# الفضاء السيبراني والقانون الدولي

## Cyberspace and international law


إعداد

د / مريم عبد العزيز بن غيث

أستاذ مساعد بقسم القانون الدولى

كلية الحقوق- جامعة الكويت

**Mrs. Dr. Maryam Abdulaziz Bin Ghaith**

***Assistant Professor at the Department of International Law Faculty of Law - Kuwait University.***

# الفضاء السيبراني والقانون الدولي

**الملخص:**

تعد تكنولوجيا المعلومات أو ما يعرف بالفضاء السيبراني أمرا بالغ الأهمية في عالمنا اليوم، حيث لا يستغنى عن الفضاء السيبراني في أعمالنا اليومية وعلى صعيد الدول، حيث يستخدم الفضاء السيبراني في جميع القطاعات من المستشفيات والبنوك، حتى عمليات المرور والعديد من الأمور، وأصبح وضعُ تنظيمٍ دولي للفضاء السيبراني أمرا في غاية الأهمية؛ نظرا للخطورة التي يشكلها الهجوم السيبراني والعمليات السيبرانية ضد البنى التحتية للدولة، وهنا يكون السؤال، هل القانون الدولي ينطبق على الفضاء السيبراني؟ والسؤال الأهم هو كيف يكون تطبيق القانون الدولي على الفضاء السيبراني؟ ولقد حاول العديد من الفقهاء الإجابة على هذا السؤال وسطروا بإجابتهم على السؤالين السابقين العديد من الآراء، فأصبح لدينا اليوم دليل (تالين) الأول والثاني والذي وضعه مجموعة من الفقهاء، وأيضا شكلت الجمعية العامة للأمم المتحدة مجموعة من الخبراء الحكوميين في محاولة لتقنين ولتنظيم الفضاء السيبراني وكيفية انطباق القانون الدولي عليه، والجدير بالذكر أن كلا المحاولتين نتج عنهما عدة قواعد تنظم وتجيب عن كيفية انطباق القانون الدولي على الفضاء السيبراني، إلا أن هذه المحاولات نتج عنها قواعد غير ملزمة مما حدا بالدول للإعلان عن توجهاتها فيما يتعلق بالفضاء السيبراني والقانون الدولي، ومنها قد نستشف كيفية انطباق القانون الدولي على الفضاء السيبراني فقد اتفقت جميع الدول والفقهاء على أن القانون الدولي ينطبق في الفضاء السيبراني.

**Abstract**

Information technology, or what is known as cyberspace, is of utmost importance in our world today, as cyberspace is indispensable in our daily work and at the level of countries, as cyberspace is used in all sectors, from hospitals and banks to traffic operations and many other matters. Establishing an international regulations for cyberspace has become extremely important due to the danger posed by cyberattacks and cyber operations against the country's infrastructure. Here the question is: Does International Law apply to cyberspace? The most important question is how does International Law apply to cyberspace? Many jurists have tried to answer this question and have written many opinions to answer such questions. Today, we have the first and second Tallinn Manual, which was developed by a group of jurists. The United Nations General Assembly also formed a group of governmental experts in an attempt to codify and regulate cyberspace and how International Law applies. It is worth noting that both attempts resulted in the consensus that International Law applies to cyberspace. However, these attempts resulted in non-binding rules, which prompted countries to announce their positions regarding cyberspace and international law. From this, we can infer how international law applies to cyberspace. All countries and jurists have agreed that international law applies to cyberspace.

## المقدمة

نظرا للتقدم التكنولوجي أصبح العالم قرية صغيرة، كما أصبح لدينا ما يسمى بالفضاء السيبراني، ونتيجة للتطور المتعلق به أصبح لدينا عدة أسئلة تستوجب الإجابة عنها، وقد حاول الفقهاء الجواب عن بعض هذه الأسئلة، إلا أننا لم نصل بعد إلى إجابات حاسمة وأعراف يمكن للدول الرجوع لها، ولقد حاولت مجموعة من الدول وضع تصور للعلاقة بين القانون الدولي والفضاء السيبراني، كما قام مجموعة من الفقهاء بالنظر في هذه العلاقة ووضع تصور لكيفية انطباق القانون الدولي على الفضاء السيبراني، وكان ذلك على المستويين الإقليمي والدولي، فقد قام عدد من الفقهاء التابعين لمنظمة (الناتو) بتبني دليل (تالين) لبيان مدى انطباق القانون الدولي على الفضاء السيبراني، كما قام مجموعة من الفقهاء -بناء على طلب الجمعية العامة للأمم المتحدة- بوضع تصور لكيفية انطباق القانون الدولي على الفضاء السيبراني، وقد توصلت هاتان المجموعتان إلى استنتاج واحد وهو أن القانون الدولي ينطبق على الفضاء السيبراني، وكان هناك بعض التباين في كيفية انطباق القانون الدولي على الفضاء السيبراني، وهذا التباين أيضا يوجد في الإعلانات الخاصة بالدول المتعلقة بكيفية انطباق القانون الدولي على الفضاء السيبراني، فهناك من توافقت آراؤه مع الفقهاء الدوليين، وهناك من اختلفت آراؤه معهم، إلا أن الجميع اتفق على انطباق القانون الدولي والقانون الدولي الإنساني في الفضاء السيبراني.

ونظرا للتطور السريع في مجال الفضاء السيبراني أصبح لدينا عدد من الهجمات السيبراني في مجال الاتصالات والحواسيب الإلكترونية، والجدير بالذكر أن الهجمات

السيبرانية ليست أمرا حديثا ورغم ذلك تطورت تطورا هائلا منذ استخدام الإنترنت، وقد يخطر ببال شخص أن الهجمات السيبرانية حديثة العهد، وذلك ليس صحيحا، فأول هجوم سيبراني كان في عام ١٨٣٤ عندما قام مجموعة من المجرمين باختراق نظام التلغراف الفرنسي؛ وذلك لسرقة المال، ومن الأمثلة -التي حدثت في السنوات الأخيرة أيضا- الهجوم الروسي السيبراني على المواقع الإلكترونية الأوكرانية، وأيضا الهجوم الذي شُنَّ على المواقع النووية الإيرانية، وغيرها الكثير من الهجمات التي قد لا نعلم عن الكثير منها؛ وذلك لعدم إعلان الدول عن تعرضها لهذه الهجمات. وتعد هذه الهجمات مخالفة للقانون الدولي لأن القانون الدولي -كما سبق - ينطبق على الفضاء السيبراني

ومنذ ذلك الحين تطورت الهجمات السيبرانية، ومن الهجمات السيبرانية الحديثة قيام روسيا بهجمات سيبرانية خبيثة ضد عدد من الشركات والحكومات الأوروبية عام ٢٠١٨[(١)]، هذا بالإضافة إلى هجوم إيراني على عدد من الجامعات الأوروبية والأمريكية في عام ٢٠١٨ أيضا[(٢)]، كما أن منطقتنا لم تخلو من الاستهداف السيبراني فقد تعرضت البنى التحتية السعودية للطاقة لهجمات عام ٢٠١٠ و٢٠١١[(٣)]، إضافة إلى تعرض شركة غاز في قطر إلى هجمات سيبرانية عام ٢٠١٢ وتكررت مرة أخرى في عامي ٢٠١٦ و٢٠١٧[(٤)].

(1) Harriet Moynihan, The Application of International Law to state Cyberattacks Sovereignty and Non-intervention, Chatham House, December 2019, page 4.

(2) Id.

(٣) عبدالرحمن فهد أحمد، (٢٠٢٣)، الإطار القانوني للأمن السيبراني لدول مجلس التعاون الخليجي، مجلة دراسات الخليج والجزيرة العربية، ٤٩ (١٩٠)، ٢٦٠.

(٤) مرجع سابق ص ٢٦٠.

ورغم ذلك فالهجمات السيبرانية ليست موضوع هذا البحث، فالبحث يركز على كيفية انطباق القانون الدولي على الفضاء السيبراني حيث ما زالت الدول تعمل على توحيد توجهاتها في هذا المجال، وما زال هناك اختلاف في الفقه فيما يتعلق بكيفية انطباق القانون الدولي على الفضاء السيبراني، ويقوم البحث بدراسة المبدأين الرئيسين في القانون الدولي، وهما مبدأ السيادة ومبدأ عدم التدخل وكيفية انطباقهما على الفضاء السيبراني.

**أهمية البحث:**

يلعب الفضاء السيبراني دورا هاما في تعاملات الدول والأفراد، وهناك من يسيئ استعمال الفضاء السيبراني، سواء على صعيد الافراد أو الدول، وسيكون اهتمامنا في هذا البحث باستعمال الدول للفضاء السيبراني، ونظرا لذلك الدور الهام للفضاء السيبراني في كل شؤون الدول أصبح من المهم تسليط الضوء على القوانين الدولية التي تنظم هذا الفضاء، وتوجهات الدول المختلفة فيما يتعلق بالفضاء السيبراني والقانون الدولي.

**إشكالية البحث:**

تكمن إشكالية البحث في عدم وجود اتفاقية دولية متعلقة بالفضاء السيبراني والقانون الدولي، نعم هناك اتفاقيات متعلقة بالجريمة السيبرانية، إلا أنه -وكما سوف نلاحظ- لا يوجد توافق دولي ملزم للدول، كل ما يوجد عبارة عن آراء للفقهاء في موضوع الفضاء السيبراني والقانون الدولي وهي آراء غير ملزمة .

**أهداف البحث:**

يهدف البحث إلى توضيح الآراء المختلفة المتعلقة بالفضاء السيبراني والقانون الدولي وكيفية انطباق القانون الدولي على الفضاء السيبراني وموقف الدول المتعلق بهذا الشأن.

**أسئلة البحث**:

تتلخص أسئلة البحث في ما يلي:

١. هل ينطبق القانون الدولي على الفضاء السيبراني؟

٢. كيفية انطباق القانون الدولي على الفضاء السيبراني؟

٣. ما موقف الفقه من الفضاء السيبراني والقانون الدولي؟

٤. ما موقف الدول من الفضاء السيبراني والقانون الدولي؟

٥. ما أهم المبادئ الدولية التي تنطبق على الفضاء السيبراني؟

**منهجية البحث**:

استُعمل في هذا البحث منهجان، وهما المنهج الوصفي والمنهج التحليلي، حيث تم الاعتماد على وصف موضوع الدراسة، وتحليله من مختلف النواحي.

**خطة البحث:**

المبحث الأول: ماهية الفضاء السيبراني

المطلب الأول: تعريف الفضاء السيبراني والمصطلحات المشابهة له

المبحث الثاني: كيفية انطباق القانون الدولي على الفضاء السيبراني

- المطلب الأول: مبدأ السيادة
- المطلب الثاني: مبدأ عدم التدخل

المبحث الثالث: موقف الدول من الفضاء السيبراني والقانون الدولي

المطلب الأول: موقف الولايات المتحدة الأمريكية

المطلب الثاني: موقف الاتحاد الأوروبي

المطلب الثالث: موقف المملكة المتحدة

المطلب الرابع: موقف الاتحاد الإفريقي

## المبحث الأول

## ماهية الفضاء السيبراني

سينتظم الحديث في هذا المبحث عن مطلب بعنوان: تعريف الفضاء السيبراني والمصطلحات المشابهة له، وذلك بقصد إيضاح وتحرير المصطلح بغية زيادة البيان، فمن المعروف أن الحكم على الشيء فرع عن تصوره، وهذا ما سيتناوله ذلك المطلب على النحو الآتي.

### المطلب الأول

### تعريف الفضاء السيبراني والمصطلحات المشابهة له

في هذا المطلب سيكون الكلام عن كلمة سيبراني، وماذا تعني؟ ولقد درج مؤخرا استعمال مصطلح سيبراني سواء كان الأمن السيبراني والهجوم السيبراني وغيرهما من المصطلحات، فمن أين أتت هذه المصطلحات؟ وماذا تعني؟

**كلمة سيبراني أو cyber:**

يرجع ظهور مصطلح الفضاء السيبراني إلى العام ١٩٨٢م على يد كاتب الخيال العلمي ويليام جيبسون[(١)]، حيث جمع جيبسون كلمت Cybernetics التي تعني علم

(١) د. علاء الدين فرحات، الفضاء السيبراني: تشكيل ساحة المعركة في القرن الحادي والعشرين، جامعة الوادي، مجلة العلوم القانونية والسياسية، المجلد ١٠، العدد ٣، ديسمبر ٢٠١٩، ص ٩٠.
=

التحكم الآلي مع كلمة فضاء space مكونا كلمة cyberspace أو الفضاء السيبراني[١]، كما هو مستعمل بالاصطلاح العربي، وقد انتشر هذا المصطلح مع انتشار شبكات الإنترنت في العالم، كما قام جيبسون بشرح كلمة الفضاء السيبراني في كتابه شارحا المصطلح بأنه يعني إنشاء شبكة كمبيوتر في عالم مليء بالذكاء الاصطناعي[٢].

