كلية الحقوق

دور منظمة الأمم المتحدة

في تحقيق الأمن السيبراني

الدكتور

مصطفى نجاح مراد

مدرس القانون الدولي العام بكلية القانون جامعة الكنوز -البصرة -العراق

محاضر بأكاديمية الشرطة المصرية بقسم القانون الدولي العام والقانون الجنائي سابقاً

محاضر بكلية الحقوق جامعة مدينة السادات بقسمي القانون الدولي العام والقانون الجنائي سابقاً

مدرس بالمعهد العالي للهندسة وتكنولوجيا المعلومات بالمنوفية سابقاً

محاضر بمعهد المحاماة بالمنوفية سابقاً

mostfanagahmourad@gmail.com

دور منظمة الأمم المتحدة في تحقيق الأمن السيبراني

الملخص

إن الإعتماد على الفضاء السيبراني يزداد بوتيرة متسارعة فإنه في المقابل زادت حدة الأنشطة السيبرانية الغير مشروعة والتهديدات السيبرانية وكذلك إستهداف البنى الأساسية للدول وهو عالم متسع رحب وبلا قانون حاكم ومسيطر على النشاط في الفضاء السيبراني، ومع تزايد قوة ونفوذ الدول في الفضاء السيبراني بات واضحاً أن يكون هناك قواعد واضحة لتنظيم هذا الأمر عبر قواعد قانونية تلتزم بها كافة الدول وما إتفقت عليه جميع الدول على أن القانون الدولي القائم (المبادئ التقليدية القديمة) يمكن أن يمتد تطبيقه على الفضاء السيبراني وفقاً لما إستقر عليه القضاء الدولي كما هو الأمر حينما تم التأييد الكامل من المجتمع الدولي للمعايير الحديثة التي أقرتها لجان الخبراء التابعة للأمم المتحدة في شأن السلوك المسؤول للدولة في الفضاء السيبراني ٢٠١٥ والتي أقرتها معظم الدول في ٢٠٢١ وكذلك إتفاقية الأمم التحدة لمكافحة الجريمة السيبرانية ٢٠٢٤ والمبادئ الحديثة التى أرستها لتعزيز الأمن السيبراني، ولا يمكن بأي حال من الأحوال أن نغفل عن قصد أو عن جهل الدور الذي قامت به وما زالت تقوم به منظمة الأمم المتحدة في مناهضة هذه التهديدات سواء عبر أجهزتها الدائمة أو الوكالات المتخصصة التابعة لها.

Summary

As reliance on cyberspace increases at an accelerating pace, so does the intensity of illegal cyber activities, cyber threats, and the targeting of state infrastructure. This is a vast world without a governing law that controls activity in cyberspace. With the increasing power and influence of states in cyberspace, it has become clear that there must be clear rules to regulate this matter through legal rules that all states adhere to. All states have agreed that existing international law (old traditional principles) can extend its application to cyberspace in accordance with established international jurisprudence. This is the case with the full support of the international community for the modern standards adopted by the United Nations Committee of Experts on Responsible State Conduct in Cyberspace (2015), which were adopted by most states in 2021, as well as the United Nations Convention against Cybercrime (2024) and the modern principles it established to enhance cybersecurity. Under no circumstances can we intentionally or ignorantly ignore the role that the United Nations has played and continues to play in combating these threats, whether through its permanent bodies or its specialized agencies.

المقدمة

إن التطور الإنساني قبل العصور والأزمنة المتعاقبة كان مصحوباً ومقترناً بتطور موازي في كافة مناحي الحياة سواء في النواحي السياسية أو الإقتصادية أو الإجتماعية أو القانونية أو العسكرية وتلك إذاً سنة الحياه من تطور وتغير دائم ومستمر ومتواصل.

ولا تخلو الطبيعة الإنسانية منذ الأزل من نزاعات وحروب وصراعات والتي سوف تظل إلى الأبد سواءاً كانت أسباب هذه الصراعات أسباباً دينية أو توسعية أو أيدولوجية أو عرقية أو تاريخية كانت سمة مميزة لعصور قد خلفت وقد صاحب ذلك تطور هائل في نمط وإسلوب الحروب من بدائية بسيطة إلى حروب أكثر تطوراً وسرعة وفتكاً من أجل فرض الهيمنة لتحقيق مآرب يعلمها صانعها ثم كانت الطفرة في سبل وأساليب الصراعات والحروب من أسلحة دمار شامل وأسلحة كيميائية وبيولوجية ونووية قد تخلف خسائر وكوارث ممتدة وشاملة وغير محدودة يستحيل تفاديها بأي حال من الأحوال مما يهدد الأمن والسلم الدوليين بشكل متزايد ومضطرد.

ثم كانت الطفرة الكبرى في العقدين الأخيرين من القرن الواحد والعشرين من إبتكار تكنولوجيا المعلومات والإتصالات عبر الفضاء وهي التكنولوجيا العابرة للحدود دون قيود بل والقارات والدول على إختلاف مشاربها والتي لا تعرف للحدود مكاناً ولا للتواجد والإنتشار زماناً.

وأصبحت تكنولوجيا المعلومات والإتصالات تلك أمراً واقعاً لا يمكن إنكاره بل لا يمكن الإستغناء عنه لدوره في كافة المناحي من تبادل المعلومات والبيانات من وسائل تواصل إجتماعي على إختلاف مشاربها بحيث يظل نفعها أكثر من إثمها، ولما كان الهدف من إبتكار تلك الآلية الجديدة هو خدمة البشرية في كافة الأنشطة السياسية والإقتصادية والتجارية والمعلوماتية والإجتماعية والتعليمية والعسكرية...إلخ

فإنها أضحت سلاحاً ذو حدين فيمكن الأخذ بالجانب الإيجابي والنافع للإنسانية ويمكن على النقيض تبني الجانب السلبي الضار من عمليات ممنهجة من إختراق وقرصنة وسيطرة على معلومات مملوكة للغير وهي دروب جديدة من الحروب عبر الفضاء لا تقل من حيث السيطرة والخسائر ما يفوق الحروب التقليدية وإن كنا نعده عداً أنها من أقصى ما يمكن أن يصل إليه يد الإنسانية من تطور في الحروب مخلفة الدمار والهلاك في الحرث والنسل.

ولما كان الفضاء اللانهائي (الفضاء السيبراني) هو الأرض الخصبة لذلك النوع من الحروب فهو يخرج بشكل كلي عن السيطرة وإحكام الرقابة من أي دولة أو حتى عدة دول مجتمعة لأنه غير محدود وغير ثابت وعابر للحدود والقارات ومجهول المصدر.

وصارت مجهودات الدول منفردة أو مجتمعة من إتفاقيات لمناهضة السلوك الإجرامي في الفضاء السيبراني أو حتى حدود أو حتى صدور تشريعات داخلية بها من أجل نفس الغرض غير مجدية بما هو مطلوب فهو أثير غير ملموس ولا مرئي.

من هنا أضحت الحاجة الملحة لقضاء جهود المنظمات الدولية والإقليمية من أجل تعزيز سبل الهيمنة والسيطرة على الممارسات غير الشرعية عبر الفضاء السيبراني أمراً يشار إليه بالبنأن وفي مقدمة ذلك كأنت الأمم المتحدة عبر أجهزتها من خلال صدور توصيات أو تشريعات دولية تصب لنفس الغاية.

أهداف الدراسة:- تهدف هذه الدراسة إلى

بيان الدور الفعال للأمم المتحدة وجهودها في تعزيز الأمن السيبراني ومجابهة السلوك السيبراني الغير مشروع في الفضاء السيبراني.

تقنين إستخدام الدول والمؤسسات والأفراد لتكنولوجيا المعلومات والإتصالات في الفضاء السيبراني الوصول لقواعد قانونية دولية ملزمة تحكم إستخدمات الفضاء السيبراني.

التعرف على الصعوبات والتحديات التى تواجه منظمة الأمم المتحدة في تطبيق مبادئ وقواعد القانون الدولي في الفضاء السيبراني.

إشكالية الدراسة: وتطرح هذه الدراسة إشكالية تتمحور حول:

- ما هو دور منظمة الأمم المتحدة في تحقيق الأمن السيبراني وتطبيق قواعد القانون الدولي على الفضاء السيبراني.

وتتضح الإجابة على الإشكالية الرئيسية في هذه الدراسة من خلال سبر غوار البحث والتدقيق والتمحيص في الإجابة على هذه الأسئلة:-

- ما مدى إلزام الدول بالقرارات والمعايير والمبادئ الحديثة الصادرة عن منظمةالأمم المتحدة في الفضاء السيبراني
- وما هو الدور الواجب على الدول الكبرى في وضع سياسات تحكم الفضاء السيبراني
- ما مدى تطبيق مبادئ القانون الدولي التقليدية في الفضاء السيبراني

- ماهى المبادئ الحديثة التى أرستها منظمة الأمم المتحدة في الفضاء السيبراني

منهج الدراسة:

سوف نتبع أكثر من منهج في هذه الدراسة، ومن ثم سوف نستخدم المنهج التاريخي في دراسة مراحل تطور دور الأمم المتحدة في وضع قواعد دولية تحكم إستخدامات الفضاء السيبراني، وكذلك المنهج التحليلي بإستعراض نصوص الإتفاقيات والنصوص الدولية المرتبطة بالدراسة وتحليلها،وكذلك المنهج الإستنباطي بقراءة الدراسات السابقة والأبحاث المتعلقة بهذا الموضوع وإستنباط الحلول والأفكار .

خطة الدراسة:

الفصل التمهيدي: الأمم المتحدة والأمن السيبراني

الفصل الأول: جهود منظمة الأمم المتحدة وأجهزتها في تحقيق الأمن السيبراني

المبحث الأول: جهود الأجهزة الدائمة للأمم المتحدة في تحقيق الأمن السيبراني

المبحث الثاني: جهود الوكالات المتخصصة في تحقيق الأمن السيبراني

الفصل الثاني: دور منظمة الأمم المتحدة في إرساء مبادئ وقواعد القانون الدولي لتعزيز الأمن السيبراني

المبحث الأول: المبادئ التقليدية المطبقة لتعزيز الأمن السيبراني

المبحث الثاني: المبادئ الحديثة التى أرستها منظمة الأمم المتحدة لتعزيز الأمن السيبراني

الفصل التمهيدي
الأمم المتحدة والأمن السيبراني

تمهيد وتقسيم:

سبق التنويه أن موضوع تكنولوجيا المعلومات والإتصالات أصبح واقعاً ملموساً ومن الجدير بالذكر أن هو نتيجة للتطور الإنساني في شتى المجالات ولا يخفى على الفطنة الجوأنب الطيبة والأيجابية لها من تيسير تبادل المعلومات والبيأنات وتيسيرعمل قاعدة بيأنات للمرافق العامة للدول لضمأن حسن سير وأنتظام عملها إلا أن الجوأنب السلبية والخبيثة لها هي أمر واقع يجب مواجهته على الصعيد الدولي والعالمي سواء من الأفراد أو المؤسسات أو الدول أو حتى عبر الإتفاقيات الدولية سواء تمت بشكل ثنائي أو جماعي وسواء كأن للمنظمات الإقليمية والدولية دور في وضع بروتوكولات حاكمة لعمل تكنولوجيا المعلومات والإتصالات.

فقد ينطوي الأمر على سلوك جائز وقد يدخل في التجريم لاسيما أنه من قبيل الجرائم العابرة للحدود فهي تقنيات يصعب السيطرة عليها أو تتبعها في الغالب الأعم من الحالات وإن لم يكن جميعها.

المبحث الأول

مفهوم الأمن السيبراني وتطوره

ليس من السهولة بمكان تناول تعريف واضح ومحدد وجامع ومانع للقواعد للأمن السيبراني سواء من الناحية القانونية أو من ناحية فقهاء القانون الدولي لذلك فهو عبارة عن عدة تعريفات في مجملها يمكن بيانها وتوضيح جوهر وطبيعة الأمن السيبراني على أنه يمكن القول بأنه مجموعة القواعد والمبادئ التي من شأنها تنظيم سلوك الدول والأفراد والمؤسسات عبر الفضاء السيبراني.

وفي تعريف آخر لوزارة الدفاع الأمريكية بأنه عبارة عن جميع الإجراءات التنظيمية اللازمة لضمان حمأية المعلومات بجميع أشكالها المادية والإلكترونية من مختلف الهجمات للتخريب أو التجسس أو الحوادث[١]

وهناك تعريف آخر تناوله الإعلان الأوروبي بأنه قدرة النظام المعلوماتية على مقاومه محاولات الإختراق أو الحوادث غير المتوقعة التي تستهدف البيانات[٢]

كما عرفه الاستاذ ريتشارد كمرر استاذ الإتصالات بجامعة كاليفورنيا بأنه عبارة عن مجموعة وسائل دفاعية من شأنها كشف وإحباط المحاولات التي تقوم بها القراصنة وهو تعريف أيده الاستاذ ادوارد امورزو، وكذلك ذهب اتجاه في الفقه الدولي بأنه النشاط الذي يؤمن حمأية الموارد البشريه والمإليه المرتبطه بتقنيات الإتصالات والمعلومات ويضمن الحد من الخسائر والاضرار التي تترتب في حال تحقيق المخاطر والتهديدات لما يتيح اعاده الوضع إلى ما كأن عليه باسرع وقت ممكن بحيث لا تتوقف عجله الأنتاج وبحيث لا تتحول الاضرار إلى خسائر دائمة[٣]

وكذلك عرفه الإتحاد الدولي للإتصالات السلكية واللاسلكية فقد تناولهم في تقريره الصادر حول إتجاهات الإصلاح في الإتصالات لعام ٢٠١٠ و ٢٠١١ بأنه مجموعة من المهمات مثل

---

[١]غترة بن مرزوق، محي الدين حرشاوي، الأمن السيبراني كبعد حديث للسياسة الدفاعية الجزائرية، الملتقى الدولي حول سياسات الدفاع الوطني،٢٠١٧، جامعة قاصدي، مرباح ورقله،ص٥٦

[٢]عجال بوزادية، إستراتيجية الجزائر في مواجهة الجرائم اليبرانية، التحديات والآفاق المستقبلية، مجلة العلوم القانونية والسياسية، ع ١١، الجزائر

[٣] مشار إليه في سمير بارة، الأمن السيبراني في الجزائر، السياسات والمؤسسات، المجلة الجزائرية للأمن السيبراني، ع١٤، ص٢٥٧

تجميع وسائل وسياسات وإجراءات أمنية ومبادئ توجيهيه ومقاربات لإدارة المخاطر وتدريبات وممارسات وتقنيات يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين[1].

ومن وجهة نظرنا نرى أن الأمن السيبراني هو مجموعة المبادئ والقوانين الدولية والمحلية الحاكمة لكافة ممارسات وأعمال الأفراد والمؤسسات غير القانونية أو الشرعية لتحقيق مكاسب أو لإحداث الأضرار أياً كان نوع المكاسب أو الأضرار والتي من شأنها الحفاظ على هوية وبيانات المستخدمين عبر الفضاء من وسائل تكنولوجيا المعلومات والإتصالات بكافة صورها وأشكالها.

وقد رأينا في هذا التعريف عدة أمور نود الإشارة إليها

١- أن المحدد للتجاوزات في مجال الأمن السيبراني قد يكون عدة مصادر قانونية نتناولها سواء كان قانون دولي أو وطني لأي دولة وكذلك المبادئ المستقرة في وجدان البشرية والتي إستقرت عليها النفوس السوية.

٢- تعدد أشكال وأنماط المعتدين ويشمل ذلك الدول أو المؤسسات سواء كانت مؤسسات عامة أو خاصة وكذلك الأفراد منفردين أو مجتمعين.

٣- ينبغي أن تكون الممارسات الخاطئة في مجال الأمن السيبراني غير قانونية وهو أمر واضح ومحقق ومتفق عليه وكذلك تضم الممارسات غير الشرعية لأن ليس كل ما هو قانوني هو شرعي والعكس بالعكس فمثلاً تجارة وتداول النقد الأجنبي من الأفراد قد يكون غير قانونيا في تشريع دولة معينة بالرغم من مشروعيته في الأساس.

٤- ينبغي أن تكون الممارسات الخاطئة والمؤثمة في مجال الأمن السيبراني عن عمد لتحقيق كسب أو الإصابة للغير بخسارة محققة أو كليهما تحقيق نفع للمعتدي عليه وعلى ذلك ينبغي وجود الإرادة الحرة المتعمدة لذلك فأن تم عن جهل بمبادئ وقواعد وعمل المجال السيبراني دخول أو ممارسة خاطئة فإن السلوك في تلك الحالة لا يمكن أن يوصم بالسلوك الآثم.

٥- ينبغي أن يكون مجال الإعتداء هو الفضاء السيبراني وعلى ذلك يخرج الإعتداء المادي أو المعنوي من نطاق التقسيم المقصود مثل الإعتداء المسلح أو السطو أو السرقة المادية التعريف الإجرائي والشكلي للأمن السيبراني.

---

[1] منى الأشقرجبور، الأمن السيبراني، التحديات ومستلزمات المواجهة، المركز العربي للبحوث القانونية والقضائية، بيروت،٢٠١٧، وكذلك إدريس عطية، الأمن السيبراني في منظومة الأمن السيبراني الجزائري،مجلة مصداقية، المدرسة العليا العليا العسكرية للإعلام ولإتصال، المجلد الأول، العدد الأول،ديسمبر ٢٠١٩،ص٤و٥

يمكن القول أن الأمن السيبراني من الناحية الإجرائية هو مجموعة الضوابط والسياسات والآليات التي يمكن أن تتخذها لهيئات سواء كانت دولاً أو حكومات أو مؤسسات أو منظمات في مجال حمأية مواردها البشرية أو المادية من كل أشكال التهديد التي يمكن أن تمس شبكات الإتصالات والحواسيب بأعمال القرصنة أو الإختراق المختلفة للنظم التكنولوجية الحديثة التي يمكن أن تؤثر عليها سواء بالإتلاف أو المحو التام أو السطو عليه[١].

يمكن القول أن التعريف الإجرائي هو بالمقام الأول يهدف إلى النواحي التقنية والفنية التي يمكن إتخاذها في هذا الشأن والتي من شأنها السيطرة والحماية من مخاطر السلوك غير المشروع في مجال الأمن السيبراني أو الفضائي وفي هذا الخصوص يمكن القول أنها عبارة عن حزمة من الضوابط والساسيات والآليات والفنيات التي يمكن إتخاذها من الكائنات المعنية أو الهيئات ذات الصلة سواء كانت مؤسسات أو منظمات حكومية أو أهلية أو حكومات الدول بهدف حمأية مقدراتها ومواردها سواء المادية أو البشرية من كافة التعديات سواء من عمليات الإختراق أو القرصنة أو السطو على نظم التكنولوجيات الحديثة والتي من شأنها أن تتعرض للتلف الجزئي أو التلف الكلي أو الكامل أو التشويش[٢].

---

[١] رغدة البهي، الردع السيبراني، المفهوم والإشكاليات والمتطلبات، مجلة العلوم السياسية والقانون، المركز الديقراطي العربي، العدد الأول،٢٠١٧

[٢] د. دحان حزام القريطي، الأمن السيبراني وحماية البيانات، دار الفكر الشرطي، الإسكندرية،٢٠٢٤، ص١٩:١٨

المبحث الثاني
منظمة الأمم المتحدة والتطور التاريخي
في علاقتها بالفضاء السيبراني

نشأت منظمة الأمم المتحدة بإعتبارها منظمة حكومية عالمية وليست إقليمية بعد أن وضعت الحرب العالمية الثانية أوزارها من أجل نشر مبادئ السلام وتسوية النزاعات الدولية بمنأى عن الصراع المسلح ونشر وتحقيق الأمن والسلم الدوليين وهو من أهم مبادئها وأدوارها المنوطة بها وإتسمت تلك المهمة – ولم تكن موجودة في عصبة الأمم السابقة على الأمم المتحدة بالإهتمام الدولي والعالمي وذلك عام ١٩٤٥ تاريخ إنشاء هذه المنظمة في الولأيات المتحدة الأمريكية وتحديداً مدينة نيويورك ومع بدأية ١٩٩٨ كأن للأمم المتحدة دوراَ جديداً غأية في الأهمية في المجتمع الدولي إرتبط بظهور نمط جديد من الممارسات الحديثة في مجال تكنولوجيا الإتصالات والمعلومات ودخول الشبكة العنكبوتية حيز التنفيذ ومرتبط بها من خطورة شديدة في الجأنب غير المشروع من السلوكيات المرتبطة بالتهديد المباشر وتقويض أسس السلم والأمن الدوليين وبات عليها أن تدفع نحو تأسيس قواعد ومبادئ دولية للحد والمنع من السلوك الخبيث في هذا المجال[١].

وتضم الأمم المتحدة نحو ١٩٣ دولة أعضاء بها وتسترشد في أعمالها ونشاطها بالمقاصد الواردة في ميثاق تأسيسها وهذا العدد من الدول ١٩٣ هم جميع الأعضاء في جمعيتها العامة ويتم قبول الأعضاء الجدد بقرار من الجمعية العامة بناء على توصية من مجلس الأمن التابع لها ولبيان دور الأمم المتحدة وأجهزتها وتطور هذا الدور في ثلاثة مراحل زمنية مختلفة نعرضها كالآتي:

المرحلة الأولى من عام ١٩٩٠ حتى عام ٢٠٠٦

كانت تلك المرحلة باكورة ظهور نمط تكنولوجيا المعلومات والإتصالات المتمثل في الشبكة الدولية للمعلومات الإنترنت وكان من غير الملاحظ دخول عالم الإنترنت في العلاقات الدولية كما أنه لم يكن يشكل أي تهديد للأمن والسلم الدوليين بأي شكل من الأشكال لذا كانت جهود الأمم المتحدة في ذلك الحين غير موجودة وغير محسوسة ولم يتم تسجيل أي حوادث كان للفضاء الرقمي فيها دور أو وجود.

---

[١] **د. سامر محيي عبدالحمزة، مدى مساهمة الأمم المتحدة في تشكيل القواعد الدولية الخاصة بالفضاء السيبراني، مجلة مركز دراسات الكوفة، العدد٦٧، ج ١، ديسمبر ٢٠٢٢، ص٣٢٥**

وكان عام ١٩٩٨ هو بداية أول ظهور لهجوم يمكن أن يمس السلم والأمن الدوليين عندما قام مجموعة من القراصنة في دولة الصين بالهجوم على المواقع الحكومية الإلكترونية لدولة أندونيسيا بسبب وجود مظاهرات في الأخيرة ضد الصين ومنذ ذلك التاريخ أيقنت الأمم المتحدة الدور الخطير الذي يمكن أن يمثله السلوك السيبراني غير المشروع[١].

وفي نفس العام ١٩٩٨ بطلب من روسيا الإتحادية تم طرح موضوع التطور المتزأيد للإنترنت وعلاقته بالأمن الدولي أمام الجمعية العامة للأمم المتحدة وبالفعل تم إدراج هذا الأمر بجدول أعمال الجمعية العامة تحت عنوان التطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في سياق الأمن الدولي وتم توجيه الطلب من الدول الأعضاء بتقديم الآراء والمقترحات في ذلك وفي نهأية الأمر نظراً للمشاركة الضعيفة من المجتمع الدولي والذي إفتقرت فيه المساهمة والمشاركة ما يقارب العشر دول فقط تم تشكيل فريق خبراء تحت إسم فريق الخبراء الحكوميين المعني بالتطورات في ميدان المعلومات والإتصالات السلكية واللاسلكية في السياق الأمن الدولي وبالفعل تم إنشاء أول فريق عام ٢٠٠٤ إلا أن جهوده لم تثمر إلى توافق وإتفاق على المبادئ الواجب إتباعها لمواجهة ذلك السلوك السيبراني الحديث وأنتهى الفريق إلى إصدار قرار بفشله في إصدار تقرير نهائي بسبب تعقيد المسائل موضوع البحث.

المرحله الثانية من عام ٢٠٠٦ حتى عام ٢٠١٧

بداية من تلك المرحلة فقد تزايدت الهجمات السيبرانية في عدة دول مثل جورجيا عام ٢٠٠٨ وكذلك في أسيتونا عام ٢٠٠٦ والتي طلبت فيها من الأمم المتحدة إصدار إدانة بهذا النوع من الهجمات وإعطاء الأهمية المناسبة لوضع وصياغة القاعدة التي تنظم السلوك السيبراني للمجتمع الدولي.

وبعد تشكيل الجمعية العامة للأمم المتحدة عدة فرق من عام ٢٠٠٩ إلى عام ٢٠١٠ ثم فريق آخر في عامي ٢٠١٢ و ٢٠١٣ دون التوصل لمبادئ تحكم السلوك السيبراني سوى التنويه إلى ضرورة مواصلة الحوار لمناقشة المعأيير المتعلقة بإستخدام الدول لتكنولوجيا المعلومات والإتصالات[٢].

---

[١] د. عبدالفتاح مراد، جرائم الكمبيوتر والإنترنت، المكتبة القانونية، طبعة أولى،١٩٩٨، ص٢٣٧

[٢] د. أحمد عبيس الفتلاوي، الهجمات السيبرانية –مفهومها –المسئولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مرجع سابق، ص٢٠

ثم نجح الفريق الرابع عام ٢٠١٤ في وضع مبادئ أولية للقواعد السلوك السيبراني حينما نص تقرير هذا الفريق على أن القانون الدولي ينطبق على السلوك السيبراني كما بين أن الدولة التي تقوم بعمل معاد كذلك تتحمل كامل المسؤولية الدولية بعد قيامها بالفعل.

غير أن الفريق الخامس قد أصيب بالفشل بالمقارنة بالفريق الرابع بسبب رفض الولايات المتحدة الأمريكية التسويق لصالح ذلك التقرير للفريق الخامس بحجة أن مسودة التقرير خلت من القواعد التي تؤكد حق الدفاع الشرعي للدول ضد الهجمات السيبرانية.

