# الاليات الدولية المتبعة لمواجهة انتهاك السيادة السيبرانية

م.م قحطان شلاش حسن
كلية الإدارة والاقتصاد– جامعة تكريت–صلاح الدين–العراق
Qahtan.sh@tu.edu.iq

# International mechanisms used to address violations of cyber sovereignty

Qahtan Shalash Hassan
College of Administration and Economics - Tikrit University/Salah al-Din/Iraq

**المستخلص:** يستعرض هذا البحث الأطر القانونية والآليات الدولية الرامية إلى حماية "السيادة السيبرانية" باعتبارها امتداداً حديثاً للسيادة الوطنية في المجال الافتراضي. وتتجلى الإشكالية القانونية في قصور القواعد التقليدية للقانون الدولي عن استيعاب الطبيعة العابرة للحدود للانتهاكات السيبرانية، وما يرافقها من تعقيد في إسناد المسؤولية القانونية للجاني بسبب غياب التواجد المادي على مسرح الجريمة. ومن خلال تحليل الصكوك الدولية والجهود المؤسسية، يخلص البحث إلى عدم كفاية الآليات الراهنة –كـ "دليل تالين" والاتفاقيات الإقليمية– لافتقارها إلى صبغة الإلزام الدولي الشامل. مما يستوجب تكييف مفاهيم "العدوان" و"حق الدفاع الشرعي" وفق المادة (51) من ميثاق الأمم المتحدة لتشمل الهجمات الرقمية الجسيمة. ويؤكد البحث على ضرورة إيجاد تنظيم تشريعي دولي يتجاوز القوانين المحلية القاصرة، مع تفعيل دور مجلس الأمن في توصيف الانتهاكات السيبرانية كتهديد مباشر للسلم والأمن الدوليين، لضمان استقرار "المجال الخامس" للسيادة الدولية

**كلمات مفتاحية:** ( سيادة ,سيبرانية, انتهاك, اتفاقية, حدود)

**Abstract**

This research examines the legal frameworks and international mechanisms aimed at protecting "cyber sovereignty" as a modern extension of national sovereignty in the virtual realm. The legal challenge lies in the inadequacy of traditional international law rules to encompass the transnational nature of cyber violations and the accompanying complexity of assigning legal responsibility to perpetrators due to the absence of physical presence at the crime scene. Through an analysis of international instruments and institutional efforts, the research concludes that current mechanisms—such as the Tallinn Manual and regional agreements—are insufficient due to their lack of universal international binding force. This necessitates adapting the concepts of "aggression" and "the right of self-defense" under Article 51of the UN Charter to include serious cyberattacks. The research emphasizes the need for an international legislative framework that transcends inadequate domestic laws, while simultaneously activating the role of the Security Council in characterizing cyber violations as a direct threat to international peace and security, thus ensuring the stability of the "fifth domain" of international sovereignty.

**Keywords**: (sovereignty, cyber, violation, agreement, borders)

**المقدمة**

شهد العالم في الأعوام الأخيرة تصاعداً ملحوظاً في الانتهاكات السيبرانية التي باتت تتجاوز الحدود الجغرافية للدول، إذ لا تقتصر آثارها على إقليم محدد بل تمتد لتطال المجتمع الدولي بأسره، مما جعلها تمثل تهديداً حقيقياً للسلم والأمن الدوليين. وعلى الرغم من عدم وجود منظومة قانونية دولية موحدة وشاملة تنظم هذه الجرائم بصورة متكاملة، فإن ذلك لا يعني غياب الجهود الدولية، فقد سعت الدول إلى تطوير آليات مختلفة لحماية مصالحها وتقليل الأضرار الناجمة عنها، كما طُرحت مجموعة من المبادرات والحلول القانونية والتقنية التي يمكن توظيفها للحد من هذه الانتهاكات وتعزيز السيطرة عليها فقد تنبأت العديد من الدول و المنظمات الدولية الحكومية وغير حكومية العالمية إلى المخاطر التي يمكن ان تنتج عن إساءة استعمال تكنولوجيا المعلومات وشبكات الاتصالات، فبادرت إلى تشجيع ومنذ فترة ليست بالبعيدة على إجراء المباحثات والمفاوضات، وتقريب الآراء بين الدول بشأن العديد من القضايا ذات الصلة باستعمال تكنولوجيا المعلومات، وبالتحديد من أجل الوصول الى المعايير التي يكون من شأنها توفير الحماية من المخاطر الناتجة عن الاستخدام لتلك التقنيات بما فيها الحاسوب الآلي وشبكة الاتصالات والانترنت، إلا أن هذه الجهود لم تنجح حتى الآن في إيجاد الإطار القانوني الذي يحد من تلك

الانتهاكات، وذلك بسبب أن الدول المهيمنة والمسيطرة على قطاع التكنولوجيا الإلكترونية ليس لديها الرغبة في إبرام أي اتفاقيات في هذا الموضوع الذي يقيد من حريتهم.

**اهمية البحث:** تتلخص اهمية البحث في التعرف عن مدى كفاية الاتفاقيات الدولية ودور المنظمات الدولية والاقليمية في الحد من انتهاك السيادة السيبرانية على المستوى الدولي.

**مشكلة البحث:** تكمن مشكلة البحث في حداثة جرائم انتهاك السيادة السيبرانية والحاجة الملحة الى عقد الاتفاقيات الدولية وتنظيم دور المنظمات الدولية والاقليمية في هذا المجال.

**فرضية البحث:** ان وجود عالم خالي من انتهاك للسيادة السيبرانية في الوقت الحاضر يعد امر شبه مستحيل لذلك نسعى من خلال هذا البحث التوصل الى التقليل من هذه الانتهاكات السيبرانية.

**نطاق البحث:** سوف نتناول في هذا البحث الاتفاقيات الدولية والاقليمية والمنظمات ذات الصلة بانتهاك السيادة السيبرانية .

**منهجية البحث:** اقتضت ضرورة البحث العلمي اتباع المنهج التحليلي في تناول هذه الجزئية العلمية من خلال الوقوف على نصوص الاتفاقيات الدولية ذات الصلة بموضوع البحث وكذلك المعاهدات المنشئة للمنظمات الدولية نطاق الدراسة.

**خطة البحث:** اقتضت ضرورة البحث العلمي تقسيم خطة البحث الى ثلاث فروع وحسب الاتي::

**الفرع الاول: التعريف بالسيادة السيبرانية**

**الفرع الثاني :دور الاتفاقيات والمعاهدات الدولية في حماية السيادة السيبرانية.**

**الفرع الثالث: دور المنظمات الدولية والإقليمية في حماية السيادة السيبرانية.**

## الفرع الاول

## التعريف السيادة السيبرانية

**أولا. مدلول السيادة السيبرانية:**

تعود الجذور التاريخية لمفهوم السيادة إلى معاهدة وستفاليا سنة 1648، التي كرّست مبدأ تمتع الدولة بسلطة عليا على إقليمها وشؤونها الداخلية بعيداً عن تدخل الدول الأخرى، وهو ما جعل السيادة أحد الأسس الجوهرية التي قام عليها بناء القانون الدولي المعاصر. وقد حظي هذا

المفهوم باهتمام واسع لدى فقهاء القانون الدولي والمنظّرين السياسيين، نظراً لما يمثله من ركيزة لتنظيم العلاقات بين الدول.([1])

ومع التحولات الرقمية المتسارعة، برز مفهوم السيادة السيبرانية بوصفه مفهوماً حديثاً نسبياً، يُعبِّر عن سعي الدول إلى بسط سيطرتها على بياناتها الوطنية وبيانات مواطنيها، وحماية فضائها الرقمي من التأثيرات الخارجية. ففي البعد العسكري، يشير المفهوم إلى قدرة الدولة على بناء منظومات أمن سيبراني دفاعية وهجومية متطورة دون الاعتماد الكلي على التكنولوجيا الأجنبية، أما في بعده الاقتصادي فيرتبط بتنظيم عمل الشركات التكنولوجية الكبرى، وفرض الأطر الضريبية عليها، فضلاً عن دعم الابتكار المحلي وإنشاء الشركات الناشئة.