ويعد مصطلح الفضاء السيبراني مصطلحًا حديثًا نسبيا، حيث ظهر هذا المصطلح بظهور تكنولوجيا المعلومات، ولا يوجد تعريف متفق عليه لذلك المصطلح، ويختلف مصطلح الفضاء السيبراني عن مصطلح الهجوم السيبراني والإرهاب السيبراني والجريمة السيبرانية، والأمن السيبراني فماذا تعني كل من هذه المصطلحات؟ إن هذا ما ستنتظم الإجابة عنه فيما يلي:

---

=

http://dspace.univ-eloued.dz/bitstream/123456789/5415/1/%d8%a7%d9%84%d9%81%d8%b6%d8%a7%d8%a1%20%d8%a7%d9%84%d8%b3%d9%8a%d8%a8%d8%b1%d8%a7%d9%86%d9%8a_%20%d8%aa%d8%b4%d9%83%d9%8a%d9%84%20%d8%b3%d8%a7%d8%ad%d8%a9%20%d8%a7%d9%84%d9%85%d8%b9%d8%b1%d9%83%d8%a9%20%d9%81%d9%8a%20%d8%a7%d9%84%d9%82%d8%b1%d9%86%20%d8%a7%d9%84%d8%ad%d8%a7%d8%af%d9%8a%20%d9%88%d8%a7%d9%84%d8%b9%d8%b4%d8%b1%d9%8a%d9%86..pdf (تم الدخول في ١١-٧-٢٠٢٢)

(1) Oğurlu, E. (2023). International Law in Cyberspace: An Evaluation of the Tallinn Manuals. Annales de la Faculté de Droit d'Istanbul, 0(73), 327-344. https://doi.org/10.26650/annales.2023.73.0010 ; W. Gibson, Neuromancer (Ace Publishing, 1984) p. 54.

(2)Cyberspace definition, Encyclopedia Britannica, https://www.britannica.com/topic/ cyberspace (accessed 11-7-2022).

١. الهجوم السيبراني (cyber attack) : وقد تم تعريف الهجوم السيبراني في دليل (تالين) -والذي سوف يتم التحدث عنه بالتفصيل لاحقا- بأنه: "عملية إلكترونية سواء هجومية أو دفاعية يتوقع أن تتسبب في إصابة أو قتل أشخاص أو الإضرار بأعيان أو تدميرها"[(١)]. وقد تؤدي الهجمات السيبرانية إلى أضرار جسيمة، وغالبا ما تكون مالية فيتم استهداف البنوك أو المواقع الحكومية التي تحتوي على بيانات هامة أو استهداف منشآت صناعية، ومن الأمثلة على الهجمات الإلكترونية ما حدث لبرنامج إيران النووي؛ حيث استُعمل فيروس لمهاجمة منشأة نووية إيرانية في عام ٢٠١٠.

٢. الجريمة السيبرانية (cyber crime): والتي تعرف أيضا بالجريمة الإلكترونية:" فهي ذلك العمل غير الشرعي المقترف بهدف الاستيلاء على ممتلكات الغير أو تخريب الأنظمة، وبمعنى آخر هي: تللك الأعمال المعاقب عليها قانونيا والتي ترتبط بالعمل الإجرامي وتكنولوجيا الاتصالات."[(٢)]

---

(1) M N. Schmitt (Ed), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge University Press, 2017)،

(٢) د. جمال بوازيدية، الإستراتيجية الجزائرية في مواجهة الجرائم السيبرانية التحديات والآفاق المستقبلية، جامعة الوادي، مجلة العلوم القانونية والسياسية، المجلد ١٠ العدد ١، ابريل ٢٠١٩، ص ١٢٦٨، http://dspace.univ-eloued.dz/bitstream/123456789/5246/1/%d8%a7%d9%84%d8%a5%d8%b3%d8%aa%d8%b1%d8%a7%d8%aa%d9%8a%d8%ac%d9%8a%d8%a9%20%d8%a7%d9%84%d8%ac%d8%b2%d8%a7%d8%a6%d8%b1%d9%8a%d8%a9%20%d9%81%d9%8a%20%d9%85%d9%88%d8%a7%d8%ac%d9%87%d8%a9%20%d8%a7%d9%84%d8%ac%d8%b1%d8%a7%d8%a6%d9%85%20%d8%a7%d9%84%d8%b3%d9%8a%d8%a8%d8%b1%d8%a7%d9%86%d9%8a%d8%a9%20_%d8%a7%d9%84%d8%aa%d8%ad%d8%af%d9%8a%d8%a7%d8%aa%20%d9%88%d8%a7%d9%84%d8%a7%d9%8=

وسلاح هذه الجريمة هي الفيروسات الإلكترونية؛ حيث تقوم هذه البرامج بالدخول غير الشرعي ونسخ البرامج الخبيثة في أجهزة المستخدمين دون أي معرفة من قبل المستخدمين ويكون ذلك لعدة أهداف منها تدمير البيانات، أو الحصول على المعلومات، أو استبدال المعلومات.

كما تم تعريف الجريمة السيبرانية بأنها تلك الجريمة التي يستخدم فيها المجرم التكنولوجيا لتحقيق جرائمه.

٣. الإرهاب السيبراني (cyber terrorism): تصدى عدة فقهاء لوضع تعريف لمصطلح الإرهاب السيبراني حيث لا يوجد تعريف متفق عليه للإرهاب السيبراني، وقد ظهر مصطلح الإرهاب السيبراني في الثمانينات، فقد عرفه باري كولن بأنه: "هجمة إلكترونية غرضها تهديد الحكومات أو العدوان عليها، سعيًا لتحقيق أهداف سياسية أو دينية أو أيديولوجية، وأن الهجمة يجب أن تكون ذات أثر مدمر وتخريبي مكافئ للأفعال المادية للإرهاب."[(١)].

٤. الأمن السيبراني (cyber security): للأمن السيبراني عدة تعريفات وكبقية المصطلحات لا يوجد تعريف موحد للأمن السيبراني؛ حيث يوجد عدة تعريفات للمصطلح وقد يكون أبرزها تعريف الاتحاد الدولي للاتصالات وهو منظمة متخصصة تابعة للأمم المتحدة حيث تم تعريف الأمن السيبراني بأنه: "مجموعة

---

=

1%d8%a7%d9%82%20%d8%a7%d9%84%d9%85%d8%b3%d8%aa%d9%82%d8%a8%d9%84%d9%8a%d8%a9_.pdf ( تم الدخول في ١١-٧-٢٠٢٢).

(١) د. وفاء لطفي، الجهود الدولية في مجال مكافحة جرائم الارهاب السيبراني: التجربة الماليزية نموذجا، جامعة القاهرة، مجلة كلية الاقتصاد والعلوم السياسية، المجلد ٢٣، العدد ١ - الرقم المسلسل للعدد ٩٠، يناير ٢٠٢٢، https://jpsa.journals.ekb.eg/article_211371.html (تم الدخول في ١٢-٧-٢٠٢٢).

السياسات والأدوات والمعايير التي تستخدم لحماية الفضاء السيبراني من الدخول غير المصرح فيه، وسوء الاستغلال، واستعادة المعلومات الإلكترونية، ونظم الاتصالات والمعلومات التي تحتويها؛ وذلك لضمان استمرار عمل نظم المعلومات، وتعزيز حماية وسرية وخصوصية المعلومات الشخصية، واتخاذ جميع التدابير اللازمة لحماية الأشخاص والمستخدمين من المخاطر في الفضاء السيبراني"[١].

ويقوم الاتحاد الدولي للاتصالات بوضع مؤشرات ومعايير لقياس مستوى الأمن السيبراني بالدول، وذلك بإنشاء مؤشر الأمن السيبراني العالمي وذلك من العام ٢٠١٥[٢]، وقام المؤشر منذ إنشائه بقياس التزام ١٩٣ دولة من دول الاتحاد الدولي للاتصالات بالإضافة إلى فلسطين[٣]، ويهدف المؤشر إلى تحديد مجالات التحسين وتشجيع البلدان على اتخاذ الإجراءات اللازمة من خلال زيادة الوعي بشأن الأمن السيبراني، ومنذ بداية المؤشر فقد تطورت المعايير بتطور الأمن السيبراني في البلدان، وترتكز هذه المعاير والمؤشرات على خمس معايير وهي:

(1) Update to Cyber Security Definition in the document TD 2761R1 (X.1250), The International Telecommunication Union (ITU), https://www.itu.int/md/T05-SG17-C-0242 (accessed 1-8-2022).

(2) Global Cybersecurity Index 2020, The International Telecommunication Union (ITU), 2020, https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E (accessed 2-8-2022).

(3) Global Cybersecurity Index 2020, The International Telecommunication Union (ITU), 2020, https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E (accessed 2-8-2022).

١. المحور التشريعي: وهو يقيس وجود بيئة تشريعية لمواجهة التحديات السيبرانية، فينظر هذا المعايير على القوانين في الدولة والمتعلقة بالأمن السيبراني فعدم وجود تشريعات يضعف وضع الدولة بالمؤشر.

٢. المحور الفني: الذي يتعلق بوجود هيئات الاستجابة السريعة للحوادث السيبرانية.

٣. المحور التنظيمي: الذي يتعلق برسم استراتيجية الأمن السيبراني.

٤. المحور العملياتي: المتعلق ببناء القدرات المحلية والتوعية بالأمن السيبراني

٥. المحور التعاوني: وهو المتعلق بوجود شراكات مع القطاع الخاص ومع المنظمات الدولية للتعاون في مجال الأمن السيبراني وفي سبيل تحقيق الأمن السيبراني[1].

ويهدف المؤشر إلى تحديد الثغرات وتحديد التزامات الدول تجاه الأمن السيبراني بالإضافة إلى تشجيع الممارسات الجيدة والممتازة في مجال الأمن السيبراني، وتقديم روى مفيدة للدول لتحسين أوضاع الأمن السيبراني لديها.

(1) Global Cybersecurity Index, The International Telecommunication Union (ITU), https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (accessed 2-8-2022).

## المبحث الثاني

## كيفية انطباق القانون الدولي على الفضاء السيبراني

وسيتناول هذا المبحث مطلبين كل مطلب لمبدأ، أولهما يتطرق لمبدأ سيادة الدول، والثاني، يتناول مبدأ عدم التدخل، على النحو الآتي بيانه.

### المطلب الأول: مبدأ السيادة

السيادة تعني حرية تصرف الدولة في أراضيها وسلطتها على إقليمها ومواطنيها وحكومتها، وتوجد عدة صعوبات فيما يتعلق بسيادة الدولة في الفضاء السيبراني وهي كالتالي:

١. عدم وجود الحدود: فالفضاء السيبراني لا يوجد به حدود، وذلك على عكس الدول التي يكون بها حدود سياسية برية وبحرية.

٢. مشكلة الإسناد: حيث إنه من الصعب إسناد الاتهام إلى دولة أو شخص معين في الفضاء السيبراني؛ وذلك لأنه من السهل التخفي في الفضاء السيبراني.

٣. الجهات الحكومية وغير الحكومية: إن السيادة تنطبق بالعادة على الدولة، لكن الأفراد (جماعات إجرامية، هاكر) جميعهم يعملون في الفضاء السيبراني.

وعليه فقد اتفق الفقهاء على أن سيادة الدولة تمتد إلى فضائها السيبراني مما يمنح الدولة السيطرة على البنية التحتية السيبرانية والكيانات والسلوك والبينات ذات الصلة

داخل أراضيها، فالسيادة وفقا للقانون الدولي هي أن للدولة سيادة على إقليمها البري والجوي والبحري، ولها الحرية بتبني القوانين التي تسري بدولتها ولها الحق بتطبيق القوانين على إقليمها، فهل تختلف عن السيادة في الفضاء السيبراني عن السيادة وفقا للقانون الدولي؟ ولقد أشار الفقهاء إلى أن السيادة في الفضاء السيبراني هي ذاتها، فللدولة أن تمارس سيادتها على إقليمها وفي الفضاء السيبراني للدولة[١]، وقد كان هناك رأي سائد بمعاملة الفضاء السيبراني معاملة أعالي البحار والفضاء الخارجي بأنها ملك للجميع تخضع للقانون الدولي، إلا أن الخبراء اتفقوا أن سيادة الدولة وحدودها تنطبق على الفضاء السيبراني[٢]، وقد أشار إلى ذلك كلٌ من دليل تالين الأول والثاني، بالإضافة إلى لجنة الخبراء الحكوميين التي شكلتها الأمم المتحدة ومجموعة العمل المفتوحة العضوية التابعة للأمم المتحدة أيضا، فالأشخاص الذين يمارسون العمل السيبراني بنطاقاته ويكونون من دول معينة ينطبق عليهم السيادة في الإقليم، بالإضافة إلى أن أجهزة الحاسوب التي تستعمل للدخول في الفضاء السيبراني تكون في دول معينة أيضا، فكل ذلك يجعلنا أمام دول لها سيادة وسيادتها تنطبق على فضائها السيبراني التابع لها.

ووفقا لمجموعة الخبراء الحكوميين التابعة للأمم المتحدة، والاسم الدقيق للمجموعة هو "فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وقد جاء تشكيل هذه المجموعة من قبل الأمين العام للأمم المتحدة بتفويض من قبل الجمعية العامة للأمم المتحدة،

(1) Ebru Og˘urul, International Law in Cyberspace: An Evaluation of the Tallinn Manuals, Istanbul University Press, p 337.

