الآليات القانونية الدولية لمواجهة الحروب السيبرانية

أ.م.د صباح فياض طلاس

كلية القانون/جامعة المثنى

sabah_fath@mu.edu.iq

الملخص

لقد أضحى الفضاء السيبراني ساحة جديدة للصراعات الدولية حيث برزت الحرب السيبرانية كظاهرة معقدة ومتطورة، تشكل تحديًا كبيرًا للقانون الدولي التقليدي. وقد كشف هذا البحث عن الطبيعة الفريدة للحرب السيبرانية، التي تتميز بالسرعة، والغموض، وصعوبة إسناد الهجمات، وتأثيراتها الواسعة التي قد تتجاوز الأهداف العسكرية لتطال البنى التحتية المدنية الحيوية. وقد تبين أن الآليات القانونية الدولية الحالية على الرغم من محاولات تكييفها لا تزال تواجه صعوبات جمة في توفير إطار شامل وملزم ينظم هذه الظاهرة بفعالية, كما وان غياب توافق دولي حول تعريف واضح للحرب السيبرانية وتحديد قواعد الاشتباك وبيان اليات الرد المشروع يترك فراغ قانوني تستغله الجهات الفاعلة في الفضاء السيبراني, فهو يضعف القدرة على ردع الهجمات السيبرانية والتصدي لها. لذا فإن الحاجة ماسة لتطوير اطار قانوني دولي جديد يأخذ في الاعتبار الخصائص المميزة للفضاء السيبراني ويضمن حماية الأمن والسلم الدوليين مع الحفاظ على المبادئ الأساسية للقانون الدولي الإنساني.

لكلمات المفتاحية : (الحرب السيبرانية, الهجمات السيبيرانية . الآليات القانونية. الفضاء السيبراني , المواجهة, الحرب التكنولوجية , الأسس العامة).

Abstract

Cyberspace has become a new arena for international conflicts, with cyber warfare emerging as a sophisticated and multifaceted phenomenon, independent of traditional international law. This research reveals the historical nature of cyber warfare, characterized by its speed, opacity, and the difficulty of assigning responsibility. It inevitably puts immense pressure on the capabilities of vital human structures. Cyber warfare challenges existing international law, despite its adaptation to the significant challenges of providing a comprehensive and binding framework to address this phenomenon. Furthermore, the lack of an Albertani consensus on a clear definition of cyber warfare, the absence of defined requirements, and the lack of legitimate response mechanisms—legal documents exploited by cyber warfare consultants—weakens the ability to deter and counter cyber aggression. Therefore, there is a pressing need for a new, more inclusive legal framework that considers the unique

characteristics of cyberspace and ensures the protection of security and peace, with a fundamentally simplified international design .

Keywords: Cyber warfare, cyber attacks, legal mechanisms, cyberspace, confrontation, technological warfare, general principles

المقدمة

يعد العصر الحديث عصر التكنولوجيا التي سيطرت على جميع مفاصل الحياة، ففي السنوات الأخيرة برزت أهمية التكنولوجيا, فالعلاقة بين التطور والتكنولوجيا علاقة طردية، أي بمعنى كلما ازداد التطور في العلاقات الدولية والتعاون الدولي برزت الأهمية لتحقيق هذا التعاون بشتى الطرق ومن ضمنها الفضاء الالكتروني، وفي ظل هذه الثورة الهائلة لتكنولوجيا المعلومات والاتصال، زادت معها المخاطر السيبرانية التي تؤدي بالنتيجة الى الحروب السيبرانية، فالحرب السيبرانية كما هو معلوم مصطلح حديث يقف عائقاً أمام الامن السيبراني (التكنولوجي) المعني بحماية الأنظمة والشبكات والبرامج والأجهزة والبيانات من الهجمات السيبرانية . ويهدف الامن السيبراني إلى حماية المعلومات الحساسة من الوصول غير المصرح به، ومنع تعطيل العمليات التجارية، والتخفيف من المخاطر المرتبطة بالتهديدات السيبرانية. فالحروب التي تجري في الفضاء الالكتروني تسمى الحروب أو الهجمات السيبرانية، والتي من شانها ان تؤدي الى تدمير البنية التحتية الرقمية للبلد سواء كان هذا التدمير بشكل كلي أو جزئي، وتؤدي الى شلل العلاقات الدولية في كافة الميادين وعلى جميع الأصعدة، فالتطور التكنولوجي الذي أصاب الحياة بجميع مفاصلها لا يقتصر على جانب دون اخر وإنما شمل جميع جوانبها مدنية كانت أم عسكرية.

أولا : أهمية موضوع البحث

تبرز أهمية هذه الدراسة – الاليات القانونية الدولية لمواجهة الحرب السيبرانية - من خلال الوقوف على مفهوم الحرب السيبرانية التي ظهرت في المجتمع الدولي الحديث، لما تتمتع به من خصائص وطبيعة قانونية تختلف عن غيرها من الحروب والجرائم التقليدية الأخرى، وكذلك معرفة الاليات القانونية الدولية لمواجهة هذا النوع من الحروب والوقوف على تقنياتها واساليبها وبيان التحديات التي تواجه المجتمع الدولي في تنظيم القواعد القانونية الدولية التي تعالجها، فالفضاء الالكتروني الدولي يشكل ميدانا لهذه الظاهرة الخطيرة.

ثانيا : منهجية البحث

هذا وقد تم اعتماد اسلوب المنهج التحليلي والوصفي في هذه الدراسة - الاليات القانونية الدولية لمواجهة الحروب السيبرانية - كونه الاسلوب الذي يتوفق مع طبيعتها والتي تتطلب تحليلاً منطقياً ووصفاً موضوعياً لمعالجة هذه الظاهرة الخطيرة وصولاً الى تحقيق غايتها الاساسية في تعزيز الامن السيبراني .

ثالثا: إشكالية البحث

قد برزت ظاهرة الحرب السيبرانية كتهديد متزايد للأمن القومي والدولي وان هذه الحروب التي تتميز بطبيعتها غير التقليدية وسرعتها وصعوبة تحديد الفاعل وتأثيرها الواسع الذي قد يتجاوز الأهداف العسكرية لتشمل البنى التحتية المدنية الحيوية ان هذا النوع من الحروب يطرح تحديات قانونية أمام المجتمع الدولي فعلى الرغم من وجود محاولات لتكييف قواعد القانون الدولي الإنساني التقليدية إلا أن غياب إطار قانوني دولي ملزم وشامل ينظم هذه الظاهرة ويحدد المسؤوليات ويضع اليات واضحة للرد المشروع، يخلق فراغا قانونيا يؤدي إلى تعقيد الواقع ويزيد من صعوبة التصدي لهذه التهديدات بفعالية وبناء على ذلك تتجلى مشكلة البحث في التساؤل حول مدى كفاية الاليات القانونية الدولية الحالية في مواجهة تحديات الحرب السيبرانية المتنامية؟ وما هي السبل الكفيلة بتطوير إطار قانوني فعال يضمن الأمن والاستقرار في الفضاء السيبراني؟

رابعا : هيكلية البحث

وعليه سوف نقسم هذه الدراسة الى مبحثين تناول في **المبحث الأول**، مفهوم الحرب السيبرانية والذي ينقسم بدورة على مطلبين، نتناول في المطلب الأول مفهوم الحرب السيبرانية وخصائصها، وفي المطلب الثاني سنتطرق فيه الى ذاتية الحرب السيبرانية وصورها. أما **المبحث الثاني** فنخصصه لبيان الأساس القانوني الدولي لمواجهة الحرب السيبرانية والتحديات التي تواجه تنظيمها، وسنقسمه ايضاً على مطلبين: الأول نبحث فيه الأساس القانوني الدولي لمواجهة الحرب السيبرانية ، وفي الثاني نذكر التحديات التي تواجه تنظيم الحرب السيبرانية وتطبيقاتها .

المبحث الأول

مفهوم الحرب السيبرانية

شهد العالم في العقد الأخير تطور تكنولوجي هائل، ومعه برزت تحديات أمنية غير مسبوقة، لعل أبرزها ظاهرة الحرب السيبرانية التي تستخدم التكنولوجيا الرقمية لشن هجمات على الأنظمة والشبكات الحاسوبية حيث أصبحت تشكل تهديدًا حقيقيا للأمن القومي والدولي، نظرا لقدرتها على إحداث أضرار جسيمة للبنى التحتية الحيوية وتعطيل الخدمات الأساسية. حيث يهدف هذا المبحث في المطلب الأول منه إلى استكشاف مفهوم الحرب السيبرانية، وخصائصها اما في المطلب الثاني منه تناولنا أنواع ذاتية الحرب السيبرانية وصورها.

المطلب الأول

تعريف الحرب السيبرانية وخصائصها

بما أن الحرب السيبرانية هي حرب غير تقليدية تستخدم التكنولوجيا لتنفيذ هجمات على الانظمة الحاسوبية والشبكات, وتهدف الى تدمير البنية التحتية الرقمية للعدو فإن التعرف على مضمونها وخصائصها يتطلب منا تقسيم هذا المطلب على فرعين، نتناول في الفرع الأول تعريف الحرب السيبرانية، وفي الفرع الثاني سنتطرق من خلاله الى خصائص الحرب السيبرانية.

الفرع الأول

تعريف الحرب السيبرانية

الحرب السيبرانية : يعبر عنها عادة بالحرب الالكترونية عبر الانترنت وهي أجراء عسكري يتضمن استخدام الطاقة الكهرومغناطيسية للتحكم في المجال الذي يتميز باستخدام الالكترونيات والطيف الكهرومغناطيسي لاستخدام بيانات التبادل عبر الانظمة الشبكية والبنى التحتية المرتبطة بها. وقد عرفها بعض الفقهاء بأنها: (أجراء أو تصرف تقوم بها الدولة وتعتبره نوع من انواع الهجوم على نظم المعلومات التابعة للعدو والتي من شأن هذا الأجراء أو التصرف أن يلحق أضراراً ينتج عنها أثار سلبية يمكن أن تساهم في تحقيق خطط واستراتيجيات عامة للحروب السيبرانية من شانها أن تلحق اضرارا تصيب العدو قدر الامكان)[1].

عرفها فيورتس(fuertes) بـأنها: "هجوم عبر الأنترنت يقوم على التسلل لمواقع إلكترونية غير مرخص بالدخول إليها؛ لتعطيل أو اتلاف البيانات المتوفرة في هذه المواقع أو الاستحواذ عليها، وعادة ما تكون هجمات إلكترونية تقوم بها دولة ضد أخرى"[2]. وعرفتها اللجنة الدولية للصليب الأحمر بأنها: " الأفعال التي يتخذها أطراف نزاع ما لتحقيق ميزة على خصومهم في الفضاء السيبراني باستخدام أدوات تقنية مختلفة، مثل اتلاف المعلومات أو التجسس السيبراني"[3].