كما تُعرَّف السيادة السيبرانية بأنها امتداد طبيعي للسيادة الوطنية داخل الفضاء الرقمي، بما يخول الدول ممارسة أنشطتها الاقتصادية والأمنية وغيرها من الأنشطة في هذا الفضاء، إلى جانب حقها في اتخاذ التدابير اللازمة لحماية نفسها من الهجمات السيبرانية. ووفق هذا التصور، فإن الفضاء السيبراني ينبغي أن يخضع لمصالح الدولة وقيمها التنظيمية، بما يسمح للحكومات بإدارة شبكة الإنترنت داخل حدودها الوطنية وفق القواعد والمعايير التي تعتمدها. ومع ذلك، فإن الطبيعة العابرة للحدود للفضاء السيبراني أفرزت تحديات جدية أمام المفهوم التقليدي للسيادة، وأثارت تساؤلات حول مدى إمكانية تطبيق قواعد القانون الدولي التقليدية عليه..[(2)]

وانطلاقاً من ذلك، يُعد هذا الاتجاه التعريفي الأقرب إلى استيعاب عناصر السيادة السيبرانية المعاصرة، لشموله الأبعاد القانونية والتقنية والأمنية معاً. فقد أدى التقدم التكنولوجي المتسارع إلى إضعاف الحواجز الإقليمية التقليدية، وأصبح التفوق التقني يمنح بعض الدول أو الجهات قدرة كبيرة على الوصول إلى المعلومات الحساسة والتجسس الإلكتروني دون إذن، الأمر الذي فرض إعادة النظر في مفهوم السيادة بوصفها سلطة مطلقة، وتحولها تدريجياً إلى سيادة نسبية مقيدة بمتغيرات البيئة الرقمية. [(3)]

وقد أسهمت عدة عوامل في هذا التحول، من أبرزها:

([1]) فاطمة بيرم: السيادة الوطنية في الفضاء السيبراني والتحولات الرقمية , بحث منشور في مجلة جامعة قسنطينة, مجلد5, العدد1 , السنة5, 2019, ص798.

([2]) فاطمة بيرم: مصدر سابق ,ص 799.

([3]) د بشير سبهان احمد :- بحث منشور في مجلة تكريت للحقوق, السنة 5, المجلد 5 , العدد3, الجزء 2, 2021, ص109.

1- ظهور أنماط جديدة من التهديدات الدولية المرتبطة بالفضاء السيبراني، مثل القرصنة الإلكترونية والحروب السيبرانية، وهو ما استدعى تعاوناً دولياً مكثفاً لإيجاد حلول قانونية وتقنية فعّالة.

2- التطور الكبير في وسائل الاتصال وتكنولوجيا المعلومات، مما أدى إلى تدفق هائل للأخبار والبيانات والأفكار عبر الحدود، الأمر الذي حدّ من قدرة الدول على احتكار المجال الإعلامي أو التحكم الكامل بمقومات هويتها الرقمية..[1]

3- تراجع إمكانية الاعتماد الذاتي الكامل في مجال الصناعات المعلوماتية، حيث فرضت طبيعة التطور التقني على الدول توسيع شبكات تعاونها مع شركات التكنولوجيا العالمية والدخول في شراكات جديدة مع القطاع الخاص، وهو ما انعكس بدوره على الدور التقليدي للدولة، لاسيما في المجالين الأمني والعسكري.([2])

ومن خلال هذه التعاريف الخاصة بالسيادة السيبرانية يمكننا تحديد الاشخاص الذين يقومون باختراق هذه السيادة وهم ذاتهم من يرتكبون الجرائم المعلوماتية بكافة انواعها:-

1- **الهواة:-** وهم من يرتكبون جرائم انتهاك السيادة السيبرانية للدول بقصد التسلية فقط.
2- **القراصنة:-** وهم متطفلون على امن النظم المعلوماتية من خلال دخولهم انظمة الحاسبات الحكومية وكسر الحواجز الامنية لألحاق الضرر او بقصد السرقة.
3- **الجريمة المنظمة:-** وهو انتهاك السيادة السيبرانية للدول عن طريق عصابات المافيا.
4- **الحكومات الأجنبية:-** اذ تقوم الدول بانتهاك السيادة السيبرانية لدول اخرى عن طريق اجهزتها المخابراتية والجاسوسية.
5- **المتطرفون:-** وهم من يقومون باستخدام افضاء السيبراني لنشر افكارهم الدينية المتطرفة.([3])

**ثانيا: تميز السيادة التقليدية عن السيادة السيبرانية**

قبل الشروع في بيان أوجه الاختلاف بين السيادة التقليدية والسيادة السيبرانية، يقتضي الأمر ابتداءً تحديد المقصود بالسيادة في صورتها التقليدية. إذ يمكن النظر إلى السيادة بوصفها سلطة سياسية

([1]) خليل يوسف جندي:- المواجهة التشريعية للجريمة المعلوماتية على المستويين الدولي والوطني, بحث منشور في مجلة كلية القانون للعلوم القانونية والسياسية , مجلد 7 , العدد26, 2018, ص88.
([2]) فاطمة بيرم:- مصدر سابق ص798.
([3]) روان عطية الصحفي: الجرائم السيبرانية. بحث منشور في المجلة الالكترونية الشاملة ,العدد24, مجلد 6, 2020,ص15

عليا تنبع من كيان الدولة ذاته، وتمتلك القدرة على فرض إرادتها وتنظيم شؤونها دون خضوع لهيمنة داخلية أو خارجية. فهي تمثل قمة هرم السلطة داخل الدولة، بما يخولها حسم النزاعات التي تنشأ بين الأفراد أو الوحدات الداخلية، مع تمتعها بالاستقلال عن أي سلطة أخرى، سواء من الناحية المادية أم المعنوية).[1]

كما عُرفت السيادة بمعناها التقليدي بأنها :- سلطة الدولة العليا على رعاياها، واستقلالها عن أية سلطة أجنبية، وينتج عن هذا أن يكون للدولة كامل الحرية في تنظيم سلطاتها التشريعية والإدارية والقضائية وأيضا لها كل الحرية في تبادل العلاقات مع غيرها في العمل على أساس من المساواة الكاملة بينها"، وعليه فهو يزيد من قدسية تصرفات الدول ويجعلها غير قابلة للانتقاد او غير مشكك في صحتها بغض النظر عن النتائج سواء كانت بين افرادها او مع دول أخرى [2]

ويمكن للباحث ان يستخلص قاسم مشترك من هذا التعاريف للسيادة هو قدرة الدولة على التصرف في شؤونها الداخلية والخارجية بحرية تامة ان اي تأثير.

