مجلة الكوفة للعلوم القانونية والسياسية

ISSN

٢٠٧٠٩٨٣٨ (مطبوع) ٣٠٠٦٧٦٧٧(إلكتروني)

العدد الثاني / المجلد الثامن عشر

تاريخ النشر/ ٣٠ / ٦ / ٢٠٢٦

انتهاك السيادة السيبرانية للدول وفق قواعد القانون الدولي العام

Violation of States' Cyber Sovereignty under the Rules of Public International Law

جامعة الحلة الاهلية

م. د. رباب محمود عامر الكسار

القانون العام – القانون الدولي العام

Rabab.Alkassar@gmail.com

المستخلص:

ادى التطور المتسارع في تكنولوجيا المعلومات والاتصالات الحديثة الى بروز الفضاء السيبراني كمجال جديد لممارسة سلطة الدول وحماية مصالحها الحيوية, الامر الذي اسهم في اعادة صياغة مفهوم السيادة التقليدي وامتداده الى ما يعرف بالسيادة السيبرانية, والتي يقصد بها حق الدول في حماية امنها السيبراني وممارسة ولايتها وسلطتها على البنية التحتية الرقمية والبيانات والانظمة والمعلومات الواقعة ضمن اقليمها او الخاضعة لسيطرتها, ويعد انتهاك السيادة السيبرانية احد ابرز التحديات المعاصرة في القانون الدولي العام, اذ يتمثل في تنفيذ عمليات سيبرانية عدائية من قبل دول او جهات منسوبة اليها ضد انظمة معلوماتية لدولة أخرى, بما يمس استقلالها السياسي او امنها الإقليمي, وتتنوع صور هذا الانتهاك بين التجسس السيبراني والهجمات على البنى التحتية الحيوية او التلاعب بالبيانات او التداخل في الشؤون الداخلية والخارجية للدول, ورغم عدم وجود معاهدة دولية شاملة تنظم صراحة المسؤولية المترتبة عن انتهاك الفضاء السيبراني للدول, الا ان قواعد القانون الدولي العام والمبادئ العامة والقواعد العرفية الدولية مازالت قابلة للتطبيق لمعالجة حالات انتهاك السيادة السيبرانية, ومع ذلك لا غنى عن إيجاد قواعد قانونية دولية تحمي بصورة مباشرة السيادة السيبرانية للدول, وتبرز اشكاليات قانونية متعددة في هذا السياق اهمها صعوبة اسناد الاعتداء السيبراني الى دولة معينة وتحديد مستوى الانتهاك الذي يرقى الى خرق السيادة او استخدام القوة, بالإضافة الى غياب اليات دولية فعالة للمساءلة والانفاذ, وفي ضوء ذلك تتجه الجهود الدولية الى تعزيز التعاون بين الدول لتطوير

قواعد قانونية دولية توفر الحماية السيبرانية للفضاء السيبراني تمهيدا لإرساء اطار قانوني دولي اكثر وضوحا ينظم السيادة السيبرانية للدول ويحد من انتهاكها.

الكلمات المفتاحية: السيادة السيبرانية للدول، العمليات السيبرانية، الفضاء السيبراني، الفعل غير المشروع دوليا، المسؤولية الدولية.

Abstract: The traditional concept of State sovereignty has undergone a fundamental transformation as a result of the rapid development of information and communication technologies and the increasing reliance on digital tools in the operation of States' critical information infrastructures. This technological evolution has significantly increased the exposure of such infrastructures to cyber targeting, giving rise to the concept of cyber sovereignty as an extension of the principle of traditional sovereignty.

The virtual space occupied by cyberspace has become a domain capable of threatening State sovereignty, owing to the ease of access to and penetration of digital systems beyond conventional geographical boundaries.Consequently, cyberspace is now regarded as a modern form of State boundaries and an essential component of national and digital security. With the emergence of cyber sovereignty, the criteria of sovereignty have been reformulated in the context of the technological age. Sovereignty is no longer confined to territorial borders alone; rather, a fourth dimension has emerged, represented by States' sovereignty over their cyber domain.

Moreover, the recognition of cyberspace as a new arena of interstate conflict has led to the exploitation of legal gaps resulting from the absence of explicit legal rules within public international law governing State behavior in this domain. This situation has highlighted the urgent need for the development of an international cyber legal framework capable of addressing contemporary challenges. This need has become particularly pressing in light of the recent escalation of cyber attacks, some of which have reached the level of aggression through the destruction or disruption of vital service infrastructures, such as energy facilities and healthcare systems thereby adversely affecting.

Consequently, cyberspace is now regarded as a modern form of State boundaries and an essential component of national and digital cocurity With the emergence of

civilian populations and resulting in substantial loss of life Accordingly, it has become necessary to reconceptualize sovereignty in a manner consistent with the information age, extending beyond geographical territory to encompass the State's digital domain. This has prompted States within the international community to enhance the protection of cyberspace by incorporating it within the scope of State sovereignty and by seeking to establish international legal rules to safeguard it against external threats, particularly through the conclusion of international agreements aimed at combating cyber attacks and regulating the use of cyberspace in a manner that promotes international peace and security.

Keywords: State cyber sovereignty**,** Cyber operations**,** Cyberspace**,** International wrongful acts**,** International responsibility

المُقدمة:

موضوع الدراسة: تغيرت اشكال الحدود السياسية للدول بتقدم وتطور التكنولوجيا, الامر الذي غير مفهوم السيادة التقليدي للدول, اذ أدى توفر الأدوات التكنلوجية والرقمية وتطور تكنلوجيا المعلومات والاتصالات وزيادة الاعتماد عليها في تشغيل العديد من التقنيات المتصلة بالبنى المعلوماتية التحتية للدول الى زيادة تعرض هذه المعلومات الى الاستهداف السيبراني, فالمساحة الافتراضية التي يشغلها الانترنت يمكن ان تهدد سيادة الدول بسبب سهولة وإمكانية الوصول اليها وخرقها, لذا عدّ الفضاء السيبراني احد انواع حدود الدول وجزء هام من امنها الرقمي, ومع ظهور السيادة السيبرانية تم اعادة صياغة معايير السيادة في عصر التكنولوجيا الحديثة, اذ لم يعد مفهوم السيادة مقتصرا على الحدود الجغرافية فقط بل اصبح للسيادة بعدا جديدا تمثل بسيادة الدول على فضاءها السيبراني, وأصبحت للدول ساحات صراع جديدة تمثلت في الفضاء السيبراني, وذلك بسبب استغلال الثغرات القانونية الناجمة عن غياب النصوص القانونية في القانون الدولي العام التي تنظم هذا المجال, الامر الذي اظهر الحاجة الى وضع تشريعات دولية حديثة متلائمة مع التحديات الجديدة, خاصة بعد ان تصاعدت وتيرة الهجمات السيبرانية في الآونة الاخيرة والتي اصبحت تصل الى مستوى العدوان المتمثل في التدمير والتعطيل الذي يطال البنية التحتية الخدمية كمحطات الطاقة والمرافق الصحية, مما يؤثر على حياة المدنيين ويسبب خسائر فادحة في الأرواح, ومع ظهور مفهوم السيادة السيبرانية اصبح لابد من اعادة صياغة معايير السيادة في عصر المعلومات, اذ لم يعد مفهوم السيادة مقتصرا على الحدود الجغرافية بل امتد ليشمل فضاءها الرقمي, مما حدا بالدول في المجتمع الدولي الى تعزيز حماية فضاءها السيبراني من خلال ضمه الى مفهوم سيادتها والعمل على إيجاد قواعد قانونية دولية

توفر الحماية له من التهديدات الخارجية, وذلك عبر ابرام اتفاقيات دولية لمكافحة الاعتداء السيبراني لهذا الفضاء.

أهمية الدراسة: تأتي اهمية الدراسة من خلال تحليل الأثر القانوني للعمليات السيبرانية على سيادة الدول واستعراض المفهوم التقليدي للقانون الدولي العام لسيادة الدول, وبيان الاتجاهات الفقهية الحديثة واثر العمليات السيبرانية على تحديث مفهوم سيادة الدول كونها تمس جوهر العلاقات الدولية المعاصرة, إضافة الى بيان التحديات العملية التي تواجه الدول في اثبات المسؤولية في البيئة السيبرانية في ظل غياب اتفاق دولي يبين ابعاد السيادة السيبرانية للدول والاثر القانوني المترتب على انتهاكها.

نطاق الدراسة: يتحدد نطاق الدراسة في حدود العمليات السيبرانية العدائية التي تمس سيادة الدول بعد ان اصبح الفضاء السيبراني بُعد جديد يضاف الى ابعاد سيادة الدول واحد طرق انتهاك سيادتها, كما تشمل الدراسة التحديات القانونية المعاصرة التي تواجه مبدأ سيادة الدول في القانون الدولي العام, ومدى إمكانية تكييف العمليات السيبرانية العدائية التي تتسم بخصائص تجعل تنظيمها باعتبارها استخداما للقوة وانتهاكا لسيادة الدول اكثر تعقيدا.

مشكلة الدراسة: تتمثل مشكلة الدراسة في غياب قواعد قانونية دولية تضع صياغة جديدة لمفهوم السيادة السيبرانية في زمن تتلاقى فيه الحدود الحقيقية مع الحدود الافتراضية, وتزداد فيه الحاجة الى اطار قانوني دولي قادر على معالجة التحديات المعاصرة لانتهاك سيادة الدول عبر العمليات السيبرانية العدائية.

