مجلة الحقوق والحريات
المجلد 11 ، العدد 1
السنة 2023 ، ص157-ص178

مفهوم الحروب السيبرانية والأمن السيبراني

The concept of cyber warfare and cyber security

د.شويرب جيلالي .ط/دمراد فائزة

(1) جامعة عمار ثليجي الأغواط.كلية الحقوق والعلوم السياسية

البريد الالكتروني:djelloulchouireb1979@gmail.com

(2) جامعة الدكتور يحي فارس المدية كلية الحقوق والعلوم السياسية /المخبر السيادة والعولمة

البريد الالكتروني المهني: merad.faiza@univ-medea.dz

تاريخ الارسال:	تاريخ القبول:	تاريخ النشر:
2022/12/26	2023/04/14	2023/04/20

ملخص:

أصبحت العلاقات الدولية تخضع لتأثيرات الفضاء الإلكتروني في السلم أو الحرب واكتست النزاعات الدولية طابعا آخر عوض الحروب التقليدية وهو الهجمات السيبرانية ،وهي العمليات التي تتخذها الدول للهجوم على نظم المعلومات لدول أخرى بغية الإضرار بالبنى التحتية للعدو، هذا الأمر جعل الدول تعمل على حماية قواعد بياناتها وفق ما يسمى بالأمن السيبراني أو مجموع الوسائل التقنية التي تحميها ضد أي إختراق مضاد،كما تعرف الحروب السيبرانية وفق القانون الدولي الإنساني بأنها إمتداد للحروب التقليدية تستخدم جيش مدني وآخر عسكري لضرب شبكات البيانات في حال قيام نزاع ، وقد إنقسم الفقه الدولي إلى رأي يرى ضرورة إلحاقها للقواعد الإنسانية ورأي يعارض ذلك لما تحمله من خصوصية.

الكلمات المفتاحية - الحروب، الفضاء السيبراني ،الأمن السيبراني ،القانون الدولي

Abstract:

International relations have become linked to cyberspace in times of peace or war, international conflicts have also become like cyber-attacks, case law has defined these attacks as "operations undertaken by countries to attack the information systems of other countries in order to harm them. This pushes states to protect their databases through cyber security

International humanitarian law has defined cyber-attacks as an extension of conventional warfare and they use both civilian and military militaries when attacking enemy electronic space. International jurisprudence is divided into two parts, one submits these wars to humanitarian law and the other opposes.

Keywords : Wars, Cyberspace, Cyber security, International Law

مقدمة:

يعتبر العصر الحديث عصر التكنولوجيا التي سيطرت على جميع نواحي الحياة والتي تتطور يوما بعد يوم بسرعة كبيرة حتى أصبح الفضاء الإلكتروني عصب الحياة المعاصرة للأفراد والدول وأصبحت شبكة الإنترنت مجالا خصبا للتواصل و الإتصال ووسيلة ربط للحياة الإجتماعية والسياسية والإقتصادية على المستوى الدولي ،وأصبح عمل جميع قطاعات الدولة يختزل في مجموعة بيانات ومعلومات مسجلة على الحواسيب والأمر نفسه بالنسبة لبيانات الأفراد ،وعلى هذا الأساس تحولت العلاقات الدولية خاصة النزاعات بين الدول إلى هذا الفضاء الإلكتروني وأصبحت أداة للهجوم وللدفاع بما يسمى بالهجمات السيبرانية وكذا إجراءات حماية المعلومات التي تتبناها كل دولة حماية لمصالحها، أو الحروب السيبرانية في حالات أشد خطورة تغير فيها المفهوم التقليدي للحروب، و اكتسى النزاع الدولي صبغة إلكترونية لم تعد تلتفت إلى المفاهيم التقليدية للصراع .

وعليه فإن من يملك المعلومة يملك القوة كما أن حرب اليوم هي حرب المعلومة ما يستلزم دراسة الموضوع لمعرفة واقع اليوم ومدى تأثير التكنولوجيا الحديثة في قوة الدول و أمنها المعرض للإختراق الذي لم يعد يقتصر على دولة معادية فقط وإنما قد يحدث من طرف فرد أو جماعة أفراد أو هيئات في شكل أداة ضغط وفي كثير من الأحيان أداة تدمير للآخر، وقد شهد العالم الحديث مثل هذا النوع من الصراعات الذي أدى إلى دمار شامل بسرعة مرعبة.

وعليه وبغية التوعية لمعرفة هذا المفهوم الجديد للنزاعات الدولية والذي تعدت آثاره الحكومات إلى الأفراد ، أصبح واجب الإحتياط و المساهمة في مكافحة هذه الظاهرة واجبا مشتركا بين كافة الأطراف .

وبناء على ما سبق نطرح إشكالية الدراسة كالتالي :

كيف شكل الفضاء السيبراني العلاقات الدولية الحديثة في السلم وفي الحرب ؟

وتندرج تحت هذ الإشكالية تساؤلات فرعية نوجزها في التالي

ما مفهوم الهجومات والدفاع السيبراني ؟

هل تلاءمت خصوصيات النزاع السيبراني مع القواعد الإنسانية للنزاعات الدولية ؟

لنحاول الإجابة عليها من خلال مبحثين خصصنا الأول للحروب السيبرانية والأمن السيبراني فعرفنا في المطلب الأول مفهوم الحروب السيبرانية وخصائصها لنتناول في المطلب الثاني ماهية الأمن السيبراني وأبعاده ثم في المبحث الثاني درسنا مدى تطابق أو خضوع هذا النوع الحديث من الحروب للقانون الدولي الإنساني من خلال مطلب أول خصصناه لبحث تطبيق قواعد هذا القانون على الحروب السيبرانية وتناولنا في المبحث الثاني مجموع الآراء الفقهية والقانونية بين مؤيد ومعارض لملائمة هذه القواعد لحروب حديثة مختلفة .

ولقد انتهجنا في بحثنا المنهج الوصفي التحليلي لعرض المفاهيم والمعلومات وشرحها وبالنسبة للدراسات التي تناولت هذا الموضوع نجد العديد ..منها كتاب للمؤلف محمد سعد محمود ،الحرب السيبرانية أدواتها وقودها خسائرها وهي دراسة حديثة صدرت العام2020

المبحث الأول :مفهوم الحرب السيبرانية والأمن السيبراني

إن الإشكال الأول هو تحديد مفهوم الحروب السيبرانية فعالم اليوم أصبح عالم المعلومات فمن يملك المعلومة يملك القوة وعليه أصبح من أولى أولويات الدول و الأشخاص كيفية إمتلاك المعلومة وحمايتها،وعليه بعدما كان الطرح حول الجريمة الإلكترونية و الإحتيال الإلكتروني أصبحت حرب المعلومات والأمن المعلوماتي أو الحرب السيبرانية والأمن السيبراني ميزة السياسات الأمنية الوطنية في جميع دول العالم[1]

[1] محمد سعد محمود ،الحرب السيبرانية أدواتها وقودها خسائرها تاريخ الاطلاع :2022/11/01سا 20.10 ،ص2 Noor-book.com2020