وبعد ان تعرفنا على مفهوم السيادة السيبرانية في الفرع الاول ومفهوم السيادة التقليدية في بداية هذا الفرع يمكننا تحديد النقاط التالية للتميز بين السيادة بنوعيها:-

1- **انتهاك السيادة السيبرانية** يتم عن طريق **( الجريمة الالكترونية الناعمة)**والتي لا تتطلب قدرات عنيفة لارتكابها كتبادل اطلاق النار او سفك دماء كذلك لا يوجد شعور لدى المجرم المعلوماتي الذي ينتهك السيادة السيبرانية بعدم اخلاقية ما يقوم به او بمساسه بمصالح أو قيم يحرص المجتمع على حمايتها ولا يعتبر ما يقوم به يدخل في عداد الجرائم , عكس **انتهاك السيادة التقليدية** والذي غالبا ما يتخذ شكل العنف المادي بالوسائل القتالية.[3]

2- **من حيث توجد الفاعل على مسرح الجريمة:-** في حالات انتهاك السيادة السيبرانية، لا يكون الفاعل حاضراً مادياً في موقع ارتكاب الفعل، بل تُنفَّذ الجريمة عن بُعد عبر الوسائط الرقمية، الأمر الذي يميّزها عن الجرائم التقليدية المرتبطة بمسرح جريمة محدد. فالجاني قد يوجد داخل إقليم دولة معينة، ومع ذلك يتمكن من الوصول إلى أنظمة معلوماتية أو اختراق ذاكرة حاسوب موجودة في دولة أخرى، مما يطرح إشكالات قانونية تتعلق بالاختصاص الإقليمي وإثبات الفعل الجرمي في البيئة السيبرانية. ويظهر ذلك

---

([1]) د. نسيب أرزقي، مستقبل السيادة والنظام العالمي الجديد، المجلة الجزائرية للحقوق والعلوم الإدارية والقانونية، 1998،ص 84

([2])د ايمن احمد الورداني , حق الشعب في استرداد السيادة , القاهرة, دار النهضة العربية, 2008, ص 37.

[3] حسين سعيد سيف , الجهود الدولية في مواجهة جرائم الانترنيت,دار الطباعة 2007,ص66.

اكثر في البرامج الخبيثة (Viruses) حيث يتم نسخها في بلد وترسل الى دول مختلفة من العالم, عكس انتهاك السيادة التقليدية والذي عادة ما تكون الصورة الرئيسية له هو حالة تواجد منتهكها على ارض الدولة. [1]

3- غياب الحدود الجغرافية للسيادة السيبرانية مقارنة بالسيادة التقليدية اذ تنتهي السيادة التقليدية للدولة بانتهاء حدودها المكانية .

4- تختلف السيادة السيبرانية عن السيادة التقليدية بصعوبة اثبات انتهاكها اذ ان انتهاك السيادة السيبرانية يتم بطرق الكترونية تعتمد على الانترنيت والنظم المعلوماتية, بعكس انتهاك السيادة التقليدية الذي يتم عادة بطرق مادية او عسكرية .

5- تعتمد السيادة السيبرانية على الذكاء الاصطناعي المرتفع عند اختراقها بالجرائم السيبرانية عكس السيادة لتقليدية والتي تنتهك بطرق مادية كما تعتمد على البرمجيات الحيثية والهندسة الاجتماعية واستغلال الثغرات .

6- تخترق السيادة الوطنية عادة بالعنف او التدخل في قرارات الدول بصورة غير قانونية بينما تخترق السيادة السيبرانية دون اللجوء الى العنف والخيار العسكري او كما يسمى عن طريق الجرائم الناعمة او الباردة. ([2])

وبذلك يمكن للباحث القول ان السيادة السيبرانية اصبحت محور اهتمام العالم والمجتمع الدولي كونها ذات اهمية كبيرة وخطورة بالغة على مستقبل الدول العالمية لاسيما الكبرى منها وهذا ما لاحظناه في الانتخابات الامريكية السابقة والمشاكل التي رافقتها والاتهامات الموجهة الى روسيا بالتدخل سيبرانيا في هذه الانتخابات , ما تطلب وضع حلول قانونية سليمة تؤمن للدول حفاظها على كيانها وسلامة بياناتها ومجالها الرقمي من الهجمات السيبرانية.

## الفرع الثاني

## دور الاتفاقيات والمعاهدات الدولية في حماية السيادة السيبرانية

### أولا : دليل تالين وأهميته في أعمال السيادة السيبرانية:

عقد حلف الشمال الأطلسي مجموعة مؤتمرات ومحادثات واجرت تغيرات في نظامه الأساسي لتطوير قدراته السيبرانية وصد الهجمات التي تستهدف أعضاءه، وأثراً على ذلك قام مركز الدفاع السيبراني التعاوني للتمييز التابع لحلف الشمال الأطلسي، بدعوة مجموعة من أبرز الخبراء

[1] خالد ممدوح ابراهيم: الجرائم المعلوماتية, دار الفكر الجامعي, 2009. ص88.

([2]) د منى الاشقر: السيبرانية هاجس العصر, المركز العربي للبحوث القانونية والقضائية, بدون سنة نشر, لبنان ص 70.

الأكاديميين وفقهاء القانون الدولي ومحامين عسكريين ومستشارين قانونيين لمنظمات غير حكومية، وكما ضم الحلف مراقبين ليس لهم حق التصويت في اللجنة الدولية للصليب الأحمر والقيادة الألكترونية الأمريكية وحلف الشمال الأطلس، وأهم ما تمخض عن تلك الإجراءات هو تقديم دليل تالين.[1]

يعدّ دليل تالين محاولة تفسيرية لبيان مدى انطباق قواعد القانون الدولي على الهجمات السيبرانية، إذ يتناول جملة من المبادئ القانونية ذات الصلة، وفي مقدمتها مبدأ مشروعية اللجوء إلى القوة، أي القواعد التي تنظّم استخدام الدول للقوة بوصفها وسيلة من وسائل سياستها الوطنية. كما يتطرق إلى قواعد سلوك الأعمال القتالية، المتمثلة بقانون النزاعات المسلحة أو القانون الدولي الإنساني، التي تُعنى بتنظيم تصرفات أطراف النزاع أثناء العمليات العدائية. ومع ذلك، فإن نطاق الدليل يظل محصوراً في معالجة العمليات السيبرانية المرتبطة بمواجهة هجمات سيبرانية معادية، دون التوسع إلى غيرها من المجالات الرقمية [2].

وقد أبدى جانب من الفقه تخوفه من هذا الدليل، ظناً منهم إن هذا الدليل قد يؤدي إلى ما يمكن أن يسمى عسكرة الفضاء السيبراني، أي وبعبارة أخرى قد يوجد عنه منافسة بين الدول لتسليح نفسها بوسائل الهجمات السيبرانية، وهذا مالم توثقه بعض الدراسات القانونية، التي اشارت إلى إن مثل تلك التنظيمات قد يخلق عنها شيء من انعدام الأمن والتوتر في المجتمع الدولي[3].

ونتيجة لهذه المخاوف قامت الأمم المتحدة في سنة ٢٠١٠ بتشكيل مجموعة من الخبراء الحكوميين من أجل دراسة الموقف، ونتج عن تلك الدراسة ثلاثة تقارير، تفيد بأن هناك قبولاً عاماً من قبل الدول لتنظيم هذه العمليات وقت السلم لهداف سلمية طبقاً للقانون الدولي و يرى جانب من الفقه، استناداً إلى ما أورده دليل تالين، أن وصف النزاع المسلح الدولي قد يتحقق إذا قامت دولة ما، تمارس سيطرة كاملة على جماعة من الأفراد، بتوجيه هذه الجماعة لتنفيذ هجمات سيبرانية ضد دولة أخرى. أما في الحالات التي تقتصر فيها علاقة الدولة بتلك الجماعة على مستوى السيطرة الفعّالة فقط، فإن الأفعال السيبرانية الصادرة عنها لا ترقى – من حيث التكييف القانوني – إلى مستوى النزاع المسلح الدولي.[4]

---

[1] نسيب أرزقي: مستقبل السيادة والنظام العالمي الجديد، المجلة الجزائرية للحقوق والعلوم الإدارية والقانونية، 1998،ص 84

[2] فاطمة بيرم: السيادة الوطنية في الفضاء السيبراني والتحولات الرقمية , بحث منشور في مجلة جامعة قسنطينة, مجلد5, العدد1 , السنة5, 2019, ص798.