(2) M N. Schmitt (Ed), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge University Press, 2017), pp١٢

وانطلاقا من قرار الجمعية العامة رقم ٢٦٦/٧٣[١]، وذلك للنظر في عدة أمور منها كيفية انطباق القانون الدولي على الأنشطة السيبرانية للدول، ومن المهم ذكر أن مجموعة الخبراء أنشئت منذ ٢٠٠٤، وعقدت عدة اجتماعات منذ ذلك الحين وقد أصدرت المجموعة أربعة تقارير وذلك في عام ٢٠١٠، ٢٠١٣[٢]، و ٢٠١٥ و٢٠٢١[٣]، وقد أيدت الجمعية العامة للأمم المتحدة هذه التقارير.

ففي عام ٢٠١٣ أقرت ١٥ دولة من الخبراء الحكوميين بانطباق القانون الدولي على الفضاء السيبراني والأنشطة السيبرانية للدول، إضافة إلى ذلك فإن التقرير الصادر عن مجموعة الخبراء الحكوميين في عام ٢٠١٥ والتي تم تشكيلها من ١٥ دولة وخبيرًا دوليًا، تم تشكيلها على أساس التوزيع الجغرافي العادل، ويتكون التقرير من ١١ قاعدة غير ملزمة لسلوك الدول فيما يخص الفضاء السيبراني[٤]، وأقر التقرير التزام الدول

(1) Application of international law to states' conduct in cyberspace: UK statement, UK Gov., 3 June, 2021, https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement (accessed 29-9-2024).

(٢) قرار الجمعية العامة للأمم المتحدة، الدورة السبعون، التطورات في ميدان الاتصالات السلكية واللاسلكية في سياق الأمن الدولي، تقرير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات السلكية واللاسلكية في سياق الأمن الدولي، ٢٢-٧-٢٠١٥

https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/33/PDF/N1522833.pdf?OpenElement A تم الدخول في ٥-٨-٢٠٢٢ (الأمم المتحدة ٧٠/١٧)

(3) Michael Schmitt, The Sixth United Nations GGE and International Law in Cyberspace, June 10, 2021, https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/ (accessed 5-8-2022).

(٤) قرار الجمعية العامة للأمم الدورة السبعون، التطورات في ميدان الاتصالات السلكية واللاسلكية في سياق الأمن الدولي، تقرير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات السلكية واللاسلكية في سياق الأمن الدولي، ٢٢-٧-٢٠١٥

=

بمبادئ ميثاق الأمم المتحدة ومبادئ القانون الدولي[١]، وخصوصا مبدأ السيادة والمساواة[٢]، وتسوية المنازعات الدولية بالطرق السلمية.

أما فيما يتعلق بالتقرير الصادر في ٢٠٢١ والذي أنشئ وفقا لقرار الجمعية العامة للأمم المتحدة رقم ٣٧/٢٦٦، وفيه أقر الخبراء الحكوميون بانطباق القانون الدولي وميثاق الأمم المتحدة على الفضاء السيبراني، وهذا ما يتوافق مع التقارير السابقة للخبراء الحكوميين، ويهدف التقرير إلى الحفاظ على الأمن والسلم الدوليين بما يتوافق مع ميثاق الأمم المتحدة، فقد نص التقرير على ضرورة التعاون الدولي في مجال الفضاء السيبراني كما أضاف التقرير بعض النقاط إلى كيفية انطباق القانون الدولي على الفضاء السيبراني، وقد أشار التقرير -كما ذكرنا سابقا- إلى انطباق القانون الدولي على الفضاء السيبراني ووضع التقرير عددا من النقاط التي ينطبق فيها القانون الدولي على الفضاء السيبراني، وأضاف تقرير الخبراء الحكوميين عددا من النقاط منها: انطباق المادة ٢ فقرة ٣ الخاصة بحل النزاعات الدولية بطرق سلمية، ومنها المفاوضة والتحقيق والوساطة والتوفيق والتحكيم والتسوية القضائية المنصوصة في المادة ٣٣ من ميثاق الأمم المتحدة، كما أكد التقرير على انطباق ميثاق الأمم المتحدة على الفضاء السيبراني، إضافة إلى ذلك فقد أشار التقرير إلى أن سيادة الدولة تمتد إلى الأنشطة السيبرانية والأجهزة السيبرانية الواقعة داخل الدولة، أما بالنسبة لمبدأ عدم التدخل فقد رأى التقرير أنه وفقا لهذا لمبدأ فلا

=

https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/33/PDF/N1522833.pdf?OpenElement

تم الدخول في ٥-٨-٢٠٢٢A (الامم المتحدة / ١٧/٧٠ الفقرة ٢٦)

(١) فقرة ٢٨ ب

(٢) فقرة ٢٧

يجوز لدولة التدخل في الشؤون الداخلية لدولة أخرى وذلك عن طريق استخدام الفضاء السيبراني.

وعليه فإن التقرير ناقش مبدأ السيادة وأن الدولة مسؤولة عن الأعمال السيبرانية في دولتها، إلا أنه أقر بأن الدولة قد تكون غير مسؤولة إذا كان العمل من دولتها دون وجود دليل.

ونظرا للانتقادات التي واجهة مجموعة الخبراء الحكوميين بأنها لا تمثل جميع الدول، فقد تم إنشاء مجموعة العمل المفتوحة العضوية التابعة للأمم المتحدة الخاصة بتكنولوجيا المعلومات والاتصالات وعلاقتها بالقانون الدولي، فأنشئت المجموعة بناء على قرار الجمعية العامة للأمم المتحدة رقم ٧٣/٢٧[(1)]، وقد أنشئت المجموعة لإعطاء كافة الدول الحق في تقديم آرائها في كيفية انطباق القانون الدولي في الفضاء السيبراني، وعقد أول اجتماع للمجموعة في ٢٠١٩، ويأتي تشكيل المجموعة لإتاحة فرصة لجميع الدول الراغبة بإبداء رأيها فيما يتعلق بالفضاء السيبراني والقانون الدولي، وقد أتاحت مجموعة العمل للفقهاء والمنظمات الدولية غير الحكومية والشركات الخاصة حرية المشاركة في النقاشات، وتصدر المجموعة آراءها بالإجماع تمامًا مثل مجموعة الخبراء الحكوميين، والفرق بينها وبين مجموعة الخبراء الحكوميين هي أن مجموعة الخبراء الحكوميين مجموعة مغلقة وتم اختيار ممثليها بالدعوة، وجاء تشكيل مجموعة العمل المفتوحة للحصول على إجماع الدول فيما يتعلق بالقانون الدولي والفضاء السيبراني، وقد اتفقت المجموعتان على أن القانون الدولي ينطبق على الفضاء السيبراني، لكن كيفية

(1) United Nations (Open Ended Working Group), https://disarmament.unoda.org/open-ended-working-group/ ( accessed 27-11-2024).

انطباق القانون الدولي على الفضاء السيبراني كان محط اختلاف بين الدول في المجموعتين وقد استطاعت الدول في المجموعة المفتوحة التوصل إلى اتفاق أوليّ نُشر - بناء عليه- تقرير يبين اتفاق الدول على كيفية انطباق القانون الدولي على الفضاء السيبراني، وذلك في مارس عام ٢٠٢١[١]، كما تم الاتفاق على استكمال المناقشات في المجموعة المفتوحة من ٢٠٢١ إلى ٢٠٢٥ على أمل التوصل إلى توافق بشأن القانون الدولي وكيفية انطباقه في الفضاء السيبراني[٢].

وقد أجمع أعضاء المجموعة المفتوحة على انطباق ميثاق الأمم المتحدة على الفضاء السيبراني، وكان هناك نقاط اختلاف في كيفية انطباق قانون حقوق الإنسان والقانون الدولي الإنساني على الفضاء السيبراني، إلا أن الدول المشتركة في المجموعة قد اتفقت على انطباق هذين القانونين في الفضاء السيبراني لكن الاختلاف كان في الكيفية، فقد رأت المجموعة المفتوحة أن القانون الدولي ينطبق في الفضاء السيبراني، كما أقرت المجموعة المفتوحة بانطباق مبدأ السيادة في الفضاء السيبراني.

كما أن هناك عملية أكسفورد لحماية القانون الدولي في الفضاء السيبراني، وهي مبادرة من معهد أكسفورد للأخلاق والقانون والصراع المسلح أُطلقت في مايو ٢٠٢٠ بالشراكة مع شركة مايكروسوفت وحكومة اليابان[٣]، حيث تم من خلال هذه المبادرة

(1) United Nation General Assembly, 10-3-2021, A/AC.290/2021/CRP.2, https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf (accessed 27-11-2024).

(2) YOO Joonkoo, UN Open-Ended Working Group Final Report: Issues and Implications, April, 2021, The Institute of Foreign Affairs and National Security (IFANS), IF2020-36E.

(3) Introduction to the Oxford Process on International Law Protections in Cyberspace, e Oxford Institute for Ethics, Law and Armed Conflict, 13-12-
=

مشاركة مجموعة من الخبراء الدوليين القانونيين من جميع دول العالم بالإضافة إلى الأكاديميين وممثلي الدول؛ وذلك بهدف تحديد وتوضيح قواعد القانون الدولي المنطبقة على العمليات السيبرانية على نطاقات مختلفة[١]، حيث اتفق الفقهاء في العملية على أن القانون الدولي ينطبق على جميع الأنشطة التي تتم عن طريق تكنولوجيا الاتصالات والمعلومات بما في ذلك العمليات والأنشطة المعلوماتية، وأنه يجب على الدول الامتناع عن العمليات والأنشطة السيبرانية التي تؤدي لانتهاك سيادة الدول[٢].

أما بالنسبة لدليل (تالين) فالدليل يتعلق بالقانون الدولي المطبق في الحرب السيبرانية أو ما يعرف باسم دليل (تالين)، وقد تم إعداده من قبل خبراء في القانون الدولي بدعوة من مركز التمييز للدفاع الإلكتروني التعاوني التابع لحلف شمال الأطلسي (الناتو)، وهي وثيقة غير ملزمة أعدتها مجموعة من الخبراء، والنسخة الأولى من الدليل نشرت في عام ٢٠١٣ وأسهم ١٩ خبيرا قانونيا وعسكريا في صياغة الدليل، كما اشتمل دليل (تالين) الأول على ٩٥ قاعدة متعلقة بمدى انطباق القانون الدولي على الفضاء السيبراني[٣]، وقد نشرت نسخة حديثة من الدليل سمي بدليل (تالين) ٢,٠، وقد نشر هذا

=

2021, https://documents.unoda.org/wp-content/uploads/2021/12/OEWG-Side-Event-Oxford-Process-Introduction.pdf (accessed 27-11-2024).

(1) The Oxford Institute For Ethics, Law and Armed Conflict, Oxford University, https://www.elac.ox.ac.uk/ (accessed 19-8-2024).

(2) The Oxford Process, The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Information Operations and Activities, https://www.elac.ox.ac.uk/the-oxford-process/the-statements-overview/the-oxford-statement-on-the-regulation-of-information-operations-and-activities/ (accessed 2-9-2024).

(3) M N. Schmitt (Ed), Tallinn Manual on the International Law Applicable to Cyber Operations (Cambridge University Press, 2013).

الدليل في ٢٠١٧، ويتكون دليل (تالين) الثاني من ١٥٤ قاعدة متعلقة بمدى انطباق القانون الدولي على الفضاء السيبراني[١]، فكل من دليل (تالين) الأول والثاني نصوا على انطباق مبدأ السيادة في الفضاء السيبراني، وقد تناول دليل (تالين) السيادة بخمس قواعد وسوف يلي بيانها على النحو التالي:

أول قاعدة تحدثت عن السيادة بشكل عام وكيف أن السيادة تنطبق على الفضاء السيبراني،[٢] أما القاعدة الثانية فتحدثت عن السيادة الداخلية، فما هي السيادة الداخلية؟ وهل هي مشابهة لما تم ذكره من أن الأجهزة والحواسيب الإلكترونية والشبكات الحاسوبية التي تقع في إقليم الدولة تخضع لسيادة الدولة الداخلية؟ وعليه فيجوز للدولة وضع قوانين تنظم الفضاء السيبراني في إقليمها وذلك فيما لا يخالف واجبات الدولة والتزاماتها الدولية[٣]، كما أن من صور سيادة الدولة على فضائها السيبراني تمتع هذا الفضاء بالحماية من قبل القانون الدولي، فللدولة الحق بإصدار التشريعات والقوانين المتعلقة بالفضاء السيبراني في إقليمها كإصدار قوانين تنظم المحتوى السيبراني ومواقع الإنترنت ومنع الجرائم السيبرانية، وهذا ما فعلته معظم الدول، إلا أن سيادة الدولة ليست مطلقة في ذلك فعلى الدولة الالتزام بقواعد القانون الدولي لحقوق الإنسان، ولكن ذلك لا يمنع الدولة من تقييد حرية الأشخاص في الفضاء السيبراني التابع لها، فللدولة -وفقا لسيادتها الداخلية- حجب مواقع معينة في دولتها، وقد قامت بعض الدول بالاتفاق مع مواقع التواصل الاجتماعي بحجب مواقع معينة ومنشورات معينة قد تؤدي إلى عدم الاستقرار والشغب، وكل ذلك يخضع لسيادة الدولة، وقد تسيء بعض الدول في استعمال

(1) M N. Schmitt (Ed), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge University Press, 2017).