المطلب الأول :مفهوم الحروب السيبرانية

إن لكل ظاهرة جذور ،نعزو إليها نشأتها ثم تطورها ،ومنذ ظهور الإنترنت كشبكة إتصال عالمية حديثة ،تغيرت المفاهيم وتغيرت معها طبيعة العلاقات الدولية والفردية ،وأصبح الفضاء المعلوماتي يحمل الكثير من التفاعلات والتعقيدات بين البشر وفي جميع نواحي الحياة ،فظهر نوع حديث من الإجرام هو الجريمة السيبرانية التي تطورت في كثير من الأحيان إلى حد الحرب السيبرانية بما تحمله الحرب من آثار مدمرة وعليه لابد أن نتعرف أولا على أسس ظهور هذه الحرب وماهيتها ثم نتناول خصائصها

الفرع الأول : أساس وتعريف الحروب السيبرانية

Kybernetes سيبرانية مشتقة من الكلمة اليونانية بمعنى القيادة والتحكم عن بعد[1]

وقد عرف ميشال شميت الهجمات السيبرانية أنها "تلك الإجراءات التي تتخذها الدولة من أجل الهجوم على نظم المعلومات للعدو بهدف التأثير و الإضرار بها والدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة و إذا سببت الهجومات السيبرانية نزاعا مسلحا بوصفها عملية إلكترونية سواء هجومية أو دفاعية مما قد يخلق إصابات أو قتل أشخاص أو الإضرار بممتلكات وتدميرها أصبحت حربا سيبرانية بمفهوم القانون الدولي الإنساني2،وتتميز الحرب السيبرانية بأنها حرب غير محددة المجال وغامضة الأهداف كونها تتحرك عبر شبكات عابرة للحدود الدولية بسرعة تتطابق وواقع سرعة المعلومة في هذا العصر مما يسبب تدميرا واسع النطاق ضد المنشآت الحيوية للدول ،وفي حال النزاع المسلح قد ينعكس الهجوم السيبراني الذي يؤدي إلى تعطيل شبكات المعلومات للدول على المدنيين ويحرمهم من الحاجات الأساسية كالمياه و الرعاية الطبية والكهرباء.

---

[1] فارس قرة،الأمن السيبراني،تاريخ النشر2019/08/28،تاريخ الاطلاع 2022/11/04،الموسوعة السياسية http://political-encyclopedia.org/dectionary

[2] نسيب نجيب،الحرب السيبرانية من منظور القانون الدولي الإنساني ،المجلة النقدية للقانون والعلوم السياسية كلية الحقوق والعلوم السياسية ،جامعة تيزي وزو،المجلد 19 ،العدد 4، 2021،ص222

وتعرف الهجمات السيبرانية بأنها " تلك الإجراءات التي تتخذها الأطراف في نزاع مسلح لكسب الميزة على خصومهم في الفضاء الإلكتروني وتحصل المزايا من خلال إتلاف أو تدمير وتعطيل أو إختراق أنظمة الحاسوب للعدو أو الحصول على معلومات سرية (التجسس السيبراني) متى كانت في إطار نزاع مسلح يصل إلى مستوى الحرب1 ،ويشير مصطلح الحرب السيبرانية إلى إستخدام الحواسيب وشبكة الإنترنت لأغراض هجومية ويدعى من يقوم بهذه الأفعال hackers أي المخترقين ،كما يستخدم الإختراق في أغراض أخلاقية مثل إعادة إسترجاع المواقع الشخصية وحماية ثغرات الأنظمة المستخدمة في الإنترنت .ويندوز لأنه نظام يدرس بصورة علمية جميع فنون الإختراق[2]

كما يستعمل مصطلح سيبراني لوصف كل مايتعلق بالشبكات الإلكترونية الحاسوبية وشبكة الإنترنت والفضاء السيبراني كل ما يتعلق بالحاسوب والإنترنت والتطبيقات المختلفة كالفيس بوك والواتساب وغيرها ... و تكمن خطورة الحروب السيبرانية في إستغلالها غير المشروع لأنظمة الحواسيب والشبكات والمنظمات التي يعتمد عملها على الإتصالات الرقمية بهدف إحداث أضرار من خلال محاولة تعطيل أو منع أو تدمير مصادر النظم المعلوماتية أو المعلومات نفسها ويعود ظهور الحروب السيبرانية إلى إنهيار الإتحاد السوفياتي 1991 أين بدأت المواجهات بين روسيا و أوكرانيا ولأجل هذا الغرض عملت روسيا على تطوير برمجياتها وطرق هجومها وسجلت أول هجماتها السيبرانية على أنظمة المعلومات للمؤسسات الخاصة ومؤسسات الدولة في أوكرانيا سنة 2013[3] .

[1] المرجع نفسه،ص222

[2] الحروب السيبرانية ،ويكيبديا،تاريخ الاطلاع 2022/11/05 سا 20.15
http://ar.m.wikipedia.org/wiki/d8

[3] متى ظهرت الحرب السيبرانية،ويكيبديا،تاريخ الاطلاع 2022/11/05 سا 21.45
http://ar.m.wikipedia.org/wiki/d8

2علي عبد الرحيم العبودي ،هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين ،المجلة الأكاديمية العلمية iraqui ،كلية العلوم السياسية،جامعة النهرين بغداد، المجلد 57 ،العراق،2019،ص 96

من ناحية أخرى يرتبط مفهوم الحرب السيبرانية بهجمات إلكترونية بقيادة عسكرية تقوم بإختراق الأنظمة الإلكترونية العالمية وتقوم بأعمال تضر بالأجهزة التي تستخدم الإنترنت مثل سرقة البيانات الخاصة.. وغيرها إلى الحد الذي قد يسبب وقوع حروب نووية

ومع إنتشار شبكة الإنترنت أصبحت أجهزة المخابرات الدولية لكل دولة تسعى لإستغلال هذه الشبكات في حروبها الدولية بواسطة التغلغل فيها والسيطرة عليها أو تعطيلها أو نفي البيانات أو إتلافها أو التحكم فيها لإخضاع دولة العدو ،ويعرف مصطلح حروب الفضاء الإلكتروني على أنه " الإجراءات التي تتخذها أي دولة أو منظمة أو مجموعة لاختراق أجهزة الحاسوب أو الشبكات الخاصة بدولة أخرى لغرض السيطرة عليها أو التحكم بها أو إتلافها أو تعطيلها عن العمل من خلال إرسال رسائل مكتوبة باللغة الرقمية الثنائية المكونة من رقمي 1-0[1]ويجدر القول إلى أن الحروب السيبرانية لا تلغي الحروب التقليدية البرية والبحرية والجوية. فمع نهايات القرن العشرين (20) بدأ إستخدام الإنترنت من طرف الأشخاص والدول سواء النامية أو المتقدمة و أصبح الفضاء السيبراني (الذي تصنعه المعلومات وتكنولوجيا الإتصالات) أداة من أدوات التنمية الاقتصادية و الإجتماعية ودخلت دول العالم في علاقة تأثرو تأثير بالنسبة لهذا الفضاء خصوصا بالنسبة لنقل المعلومات والبيانات و تحولت الحروب من الرغبة في تدميرالعدو إلى الرغبة في التحكم فيه والسيطرة على تصرفاته وسلوكه وعليه إنبثق مفهوم حرب المعلومات أو الحروب الإلكترونية وهي تحمل في مضمونها هذا التوجه الحديث ولأن الصراع بين الفاعلين cyberspace في الفضاء السيبراني ما هو إلا إنعكاس للمصالح المادية بين الدول والجماعات فقد أصبح الفضاء الإلكتروني مجالا مركبا مادي وغير مادي يشمل مجموعة من العناصر وهي أجهزة الكمبيوتر، أنظمة الشبكات والبرمجيات ،حوسبة المعلومات، نقل وتخزين البيانات مستخدمو كل هذه العناصر.