[3] نسيب أرزقي: مصدر سابق ،ص 84

[4] د منى الاشقر: السيبرانية هاجس العصر, المركز العربي للبحوث القانونية والقضائية, بدون سنة نشر,ص 70.

ورغم الأهمية التي يتمتع بها دليل تالين بعده وثيقة مهمة في مجال تنظيم الهجمات السيبرانية، وخطوة مهمة في نطاق تنظيم الفضاء السيبراني ، إلا أنه لا يمكن عده صكاً دولياً ملزماً، فهو لا يمثل وجهة نظر منظمة حلف شمال الأطلس، ولا يمثل وجهة نظر الدول التي يحمل جنسيتها الخبراء الذين شاركوا في إعداد الدليل، وإنما يمثل فقط وجهة نظر الخبراء بصفتهم الشخصية [1].

من خلال ما تقدم نرى أنه هنالك دعوات لتضافر الجهود الدولية من أجل ضمان بقاء أنظمة المعلومات وشبكات الاتصالات على حالة من الاستقرار والموثوقية، وكذلك يتبين أنه هنالك استعداداً صارما للحد من نشوب نزاعات مسلحة في تنتهك السيادة السيبرانية، كون الحرب في المستقبل سوف تكون في المجال السيبراني نظراً في الزيادة الحاصلة في القدرات الهجومية السيبرانية، إذ كان لابد من السعي لتحقيق السلام السيبراني وإيلاء الاهتمام بذلك الجانب، إذ تسعى التحالفات الدولية وعلى مختلف مستوياتها الاستعداد لهذه الحرب، وذلك عن طريق تطوير القدرات القانونية والاستراتيجية، ومن خلال إنشاء المراكز والوكالات والمعاهد التدريبية، فضلاً عن صياغة القوانين والأنظمة التي تحمي السيادة السيبرانية.

**ثانيا: الاتفاقيات الاوربية:**

يُمثل "توجيه أمن الشبكات والمعلومات" (NIS Directive)، الذي أطلقه الاتحاد الأوروبي في أغسطس عام 2016، حجر الزاوية التشريعي الأول لحماية السيادة السيبرانية لدول الاتحاد. يفرض هذا التوجيه على مزودي الخدمات الحيوية وبنية المعلومات التحتية اعتماد معايير أمنية توازي حجم المخاطر المحتملة، مع التركيز على ضمان ديمومة العمل، وإدارة الثغرات، والالتزام بعمليات التدقيق والرقابة وفق المقاييس العالمية. [2].

في السادس من حزيران، أقرّ الاتحاد الأوروبي بصفة رسمية التوجيه التشريعي رقم (60/1148) الخاص بـ **أمن الشبكات والأنظمة المعلوماتية** .ويهدف هذا الإطار القانوني إلى توحيد معايير الحماية الرقمية وضمان أمن الفضاء السيبراني المشترك بين الدول الأعضاء. وبموجب هذا التوجيه، أصبحت الدول ملزمة بتبني سياسات وطنية شاملة للأمن السيبراني، وتأسيس هيئات

[1] شوان عمر خضر، الحماية الجزائية للمال المعلوماتي، أطروحة دكتوراه مقدمة إلى كلية العلوم الأنسانية والاجتماعية، جامعة كويه، ٢٠١٣، ص15

[2] د ايمن احمد الورداني , حق الشعب في استرداد السيادة , القاهرة, 2008, ص 37.

رقابية متخصصة، بالإضافة إلى تشكيل وحدات فنية للتدخل السريع والاستجابة للهجمات التي قد تمس السيادة الرقمية للدول.[1].

وشهد عام 2013 تحولاً جوهرياً في المقاربة الأوروبية للأمن الرقمي، حيث أطلق الاتحاد **استراتيجية شاملة للأمن السيبراني** ركزت على بناء فضاء إلكتروني موحد ومحصن ضد التهديدات والاضطرابات التقنية. استندت هذه الرؤية إلى ركائز استراتيجية تمثلت في:

1. الارتقاء بقدرات الدفاع الإلكتروني ضمن منظومة الأمن والدفاع المشترك.
2. تحفيز الابتكار في الموارد التكنولوجية والصناعات الأمنية المحلية.
3. صياغة سياسة دولية موحدة تعزز **السيادة السيبرانية للاتحاد** وتحمي قيمه الجوهرية.

ولتحويل هذه التوجهات إلى واقع ملموس، أقر المجلس الأوروبي في عام 2018 **السياسة الإطارية للدفاع السيبراني** خلال اجتماع وزراء الدفاع، حيث تم التأكيد على أن حماية الفضاء الرقمي والسيادة التكنولوجية تأتي في مقدمة الأولويات. كما سعت هذه السياسة إلى مد جسور التعاون مع القوى الدولية الفاعلة، ودعم البحث العلمي والتطوير التقني في هذا الميدان [2]

**ثالثا: الاتفاقية الامريكية المتعلقة بجرائم الحاسوب الآلي والأنترنت لعام 1999**

تم عقد هذه الاتفاقية في الفترة من (6–7 كانون الأول لعام ١٩٩٩) في جامعة استانفورد في كاليفورنيا في الولايات المتحدة الامريكية، شارك فيها العديد من الخبراء القانونيين والهيئات والمنظمات الدولية، وكان الهدف من هذه الاتفاقية هو تعزيز حماية أمن الحاسوب الآلي من الجرائم التي تنتهك السيادة السيبرانية ، وقد بين المؤتمر أن الحاجة تكمن أن الجرائم المتصلة بالحاسوب الآلي وتعد من الجرائم العالمية والتي تستوجب وجود اتفاقية متعددة الأطراف ووجود ردود فعل عالمية من اجل مكافحتها، ولقد تناول المؤتمر المخاطر الناتجة عن المعلوماتي والتهديدات الألكترونية فقد عجزة القدرات الفردية والثنائية عن مواجهتها [3].

وسعياً لتأطير المفاهيم القانونية لهذه الاتفاقية، خصصت المادة الأولى حيزاً تعريفياً شمل اثني عشر مصطلحاً جوهرياً، وفي مقدمتها 'الجريمة المعلوماتية' و'السيادة السيبرانية'. أما المادة

---

[1] حازم حسين أحمد الجمل، الحماية الجنائية للأمن السيبراني في ضور رؤية المملكة، كلية الملك فهد الأمنية -مركز الدراسات والبحوث، مجلد ٣٠,٢٠٢٠، ص٢٦٣

[2] حسين سعيد سيف , الجهود الدولية في مواجهة جرائم الانترنيت, 2007,ص66.