(2) Id. at 11

(3) Id. at 13.

هذا الحق، فنرى ما فعله الاحتلال الصهيوني في الحرب على غزة حيث قام بقطع الإنترنت عن القطاع منعا لنقل الجرائم التي يرتكبها الاحتلال الإسرائيلي على المدنيين الفلسطينيين.

بالإضافة إلى ذلك فإن السيادة الداخلية للدولة والتي تشمل حرية الدولة باتخاذ وتحديد سياساتها الاقتصادية والاجتماعية والسياسية والثقافية والقانونية، كما أشار الفقهاء إلى أن الدولة تملك حق السيادة تجاه بياناتها الحكومية الخاصة بمواطنيها حتى ولو كانت البيانات محتفظا بها خارج إقليمها[١]، إلا أن هذه النقطة كانت موضع خلاف بين الفقهاء، فالبعض الآخر قال بأن الدولة لا تملك حق السيادة على بيانات مواطنيها التي تم الاحتفاظ بها خارج إقليم الدولة إلا إذا تم النص على ذلك وفقا للقانون الدولي، وهذا ما لم يحدث حتى الآن. كما أشار الفقهاء إلى أن السيادة لا تفرض حقوقًا فقط إنما تشمل التزامات ومن هذه الالتزامات وجوب التحقق من الهجمات السيبرانية التي قد تنطلق من إقليم الدولة.

أما القاعدة الثالثة فهي تتعلق بالسيادة الخارجية: والقاعدة هي حرية الدولة في ممارسة الأنشطة السيبرانية في علاقاتها الدولية شريطة أن لا يتناقض ذلك مع التزاماتها بالقانون الدولي الملزم لها[٢]، ومعنى هذه القاعدة أن الدولة لها سيادة خارجية مأخوذة من السيادة والمساواة في السيادة بين الدول وهذا ما نص عليه ميثاق الأمم المتحدة؛ حيث إن على كل دولة احترام سيادة الدول الأخرى فكل الدول متساوية ولا توجد دولة متقدمة على الدول الأخرى من الناحية القانونية، كما تعني السيادة الخارجية بأن الدولة مستقلة

(1) Id. at 15

(2) M N. Schmitt (Ed), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge University Press, 2017), p 16.

ولا تخضع لأحد في علاقاتها الدولية ولها الحق في ممارسة الأنشطة السيبرانية خارج إقليمها بما يتوافق مع القانون الدولي، وحرية الدولة في تحديد سياساتها الخارجية والدخول في اتفاقيات دولية، فمن هذا المنطلق للدول الحرية في تحديد سياساتها السيبرانية والدخول في اتفاقيات دولية متعلقة بالفضاء السيبراني أو رسم الطريق وتحديد سياسة الدولة السيبرانية؛ حيث إن الدولة غير ملزمة بالدخول في اتفاقيات تلزمها أو تلزم مواطنيها في إقليمها، فالسيادة الخارجية هي مصدر حصانة الدولة.

أما بالنسبة للقاعدة الرابعة فهي تتعلق بمخالفة السيادة: "وتعني هي أن الدولة يجب ألا تجري عمليات سيبرانية تخالف وتعتدي على سيادة دولة أخرى"[١]، وتعني القاعدة أنه لا يجوز لدولة أن تعتدي على السيادة الخارجية أو الداخلية لأي دولة ولهذه القاعدة استثناءان: الاستثناء الأول في حالة كان ذلك بناء على أمر من مجلس الأمن، والثاني إذا كان ذلك استعمالا لحق الدفاع عن النفس، ففي هاتين الحالتين يجوز استعمال عمليات سيبرانية تخالف السيادة وتعتدي على دولة أخرى، أما المثال على هذه القاعدة فهي قيام عنصر تابع للدولة باستخدام فلاش به فيروس تم إعداده في دولة واستخدامه في دولة أخرى بهدف شل الحركة في هذه الدولة ففي هذه الحالة يتحقق الاعتداء على سيادة هذه الدولة.

وقد قدر الفقهاء أن الاعتداء السيبراني الذي ينتج عنه الفقدان المادي أو الوظيفي يعد اعتداء على السيادة[٢]، كما تبنى الفقهاء الرأي الذي يقول بأنه اعتداء على السيادة عندما تقوم دولة بأنشطة سيبرانية تتدخل بالوظائف الحكومية لدولة أخرى.[٣]

(1) M N. Schmitt (Ed), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge University Press, 2017), p 17.

(2) Id. at 21.

(3) Id. at 21.

كما أن للدولة أن تسمح بقيام دولة أخرى بالتدخل السيبراني في إقليمها وذلك دفعا لهجوم سيبراني لا تملك الدولة الأولى مواجهته وصده، ففي هذه الحالة لا يعد تدخل الدولة الثانية خرقا لسيادة الدولة الأولى.

أما القاعدة الخامسة والأخيرة المتعلقة بالسيادة فهي متعلقة بالحصانة السيادية وحرمة السيادة، ونصت القاعدة على التالي: "أي تدخل من جانب دولة لها بنية تحتية سيبرانية في الخارج أينما كانت وتتمتع بالحصانة السيادية يعد انتهاكا للسيادة"[1]، والقانون الدولي يعطي الحصانة السيادية لعدد من الأشياء التي تستعمل في الأغراض غير التجارية والأغراض الحكومية بغض النظر عن أماكن وجودها، ومثال ذلك السفن الحربية التي يتم استخدامها عن طريق دولة معينة والتي يتم استخدامها لأغراض حكومية غير تجارية حيث تتمتع هذه السفن الحربية بالحصانة السيادية فلا تتبع سيادة دولة أخرى غير دولة العلم للسفينة، كما ينطبق ذلك على الطائرات التابعة لدولة معينة دولة العلم والتي تتمتع أيضا بالحصانة السيادية؛ حيث إن الأشخاص الذين يقومون بعمليات سيبرانية على هذه السفن أو الطائرات يتمتعون بالحصانة الإجرائية من قبل الدول الأخرى، ولكي يتمتع هؤلاء الأشخاص بالحصانة الإجرائية فيجب أن يكون العمل الذي يقومون به عملًا حكوميًا بحتًا، وأي خرق لهؤلاء يعد اعتداء على القانون الدولي، ويجب على هؤلاء الالتزام بمبادئ وقواعد القانون الدولي ومن أمثلة ذلك الالتزام باحترام سيادة الدول الأخرى، وذلك من خلال عدم دخول الطائرة الحربية إلى الأجواء الجوية لدولة أخرى لإجراء عملية سيبرانية بالرغم من تمتع الطائرة بالحصانة، ففي هذه الحالة يكون للدولة التي تم خرق أجوائها الجوية الحق في الرد، بما في ذلك الحق في حالات معينة تمكنها من استعمال القوة، كذلك ينطبق هذا الأمر على السفن الحربية التي تجري عمليات

(1) Id. at 17.

سيبرانية في المياه الإقليمية لدولة أخرى مخالفة بذلك لحق المرور البريء، وفي كلتا الحالتين تتمتع كلٌ من السفينة والطائرة بالحصانة السيادية، إلا أن ذلك لا يمنع الدولة المتعدَّى عليها من حقها في الرد على هذه العمليات ردا قانونيا ومناسبا وضروريا وذلك لحماية مصالحها، كما اتفق الفقهاء على أنه في حالة النزاعات المسلحة الدولية فإن مبدأ الحصانة السيادية بين الطرفين لا يطبق في العلاقة بين الدولتين المتنازعتين حيث يمكن لأطراف النزاع استهداف الطائرة أو السفينة متى ما كانت حربية وطرفا في النزاع وتكون هدفا عسكريا.

رأينا في مبدأ السيادة المطبق في الفضاء السيبراني ومحاولة دليل (تالين) تقنين هذا المبدأ وتطبيقه على الفضاء السيبراني، مما نرى فإن الفقهاء قد أحاطوا أهم مبادئ القانون الدولي بالفضاء السيبراني بالحديث، وقد أوضح الفقهاء مكان وكيفية تطبيق مبادئ القانون الدولي الأساسية على الفضاء السيبراني، وقد كانت الصعوبة تكمن في كيفية تطبيق السيادة على الفضاء السيبراني الذي لا يوجد به حدود واضحة، وقد تصدى دليل (تالين) لذلك جاعلا للدولة على الأنشطة السيبرانية التي تحصل في دولتها والتي تنشأ من دولتها سيادة على ذلك، ومن الأجهزة الموجودة في دولتها سيادة عليها، كما أوضح الدليل الأشخاص الذين يتمتعون بالحصانة من الأعمال السيبرانية مثل رؤساء الدول ورؤساء الوزراء ووزراء خارجية الدول وغيرهم ما لم يتطرق له الدليل، وهو قيام هؤلاء نتيجة للحصانة التي يتمتعون بها بالقيام بالأعمال السيبرانية، ففي هذه الحالة نعتقد نحن بأن الحصانة تظل لكن يتم اعتبار هؤلاء الأشخاص شخصيات غير مرغوب فيها.

إن بعض الدول تعتبر أن لها السيادة في الفضاء السيبراني، وذلك في حدود دولتها؛ حيث إن للدولة الحق في تنظيم وتشريع الفضاء السيبراني في حدود دولتها، ونحن نؤيد ما توصل إليه دليل (تالين) فيما يتعلق بالسيادة حيث أوضح الدليل وضع السيادة وكيفية تطبيقها في الفضاء السيبراني.

## المطلب الثاني: مبدأ عدم التدخل

يعتبر مبدأ عدم التدخل من المبادئ الأساسية في القانون الدولي، وقد تم النص عليه في ميثاق الأمم المتحدة، ويتعبر جزءًا من قواعد القانون الدولي العرفي[١]، وتم النص على مبدأ عدم التدخل في الدستور الفرنسي عام ١٧٩٣، وذلك عندما نص الدستور الفرنسي على أن فرنسا لن تتدخل في الأمور الداخلية للدول الأخرى ولن تقبل تدخل الدول في شؤونها الداخلية[٢]، وبعد ذلك أخذت به الدول الأخرى كمبدأ عرفي[٣]، وقد تم تقنين هذا المبدأ في ميثاق الأمم المتحدة وتحديدا المادة ٢ فقرة ٧ من الميثاق والتي نصت على التالي: "ليس في هذا الميثاق ما يسوغ "للأمم المتحدة" أن تتدخل في الشؤون التي تكون من صميم السلطان الداخلي لدولة ما....."[٤] كما حددت ذات المادة الحالة الوحيدة التي يسمح للأمم المتحدة التدخل في الشؤون الداخلية للدول فقط وفقا للفصل السابع من الميثاق وهي الحالات التي يحدث فيها عدوان وأعمالٌ تهدد الأمن والسلم الدوليين[٥].

وكما سبق وذكرنا، فإن مبدأ عدم التدخل يعد عرفًا دوليًا، وهو ما أشارت إليه محكمة العدل الدولية في حكمها الشهير في قضية نكاراغوا ضد الولايات المتحدة الأمريكية، حيث نصت القضية على أن: "يتضمن مبدأ عدم التدخل حق كل دولة ذات

(1) Jianming Shen, The Non-Intervention Principle and Humanitarian Interventions under International Law, 7 INT'l LEGAL THEORY 1 (2001), p 2.

(2) Id.

(3) Id.

(٤) المادة ٢ فقرة ٧ من ميثاق الأمم المتحدة لعام ١٩٤٥

(٥) الفصل السابع من ميثاق الأمم المتحدة لعام ١٩٥٤

سيادة في إدارة شؤونها دون تدخل خارجي"[١] كما أشار ذات الحكم إلى أن مبدأ عدم التدخل يعتبر مبدأ عرفا من مبادئ القانون الدولي، وقد أشارت نفس القضية إلى أن مبدأ عدم التدخل قد يحدث مع أو بدون القوات المسلحة[٢]، وعليه تم اختيار مبدأ عدم التدخل لرؤية كيفية انطباق مبدأ عدم التدخل في الفضاء السيبراني حيث نواجه ذات المشكلة التي واجهناها في مبدأ السيادة حيث لا توجد حدود في الفضاء السيبراني، ويلعب هذا المبدأ دورا أساسيا في الفضاء السيبراني؛ حيث إن معظم العمليات السيبرانية تقع تحت عتبة استخدام القوة، ونظرا إلى ذلك فقد حاول الفقهاء التصدي لهذا الأمر وسوف نتناول بعض هذه الآراء:

إن مجموعة الخبراء الحكوميين -التي شكلتها الأمم المتحدة- أشارت إلى مبدأ عدم التدخل، فقد توافق تقرير لجنة الخبراء مع رأي الفقه وذلك بعدم جواز تدخل الدول في الأمور الداخلية والخارجية لدول أخرى عن طريق الفضاء السيبراني[٣]، وهذه نقطة مهمة في ضوء وسائل التواصل الاجتماعي التي تلعب دورا هاما في الانتخابات سواء البرلمانية أو الرئاسية للدول أو أيضا استعمال وسائل التواصل لزيادة تأجيج العنصرية

(1) Jianming Shen, The Non-Intervention Principle and Humanitarian Interventions under International Law, 7 INT'l LEGAL THEORY 1 (2001), p 4.

(2) Nicaragua v. United States case (ICJ Report, 1986, p.14. 202-204).