كل هذه العناصر صنعت خصوصيته وبالتالي خصوصية كل الأفعال التي تجري بداخله وهو ما سنتحدث عنه في الفرع الآتي من خلال تناولنا لخصائص هذا النمط من الحروب .

الفرع الثاني :خصائص الحروب السيبرانية

تتميز الحروب السيبرانية عن الحروب التقليدية ب

1-الحرب الرقمية هي حرب تقنية متطورة فباعتبار محورها هو شبكة الإنترنت بما تمتاز به من تطور مستمر و تنوع و إبتكار في وسائلها وتقنياتها كما أنها ترتبط بالمصالح الحيوية للدول

2-تتميز بالسرعة و بإمكانية المراوغة والتي تعطي المهاجم أفضلية واضحة على المدافع

3-حرب غير محددة الأهداف والتأثير إذ قد تتعدى مخاطرها ميادين القتال التقليدية لتمس أكثر المواقع السيادية والحساسة تحصينا وبعيدا عن دائرة القتال

4-فشل نماذج الردع المعروفة كون الهجمات الإلكترونية في الغالب لا تترك أثرا أو دليلا على حصولها، كما أن الدمار الذي تخلفه الحروب السيبرانية قد يتضمن التجسس والتسلل والنسف بدون أي دماء أو أنقاض فضلا على أن أطرافه غير واضحة وتداعياته خطيرة من خلال تدمير المواقع على الإنترنت وقصفها بوابل من الفيروسات ونسفها كما أن سعة هذا الفضاء قد تسمح بزيادة عدد المهاجمين وإمتداد الصراع في الزمان والمكان[1]

وبالنسبة للفاعلين بهذا الفضاء. فيمكن أن تكون..الدول والحكومات ،الشركات متعددة الجنسيات، الجماعات الإرهابية، الفرد، الجماعات الإحتجاجية المنتشرة في العالم مثل Wikileaks تعمل في السياسة وهي جماعات تنتمي لمنظمات غير حكومية وتقوم بنشر ملفات سرية عن الحكومات تحتوي معلومات حساسة ومهمة بدون ذكر هوية Anonymous

[1] المرجع نفسه،ص99 ،100

وهم مجموعة مخترقين غير معروفي الهوية يدعون أنهم مجموعة دولية من كل دول العالم وقد قاموا بعدة هجمات ضد مواقع حساسة و أمنية للدول والحكومات مثل إختراقهم لمواقع الشرطة الأمريكية وتهديدها بفضح ملفات سرية[1]

وعليه فإن خصوصية هذه الحروب تتصل بخصوصية الفضاء السيبراني من سرعة وسهولة ولا محدودية في الإنتشار، فضلا على سريتها و صعوبة تتبعها أو الحصول على أدلة إثبات الأفعال المدمرة التي تخلفها وهذا الطابع غير المادي هو ما جعل التهديد أكبر وأكثر رعبا وإخلالا بالعلاقات الدولية وجعل المتحكم في هذا الفضاء هو الطرف الأقوى ولو إمتلك الآخر جيوشا قوية ،كل هذا تطلب إيجاد حلول فعالة من الدول تناسب هذا النمط من الحروب فإتجهت نحو تكريس أمنها السيبراني كمفهوم حديث للأمن والسلم الدوليين، وهو ما سنتناوله بالشرح والتفصيل

المطلب الثاني :مفهوم الأمن السيبراني

من أجل حماية قواعد البيانات الحساسة لكل دولة سيما البيانات المتعلقة ب مؤسساتها أو حتى مواطنيها ما يشكل أمنها القومي ، عملت الدول على سن القوانين وتوفير الوسائل والتقنيات ،فضلا على التعاون في ما بينها لمكافحة كل أنواع الإختراقات التي تمس بأمنها وتدمر إقتصادها فضلا على مساسها بحقوق الإنسان بداخلها ،وعليه تعمل على تكريس أمنها داخل البيئة السيبرانية وفق ما يسمى بالأمن السيبراني ،وعليه نتناول مفهوم الأمن السيبراني و أبعاده ومن ثم الآليات التي تؤطره في إطار من التعاون الدولي لأجل الحماية .

الفرع الأول : ماهية الأمن السيبراني

يشكل الأمن السيبراني جزءا أساسيا من أي سياسة أمنية وطنية فقد أصبحت الدول تصنف مسائل الدفاع السيبراني كأولوية في سياساتها الدفاعية كما خصصت أكثر من 130 دولة أقساما خاصة بالأمن السيبراني في فرقها الأمنية الوطنية،ويقصد بالأمن السيبراني مجموع الأطر القانونية والتظيمية والهياكل التنظيمية والوسائل التكنولوجية الوطنية والدولية التي تهدف إلى حماية

[1] أكرم القصاص،من هم هاكرز الأنونيموس ولماذا تردد إسمهم في الإحتجاجات الأمريكية ،مجلة اليوم السابع، تاريخ النشر 2020/06/08 سا12: 5 تاريخ الإطلاع 2022/12/25سا 00: 16
https://www.youm7.com/story/2020/6/8/4814263/

الفضاء السيبراني الوطني كما تركز على حماية بيانات الأفراد ومؤسسات الدولة من الإستخدام غير المصرح به أو أي أذى يلحق بشبكة البيانات[1]

إذن فالأمن السيبراني له 3 جوانب

*حماية بيانات الأشخاص الإلكترونية

*ومن خلالها حماية الشركات ومؤسسات الدولة وبياناتها وعملائها

*ثم حماية الأمن القومي وسلامة المواطنين ورفاهيتهم وخصوصيتهم لألا تستخدم هذه البيانات بطرق غير شرعية أو ضد أصحابها

ويعتبر وجها لإحدى وجوه واقع العلاقات الدولية المعاصرة والتي وضعت مفهوم الأمن الوطني أو القومي كمحرك لهذه العلاقات ومعيارا للسيادة الوطنية كما أصبح هاجسا لكافة الدول إعتبارا بهدفها الأسمى في حماية سلمها و أمنها وإلتزاما بإحترامها للأمن والسلم الدوليين بالموازاة مع محاربة الجريمة الإلكترونية والإحتيال الإلكتروني وغيرها من المخاطر التي يأتي الأمن السيبراني على رأسها