منهج الدراسة: تعتمد هذه الدراسة على المنهج التحليلي من خلال تحليل النصوص القانونية الدولية ذات الصلة, والاتجاهات الفقهية التي بينت مفهوم السيادة للدول, وبيان حاجة هذه النصوص الى التحديث بما يتوافق مع حالات انتهاك السيادة عبر الفضاء الالكتروني, وكذلك تعتمد الدراسة المنهج الوصفي من خلال التوصيف الواقعي للتهديدات السيبرانية عبر الفضاء السيبراني وأنواع العمليات السيبرانية الالكترونية التي تمس بسيادة الدول وطبيعة الفضاء السيبراني الذي يُستغل لتنفيذ العمليات السيبرانية العدائية .

هيكلية الدراسة: تتألف الدراسة من مبحثين مع مقدمة وخاتمة نبين في محتواها اهم النتائج والتوصيات التي توصلت اليها الدراسة, المبحث الأول سنبين من خلاله مفهوم السيادة السيبرانية وفق قواعد القانون الدولي العام, وسنقسم المبحث على مطلبين في المطلب الأول سنتطرق الى المدلول الفقهي والقانوني لمبدأ سيادة الدول في القانون الدولي العام, اما المطلب الثاني سنشرع من خلاله الى تعريف السيادة السيبرانية للدول وفق قواعد القانون الدولي العام, وفي المبحث الثاني سنعرج الى بيان الأثر القانوني للعمليات السيبرانية على سيادة الدول وفق قواعد القانون الدولي العام, وذلك بعد تقسيم المبحث على مطلبين سنبين في الأول تعريف العمليات السيبرانية وفي المطلب الثاني سنتطرق الى المسؤولية الدولية المترتبة عن انتهاك السيادة السيبرانية للدول وفق قواعد القانون الدولي العام.

المبحث الأول

مفهوم السيادة السيبرانية وفق وقواعد القانون الدولي العام

اصبح مفهوم سيادة الدول عرضة للتغير والتبدل بسبب الاحداث المعاصرة التي يمر بها المجتمع الدولي, اذ اخذ مبدأ سيادة الدول يتأثر من حيث المدلول والمفهوم والمحتوى القانوني, فمنذ ان نشأت منظمة الامم المتحدة اخذ ميثاق المنظمة على عاتقه مهمة إدخال مبادئ جديدة تدعم سيادة الدول من خلال تحريم الحرب واللجوء اليها, واكد الميثاق كذلك على المساواة في السيادة بين الدول الاعضاء في المادة (٢/ ١)[٥], كما منعت الفقرة (٧) من نفس المادة صراحة التدخل في الشؤون التي تكون من صميم السلطان الداخلي للدول الأعضاء, وعلى اثر ذلك تواترت الدول على تضمين هذا المبدأ في المعاهدات الدولية الثنائية والجماعية, الامر الذي جعل هذا المسلك يتحول الى قاعدة دولية عرفية تحضر على الدول والمنظمات الدولية انتهاك سيادة الدول الأخرى.

وبعد ان نشأ ما يعرف بالفضاء السيبراني نتيجة التطور الهائل في مجال المعلومات التكنلوجية اصبح المجتمع الدولي يواجه مخاطر جديدة تمس بسيادة الدول وفضائها السيبراني, وظهرت العمليات السيبرانية التي تؤثر بشكل مباشر على سيادة الدول من خلال انتهاك البيانات والمعلومات التي تمس بسيادها واستهداف البنى التحتية لها, مما يتسبب في مخاطر حقيقية وكارثية على المدنيين والاعيان المدنية, ولبيان مفهوم السيادة السيبرانية للدول نقسم المبحث على مطلبين نبين في المطلب الاول المدلول الفقهي والقانوني لمبدأ سيادة الدول في القانون الدولي العام, وفي المطلب الثاني نبين مفهوم العمليات السيبرانية.

المطلب الأول

المدلول الفقهي والقانوني لمبدأ سيادة الدول في القانون الدولي العام

ظهر مفهوم السيادة الدولية في اوروبا بعد معاهدة وستيفاليا سنة ١٦٤٨ واصبح من المبادئ الاساسية التي يرتكز عليها القانون الدولي العام, اذ اكد على حق كل دولة في ممارسة سلطتها بشكل كامل داخل حدود اقليمها وعلى قدم المساواة مع الدول الاخرى[٥].

كما خضع مفهوم السيادة لتحولات جوهرية متسارعة في ظل العولمة والتأويلات المتعددة والمتغيرة, مما ادى الى عدم ملائمة المفهوم التقليدي للسيادة مع التحديات المعاصرة[٢], وقد عرف بعض الفقه السيادة بانها " تفرد السلطة بإدارة الشؤون الداخلية والخارجية ضمن حدود اقليمها دون منازع, وتمتعها بالتحكم المطلق بالقرارات والافعال الصادرة عنها"[٤].

كما عرف جان بودان السيادة بانها "سلطة الجمهورية العليا والمطلقة والابدية", وصاحب السيادة هو الحاكم الذي لا يقبل اي قانون سوى القانون الالهي او القانون الطبيعي وقانون الأمم, ولا يُخضِع بودان السلطة لأي قيود قانونية او حدود زمنية, فهي السلطة التي تستمد صلاحيتها من ذاتها ولا تحتاج الى موافقة او اعتراف من اي جهة أخرى, ويذهب بودان الى ان السيادة هي الاساس الذي تقوم عليه الدولة الحديثة والتي تمكنها من التماسك والوحدة فيما بينما, في حين

يعرف ادم سميث السيادة بانها "تلك القوانين والاليات التي تمنع شيوع الفوضى والظلم عندما يسعى الافراد الى تحقيق مصالحهم الخاصة"[٩].

اما كلسن فقط ذهب الى ان القانون الوضعي القائم لا يمكن ان نشتق منه طبيعة السيادة من الناحية الفقهية اذ يرى ان السيادة هي مجموعة الاختصاصات الموضوعية, ويصف السيادة بانها " نظاما قانونيا يقف فوق الدول ويضعها تحت الالتزام"[١٠]. والسيادة باعتبارها السلطة القانونية العليا تكون محددة في نطاق المجتمع الدولي, اذ لا تملك دولة سلطة على الدول الاخرى بصورة عامة, وكذلك لا سلطة للدول على هذه الدولة[١١].

وتتصف السيادة بمجموعة من الخصائص منها الاطلاق, أي انها سلطة مطلقة ليس هناك سلطة اعلى منها في الدولة, كما تتصف بانها شاملة فهي تشمل جميع المواطنين في الدولة باستثناء الاشخاص الذين يتمتعون بالحصانة الدولية[١٢], كذلك فان السيادة لا تستطيع الدول التنازل عنها والا فقدت وجودها, فهي صفة ملاصقة للدولة وبانتهائها تنتهي الدولة, وهي صفة غير قابلة للتجزئة[١٣].

يعد مبدأ احترام سيادة الدولة من المبادئ الاساسية في العلاقات الدولية, اذ من خلاله تلتزم الدول في سلوكها الخارجي بعدم اتباع سلوك يشكل اعتداء على سيادة دولة أخرى وذلك من خلال التدخل في شؤونها الداخلية, فالسيادة ركن اساسي تبنى عليه نظرية الدولة في الفكر القانوني, كما تعد السيادة مبدأ اساسي في العلاقات الدولية المعاصرة, فالمفهوم القانوني للسيادة يعبر عن مجموعة من القوانين والاعراف الدولية, اذ وفق مبدأ السيادة تكون الدولة على قدم المساواة مع الدول الاخرى في المجتمع الدولي[١٤].

كما تمنح السيادة للدولة وضع قانوني وسلطان تواجه به الافراد في داخل اقليمها وبقية الدول في الخارج, وبموجب مبدأ السيادة يكون للدولة حرية التصرف في شؤونها الداخلية والخارجية, وقد عرفت محكمة العدل الدولية السيادة في قضية مضيق كورفو سنة ١٩٤٩ " السيادة بحكم الضرورة هي ولاية الدولة في حدود اقليمها ولاية انفرادية مطلقة, وان احترام السيادة الاقليمية فيما بين الدول المستقلة يعد اساسا جوهريا من اسس العلاقات الدولية"[١٥], ووفق مبدأ السيادة فان الدولة لا يقيدها في الميدان الدولي الا الاتفاقيات الدولية التي تعّبر عن سيادتها واستقلالها[١٦].

كما ان تنظيم العلاقات الخارجية بين الدول يقوم على اساس الاستقلال واحترام السيادة, وهذا يعني ان الدول تكون على قدم المساواة مع غيرها من الدول ذات السيادة, على ان ذلك لا يعني عدم تقيد الدولة بالتزاماتها الدولية والمعاهدات الدولية مع غيرها من الدول, ويرتبط مبدأ السيادة بالهوية القانونية للدول, فمن خلاله يعم النظام والاستقرار في العلاقات الدولية, وبذلك يمكن لنا تعريف سيادة الدولة بانها" السلطة القانونية العليا والمستقلة التي تتمتع بها الدولة على اقليمها وسكانها باعتبارها كيان مستقل لا يخضع لسلطة اعلى منها في إدارة شؤونه الداخلية والخارجية, مع التزامها بقواعد القانون الدولي".

الا ان مفهوم السيادة تطور مع تطور المجتمع الدولي المعاصر وظهور الفضاء السيبراني واتخذ معنى أوسع شمل السيادة السيبرانية للدول الامر الذي سيتم بيانه في المطلب القادم.

المطلب الثاني

تعريف السيادة السيبرانية للدول وفق قواعد القانون الدولي العام

ادى التطور التكنولوجي الذي يشهده العصر الحديث الى تغيير مفهوم سيادة الدول, فقد اصبح الامن السيبراني مكونا أساسيا من مكونات أي تحول رقمي, حيث ان حماية البيانات والبنى التحتية ستكون مصدر قلق كبير للحكومات بسبب زيادة وتنوع العمليات السيبرانية, لذلك يعد الامن السيبراني سلاحا استراتيجيا تسعى الدول من خلاله الى حماية فضائها السيراني ولا سيما ان الحرب السيبرانية أصبحت جزءا من التكتيكات الحديثة للحروب والهجمات بين الدول[٢].

