته

كما عرّفت لجنة الصليب الأحمر الحرب السيبرانية بأنها: "عمليات ضد حاسوب، أو نظام حاسوبي، أو أي جهاز آخر متصل بالإنترنت، عندما يُستخدم باعتبارها وسائل وأساليب للقتال في سياق نزاع مسلح، وتعتمد هذه العمليات السيبرانية على تكنولوجيا المعلومات والاتصالات"².

أما قاموس أوكسفورد الإنكليزي، فقد عرّف الحرب السيبرانية بأنها: "استخدام تقنيات الحاسوب، لتخريب نشاطات دولة، أو منظمة، وبخاصة الهجوم على منظومات المعلومات الخاصة، وذلك لغايات استراتيجية أو عسكرية".

وعليه يمكن القول بأن الحرب السيبرانية، هي تلك العمليات التي تشن في الفضاء السيبراني، لتدمير أو تعطيل مجموعة من الأهداف في العالم الحقيقي، سواء كانت هذه الأهداف عسكرية، أو غير محددة عسكرية ومدنية، قد تؤدي إلى خسائر مادية وبشرية كبيرة، فعلى سبيل المثال من النتائج المحتملة لهذه الهجمات السيبرانية، المساس بنظام المراقبة الجوية، أو بنظم المنشآت النووية.

ونشير هنا إلى أن الحرب السيبرانية تتميز بعدة خصائص من أهمها³:

1- أنها حرب لا تناظرية (Asymmetric)، أي أنه لا تتطلب تكاليف عالية لشن مثل هذه الحرب، فلا تحتاج الدول إلى صناعة عسكرية ضخمة ومكلفة، كالإبواب وحاملات الطائرات وغيرها، لتفرض تهديدا حقيقيا ضد دول كبرى، مثل الولايات المتحدة الأمريكية، أو روسيا الاتحادية أو الصين.

2- في الحروب السيبرانية، المهاجم يتمتع بأفضلية واضحة وكبيرة، بالمقارنة مع المدافع، لأن هذه الحروب تتميز بالسرعة والمرونة والمراوغة.

3- عدم فعالية نماذج الردع المعروفة في الحرب التقليدية، لأن في مثل هذه الحروب من الصعوبة بمكان رصد هذه العمليات وتحديددها في وقت قصيرة، وفي حالات كثيرة إذا تم تتبع مصدرها يتبين أنها لفاعلين غير حكوميين، وفي هذه الحالة لن تكون هناك قواعد وإجراءات واضحة للرد عليها.

4- المخاطر الناتجة عن الحرب السيبرانية، تتعدى استهداف المنشآت العسكرية إلى استهداف البنى التحتية المدنية الحساسة.

¹ هذا التعريف منسوب إلى (Sharkariau Paulo)، قلا عن سامر نمر سالم الجاروشة، الجرائم السيبرانية وحقوق الإنسان في القوانين الدولية الوطنية، دار النهضة العربية، ط1، 2023، ص 116.

² القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة، اللجنة الدولية للصليب الأحمر، نوفمبر 2019، ص 02.

³ سنوسي علي، الهجمات السيبرانية في ضوء أحكام القانون الدولي الإنساني والاتفاقيات الدولية، مجلة الحقوق والعلوم السياسية، جامعة خنشلة، المجلد 10، العدد 02، 2023، ص 247.

ولهي المختار

ونشير بهذا الصدد الى انه تكاد تجمع الدراسات، على ان الهجمات السيبرانية الروسية ضد إستونيا بتاريخ 27 أبريل 2007 امتدت على أسابيع، ومست عدة مواقع، من أهمها مواقع حكومية والبرلمان، فضلا عن المواقع الالكترونية، والتجارية والمصرفية، والإعلامية مسببة شللا، وبالتالي تكبدها خسائر كبيرة.

ونفس الشيء وقع مع إيران عام 2010، حيث تعرّض مفاعل بوشهر النووي إلى هجوم سيبراني مشترك بين إسرائيل والولايات المتحدة الأمريكية، بواسطة فيروس ستكسن (Styxent) الذي قام باختراق نظام المفاعل النووي، مما أدى إلى تعطيل أجهزة الطرد المركزي.

2.1.1: مفهوم النزاعات الدولية كهجوم سيبراني

إن الحرب السيبرانية هي ظاهرة جديدة نسبيا لاعتمادها على أدوات تكنولوجيا المعلومات، وقد انتشرت

على نطاق واسع في السنوات الأخيرة، وتتميز بالقدرة الهائلة على التدمير دون ضرورة للتواجد المادي على مسرح المعركة، وبالنتيجة دون خسائر للطرف الذي ينفذ الهجوم، وتحدث هذه الحرب السيبرانية، في حالة السلم، أو في إطار نزاع مسلح، سواء أكان دوليا أو داخليا، فإذا كانت في وقت السلم، تعتبر عمليات تجسس، بينما تعتبر عمليات عسكرية أثناء النزاعات المسلحة.

ومن ثم فإنه قد يتطلب الأمر، تحديد الظروف التي يمكن في إطارها اعتبار الهجمات السيبرانية، بوصفها تحدث في أثناء النزاع المسلح، أو تؤدي في حد ذاتها الى نشوب نزاع مسلح، سواء أكان دوليا أم غير دولي.

وتطرح في هذه المسألة، إشكالات متعددة بطبيعة النزاع المسلح غير الدولي، والذي يعرف بأنه نزاع مسلح بين السلطة الشرعية وجماعة مسلحة منظمة متمردة، أو بين مجموعتين مسلحتين منظمتين، داخل إقليم دولة واحدة¹، لكن قد تستغل هذه المجموعات المسلحة المنظمة المنشقة عن الحكومة المركزية، ضعف السلطة وقد تشن هجمات إلكترونية على الدولة من خارج إقليمها، وهنا نكون أمام نزاع مسلح غير دولي لكنه عابر لحدود.

أما النزاعات المسلحة الدولية، والتي تكون بين دولة وأخرى في صورتها الأولى، لكن أن تكون فيها هجمات إلكترونية (حرب سيبرانية)، متزامنة بين الأعمال العدائية في الميدان، أي عنف مباشر أو اشتباك مسلح، وهذه الحالة تنطبق على الحرب الروسية-الأوكرانية، حيث قامت أوكرانيا بشن هجمات سيبرانية ضد روسيا بتاريخ 22 مارس، 2022 استهدفت شبكات الطاقة والسكك الحديدية، كما تعرضت أوكرانيا إلى عدة هجمات إلكترونية من طرف روسيا، من أهمها الهجوم على مؤسسة الطاقة النووية الأوكرانية (Energoatom)، بتاريخ 16 أوت 2022.

¹ انظر المادة 3 المشتركة بين اتفاقيات جنيف لعام 1949 والمادة الأولى من البروتوكول الإضافي الأول لعام 1977.

القانون الدولي الإنساني والحرب السيبرانية: حدود التطبيق وإمكانياته

أما الصورة الثانية للنزاع المسلح الدولي، وهي تلك النزاعات المسلحة الداخلية التي تعرف بالنزاعات المدولة (Internationalised)، وقد تأخذ هذه النزاعات الصور التالية:

- 1- تدويل صراع مسلح بين جماعتين وطنيتين، داخل إقليم دولة واحدة إذا ما ساندت كل منها دولة أو دول أجنبية.
- 2- التدخل العسكري المباشر لدولتين أجنبيتين، كل منهما في مواجهة الأخرى، دعماً للأطراف الداخلية المتنازعة.

3- التدخل الأجنبي دعماً لحركة ثورية في صراع مع الحكومة القائمة.

ولأن هذه الصور تنطبق على الدعم المباشر، لهذه الجماعات المنشقة داخل الدولة الواحدة، لكن قد يأخذ هذا الدعم مجهوداً إلكترونياً، يأخذ طابع المساعدة لإحدى الجماعات المنظمة المنشقة بواسطة وسائل إلكترونية لشن هجمات إلكترونية ضد السلطة الحاكمة، أو ضد مجموعة أخرى منشقة.

ويمكن الإشارة هنا إلى حكم محكمة العدل الدولية، في القضية المتعلقة بالأنشطة العسكرية وشبه العسكرية في نيكاراغوا وضدها، الصادر في 27 جوان 1986، حيث قررت بأن الولايات المتحدة الأمريكية من خلال انتاجها لكتاب، كدليل لقوات معارضة "الكونترا" بعنوان "العمليات النفسية في حرب العصابات"، قد شجّع هذه المعارضة على ارتكاب أعمال تخالف قواعد القانون الإنساني¹، ومن هنا بالقياس على ذلك، يمكن القول بأن المساعدة الإلكترونية للمجموعات المسلحة المنظمة، لشن هجمات إلكترونية ضد الحكومة من شأنه أن يكون منافياً لقواعد القانون الدولي الإنساني، وفي نفس الوقت رأت محكمة العدل الدولية في نفس القضية، بأن مسؤولية الولايات المتحدة الأمريكية متوقفة على إثبات سيطرتها الفعلية على العمليات²، لكن مع التطورات التكنولوجية الحالية، فنتائج الحرب هي نفسها التدمير والقتل وغيرها، لكن بوسائل جديدة.

فلا يمكن هنا القول، بأن السيطرة الفعلية تعتبر أساساً لإثبات المسؤولية الدولية، وبالمقابل المسؤولية الجنائية الدولية للفرد تبقى قائمة، دون اشتراط التواجد الفعلي في الميدان أو السيطرة الفعلية على الأرض وهذا ما ينطبق على أولئك الذين يشنون هجمات إلكترونية، أو يساعدون مجموعات مسلحة على القيام بذلك.

ومن بين النزاعات المسلحة الدولية، التي يمكن أن تكون من ضمنها، أو في سياق الحروب السيبرانية، هي نزاعات التحرر الوطني المسلحة ضد الاحتلال³، سواء كانت هذه العمليات الإلكترونية هجومية، أو دفاعية

¹ سلافة طارق الشعلان، تكييف استخدام الحرب الإلكترونية، في النزاعات المسلحة وفقاً للقانون الدولي الإنساني، مجلة الكوفة، المجلد 01، العدد 26، 2016، ص 131.

² المرجع نفسه، الصفحة نفسها.

³ تنص الفقرة 4 من المادة الأولى من البروتوكول الإضافي الأول لعام 1977، على أنه يقصد بحروب التحرير: "تتضمن الأوضاع المشار إليها في الفقرة السابقة، المنازعات المسلحة التي تناضل بها الشعوب ضد التسلط الاستعماري والاحتلال الأجنبي وضد الأنظمة العنصرية، وذلك

ولهي المختار

يجب أن تكون مميّزة بالعنف المقصود في المادة 49 من البروتوكول الإضافي الأول لعام 1977¹، ويترتب عليه نتائج وخيمة من حيث الأضرار، مثل الخسائر وتدمير الممتلكات.