ويعرف الأمن السيبراني بأنه "مجموعة من الوسائل التقنية والتكنولوجية والعمليات التي يتم إستخدامها لحماية الشبكات و الأجهزة والبرامج والبيانات ومن الهجمات أو التسلل الغير مسموح به ويعرف أيضا بأنه أمن تكنولوجيا المعلومات أو حماية المعلومات ،كما يعرف أنه "النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الإتصال كمايحد من الأضرار في حال حصول هجمات أو تهديدات سيبرانية ويعيد الوضع إلى ماكان عليه بأسرع وقت[2]

ومن أهم الأهداف التي يحققها الأمن السيبراني

*المحافظة على أمن المجتمع و إستقراره

*الحفاظ على سلامة عمل قطاعات الدولة الإلكترونية من أي إختراق

---

[1] فيصل محمد عسيري،الأمن السيبراني وحماية أمن المعلومات،تاريخ الإضافة 02-2019 ،16.51سا،ص1

Application pdf http://www.kutub.info/librairy/book.21854

[2] المرجع نفسه،ص2

*حفظ البيانات والمعلومات الإلكترونية الهامة

حماية شبكة المعلومات بأسلوب علمي وتقني محكم

*تشفير التعاملات الإلكترونية بحيث لا يستطيع أي مخترق الدخول إليها ويعتبر التشفير أحد أهم أساليب الحماية ،وعليه فإن الأمن السيبراني بجميع تفاصيله التقنية ضرورة للدفاع القومي ولحماية القطاع العسكري والسياسي والإجتماعي والأمني للدولة وهو إحدى الإستراتيجيات الحديثة التي تتطلب جهودا أكبر من أي دولة في تدريب متخصصين وتبادل خبرات وتطوير الوسائل التي تمتلكها حماية لنفسها ولحاقا بالركب الدولي والذي أصبحت فيه الدول المتقدمة هي من تملك وتتحكم في المعلومة وصارت الدول النامية هي الدول المتخلفة تكنولوجيا .

الفرع الثاني :أبعاد الأمن السيبراني

بغية تحقيق أمن قومي متكامل للدول ضد الهجمات السيبرانية يحمل مفهوم الأمن أبعادا كثيرة

أولا -البعد العسكري: أين يوفر الأمن السيبراني للقوات العسكرية التواصل وتبادل المعلومات و الأوامر عن بعد بشكل آمن مع وجوب أن يكون قادرا على صد أي محاولة إختراق تؤدي إلى تدمير البيانات العسكرية لدولة العدو، بحيث يمس الأمن القومي مثلما حدث في إيران عند إختراق منشآتها النووية[1]

ثانيا-البعد الإقتصادي: تظهر أهمية الأمن السيبراني بشكل أوسع وأكبر في المجال الإقتصادي لأن الفضاء الإلكتروني أصبح أساسا للتعاملات التجارية والمالية والإقتصادية و أصبح الحاسوب أداة لتسيير الصناعة و الإقتصاد وهذا يستدعي الحرص على تحقيقه

ثالثا-البعد الإجتماعي :يأخذ الأمن السيبراني شكلا مهما ومختلفا تماما في المجال الإجتماعي،فقد أصبحت مواقع التواصل الإجتماعي أداة إتصال عالمية بين البشر تمد بالمعلومات و الأفكار ولكن من ناحية أخرى قدعرضت أخلاق المجتمع للخطر من ناحية أنه يمس هوية الأشخاص ويهدد

[1] محمود علي عبد الرحمن،أسامة فاروق مخيمر،الفضاء الإلكتروني وأثره على مفاهيم القوة والأمن والصراع في العلاقات الدولية،مجلة كلية السياسة و الإقتصاد، جامعة محمد البشير الإبراهيمي ،برج بوعريريج، المجلد السادس عشر، العدد الخامس عشر، الجزائر ،2022،ص438

السلم الإجتماعي وعليه لابد من العمل أولا على تكريس مفهوم الأمن السيبراني ثم توعية الأفراد بمخاطر إختراقه

رابعا-البعد السياسي:قد يشكل الأمن السيبراني وسيلة حماية للمعلومات و الوثائق الأساسية الحساسة لعمل قطاعات الدولة ،وعليه لابد من تحقيقه حتى لاتخلق خلافات دبلوماسية بين الدول،وفي حالات أخطرشهدت العلاقات الدولية حروب فعلية شرسة جراء إختراق الأمن السياسي وأبرز مثال الحرب الروسية الأوكرانية2022 التي بدأت بحرب سيبرانية إنتهت بحرب فعلية مدمرة

خامسا-البعد القانوني : يمثل القانون أداة ضبط المجتمعات وهو يحمل نفس الوظيفة بالنسبة للفضاء الإلكتروني إذ لابد أن تكرس الدول تشريعات خاصة و أطر قانونية تحدد الأعمال القانونية وغير القانونية في الفضاء الإلكتروني لأن الشئ الملاحظ أن الجريمة القانونية تفتقر للصرامة في التعامل معها سيما بالنسبة للتشريعات الجنائية ،كما أصبح الأمن الإلكتروني حقا جماعيا من الحقوق الحديثة وتفرعت منه عدة حقوق كحق النفاذ إلى الشبكة العالمية للمعلومات وحق إنشاء المدونات الإلكترونية والحق في حماية البرامج المعلوماتية ويقابلها مجموع إلتزامات مثل إلتزام الإبلاغ عن مخالفات وجرائم خاصة بالمحتوى ،كل هذا يتطلب وجود قوانين تواكب هذا التطور [1]

الفرع الثالث :آليات حمايةالبيئة السيبرانية دوليا

من أجل وضع إستراتيجية أمن سيبراني يجعل الدولة في منأى عن أي تهديد أو إختراق لأنظمة معلوماتها،لابد من أطر تشريعية وتنظيمية فضلا على آليات إجرائية للحماية تتمثل أساسا في التعاون الدولي والسياسات الدولية الوقائية والدفاعية ونخصص هذا الفرع للتطرق لآلية التعاون الدولي و كذلك للبرامج العالمية المتعلقة بالأمن السيبراني نظرا لدولية الحروب السيبرانية التي تجعل الأمن السيبراني مسؤولية إتفاقية مشتركة