والهجمات السيبرانية يمكن أن تكون جزءاً من حرب سيبرانية متى ما استخدمت في اطار نزاع مسلح واستهدفت تحقيق اهداف عسكرية ومن ثم فهي إجراءات تتخذها الأطراف في نزاع مسلح لكسب الميزة على خصومهم في الفضاء السيبراني باستخدام مختلف الادوات التكنولوجية والاشخاص التقنيين ويحصل على مزايا من جراء تلك الهجمات من خلال اتلاف أو تدمير أو تعطيل أو اغتصاب أنظمة الحاسوب للعدو أو من خلال الحصول على المعلومات الت يرغب العدو في أن تبقى سرية أو ما يعرف بالتجسس السيبراني أو الاستغلال لشبكات الحاسوب متى ما كانت في أطار نزاع مسلح يصل إلى مستوى الحرب[4].

يتضح لنا مما سبق أن هناك تنوع في الأدوات والوسائل واشكال الهجمات والحروب السيبرانية بما في ذلك بث الفيروسات والبرامج التخريبية والمدمرة للأنظمة والشبكات الحاسوبية أو اختراق حسابات والوصول إلى معلومات سية وتسريبها أو الاستفادة منها لأغراض عسكرية وأمنية عدائية.

---

(1) احمد حميدي علي, الحرب في الاسلام والقانون الدولي الإنساني, المكتبة الازهرية للتراث, القاهرة, 2020, ص42. كذلك خالد وليد محمود, الهجمات عبر الانترنت – ساحة الصراع الالكتروني الجديدة- سلسلة دراسات ودراسة السياسات, المركز العربي للأبحاث, قطر, 2013, ص57.

(2)عبد الله صادق دحلان ، الامن السيبراني علم ينبغي ان يدرس ، تقرير متاح على الموقع الإلكتروني لقناة العربية : https://share.google/flz3fBpJFTezfUT4e .

(3) هربت لين، النزاع السيبراني والقانون الدولي الانساني، مجلة اللجنة الدولية للصليب الاحمر، مجلد 94 , العدد 886, 2012, ص515.

(4) عادل عبد الرزاق, الارهاب الالكتروني- القوة في العلاقات الدولية- نمط جديد وتحديات مختلفة, مركز الدراسات السياسية والاستراتيجية بالأهرام, القاهرة, 2009,ص87.

وعلى ضوء ما تقدم يمكن تعريف الحرب السيبرانية على أنها: (هجمات الكترونية تقوم بها أجهزة حكومية رسمية, ضد أجهزة حكومية رسمية في دولة معادية, وهي جزء من الحرب الشاملة, تهدف الى الحاق خسائر بالنظام المعلوماتي للعدو بحيث يتم الحصول على المعلومات المخزنة, أو حرمان العدو من استخدامه, او تحويله إلى نظام يهاجم العدو بحيث يتحول إلى نظام تخريب ذاتي, وهو ما يتحقق نتيجة لتعطيل النظام وافتقاد العدو سلطة التحكم به, وذلك عن طريق الاختراق أو بث الفيروسات الالكترونية, والتي تحول النظام الرقمي من نظام مساعد إلى نظام معادٍ).

الفرع الثاني

خصائص الحرب السيبرانية

الحرب السيبرانية مصطلح مغاير للحرب التقليدية يراد به أي هجوم يحدث في الفضاء الالكتروني ويكون له طابع دولي, وتتميز عن الحرب التقليدية التي تكون على أرض الواقع سواء كانت بين دولتين او اكثر، والتي تستخدم فيها الدول جيوش نظامية، ويسبقها غالباً تصريح بإعلان الحرب، بينما الحرب السيبرانية مجالها الفضاء الالكتروني، وهي غالباً ما تكون حرب غامضة لا يفهم ما يراد منها ولا غاياتها او أهدافها، إضافة الى اعتمادها على الأسلحة الالكترونية التي تتلاءم والسباق الالكتروني الذي يعيشه العالم .

وعليه وبالاستناد على ما تقدم من مضامين وتعريفات للحرب السيبرانية تتضح أن هناك خصائص [1] لها تميزها عن الحروب التقليدية يمكن أجمالها بما يلي:

1- تعد الحرب السيبرانية حرب تقنية وذلك لان محورها هو الانترنت ومجالها الفضاء الالكتروني ، وهذا النوع من الحروب يتميز بتطوره المستمر، كما انها تشكل اعتداء على المصالح الأساسية التي تسعى الدول لحمايتها.

2- تتميز الحرب السيبرانية بالسرعة والخفاء والخداع فهي تعطي الطرف الذي يبدأ الهجوم افضلية على الطرف الاخر الذي يدافع.

3- تتميز الحرب السيبرانية بأن أهدافها تكون غير محدده وكذلك فأن آثارها قد تتجاوز المدى المحدد، اذ قد يتجاوز تأثير الحرب السيبرانية ميادين القتال التقليدية، وهي بذلك تمس مواقع ومراكز حساسة وبعيدة عن ميادين القتال.

4- تعتمد الحرب السيبرانية بالدرجة الأولى على البرامج والأجهزة، وقد يتم الاعتماد او اللجوء اليها، بسبب انخفاض تكاليف المواجهة اذا ما قارنا ذلك مع تكاليف الحروب التقليدية التي تجري على ارض الواقع،

([1]) صلاح حيدر عبد الواحد، حروب الفضاء الالكتروني (دراسة في مفهومها وخصائصها وسبل مواجهتها)، رسالة ماجستير ، جامعة الشرق الأوسط ، كلية الآداب والعلوم ، 2021 ، ص 40-47 .

فحروب الفضاء الالكتروني لا تحتاج الى تجهيزات وجيوش، كما انها لا تتسبب في وقوع ضحايا بشرية فهي تقوم على مبدأ (الحاق اكبر ضرر ممكن بأقل تكلفه ممكنه)[1] .

5- تتميز الحرب السيبرانية بأنها لا تقتصر على الهدف العسكري فهي قد تستهدف البنية التحتية المدنية إضافة الى العسكرية للدولة المستهدفة.

يتضح لنا مما تقدم من خصائص للحرب السيبرانية انها تعد نوع أساسي من أنواع الحروب في العالم المعاصر وذلك بفعل الثورة الصناعية والتحول الرقمي وتطور الأسلحة والروبوتات، فهي ليس لها حدود مكانية او زمانية وليس من اليسير فيها اكتشاف مصدر الهجمات السيبرانية، كما ان الحرب السيبرانية لا يراعى فيها القواعد والتكتيك السائد في الحروب التقليدية التي تخضع الى مجال واثر محدد بشكل شبة يقيني، فالحرب التقليدية قائمة على أساس التنقل والحركة والتكتيك الميداني، وهذا نقيض ما عليه الحرب السيبرانية.

المطلب الثاني

ذاتية الحرب السيبرانية وصورها

تعد الحرب السيبرانية صراعاً يدار في الفضاء الرقمي بين الدول أو الجهات الفاعلة، وتكمن ذاتيتها في تميزها عن غيرها من الأنشطة العدائية كالجرائم السيبرانية التي يقف خلفها أفراد بدوافع مادية، وعن الإرهاب السيبراني الذي يسعى لبث الرعب، وكذلك عن التجسس الذي يهدف لسرقة المعلومات بهدوء. بينما تنحصر صورها الرئيسية في الشقين الهجومي والدفاعي؛ فالهجومي يستهدف اختراق أنظمة الخصم وتعطيلها، بينما يركز الدفاعي على حماية البنية المعلوماتية والتصدي للتهديدات.

وعليه سوف نقسم هذا المطلب على فرعين , نتناول في الاول ذاتية الحرب السيبرانية أما الثاني فسنتطرق فيه إلى صور الحرب السيبرانية

الفرع الأول

ذاتية الحرب السيبرانية

بعد بيان مفهوم الحرب السيبرانية والوقوف على الخصائص التي تميزها عن الحرب التقليدية يقتضي بنا الوقوف على ذاتيتها . وذلك من خلال تمييزها عن بعض المصطلحات التي تتشابه معها : مثل الهجمات السيبرانية، والجريمة السيبرانية، والتجسس السيبراني، والإرهاب السيبراني. ذلك أن الحرب السيبرانية تشكل تحدياً قانونياً يتمثل في آلية معالجة هذه الظاهرة الخطيرة، وهو ما سنبحثه في هذا الفرع تباعاً:

اولاً : تمييز الحرب السيبرانية عن الهجمات السيبرانية .

---

(1) محمد اكرم محسن , أ.م.د. مروان سالم علي , السيبرانية "الماهية ,الخصائص, الفواعل ,الابعاد الاستراتيجية" , جامعة الموصل , كلية العلوم السياسية , مجلة حمورابي للدراسات , العدد 43 , السنه الحادية عشرة , 2022 , ص 392_393.

بادئ ذي بدء ان الحرب السيبرانية وان كانت تتشابه مع الهجمات السيبرانية في الكثير من الوجوه الا ان هذا لا يعني عدم وجود ما تتميز به الحرب السيبرانية عن الهجمات السيبرانية ، فالحرب السيبرانية ماهي الا مجموعة من العمليات التي تحصل في نزاع مسلح والتي يتخلف عنها اثار مادية تشبه الى حد كبير الاثار التي تخلفها الهجمات المسلحة بصورتها التقليدية، أما الهجمات السيبرانية هي كل فعل او نشاط سيبراني يضر بمصالح الدول الأخرى يقع في وقت السلم سواء نتج عنه أضرار مادية جسيمة او لم ينتج عنه. مادام كان هذا النشاط مرتكب لأغراض عسكرية او احداث خلل أو تشويش انظمة الكمبيوتر في عمل حكومة تلك الدولة[1].

ومن ثم فالهجمات السيبرانية هي الاداة او الفعل المستخدم بينما الحرب السيبرانية هي السياق الاوسع الذي يحدث فيه هذا الفعل والتي تتضمن سلسة من الهجمات المنسقة ضمن استراتيجية صراع شاملة, وتشن لأسباب سياسية أو عسكرية بحتة. فكل حرب سيبرانية تتضمن هجمات سيبرانية ولكن ليس كل هجوم سيبراني هو حرب سيبرانية.

ثانياً : تمييز الحرب السيبرانية عن الجرائم السيبرانية .

الجرائم السيبرانية ترتكب عادة من قبل افراد أو جماعات إجرامية بهدف تحقيق مكاسب مالية أو شخصية وتعرف الجريمة السيبرانية بانها (فعل غير مشروع يمس حق أو مصلحة تتعلق بالمكونات المادية وغير المادية للوسائل السيبرانية. ويكون المشرع قد نص على حمايتها بان الاعتداء عليها جريمة معاقب عليها)[2].