2.1: التفسير الموسع لمفهوم استخدام القوة والحرب السيرية

لقد وضع ميثاق الأمم المتحدة حدوداً لاستخدام القوة أو التهديد بها، واعتبر أن استخدام القوة يكون مشروعاً في حالتين فقط، وهما حالة الدفاع عن النفس طبقاً لأحكام المادة 51 من الميثاق، وحالة تدخل مجلس الأمن للمحافظة على السلم والأمن الدوليين، أو إعادتهما إلى نصابهما، تطبيقاً لنص المادة 42 من الميثاق، لكن مع التطورات التكنولوجية أصبح استخدام الوسائل الإلكترونية في الحرب، يُثير تساؤلات في غاية الأهمية تتمثل في كيفية تحديد فكرة استخدام القوة في الفضاء السيرياني.

1.2.1: مبدأ حظر استخدام القوة والحرب السيرية

تنص المادة الثانية من ميثاق الأمم المتحدة، على ضرورة امتناع أعضاء المنظمة عن اللجوء إلى التهديد بالقوة أو استخدامها، وهنا يُطرح سؤال مفاده: ما هو مفهوم القوة في القانون الدولي، وهل أنه يقتصر - على القوة العسكرية فقط، بمعنى استبعاد الحصار الاقتصادي، أي استناداً إلى الفقرة الرابعة من المادة الثانية من الميثاق، وكذا المادة 51 من الميثاق.

أما الاتجاه الآخر، فيرى أن مفهوم القوة في القانون الدولي، يشمل بالإضافة إلى القوة العسكرية، الحصار الاقتصادي وغيرها من التدابير، طبقاً لأحكام المادتين 41 و42 من الميثاق، لكن اتجاه ثالث اعتمد في تعريف القوة استناداً إلى آثارها، فإذا كانت تمس سلامة الأرض، أو الاستقلال السياسي، فهناك تكمن القوة وهي التي توصف بالجريمة الدولية².

ومن خلال ما سبق كيف يتم تحديد مفهوم القوة في الفضاء السيرياني؟

في ممارستها لحق الشعوب في تقرير المصير، كما كرسه ميثاق الأمم المتحدة والإعلان المتعلق بمبادئ القانون الدولي الخاصة بالعلاقات الودية والتعاون بين الدول طبقاً لميثاق الأمم المتحدة".

¹ تنص المادة 49 من البروتوكول الإضافي الأول لعام 1977 على أن:

"1- تعني "الهجمات" أعمال العنف الهجومية والدفاعية ضد الخصم.

2- وتنطبق أحكام هذا الحق "البروتوكول" المتعلقة بالهجمات على كافة الهجمات في أي إقليم تشن منه، بما في ذلك الإقليم الوطني لأحد أطراف النزاع والواقع تحت سيطرة الخصم.

3- تسري أحكام هذا القسم، على كل عملية حربية في البر كانت أم في الجو أم في البحر، قد تصيب السكان المدنيين أو الأفراد المدنيين، أو الأعيان المدنية على البر، كما تنطبق على كافة الهجمات الموجهة من البحر أو من الجو، ضد أهداف على البر، ولكنها لا تمس بطريقة أخرى قواعد القانون الدولي التي تنطبق على النزاع المسلح في البحر أو في الجو.

4- تعد أحكام هذا القسم إضافة إلى القواعد المتعلقة بالحماية الإنسانية، التي تحتويها الاتفاقية الرابعة، وعلى الأخص الباب الثاني منها، والاتفاقيات الدولية الأخرى الملزمة للأطراف السامية المتعاقدة، وكذا قواعد القانون الدولي المتعلقة بحماية الأشخاص والأعيان المدنية، في البر والبحر والجو ضد آثار الأعمال العدائية".

² سامر غر سالم الجاروشة، مرجع سابق، ص 42 - 43.

القانون الدولي الإنساني والحرب السيبرانية: حدود التطبيق وإمكاناته

وللإجابة على هذا السؤال، يجب العودة إلى تقرير الفريق الأممي السادس الذي، أنشأته الجمعية العامة للأمم المتحدة في 02 جانفي 2019¹، والذي أصدر تقريره النهائي المتضمن معايير السلوك المقبول في الفضاء السيبراني، حيث جاء فيه: "يجب على الدول عند استخدامها لتكنولوجيات الاتصالات، والمعلومات ووفقا لميثاق الأمم المتحدة، أن تمتنع عن في علاقاتها الدولية عن التهديد باستخدام القوة، أو استعمالها ضد السلامة الإقليمية، أو الاستقلال السياسي لأية دولة، أو بأي طريقة أخرى تتعارض مع مقاصد الأمم المتحدة"².

وفقا لما سبق، فإن الدول ملزمة بعدم استخدام القوة في الفضاء، على كل أشكال الاختراق الإلكتروني التي تسبب في تعطيل، أو تدمير البنى التحتية للدولة، وهنا وجب التمييز بين الهجمات السيبرانية، التي لها نفس الأهداف والأغراض العسكرية، مع الهجمات التقليدية والمتشابهة أساسا في استهداف البنية التحتية العسكرية للدول، وأمن المعلومات العسكرية، وبين الهجمات السيبرانية الأخرى، التي ليس لها هدف عسكري كالحرب الإعلامية ونشر الإشاعات وغيرها.

ومن هنا يتضح ان العمليات السيبرانية التي تقوم بها دولة ضد دولة أخرى، وتنتهك بها حظر استخدام القوة إذا كانت الآثار الناجمة عنها تضاهي، أو تتجاوز الآثار الناجمة عن استخدام الأسلحة التقليدية³.

وخلاصة القول أن ما ورد في الفقرة 4 من المادة 2 من الميثاق هو "القوة"، دون اقترانه بأي مصطلح آخر، أي دون تحديد لطبيعة أو لنوع القوة، حيث جاءت الفقرة شاملة لكل صور القوة الممكنة، وهذا بخلاف المواطن الأخرى لاستعمال مصطلح القوة في الميثاق، أين جاء مقترنا بمصطلح "المسلحة"⁴، وعليه فإن مفهوم القوة يشمل كل أنواع التهديد، ولا ينحصر فقط في القوة العسكرية، وبغض النظر عن الوسيلة المستخدمة طالما أن النية عدائية⁵.

2.2.1: جريمة العدوان والحق في الدفاع عن النفس في الفضاء السيبراني

بالرجوع إلى المادة 8 مكرر من النظام الأساسي للمحكمة الجنائية الدولية، نجد انها عرّفت العدوان بأنه: "قيام شخص ما، له وضع يمكنه فعلا من التحكم في العمل السياسي أو العسكري للدولة، أو من توجيه

¹ هذا الفريق متكون من 25 دولة على أساس التوزيع الجغرافي العادل، أنظر قرار الجمعية العامة الصادر في 02 ديسمبر 2019 الوثيقة (A/Res/73/266).

² تقرير الخبراء المذكور في مذكرة الأمين العام للأمم المتحدة في 14 جوان 2021، الوثيقة (A/76/135)، ص 01.

³ خلافي سفيان، تطبيق الهجمات السيبرانية في ضوء أحكام القانون الدولي، المجلة الأكاديمية للبحث القانوني، المجلد 13، العدد 02، 2022، ص 313.

⁴ أنظر ديباجة الميثاق والمادة 44 منه.

⁵ علي فاضل علي سلجان، حق الدفاع الشرعي على الهجمات السيبرانية، مجلة جامعة تكريت للحقوق، السنة 04، العدد 04، الجزء 01، 2020، ص 8.

ولهي المختار

هذا العمل بتخطيط، أو إعداد أو بدء أو تنفيذ فعل عدواني يشكل بحكم طابعه، وخطورته ونطاقه انتهاكا واضحا لميثاق الأمم المتحدة¹.

ويتمثل فعل العدوان حسب المادة 8 مكرر المشار إليه، بأنه استعمال القوة المسلحة من جانب دولة ما ضد دولة أخرى أو سلامتها الإقليمية، أو استقلالها السياسي، أو بأي طريقة أخرى تتنافى والميثاق الأممي وسواء بإعلان الحرب أو بدونه، وهذا وفقا لما ورد في قرار الجمعية العامة للأمم المتحدة رقم 3314 (د - 29) الصادر في 14 ديسمبر 1974².

ومن خلال قراءة نص المادة 8 مكرر من نظام روما الأساسي، خاصة الفقرتين الأولى والثانية، نجد أن المسؤولية عن أي عمل عدواني، لا يمكنه ان يُعزى إلا إلى دولة أو فرد وفي وضع يسمح له فعليا بالتحكم والسيطرة على العمل السياسي، أو العسكري للدولة أو توجيهه، وبما أن الدول غالبا ما تستعمل مجموعات من الوسطاء في تنفيذ العمليات السيرية، بما في ذلك الأشخاص، أو المجموعات المدنية، فإن القيام بهذا التحكم والسيطرة الفعالة قد لا يكون متيسرا وسهلا، وعليه فإن نص المادة 8 مكرر من النظام الأساسي للمحكمة الجنائية الدولية، لا يمكن أن يشمل بما يسمى العدوان السيرياني، لعدم إثبات السيطرة، أو التحكم الفعليين لمنفذ الهجوم أو الموجه له.

ونشير إلى أنه ثمة من يرى بأن الهجمات الالكترونية الدولية، التي وقعت في العالم لم تصل إلى درجة العدوان والهجوم المسلح، فحتى الهجوم السيرياني الروسي ضد إستونيا أو الحرب السيرية الروسية الأوكرانية، لم يتم وصفها علنا من طرف المجتمع الدولي أنه عدوان مسلح، ونفس الشيء بالنسبة للهجوم الإسرائيلي الأخير ضد حزب الله اللبناني عن طريق تفجير أجهزة البيجر والراديو، لم توصف بأنها عدوان مسلح، لكن الهجوم السيرياني على المفاعل النووي الإيراني "بوشهر" عام 2010، بواسطة فيروس ستكسنت (Stuxent) اعتبره بعض الخبراء، بأنه ممكن أن يصل إلى درجة الهجوم المسلح، نتيجة الأضرار التي أحدثها³.

ومن خلال ما سبق الإشارة إليه، إذا تم تكييف هجوم سيرياني بمثابة حرب عدوانية سيرية تجاه دولة أخرى، فهل تكون هاته الأخيرة في حالة يمكنها ممارسة حقها في الدفاع عن النفس، طبقا لأحكام المادة 51 من الميثاق، وباستقراء نص المادة 51 سالف الذكر، يتضح أن الميثاق قد أجاز للدول استخدام القوة المسلحة في حالة الاعتداء عليها، وذلك إلى أن يتخذ مجلس الأمن التدابير اللازمة، لحفظ السلم والأمن الدوليين.

