Journal Of the Iraqia University (71-3) August (2024)

ISSN(Print): 1813-4521 OnIine ISSN:2663-7502
Journal Of the Iraqia University
available online at: https://www.mabdaa.edu.iq

الطبيعة القانونية للحروب والنزاعات السيبرانية من منظور القانون الدولي

هاورى على محمدامين

حكومة إقليم كردستان – وزارة التعليم العالي والبحث العلمي

The legal nature of cyber wars and conflicts from the perspective of international law

hawre.ameen@gmail.com

Hawri Ali Muhammad Amin

Kurdistan Regional Government - Ministry of Higher Education and Scientific Research

الملخص

يركز البحث على الطبيعة القانونية للحروب والنزاعات السيبرانية من منظور القانون الدولي وبيان أنواع الحروب والنزاعات سيبرانياً ووسائل حماية الأمن سيبرانياً التي من شأنها أن تساعد في منع الحروب والنزاعات بين الدول، وتمنع انتهاك الحيز الرقمي للدول، ويستعرض دور الأمم المتحدة في حفظ السلم والأمن السيبرانيان، وسبل تعزيز الأمن الدولي بأبعاده المختلفة، وآليات حماية المنشآت الحيوية للدول من كافة أوجه الاستخدام غير المشروع لتكنولوجيا الاتصالات والمعلومات، ويدرس البحث الطرق القانونية لحل النزاعات ومنع العدوان وحماية الأمن السيبراني من التهديدات التي تعدها الدول المتقدمة عدواناً لا يختلف عن العدوان باستخدام القوات العسكرية، وتطالب الدول الحد من لمخاطر الإلكترونية التي تستهدف تهديد امنها وسيادتها، بعد اختراق منظومات المعلومات السرية لها، أو هدم منظومة القيم والأخلاق في المجتمع الدولي عن طريق بث الأفكار والمعتقدات مغايرة لما سائد، وذلك عن طريق تطبيق الوسائل الاحترازية –الوقائية / الاستباقية أو الجزائية التي أباحها ونص عليها القانون الدولي، والتي من شأنها أن تحمي المجتمع من أخطار تلك الهجمات الرقمية، والحفاظ على أمنها وسلامتها واستقرارها في هذا المجال، ولهذا تشخص العملية البحثية خياريين دوليين، الأول: التكيف القانوني للتحول السيبراني، والثاني: تشريع القوانيين السيبرانية لتنظيم العلاقات الدولية في الفضاء السيبراني، ولهذا اضحى الزام على الدول التي تريد أن تحافظ على أمنها واستقرارها وسيادتها، وتحمي مكتسباتها التنموية، وتحقق تقدمها في العالم الرقمي، أن تهتم اهتماماً حقيقياً بهذه بوسائل الحماية القانونية، وأن تتخذ جميع الإجراءات الضرورية لحماية المستخدمين للمعلومات والبيانات الإلكترونية من أخطار الحروب والنزاعات السيبرانية، لما لهذا الحيز من قدرة تأثيرية عالمية، وتناولت العملية البحثية الطبيعة القانونية للحروب والنزاعات الدولية في الفضاء السيبراني الذي يعد المجال الخامس لتفاعل الدول بعد مجال الأرض والبحر والجوي والفضاء، واستعراض قوانين الجرائم المعلوماتية، وقوانين الخصوصية الرقمية، وقوانين الفضاء السيبراني، وقياس مدى صلاحيتها لمواجهة جميع أنواع الحروب والنزاعات السيبرانية بين الدول، واستنتج البحث أن الإطار القانوني القائم في العالم الواقعي واجب التطبيق ويجب احترامه حتى في الفضاء السيبراني، فما من فراغ قانوني في الفضاء السيبراني.

الكلمات المفتاحية: الطبيعة القانونية، الحروب والنزاعات السيبرانية، الأمن السيبراني للدول، التكيف القانوني، الدول، القانون الدولي.

Abstract

The research focuses on the legal nature of cyber wars and conflicts from the perspective of international law and an explanation of the types of cyber wars and conflicts and means of protecting cyber security that would help prevent wars and conflicts between states, and prevent violations of the digital space of states, and reviews the role of the United Nations in maintaining cyber peace and security, and ways Enhancing international security in its various dimensions, and mechanisms for protecting the vital installations of states from all aspects of the illegal use of communication and information technology. The research studies legal methods for resolving disputes, preventing aggression, and protecting cybersecurity from threats that developed countries consider aggression that is no different from aggression using military forces. From electronic risks that aim to threaten its security and

sovereignty, after the penetration of its confidential information systems, or the destruction of the system of values and morals in the international community by spreading ideas and beliefs contrary to what prevails, by applying the precautionary - preventive / proactive or punitive means that are permitted and stipulated by the law This is why the research process diagnoses two international options, the first: legal adaptation to cyber transformation, and the second: legislation of cyber laws to regulate international relations in cyberspace, and for this It has become obligatory for countries that want to preserve their security, stability, and sovereignty, protect their development gains, and achieve progress in the digital world, to pay real attention to these means of legal protection, and to take all necessary measures to protect users of electronic information and data from the dangers of wars and cyber conflicts, because of this. The space has a global influence, and the research process dealt with the legal nature of international wars and conflicts in cyberspace, which is the fifth field of interaction of states after the field of land, sea, air and space, reviewing information crime laws, digital privacy laws, and cyberspace laws, and measuring their suitability to confront all types of Cyber wars and conflicts between countries, and the research concluded that the existing legal framework in the real world is applicable and must be respected even in cyberspace, as there is no legal vacuum in cyberspace.**Keywords**: Legal Nature, Cyber Wars and Conflicts, Cyber security of states, Adaptation.

المقدمة

لا ينكر الدور الايجابي للتقدم التقني في مجال المعلومات الرقمية التي احدثتها الثورة التكنولوجية، لكن في الوقت ذاته هناك جانب سلبي في استخدام هذه التقنية، عن طريق الاستخدام غير المشروع والتي وصفت بإنها تهديد جديد للامن وسيادة الدول، إذ تطور تلك الهجمات الى حروب ونزاعات في الفضاء اليسيبراني، التي توصف بالحروب الصامته المهجنة، واهدافها ترصد وتضرب عبر الشبكات الالكترونية باستخدام اسلحة الالكترونية فالعالم الافتراضي هو الحيز الذي تحدث فيه الحروب والنزاعات، وما ان انتشرت تلك الظاهرة الرقمية حتى بدأت الدول تبحث في طريقة لتطبيق القوانين وتحميل المسؤولية الدولية لضمان الفضاء السيبراني الذي يعد نظام دولي الالكتروني فيه العلاقات الدولية والقوانيين الدولية والاقتصاد الرقمي والثقافة والقيم وغيرها من مظاهر النظام الدولي الواقعي، فمن يتسبب بأضرار سيبرانية يفترض أن يتحمل المسؤولية على غرار الذي يحدث ضرر دولي في النظام الدولي الواقعي، والعلمية البحثية تحاول البحث في امكانية وصحة تطبيق القانون الدولي والمسؤولية الدولية في العالم الرقمي، وهنا لا بد من عرض بعض متطلبات البحث العلمي وعلى النحو لاتي :

- **الاهمية:** حمل الموضوع اهميتين الاولى: علمية وهي أن هناك نقص علمي في مجالات الكتابات القانونية تقنن الفضاء السيبراني وتحل النزاعات وتوقف الحروب والهجمات السيبراني وتمنع انكشاف الدول امام تلك الخروقات التي تؤثر على العلاقات الدولية وتنتهك قواعدالقانون الدولي وتحفظ السلم والامن الدولي السيبراني، أما الاهمية العملية هي تطبيق القوانين الدولية على العالم السيبراني؛ كونه انعكاس للنظام الدولي، فهناك ضرورة لتطبيق القانون الدولي على العالم الرقمي وابتكار قوانين جديدة في الحالات النزاعية والحروب التي لا يوجد نص قانوني يحمها لحداثتها.
- **الاشكالية:** هي أن الفضاء السيبراني فاعلية كثيرين ومجهولي الهوية والانتماء مما يصعب تطبيق القوانين الدولية التي اولى اشخاصها الدولة واخرهم الفرد، وهنا يظهر تساؤل اساس هو: ما الطبيعة القانونية للحروب والنزاعات السيبرانية؟ وما مدى إمكانية تطبيق المسؤولية الدولية عن أضرار التي يخلفها الهجوم السيبراني؟
- **الفرضية:** بني البحث على فرضية "إن القوانين الدولية يمكن تطبيقها في الفضاء السيبراني، في حالات الحروب والنزاعات السيبرانية لحفظ السلم والامن الدوليين، فما من فراغ قانوني في الفضاء السيبراني".
- **الهدف:** التعريف بالقوانين الواجب تطبيقها في الحروب والنزاعات السيبرانية وقياس مدى صلاحية القوانين الدولية في العالم الرقمي، كما يكمن الهدف من الموضوع في تسليط الضوء على إمكانية المسؤولية الدولية عن الاضرار التي تخلفها النزاعات والحروب السيبرانية ومدى انطباق قواعد المسؤولية الدولية التقليدية عليها، في ضوء نتشارها نتيجة تزايد ارتباط العالم بالفضاء الاكتروني.
- **النطاق:** تحدد البحث على النحو الاتي :

١. **موضوعياً:** الحروب والنزعات السيبرنية .
٢. **شكلياً:** القوانين في الفضاء السيبراني.
٣. **زمانياً:** ما بعد ٢٠٠٣ وانتشار استخدام الفضاء السيبراني في الحروب والنزاعت الدولية.
٤. **مكانياً:** اتسع ليشمل الساحة الدولية الواقعية والسيبرانية .