المرحلة الثالثة من عام ٢٠١٨[١]

في بداية تلك المرحلة شكلت الجمعية العامة فريق سادس مكون من ٢٥ دولة على أساس التوزيع الجغرافي العادل وذلك عام ٢٠١٩ وإستطاع ذلك الفريق أن يضع ويصدر تقرير نهائي بتوافق جميع الأعضاء المشتركين متضمناً معايير السلوك المقبول في الفضاء السيبراني عام ٢٠٢١ وهو ما إصطلح على تسميته مبادئ السلوك السيبراني في تقرير الخبراء لعام ٢٠١٠ وما سوف نتناوله بشيء من التفصيل في معرض بحثنا نظراً لأهميته البالغة.

ولكن لم يكتب لتلك الجهود النجاح بالشكل المنشود حتى عام ٢٠٢١ والذي كأن البدأية الحقيقية نحو إقرار قواعد دولية حاكمة للفضاء السيبراني.

ويمكن إجمالي الأسباب والتداعيات التي تجعل من وضع قواعد دولية للفضاء السيبراني من منظمة الأمم المتحدة وأجهزتها أمراً غاية في الصعوبة كالآتي[٢]:

١- الأسباب التقنية والفنية للمشكلة لإرتباطها بتكنولوجيا المعلومات والإتصالات غير المحددة والواضحة والتي تقتصر فيها المعرفة بالخبراء والمختصين بهذا المجال وهذه العلوم على النقيض من ذلك من تنظيم ووضع قواعد لمجالات والصراعات البحار أو الجو الذي كان محدداً وواضحاً.

٢- تضارب مصالح المجتمع الدولي ومدى الإستفادة من إقرار قواعد تنظيم الفضاء السيبراني من عدمه ٣- حداثة الموضوع على الساحة الدولية حيث أنه بدا مع أواخر فترة التسعينات من القرن المنصرم مما جعل صعوبة في وضع قواعد ومبادئ وأعراف دولية أو أخلاقية تنظم هذا الموضوع من كافة جوانبه وجميع أشكاله.

---

[١]د. رزق أحمد سمودي، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام،مجلة جامعة الشارقة للعلوم القانونية، مجلد ١٥، العدد ٢، ٢٠١٨، ص٣٣٨

[٢]د. نهلا عبد القادر المؤمني، الجرائم المعلوماتية، الثقافة للنشر والتوزيع، عمان، الأردن،٢٠١٦،ص٥٢

٤- التطور والتعقيد المتواصل والسريع في عالم الفضاء السيبراني فكلما كانت مواجهة جديدة لنمط سيبراني حديث تصبح قديمة لظهور الأحدث فهو تطورات تجعل من عمليات الدراسة والتعقب غأية في الصعوبة إلى أن وصلنا للجيل الخامس الأكثر تعقيداً.

٥- عدم التفرغ المطلوب للأمم المتحدة وأجهزتها الذي يُمكنها من معرفة تفاصيل الفضاء السيبراني ودراسته من أجل وضع الضوابط الدولية الحاكمة له.

وإتساقاً مع ما تقدم ولمزيد من توضيح وعرض علاقة الأمم المتحدة وأجهزتها المختلفة بالفضاء السيبراني فسوف نجد أن إتجاه وعمل منظمة الأمم المتحدة لمواجهة السلوك غير المشروع في الفضاء السيبراني قد تدرج عبرطريقتين على النحو التالي[١].

الأولى: إتجاه الأمم المتحدة إلى تطبيق المبادئ التقليدية على الفضاء السيبراني.

الثانية: إتجاه الأمم المتحدة إلى تطبيق مبادئ جديدة ومستحدثة في الفضاء السيبراني ونعرضها كالآتي:

المرحلة الأولى: إتجاه منظمة الأمم إلى تطبيق القواعد والمبادئ التقليدية على الفضاء السيبراني وفي تلك المرحلة حاولت المنظمة أن يكون تطبيق ما إستقر عليه القضاء الدولي من مبادئ وأسس على الفضاء السيبراني طالما قد توافق أعضاء المنظمة عليها منذ مدة طويلة وذلك مثل مبدأ حل النزاعات بالطرق السلمية ومبدأ عدم جواز إستخدام القوة في العلاقات الدولية وكذلك مبدأ عدم جواز التدخل في الشؤون الداخلية لدولة ما ومبدأ إحترام سيادة الدول وفيما يلي أهم القرارات الصادرة عن الأمم المتحدة من أجل تطبيق هذه المبادئ على الفضاء السيبراني.

المرحله الثانية: إتجاه الأمم المتحدة نحو تطبيق مبادئ جديدة على الفضاء السيبراني لم تقف القواعد والمبادئ التقليديه العتيقة المستقرة في وجدان المجتمع الدولي في مواجهة أخطار الممارسات السيبرانية الجائره لذلك فقد أضافت الأمم المتحدة العديد من المبادئ الحديثة في هذا الصدد

---

[١] د. السيد محمد السيد أحمد، القانون في الفضاء السيبراني، المنصة القانونية، مقال منشور في ٢٠٢٢/٦/٧ على الرابط http:/wwwsaiplus.com

الفصل الأول
جهود منظمة الأمم المتحدة وأجهزتها
في تحقيق الأمن السيبراني

تمهيد وتقسيم:

إن إطلاع الأمم المتحدة منذ إنشائها عام ١٩٤٥ بمهام عديدة يأتي على رأسها عمل كل ما يلزم من أجل الحفاظ على السلم والأمن الدوليين بإعتبار أن ذلك هو الهدف الأسمى والغأية العظمى للمجتمع الدولي برمته بعد معاناته من ويلات الحروب التقليدية من حرب عالمية أولى تلتها الثانية.

ولما كان مصطلح الأمن والسلم الدوليين هو يتسع لكافة الممارسات والأعمال والأنشطة التي من شأنها أن تؤجج الصراعات والخلافات بين دول المجتمع الدولي ولا ريب أن إستحداث تكنولوجيا الإتصالات والمعلومات في الأحقاب الأخيرة وما يمثله ذلك من أشكال ومماراسات غير مشروعه من شأنها تهديد الأمن والسلم الدوليين بشكل مباشر مما يقوض من كافة الجهود المبذولة من المجتمع الدولي في سبيل سيادة السلم والأمن بين كافة الدول بشكل عادل ومنصف.

وعلى ذلك فقد تزأيد الإهتمام بهذه القضية على كافة الأصعدة سواء من الدول ذاتها أو من كافة المنظمات على إختلاف مشاربها سواء كانت منظمات إقليمية أو عالمية على السواء، ويأتي في طليعة المنظمات التي تولي قضية الأمن السيبراني عنأية وإهتمام شديدين منظمة الأمم المتحدة بوصفها الجامعه لكافة أو معظم دول المجتمع الدولي نظراً للإعتماد الشديد من كافة الدول على تكنولوجيا المعلومات والإتصالات والزيادة المتنامية في الإستخدام غير المشروع.

وفي هذا المقام سارعت الأمم المتحدة بكافة أجهزتها الرئيسية أو الفرعية للتصدي لهذه القضية بكل حزم وقوة وسرعة ولسوف نعرض في هذا المقام جهود الأجهزة الدائمه للأمم المتحدة وكذلك الوكالات المتخصصة لها من أجل العمل على تحقيق الأمن السيبراني المنشود.

المبحث الأول
جهود الأجهزة الدائمة للأمم المتحدة
في تحقيق الأمن السيبراني

آثرنا عرض وشرح الوضع الإقليمي والدولي الخاص بتأثير الهجمات والإعتداءات السيبرانية وبيان أضرارها ليكون ذلك من أجل توجيه النداء لكافه دول المجتمع الدولي من أجل التعاون المشترك وتظافر الجهود لمواجهة هذا الخطر الجسيم المخرب بالإنسانية جميعها، وفي هذا المقام ينبغي الإشارة هنا لما قامت به منظمة الأمم المتحدة بوصفها أكبر منظمة عالمية وما تملك من الآليات وإمكانيات ما يجعل مجهودات أجهزتها ذات تأثير يجب تنفيذه من كافة الدول

المطلب الأول: دور الجمعية العامة في تحقيق الأمن السيبراني.

الفرع الأول: فريق الخبراء ومبادئ السلوك السيبراني من عام ٢٠١٥ حتى عام ٢٠٢١.

الفرع الثاني: دور إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية لعام ٢٠٢٤.

الفرع الأول: جهود ومساعي فريق الخبراء ومبادئ السلوك السيبراني ٢٠٢١.

مع بداية الألفية الثالثة وإرتباطهم بالنشاط المتنامي في عالم تكنولوجيا المعلومات والإتصالات وما تبع ذلك من تزأيد الهجمات السيبرانية بين مختلف الدول بشكل واضح مما يقوض السلم والأمن الدوليين بشكل مباشر ومنظمة الأمم المتحدة بوصفها المنوط بها حفظ السلم والأمن الدوليين وما قد يؤدي إلى زعزعة هذا المبدأ وعلاقات الدول بالمجتمع الدولي.

وإنطلاقا مع صحوة الأمم المتحدة منذ عام ١٩٩٨ بالدفع نحو تأسيس ووضع قواعد دولية حاكمة للسلوك السيبراني في الجانب الخبيث منه ورغم تلك المساعي الحميدة المستمرة المضطردة منها إلا أن تلك المحاولات وهذه الجهود لم يكتب لها التوفيق والنجاح بالقدر الكافي.

ومع بداية عام ٢٠٢١ قامت منظمة الأمم المتحدة بإقرار مجموعة من القواعد والمبادئ في مجال الفضاء السيبراني رغبة منها ومن كافة دول المجتمع الدولي في مواجهة ذلك الخطر الجسيم المحدق والذي قلما تنجو منه أي دولة حتى الدول العظمى[١].

---

[١] **٣٣٢ د. سامر عبد الحمزة، مدى مساهمة الأمم المتحدة في تشكيل القواعد الدولية الخاصة بالفضاء السيبراني، مرجع سابق، ص**

وبتاريخ ٢٠٢١/٧/١٤ تم صدور تقرير تابع لهيئة نزع السلاح وهو تقرير الخبراء الحكومي معلنا للكافة الإتفاق على وضع قواعد دولية غير ملزمة للسلوك الأمثل للدول الأعضاء في مجال الفضاء السيبراني والرقمي.

رأي الباحث:

أولا: نحن نرى في هذا التقرير صفة عدم الإلزام ولا يخفى ما في ذلك من إطلاق الحرية للدول ومراعاه أو إغفال تلك المبادئ والقواعد حسب ما ترى ووفق ما يتفق مع مصالحها وكنا نأمل أن يكون هذا التقرير متمتعا بصفه الإلزام وإجبار الدول بأي وسيلة حتى لو أدى الأمر لصدور قرارات إقتصادية في أقل الأحوال على الدول التي لم تلتزم بما جاء بذلك التقرير لأن القاعدة العامة في فلسفة القانون أن القاعدة القانونية بدون جزاء هي والعدم سواء حيث أن الجزاء للمخالف هو ما يضمن تحقيق سياسيتي الردع الخاص لمرتكب الواقعه والردع العام لباقي أفراد المجتمع ممن أحيطوا علماً بتلك العقوبة وذلك الجزاء

ثانياً: نحن نرى أن صراع الدول الكبرى وخلافاتهم وإختلاف الأجندات والإستراتيجيات السياسية والإقتصادية قد يصيب تلك المبادئ بالجمود مما قد يدفعها لتوجيه عمل منظمة الأمم المتحدة نحو مصالحها وما قد يخدم هذا الإتجاه صوب مصالحهم فقط دون إعتبار لمصلحة المجتمع الدولي بشكل عام

وبالرغم من ذلك كانت تلك هي باكورة صيغة مبادئ وقواعد دولية وأن لم يكن لها صفة الإلزام والإجبار إلا أنها وضعت الأساس واللبنة الأولى نحو صياغة سياسة التعامل مع الفضاء السيبراني وقد صحبها تفاؤل كبير لدرجة أن الاستاذ مأيكل شميث أستاذ القانون الدولي بإنجلترا رأى أن إقرا المبادئ الواردة بتقرير الخبراء الصادر في عام ٢٠٢١ سوف تتحول في القريب العاجل إلى قواعد ملزمة لا يمكن غض الطرف عنها من أي من دول العالم وسوف تكون حاكمة ومحددة وضابطة للتعامل في الفضاء السيبراني اما القواعد الأخرى فسوف تكتسب صفة الإلزام من خلال تحولها بمرور الزمن لقواعد عرفية[١]

---

[١] **Michael Schmitt, The sixth united nations GGE and international law in cyberspace ,2021. at https://www.justsecurity.org/76864/the- sixth- united- nations- gge-and- international- law- in- cyberspace/**

الفرع الثاني
مبادئ السلوك السيبراني
في تقرير الخبراء لعام ٢٠٢١

كأن ذلك التقرير هو البادرة الأولى للمجتمع الدولي للإجماع والإتفاق على قواعد عامة حاكمة للسلوك السيبراني حتى وإن كان عدم التوصل لبعض الحالات والمسائل المتعلقة بالقانون الدولي والخاصة مثلاً بمدى إنطباق حالات الدفاع الشرعي ضد الهجمات السيبرانية للحاجة لمزيد من الدراسه لتقرير وجواز ذلك من عدمه

وقد إتجهت منظمة الأمم المتحدة بشكل مباشر لمزيد من السرعة والسهولة في إصدار تلك المبادئ الواردة بذلك التقرير عام ٢٠٢١ نحو الإنطلاق من المبادئ المستقرة الواردة بميثاق تأسيس الأمم المتحدة وكذلك مجموعة القواعد القانونية الدولية التي إستقرت في وجدان الدول كافة ولذلك الإنطلاق نحو تأسيس قواعد دولية جديدة ومستحدثة تواكب التطور والتقدم المتسارع في عالم التكنولوجيا وثورات المعلومات والإتصالات ونعرض ذلك على النحو التالي

المرحلة الأولى: الإتجاه نحو تطبيق المبادئ التقليدية الواردة بميثاق تأسيس المنظمة

كان من الأسهل والأسرع والأدق هو إتجاه منظمة الأمم المتحدة نحو تبني القرارات التي تم الإتفاق والإجماع عليها من كافة الدول على الفضاء السيبراني وما يتعلق بتلك الممارسات بما يشكل مساساً بالسلم والأمن الدوليين مثل مبدأ حل النزاعات بالوسائل السلمية ومبدأ عدم جواز إستخدام القوة في تسوية العلاقات الدولية وكذلك مبدأ عدم جواز التدخل في الشؤون الداخلية لأي دولة حفاظاً على مبدأ السيادة المقررة لكل دولة وفقا لقواعد القانون الدولي العام.[١]

المرحلة الثانية: الإتجاه نحو تطبيق مبادئ جديدة في عالم تكنولوجيا المعلومات والإتصالات

إن القواعد التقليدية سالفة البيان التى تبنتها منظمة الأمم المتحدة لم تسعفها في مواجهة أخطار العمل السيبراني المتجدد والمتغير والمتطور في كل وقت وحين كان لزاماً البحث عن مبادئ حديثة وجديدة تواكب هذا النمط الجديد الذي فرضته طبيعة الفضاء السيبراني بما يضمن محاولات

---

[١] ص٦ A/G.1/73/I.27) مذكرة الأمين العام للأمم المتحدة في عام ٢٠١٨ وثائق الأمم المتحدة – (الوثيقة

جادة لشمول كافة أنشطة وصور العمل السيبراني والأنشطة الخاصة به ومنها مبدأ التعاون الدولي ومبدأ إحترام حقوق الإنسان في الفضاء السيبراني وغيرها وسوف نتناولها بمزيد من التفصيل لاحقاً.

ومجمل تلك المبادئ وهدفها السيطرة ومحاولة ضبط العمل في المجال السيبراني من كافة الدول وعلى كافة الدول بما يتناسب مع السبل الحديثة في مجال تكنولوجيا المعلومات ومحاصرة كل نشاط آثم وغير مشروع بالتعاون الفعالي بين كافة الدول التي هي جميع ليس بمنأى عن خطورة هذا النمط من التكنولوجيا مما يجعل أمر التعاون الدولي هو امر مفروض واجب وليس من قبيل الرفاهية التي يمكن النجاة من أخطارها.

تقييم الباحث لمجمل مبادئ تقرير الخبراء لعام ٢٠٢١ المنبثق عن الأمم المتحدة

بعد إستعراض ما ورد بتقرير الخبراء لعام ٢٠٢١ الصادر عن الأمم المتحدة سواء بإقراره المبادئ التقليدية لميثاق الأمم لمتحدة وتطبيق هذه المبادئ على الفضاء السيبراني أو بإستحداث مبادئ دولية جديدةلأجل السعي الدؤوب لمحاصرة وتحديد وضبط كل أشكال وصور السلوك السيبراني غير المشروع.

وبالرغم من التفاؤل الدولي بصدور هذا التقرير الذي وضع اللبنة الأولى في الشرح العظيم المأمول لضبط وتيرة العمل والنشاط السيبراني إلا أن بعض المثالب قد إقترنت بذلك التقرير من وجهة نظرنا المتواضعة.

ا- بإستقراء ما سبق من المبادئ التي أرساها التقرير إلا أن جانب الإلزام المراد لضمان التطبيق الفعلية غائب بشكل يفرغ التقرير من محتواه ولا يليق أبداً بالأمم المتحدة ذلك الكيان الدولي والعالمي الكبير أن يكون عملها قاصراً على إصدار المبادئ أو توصيات إسترشادية للدول غير مجبرة على الإلتزام بما جاء بمحتوى تلك المبادئ.

ب- غياب دور التقرير في مواجهة المشاكل والسلوكيات التي تتسم بالخطورة التي تنجم من جراء الهجمات السيبرانية حتى مجرد فرض آلية تعويض الدول المضرورة غير وارد إطلاقاً بهذا التقرير.

ج- وجود كيانات موازية إقليمية لتلك المبادئ التي أقرها تقرير ٢٠٢١ تلك الكيانات تم تأسيسها على أسس أيدولوجية وفكرية وإقتصادية مناهضة لما جاء بالتقرير أو على الأقل لا تسير على نفس خطاه.

المطلب الثاني

دور إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية لعام٢٠٢٤ [١]

من منطلق الحرص المتواصل والدؤوب لمنظمة الأمم المتحدة نحو الحرص على مجابهة كافة الأنشطة والسلوكيات السيبرانية غير المشروعة وتنظيم سلوك الدول في ذلك الشأن.

وفي تاريخ التاسع والعشرين من شهر يوليو إلى التاسع من شهر أغسطس عام ٢٠٢٤ كلفت الأمم المتحدة اللجنة المخصصه لوضع اتفاقية دولية شاملة بشأن مكافحة إستخدام تكنولوجيا المعلومات والإتصالات للأغراض الإجرامية وتعزيز التعاون الدولي لمكافحة جرائم معينة تم إرتكابها بواسطة نظم تكنولوجيا المعلومات والإتصالات وكذلك تبادل الأدلة في شكل إلكتروني على الجرائم ذات الخطورة.

وبناء على ذلك سارعت تلك اللجنة لوضع إطار شامل لأجل مكافحة الجريمة السيبرانية وقد جاء بمطلع الإتفاقية ما يلي:-

من الملاحظ أن تكنولوجيا المعلومات والإتصالات بالرغم من أنها تتيح إمكانيات هائلة لتنمية المجتمعات فأنها تخلق فرصاً جديداً للجناة وقد تسهم في زيادة معدل الأنشطة الإجرامية وتنوعها وقد يكون لها أي أثر على الدول والمؤسسات وعلى رفاة الأفراد والمجتمع ككل.

وبناء عليه فقد تم صياغة وإقتراح مشروع هذه الإتفاقية المكون من تسعة فصول من قبل اللجنة التابعة للجمعية العامة للأمم المتحدة وسوف نعرض لهما كالتالي الفصل الأول تناول الأحكام العامة والفصل الثاني يتناول التجريم والفصل الثالث الولأية القضائية والفصل الرابع التدابير الإجرائية وإنفاذ القانون والفصل الخامس التعاون الدولي في تحقيق الأمن السيبراني والفصل السادس التدابير الوقائية وكذلك الفصل السابع تناول المساعدة التقنية وتبادل المعلومات والفصل الثامن تناول آليات التنفيذ والفصل التاسع والأخير تناول الأحكام الختامية ونود أن نشير هنا أننا سوف نعرض لأهم المواد التي تتعلق بجهود هذه اللجنة التابعة للجعية العامة للأمم المتحدة في شأن تعزيز وتحقيق الأمن السيبراني والتي تخدم جوهر ومضمون تلك الدراسة دون الإلتزام بعرض كل المواد الواردة في فصولها.

---

[١] **إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية الصادرة في ٢٧-١١-٢٠٢٤ (A/79/460)**

الفصل الأول
الأحكام العامة

ورد في المادة الأولى من الفصل الأول في هذا المشروع الخاص بالإتفاقية أن الغرض والهدف المرجو منها في شأن مجال الأمن السيبراني لكافة الدول المجتمع الدولي حيث نصت هذه الإتفاقية تشجيع وتعزيز التدابير الرامية إلى منع ومكافحة الجريمة السيبرانية على نحو أكثر كفاءة وفاعلية وكذلك في الفقرة ج من نفس المادة تشجيع وتيسير ودعم المساعدة الفنية والتقنية وبناء القدرات من أجل منع ومكافحة الجريمة السيبرانية وخصوصاً لصالح البلدان النامية.

وهنا نلاحظ أن مواد الإتفاقية المادة الأولى تناولت أحكام عامة أنها سابقة لحدوث الجريمة السيبرانية للوقأية من حدوثها وعمل كافة ما يلزم وكذلك دعم الوسائل الفنية والتقنية والتكنولوجية التي تساهم في كشف مكافحة هذا النوع من الجرائم ذات الطابع الخاص سواء في اجراءات تحديدها أو ضبطها أو الوصول لمرتكبيها أو توقيع الجزاء المناسب له[1].

وتناولت أيضاً في المادة الثانية التي تسلط الضوء على حقيقة وطبيعة الشأن السيبراني الذي يعد أرضاً خصبة لإرتكاب الجريمة السيبرانية وذلك حينما تضمنت أن نظام التكنولوجيا المعلومات والإتصالات يعني أي جهاز أو مجموعة من الأجهزة المرتبطة أو ذات الصلة التي تقوم بها واحداً أو أكثر وفقا لبرنامج ما بجمع وتخزين بيانات إلكترونية ومعالجتها آلياً، وكذلك في الفقرة ب من نص المادة أوضحت ماهية البيانات الإلكترونية بأنها تمثل حقائق أو معلومات أو مفاهيم ما في شكل يتيح معالجتها في نظام تكنولوجيا معلومات وإتصالات بما في ذلك أي برامج تتيح جعل نظام تكنولوجيا المعلومات والإتصالات يؤدي إلى وظيفة ما، وفي الفقرات التالية من المادة الثانية نجد أنها أوضحت جملة من المفاهيم التي كانت محلاً للخلاف والغموض قبل ذلك ومنها.

في الفقره الثانية من المادة الثانية عرفت بيانات المحتوى بأنها عبارة عن بيانات إلكترونية بخلاف المعلومات المشتركة أو بيانات الحركة تتعلق بمضمون البيانات المنقولة بواسطة تكنولوجيا المعلومات أو الإتصالات مثل الصور أو الرسائل الصوتية وتسجيلات الصوت والفيديو.

---

[1] **انظر المادة الأولى من إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية الصادرة في ٢٧-١١-٢٠٢٤ (A/79/460)**

وكذلك عرفت مقدم الخدمة في هذه المادة بأنه هو من يوفر الخدمة والقدرة على الإتصال عن طريق نظام تكنولوجيا المعلومات، وكذلك أيضاً عرفته بأنه من يعالج بيانات إلكترونية أو يخزنها نيابة عن خدمة الإتصالات.

وكذلك عرفت معلومات المشترك وتناولتها في الفقرة ومن المادة الثانية بقولها تعني أي معلومات يحتفظ بها مقدم الخدمة وتتعلق بمشتركين في خدمات تغيير بيانات الحركة أو المحتوى.

وأيضاً عرفت هوية المشترك بأنه عبارة عن عنوان أو البريد الالكتروني أو الجغرافي أو رقم هاتفه أو غيره من أرقام الوصول أو المعلومات المتعلقة بتحرير الفواتير والدفع المتاحة على أساس نفقات الخدمة أو ترتيب الخدمة.

وكذلك أيضاً عرفت الجريمة الخطيرة وتناولتها المادة الثانية بأنها هي السلوك الذي يمثل فعلاً إجرامياً يعاقب عليه بالحرمان من الحرية لمدة قصوى لا تقل عن أربعة سنوات أو بعقوبه أشد.

وعرفت أيضاً العائدات الإجرامية وتناولتها الفقرة من نفس المادة بقولها أنها عبارة عن الممتلكات المتحصل عليها بشكل مباشر أو غير مباشر من إرتكاب جريمة[١].

وتسري أحكام هذه الإتفاقية على الأفعال والسلوك المؤثم للسلوك والعمل السيبراني والأفعال المجرمة وفقاً لبنود تلك الإتفاقية وهو ما أكدته المادة الثالثة في فقراتها جميعاً وهي منع الأفعال المجرمة وفقاً لهذه الإتفاقية والتحقيق فيها وملاحقة مرتكبيها بما يشمل تجميد العائدات المستمدة منها وحجزها ومصادرتها وإعادتها وكذلك جمع الأدلة في شكل إلكتروني وكذلك الحفاظ عليها وتبادلها لأغراض التحقيقات أو الإجراءات الجنائية على النحو الوارد في المادتين٢٣ و٣٥ من هذه الإتفاقية[٢].