وفي حالة الهجوم السيرياني، تشير الدراسات إلى أن الدولة الضحية لهجوم سيرياني لن يكون بوسعها استخدام القوة للدفاع عن النفس، إلا إذا توفرت الشروط التالية⁴:

¹ الفقرة الأولى من المادة 8 مكرر من نظام روما الأساسي.

² الفقرة الثانية من المادة 8 مكرر من نظام روما الأساسي.

³ سامر نمر سالم الجاروشة، مرجع سابق، ص 45.

⁴ سامي محمد عبد العال، الدفاع الشرعي ضد الهجمات السيرية، المجلة المصرية للقانون الدولي، المجلد 79، 2023، ص 43.

القانون الدولي الإنساني والحرب السيبرانية: حدود التطبيق وإمكاناته

أ- الهجوم السيبراني استخدام للقوة

رغم أن هناك خلاف بخصوص مصطلح القوة، هل يشمل القوة العسكرية فقط، أم يتعدى ذلك إلى صور أخرى، مثل الضغط الاقتصادي على الدولة وما إلى ذلك، لكن الرأي الراجح فقها وقضاء¹، أن استخدام القوة يكون بأي شكل من الأشكال، دون الاقتصار على القوة المسلحة دون غيرها.

ومن هنا يمكن للهجوم السيبراني، أن يرقى إلى استخدام القوة، مثل توفير برامج ضارة لمجموعات متمردة وتدريب أعضائها على استخدام هذه البرامج بطريقة مدمرة².

ب: أن يكون الهجوم السيبراني هجوما مسلحا

لا يكفي وصف الهجوم بأنه استخدام للقوة، حتى يحق للدولة استخدام حق الدفاع الشرعي، وإنما يجب أن يوصف الهجوم السيبراني، بأنه هجوما مسلحا لأن مصطلح "الهجوم المسلح" يختلف عن مصطلح "استخدام القوة" وهو ما ذهبت إليه محكمة العدل الدولية في قضية الأنشطة العسكرية وشبه العسكرية في نيكاراغوا حيث أكدت على ضرورة التمييز بين حظر استخدام القوة — تلك التي تشكل هجوما مسلحا — وبين صور وأشكال استخدام القوة الأقل خطورة، أي أن جميع الهجمات المسلحة هي استخدام القوة، ولكن كل استخدام للقوة هجوم مسلح³.

ومما سبق الإشارة إليه، يُطرح تساؤل مفاده هل يمكن اعتبار الهجوم السيبراني هجوما مسلحا؟

من المعلوم أن غالبية الفقه الدولي تشترط في فعل العدوان، أن يكون عدوانا مسلحا حتى يبرر قيام الدفاع الشرعي، غير أن هناك اتجاه فقهي يرى أن الهجمات الالكترونية يمكن أن تشكل هجوما مسلحا، وعليه فإنه من الممكن أن يرقى إلى درجة من الخطورة، وقد يصل إلى مستوى الهجوم المسلح، مما يستوجب معه استخدام

¹ من الآراء الفقهية التي تؤيد ذلك نذكر ما أورده الفقيه (كلسن Kelsen)، بأن استخدام القوة يكون بأي شكل من الأشكال دون الاقتصار على القوة المسلحة دون غيرها، واستند في رأيه إلى الفصل السابع من ميثاق الأمم المتحدة، وخصوصا المادتين 41 و42، حيث أوردت إجراءات وتدابير لقمع العدوان، من خلال وسائل لا تضم القوات المسلحة، في حين أوردت المادة 42 إجراءات وتدابير أخرى لرد العدوان، لا تتضمن استخدام القوات المسلحة.

أنظر في ذلك:

Kelsen, Hens : Principles Of International Law, 2 éditions, Holt, Rinehart and Winston, New York, 1966, p 41-43.

أما بخصوص الاجتهادات القضائية فقد رفضت محكمة العدل الدولية التفسير الضيق لمفهوم القوة، حيث أكدت على أنه لا يجوز اقتصار مفهوم القوة على العمليات العسكرية، وهذا بمناسبة نظرها في القضية المتعلقة بالأنشطة العسكرية وشبه العسكرية في نيكاراغوا وضدها الصادر في 27 جوان 1986: "أن تسليح الدولة للعصابات المنخرطة في أعمال عدائية ضد دولة أخرى يعتبر استخداما للقوة".

أنظر في ذلك:

- C.I.J., Recueil 1986, p 195 – 228.

² وهو ما نصت عليه القاعدة 11 من دليل تالين بأن: "العملية السيبرانية تشكل استخداما للقوة عندما يكون حجم الضرر والآثار قابلة للمقارنة بالعمليات غير السيبرانية التي ترقى إلى مستوى استخدام القوة".

³ - C.I.J., Recueil 1986, p 23.

ولهي المختار

القوة، ويذهب الخبراء في تقدير الخطورة لا سيما في ضوء قدرتها على إحداث إصابات أو القتل¹، ويذهب الخبراء في تقدير الخطورة إلى تقييم مدى تأثير العملية على الدولة المتضررة، بحيث يؤثر على قدرة الدولة في تنفيذ المهام الأساسية، وبالتالي التأثير على الاستقرار الاجتماعي والسياسي، مثلاً قد تؤدي بعض العمليات السيبرانية، إلى إحداث أضرار يتعذر تداركها، كأن تصيب هذه العمليات أجهزة التحكم في السدود مثلاً، مما يؤدي إلى فيضان يؤدي بحياة كثير من المدنيين، وبالتالي يمكن القول بأن هذه الهجمات السيبرانية، ترقى إلى مستوى الهجوم المسلح الوارد في المادة 51 من الميثاق.

ج: أن يكون الهجوم السيبراني غير مشروع

أي لا محل للدفاع الشرعي، إذا كان مصدر الخطر مشروعاً، فمثلاً إذا كان مصدر الخطر بدوره استعمالاً لحق الدفاع الشرعي، فإنه يكون مباحاً، ولا يمكن الرد عليه (فلا يجوز الدفاع ضد الدفاع).

ونشير إلى أن هناك إشكالية تتعلق بمدى جواز، أو عدم جواز الدفاع الشرعي الاستباقي ضد الهجمات السيبرانية، هذه المسألة كانت محل نقاشات واسعة، لكن هناك جانب كبير في الفقه، يرى أنه لا ينبغي للدولة أن تنتظر الهجوم، عندما يكون وشيكاً لكي تتخذ التدابير الاحترازية، لأن عدم استخدام حق الدفاع الشرعي قبل شن الهجوم، سيؤدي بالضرورة إلى عدم قدرة الدولة الضحية على التصدي للهجوم².

وختاماً يمكن أن نخلص إلى أنه توجد عدة ضوابط، يجب توافرها، لكي يكون استعمال الدفاع الشرعي ضد الهجمات السيبرانية مشروعاً وهي:

1- أن يكون العدوان، أو الهجوم السيبراني حالاً ومباشراً.

2- الضرورة والفورية ضد الهجمات السيبرانية

3- ضرورة تناسب الدفاع الشرعي والهجمات السيبرانية

4- خضوع أعمال الدفاع الشرعي لرقابة مجلس الأمن

2: موقف القانون الدولي الإنساني من الحرب السيبرانية

لقد افرد القانون الدولي الإنساني مجموعة من القواعد، التي تحد من الآثار الوخيمة للنزاعات المسلحة، سواء أكانت دولية أم غير دولية، وهذا عن طريق تقييد وسائل القتال وأساليبه، لكن وبسبب التطور التكنولوجي المتسارع، لجأت الكثير من الدول إلى الهجمات الإلكترونية في سياق النزاعات المسلحة، أو ما بات يعرف بـ "الحرب السيبرانية"، مما جعل البعض يتساءل بخصوص وجود قواعد قانونية إنسانية، تشمل

¹ سامي محمد عبد العال، مرجع سابق، ص 59، نقلاً عن:

- Thomas Wingfield: When is a Cyberattack an "Armed Attack?": Legal Thresholds for Distinguishing military activities in cyberspace, Cyber Conflict Studies Association, 2006.

² سامر نمر سالم الجاروشة، مرجع سابق، ص 47.

القانون الدولي الإنساني والحرب السيبرانية: حدود التطبيق وإمكانياته

هذا النوع من الحروب وهل رواد القانون الدولي الإنساني تنبؤوا لهذه التطورات، التي قد تحدث في وسائل وأساليب القتال في المستقبل، وضمّنوا اتفاقيات القانون الدولي الإنساني القواعد اللازمة، التي تحكم هذه النزاعات الحديثة، أم أنه لابد من وضع قواعد جديدة تتماشى والتطور الحاصل.

وعليه ما هو موقف القانون الدولي الإنساني، من الحرب السيبرانية (المطلب الأول)، وما هي صعوبات تطبيق بعض المبادئ الإنسانية عليها (المطلب الثاني).

1.2: الحروب السيبرانية من منظور القانون الدولي الإنساني

عاجت الكثير من الدراسات في القانون الدولي الإنساني، مسألة الحروب السيبرانية باعتبارها من المسائل المستجدة، وتوقفوا عند القانون واجب التطبيق عليها، وإن كانت أغلب هذه الدراسات، أكدت أو قواعد القانون الدولي الإنساني يمكن تطبيقها على هذه الحروب، مع وجود بعض الإشكالات والصعوبات، في تحديد الأهداف المشروعة لهذه الحروب.

1.1.2: مدى إمكانية تطبيق القانون الدولي الإنساني على الحروب السيبرانية

هناك خلاف فقهي بخصوص مدى انطباق القانون الدولي الإنساني، على الحروب السيبرانية من عدم فهناك من يرى بأن الحروب السيبرانية غير منظمة في النزاعات المسلحة، حيث أصبحت وسائل وأساليب الحروب متطورة، إلى درجة لم يكن يتصورها واضعو اتفاقيات القانون الدولي الإنساني، ولعل الاستخدام المتزايد للفضاء السيبراني للأغراض العسكرية، أحد أهم الأسباب التي تدعو إلى إعادة النظر في القواعد، التي تنظم سير النزاعات المسلحة، وصياغتها بالشكل الذي يتوافق ويتلاءم مع هذه الاستخدامات¹.

ويشير أصحاب هذا الرأي أيضا أن قواعد القانون الدولي الإنساني وضعت لتنظيم وسائل وأساليب القتال ذات الطبيعة المتحركة، التي تنتج عنها آثار مادية غير متوفرة في الحروب السيبرانية، وبالتالي لا يمكن تطبيق قواعد القانون الدولي الإنساني عليها، لأنها ليست هجمات مسلحة².