[1] المرجع نفسه،ص440.439

أولا –التعاون الدولي:نظرا للطبيعة الدولية للحروب السيبرانية لابدأن يكون العمل على تكريس أمن سيبراني تبادليا للخبرات بين الدول من الجانب الإجرائي والموضوعي ومن خلال عقد إتفاقيات حماية أي أن تكون القوانين موحدة أو على الأقل متقاربة وأن تكون الإجراءات القضائية والأمنية متعاونة فيما بينها فضلا على الإستفادة من التقنيات الحديثة والتي تمتلكها الدول المتطورة تكنولوجيا وتحتاجها باقي الدول،ويعتبر التعاون الدولي ضرورة حتمية في عالم اليوم لا منأى لأي دولة عنه حفاظا على سلمها وأمنها من خلال الحفاظ على السلم والأمن الدولي ، ومن أمثلة التعاون الدولي في مجال الفضاء السيبراني ما إتفقت عليه الدول في القمة العالمية لمجتمع المعلومات WSIS 2003 بين و الوطني و الدولي المستوى على فعالة آليات وضع بضرورة 2005 للنهوض بالتعاون الدولي في مجال الأمن السيبراني[1]،كذلك الإتفاقية الأوروبية لمكافحة الجريمة السبيرانية التي عددت الأفعال التي تعتبر جرائم سيبرانية مثل الجرائم ضد سرية المعلومات وتوفرها والتي قد تسبب حروبا شرسة بين الدول ،مثاله مع حصل في الحرب الروسية الأوكرانية 2021 من إختراقات لمواقع حكومية أوكرانية من طرف الروس كادت أن تشل الحياة في أوكرانيا وأججت نيران الحرب وبالمقابل واجهت أوكرانيا الأمر بمهاجمتها لمواقع خدمات روسيا هجوما واسع النطاق[2] ،وتبعا لهذا السياق وضعت الدول المتقدمة سياسات وقائية ودفاعية مثل ما قامت به الولايات المتحدة الأمريكية وأستراليا و إنجلترا بتخصيصها مبالغ كبيرة لوضع سياسات أمن سيبراني تحميها من مثل هذه النتائج ،من خلال وضع تدابير قانونية وتنظيمية وتقنية لحماية البيانات و تأمين شبكة المعلومات والإتصالات، ضف إلى ذلك العمل على نشر ثقافة الأمن السيبراني من خلال التعليم العام ووسائل النشر و الإتصال الحديثة ولاتي تعد سلاحا ذو حدين بإمكانه التوعية في المجال السيبراني بأقصى سرعة وسهولة [3].

---

[1] إسلام فوزي،الأمن السيبراني أبعاده الإجتماعية والقانونية –تحليل سوسيولوجي-المجلة الإجتماعية القومية للبحوث الإجتماعية والجنائية ،مصر،المجلد56،العدد2019،2،ص 115.114

[2] محمد دنكر، أسوأ الإختراقات الإلكترونية في 2022،تاريخ النشر 2022/09/20،تاريخ الإطلاع 2022/12/15 سا 16:00 https://www.alaraby.co.uk/entertainment_media

[3] المرجع نفسه،ص 118

ثانيا –أ-برامج الأمن السيبراني العالمية : إذ لابد من إستراتيجية مسبقة تحكم التعاون الدولي من خلال برامج مدروسة ، وقد تم وضع البرنامج العالمي لعام 2007 والذي يهدف إلى تكريس أمن مجتمع المعلومات من خلال مبادئ أساسية كالتدابير القانونية والإجرائية والتقنية والهياكل التنظيمية كمراكز الوقاية مثلا فضلا على بناء القدرات من خلال تبادل الخبرات والكفاءات والتبادل الدولي كإطار لكل هذه العمليات .

ب-إعلان إيريتشي لمبادئ السلام السيبراني 2009 والذي يدعو إلى تحليل آثار و أضرار الجرائم السيبرانية من جهة ،وتقييم الأطر القانونية المنظمة لها على المستوى الدولي ومن ثم العمل على تكريس أمن عالمي ووضع خطط حماية مستقبلية [1]

وجدير بالذكر أن من أهم الإتفاقيات الدولية التي تناولت الجريمة الإلكترونية والتي تشكل الجانب المادي للحروب السيبرانية ،نجد إتفاقية بودابست للجريمة الإلكترونية 2001/11/23 المنبثقة عن مجلس أوروبا والتي نصت على فحوى هذا النوع من الإجرام وعلى سبل مكافحته فتناولته من الجانب الموضوعي بنصها على تجريمه ثم الجانب الإجرائي لمحاربته، كما أكدت على جانب التعاون الدولي والإقليمي لتوحيد الجهود بغية مكافحة هذا النوع من الجرائم ووقف الحروب التي قد تنجر عنها[2]،

المبحث الثاني :مفهوم الحروب السيبرانية من منظور القانون الدولي الإنساني

وبالنسبة لمفهوم الحروب السيبرانية من منظور القانون الدولي الإنساني فقد حاول فقهاء القانون الدولي إستخدام أو تطبيق القواعد القابلة للتطبيق على النزاع المسلح التقليدي ومدى إستيعاب هذه القواعد لخصوصية الحروب السيبرانية خاصة بالنسبة لحماية المدنيين أي الأفراد العاديين داخل هذا الفضاء وعليه نبحث مدى إمكانية ذلك من خلال المطلبين الآتيين:

[1] المرجع نفسه ،ص 119

[2] قطاف سليمان.بوقرين عبد الحليم،الآليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل إتفاقية بودابست والتشريع الجزائري ،المجلة الأكاديمية للبحوث القانونية والسياسية ،كلية الحقوق والعلوم السياسية جامعة عمار ثليجي الأغواط،المجلد السادس ،العدد الأول،الجزائر،2022،ص 339

المطلب الأول : إرتباط الحروب السيبرانية بالقانون الدولي الإنساني

تميزت الحروب التقليدية بشراستها وأسلوبها المدمر الذي لم يراعي أي إعتبارات إنسانية أثناء النزاع إلى حين تبلور مبادئ القانون الدولي الإنساني وما جاء به من قواعد لأنسنة الحرب ،وعليه أصبحت مبادئ دولية آمرة تطبق في حال النزاع سواء كان دوليا أو غير دولي ،ولما كان كذلك فإن العمل الدولي أصبح عن إمكانية إخضاع الحروب الحديثة بما تحمله من خصوصية لقواعد هذا الأخير،وكيف يمكن ملائمة شراسة الهجمات السيبرانية والحد من مدى دمارها حماية لحقوق الإنسان بالدرجة الأولى .

الفرع الأول : إرتباط المفهوم الحديث للحرب بالقواعد الإنسانية

لما كان القانون الدولي الإنساني يعنى بالنزاع المسلح سواء كان دوليا أو غير دولي فعليه يمكن إعتبار الهجمات السيبرانية جزءا من حرب سيبرانية متى استخدمت في إطار نزاع مسلح وتحقيقا لأهداف عسكرية

وهناك عنصران جعلا تعريف الحروب السيبرانية غير محدد ولا يخضع لإجماع واسع من حيث خضوعها لقواعد القانون الدولي الإنساني

1-الهجمات السيبرانية عن طريق الإنترنت من جهة ومن جهة أخرى الهجمات على شبكات الحواسيب كظاهرة حديثة

بالنسبة لفقهاء القانون الدولي الإنساني فقد عرفوها بأنها "أعمال تقوم بها دولة وتحاول من خلالها إختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها "ريتشارد كلارك وروبرت كناكي[1]

فكيف تطبق إذن أحكام القانون الدولي الإنساني على الحروب السيبرانية عمليا بإعتبارها وجها معاصرا للنزاعات بين الدول بما يطرح التساؤل عن تأثيرها على السلم والأمن الدوليين زد على ذلك غموض المعالم الدقيقة لهذه الحرب وقد زاد توجه الدول إلى هذا النوع من الحروب نظرا لطبيعة

[1] نسيب نجيب،مرجع سابق،ص222

وسائلها وسهولة أسلحتها مثل الفيروسات وبرامج التجسس وقرصنة المعلومات العسكرية والإستراتيجية [1]كذلك حجم الدمار الذي يمكن أن يسببه للعدو في ظرف وجيز.