قدمت وزارة الدفاع الامريكية تعريفا للأمن السيبراني اذ عرفته بانه "جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع اشكالها المادية والالكترونية من مختلف الجرائم والهجمات والتخريب والتجسس والحوادث"[٤]. كما عرف البعض الأمن السيبراني بانه "مجموعة العمليات التقنية الحديثة والممارسات التي تحمي الشبكات واجهزة الكمبيوتر والبيانات من الهجمات والاضرار والوصول غير المصرح به", ويعد الامن السيبراني نشاط يحمي الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات ويضمن امكانية الحد من الخسائر والاضرار[٥].

كما اصبح الامن السيبراني يمثل جانب من جوانب سيادة الدولة وشكل من اشكال الجغرافية السياسية, الامر الذي حدى الدول ببذل جهود من اجل حماية امنها السيبراني من الاختراق باعتباره مظهر من مظاهر سيادتها, فالفضاء السيبراني اصبح احد الميادين الحيوية التي تعاد من خلاله صياغة العديد من المفاهيم التقليدية, وهو احد انواع حدود الدولة والذي يمكن من خلال اختراقه ان تتعرض مصالح الدولة للانتهاك, لذلك يعد الامن السيبراني للدول جزءا هام من امنها القومي ومكانتها الدولية.

وقد عرفت الامم المتحدة والاتحاد الدولي للاتصالات الفضاء السيبراني بانه "التضاريس المادية وغير المادية التي تم إنشائها وتكوينها من بعض أو كل ما يلي: أنظمة وأجهزة الكمبيوتر والشبكات، والبرامج وبيانات الكمبيوتر، وبيانات المحتوي وبيانات كلمات المرور للمستخدمين"[٦].

عرف الفقيه الأمريكي جوزيف "Joseph S. Nye" الفضاء السيبراني على انه "مجال تشغيلي محكم باستخدام المعلومات عبر الأنظمة المترابطة والبنية التحتية المرتبطة بها" وصنف الفضاء السيبراني الى طبقتين, الأولى مادية والتي تحكمها القوانين السياسية والاقتصادية والتي تخضع للسلطة القضائية, وتتكون من الأنظمة والبنية التحتية المادية للفضاء السيراني, اما الطبقة الثانية والتي لا تخضع للسلطة القضائية والتي تتكون من المعلومات الافتراضية والبرمجيات, ويكون من السهل شن هجمات من الطبقة الافتراضية ذات التكلفة المنخفضة ضد الطبقات المادية ذات المواد المكلفة والمرتبطة بالبنى التحتية والمتحكمة بالاتصالات والمعلومات والمتصلة بالأنترنت[٧].

كما ساهم ظهور مفهوم السيادة السيبرانية للدول في فرض تحولات على مفهوم السيادة التقليدية وعناصرها, اذ تحولت السيادة التقليدية الى سيادة رقمية من خلال رقمنة الافراد والبنى التحتية, وهكذا اصبح للسيادة السيبرانية طابع داخلي يتمثل بالاستقلال والاشراف والمراقبة في ادارة شؤون الانترنت الخاصة بالدولة, وطابع خارجي يشير الى حماية السيادة السيبرانية للدول من الغزو الخارجي الذي يتمثل بالعمليات السيبرانية العدائية التي تستهدف المعلومات الالكترونية والبنى التحتية المتصلة بها والخدمات الرقمية(١٩).

كما تشير السيادة السيبرانية الى سيطرة الدولة والتحكم في فضائها السيبراني داخل حدودها الجغرافية وتوفير الحماية لها من التهديد الخارجي عن طريق توفير الامن السيبراني, اذ تمارس السيادة السيبرانية في الفضاء السيبراني, والذي هو مجال افتراضي يتكون من الشبكات الالكترونية المتصلة بالبنى التحتية الرقمية التي ترتبط عن طريق الانترنت, لذلك تلجأ الدول الى تعزيز سلطتها في ادارة العمليات الرقمية والتي تكون على اتصال مباشر بأمنها الخارجي, ونتيجة لذلك قامت روسيا والصين بتبني مفهوم السيادة السيبرانية الذي يبرر مراقبة المحتوى الرقمي على خلاف السيادة السيبرانية لدى الدول الليبرالية التي تتمثل بالولايات المتحدة الامريكية والدول الاوروبية(١٩).

ووفقا للمفهوم الحديث للسيادة اصبحت للدول سيادة تشمل فضاءها السيبراني والذي يمثل سيادتها السيبرانية, تؤمن له الدول الحماية من خلال مجموعة من الاستراتيجيات التقنية والسياسية الوطنية التي توفير الامن السيبراني والسيطرة على الفضاء الالكتروني, الذي يشكل ميدان المعركة الخامس للقوى الدولية بعد البر والبحر والجو والفضاء, وبعد ان اصبح استهداف البنى التحتية المعلوماتية هو الشغل الشاغل للمعظم الدول نظرا لقدرته الفائقة على احداث خسائر تطال الأهداف العسكرية والمدنية والبنى التحتية في حال الاعتداء عليها.

يتم توفير الحماية للسيادة السيبرانية عبر فرض الرقابة على البرمجيات والخوارزميات من خلال ادوات الذكاء الاصطناعي(٢٠), ولكي تحمي الدول سيادتها السيبرانية تقوم بتجزئة الفضاء السيبراني الى اجزاء مختلفة يخضع كل جزء لسيادة دولة معينة, الامر الذي يفضي الى التفاوت في التعامل بين الدول ذات الانظمة الديمقراطية والدول ذات الانظمة القمعية, وذلك عندما تفرض بعض الدول تقنيات التجسس الرقمي لمراقبة الانشطة التي يمارسها مواطنيها من خلال سن القوانين التي تقيد حرية استخدام الفضاء الالكتروني(٢٠).

تتمثل السيادة السيبرانية الدولية من الناحية الدولية في حرية الدول في ممارسة الانشطة السيبرانية في علاقتها مع الدول الاخرى في المجتمع الدولي ووفق قواعد القانون الدولي, اذا تتمتع جميع الدول بالمساواة في السيادة السيبرانية وفق المادة (١/٢) من ميثاق الامم المتحدة, كما يحق للدول الانضمام الى معاهدات تنظم الانشطة السيبرانية والاشتراك في العمليات السيبرانية بحكم سيادتها الخارجية, على ان لا تكون مخالفة لقواعد القانون الدولي والاعراف الدولية والتي تنص على عدم التدخل او استخدام القوة ضد دولة أخرى.

بعد ان بينا مفهوم السيادة الدولية والامن السيبراني والفضاء السيبراني للدول, يمكننا ان تعرف السيادة السيبرانية الدولية بانها " سلطة الدولة الكاملة على فضاءها السيبراني والمتمثل ببنيتها

التحتية الرقمية من حيث الإدارة والتشغيل داخل اقليمها, وتحقيق امنها السيبراني من خلال حمايته من التدخل الخارجي غير المشروع وذلك وفق قواعد القانون الدولي العام".

المبحث الثاني

الأثر القانوني للعمليات السيبرانية العدائية على سيادة الدول

بعد التقدم التكنلوجي في مجال التقنيات الرقمية وظهور الفضاء السيبراني اصبح للدول مجالا جديدا يمكن من خلاله ان تُنتهك سيادتها, اذ تستند العمليات السيبرانية الى وسائل الكترونية في الاعتداء على سيادة الدول الأخرى, والتي قد تُشن من قبل افراد او جماعات او حتى دول, ويعتبر هذا الاعتداء هو نوع من أنواع استخدام القوة التي يمثل تهديدا مباشرا للبنى التحتية الحيوية والأنظمة السياسية والاقتصادات الوطنية, اذ تسعى الدول من خلال العمليات السيبرانية الى تقويض قدرات دولة اخرى لأغراض سياسية او اقتصادية, الامر الذي يؤثر على سيادة الدول والذي تعد حجر الأساس في النظام الدولي, ولبيان الأثر القانوني للعمليات السيبرانية على سيادة الدول نقسم المبحث على مطلبين نعرف في الاول العمليات السيبرانية وفي الثاني نبين المسؤولية الدولية المترتبة عن انتهاك السيادة السيبرانية للدول.

المطلب الأول

تعريف العمليات السيبرانية

لم يتفق المجتمع الدولي على تعريف دقيق للعمليات السيبرانية نتيجة لحداثة اسلوب العمليات التي تتخذ من شبكات الحاسوب مجالا لها[٢٢], اذ يذهب البعض الى ان الحرب السيبرانية هي امتداد للحروب التقليدية فهي تشن من قبل افراد عسكريين ومدنيين ولها اهداف عسكرية تتمثل في تدمير البنى والتحتية للعدو وتستخدم وسائل متعددة كأن تضرب المعلومات الحيوية والتقنية والرقمية وغيرها[٢٣].

عرف خبراء تالين العمليات السيبرانية على انها (عمليات سيبرانية سواء كانت هجومية او دفاعية يُهدف من خلالها التسبب بإصابة او وفاة الاشخاص او الاضرار او تدمير الأهداف)[٢٤], وتستهدف العمليات السيبرانية النشاط الرقمي والبيانات السرية غير المادية عبر الفضاء السيبراني, فهي عملية معقدة تتصف بتقنية عالية وتتعلق ببرمجة المكونات المتصلة بالشبكة, فالعمليات السيبرانية لها تأثير خطير على نشاطات الافراد والنظم المعلوماتية من خلال الفضاء الالكتروني, اذ تسبب خلل في النظم الرقمية وتكنولوجيا المعلومات والاتصالات[٢٥].