ويعتقد أصحاب هذا الرأي أيضا، بأنه من غير الممكن تطبيق المبادئ العامة للقانون الدولي الإنساني على الحروب السيبرانية، لأن أساليبها ووسائلها غير واضحة بشكل كاف، كونها تتم في سرية، كما أنها هجمات استباقية وغير محددة المجال، ولا أهدافها أيضا محددة بخلاف الحروب التقليدية، كما أن الحرب السيبرانية غير معروفة وليست موجودة أو محددة في دولة بعينها، سواء أكانت هدفا للحرب أو مشاركة فيها، وأن هذه الحرب

¹ المرجع نفسه، ص 126.

² أسامة صبري محمد، الحرب الإلكترونية ومبدأ التمييز في القانون الدولي الإنساني، مجلة القانون للدراسات والبحوث القانونية العدد 07، 2013، ص 08.

ولهي المختار

بالإضافة إلى ما سبق، قد تكون متعددة الأوجه ومتشابكة مع غيرها، فهي تتشابك مع الحرب الإعلامية وحرب شبكات الاتصالات، والحرب السياسية والحرب التكنولوجية والإرهاب¹.

ورغم الحجج التي أوردها أصحاب هذا الرأي، فإنه لا يمكن التسليم بعدم انطباق قواعد القانون الدولي الإنساني على هذه الحرب السيبرانية، قياساً على حكم محكمة العدل الدولية في رأيها الاستشاري، المتعلق بمدى مشروعية التهديد باستخدام الأسلحة النووية، حيث أشارت إلى أن: "المبادئ والقواعد الإنسانية قد وضعت قبل اختراع الأسلحة النووية، ولكن هذا لا يمنع من تطبيق قواعد القانون الدولي الإنساني عليها، ولا يمكن التمسك بعدم انطباق القانون الدولي الإنساني على هذه الأسلحة، بحجة أنها لم تكن معروفة عند وضع قواعده وهذا ما لا يمنع من تطبيقه على الأسلحة النووية"².

أما الرأي الآخر وهو الرأي الغالب، فيرى أن القانون الدولي الإنساني يطبق على أي نزاع مسلح، بما فيه الحروب السيبرانية، وهو ما أكدته اللجنة الدولية للصليب الأحمر، بأنه لا يراودها أي شك في أن قواعد القانون الدولي الإنساني، تطبق على هذا النوع من الحروب (العمليات السيبرانية)، خلال النزاعات المسلحة ويقتد استخدامها، تماماً مثلما ينظم استخدام الأسلحة والوسائل والأساليب الأخرى للقتال، في أي نزاع مسلح جديدة كانت أم قديمة³، وإذا سلمنا جدلاً أن اتفاقيات القانون الدولي الإنساني، لم تشر صراحة إلى هذا النوع من الحرب السيبرانية، فإن شرط مارتينز (Fyodor Fyodorovich Martens)⁴، كفيل بسد هذا الفراغ كونه من المبادئ الراسخة في القانون الدولي الإنساني، والذي ينص صراحة على أن المدنيين والمقاتلين، يضلون تحت سلطة وحماية مبادئ القانون الدولي الإنساني المستمدة من التقاليد الراسخة، ومن مبادئ الإنسانية وما يمليه الضمير العام.

وعليه فإنه وحتى في غياب قواعد قانونية خاصة بالحروب السيبرانية، لا يمكن القول بأن مثل هذه الحروب لا تخضع لقواعد القانون الدولي الإنساني، لأن وسائل وأساليب هذه الحروب تؤدي إلى نفس النتائج والآثار المترتبة عن الأسلحة والحروب التقليدية، من تدمير وإصابات للأفراد وتقتيل، وبالتالي يجمع الفقه الدولي على اعتبار الحرب السيبرانية، هي حرب بالمعنى الصحيح، بالنظر إلى آثارها ونتائجها.

¹ عمر محمود اعمر، الحرب الإلكترونية في القانون الدولي الإنساني، مجلة الشريعة والقانون، الجامعة الأردنية، الأردن، المجلد 46، العدد 03، 2019، ص 137.

² C.I.J., Recueil 1996, p p 241 – 242.

³ المجلة الدولية للصليب الأحمر، القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة، 2011، على موقع اللجنة، ص 36 – 37.

⁴ شرط مارتينز تمت تسميته بهذا الاسم نسبة إلى المندوب الروسي لدى مؤتمر لاهاي للسلام عام 1899 (Fyodor Fyodorovich Martens)، حيث ذكر هذا الشرط بعدما فشل المندوبون في المؤتمر بخصوص مسألة مركز المدنيين الذين يشهرون السلاح ضد قوات الاحتلال، فالدول الكبرى كانت ترى أنه يجب معاملة هؤلاء المدنيين بوصفهم جنوداً غير نظاميين، يخضعون لعقوبة الإعدام، في حين رأت الدول الضعيفة آنذاك بوصفهم محاربين نظاميين، ونتيجة لذلك الخلاف قدم مارتينز رأيه الذي أصبح يعرف بشرط مارتينز.

وقد تم ذكر هذا الشرط في أغلب اتفاقيات القانون الدولي الإنساني ابتداءً من ديباجة اتفاقية لاهاي الأولى لعام 1899 والثانية عام 1907، وكذا بعض نصوص اتفاقيات جنيف لعام 1949 والبروتوكولين الإضافيين لعام 1977، وأخيراً ديباجة اتفاقية حظر أو تقييد استعمال تقليدية معينة يمكن اعتبارها مغرطة الضرر أو عشوائية الأثر لعام 1980.

القانون الدولي الإنساني والحرب السيبرانية: حدود التطبيق وإمكاناته

وفي نفس السياق تلزم المادة 36 من البروتوكول الإضافي الأول لعام 1977، كل دولة من الدول الأطراف التحقق من امتثال أي أسلحة جديدة تقوم بنشرها أو تدرس مسألة نشرها لقواعد القانون الدولي الإنساني¹.

فوفقاً لهذا النص إذا تم تكييف الهجمات السيبرانية، بأنها سلاح، أو أسلوب حرب فعلى الدول ضرورة التحقق من مدى امتثالها لقواعد هذا البروتوكول، أو أية قاعدة أخرى من قواعد القانون الدولي، وهو ما يؤكد انطباق أحكام القانون الدولي الإنساني على الحرب السيبرانية.

وهذا ما ذهب إليه "دليل تالين"²، حيث يشير إلى أن انطباق القانون الدولي الإنساني على الحرب السيبرانية، لا يخرج عن التقسيم التقليدي للنزاعات المسلحة "دولية وغير دولية"، ويُقر هذا الدليل بأن العمليات الإلكترونية وحدها، قد تشكل نزاعات مسلحة تبعاً للظروف، وقد اعتبر الهجوم الإلكتروني بمثابة استخدام للقوة، إذا كان أثر هذا الهجوم عند مقارنته بالاستخدام الفعلي للقوة، مساوياً له أو قريباً منه، ففي هذه الحالة يجب إخضاع هذا النوع من الهجمات لقانون النزاعات المسلحة³، كما أعطى هذا الدليل الحق للدولة، التي تتعرض لهجوم إلكتروني شن حرب هجومية إلكترونية مضادة على الدولة الأخرى، كما يمكن استخدام القوة العسكرية الحقيقية، في حالة ما إذا تم شن هجوم إلكتروني على دولة وأدى هذا الهجوم لخسائر بالأرواح البشرية⁴.

ونشير هنا إلى الذين يرون بأن غياب أي إشارات في القانون الدولي الإنساني بخصوص استهداف المدنيين والأعيان المدنية، أثناء العمليات التي تدور في الفضاء السيبراني، مما يعني أن قواعد القانون الدولي الإنساني، لا تشمل ولا تغطي وسائل وأساليب الحرب السيبرانية، وهذا غير صحيح ما دامت هذه الوسائل والأساليب تنتج نفس الآثار التي يمكن أن تنتج عن الأسلحة التقليدية.

ويؤكد هذا الرأي محكمة العدل الدولية في رأيها الاستشاري، بخصوص مدى مشروعية التهديد بالأسلحة النووية أو استخدامها لعام 1996، حيث أكدت أن المبادئ والقواعد الإنسانية، قد وضعت قبل الأسلحة النووية، ومع ذلك لا يوجد شك بانطباق القانون الدولي الإنساني على الأسلحة النووية، وليس هناك ما يدعو

¹ تنص المادة 36 من البروتوكول الإضافي الأول لعام 1977 على أن: "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 "البروتوكول"، أو أية قاعدة أخرى من قواعد القانون الدولي، التي يلتزم بها هذا الطرف السامي المتعاقد".

² دليل تالين هو دليل أعدته لجنة من الخبراء العسكريين والقانونيين بدعوة من مركز التميز للدفاع السيبراني التعاوني التابع لحف شبال الأطلسي- وصدر عام 2013، ويتكون من 95 قاعدة قانونية ويركز على الهجمات السيبرانية الأشد خطورة، التي تنتهك حظر استخدام القوة في العلاقات الدولية، وتحوّل الدول ممارسو حق الدفاع عن النفس، أو الهجمات التي ترتكب أثناء النزاعات المسلحة، ويطبق عليها قواعد القانون الدولي الإنساني.

³ عمر محمود اعمر، مرجع سابق، ص 139.

⁴ انظر الفصل 14 من دليل تالين.

ولهي المختار

للتمييز بين الأسلحة النووية وأسلحة الحاسوب، من حيث الزمن الذي استحدثت فيه، مما يعني إمكانية تطبيق القانون الدولي الإنساني عليها¹.

كما أشارت محكمة العدل الدولية أيضا في هذا الرأي، إلى أن القانون الدولي الإنساني قد تطور ليأخذ بعين الاعتبار تغير الظروف، ولا يقتصر تطبيقه على الأسلحة التقليدية، بل يتعدى تطبيقه إلى الأسلحة الجديدة². وعلى هذا الأساس لا يمكن القول بأن تطبيق القانون الدولي الإنساني، يعتمد على الفاعل، بل من الملائم وبدرجة عالية، يعتمد على آثار الفعل أو السلوك، فعلى سبيل المثال أن الحرب البيولوجية أو الكيميائية تخضع للقانون الدولي الإنساني، رغم أنها لا تتضمن أسلحة (حركية)، وهو ما ينطبق على الأسلحة الإلكترونية أيضا وعليه فالعبرة هنا بالآثار والنتائج التي تحدثها هذه الحرب³.