• **المنهجية** : استخدمنا المنجان الوصفي والقانوني لوصف الحروب والنزاعات السيبرانية ومنظور القانون الدولي لها.

• **الهيكلية:** نقسم البحث المعنون "الطبيعة القانونية للحروب والنزاعات الدولية في الفضاء السيبراني" الى مبحثين الاول: ركز على الحروب والنزاعات السيبرانية والثاني اهتم بالقوانين التي تحد من الجرائم المعلوماتية، وقوانين الخصوصية الرقمية، وقوانين الفضاء السيبراني، والثاني اهتم بالتكيف القانوني وقياس مدى صلاحيتها لمواجهة جميع أنواع الحروب والنزاعات السيبرانية بين الدول وامكانية تقرير المسؤولية الدولية عن الاضرار الناجمة عن تلك الحروب والنزاعات، واستنتج البحث إن الإطار القانوني القائم في العالم الواقعي واجب التطبيق ويجب احترامه حتى في الفضاء السيبراني، فما من فراغ قانوني في الفضاء السيبراني.

المبحث الأول الحروب والنزاعات السيبرانية

عدّ الفضاء السيبراني مسرحاً للحروب والنزاعات مستغلين ثغرة عدم وجود نصوص في القانون الدولي تنظم ذلك الفضاء وازدادت الحاجة الى القوانين السيبرانية بعد تفاقم خطر تعرض البنية التحتية في النظام الدولي للمعلومات لهجوم إلالكتروني، فضالاً عن استخدامه من قبل أطراف فاعلة من غير الدول، خاصة المجاميع المسلحة والمافيات والتجارة الممنوعة وغيرها، ولهذا تتعرض الدول لمخاطر كبيرة في هذا الجانب في مجميع هياكلها المؤسساتية لاعتمادها على المنظومة الالكترونية، مما يمس أمنها وسيادتها ويؤثر على مصالحها.إن افتراض "الحروب والنزاعات السيبرانية توجد قوانين تجرمها وتحمل مرتكبيها المسؤولية الدولية"، فتراض بحاجة الى تحقق كون القوانين الدولية تحدثت عن الحروب والنزاعات التقليدية الواقعية بانواعها ومواقع حدوثها برياً وبحرياً وجوياً والفضاء الخارجي لكن الحيز الخامس(الجو ، البر، البحر، الفضاء الكوني، الفضاء السيبراني) لم يكن ضمن تلك القوانين، وازداد الامر تعقيداً بعد ظهور فريق ينكر صلاحية القانون الدولي في الفضاء السيبراني، وعدم جواز التكييف القانوني للهجمات السيبرانية، ونعرض ذلك على النحو الاتي:

المطلب الأول الوصف الدلالي للحروب والنزاعات السيبرانية

لعل الجميع يلحظ إن كثيرا ما نتشرت مصطلحات وقوانين لم تكن موجودة سابقا في القرن الحادي والعشرين، مثل قوانين الجرائم المعلوماتية، قوانين الخصوصية الرقمية، قوانين الفضاء السيبراني، ويصاحبها مفاهيم جديدة مثل مفهوم الحوكمة السيبرانية والفضاء السيبراني والعلاقات الدولية السيبرانية والتجارة والاستثمار عبر الانترنيت [١].وذا ما تجذرنا أصل كلمة سايبر (*cyber*) تعود الى اليونان(Kybernetes) والتي جاءت بمعنى التحكم عن بعد [٢]، ثم بدأ يشار إلى قانون الأمن السيبراني أو قانون تكنولوجيا المعلومات باسم قانون الإنترنت، وهذا يعني أنه يمكن تعريف قانون الأمن السيبراني بأنه نظام قانوني مصمم للتعامل مع الإنترنت والحوسبة والفضاء السيبراني والقضايا القانونية ذات الصلة، بمعنى اخر، الوصف الملائم لقانون الإنترنت هي: إيجاد "قوانين ورقية" لتنظم "العالم اللاورقي".دون شك، إن العالم بعد فايروس كورونا انتقل نقلة نوعية باتجاه الفضاء السيبرانية ترافق معه ارتفاع في حجم النزاعات والحروب السيبرانية، وبدأ الباحثين والمختصين والمهتمين يبحثون عن وصف متفق عن الحروب والنزاعات السيبرانية بين فقهاء القانون الدولي فعرفها جانب من الفقه على أنها عملية استغلال متعمد لأنظمة شبكات الأنترنيت لارسال برامج ضارة[٣]، كما وصفت على أنها سلوك عدواني الالكتروني بقصد الحاق الاذى بالاخرين[٤]، ووصفت على أنها تلك الاجراءات التي تتخذها الدولة من أجل الهجوم على النظم المعلوماتية للعدو بهدف التأثير فيها والدفاع عن نظم الـمعلومات الخاصة بالدولة المهاجمة [٥]وهنا نلمس مقاربة بين الهجوم السيبراني والهجوم العادي في أن الـقائم بكـلا الهجومين له دافع للقيام بالهجوم، وضحية ممكن أن يكون شخص طبيعي أو معنوي، أما لاختلاف بينهما يظهر في أداة الهجوم ومكان الهجوم، ففي الهجوم السيبراني الاداة تكون ذات تقنية عالية، والمكان الذي انطلق منه الهجوم لا يتطلب انتقال فاعله انتقال جسمانياً؛ لـأنه يتم عن بعد بواسطة خطوط وشبكات الاتصال بين المهاجم ومكان الهجوم، لا تنفذ هجمات السيبرانية من أشخاص عاديين، بل يتم تنفيذها من مجموعة من محترفي اختراق الحاسبات عن طريق الشبكات الالكترونية يشكلون جيشاً سيبرانياً [٦].ومن الواضح إن من مسببات الحروب والنزاعات السيبرانية ضعف الامن السيبراني للدول، وظهور فواعل من غير الدول كثيرة في العالم السيبراني لا يمكن السيطرة عليهم او فرض القوانين عليهم بسهولة، لاسيما مع امتلاكهم قدرات تقنية تفوق الحكومات، فالتهديد العالي مقابل الامن الضعيف يكون فرصة سانحة للاختراق العداوني السيبراني [٧].

المطلب الثاني النزاعات والحروب السيبرانية وانعكاساتها على السلم والامن الدوليين

دون شك، إن انتشار الهجمات السيبرانية الضارة والمدمرة بعد ٢٠١١ دولياً يعود الى ضعف المنظومات الامنية السيبرانية في دول العالم؛ الأمر الذي جعل تهديد السلم والأمن الدوليين مر وارد دائماً، إذ ظهرت هذه الهجمات في حالات عديدة منها ثورات التغيير العربية (الربيع العربي) استونيا و ايران واتضحت اكثر في الحرب الروسية – الأوكرانية، فضلاً عن تسريبات أوراق بنما، وواقعة اختراق وكالة أبحاث الإنترنت الروسية،