(3) Michael Schmitt, The Sixth United Nations GGE and International Law in Cyberspace, June 10, 2021, https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/ (accessed 5-8-2022); General Assembly, Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, 14-7-2021, https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf , A/76/135, (accessed 13-9-2024).

والطائفية بين الشعوب والدول وذلك كما حدث لأقلية الروهينغا في ميانمار حيث تم استخدام فيسبوك لنشر الدعايات العنصرية ضد أقلية الروهينغا وإبادتهم، وإن الفضاء السيبراني والهجمات السيبرانية لهو أمر خطير ويحتاج إلى تنظيم ووضع آليات وقوانين منظمة له، واعتراف مجموعة الخبراء الحكوميين بأن القانون الدولي ينطبق على الفضاء السيبراني لهو خطوة بالاتجاه الصحيح وقد ناقش الخبراء مبدأ السيادة ومبدأ عدم التدخل بالإضافة لانطباق قانون حقوق الإنسان وأهمية تطبيقه في نطاق الفضاء السيبراني حيث يجب حماية حق الأفراد في حرية التعبير لكن في نفس الوقت منع إشاعة البغضاء والعنصرية. كما أشار تقرير لجنة الخبراء الحكوميين إلى وجوب امتناع الدول في علاقاتها الدولية عن التهديد باستخدام القوة أو استخدامها ضد السلامة الإقليمية أو الاستقلال السياسي لأي دولة، واحترام حقوق الإنسان والحريات الأساسية، وعدم التدخل في الشؤون الداخلية للدول الأخرى، وقد أقر التقرير انطباق هذه المبادئ على الفضاء السيبراني[1].

بالإضافة إلى ذلك فتم منع الدول عن مهاجمة البنى التحتية السيبرانية بما يخالف القانون الدولي وعدم مهاجمة البنى التحتية التي تقدم خدمات للجمهور والتي تقدم خدمات حيوية ومنها المستشفيات وغيرها، فعلى الدول أن تعمل على حماية البنى التحية السيبرانية من الاستهداف، كما ينبغي للدول أن تتعاون في حال تعرضت دولة إلى استهداف سيبراني في بنيتها التحتية، ويجب على الدول العمل معا في تحديد مواطن

(1) General Assembly, Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, 14-7-2021, https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf , A/76/135, (accessed 13-9-2024).

الضعف في الفضاء السيبراني وكيفية حل هذه المواضع وذلك في سبيل حماية البنى التحية التي تعمل في الفضاء السيبراني، وعلى الدول عدم استهداف فرق الطوارئ للفضاء السيبراني التابعة لأي دولة، كما لا يجوز استخدام هذه الفرق لشن هجوم خبيث على دول أخرى، فعدم مهاجمة الدول الأخرى سيبرانيا يعد من قبيل عدم التدخل في الشؤون الداخلية للدول واستعمال القوة المحظور وفقا لميثاق الأمم المتحدة، كما يجب على الدول أن تمتنع عن التهديد باستخدام القوة في الفضاء السيبراني أو استخدام القوة ضد السلامة الإقليمية والسياسية لأي دولة، فيجب استخدام الفضاء السيبراني للمصلحة العامة للبشرية.

كما أشارت عملية أكسفورد إلى مبدأ عدم التدخل حيث أشار الفقهاء واتفقوا أنه يجب عدم التدخل في الشؤون الداخلية والخارجية للدول[١]. بالإضافة إلى ذلك فقد تناول البيان الثالث لعملية أكسفورد العمليات الانتخابية والتدخل السيبراني فيها وكيفية مواجهته[٢].

أما بالنسبة لمبدأ عدم التدخل وفقا لدليل (تالين) فقد أشار ونص الدليل على الحق في عدم التدخل في القاعدة رقم ٦٦ والقاعدة ٦٧ الخاصة بالتدخل من قبل الأمم المتحدة،

(1) The Oxford Process, The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Information Operations and Activities, https://www.elac.ox.ac.uk/the-oxford-process/the-statements-overview/the-oxford-statement-on-the-regulation-of-information-operations-and-activities/ (accessed 2-9-2024).

(2) Introduction to the Oxford Process on International Law Protections in Cyberspace, e Oxford Institute for Ethics, Law and Armed Conflict, 13-12-2021, https://documents.unoda.org/wp-content/uploads/2021/12/OEWG-Side-Event-Oxford-Process-Introduction.pdf (accessed 27-11-2024).

فأولا وفقا للقاعدة ٦٦ من دليل (تالين) الخاصة بعدم التدخل فنصت على التالي: "أن الدولة لا يجوز أن تتدخل سيبرانيا في الشؤون الداخلية أو الخارجية لدولة أخرى"[(١)]، إن الفضاء السيبراني يعطي الدول فرصا للتدخل في الشؤون الداخلية أو الخارجية للدول الأخرى وذلك نتيجة لارتباط العالم الذي أصبح قرية صغيرة نتيجة للتكنولوجيا والفضاء السيبراني الذي ربط الجميع ببعض، فالقاعدة تمنع التدخل القسري السيبراني في الشؤون الداخلية والخارجية لدولة أخرى، حيث إن ذلك تم النص عليه كمبدأ من مبادئ القانون الدولي الخاص بسيادة الدول، حيث يعد هذا المبدأ من المبادئ العرفية للقانون الدولي وقد قامت كلٌ من محكمة العدل الدولية، والمنظمات الدولية بالتأكيد على الطبيعة العرفية لمبدأ عدم التدخل، ولكن كيف يكون ذلك تدخلا سيبرانيا بالشؤون الخارجية والداخلية للدولة مثال ذلك قد يكون بالتدخل في العمليات السيبرانية للانتخابات وذلك بتغير نتائج الانتخابات إلكترونيا، وقد يكون التدخل أيضا عن طريق غير سيبراني لكن يتدخل بصورة غير مباشرة في ذلك مثال ذلك إجبار الدولة على عدم التصديق على اتفاقية دولية تتعلق بالفضاء السيبراني أو تبني قوانين خاصة تتعلق بتوفير الإنترنت في الدولة، فالسؤال المطروح هنا ماذا يعني عدم التدخل أو التدخل بصفة عامة بالقانون الدولي فقد تم تعريف ذلك في أحكام محكمة العدل الدولية وقد وضع الفقهاء تعريفا للتدخل فقد نص تعريف الفقهاء في دليل (تالين) للتدخل بأنه: "الأفعال التي تقوم بها الدول والتي تتدخل فيها الدول وتعتدي على حقوق محفوظة لسيادة دول الأخرى " [(٢)]

(1) M N. Schmitt (Ed), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge University Press, 2017), p 312

(2) M N. Schmitt (Ed), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge University Press, 2017), p313

وقد وجد الفقهاء أن لانطباق مبدأ عدم التدخل يجب توافر شرطين مهمين وهما: ١. أن يكون العمل متعلقًا بالشؤون الداخلية أو الخارجية للدولة موضع التدخل[١]، ٢. يجب أن يكون العمل بطبيعته قسريا[٢]، فالبنسبة للشؤون الداخلية فهي تعني كل الأمور غير المذكورة بالقانون الدولي والتي تترك للدولة في تحديدها دون تدخل من أحد ومن دول أخرى، حيث يترك الأمر للدولة في تحديدها وهو ما أشارت إليه محكمة العدل الدولية في قضية نيكاراغوا، وتشمل الأمور الداخلية الأمور السياسية والاقتصادية والاجتماعية والثقافية وتحديد السياسات الخارجية للدولة، وعليه فإن أي تدخل سيبراني في هذه الأمور يكون مخالفًا لمبدأ عدم التدخل الذي ينطبق على الفضاء السيبراني وعلى صعيد الدول أيضا.

وقد ضرب دليل (تالين) مثالا على عدم جواز التدخل السيبراني خلال وجود لغة للأغلبية ولغة للأقلية في دولة ما، وقد أقر قانون لتصبح لغة الأغلبية هي اللغة الرسمية للدولة، فقامت الدولة المجاورة ذات نفس لغة الأقلية بشن عمليات سيبرانية على مواقع إلكترونية للدولة الأولى حتى لا يتم الاستغناء عن لغة الأقلية، ولأن التدخل في تحديد اللغة الرسمية للدولة يعد من الأمور الداخلية فلا يجوز للدولة الثانية التدخل وفقا لمبدأ عدم التدخل[٣].

ومثال آخر ضربه الفقهاء في دليل (تالين) هو قيام دولة بتمكين جماعة منشقة عن الحكومة في دولة أخرى من الدخول على معلومات سيبرانية سرية في الدولة ففي هذه

(1) Id. at 314.
(2) Id. at 314.
(3) Id. at 315.

الحالة تعد الدولة متدخلة في شؤون الدولة الأخرى ويعد هذا التدخل مخالفًا للقانون الدولي.

وأما ما لا يعد تدخلًا فهو قيام دولة بحملة عن طريق وسائل التواصل الاجتماعي لإقناع دولة أخرى بالتوقيع على اتفاقية، ففي هذه الحالة لا يعد الفعل تدخلا وفقا للقانون الدولي نتيجة لغياب الإجبار، وأيضا قيام وزارة الخارجية لدولة ما بنشر معلومات في وسائل التواصل الاجتماعي تخص الشؤون الداخلية والخارجية لدولة أخرى فهذا أيضا لا يعد من التدخل وفقا للقانون الدولي.

فغياب القسر من العمل من عدمه هو الذي يجعل العمل مخالفا للقانون الدولي، وقد اختلف الفقهاء في ذلك حيث أقر بعضهم بأنهم من الصعب معرفة إذا كان الأمر قسرا أم لا، إلا أن الفقهاء اتفقوا على أن استعمال القوة في الفضاء السيبراني يعد من التدخل القسري ويعد تدخلا وفقا للقانون الدولي [١]

ووفقا للقانون الدولي وفي قضية نيكاراغوا عرفت محكمة العدل الدولية مبدأ عدم التدخل بأنه : "على جميع الدول أو مجموعة الدول عدم التدخل بشكل مباشر أو غير مباشر في الشؤون الداخلية أو الخارجية لدول أخرى."[٢]

فالمبدأ ذاته ينطبق على الفضاء السيبراني، فكيف يكون ذلك؟ وتكمن الإجابة عن هذا السؤال في أنه لو قامت دولة بتوفير برامج سيبرانية خبيثة لأفراد منشقين لاستعمالها ضد الدولة في التدخل في شؤون الداخلية والخارجية فمثل هذا التدخل يعد تدخلا مخالفا في القانون الدولي، وذلك بناء على مبدأ عدم التدخل وحكم محكمة العدل

(1) Id. at 319.

(2) Nicaragua v. United States case (ICJ Report, 1986, p.14. 202-204).

الدولية في قضية نيكارغوا؛ حيث يعد ذلك تدخلا غير مباشر في الشؤون الداخلية والخارجية للدولة.

لكن السؤال الذي يطرح هو ماذا لو كان الهجوم السيبراني لا يعرف من أي دولة أتى ومن هي الدولة التي وراء هذا الاعتداء السيبراني؟ وكان رأي الفقهاء أن عدم معرفة الفاعل الرئيسي وراء الهجوم السيبراني لا يعني أنه لا يوجد تدخل محظور وفقا للقانون الدولي ما دام كان التدخل قسرا وبالشؤون الداخلية والخارجية للدولة، وقد حدث ذلك فعلا من خلال الهجوم الذي قامت به دولة أو دولتان باختراق البرنامج النووي الإيراني فيما يعرف بهجمة سانتكس؛ حيث إنه حتى الآن لا يعرف من قام بهذا الهجوم هل هم الولايات المتحدة الأمريكية أو إسرائيل.

القاعدة ٦٧ التدخل عن طريق الأمم المتحدة وتنص هذه القاعدة على التالي: "الأمم المتحدة لا تملك حق التدخل حتى عن الطريق السيبراني في المسائل التي تعد من السلطة الداخلية للدولة بحيث لا يخل هذا المبدأ باتخاذ التدابير التنفيذية التي يقررها مجلس الأمن التابع للأمم المتحدة تبعا للفصل السابع من ميثاق الأمم المتحدة[1].

وتعد هذه القاعدة مستوحاة من المادة الثانية فقرة سبعة من ميثاق الأمم المتحدة والتي تقضي بعدم أحقية الأمم المتحدة بالتدخل في الأمور التي تعد ضمن الاختصاص المحلي لأي دولة، وعليه فإن هذه القاعدة تنطبق فقط على أنشطة الأمم المتحدة ولا تشمل الأنشطة التي تقوم بها الدول، كما لا تشمل القاعدة الأمور التي تتعلق بالأمن والسلم الدوليين. وانطباقها على الفضاء السيبراني والذي قد يؤدي اتباع دولة للتأثير في الأمن والسلامة الدوليين؛ نظرا لعدم وجود الحدود السياسية فيه، وعليه -ووفقا لميثاق الأمم

(1) M N. Schmitt (Ed), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge University Press, 2017), p٣٢٥

المتحدة ووفقا لنظرة الفقهاء في دليل (تالين)- فإن الأمم المتحدة لا يحق لها التدخل بالطرق السيبرانية في المسائل الداخلية للدول، والمثال على ذلك هو أن الأمم المتحدة لا تستطيع أن تفرض على دولة تبني قانون متعلق بالأنشطة السيبرانية في إقليمها؛ حيث إن ذلك متعلقٌ بالشؤون الداخلية للدولة.