2.1.2: إشكالية تحديد الأهداف المشروعة أثناء الحرب السيبرانية

لا تختلف الحرب السيبرانية عن الحرب التقليدية، بخصوص الأهداف المحتملة، فهي تُصنف إلى ثلاثة أصناف هم: المقاتلون والأهداف العسكرية، وكذا المدنيين والأهداف المدنية، بالإضافة إلى الأهداف المزدوجة.

أولا: المقاتلون والأهداف العسكرية

يكون الاستهداف في الحروب السيبرانية، مشروعا لأفراد القوات المسلحة وأعضاء الجماعات المسلحة المنظمة، والمدنيون الذين يشاركون مباشرة في العمليات العدائية، والأفراد الذين يقاومون المحتل في الهبة الجماهيرية، أو الشعبية سواء في النزاعات المسلحة الدولية أو غير الدولية، وفي هذ السياق يُطرح تساؤل مفاده، من هو الشخص الذي يشترك في العمليات العدائية السيبرانية ويتمتع بصفة المقاتل؟

فالمقاتل هو عضو القوات المسلحة، أو من الفئات المشار إليها سابقا، وهو الذي يسمح بتوجيه هجمات على شبكات الحاسوب ضد المقاتلين، مثل جعل نظام التحكم في القوات الجوية ينقل معلومات ملاحية خاطئة لكي تُسبب هلاك القوات العسكرية التي يتم نقلها⁴، وبخصوص الجماعات المسلحة المنظمة، يشترط مشاركتها في الأعمال العدائية، أي وضوح ارتباطها بطرف النزاع، وهو ما ينطبق على أعضاء الشركات الأمنية الخاصة (قوات فاغنر الروسية مثلا)، نظرا للعقد الموقع بين هذه الشركات وواحد أطراف النزاع، لكن مفهوم مشاركة المدنيين بشكل مباشر في الأعمال العدائية، يقتصر على الأفراد الذين يشاركون في الأعمال العدائية، دون الانتماء إلى جماعة مسلحة ذات مهمة قتالية مستمرة⁵.

¹ مايكل ن. شميت، الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الحاسوب، المجلة الدولية للصليب الأحمر، مختارات من أعداد 2002، ص 91.

² C.I.J., Recueil 1986, p p 37 – 38.

³ مايكل ن. شميت، مرجع سابق، ص ص 94 – 95.

⁴ مايكل ن. شميت، مرجع سابق، ص 99.

⁵ سامر غر سالم الجاروشة، مرجع سابق، ص 52.

القانون الدولي الإنساني والحرب السيبرانية: حدود التطبيق وإمكاناته

ولابد من الإشارة هنا الى أنه يتطلب تعريف المقاتل الشرعي، بموجب قواعد القانون الدولي الإنساني مستوى من المسؤولية المنظمة أو قيادة دولة، وهذه السمات موجودة لدى الدول التي لديها قوات مسلحة ذات قدرات سيبرانية فقط، كالولايات المتحدة الأمريكية والصين وبعض الدول الأخرى.

أما بخصوص الاهداف العسكرية، فوفقا للفقرة الثانية من المادة 52 من البروتوكول الإضافي الأول لعام 1977¹، فإنه يشترط في الهدف المشروع شرطين هما:

- 1- يجب أن يسهم الهدف مساهمة فعالة في العمل العسكري للطرف المعادي، ويتم ذلك بأحد المعايير الآتية:
 - أ- بحكم طبيعته، أي أن يكون في أساسه وجوهه واستخدامه، وتعتبر أجهزة الحاسوب العسكرية والبنى التحتية العسكرية السيبرانية مثال على ذلك، فهي الأشياء التي تلبي معيار الطبيعة.
 - ب- المعيار الثاني بحكم موقعه، هذا المعيار تقليدي يشير الى المنطقة الجغرافية، لكن بالنسبة للحرب السيبرانية، فيمكن ان يساهم الهدف في العمل العسكري عن بُعد.
 - ج- المعيار الثالث بحكم استخدامها، أي عندما يتم الاستخدام لأهداف وأغراض عسكرية تصبح أجهزة شبكة الكمبيوتر المستخدمة، لأغراض عسكرية هدفا عسكريا.
 - د- المعيار الرابع بحكم الهدف، وهذا يشير إلى الاستخدام المستقبلي، فإذا كان الهدف لا يُستخدم الآن لأغراض عسكرية، ولكن يمكن أن يستخدم في المستقبل، وفي هذه الحالة يكتسب صفة الهدف العسكري بمجرد أن يتضح هذا الهدف أو الغرض.
- 2- يجب أن يكون تدمير الهدف، أو الاستيلاء عليه، أو تعطيله يُؤقّر للطرف المهاجم ميزة عسكرية أكيدة. والميزة العسكرية لم يتم تحديدها كليا ولا يمكن ذلك، بل يجب تقييم هذه الميزة العسكرية وفقا للظروف في وقت حدوث العمل العسكري، وعليه تُستبعد الهجمات التي تقدم ميزة محتملة أو غير محددة، لكن على خلاف ذلك الولايات المتحدة الأمريكية، تُدخل الأهداف الاقتصادية التي تعزز قدرات العدو على القتال في الحرب وتقويها بشكل غير مباشر ولكن بشكل فعال³.

¹ تنص الفقرة الثانية من المادة 52 من البروتوكول الإضافي الثاني لعام 1977 على أن: "تقتصر الهجمات على الأهداف العسكرية بحسب، وتنحصر الأهداف العسكرية فيما يتعلق بالأعبان على تلك التي تسهم مساهمة فعالة في العمل العسكري، سواء كان ذلك بطبيعتها أو بموقعها أم بغايتها أم باستخدامها، والتي يحقق تدميرها التام أو الجزئي أو الاستيلاء عليها أو تعطيلها في الظروف السائدة حينذاك ميزة عسكرية أكيدة".

² نور أمير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الإنساني، مذكرة ماجستير، الجامعة الافتراضية السورية، 2021، ص 37 - 38.

³ مايكل ن. شميت، مرجع سابق، ص 99.

ثانيا: المدنيون والأهداف المدنية

المدنيون هم الأشخاص الذين لا يقاتلون¹، ويشمل مفهوم "الأشخاص المدنيين" جميع الأشخاص المدنيين كما وضحت ذلك المادة 50 في فقرتها الثانية من البروتوكول الإضافي الأول لعام 1977، وفي حالة الشك حول ما إذا كان شخص ما مدنيا، أو غير مدني فإن ذلك الشخص يعد مدنيا، ولا يجوز تجريد السكان المدنيين من صفتهم المدنية بسبب وجود أشخاص منعزلين بينهم لا يستجيبون لشروط تعريف المدنيين²، ويتمتع المدنيون بحصانة من الهجمات، ما لم يقوموا بدور مباشر في الأعمال العدائية، وعلى مدى الوقت الذي يقومون خلاله بهذا الدور³.

لكن إذا قام المدني بالتدخل في العمليات العدائية، من خلال قيامه بهجوم سيراني لفترة قصيرة، قد لا تتعدى خمس دقائق، فإنه سوف يفقد حصانته خلال هذه المدة، وبالمقابل كيف يطبق النص سالف الذكر، في حال أن آثار هذا العمل العدواني لم تظهر فورا، وإنما استغرق ساعات، أو أيام لظهور آثاره التدميرية⁴.

ويمكن الإشارة إلى مسألة أخرى، في حالة قيام شخص مدني بوظيفة مستمرة تتضمن التحضير، أو التنفيذ أو القيادة لأعمال — (هجمات سيرانية) — ترقى إلى المشاركة المباشرة في الأعمال العدائية، فإن ذلك يترتب عليه فقدان صفة المدني، مما يجعله هدفا مشروعاً وبالتالي يمكن استهدافه.

أما بخصوص الأعيان المدنية، فإنه لا يجب أن تكون محلا للهجوم، أو لهجمات الردع⁵، والأعيان المدنية هي كافة الأعيان التي ليست أهدافا عسكرية، وهذا يعني أن الأهداف المسموحة بموجب القانون الدولي الإنساني فيما يتعلق بالعمليات السيرانية هي فقط الأهداف العسكرية، والتي هي من قبيل الحواشيب، أو نظم الحواشيب المستخدمة لدعم البنية التحتية العسكرية، أو البنية التحتية المستخدمة على وجه خاص لأغراض عسكرية، أي بمفهوم المخالفة، الحواشيب المستخدمة في المرافق الطبية مثلا، لا توجه لها الهجمات.

لكن هناك نوع من التلق في هذا الصدد، في أن الفضاء السيراني يتميز بالتوصيل بين نظم الحواشيب المتصلة ببعضها بعضا في أرجاء العالم، وغالبا ما يكون نظام الحواشيب العسكرية، متصلة بالنظم المدنية، أو التجارية وتعتمد عليها كليا أو جزئيا، وبالتالي يصعب شن هجوم سيراني على بنية تحتية عسكرية، وجعل الآثار تقتصر - على هدف عسكري فحسب⁶.

¹ المادة 50، الفقرة 1 من البروتوكول الإضافي الأول لعام 1977.

² الفقرة الثالثة من المادة 50 من البروتوكول الإضافي الأول لعام 1977.

³ الفقرة الثانية من المادة 43 من البروتوكول الإضافي الأول لعام 1977.

⁴ سلافة طارق الشعلان، مرجع سابق، ص 138.

⁵ الفقرة الأولى من المادة 52 من البروتوكول الإضافي الأول لعام 1977.

⁶ سلافة طارق الشعلان، مرجع سابق، ص 138.

القانون الدولي الإنساني والحرب السيبرانية: حدود التطبيق وإمكاناته

وتعد البيانات المدنية الأساسية، مثل البيانات الطبية والبيانات البيومترية وبيانات الضمان الاجتماعي وقوائم وسجلات الانتخابات وغيرها، عنصراً مهماً في المجتمعات الرقمية، لكونها أساسية لسير معظم جوانب الحياة، وأصبحت حمايتها أمراً مثيراً للقلق، لأنه قد يؤدي العبث بهذه البيانات الأساسية، أو حذفها في إحداث أضرار للمدنيين، قد تضاهي أو تفوق تدمير الأعيان المدنية، وهذه مسألة في غاية الأهمية، كون القانون الدولي الإنساني لا يحظر هذه الأعمال، لكن مع التطور الحاصل في عالم اليوم الذي يعتمد بشكل كبير على البيانات من الصعب استثناء البيانات المدنية من الحماية، التي يوفرها القانون الدولي الإنساني للأعيان المدنية¹.