بذلك نجد ان العمليات السيبرانية هي تصرف يدور في عالم افتراضي من خلال استخدام بيانات رقمية ووسائل اتصال تعمل الكترونيا قد يكون الغرض منها سياسي او استخباراتي او امني, الا ان هذا المفهوم قد تطور مع تطور التكنولوجيا الرقمية اذ اصبح من غاياته تحقيق ميزة عسكرية ملموسة ومباشرة واختراق مواقع الكترونية حساسة بهدف الوصول الى انظمة حماية لها تأثير واسع النطاق مثل محطات الطاقة النووية او البنى التحتية.

وتختلف العمليات السيبرانية عن الهجوم السيبراني الذي عرفه سمث بانه (اي تصرف الكتروني دفاعيا كان او هجوميا يتوقع منه وعلى نحو معقول في التسبب بجرح او قتل شخص او الحاق اضرار مادية او دمار بالهدف المهاجم)[٢٦], وبذلك نجد ان الهجوم السيبراني نوع محدد من العمليات السيبرانية يهدف الى احداث اذى او تعطيل او تدمير بنية تحتية رقمية او أنظمة او بيانات, بينما العمليات السيبرانية ليست بالضرورة تدميرية او ضارة.

من امثلة الهجمات السيبرانية العدائية هو الخرق المتعمد وغير المصرح به للوصول الى نظم المعلومات لأغراض التجسس, او يستهدف اضرار مادية تعطل عمل البنى التحتية الحيوية مما يسبب توقف الخدمات الأساسية والمرافق الحكومية, او يستهدف اضرار معنوية كالاضطرابات, وهي بذلك لها عواقب على سرية او سلامة المعلومات او نظم المعلومات, فالهجمات السيبرانية هي عمليات عدائية تستهدف تكنولوجيا المعلومات والاتصالات ويضر بسرية البيانات او الخدمات او توافرها او سلامتها.

كما تتميز الهجمات السيبرانية بانها تتم بواسطة شخص او اكثر من خلال استخدام جهاز كمبيوتر مزود بعدد كبير من الفيروسات تؤدي الى اضرار مادية او معنوية عبر ارسالها الى الهدف المراد الحاق الضرر به من خلال استهداف واعتراض بيانات تؤدي الى تخريب او تعطيل او تدمير الاموال والضرر بالأشخاص من خلال توقف النظام عن اداء الخدمات التي كان يقدمها, او تعرض اسرار المؤسسات والافراد للخطر, او قد تؤدي الهجمات السيبرانية الى تلف البيانات الحساسة وبث معلومات مغلوطة[٢٧].

وهناك من يرى ان العمليات السيبرانية العدائية تقترب من الاعمال الارهابية ويعزون ذلك الى انها تنشر الرعب عبر شبكات الانترنت وتروع امن الافراد والجماعات ومؤسسات الدولة, ويعد العمليات السيبرانية هي نوع من الارهاب الصامت[٢٨].

العمليات السيبرانية العدائية سلاح ذو حدين وذلك وفق التحكم والسيطرة المتقنة عليها وبحسب من يستخدمها فيما اذا اراد ان يقلل من الخسائر المترتبة عليها من عدمه, او قد تتحول هذه البرامج الى اسلحة مارقة نتيجة سوء استخدامها او العيوب فيها بما يؤدي الى خلاف النتائج المتوقعة منها, اذ قد تتسبب في اضرار اوسع مما اراد مستخدم هذه البرمجيات منها, وبذلك نجد ان استخدام العمليات السيبرانية قد يكون لها تأثير اكبر فيما لو اساء استخدامها او من يتحكم بها اراد تحقيق اضرار اكبر مما استخدمت من اجله مما يسبب الآم لا مبرر لها.

وتتسم العمليات السيبرانية العدائية بانها غير ملموسة وغير مادية, اضافة الى صعوبة ايجاد الصلة بين مرتكب العمليات السيبرانية والاثار الناتجة عنها بسبب بعد المسافة بين منفذ العملية والاثار المترتبة عليها, اضافة الى سهولة اخفاء هوية مرتكب العمليات السيبرانية, وبالتالي صعوبة اسناد هذه الهجمات التي قد تتم عبر اكثر من وسيط ووسط الكتروني[٢٩].

كما ان مجهولية هوية الفاعل في العمليات السيبرانية تصعب عملية تحديد المسؤول, ومن ثم تحميله المسؤولية الدولية عن العمليات السيبرانية التي تحصل في الفضاء السيبراني, وهذه المجهولية هي قاعدة وليس استثناء, اذ من المستحيل في بعض الحالات اقتفاء اثر المصدر كون

الفاعل شخص فتنطبق عليه قواعد القانون الدولي الانساني, او مؤسسة حكومية فتنطبق عليها قواعد القانون الدولي العام[٣٠].

قد تتحول العمليات السيبرانية الى حرب سيبرانية, فالحرب هي احدى اشكال العنف او التدخل السياسي, تستخدم فيها المجموعات المتحاربة وسائل وأساليب وتقنيات مختلفة, الغرض منها هو الحاق الأذى بالعدو سواء في قدرته العسكرية او في مقدراته المدنية, ويتم الاستعانة بالمعلومات العسكرية بهدف التدمير المنظم للقدرات العسكرية من خلال الحصول عليها من الأجهزة العسكرية الاستخباراتية[٣١] اما الحرب السيبرانية فهي تشمل وسائل واساليب قتالية من خلال عمليات الكترونية ترقى الى مستوى النزاع المسلح او تستخدم في سياقه, ويعرف البعض الحرب السيبرانية بانها "استعمال الحواسيب كسلاح او اداة للقيام بأعمال عنف بقصد بث الرعب او تغيير راي مجموعة او دولة ما, ويتم استخدامه لأغراض سياسية او ايدلوجية عن طريق استهداف البنى التحتية الحيوية كالطاقة والنقل والاتصالات والخدمات الضرورية"[٣٢].

عرفت اللجنة الدولية للصليب الاحمر الحرب السيبرانية بانها "الاستغلال المتعمد لعدد من الانشطة بهدف افساد او اتلاف او تدمير الانظمة الخاصة بالحاسب الالي, او الشبكات الرقمية الخاصة بالخصم, وتستهدف المعلومات والبيانات والانظمة والشبكات واي كيان يرتبط مع هذه الانظمة والشبكات"[٣٣], والغرض من العمليات السيبرانية اما للإضرار بالممتلكات الالكترونية للخصم, او لحرمانهم من استخدام هذه الممتلكات عن طريق منعه من الولوج للمواقع الرسمية الخاصة به واستخدامها على النحو الذي يراه, كما قد يكون الهدف من هذه العمليات على نحو عكسي في الدفاع عن المنشآت الالكترونية للدول, وذلك عن طريق منع اي دخول غير مرخص له للمواقع الالكترونية الخاصة بالدول.

ويمكن تعرف الحرب السيبرانية بانها " الاعمال العدائية التي تنفذ عبر الوسائل والأساليب السيبرانية ومن خلال الفضاء السيبراني, وترقى في اثارها الى مستوى استخدام القوة او النزاع المسلح, والتي تستهدف شبكات المعلومات والبنى التحتية الحيوية للدولة بقصد اضعاف قدرتها العسكرية او الاقتصادية او الأمنية او انتهاك سيادتها, دون اللجوء الى الوسائل العسكرية التقليدية".

ونتيجة لضعف الامن السيبراني للدول وتطور وسائل واساليب العمليات السيبرانية بالمقارنة مع تطور انظمة الحماية والامن السيبراني, سهل ذلك من تحقيق الغرض من تنفيذ العمليات السيبرانية والتي عادة ما يتم تنفيذها عن طريق أدوات ذات تقنية عالية ومن مكان بعيد جدا عن الهدف المحدد[٣٤].

تستخدم العمليات السيبرانية العدائية لغرض كسب ميزة على العدو من خلال استخدام الفضاء السيبراني وتسخير الادوات الالكترونية والاشخاص الفنيين, وعادة ما تتمثل المزايا العسكرية بتدمير او اتلاف انظمة الحاسوب للعدو او من خلال الحصول على معلومات لا يرغب العدو في الافصاح عنها, ويرى البعض ونحن معه ان الحرب السيبرانية هي اوسع نطاقا من الهجوم

السيبراني وقد اخذ بهذا التوجه كل من توماس رد وبيتر ماكبورني المختصان في القانون الدولي الانساني[٣٩].

لتحقيق الردع السيبراني لابد من وجود انظمة دفاعية سيبرانية فعالة لحماية القطاعات المدنية والعسكرية والدفاع عن البنى التحتية الأساسية, ويكون ذلك من خلال تقليل فرص نجاح العمليات السيبرانية العدائية عِبر امتلاك مجموعة واسعة من القدرات الهجومية السيبرانية المضادة للتأكيد على قوة الدولة لتحقيق الردع قبل واثناء الهجوم السيبراني, وتعزيز البنى التحتية الحيوية المرنة والقابلة للتعافي السريع, وتحقيق التعاون مع الوكالات الاستخباراتية الدولية الحليفة والصديقة.

ويستطيع المهاجم في الاسلحة الهجومية السيبرانية ان يستغل الثغرات غير المعروفة من قبل العدو من اجل تعطيل الانظمة المعلوماتية, اما في الاسلحة الدفاعية السيبرانية يتم الكشف المبكر للثغرات ويمكن للمدافعين من خلال ذلك معالجتها واغلاق هذه الثغرات وايقاف المزيد من الهجمات, فالأسلحة الهجومية تستغل ثغرة او عيب غير معروف من الطرف الاخر عند بداية الهجوم, ثم يتدافع المبرمجين لسد الثغرة وتصحيحها[٣٦].