أما الحرب السيبرانية تشنها دول أو جماعات مدعومة من دول بهدف تحقيق اهداف جيوسياسية أو استراتيجية وتتشابه الجريمة السيبرانية مع الحرب السيبرانية في ان الاثنين يحصلان في نفس المجال او البيئة الا وهي الفضاء الالكتروني ، الا ان ما يميز الحرب عن الجريمة هو ان الجريمة عبارة عن تصرف يصدر عن جهة لا تمثل الدولة ولا مؤسساتها الرسمية، سواء كانت هذه الجهة شخص طبيعي او اعتباري، كما تتميز الجريمة السيبرانية عن الحرب السيبرانية من حيث هدف كل منهما ، فالجريمة السيبرانية يكون هدفها تحقيق ربح مالي من خلال خرق شبكات الدولة العامة او الخاصة ، وذلك على العكس من هدف الحرب السيبرانية التي ترمي الى خرق الشبكات التي تتحكم في البنية الأساسية في الدولة وتدميرها لتحقيق اهداف عسكرية او امنية او قومية [3]،

وعليه يمكن القول أن الضرر الذي تسعى الى تحقيقه الحرب السيبرانية يكون عام شامل، بينما ينحصر ضرر الجرائم السيبرانية على مستخدمين معينين، أضف إلى ذلك ان القواعد التي تنظم الحرب السيبرانية هي

---

(1) Clarke, Richard A., and Knake, Robert K. Cyber War: The Next Threat to National Security and What to Do About It. 2nd ed., HarperCollins, New York, 2010, p. 6 .

(2) Schmitt, Michael N. (ed.). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, Cambridge, 2017, p. 375.

(3) Brenner, Susan W. "At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare." Journal of Criminal Law and Criminology, vol. 97, no. 2, 2007, p. 382.

قواعد القانون الدولي العام (قوانين النزاعات المسلحة أو ما تسمى بقوانين الحرب) وتخضع الحرب السيبرانية لمبادئ القانون الدولي الانساني (مبدأ التمييز ومبدأ التناسب) بينما القواعد التي تنظم الجرائم السيبرانية هي قواعد القانون الجنائي المحلية والدولية الخاصة بمكافحة الجريمة .

ثالثاً : تمييز الحرب السيبرانية عن الإرهاب السيبراني .

يعرف الإرهاب السيبراني بانة " استخدام شبكات المعلومات والكمبيوتر من قبل المجموعات الإرهابية من اجل نشر الخوف والرعب بين الناس والدول والشعوب من اجل الضغط عليها للرضوخ لأهداف تلك الجماعات ومن ثم فهو إلى بث الرعب والخوف بين المدنيين والتأثير على حكومة أو جمهور لتحقيق اهداف ايديولوجية أو دنية أو سياسية, "[1].

ومن ثم فإن الإرهاب السيبراني يمثل شكلا من اشكال العمليات الإرهابية. أما الحرب السيبرانية فتهدف إلى أضعاف القدرة العسكرية والاقتصادية للخصم. هذا وتتشابه الحرب السيبرانية مع الإرهاب السيبراني في أن الاثنين يستخدمان الفضاء السيبراني لإلحاق الضرر سواء بحكومة دولة من الدول أو بقطاع من قطاعات هذه الدول .

رابعاً : تمييز الحرب السيبرانية عن التجسس السيبراني .

أن الهدف من وراء التجسس السيبراني هو جمع المعلومات أياً كانت هذه المعلومات سواء كانت معلومات حكومية او خاصة، وهو عموما يعني سرقة الاسرار التجارية وكذلك الملكية الفكرية والمعلومات الحكومية السرية، وبما ان التجسس الفكري بمعناة العام ينطوي على جمع المعلومات فهو غالباً لا يتسبب بأضرار مادية ، وكذلك يكون من الممكن القيام بالتجسس السيبراني سواء من قبل فرد واحد او مجموعة من الافراد، يهدف الى تحقيق ربح او مكسب مالي او ميزه عسكرية، وغالباً والتجسس السيبراني لا تنطبق علية قواعد القانون الدولي ويرجع ذلك الى أن اعمال التجسس السيبراني بحاجة الى استجابة قانونية جنائية سواء كانت محلية او دولية"[2]، ومن الجدير بالذكر أن القانون الدولي لا يتطرق الى التجسس بحد ذاته ولا يتم التعامل معه كمسألة من مسائل القانون الدولي العام الا اذا انتهك التجسس جوانب قانونية محظورة دولياً على سبيل المثال التجسس السيبراني الذي يمس الاتصالات الدبلوماسية [3] .

الفرع الثاني

([1]) Denning, Dorothy E. "Cyber Conflict and Cyber Terrorism." The Routledge Handbook of Terrorism Research, edited by Andrew Silke, Routledge, London, 2010, p. 392 .

([2]) , Libicki, Martin C. Cyberdeterrence and Cyberwar. RAND Corporation, Santa Monica, 2009, p. 38.

([3]) د. زياد محمد جفال ، عمر احمد السعيد ، مدى اعتبار الهجمات السيبرانية انتهاكاً للحظر المفروض على استخدام القوة او التهديد بها في ضوء احكام القانون الدولي للجوء للحرب ، مجلة جامعة الامارات للبحوث القانونية ، كلية القانون ، جامعة العين – الامارات ، 2024 ، ص15-20 .

صور الحرب السيبرانية

ان الحروب السيبرانية تتعدد أنواعها وصورها تبعا للأثار والاهداف التي تسعى الى تحقيقها , الا انها لا تخرج عن صورتين رئيسيين وهما كالاتي:

أولا: الحرب السيبرانية الهجومية:

يقصد بها استخدام الوسائل والتقنيات الرقمية بقصد اختراق الأنظمة المعلوماتية للدول او تعطيلها او افساد البيانات والمعلومات المخزنة فيها , وهذا يؤدي الى الاضرار بالبنية التحتية المعلوماتية للدول الأخرى او التشكيك في دقه المعلومات المتداولة , ومن ابرز صورها عمليات التنصت الالكتروني , والقرصنة الالكترونية , والهجمات الإرهابية عبر الفضاء السيبراني, واستهداف أنظمة الاتصالات والمواصلات والانترنيت , فضلا عن استهداف المواقع النووية والسدود المائية وغيرها [1]. كما وتعتمد هذه العمليات سابقه الذكر على مجموعه من الأدوات التقنية ومن بينها الفيروسات الإلكترونية بمختلف أنواعها, مثل :(Back Doors, Logic Doors) المستخدمة في الدخول الخفي او غير المصرح للنظام , فضلا عن عمليات الاختراق الالكتروني (Penetration E.) والعمليات التنصتية (man in the middle attacks) [2] .

ثانيا: الحرب السيبرانية الدفاعية:

يتمثل هذا النوع من الحروب في مجموعة التدابير والإجراءات التقنية والتنظيمية التي تتخذها الدول بهدف حماية أنظمتها المعلوماتية وشبكاتها الرقمية من أي هجمات سيبرانية , ومحاولة الحد من اثارها المحتملة , وتشمل هذه التدابير استخدام التقنيات الوقائية وأنظمة الامن السيبرانية المختلفة. وذلك من اجل الكشف المبكر عن الهجمات السيبرانية والتصدي لها وذلك يسهم في حماية البنيه التحتية المعلوماتية للدول من التهديدات السيبرانية التي قد تصدر من الدول الأخرى او غيرهم من غير الدول مثل المنظمات العسكرية [3] .

المبحث الثاني

الأساس القانوني الدولي لمواجهة الحرب السيبرانية والتحديات التي تواجه تنظيمها

في عصر الرقمنة، برزت الحرب السيبرانية كأخطر تهديد للأمن الدولي، مستحدثةً ساحة معركة جديدة تتجاوز الحدود الجغرافية التقليدية. يواجه القانون الدولي تحدياً كبيراً في مواكبة هذا الشكل الجديد من النزاعات،

([1]) محمد الجنون، الحرب السيبرانية "كل ما تود معرفته عن معارك تدار بلا رصاص " , 6 سبتمبر 2025 , مقال منشور على موقع التلفزيون العربي , الموقع الالكتروني https://share.google/lzDlCChNlDAnbUhoT .

([2]) نسرين الصباحي , الحروب السيبرانية وتحديات الامن العالمي , المركز العربي للبحوث والدراسات , 26 سبتمبر 2017 , على الموقع الالكتروني https://www.acrseg.org/40594

([3]) تعرضت أكثر من مائتي دولة حول العالم لهجمات سيبرانية معقدة اطلق عليها هجمات (الفدية الخبيثة)، تم خلالها حدوث حالات من الابتزاز المالي وتشفير ملفات الكترونية على أجهزة حاسبات مؤسسات ومرافق هذه الدول وتسبب ذلك في أضرار مادية ومعنوية جسيمة لهذه الدول، وقد نسب تنفيذها إلى مجموعة هاكرز، كما كانت هناك هجمات بيتيا حيث لم تقتصر على تشفير الملفات، بل قامت بتشفير وحدة (MRC) بالهارد ديسك كله، واتهمت أوكرانيا روسيا بأنها المتسببة في هجمات بيتيا الأخيرة.

حيث تتصارع الدول لتطبيق مفاهيم كالعدوان المسلح والدفاع الشرعي على هجمات سيبرانية غالباً ما تكون مجهولة المصدر. عليه يستعرض هذا المبحث أبرز الآليات القانونية الدولية المقترحة لتنظيم هذه الحرب، وعلى رأسها دور الأمم المتحدة والقانون الدولي الإنساني. أضافة إلى اتفاقية بودابست ودليل تالين كآليات خاصة , كما يسلط الضوء على أبرز التحديات التي تعترض هذا التنظيم، وفي مقدمتها غموض قواعد الإسناد، وتباين المصالح السياسية للدول الكبرى. بناءً على ما تقدم سوف نقسم هذا المبحث على مطلبين نتطرق في المطلب الأول للأساس القانوني الدولي لمواجهة الحرب السيبرانية, اما الثاني نخصصه لدراسة التحديات التي تواجه تنظيمها.

المطلب الأول

الأساس القانوني الدولي لمواجهة الحرب السيبرانية

يقوم التنظيم القانوني الدولي لمواجهة الحرب السيبرانية على ركيزتين أساسيتين: الأولى هي القواعد العامة للقانون الدولي التي نشأت لتنظيم النزاعات التقليدية ولكنها تمتد لتشمل الفضاء السيبراني، والثانية هي الجهود التعاهدية الخاصة التي استهدفت تنظيم هذا الفضاء بشكل مباشر. وعليه يمكن تقسيم الأساس القانوني لمواجهة الحرب السيبرانية في القانون الدولي إلى أساس قانوني عام أو غير مباشر والذي يتضمن الاتفاقيات الدولية التي تتناول موضوع الحرب السيبرانية بصورة عامة وأساس قانوني خاص أو مباشرة والذي يتمثل بالاتفاقيات الدولية الخاصة بتنظيم الحرب السيبرانية . وذلك من خلال فرعين نتناول في الأول: الأساس القانوني الدولي غير المباشر (العام) . أما الفرع الثاني فنتطرق فيه إلى الأساس القانوني الدولي المباشر (الخاص) .