إلا أن ذلك لا يمنع مجلس الأمن من التدخل السيبراني وفقا للفصل السابع من ميثاق الأمم المتحدة وذلك حفاظا على الأمن والسلم الدوليين، وعند قيام الأمم المتحدة بذلك فعلى جميع الدول الامتثال لهذه القرارات حيث إن لمجلس الأمن أن يصدر قرارا ملزما للدول يفرض حظرا على الاتصالات السيبرانية لدولة أو القيام في عمليات سيبرانية ضد دولة؛ حيث إن الالتزام بهذا لا يخل بالقاعدة الموضحة أعلاه.

ومما سبق بيانه، نرى أن القانون الدولي ينطبق على الفضاء السيبراني وقد قمنا بتوضيح كيفية انطباق أهم المبادئ للقانون الدولي وهما مبدأ السيادة ومبدأ عدم التدخل فرأينا أنه بالرغم من عدم وجود حدود في الفضاء السيبراني فإن مبدأ السيادة ينطبق على الأجهزة والاتصالات التي تستعمل بالدولة للقول بوجود السيادة للدولة في الفضاء السيبراني، ورأينا كيف يتم تطبيق مبدأ عدم التدخل في الفضاء السيبراني أيضا وذلك عن طريق عدم جواز استعمال الفضاء السيبراني في التدخل في الشؤون الداخلية والخارجية للدولة حيث يعد ذلك تعديا وفقا للقانون الدولي، وقد وضحت الأمثلة التي تم بيانها كيفية انطباق السيادة ومبدأ عدم التدخل في الفضاء السيبراني حيث تم ربط الفضاء السيبراني على المبدأين وأخيرا رأينا كيف أن لمجلس الأمن الحق في التدخل السيبراني إذا كان الأمر يتعلق بالأمن والسلم الدوليين.

## المبحث الثالث

## موقف الدول من القانون الدولي ومدى انطباقه على الفضاء السيبراني

لا توجد اتفاقية شاملة تتعلق بالفضاء السيبراني، إلا أن هناك بعض المعاهدات التي تتناول القضايا السيبرانية، مثال ذلك الجرائم السيبرانية (اتفاقية بوداباست)، أما الاتفاقيات العالمية الشاملة لموضوع الفضاء السيبراني لا زالت في طور التطور وما زالت المناقشات قائمة لتبني اتفاقية دولية خاصة بالفضاء السيبراني، إلا أنه يوجد مجموعة من الممارسات التي تتبناها الدول متعلقة بسلوكها بالفضاء السيبراني، فالدول مترددة في تبني ممارسات وسلوكيات متعلقة بالفضاء السيبراني، وفي الآونة الأخيرة تبنى عددٌ من الدول ممارسات ونشرت موقفها من القانون الدولي والفضاء السيبراني وكيف ينطبق برأيها القانون الدولي في الفضاء السيبراني، هذا وقد تبنت بعض الهيئات الدولية خارطة طريق لسلوك الدول في الفضاء السيبراني ومن هذه الهيئات هيئة الأمم المتحدة وحلف الناتو، وذلك كما سبق ذكره في هذا البحث، وفي هذا المبحث سيتم التطرق إلى اتجاهات الدول وموقفها في السؤال المتعلق بكيفية انطباق القانون الدولي في الفضاء السيبراني بما أنه لا توجد اتفاقيات ملزمة متعلقة بالفضاء السيبراني، فنتجه إلى العرف والذي هو أيضا مصدر من مصادر القانون الدولي، إلا أنه لم يوجد وقت كافي لتكوّن العرف الدولي بخصوص الفضاء السيبراني وأن الدول قد وضعت قواعد خاصة بالفضاء السيبراني، فيجب أن نتذكر أن الفضاء السيبراني ليس فلكًا بلا قانون، حيث تحكم القوانين الدولية المعمول بها في السلوكيات السيبرانية واستخدام الأسلحة السيبرانية، بالإضافة إلى ذلك يجب أن يتم تطبيق النظام القانوني الدولي الموجود بالكامل على الفضاء السيبراني، وهو موقف تم قبوله من قبل عدة دول بما فيها الولايات المتحدة

الأمريكية. لقد اتفقت الدول على أن الفضاء السيبراني يخضع للقانون الدولي وينطبق عليه، بالإضافة إلى ذلك فإن هناك توافقًا دوليًا على أن القانون الدولي الإنساني أيضا ينطبق على الفضاء السيبراني لكن السؤال المطروح هو كيف ينطبق القانون الدولي على الفضاء السيبراني وهو السؤال الذي يحاول هذا البحث الإجابة عنه، ولكنه ليس بالأمر الهين فهناك عدة أمور يجب التطرق لها للإجابة عن هذا السؤال ومن الممكن أن يتم الإجابة على هذا السؤال من خلال معرفة مواقف الدول تجاه هذا السؤال والتي نستطيع أن نستشف منها مواقف الدول وتوجهاتها فيما يتعلق بالفضاء السيبراني، ومن هذه الدول الولايات المتحدة الأمريكية وبريطانيا وبعض الدول الأوروبية وسنبين موقف كلٍّ من هذه الدول:

**موقف الدول المتعلق بالفضاء السيبراني:**

## المطلب الأول

## موقف الولايات المتحدة الأمريكية

تلعب الولايات المتحدة الأمريكية دورا مهما في مجال الأمن السيبراني والتعامل مع التهديدات السيبرانية، ففي مارس ٢٠٢٣ أعلن الرئيس الأمريكي جو بادين إستراتيجية الولايات المتحدة الأمريكية فيما يتعلق بالأمن السيبراني(١)، كما قامت

(١) الولايات المتحدة تعلن عن إستراتيجية وطنية جديدة للأمن السيبراني، aitnews، ٢-٣-٢٠٢٣، https://aitnews.com/2023/03/02/%D8%A7%D9%84%D9%88%D9%84%D8%A7%D9%8A%D8%A7%D8%AA-%D8%A7%D9%84%D9%85%D8%AA%D8%AD%D8%AF%D8%A9-=

الولايات المتحدة الأمريكية بتقديم آرائها بما يتعلق بالقانون الدولي والفضاء السيبراني إلى لجنة الخبراء الحكوميين وفيها عبرت الولايات المتحدة الأمريكية عن آرائها وتوجهاتها في هذا الشأن وبالرغم من عدم أخذ لجنة الخبراء بالرأي الأمريكي المتعلق بالقانون الدولي الإنساني فإننا نرى أن التوجه الأمريكي كان في تقسيم قانون النزاعات المسلحة إلى قسمين وهما استخدام القوة في وقت الدفاع عن النفس، والقانون الذي ينظم النزاعات المسلحة، وقد قامت الولايات المتحدة الأمريكية بتقديم توجهها المتعلق بالقانون الدولي في الفضاء السيبراني في لجنة الخبراء في العامين ٢٠١٣ و٢٠١٥ هذا بالإضافة إلى تقرير ٢٠٢١ وفيهما أقرت الولايات المتحدة بانطباق القانون الدولي بالفضاء السيبراني وانطباق ميثاق الأمم المتحدة في الفضاء السيبراني، هذا وقد أشارت الولايات المتحدة إلى انطباق المادة ٢ فقرة ٤ المتعلقة بتحريم استخدام القوة ضد السيادة الإقليمية والسياسية للدول، كما أباح موقف الولايات المتحدة للدول الدفاع عن نفسها وهذا ما جاءت به المادة ٥١ من ميثاق الأمم المتحدة.

هذا وقد قامت الولايات المتحدة الأمريكية بتحديد كيفية انطباق القانون الدولي الإنساني على الفضاء السيبراني بالتفصيل وذلك في دليل قانون الحرب الخاص بوزارة الدفاع الأمريكية، وقد قامت الولايات المتحدة أيضا بتحديد كيفية انطباق القانون الدولي على الفضاء السيبراني في موضع آخر منها موقف الحكومة الأمريكية من مبدأ السيادة وكيفية انطباقه على الفضاء السيبراني، فقد أشار التقرير إلى انطباق مبدأ السيادة في الفضاء السيبراني وجاء ذلك متوافقا مع اتجاه الولايات المتحدة الأمريكية في مشاركتها

=

%D8%AA%D8%B9%D9%84%D9%86-%D8%B9%D9%86-%D8%A5%D8%B3%D8%AA%D8%B1%D8%A7%D8%AA%D9%8A%D8%AC%D9%8A%D8%A9-%D9%88/.(تم الزيارة ١٩-٣-٢٠٢٤)

في لجنة الخبراء لسنة ٢٠١٣ و٢٠١٥، وتعقيبا على هذين التقريرين فقد أقرت الولايات المتحدة الأمريكية بانطباق السيادة الإقليمية في الفضاء السيبراني، إلا أن الولاية الإقليمية ليست مطلقة وفقا للرأي الأمريكي فيجب أن تكون متوافقة مع القانون الدولي وقوانين حقوق الإنسان(١)، كما جاء ذكر مبدأ عدم التدخل في تقرير لجنة الخبراء لعام٢٠١٥ وهو المبدأ المنصوص عليه في قضية نيكاراغوا وهو يعتبر من القانون الدولي العرفي، فلا يجب التدخل في الأمور السياسية والاقتصادية والاجتماعية والثقافية للدولة وفقا لهذا المبدأ، ومثال على ذلك في الفضاء السيبراني قيام دولة بالتدخل السيبراني لتغير نتيجة الانتخابات في دولة أخرى فهذا يعد تدخلا سافرا في السيادة الإقليمية للدولة، كما أنه في بعض الأحوال يعتبر التدخل السيبراني الذي لا يرقى إلى استخدام القوة أو مبدأ عدم التدخل قد يكون مخالفًا للقانون الدولي، لكن من الجدير بالذكر أن العمليات السيبرانية التي تقام عن بعد والتي تقوم بها دولة عن طريق أجهزة الحاسوب أو أجهزة أخرى متصلة بشبكة تقع على أراضي دولة أخرى لا تشكل بحد ذاتها انتهاكا للقانون الدولي حيث لا يوجد حظر في القانون الدولي على مثل هذه العمليات.

كما أن سيادة الدولة على إقليمها ليست مطلقة حيث يجب عليها أن تكون متوافقة مع قوانين حقوق الإنسان مثل الإعلان العالمي لحقوق الإنسان والعهد الدولي للحقوق المدنية والسياسية والعهد الدولي للحقوق الاقتصادية والثقافية والاجتماعية بما في ذلك حق التعبير عن الرأي الذي يتم باستخدام الفضاء السيبراني.

(١)الجمعية العامة للأمم المتحدة، الدورة السابعة والسبعون
13-7-2021, A/76/136 https://documents.un.org/doc/undoc/ gen/n21/ 189/46/ pdf/n2118946.pdf

أما بالنسبة لمبدأ العناية الواجبة الذي أشارت إليه بعض الدول في آرائها فإن الولايات المتحدة الأمريكية ترى أنه في يجب على الدولة أن تمنع الأنشطة الصادرة عن أراضيها والتي تضر بالدول الأخرى، وهذا الالتزام منصوص عليه بالقانون الدولي ومن الأجدر أن ينطبق على الفضاء السيبراني، وقد خلص تقريرا فريق الخبراء الحكوميين لعامي ٢٠١٣ و٢٠١٥ إلى أن الدول يجب أن تفي بالتزاماتها الدولية فيما يتعلق بالأفعال غير المشروعة دوليًا والمنسوبة إليها بموجب القانون الدولي. وبالإضافة إلى ذلك، يجب ألا تستخدم وكلاء لارتكاب أفعال غير مشروعة دوليًا باستخدام تكنولوجيا المعلومات والاتصالات.

## المطلب الثاني

## موقف الدول الأوربية

تعددت أراء الدول الأوروبية، وهي -وإن اختلفت في بعض المواضع- قد اتفقت في مواضع أخرى، فالنسبة إلى موقف الدول الأوربية، فالعديد من الدول الأوربية قد قامت بنشر موقفها تجاه الفضاء السيبراني وكيفية انطباق القانون الدولي عليه، إلا أنه يوجد توجه بتوحيد هذه الممارسات والمواقف، وهنا سنبحث موقف الدول الأوربية متمثلة بوقف الاتحاد الأوروبي من الفضاء السيبراني، وكيفية انطباق القانون الدولي عليه، فمما لا شك فيه أن القانون الدولي ينطبق على الفضاء السيبراني وهو ما وافقت عليه وأجمعت عليه العديد من الدول، فمعظم الدول قد أشارت إلى انطباق القانون الدولي على الفضاء السيبراني لكن كيف؟ وذلك موضع اختلاف، فالعديد من الدول لم تصرح بكيفية ذلك، إلا أنه في الآونة الأخيرة قامت العديد من الدول بتحديد موقفها تجاه ذلك ومن هذه الدول دول

الاتحاد الأوربي، والذي يعمل على توحيد موقفه من كيفية انطباق القانون الدولي على الفضاء السيبراني وسنستعرض مواقف الاتحاد الأوروبي التي تم التصريح بها:

**أولا:** إن دول الاتحاد الأوروبي كلها قد اتفقت على انطباق القانون الدولي في الفضاء السيبراني، كما أقرت بانطباق ميثاق الأمم المتحدة على الفضاء السيبراني فلم يعد الفضاء السيبراني بلا تنظيم، ثانيا بالنسبة لمبدأ السيادة والذي تم إقراره -كما سبق بيانه في لجنة الخبراء الحكوميين التابعة للأمم المتحدة، بالنسبة للاتحاد الأوربي- نشرت ٩ دول من دول الاتحاد رأيها بالتفصيل عن انطباق مبدأ السيادة في الفضاء السيبراني، كما اتفقت ٢٣ دولة على انطباق مبدأ السيادة في الفضاء السيبراني ومن هذه الدول هولندا وفرنسا اللتان أوضحتا صراحة انطباق هذا المبدأ وتلت ذلك دول أوربية أخرى هي إستونيا، النمسا، فنلندا، الشيك، ألمانيا، رومانيا، إيطاليا[1].