إلى جانب نشر وسائل الإعلام تفاصيل منزل الرئيس الروسي فلادمير بوتين، مع توسع هذه الهجمات، بدا التساؤل المطروح، لماذا لا يوجد نظام مساءلة ومحاسبة دولي للحد من هذه الهجمات السيبرانية؟لذلك، تكمن اهمية القوانين السيبرانية في إنها؛ تفرض إجراءات للاستخدام وتقيس وردود الفعل العام في الفضاء السيبراني، وترتفع نسبة الامان والحماية للمعاملات التي تجرى عبر الإنترنت، وتخضع جميع الأنشطة عبر الإنترنت للمراقبة من قبل مسؤولي القانون السيبراني، وتوفير الحماية لجميع البيانات والممتلكات الخاصة بالأفراد والمنظمات والحكومة، ويساعد في الحد من الأنشطة السيبرانية غير القانونية عن طريق بذل الرقابة والعناية الواجبة من قبل مؤسسات الدولة المختصة، وردود الفعل التي يتم قياسها على أي فضاء إلكتروني لها زاوية قانونية مرتبطة بها تختلف باختلاف توجهها، سواء كان يتعلق بالتجارة أو بالخدمات أم الامن بمختلف انواعه، ووجود قوانين سيبرانية يعني وجود اتفاقيات دولية في هذا المجال مما يتيح تتبع جميع السجلات الإلكترونية عن طريق تحقيق التعاون الدولي لتتبع الجرائم المنظمة، ويساعد على إنشاء الحوكمة الإلكترونية والتي بدورها ترفع جودة حياة المستفيدين من خدمات الحكومة الالكترونية[٨].مما لايمكن نكرانه هو الآثار الناجمة عن النزاعات و الحرب السيبرانية ومن عواقب وخيمة على المدنيينفهناك ضرورة لتطبيق القانون الدولي على العمليات السيبرانية في النزاعات المسلحة والحروب، لوجود ضرر على المؤسسات والافراد وانتهاك للامن وسيادة الدول[٩].وهنا نستذكر "مبدأ التمييز وحظر الهجمات العشوائية وغير المتناسبة"، يتطلب مبدأ التمييز أن تميز أطراف النزاعات دوماً بين المدنيين والمقاتلين، وبين الأهداف المدنية والأهداف العسكرية، ففي اطار تطبيق مبدأ التميز على الهجمات السيبرانية اشار دليل تالين، بالرغم من عدم الزامية قواعده، بأنه لا يجوز أن تكون الاعيان المدنية هدفاً للهجمات السيبرانية، فلا يجوز على سبيل المثال توجيه الهجمات السيبرانية التي من شأنها تدمير الأنظمة المدنية والبنية التحتية، ما لم تعج هذه الأنظمة من قبيل الأهداف العسكرية التي يجوز استهدافها وفقاً للظروف السائدة[١٠]وبما إن الفضاء السيبراني يتألف من عدد لا يُحصى من نظم الحواسيب المتصلة ببعضها البعض في أرجاء العالم وغالباً ما يبدو أن نظم الحواسيب العسكرية تتصل بالنظم التجارية والمدنية وتعتمد عليها كلياً أو جزئيا، ومن ثم، يكون فعلاً من المستحيل شنّ هجوم سيبراني على بنية تحتية عسكرية وجعل الآثار تقتصر على هدف عسكري فحسب، وعلى سبيل المثال، من شأن استخدام دودة تتكاثر ولا يمكن السيطرة عليها و تتسبب بأضرار كبيرة في بنية تحتية مدنية أن يشكل انتهاكاً للقانون الدولي الإنساني ،يعد تطبيق مبدأ وجوب التمييز بين المقاتلين والمدنيين على الهجمات السيبرانية مسألة في غاية التعقيد على عكس الهجمات التقليدية إذ سيكون المهاجم في الأغلب بعيداً عن المكان المئات من الكيلومترات، ما يعني أن التمييز بين تتجاوز المستهدف من الهجوم ولمسافة ربما المقاتلين والمدنيين هو أمر صعب إذا لم يكن مستحيال، كما أن مسألة التمييز بين الأهداف، إذ يعد التميز بين الاهداف المدنية والعسكرية في الهجمات السيبرانية صعبة، خاصة أن نظم الحواسيب العسكرية غالب ما تتصل بالنظم التجارية والمدنية وتعتمد عليها كليا أو جزئيا، بل وربما يكون هناك تداخل بين الاستخدامات المدنية والعسكرية بارتباطهما بشبكة واحدة ووسيط واحد هو الفضاء السيبراني، ومن ثم يكون من المستحيل شن هجوم سيبراني على بنى تحتية عسكرية وجعل آثارها تقتصر على هدف عسكري فقط دون الأضرار بالمدنيين والمنشآت المدنية[١١].

المبحث الثاني موقف المنظمات الدولية من الحروب والنزاعات السيبرانية

إن البحث في امكانية تطبيق قواعد القانون الدولي على الحرب السيبرانية يستلزم ابتداءً التكييف القانوني لتلك المسألة من حيث شرعية وعدم شرعية الحرب السيبرانية في ضوء استخدام القوة في العلاقات الدولية، فالعلاقة بين حق اللجوء إلى الحرب وقانون الحرب تتسم بأنها علاقة توتر لا بد منه، فالقواعد المعاصرة للقانون الدولي تحظر استخدام القوة، بأستثناء حق الدول فرادى أو جماعات في الدفاع عن إما، أو بمقتضى استخدام تدابير انفاذ القانون التي يتخذها مجلس الأمن، هذا الامر يتطلب موقف للمنظمات الدولية مثل الامم المتحدة لتطبيق القانون الدولي على مرتكبي السلوك العدواني السيبراني ونبين ذلك وعلى النحو الاتي:

المطلب الأول دور الامم المتحدة في تقنين الفضاء السيبراني

ما إن بلغ عدد سكان العالم (٧.٩) مليار نسمة حسب إحصائيات الأمم المتحدة وأكثر من نصف هذا العدد يستخدم الانترنت، ليس ذلك فحسب، بل إن محرك كوكل وحده يستقبل يوميا (٣.٥) مليار بحث في المتوسط، وعدد الأجهزة المتصلة بالانترنت يتوقع أن يبلغ (٥٠) مليار جهاز في سنوات قليلة، أضف إلى ذلك أن منصة فيسبوك يستخدمها في الشهر أكثر من(٢.٩) مليار مستخدم وفي اليوم أكثر من (١.٩) مليار شخص، حتى ازدات الاهجمات ولنزاعات والحروب السيبرانية والاعمال العدوانية الاخرى من الكراهية والابتزاز والتجارة الالكترونية غير المشروعة في الفضاء السيبراني[١٢]مما دعى منظمة الأمم المتحدة في عام ٢٠١٥ لوضع معايير محددة لمواجهة الهجمات السيبرانية، وتم الاتفاق عليها في عام ٢٠٢١ بالإجماع من قبل جميع أعضاء دول منظمة الأمم المتحدة، من أجل وضع إطار ملزم سياسياً لجميع الدول التي تستخدم الفضاء الإلكتروني، من ضمن هذه المعايير أن تتعهد الدول بمنع استخدام شبكات الإنترنت في الأعمال التي تهدد أو تضر بالسلم والأمن الدوليين، وعدم السماح عن