الفرع الأول

الأساس القانوني الدولي غير المباشر(العام)

الحرب السيبرانية تختلف بطبيعتها عن غيرها من الحروب الأخرى وذلك لان الحرب السيبرانية في داخل الفضاء الالكتروني تكون غير مضمونة النتائج ، فهي تستهدف الامن العام والنظام العام للبلد الذي تتعرض له مما يؤدي الى شلل او تعطيل الأنظمة المعلوماتية التي يقوم عليها النظام في ذلك البلد[1]. فالحرب السيبرانية تتميز بانها ديناميكية خفية، ويرى **جانب من الفقه القانوني**: أنه لا يمكن تطبيق قواعد القانون الدولي بصورة عامة، وقواعد القانون الدولي الإنساني بصورة خاصة على الحروب والهجمات السيبرانية ويرجعون سبب ذلك الى ان الفضاء الالكتروني هو منطقة خالية من القانون، فما هو حسب ما يرون الا عالم افتراضي غير محدد في نطاق معين او دولة معينة، وبسبب ذلك لا يمكن لهذا الفضاء وما يحدث فيه ان يخضع لقواعد القانون الدولي العام ولا لقواعد القانون الدولي الإنساني المتعلقة بتنظيم قواعد الحرب الدولية وذات الطابع غير الدولي، ويستندون في ذلك

([1]) ربيعي حسين و سمر محمود ، الحروب السيبرانية - المخاطر واستراتيجيات تحقيق الامن السيبراني الدولي والداخلي ، المجلة الجزائرية للأمن السيبراني ، مج7 , ع2، 2022، ص 172.

الى إن الفضاء الالكتروني جديد وهو على عكس الواقع المادي فالحرب في نظرهم تستدعي لتطبق قواعد القانون الدولي الإنساني عليها جملة عوامل **أهمها:-**

1. أن يسبق الحرب اعلان من جانب الأطراف المتحاربة.
2. أن يكون ميدان الحرب وساحاته محددة.
3. أن تقوم الدول بخوضها بواسطة جيوشها النظامية.

وجانب أخر من الفقه القانوني يؤيد تطبيق قواعد القانون الدولي على الحرب السيبرانية على أساس ان تلك الهجمات يتم ارتكابها أثناء النزاعات المسلحة الدولية او النزاعات ذات الطابع غير الدولي أو في وقت السلم[1]. وبالرغم من ان ميثاق الأمم المتحدة لم ينظم بصورة مباشرة مسألة العمليات أو الحروب السيبرانية في نصوصه، إلا أن قواعده المتسمة بالمرونة قابلة لأن تتضمن هذه الظاهرة، لعلمنا بأن الحروب السيبرانية بصورة أو بأخرى تمثل خرقاً للمبادئ الواردة فيه، وهذا ما جاءت به المادة الثانية الفقرة الرابعة , حيث نبهت إلى عدم اللجوء إلى استخدام القوة أو التهديد باستخدامها، وهو ما يتحقق فعليًا في الحروب السيبرانية، كونها عدوانًا موجهًا ضد إقليم دولة ما، يُصطلح عليه فقهيًا بـ"الفضاء السيبراني" أو "الفضاء الرقمي"، إذ تقوم هذه الحروب بالتحكم في عدد من المجالات الحيوية للدولة، فتوقف أو تشل حركتها أثناء تنفيذها. ومن ثم، فإن ذلك يُوجب للدولة المعتدى عليها أن تدفع العدوان بنفسها أو بمعاونة غيرها، وهو حق طبيعي أكده الميثاق في المادة 51، التي تنص على أن للدولة حق الدفاع عن نفسها منفردة أو بالاشتراك مع غيرها من أعضاء الأمم المتحدة[2] . أضف إلى ذلك أن مقصد الأمم المتحدة الأساسي هو الحفاظ على السلم والأمن الدوليين، وبما أن الحرب السيبرانية – التي أوجدتها ضرورات التطور في الحياة الدولية – أصبحت تهديدًا فعليًا لهذا السلم، فإن من واجب الأمم المتحدة أن تتصدى لهذا النوع من الحروب بما يناسب طبيعتها. انطلاقا من واجب الأمم المتحدة الأساسي وهو الحفاظ على السلم والأمن الدوليين شهدت الأمم المتحدة خلال عامي(2023)و(2024)تحركات ملموسة بشأن هذه المسألة :

أولًا: تبنت الجمعية العامة للأمم المتحدة في ديسمبر 2024 اتفاقية دولية جديدة لمكافحة الجرائم السيبرانية، أكدت فيها على أهمية التعاون الدولي وبناء قدرات الدول النامية في مواجهة التهديدات الرقمية.[3]

ثانيًا: ناقش مجلس الأمن في عدة جلسات عام 2024 التهديدات السيبرانية بوصفها من أبرز مخاطر العصر، وأكد الأعضاء على ضرورة تنظيم ردود جماعية لهذه الحروب، نظرًا لما تشكله من خطر جسيم على أمن الدول.[4]

---

(1) م. عبد الرحمن شامل عبد الرحمن و د. زيد لقمان ، الطبيعة القانونية للهجمات السيبرانية في ضوء القانون الدولي الإنساني، مجلة النور للدراسات القانونية ، ، مج1 ، ع2 , 2024 ، ص162.

(2)"ميثاق الأمم المتحدة"، المادة (4/2) والمادة (51)، الأمم المتحدة، https://www.un.org/ar/about-us/un-charter .

(3)"الجمعية العامة للأمم المتحدة تعتمد اتفاقية مكافحة الجرائم السيبرانية"، مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC)، https://www.unodc.org/unodc/ar/press/releases .

(4) "مجلس الأمن يناقش تهديدات الأمن السيبراني"، أخبار الأمم المتحدة، https://news.un.orgar / .

ثالثًا: أطلقت الأمم المتحدة في ذات العام "الميثاق الرقمي العالمي" الذي يهدف إلى ضمان الاستخدام المسؤول للتكنولوجيا الرقمية، بما في ذلك الحروب السيبرانية.[1]

رابعًا: استضافت الرياض منتدى حوكمة الإنترنت 2024، وناقش المشاركون فيه سبل تعزيز الأمن السيبراني من خلال التعاون بين الدول ومنظمات المجتمع المدني.[2] حيث تكشف هذه التحركات عن توجه أممي واضح نحو الاعتراف بخطورة الحروب السيبرانية، والعمل على تطوير أدوات القانون الدولي للتعامل معها بالشكل المناسب. وبينما تطبق قواعد القانون الدولي العام وابرزها ميثاق الأمم المتحدة في أوقات السلم والحرب , فإن قواعد القانون الدولي الإنساني يطبق في حالة وجود نزاع وهنا يجب توضيح أن القانون الدولي الإنساني يرتكز على مجموعة من المبادئ الأساسية، من أبرزها مبدأ التناسب ومبدأ الضرورة العسكرية[3].

حيث ان مبدأ التناسب يقتضي أن تكون الوسائل والأساليب المستخدمة في النزاع متناسبة مع الهدف العسكري المشروع، وأن لا تُفضي إلى أضرار مفرطة بالمدنيين أو بالأعيان المدنية مقارنة بالمكاسب العسكرية المتوقعة. وفي سياق الهجمات السيبرانية، فإن تقييم التناسب يزداد تعقيداً بالنظر إلى الطبيعة الرقمية للهجوم، وإمكانية اتساع نطاق الأثر دون قصد مباشر[4].

أما مبدأ الضرورة العسكرية، فيسمح باستخدام القوة فقط بالقدر اللازم لتحقيق غرض عسكري مشروع، ويُحظر أي استخدام غير مبرر للقوة يتجاوز هذا الغرض. وتطبيق هذا المبدأ على الهجمات السيبرانية يتطلب التحقق من كونها ضرورية لتحقيق نتيجة عسكرية ملموسة، وليس مجرد إحداث ضرر تقني أو تعطيل للبنية التحتية دون هدف عسكري واضح[5].

,وبناء على ما تقدم يتبادر تساؤل معين وهو هل تفي الهجمات السيبرانية بـ "عتبة" النزاع المسلح، وبالتالي ينطبق عليها قواعد القانون الدولي الإنساني وللاجابة عن هذا السؤال ينبغي التفريق بين حالتين:-

الحالة الأولى: وجود نزاع مسلح قائم بالفعل، وفي هذه الحالة فإن الهجمات السيبرانية تعد مكوناً أو جانباً من العمليات العدائية المستمرة داخل هذا النزاع المستمر، ومثال ذلك، الهجمات السيبرانية بين روسيا وجورجيا عام, 2008 كانت ضمن نزاع مسلح دولي وبالتالي فهي خاضعة لقواعد القانون الدولي الإنساني، وبالتالي فهي خاضعة أياً كانت تبعاتها ولا خلاف في ذلك.

---

(1) "الميثاق الرقمي العالمي"، الأمم المتحدة، https://www.un.org/ar/global-Digital-Compact .
(2) "منتدى حوكمة الإنترنت 2024"، الهيئة الوطنية للأمن السيبراني – السعودية، https://www.nca.gov.sa
(3) محمد مجدي عبد الله، القانون الدولي الإنساني والنزاعات المسلحة المعاصرة ,بيروت, المؤسسة الجامعية للدراسات والنشر، 2020، ص112.
(4) المرجع نفسه، ص118.
(5) أنور سلطان، القانون الدولي الإنساني, المبادئ والتطبيقات, دار النهضه العربية , القاهرة, 1983, ص 92.

الحالة الثانية: عدم وجود نزاع قائم بالفعل، في هذه الحالة هل الهجمات السيبرانية - التي تحدث في غياب نزاع مسلح حركي Conflict Armed Kinetic قائم بالفعل - تخضع للقانون الدولي الإنساني؟

وعلية فإن القانون الدولي الإنساني لا يطبق إلا في حالة وجود نزاع مسلح، ولم يعرف القانون الدولي الإنساني المقصود بـ "النزاع المسلح"، ولكنه توسع في التمييز بين نوعين من النزاعات المسلحة وهما: النزاع المسلح الدولي، والنزاع المسلح غير الدولي, بالنسبة للنزاع المسلح الدولي، فقد تم التمييز بين اتجاهين: إذا كانت الهجمات السيبرانية تؤدي إلى تبعات عنيفة؛ فإنها تخضع في هذا الفرض إلى قواعد القانون الدولي الإنساني، أما إذا كانت لا تؤدي إلى تبعات عنيفة وكما يلي :

الاتجاه الأول: يرى هذا الاتجاه أن القانون الدولي الإنساني لا ينطبق إلا على الهجوم الذي يؤدي لتبعات عنيفة فقط، وتعرف المادة 49/ 1 من البروتوكول الإضافي الأول الهجمات بأنها: "أعمال العنف الهجومية والدفاعية ضد الخصم". وقد كان المقصود من "أعمال العنف" خلال المؤتمرات التحضيرية لوضع البروتوكول أعمال العنف المادي التي تتم بشكل حركية فقط (actions Kinetic) إلا أنه مع التطور العلمي الحديث، واستخدام الأسلحة البيولوجية والكيماوية في النزاعات المسلحة، تم توسيع المقصود من كلمة "أفعال العنف" الواردة بالبروتوكول لتشمل العمليات العسكرية التي تؤدي إلى تبعات عنيفة، حتى وإن كان الفعل المكون لها غير عنيف، وذلك مثل الأسلحة البيولوجية والكيماوية، إذ قد تتم الهجمات من خلال إتيان أفعال غير عنيفة، مثل إطلاق حيوان ملوث بمرض لنشره بين السكان؛ إلا أن آثارها تؤدي إلى الوفاة، أو الإصابات الخطيرة وبالتالي فهي تؤدي إلى تبعات عنيفة [1].