ثالثاً: الأعيان مزدوجة الاستخدام

الأعيان مزدوجة الاستخدام، هي التي تضم أغراضاً عسكرية ومدنية على حد سواء²، وإذا كانت إحدى الأعيان تستخدم للأغراض العسكرية، فإنها تعتبر هدفاً عسكرياً معرضاً للهجوم، بما في ذلك الهجوم على شبكات الحاسوب، وحتى وإن كانت الأغراض العسكرية ثانوية بالنسبة للأغراض المدنية³، وينبغي التأكيد على أن تعبير الاستخدام المزدوج ليس مصطلحاً قانونياً، وترى اللجنة الدولية للصليب الأحمر، أن طبيعة أي هدف يجب تقديرها طبقاً لتعريف الأهداف العسكرية، الواردة في البروتوكول الإضافي الأول لعام 1977.

وقد أشار بعضهم، إلى أن العين التي تحمل إمكانية الاستخدام العسكري، ولكنها تُستخدم في الوقت الحالي لأغراض مدنية فقط، تعتبر هدفاً عسكرياً، إذا كان احتمال الاستخدام العسكري معقولاً، وغير بعيد في إطار النزاع المحدد الجاري⁴.

رابعاً: الأعيان التي تتمتع بحماية محددة

هناك بعض الأعيان التي تتمتع بحماية محددة، على غرار السدود والحواجز ومحطات توليد الكهرباء ومحطات توليد الطاقة النووية وغيرها، وبما أنها تعتمد في استغلالها وتشغيلها على الحاسوب وشبكات الحاسوب، فإنها ضعيفة للغاية أمام الهجمات السيبرانية، وقد أكدت المادة 56 في فقرتها الأولى من البروتوكول الإضافي الأول لعام 1977⁵ على أنه يُمنع الهجوم على هذه المنشآت، إذا كان هذا الهجوم قد يسبب إطلاق قوة خطيرة مثل المياه، أو النشاط الإشعاعي، وما يترتب عليها من خسائر كبيرة بين المدنيين، وينطبق هذا الحظر حتى إذا كانت هذه الأهداف عسكرية، ويشير البعض أنه باستخدام العمليات السيبرانية على

¹ اللجنة الدولية للصليب الأحمر، القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة، ورقة موقف اللجنة الدولية للصليب الأحمر، 2019، ص 7 - 8.

² من الأمثلة على الأعيان المزدوجة الاستخدام نذكر المطارات، خطوط السكك الحديدية، شبكات الكهرباء، المصانع التي تنتج أدوات وأشياء يستخدمها العسكريون والمدنيون، الأقمار الصناعية وغيرها.

³ مايكل ن. شبيت، مرجع سابق، ص 102.

⁴ سلافة طارق الشعلان، مرجع سابق، ص 142.

⁵ مايكل ن. شبيت، مرجع سابق، ص 102.

ولهي المختار

المنشآت، يؤدي إلى تعطيلها دون أن تتسبب في إطلاق قوى خطيرة، بعكس استخدام الأسلحة التقليدية (الحركية)، فإن أمر تعطيلها من الصعوبة بمكان.

خامسا: والممتلكات والأعيان التي لا غنى عنها لبقاء السكان المدنيين

يحظر القانون الدولي الإنساني، تلك الهجمات التي تؤدي إلى تجويع السكان المدنيين أو تدمير ممتلكاتهم التي لا غنى عنها، حتى وإن كان قوات العدو هي الضحية، وتشمل هذه الممتلكات التي لا غنى عنها أشياء مثل المواد الغذائية، والمحاصيل والماشية ومياه الشرب¹، وبالتالي فإنه لا يسمح بالقيام بهجمات سيرانية، على شبكات الحاسوب ضد مخازن الطعام ونظم التوزيع، أو محطات معالجة المياه، التي تخدم السكان المدنيين حتى ولو كانت القوات المسلحة أيضا تعتمد عليها².

كما أن البروتوكول الإضافي الأول لعام 1977، حظر العمليات العسكرية التي يُحتمل أن تتسبب في أضرار جسيمة بالبيئة وطويلة الأجل³، وقد تُسبب الهجمات السيرانية على شبكات الحاسوب، مثل هذه الأضرار والدمار، فعلى سبيل المثال الهجوم على شبكات الحاسوب لإطلاق مواد كيميائية، من مخازن أو منشآت الإنتاج، أو لقطع خطوط أنابيب رئيسية للنفط، قد يتسبب ذلك في دمار هائل للبيئة، ولهذا فإن مثل هذه الأفعال محظورة بموجب قواعد القانون الدولي الإنساني.

2.2: تطبيق المبادئ العامة للقانون الدولي الإنساني على الحرب السيرانية

إذا سلمنا أنه لا يجوز شن الهجمات السيرانية (الحرب السيرانية)، في النزاعات المسلحة إلا بالقدر الذي يكفل احترام قواعد القانون الدولي الإنساني سارية المفعول، وبالتالي يتطلب من أطراف النزاع التي تستخدم هذا النوع من الهجمات، أن تراعي عديد المبادئ التي تضمن تحقيق متطلبات المشروعية، لكن قد تظهر صعوبات أثناء تطبيق بعض مبادئ القانون الدولي الإنساني.

1.2.2: المبادئ الواجبة التطبيق قبل البدء في تنفيذ الهجوم السيراني

تمثل هذه المبادئ، في مبدأ التمييز بين ما يمكن استهدافه، وما لا يمكن استهدافه، بالإضافة إلى مبدأ الاحتياط، والذي يتضمن التدابير الوقائية لتجنب وقوع انتهاكات للقانون الدولي الإنساني.

¹ راجع المادة 54 من البروتوكول الإضافي الأول لعام 1977.

² مايكل ن. شميت، مرجع سابق، ص 104.

³ المادة 55 من البروتوكول الإضافي الأول لعام 1977.

القانون الدولي الإنساني والحرب السيبرانية: حدود التطبيق وإمكاناته

أولاً: مبدأ التمييز

لقد نصت الكثير من قواعد القانون الدولي الإنساني على مبدأ التمييز¹، الذي يعتبر من أهم المبادئ، التي تهدف إلى التمييز بين المقاتلين وغير المقاتلين، من جهة وبين الأعيان المدنية والأعيان العسكرية من جهة أخرى.

وهذا المبدأ واجب التطبيق على الحرب السيبرانية، في سياق نزاع مسلح، لكن قد تكون مسألة التمييز بين المدنيين والمقاتلين، وبين الأهداف المدنية والأهداف العسكرية، مسألة في غاية الصعوبة، عكس ما هي عليه العمليات العسكرية التقليدية، لكون المهاجم يوجد في مكان بعيد عن المكان المستهدف من الهجوم، مما يؤدي إلى استحالة التمييز بين المدنيين والمقاتلين، ومن الأمثلة على تلك الهجمات مجهولة المصدر، كالطائرات بدون طيار²، كما أنه بالنظر إلى مبدأ التمييز، الذي يقتد حظر الأسلحة التي يمكن بطبيعتها أن تستخدم بطريقة لا تميز بين الأهداف العسكرية والأهداف المدنية، فإن هذا الأمر لا يمكن الجزم به في الفضاء الإلكتروني، لأنه ببساطة كل عناصر البنية التحتية الإلكترونية، تكاد تكون ثنائية الاستخدام، وأن القوات العسكرية تستخدم إلى حد كبير نفس المنشآت الإلكترونية التي تُستخدم في الأغراض المدنية، نظراً للطبيعة المترابطة لشبكات الحاسوب.

وعليه فإنه يكون من المستحيل شن هجوم سيبراني، على منشآت وبنى تحتية عسكرية وجعل آثارها تقتصر - على هدف عسكري فقط، دون أن تتعدى هذه الأضرار إلى المدنيين والمنشآت المدنية، لأن مبدأ التمييز يحظر استخدام السلاح، الذي لا يمكن لآثاره أن تميز بين الأهداف العسكرية والأهداف المدنية، فهل الهجمات الإلكترونية، إذا وُجّهت إلى هدف عسكري، كان بالاستطاعة التحكم في الآثار الناتجة عن استخدامها، أي إصابة الهدف العسكري في المقام الأول؟

إن ما يصيب المدنيين أو الأهداف المدنية، من جزاء الهجمات السيبرانية من أضرار، لا يمكن اعتبارها غير مقصودة، أو ملازمة لاستخدام السلاح، وبالتالي يكون استخدام هذا السلاح غير مشروع في هذه الحالة.

ويمكن الإشارة هنا، إلى صعوبة التمييز بين الأهداف العسكرية والأهداف المدنية في الحروب السيبرانية فالأعيان التي تُستخدم لأغراض مدنية وعسكرية، تتحول إلى أهداف عسكرية بمجرد مشاركة الأعمال العدائية، فعلى سبيل المثال أجهزة الرادار التابعة لدولة ما وظيفتها مراقبة الطائرات والسفن المدنية، تصبح هدفاً عسكرياً مشروعا، إذا تم استخدامها لرصد طائرة أو سفينة عسكرية، وهذا لكون هذه الأجهزة والمنشآت

¹ قواعد القانون الدولي الإنساني العرفي، (المواد من 1 إلى 10) والبروتوكول الإضافي الأول لعام 1977 (المادتان 51 - 52)، اتفاقية جنيف 1980 المتعلقة بحظر أو تقييد استعمال أسلحة تقليدية معينة يمكن اعتبارها مفرطة الضرر أو عشوائية الأثر (ديباجة الاتفاقية) والمادة الثالثة من البروتوكول الثاني المعدل والمتعلق بحظر أو تقييد استعمال الألغام والأشراك الخداعية والنبائط الأخرى لعام 1996.

² عمر محمود عمر، مرجع سابق، ص 144.

ولهي المختار

مزدوجة الاستخدام، لكن في حالة الشك فيما إذا كانت هذه العين، التي تُستخدم في الأصل لأغراض مدنية، وتُستخدم لتقديم مساهمة فعالة في العمليات العسكرية هل يجوز استهدافها؟

هذه المسألة أجابت عنها القاعدة (100) من دليل تالين، التي أشارت إلى ضرورة التقييم الدقيق لإثبات الاستخدام العسكري، ويجب على المهاجم مراعاة جميع المعلومات المتاحة، للوصول إلى قناعة حول هذا الاستخدام، ووضوح المعلومات والاستنتاجات، بما في ذلك مصداقية المصدر، أو أجهزة الرصد والاستشعار، وتاريخ المعلومات واحتماله التعرض للخداع وإمكانية سوء تفسير البيانات، ولكن هذا الأمر في غاية الصعوبة، فهل يمكن تحديد طبيعة استخدام كل جهاز حاسوب، أو شبكة حاسوبية موجودة في البنية التحتية الإلكترونية للدولة؟ لأن الفضاء السيبراني هو عالم افتراضي، لا تنطبق عليه المعايير المادية للتمييز¹.