وتناولت في الفصل الثاني تجريم الأفعال الغير مشروعة التي تحدث في الفضاء السيبراني وهو من أهم الأمور التي وردت في هذه الإتفاقية وذلك لأنها وضعت وحددت الجزاءات المناسبة لكل سلوك سيبراني غير مباشر أياً كأن طبيعة ذلك الجزاء سواء كان عقوبة سالبة للحرية أو عقوبة مالية

---

[١] انظر المادة الثانية من إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية الصادرة في٢٧-١١-٢٠٢٤ (A/79/460)

[٢] انظ المادة الثالثة من إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية الصادرة في٢٧-١١-٢٠٢٤ (A/79/460)

وعلى كافة الدول إتخاذ ما يلزم بوضع التشريعات المحلية التي تنظم كافة الأنشطة والأعمال السيبرانية لتحقيق سياسة الردع العام والردع الخاص على السواء

وسوف نعرض في هذا الصدد لأهم المواد التي تناولت عمليات التجريم في مجال تكنولوجيا المعلومات والإتصالات الواردة بهذه الإتفاقية وقد ورد بالمادة الثامنة في الفقرة الأولى والثانية كالآتي:-

الفقرة الأولى من المادة الثامنة والتي تخص الإعتراض غير المشروع بأن" تعتمد كل دولة طرف في هذه في هذه الإتفاقية إتخاذ جميع التدابير التشريعية والتدابير الأخرى لكي يجرم قانونها الداخلي الإعتراض بوسائل تقنية لعمليات إرسال غير عمومية البيانات الإلكترونية إلى نظام تكنولوجيا معلومات وإتصالات أو داخله عندما يرتكب هذا الفعل عمداً ودون وجه حق ويشمل ذلك إعتراض الإنبعاثات المغناطيسية من نظام تكنولوجيا معلومات والإتصالات يحمل هذه البيانات".

وكذلك في الفقرة الثانية منها أنه يجوز للدولة الطرف أن تشترط أن يكون الفعل الإجرامي قد إرتكب بقصد غير نزية وبقصد إجرامي أو فيما يتعلق بنظام تكنولوجيا إتصالات ومعلومات متصل بنظام تكنولوجيا إتصالات ومعلومات آخر[١].

وسار على نفس الدرب في المواد التالية سواء المادة التاسعة والخاصة بالتدخل في البيانات الإلكترونية وتناولت المادة الحادية عشر الإستخدام السيء للأجهزة والمادة الثانية عشر جرائم التزوير المتعلق بنظم تكنولوجيا الإتصالات والمعلومات والمادة الرابعة عشر تناولت الجرائم المتعلقة بمواد الإنترنت الخاصة بالإعتداء الجنسي على الأطفال أو إستغلالهم جنسياً.

فيما أوردت المادة السادسة عشر تجريم عمليات النشر غير التوافقي للصور الحميمة بينما تناولت المادة السابعة عشر غسيل العائدات الإجرامية في حين تناولت المادة الثامنة عشر مسؤولية الأشخاص الإعتبارية عن الجرائم السيبرانية التي ترتكب في الفضاء السيبراني وكذلك أحكام المشاركة والشروع في مادتها التاسعة عشر.

اما الفصل الثالث فقد تناول الولاية القضائية ومن أهم ما ورد بمشروع هذه الإتفاقية الخاص بالولأيات القضائية والإختصاص القضائي وما تضمنته المادة الثانية والعشرون في فقرتها الأولى أن

---

[١] **انظر المادة الثامنة من إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية الصادرة في ٢٧-١١-٢٠٢٤ (A/79/460)**

تعتمد كل دولة طرف في الإتفاقية ما قد يلزم من تدابير لفرض ولايتها وبسط نفوذها القضائية على الأفعال الغير مشروعة وفقا لمشروع هذه الإتفاقية في الحالات الآتية

١- عندما يرتكب الفعل الإجرامي في إقليم تلك أو في إقليم الدولة الطرف في مشروع الإتفاقية

٢ عندما يرتكب السلوك الإجرامي على متن سفينة ترفع علم تلك الدولة الطرف أو طائرة مسجلة ومقتضى قوانين تلك الدولة الطرف وقت إرتكاب الفعل.

أما في المادة الثانية والتزاماً بأحكام المادة الخامسة من مشروع هذه الإتفاقية يجوز للدولة الطرف أن تخضع أيضاً أي فعل إجرامي من هذا القبيل لولأيتها القضائية في الحالات الآتية

١-عندما يرتكب الفعل الإجرامي أو السلوك الإجرامي ضد أحد مواطني الدولة الطرف في الإتفاقية

٢ عندما يرتكب السلوك الإجرامي أو الفعل الإجرامي أحد مواطني الدول الاطراف أو شخص عديم الجنسية يكون محل إقامته في إقليمها

٣- عندما يكون السلوك الاجرامي واحداً من الأفعال المجرمة الواردة بالفقرة ب مادة ١٧ من مشروع هذه الإتفاقية وكذلك الفقرة ا من المادة ١٧

وأنتهي الفصل الثالث بالفقرة السادسة من ذات المادة التي حددت إطاراً عاماً للولايات القضائية بينما أوردت وتضمنت عدم المساس بقواعد القانون الدولي وألا تمنع هذه الإتفاقية من ممارسة الدولة لأي ولاية قضائية جنائية تقيمها دولة أخرى طرف وفقاً لقانونها الوطني[١].

أما الفصل الرابع فقد تناول عمليات التدابير الإجرائية وإنفاذ القانون لكافة الجرائم التي يتم إرتكابها في مجال تكنولوجيا المعلومات والإتصالات من جمع الأدلة لكافة الجرائم الجنائية الأخرى وتنفيذ كل دولة للصلاحيات والإجراءات الواردة بالإتفاقية وعمليات الإحتفاظ ببيانات الحركة والإفصاح الجزئي عنها وتفتيش البيانات الإلكترونية المخزنة وحجزها وتجميد العائدات الإجرامية الناتجة عن الجرائم التي تحدث في الفضاء السيبراني ومصادرتها وإنشاء سجل جنائي وحماية الشهود ومساعدة الضحايا وحمايتهم، وكذلك تناولت في فصلها الخامس التعاون الدولي في تحقيق وتعزيز الأمن السيبراني من خلال المبادئ العامة للتعاون الدولي بشأن الجرائم السيبرانية من خلال التحقيق والملاحقة وجمع الأدلة ويشمل ذلك أيضاً تجميد العائدات الناتجة عن تلك الجرائم وإعادتها والتعاون الدولي أيضاً في نقل الأشخاص المحكوم عليهم والمبادئ والإجراءات العامة المتعلقة بالمساعدة

---

[١] **انظر المادة الثانية والعشرين من إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية الصادرة في ٢٧-١١-٢٠٢٤ (A/79/460)**

القانونية المتبادلة بين الدول الأطراف في مشروع هذه الاتفاقية وأهمية الشبكة العاجلة على مدار الساعة وطوال أيام الإسبوع من أجل ضمان توفير المساعدة الفورية لأغراض التحقيقات والملاحقة القضائية وكذلك تناولت المادة الثامنة والأربعين من هذه الإتفاقية التحقيقات المشتركة للدول وآليات إسترداد الممتلكات من خلال التعاون الدولي المشترك.

أما في الفصل السادس قد تناولت التدابير الوقائية وتناول هذا الفصل أحكام التدابير الوقائية من خلال جهود الدول الأطراف وسعيها إلى وضع وترسيخ سياسات تتسم بالفاعلية والإتساق من أجل إستغلال الفرص القائمة أو المستقبلية للجريمة السيبرانية من خلال تدابير مختلفة سواء كانت إدارية أو تشريعية أو أي تدابير وقائية أخرى.

أما في الفصل السابع من هذه الإتفاقية فقد تضمن عملية المساعدة التقنية والفنية وتبادل المعلومات من جميع الدول الأطراف لمزيد من محاصرة ومكافحة الجريمة السيبرانية وأن تلتزم جميع الدول وفقاً لقدراتها بتبادل أكبر قدر ممكن من المساعدة التقنية والفنية وبناء القدرات بما في ذلك التدريب وغيره من أشكال المساعدة وتبادل الخبرات ذات الصلة والمعارف الشخصية ونقل التكنولوجيا ووضع شروط متفق عليها أو وفق شروط متفق عليها مع إعتبار خاص لمصالح وإحتياجات الدول الأطراف النامية بهدف كشف الجرائم المشمولة بتلك الإتفاقية والتحقيق فيها وملاحقة مرتكبيها[1] وأوجبت كذلك المادة ٥٦ من هذه الإتفاقية أهمية تنفيذ الإتفاقية من خلال التنمية الإقتصادية وكافة أوجه المساعدة الفنية.

بينما تناولت في فصلها الثامن آلية تنفيذ مشروع هذه الإتفاقية من حيث إستراتيجيات تنفيذ ما ورد بالإتفاقية وذلك بالنص في المادة على بأن تضمنت أن ينشأ بمقتضى هذا الصك مؤتمر للدول الأطراف في الإتفاقية من أجل تحسين قدرة الدول الأطراف وتعاونها على تحقيق الأهداف الواردة بالإتفاقية ومن أجل تشجيع تنفيذها وإستعراض الإستراتيجية والآلية الخاصة بتنفيذ ذلك وتناولت أيضاً في الفقرة الثانية دعوة الأمين العام للأمم المتحدة إلى عقد مؤتمر للدول الأطراف في موعد ثمانية في موعد غأيته سنة واحدة بعد بدء نفاذ هذه الإتفاقية وبعد ذلك تعقد إجتماعات المنظمة للمؤتمر وفقاً للنظام الداخلي الذي يعتمده المؤتمر وكذلك التعاون مع كافة المنظمات الدولية وكذلك مع المنظمات غير الحكومية ومنظمات المجتمع المدني والمؤسسات الأكاديمية وكائنات القطاع الخاص ووضع إعتماد بروتوكولات تكميلية لهذه الإتفاقية إستناداً إلى ما ورد بالمادة ٦١ و٦٢ من

---

[1] **انظر المادة الرابعة والخمسين من إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية الصادرة في ٢٧-١١-٢٠٢٤ (A/79/460)**

هذه الإتفاقية[1] بينما تناولنا في الفصل التاسع وهو خاص بالأحكام الختامية لهذه الإتفاقية كما ورد في المواد ٥٩ من الإتفاقية ومايليها.

نجد في المادة ٥٩ بفقرتها الأولى والثانية ما يجب على الدول الأعضاء في الإتفاقية من وضع التدابير وإجراء وتشريعات ما يناهض الجريمة السيبرانية هو بذلك قد حالة على الدول الأعضاء لإتخاذ ما يلزم في سبيل ذلك حيث تضمنت في الفقرة الأولى منها بأن تتخذ جميع الدول الأطراف وفقا للمبادئ الأساسية لقانونها الداخلي ما يلزم من تدابير بما فيها التدابير التشريعية والإدارية لضمان تنفيذ إلتزاماتها بموجب هذه الاتفاقية.

والفقره الثانية من المادة ٥٩ يجوز لكل دولة طرف من أطراف هذه الإتفاقية أن تعتمد تدابير أكثر صرامة وشدة من التدابير المنصوص عليها في هذه الإتفاقية من أجل التصدي ومنع مكافحة الأفعال الإجرامية التي تحدث في الفضاء السيبراني وفقاً لما هو منصوص عليه في هذه الإتفاقية.

وترتيباً على ذلك فإن الدول الأطراف في هذه الإتفاقية يقع عليهم عبء وواجب صياغة ما يلزم من التشريعات أو القرارات الإدارية أو التنفيذية أو أي تدابير أو إجراءات أخرى للتصدي ومكافحة ما يلزم من أي تعدي أو تجاوز وفقاً لما جاء ببنود هذه الإتفاقية بما قد تمثله من أي شكل من أشكال الجرائم السيبرانية في تحقيق وتعزيز الأمن السيبراني.

وكذلك تناولت الماده ٦١ من تلك الإتفاقية إمكانية وضع بروتوكولات أخرى للتعاون تكون بروتوكولات مكملة لهذه الإتفاقية وهو بذلك يفتح الأبواب لمزيد من أي أعمال أو إتفاقيات ثنائية أو جماعية من أي مجموعة من الدول تكون أطراف هذه الإتفاقية أو غير أطراف فيها ويكون من أولى إهتماماتها تكملة وإستمرار بتلك الإتفاقية بحيث تظل الإتفاقية أصلا الذي يمكن أن ينبثق منه أي فرع آخر مكملاً أو متمماً له ما يصيب في نهية المطاف لنفس أهداف الإتفاقية[2]

وذلك قد وضعت تلك المادة في الفقرة الثانية قيداً على أي دولة أو منظمة تسعى لتكامل إقتصادي مع دولة أو مجموعة دول أخرى أو منظمة أن تكون هذه الدولة أو المنظمة طرفاً في تلك المنظمة وذلك لضمان أن يلتزم أن تلتزم الدول في حالة الرغبة في عمل تكامل إقتصادي ببنود تلك

---

[1] انظر المادة السابعة والخمسين من إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية الصادرة في ٢٧-١١-٢٠٢٤ (A/79/460)

[2] انظر المادة الواحدة والستين من إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية الصادرة في ٢٧-١١-٢٠٢٤ (A/79/460)

الإتفاقية خاصة أن الشأن الإقتصادي والمالية والإستثماري هو أكثر المجالات التي يمكن أن تكون محلاً للأعمال السيبرانية الغير مشروعة الخبيثة والضارة.

وكذلك تناولت المادة الثالثة والستون وضع إطار محدد يمكن اللجوء إليه والركون إليه في حالة وجود أي نزاع أو صراع أو خلاف بين دول أطراف في هذه الإتفاقية وهو الإستعانة بالوسائل السلمية لتسوية النزاعات مثل التفاوض والتحكيم والوساطة وغيرها من الطرق السلمية وذلك في إطار السلمية والبعد عن إستخدام القوة بأي شكل من الأشكال في خصوص تفسير أو تطبيق بنود هذه الإتفاقية.

وكذلك تناولت الفقرة الأولى من هذه المادة أن تسعى جميع الدول الأطراف لتزويد المنازعات المتعلقة سواء كان بتفسير أو تطبيق هذه الإتفاقية عن طريق التفاوض أو أي وسيلة من الوسائل السلمية التي تختارها.

رأي الباحث في تلك الإتفاقية بعد عرض الخطوط والأحكام الرئيسية للاتفاق لمشروع إتفاقية الجمعية العامة اللجنة المختصة التابعة للجمعية العامة للأمم المتحدة لعام ٢٠٢٤ تلاحظ لنا الآتي:

الملاحظة الأولى في هذا الشأن وبعد إستعراض ما جاء بها نجد أن ما ورد بها قاصر فقط على الأعضاء الأطراف في الإتفافية دون كافة الدول الأعضاء في الأمم المتحدة الذين يقدر عددهم ب ١٩٣ دولة فكيف يمكن الاحتجاج بماجاء بها على أي دولة لم تكن طرفاً فيها.

بطبيعة الحال ووفقاً للمبادئ القانونية المستقرة فلا يجوز الإحتجاج بها في مواجهة ما لم يكن طرفاً فيها ولا تنسحب أحكامها على ما عدا أطرافها حتى ولو كانت دولة عضواً في منظمة الأمم المتحدة ولم تشارك في الإتفاقية وبذلك فقط ضاق مجال الإحتجاج بها في عدد معين ومحدود من الدول المشاركة فيها بما يضعف ما جاء بها من قواعد وأحكام وتوصيات في خصوص الجرائم السيبرانية وتعزيز الأمن السيبراني والتي تتسم بكونها عابرة للحدود والدول وبجعلها إتفاقية محدودة النطاق والأثر.

والملاحظة الثانية كان من الأولى والأجدر على واضعي تلك الإتفاقية لضمان تنفيذ ما جاء بمحتواها بعد صياغة الإتفاقية للتنفيذ أن تكون هناك لجنة أو هيئة تابعة للأمم المتحدة تكون مسؤولة عن مراقبة تنفيذ الدول بماجاء بالبنود الإتفاقية وكذلك تلقي الشكاوي من أي دولة في حال تعرضها لأي عمل سيبراني غير مشروع وجمع الأدلة وصياغة التقرير بالحالة والواقعة وتحديد من يقع عليه المسؤولية أمام الأمم المتحدة لتكون الصورة كاملة وتحديد من له الحق وكيفية جبر الضرر الواقع

على أي دولة سواء بالتعويض المالية أو أي جزاء آخر تراه منظمة الأمم المتحدة ولا يخص ما في ذلك من ضمان الجدية والسرعة في تنفيذ وإلتزام كافة الدول بما جاء الإتفاقية.

الملاحظة الثالثة أوردت الإتفاقية في الغالب من موادها عبارة " يجوز لكل دولة ..... " مثل حالة جواز إتخاذ أي دولة من التدابير والإجراءات والتشريعات ما يلزم لضمان تنفيذ ماجاء بالإتفاقية من أحكام فإذا كان الأمر جوازي وليس إجباري فكيف يكون ضمان أن تضع كل دولة ما يلزم من تلك التدابير أو التشريعات الخاصة بمنع ومكافحة الجريمة السيبرانية فكان من الأولى على واضعي تلك الإتفاقية أن تكون عبارات ومواد الإتفاقية واضحة في الزمن وإجبار كافة الدول على إتخاذ مثل هذه التدابير وإلا ماذا سيكون الأمر لو تراخت أي دولة بالنظر لمصالحها عن الإلتزام بذلك فإطلاق حرية الدول في ذلك يفرغ الإتفاقية من محتواها وتأثيرها والإلتزام بعمل ما يلزم له

الملاحظة الرابعة كنا نتمنى أن تنص الإتفاقية في موادها المختلفة على إمكانية تدخل الأمم المتحدة بفرض جزاءات سواء كانت سياسية أو إقتصادية أو مالية على الدول المخالفة لبنود ما جاء بتلك الإتفاقية لتحقيق الردع العام والخاص سواء للدول أو المؤسسات أو المنظمات أو حتى الأفراد في حالة وجود أي سلوك أو نشاط سيبراني غير مشروع فكثيراً ما قامت الأمم المتحدة بفرض جزاءات غاية في القسوة على الدول التي تنتهك القانون الدولي مثل الحظر الإقتصادي مثلاً لأن الجريمة السيبرانية هي الأخطر على الساحة الدولية الآن ولضبط تلك الأنشطة ينبغي أن يكون مقروناً بجزاء دولي لضمان التنفيذ والإلتزام من كافة دول المجتمع الدولي.

المبحث الثاني

جهود الوكالات المتخصصة في تحقيق الأمن السيبراني

ماهي الوكالات المتخصصة ودورها

هي عبارة عن منظمات متخصصة تابعة للأمم المتحدة ذات طابع إختصاصي يكون دورها تبني قضية أو مسألة ما بالدراسة بحكم خبرائها ومختصيها لتقديم الدعم والمشورة الفنية لأجهزة الأمم المتحدة ليتسنى إتخاذ ما يلزم بشأنها على أسس علمية سليمة وفنية نتيجة لدراسة عملية من تلك الوكالات وتلك الكيانات بحكم تأسيسها ودورها المحدد سلفاً وهي وكالات ذات إختصاص ودور محدد ومعين في أي مسألة،طبيعة عمل تلك الوكالات هي منظمات مستقلة تعمل مع الأمم المتحدة ومع بعضها البعض من خلال آلية التنسيق التابعة للمجلس الإقتصادي والإجتماعي للأمم المتحدة على المستوى الحكومي الدولي من خلال مجلس الرؤساء والتنفيذين للتنسيق على مستوى الأمانات المشتركة.

وسوف نتناول دور الإتحاد الدولي للإتصالات هنا في تحقيق الأمن السيبراني وذلك إستناداً لإرشادات القمة العالمية لمجتمع المعلومات ومؤتمر المندوبين المفوضين لهذا الإتحاد وهو هدف أساسي له يتمثل في بناء الثقة والأمن في إستخدام تكنولوجيا المعلومات والإتصالات.

المطلب الأول

دور الإتحاد الدولي للإتصالات

في تحقيق الأمن السيبراني

من أهم الوكالات المتخصصة التابعة للأمم المتحدة في هذا الشأن هو الإتحاد الدولي للإتصالات السلكية واللاسلكية الرائد والفعال في مجال تكنولوجيا الإتصالات والمعلومات والذي يحاول جاهداً مراقبة كل التطورات المتلاحقة في هذا الشأن[1].

---

[1] **د. نسرين الصباحي، الحروب السيبرانية وتحديات الأمن العالمي، منشور في المركز العربي للبحوث والدراسات ٩/ ٢٠١٧ على الرابط**

http: www.icrsegoorg 40594

قد تم تدشين هذا الإتحاد على أنقاض الإتحاد الدولي للتلغراف على أساس الإتفاقية الدولية للتلغراف التي وقعها عدد ٢٠ دولة أوربية وهو بذلك أقدم منظمة دولية ما زالت قائمة حتى هذه اللحظة[١].

ومع مطلع عام ١٩٤٧ وإنعقاد مؤتمر أطلانطا ومع بدأية ظهور التطورات التي طرأت على عالم تكنولوجيا المعلومات والإتصالات ظهر الدور الرائد للإتحاد الدولي للإتصالات في مراجعة إجراءات تسجيل وتأمين الإعتراف الدولي بإستخدام الفضاء ونتيجة لذلك ظهرت خطة متصلة لتقديم تلك الخدمات في إطار منظم ومحدد في أقاليم ثلاثه لمزيد من ضبط الأمور وهم[٢]:- الإقليم الأول عبارة عن أوروبا وأفريقيا والإقليم الثاني وهو يضم الأمريكتين والإقليم الثالث هو عبارة عن آسيا وجنوب المحيط الهادي.

وأصبح دور الإتحاد الدولي للإتصالات متزأيداً بشكل كبير وذلك نتيجة التقدم التكنولوجي وتعدد المستثمرين في مجال الإتصالات وكذلك الشركات العاملة في مجال أجهزة الإتصالات فأصبح هذا الإتحاد منظمة كونية عالمية رئيسية في مجال قطاع الإتصالات و من الأهمية بيان وعرض كيفية وآلية عمل الإتحاد في شأن الأمن السيبراني وذلك كونه ينفذ إستراتيجية على مرحلتين لمزيد من التصدي المحكم لشكل السلوكيات والأنشطة في المجال السيبراني.

المرحلة الأولى: وهي تحديد آليات وأهداف وإستراتيجيات رئيسية من أجل التنسيق لإستجابة المجتمع الدولي لتحديات الأمن السيبراني وتعزيز وبناء الثقة في مجتمع المعلومات والإتصالات

المرحلة الثانية: تسهيل وتشجيع عمل برامج الأنشطة ذات الصلة بالفضاء السيبراني للدول أعضاء الإتحاد وكذلك البلدان النامية من أجل الإلتزام بمعأيير متكاملة والعمل متطلبات والإحتياجات على الصعيد الدولي والإقليمي على السواء.

ولا نستطيع أن نغفل دور البرنامج العالمي للأمن السيبراني في التعاون مع الإتحاد الدولي للإتصالات من توفير إطار للتعاون في مجال الأمن السيبراني بشكل قوي ومتواصل ومضطرد على

---

[١] **د. حسني محمد نصر، عبد الله الكندي، الإعلام الدولي، النظريات والإتجاهات الملكية الإمارات العربية المتحدة، دار الكتاب الجامعي،٢٠١١، ص٤١٤**

[٢] **د. حسني محمد نصر، نفس المرجع السابق، ص٤١٥**

كافة الأصعدة والأمثلة على ذلك متعددة مثل مجموعة إستراتيجيات وطنية وتدابير الأعضاء وكذلك قيامه بالتنسيق داخل الإتحاد الدولي وخارجياً داخلياً[١].

جهود معبرة للإتحاد في المجال السيبراني الأمن العالمي يمكن عرض تلك الجهود في النقاط الآتية:

١- يعد الإتحاد هو الوكالة الرائدة والأصيلة لمنظمة الأمم المتحدة في كافة قضايا تكنولوجيا المعلومات والإتصالات بحكم طبيعة الإتحاد.

٢- هو المصدر الرئيسي لعمليات التدريب والتثقيف وكافة المعلومات في هذا المجال وقد نجح في ذلك نجاحاً يشار إليه بالبنان.

٣- يمثل الإتحاد قمة الحرية في عالم التكنولوجيات وكذلك مواكبة والإضطلاع على كافة التغيرات والمستحدثات في ذلك القطاع.

٤- قيام الإتحاد بالدعوة لعقد إجتماعات ومتواصلة ومنتديات ومؤتمرات عالمية وإقليمية في مجال تكنولوجيا المعلومات والإتصالات بهدف مواكبة التطورات والتحولات الرهيبة التي يشهدها العالم في مجال تكنولوجيا المعلومات والإتصالات وفيما يلي نعرض أهمها.

١- المؤتمر العالمي لتنمية الإتصالات عام ٢٠٠٦ بالدوحه قطر:

برعاية الإتحاد الدولي للإتصالات التنمية التابع للإتحاد الدولي للإتصالات وذلك في عام ١٩٨٩ وذلك القطاع يعني بالمقام الأول عملية تنمية الإتصالات من خلال أمانة ذلك القطاع وذلك وفق معأيير تأسيسية وإلحاقه بالإتحاد الدولي للإتصالات التي صدرت للقطاع عام ٢٠٠٦[٢] وتناول مؤتمر الدوحة ضمن أعماله خطة عمل الدوحة التي حددت أنشطة قطاع التنمية التابعة للإتحاد وذلك خلال الفترة من ٢٠٠٧ إلى ٢٠١٠ من أهم ملامح تلك الخطة دعم أنشطة ذلك القطاع كذلك تشجيع قواعد إستعمال تكنولوجيا الإتصالات والمعلومات على أكبر نطاق لتحقيق كافة أهداف ومحاولة التنمية التي وضعتها الأمم المتحدة وكذلك مد يد العون للبلدان النامية في هذا المجال[٣].