قصد باستخدام أراضيها في أفعال غير مشروعة.وأظهرت التجربة الدولية أن الاتفاق على المعايير والقواعد السيبرانية الدولية لا يكفي في حد ذاته لتحقيق الأمن السيبراني، بل يجب تطوير استراتيجية دبلوماسية جماعية لمراقبة تنفيذ هذه المعايير، وفرض العقوبات عند تجاوزها، وهذا يتطلب حراك في السياسة الدولية لتفعيل النظام القانوني في الفضاء السيبراني.ومن أوجه القصور في المعايير التي وافقت عليها الأمم المتحدة هو افتقارها إلى القدرة على المساءلة عن الهجمات السيبرانية الإضارة–لخبيثة، فمن الناحية النظرية، يعد اتخاذ أي إجراء فعلي مسؤولية المجتمع الدولي الذي يعمل عن طريق مجلس الأمن التابع للأمم المتحدة.ولكن الواقع يشير إلى إن التوصل إلى اتفاق داخل الأمم المتحدة لمواجهة الأنشطة الإلكترونية غير القانونية والتي تنافي الشرعية الدولية والتي توصف بالعدوانية أمراً محدوداً للغاية، وذلك لأن المجتمع الدولي يتحرك فقط عندما تستخدم القوة، وهو أمر غير متوفر في الهجمات الإلكترونية، فلم يحدث أن تسبب هجوم إلكتروني في وفاة أحد الأشخاص.لهذا السبب، لم تُطرح قضية الأمن السيبرانيي أمام مجلس الأمن الدولي حتى عام ٢٠٢٠، مما يجعلها قضية غير خطيرة في رأى معظم الدول الأعضاء غير المُشاركة بشكلٍ مباشر في الصراع السيبرانيي، لكن هذا الوضع بدأ يتغير مع زيادة مخاطر الأنشطة الإلكترونية غير المشروعة، وتزايد الاعتماد على الشبكات العالمية، وتطور المنافسة بين القوى العظمى، وللتغلب على هذه المشكلة، يرى القائمون على الامم المتحدة ضرورة القيام ببعض الإجراءات المتسقة مع القانون الدولي والمعايير المتفق عليها، من أجل خلق المساءلة الدولية لمواجهة الهجمات الإلكترونية؛ كونها قضايا خطيرة [١٣]والإشكالية هي إسناد قضايا الأمن السيبراني لكيان مستقل تابع لجهة خارجية لن يحظى بالدعم الدولي، إذ أظهرت المناقشات في هذا الخصوص صعوبة التحقيق مع قوى إلكترونية كبرى مثل، الصين أو الولايات المتحدة الامريكية لكنها مع ذلك أبدت استعدادها للتحقيق مع عدد قليل من الدول الضعيفة، مثل كوريا الشمالية أو مع مجرمي الإنترنت، إذا كان من الممكن تحديد أنهم لا يتصرفون بصفة وكيل لدولة ما، فمن ضمن التحديات التي تواجه المعايير المقدمة عام ٢٠١٥ أنها تدعو جميع الدول للمشاركة في التحقيق اللازم لتوضيح ملابسات الهجوم الإلكتروني، مما يجعل الإسناد مهمة معقدة، لأنه في حالة وقوع حادث إلكتروني سيتطلب من الدول الإفصاح عن جميع المعلومات ذات الصِلة بالحادث، ومن المتوقع أن تعترض الدول على هذا التدخل، فالإقتراح الروسي الذي قدم ينص على أن تكون هناك حدود للاعتراضات المحتملة من الدول المعنية في حالة إسناد حادث إلكتروني إلى دولة بعينها أو توجيه الاتهام لها، وبالطبع، ستنكر الصين وروسيا (أو على الأرجح أي قوة إلكترونية) الاتهام لكن الهدف ليس إقناعهما بقبول الاتهام وإنما إقناع القادة الوطنيين والجمهور العالمي، أما فيما يتعلق بالشركات الخاصة مثل شركات FireEye أو Cloudstrike، فلديها حالياً قدرة على كشف مصدر الهجوم السيبراني العدائي، لكن هذا التقدم في تحديد المصدر غير معترف به في المجتمع الدولي، فلا يوجد اتفاق حول مستوى الإسناد المطلوب للعمل التعاوني بين الدول[١٤].ويحظى هذا الاستنتاج بدعم قوي في فتوى محكمة العدل الدولية بعنوان "مشروعية التهديد بالاسلحة النووية أواستخدامها"، حيث أشارت المحكمة إلى أن المبادئ والقواعد الثابتة للقانون الدولي الانساني السارية في النزاعات المسلحة تنطبق "على كافة أشكال الحرب وعلى كافة أنواع وتر اللجنة الدولية أن هذا الاستنتاج ينطبق على استخدام العمليات السيبرانية اثناء النزاعات المسلحة [١٥].لهذا يجب على الطرف المسؤول عن هجوم ما اتخاذ التدابير، إلى أقصى قدر ممكن، من أجل تفادي أو تخفيف الضرر العرضي الذي يلحق بالبنية التحتية المدينة أو يؤذي المدنيين. وهذا سيتطلب التحقق من طبيعة النظم التي تتعرض للهجوم والأضرار المحتملة التي تنجم عن أحد الهجمات، وهذا يعني أنه عندما يصبح جلياً أن هجوماً سيتسبب بإصابات أو أضرار مدنية عرضية، يجب إلغاؤه.علاوة على ذلك، يجب على أطراف النزاعات أن تلتزم باتخاذ الاحتياطات اللازمة من آثار الهجمات، ونتيجة لذلك، تكون النصيحة الموجهة إلى هذه الأطراف هي تقييم ما إذا كانت نظم الحواسيب العسكرية منفصلة بما يكفي عن تلك المدنية، بغية حماية السكان المدنيين من آثار الهجمات العرضية، ويُمكن للاعتماد على نظم الحواسيب العسكرية والتوصيل بين نظم الحواسيب التي يديرها متعاقدون مدنييون وتُستخدم أيضاً لأغراض مدنية أن يثير القلق.وعلى صعيد آخر، قد تساهم تكنولوجيا المعلومات أيضاً في الحد من الأضرار العرضية التي تلحق بالمدنيين أو البنية التحتية المدنية، وعلى سبيل المثال، يلحق تعطيل خدمات معينة تُستخدم لأغراض عسكرية ومدنية أضراراً أقل مما يُلحق تدمير البنية التحتية تماما، وفي هذه الحالات، يفرض مبدأ الاحتياط القابل للجدل التزاماً على الدول باختيار الوسائل الأقل ضرراً بغية تحقيق أهدافها العسكرية، وفي الحالات التي لا تشملها القواعد الحالية للقانون الدولي الإنساني، يظل المدنيون والمقاتلون محميين بما يسمى"شرط مارتنز"، مما يعني أنهم يظلون تحت حماية وسلطان مبادئ القانون القانون الدولي كما استقر بها العرف، و مبادئ الإنسانية، وما يمليه الضمير العام"[١٦]وشهدت هذه المرحلة بدايات ظهور الشبكة الدولية للمعلومات إذيرجع ضهورها لعام ١٩٩١ بجهود العالم البريطاني "تيم بيرنرز لي" اثناء عمله في المنظمة االوروبية للبحوث النووي[١٧]، وكان اول هجوم الكتروني ممكن أن يهدد الامن والسلم الدوليين في شهر ايار من عام ١٩٩٨ ، إذ قام به مجموعة قراصنة من الصين تطلق على نفسها "مركز الرد السريع للقراصنة الصينيين" مؤلف ٣٠٠٠ قرصان الكتروني بالهجوم على المواقع الالكترونية

الحكومية لأندنوسيا بسبب انتشار مظاهرات في ومن هذه الحادثة ادرك القائمون على منظمة الامم المتحدة الخطر الحقيقي لذي من الممكن أن تشكله إندونيسيا ضد الصين [١٨].وزداد الاهتمام الدولي بعد الطرح الروسي موضوع علاقة تطورات الانترنت بالأمن الدولي أمام الجمعية العامة عام ١٩٩٨ بطلب من قبل روسيا الاتحادية، إذ قررت الجمعية العامة أن تدرج في جدول اعمالها هذا الموضوع تحت عنوان "التطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الامن الدولي "وطلبت فيه من الدول ابداء آرائها [١٩].واستجابت الأمم المتحدة لذلك بإنشاء أول فريق خبراء عام ٢٠٠٤، واستمرت اجتماعاته لمدة تزيد عن السنتين بين عامي ٢٠٠٤ و ٢٠٠٥، إلا إنه لم يتوصل الى توافق بشأن المبادئ الواجب إتباعه الصعوبة الرقابة والتجريم في هذا المجا وعد اعارة الإهتمام الدولي الكافي له بوصفه لا يرتقي الا عدوإن أو تهديد حقيقي[٢٠]، إلا إن عامي ٢٠٠٦ –٢٠٠٧ شهدت تزايد الهجمات السيبرانية كان أهمها في استونيا عام ٢٠٠٦ التي عطلت معظم مرافقها ونتيجة الدولة تلت ذلك حوادث مماثلة في جورجيا٢٠٠٨ وكانت الاتهامات موجهة الى روسيا لكنها دون اثبات[٢١]ولأضرار التي لحقت بإستونيا دفعها لطلب في عام ٢٠٠٧ من الامم المتحدة إدانة هذه الهجمات وإعطاء أهمية أكبر للقواعد التي تنظم السلوك السيبراني للدول[٢٢]، وفعلاً قررت الجمعية العامة انشاء فريق ثاني عام٢٠٠٩ يتكون منخمسة عشر عضوا١٥[٢٣]، وكلا الفريقين عقداجتماعات من ٢٠٠٩ الى ٢٠١٠ ثم تبعه فريق ثالث باشر بالعمل من ٢٠١٢ الى ٢٠١٣ مطولة وتفصيلية من غير التوصل الى مبادئ عن السلوك السيبراني[٢٤] سوى الاشارة الى "ضرورة مواصلة الحوار لمناقشة المعايير المتعلقة باستخدام الدول لتكنولوجيا المعلومات والاتصالات" [٢٥]،استطاع التوصل الى مبادئ اولية لقواعد السلوك إلا إن الفريق الرابع الذي شكلته المنظمة عام٢٠١٤[٢٦]، وضح إن الدولة التي تقوم بعمل معادٍ تتحمل المسؤولية الدولية بعد اثبات قيامها بالفعل في الفضاء السيبراني، إذ نص التقرير للمرة الأولى إن القانون الدولي ينطبق على الفضاء السيبراني[٢٧]، وتشكل الفريق الخامس عام ٢٠١٦ يكمل عمل الفريق السابق[٢٨]، لكنه أعلن عدم استطاعته للتوصل الى توافق بشأن المبادئ الاولية للسلوك[٢٩]، أنشأت فريقاً سادساً على اساس التوزيع الجغرافي العادل للدول في٢ كانون الثاني٢٠١٩ وبعد اجتماعات لمدة سنتين وظهور بوادر توافق سياسي بين الدول الأطراف استطاع الفريق أن يصدر[٣٠].تقرير نهائي بالتوافق بين جميع اعضاءه وتضمن للمرة الأولى معايير السلوك المقبول في الفضاء السيبراني في ١٤ تموز عام ٢٠٢١ إلا إن هذه المرحلة شهدتً أنشاء فريق خبراء ثاني وباقتراح من روسيا الاتحادية، وأطلق عليه (الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق جميع أعضاء الجمعية العامة للامم المتحدة[٣١].ومن هنا نستنتج امكانية تطبيق المبادئ التقليدية على الفضاء السيبراني مثل (مبدأ احترام السيادة في الضاء السيبراني، ومبدأ عدم استخدام القوة في العلاقات الدولية السيبرانية، ومبدأ حل المنازعات السبرانية بالطرق السلمية، ومبدأ عدم التدخل في الشؤون الداخلية سيبرانياً، وضع قواعد تخص الفضاء السيبراني الدولي، مبدأ التعاون الدولي في الفضاء السيبراني، ومبدأ التحقيق في القضايا السيبرانية، ومبدأ احترام حقوق الانسان في المجال السيبراني.وتعليل ضرورة التطبيق ظهور وانتشار قواعد إقليمية منافسة للقانون الدولي العام لتنظيم القواعد السيبرانية اقليمياً، فهناك حالياً ثالث مجموعات للقواعد التي تنظم موضوع خضوع الانترنت مثل:

١. قواعد (Tallinn) للقانون الدولي في الفضاء السيبراني ٢٠١٧ والتي تتكون من (١٥٤) قاعدة قانونية[٣٢].
٢. قواعد باريس (Paris Call) لعام ٢٠١٨، تتكن من (٩) مبادئ لتنظيم الفضاء السيبراني ، انضمت لها (٨١) دولة[٣٣].
٣. واعد شنغهاي لعام ٢٠١٥ ، والذي اطلقته منظمة شنغهاي لتظيم العمل في الفضاء السيبراني[٣٤].

المطلب الثاني ضوابط المساءلة وتحميل المسؤولية

إن الإسناد هو الخطوة الأولى لتحقيق الأمن السيبراني، لكنه لا يكفي، فربما تعلم الامم المتحدة جيداً من هو المسؤول لكنها لا تتخذ أي إجراء فعلي، إذ يتطلب الأمر اتخاذ قرار عن طريق مجلس الامن وبطلب من الدولة المعتدى عليها، فيما يتعلق بالتدابير الحالية، فلا يمكن التغافل عن بعض الجهود الدولية المبذولة لتحقيق المساءلة، وتحديد شروط العمل الجماعي والاتفاق عليها، مثل، إطار الاستجابة الدبلوماسية السيبرانية في الاتحاد الأوروبي، والقانون الدولي للفضاء السيبراني، والالتزامات التعهدية الأخرى للدفاع الجماعي عن النفس، والبيان المشترك الصادر عن وزارة الخارجية الأمريكية في سبتمبر ٢٠١٩ بشأن تعزيز سلوك الدولة المسؤولة في الفضاء الإلكتروني، إذ اتفقت (٢٨) دولة على العمل معاً على أساس طوعي لمحاسبة الدول عندما تتصرف بشكلٍ مخالف عن طريق اتخاذ تدابير وفقاً لقانون الدولي، بهدف توسيع مراعاة معايير ٢٠١٥ وزيادة الأمن السيبراني، أضف لذلك إلى العقوبات من قبل الاتحاد الأوروبي أو لوائح الاتهام والعقوبات من قبل الولايات المتحدة الامريكية.إن التأكيد على إن القانون الدولي الإنساني بما في ذلك مبادئ التمييز والتناسب والاحتياط –ينطبق على العمليات السيبرانية اثناء النزاعات المسلحة بموجب أحكامه، ومنها :

١. يحظر استخدام القدرات السيبرانية العشوائية الطابع التي تصنف على أنها أسلحة.
٢. يحظر توجيه الهجمات المباشرة ضد المدنيين والاعيان المدنية، بما فيذلك عند استخدام وسائل أو أساليب الحرب السيبرانية.
٣. حظر أعمال العنف أو التهديد إلىً الرامية أساس بث الرعب بين السكان المدنيين، بما في ذلك عند ارتكابها عبر وسائل أو أساليب الحرب السيبرانية.
٤. حظر الهجمات العشوائية، أي الهجمات التي من شأنها أن تصيب الاهداف العسكرية والاشخاص المدنيين أو الاعيان المدنية دون تمييز، بما في ذلك عند استخدام وسائل أو أساليب الحرب السيبرانية.
٥. حظر الهجمات غير المتناسبة، بما في ذلك عند استخدام وسائل أو أساليب الحرب السيبرانية، الهجمات غير المتناسبة هي تلك التي توقع منهُ اي أن تسبب خسائر عرضية في أرواح المدنيين أو إصابة بهم أو بالاعيان أضرار المدنية أو أن دت امن هذه الخسائرً حدث خلط والاضرار، يفرط فيتجاوز ما ينتظر أن تسفر عنه تلك الهجمات من ميزة عسكرية ملموسة ومباشرة.
٦. حظر مهاجمة أو تدمير أو نقل أو تعطيل الاعيان التي لا غنى عنها لبقاء السكان المدنيين، بماُ في ذلك عند استخدام وسائل أو أساليب الحرب السيبرانية.
٧. يجب حماية الوحدات الطبية واحترامها، بما في ذلك عند تنفيذ العمليات السيبرانية اثناء النزاعات المسلحة.
بذل رعاية متواصلة في إدارة العملياتُ العسكرية، بما في ذلك عند استخدام وسائل أو أساليب الحرب السيبرانية، من أجل تفادي السكان المدنيين والاعيان المدنية؛ و تتخذ جميع الإحتياطات المستطاعة عند تنفيذ الهجمات من أجل تجنب إلحاق الضرر بالمدنيين، وذلك بصفة عرضية، بما في ذلك عند استخدام وسائل أو أساليب الحرب السيبرانية.

المطلب الثالث التكيف القانوني للنزاعات والحروب السيبرانية

انطلاقاً من مقولة كوردولا دروغيه المستشارة القانونية في اللجنة الدولية "ما من فراغ قانوني في الفضاء السيبراني"[٣٥]، ففي كل أرجاء العالم، ينظر واضعو السياسات والقادة العسكريون في تداعيات الحرب السيبرانية، وتشرح السيدة "كوردولا دروغيه" المستشارة القانونية في اللجنة الدولية أن الإطار القانوني القائم واجب التطبيق ويجب احترامه حتى في الفضاء السيبراني، اذ تصفه بالسلوك الالكتروني الذي يؤدي الى إحداث أثر في "العالم الحقيقي"، ولم يجرِ الاتفاق دولياً بالمثل على معنى قانوني لعبارات مثل "الهجمات السيبرانية" أو "العمليات السيبرانية" أو "الهجمات على شبكات الحواسيب"، التي يقصد بها الهجمات والنزاعات والحروب عبر الاجهزة الالكترونية[٣٦]وان من اخطر استعمالاتها ضد النزاع في كوسوفو١٩٩٩ من قبل حلف الشمال الاطلسي، وبعد استهداف طيران حلف شمال الأطلسي للسفارة الصينية في بلغراد، قام عددمن القراصنة الصينيين وكردة فعل بمهاجمة مواقع الكترونية رسمية منتخبة تابعة للولايات المتحدة الأمريكية، وبالذات الموقع الألكتروني للبيت الأبيض نجم عنها الاستحواذ على آلالف من البيانات الرقمية المنصفة آنذاك بأنها عالية السري[٣٧]وهناك الهجوم السيبراني الذي تعرض له المفاعل النووي الأمريكي "ديفيد بيس" لتوليد الطاقة الكهربائية في أوهايو في٢ جوان ٢٠٠٣ بفعل أنظمة اختراق وتعطيل لشبكات السيطرة والتحكم الالكترونية في المفاعل نفسه [٣٨].ومن المعروف إن القانون الدولي الإنساني لا ينطبق إلا إذا ارتكبت العمليات السيبرانية في سياق نزاع مسلح، أكان بين دول أم بين دول وجماعات مسلحة منظمة، أو بين جماعات مسلحة منظمة[٣٩]، وبالنتيجة، هناك حاجة إلى التمييز بين لمسألة العامة للأمن السيبراني وبين المسألة الخاصة بالعمليات السيبرانية في النزاع المسلح، ففي حالات النزاعات المسلحة، ينطبق القانون الدولي الإنساني عندما تلجأ الأطراف إلى أساليب الحرب ووسائلها التي تعتمد على عمليات سيبرانية[٤٠].إن استخدام العمليات السيبرانية أثناء النزاعات المسلحة حقيقة واقعة، فبينما أقر عدد ضئيل من الدول علانية بإجراء مثل هذه العمليات، مع تزايد عدد الدول التي تطور قدرات سيبرانية لاغراض عسكريةً فمن المرجع أن يزداد استخدامها مستقبلا.[٤١]وتُطور دوماً تكنولوجيات جديدة من كل الأنواع، والقانون الدولي الإنساني شامل بما يكفي ليتسع لهذه التطورات، غير أنه ينظم، عن طريق قواعده العامة، كلّ أساليب الحرب ووسائلها، بما فيها استخدام كلّ الأسلحة، ولا سيما أن المادة (٣٦) من الملحق (البروتوكول) الأول الإضافي لاتفاقيات جنيف تنص على ما يلي: "يلتزم أي طرف سام متعاقد، عند دراسة أو تطوير أو اقتناء سلاح جديد أو أداة للحرب أو اتباع أسلوب للحرب، بأن يتحقق مما إذا كان ذلك محظوراً في جميع الأحوال أو في بعضها بمقتضى هذا الملحق "البروتوكول" أو أية قاعدة أخرى من قواعد القانون الدولي التي يلتزم بها الطرف السامي المتعاقد"، وفي ما يتعدى نطاق الالتزام المحدد الذي تفرضه هذه القاعدة على الدول الأطراف، تبين أن القواعد العامة للقانون الدولي الإنساني تنطبق على التكنولوجيا الجديدة[٤٢].وهذا لا يعني أنه لا توجد حاجة إلى زيادة تطوير القانون في حين تتطور التكنولوجيات، أو أن آثارها الإنسانية مفهومة على نحو أفضل، ويجب أن تقرر الدول هذا الأمر، وان لم