فبالنظر لهذه الدول نجد أن السيادة ينشأ عنها حقوقٌ وواجبات، وأن خرق أي دولة للفضاء السيبراني ينشأ عنه عمل غير مشروع دوليًا، فوفقا لألمانيا والشيك فإن السيادة مرتبطة بإقليم الدولة، أما فنلندا فقد نصت على حماية إقليمها من أي تأثير ضار، كما أن كلًا من فرنسا وفنلندا وإستونيا فتحوا المجال أمام أن يكون الهجوم السيبراني خارج إقليمها وذلك مثل السحاب الإلكتروني، أما هولندا فإن سياستها المعلنة قد وافقت ما يخص السيادة الإقليمية مع دليل (تالين) حيث أقرت أن أي انتهاك لسلامة أراضي الدولة، بالإضافة إلى تدخل في الوظائف الحكومية للدولة

(1) Anna-Maria Osula, Agnes Kasper & Aleski Kajander, EU Common Position on International Law and Cyberspace, 16 MASARYK U. J.L. & TECH. 89 (2022).

يعد انتهاكًا لسيادة الدولة، أما كلٌ من الشيك وفنلندا فرأت -بالإضافة إلى الضرر المادي- أنه يجب أن يتوافر فقدان العمل المادي الذي قد يكون أيضا أساسا للمطالبة بانتهاك السيادة، وقد أوضحت فرنسا أن أي اعتداء سيبراني على إقليم فرنسا موجه من دولة ضد سلامة أجهزة الاتصالات والفضاء السيبراني في إقليم فرنسا يعد انتهاكا للسيادة الفرنسية، كما أن فرنسا تعتبر الهجوم السيبراني الفاشل اعتداء على سيادتها حيث تتطلب فرنسا شرطين: ١) أن تكون العملية السيبرانية هجوما إلكترونيا ٢) أن يكون باسم الدولة وإشرافها.

أما فيما يتعلق بمبدأ عدم التدخل فإن دول الاتحاد الأوربي من بينها ٧ دول عبرت عن رأيها في مبدأ عدم التدخل، وهو كالتالي يجب على الدول عدم التدخل قسرا في الشؤون الداخلية أو الخارجية للدول، وبالرغم من عدم النص صراحة على مبدأ عدم التدخل في ميثاق الأمم المتحدة فإنه يمكن أن يعتبر جزءًا من مبدأ السيادة أو القانون الدولي العرفي، وقد اتفقت الدول السبع أنه لا بد من توافر ركنين ليتم إقرار أمر ما على أنه تدخل، الأول: يكون الفعل تدخلا في المسائل الداخلية للدولة أي أن تتدخل في اختصاص دولة أخرى، ثانيا: يجب أن يكون التدخل قسريا. لكن ما يؤخذ على هذين الشرطين هو أن طبيعة الفعل القسري لم يتم الاتفاق عليها، وقد قامت ألمانيا بضرب مثال على ذلك وهو قيام دولة بنشر معلومات غير صحيحة عن طريق الإنترنت ووسائل التواصل الاجتماعي وذلك للتحريض على العنف السياسي وأعمال الشغب والصراعات الأهلية في بلد أجنبي، كما تعمل على إعاقة سير الانتخابات وأيضا التلاعب بالانتخابات فكل هذه الأمور تعد تدخلا في الشؤون الداخلية للدول، إلا أن هناك آخرين كانوا أكثر حذرا حيث يعتبرون أنه لكي يعد الفعل إكراها، فإنه ينبغي أن تحرم الدولة المستهدفة فعليا من قدرتها على التحكم وإدارة الأمور، ففرنسا ترى أن أي تدخل إلكتروني في شؤونها الداخلية أو الخارجية يعتبر تدخلا غير مقبول.

## المطلب الثالث

## موقف بريطانيا من الفضاء السيبراني والقانون الدولي

نشرت بريطانيا تقريرا يبين موقفها من الفضاء السيبراني والقانون الدولي في ٣ -٦-٢٠٢١[(١)]، ويعد هذا التقرير ضمن إسهام بريطانيا في مجموعة الخبراء الحكوميين التي أنشئت بناء على قرار من الجمعية العامة للأمم المتحدة، وقد عبرت بريطانيا عن موقفها من خلال سبع صفحات، وقد أيد التقرير ما توصلت إليه لجنة الخبراء السابقة من أن القانون الدولي وميثاق الأمم المتحدة ينطبق على الفضاء السيبراني، وقد أوضح التقرير أنه لا يوجد تعريف متفق عليه فيما يتعلق بالفضاء السيبراني، وعرف التقرير الفضاء السيبراني بأنه: "مجال الأفعال التي يتم تنفيذها باستخدام شبكة مترابطة من البنى التحتية لشبكة المعلومات والتي تشمل الإنترنت وشبكات الاتصالات المتصلة بالإنترنت، أنظمة الحاسوب والأجهزة المتصلة بالإنترنت"[(٢)]. وقد أقر التقرير بأن ميثاق الأمم المتحدة ينطبق على تعاملات الدول في الفضاء السيبراني وقد خصَّ التقرير بالذكر المادة ٢ فقرة ٤ المتعلقة بحظر استخدام القوى في القانون الدولي، وعليه فقد أقر التقرير بحظر استخدام القوى المتعلقة بالفضاء السيبراني للتعدي على سيادة دولة أخرى، وعد استخدام الهجمات السيبرانية فعلًا عدائيًا يفعل حالة الدفاع الشرعي سواء الدفاع الفردي أو الدفاع

(1) Application of international law to states' conduct in cyberspace: UK statement, UK Gov., 3 June, 2021, https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement (accessed 29-9-2024).

(2) Id.

الجماعي وفقا للمادة ٥١ من ميثاق الأمم المتحدة، وهذا ما يؤكد على موقف بريطانيا من أن ميثاق الأمم المتحدة ينطبق على الفضاء السيبراني، ويكون الرد على الهجوم إما سيبرانيا أو بواسطة الجيش على أن يكون الهجوم موافقا ويستوفي متطلبات الضرورة والتناسب، بالإضافة إلى ذلك فتنطبق المادة ٢ فقرة ٣ من ميثاق الأمم المتحدة وأيضا الفصل السادس من الميثاق والمتعلقة بالتسوية السلمية للنزاعات على الفضاء السيبراني، ووفقا للمادة ٣٣ فقرة ١، فإن الدول التي هي طرف في نزاع دولي متعلق بالفضاء السيبراني، والذي من الممكن أن يؤدي إلى الإخلال بالأمن والسلم الدوليين، فيجب عليها محاولة حل النزاع بالوسائل السلمية، أما بالنسبة إلى مبدأ السيادة وعدم التدخل فإن الموقف البريطاني منه كالتالي: تناول التقرير موقف بريطانيا من السيادة وعدم التدخل وقد قرر التقرير أن عدم التدخل يعد من القانون العرفي وينطبق على الفضاء السيبراني حيث لا يجوز للدول التدخل في الشؤون الداخلية لدول أخرى وهذا ما تم النص عليه في قضية نيكاراغوا وقد سبق بيان القضية وكيفية انطباقها على مبدأ عدم التدخل ومبدأ عدم التدخل مرتبط بمبدأ السيادة ارتباطا وثيقا فللدولة الحرية في اختيار أمورها السياسية والاجتماعية والاقتصادية والثقافية دون تدخل من أحد، وأوضحت بريطانيا أن عدم التدخل هو موضع نقاش وعدم اتفاق، إلا أن بريطانيا ترى أن التدخل السيبراني لدولة في الشؤون الاقتصادية أو الانتخابات العامة وتغير نتيجة هذه الانتخابات والتدخل في الشؤون الصحية في المستشفيات كل ذلك يعد تدخلا محرمًا وفقا للقانون الدولي.

وقد قررت محكمة العدل الدولية أن التدخل المحظور هو التدخل الذي يتعلق بأمور يُسمح لكل دولة، بموجب مبدأ سيادة الدولة، بأن تقررها بحرية. والسيادة، كمبدأ عام ومفهوم أساسي في القانون الدولي. وتذكّر المملكة المتحدة بأن أي حظر على أنشطة الدول سواء فيما يتصل بالفضاء الإلكتروني أو غيره من الأمور، يجب أن يكون منصوصًا عليه بوضوح إما في القانون الدولي العرفي أو في معاهدة ملزمة للدول

المعنية، ولا ترى المملكة المتحدة أن المفهوم العام للسيادة في حد ذاته يوفر أساسًا كافيًا أو واضحًا لاستقراء قاعدة محددة أو حظر إضافي للسلوك الإلكتروني يتجاوز عدم التدخل المشار إليه أعلاه.

وقد تحدث التقرير أيضا عن مسؤولية الدولة والتدابير المضادة إضافة إلى القانون الدولي لحقوق الإنسان والقانون الدولي الإنساني.

## المطلب الرابع

## موقف الدول الإفريقية من الفضاء السيبراني والقانون الدولي

في التاسع والعشرين من يناير ٢٠٢٤ تبنى الاتحاد الإفريقي موقفه المتعلق بالفضاء السيبراني والقانون الدولي، وتمت الموافقة عليه من قبل البرلمان الإفريقي في الثامن عشر من فبراير ٢٠٢٤[1]، ويمثل هذا الرأي توجهات ٥٥ دولة من الاتحاد الإفريقي ورأيها في كيفية انطباق القانون الدولي في الفضاء السيبراني، ويتكون رأي الاتحاد الإفريقي من ديباجة وأحد عشر فصلا، ويشمل رأي الاتحاد الإفريقي عدة مواضيع منها السيادة، وعدم التدخل، وحل النزاعات بالطرق السلمية، وتحريم التهديد

(1) Russell Buchan, Nicholas Tsagourias, The African Union's Statement on the Application of International Law to Cyberspace: An Assessment of the Principles of Territorial Sovereignty, Non-Intervention, and Non-Use of Force, Feb. 20, 2024, https://www.ejiltalk.org/the-african-unions-statement-on-the-application-of-international-law-to-cyberspace-an-assessment-of-the-principles-of-territorial-sovereignty-non-intervention-and-non-use-of-force/ (accessed on 30-8-2024).

باستخدام القوة، بالإضافة إلى القانون الدولي لحقوق الإنسان والقانون الدولي الإنساني، وهي كما نرى مشابهة لما تم مناقشته في كلٍّ من دليل (تالين)، ولجنة الخبراء الحكوميين التابعة للأمم المتحدة، وأيضا هي ذات المواضيع التي تم النص عليها في تقرير بريطانيا المتعلق بالفضاء السيبراني والقانون الدولي، ففيما يتعلق بالسيادة تم النص عليها في الفصل الثاني من ورقة الاتحاد الإفريقي حيث نصت الورقة على أن واجب احترام سيادة الدول يعد مبدأ أساسيًا من مبادئ القانون الدولي وتؤكد الورقة أن القانون الدولي ينطبق على الفضاء السيبراني، وقد نصت الورقة على أنه لا يجوز لدولة التدخل في أراضٍ أجنبية ردا على أنشطة إلكترونية غير قانونية[1]، كما نصت الورقة بأن أي دخول غير مصرح به من قبل دولة على الفضاء السيبراني لدولة أخرى يعد محظورًا، كما نصت الورقة على أن اللجوء إلى استخدام القوة محظورٌ في القانون الدولي ويعد من القواعد الآمرة في القانون الدولي والتي لا يجوز مخالفتها إلا في حالتين وهما حالة الدفاع الشرعي وفي حالة أقر مجلس الأمن بذلك وفقا للفصل السابع من ميثاق الأمم المتحدة، وقد نصت الورقة على انطباق المبدأ والحالتين الاستثنائيتين على الفضاء السيبراني ويبقى السؤال الرئيسي هو كيفية انطباق المبدأ على الفضاء السيبراني فقد نصت الورقة على أن السيادة الإقليمية للدولة هي مبدأ أساسي في القانون الدولي وتنطبق على الفضاء السيبراني أيضا، فوفقا للسيادة الإقليمية فإن الدولة تمارس كافة سلطاتها في إقليمها وعلى الأشخاص في إقليمها وعليه فكافة الأدوات السيبرانية الموجودة في الدولة تخضع لسيادة الدولة، وعليه فإن أي تدخل غير مصرح فيه في الفضاء السيبراني للدولة يعد انتهاكا

(1) Mohamed Helal , The Common African Position on the Application of International Law in Cyberspace: Reflections on a Collaborative Lawmaking Process, Feb. 5, 2024, https://www.ejiltalk.org/the-common-african-position-on-the-application-of-international-law-in-cyberspace-reflections-on-a-collaborative-lawmaking-process/ (accessed 27-11-2024).