Marco Rochiniوقد عرفها الأستاذ

أنها "تطويع الإمكانيات الإلكترونية العسكرية لأجل التأثير في مواقع إلكترونية أخرى وتعطيلها أو تدميرها سواء أكانت تقدم خدمات مدنية أو عسكرية "

ويعتبرها آخرون "إمتداد للحروب التقليدية والمادية إذ يتألف جيشها من المدنيين والعسكريين في آن واحد كما أنها حروب أدمغة بالدرجة الأولى لأنها تستهدف بالدرجة الأولى تدمير البنية العلمية والمعلوماتية للهدف و تأخذ عدة أشغال كإضعاف شبكات الدول و الإمدادت اللوجيستية[2] وضرب المعلومات الإقتصادية والعبث بالمحتوى الرقمي والتقني وغيرها ...

أما بالنسبة للتعريف القانوني، فيعرفها بعض القانونيين بأنها «نظام قائم على الرعب المنتشر في شبكة الإنترنت والتي تهدف إلى تنفيذ العديد من الأعمال لترويع أمن الأفراد والجماعات والمؤسسات والدول و إدخالهم في أزمات نفسية و إقتصادية وسياسية و إجتماعية كما تعرف من هذا المنظور القانوني- بالإرهاب الصامت -وقد عرفها خبراء حلف الناتو بأنها"كل العمليات السيبرانية سواء دفاعية أو هجومية والتي قد تسبب إصابات أو وفيات للبشر أو تلف أو ضرر للأشياء المادية "وهو تعريف يرتبط بمدى إرتباط أو خضوع هذه الهجمات أو الحروب لقواعد القانون الدولي الإنساني[3]

مما سبق من تعاريف نرى أن هذه الحروب رغم إستعمالها للوسائل التكنولوجية الحديثة إلا أنها تستهدف البشرمن خلال تأثير الدمار الذي تخلفه على حياتهم في أقسى حالاتها أو على باقي حقوقهم كحقهم في العيش الكريم أو حقهم في العمل أو حقهم في التملك و التنقل فضلا على أنها

[1] المرجع نفسه،ص220

[2] نعني بكلمة اللوجيستية في مجال الخدمات الموارد المادية مثل الأغذية والمعدات وكذا المعلومات أما في العلوم العسكرية فتعني الحفاظ على خطوط الإمداد للجيش مع تعطيل خطوط العدو ويدير موظفوا اللوجستيات كيفية ومكان نقل الموارد إلى الأماكن التي يحتاجون إليها. الدعم اللوجستي، ويكيبيديا ،تاريخ النشر 2023/01/02 سا 16:00 تاريخ الإطلاع 2023/03/30 https://ar.wikipedia.org/wiki/%D8%A7

[3] نسيب نجيب،مرجع سابق،ص223

تمس بمصالح المدنيين الذين ليس لهم دخل في الصراع الإلكتروني بين دولتين أو عدة دول مما يستدعي حمايتهم وفق القواعد الإنسانية التي يكرسها القانون الدولي الإنساني.

الفرع الثاني :الحروب السيبرانية ومبدأ الإمتثال للقواعد الإنسانية

إضافة إلى حروب الفضاء الإلكتروني أنتجت التكنولوجيا الحديثة وسائل جديدة مثل الطائرات بدون طيار والأسلحة ذات نظام التشغيل الذاتي مما أثار إشكالا في ما يخص مدى إمتثال هذه الوسائل لقواعد القاون الدولي الإنساني

و إذا ما رجعنا لنص المادة 36 من البروتوكول الأول لإتفاقية جنيف 1949 نجدها تنص على إلزام كل دولة تقتني أو تطور سلاح جديد بالتأكد إذا ما كان محظورا بموجب القانون الدولي الإنساني ،كمت نجد المادة 82 قد إستكملت ما قضت به المادة 36 بنصها على وجوب إستشارة مستشارين قانونيين لتقديم المشورة للقادة العسكريين بالنسبة لهذا الموضوع[1]

وهذا ما يوفر لأي دولة إمكانية إستعمال أسلحة جديدة دون الخروج عن إلتزاماتها الدولية في ما يخص الأمن والسلم الدوليين و إحترام القواعد الإنسانية الدولية ،ورغم ما يعتري الحروب السيبرانية من غموض خصوصا بالنسبة لصعوبة التفرقة بين الأهداف العسكرية والمدنية في حال هجوم أو إختراق إلكتروني إلا أنها تخضع لضوابط القانون الدولي الإنساني من ناحية خطر المساس بالمدنيين والأعيان المدنية .

ونفس الأمر بالنسبة للأسلحة ذات التشغيل الذاتي والتي تعمل في الجو والبر والبحر، فالتحدي يكون أكبر في ما إذا كانت هذه الأسلحة تستطيع التميز بين المقاتلين و المدنيين و الأعيان المدنية عند القتال و إذا ماكانت تستطيع التحلي بقواعد التميز والتناسب والإحتياط في الهجوم وهي قواعد يكرسها القانون الدولي الإنساني وتخضع لأحكام البشر ورقابتهم ،الأمر الذي يجعل هذه التكنولوجيا بعيد عن الإمتثال التام لقواعدالقانون الدولي الإنساني كما تخضع الطائرات بدون طيار لنفس الوضع حيث أظهرت حالات كثيرة أنها أحدثت مقتل مدنيين و إصابتهم عن طريق

[1] الإتحاد البرلماني الدولي و اللجنة الدولية للصليب الأحمر 2016. القانون الدولي الإنساني ،دليل البرلمانيين 25 ص76

الخطأ والتي يخضع إمتثالها للقانون الدولي الإنساني لأمر مسيرها من البشر ،و يبقى الحل بالنسبة لهذه الوسائل راجعا لسلطات الدول الأطراف عند إستخدامها سواء بالنسبة للفضاء الإلكتروني أو الأسلحة الحربية من خلال تقييمها لمدى ملائمة الوسائل للقواعد الإنسانية [1]

المطلب الثاني :حجج المؤيدين والمعارضين لملائمة القواعد الدولية الإنسانية للحروب السيبرانية

لابد لنا من التطرق إلى الجدلية التي قامت حول مدى إنطباق قواعد القانون الدولي الإنساني على الحروب السيبرانية بما تحمله من خصوصية والتي أساسها عدم مرئية هذه الحروب من جهة وعدم تنظيمها القانوني المحكم دوليا ووطنيا مما صعب من التحكم فيها وفي مدى أضرارها

وعليه إنقسم الفقه القانوني إلى مؤيد ومعارض كل له حججه في إمكانية تطبيق القواعد الإنسانية على نزاع سيبراني معلوماتي داخل فضاء تميزه المعلومة بدل الجيوش والأسلحة ونستعرض كلا الرأيين

الفرع الأول :الرأي القائل بعدم إمكانية تطبيق القانون الدولي الإنساني على الحروب السيبرانية

تزعم هذا الإتجاه بعض السياسيين والعلماء الأمريكيين برفقة بعض فقهاء القانون الدولي والذين رفضوا إعتبار قواعد القانون الدولي الإنساني قواعد تستوعب هذه الهجمات السيبرانية والتي تشكل وجها حديثا للنزاعات الدولية وحجتهم في ذلك

أن فضاء الإنترنت هو فضاء حر لا تملك أي سلطة لأي دولة التحكم فيه كما يتعذر إخضاع هذه الحروب لقانون واحد مشترك نظرا لإشتراك جميع الدول في هذا الفضاء.