[3] د محمود أحمد عبابنة، جرائم الحاسوب وابعادها الدولية، ط1، دار الثقافة للنشر والتوزيع، الأردن، ٢٠٠٩، ص ١٣٨

الثانية، فقد ركزت على توحيد المعايير الإجرائية لمكافحة هذه الجرائم، مسترشدةً بالتوصيات الصادرة عن وكالات حماية البنية التحتية المعلوماتية. وفيما يخص التصنيف الجرمي، فقد حددت المادة الثالثة الأفعال المحظورة، والتي شملت النفاذ غير المشروع للأنظمة، والتلاعب بالبيانات عبر الحذف أو التعديل بقصد الإضرار بالمؤسسات، أو تزوير المعلومات لتضليل الأفراد وإلحاق الأذى بأصحاب الحقوق.[1]

واستكملت الاتفاقية إطارها الإجرائي في **المادة (6)** التي نظمت آليات المساعدة القانونية المتبادلة بين الدول الأطراف، لا سيما في شؤون التحقيقات والملاحقات القضائية. ولضمان عدم الإفلات من العقاب، أوجبت **المادة (7)** إدراج الجرائم السيبرانية المنصوص عليها ضمن قوائم الجرائم التي تستوجب تسليم المجرمين في التشريعات الوطنية. وفي سياق متصل، شددت **المادة (8)** على فاعلية المسار القضائي وضرورة تقديم المتورطين للسلطات المختصة دون إبطاء لضمان سير العدالة.

أما الجانب التعاوني المؤسسي، فقد استعرضته **المواد(12–9)** ، حيث رسمت خارطة طريق للتعاون القضائي والإداري في إقامة الدعاوى وتنفيذ الأحكام، مع وضع نظام أساسي لـ **'وكالة حماية البنية التحتية '**يشمل هيكليتها التنظيمية، ومواعيد اجتماعاتها، وآليات تمويلها.

ولم تغفل الاتفاقية الجانب الحقوقي؛ إذ أفردت **المادة (13)** نصاً صريحاً لحماية حقوق الإنسان وصون الخصوصية الرقمية. واختتمت الوثيقة بـ **المواد (22–14)** التي تناولت الأحكام الختامية والتنظيمية، ومنها:

1. الالتزام بتقديم تقارير سنوية لوكالة حماية البنية التحتية حول منجزات التنفيذ.
2. إجراءات التوقيع، الانضمام، التحفظ، والانسحاب، بالإضافة إلى آليات التعديل.
3. إقرار الحجية القانونية المتساوية للنصوص المحررة باللغات الثلاث (الإنجليزية، الفرنسية، والروسية)[2].

[1] خالد ممدوح ابراهيم: الجرائم المعلوماتية, دار الفكر الجامعي, 2009. ص88.

[2] محروسي نصار غايب، الجريمة المعلوماتية، مجلة التقني، هيئة التقني، مج ٢٤، 9، العراق، ٢٠١١، ص٢١.

وبذلك يلاحظ الباحث بأن هذه الاتفاقية تناولت الإجراءات التي تعزز من دور التعاون في سبيل مكافحة الجرائم والانتهاكات التي تجري في السيادة السيبرانية، والمحافظة على الحقوق وصيانة الحريات الشخصية، وتقديم الحماية اللازمة لمؤسسات الدولة والأشخاص من الأضرار التي تنتج عن الجرائم المعلوماتية، والأخذ بسبل التعاون بين الدول في المجالات القانونية والقضائية للحد من تلك الجرائم.

**رابعا: الاتفاقية العربية لمكافحة جرائم تكنولوجيا المعلومات لعام 2010:**

أدت جهود الجامعة العربية في مكافحة الجرائم الألكترونية إلى توقيع الاتفاقية العربية بمكافحة المعلومات لعام ٢٠١٠ والتي نظمت لغرض تدعيم وتعزيز التعاون العربي في هذا المجال بهدف مكافحة جرائم انتهاك السيادة السيبرانية، اذ تشتمل هذه المعاهدة على (43) مادة، والتي وافق عليها مجلس وزراء الداخلية والعدل العرب في مقر الأمانة العامة لجامعة الدول العربية، في القاهرة في الاجتماع التي تم انعقاده بتاريخ ٢١ كانون الأول من عام ٢٠١٠، ودخلت الاتفاقية حيز النفاذ في 7 شباط من عام ٢٠١٤ [1].

وقد ترجم مجلس الوزراء العرب التعاون على المستوى العربي في عدد من الاتفاقيات العربية والمقترحات المتعلقة بمكافحة الجرائم، في مجال انتهاك السيادة السيبرانية، فقد أصدر مجموعة من التوصيات تتعلق بهذا النوع من الجرائم في المؤتمر المنعقد في تونس عام ١٩٩٨، دعا فيه الدول الأعضاء إلى تشكيل لجان وطنية تتولى دراسة الأحكام الموضوعية والمتمثلة في تجريم الأفعال المكونة لجرائم تقنية المعلومات وهي، الاعتراض، والاختراق، والاعتداء على سلامة البيانات والملكية الفكرية، وإساءة استعمال وسائل تقنية المعلومات، والاحتيال والتزوير، والاستعمال غير مشروع لأدوات الائتمان والوثائق الإلكترونية، فضلاً. تشديد العقوبات على الجرائم التقنية التي ترتكب عن طريق تقنية المعلومات [2]

وكما حثت الدول الأعضاء إلى انشاء مركز أمني متخصص لمكافحة الجرائم الناجمة عن اساءة استخدام التكنولوجية، ومتابعة المستجدات التابعة لها(4). عن وتتكون هذه الاتفاقية من (43) مادة كما بينا، منها (٢١) مادة في باب التجريم، و(٨) مواد إجرائية تتعلق بحقوق السلطات وجمع المعلومات وتتبع المستخدمين، وضبط المواد المخزونة على الحواسيب الشخصية والأجهزة

[1] أياد خلف محمد المفرجي، المنازعات الدولية ذات الطابع الألكتروني، رسالة ماجستير، كلية القانون والعلوم السياسية، جامعة كركوك، ٢٠١٩، ص74.

[2] د. رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة في ضوء الاتفاقيات والمواثيق الدولية، ط١، دار النهضة العربية، القاهرة، ٢٠١١، ص 75.

التقنية، ويتكون الفصل الرابع من (14) مادة وهي أساس هذه الاتفاقية التي تنص على تنظيم التعاون بين الدول الأعضاء في تبادل المعلومات، ويكون نطاق سريان هذه الاتفاقية.[1]

## الفرع الثالث

## دور المنظمات الدولية والإقليمية في حماية السيادة السيبرانية

### اولا: دور الامم المتحدة:

تبنت المنظمة الدولية جملة من القرارات الأممية الرامية إلى معالجة الخروقات في الفضاء السيبراني، مواكبةً بذلك الطفرة النوعية في تقنيات المعلومات والاتصالات وانعكاساتها على منظومة الأمن القومي والدولي. وقد شددت هذه التوجهات الدولية على الخطورة الكامنة في احتمالية تسخير هذه الابتكارات التقنية في أنشطة وممارسات تقوض ركائز السلم والأمن الدوليين، أو توظيفها في غايات تتنافى مع المواثيق والأعراف المنظمة للاستقرار العالمي"وايضاً على "أن انتشار البيانات واستعمال التقنيات والأساليب المعلوماتية قد تؤثر على مصالح المجتمع الدولي"[2].

وفي سياق الجهود الأممية الرامية لتأطير العمل الدولي المشترك، برز قرار الجمعية العامة للأمم المتحدة رقم **(49/159)**الصادر في ديسمبر 1994 خلال دورتها التاسعة والأربعين، والذي اقترن بتبني **'إعلان نابولي السياسي وخطة العمل العالمية .'**وقد جسّد هذا القرار التزاماً جماعياً لمواجهة الأنماط المستحدثة للجريمة المنظمة عابرة الحدود، حيث تضمن دعوة صريحة لكافة الوحدات الدولية والمنظمات العالمية لتوفير الإسناد اللازم لبرنامج الأمم المتحدة المعني بمنع الجريمة والعدالة الجنائية، لضمان قدرته على إنفاذ استراتيجياته وتحقيق غاياته المؤسسية[3].