لسيادتها الإقليمية، كما حضرت الورقة أن تقوم الدولة بالتدخل السيبراني في دولة أجنبية حيث يعد ذلك اعتداء على السيادة الإقليمية للدولة، فوفقا للاتحاد الإفريقي فإن السيادة في الفضاء السيبراني هي ذاتها السيادة الإقليمية للدولة ويجب احترامها وعدم المساس بها.

كما ناقشت الورقة موضوع عدم التدخل وفيه وضحت الورقة بأن مبدأ عدم التدخل من مبادئ القانون الدولي والتي تحرم التدخل في الشؤون الداخلية والخارجية للدولة وقد قرر الاتحاد الإفريقي بأن ذلك ينطبق أيضا على الفضاء السيبراني.

وكما رأينا فإن جميع الدول قد أجمعت على انطباق القانون الدولي على الفضاء السيبراني، وتناولت كل دولة كيفية انطباق القانون الدولي على الفضاء السيبراني، فلم يُترك هذا الفضاء دون تنظيم، ورأينا كيف أن مبدأ السيادة ومبدأ عدم التدخل ينطبق على الفضاء السيبراني وهما مبدآن مهمان في القانون الدولي، ومن الملاحظ أن كلا من الدول المتطورة مثل الولايات المتحدة وبريطانيا أقرت بحقها في الدفاع عن نفسها مقابل الهجمات السيبرانية التي تتعرض لها فقد أقرت هذه الدول بحقها بالرد عن طريق الهجوم بالجيش أو الهجوم السيبراني، بالمقابل توجهت الدول الأقل تطورا إلى الاستعانة بدول أخرى للرد على الهجمات السيبرانية، كما أشارت الدول الأفريقية بعدم جواز الهجوم السيبراني ونحن نرى أن دول الخليج عليها اتباع النهج الذي سارت عليه الدول الأفريقية، كما يجب على عليها تحديد موقفها من الفضاء السيبراني والذي لا يخرج عن مواقف الدول التي تم الإشارة لها.

## الخاتمة

كما رأينا فإن كلًا من الأمم المتحدة والمنظمات الإقليمية وفقهاء القانون قد اتفقوا على رأي واحد وهو انطباق القانون الدولي على الفضاء السيبراني، هذا وقد كان يعد الفضاء السيبراني فضاء بلا قانون ينظمه إلى أن تم إنشاء لجنة الخبراء الحكوميين التابعة للأمم المتحدة، وجاء دليل (تالين، واحد واثنان) ليؤكد ذلك كما أسهم فقهاء القانون في الوصول إلى هذه النظرية، بالإضافة إلى قيام العديد من الدول بنشر آرائها بما يتعلق بالقانون الدولي والفضاء السيبراني.

ومن ناحية أخرى، يمكن اعتبار الفضاء السيبراني كالفضاء الخارجي ومنطقة أعالي البحار التي يحكمها القانون الدولي، وسعت كل دولة إلى تحديد كيفية انطباق القانون الدولي على الفضاء السيبراني حيث لا يوجد حدود ولا فواصل في الفضاء السيبراني، وفي سبيل ذلك فقد أقرت معظم الدول أن مبدأ السيادة ينطبق في الفضاء السيبراني، كما اتفقت الدول والفقهاء على أن مبدأ عدم التدخل ينطبق على الفضاء السيبراني فلا يجوز للدول التدخل في الشؤون الداخلية أو الخارجية للدول الأخرى عن طريق الفضاء السيبراني وقد قمنا بتوضيح آراء الدول المختلفة فيما يتعلق بمبدأ السيادة ومبدأ عدم التدخل ولاحظنا أن معظم الدول اتفقت على آليات متشابهة فيما يتعلق بهذه المبادئ.

كما قامت دول بتوضيح أن مبدأ السيادة وعدم التدخل لا ينطبقان في مجال حقوق الإنسان وأنه يجب حماية حق الإنسان في التعبير وغيره من الحقوق في الفضاء السيبراني، كما شاركت عدد من الدول برأيها في أن القانون الدولي الإنساني ينطبق على

الفضاء السيبراني، وهناك من لم يصرح بذلك إلا أنه أشار إلى انطباق مبدأ التمييز والتناسب والضرورة الخاصين بالقانون الإنساني على الفضاء السيبراني.

وعليه -وبالرغم من عدم وجود اتفاقية دولية تنظم الفضاء السيبراني والتي قد تكون ذلك سببا في خرق وارتكاب هجمات سيبرانية- فإن هناك توافقًا على المبادئ الأساسية، وإن موطن الاختلاف بين الدول وسبب عدم التوصل إلى اتفاقية دولية هو عدم رغبة بعض الدول إلى وجود قواعد الزامية تمنعها من شن هجمات سيبرانية، إلا أن هناك توافقًا بين آراء الدول، ويكمن الاختلاف في أن الدول الأضعف قدراة سيبرانية كانت الأكثر قبولا لوجود تعاون دولي في مجال الفضاء السيبراني، وقد تشكل آراء الدول إذا ما تم العمل بها قانونا دوليا عرفيا، إلا أننا نرى أنه من الأفضل وجود اتفاقية دولية تنظم الفضاء السيبراني، لكن الوصول إلى اتفاقية دولية متعلقة بالفضاء السيبراني أمر قد يأخذ سنوات طويلة وعدة اجتماعات ونقاشات، وعليه فإن آراء الدول واتفاقاتها سواء الإقليمية أم الفردية أمر في غاية الأهمية وذلك لتوضيح كيفية عمل القانون الدولي في الفضاء السيبراني، وأن محاولات الناتو -عن طريق دليل (تالين، الأول والثاني) إضافة إلى عمل لجنة الخبراء الحكوميين في الأمم المتحدة- لهي الاتجاه الصحيح الذي يجب أن تمضي فيه الدول لمحاولة تنظيم الفضاء السيبراني.

**المراجع**:

**١. الاتفاقيات والمعاهدات الدولية:**

- ميثاق الأمم المتحدة
- اتفاقية بودباست

**٢. قرارات الأمم المتحدة:**

- قرار الجمعية العامة للأمم الدورة السبعون، التطورات في ميدان الاتصالات السلكية واللاسلكية في سياق الأمن الدولي، تقرير فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات السلكية واللاسلكية في سياق الأمن الـــــــــــــــــــــــــدولي، ٢٢-٧-٢٠١٥، https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/33/PDF/N1522833.pdf?OpenElement) تم الدخول في ٥-٨-٢٠٢٢A (الامم المتحدة / ١٧/٧٠ الفقرة ٢٦
- جمعية العامة للأمم المتحدة، الدورة السابعة والسبعون، ١٣-٧-٢٠٢١، A/76/136 https://documents.un.org/doc/undoc/gen/n21/189/46/pdf/n2118946.pdf
- United Nations (Open Ended Working Group), https://disarmament.unoda.org/open-ended-working-group/ ( accessed 27-11-2024).
- United Nation General Assembly, 10-3-2021, A/AC.290/2021/CRP.2, https://front.un-arm.org/wp-

content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf (accessed 27-11-2024).

**٣. الكتب الأجنبية:**

- M N. Schmitt (Ed), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge University Press, 2017).
- M N. Schmitt (Ed), Tallinn Manual on the International Law Applicable to Cyber Operations (Cambridge University Press, 2013).
- W. Gibson, Neuromancer (Ace Publishing, 1984) .

**٤. الأبحاث والتقارير العربية**

- علاء الدين فرحات، الفضاء السيبراني: تشكيل ساحة المعركة في القرن الحادي والعشرين، جامعة الوادي، مجلة العلوم القانونية والسياسية، المجلد ١٠، العدد ٣، ديسمبر ٢٠١٩، ص 90.
- د. وفاء لطفي، الجهود الدولية في مجال مكافحة جرائم الإرهاب السيبراني: التجربة الماليزية نموذجا، جامعة القاهرة، مجلة كلية الاقتصاد والعلوم السياسية، المجلد ٢٣، العدد ١ - الرقم المسلسل للعدد ٩٠، يناير ٢٠٢٢، https://jpsa.journals.ekb.eg/article_211371.html (تم الدخول في ١٢-٧-٢٠٢٢).

- د. جمال بوازيدية، الإستراتيجية الجزائرية في مواجهة الجرائم السيبرانية التحديات والآفاق المستقبلية، جامعة الوادي، مجلة العلوم القانونية والسياسية، المجلد ١٠ العدد ١، ابريل ٢٠١٩، ص ١٢٦٨.
- عبدالرحمن فهد أحمد، (٢٠٢٣)، الإطار القانوني للأمن السيبراني لدول مجلس التعاون الخليجي، مجلة دراسات الخليج والجزيرة العربية، ٤٩ (١٩٠)،٢٥٧-٢٩٨.

**٥. الأبحاث والتقارير الأجنبية**

- Oğurlu, E. (2023). International Law in Cyberspace: An Evaluation of the Tallinn Manuals. Annales de la Faculté de Droit d'Istanbul, 0(73), 327-344.
- Application of international law to states' conduct in cyberspace: UK statement, UK Gov., 3 June, 2021, https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement
- Michael Schmitt, The Sixth United Nations GGE and International Law in Cyberspace, June 10, 2021, https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/ (accessed 5-8-2022).

- Anna-Maria Osula, Agnes Kasper & Aleski Kajander, EU Common Position on International Law and Cyberspace, 16 MASARYK U. J.L. & TECH. 89 (2022)
- General Assembly, Group of Governmental Experts on Advancing Responsible
  State Behaviour in Cyberspace in the Context of
  International Security, 14-7-2021, https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf , A/76/135, (accessed 13-9-2024).
- Harriet Moynihan, The Application of International Law to state Cyberattacks Sovereignty and Non-intervention, Chatham House, December 2019.
- YOO Joonkoo, UN Open-Ended Working Group Final Report: Issues and Implications, April, 2021, The Institute of Foreign Affairs and National Security (IFANS), IF2020-36E.
- Jianming Shen, The Non-Intervention Principle and Humanitarian Interventions under International Law, 7 INT'l LEGAL THEORY 1 (2001).

٦. المواقع الإلكترونية

- الولايات المتحدة تعلن عن إستراتيجية وطنية جديدة للأمن السيبراني، aitnews، ٢-٣-٢٠٢٣،

https://aitnews.com/2023/03/02/%D8%A7%D9%84%D9%88%D9%84%D8%A7%D9%8A%D8%A7%D8%AA-%D8%A7%D9%84%D9%85%D8%AA%D8%AD%D8%AF%D8%A9-%D8%AA%D8%B9%D9%84%D9%86-%D8%B9%D9%86-%D8%A5%D8%B3%D8%AA%D8%B1%D8%A7%D8%AA%D9%8A%D8%AC%D9%8A%D8%A9-%D9%88/

- Russell Buchan, Nicholas Tsagourias, The African Union's Statement on the Application of International Law to Cyberspace: An Assessment of the Principles of Territorial Sovereignty, Non-Intervention, and Non-Use of Force, Feb. 20, 2024, https://www.ejiltalk.org/the-african-unions-statement-on-the-application-of-international-law-to-cyberspace-an-assessment-of-the-principles-of-territorial-sovereignty-non-intervention-and-non-use-of-force/
- Global Cybersecurity Index, The International Telecommunication Union (ITU), https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (accessed 2-8-2022).

- Update to Cyber Security Definition in the document TD 2761R1 (X.1250), The International Telecommunication Union (ITU), https://www.itu.int/md/T05-SG17-C-0242 (accessed 1-8-2022).
- Cyberspace definition, Encyclopedia Britannica, https://www.britannica.com/topic/cyberspace (accessed 11-7-2022).
- The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Information Operations and Activities, The Oxford Process, https://www.elac.ox.ac.uk/the-oxford-process/the-statements-overview/the-oxford-statement-on-the-regulation-of-information-operations-and-activities/#/ ( accessed on 1-9-2024).
- Russell Buchan, Nicholas Tsagourias, The African Union's Statement on the Application of International Law to Cyberspace: An Assessment of the Principles of Territorial Sovereignty, Non-Intervention, and Non-Use of Force, Feb. 20, 2024, https://www.ejiltalk.org/the-african-unions-statement-on-the-application-of-international-law-to-cyberspace-an-assessment-of-the-principles-of-territorial-sovereignty-non-intervention-and-non-use-of-force / (accessed on 30-8-2024).

- Introduction to the Oxford Process on International Law Protections in Cyberspace, e Oxford Institute for Ethics, Law and Armed Conflict, 13-12-2021, https://documents.unoda.org/wp-content/uploads/2021/12/OEWG-Side-Event-Oxford-Process-Introduction.pdf (accessed 27-11-2024).
- The Oxford Institute For Ethics, Law and Armed Conflict, Oxford University, https://www.elac.ox.ac.uk/ (accessed 19-8-2024).
- Mohamed Helal , The Common African Position on the Application of International Law in Cyberspace: Reflections on a Collaborative Lawmaking Process, Feb. 5, 2024, https://www.ejiltalk.org/the-common-african-position-on-the-application-of-international-law-in-cyberspace-reflections-on-a-collaborative-lawmaking-process/ (accessed 27-11-2024).