تقرر بعد، فمن الضروري التشديد على أنه ما من فراغ قانوني في الفضاء السيبراني، وبعيداً عن ذلك[٤٣].غير أن الفواعل مجهولة الهوية تشكل جانباً من جوانب صعوبة تحميلاً المسؤولية في الفضاء السيبراني، ففي العمليات السيبرانية التي تحصل يومياً، جهل الهوية قاعدة وليس استثناء، ويتبين أنه من المستحيل في بعض الحالات إقتفاء أثر المصدر؛ كون الفاعل شخص فيطبق عليه القانون الدولي الإنساني ، او مؤسسة حكومية ليطبق القانون الدولي العام[٤٤].ويجدر التوضيح أن التأكيد على انطباق القانون الدولي الانساني على العمليات السيبرانية اثناء النزاعات المسلحة لا يضفي الشرعية على الحرب السيبرانية أو يشجع على عسكرة الفضاء السيبراني، في الواقع، يفرض القانون الدولي الإنساني بعض القيود على عسكرة الفضاء، وعلاوة على ذلك، يظل أي لجوء إلى القو من الدول السيبرانية عن طريق حظر تطوير القدرات السيبرانية العسكرية التي تنتهك القانون الدولي الإنساني ذات الطابع السيبراني أو الحركي محكوم بميثاق الامم المتحدة وقواعد القانون الدولي العرفي ذات الصلة، لا سيما حظر اللجوء للقوة، و يجب تسوية النزاعات الدولية بالوسائل السلمية، في الفضاءالسيبراني كما في جميع المجلات الاخرى[٤٥].وصدر تقرير فريق الخبراء عام ٢٠٢١ متضمناً مجموعة من المبادئ حول تطبيق القانون الدولي العام على العمليات التيتقوم بها الدول في الفضاء السيبراني، وكان لمنظمة الأمم المتحدة الدور الاساس في تشكيل الفريق والذي ساهم في اعداد هذه المبادئ، وهو ما يبين اهمية دور المنظمة في تكوين قواعد متكاملة لما يخص التهديدات التي فرضها الفضاء السيبراني على الامن والسلم الدوليين.

الخاتمة

وخلاصة لكل ما ورد اعلاه، نجد إن القانون الدولي لا ينطبق على معظمها، إذ لا ينطبق القانون الدولي العام إلّا على العمليات السيبرانية ا لتي تُنفذ في سياق حرب عدوانية تشنها دولة ضد دولة او مجموعة من الدولة بقصد الحاق الضر فيها وتدمير بناها التحتية ، وكذلك لا ينطبق ا لقانون الدولي الإنساني على معظم تلك الاعمال السيبرانية غير المشروعة، إذ لا ينطبق القانون الدولي الإنساني إلّا على العمليات السيبرانية ال تي تُنفذ في سياق نزاع مسلح، ومن المسلّم به أن مسألة انطباق القانون الدولي الإنساني على العمليات السيبرانية هي نقطة خلاف في النقا شات الجارية بتفويض من الأمم المتحدة في موضوع العمليات السيبرانية.

أظهرت الدراسة العديد من النتائج وأهمها :

١. القانون الدولي بفروعه يطبق على السلوك العدواني السيبراني كلاً حسب اختصاصه بشرط وجود دليل اثبات بشخصية مرتكب الجريمة شخص طبيعي (فرد) ام معنوي (كيان او مؤسسة رسمية)، فلا وجود لفراغ قانوني في الفضاء السيبراني.

٢. أن أغلب الدول تفتقد إلى وجود تشريعات تنظم عملا افرادها ومؤسساتها وسياساتها في الفضاء السيبراني وفي حال وجود قوانين فإنه يوجد ثغرات قانونية بهذا الخصوص.

٣. إن وضع الهجمات السيبرانية في الاطار القانوني الدولي القائم، أمر صعب جدا؛ وذلك بسبب الطبيعة الخاصة لها، إضافة إلى عدم وجود بيان قانوني رسمي ونهائي متفق عليه بشأن هذه الظاهرة للتسلح السيبراني والألكتروني بين الدول.

٤.يعد التكيف القانوني لتجريم العمليات السيبرانية العدوانية دولياً من الامور التي تحمل المسؤولية للدولة على ما تقوم به من هجمات سيبرانية تلحق أضرارا بدولة أخرى على الأعمال لسيبرانية التي تقوم بها الدولة .

٥. يعد الهجوم السيبراني استخداما للقوة غير مشروع نتيجة الآثار التي يخلفها مقارنة بالهجوم المسلح، وكالهما يحقق ذات النتيجة ويمكن أن تكون نتائج الهجوم السيبراني أكثر تدميرا وخطورة لذا فهو يرتقي إلى مستوى الهجوم التقليدي .

٦. إن الجرائم السيبرانية بوصفها جرائم عالمية عابرة للحدود لا تتحقق مكافحتها الا عن طريق التعاون الدولي على المستوى الإجرائي الجنائي.

واستناداً الى النتائج صحت فرضية البحث "إن القوانين الدولية يمكن تطبيقها في الفضاء السيبراني، في حالات الحروب والنزاعات السيبرانية لحفظ السلم والامن الدوليين، فما من فراغ قانوني في الفضاء السيبراني".

التوصيات:

وبناء على على ما جاء في البحث من محتوى وم اخرج فيه من نتاج نوصي:

١. ايجاد تشريع دولي باسم "القانون الدولي السيبراني" يطبق في حالات النزاعات والحروب بين الدول والافراد.

٢. ايجاد تشريعات وطنية تنظم عمل الافراد والمؤسسات الحكومية في الفضاء السيبرانية.

٣. تطوير البنية التشريعية الجنائية الوطنية، بما يتماشى مع الجهود الدولية في مكافحة الجرائم السيبرانية .

٤. تفعيل التعاون الدولي، ودور المعاهدات الدولية،ومبدأ المساعدة القانونية والقضائية والامنية المتبادلة في مجال مكافحة الجرائم السيبرانية.

٥. إنشاء شراكات بين القطاعين العام والخاص على المستوى الوطني والاقليمي والدولي لمكافحة الجرائم السيبرانية، وتبادل الخبرات، وتح سين طرق مكافحتها؛ بوصفها جرائم عابرة للحدود الوطنية قبل ان تطور الى نزاعات وحروب تخل بالسلم والامن الدوليين.

٦.تعزيز العمل والتعاون وتبادل المعلومات مع جميع المنظمات الدولية واللإقليمية ذات الصلة فيما يتعلق بالمبادرات المتصلة بالأمن السيبراني في مجالات اختصاصاتها،مع مراعاة احتياجات مساعدة البلدان النامية .

٧.تعيين نظام سريع وفعال للتعاون الدولية، والحفاظ بشكل سريع على البيانات المخزنة على أجهزة الكمبيوتر وحفظها والإفصاح الجزئي عن حركة هذه البيانات المخزنة على الكمبيوتر وتدريب الكوادر الوطنية في الاستثمار في الأمن الألكتروني وحماية البنية التحتية الرقميه بها.