وفي إطار الاستجابة الأممية للمتغيرات التقنية المتسارعة، تبرز الأهمية القانونية لقرار الجمعية العامة رقم **(A/RES/70/53)**الصادر في نوفمبر 1998، والذي ركز بصفة محورية على تداعيات التقدم في منظومة المعلومات والاتصالات السلكية واللاسلكية على مقتضيات الأمن الدولي. وقد عكس هذا القرار هواجس المجتمع الدولي حيال إمكانية انحراف هذه الطفرة التكنولوجية نحو غايات تتقاطع مع استقرار الدول وتؤثر سلباً على أمنها السيادي. ومن هذا

---

[1] . عبد الكريم الردايدة،الجرائم المستحدثة واستراتيجية مواجهتها، ط1، دار ومكتبة حامد للنشر والتوزيع، عمان، (٣)٢٠١٣، ص٢٥٧.

[2] القرار رقم (٣٢/٥٨) في 8 كانون الأول ٢٠٠٣، الجمعية العامة للأمم المتحدة

[3] القرار رقم (١٥٩/٧٠) ٢٣ كانون الاول 1994، الجمعية العامة للأمم المتحدة

المنطلق، حث القرار الدول الأعضاء على تبني رؤية شاملة لتقييم التهديدات السيبرانية القائمة والمستقبلية، مع التأكيد على ضرورة بلورة مفاهيم موحدة لأمن المعلومات، لاسيما فيما يتعلق بالولوج غير المشروع للأنظمة المعلوماتية، والتصدي للتوظيف الإرهابي والإجرامي للفضاء الرقمي. [1].

وكذلك بينت في قراراتها على أهمية **السيادة السيبرانية**، ومن أهم تلك القرارات "إنشاء ثقافة عالمية للأمن السيبراني وحماية الهيكل الأساس للمعلومات الذي اعتمد من الجمعية العامة للأمم المتحدة"[2]،

وكذلك القرار المتعلق " بأنشاء ثقافة علمية أمنية للفضاء السيبراني"، والذي اعتمد من قبل الجمعية العامة"، إذ اعتمدت فيه قراراً بشأن السيادة السيبرانية والذي قررت فيه بوجوب تدعيم وتكثيف الحلول الوطنية في مجال والتعاون وتبادل المعلومات في هذا الإطار على المستوى الوطني والإقليمي والدولي، كي يتسنى مواجهة لهذه التهديدات السيبرانية، من طابعها العابر للحدود، كما أكدت في قرارها أن الأمن السيبراني والهيكلية الأساسي الحيوية مسؤولية ملقاة على عاتق الحكومات ومجال يجب عليها أن تحمل فيه لواء الصدارة وطنياً بالتنسيق مع أصحاب المصلحة في هذا الشأن.[3]

والقرار المتعلق "بأنشاء ثقافة عالمية بشأن الأمن السيبراني والاستفادة من الجهود الوطنية لحماية البنى التحتية الأساسية للمعلومات السيبرانية"[4]،

والقرارين " بمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية والذين اعتمدا من الجمعية العامة للأمم المتحدة"[5].

والقرار الذي يوضح "بدور العلم والتكنولوجيا في سياق الأمن الدولي ونزع السلاح"[6]

وفي إطار الجهود الاستشارية الدولية، شهد عام 1999 انعقاد اجتماع الخبراء في جنيف تحت مظلة الأمم المتحدة، مخصصاً لبحث التداعيات الأمنية المتولدة عن تكنولوجيا المعلومات, وبالقراءة التحليلية لقرارات الجمعية العامة اللاحقة، يُلاحظ نزوعها نحو تكثيف الدعوات لإجراء المزيد من الدراسات الأكاديمية حول 'الأمن السيبراني' والمعلوماتية الدولية، دون بلورة آليات

---

[1] القرار ذو رقم (53/49) 4 كانون الاول ١٩٩٨، الجمعية العامة للأمم المتحدة

[2] القرار ذو رقم (١٩٩/٥٨) 30 كانون الثاني ٢٠٠٤.، الجمعية العامة للأمم المتحدة

[3] القرار ذو رقم (٢٣٩/٥٧) في 31 كانون الاول ٢٠٠٣، الجمعية العامة للأمم المتحدة

[4] القرار ذو رقم (٢١١/٦٤) في ٣٠كانون الثاني ٢٠٠٤، الجمعية العامة للأمم المتحدة

[5] القرارين المرقمين (63/55) في كانون الثاني ٢٠٠١، و(١٢١/٥٦) في ٢٣ كانون الثاني٢٠٠٢، الجمعية العامة للأمم المتحدة.

[6] القرار ذو رقم (73/53) في 4 كانون الثاني ١٩٩٩.، الجمعية العامة للأمم المتحدة.

تنفيذية أو إجراءات زجرية رادعة. وقد تجلى هذا القصور الإجرائي بوضوح في مخرجات القمة العالمية لمجتمع المعلومات التي عُقدت على مرحلتين (جنيف 2003، وتونس 2005)؛ إذ لم تسفر تلك المداولات عن نتائج ملموسة ترقى لمستوى التحديات القائمة. وبالتوازي مع ذلك، انخرط المجلس الاقتصادي والاجتماعي في هذا المسار عبر حزمة قرارات استهدفت توظيف المنجز العلمي والتقني في خدمة غايات التنمية [1].

**وبذلك يرى الباحث مع كل ما تقدم أن الأمم المتحدة بالرغم من عدم تمكنها من الوصول إلى إبرام اتفاقيات دولية ملزمة بشأن الأمن السيبراني، إلا أنها بموجب تلك المقترحات والقرارات قد مهدت الطريق امام المجتمع في سبيل لا برام مثل هذه الاتفاقيات مستقبلا لمواجهة تلك التهديدات التي تطال الأمن السيبراني بكل أبعاده.**

**ثانيا: دور اللجنة الدولية للصليب الأحمر في مجال السيادة السيبرانية:**

تضطلع اللجنة الدولية للصليب الأحمر بمسؤولية محورية في الرقابة على إنفاذ قواعد القانون الدولي الإنساني، مع العمل الدؤوب على موائمة هذه القواعد مع المستجدات التقنية والأسلحة السيبرانية المبتكرة. وفي إطار سعيها لضمان نجاعة الأطر القانونية، أفرز المؤتمر الدولي الثامن والعشرون للصليب الأحمر والهلال الأحمر توصيات ملزمة للدول بضرورة إخضاع الأسلحة والوسائل الحربية المستحدثة لمراجعات دقيقة ومتعددة التخصصات؛ تلافياً لاتساع الفجوة بين الطفرة التكنولوجية ومقتضيات الحماية القانونية. وعليه، فإن العمليات السيبرانية الموظفة في النزاعات المسلحة، والتي تنتهك السيادة الرقمية للدول، تقع في صلب الاختصاص الموضوعي والمعياري الذي أقرته اللجنة الدولية للصليب الأحمر [2].

وهو ما يتلائم مع المادة السادسة والثلاثون من البرتوكول الإضافي الأول لعام ١٩٧٧ الملحق باتفاقيات جنيف الأربعة لعام 1949 التي جاء فيها "يلتزم أي طرف سام متعاقد، عند دراسة أو تطوير أو اقتناء سلاح جديد أو إداة للحرب أو اتباع أسلوب للحرب، بأن يتحقق مما إذا كان ذلك

---

[1] الأمم المتحدة، المجلس الاقتصادي والاجتماعي، القرارات ذات الأرقام (46) في ٢٠٠٦، و (A/63/3/Rev.1) في ٢٠٠٧، و (٢١٧، ٢١٨، ٢١٩، ٢٢٠)في ٢٠٠٨، (٧، ٨) في ٢٠٠٩

[2] عادل عبد الصادق، دور الامم المتحدة ودعم الاستخدام السلمي للفضاء الألكتروني، مقال منشور على الرابط الالكتروني http://accronline.com/article_detail.aspx?id=22762 آخر زيارة للرابط في 2022/10/17.