عندما نظمت القواعد القانونية المتعلقة بأساليب ووسائل القتال لم تكن العمليات السيبرانية قد ظهرت في ساحة النزاعات المسلحة, مما جعل هذه القواعد قاصرة عن تنظيم العمليات السيبرانية, وشكلت عائق كبير امام المختصين في القانون الدولي الانساني لتكييف هذه العمليات, الامر الذي ادى الى الاختلاف بين اراء المختصين حول انطباق مبادئ وقواعد القانون الدولي الانساني على العمليات السيبرانية, فمنهم من يرى ان هذه القواعد من الممكن تطبيقها على العمليات السيبرانية, ومنهم من ينكر ذلك ويرى ان الفترة الزمنية التي جرى فيها تقنين القواعد القانونية المتعلقة باستخدام وسائل واساليب القتال لم تكن للعمليات السيبرانية وجود يذكر, وهذا يعني انها غير مقننة وبالتالي فأنها خارج اطار قواعد القانون الدولي الانساني[٣٧].

وبالاستناد الى ما ذهبت اليه محكمة العدل الدولية بخصوص مشروعية التهديد او استخدام الاسلحة النووية حيث اشارت المحكمة الى ان استخدام القوة في العلاقات الدولية غير محدد بنوع معين من الأسلحة, بل تشمل كل انواع القوة المستخدمة بغض النظر عن نوع الاسلحة[٣٨], نجد ان المحكمة قد عولت على معيار الوسيلة المستخدمة لبيان فيما اذا كان استخدام للقوة في العلاقات الدولية من عدمه, وبذلك فأن العمليات السيبرانية العدائية هي فعلا استخدام للقوة في العلاقات الدولية ووفق القانون الدولي الإنساني, اذا كانت العمليات السيبرانية تستند الى وسائل تخضع للقواعد القتالية.

في حين عول رأي اخر ونحن معه على معيار الاثر المترتب عن العمليات السيبرانية وليس على الوسيلة المستخدمة في الهجوم, وهذا المعيار اخذ به دليل تالين في القاعدة رقم (١١) اذ اشارت الى ان العمليات السيبرانية تعد استخدام للقوة اذا كانت اثارها من حيث الخطورة والنطاق مماثلة للآثار الناجمة عن استخدام القوة التقليدية, وبذلك فأن دليل تالين لا يشترط وجود تدمير مادي مباشر, بل يركز على طبيعة وحجم الأثر الملموس, فاذا بلغ مستوى مماثلا للقوة التقليدية, فأن العملية السيبرانية تعد استخداما للقوة.

تختلف الحرب التقليدية الحركية عن الحرب السيبرانية من حيث الوسائل, اذ ان الاولى تنطوي على استخدام اسلحة تقليدية من قبل الجيوش النظامية بعد ان يتم الاعلان عن قيام حالة الحرب بين اطراف محددة وفي حدود مساحات اقليمية محددة, وهذا عكس ما نجده في الحرب السيبرانية والتي يستخدم فيها أدوات رقمية وبرمجيات خبيثة ومن خلال مجال فضائي مفتوح كونها تتم عبر شبكات اتصالات الكترونية غير واضحة الحدود والمصدر, وعادة ما يتم توجيه هذه العمليات ضد منشآت حيوية لها الاثر الاكبر في تحقيق اهداف عسكرية دون ان يكون هناك اعلان مسبق, كما يمكن التمييز بين العمليات السيبرانية والعمليات الحركية التقليدية من خلال طبيعة الأسلوب المستخدم في العمليات السيبرانية والتي يستخدم فيها بيئة غير تقليدية والتي تتمثل بالفضاء الرقمي أي عبر شبكات الحاسوب والانترنت, بينما العمليات الحركية التقليدية تتم في بيئة مادية ملموسة ومعروفة.

يقترب الهجوم السيبراني في اطار الحرب السيبرانية مع الهجوم الحركي في الحرب التقليدية, في ان كلاهما يكون بدافع اضعاف الخصم وتحقيق ميزة ضد العدو بهدف اجباره على تغيير سلوكه, مما يحقق اهداف سياسية او عسكرية او امنية, كما يهدف الى ان يكون له اضرار سواء على الأشخاص الطبيعيين او المعنويين, وان كلاهما يخضع للقانون الدولي الإنساني والقانون الدولي العام عند بلوغ مستوى استخدام القوة في العلاقات الدولية.

قد عرفت لجنة الاسلحة التقليدية التابعة للأمم المتحدة في عام ١٩٦٨ الاسلحة غير التقليدية بانها "اسلحة الانفجارات الذرية والاسلحة المصنوعة من مادة ذات نشاط اشعاعي واسلحة الفتك الكيميائية والبيولوجية واي نوع من الاسلحة الاخرى التي يتم تصنيعها في المستقبل والتي تشابه في خصائصها الاثر التدميري مع القنبلة الذرية او الاسلحة الأخرى"[٣٩].

ووفقا لهذا التعريف فان الاسلحة غير الحركية كل سلاح يتم تصنيعه في المستقبل له اثر تدميري وهذا يشمل الاسلحة السيبرانية والتي يكون لها اثر تدميري قد يفوق الاثر المتحقق من الاسلحة الحركية التقليدية, اذ ان الهجوم السيبراني الذي يُشن في نطاق العمليات السيبرانية يعرض المدنيين والاعيان المدنية للخطر, وذلك من خلال تعطيل الانظمة المتحكمة بالسدود والمحطات النووية والمستشفيات والمطارات والتي تسبب اضرار اكبر ما تسببه الاسلحة الحركية مما يشكل اثر تدميري هائل.

المطلب الثاني

المسؤولية الدولية المترتبة عن انتهاك السيادة السيبرانية للدول

تعد العمليات السيبرانية احدى الوسائل والاساليب التي تنتهجها الدول في انتهاك سيادة دولة أخرى من خلال استخدام القوة كونها قادرة على شل الانظمة الاقتصادية والامنية والعسكرية والبنى التحتية لدولة ما دون ان تكبد الدولة المعتدية تكاليف باهضه او خسائر في الأرواح, وذلك بالاعتماد على التطور التكنولوجي والعلمي الذي يتميز بالسرعة وسهولة التنفيذ.

وقد واجه مبدأ سيادة الدول نوع جديد من التعدي والانتهاك تمثل بالعمليات السيبرانية عبر الفضاء الالكتروني والتي يكون مصدرها دولة أخرى, وبذلك اصبح للحدود الاقليمية مفهوم

مختلف عن المفهوم التقليدي[٤٥], اذ اصبح مبدأ السيادة يشمل الفضاء السيبراني وما تتصل به من بنية تحتية الكترونية كأجهزة الحاسوب وشبكات الاتصال عبر الانترنت وغيرها, واصبح للدولة سلطة سيادية عليها, على ان تكون هذه السلطة مقيدة بالقواعد العرفية وقواعد قانون الدولي المقننة, ووفقا لذلك فان اي اعتداء على سيادة الدولة عبر فضاءها الالكتروني يكون خاضع الى قواعد القانون الدولي المتعلقة بالمسؤولية الدولية عن انتهاك سيادة الدول.

فاذا كان الاعتداء السيبراني قد حدث في اطار حالة حرب, فالتصرف يخضع لقواعد القانون الدولي الانساني التي تتعلق بالعمليات القتالية وتصرفات المقاتلين, وقد نظم دليل تالين المسؤولية القانونية الناجمة عن الهجمات السيبرانية التي يتم تنفيذها في حالة الحرب السيبرانية, اذ نصت القاعدة (٦) على ان " تتحمل الدولة المسؤولية القانونية الدولية للعمليات السيبرانية التي تنسب اليها والتي تشكل خرق لالتزام دولي".

اما اذا كانت العمليات السيبرانية نفذت في وقت السلم فالمسؤولية في هذه الحالة ناتجة عن خرق قواعد ومبادئ عامة عرفية او مقننة في القانون الدولي العام, وبذلك تُسأل الدولة عن فعل غير مشروع دوليا والذي يمثل خرق لالتزام دولي يقضي بعدم التدخل في الشؤون الداخلية للدول الوارد ذكره في المادة (٢) من ميثاق الامم المتحدة, اذ اشار الميثاق الى ان انتهاك سيادة الدول يكون من خلال انتهاك مبدأين دوليين هما مبدأ عدم التدخل في الشؤون الداخلية للدول ومبدأ عدم استخدام القوة في العلاقات الدولية, اللذان يعتبران حجر الزاوية في العلاقات الدولية.

تعد العمليات السيبرانية العدائية انتهاك لسيادة الدول اذا كانت في سياق تدخل في الشؤون الداخلية لدولة أخرى, وذلك عندما تقوم بإحداث اضرار عند اختراقها الانظمة الحكومية او التدخل في الشؤون الداخلية للدول, فالقيام بالعمليات السيبرانية يرتب مسؤولية دولية بحق الدولة المنتهِكة, اذ لا يجوز لدولة ان تقوم بعمليات سيبرانية تنتهك من خلالها سيادة دولة اخرى قانونا, الا اذا كان لغرض الدفاع عن النفس, فالدولة التي تتعرض الى العمليات السيبرانية وتؤدي الى ضرر مادي باي شكل من الاشكال فهو انتهاك للسيادة السيبرانية لتلك الدولة.

كما اشارت المادة (٤)[٤٦]من مسودة لجنة القانون الدولي عن مسؤولية الدول عن الافعال غير المشروعة والتي تناولت مسؤولية الدولة عن التصرفات الدولية الخاطئة الصادرة عن سلطتها التشريعية والتنفيذية والقضائية, والمادة (٨) التي تضمنت مسؤولية الدول عن تصرفاتها وتصرفات المجموعات التي تسيطر عليها[٤٧].