ثانيا: مبدأ الاحتياط (إعمال التدابير الوقائية)

إن التدابير الوقائية الواجب اتخاذها أثناء القيام بالعمليات العدائية، نص عليها البروتوكول الإضافي الأول لعام 1977، ويشمل النزاعات المسلحة الدولية، أما البروتوكول الإضافي الثاني لعام 1977، لم ينص على مثل هذه التدابير الوقائية في النزاعات المسلحة الداخلية²، ولإعمال هذه التدابير بخصوص الحروب السيبرانية، تُطرح عدة إشكالات نظرا لطبيعة الفضاء السيبراني، وقد أورد دليل تالين الطرق والتقدير التي يجب اتخاذها عند تنفيذ الهجمات السيبرانية وهي³:

1- احتياطات يجب اتخاذها قبل شن الهجمات السيبرانية، وتمثل في الرعاية المستمرة أثناء العمليات العدائية والتحقيق من الأهداف وكذا اختيار الوسائل المستخدمة في الهجوم، فضلا عن إمكانية إلغاء الهجوم، أو إيقافه، بالإضافة إلى القيام بالتحذيرات اللازمة، عن طريق توجيه إنذار مسبق بشأن الهجمات السيبرانية التي قد تؤثر على السكان المدنيين⁴.

وعموما تشمل التدابير الوقائية، التي ينبغي أخذها بعين الاعتبار: فصل البنية التحتية والشبكات السيبرانية العسكرية عن المدنية، والعمل على تحديد هوية البنية التحتية والشبكات السيبرانية، التي تخدم بشكل خاص الاعيان المشمولة بالحماية مثل المستشفيات⁵.

¹ عمر محمود اعمر، مرجع سابق، ص 145.

² النزاعات المسلحة الداخلية تطبق عليها التدابير الوقائية المكرسة في القانون الدولي الإنساني (القاعدة 15).

³ سلافة طارق الشعلان، مرجع سابق، ص 48 - 50.

⁴ يمكن القياس بخصوص الهجمات السيبرانية على ما أوردته المادة الثالثة في فقرتها الحادية عشر- من البروتوكول الثاني المتعلق بحظر أو تقييد استعمال الألغام والأشراك والنبائط الأخرى لعام 1996، حيث جاء في هذه الفقرة: "يجب إعطاء إنذار مسبق فعال بأي زرع للألغام وأشراك خداعية أو نبائط أخرى، قد تؤذي السكان المدنيين، ما لم تحل الظروف دون ذلك".

⁵ اللجنة الدولية للصليب الأحمر، القانون الدولي الإنساني وتحديات النزاعات المعاصرة، مرجع سابق، ص 43.

القانون الدولي الإنساني والحرب السيبرانية: حدود التطبيق وإمكانياته

2- احتياطات ينبغي اتخاذها لتلافي آثار الهجمات السيبرانية، وتتمثل في القيام بعزل البنى التحتية الإلكترونية العسكرية عن المدينة، ودعم البيانات المدنية الرقمية بنسخ احتياطية واستخدام الإجراءات المضادة لفيروسات الحاسوب، لحماية النظم المدنية وتطوير قدرات رد الفعل، لمنع التسلل من قبل الأطراف المعادية للنظم الإلكترونية المدنية.

2.2.2: المبادئ التي تحكم سير العمليات العدائية أثناء استخدام الهجمات السيبرانية

يعتبر مبدئي التناسب والضرورة، من أهم المبادئ الأساسية في القانون الدولي الإنساني التي يجب احترامها، والخضوع لها أثناء سير العمليات العدائية، ولو باستخدام أسلحة جديدة كالفضاء السيبراني.

أولاً: مبدأ التناسب

يهدف مبدأ التناسب إلى إقامة نوع من التوازن، بين مصلحتين متعارضتين، تتمثل أولاهما فيما تمليه اعتبارات الضرورة العسكرية، من استخدام أكثر الأسلحة العسكرية قدرة على تحقيق ميزة عسكرية، وثانيهما تتمثل فيما تمليه الاعتبارات الإنسانية، من ضرورة العمل على تجنب الأضرار قدر الإمكان بغير المقاتلين، أو بالأهداف المدنية¹، وقد نص على هذا المبدأ المادة 51 من البروتوكول الإضافي الأول لعام 1977، إلى جانب القانون الدولي الإنساني العرفي.

وبخصوص تطبيق مبدأ التناسب، عندما يتم توجيه هجمات سيبرانية ضد منشآت مزدوجة الاستخدام يكون الأمر في غاية الصعوبة، لأن الميزة العسكرية لن تكون واضحة وجليّة بالقدر الكافي لتطبيق هذا المبدأ، لا سيما أن الميزة العسكرية الملموسة والمباشرة المنتظرة من هجوم على هدف مشروع، قد تتغير باستمرار وفقاً للواقع الميداني، المتعلق بخطط القادة الميدانيين، وتطور العمليات العسكرية على كلا الجانبين².

كما أن البعض يشير أيضاً، إلى أن مسألة التناسب تعتبر معادلة في غاية الصعوبة والدقة، حتى أثناء العمليات الحربية التقليدية، كون تحقيق المهمة القتالية وإحراز النصر- هدف أساسي للقوات العسكرية، وتنفيذ القوانين وضبط التدمير وعدم إلحاق أضرار مفرطة بالخصم، التزام قانوني واجب النفاذ، ولذلك يحتاج الأمر إلى قائد ماهر شديد لكي يسوي ميزان هذه المعادلة³، والأمر بدون شك يزداد تعقيداً إذا ما تعلّق بالهجمات السيبرانية⁴، بالنظر إلى مخاطر هذه الهجمات، بسبب الترابط بين الأنظمة المدنية والعسكرية، والآثار التي لا يمكن التحكم فيها، التي تصيب البنى التحتية، وهذا جعل بعض الفقهاء ومنهم (Sliw) يؤكدون على أن مبدأ

¹ محمود مجازي محمود، حيازة واستخدام الأسلحة النووية في ضوء أحكام القانون الدولي، مطبعة العشري، جمهورية مصر العربية، 2005، ص 52.

² يحيى ياسين سعود، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، المجلة القانونية، الخرطوم، السودان، المجلد 04، العدد 04، 2018، ص 96.

³ أحمد الأنوار، قواعد وسلوك القتال، دراسات في القانون الدولي الإنساني، مؤلف جامعي، إعداد نخبة من المتخصصين والخبراء، دار المستقبل العربي، القاهرة، ط 1، 2000، ص ص 319 - 320.

⁴ يحيى ياسين سعود، مرجع سابق، ص 97.

ولهي المختار

التناسب، لا يزال غامضا بخصوص استخدام القوة السيبرانية ولا يزال يحتاج إلى أجوبة أهمها: كيف يمكن ضمان مبدأ التناسب في الرد على الهجمات السيبرانية¹.

ثانيا: مبدأ الضرورة العسكرية

يعتبر مبدأ الضرورة العسكرية من أهم المبادئ الأساسية للقانون الدولي الإنساني، ويقصد به استخدام القوة العسكرية الضرورية لتحقيق الهدف الرئيسي - من القتال وهو تحقيق النصر - ، مع مراعاة قواعد القانون الدولي الإنساني المنظمة للنزاع المسلح، ولهذا فإن أطراف النزاع يمكنهم مهاجمة أعيان مدنية كضرورة ملحة إذا كانت هاته الأخيرة تُسهم بطريقة غير مباشرة في تحقيق ميزة عسكرية أكيدة، وقد تم الإشارة إلى مبدأ الضرورة في عديد الاتفاقيات، نذكر منها على سبيل المثال اتفاقية لاهاي لعام 1907 (المواد 43، 54) والبروتوكول الإضافي الأول لعام 1977 من خلال المواد (2/52 و 5/54 و 1/62 و 4/67 و 3/71)، كما اعتبر النظام الأساسي للمحكمة الجنائية الدولية انتهاك مبدأ الضرورة جريمة حرب².

وقد تم تحديد الشروط الواجب توافرها، عند اللجوء لمبدأ الضرورة العسكرية في القانون الدولي الإنساني وهي:

1- أن يكون هذا التجاوز ظرفيا، أي مؤقتا ومرتبطا بالمدة التي تقتضيها الضرورة.

2- أن يكون على أهداف محددة.

3- أن يكون الغرض منها تحقيق ميزة عسكرية أكيدة

4- أن يتم مراعاة قواعد القانون الدولي الإنساني.

وقد أشار (دليل تالين) إلى أن الهدف يجب أن يكون اختياره للهجوم السيبراني هو ذلك الهدف الذي يتوقع منه أن يسبب خطرا أقل على المدنيين والأعيان المدنية، وفي حالة وجود العديد من الأهداف إلا أن إحداها تُحقق ميزة عسكرية أكثر من مثيلاتها ففي هذه الحالة من حق المهاجم توجيه الهجمات السيبرانية المباشرة ضد الهدف العسكري، الذي يُحقق أكثر ميزة عسكرية ممكنة في إطار النزاع المسلح.

وعليه يجب أن يُنظر بشأن الهجمات السيبرانية، إلى الأضرار التي تلحق بالمنشآت والبنى التحتية ذات الأهمية بالنسبة للمدنيين، فضلا عما تُسببه هذه الأضرار التي تلحق بالمدنيين من الحرمان من وظائف وخدمات هذه المنشآت، تطبيقا لمبدأ الضرورة³.

¹ هذا الرأي مشار إليه عند أحمد عيسى- الفتلاوي، الهجمات السيبرانية - مفهومها - والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، المجلد 8، العدد 4، 2016، ص 638.

² نصت المادة (4/2/8) من نظام روما الأساسي على أن: "الحاق تدمير واسع النطاق بالممتلكات والاستيلاء عليها دون أن تكون هناك ضرورة عسكرية تبرر ذلك وبالمخالفة للقانون وبطريقة عابثة".

³ بنجي ياسين سعود، مرجع سابق، ص 94.

القانون الدولي الإنساني والحرب السيبرانية: حدود التطبيق وإمكاناته

وانطلاقاً مما سبق ذكره، فإن تطبيق هذا المبدأ، قد يطرح بعض الصعوبات فيما يتعلق بالهجمات السيبرانية، نظراً لصعوبة التمييز بين الأهداف المدنية والأهداف العسكرية في الفضاء السيبراني، ذلك لأن المنشآت التي تُقدّم خدمة للجهد العسكري، هي في الوقت نفسه تُقدم خدمة للقطاع المدني، وعليه فإنه يجب على المقاتل السيبراني تحديد كل حالة على حدة، أي أنه في حالة يجب عليه أن يقرر بشكل قاطع، أن الهجوم السيبراني يُوفر ميزة عسكرية لتحقيق هدف عسكري¹.