محظور في جميع الأحوال او في بعضها بمقتضى هذا الملحق أو أية قاعدة أخرى من القواعد القانون الدولي التي يلتزم بها هذا الطرف السامي المتعاقد [1].

وكما شاركت اللجنة الدولية للصليب الأحمر في مؤتمر الخبراء الدولي المنعقد في ستوكهولم للفترة من 17–19 تشرين الثاني ٢٠٠٤حول الهجمات السيبرانية التي تنتهك السيادة السيبرانية وإمكانية تطبيق القانون الدولي الإنسان.[2]

كما عقد المؤتمر ونتج عنه اتفاق جميع الأطراف المشاركة على أن القانون الدولي ينطبق على الهجمات السيبرانية التي تنتهك السيادة السيبرانية التي تستخدم في أثناء النزاعات المسلحة الدولية وغير دولية، وفي سنة ٢٠١١ قدمت اللجنة الدولية تقرير تناول فيه خصوصية الفضاء السيبراني كمجال محتمل للقتال الحربي تحت عنوان " القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة "، إذ أوجبت اللجنة على الالتزام بقواعد القانون الدولي بخصوص التقنيات الجديدة القائمة [3].

وكما عقدت اللجنة في الفترة ما بين 8–10 كانون الأول من سنة ٢٠١٥ المؤتمر الدولي الثاني والثلاثين للصليب الأحمر تحت عنوان " تقرير عن القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة، وقد تمحور المؤتمر عن أنّه " أي لجوء للقوة سواء كان سيبرانياً أو حركياً (مادياً) بحسب طبيعته يظل دائماً محكوماً بميثاق الأمم المتحدة وقانون اللجوء إلى الحرب، وأن القيود موجودة بمقتضى القانون الدولي إذا ما لجأت أو عندما تلجأ الدول أو الجماعات المسلحة إلى اعتداء سيبرانية في أثناء النزاع المسلح"[4].

و أوضحت اللجنة الدولية للصليب الأحمر أنّها "ترحب بقيام الخبراء بدراسة تبعات الحرب السيبرانية والقانون المنطبق عليها وأن اللجوء إلى العمليات في الفضاء السيبراني في أثناء النزاعات المسلحة يحتمل أن تكون له تبعات إنسانية وخيمة، وترى اللجنة أنه من الضروري تحديد سبل للحد من التكلفة الإنسانية للعمليات السيبرانية، لاسيما إعادة التأكيد على الصلة بين القانون الدولي وهذه التكنلوجيا الجديدة عند استخدامها في أثناء النزاعات المسلحة"[5].

---

[1] المصدر نفسه : ص 87.

[2] ينظر: اللجنة الدولية للصليب الأحمر، المؤتمر الدولي الثامن والعشرين للصليب الأحمر والهلال الأحمر المنعقد في 6-3 كانون الأول عام ٢٠٠٣.

[3] أسامة صبري محمد، الحرب الألكترونية ومبدأ التمييز في القانون الدولي الإنساني،، مجلة القانون للدراسات والبحوث القانونية، كلية القانون، جامعة ذي قار، ٢٠١٣، ص74.

[4] اللجنة الدولية للصليب الأحمر، تقرير عن القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة، المؤتمر الدولي الثاني والثلاثون للصليب الأحمر والهلال الأحمر المنظم في الفترة ما بين 8-10 كانون الأول عام ٢٠١٥.

[5] ينظر: الأمانة العامة لمنظمة الاستشارية الآسيوية - الأفريقية، القانون الدولي في الفضاء السيبراني، الهند، ٢٠١٨

**يتضح من ما تقدم أن دور اللجنة الدولية للصليب الأحمر في مجال الأمن السيبراني بمثابة دعوة لتظافر الجهود الدولية من أجل ضمان بقاء شبكات وأنظمة المعلومات على حالة من الاستقرار، فضلاً عن ذلك الاستعداد للحد من احتمالية نشوب نزاع مسلح في المجال السيبراني، بعدة الزيادة الحاصلة في القدرات الهائلة للهجمات السيبرانية، كان لابد من السعي في إطار تحقيق السلم والأمن الدوليين وإيلاء الاهتمام بشكل خاص بالجانب الحربي الواقعة ضمن الفضاء السيبراني التي تقوم بها الدول أو الأطراف الأخرى من غير الدول وللحد من هذه الظاهرة.**

## الخاتمة

بعد ان انتهينا من موضوع البحث توصلنا الى جملة من النتائج والتوصيات:

**النتائج:**

1- تبين لنا ان الفضاء السيبراني اصبح "المجال الخامس" للسيادة إلى جانب البر والبحر والجو والفضاء الخارجي واصبح للدولة الحق المطلق في تشريع القوانين الوطنية التي تنظم تدفق البيانات وحماية أمنها القومي الرقمي، شريطة عدم التعارض مع التزاماتها الدولية.

2- ان انتهاك السيادة السيبرانية بصورة متكررة في الآونة الاخيرة لفت نظر العالم الى ضرورة بذل الجهود الدولية وعقد الاتفاقيات الدولية لحماية السيادة السيبرانية.

3- تلعب المنظمات الدولية والاقليمية دورا كبيرا في مجال حماية السيادة السيبرانية بالنظر لما تمتلكه من صلاحيات تنازلت عنها الدول الموقعة على مواثيق انشائها ولعل دور منظمة الامم المتحدة يعد الابرز بينها.

4. برزت الكثير من الجهود الدولية ذات الصلة بحماية السيادة السيبرانية والتي اتفقت في مضمونها ان حماية السيادة السيبرانية من اهم أدوات الاستقرار على المستوى الدولي.

**التوصيات:**

1- نوصي بضرورة عقد الاتفاقيات الدولية المتعلقة بحماية السيادة السيبرانية بين الدول لحماية الامن السيبراني للدول والعالم جميعا من الهجمات السيبرانية.

2- نوصي بتفعيل دور مجلس الامن كجهاز تنفيذي عالمي في مجال انتهاك السيادة السيبرانية واعتبار هذه الانتهاكات بمثابة تهديد للسلم الدولي.

3- بما أن الفضاء السيبراني عابر للحدود، لا تكفي القوانين المحلية وحدها؛ لذا نوصي بتفعيل التعاون القضائي الدولي لتسهيل تسليم المجرمين السيبرانيين وتبادل الأدلة الرقمية.

4. ضرورة حث الدول في اجتماعات المنظمات الدولية كافة على حماية سيادة الدول السيبرانية وتأشير أي خرق من قبلها واتخاذ إجراءات ضد أي دولة لا تحافظ على الحدود السيبرانية لدول العالم.

5.ضرورة تحديد قواعد الاشتباك الرقمي ووضع أطر قانونية واضحة تحدد متى يُعتبر الهجوم السيبراني "عملاً عدائياً" يبيح للدولة حق الدفاع الشرعي عن النفس وفقاً للمادة (51) من ميثاق الأمم المتحدة.

## قائمة المصادر


**الكتب القانونية:**

1- د منى الاشقر: السيبرانية هاجس العصر, المركز العربي للبحوث القانونية والقضائية, بدون سنة نشر.