٨. اتخاذ الاجراءات من قبل الدول لضمان حمايتها من الهجمات السيبرانية عن طريق تعزيز مختلف المؤسسات على كيفية التعامل مع الهجمات السيبرانية، و مواجهتها و الحد من تداعيتها وكذا نشر الوعي السيبراني في المجتمع، وبنأء المنظومة الامنية السيبرانية لضمان حمايها الامن والسيادة.

المصادر

اولاً: المصادر العربية:

ـالوثائق والمنشورات الدولية

١. اللجنة الدولية، القانون الدولي الانساني وتحديات النزاعات المسلحة المعاصرة ،٢٠١٥ .

٢. محكمة العدل الدولية، مشروعية التهديد بالأسلحة النووية أو استخدامها، فتوى،٨ تموز /يوليو ،١٩٩٦ الفقرة .٨٦

٣. المادة ١-٢، البروتوكول الاضافي الاول ،التفاقيات جنيف المؤرخ ٨ حزيران /يونيو ١٩٧٧؛ الفقرة ٩ من ديباجة اتفاقية الهاي الثانية لعام ١٨٩٩؛ والفقرة٨ من ديباجة اتفاقية الهاي الرابعة لعام .١٩٠٧

٤. المادة(٣٦) من الملحق (البروتوكول) الأول الإضافي لاتفاقيات جنيف.

٥. الفقرة (٤) من قرار الجمعية العامة لأمم المتحدة في ٦ كانون الثاني، ٢٠١٤ وثائق الامم المتحدة، الوثيقة (A/RES/68/243).

٦. الفقرة (٥) من تقرير الامين العام لأمم المتحدة في ١٤ اب٢٠١٧، وثائق الامم المتحدة، الوثيقة (A/72/327).

٧. الفقرة (٣)من قرار الجمعية العامة لأمم المتحدة في 2كانون الثاني٢٠١٩ وثائق الامم المتحدة، الوثيقة(A/RES/73/266).

٨. تقرير الخبراء المذكور في مذكرة الامين العام لـلأمم المتحدة في ١٤ تموز ، ٢٠٢١ وثائق الامم المتحدة، الوثيقة (A/76/135).

٩. قرار الجمعية العامة لألمم المتحدة في ٤ كانون الثاني ١٩٩٩، وثائق الامم المتحدة، الوثيقة (A/RES/53/70).

١٠. مذكرة الامين العام للامم المتحدة في ٥ اب ٢٠٠٥ ،وثائق الامم المتحدة، الوثيقة (A/60/202) .

١١. قرار الجمعية العامة لألمم المتحدة في ٦ كانون الثاني٢٠٠٦، وثائق الامم المتحدة، الوثيقة (A/RES/60/45).

١٢. قرار الجمعية العامة لألمم المتحدة في ١٣ كانون الاول، ٢٠١١ وثائق الامم المتحدة، الوثيقة (A/RES/66/24).

١٣. قرار الجمعية العامة لـلأمم المتحدة في ٣٠ كانون الثاني٢٠١٥ ،وثائق الامم المتحدة، الوثيقة (A/RES/70/237).

١٤. مذكرة الامين العام لـلأمم المتحدة، في ٣٠ تموز ،٢٠١٠ وثائق الامم المتحدة، الوثيقة (A/65/201).

١٥. مذكرة الامين العام لأمم المتحدة في ٢٢ تموز ،٢٠١٥ وثائق الامم المتحدة، الوثيقة(A/70/174).

ـالكتب:

١. عادل عبد الصادق، أسلحة الفضاء الألكتروني في ضوء القانون الدولي الإنساني، مكتبة المستقبلية، مصر، ٢٠١٦ .

٢.هنكرتس ودوزوالد –بك، القانون الدولي الانساني العرفي، المجلد الاول، القواعد، اللجنة الدولية، مطبعة جامعة كامبريدج، كامبريدج، ٢٠٠٥.

ـالمجلات والدراسات

١.احمد عبيس نعمة الفتلاوي، الهجمات السيبرانية :مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحق ق الحلي للعلوم القانونية والسياسية، جامعة بابل ، كلية القانون، العدد ٤، السنة الثامنة، ٢٠١٦.

٢.رزق أحمدسمودي، ٢٠١٨، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية ، ديسمبر ٢٠١٨.

٣.مايكل شميت، الحرب بواسطة شبكات االتصال :الهجوم على شبكات الكومبيوتر (الحاسوب) والقانون في الحرب، المجلة الدولية للصليب الأحمر،عدد ٢٠٠٢،٨٦٤.

الانترنيت

١.السيد محمد السيد احمد، القانون في الفضاء السيبراني، المنصة القانونية مقال منشور في ٧/ ٦/ ٢٠٢٢ ، اطلع عليه في ٨/ ٨/ ٢٠٢٣، على الرابط :http://www.sajplus.com

٢.كوردولا دروغيه ، ما من فراغ قانوني في الفضاء السيبراني، اللجنة الدولية للصليب الاحمر ، مقابلة اجريت بتاريخ ٢٠١١/٨/١٦ مقابلة اطلع عليها في ٢٠٢٣/٨/٧، على الرابط: https://www.icrc.org/ar/doc/resources/documents/interview/٢٠١١/cyber-warfare-interview

٣. الهجمات السيبرانية وحالات التعاون ضدها ، الامم المتحدة ، على الرابط :

https://news.un.org/en/story/2007/09/232832-estonia-urges-un-member-states cooperate-against-cyber-crimes

ثانياً: المصادر الاجنبية:

-Books

1. Gerard O'Regan, Introduction to the History of Computing a Computing History Primer, Springer International Publishing, Switzerland, 2016.
2. Jeffrey Carr, Inside Cyber Warfare, O'Reilly Media Inc, United States of America, 2012.
3. Michael N.Schmit, (Tallinn manual on the international law applicable to cyber warfare), Cambridge university press, first publishes, 2013.
4. Tallinn manual 2.0 on the international law applicable to cyber operations, Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, 2017.

Journals - Studies

1. Andreea bendovschi, cyber -attacks - trends, patterns and security counter measures, procedia economics and finance, Elsevier, Vol .28,2015.
2. Andrzej Kozlowski, Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan, European Scientific Journal /Special edition Vol.3 No.1,February 2014.
3. Brent Kesler, 2011,the vulnerability of Nuclear Facilities to Cyber Attack, Strategic Insight Journal, Vol.10, No. 01. 2011.
4. Danielle Flonk, Emerging illiberal norms: Russia and China as promoters of internet content control, International Affairs Vol. 97, No.2, 2021.
5. Herbert Lin, Cyber conflict and international humanitarian law International review of the red cross, Vol. 94, No.886 ,2012.
6. Herbert Lin, Cyber conflict and international humanitarian law, International Review of the red cross, Vol .94,No. 886 , 2012.
7. James Andrew Lewis, Creating Accountability for Global Cyber Norms, Center for Strategic and International Studies (CSIS), February ٢٣ ,2022.
8. Jeffrey T. G Kelsey, Hacking in to international humanitarian law: The principles of distinction and neutrality in the age of cyber warfare, Michigan law review, Vol. 106, No.7,2008, .
9. Junaidu Bello Marshall, Cyber attacks (the legal response, International journal of international law) , Vol. 1 , No. 2 , universal multidisciplinary research institute , India , 2000.
10. Michael N. Schmitt & Jeffery S. Thumher, Autonomous weapon systems and the law of armed conflict, Harvard notional security journal,No.231,May 22, 2013
11. Priyanka R. Dev,2015, (Use of Force and Armed Attack) Thresholds in Cyber Conflict; The Looming Definitional Gaps and the Growing Need for Formal U.N. Response), Texas International Law Journal Vol. 50, No. 2, 2015 .

10.Schmitt, M.N,(computer network attack and the use force in international law through on normative), the Colombia journal of transitional law, Vol.27,No. 885,1999.

11. Thomas W. Smith , The New Law of War: Legitimizing Hi-Tech and Infrastructural , International Studies Quarterly, Vol. 46. , 2002.

-Phd Thesis

1. Heather Harrison Dinniss, The status and use of computer network attacks in international law, Phd thesis, London school of a economics and Political science, 2008.

-Internet

1. The Potential Human Cost of Cyber Operations ,2019 , https://www.icrc.org/en/download/file/96008/the-potential-human-cost-of-cyber-operations.pdf
2. Paris Call ,Trust and Security in Cyberspace of 12 November 2018, https://pariscall.international/en/2018

هوامش البحث

(١)Andreea bendovschi, cyber -attacks - trends, patterns and security counter measures, procedia economics and finance, Elsevier, Vol .28,2015, p. 3.