٢- المنتديات الإنمائية الإقليمية الخمسة لسنه ٢٠٠٦ تحت رعأية الإتحاد الدولي للإتصالات

---

[١]الإتحاد الدولي للإتصالات السلكية واللاسلكية، الإجتماع الإقليمي التحضيري للمؤتمر العالمي لتنمية الإتصالات ٢٠١٠، منطقة الدول العربية، قطاع تنمية الإتصالات من ١٧: ١٩ على الرابط

http/:www.comferas-com

[٢]انظر الإتحاد الدولي للإتصالات، نفس المرجع السابق

[٣]انظر تقرير الأمين العام للأمم المتحدة حول متابعة نتائج مؤتمر القمة العالمي لمجتمع المعلومات على الصعيد الإقليمي والعالمي، ص٢٢

وفي تلك المنتديات الخمس تناول الإتحاد الدولي للإتصالات التركيز على ستة محاور وهي:

- إستخدام أداة إلكترونية لتقييم مدى تطور تكنولوجيا المعلومات والإتصالات.
- الموائمة بين سياسات تكنولوجيا المعلومات في كافة المناطق.
- إطلاق مبادرات عالمية تتناول مواضيع محددة تتعلق بالهياكل الأساسية لتكنولوجيا المعلومات والإتصالات.
- إنشاء منصة للتمويل الإفتراضي.
- أيجاد مبادرات إقليمية ومبادرات وطنية واسعة النطاق.
- تعزيز كافة الإستراتيجيات الوطنية لتكنولوجيا الإتصالات والمعلومات.

٣ - القمة العالمية لمجتمع المعلومات برعاية الإتحاد الدولي للإتصالات

وفي تلك القمة التي تم عقدها على مرحلتين إحداهم عام ٢٠٠٣ في جنيف والأخرى عام ٢٠٠٥،وتعد تلك القمة من أهم أعمال منظمة الأمم المتحدة على الإطلاق في مجال تكنولوجيا المعلومات والإتصالات والذي قام الإتحاد الدولي للإتصالات بدور قوي ورائد وفعال بوصف تلك القمة محاولة جدية وطموحة لمواجهة كافة المسائل التي تثيرها تكنولوجيا المعلومات والإتصالات في العقدين الأخيرين[١].

ومن أهم معالم تلك القمة سالفة الذكر أنها إتخذت منهجاً يشترك فيه جميع أصحاب المصلحة بمشاركة المجتمع المدني والحكومات والمنظمات الدولية والتقدم بمبادرة ربط العالم بقيادة الإتحاد الدولي للإتصالات والعمل على بناء جسور الثقة من أجل سد الفجوة الرقمية بشكل عام[٢].

وهو من أهم الأولويات للإتحاد خاصة في ظل التطور المتسارع في عالم التكنولوجيا والأدوات التي إعتمد عليها من جهة وكذلك نتيجة ظهور أنماط متعددة للتحديد الذي قد ينتج عن تلك التكنولوجيا والإستعداد لمواجهة أي خطر أو تهديد أو حتى مجرد أنه قابل للتوقع وصياغة وأيجاد الآليات الكفيلة بالتعامل مع تلك الأخطار المستجدة.

---

[١] لإتحاد الدولي للإتصالات السلكية واللاسلكية، وثيقة صادرة عن القمة العالمية لمجتمع المعلومات، جنيف 2003، وتونس ٢٠٠٥،https:/www.itu

[٢] الإتحاد الدولي للإتصالات، المؤشرات الأساسية لتكنولوجيا المعلومات والإتصالات ٢٠١٠، جنيف – مكتب تنمية الإتصالات من ص٥: ٨

ووفقاً لما سبق بيانه فقد شرع الإتحاد الدولي للإتصالات بتطوير مؤشر معيار الأمن السيبراني.

وهذا المؤشر يهدف إلى قياس مدى إلتزام الدول في خمسة مجالات مرتبطة إرتباط لا يقبل التجزئة بالأمن السيبراني وهي التدابير القانونية، التدابير التقنية والفنية،التدابير التنظيمية،عمليات بناء القدرات، التعاون الدولي بين كافة الدول.

وتلك المعايير الخمسة هي نفسها المعأيير التي حددتها الأجندة العالمية للأمن السيبراني والتي سبق وأن أطلقها الإتحاد الدولي للإتصالات عام ٢٠٠٧[١].

وحرص الإتحاد الدولي للإتصالات على أيجاد وتوفير لمحة ومعيار محدد لبيان مدى ما وصلت له الدول في تناولها لقضية الأمن السيبراني على صعيدها المحلي أو الوطني وتتمثل تلك الرؤية في دعم النهوض بالوعي العام بالأمن السيبراني وأهمية الدور الحكومي للدول في دمج الآليات لدعم نظم تكنولوجيا المعلومات بحيث يضحي الأمر من مجرد حمأية الفضاء السيبراني إلى تطوير الأمن السيبراني وتعزيزه[٢].

وسوف نعرض لعدة تقارير توضح الترتيب العالمي في مجال الأمن السيبراني للخمس دول الأولى وذلك بالنظر للتقارير الصادرة عن سنوات ٢٠١٥ و٢٠١٧ و٢٠١٨ والتي قد يتغير ترتيبها من تقرير لآخر حسب الأحوال[٣].

ففي تقرير عام ٢٠١٥ إحتلت الولأيات المتحد الأمريكية المركز الأول في الأمن السيبراني والسلامة السيبرانية وتلاها بعد ذلك عدة دول مثل كندا وإستراليا وماليزيا وعمان وغيرها من الدول وفي تقرير عام ٢٠١٧ إحتلت سنغافورة المركز الأول وتلاها عدة دول مثل الولايات المتحدة الأمريكية وماليزيا وأسيتونا.

وفي تقرير عام ٢٠١٨ إحتلت المملكة المتحدة المركز الأول وتلاها الولأيات المتحدة الأمريكية وفرنيا وغيرها من الدول.

---

[١] د. رضوان، الأمن السيبراني أولوية في إستراتيجيات الدفاع، مجلة الجيش، ع ٣٠، جانفي ٢٠١٧، ص١١

[٢] أنظر الإتحاد الدولي للإتصالات، مرجع سابق، ص١٥

[٣] أنظر تقارير الإتحاد الدولي للإتصالات حول الأمن السيبراني لسنوات ٢٠١٥، ٢٠١٧، ٢٠١٨ على الموقع https:/www.itu

(البرنامج العالمي للأمن السيبراني)[1]
تطور المشهد القانوني منذ عام ٢٠٠٨

وفي عام ٢٠١٩ كلف المجلس الأمين العام للإتحاد الدولي للإتصالات بأن يقدم بالتوازي إلى دورة المجلس التالية مباشرة عدداً من المسائل منها:-

١- تقرير يوضح كيف يستعمل الإتحاد الدولي للإتصالات إطار البرنامج العالمي للأمن السيبراني

٢- مبادئ توجيهية مناسبة وملائمة يتم إعدادها ومشاركة الدول الأعضاء وذلك بشأن إستعمال الإتحاد للبرنامج العالمي للأمن السيبراني وتمهيداً لنظر المجلس له والموافقة عليه في الوثيقتين (C19/117،C19/58)

ووفقا لما تقدم وتلك التوجيهات سالفة الذكر تم بالفعل صياغة مشروع المبادئ التوجيهية بدعم من الرئيس السابق لفريق الخبراء رفيع المستوى وكذلك ومشاركة الدول الأعضاء وتمهيداً لنظر المجلس فيها والموافقة على ذلك المشروع الخاص بالمبادئ التوجيهية.

وبالفعل تم وضع مشروع المبادئ التوجيهية بعد المشاورات المفتوحة لجميع أصحاب المصلحة المعنيين بالقمة العالمية لمجتمع المعلومات في ٢٠/٤/٢٣ذلك لتلقي أي تعليقات على ذلك المشروع[2].

الأحكام العامة للبرنامج العالمي للأمن السيبراني بوصفه إطاراً عالمياً للعمل في مجال الأمن السيبراني في عام ٢٠١٨ كما أوضحنا إعتمد مؤتمر المندوبين المفوضين التابع للإتحاد الدولي للإتصالات والتي تم إنعقاده في العاصمة الإماراتية دبي القرار رقم ١٣٠ كأول بادرة حقيقية في شأن تعزيز دور الإتحاد الدولي للإتصالات فيما يخص الثقة والأمن في مجال تكنولوجيا المعلومات والإتصالات وقد تناول القرار سالف الذكر في أهم مسائله على ضرورة إستخدام إطار البرنامج العالمي للأمن السيبراني لمواصلة توجيه عمل الإتحاد في جهوده الرامية لبناء الثقة والأمن في العمل السيبراني.

---

[1] انظر القرار رقم ١٣٠ في دبي ٢٠١٨ لمؤتمر المندوبين المفوضين، البرنامج العالمي للأمن السيبراني الوثيقة C20/3، ٦C20/inf/11

[2] ٦ C20/3 20/inf/11, انظر القرار رقم ١٣٠ في دبي ٢٠١٨ لمؤتمر المندوبين المفوضين، البرنامج العالمي للأمن السيبراني الوثيقة

ومن أجل مزيد من التشاور بين الدول الأعضاء والوصول لأفضل صيغة طلب الإتحاد من الرئيس السابق لفريق الخبراء أن يقدم تقريره إلى دورة مجلس الإتحاد العام في دورته لعام ٢٠١٩ والذي إنتهى بالفعل إلى امكانيه وضع مبادئ توجيهية مناسبة لتحسين الإستفادة القصوى من البرنامج العالمي للأمن السيبراني[١].

ووفقاً لعملية إعداد مشروع المبادئ التوجيهية الواردة في الرسالة المعممة رقم (CL-20/18) تم عقد جلسة مشاورات مفتوحة لجميع أصحاب المصلحة المعنيين بالقمة العالمية لمجتمع المعلومات في ٢٣-٤-٢٠٢٠ وحضر ذلك الإجتماع أكثر من ١٦٠ مشاركاً وقدموا بالفعل تعليقات جوهرية على مشروع المبادئ التوجيهية وأدت أمانة الإتحاد مرخصاً بتلك التعليقات والإقتراحات في الوثيقة(C20/Inf/11).

شمل هذا البرنامج خمسة ركائز أو مجالات أو موضوعات وهي:

التدابير التقنية والإجرائي والتدابير القانونية والهياكل التنظيمية وبناء القدرات والتعاون الدولي ولا يخفى أن هذا البرنامج تم وضعه ليكون ميثاق يلتزم به ويراعي تطبيق الإتحاد الدولي للإتصالات وهو مصمم من أجل التعاون بين كافة الشركاء المعنيين وأصحاب المصلحة وكذلك تشجيع التعاون مع جميع الشركاء من أجل تجنب تكرار الجهود في هذا الشأن.

وهنا يثور تساؤل عن ما هو رد الفعل الدولي على الإطار الذي يضم الركائز الخمسة للبرنامج العالمي للامن السيبراني ويمكن عرض ذلك في النقاط الآتية[٢]:-

١- حظى ذلك الإطار المتضمن الركائز الخمسة للبرنامج بتقدير واسع للغأية من جانب كافة الدول الأعضاء في الإتحاد الدولي للإتصالات على جملته

٢- ما زال هذا البرنامج يوفر إطاراً واسعاً للتعاون الدولي في كافة مسائل الأمن السيبراني وذلك في إطار الوثائق الختامية للقمة العالمية لمجتمع المعلومات وكذلك فإن التوصيات ذات الصلة التي تضمنها الفريق عام ٢٠٠٨ لا تزال سارية حتى اليوم وذلك بإستثناء القليل من المسائل التي أصبحت في عداد المتقادمة أو البالية أو تجاوزتها أحداث جديدة أخرى

---

[١] محضر الجلسة العامة السابعة عشر لمؤتمر المندوبين المفوضين في دبي ١٥-١١-٢٠١٨ متاح على الموقع https:/www.itu. int/md/s18-pp

[٢] الوثائق الختامية للقمة العالمية لمجتمع المعلومات

https:www.itu/en/action/cybersecurity/pages/gca

٣- لا شك أن تغير عالم تكنولوجيا المعلومات والإتصالات قد تغير بشكل جذري من عام ٢٠٠٨ لأنها أصبحت تشكل الأساس في أي قطاع من قطاعات المجتمع وظهور تكنولوجيا إتصالات جديدة وإعتمادها بوتيرة سريعة قد يجعل من عملية إعادة النظر في ذلك البرنامج الآن أمراً واجباً ومطلوباً من كافة الدول الأعضاء[١]

رأي الباحث في جدوى إستمرار العمل بالبرنامج العالمي للأمن السيبراني حتى الوقت الراهن بالرغم من تقديرنا الكامل لما ورد بالركائز الخمسة التي تضمنها البرنامج العالمي للأمن السيبراني وما سبقها من مشاورات وتعليقات من كافة الدول الأعضاء وكذلك توصيات ورؤية فريق الخبراء في هذا الشأن والإرتياح الدولي لهذا البرنامج ومتابعة الإتحاد الدولي للإتصالات للعمل إلا أننا نرى عدة ملاحظات منها:-

١- لابد من إعادة النظر في كافة بنود البرنامج على الأقل كل عقد من الزمن بمرور عشر سنوات وذلك للأسباب التالية

أولاً: عمليات التوسع المتزأيد المطرد في الإعتماد على الإنترنت في ظل وجود مئات الملأيين من أجهزة جديدة متصلة فيما بينها مع وجود نقاط ضعف جديدة محتملة يمكن من خلالها الإختراق وعمل وممارسة كافة السلوك السيبراني غير المشروع

ثانياً: ظهور وتطوير نمط جديد من الذكاء الإصطناعي القادر على الإستفادة من البيانات فضلاً عن تمكين الآلآت والأجهزة من إتخاذ قرارات بشكل منفصل ومستقل وزكي دون تدخل الإنسان مما يثير تحديات الأمن والثقة مرة أخرى على الخريطة الدولية للأمن السيبراني

ثالثاً: ظهور أنماط الجيل الخامس من التكنولوجيا ومعأيير جديدة للإتصالات والذي يتيح سرعة الإتصال تفوق أضعاف السرعة الموجودة الآن

رابعاً: عمليات الحوسبة الحكومية التي تتيح سرعات حاسوبية فائقة مما قد يعرض خوارزميات التشفير الحالية للخطر الشديد.

خامساً: ظهور تكنولوجيا الأمن الجديدة وخير مثال لها تكنولوجيا السجلات الموزعة وأكثر التطبيقات شيوعاً لها هي سلاسل الكتل والتي توفر وسائل حديثة وأفضل للحفاظ على الأنظمة والبيانات ذات الصلة كذلك ظهور وإعتماد أنظمة الهوية الرقمية.

---

[١] **حل توجيهية البرلمان الأوربي ومجلس الإتحاد الأوربي بتاريخ ٢٠١٣/٨/١٢ بشأن الهجمات على أنظمة المعلومات محل القرار الإطاري للمجلس ٢٠٠٥**

سادساً: زيادة عدد المستخدمين من عام ٢٠٠٨ على الصعيد العالمي للشبكات الإجتماعية مثال ذلك فيسبوك أكثر من ٢,٥ مليار مستخدم نشط شهرياً في ديسمبر٢٠١٩[١] مما يضع أمن وخصوصية المستخدمين وبياناتهم على المحك فضلاً عن نشر المحتوى المحرض على الكراهية.

سابعاً: ظهور شبكات أخرى في غأية السرية والخطورة مثل شبكات الويب المظلمة والتي تمارس نشاط إجرامي في الفضاء السيبراني.

وبناء على ما تقدم باتت الحاجة نظراً لتلك التطورات والإعتراف المتزأيد من جميع أصحاب المصلحة بما فيها حكومات الدول بتتبع الإجراءات العاجلة التي يتعين مراعاتها في سبيل النهوض بالأمن السيبراني ذات التطور المتلاحق بدءاً من حمأية البنية التحتية إلى حمأية خصوصية المستخدم.

مع الأخذ في الإعتبار ظهور وباء كوفيد ١٩ عام ٢٠٢٠ الذي لفت إنتباه المجتمع الدولي على أهمية تكنولوجيا الإتصالات والمعلومات في شأن الصحة والسلامة في المجتمع البشري الدولي وفيما يلي سوف نعرض للأسس والركائز الخمسة للبرنامج العالمي للأمن السيبراني.

أولا: الركيزة القانونية:

المحور أو البعد القانوني للأمن السيبراني في غاية الأهمية كأساس لضمان إحتفاظ المواطنين في جميع دول العالم بالثقة والأمان في مجال تكنولوجيا المعلومات والإتصالات وهو ما أشرنا إليه في تقرير الخبراء رفيع المستوى المعني والمهتم بالشأن السيبراني لعام ٢٠٠٨ إلى أهمية البعد القانوني وذلك من خلال الإستجابات التشريعية لمعالجة القضايا القانونية في المجال السيبراني بما في ذلك كيفية التعامل مع الأنشطة الإجرامية المرتكبة عبر الإنترنت[٢] من خلال تشريعات متوافقة ومتكاملة دولياً وعالمياً بين كافة الدول من أجل سد أي ثغرات في البناء القانوني الخاص بالأمن السيبراني وكذلك التوجيه بالمبادرات الإقليمية ذات الصلة بنفس الموضوع ومثال ذلك إتفاقية مجلس أوروبا بشأن الجريمة السيبرانية لعام ٢٠٠١

---

[١] عدد مستخدمي فيس بوك النشطاء شهرياً في جميع أنحاء العالم في الربع الأخير من عام ٢٠١٩ متاح على https/ number-of- monthly-com/ statistics/264810/number-of- monthly-active-facebook-users

[٢] القاضي شتاين شولبرغ ٢٠١٨ وكذلك ٢٠١٩ متاح على الموقع: http://www.cybercrime law.net/cybercrime law html

وفي هذا الشأن ومن الجدير بالذكر أن بعض الخبراء قد إقترح أن يفهم القانون الجنائي التكنولوجيا الجديدة وإسلوب وطرق السلوك في الفضاء السيبراني خاصة إذا توفر القصد الجنائي في السلوك السيبراني الغير مشروع[1]، وذلك في الأنشطة التي تندرج ضمن الجريمة السيبرانية وتيسير العمل والتعاون والمشاركة من كافة الدول الأعضاء مثل مذكرات التفاهم مع المنظمات الدولية وأصحاب المصلحة كافة من ذوي الصلة مثل مكاتب الأمم المتحدة المهتمة بالجريمة والمخدرات والإنتربول الدولي.

وقد شمل هذا التعاون مساعدة الدول الأعضاء على فهم وتدقيق الجوانب القانونية الخاصة بالأمن السيبراني من خلال مواد وتشريعات الجرائم السيبرانية للإتحاد الدولي للإتصالات ومستودع الجريمة السيبرانية لمكتب منظمة الأمم المتحدة المعني بالجريمة والمخدرات وبالفعل جرت مساعدة الدول الأعضاء في الشأن القانوني الخاص بالفضاء السيبراني، وذلك من خلال تقديم المساعدة في صياغة وموائمة التشريعات واللوائح المتعلقة بكافة أوجه وصور تكنولوجيا المعلومات والإتصالات وتبادل الخبرات في الشأن القانوني والتشريعي لكافة الجرائم السيبرانية.

وفي سبيل تحقيق الركيزة الأولى الخاصة بالتدابير القانونية فإنه قد يلزم مراعاة مبادئ إرشارية وتوجيهية لحسن تطبيق وإستخدام تلك الركيزة وهي.

المبادئ الإرشاديه والتوجيهية لإستخدام ركيزة التدابير القانونية

- على الإتحاد الدولي للإتصالات أن يواصل جهوده المتصلة من أجل تيسير عمليات المناقشات والحوار بين كافة أصحاب المصلحة وذلك بشأن كافة التحديات والعقبات الخاصة بالأمن السيبراني لمواكبة التطور السريع المتلاحق لمعدل التغير في عالم الفضاء السيبراني لأن ذلك قد يجلب مزيد من التحديات الجديدة للأمن السيبراني مع مراعاة تقديم كافة أشكال المساعدة لكل الدول الأعضاء في ذلك
- يجب أيضاً على الإتحاد بالتعاون مع الشركاء العمل على تطوير المواد الخاصة بالتشريعات التي تواجهها الجرائم السيبرانية لزيادة خبرة الدول في الجوانب القانونية والتشريعية للأمن السيبراني مع دعم وتبادل الخبرات بهدف تعظيم الجهود التي تهدف لوضع الإطار التشريع الملائم والخاص بجرائم الفضاء السيبراني
- مطالبة الدول الأعضاء بتطوير كافة التدابير القانونية المناسبة لدورها في مجال حقوق الإنسان

[1] **شتاين شولبرغ – تاريخ الجريمة السيبرانية (الطبعة الثانية – فبراير –٢٠٢٠)**

- على كافة الدول الأعضاء في الإتحاد الدولي للإتصالات إتخاذ تدابير قانونية مناسبة لمنع ومواجهة أي برامج خاصة بالإعتداء الجنسي على الأطفال ووقف ومنع نشر كافة المواد الإلكترونية الخاصة بذلك بما في ذلك وضع إجراءات إستباقية للوقاية وكشف وتفكيك وتعطيل كافة الشبكات أو المنظمات التي تستخدم لإنتاج أو توزيع مواد على الإنترنت تتعلق بالإعتداء الجنسي على الأطفال
- أن سيادة الدول تمتد أيضاً على الفضاء السيبراني وعلى ذلك يجب على الدول الأعضاء العمل على وضع آليات لحمأية الحقوق الأساسية للمواطنين وكافة الأفراد على أراضيها مع تيسير النفاذ المشروع لمحتوى الإتصال[١]

ثانياً: الركيزة الخاصة بالتدابير الفنية والإجرائية

من المعلوم تماماً أن التكنولوجيا الخاصة بعالم الإتصالات في حالة تطور وتغير مستمر بشكل متزأيد للغأية وهو ما تناوله البرنامج العالمي للأمن السيبراني بمزيد من الإهتمام واضعاً عدداً من المبادرات بهدف الوصول للنضج الكافي بشأن متغيرات الجريمة السيبرانية على المستويات العالمية والإقليمية والدولية من أجل تلبية الحاجة لوضع تدابير وإجراءات تتسم بالفاعلية في مجال الأمن السيبراني سواء على المستوى التشغيلي أو الإستراتيجي.

وهنا ينبغي الإشارة إلى التوجيه الصادر من فريق الخبراء رفيع المستوى العام ٢٠٠٨ فيما يتعلق بتعزيز كافة وجوه التعاون بشأن الأمن السيبراني حتى خارج الإتحاد وينبغي عمل مراكز الخبرة القائمة لتحديد وتشجيع وتعزيز إعتماد فريق من التدابير الأمنية والتقنية والفنية في هذا الشأن[٢].

كذلك أورد تقرير الخبراء في توصيته رقم ٢،٢ المعني بالأمن السيبراني في سبيل وضع القياسات الدولية للأمن السيبراني في عام ٢٠٠٨ للتعامل مع المعأيير والقياسات الدولية المتصلة والخاصة بالتدابير الفنية والإجرائيه وفي سبيل ذلك يجب دعم وتشجيع الدول الأكثر تقدماً من النواحي التكنولوجية على المشاركة في أنشطة الإتحاد والتعاون المثمر من أجل وضع المعأيير السليمة للنواحي الإجرائية والفنية بما في ذلك معايير الأمن.

---

[١] هذا المبدأ التوجيهي يستند إلى التوصيات رقم ١،٩، ١،١٤،١،١٢، الذي ورد في تقرير الخبراء رفيع المستوى المعني بالأمن السيبراني عام ٢٠٠٨

[٢] تقرير فريق الخبراء رفيع المستوى المعني بالأمن السيبراني عام ٢٠٠٨ الفقره ٢،١ ص ٩

كذلك أشار تقرير الخبراء بوضع تلك المعأيير على أساس المعاملة بالمثل بحيث يكون ضمان الأمن من الطرفين عن طريق عمليات التصميم وتقييم المخاطر وإتخاذ التدابير للتصدي لمواطن الضعف في البرمجيات بما في ذلك البروتوكولات والمعأيير الأساسية وفي ذلك يجب مراعاة الأمور الآتية[1]

ا- ضرورة وضع مقأييس مناسبة لتحديد مستوى درجة الأمن في مراحل التنفيذ

ب- الحاجة إلى عمليات تقييم مستمر وإصدار شهادات دورية ومتواصلة للمفاجأة على مستوى أمن البيانات والمعلومات والأنظمة والخدمات

ج- الحاجة الملحة إلى مستوى آمن من الإستخدام عن طريق التصميم الآمن في كافة مراحله المبادئ الإرشاديه والتوجيهيه لإستخدام ركيزة التدابير الإجرائية والتقنية

تلك التوصيات المتعلقة بركيزة ومحور التدابير الإجرائية والتقنية لتقرير الخبراء رفيع المستوى في عام ٢٠٠٨ وهي كالآتي

- على اللجان التابعة للإتحاد الدولي للإتصالات والخاصة بدراسات تكنولوجيا الأمن الحديثة والناشئة دراسة وصياغة ووضع مبادئ إرشادية وتوجيهيه لإستخدام كافة التكنولوجيا ذات الصلة وحث الدول الأعضاء على تطبيق تلك التقنيات في الأوقات المناسبة من أجل مواجهة كافة التهديدات السيبرانية المتغيرة بشكل دائم والمتصاعدة بشكل مضطرد[2].
- ضرورة إنشاء آليات وإستراتيجيات من أجل التعاون الوثيق بين مختلف لجان دراسة قطاع قياسات الإتصالات فيما يتعلق بمسائل الأمن مع أهميه قيام اللجنة بدور تنسيقي وقيادي للحفاظ على أقصى درجة من الأمن طوال عمليات فترة وضع القياسات لكافة منتجات المعلومات والإتصالات.
- تشجيع التعاون والتنسيق على أسس المعاملة بالمثل التي يضعها الإتحاد مع المنظمات الأخرى المعنية بوضع معأيير ضمان الحفاظ على أمن المنتجات من البدأية للنهأية لمختلف التطبيقات
- ضرورة أن يواصل الإتحاد جمع كافة المعأيير الأمنية العالمية لتكنولوجيا الإتصالات ومواصلة ومتابعة تنفيذ تلك التوصيات وتشجيع كافة المنظمات المعنية بوضع معأيير بشأن التدابير التقنية والإجرائية لقطاع قياس الإتصالات من أجل الوصول لإعتمادها كتوصيات عامة للدول الأعضاء.