2- د ايمن احمد الورداني , حق الشعب في استرداد السيادة , القاهرة, 2008.

3- د محمود أحمد عبابنة، جرائم الحاسوب وابعادها الدولية، ط1، دار الثقافة للنشر والتوزيع، الأردن، ٢٠٠٩.

4- خالد ممدوح ابراهيم: الجرائم المعلوماتية, دار الفكر الجامعي, 2009.

**5**- د. رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة في ضوء الاتفاقيات والمواثيق الدولية، ط، دار النهضة العربية، القاهرة، ٢٠١١.

**6**- عبد الكريم الردايدة،الجرائم المستحدثة واستراتيجية مواجهتها، ط1، دار ومكتبة حامد للنشر والتوزيع، عمان، ٢٠١٣.

**7**- حسين سعيد سيف , الجهود الدولية في مواجهة جرائم الانترنيت, 2007,

**الرسائل والاطاريح:**

**1**- شوان عمر خضر، الحماية الجزائية للمال المعلوماتي، أطروحة دكتوراه مقدمة إلى كلية العلوم الأنسانية والاجتماعية، جامعة كويه، ٢٠١٣.

2- أياد خلف محمد المفرجي، المنازعات الدولية ذات الطابع الألكتروني، رسالة ماجستير، كلية القانون والعلوم السياسية، جامعة كركوك، ٢٠١٩.

**البحوث المنشورة:**

**1**- نسيب أرزقي: مستقبل السيادة والنظام العالمي الجديد، المجلة الجزائرية للحقوق والعلوم الإدارية والقانونية، 1998

**2**- محروسي نصار غايب، الجريمة المعلوماتية، مجلة التقني، هيئة التقني، مج ٢٤، 9، العراق، ٢٠١١،

3- أسامة صبري محمد، الحرب الألكترونية ومبدأ التمييز في القانون الدولي الإنساني،، مجلة القانون للدراسات والبحوث القانونية، كلية القانون، جامعة ذي قار، ٢٠١٣.

**4**- فاطمة بيرم: السيادة الوطنية في الفضاء السيبراني والتحولات الرقمية , بحث منشور في مجلة جامعة قسنطينة, مجلد5, العدد1 , السنة5, 2019.

**5**- حازم حسين أحمد الجمل، الحماية الجنائية للأمن السيبراني في ضور رؤية المملكة، كلية الملك فهد الأمنية –مركز الدراسات والبحوث، مجلد ٣٠ .٢٠٢0,

**القرارات:**

**1**- القرار رقم (١٥٩/٧٠) ٢٣ كانون الاول 1994، الجمعية العامة للأمم المتحدة.

2- القرار ذو رقم (53/49) 4 كانون الاول ١٩٩٨، الجمعية العامة للأمم المتحدة

3- القرار ذو رقم (73/53) في 4 كانون الثاني ١٩٩٩.، الجمعية العامة للأمم المتحدة.

4- القرارين المرقمين (63/55) في كانون الثاني ٢٠٠١، و(١٢١/٥٦) في ٢٣ كانون الثاني٢٠٠٢، الجمعية العامة. للأمم المتحدة

**5**- القرار ذو رقم (٢٣٩/٥٧) في 31 كانون الاول ٢٠٠٣، الجمعية العامة للأمم المتحدة.

**6**- القرار رقم (٣٢/٥٨) في 8 كانون الأول ٢٠٠٣، الجمعية العامة للأمم المتحدة.

7- القرار ذو رقم (١٩٩/٥٨) 30 كانون الثاني ٢٠٠٤.، الجمعية العامة للأمم المتحدة

**8**- الأمم المتحدة، المجلس الاقتصادي والاجتماعي، القرارات ذات الأرقام (46) في ٢٠٠٦، و (A/63/3/Rev.1) في ٢٠٠٧، و (٢١٧، ٢١٨، ٢١٩، ٢٢٠)في ٢٠٠٨، (٧، ٨) في ٢٠٠٩.

**المقالات المنشورة:**

1- عادل عبد الصادق، دور الامم المتحدة ودعم الاستخدام السلمي للفضاء الألكتروني، مقال منشور على الرابط الالكتروني

http://accronline.com/article_detail.aspx?id=22762 آخر زيارة للرابط في .2025/10/17

**List of Sources**

**Legal Books:**

-1Dr. Mona Al-Ashqar: Cybersecurity: The Obsession of Our Time, Arab Center for Legal and Judicial Research, no publication date.

-2Dr. Ayman Ahmed Al-Wardani, The People's Right to Regain Sovereignty, Cairo, .2008

-3Dr. Mahmoud Ahmed Ababneh, Computer Crimes and Their International Dimensions, 1st ed., Dar Al-Thaqafa for Publishing and Distribution, Jordan, .2009

-4Khaled Mamdouh Ibrahim: Information Crimes, Dar Al-Fikr Al-Jami'i, .2009

-5Dr. Rami Metwally Al-Qadi, Combating Information Crimes in Comparative Legislation in Light of International Agreements and Conventions, 1st ed., Dar Al-Nahda Al-Arabiya, Cairo, .2011

-6Abdul Karim Al-Radaideh, Emerging Crimes and Strategies for Confronting Them, 1st ed., Dar and Library of Hamed for Publishing and Distribution, Amman, 2013. 7- Hussein Saeed Saif, International Efforts to Combat Cybercrime, .2007

**Theses and Dissertations:**

-1Shwan Omar Khader, Criminal Protection of Digital Assets, PhD dissertation submitted to the College of Humanities and Social Sciences, University of Koya, .2013

-2Ayad Khalaf Mohammed Al-Mufarji, International Disputes of an Electronic Nature, Master's Thesis, College of Law and Political Science, University of Kirkuk, .2019

**Published Research:**

-1Nassib Arzki: The Future of Sovereignty and the New World Order, Algerian Journal of Law, Administrative and Legal Sciences, 1998

-2Mahroussi Nassar Ghaib, Cybercrime, Al-Taqni Journal, Al-Taqni Authority, Vol. 24, No. 9, Iraq, 2011

-3Osama Sabri Muhammad, Electronic Warfare and the Principle of Distinction in International Humanitarian Law, Journal of Law for Legal Studies and Research, College of Law, University of Dhi Qar, 2013. 4-Fatima Bayram: National Sovereignty in Cyberspace and Digital Transformations, research published in the University of Constantine Journal, Volume 5, Issue 1, Year 5, .2019

-5Hazem Hussein Ahmed Al-Jamal, Criminal Protection of Cybersecurity in Light of the Kingdom's Vision, King Fahd Security College - Center for Studies and Research, Volume 30, .2020

**Resolutions:**

-1Resolution No. (159/70) of December 23, 1994, United Nations General Assembly.

-2Resolution No. (53/49) of December 4, 1998, United Nations General Assembly.

-3Resolution No. (73/53) of January 4, 1999, United Nations General Assembly.

-4Resolutions No. (63/55) of January 2001and (121/56) of January 23, 2002, General Assembly. United Nations

.5Resolution 239/57of 31December 2003, United Nations General Assembly.

.6Resolution 32/58of 8December 2003, United Nations General Assembly.

.7Resolution 199/58of 30January 2004, United Nations General Assembly.

.8United Nations Economic and Social Council, Resolutions 46of 2006, A/3/63/Rev. 1of 2007, 217, 218, 219, and 220of 2008, and 7and 8of .2009

**Published Articles:**

-1Adel Abdel Sadek, The Role of the United Nations and Supporting the Peaceful Use of Cyberspace, an article published at the following link: http://accronline.com/article_detail.aspx?id=22762, last accessed on /17/10/2025