وبتطبيق هذا المفهوم على الهجمات السيبرانية، فهي هجمات تتم من خلال إتيان أفعال غير عنيفة؛ إذ إنها مجرد دخول في الفضاء السيبراني لإحداث التأثير المطلوب عن طريق برنامج ضار، وهي بذلك أفعال غير عنيفة في طبيعتها، وإنما تؤدي لتبعات عنيفة. فعلى سبيل المثال، فإن الأفعال التي تستهدف إحداث تعطل في نظام الطائرات المحلقة (أفعال غير عنيفة) تؤدي لحدوث وفيات، أو إصابات بليغة لأشخاص، أو أضرار بالأعيان (تبعات عنيفة)، وبالتالي فهي تقع ضمن مفهوم الهجوم الوارد في البروتوكول الإضافي الأول. ويتفق ذلك مع التعريف الوارد في دليل تالين للهجوم السيبراني بأنه: "عملية سيبرانية، هجومية أو دفاعية، يتوقع منها بشكل معقول أن تحدث إصابة أو وفاة في صفوف الأشخاص أو أضرار في الأعيان[2]."

الاتجاه الثاني: يرى أن كافة الهجمات السيبرانية غير عنيفة في طبيعتها, أما تبعاتها، ففي معظم الأحوال، هي تبعات غير عنيفة، وغير مباشرة في العالم المادي، ومثال ذلك، الأفعال التي تستهدف إحداث تعطل في تدفق

---

(1) كوردولا دوريجي, لا تقرب حدود فضائي الالكتروني, الحرب الالكترونية والقانون الدولي الانساني وحماية المدنيين, المجلة الدولية للصليب الاحمر, مج 94, ع886, 2012, ص540.

(2) د. سلوى يوسف الاكيابي, مدى انطباق القانون الدولي الإنساني على الهجمات السيبرانية, بحث منشور في مجلة روح القوانين, ع 101, ج2, 1923 , ص 1312.

البيانات - على سبيل المثال قد تؤدي لفقدان القدرة على الاتصال بالعالم الخارجي، أو مباشرة الأنشطة التجارية أو غيرها. فهل تندرج ضمن مفهوم "الهجوم الوارد في البروتوكول الإضافي الأول؟

يوجد اتجاهان في الفقه حول هذا الشأن:

الاتجاه الأول: يرى أن الهجوم الذي لا يؤدي إلى إضرار مادية بالأشخاص أو تدمير الممتلكات لا يندرج ضمن مفهوم "الهجوم" الوارد في المادة 49 / 1 من البروتوكول الإضافي الأول. لا يستثنى من ذلك العمليات السيبرانية طالما أنها لا تؤدي الى معاناة بشرية.

الاتجاه الثاني: قد يرى أن الهجوم السيبراني يمكن أن يُعتبر هجومًا ضمن مفهوم المادة 49 /1 من البروتوكول الإضافي الأول، حتى لو لم يؤدي إلى إضرار مادية مباشرة، إذا كان له تأثير كبير على الأهداف المدنية أو العسكرية. وعليه، فإن إخضاع الهجمات السيبرانية لقواعد القانون الدولي الإنساني ليس مجرد مسألة نظرية، بل يرتبط بمدى قدرة المجتمع الدولي على تكييف هذه القواعد التقليدية مع طبيعة النزاعات الحديثة، بما في ذلك الحروب السيبرانية التي قد لا تتطلب استخداماً مباشراً للقوة المسلحة، ولكنها قد تُخلّف آثاراً لا تقل خطورة عن الأسلحة التقليدية. وتجدر الإشارة إلى أن اللجنة الدولية للصليب الأحمر قد أكدت في تقاريرها الحديثة أن قواعد القانون الدولي الإنساني تنطبق كذلك على الحرب السيبرانية التي تُشن أثناء النزاعات المسلحة، وشددت على أن مبادئ القانون الدولي الإنساني، ولا سيما مبدأي التناسب والتمييز، تظل واجبة الاحترام حتى في الفضاء السيبراني، وذلك لضمان حماية المدنيين والبنى التحتية المدنية من الأذى غير المبرر أو المفرط. [1] وقد شهد العالم عدد من الحروب السيبرانية التي تصدرت خلال الفترة الاخيرة الساحة الخارجية منبئة عن تحول كبير في اسلوب القتال ومن بين تلك الحروب ما قامت به الولايات المتحدة الأمريكية وإسرائيل على ايران وما شنتها روسيا على أوكرانيا, وكذلك بين الصين والولايات المتحدة الأمريكية.

الفرع الثاني

الأساس القانوني الدولي المباشر (الخاص)

ان الأساس القانوني المباشر –الخاص- لمواجهة الحرب السيبرانية في القانون الدولي العام يتضمن الاتفاقيات الدولية التي تتناول موضوع الحرب السيبرانية بصورة خاصة ومباشرة حيث هناك اتفاقيات دولية خاصة للحروب السيبرانية مثل اتفاقية بودابست لعام 2001 والاتفاقية العربية لعام 2010 ودليل تالين وهي كما يلي:

أولا: اتفاقية بودابست لعام 2001:

([1]) اللجنة الدولية للصليب الأحمر، القانون الدولي الإنساني في مواجهة التحديات المعاصرة , جنيف , منشورات اللجنة، 2023، ص 29. https://www.icrc.org/ar/publication /

تعد اتفاقية بودابست من أول الاتفاقيات التي اهتمت بموضوع الحرب السيبرانية، إذ تم اعتمادها من قبل مجلس أوربا بشأن الحروب السيبرانية في عام 2001م . حيث وضعت هذه الاتفاقية مبدأ توجيهياً لأي بلد لوضع تشريع وطني شامل لمكافحة جرائم الإنترنيت.

حيث أوصت الدول باتخاذ كافة الإجراءات التشريعية من أجل جعل الدخول إلى أي نظام الكتروني أو أي جزء منه جريمة إلكترونية، كما تحرص هذه الاتفاقية على الملائمة بين أحكامها وأحكام القوانين الوطنية[1]. وعليه فإن الدول التي تصادق على الاتفاقية ملزمة بتجريم تسعه جرائم منها:-

1- الدخول غير قانوني.
2- الاعتراض غير القانوني.
3- التدخل المتعمد أو الارادي في المعطيات بالتدمير أو الحذف أو التشوية والافساد أو تبديلها أو تغييرها أو تعديلها أو تعطيلها أو كبتها أو إخمادها.
4- التدخل المتعمد في الأنظمة.
5- التزوير المتعمد باستخدام جهاز الحاسوب.
6- إساءة استخدام الأجهزة.
7- الاحتيال المتعمد باستخدام الحاسوب.
8- الجرائم المرتبطة بدعارة الأطفال.
9- الجرائم المرتبطة بحق المؤلف. [2]

جاء في مقدمتها الآتي: " نتيجة للتغيرات العميقة التي نجمت عن الظاهرة الرقمية، وعن التقارب الرقمي والعولمة المستمرة لشبكات الحاسوب، وإدراكا للدول الأطراف فيها بالمخاطر التي قد تنجم عن استخدام شبكات الحاسوب والمعلومات السيبرانية، في ارتكاب أفعال جنائية، لاسيما وان المكافحة الفعالة لجرائم الفضاء المعلوماتي، تستلزم المزيد من التعاون الدولي السريع والفعال في المسائل الجنائية "[3].

ومن ثم أشارت إلى جملة من المصطلحات التي تشكل الأساس في كل جريمة الكترونية، وعليه خصصت المادة الأولى إلى بيان هذه المصطلحات وهي:

([1]) نصت الفقرة الأخيرة من الديباجة اتفاقية بودابست للجرائم السيبرانية لعام 2001 , على الآتي: "اقتناعًا بأن هذه الاتفاقية ضرورية لردع الأفعال الموجّهة ضد سرية وسلامة وتوافر أنظمة الحاسوب والشبكات وبيانات الحاسوب، وكذلك إساءة استخدام هذه الأنظمة والشبكات والبيانات، وذلك من خلال تجريم مثل هذا السلوك كما (هو موصوف في هذه الاتفاقية)، واعتماد صلاحيات كافية لمكافحة هذه الجرائم بفعالية، عبر تسهيل كشفها والتحقيق فيها وملاحقة مرتكبيها قضائيًا على المستويين الوطني والدولي، وكذلك من خلال توفير ترتيبات للتعاون الدولي السريع والموثوق" .

([2]) المواد من (2-10) , اتفاقية بودابست للجرائم السيبرانية لعام 2001.

([3]) الديباجة الواردة في اتفاقية بودابست للجرائم السيبرانية لعام 2001 .

يقصد بـ " منظومة الكومبيوتر " أي جهاز | جهاز أو مجموعة من الأجهزة المتصلة أو ذات الصلة. والتي يقوم واحد منها أو أكثر وفاقا لبرنامج ما، بالمعالجة الآلية للبيانات.

يقصد بـ " بيانات الكومبيوتر " أي عمليات عرض للحقائق أو المعلومات أو المفاهيم في صيغة مناسبة لمعالجتها عبر نظام الكومبيوتر، بما في ذلك برنامج مناسب يساعد نظام الكومبيوتر في أداء وظيفة للبيانات . [1]

يقصد بـ "مزود الخدمة" اي جهة عامة أو خاصة توفّر لمستخدمي خدماتها إمكانية الاتصال أو التواصل بواسطة نظام حاسوب, أي جهة أخرى تقوم بمعالجة أو تخزين بيانات الحاسوب نيابة عن خدمة الاتصال أو عن مستخدمي تلك الخدمة.

يقصد بـ "بيانات حركة الاتصال "تعني أي بيانات حاسوبية تتعلق بعملية اتصال تتم عبر نظام حاسوب، ويتم إنشاؤها بواسطة نظام حاسوب كان جزءًا من سلسلة الاتصال، وتبين(مصدر الاتصال , وجهته , مسار الاتصال, الوقت والتاريخ , حجم البيانات, مدة الاتصال, نوع الخدمة المستخدمة). [2]

وقد واجهت اتفاقية بودابست انتقادات عديدة أهمها:-

1- أنها تركز بالدرجة الأولى على الجرائم الفردية بدلاً من النزاعات بين الدول.

2- عدم تطبيق قواعد هذه الاتفاقية - اتفاقية بودابست - على الحرب السيبرانية.