وقد اخذ القضاء الدولي بمبدأ عدم التدخل في الشؤون الداخلية للدول في قضية الانشطة العسكرية وشبه العسكرية بين نيكاراغوا والولايات المتحدة الامريكية عندما قدم سفير نيكاراغوا طلبا لتسجيل دعوى امام محكمة العدل الدولية ضد الولايات المتحدة الامريكية مدعيا انها قد قامت بتدريب وتجهيز وتسليح وتمويل ومساعدة قوات الكونترا وان هذا السلوك يعتبر انتهاك للمادة (٤/٢) من ميثاق الامم المتحدة واستندت في الدعوى على سيطرة الولايات المتحدة الامريكية الكاملة على قوات الكونترا, في حين عارضت الولايات المتحدة الامريكية هذا الادعاء واختصاص المحكمة في النظر بالدعوى, ولكن المحكمة ردت على هذا الاعتراض وقضت بمسؤولية الولايات المتحدة الامريكية استنادا الى معيار السيطرة الفعالة[٤٨].

والضرر المادي قد يكون على شكل استخدام غير قانوني للقوة او هجوم مسلحا عندما تقوم دولة بعمل ينتهك التزاماتها الدولية, فأنها تصبح مسؤولة دوليا عن ذلك الفعل, اذ تحضر قواعد قانون الدولي التدخل في شؤون الدول باستخدام القوة, بما في ذلك الوسائل السيبرانية.

يتم التدخل في الشؤون الداخلية او الخارجية للدول من خلال العمليات السيبرانية التي تتم بصور رقمية او عبر الوسائل الالكترونية, الامر الذي يسبب تداعيات في العلاقات الدولية وبردود افعال دبلوماسية ضد الدولة التي قامت بالهجوم, وقد يتجاوز الرد بعض الاحيان الاجراء الدبلوماسي الى نزاعات وتوترات بين الدول, اذ يحق للدولة المتضررة بالمطالبة بالتعويض عن الاضرار التي لحقت بها او اتخاذ تدابير مضادة كرد فعل على انتهاك سيادتها السيبرانية, بالاستناد الى حق الدول في الدفاع عن نفسها وفق المادة(٥١) من ميثاق الأمم المتحدة.

فهل تعد العمليات السيبرانية استخدام للقوة؟

اختلفت الاتجاهات الفقهية في تفسير مصطلح (القوة) فالبعض ذهب الى ان مصطلح القوة يعني استخدام القوة المسلحة في اطار عدوان او هجوم مسلح ترتكبه الدول باستخدام قواتها المسلحة او جماعات منظمة تابعة لها, ويذهب راي اخر الى ان القوة بالإضافة الى ذلك يشمل استخدام الضغط الاقتصادي او السياسي[٤٠].

نرى ان استخدام القوة ضد دولة اخرى لا يقتصر على العمليات العسكرية الحركية التقليدية فقط, اذ قد تستخدم الدول قوى غير حركية بهدف تحقيق اهداف عسكرية ومنها العمليات السيبرانية العدائية, حيث لعب الفضاء الالكتروني دورا اساسيا في تنفيذ عمليات ذات فعالية في تحقيق الميزة العسكرية من خلال الاعتماد على وسائل وأساليب لها نفس الأثر في الفضاء الالكتروني عبر الهجوم على انظمة التحكم والسيطرة, لذلك اصبح من الضروري ان يتسع مفهوم القوة ليشمل جميع الوسائل والاساليب المادية وغير المادية والتي لها تأثير مباشر او غير مباشر في تحقيق الاهداف العسكرية, وهكذا اصبح استخدام القوة وانتهاك سيادة الدول يتم عبر الفضاء السيبراني لتلك الدول دون اللجوء الى الطائرات والمتفجرات او الاستيلاء على الأرض, وقد يكون لها تأثير يفوق استخدام القوة التقليدية وذلك بالنظر الى اثاره المدمرة.

مع زيادة المخاطر الامنية على الدول من خلال عمليات الاختراق الالكترونية والذي يؤثر على سيادة الدول واستقلالها من خلال اختراق امنها السيبراني مع ظهور الفضاء الالكتروني وسهولة اختراقه اصبحت دائرة الاستهداف اكثر اتساعا بالإضافة الى زيادة عدد المهاجمين وعدد الاهداف المراد اختراقها, ما دفع الدول الى العمل على تطوير قدرتها وادواتها الهجومية والدفاعية الالكترونية وتعزيز التنافس والسيطرة على المعلومات عبر الفضاء الالكتروني وزيادة نفوذها وتأثيرها على نطاق دولي, وبدأت الدول استخدام شتى انواع اسلحة التدمير الممكنة, وبذلك تغيرت وسائل واساليب انتهاك سيادة الدول من حالة اعتداء على الاراضي واستيلاء على الموارد الى التحكم بأراداته وخياراته من خلال استيلاء على المعلومات المرتبطة بالبنى التحتية والتحكم بها[٤١].

هكذا اصبح الصراع بين الدول لا يعد صراعا تقليديا بل اتخذ شكلا اكثر تعقيدا وتداخل من خلال شن الحروب الالكترونية واسعة النطاق والتي تتخذ اشكالا متعددة تتمثل بالاختراقات

والتجسس وسرقة المعلومات, وهي بذلك لا ترقى الى عمل عسكري, انما عمليات تتصف بانها قليلة التكلفة قياسا بالعمليات الحركية التقليدية, وقد يكون مصدرها مجموعة من الافراد او دولة او شركات.

وبعد التقدم الهائل في مجال الذكاء الاصطناعي اصبح من الممكن ان تنفذ هذه الهجمات من قبل روبوت من اي موقع جغرافي, اذ ان ما كان يعتبر من اسرار الدولة التي لا تستطيع الدول الاخرى الاطلاع عليها تحول بعد الثورة التكنولوجية الى معلومات في متناول جميع الدول وخاصة الدول التي تتحكم في الاقمار الاصطناعية سواء تعلق الامر بقدرات اقتصادية او عسكرية او بالبنى التحتية, الامر الذي عرض سيادة الدول الى الانتهاك عبر الفضاء الالكتروني.

الخاتمة:

بعد ان اتممنا الدراسة المتعلقة بموضوع انتهاك السيادة السيبرانية للدول وفق قواعد القانون دولي العام توصلنا الى مجموعة من النتائج والتوصيات تجمع بين الجوانب القانونية والفنية كون ان العمليات السيبرانية والتطور التكنلوجي يتحرك بسرعة كبيرة مما يتوجب معه سرعة تطور القواعد القانونية كي تواكب هذا التطور.

أولا: النتائج

١- مبدأ احترام سيادة الدول من المبادئ الأساسية في العلاقات الدولية باعتبار ان السيادة ركن أساسي تبنى عليه نظرية الدولة.
٢- تعرض مفهوم السيادة الى تحولات جوهرية من حيث المدلول والمفهوم والمحتوى القانوني بعد ان نشأ ما يُعرف بالفضاء السيبراني, بسبب الاحداث المعاصرة التي يمر بها المجتمع الدولي.
٣- الفضاء السيبراني هو مجال افتراضي عالمي يتم من خلاله انشاء وتخزين وتبادل المعلومات عبر شبكات الانترنت.
٤- السيادة السيبرانية مفهوم حديث يمثل جانب من جوانب سيادة الدول واصبح من الميادين الحيوية التي تستوجب بذل جهود من اجل حمايته.
٥- العمليات السيبرانية هي تصرفات تدور في مجال عالم افتراضي من خلال استخدام بيانات رقمية ووسائل اتصال تعمل الكترونيا, وقد تكون هذه العمليات عدائية لغرض تحقيق اهداف عسكرية او سياسية او استخباراتية.
٦- تتسم العمليات السيبرانية العدائية بانها غير ملموسة وغير مادية, مما يصعب معها معرفة مرتكب العمليات السيبرانية, اضافة الى سهولة اخفاء هوية مرتكب العمليات السيبرانية, ومن ثم صعوبة اسناد المسؤولية الدولية.
٧- تختلف العمليات السيبرانية العدائية عن العمليات الحركية العدائية التقليدية من حيث طبيعة الاسلوب والوسيلة المستخدمة.
٨- تتحمل الدول المسؤولية الدولية القانونية عن العمليات السيبرانية التي تنسب اليها والتي تشكل خرق لالتزام دولي.

ثانيا: التوصيات

١- وضع تعريف دولي موحد لمفهوم السيادة السيبرانية من قبل مجموعة من الخبراء الدوليين وعبر الأمم المتحدة, بحيث يتم تحديد نطاق التطبيق ومعايير انتهاك السيادة, ومسؤولية الدول عند خرقها.

٢- تطوير قواعد ملزمة دوليا وحاكمة تنظم السلوك السيبراني بين الدول, وذلك من خلال معاهدة دولية ملزمة يوقع عليها اكبر عدد من الدول تستند اليها الدول في حالة انتهاك سيادتها السيبرانية, يمكن من خلالها تحديد القواعد المتعلقة بالعمليات السيبرانية, ويحدد من خلالها مبدأ المسؤولية الدولية عن الأفعال السيبرانية, وبيان طريقة اسناد العملية السيبرانية إلى دولة ما.

٣- ضرورة إنشاء آلية تحقيق دولية متخصصة في العمليات السيبرانية وتعزيز الحماية القانونية للبنى التحتية الحيوية للدول من خلال إدراج البنى الرقمية ضمن الأعيان المدنية المحمية بحيث يعد استهداف شبكات الكهرباء او المستشفيات والمياه والاتصالات او التدخل السياسي بالتأثير على الانتخابات عبر العمليات السيبرانية بمثابة انتهاك لسيادة الدولة وعمل عدواني غير مشروع.