فضلا على أن قواعد القانون الدولي الإنساني لا تحمل أي تعامل أو تنظيم مباشر لهذا النوع من الهجمات لأنها لا تعتبر من ضمن النزاعات المسلحة والتي تخلف آثارا مادية كما أن الهجمات السيبرانية تطورت في وقت لاحق على وضع قواعد هذا القانون .

[1] المرجع نفسه،ص 80.81.82

فضلا على أن مصطلح حرب في حد ذاته غير دقيق "لأن الحرب ترتكز على إستخدام جيوش نظامية كما يسبقها إعلان واضح لحالة الحرب وميدان القتال بينما تعتبر الهجمات السيبرانية غير محددة المجال أو الأهداف كونها تتعدى الحدود الدولية وهذا يجعلها أقرب إلى الإرهاب الدولي من الحرب، خصوصا من ناحية إستعمالها لأسلحة معلوماتية يتم نشرها في سرية تامة وبدون سابق إنذار .

كما تتشابك الحرب السيبرانية مع الحروب الإعلامية وحرب الإتصالات والحرب السياسية والنفسية والتكنولوجية والإرهاب[1]

الفرع الثاني :الرأي القائل بإمكانية تطبيق القانون الدولي الإنساني على الحروب السيبرانية

يرى مؤيدي هذا الرأي أنه بإعتبار تنظيم القانون الدولي الإنساني لوسائل إتصال مثل الهاتف والفاكس وغيرها في حالة النزاع المسلح إذن فهي قادرة أيضا على تنظيم الهجمات السيبرانية كما يمكن تطبيق المبادئ القانونية الراسخة في القانون الدولي الإنساني على الحالات التي لا تغطيها إتفاقيات دولية خاصة مثل حالة الهجمات السيبرانية وعلى هذا الأساس فكل تصرف أو اعتداء يقع أثناء النزاع المسلح تغطيه قواعد القانون الدولي الإنساني .

وبرجوعنا للمادة 36 من البروتوكول الإضافي الأول لإتفاقية جنيف 1949 نجدها تنص على "يلتزم أي طرف سام متعاقد عند دراسة أوتطوير أو إقتناء سلاح جديد أو أداة حرب أو إتباع أسلوب حرب،بأن يتحقق ما إذا كان ذلك الفعل محظورا في جميع الأحوال أو في بعضها بمقتضى هذا الملحق أو أية قاعدة أخرى من قواعد القانون الدولي التي يلتزم بها الطرف السامي المتعاقد"[2]

إذا فعلى الدول التحقق إعتبارا بأن الهجمات السيبرانية سلاح حديث من أسلحة النزاعات الدولية من مشروعية إستخدامها وفقا لقواعد البروتوكول وهو ما يؤكد إنطباق هذه الأحكام الآمرة على الهجمات السيبرانية وقد سارت محكمة العدل الدولية على مثل هذه القواعد في مسألة مدى مشروعية التهديد بالأسلحة النووية و إستخدامها إذ أكدت في رأيها الإستشاري أن القانون الدولي

[1] نسيب نجيب ،مرجع سابق ،ص227

[2] يحي ياسين سعود، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني ،المجلة القانونية -مجلة متخصصة في الدراسات والبحوث القانونية - كلية الحقوق ،فرع الخرطوم ،جامعة القاهرة ،مجلد03،عدد04، 2018،ص90

الإنساني قد تطور ليأخذ بعين الإعتبار تغير الظروف ولا يقتصر تطبيقه على أسلحة الماضي و إنما ينطبق ذلك على الأسلحة الحديثة كذلك وبالنسبة لإعتبار الهجمات السيبرانية ليست نزاعا مسلحا وحجة القائلين بهذا أنها لاتحمل عملا عدائيا تقليديا فهذه قد أصبحت مسألة نسبية في الوقت الراهن،لأن حرب المعلومات لا تحمل معيار الفاعل فقط و إنما تحمل معيار آثار الفعل بصفة أكبر وعليه يمكن إخضاعها لقواعد القانون الدولي الإنساني مثلها مثل الحروب البيولوجية أو الكيميائية ."[1]

وعليه فإن مبادئ القانون الدولي الإنساني تنطبق أينما تمت هجمات سيبرانية على دولة بشكل مكثف فلا يمكن إعتبار أي إعتداء سيبراني أو إختراق لبيانات إلكترونية هو بمثابة أعمال عنف مسلح إذ يجب أن تهدف هذه الهجمات إلى إلحاق الأذى أو الوفاة للأفراد المدنيين أو إحداث أضرار بالبنى التحتية للدولة المستهدفة كما تظهر صعوبة تطبيق قواعد القانون الدولي الإنساني على الهجمات السيبرانية عمليا من خلال مبادئ منها :مبدأ التناسب ،مبدأ التمييز ،مبدأ الضرورة العسكرية

الخاتمة:

نخلص إلى أن حروب اليوم هي حروب التكنولوجيا و أن التسابق نحو التسلح الذي ميز العلاقات الدولية في عقود سابقة أصبح سباقا نحو الرقمية فأصبح المهاجم يستعمل سلاح المعلومة و المدافع يدافع عن أمنه بإمتلاكه للمعلومة وحمايتها، كما خلق الفضاء الإلكتروني أو السيبراني وهو الفضاء التي تتحكم فيه شبكة الإنترنت إضافة إلى الإجراءات الرقمية الحديثة وشبكات الحواسيب وأنظمةالبيانات ووسائل التواصل والإتصال ،خلق مفهوما مختلفا للنزاعات بين الدول التي أصبحت الحرب فيها تقوم من خلال

إجراءات تقوم بها الدول للهجوم على نظم المعلومات لدول أخرى بغية الإضرار بها من خلال تعطيلها أو إتلافها أو إستعمالها على وجه مضر بالأفراد أو القطاعات الحساسة للدول وهو ما

[1] نسيب نجيب،مرجع سابق،ص229

شهده الواقع الدولي في عديد النزاعات المسلحة التي استخدمت الهجمات السيبرانية وحولتها إلى حروب ،مثل حرب روسيا وأوكرانيا منذ 1991 إلى الحرب الحالية.

وهي حروب تتميز بتقنيتها التي تدور داخل فضاء رقمي فتأخذ خاصية السرعة والتطور واللامحدودية منه وكذا عدم المرئية، الأمر الذي صعب التحكم في آثارها وإتاحة أدلة لإثبات حصولها ،فضلا على عدم وضوح أطرافها

وبالمقابل أصبحت الدولة المتضررة تحاول استخدام هذا الفضاء لحماية معلوماتها وتأمينها من خلال الأمن السيبراني أي مجموع الوسائل التقنية والتكنولوجية التي يتم استخدامها لحماية الشبكات والبيانات الحساسة من التسلل والهجمات وهذا حفاظا على أمن المجتمع وقطاعات الدولة بما يحمله من أبعاد عسكرية، إقتصادية إجتماعية ، قانونية وسياسية .