ثانيا : الاتفاقية العربية لمكافحة جرائم تقنية المعلومات 2010:

وبعد أن تناولنا اتفاقيه بودابست التي اعتمدت من قبل مجلس اوربا وجب الكلام عن الجانب الإقليمي , وعليه سنتناول الاتفاقية العربية لمكافحة جرائم تقنية المعلومات حيث ابرمت الاتفاقية في مصر في القاهرة وذلك ضمن أعمال جامعه الدول العربية , وتم التوقيع عليها بتاريخ 21/12/2010 وان الهدف منها هو تعزيز التعاون بين الدول العربية في مكافحة الجرائم المرتبطة بتقنية المعلومات لدرء اخطار هذه الجرائم حفاظا على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وافرادها[3]. كما تلتزم كل دولة طرف في هذه الاتفاقية بتبني الإجراءات التشريعية الضرورية اللازمة لوضع هذه الاتفاقية موضع التنفيذ [4] .

وصدقت عدد من الدول العربية هذه الاتفاقية ومنها العراق حيث وقعها في القاهرة بتاريخ 21/12/2010 ومن ثم تصديقها من قبل السلطة التشريعية , بعد المصادقة عليها تم نشر الاتفاقية في جريدة الوقائع العراقية بتاريخ 30/9/2013.[5]

---

(1) المادة الأولى , الفقره(أ, ب), اتفاقية بودابست للجرائم السيبرانية لعام 2001.
(2) المادة الأولى, الفقرة (س, د) من اتفاقية بودابست للجرائم السيبرانية .
(3) المادة الأولى, من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات .
(4) الفقرة رقم (1) , من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات .
(5) جريدة الوقائع العراقية , قانون تصديق الاتفاقية العربية لمكافحة جرائم تقنية المعلومات رقم (31) لسنة 2013 , العدد 4292 , تم نشر القرار رقم (30) بتاريخ 30/9/2013 .

وعلية فأن الدول التي صادقت على الاتفاقية ملزمة بتجريم الجرائم الاتية [1]:

1_جريمة الدخول غير المشروع.

2_جريمة الاعتراض غير المشروع.

3_جريمة الاعتداء على سلامة البيانات.

4_جريمة إساءة استخدام وسائل تقنية المعلومات.

5_ جريمة التزوير.

6_جريمة الاحتيال.

7_الجرائم الإباحية.

8_الجرائم الأخرى المرتبطة بالإباحية.

9_جريمة الاعتداء على حرمة الحياة الخاصة.

10_الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات.

11_الجرائم المتعلقة بالجرائم المنظمة والمرتكبة بواسطة تقنية المعلومات.

12_ الجرائم المتعلقة بانتهاك حق المؤلف والحقوق المجاورة.

13_ الاستخدام غير المشروع لأدوات الدفع الالكترونية.

14_الشروع والاشتراك في ارتكاب الجرائم.[2]

كما وجاء في مقدمة الاتفاقية: "ان الدول العربية الموقعة رغبة منها في تعزيز التعاون فيما بينها لمكافحة تقنية المعلومات التي تهدد امنها ومصالحها وسلامة مجتمعاتها, واقتناعاً منها بضرورة الحاجة إلى تبني سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد جرائم تقنية المعلومات واخذاً بالمبادئ الدينية والأخلاقية السامية ولا سيما أحكام الشريعة الإسلامية، وكذلك بالتراث الإنساني للأمة العربية التي تنبذ كل أشكال الجرائم، ومع مراعاة النظام العام لكل دولة , والتزاماً بالمعاهدات والمواثيق العربية والدولية المتعلقة بحقوق الإنسان ذات الصلة من حيث ضمانها واحترامها وحمايتها" [3] ومن ثم أشارت إلى جملة من المصطلحات التي تشكل الأساس في كل جريمة الكترونية، وعليه خصصت المادة الثانية إلى بيان هذه المصطلحات وهي نفس تعريف المصطلحات التي وردت في اتفاقية بودابست السابق ذكرها[4]

وقد واجهت الاتفاقية العربية لمكافحة تقنية المعلومات انتقادات منها :

---

(1) المادة الخامسة من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات .
(2) المواد من(6_19) ,من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات .
(3) ديباجة الاتفاقية العربية لمكافحة تقنية المعلومات .
(4)المادة الثانية من الاتفاقية العربية لمكافحة تقنية المعلومات .

1. أنها تركز بالدرجة الأولى على الجرائم الفردية بدلاً من النزاعات بين الدول وهذا الانتقاد مشابه للانتقاد الموجة لاتفاقية بودابست بالرغم من انها تكلمت عن الجرائم المتعلقة بالإرهاب المرتكب بواسطة تقنية المعلومات, [1] وأيضا تناولت الجرائم المنظمة والمرتكبة بواسطة تقنيه المعلومات[2] إلا انها لم تتوسع في الحديث عن الحروب السيبرانية بصورة متكاملة .
2. لم تطبق قواعدها على الحروب السيبرانية التي قد تجري بين الدول المنظمة الى الاتفاقية.

ثالثا: دليل تالين:

يمثل دليل تالين أحد أبرز الجهود الفقهية التي حاولت أن تواكب التغير الحاصل في طبيعة النزاعات المعاصرة، خصوصاً تلك التي تتخذ من الفضاء السيبراني ميدانًا لها. وقد جاء هذا الدليل في مرحلتين أساسيتين، تعبيراً عن تطور الفهم القانوني لموضوع الحرب السيبرانية في سياق قواعد القانون الدولي[3]

- **فالمرحلة الأولى:** من الدليل التي صدرت سنة 2013، ركزت على القواعد المتعلقة بالحرب السيبرانية في حال قيام نزاع مسلح بين الدول، واستندت إلى مبادئ القانون الدولي الإنساني كالتناسب والتمييز، وحاولت تكييفها على البيئة الرقمية، كما أقرت بإمكانية أن تُعد الحرب السيبرانية استخدامًا للقوة في ضوء المادة 4/2 من ميثاق الأمم المتحدة، وقد تصل في بعض صورها إلى حد العدوان الموجب لتطبيق المادة 51 المتعلق بالدفاع الشرعي

- **أما المرحلة الثانية:** والتي حملت عنوان "دليل تالين 2.0" وصدرَت سنة 2017، فقد توسعت لتشمل القواعد القانونية المطبقة في أوقات السلم أيضاً، وأدخلت موضوعات جديدة كاحترام سيادة الدولة في الفضاء السيبراني، وعدم التدخل، والمسؤولية الدولية عن الأفعال السيبرانية الصادرة من داخل إقليم الدولة أو من كيانات تابعة لها، حتى وإن لم ترقَ هذه الأفعال إلى مستوى النزاع المسلح [4]

وبذلك فإن دليل تالين بشقيه لم يُنشئ قواعد جديدة، بل سعى إلى تفسير القواعد القائمة على ضوء التطور الرقمي، في محاولة لإيجاد قراءة منسجمة ما بين الفقه والقانون مع واقع الحرب السيبرانية [5]. كما ان دليل تالين تم اعداده من قبل خبراء في القانون الدولي وذلك بناء على دعوة من منظمة اللجنة الدولية للصليب الأحمر. ويعد هذا الدليل- دليل تالين- الوثيقة القانونية الدولية الوحيدة التي تنظم مثل هكذا نوع من الحروب التي تقع بين الدول. ويتكون هذا الدليل من (95) مادة استمدت غالبيتها من القانون الدولي العام بمعناة الواسع، وكان

([1])المادة (15) من الاتفاقية العربية لمكافحة تقنية المعلومات .
([2])المادة (16) من الاتفاقية العربية لمكافحة تقنية المعلومات .
([3]) محمد سليم العواد، "دليل تالين والقانون الدولي في الفضاء السيبراني"، المجلة الدولية للقانون، العدد 4, 2019, ص 56.
([4]) المرجع نفسه، ص58.
([5])خالد عبد الله الغامدي، "الضوابط القانونية للحرب السيبرانية: دراسة في ضوء دليل تالين 2.0"، مجلة جامعة نايف للعلوم الأمنية، العدد 65, 2021, ص 103.

السبب وراء وجود دليل تالين هو القصور في قواعد القانون الدولي في مجال الحرب السيبرانية، بسبب عدم وجود أي أساس قانوني ينظم اللجوء الى مثل هكذا نوع من الحروب او ينظم سير العمليات الحربية خلال اندلاعها فهو بمثابة صك قانوني بالإمكان الرجوع الية اثناء الحرب.

وقد تعرض دليل تالين لانتقادات عديدة أهمها:-

1- أن نصوص دليل تالين لا تطبق على الحالات التي يتم فيها النزاع تقليدياً. وهذا ما جاء في المادة 20 من الدليل.

2- ان نصوص دليل تالين وأحكامه لا يتمتع بصفة الالزام، ومن ثم فهو لا يرقى الى مرتبة الاتفاقيات الدولية.

3- ان دليل تالين واجهه معارضة كبيرة من الدول التي لم تشارك في اعداده ومنها على سبيل المثال روسيا والصين.

4- عند وضع دليل تالين واحكامه القانونية لم يتم مراعاة آليه التمثيل العالمي في اختيار الدول [1].

نستنتج مما سبق أعلاه أن للهجمات السيبرانية التي تحصل ما بين الدول تتمتع بطبيعة خاصة تحكمها، وتحكمها قواعد القانون الدولي كتلك التي تلزم الدول على احترام سيادة الدول الأخرى وتجرم استخدام القوه في علاقات الدول فيما بينها وتحظر التمييز العنصري.

المطلب الثاني

التحديات التي تواجه تنظيم الحرب السيبرانية وتطبيقاتها

لا غرو أن كل بناءٍ لا يستند إلى ركائز متينة يكون مهدداً بالانهيار، وقد لا يكتمل أساساً. وهذا ما ينطبق على قواعد القانون الدولي، سواء في صورته التقليدية أو الحديثة، إذ رافقته منذ نشأته جملة من التحديات، أبرزها الطابع الاتفاقي والاختياري لكثير من قواعده، إضافة إلى تضارب المصالح بين الدول الكبرى – خاصة خلال الحقبة الاستعمارية – حيث سعت قوى أوروبية إلى تطويع تلك القواعد لخدمة أهدافها السياسية والاقتصادية. وتُعيد هذه التحديات إنتاج نفسها اليوم في سياق الحرب السيبرانية ولكن بصورة أكثر تعقيداً اذ لا تقتصر على سن قواعد جديدة، بل تمتد إلى كيفية تكييف النصوص القائمة – التي لم تُصمم لمثل هذه الظواهر – مع واقع الحرب السيبرانية .

الفرع الأول

التحديات التي تواجه التنظيم القانوني للحروب السيبرانية

1. **صعوبة اسناد المسؤولية عن الحروب السيبرانية:** تُعد مسألة "النسب" في الحرب السيبرانية من أعقد الإشكاليات القانونية، إذ كثيرًا ما تُشن هذه الهجمات من أطراف غير حكومية، كالأفراد أو الجماعات أو حتى عبر

([1]) د.منزر رابح ، أ.درويش سعيد ، الطبيعة القانونية للهجمات السيبرانية التي تقع بين الدول ، مجلة صوت القانون ،العدد1، المجلد 8، 2021، ص547-548.