٤- تعزيز التعاون الدولي في تحقيق المشاركة الدولية في الانذار المبكر ومواجهة العمليات السيبرانية العدائية من خلال مراكز إقليمية لمشاركة المعلومات الاستخباراتية أو آليات إنذار مشتركة بين الدول تسهل عملية اكتشاف مصدر الاعتداء السيبراني, وذلك لتقليل الاثار المادية الضارة للعمليات السيبرانية المعادية.

٥- تعزيز الشفافية بين الدول حول العقائد العسكرية السيبرانية من خلال اعلان الدول عن سياساتها الدفاعية السيبرانية, عبر توضيح مفهوم الاستخدام المشروع للقوة في الفضاء السيبراني.

٦- بناء قدرات الدول النامية في مجال الأمن السيبراني, لأن الدول ذات البنية الضعيفة تكون أهدافا سهلة, وذلك من خلال تقديم دعم تقني دولي وتدريب الكوادر الحكومية وتطوير التشريعات الوطنية لتتلاءم مع القانون الدولي.

٧- موائمة التشريعات الوطنية مع قواعد القانون الدولي, بوضع قواعد قانونية للدول تحدد من خلالها المسؤولية عن العمليات السيرانية داخل اقليمها.

٨- إنشاء آلية دولية لتسوية النزاعات السيبرانية من خلال محكمة دولية تتولى مهمة الفصل في النزاعات السيبرانية الدولية, او دائرة خاصة داخل محكمة العدل الدولية أو آلية تحكيم سيبراني دولي, الغرض منها هو البت في قضايا انتهاك السيادة السيبرانية.

٩- العمل على إيجاد طرق ميسرة لتحليل المعلومات الضخمة واختزالها في المجال السيبراني لمواجهة اخطار اتساع استخدام الفضاء السيبراني.

١٠- المحافظة على الامن السيبراني للدول من خلال أدوات القوة المتعلقة بالوسائل والطاقات والامكانيات المادية وغير المادية والتحكم والسيطرة على المعلومات وأجهزة الحاسوب وشبكات الانترنت والبنية التحتية من خلال تدريب كوادر ومهارات بشرية لها الدور المؤثر في حماية الامن السيبراني للدول.

الهوامش:

(١) تنص المادة (١/٢) من ميثاق الأمم المتحدة (تقوم الهيئة على مبدأ المساواة في السيادة بين جميع أعضائها).
(٢) محمد القاسمي, مبادئ القانون الدولي العام, منشورات الحلبي الحقوقية, بيروت, ٢٠١٥, ص٢٢٣.
(٣) سارة عبد الله سعيد, تأثير قواعد القانون الدولي العام على مفهوم السيادة الوطنية في ضوء المعاهدات الدولية, المجلة العربية للنشر العلمي, الإصدار السابع, العدد ٧٢, ٢٠٢٥, ص١٢٨.
(٤) عمر الحضرمي, جدلية السيادة والقانون الدولي, فضاءات المطلق وقيود الالتزام, ط١, دار جرير للنشر والتوزيع, عمّان, ٢٠١٧, ص٢٠.
(٥) مشار اليه عند د. منال وجدي علي, مفهوم السيادة والسلطة المطلقة في فلسفة جان بودان, مجلة كلية الآداب والعلوم الإنسانية, المجلد الرابع, العدد ٣٩, ٢٠٢١, ص١١٧.
(٦) Jochen Von Bernstorff, the international law theory of Hans Kelsen, Cambridge studies in international and comparative law, Cambridge MA: Cambridge university press, 2010, p. 66.
(٧) Oppenheim ,s international law, Vol. l: peace, 9thed. London: longman, Robert Y. Jennings and Arthur, 1996, p. 25.
(٨) ميلود بن عبد العزيز ونورة عبد الله, العلاقة بين مبدأي السيادة الإقليمية وحق تقرير المصير في ضوء القانون الدولي العام, مجلة المفكر, العدد ١٦, ٢٠١٧, ص١٥٩.
(٩) محمد ممدوح الهذال, اثر التحولات الدولية على مفهوم السيادة الوطنية, رسالة ماجستير, جامعة ال البيت, ٢٠١٩, ص٨.
(١٠) د. سامي الطيب ادريس محمد, دواعي واثار خرق السيادة في ظل المتغيرات الدولية, مجلة الدراسات القانونية والاقتصادية, المجلد العاشر, العدد الثاني, ٢٠٢٤, ص١٤١٢.
(١١) موجز الاحكام والفتاوى والاوامر الصادرة عن محكمة العدل الدولية, الوثيقة(ST/LEG/SER-F/1)، ١٩٤٨-١٩٩١. ص٣.
(١٢) د. سامي الطيب ادريس محمد, مرجع سابق, ص١٤١٣.
(١٣) د. وائل الهنيدي, سيكولوجية الامن السيبراني فهم العقول وحماية البيانات , ط١, دار ابهار للتوزيع والنشر, الامارات, ٢٠٢٤, ص١٢.
(١٤) مشار اليه عند نور الدين حامد علي إبراهيم, الفضاء السيبراني: المفاهيم والابعاد, المجلة العلمية للبحوث والدراسات التجارية, المجلد ٣٨, العدد ٢, ٢٠٢٤, ص٧٢١.
(١٥) د. لامية طالة, الإرهاب السيبراني والامن القومي, قراءة في تحولات الاستراتيجية الدفاعية, حوليات جامعة الجزائر, المجلد ٣٥, العدد الرابع, ٢٠٢١, ص٣٥٦.
(١٦) مشار اليه عند نور الدين حامد علي إبراهيم, مرجع سابق, ص٧٢١.
(١٧) Joseph S. Nye, Syber power, Belfer center for science and international affairs, Harvard Kennedy school, Cambridge, May 2010, p.3.
(١٨) محمد محمود زيتون, العمليات السيبرانية وتأثيرها على تحولات السيادة في الفضاء السيبراني, المجلة العربية للنشر العلمي, الإصدار الثامن العدد ٧٧, اذار ٢٠٢٥, ص١٦٠.
(١٩) المرجع نفسه, ص١٦١.
(٢٠) الذكاء الاصطناعي هو "جزء من علوم الحاسب الالي الذي يهدف لمحاكاة قدرة معرفية لاستبدال الانسان في اداء وظائف مناسبة في سياق معين اعتمادا على الذكاء الالي" ينظر د. فاطمة الزهراء بلحمو, مساهمة الأنظمة الخبيرة في تحسين اتخاذ القرار في المؤسسات, جامعة أبوبكر بلفايد, الجزائر, ٢٠١٧, ص٩٦.
(٢١) محمد محمود زيتون, مرجع سابق, ص١٦٢.