---

[1] **تقرير فريق الخبراء رفيع المستوى المعني بالأمن السيبراني عام ٢٠٠٨ الفقرة ٢،٢ ص٩**

[2] **تقرير فريق الخبراء رفيع المستوى المعني بالأمن السيبراني عام ٢٠٠٨ الفقرة ١،٢ ص٩**

- العمل على تشجيع المجتمع الدولي على الإلتزام ببروتوكول ورؤية عالمية مشتركة للأمن السيبراني والعمل على تنفيذها والإلتزام بها ودعم الإتحاد لكي يصبح مركزاً للتميز العلمي بشأن التدابير الإجرائية والتقنيه للأمن السيبراني في المجالات التي تندرج تحت ولايته.
- على الدول المشاركة الفعالة في وضع ترتيبات إصدار الشهادات المتبادلة لوضع إطار عالمي لإدارة الأمن السيبراني مستنداً في ذلك على معأيير متفق عليها بين الدول الأعضاء.

ثالثاً: الركيزة الخاصة بالهياكل التنظيمية

إنه لمن المستقر وبحق أنه قد تم إحراز تقدم ملحوظ في تلك الركيزة وذلك المحور في العقد الماضي من حيث إنشاء العديد من المنظمات الوطنية والدولية والإقليمية لمعالجة مسائل الأمن السيبراني.

ولكن التنسيق فيما بين تلك الهياكل التنظيمية قد يكون بهدف التعاون فيما بينهم سواء على المستوى التشغيلي أو المستوى الإستراتيجي وتركز تلك المؤسسات سالفة البيان على إقامة علاقات تعاونية مثمرة خاصة في تنفيذ العمليات المشتركة في حالة وقوع أي حوادث سيبرانية وكذلك تداول المعلومات وتبادلها بسرعة للإستجابة للحوادث السيبرانية المستجدة[1]، وعلى الصعيد الوطني المحلي للدول يجب وضع آليات وهياكل مؤسسية مختلفة وفعالة إستعداداً لأي حوادث سيبرانية على نحو موثوق فيه وآمن ومن أمثلة هذه الهياكل التنظيمية الوطنية والإقليمية التي تم إنشائها.

شرطة مجلس التعاون الخليجي و مركز أوقيانوسيا للأمن السيبراني و مركز الأمن السيبراني الإسترالي والمركز الأوروبي للجرائم الإلكترونية ومركز تنسيق الجرائم الإلكترونية بالهند ومركز التحكم في الجرائم السيبرانية والوكالة الماليزية للأمن السيبراني والوكالة الوطنية الفرنسية للأمن السيبراني و المركز الوطني للأمن السيبراني في سويسرا والمركز الوطني للأمن السيبراني في إنجلترا وبرنامج الأمن السيبراني السعودي.

ثانياً: أشكال من مبادرات منظمات دولية في شأن الهياكل التنظيمية

لم تقتصر جهود عمل الهياكل والمؤسسات التنظيمية على الدول بشكل منفرد إنما بادرت عدة منظمات دولية في هذا الشأن نذكر منها الآتي:

---

[1] **الفرق الوطنية للإستجابة للحوادث الحاسوبية – الإتحاد الدولي للإتصالات تمت الزيارة في ٩-٧-٢٠٢٥**
itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx

المركز العالمي لقدرات الأمن السيبراني:- وهو مركز دولي لكافة البحوث الخاصة بالقدرات الفعالة في مجال الأمن السيبراني.

المنتدى العالمي للخبرة السيبرانية: الذي أنشئ في عام ٢٠١٥ لهدف تبادل الممارسات الجيدة وتقديم الخبرات في مجال بناء القدرات السيبرانية للدول والمنظمات وكذلك القطاع الخاص بالتعاون مع الإتحاد الدولي للإتصالات.

المجمع العالمي للإبتكار التابع للإنتربول: الذي بدأ عمله في عام ٢٠١٥ في سنغافورة لدعم وتدريب المتخصصين في مجال إنفاذ القانون الوطني إستجابة منه للتغيرات المتلاحقة في الجريمة السيبرانية.

مركز التميز المعني بالدفاع الحاسوبي التعاوني CCDCOE: وهو يتبع حلف شمال الأطلنطي والذي بدأ في تالين عام ٢٠٠٨ وذلك لمنح التدريب والتنمية والتمرين للخبراء التقنيين والموظفين والعسكريين وكافة الدول المعنية بالشأن السيبراني.

المبادئ الإرشاديه التوجيهية لإستخدام ركيزة الهياكل التنظيمية

لا شك أن تقرير الخبراء رفيع المستوى المعني بالأمن السيبراني لعام ٢٠٠٨ قد ساهم بشكل عظيم في دعم جهود الإتحاد الدولي في محور الهياكل التنظيمية بشكل متزأيد وقد أورد مكتب تنمية الإتصالات التابع للإتحاد الدولي للإتصالات جملة من المبادئ الإرشادية في شأن الجهود المبذولة بشأن الهياكل والمؤسسات التنظيميه لضمان حسن قيامها بعملها.

- على الإتحاد إعطاء أولوية للدول التي لم ينفذ فيها للآن هياكل تنظيمية للأمن السيبراني.
- ينبغي على الإتحاد الدولي للإتصالات بذل المزيد من التشجيع للتعاون بين مختلف وكافة المنظمات سواء كانت إقليمية أو دولية في جهود إنشاء هياكل تنظيمية وطنية قادرة على القيام بدورها بشكل مستدام وتجنب إزدواج الجهود.
- على الإتحاد تقديم يد العون للبلاد النامية في تنفيذ الفرق الوطنية للإستجابة للحوادث السيبرانية كافة المنظمات التقنية والفنية الأخرى ذات الصلة.
- على الإتحاد تعزيز كافة الجهود التي تهدف لقياس الإلتزامات المؤسسية للدول الأعضاء والإستفادة من الأدوات الخاصة بذلك مثل المؤشر العالمي للأمن السيبراني.

- على الإتحاد فيما يخص الهياكل التنظيمية الوطنية بوجه خاص مساعدة الدول الأعضاء لتطوير إطار تنسيقي يضم كل القطاعات الحكومية لتحسين الجهود الوطنية الخاصة بالأمن السيبراني.
- على الإتحاد تعزيز كافة أوجه التعاون بين الهياكل التنظيمية للأمن السيبراني على كافة الأصعدة سواء الإقليمي أو العالمي.

رابعاً: محور بناء القدرات

من أهم الأمور الحاسمة في مجال الأمن السيبراني هو نشر المهارات وثقافة الأمن السيبراني والممارسات الجيدة بين جميع أصحاب المصلحة ولذلك فأن معظم الدول وجميع المنظمات في إحتياج للموارد والمهارات البشريه الضرورية والكافية من أجل الأنشطة التاليه في مجال الأمن السيبراني[١].

- السيطرة على المخاطر
- إدارة الأزمات الخاصة بوقوع هجمات سيبرانية
- تطوير سلوكيات وممارسات منظمة ومنسقة
- تنفيذ كافة التدابير التشغيلية والإستراتيجيه للأمن السيبراني
- تطوير وتعزيز كافة البنى التحتيه وقدرتها على الصمود والإستمرار

المبادئ الإرشادية التوجيهية لإستخدام ركيزة بناء القدرات

يمكن إجمالي تلك المبادئ الصادرة من البرنامج العالمي للأمن السيبراني وتوصياته في شأن تلك الركيزة وإستناداً لتقرير الخبراء لعام ٢٠٠٨ الذي يوفر إطار يشجع بناء القدرات للموارد البشرية ويجب على الإتحاد من خلال قطاع تنمية الإتصالات التابع له العمل على ما يلي[٢].

١- دعم البلاد النامية في جهود بناء القدرات في مجال الأمن السيبراني بدعم من المجتمعات الوطنية والدولية المعنية ببناء القدرات في هذا الشأن

---

[١] **المبادئ التوجيهية للإتحاد الدولي للإتصالات في مجال الأمن السيبراني متاح على الموقع**
http:/webfoundation org/2019

[2] **Epfl, Prss Cyber Power, crime. conflict and security in cyber space,2013 Lorans Braford ,Cyber security needs women , Here's Why.**

٢- تشجيع تيسير كافة الممارسات الجيدة للدول الأعضاء في مساعدة البلدان النامية على اللحاق بالخبرة المتخصصة في مجال الأمن السيبراني وتقليص الفجوة في القدرات بينها وبين الدول المتقدمة
٣- مواصلة التعاون الشامل بمختلف المنظمات الدولية والإقليمية والعالمية للمشاركة في بناء القدرات من أجل ضمان التأثير في مجال الأمن السيبراني.
٤- وضع وتحديد إستراتيجيات وخطط وسياسات وقدرات وطنية في مجال الأمن السيبراني للإستجابة لمستجدات الحوادث.
٥- التركيز على إحتياجات الفئات الأكثر ضعفاً كالنساء والأطفال وذوي الإعاقة في جهود بناء القدرات ٦- وضع دليل بشأن تنفيذ برنامج التعليم في مجال الأمن السيبراني بهدف تقديم الدعم للدول الأعضاء في تطوير قدرات الشباب في كافة المراحل التعليمية لمزيد من التدريب في مجال الأمن السيبراني.
٧- مواصلة تعزيز نشر ودعم ثقافة الأمن السيبراني.
٨- مواصلة وتعزيز ودعم البرنامج العالمي للامن السيبراني بإعتباره آلة رئيسية لبناء القدرات في كافة البلدان.
٩- دعم كافة الأنشطة في مجال التكنولوجيا الناشئة والذكاء الإصطناعي المتصلة بالأمن السيبراني بين مختلف أصحاب المصلحة.

خامساً: المحور أو الركيزة الخاصة بالتعاون الدولي:

من أهم المحاور في ظل التحديات الراهنة وبوصف الجريمة السيبرانية عابرة الحدود في أغلب حالاتها هو التعاون والشراكة الفعالة بين كافة الأطراف الفاعلة والدول والمؤسسات في مجال تبادل المعلومات والتعاون بشأن الأمن السيبراني وذلك من أجل أن التعاون الدولي هي ركيزة شاملة للبرنامج العالمي للأمن السيبراني لأنها تشكل الأساس المتين لبناء الثقة والأمن في إستخدام كافة اشكال تكنولوجيا المعلومات والإتصالات وهو ما تناوله تقرير الخبراء عام ٢٠٠٨ من أهمية التعاون والحوار والتنسيق على الصعيد الدولي مع أي تهديدات سيبرانية[١].

[١] **انظر المبادئ التوجيهية للإتحاد الدولي للإتصالات في مجال الأمن – الملحق رقم ١ وثيقة (٤٧٠٩٣٨)**

ومن أمثلة التعاون الدولي في مجال الأمن السيبراني التى تمثلت في عدة مظاهر منها

- منظمة الأمم المتحدة بما تتمتع به من إمكانية عقد الإجتماعات والمنتديات في شأن التعاون والتنسيق على الصعيد الدولي من جميع أصحاب المصلحة من جميع الدول[١].
- المناقشات الثنائية الجارية بين الدول والمناطق المتقدمة تكنولوجياً مثل الحوارات المشتركة بين الولايات المتحدة والصين وبين روسيا والولأيات المتحدة والحوار بين الهند وإنجلترا بشأن الأمن السيبراني وكذلك الحوار بين استراليا وكوريا بشأن السياسات السيبرانية[٢].
- إنتهاج الكثير من الدول لنهج يشمل كامل الحكومة بأسرها مع إنشاء آليات تنسيق مركزية شاملة لعدة قطاعات تكون مسؤولة بشكل مباشر أمام رؤساء الدول والحكومات.
- منتدى القمة العالمية لمجتمع المعلومات لأغراض التنمية ومنتدى إدارة الإنترنت لأغراض الإدارة وهو اكبر تجمع ثانوي لمجتمع عالم تكنولوجيا المعلومات والإتصالات وذلك من أجل التصدي للتحديات الخاصة بالتنمية المتعلقة ببناء الثقة والأمن في إستخدام تكنولوجيا الإتصالات والمعلومات.
- المبادئ الإرشادية والتوجيهية لإستخدام ركيزة التعاون الدولي

بوصف تلك الركيزة هي ذات طابع شامل فأنه من الأهمية أن تعمل كافة قطاعات الإتصالات بشكل جماعي وثيق مع تنسيق الجهود داخليً وخارجياً وفي هذا الشأن ومع وضع توصيات فريق الخبراء في الإعتبار فأنه يجب مراعاة تلك المبادئ الآتية في سبيل إستخدام ركيزة التعاون الدولي

- ينبغي مواصلة تشجيع ودعم المناقشات الثنائية المتعددة الأطراف من كافة الجهات الفاعلة الرئيسية نظراً للطابع العابر للحدود للتهديدات السيبرانية
- يجب على الإتحاد الدولي للإتصالات أن يواصل إستنباط وإستكشاف آليات جديدة ومرنة وفعالة وسريعة لبناء الشراكة وبشكل متواصل
- على الإتحاد كذلك مضاعفة الجهود مع الوكالات الرئيسية داخل الأمم المتحدة لتنسيق الجهود الداخلية للأمم المتحدة والعمل على تبسيط كافة برامجها المتعلقه بالأمن السيبراني

---

[١] **تقرير فريق الخبراء رفيع المستوى ٢٠٠٨ الفقرة ١٥،١ ص٩**

[2] **https://obama whitehouse.archives.gov/the-press-office/2013/6/17/fact-sheet-us-russian. Cooperation- information and communication – techand.**

- على الإتحاد أيضاً أن يساعد في تعزيز ورفع كافة الجهود في التيسير للجمع بين كافة الأطراف الفاعلة وذلك من خلال منتدى القمة العالمية لمجتمع المعلومات
- على الإتحاد توسيع دائرة تعاونه ومشاركته بما يعود بالفائدة الجماعية على جميع أصحاب المصلحة من أجل تقاسم المعرفة والمعلومات والخبرات[1]
- على الإتحاد العالمي للإتصالات عند قيامه بعمله أن يسترشد بالبرنامج العالمي للأمن السيبراني ومراعاة أهداف واحتياجات أعضائه والنواتج المطلوبة
- يجب تشجيع كافة الدول على مواصلة الإرتقاء والتطوير بمسألة الأمن السيبراني لأعلى مستوى مع وضع السياسات الخاصة بذلك داخل حكوماتها
- وأخيراً يجب على الإتحاد أن يكون مستودعاً للمعلومات لمختلف الأنشطة والمقدرات والمشروعات العالمية التي تم تنفيذها في مختلف جوانب الأمن السيبراني بالشراكة مع المنظمات الأخرى النشطة في هذا المجال مع تعاون أصحاب المصلحة الآخرين في هذا الشأن .

[1] **للمزيد من المعلومات على الموقع التالي**

https:/www.un.org/org/en/digital-cooperation- penal

الفصل الثاني

دور منظمة الأمم المتحدة

في إرساء مبادئ وقواعد القانون الدولي العام لتعزيز الأمن السيبراني

لا يمكن بأي حال من الأحوال أن نغفل عن قصد أو عن جهل الدور الذي قامت به وما زالت تقوم به منظمة الأمم المتحدة في شأن السلوك غير المشروع أو الخبيث في الفضاء السيبراني سواء عبر أجهزتها الدائمة أو الوكالات المتخصصة التابعة لها وسوف نعرض لهذا الدور على النحو التالي:-

المبحث الأول
المبادئ التقليدية المطبقة
لتحقيق الأمن السيبراني

تمهيد وتقسيم:

بحسب إحصائيات الأمم المتحدة فإن عدد سكان العالم الأن حوالي ٧,٩ مليار نسمة وأكثر من نصف هذا العدد يستخدم الإنترنت وكذلك يستقبل محرك البحث جوجل يوميا نحو ٣,٥ مليار بحث ويبلغ عدد الأجهزة المتصلة بالإنترنت حوالي ٥٠ مليار جهاز في بضع سنوات أضف إلى ذلك منصة فيسبوك حوالي ٢,٩ مليار مستخدم في اليوم الواحد مرتبط ذلك بزيادة عدد الهجمات والحروب السيبرانية وكافة الأعمال العدوانية من كراهية وإبتزاز وتجارة إلكترونية غير مشروعة عبر الفضاء السيبراني[١]

وهذا ما دعا منظمة الأمم المتحدة في عام ٢٠١٥ لمحاولة وضع معايير لمواجهة الهجمات السيبرانية وتم الإتفاق عليها بالإجماع من جميع الدول في عام ٢٠٢١ من أجل إطار ملزم لجميع الدول التي تستخدم الفضاء السيبراني، أنه بصدور مبادئ السلوك السيبراني الوارد بتقرير الخبراء عام ٢٠٢١ لكافة الدول وفي ذلك التقرير الذي يعتبر إنطلاقاً من المبادئ الواردة بميثاق الأمم المتحدة وكذلك مبادئ القانون الدولي المستقرة في وجدان المجتمع الدولي لأنه جعل من القواعد القديمة نقطة إنطلاق للقواعد الجديدة أفضل كثيراً وأسرع ولسوف نعرض القواعد التقليدية القديمة على النحو التي رأت الأمم المتحدة الإستمرار في تطبيقها على الفضاء السيبراني على النحو التالي[٢]

---

[١] انظر د. عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، مكتبة المستقبل، مصر،عام ٢٠١٦، ص٩٦

[٢] ا.د سامر محي عبد الحمزة، مدى مساهمة الأمم المتحدة في تشكيل القواعد الدولية بالفضاء السيبراني، دراسة في ضوء تقرير الخبراء الدولي، كلية الحقوق، جامعة واسط، العدد ٦٧،ج١، ٢٠٢١،ص٢٣٣

المطلب الأول

مبدأ إحترام السيادة السيبرانية

سبق وأن عرضنا في أول دراساتنا ذلك الموضوع لأهمية تقرير الخبراء ٢٠٢١ وفيما إتجهت منظمة الأمم المتحدة أن تمد تطبيق القواعد المستقرة سلفاً والتي تم الإتفاق عليها من الأعضاء في الفضاء السيبراني بإعتبارها قواعد تقليدية نالت إتفاق الجميع منذ فترة طويلة وتم إقرارها من القضاء الدولي[١] وأمثلة ذلك مبدأ ضرورة حل المنازعات بالطرق السلمية عدم جواز إستخدام القوة في العلاقات الدولية ومبدأ عدم جواز التدخل في الشؤون الداخلية لأي دولة بما فيها الفضاء السيبراني الخاص بتلك الدولة ووفقاً لذلك المبدأ نص التقرير على أن الدول بمقتضى سيادتها للولايات الكاملة على البنية التحتية الخاصة بها والمتعلقة بتكنولوجيا الإتصالات والمعلومات داخل أراضيها ولها أن تضع القوانين والسياسات والآليات اللازمة لحماية البنية التحتية في هذا الشأن من أي خطر يهددها وفي النص إشارة إلى إمتداد سيادة الدول على كامل إقليمها بما فيه البنية التحتية لوسائل تكنولوجيا الإتصالات والقدرات السيبرانية لها[٢].

ومن أهم القواعد التقليدية المستقرة في وجدان الأمم المتحدة وأعضائها وكانت محل إجماع كافة المواثيق وهي تقوم على أساس أهمية إلتزام الدولة بمنع أي نشاط سيبراني عدائي ينطلق من أراضيها ضد دولة أخرى من قبل طرف ثالث ولا شك أن الأمر به بعض الصعوبة الشديدة في حاله التصدي لمنع أي هجمات سيبرانية خاصة لدى الدول التي لا تتمتع بإمكانيات تكنولوجية متقدمة تؤهلها لمعرفة وقوع هجوم أو مكانه أو القائم عليه أو مجرد تعقبه لذلك فإن الإتجاه هنا داخل الأمم المتحدة والمجتمع الدولي هو السماح لهذه الدولة بإمكانية طلب المساعدة من دولة أخرى أكثر تقدماً في هذا الشأن[٣].

قد تناول ذلك تقرير الخبراء عام ٢٠٢١ والذي نص على أن "الدولة بمقتضى سيادتها لها الولايات الكاملة على البنية التحتية لتكنولوجيا المعلومات والإتصالات داخل أراضيها ولها أن تضع السياسات والقوانين والآليات اللازمة لحماية البنى التحتية لتكنولوجيا الإتصالات من أي خطر يهددها" [٤]

---

[1] **U.N.G.A,2021, Doc (A/76/135), op. Cit**

[٢] **قرار الجمعية العامة للأمم المتحدة في ٢٩-٣-٢٠١٢ – وثائق الأمم المتحدة (13 L /20)**

[3] **Rule (17) of Tallin 2,0 Op Cit, P94**

[٤] **إنظر الفقرة ب من المادة ٧١ من مذكرة الأمين العام للأمم المتحدة في ٢٠٢١/٧/١٤**

ولا شك أن مبدأ السيادة المعمول به في القانون الدولي والذي بمقتضاه تكون سيادة الدولة على الإقليم البري وكذلك الإقليم الجوي والمياة الإقليمية ينبغي أيضاً أن تسري أحكامها على الفضاء السيبراني للدولة بإعتباره جزء من سيادة أي دولة، والنص السابق يمثل إعتراف صريح ومباشر على أحقية الدولة لسيادتها على إقليمها بما فيه البنى التحتية للقدرات التكنولوجية.

ومع ذلك لم يوضح النص السابق لبعض الأمور التفصيلية التي قد تكون محلا للنقاش في بعض الحالات مثل هل من حق الدولة أن تطلع على البيانات التي تمر بأراضيها أو لها الحق في تقييدها أو منعها.

ويرجع السبب في ذلك إلى الإختلاف في مفهوم وطابع تفسير السيادة في الفضاء السيبراني ففي حين ترى الصين وروسيا بأحقيه كل منهم بالسيادة المطلقة على الفضاء السيبراني بنفس قدر سيادتها الإقليمية مما حدد بعض فقهاء القانون الدولي بوصف الصين وروسيا في ذلك بأنهما "يريدا قبضة حديدية على الفضاء السيبراني" [١]

وفي الجانب الآخر ترى الولايات المتحدة الأمريكية وأوروبا أن سيادة الدولة يجب أن تكون لها حدود ومقيدة في الفضاء السيبراني بإحترام الحريات الأساسية ومن أهم تلك الحقوق الحق في الخصوصية وحرية التعبير [٢] وإتصالا بذلك المبدأ الخاص بإحترام السيادة السيبرانية لكافة الدول فإن تقرير الخبراء أيضاً تضمن " ألا تتدخل الدول بشكل مباشر أو غير مباشر بالشؤون الداخلية لدولة أخرى ويتضمن ذلك عدم التدخل في أي شأن عن طريق تكنولوجيا المعلومات والإتصالات، وأصبح لهذا المبدأ قيمة عظيمة مع إمكانية التأثير على السياسات الداخلية للدولة عن طريق التخريب أو الإختراق.

ولقد تضمنت إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية في المادة الخامسةعلى إلتزام جميع الدول الأطراف بالإلتزامات المنصوص عليها في هذه الإتفاقية بما ويتفق مع مبادئ المساواة في السيادة والسلامة الإقليمية للدول وهذه الإتفاقية أيضاً لم تتيح لأي دولة طرف أن تقوم في إقليم

---

[1] Lauren Zabierek and others, us-Russian contention in cyberspace are " Rules of the road Necessary of possible , June, 2021,p,41

[2] National security council (U.S) and United states executive Office of the president international strategy of cyberspace (national security council ,2011,p9

أي دولة أخرى طرف في هذه الإتفاقية بممارسة أي من الإختصاص القضائي او الولاية القضائية وأداء بعض المهام المنوط بها حصراً لسلطات هذه الدولة وفقاً لقانونها الداخلي[١]

ولعل أكبر واقعة في العصر الحديث في ذلك هو إتهام الولأيات المتحدة لروسيا بالتدخل في الإنتخابات الرئاسية الأمريكية عام ٢٠١٨ [٢].

المطلب الثاني
عدم إستخدام القوة
في العلاقات الدولية السيبرانية

وفقاً لهذا المبدأ يجب على الدولة عند إستخدامها لتكنولوجيا الإتصالات والمعلومات وإتساقاً مع ميثاق الأمم المتحدة أن تمتنع في علاقتها الدولية عن التهديد بإستخدام القوة وإستعمالها ضد السلامة الإقليمية أو الإستقلال السياسي لأي دولة أو بأي طريق يتعارض مع مقاصد وأهداف الأمم المتحدة والقوة المقصودة هنا تشمل أيضاً كافة سلوكيات وأشكال الإختراقات أو إستعمال البرامج الخبيثة من أجل تعطيل أو إتلاف أو محو البنية التحتية لأي دولة[٣].

مما لاشك فيه أن هذا المبدأ من المبادئ المستقرة في القانون الدولي منذ عقود طويلة نتيجة الويلات التي واجهتها البشرية عبر الحروب التي أهلكت العباد والمقدرات، وقد وردت تلك القاعدة في معظم الوثائق في كافة المنظمات سواء منظمات الإقليمية والدولية وعلى رأسها منظمة الأمم المتحدة التي وردت في تقرير خبراء ٢٠٢١ ووفقاً لتلك القاعدة فيما يخص الشأن السيبراني لا يمتنع أنه يمتنع في كافة العلاقات الدولية إستخدام القوة أو التلويح بإستخدامها أو حتى مجرد التهديد بها وهنا في الشأن السيبراني فأنه يمتنع إستخدام الفضاء السيبراني لأي دولة في أي من أساليب إستخدام القوة بأي طريقة تتعارض مع مقاصد الأمم المتحدة.

---

[١] انظر المادة الخامسة الفقرة الأولى من إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية الصادرة في ٢٧-١١-٢٠٢٤ (A/79/460)

[2] Us Department of justic Report on the investigation into Russian interference in 2016

[٣] انظر المادة ٧١- فقرة ج – مذكرة الأمين العام للأمم المتحدة في ١٤-٧-٢٠٢١

ونكاد نجزم أنه لا توجد دولة في العالم تعارض تلك القاعدة وأن كان الخلاف فقط هو حول المقصود بكلمة القوة في الفضاء السيبراني.