وسطاء تقنيين، وقد تجري من داخل أراضي دولة معينة دون علم أو موافقة حكومتها. وهذا الغموض يجعل من الصعب تحميل المسؤولية لدولة معينة، ويُعقّد من تطبيق قواعد المسؤولية الدولية، كما يُتيح للدول التنصل من المسؤولية، ويُغذي حالة الإرباك القانوني في ميدان النزاعات الحديثة . [1]

2. **عدم إمكانية التنبؤ أو الرصد المسبق للهجمات السيبرانية:** إن كان مسألة التعرف على منفذها تواجه صعوبة فمن باب أولى أن لا يتم التنبؤ بها. إذ تتسم الهجمات السيبرانية بطبيعتها المفاجئة وسرعتها العالية، ما يُصعّب من رصدها أو التنبؤ بها قبل وقوعها وعلى خلاف الهجمات العسكرية التقليدية التي قد تسبقها مؤشرات استخباراتية أو تحركات على الأرض، فإن الهجوم السيبراني قد يُنفذ في ثوانٍ ومن دون أي إنذار مسبق، مما يُضعف من قدرة الدول على اتخاذ تدابير استباقية فعالة. كما أن سرعة التطور التكنولوجي في هذا المجال تجعل نظم الإنذار المبكر أقل قدرة على التكيف مع تقنيات الهجوم الجديدة، مما يعزز من صعوبة التصدي لهذا النوع من الحروب.

3. **مبدأ التناسب والتمييز في الحرب السيبرانية:** يعد مبدأ التناسب والتمييز من المبادئ الأساسية في القانون الدولي الإنساني، حيث يُشترط أن يتم تمييز الأهداف العسكرية عن المدنية وأن يكون الضرر الناتج عن الهجوم متناسبًا مع الهدف العسكري. لكن في الحرب السيبرانية، يصعب تطبيق هذا المبدأ بشكل فعال، نظرًا لصعوبة تحديد الأثر الفعلي للهجوم على الأهداف المدنية. فقد يؤدي الهجوم على بنية تحتية حيوية، مثل شبكات الكهرباء أو المستشفيات، إلى أضرار غير مباشرة قد تؤثر على المدنيين بشكل غير متناسب. كما أن التداخل بين الأنظمة العسكرية والمدنية في الفضاء السيبراني يعقد مسألة التمييز بين الأهداف العسكرية والمدنية، مما يجعل من الصعب تقييم مدى مشروعية الهجوم. [2]

4. **غياب الإرادة السياسية الموحدة بين الدول:** يُعد هذا التحدي من أخطر العوائق أمام تقنين الحرب السيبرانية، إذ تتباين مواقف الدول الكبرى بشأن وضع إطار قانوني ملزم، حيث تخشى بعض الدول – ذات القدرات السيبرانية الهجومية المتقدمة – من أن يؤدي الاتفاق إلى تقييد حرية استخدامها لتلك القدرات أو كشف استراتيجياتها، مما يجعلها غير متحمسة للانخراط في مفاوضات جدية. هذا التباين يعطل الوصول إلى توافق دولي، ويُبقي المسألة في نطاق المبادرات غير الملزمة، وهو ما يؤدي إلى استمرار الهجمات السيبرانية دون مساءلة قانونية واضحة، ويُضعف من قدرة المجتمع. [3]

([1])عبد الرحمن شامل عبد الرحمن , زيد لقمان ، الطبيعة القانونية للهجمات السيبرانية في ضوء القانون الدولي الإنساني , مصدر سابق , ص(106).

([2]) احمد مؤيد فتحي محمد- تحديات تطبيق مبدأ التناسب على الهجمات السيبرانية -مجلة دراسات إقليمية مجلد (17), عدد (58), 2023, ص (246).

([3]) صلاح حيدر , حروب الفضاء الالكتروني دراسة في مفهومها وخصائصها وسبل مواجهتها , رسالة ماجستير ,جامعة الشرق الأوسط, 2021, ص (55).

رغم الجهود المبذولة في مجال تنظيم الحرب السيبرانية، إلا أن هناك تأخرًا ملحوظًا في وضع إطار قانوني دولي ملزم ينظم هذا النوع من الحروب. حتى الآن، تقتصر الإسهامات القانونية على مبادرات غير ملزمة مثل "دليل تالين"، الذي يقدم توجيهات نظرية حول تطبيق قوانين الحرب التقليدية على الهجمات السيبرانية. ولكن، لا يوجد حتى اللحظة اتفاق دولي شامل يلزم الدول بتطبيق قواعد قانونية موحدة ومتفق عليها. هذا الفراغ القانوني يترك مجالًا واسعًا للتفسير الفردي من قبل الدول ويعوق جهود التنسيق الدولي لمكافحة الهجمات السيبرانية وتحديد المسؤوليات، مما يزيد من تعقيد المسألة ويؤثر سلبًا على استقرار النظام القانوني الدولي في هذا المجال.

الفرع الثاني

تطبيقات الحروب السيبرانية في العلاقات الدولية

شهد العالم عدد من الحروب السيبرانية التي تصدرت خلال الفترة الاخيرة الساحة الخارجية منبئة عن تحول كبير في اسلوب القتال ومن بين تلك الحروب ما شنتها روسيا على أوكرانيا والولايات المتحدة الأمريكية واسرائيل على ايران وبين الصين والولايات المتحدة الأمريكية وعليه نتناول تلك التطبيقات بشيء من التفصيل وكما يلي:

أولاً: الهجوم السيبراني على البرنامج النووي الإيراني (2010):

في عام 2010، استُخدم فيروس "ستاكسنت" لتعطيل أجهزة الطرد المركزي بمنشأة نطنز النووية الإيرانية. يُعتقد أن الهجوم نُفّذ بتعاون أمريكي-إسرائيلي، ويُعد أول سلاح سيبراني يستخدم لتخريب منشأة عسكرية دون إطلاق رصاصة واحدة.حيث الحق الفيروس اضرار جسيمة بالمنشأت النووية الإيرانية وادى في نهاية المطاف الى تأخير تشغيل محطة بوشهر النووية الإيرانية,[1] حيث تعاونت الاستخبارات الأمريكية والإسرائيلية لتطوير الفيروس المعلوماتي "ستاكسنت" الذي كان أساس استهدافه للبرنامج النووي الإيراني، مما أدى إلى تعطيل آلاف أجهزة الطرد المركزي دون أن تلاحظ طهران ذلك إلا بعد فوات الأوان. وقد شكّل هذا الهجوم نقلة نوعية في توظيف الفضاء السيبراني كأداة للهجوم المادي على منشآت حساسة، مما طرح تساؤلات جوهرية حول مدى انطباق قواعد القانون الدولي الإنساني على الهجمات السيبرانية التي تستهدف بنى تحتية ذات طابع عسكري ولكنها تقع في أوقات سلم ظاهر.[2]

ثانياً: الهجمات السيبرانية الروسية على أوكرانيا (2022–2023):

مع اندلاع الحرب الروسية الأوكرانية، كثّفت موسكو هجماتها السيبرانية على المؤسسات الحكومية والبنية التحتية الأوكرانية. شملت هذه الهجمات تخريب شبكات الكهرباء والاتصالات، وسرقة بيانات حساسة، مما تسبب

---

(1)zhong-hua pang , international journal of Systems Science, volume 53 , 2022, issue 16.

(2) جوشوا الفاريز , ستوكسنت اول سلاح سيبراني في العالم , مقال منشور على موقع جامعه ستانفورد , الموقع الالكتروني https://share.google/nJQNrKdQxBCQ5YALZ , تم النشر بتاريخ 3/2/2015 .

في شلل جزئي للخدمات الحيوية. أعلنت كييف أن روسيا شنت أكثر من 4500 هجوم إلكتروني خلال عام 2022 وحده، استهدفت بشكل مباشر الأنظمة المصرفية والمؤسسات الحكومية وشبكات الطاقة،[1] وهو ما اعتبره خبراء الأمن السيبراني جزءاً من استراتيجية هجومية متكاملة توازي العمليات العسكرية على الأرض. وتشير هذه الحملة الواسعة إلى تحول الهجمات السيبرانية من مجرد أدوات تجسس أو إزعاج إلى وسائل ضغط فعّالة قادرة على إضعاف الخصم وشلّ قدرته على الاستجابة، ما يستدعي إعادة النظر في قواعد "التمييز" و"التناسب" عند تطبيق القانون الدولي الإنساني على الفضاء الرقمي.[2]

ثالثاً: الصين والولايات المتحدة :

في السنوات الأخيرة، تصاعد التوتر السيبراني بين بكين وواشنطن، حيث تبادل الطرفان الاتهامات بتنفيذ هجمات تستهدف المؤسسات الحساسة. تتهم الصين أمريكا باختراق شبكاتها الحيوية، بينما تتهم واشنطن بكين بسرقة بيانات استخباراتية وتجارية، في سياق تنافس جيوسياسي وتكنولوجي متزايد. صرّحت وزارة الخارجية الصينية أن وكالة الأمن القومي الأمريكية أطلقت هجمات سيبرانية طويلة الأمد على البنية التحتية الحيوية الصينية، وردّت واشنطن باتهامات مماثلة ضد الصين، مما يكرّس واقع الحرب السيبرانية كجبهة متقدمة في صراع القوى الكبرى. وتُبرز هذه الحالة غموض الوضع القانوني في حالة "الحرب السيبرانية الباردة"، حيث تكون الهجمات خارج نطاق النزاع المسلح التقليدي ولكنها تثير تهديدات استراتيجية واقتصادية، دون وجود اتفاق دولي صريح ينظم هذه المواجهات.[3]

الخاتمة

توصلنا بعد الانتهاء من هذا البحث الموسوم بالآليات القانونية الدولية لمواجهة الحروب السيبرانية الى جملةٍ من النتائج كان بعضها متعلقاً بمضمون الحرب السيبرانية وخصائصها وذاتيتها , وبعضها خاص بالأسس القانونية الدولية لمواجهة الحرب السيبرانية والتحديات التي تواجه تنظيمها، وفيما يأتي اهم هذه النتائج :

اولاً: النتائج :

1- الحرب السيبرانية بشكل عام هي نزاع بين طرفين يحدث في مجال الفضاء الالكتروني.

---

(1) آية رجب أبو اليزيد , العمليات السيبرانية بين روسيا وأوكرانيا: قراءة في الأسباب والنتائج, المركز الديمقراطي العربي للدراسات الاستيراتجية والسياسية والاقتصادية: متاح على الرابط التالي: https://democraticac.de/?p=99262 .

(2) "روسيا شنت 4500 هجوم إلكتروني ضد أوكرانيا في 2022"، قناة الحرة، 26 ديسمبر 2022، على الموقع الالكتروني https://www.alhurra.com/ukrainewar/2022/12/26/ .

(3) "اتهامات متبادلة بين الولايات المتحدة والصين بشأن هجمات إلكترونية"، الجزيرة نت، 26 مايو 2023، https://www.aljazeera.net/news/2023/5/26 .

2- تختلف الحرب السيبرانية بطبيعتها عن الحروب التقليدية التي تحدث في الواقع وذلك لان الحروب السيبرانية في داخل الفضاء الالكتروني تكون غير مضمونة النتائج فالحرب السيبرانية تتصف بطبيعة ديناميكية خفية وقد ذهب البعض الى عدم إمكانية تطبيق قواعد القانون الدولي العام بشأنها.