ولأجل تكريسه وجب وضع آليات دولية تتمثل أساسا في التعاون الدولي وفي الإتفاقات الدولية و التشريعات الجنائية المتقاربة لأجل مكافحة هاته الحروب .

و بالنسبة لقواعد القانون الدولي الإنساني التي تحمي على وجه الخصوص المدنيين فقد نشأ جدال فقهي عن مدى إمكانية تطبيقها على الحروب السيبرانية من خلال أنسنة هذه الأخيرة وحماية الأفراد من أضرارها ومن هذا المنظور عرفها البعض على أنها أساليب هجومية ودفاعية تسبب أضرارا ووفيات للأفراد وأضرارا مادية أخرى .

الأمر الذي جعل الآراء تنقسم بين مؤيد لخضوعها للقواعد الإنسانية مبررا ذلك بعدة قواعد دولية منها المادة 36 من البروتوكول الإضافي الأول لإتفاقية جنيف 1949 ومعارض يبرر رأيه أنها حروب تطورت بعد وضع القانون الدولي الإنساني كما غاب الجانب المادي لها.

ويبرز الواقع الدولي آثارا سلبية لحروب ابتعدت كل البعد عن هذه المبادئ الإنسانية إلا في مواضع قليلة أين جعلت حماية المدنيين تؤخذ بعين الإعتبار، الأمر الذي يحتم على المجتمع الدولي اليوم نشر توضيحات للأفراد حول عدة مفاهيم تجعلها تستوعب الأمر الحاصل في هذا الفضاء وتتعامل معه بوعي أكبر من خلال :

*إدراج هذه المفاهيم الحديثة كالحرب السيبرانية، الأمن السيبراني، الجريمة الإلكترونية ،الإختراق الإلكتروني وغيرها في التعليم العام على المستوى المحلي والدولي وجعلها ثقافة سائدة بين الدول والأفراد .

* تفعيل التشريعات الجنائية الرادعة لكل محاولات الإختراق الإلكتروني ضد الدول بل وضع ترسانة قانونية جزائية تطبق على الجريمة الإلكترونية إن كان على المستوى الدولي أو الوطني.

*التوعية الإعلامية بنفس وسائل التكنولوجيا وداخل نفس الفضاء الإلكتروني والذي هو سلاح ذو حدين، وعليه وجب إستخدامه لأجل التوعية بمفهوم وبأخطار وآثار هذه الحروب الحديثة .

*إلتزام الدول بمبدأ التعاون لأجل مكافحة هذه الحروب من جهة وتكريس الأمن الضروري من جهة أخرى ويتطلب هذا الإلتزام تطبيق الإتفاقيات التي أبرمتها أو إنضمت إليها والوفاء بعهودها الدولية وعدم التخلي عن إلتزاماتها وهو من الأسباب التي أثبت الواقع الدولي أنها أخلت بالأمن والسلم الدوليين .

* تطوير قواعد القانون الدولي الإنساني من خلال عقد الإتفاقيات الدولية إلى مستوى يستوعب مثل هذه الجرائم من نقطة البداية ويضبط جميع مراحل هذه الحروب ،كما يلائم خصوصيتها كي لا تخلف دمارا دوليا تتعدى نتائجه ما خلفته الحروب التقليدية بإعتباره دمارا قادرا على شل جميع القطاعات الحساسة في العالم أجمع وفي نفس اللحظة وبنفس السرعة إذا لم تردعه الضوابط القانونية وهي وظيفة القانون الدولي الإنساني.

قائمة المصادروالمراجع:

المقالات

1*إسلام فوزي،الأمن السيبراني أبعاده الإجتماعية والقانونية –تحليل سوسيولوجي-المجلة الإجتماعية القومية للبحوث الإجتماعية والجنائية،مصر،المجلد56،العدد 2 ،2019

2*علي عبد الرحيم العبودي ،هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين ،المجلة الأكاديمية ،كلية العلوم السياسية،جامعة النهرين بغداد ،مجلد 57 ،العراق،2019 iraqiالعلمية

3*قطاف سليمان.بوقرين عبد الحليم،الآليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل إتفاقية بودابست والتشريع الجزائري ،المجلة الأكاديمية للبحوث القانونية والسياسية ،كلية الحقوق والعلوم السياسية جامعة عمار ثليجي الأغواط،المجلد السادس ،العدد الأول،الجزائر،2022

4* محمود علي عبد الرحمن،اسامة فاروق مخيمر،الفضاء الإلكتروني وأثره على مفاهيم القوة والأمن والصراع في العلاقات الدولية،مجلة كلية السياسة و الإقتصاد، ،جامعة برج بوعريريج،الجزائر،ا لمجلد السادس عشر.العدد الخامس عشر،جوان 2022

5*نسيب نجيم،الحرب السيبرانية من منظور القانون الدولي الإنساني ،المجلة النقدية للقانون والعلوم السياسية كلية الحقوق والعلوم السياسية ،جامعة تيزي وزو ،مجلد19 .عدد04، 2021

6*يحي ياسين سعود،الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني ،المجلة القانونية (مجلة متخصصة في الدراسات والبحوث القانونية) ،كلية الحقوق ،فرع الخرطوم ،جامعة القاهرة ،مجلد03،عدد04 2018

التقارير

الإتحاد البرلماني الدولي و اللجنة الدولية للصليب الأحمر،القانون الدولي الإنساني،دليل البرلمانيين25، 2016.

المو اقع الإلكترونية

1*الحروب السيبرانية ،ويكيبديا،تاريخ الاطلاع 2022/11/05 سا 20.15

http://ar.m.wikipedia.org/wiki/d8

2*متى ظهرت الحرب السيبرانية،ويكيبديا،تاريخ الاطلاع 2022/11/05 سا 21.45 http://ar.m.wikipedia.org/wiki/d8

3*أكرم القصاص، من هم هاكرز أنونيمس ولماذا ترددإسمهم في الإحتجاجات الأمريكية 2020/06/08 سا 5:12 تاريخ الإطلاع 2022/12/25 سا 16:00.

https://www.youm7.com/story/2020/6/8

النشر28/08/2019،تاريخ الإطلاع 2022/11/04 الموسوعة السياسية 4* فارس قرة،الأمن السيبراني،تاريخ

http://political-encyclopedia.org/dectionary

5*فيصل محمد عسيري،الأمن السيبراني وحماية أمن المعلومات،تاريخ الإضافة 02-2019 ،16.51سا

Application pdf http://www.kutub.info/librairy/book.21854

6*محمد سعد محمود ،الحرب السيبرانية أدواتها وقودها خسائرها تاريخ الاطلاع :2022/11/01سا 20.10

Noor-book.com2020

2*محمد دنكر، أسوأ الإختراقات الإلكترونية في 2022،تاريخ النشر 2022/09/20،تاريخ الإطلاع 2022/12/15 سا 16:00 https://www.alaraby.co.uk/entertainment_media