هل يعتبر التجسس في قرصنة الحسابات من قبيل إستخدام القوة

حاول فريق الخبراء التابع لمنظمة الناتو أن يضع معياراً لقياس مدى إعتبار الهجوم السيبراني هو إستخداماً للقوى من عدمه وهذا المعيار هو قيمة ومقدار الضرر المترتب على السلوك السيبراني أي أنه وفق هذا المعيار يجب أن ينتج عن الهجوم السيبراني ضرراً كبيراً تحقق بالفعل متمثلاً بقتل أو جرح أحد الأشخاص أو تدمير الممتلكات أو أي أو أي أحداث أضرار جسيمة للواقع عليه الهجوم السيبراني[١].

وفقاً لميثاق الأمم المتحدة فأنه يجب على كافة الدول في علاقاتها الدولية خاصة في جانب تكنولوجيا الإتصالات والمعلومات عن التهديد بأي شكل من أشكال القوة أو إستعمالها ضد السلامة الإقليمية أو الإستقلال السياسي لأي دولة أو بأي طريقة أخرى تتعارض مع مقاصد وأهداف الأمم المتحدة[٢].

وهنا المقصود بالقوة وكل أشكال إختراق السيبراني والإكتروني وكافة البرامج الخبيثة التي تتسبب في إتلاف أو تدمير أو تعطيل البنية التحتية لأي دولة.

ونحن نرى أن مبدأ حظر إستخدام القوة في العلاقات الدولية ولمزيد من الإنصاف ووصف دقيق لحقائق الأمور في المجتمع والعلاقات الدولية فأنه لا شك أن مصالح الدول الكبرى هي المسيطرة على كافة علاقاتهم بالدول الأخرى خاصة فيما يخص عالم تكنولوجيا المعلومات والإتصالات خاصة مع خصوصية الجريمة السيبرانية من صعوبة تحديد القائم بها أو تحديد مكان الولوج لقاعدة البيانات في حالات الجرائم السيبرانية خاصة مع إستحالة إثبات وإقامة الدليل على الجاني أو القائم بالجريمة السيبرانية أو مرتكبها وسهولة محو الدليل بمنتهى السرعة.

كل تلك الإعتبارات تجعل من إثبات الجريمة السيبرانية أو تعقب مرتكبيها أو إقامة الإثبات أو الدليل هو أمر في منتهى الصعوبة وأن لم يكن في الإستحالة خاصة وأن عالم تكنولوجيا المعلومات والإتصالات المعروف بالحداثة والتطور به خاصة على الدول الكبرى فقط وهي وحدها من تستطيع تطوير تلك التكنولوجيا والإستفادة القصوى منها مع صعوبة إثبات ذلك على تلك الدول

---

[1] **Tallin manual 20 on tge international law applicable to cyber operations, op. cit ,p333**

[٢] **المادة ٧١ الفقرة د من مذكرة الأمين العام للأمم المتحدة ١٤-٧-٢٠٢١**

فضلاً عن غياب إليه للمجتمع الدولي لجبر الضرر حتى ولو بالتعويض المالي للضرر الحادث نتيجة السلوك السيبراني الخبيث أو بمعنى آخر للجريمة السيبرانية بمعنى عام.

المطلب الثالث

مبدأ عدم التدخل

في الشؤون الداخلية لأي دولة

أورد تقرير الخبراء لعام ٢٠٢١ في ذلك الآتي[١] "وجوب ألا تتدخل الدول بشكل مباشر أو غير مباشر بالشؤون الداخلية لدولة أخرى بما في ذلك عن طريق تكنولوجيا الإتصالات والمعلومات لأن عمليات التأثير بالإختراق أو التخريب في مجال الأمن السيبراني هي من قبيل التدخل بالشؤون الداخلية بشكل مباشر وهو ما حدث عندما إتهمت الولايات المتحدة روسيا بالتدخل في الإنتخابات الأمريكية عام ٢٠١٦ عن طريق الإختراق لمنظومة البنيه التحتية لوسائل الإتصالات وتكنولوجيا المعلومات للولايات المتحدة

من أهم ما أنتهى إليه تقرير الخبراء ٢٠٢١ بأنه لا يجوز أن تتدخل أي دولة سواء كانت تدخل بشكل مباشر أو غير مباشر بالشؤون الداخلية لدولة أخرى بما في ذلك عن طريق تكنولوجيا المعلومات والإتصالات[٢]

كما أكدت على ذلك المادة ٥ من إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية بإلتزام جميع الدول الأطراف في الإتفاقية بما هو منصوص عليه في الإتفاقية بما يتفق مع مبدأ عدم التدخل في الشئون الداخلية لأي دولة أخرى طرف في الإتفاقية[٣]

فمن الملاحظ أنه مع التطور السريع والمتلاحق في عالم تكنولوجيا الإتصالات والمعلومات أصبحت إمكانية الولوج لقاعدة بيانات ومعلومات الشبكة العنكبوتية لأي دولة أمراً يسيراً سواء تم ذلك عن طريق الإختراق أو التخريب أو محو البيانات مؤثراً بذلك على السياسات الداخلية لأي دولة وقد يكون ذلك نشر شائعات بهدف تلبية الجبهة الداخلية للدولة علاوة على ذلك فأن التدخل في الشؤون الداخلية لأي دولة يعتبر مساساً بسيادة تلك الدولة وهو ما يخالف قواعد القانون الدولي[٤]

---

[١] د. عبد الفتاح مراد، جرائم الكمبيوتر والإنترنت، منشأة المعارف، ١٩٩٨، ص٣٧

[٢] المادة ٧١ الفقرة ج من مذكرة الأمين العام للأمم المتحدة ١٤-٧-٢٠٢١

[٣] انظر المادة الخامسة الفقرة الأولى من إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية الصادرة في ٢٧-١١-٢٠٢٤ (A/79/460)

[4] Rule 27 of Tallinn 2.0 ,op , cit P.142

وفي ذلك ينبغي زيادة أواصر التعاون الدولي بين كافة الدول لأن الفضاء السيبراني هو مجموعة مترابطة من الشبكات بحيث لا يمكن فصله عن بعضه البعض لذلك فإن تبادل المعلومات يساهم بشكل كبير في التصدي لأي سلوك سيبراني من شأنه التدخل بشكل مباشر أو غير مباشر في أي شأن داخلي لأي دولة فعلى الدول تبادل المعلومات بشكل أكبر حتى تستطيع حمأية نفسها وحمأية الآخرين في نفس الوقت من أي تدخل عبر الشبكة العنكبوتية لأي من هياكلها السيبرانية وكذلك حمأية البنية التحتية لها

فمن المعلوم لنا أننا نعيش في عصر تكنولوجيا المعلومات والإتصالات بشكل متسارع وأصبحت كافة بيانات ومعلومات الدول كافة محفوظة على شبكتها العنكبوتية بما في ذلك البيانات العسكرية والإقتصادية والمرافق الحيوية من الطاقة وغيرها فأن الوصول لأي منها عبر أي نشاط سيبراني خبيث لأي دولة يؤدي لخسائر مفادها لا يمكن تعويضها خصوصاً وأن الجناة في تلك الحالات مجهولين تماماً وقد يصعب تعقبهم أو إقامة الدليل أو الإثبات نحوهم[1]

المطلب الرابع

مبدأ حل المنازعات بالطرق السلمية

مقتضى هذا المبدأ أن على الدول كافة أن يكون حل أي نزاع في الفضاء السيبراني فيما بينهم بالطرق السلمية وتحديداً وفقاً لميثاق الأمم المتحدة الذي يأتي في جوهرهم ضرورة حل أي نزاع سواء عسكري أو غيره وفقا لمبادئ القانون الدولي ومن ثم ينسحب حكم نفس الميثاق إلى المنازعات السيبرانية بإعتبارها قد تؤدي لخسائر تفوق النزاع العسكري بين الدول

وهو ما أوجبه التقرير سالف الذكر من أنه على الدول الأعضاء في حالة أي نزاع دولي خاص بتكنولوجيا الإتصالات والمعلومات أن يتم تسويته بالشكل والإسلوب السلمي ووفق الطرق الدبلوماسية والسياسية الواردة في المادة ٣٣ من ميثاق الأمم المتحدة من وسائل مثل التحكيم والتحقيق والمفاوضة بين الأطراف أو حتى التسوية القضائية للنزاع[2].

وقد تتنوع تلك الطرق من تحكيم دولي أو مفاوضة أو تحقيق أو وساطة أو توفيق بحسب الأحوال، وقد تكون التسوية عبر محكمة العدل الدولية بوصفها الجهة القضائية ذات الإختصاص بالتعرض للنزاع بين الدول وقد يكون هناك الطريق الخاص باللجوء للوكالات والمنظمات الإقليمية

---

[1] **Rule 17 of Tallinn 2,0 ,op ,cit p 99**

[2] **انظر المادة ٧١ – فقرة د– مذكرة الأمين العام للأمم المتحدة في ٢٠٢١/٧/١٤**

مثل حالة أن تلجأ إحدى الدول العربية لجامعة الدول العربية إبتغاء عرض أي نزاع من دولة عربية أخرى عضواً بنفس المنظمة [١]

وقد أوجب تقرير الخبراء لعام ٢٠٢١ على الدول الأعضاء في أي نزاع خاص بالتكنولوجيا الخاصة بالإتصالات والمعلومات قد يعرض إستمرار النزاع إلى تهديد السلم والأمن الدوليين للخطر وأن تسعى الدول للطرق الدبلوماسية والقنصلية لحل النزاع بالطريق الدبلوماسي كما ورد في المادة ٣٣ من ميثاق الأمم المتحدة[٢]

على أنه يجب ملاحظة أنه ليست كافة النزاعات تستدعي الحل بالطريق السلمي طالما لم تهدد السلم والأمن الدوليين بالنسبة للنزاعات السيبرانية وفي ذلك إتجه فريق الخبراء التابع لحلف الناتو إلى تقرير مثلا لذلك مثل حالة أن تجد دولة أن دولة أخرى تقوم بنشاط سيبراني يهدف إلى التجسس عليها وضد مواقعها الإلكترونية فيمكن في تلك الحالة إستدعاء سفير الدولة القائمة بعملية التجسس وإبلاغه إحتجاج رسمي ضد عمليات التجسس التي تقوم بها الدولة التابع لها السفير [٣]

لأن ذلك لا يعد نزاعاً يرقى إلى تهديد السلم والأمن الدوليين وبالتالي لايستوجب ضرورة حله بالطرق السلمية[٤]

---

[١] **انظر الفصل السادس من ميثاق الأمم المتحدة والنظام الأساسي لمحكمة العدل الدولية – نيويورك ١٩٩٤**

[2] **Rule 27 of Tallinn 2.0 op cit p.142 and Article 9 of Shanghi Code of conducts at UNG.20.15 Doc(A/69/723)**

[3] **Tallin manual 2.0 on the international law Application to cyber operations op.cit p.3**

[4] **Tim Amaurer cyber norm Emergence at the united nation – An analysis of the uns activites regarding – paper ,2011**

المبحث الثاني
المبادئ الحديثة للأمم المتحدة
لتحقيق الأمن السيبراني

تمهيد وتقسيم:

لا شك أن النمو والتطور الرقمي لتكنولوجيا المعلومات والإتصالات بات جذرياً في حياة البشر لا سيما في العقدين الأخيرين وليس البشر فحسب إنما إمتد للشركات والمؤسسات بمختلف أنشطتها بهدف رفاهية الإنسان وراحته وإخراجه من الفقر وكذلك تمكين الشعوب من التواصل السريع عبر الطرق الحديثة كما أنه يجعل من العالم بشكل عام مترابط ومتصل فيما بينهم ويدعم العولمة من خلال زيادة قدرات التواصل والوصول للأسواق الحرة والتجارة العالمية وزيادة معدلات الإستثمار

وكما كان الإعتماد على الفضاء الإلكتروني أو السيبراني يزداد بوتيرة متسارعة فأنه في المقابل زادت حدة الأنشطة السيبرانية الغير مشروعة والحوادث السيبرانية وكذلك إستهداف البنى الأساسية للدول وهو عالم متسع رحب وبلا قانون حاكم ومسيطر على النشاط السيبراني أو على النشاط في الفضاء السيبراني ونحن هنا نحاول أن نلتمس الطريق بعيداً عن المبادئ التقليدية للسلوك السيبراني والتي نلقي عليها الضوء نحو معايير حديثة تواكب الحداثة المضطردة في عالم تكنولوجيا الإتصالات والمعلومات من أجل تحديد السبيل نحو تطبيق القانون الدولي على سلوكيات الدول في الفضاء السيبراني، ولسوف نتناول ذلك بشيء من التفصيل من خلال معايير الأمم المتحدة الحديثة التي تشكل جزءاً من إطار الأمم المتحدة للسلوك المسؤول في الفضاء السيبراني[1]، وأيضاً من خلال إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية ٢٠٢٤

وإتفاقاً مع ما يشهده العقدين الأخيرين من صدور العديد من القواعد الدولية والمبادئ التي إستقر عليها المجتمع الدولي بهدف تنظيم سلوك الدول في الفضاء السيبراني بشكل منظم وكل ما تهدف إليه تلك المبادئ والقواعد التي يسعى المجتمع الدولي لإقرارها سواء عن طريق جهود منظمات

---

[1] Bart Hogeveen, Sydney recommendations– practical futures for cyber confidence building in the ASEAN region, 18 september, 2018. aspi.org.au/report/Sydney, C20/36 , C20/inf/11

وكذلك انظر الجمعية العامة للأمم المتحدة – فريق الخبراء الحكوميين المعني بالتطورات في مجال تكنولوجيا المعلومات والإتصالات في سياق التعاون الدولي. الأمن، الفقرة١٠ يوليو ٢٠١٥، A/174.22

دولية كمنظمة الأمم المتحدة او منظمات إقليمية او حتى إتفاقيات ثنائية أو جماعية إقليمية أو دولية جميعاً تهدف إلى وضع معايير في الفضاء السيبراني بشكل لا يهدد السلم والأمن الدولي بأي وجه من الوجوه

ما هو الأثر المنطوي على تنفيذ تلك المعايير الدولية السالفة البيان[1]

من ناحية البحث في الفقه القانوني لذلك نجد أن بعض فقهاء القانون الدولي قد إعتبر تلك المعايير هي من قبيل الأعراف الدولية وهي ملزمة بطبعها لأنها تطورت وإستمرت وأصبحت من العرف الدولي الذي لا يجوز تجاهله في أي سلوك سيبراني يصدر منها[2]

وإتجه فريق آخر من فقهاء القانون الدولي أنها –تلك المعايير السابقة– من قبيل القواعد الدولية المرنة أي أنها قواعد استرشد بها المجتمع الدولي في ممارساته السيبرانية فهي تحمل صفات القاعدة القانونية وتلك القواعد الدولية المرنة هو مصطلح جديد على الساحة الدولية يشير إلى وصف قواعد دولية لم تنشأ بالطرق التقليدية مثل المعاهدات والعرف المستقر في الوجدان الذي يحمل طابع الإلزام المعنوي وإلا كان إستهجان المجموع لمن يخالف ذلك العرف[3]

أما بالنسبة للأثر المنطوي على تلك المعايير فأنه يجب أن يتم على المستويات التالية[4]

المستوى الأول التأييد السياسي وذلك من خلال المشاركة في التصويت لصالح كافة القرارات ذات الصلة في الجمعية العامة للأمم المتحدة

المستوى الثاني أن تعمل الدول على دمج تلك المعأيير وإدراجها ضمن التشريعات الخاصة بها وكافة الإستراتيجيات الوطنية

---

[1] Paul P.polanski, cyber space Anew branch of International Customary law Computer law, security. Review Volume33, Issue3,June 2017, P2

[2] Tim maurer " Cyber norm Emergen of the United Nation " discussion paper,2011

[3] Gary Brown and Keire poellet op. cit p.128

[4] Andrew T.Guzman and Timothy l.meyer international soft law journal of legal analysis spring 2010, vol 2 , No 1 ,P 71

المستوى الثالث يمكن للدول أن تثبت جديتها في تنفيذ تلك المعأيير من خلال الإعلان عن ممارستها وقدرتها المؤسسية وإجراءاتها لأن تلك الممارسات يمكن أن تعطي إنطباعاً ودليلاً فعلياً وجدياً في الإلتزام الدولة بتلك المعايير

ويثور هنا سؤال من الباحث هل يقع عبء الإلتزام بتنفيذ تلك المعايير على الحكومات فقط وبطبيعة الحال فإن المسؤولية الأولى والأخيرة في مدى الإلتزام بتلك المعايير ومراعاة تنفيذها يقع على عاتق حكومات الدول غير أن الإستعداد الحكومي لذلك غير كاف تماماً فيجب أيضاً الإلتزام الكامل من منظمات المجتمع المدني وكافة المجتمعات التقنية والأكاديمية المرتبط عملها بشبكة الإنترنت وبالإضافة الى أهميه قدرة الحكومات على إتباع منهج حكومي شامل وعام ومستمر ودقيق

المطلب الأول

التعاون الدولي وتبادل المعلومات

من منطلق عدم محدودية المجال السيبراني بحدود الدول بما يجعل عمليات التعقب والتحديد تتسم بصعوبة بالغة على دولة واحدة لذلك فإن مواجهة الخطر السيبراني تستلزم تكاتف وتعاون بين كافة الدول في ذلك وتأكيدا لهذا المبدأ فقد تم إطلاق (عصر الاعتماد الرقمي المتبادل) على المرحلة الراهنة من قبل الأمم المتحدة عام ٢٠١٩ أن ذلك هو الطريق الامثل لمواجهة تحديات الفضاء السيبراني ويمكن أن يتخذ ذلك التعاون أحد الصور أو الأشكال الآتية.

١- وضع آليات وتدابير مشتركة بين الدول لزيادة معدلات الأمن السيبراني

٢- التعاون الدولي في مقاضاة المسؤولين عن إستخدام المجال السيبراني في أعمال غير مشروعة " أغراض الاجرامية أو إرهابية"

٣- على الدول الإستجابة لطلبات المساعدة بكافة لكافة الدول التي تتعرض للخطر السيبراني

٤- ضروره تبادل المعلومات الخاصة بالوسائل الوطنية المتبعة لإكتشاف وتحديد المخاطر السيبرانية وكيفية مواجهتها.

ويعد من أهم المبادئ التي تناولتها كافة المواثيق ذات الصلة بالشأن السيبراني نظراً للطبيعة الخاصة للجريمة السيبرانية العابرة للحدود الدولية والتي لا تقتصر على دولة بعينها أو إقليم محدد فإن أهميه تظافر جهود جميع الدول في شأن أهمية التعاون الدولي كونه مجموعة مترابطة من الشبكات التي لا يمكن فصل البعض عن الآخر لذلك فإن عمليات تبادل المعلومات والبيانات

والخبرات من كافة الدول وفي غأية الضرورة خاصة فيما يتعلق بالأنشطة الإرهابية او الإجرامية فيكون تبادل المعلومات بين الدول هو الحاكم والحامي للدول وللآخرين في نفس الوقت

وفيما يخص مبدأ التعاون الدولي في شأن مكافحة الجريمة السيبرانية لقد تضمنت إتفاقية الأمم المتحدة في مادتها الخامسة والثلاثون المبادئ العامة للتعاون الدولي بأن تتعاون الدول فيما بينها وفقاً لأحكام هذه الإتفاقية وكذلك الأحكام السابقة من الإتفاقيات والصكوك الدولية المتعلقة بالتعاون الدولي في المسائل الجنائية وكذلك المنصوص عليها في القوانين الداخلية مثل التحقيقات والإجراءات القضائية والملاحقات التي تتعلق بالأفعال الإجرامية المنصوص عليها في هذه الإتفاقية وجمع الأدلة في الشكل الإلكتروني عن الإفعال الإجرامية الخبيثة الغير مشروعة المنصوص عليها في هذه الإتفاقية والحصول على هذه الأدلة والإحتفاظ بها وتبادلها بين الدول الأطراف في الإتفاقية وكذلك أيضاً جمع الأدلة الخاصة بأي جريمة خطيرة بما في هذه الجرائم المنصوص عليها في إتفاقيات الأمم المتحدة وبروتوكلاتها السابقة النافذة وقت إعتماد هذه الإتفاقية وكذلك أيضا إعتمدت ونصت في مسائل التعاون الدولي على إستيفاء شرط إزدواجية التجريم وإعتبر ذلك الشرط مستوفي في حال وجوده في قوانين إحدى الدول أطراف هذه الإتفاقية وكذلك أيضا أقرت التعاون في تسليم المطلوبين من حيث إنطباق المادة على الأفعال الإجرامية الغير مشروعة في الفضاء السيبراني وفقاً لهذه الإتفاقية عندما يكون الشخص موضوع طلب التسليم موجود في إقليم الدولة الطرف متلقية الطلب والشرط الأساسي في هذه الحالة أن الجريمة التي يلتمس بشأنها التسليم تكون خاضعة للعقاب بموجب القانون الداخلي للدولتين طالبة التسليم والمطلوب منها التسليم وكذلك أيضاً المساعدة القانونية أقرت هذه الإتفاقية في المادة ٤٠ بأن تقدم الدول الأطراف في الإتفاقية المساعدة الى بعضها البعض على أوسع نطاق ممكن من التحقيقات والملاحقات القضائية والإجراءات التي تتعلق بالأفعال الغير مشروعة المنصوص عليها في هذه الإتفاقية وجمع الأدلة أيضاً في شكل إلكتروني وتقديم المساعدة الى أقصى مدى ممكن بمقتضى قوانين الدولة الطرف التي تتلقى طلب المساعدة وفقاً لمعاهداتها وإتفاقياتها والترتيبات ذات الصلة الخاصه بذلك ويجوز أيضاً طلب المساعدة القانونية المتبادلة التي تقدم وفقاً لهذه المادة في الأغراض الآتية

ومنها الحصول على الأدلة وأقوال من الأشخاص وتبليغ المستندات وتنفيذ عمليات التفتيش والحجز والتجميد وكذلك جمع بيانات الحركة وفحص الأشياء والمواقع وتقديم أصول المستندات وتقديم المعلومات والأدلة وتقييمات الخبراء ومسؤول الأشخاص توعية في الدولة الطرف الطالبة لذلك

وكذلك أيضاً إحالة المعلومات المتعلقة بالمسائل الجنائية إلى سلطة مختصة في دولة طرف مع الدولة الأخرى[١]

وكذلك جاءت التوجيهات أو المعايير الحديثة للأمم المتحدة في هذا الشأن بالحكم التالي في حالة وجود حوادث تتعلق بتكنولوجيا المعلومات والإتصالات ينبغي مراعاة الآتي:-

المعيار الأول[٢] أنه من أهم أهداف الامم المتحدة الحفاظ على السلم والأمن الدوليين وعليه ينبغي.

ا-وضع وتطبيق التدابير التى تهدف إلى زيادة الإستقرار والأمن في إستخدام تكنولوجيا المعلومات والإتصالات .

ب- منع ممارسات تكنولوجيا المعلومات والإتصالات التى يعترف بأنها ضارة وقد تشكل تهديدات للأمن والسلم الدوليين .