ويمكن الإشارة أيضاً، إلى أن الضرورات العملية لتطبيق مبدأ الضرورة العسكرية، يصعب تطبيقها على الهجمات السيبرانية، فعلى سبيل المثال يمكن تحقيق الأهداف المرجوة بأسر المقاتلين فقط دون قتلهم، فوجود المقاتل في ساحة القتال أفضل دائماً لقدرته على اتخاذ القرار المناسب، والقدرة على التمييز بين الذي يدّعي الإصابة، وفي الحقيقة هو يمثل تهديداً، وبالتالي يمكن استهدافه طبقاً لمبدأ الضرورة العسكرية، وبين ذلك المقاتل الذي أصيب وكان جرحه بالغا، ولم يعد يُمثل تهديداً، وعليه يمكن القول بأن مبدأ الضرورة العسكرية يستلزم أن تكون القوة المسلحة لا تتضمن عمليات الثأر، بالإضافة إلى عدم وجود بدائل أخرى، للتدابير والإجراءات المزمع اتخاذها، استناداً لمبدأ الضرورة².

خاتمة:

تعتبر الحرب السيبرانية، من المواضيع الحديثة في القانون الدولي العام والقانون الدولي الإنساني، باعتبارها ثورة في الوسائل والأساليب المستخدمة، في النزاعات المسلحة التقليدية، حيث أصبحت الدول تتجه إلى هذا النوع من الحروب، التي لا تتطلب تكاليف كبيرة لتوفرها بالمقارنة مع الأسلحة التقليدية، التي تتطلب في الغالب أموالاً كبيرة، لكن ما زالت هناك عدة زوايا غامضة بخصوص هذه الحرب، والتي تتعلق بالضوابط القانونية التي تحكمها، رغم اعتبار البعض بأن هذه الحرب تعتبر بمثابة حرب فعلية وحقيقية، ولا تختلف عن الحروب التقليدية لما تُخلّفه من آثار مدمرة وأضرار جسيمة.

ولا شك في أن تطبيق قواعد القانون الدولي العام، والقانون الدولي الإنساني، على الحرب السيبرانية ليست عملية مثلاً هو عليه في النزاعات المسلحة التقليدية، بسبب الفوارق الجوهرية بين الهجوم السيبراني، والهجوم المسلح المادي.

وانطلاقاً مما سبق نخلص إلى مجموعة من النتائج من أهمها:

¹ نور أمير الموصللي، مرجع سابق، ص 53، نقلاً عن:

- Gervais, Michael: "Cyber Attacks and The Laws of War", Berkeley Journal of International Law, Volume 30, Issue 2, Article 6, 2012, p 33.

² نجى ياسين سعود، مرجع سابق، ص 96.

ولهي المختار

1- الحرب السيبرانية من المفاهيم الحديثة، التي لا يوجد إجماع على تعريفها، لأنها تدور في فضاء ومجال جديد أصطلح على تسميته الفضاء السيبراني، ويفرض على المجتمع الدولي إعادة التفكير في مفهوم الأمن الدولي ولتتمكن الدول من حماية أراضيها واستقلالها السياسي.

2- قد ينطبق القانون الدولي الإنساني على الحرب السيبرانية، في كثير من العمليات السيبرانية، التي تقع في سياق النزاع المسلح، لكن لا ينظمها كافة، لعدة عوامل من أهمها صعوبة التمييز بين المدني والمقاتل، بالإضافة إلى أنه ليس من اليسير تحديد هوية الفاعل أو المكان الذي تنطلق منه الهجمات السيبرانية، فضلا عن الصعوبة نفسها في تطبيق مبادئ الضرورة العسكرية والتناسب.

3- يدعم كثير من الفقهاء وخبراء القانون الدولي (على غرار الخبراء الذين أعدوا دليل تالين) اعتبار الأسلحة السيبرانية، مثل الأسلحة التقليدية، وأنه يمكن إخضاعها لقواعد القانون الدولي الإنساني، على غرار شرط مارتينز والمادة 36 من البروتوكول الإضافي الأول لعام 1977 أو قياسا على آراء محكمة العدل الدولية، خاصة رأيها الاستشاري حول الأنشطة العسكرية وشبه العسكرية في نيكاراغوا لعام 1986.

4- عدم تحديد معايير دقيقة لاستخدام الأسلحة الالكترونية، في الهجمات السيبرانية التي تحدث في سياق النزاع المسلح، يطرح صعوبة عدم إمكانية تطبيق بعض الشروط الواجب توافرها، من أجل تفعيل المادة 51 من الميثاق على الهجمات السيبرانية، وبالأخص تحديد شرطي الضرورة والفورية، في رد الهجوم لكي تقوم الدولة المعتدى عليها، باتخاذ إجراءات الدفاع عن النفس، وهذا لصعوبة معرفة الجهة التي قامت بالهجوم، إلا بعد مدة زمنية طويلة، وعندها يسقط حقا الدولة في الدفاع عن نفسها.

وبناء على سبق ذكره، يمكن إبداء بعض المقترحات لعل أهمها:

1- الحاجة الماسة لتطوير قواعد القانون الدولي الإنساني، لتغطية كل جوانب الحرب السيبرانية، بغية توفير الحماية الكافية للسكان المدنيين، والأعيان المدنية، ومواكبة التطورات المتسارعة للوسائل التكنولوجية الحديثة المستخدمة في هذه الحرب.

2- دعوة المجتمع الدولي من دول ومنظمات دولية، لاعتماد اتفاقية دولية من شأنها وضع قواعد قانونية، تحكم حالات الحرب والنزاع في الفضاء السيبراني، أو على الأقل للحد من التسلح داخل الفضاء السيبراني، مثل تلك الاتفاقيات التي تم إبرامها سابقا بشأن حظر الانتشار النووي والكيميائي والبيولوجي.

3- يقع على منظمة الأمم المتحدة دور هام وبارز، لتطوير التشريع الدولي المتعلق بالحرب السيبرانية، وهذا لاستيعاب هذا النوع الجديد من الحروب، وحالات العدوان السيبراني وكذا حالات الدفاع عن النفس، بما يحافظ على السلم والأمن الدوليين.

4- ضرورة إقرار مسؤولية الدولة على جميع التصرفات، التي يقوم بها بعض الأفراد أو المجموعات الذين يعملون وفق توجيهاتها، أو تحت إدارتها والذين يقومون بتطوير البرامج الالكترونية، بغية المساس بسيادة الدول

القانون الدولي الإنساني والحرب السيبرانية: حدود التطبيق وإمكانياته

الأخرى ومصالحها الحيوية، واعتبار ذلك خرقاً لالتزام دولي، وتفعيل المسؤولية الجنائية الفردية تجاههم، واتجاه من يقومون وراءهم، سواء أمام القضاء الوطني، أو أمام المحكمة الجنائية الدولية.

قائمة المصادر والمراجع

أولاً: المراجع باللغة العربية

أ- الكتب

1- أحمد عيسى نعمة الفتلاوي، الهجمات السيبرانية (دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر)، ط 01، منشورات زين الحقوقية، بيروت، 2018.

2- القانون الدولي الإنساني والعمليات السيبرانية خلال النزاعات المسلحة، اللجنة الدولية للصليب الأحمر، نوفمبر 2019.

3- سامر نمر سالم الجاروشة، الجرائم السيبرانية وحقوق الإنسان في القوانين الدولية والوطنية، دار النهضة العربية، ط 1، 2023.

4- محمود حجازي محمود، حيازة واستخدام الأسلحة النووية في ضوء أحكام القانون الدولي، مطبعة العشري، جمهورية مصر- العربية، 2005.

5- محمود محارب، إسرائيل والحرب السيبرانية - قراءة في كتاب حرب في الفضاء الإلكتروني: اتجاهات وتأثيرات على إسرائيل، مراجعة كتب صادرة عن المركز العربي للأبحاث ودراسة السياسات، 2011.

ب- الرسائل الجامعية

نور أمير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الإنساني، مذكرة ماجستير، الجامعة الافتراضية السورية، 2021.

ج- المقالات

1- أحمد الأنوار، قواعد وسلوك القتال، دراسات في القانون الدولي الإنساني، مؤلف جماعي، إعداد نخبة من المتخصصين والخبراء، دار المستقبل العربي، القاهرة، ط 1، 2000.

2- أحمد عيسى الفتلاوي، الهجمات السيبرانية - مفهومها - والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر مجلة المحقق الحلي للعلوم القانونية والسياسية، المجلد 8، العدد 4، 2016

3- أسامة صبري محمد، الحرب الإلكترونية ومبدأ التمييز في القانون الدولي الإنساني، مجلة القانون للدراسات والبحوث القانونية العدد 07، 2013.

4- عمر محمود اعمر، الحرب الإلكترونية في القانون الدولي الإنساني، مجلة الشريعة والقانون، الجامعة الأردنية، الأردن، المجلد 46، العدد 03، 2019.

5- دخلافي سفيان، تطبيق الهجمات السيبرانية في ضوء أحكام القانون الدولي، المجلة الأكاديمية للبحث القانوني، المجلد 13 العدد 02، 2022.

ولهي المختار

- 6- سامي محمد عبد العال، الدفاع الشرعي ضد الهجمات السيبرانية، المجلة المصرية للقانون الدولي، المجلد 79، 2023.
- 7- سنوسي علي، الهجمات السيبرانية في ضوء أحكام القانون الدولي الإنساني والاتفاقيات الدولية، مجلة الحقوق والعلوم السياسية، جامعة خنشلة، المجلد 10، العدد 02، 2023.
- 8- سعيد درويش، الحروب السيبرانية وأثرها على حقوق الانسان: دراسة على ضوء أحكام دليل تالين، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية، المجلد 54، العدد 5، 2017.
- 9- سلافة طارق الشعلان، تكييف استخدام الحرب الالكترونية، في النزاعات المسلحة وفقا للقانون الدولي الإنساني، مجلة الكوفة، المجلد 01، العدد 26، 2016.
- 10- علي فاضل علي سلمان، حق الدفاع الشرعي على الهجمات السيبرانية، مجلة جامعة تكريت للحقوق، السنة 04، العدد 04، الجزء 01، 2020.
- 11- مايكل ن. شميت، الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الحاسوب، المجلة الدولية للصليب الأحمر، مختارات من أعداد 2002.
- 12- يحيى ياسين سعود، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، المجلة القانونية، الخرطوم، السودان، المجلد 04، العدد 04، 2018.

ثانيا: قائمة المصادر والمراجع باللغة الاجنبية

1. Kelsen, Hens : Principes Of International Law, 2 éditions, Holt, Rinehart and Winston, New York, 1966.