(٢٢) أسامة صبري محمد, الحرب الالكترونية ومبدأ التمييز في القانون الدولي الإنساني, مجلة القانون للدراسات والبحوث القانونية , مجلد ٢٠١٣ , العدد ٧, ٢٠١٣, ص٥.
(٢٣) نسيب نجيب, الحرب السيبرانية من منظور القانون الدولي الإنساني, المجلة النقدية للقانون والعلوم السياسية , كلية الحقوق والعلوم السياسية, جامعة تيزي وزو, مجلد ١١٦, العدد ٤, ٢٠٢١, ص ٢٢٢.
(٢٤) مشار اليه عند د. حيدر كاظم عبد علي ود. رباب محمود عامر, التنظيم القانوني للهجمات السيبرانية على المنشآت ذات القوى الخطرة, مجلة الكوفة للعلوم القانونية والسياسية, مجلد ١٢, العدد ٤٧, ٢٠٢٠, ص١١٠.
(٢٥) اماني تموز عبد الرحمن الخفاجي, الحماية التأمينية للشركات التجارية من المخاطر السيبرانية, رسالة ماجستير قدمت الى مجلس كلية القانون , جامعة ميسان, ٢٠٢٤, ص١٠.
(٢٦) Michael N. schmit "Tallinn manual on the international law applicable to cyber warfare", Cambridge university press, first publishes, 2013, p.92.
(٢٧) د. يحيى ياسين سعود, الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني, المجلة القانونية, جامعة القاهرة, كلية الحقوق, ٢٠١٨, ص٨٥.
(٢٨) نسيب نجيب, مرجع سابق, ص٢٢٣.
(٢٩) د. احمد عبيس الفتلاوي وقاسم محمد مهدي الغزي, الدليل الى فهم جريمة العدوان السيبرانية, دراسة في اطار مواجهة قانونية وسياسية فاعلة, ط١, منشورات زين الحقوقية, بيروت, ٢٠٢٥, ص٥٣.
(٣٠) عبد الرحمن شامل عبد الرحمن, الطبيعة القانونية للهجمات السيبرانية في ضوء القانون الدولي الإنساني, مجلة النور للدراسات القانونية, المجلد ١, العدد ٢, ٢٠٢٤, ص٦٢.
(٣١) د. علي زياد العلي, ود. علي حسين حميد, تكتيكات الحروب الحديثة والامن السيبراني والحروب المعززة والهجينة, ط١, العربي للنشر والتوزيع, القاهرة, ٢٠٢٣, ص٣٧.
(٣٢) نسيب نجيب, مرجع سابق, ص١١٠.
(٣٣) مشار اليه عند خديجة بن قطاط, تداعيات الحروب السيبرانية على السيادة الرقمية, مجلة القانون العام الجزائري والمقارن, مجلد ١٠, العدد الثاني, ٢٠٢٤, ص٢٨٣.
(٣٤) د. حازم محمد موسى وجاسم محمد عز الدين, الطبيعة القانونية للحروب والنزاعات السيبرانية من منظور القانون الدولي, كلية القانون والعلاقات الدولية, جامعة الكتاب, بلا سنة نشر, ص٤٥.
(٣٥) مشار اليه عند نسيب نجيب, مرجع سابق, ص١١١.
(٣٦) نور الدين حامد علي إبراهيم, مرجع سابق, ص٧٢٨.
(٣٧) د. حيدر كاظم عبد علي ود. رباب محمود عامر, مرجع سابق, ص١١٨.
(٣٨) موجز الاحكام والفتاوى الصادرة عن محكمة العدل الدولية, مرجع سابق, ١٩٩٢-١٩٩٦, ص١٠٧.
(٣٩) دراسة منشورة على الموقع الالكتروني https://disarmament.unoda.org/ar/our-work/conventional-arms تمت الزيارة بتاريخ ٢٠٢٥/١٢/١
(٤٠) د. احمد عبيس الفتلاوي وزهراء عماد محمد, تكييف الهجمات السيبرانية في ضوء القانون الدولي, مجلة الكوفة للعلوم القانونية والسياسية, مجلد ٤٤, العدد ١, كلية القانون والعلوم السياسية, جامعة الكوفة, ٢٠٢٠, ص٥٧.
(٤١) نصت المادة (٤) من مسودة لجنة القانون الدولي على مسؤولية الدول عن الافعال غير المشروعة على ان (١- يعد تصرف اي جهاز من اجهزة الدولة فعلا صادرا عن هذه الدولة بمقتضى القانون الدولي, سواء كان الجهاز يمارس وظائف التشريعية ام تنفيذية ام قضائية ام اية وظائف أخرى, وايا كان المركز الذي يشغله في تنظيم الدولة, وسواء كانت صفته انه جهاز من اجهزة الحكومة المركزية ام جهاز من اجهزة وحدة اقليمية من وحدات الدولة, ٢- يشمل الجهاز اي شخص او كيان له ذلك المركز وفقا للقانون الداخلي للدولة), تقرير لجنة القانون الدولي ٢٠٠١ , الدورة (٥٣), الوثيقة A/CN.4/SER.A/2001/ADD.IC.PART2.
(٤٢) نصت المادة (٨) من مسودة لجنة القانون الدولي عن مسؤولية الدول عن الافعال غير المشروعة على انه (يعتبر فعلا صادرا عن الدولة بمقتضى القانون الدولي تصرف شخص او مجموعة من الاشخاص اذا كان الشخص او مجموعة الاشخاص يتصرفون في الواقع بناء على تعليمات تلك الدولة او توجيهات منها او تحت رقابتها لدى القيام بذلك التصرف), المرجع نفسه.
(٤٣) موجز الاحكام والفتاوى والاوامر الصادرة عن محكمة العدل الدولية, مرجع سابق, ص١٦٧.
(٤٤) د. يحيى ياسين سعود, مرجع سابق,ص٨٩.
(٤٥) عادل عبد الصادق, أنماط الحرب السيبرانية وتداعياتها على الامن العالمي السياسية والدولية, القاهرة, ٢٠١١, ص١٧.

قائمة المراجع:

أولا: الكتب باللغة العربية

١. د. احمد عبيس الفتلاوي وقاسم محمد مهدي الغزي, الدليل الى فهم جريمة العدوان السيبرانية, دراسة في اطار مواجهة قانونية وسياسية فاعلة, ط١, منشورات زين الحقوقية, بيروت, ٢٠٢٥.
٢. حازم محمد موسى وجاسم محمد عز الدين, الطبيعة القانونية للحروب والنزاعات السيبرانية من منظور القانون الدولي, كلية القانون والعلاقات الدولية, جامعة الكتاب, بلا سنة نشر.
٣. عادل عبد الصادق, أنماط الحرب السيبرانية وتداعياتها على الامن العالمي السياسية والدولية, القاهرة, ٢٠١١.
٤. د.على زياد العلي, ود. علي حسين حميد, تكتيكات الحروب الحديثة والامن السيبراني والحروب المعززة والهجينة, ط١, العربي للنشر والتوزيع, القاهرة, ٢٠٢٣.
٥. عمر الحضرمي, جدلية السيادة والقانون الدولي, فضاءات المطلق وقيود الالتزام, ط١, دار جرير للنشر والتوزيع, عمّان, ٢٠١٧.
٦. محمد القاسمي, مبادئ القانون الدولي العام, منشورات الحلبي الحقوقية, بيروت, ٢٠١٥.
٧. وائل الهنيدي, سيكولوجية الامن السيبراني فهم العقول وحماية البيانات , ط١, دار ابهار للتوزيع والنشر, الامارات, ٢٠٢٤.

ثانيا: الرسائل والاطاريح الجامعية

١. اماني تموز عبد الرحمن الخفاجي, الحماية التأمينية للشركات التجارية من المخاطر السيبرانية, رسالة ماجستير قدمت الى مجلس كلية القانون , جامعة ميسان, ٢٠٢٤.
٢. محمد ممدوح الهذال, اثر التحولات الدولية على مفهوم السيادة الوطنية, رسالة ماجستير, جامعة ال البيت, ٢٠١٩.

ثالثا: البحوث والمجلات

١. د.احمد عبيس الفتلاوي وزهراء عماد محمد, تكييف الهجمات السيبرانية في ضوء القانون الدولي, مجلة الكوفة للعلوم القانونية والسياسية, مجلد ٤٤, العدد ١, كلية القانون والعلوم السياسية, جامعة الكوفة, ٢٠٢٠.

٢. أسامة صبري محمد, الحرب الالكترونية ومبدأ التمييز في القانون الدولي الإنساني, مجلة القانون للدراسات والبحوث القانونية , مجلد ٢٠١٣ , العدد ٧, ٢٠١٣.
٣. حيدر كاظم عبد علي ود. رباب محمود عامر, التنظيم القانوني للهجمات السيبرانية على المنشآت ذات القوى الخطرة, مجلة الكوفة للعلوم القانونية والسياسية, مجلد ١٢, العدد ٤٧, ٢٠٢٠.
٤. خديجة بن قطاط, تداعيات الحروب السيبرانية على السيادة الرقمية, مجلة القانون العام الجزائري والمقارن, مجلد ١٠, العدد الثاني, ٢٠٢٤.
٥. سارة عبد الله سعيد, تأثير قواعد القانون الدولي العام على مفهوم السيادة الوطنية في ضوء المعاهدات الدولية, المجلة العربية للنشر العلمي, الإصدار السابع, العدد ٧٢, ٢٠٢٥.
٦. سامي الطيب ادريس محمد, دواعي واثار خرق السيادة في ظل المتغيرات الدولية, مجلة الدراسات القانونية والاقتصادية, المجلد العاشر, العدد الثاني, ٢٠٢٤.
٧. عبد الرحمن شامل عبد الرحمن, الطبيعة القانونية للهجمات السيبرانية في ضوء القانون الدولي الإنساني, مجلة النور للدراسات القانونية, المجلد ١, العدد ٢, ٢٠٢٤.

٨. لامية طالة, الإرهاب السيبراني والامن القومي, قراءة في تحولات الاستراتيجية الدفاعية, حوليات جامعة الجزائر, المجلد ٣٥, العدد الرابع, ٢٠٢١.
٩. محمد محمود زيتون, العمليات السيبرانية وتأثيرها على تحولات السيادة في الفضاء السيبراني, المجلة العربية للنشر العلمي, الإصدار الثامن العدد ٧٧, اذار ٢٠٢٥.
١٠. منال وجدي علي, مفهوم السيادة والسلطة المطلقة في فلسفة جان بودان, مجلة كلية الآداب والعلوم الإنسانية, المجلد الرابع, العدد ٣٩, ٢٠٢١.

١١. ميلود بن عبد العزيز ونورة عبد الله, العلاقة بين مبدأي السيادة الإقليمية وحق تقرير المصير في ضوء القانون الدولي العام, مجلة المفكر, العدد ١٦, ٢٠١٧.
١٢. نسيب نجيب, الحرب السيبرانية من منظور القانون الدولي الإنساني, المجلة النقدية للقانون والعلوم السياسية , كلية الحقوق والعلوم السياسية, جامعة تيزي وزو, مجلد ١١٦, العدد ٤, ٢٠٢١.
١٣. نور الدين حامد علي إبراهيم, الفضاء السيبراني: المفاهيم والابعاد, المجلة العلمية للبحوث والدراسات التجارية, المجلد ٣٨, العدد ٢, ٢٠٢٤.

رابعا: المواثيق والتقارير الدولية
١- ميثاق الأمم المتحدة الصادر عام ١٩٤٥.
٢- موجز الاحكام والفتاوى والاوامر الصادرة عن محكمة العدل الدولية, الوثيقة (ST/LEG/SER-F/1).
٣- دليل تالين بشأن القانون الدولي المطبق على الحروب السيبرانية.

خامسا: المواقع الالكترونية
الموقع الالكتروني https://disarmament.unoda.org/ar/our-work/conventional-arms
سادسا: المراجع باللغة الإنكليزية
1. Jochen Von Bernstorff, the international law theory of Hans Kelsen, Cambridge studies in international and comparative law, Cambridge MA: Cambridge university press, 2010.
2.Joseph S. Nye, Syber power, Belfer center for science and international affairs, Harvard Kennedy school, Cambridge, May 2010.
3.Michael N. schmit "Tallinn manual on the international law applicable to cyber warfare", Cambridge university press, first publishes, 2013.
Oppenheim ,s international law, Vol. l: peace, 9thed. London: longman, 4.Robert Y. Jennings and Arthur, 1996.