والنص المتفق عليه(المعيار) الرابع[٣] الصادر عن الجمعية العامة للأمم المتحدة أكد على التعاون الدولي من حيث أنه ينبغي للدول أن تدرس أفضل السبل لتحقيق الآتي:

١- التعاون في تبادل المعلومات ومساعدة بعضها البعض

٢- ملاحقة الإستخدام الخبيث لتكنولوجيا المعلومات لأغراض إرهابية او إجرامية

٣- إتخاذ وتنفيذ مجموعة تدابير تعاونية أخرى لمعالجة مثل هذه التهديدات

وفي سبيل دعم عمليات التعاون الدولي في الشأن السيبراني نجد أن هناك عدد من المنتديات والقرارات والإتفاقيات والعمليات التي صدرت نعرض لأمثلة منها

ا- قرار الجمعية العامة للأمم المتحدة بشأن تعزيز المساعدة التقنية وبناء القدرات لتعزيز التدابير الوطنية والتعاون الدولي[٤]

---

[١]انظر المادة (٣٥،٣٧، ٤٠) من إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية الصادرة في ٢٧-١١-٢٠٢٤ (A/79/460)

[٢]إنظر المعيار الأول من معايير الأمم المتحدة للسلوك السيبراني للسلوك المسئول للدولة في الفضاء الإلكتروني – إرشادات بشأن التوضيح للدول الأعضاء في رابطة دول جنوب شرق آسيا، مارس ٢٠٢٢

[٣]إنظر المعيار الرابع من معايير الأمم المتحدة للسلوك السيبراني للسلوك المسئول للدولة في الفضاء الإلكتروني – إرشادات بشأن التوضيح للدول الأعضاء في رابطة دول جنوب شرق آسيا، مارس ٢٠٢٢

[٤] قرار الجمعية العامة للأمم المتحدة رقم ٧٤/١٧٣ بشأن تعزيز المساعدة التقنية وبناء القدرات لتعزيز التدابير الوطنية والتعاون الدولي

ب – توصيات مجموعة الخبراء والحكوميين الدولية المفتوحة العضوية لإجراء دراسات شاملة لمشكلة الأمن السيبراني[1] بالإضافة إلى إتفاقية بودابست ٢٠٠١

ج– قرار الجمعية العامة من أجل معالجة التهديدات التي يفرضها إستخدام الإرهابيين والجرائم لتكنولوجيا المعلومات والإتصالات والتعاون لمواجهتها[2]

وكذلك النص المتفق عليه (المعيار) الثامن والذي يتضمن أنه ينبغي على الدول الإستجابة لطلبات المساعدة التى تطلبها دولة أخرى تتعرض للإعتداءات السيبرانية الخبيثة والغير مشروعة على بنيها التحتية الحيوية في مجال تكنولوجيا الإتصالات والمعلومات وكذلك الإستجابة لطلبات تخفيف النشاط السيبراني الخبيث والغير مشروع الذي يستهدف البنية التحتية لدولة أخرى قادماً من أراضيها بما لا يخالف مبدأ السيادة وينبغي على الدولة التى طلبت منها المساعدة أن تلبي ذلك الطلب بما يتناسب مع الظروف القائمة ووفقاً ووفقاً للإتفاقيات الثنائية أو الجماعية بين هذه البلاد وتحديد إجراءات طلب المساعدة والوسائل وطرق الإتصالات وتقديم المعلومات الكافية والدقيقة عن الحوادث لحل الأزمات وتيسير التعاون[3]

---

[1] انظر الجرائم الإلكترونية قرار الجمعية العامة للأمم المتحدة ٦٥/٢٣٠

[2] قرار الجمعية العامة رقم ٢٤٧/ ٧٤ بشأن مكافحة إستخدام تكنولوجيا الإتصالات والمعلومات لأغراض خبيثة

[3] Bart Hogeveen, Sydney recommendations– practical futures for cyber confidence building in the ASEAN region, 18 september ,2018. aspi.org.au/report/Sydney

فيما يلي نعرض لبعض صور هياكل التعاون الدولي في مجال الأمن السيبراني[1]

وذلك من خلال إلزام دول آسيا بالتعاون الدولي في منع الجريمة السيبرانية مثل رابطة دول جنوب شرق آسيا والإعلان الخاص بشأن الجريمة العابرة للحدود عام ١٩٩٧ وكذلك منتدى الآسيان الإقليمي بشأن التعاون في مكافحة الهجمات السيبرانية وإستخدام الإرهابيين للفضاء السيبراني عام ٢٠٠٦ وكذلك رابطة دول جنوب شرق آسيا خطة العمل لمكافحة الجريمة للعابرة للحدود في عام ٢٠١٠ و ٢٠١٧ و٢٠٢٥ وكذلك أيضاً العديد من المنظمات والشبكات الحكومية الدولية متعددة الأطراف التي تعالج التعاون الدولي في مكافحة الجريمة السيبرانية وإستخدام الإرهابيين للإنترنت

الجرائم الإلكترونية مثل جرائم الإنترنت في الفلبين مركز ضد الاطفال الإنتربول رابطة جنوب شرق آسيا تنمية القدرات مكتب العمليات كبار المسؤولين في رابط جنوب شرق آسيا مجموعة العمل المعنية بالجرائم الإلكترونية، ولمكافحة الإرهاب مثل نداء كراستشيرش للعمل ومنتدى الإنترنت العالمي مكافحة الإرهاب مركز جاكرتا للقانون التعاون في مجال تنفيذ التكنولوجيا ضد الإرهاب وإقليم جنوب شرق آسيا مركز مكافحة الإرهاب وكبار المسؤولين في رابطة جنوب شرق آسيا مجموعة العمل المعنية بمكافحة الإرهاب.

ونؤكد دائماً على أهمية تعزيز وزيادة التعاون الدولي من كافة الدول سواء في الشرق الأوسط او الغرب او الولأيات المتحدة الأمريكية في سبيل محاصرة كافة أوجه الإستخدام الخبيث لأي من شبكات تكنولوجيا المعلومات والإتصالات دوماً

ونحن نرى أنه لما كان التعاون الدولي في مجال الامن السيبراني بهذه الأهمية القصوى من كونه أقوى الآليات الخاصة بمكافحة وكشف وضبط الجريمة السيبرانية او بمعنى آخر أي سلوك سيبراني خبيث فأنه على كافة الدولة المجتمع الدولي عمل المزيد من الإتفاقيات إبرام المزيد من الإتفاقيات الثنائية والجماعية ومواثيق تربط بين كافة الدول لضمان أكبر قدر من التعاون وتبادل المعلومات وكذلك يمكن أيضاً زيادة آفاق معاهدات تسليم المجرمين بين كافة الدول نظراً لأن الفاعلين او الجناة قد يكونوا في دولة ويكون نشاطهم الآثم السيبراني في دولة أخرى تماماً لذلك فأن محاصرة كافة أوجه السلوك السيبراني غير المشروع ومحاصرة الجناة أمر لا يمكن تحقيقه بشكل فعال إلا من خلال ترسيخ وزيادة وفعالية التعاون الدولي بشكل عام في كل زمان ومكان

---

[1]إنظر معايير الأمم المتحدة للسلوك السيبراني للسلوك المسئول للدولة في الفضاء الإلكتروني – إرشادات بشأن التوضيح للدول الأعضاء في رابطة دول جنوب شرق آسيا، وكذلك الجمعية العامة للأمم المتحدة – فريق الخبراء الحكوميين – المعني بتعزيز السلوك السيبراني في سياق الأمن الدولي مارس،٢٠١٤/٧٥/ A

المطلب الثاني

مبدأ التحقيق في الجرائم السيبرانية

فحوى وجوهر هذا المبدأ أنه عند تعرض أي دولة لهجوم سيبراني فأن الدولة المعتدى عليها يجب أن تقوم بإجراءات التحقيق الشامل بشأن ذلك الهجوم ليكون الإتهام موجهاً بدلائل وأسانيد واضحة وواضح فيها الإتهام وملامحه وسماته بدلائل وأسانيد موضحاً بذلك الإتهام ملامح وسمات ذلك الهجوم وحجمه ونطاق الضرر الناشئ عنه، وهدفنا هنا في هذا المبدأ منع الإتهامات غير الدقيقة وغير التقنية ومنع الإدعاء بغير دليل حتى لا يكون سريعة لمهاجمة دولة ما بما يهدد الأمن والسلم الدوليين في العلاقات الدولية بين الدول

ويعتبر هذا المبدأ من أهم المبادئ المعمول بها في العلاقات الدولية فيما يخص أي هجوم سيبراني يقتضى ذلك المبدأ أن تقوم أي دولة قبل توجيه أي إتهام لدولة أخرى بشأن هجوم سيبراني ضدها وذلك بمشاركة كافة سلطاتها المختصة ومن لهم الخبرة والدراسة بالأمور الفنية والتقنية والتكنولوجية وكذلك تبادل المعلومات مع أي دولة أخرى في هذا الشأن إن كان ذلك منتجاً في تحديد السمات التقنية للحادث السيبراني ونطاقه وحجم تأثيره[١].

ولا شك أن الأهمية الشديدة لهذا المبدأ والسبب في إقراره بحيث أنه أصبح قاعدة ملزمة في هذه الحالات هو تعقيد وخصوصية الحوادث السيبرانية وصعوبة تتبعها وتعقبها بشكل سهل وسريع ومعرفة الجناة وتحديدهم لسهولة الطمس وازالة الدليل في العالم السيبراني غير المحدود[٢].

لذلك جاء هذا المبدأ ليفرض على الدول بشكل قاطع ضرورة التأكد من طبيعة الهجوم لأن إغفال ذلك المبدأ وعدم العمل به ومراعاته قد يفتح الباب للإدعاء بوجود هجوم على غير الحقيقة لإتخاذه ذريعة لمهاجمة دولة أخرى مما يشكل تهديداً للسلم والأمن الدوليين

وعلى الجانب الآخر نجد أن قرار الجمعية العامة للأمم المتحدة رقم ١٩٩/ ٥٨ قد تناول مسألة أهمية التحقيق في مسائل الحوادث السيبرانية في الفقره ٩ من المادة المذكورة حينما نص على

---

[١] **انظر الفقرة ٢٢ من مذكرة الأمين العام للأمم المتحدة في ٢٠٢١/٧/١٤ الوثيقة (A/76/135)**

[2] **U.N.G.A 2021, Doc (A/76/135), op. cit,p.20**

- على الدولة أن يكون لديها قوانين موضوعية وإجرائية كافية وموظفون مدربون لتمكين الدولة من التحقيق في الهجمات السيبرانية على البنية التحتية للمعلومات الحيوية وملاحقة مرتكبيها وتنسيق مثل هذه التحقيقات مع الدول الأخرى حسب الإقتضاء والحاجة
- كذلك تناولت الفقره ٧، ٨ من القرار رقم ١٩٩/ ٥٨ الصادر عن الجمعية العامة للأمم المتحدة

على الدولة إجراء التدريبات والتمارين لتعزيز الإستجابة وإختيار خطط الإستمرارية والطوارئ في حالة وقوع هجوم على البنى التحتية للمعلومات وتشجيع أصحاب المصلحة على المشاركة في أنشطة مماثلة، ولا يخفى من أهميه التدريب المستمر والمتابعة المتواصلة لكل جديد وتحديثات في عالم تكنولوجيا المعلومات والإتصالات للوقوف على تفاصيل وحقائق السلوك السيبراني والوصول إلى الجناة الفعليون في أي حادث سيبراني وتقديم الدليل الفني والتقني المعزز للإتهام

وقد أكدت ذلك المادة ٤٨ من إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية على أن جميع الدول الأطراف في هذه الاتفاقية ينبغي عليها إبرام إتفاقيات أو معاهدات ثنائية أو متعددة الأطراف تتيح للسلطات المختصة أن تقوم بإنشاء هيئات تحقيق مشتركة بين هذه الدول للتحقيق في الأفعال الغير مشروعة والخبيثة وفقاً لهذه الإتفاقية الخاصة بالتحقيقات الجنائية أو الملاحقات أو جميع الاجراءات والتدابير القضائية في دولة واحدة او أكثر من دولة وفي حالة عدم وجود إتفاقيات أو معاهدات ثنائية او متعددة او ترتيبات او تنظيمات بين هذه الدول يجوز في هذه الحالة إجراء التحقيقات المشتركة في هذه الجرائم بالاتفاق بين كل من هذه الدول في كل حالة على حده وان تكفل الدول الاطراف بذلك الإحترام الكامل لسيادة الدولة التي تجري التحقيقات على أراضيها[١].

أما فيما يخص مبدأ التحقيق في الجرائم السيبرانية الوارد في معايير السلوك للأمم المتحدة السابق ذكرها والتي أقرتها منظمة الأمم المتحدة كمعايير حديثة للسلوك السيبراني في الفضاء السيبراني من خلال (المعيار الثاني)[٢] والذي يتضمن أنه في حالة وقوع حوادث تتعلق بتكنولوجيا المعلومات والإتصالات ينبغي للدول أن

١- يؤخذ في الإعتبار جميع المعلومات ذات الصلة بما في ذلك السياق الأوسع للحدث

---

[١] انظر المادة الثامنة والأربعون من إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية الصادرة في ٢٧-١١-٢٠٢٤ (A/79/460)

[٢] إنظر المعيار الثاني من معايير الأمم المتحدة للسلوك السيبراني للسلوك المسئول للدولة في الفضاء الإلكتروني – إرشادات بشأن التوضيح للدول الأعضاء في رابطة دول جنوب شرق آسيا، مارس ٢٠٢٢، والجمعية العامة للأمم المتحدة (الأمن ٧/١٧٤٠٢٢/يوليه الفقرة ١٠

٢- عمليات التحديات الخاصة بالإسناد في بيئة تكنولوجيا المعلومات والإتصالات

٣- طبيعة ومدى العواقب والنتائج

ووفقاً للنص السابق فأنه يجب على الدول مراعاة الحذر في توجيه الإتهام بدولة أخرى وذلك في حالة تنفيذ او تنظيم أفعال غير مشروعة لأن تحميل دولة أخرى مسؤولية إرتكاب عمل سيبراني خبيث قائم على إعتبارات تقنية وقانونية وسياسية معقدة، وعلى الدول التي تتعرض لأي هجوم وكافة السلطات المختصة ذات الصلة أن تستفيد من جميع الخيارات السياسية والدبلوماسية والقانونية وتبادل المعلومات لتسوية الخلافات والنزاعات ويتطلب الإلتزام بتلك القاعدة ما يلي[١]

١-أن تقوم الدولة بإنشاء وتعزيز الهياكل الوطنية ذات الصلة

٢- وضع السياسات والعمليات والأطر التشريعية المتعلقة بتكنولوجيا المعلومات

٣- كافة أشكال التنسيق والمفارقة مع الجهات ذات الصلة

٤-وسوف نقوم بتوضيح مفهوم الإسناد أنه هو إسناد المسئولية عن فعل ما إلى شخص ما، وفي حالة إسناد الحوادث السيبرانية يعني التوصل إلى قرار سياسي بتحميل دولة أو جهة فاعلة غير حكومية مسئولية الحادث السيبراني بشكل عام أو بشكل خاص

ولقد تضمنت إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية إسناد المسئولية عن الأفعال المجرمة في المادة ١٨ في فقرات متتالية ومنها أن كل دولة تعتمد ما قد يلزم من تدابير تتفق مع المبادئ القانونية لتقرير مسؤولية الأشخاص الإعتباريين عن مشاركتهم في الأفعال الغير مشروعة والخبيثة وفقاً لما ورد بهذه الإتفاقية وهذه المبادئ القانونية للدول الأطراف في الإتفاقية ومن الممكن أن تكون مسؤولية الأشخاص الإعتباريين مسؤولية جنائية أو مدنية أو إدارية وألا تخل هذه المسؤولية بالمسؤولية الجنائية للأشخاص الطبيعين الذين إرتكبوا هذه الجرائم وأيضا تكفل كل الدولة الطرف في الإتفاقية إخضاع جميع الأشخاص الإعتباريين الذين تلقي عليهم المسؤولية وفقاً لهذه المادة إلى عقوبات جنائية أو عقوبات مدنية أو مادية فعالة ورادعة[٢]

---

[1]Florian J. Egolf – Max Smeets 'Publicly Attributing Cyber Attacks: A Framework', Journal of Strategic Studies. external page Chesney, 2021, https://doi/10.1080/01402390.2021.1895117

[٢]انظر المادة الثامنة عشر من إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية الصادرة في ٢٧-١١-٢٠٢٤ (A/79/460)

وكذلك تضمنت المادة ١٩ على إسناد المسؤولية في حالة المشاركة والشروع فأقرت أن جميع الدول الأطراف في الإتفاقية بأن تعتمد تدابير تشريعية وقانونية تجرم وفقاً للقوانين الداخلية الخاصة بها إرتكاب الشخص الفعل عن عمد كطرف شريك أو مساعد في أي فعل من الأفعال الغير مشروعة والجرايم السيبرانية وأن كل طرف يقر التدابير التشريعية والتدابير الأخرى بما يتفق مع القانون الداخلي لتجريم أي شروع يرتكب عن طريق العمد في الأفعال المجرمة في هذه الإتفاقية ويجوز لكل دولة طرف ان تقر أيضا ما يلزم من تدابير ومن قوانين لتجرم طبقاً للقانون المحلي الإعداد أو التجهيز الذي يرتكب عمدا لفعل مجرم أو الأعمال التحضيرية وكل صور الشروع أوالمساعدة أو المساهمة[١] .

وواقع الأمر أن جوهر هذا المبدأ أو تلك القاعدة هو دعوة الدول كافة الى ممارسة ضبط النفس عند النظر في إسناد المسؤولية عن الحادث السيبراني لدولة أخرى ولا يعتد بالإستنتاجات المتسرعة أو غير الدقيقة[٢]

---

[١] انظر المادة التاسعة عشر من إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية الصادرة في ٢٧-١١-٢٠٢٤ (A/79/460)

[٢] وزارة الإتصالات والمعلومات، التقرير العام للجنة التحقيق في الهجوم الإلكتروني على الخدمات الصحية في سنغافورة، حكومة سنغافورة، ٢٠١٩

المطلب الثالث

مبدأ إحترام حقوق الإنسان

في الفضاء السيبراني

(الحق في التعبير والحق في الخصوصية)

أكدت منظمة الأمم المتحدة أنه على جميع الدول أن تلتزم بقرارات مجلس حقوق الإنسان في إطار الإستخدام الآمن لتكنولوجيا المعلومات والإتصالات وإحترام قرارات الأمم المتحدة بشأن مراعاة الحق في الخصوصية في المجال السيبراني والرقمي وكذلك الحق في التعبير عن الرأي لضمان الإلتزام الكامل بحقوق الإنسان بشكل عام وحق في الخصوصية وحق التعبير بشكل خاص

ولقد تضمنت إتفاقية الأمم المتحدة لمكافحة الجريمة والسيبرانية في الباب الثاني في المادة السادسة وإختصت بذلك حقوق الإنسان في فقرتها الأولى بأن تكفل الدول الأطراف أن يكون تنفيذ إلتزاماتها وموجب هذه الإتفاقية متناسباً مع إلتزاماتها بموجب القانون الدولي لحقوق الإنسان وعدم مخالفته وإتباع القواعد القانونية للقانون الدولي لحقوق الإنسان، وتضمنت أيضاً في الفقرة الثانية أن هذه الإتفاقية لا يوجد فيها ما يفسر بالسماح بقمع حقوق الإنسان أو الحريات الأساسية التي تنص عليها المواثيق والمعاهدات الدولية بما في ذلك الحقوق التي تخص حرية التعبير أو حرية الرأي أو الدين أو الضمير أو الحق في الخصوصية وحرية التجمعات السلمية وتكوين الجمعيات وفقاً للقانون واجب التطبيق (القانون الدولي لحقوق الإنسان) ويجب مع ذلك الإتفاق معه وعدم مخالفته ولم تخالف هذه الإتفاقية قواعد القانون الدولي لحقوق الإنسان[1]

وورد من ضمن المعايير الحديثة للأمم المتحدة سالفة البيان حق أصيل خاص بحماية حقوق الإنسان فقد ورد النص الصادر من الجمعية العامة للأمم المتحدة المتفق عليه (المعيار الخامس) من المعايير الحديثة للأمم المتحدة كالآتي

ينبغي للدول في ضمان الإستخدام الآمن لتكنولوجيا المعلومات والإتصالات أن تحترم قراري مجلس حقوق الإنسان رقم ٢٠/٨ و ٣١/٦٢ بشأن تعزيز وحماية والتمتع بحقوق الإنسان على الإنترنت فضلاً عن قراري الجمعية العامة ١٦٧ / ٦٨ و ٩٦/ ٦٦١ بشأن الحق في الخصوصية في العصر الرقمي لضمان الإحترام الكامل لتحقيق لحقوق الإنسان لما في ذلك الحق في حرية التعبير

---

[1] **انظر المادة السادسة من إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية الصادرة في ٢٧-١١-٢٠٢٤ (A/79/460)**

وقد وردت تلك القاعدة في أغلب المواثيق محل الدراسة مؤكدة إحترام حقوق الإنسان والحق في التعبير عبر الفضاء السيبراني[١]، ومنطلق تلك القاعدة هو أن حقوق الإنسان التي يتمتع بها في الواقع يجب أن تكون متوفرة ومحمية بنفس القدر في العالم الإفتراضي

ويتضمن ذلك المبدأ كذلك حرية الإنسان في التعبير بما يشمله ذلك من حريته المطلقة بالبحث عن المعلومات والتعامل معها سواء تبليغها أو نقلها بأي وسيلة عبر الحدود وغير ذلك من كافة الأحكام والمبادئ المقررة في هذا الشأن والمنصوص عليها في العهد الدولي الخاص بالحقوق السياسية والمدنية وكذلك ما ورد بالإعلان العالمي لحقوق الإنسان بالمادة ١٩ والتى تتضمن أن حرية التعبير والرأي حق أساسى من حقوق الإنسان متمثلاً في حرية إعتناق الآراء والتماس الأفكار والأنباء ونقلها وتلقيها بأي وسيلة أو عبر أي وسيط بدون أي عوائق أو حدود تمنع ذلك بإعتبار الأخير هو الأساس المتين في حماية والحفاظ على حقوق الإنسان بشكل عام[٢]

وعلى الحكومات الإمتناع عن إتباع ذلك والتخلي عن أي ممارسات تعسفية مثل المراقبة الجماعية للأفراد أو غير القانونية مما يشكل تعارضاً فجاً على ممارسات حقوق الإنسان وخاصة الحق في الخصوصية واجبات وأعباء على الدول من أجل الإلتزام بهذا المبدأ ويجب على الدول وحكوماتها مراعاة ما يلي من أجل وضع ذلك المبدأ موضع التطبيق الفعلي

١-على الدول المشاركة الفعالة في كافة المنتديات والفعاليات المخصصة داخل الأمم المتحدة والخاصة بقضايا حقوق الإنسان والإطلاع عليها والمشاركة فيها

٢- يجب أن يشارك أصحاب المصلحة في عملية وضع السياسات ذات الصلة بأمن تكنولوجيا الإتصالات والمعلومات ودعم كافة الجهود التي تعزز وتدعم تعزيز حقوق الإنسان والتمتع بها في الفضاء السيبراني وكذلك المساعدة في تقليل وتوضيح كافة التأشيرات الضارة والسلبية المحتملة على الأفراد[٣]

---

[1] **Rule 34 of Tallin 2, op cit , Article 7 of shanghai code of conducts at U.N.G.A.15 Doc (A/69/723) p.5**

[٢] **انظر المادة ١٩ من الإعلان العالمي لحقوق الإنسان ١٩٤٨**

[3] **U.N.G.A 20,3.Doc(A/68/167) p.2**

٣-ينبغي على الدول الأخذ بجدية بالتوجيهات الواردة في القرارات ذات الصلة وكذلك كافة القرارات الجديدة والحديثة في هذا الشأن منذ تقرير مجموعة الأمم المتحدة للمساواة بين الجنسين وكذلك تمكين المرأة عام ٢٠١٥[١]

ونحن نرى في ذلك الشأن الخاص بحقوق الإنسان أنه من دواعي الإنصاف التأكيد على أن هذا المبدأ لا تتقبله كافة الأنظمة السياسية أو الديكتاتورية والإستبدادية وتضيق به ذرعاً وكافة الأنظمة ذات الحكم الفردي مثل الصين أو روسيا وغيرها فلا يسمح بها من أي إنتقاد نحو الحاكم سواء في الواقع أو عبر الفضاء السيبراني لأنه قد يفتح الباب للمطالبة بالمزيد من الحقوق والحريات وتحقيق مزيد من الديمقراطية وتداول السلطة ولذلك يكون التضييق على كافة الحقوق الأصلية للإنسان كالحق في التعبير أو النقد أو الحق في الخصوصية في أقل درجاتها أما بالنسبة للدول المتقدمة أو ذات الديمقراطية فقد تكون حقوق الإنسان مصانة بشكل أكبر وإن كانت لا تحقق بالنسبة الكاملة دائماً

وتأكيداً لرأينا السابق نجد أن منظمة شنغهاي للتعاون حينما أوردت ذلك المبدأ في مدونة السلوك أشارت إلى نص المادة ١٩ من العهد الدولي للحقوق المدنية والسياسية التي قد تجيز الحريات الفردية لأهداف تعلنها الدول مثل حماية الأمن القومي أو النظام العام او الآداب العامة أو الصحة العامة

وعلى الدول في هذا الصدد مراعاة المتطلبات التالية للوصول إلى تطبيق ذلك المعيار[٢]

١- يجب مكافحة كافة دعوات الكراهية أو التحريض على العنف لا تشكل تحريضاً على التمييز بين البشر بسبب العرق أو اللون أو الدين أو التوجه السياسي

٢- الإستفادة من الطبيعة العالمية والعابرة للحدود للإنترنت في تسريع التقدم نحو التنمية الاجتماعية أو الإقتصادية او الثقافية او العلمية

٣-تمكين الأفراد من الوصول إلى الإنترنت والتعاون الدولي الهادف لتطوير وسائل المعلومات

٤-يجب معالجة المخاوف الأمنية على الإنترنت وفق إلتزامات حقوق الإنسان لضمان حرية التعبير وحرية تكوين الجمعيات وكافة أوجه الخصوصية

---

[١]انظر الفصل السادس من ميثاق الأمم المتحدة والنظام الأساسي لمحكمة العدل الدولية، نيويورك،١٩٩٤

[2]Paul P.polanski, cyber space Anew branch of International Customary law Computer law, security,Op, P6

المطلب الرابع

مبدأ الحفاظ على إطار الإستقرار السيبراني

وهذا المعيار العاشر ضمن المبادئ والمعايير الحديثة أيضاً للأمم المتحدة عبر جمعيتها العامة والذي يراعي حماية نقاط الضعف في تكنولوجيا المعلومات والإتصالات كالآتي[1]

ينبغي على الدول أن تشجع الإبلاغ المسؤول عن نقاط الضعف في تكنولوجيا المعلومات والإتصالات وتبادل المعلومات المرتبطة بها بشأن الحلول المتاحة لنقاط الضعف من أجل الحد من التهديدات المحتملة لتكنولوجيا المعلومات والإتصالات والبنية الأساسية المعتمدة على تكنولوجيا المعلومات والإتصالات والقضاء عليها

والقاعدة سالفة البيان تفرض على الدول أهمية ضمان معالجة كافه نقاط الضعف في تكنولوجيا الإتصالات والمعلومات وذلك لتفادي الإستخدام غير المشروع او الخبيث من أي جهة لأن الإكتشاف في الوقت المناسب والإفصاح المسؤول والإبلاغ عنها وعن نقاط الضعف الخاصة بالشبكات من شأنه منع أي ممارسة ضارة ويزيد من معدلات الثقة لدى المستخدمين ويقلل بشكل كبير من التهديدات ذات السرعة التي قد تمس السلم والأمن الدوليين وضرورة وضع السياسات وبرامج الكشف عن الثغرات

فضلاً عن زيادة فرص التعاون الدولي في ذات الشأن والكشف المنسق عن الثغرات التي تقلل من حجم الضرر الذي قد يلحق بالمجتمع وطلب المساعدة بين البلدان وفرق الإستجابة للطوارئ ويجب أن كذلك أن تكون تلك العمليات والإجراءات متفقة مع التشريعات المحلية والوطنية لمزيد من فرض الحماية.