(٢) احمد عبيس نعمة الفتلاوي، الهجمات السيبرانية :مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، جامعة بابل ، كلية القانون، العدد ٤، السنة الثامنة، ٢٠١٦، ٦١٤..

(٣) Junaidu Bello Marshall, Cyber attacks (the legal response, International journal of international law) , Vol. 1 , No. 2 , universal multidisciplinary research institute , India , 2000, p. 3.

(٤) Michael N.Schmit, (Tallinn manual on the international law applicable to cyber warfare), Cambridge university press, first publishes, 2013, p. 92.

(٥) Schmitt, M.N,(computer network attack and the use force in international law through on normative), the Colombia journal of transitional law, Vol.27,No. 885,1999, p. 07.

(٦) Heather Harrison Dinniss, The status and use of computer network attacks in international law, Phd thesis, London school of a economics and Political science, 2008, p. 33.

(٧) Jeffrey T. G Kelsey, Hacking in to international humanitarian law: The principles of distinction and neutrality in the age of cyber warfare, Michigan law review, 2008, Vol. 106, No.7, p.1437.

(٨) Herbert Lin, Cyber conflict and international humanitarian law International review of the red cross, 2012, Vol. 94, N886, p.515.

(٩) رزق أحمدسمودي، ديسمبر ٢٠١٨، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية ، ٢٠١٨، ص ٣٣٨ .

(١٠) مايكل شميت، الحرب بواسطة شبكات االتصال :الهجوم على شبكات الكومبيوتر (الحاسوب)والقانون في الحرب، المجلة الدولية للصليب الأحمر، ٢٠١٢، ص٩١٥.

(١١) إن قيام المسؤولية الموضوعية تشترط وجود علاقة سببية بين النشاط الخطر و الاضرار الناتجة عنها، عادل عبد الصادق، أسلحة الفضاء الألكتروني في ضوء القانون الدولي الإنساني، مكتبة المستقبلية، مصر، ٢٠١٦، ص٩٦.

(١٢) السيد محمد السيد احمد،القانون في الفضاء السيبراني، المنصة القانونية مقال منشور في ٧/ ٦/ ٢٠٢٢، اطلع عليه في ٨/ ٨/ ٢٠٢٣، على الرابط :http://www.sajplus.com

(١٣) James Andrew Lewis, Creating Accountability for Global Cyber Norms, Center for Strategic and International Studies (CSIS), February ٢٣ ,2022,p1-5.

(١٤) ,Op.Cit,p5-8.James Andrew Lewis, Creating Accountability for Global Cyber Norms

(١٥) محكمة العدل الدولية، مشروعية التهديد بالأسلحة النووية أو استخدامها، فتوى،٨ تموز /يوليو ١٩٩٦، الفقرة٨٦.

(١٦) المادة ١-٢، البروتوكول الاضافي الاول ،التفاقيات جنيف المؤرخ ٨ حزيران /يونيو ١٩٧٧؛ الفقرة ٩ من ديباجة اتفاقية الهاي الثانية لعام ١٨٩٩؛ والفقرة ٨ من ديباجة اتفاقية الهاي الرابعة لعام ١٩٠٧.

(١٧) Gerard O'Regan, Introduction to the History of Computing a Computing History Primer, Springer International Publishing, Switzerland, 2016, p.163.

(١٨) Jeffrey Carr, Inside Cyber Warfare, O'Reilly Media Inc, United States of America, 2012, p.2.

(١٩) قرار الجمعية العامة لألمم المتحدة في ٤ كانون الثاني ١٩٩٩، وثائق الامم المتحدة، الوثيقة (A/RES/53/70).

(٢٠) مذكرة الامين العام للامم المتحدة في ٥ اب ٢٠٠٥ ،وثائق الامم المتحدة، الوثيقة (A/60/202) .

(٢١) Andrzej Kozlowski, Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan, European Scientific Journal February 2014 /Special edition Vol.3 ISSN, pp.238,239.

(٢٢) الهجمات السيبرانية وحالات التعاون ضدها ، الامم المتحدة ، على الرابط :
https://news.un.org/en/story/2007/09/232832-estonia-urges-un-member-states cooperate-against-cyber-crimes

(٢٣) قرار الجمعية العامة لألمم المتحدة في ٦ كانون الثاني٢٠٠٦، وثائق الامم المتحدة، الوثيقة (A/RES/60/45).

(٢٤) قرار الجمعية العامة لألمم المتحدة في ١٣ كانون الاول، ٢٠١١ وثائق الامم المتحدة، الوثيقة (A/RES/66/24).

(٢٥) مذكرة الامين العام لألمم المتحدة، في٣٠ تموز ،٢٠١٠ وثائق الامم المتحدة، الوثيقة (A/65/201).

(٢٦) الفقرة (٤) من قرار الجمعية العامةلألمم المتحدة في ٦ كانون الثاني، ٢٠١٤ وثائق الامم المتحدة، الوثيقة (A/RES/68/243).

(٢٧) مذكرة الامين العام لـلأمم المتحدة في ٢٢ تموز ،٢٠١٥ وثائق الامم المتحدة، الوثيقة(A/70/174).
(٢٨) قرار الجمعية العامة لـلأمم المتحدة في ٣٠ كانون الثاني٢٠١٥ ،وثائق الامم المتحدة، الوثيقة (A/RES/70/237).
(٢٩) الفقرة(٥) من تقرير الامين العام لـلأمم المتحدة في ١٤ اب٢٠١٧ ،وثائق الامم المتحدة، الوثيقة (A/72/327).
(٣٠) الفقرة (٣)من قرار الجمعية العامة لـلأمم المتحدة في ٢ كانون الثاني٢٠١٩ وثائق الامم المتحدة، الوثيقة (A/RES/73/266).
(٣١) تقرير الخبراء المذكور في مذكرة االمين العام لـلأمم المتحدة في ١٤ تموز ، 2021وثائق الامم المتحدة، الوثيقة (A/76/135).
(٣٢) Tallinn manual 2.0 on the international law applicable to cyber operations, Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, 2017, p.3.
(٣٣) Paris Call ,Trust and Security in Cyberspace of 12 November 2018, https://pariscall.international/en/2018
(٣٤) Danielle Flonk, Emerging illiberal norms: Russia and China as promoters of internet content control, International Affairs Vol 97, No:2, 2021, p.1931.
(٣٥) كوردولا دروغيه ، ما من فراغ قانوني في الفضاء السيبراني، اللجنة الدولية للصليب الاحمر ، مقابلة اجريت بتاريخ ٢٠١١/٨/١٦ مقابلة اطلع عليها في ٢٠٢٣/٨/٧، على الرابط: https://www.icrc.org/ar/doc/resources/documents/interview/٢٠١١/cyber-warfare-interview (٢٠١١-٠٨-١٦.htm
(٣٦) Yan Xuetong, Bipolar Rivalry in the Early Digital Age, The Chinese Journal of International Politics, 2020, p.313.
(٣٧) Thomas W. Smith,2002 ,) The New Law of War: Legitimizing Hi-Tech and Infrastructural, International Studies Quarterly, Vol 46. , 2002, p. 366.
(٣٨) Brent Kesler, 2011,the vulnerability of Nuclear Facilities to Cyber Attack, Strategic Insight Journal, Vol 10, Issue 01. 2011, p. 19.
(٣٩)Herbert Lin, Cyber conflict and international humanitarian law, International Review of the red cross, Vol .94,No. 886 , 2012, p. 515.
(٤٠) Michael N. Schmitt & Jeffery S. Thumher, Autonomous weapon systems and the law of armed conflict, Harvard notional security journal, P. 232.
(٤١) The Potential Human Cost of Cyber Operations ,2019 , https://www.icrc.org/en/download/file/96008/the-potential-human-cost-of-cyber-operations.pdf
(٤٢) المادة(٣٦) من الملحق (البروتوكول) الأول الإضافي لاتفاقيات جنيف
(٤٣)اللجنة الدولية، القانون الدولي الانساني وتحديات النزاعات الـمسلحة الـمعاصرة ،٢٠١٥ ،ص .٤٢.
(٤٤) . Priyanka R. Dev,2015, (Use of Force and Armed Attack) Thresholds in Cyber Conflict; The Looming Definitional Gaps and the Growing Need for Formal U.N. Response), Texas International Law Journal Vol 50, Issue 2, 2015, p. 380.
(٤٥) هنكرتس ودوزوالد -بك، القانون الدولي الانساني العرفي، الـمجلد الاول، القواعد، اللجنة الدولية، مطبعة جامعة كامبريدج، كامبريدج، ٢٠٠٥ ٢٣-٤٤.