3- ان تنظيم الحرب السيبرانية مازال يواجه تحديات بنيوية معقدة تبدأ من صعوبة الاسناد القانوني وتنتهي بغياب التوافق الدولي .

4- تمثل الحرب السيبرانية تهديداً على الامن والاستقرار الدوليين مما يفرض بدوره ضرورة ملحة لتجاوزها من حلال العمل على تطوير أدوات تنظيمية قادره على ان تواكب التطور التقني المتسارع .

5- يمثل دليل تالين بمراحله خطوه موفقة وممهد للمجتمع الدولي في تنظيم القواعد القانونية المتعلقة بالحرب السيبرانية .

6- عدم وجود اتفاقية دولية ملزمة تنظم الحرب السيبرانية ، وتحدد تعريفها ، وتضع اطاراً قانونياً مشتركاً لأساليب الرد المشروع عليها .

7- يظل تحديد ما يشكل "هجوم مسلح" في الفضاء السيبراني والذي يخول الدول الحق في الدفاع عن نفسها بموجب المادة 51 من ميثاق الأمم المتحدة , غامضا وغير واضح وهذا الغموض يعيق تطبيق مبدأ الدفاع عن النفس ويفتح الباب امام تفسيرات متنوعه قد تؤدي الى تصعيد النزاعات .

8- ان الحروب السيبرانية وهجماتها تثير تساؤلات حول انتهاك السيادة الوطنية للدول خاصه عندما تستهدف البنى التحتية الحيوية او تجمع البيانات الاستخبارية من دون موافقه تلك الدول , حيث انه لا يوجد اجماع دولي واضح حول حدود السيادة في الفضاء السيبراني , وهذا يخلق منطقه رماديه .

ثانياً:- التوصيات:

1- ضرورة ابرام اتفاقية دولية ملزمة تنظم الحرب السيبرانية ، وتحدد تعريفها ، وتضع اطاراً قانونياً مشتركاً لأساليب الرد المشروع عليها .

2- انشاء هيئة دولية مستقلة ضمن منظومة الأمم المتحدة تعنى بمتابعة العمليات السيبرانية وتقييم مدى توافقها مع القانون الدولي العام .

3- تعزيز التعاون التقني والقانوني بين الدول لتطوير أدوات الاسناد الرقمي ، بما يضمن محاسبة المسؤولين عنها. وادماج مبادئ القانون الدولي الإنساني في السياسات السيبرانية للدول ، مع تدريب القوات والجهات المختصة على احترام هذه المبادئ في الفضاء الرقمي . وعلى المجتمع الدولي من خلال المنظمات الدولية والاتفاقيات وضع معايير واضحة وتعاريف لبيان ماهيه " الهجوم المسلح " في الفضاء السيبراني , لتمكين الدول من الدفاع عن نفسها ضمن أطار قانوني.

4- تشجيع البحث العلمي القانوني والتقني المشترك بين الجامعات ومراكز الفكر لتطوير فهم اعمق واكثر توازنا لطبيعة الحرب السيبرانية وآثارها .

المصادر

أولا: الكتب

1. احمد حميدي علي, الحرب في الاسلام والقانون الدولي الإنساني, المكتبة الازهرية للتراث، القاهرة, 2020.
2. أنور سلطان، القانون الدولي الإنساني, المبادئ والتطبيقات , دار النهضه العربية , القاهرة , 1983 .
3. خالد وليد محمود, الهجمات عبر الانترنت – ساحة الصراع الالكتروني الجديدة- سلسلة دراسات ودراسة السياسات, المركز العربي للأبحاث، قطر, 2013.
4. عادل عبد الرزاق، الارهاب الالكتروني- القوة في العلاقات الدولية- نمط جديد وتحديات مختلفة, مركز الدراسات السياسية والاستراتيجية بالأهرام, القاهرة, 2009.
5. محمد مجدي عبد الله، القانون الدولي الإنساني والنزاعات المسلحة المعاصرة، بيروت, المؤسسة الجامعية للدراسات والنشر، 2020.

ثانيا: الرسائل والاطاريح

1. صلاح حيدر عبد الواحد، حروب الفضاء الالكتروني (دراسة في مفهومها وخصائصها وسبل مواجهتها)، رسالة ماجستير، جامعة الشرق الأوسط، كلية الآداب والعلوم ، 2021.

ثالثا:البحوث والدوريات

2. احمد مؤيد فتحي محمد- تحديات تطبيق مبدأ التناسب على الهجمات السيبرانية -مجلة دراسات إقليمية مجلد17 , عدد 58, 2023.
3. خالد عبد الله الغامدي، "الضوابط القانونية للحرب السيبرانية: دراسة في ضوء دليل تالين 2.0"، مجلة جامعة نايف للعلوم الأمنية، العدد 65, 2021.
4. ربيعي حسين وسمر محمود، الحروب السيبرانية - المخاطر واستراتيجيات تحقيق الامن السيبراني الدولي والداخلي، المجلة الجزائرية للأمن السيبراني، مجلد7 ,عدد2، 2022.
5. زياد محمد جفال، عمر احمد السعيد، مدى اعتبار الهجمات السيبرانية انتهاكاً للحظر المفروض على استخدام القوة او التهديد بها في ضوء احكام القانون الدولي للجوء للحرب، مجلة جامعة الامارات للبحوث القانونية، كلية القانون، جامعة العين – الامارات، 2024.
6. سلوى يوسف الاكيابي, مدى انطباق القانون الدولي الإنساني على الهجمات السيبرانية, بحث منشور في مجلة روح القوانين، عدد 101, الجزء الثاني .

7. عبد الرحمن شامل عبد الرحمن , زيد لقمان ، الطبيعة القانونية للهجمات السيبرانية في ضوء القانون الدولي الإنساني، مجلة النور للدراسات القانونية، ، مجلد 1، عدد2 , 2024.
8. كوردولا دوريجي, لا تقرب حدود فضائي الالكتروني، الحرب الالكترونية والقانون الدولي الانساني وحماية المدنيين, المجلة الدولية للصليب الاحمر، مجلد 94, عدد886, 2012.
9.محمد اكرم محسن , مروان سالم علي , السيبرانية "الماهية ,الخصائص, الفواعل ,الابعاد الاستراتيجية" , جامعة الموصل , كلية العلوم السياسية , مجلة حمورابي للدراسات , العدد 43 , السنه الحادية عشرة , 2022.
10.محمد سليم العواد، "دليل تالين والقانون الدولي في الفضاء السيبراني"، المجلة الدولية للقانون، العدد4 , 2019 .
11.منزر رابح، درويش سعيد ، الطبيعة القانونية للهجمات السيبرانية التي تقع بين الدول ، مجلة صوت القانون، العدد1، المجلد 8، 2021.
12. هربت لين، النزاع السيبراني والقانون الدولي الانساني، مجلة اللجنة الدولية للصليب الاحمر،مجلد 94 العدد 886, 2012.

رابعا: المقالات الالكترونية

1. "اتهامات متبادلة بين الولايات المتحدة والصين بشأن هجمات إلكترونية"، الجزيرة نت، 26 مايو 2023، https://www.aljazeera.net/news/2023/5/26 .
2. آية رجب أبو اليزيد , العمليات السيبرانية بين روسيا وأوكرانيا: قراءة في الأسباب والنتائج, المركز الديمقراطي العربي للدراسات الاستيراتجية والسياسية والاقتصادية: متاح على الرابط التالي: https://democraticac.de/?p=99262.
3. "الجمعية العامة للأمم المتحدة تعتمد اتفاقية مكافحة الجرائم السيبرانية"، مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC)، https://www.unodc.org/unodc/ar/press/releases .
4. جوشوا الفاريز , ستوكسنت اول سلاح سيبراني في العالم , مقال منشور على موقع جامعه ستانفورد , الموقع الالكتروني https://share.google/nJQNrKdQxBCQ5YALZ , تم النشر بتاريخ 3/2/2015 .
5. روسيا شنت 4500 هجوم إلكتروني ضد أوكرانيا في 2022"، قناة الحرة، 26 ديسمبر 2022، على الموقع الالكتروني: https://www.alhurra.com/ukrainewar/2022/12/26 / .
6. عبد الله صادق دحلان ، الامن السيبراني علم ينبغي ان يدرس ، تقرير متاح على الموقع الإلكتروني لقناة العربية: https://share.google/flz3fBpJFTezfUT4e .
7. اللجنة الدولية للصليب الأحمر، القانون الدولي الإنساني في مواجهة التحديات المعاصرة , جنيف , منشورات اللجنة، 2023، https://www.icrc.org/ar/publication / .

8. "مجلس الأمن يناقش تهديدات الأمن السيبراني"، أخبار الأمم المتحدة،https://news.un.orgar
9. "محمد الجنون، الحرب السيبرانية "كل ما تود معرفته عن معارك تدار بلا رصاص " , 6 سبتمبر 2025 , مقال منشور على موقع التلفزيون العربي , الموقع الالكتروني
https://share.google/lzDlCChNlDAnbUhoT .
10."منتدى حوكمة الإنترنت 2024"، الهيئة الوطنية للأمن السيبراني – السعودية،
https://www.nca.gov.sa
11. نسرين الصباحي , الحروب السيبرانية وتحديات الامن العالمي , المركز العربي للبحوث والدراسات , 26 سبتمبر 2017 , على الموقع الالكتروني https://www.acrseg.org/40594

خامسا : القوانين والاتفاقيات

1. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات .
2. اتفاقية بودابست للجرائم السيبرانية لعام 2001.
3. جريدة الوقائع العراقية , قانون تصديق الاتفاقية العربية لمكافحة جرائم تقنية المعلومات رقم (31) لسنة 2013 , العدد 4292 , تم نشر القرار رقم (30) بتاريخ 30/9/2013 .
4. "ميثاق الأمم المتحدة"، الأمم المتحدة، https://www.un.org/ar/about-us/un-charter .
5. "الميثاق الرقمي العالمي"، الأمم المتحدة، https://www.un.org/ar/global-Digital-Compact

سادسا: المصادر الأجنبية :

1_ Schmitt, Michael N. (ed.). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, Cambridge, 2017, p. 375.
2_zhong-hua pang , international journal of Systems Science, volume 53 , 2022, issue 16.
3_, Libicki, Martin C. Cyberdeterrence and Cyberwar. RAND Corporation, Santa Monica, 2009, p. 38.
4_Brenner, Susan W. "At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare." Journal of Criminal Law and Criminology, vol. 97, no. 2, 2007, p. 382.
5_Clarke, Richard A., and Knake, Robert K. Cyber War: The Next Threat to National Security and What to Do About It. 2nd ed., HarperCollins, New York, 2010, p. 6 .
6_ Denning, Dorothy E. "Cyber Conflict and Cyber Terrorism." The Routledge Handbook of Terrorism Research, edited by Andrew Silke, Routledge, London, 2010, p. 392 .