واجبات على الدول يجب مراعاتها الإلتزام بتلك القاعدة

١-يجب على الدول أن تضع الأطر والمعايير والسياسات القانونية والبرامج المحايدة بشأن التعامل مع نقاط الضعف في تكنولوجيا المعلومات والإتصالات لديها والحد من التوزيع التجاري لتلك البرامج كوسيلة للحماية من سوء الإستخدام الذي قد يشكل خطراً على السلم والأمن الدوليين وذلك على كافة المستويات الوطنية او المحلية او الإقليمية او الدولية

٢-على الدول أن تضع حماية قانونية فعالة متجددة لكل الباحثين ومختبري عمليات الإختراق

---

[1] **Michael P scharf, Accelerated Formation of Customary International Law Op.Cit P335**

٣-يجب على الدول كذلك التشاور مع الصناعات وكل أصحاب المصلحة من الجهات الفاعلة في مجال أمن تكنولوجيا المعلومات والإتصالات بوضع إرشادات وحوافز تتفق مع المعايير الفنية الدولية المعترف بها وكذلك الإبلاغ المسؤول عن نقاط الضعف في الشبكات وتبادل المعلومات بشكل فعال في تبادل المعلومات الفنية حول حوادث الفضاء السيبراني وكيفية التعامل الآمن والجيد مع البيانات الحساسة وضمان أمن المعلومات وسريتها

وكذلك المعيارالسابع والذي يتضمن ضرورة أن تتخذ الدول التدابير اللازمة والمناسبة لحماية البنية الأساسية الحيوية من التهديدات الخبيثة الغير مشروعة لتكنولوجيا الإتصالات والمعلومات مع مراعاة قرار الجمعية العامة للأمم المتحدة رقم ٥٨/١٩٩ المتعلق بإنشاء ثقافة عالمية للأمن السيبراني وحماية البنية الأساسية الحيوية للمعلومات والقرارت ذات الصلة والإجراءات الوادة في هذا القرار مثل التدابير اللازمة لأمن وسلامة منتجات تكنولوجيا المعلومات والإتصالات واتخاذ تدابير مناسبة لتصنيف هذه الإعتداءات من حيث حجمها وخطورتها وكذلك إنشاء شبكات تحذير طارئة لنقاط الضعف والحوادث السيبرانية ورفع مستوى الوعي بالأمن السيبراني وفحص البنى التحتية وإنشاء شبكات الإتصالات في حالات الأزمات وصيانتها للتأكد من بقائها آمنة وتعزيز البحث والتطوير على العيد الوطني والدولي وتطبيق التقنيات الأمنية التى تتوافق مع المعايير الدولية [١].

لقد تضمنت إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية بعد المواد الخاصة بالحفاظ على إستقرار الإطار السيبراني ومنها المادة السابعة المتعلقه بالوصول غير المشروع أو الدخول غير المشروع وألزمت كل دولة طرف في الإتفاقية بإعتماد التدابير التشريعية والتدابير القانونية اللازمة لتجريم الوصول دون وجه حق إلى نظام تكنولوجيا الإتصالات والمعلومات بأكمله أو اي جزء من أجزائه في حالة إرتكاب هذا الفعل عن عمد بموجب القوانين الداخلية وكذلك ايضا ان تشترط الدولة الطرف في الاتفاقية ان الفعل الاجرامي يكون ارتكب من خلال انتهاك لتدبير أمني بقصد الحصول على المعلومات والبيانات الالكترونية او بقصد أو نية إجرامية سيئة فيما يتعلق بنظام تكنولوجيا المعلومات والاتصالات المتصل بنظام معلومات وإتصالات آخر [٢]

---

[1] Oleg Demidov and Giacomo Persi Paoli , supply Chain Security in the Cyber Age:sector Trends, Current Threats And Multi-stakeholder Responses UNIDR Geneva,2020 . unidir.org/publication/sup.

[٢] انظر المادة السابعة من إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية الصادرة في ٢٧-١١-٢٠٢٤ (A/79/460)

وكذلك المادة الثامنة من هذه الإتفاقية التي أقرت الإعتراض غير المشروع وأوجبت على كل دولة طرف في الإتفاقية أن تعتمد التدابير اللازمة لتجريم وفقاً لقوانينها الداخلية الإعتراض بوسائل تقنية لعمليات إرسال غير عمومية لبيانات إلكترونية إلى نظام تكنولوجيا معلومات وإتصالات منه أو إليه وفي حالة إرتكاب هذا الفعل بعمد ودون وجه حق وكذلك أيضا يشمل ذلك الإعتراض الإنبعاثات الكهرومغناطيسية من نظم تكنولوجيا المعلومات والإتصالات التي تحمل هذه البيانات والمعلومات الإلكترونية وأيضا أن يجوز للدولة الطرف أن تشترط أن يكون الفعل الإجرامي إرتكب بسوء نية بقصد غير سليم أي توافر القصد الاجرامي فيما يتعلق بتكنولوجيا المعلومات والإتصالات متصل بنظام تكنولوجيا ومعلومات إتصالات آخر[١]

وكذلك التدخل في البيانات الإلكترونية التي تضمنته المادة التاسعة وأيضا إلزام الدول الأطراف وفقاً للقانون المحلي بإتخاذ ما يلزم من تدابير سواء كانت التشريعية أو تدابير أخرى لتجريم إتلاف البيانات الإلكترونية أو تحويرها أو طمسها أو إفسادها أو حذفها في حالة إرتكاب هذه الأفعال عن عمد ودون وجه حق ويشترط أيضا في هذه الأفعال حدوث الضرر الجسيم وكذلك أيضا جرمت التدخل في نظام تكنولوجيا المعلومات والإتصالات كذلك الأمر تجريم هذه الأفعال طبقاً للقانون الداخلي وإتخاذ والتدابير الإجرائية اللازمة في حالة أي إعاقة خطيرة لعمل نظام إلكتروني من خلال نظام تكنولوجيا المعلومات والإتصالات سواء كان عن طريق إرسال بيانات إلكترونية او إدخال بيانات الكترونية أو طمسها او إتلافها أو حذفها عمداً أو في حالة إرتكاب هذا الفعل عن عمد وبدون وجه حق[٢]

وكذلك أيضاً إساءة إستخدام الأجهزة في المادة الحادية عشر فأوجبت أيضاً إتخاذ جميع ما يلزم من إجراءات وتدابير وتجريم هذه الأفعال في حالة إرتكابها عن عمد وبدون وجه حق مثل تصميم برنامج أوتصنيع جهاز بغرض إرتكاب هذه الأفعال المجرمة في المواد سالفة الذكر من المادة السابعة الى المادة العاشرة وكذلك إكتساب الأشياء وإنتاجها أو بيعها أو شرائها بغرض إستخدامها أو

---

[١]انظر المادة الثامنة من إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية الصادرة في ٢٧-١١-٢٠٢٤ (A/79/460)

[٢]انظر المادة التاسعة من إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية الصادرة في ٢٧-١١-٢٠٢٤ (A/79/460)

توزيعها بأي طريقة وإستخدام كلمة مرور او بيانات إعتماد بتسجيل دخول لموقع الكتروني وكذلك حيازه بعض هذه الأشياء بغرض إستخدامه في الأفعال غير المشروعة وفقاً لهذه الإتفاقية[1]

ونحن نرى في هذا الخصوص أن عملية الحفاظ على إطار يمتاز بالإستقرار السيبراني غاية في الصعوبة وإن لم تكن في حكم الإستحالة المطلقة لأن عمليات الولوج للكائنات وإختراق نقاط الضعف في الشبكات أمر مؤقت للغاية ومتطور بشكل متسارع جداً مما يجعل الحيلولة دون حماية كاملة من نقاط الضعف أو الإختراق أو الولوج هو أمر واقعي وملموس ونقول نحن في هذا على أهمية التعاون الدولي بشأن كل البرامج الحديثة ومواجهة نقاط الضعف خاصة من الدول الرائدة والمتقدمة مما يجعل من أمر محاصرة كافة صوره أو نقل خبراتها للدول النامية والأقل تقدماً في شأن تكنولوجيا المعلومات والإتصالات ومع ذلك يبقى جانب أو قدر ضئيل يكون من الإستحالة تأمين كامل لكافة وجوه إستخدام الشبكات ولعل رغبة الدول في تطوير تشريعاتها الوطنية القائمة والخاصة بتجريم كافة أشكال السلوك الخبيث للفضاء السيبراني وأمر مطلوب أيضاً ويساهم بشكل كبير في إستقرار العالم السيبراني

[1] **انظر المادة الحادية عشر من إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية الصادرة في ٢٧-١١-٢٠٢٤ (A/79/460)**

الخاتمة

أن مصطلح الأمن السيبراني المنشود يشمل تحت طياته مجموعه من الأنشطة المتزامنة من جمع معلومات وأجهزة الكمبيوتر ومعلومات الأفراد والبرامج المعلوماتية كذلك نظم الإتصالات سواء السلكية أو اللاسلكية وخلاصة القول مجمل جميع المعلومات وكذلك المعلومات المخزنه في كافة الأجهزة الإلكترونية وبشكل عام تختلف والتقنيات المستخدمة عبر شبكة الإنترنت.

هنا تجدر الإشارة إلى أن القانون الدولي يمكن أن يشمل حماية وتقنين لتلك التقنيات بإعتباره الإطار القانوني الدولي الذي قد يصل إتفاق المجتمع الدولي على قواعدة إتفاقاً قد يعادل الإجماع على إنطباق قواعده على الفضاء السيبراني أو الإلكتروني ودليل ذلك ما أيدته جميع الدول للمعايير التي أرستها الأمم المتحدة للسلوك الغير مسئول في الفضاء السيبراني

وقد كان من أهم مهام وأدوار منظمة الأمم المتحدة الحفاظ على السلم والأمن الدوليين فإن جهودها في هذا الصدد يجب أن تشمل مجابهة السلوك الجائر والغير شرعي للهجمات السيبرانية التي أصبحت سمة مميزة منذ بداية الألفية الثالثة بين كافة الدول ولم ينجو منها أيا منهم.

وحقيقة الأمر أن منظمة الأمم المتحدة قد بدأت جهودها في هذا الشأن منذ عام ١٩٩٨ رامية نحو تأسيس مجموعة من القواعد الدولية والمبادئ والأسس التي تمنع إستعمال مجال الفضاء السيبراني في أعمال من شأنها تهديد السلم والأمن الدوليين،وبالرغم من ذلك لم تكن تلك الجهود مكللة بالنجاح والتوفيق حتى بداية عام ٢٠٢١ والذي هو بداية حقيقية لإقرار قواعد حاكمة لإستخدامات الفضاء السيبراني.

النتائج

١) إن الفضاء السيبراني أصبح أخطر المهددات للأمن والسلم الدوليين بالرغم المحادثات الجاده لمنظمة الأمم المتحدة نحو وضع قواعد دولية تحكم سلوك وتصرفات الدول في الفضاء السيبراني الا أن تضارب المصالح هو إختلاف الأيديولوجيات بين الدول الأعضاء في المنظمة قد وقف عائقا نحو تاسيس اتفاقيه دولية ملزمه في هذا الشأن

٢) دول المجتمع الدولي جميعاً مضطرة لأن تتبنى نظاماً آمناً وموحداً لسلوك الدول في العالم السيبراني لأن البديل الوحيد لعدم تحقيق ذلك هو الفوضى وشيوع المسؤولية ويصبح الفضاء السيبراني غير امن وبيئه خصبة لكافة الجرائم السيبرانية .

٣) عدم تفعيل لجان فنية وتقنية تابعة لمنظمة الأمم المتحدة متخصصة في التصدى لإختراقات البنى التحتية لمؤسسات الدول والقطاع الخاص وكيفية مواجهتها والتغلب عليها.

٤) إن إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية ٢٠٢٤ تعتبر اللبنة الأولى والخطوة الأهم لإقرار قواعد قانونية دولية ملزمة تحكم إستخدام الدول والمؤسسات للفضاء السيبراني .

٥) أوردت الإتفاقية في الغالب من موادها عبارة " يجوز لكل دولة ..... " مثل حالة جواز إتخاذ أي دولة من التدابير والإجراءات والتشريعات ما يلزم لضمان تنفيذ ماجاء بالإتفاقية من أحكام فإذا كان الأمر جوازي وليس إجباري فكيف يكون ضمان أن تضع كل دولة ما يلزم من تلك التدابير أو التشريعات الخاصة بمنع ومكافحة الجريمة السيبرانية فكان من الأولى على واضعي تلك الإتفاقية أن تكون عبارات ومواد الإتفاقية واضحة في إلزام وإجبار كافة الدول على إتخاذ مثل هذه التدابير وإلا ماذا سيكون الأمر لو تراخت أي دولة بالنظر لمصالحها عن الإلتزام بذلك فإطلاق حرية الدول في ذلك يفرغ الإتفاقية من محتواها وتأثيرها والإلتزام بعمل ما يلزم له.

٦) لم تنص الإتفاقية في موادها المختلفة على إمكانية تدخل الأمم المتحدة بفرض جزاءات سواء كانت سياسية أو إقتصادية أو مالية على الدول المخالفة لبنود ما جاء بتلك الإتفاقية لتحقيق الردع العام والخاص سواء للدول أو المؤسسات أو المنظمات أو حتى الأفراد في حالة وجود أي سلوك أو نشاط سيبراني غير مشروع فكثيراً ما قامت الأمم المتحدة بفرض جزاءات غاية في القسوة على الدول التي تنتهك القانون الدولي مثل الحظر الإقتصادي مثلاً لأن الجريمة السيبرانية هي الأخطر على الساحة الدولية الآن ولضبط تلك الأنشطة ينبغي أن يكون مقروناً بجزاء دولي لضمان التنفيذ والإلتزام من كافة دول المجتمع الدولي.

التوصيات

١) يوصي الباحث الدول بوضع تشريعات وطنية داخلية تنظم سلوك الأفراد والمؤسسات في الفضاء السيبراني وخضوعهم للمسائلة والعقاب

٢) سن قوانين داخلية تعرف الجرائم السيبرانية بكافة صورها وأشكالها وكذلك إنشاء محاكم متخصصة في الجرائم السيبرانية

٣) التوصل الى نظام دولي سريع وفعال للتعاون الدولي والحفاظ على سرية البيانات وتدريب الكوادر الوطنيه للأمن السيبراني وحماية البنية التحتية الرقمية بها

٤) أن تضع منظمة الأمم المتحدة وتدعم المزيد من البرامج التدريبية والتعليمية من خلال الشراكة بين مؤسسات الدول ومؤسسات القطاع الخاص لتدريب الأفراد المتخصصين في هذا المجال والفنيين وكذلك زيادة الوعي والإدراك بالأمن السيبراني وتحدياته

٥) إنشاء جهات رقابية دولية لمراقبة النشاط الدولي السيبراني وكذلك فرق تحقيق متخصصة في الجوانب الفنية وتبادل المعلومات في الجرائم السيبرانية

٦) إلزام الدول بتطبيق قواعد ومبادئ القانون الدولي وكذلك القانون الدولي الإنساني على الفضاء السيبراني

٧) توسيع دور المنظمات المتخصصة المحايدة في إقتراح القواعد السيبرانية مثل الإتحاد الدولي للإتصالات وكذلك إنشاء هيئات تقدم خدمات إستشارية للدول لمساعدتها في صياغة القوانين السيبرانية

٨) إنشاء الشراكة بين القطاعين العام والخاص على المستوى الوطني والإقليمي والدولي لمكافحة الجريمة السيبرانية ذات الصلة فيما يتعلق بالمبادرات والندوات والمؤتمرات الخاصة بالأمن السيبراني

٩) أن يقوم مجلس الأمن بدور فعال في محاسبة ومعاقبة الدول والمؤسسات التي ترتكب سلوك غير مشروع في الفضاء السيبراني بما لديه من إختصاصات .

١٠) إنشاء لجنة فنية متخصصة من خبراء علميين وفنيين تابعة للأمم المتحدة تختص بإبتكار برامج للرصد والتنبؤ المبكر بالحوادث الغير مشروعة في الفضاء السيبراني

١١) إنشاء لجنة أو هيئة تابعة للأمم المتحدة تكون مسؤولة عن مراقبة تنفيذ الدول بماجاء بالبنود الإتفاقية وكذلك تلقي الشكاوي من أي دولة في حال تعرضها لأي عمل سيبراني غير مشروع وجمع الأدلة وصياغة التقرير بالحالة والواقعة وتحديد من يقع عليه المسؤولية أمام الأمم المتحدة

لتكون الصورة كاملة وتحديد من له الحق وكيفية جبر الضرر الواقع على أي دولة سواء بالتعويض المالية أو أي جزاء آخر تراه منظمة الأمم المتحدة

المراجع

المراجع العربية

١) أحمد عبيس الفتلاوي، الهجمات السيبرانية –مفهومها –المسئولية الناشئة عنها في ضوء التنظيم الدولي المعاصر

٢) إدريس عطية، الأمن السيبراني في منظومة الأمن السيبراني الجزائري،مجلة مصداقية، المدرسة العليا العليا العسكرية للإعلام والإتصال، المجلد الأول، العدد الأول،ديسمبر ٢٠١٩

٣) ج. رضوان الأمن السيبراني أولوية في إستراتيجيات الدفاع، مجلة الجيش، ع ٣٠، جانفي ٢٠١٧

٤) حسني محمد نصر، عبد الله الكندي، الإعلام الدولي، النظريات والإتجاهات الملكية الإمارات العربية المتحدة، دار الكتاب الجامعي،٢٠١١

٥) حجازي عبد الفتاح بيومي، جرائم الكمبيوتر والإنترنت والتشريعات العربية (دراسة مقارنة مع تطبيق نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية، القاهرة، دار النهضة،٢٠٠٩.

٦) حل توجيهية البرلمان الأوربي ومجلس الإتحاد الأوربي بتاريخ ٢٠١٣/٨/١٢ بشأن الهجمات على أنظمة المعلومات محل القرار الإطاري للمجلس ٢٠٠٥

٧) دحان حزام القريطي، الأمن السيبراني وحماية البيانات، دار الفكر الشرطي، الإسكندرية،٢٠٢٤

٨) رزق أحمد سمودي، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام،مجلة جامعة الشارقة للعلوم القانونية، مجلد ١٥، العدد ٢، ٢٠١٨

٩) رغدة البهي، الردع السيبراني، المفهوم والإشكاليات والمتطلبات، مجلة العلوم الساسية والقانون، المركز الديقراطي العربي، العدد الأول،٢٠١٧

١٠) سامر محيي عبدالحمزة، مدى مساهمة الأمم المتحدة في تشكيل القواعد الدولية الخاصة بالفضاء السيبراني، مجلة مركز دراسات الكوفة، العدد٦٧، ج ١، ديسمبر ٢٠٢٢

١١) سامر مؤيد عبد اللطيف، الحرب في الفضاء الرقمي رؤية مستقبلية، مجلة رسالة الحقوق السنة السابعة، العدد ٢، ٢٠١٥.

١٢) سمير بارة، الأمن السيبراني في الجزائر،السياسات والمؤسسات، المجلة الجزائرية للأمن السيبراني،ع١٤

١٣) شادي عبد الوهاب منصور، حروب الجيل الخامس،أساليب التفجير من الداخل على الساحة الدولية،القاهرة، المستقبل للأبحاث والدراسات المتقدمة، العربي للنشر والتوزيع،٢٠١٩
١٤) شتاين شولبرغ – تاريخ الجريمة السيبرانية (الطبعة الثانية – فبراير –٢٠٢٠)
١٥) ص٢٧٦A/G.1/73/I.) مذكرة الأمين العام للأمم المتحدة في عام ٢٠١٨ وثائق الأمم المتحدة – (الوثيقة
١٦) عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، مكتبة المستقبل، مصر،عام ٢٠١٦
١٧) عبدالفتاح مراد، جرائم الكمبيوتروالإنترنت، المكتبة القانونية،طبعة أولى،١٩٩٨،
١٨) عجال بوزادية، إستراتيجية الجزائر في مواجهة الجرائم اليبرانية،التحديات والآفاق المستقبلية، مجلة العلوم القانونية والسياسية،ع ١١،الجزائر
١٩) غترة بن مرزوق، محي الدين حرشاوي،الأمن السيبراني كبعد حديث للسياسة الدفاعية الجزائرية، الملتقى الدولي حول سياسات الدفاع الوطني،جامعة قاصدي، ٢٠١٧
٢٠) منى الأشقرجبور، الأمن السيبراني، التحديات ومستلزمات المواجهة، المركز العربي للبحوث القانونية والقضائية، بيروت،٢٠١٧،
٢١) نسرين الصباحي، الحروب السيبرانية وتحديات الأمن العالمي، منشور في المركز العربي للبحوث والدراسات ٢٠١٧
٢٢) نهلا عبد القادر المؤمني، الجرائم المعلوماتية، الثقافة للنشر والتوزيع، عمان، الأردن،٢٠١٦

المراجع الإنجليزية:

1) Andrew T.Guzman and Timothy I.meyer international soft law journal of
2) Bart Hogeveen, Sydney recommendations- practical futures for cyber confidence building in the ASEAN region, 18 september،2018 . aspi.org.au/report/Sydney
3) C20/3. ،٦C20/inf/11
4) Epfl, Prss Cyber Power, crime. conflict and security in cyber space,2013 Lorans Braford،Cyber security needs women، Here's Why.
5) Florian J. Egolf – Max Smeets 'Publicly Attributing Cyber Attacks: A Framework', Journal of Strategic Studies. external page Chesney, 2021, https://doi/10.1080/01402390.2021.1895117.
6) Lauren Zabierek and others, us-Russian contention in cyberspace are " Rules of the road Necessary of possible، June, 2021.
7) Michael P scharf, Accelerated Formation of Customary International Law Op.
8) Michael Schmitt, The sixth united nations GGE and international law in cyberspace،2021. at https://www.justsecurity.org/76864/the- sixth- united- nations- gge- and- international- law- in- cyberspace.
9) National security council (U.S) and United states executive Office of the president international strategy of cyberspace (national security council،2011.
10) Oleg Demidov and Giacomo Persi Paoli، supply Chain Security in the Cyber Age:sector Trends, Current Threats And Multi-stakeholder Responses UNIDR Geneva, 2020. unidir.org/publication/sup.

11) Paul P.polanski, cyber space Anew branch of International Customary law Computer law, security. Review Volume33, Issue3, June 2017.
12) Paul P. Polanski، cyber space Anew branch of International Customary law Computer law, security.
13) Rule (17) of Tallin.
14) Rule 27 of Tallinn.
15) Article 9 of Shanghai Code of conducts at UNG.20.15 Doc (A/69/723)
16) Rule 34 of Tallin 2.0
17) Article 7 of shanghai code of conducts at U.N.G.A.15 Doc (A/69/723).
18) Tallin manual 2.0 on the international law Application to cyber operations.
19) Tim Amaurer cyber norm Emergence at the united nation – An analysis of the UNS activites regarding – paper،2011.
20) U.N.G.A 20,3.Doc(A/68/167) .
21) U.N.G.A 2021, Doc (A/76/135).
22) Us Department of justic Report on the investigation into Russian interference in 2016

المقالات العلمية والمواقع الإلكترونية

١) السيد محمد السيد أحمد، القانون في الفضاء السيبراني، المنصة القانونية، مقال منشور في ٢٠٢٢/٦/٧ على الرابط http:/wwwsaiplus.com

٢) الوثائق الختامية للقمة العالمية لمجتمع المعلومات

https:www.itu/en/action/cybersecurity/pages/gca

٣) الإتحاد الدولي للإتصالات السلكية واللاسلكية، الإجتماع الإقليمي التحضيري للمؤتمر العالمي لتنمية الإتصالات ٢٠١٠، منطقة الدول العربية، قطاع تنمية الإتصالات من على الرابط http/:www.comferas.com

Bart Hogeveen – Head of Capacity Building – March 2022 Available on www.aspistrategist.org.au.facebook.com/Aspi.org

http: www.icrsegoorg 40594

https://obama whitehouse.archives.gov/the-press-office/2013/6/17/fact-sheet-us-russian. Cooperation- information and communication – technical.https:/www.itu. int/md/s18-pp

٤) المبادئ التوجيهية للإتحاد الدولي للإتصالات في مجال الأمن السيبراني متاح على الموقع http:/webfoundation org/2019

٥) القاضي شتاين شولبرغ ٢٠١٨ وكذلك ٢٠١٩ متاح على الموقع:

http://www.cybercrime law.net/cybercrime law html

٦) الإتحاد الدولي للإتصالات السلكية واللاسلكية، وثيقة صادرة عن القمة العالمية لمجتمع المعلومات، جنيف 2003، وتونس ٢٠٠٥،https:/www.itu

https:/www.un.org/org/en/digital-cooperation- penal

٧) الفرق الوطنية للإستجابة للحوادث الحاسوبية – الإتحاد الدولي للإتصالات

itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx

٨) عدد مستخدمي فيس بوك النشطاء شهرياً في جميع أنحاء العالم في الربع الأخير من عام ٢٠١٩ متاح على

https/ number-of- monthly-com/ statistics/264810/number-of- monthly-active-facebook-users

٩) الإتفاقيات والقرارات والتقارير الدولية

١٠) إتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية الصادرة في ٢٧-١١-٢٠٢٤ (A/79/460)

١١) الإعلان العالمي لحقوق الإنسان ١٩٤٨

١٢) مذكرة الأمين العام للأمم المتحدة في ٢٠٢١/٧/١٤

١٣) المبادئ التوجيهية للإتحاد الدولي للإتصالات في مجال الأمن – الملحق رقم ١ وثيقة (٤٧٠٩٣٨)

١٤) معايير الأمم المتحدة للسلوك السيبراني المسئول للدولة في الفضاء الإلكتروني – إرشادات بشأن التوضيح للدول الأعضاء في رابطة دول جنوب شرق آسيا

١٥) القرار رقم ١٣٠ في دبي ٢٠١٨ لمؤتمر المندوبين المفوضين، البرنامج العالمي للأمن السيبراني.

١٦) وزارة الإتصالات والمعلومات، التقرير العام للجنة التحقيق في الهجوم الإلكتروني على الخدمات الصحية في سنغافورة، حكومة سنغافورة، ٢٠١٩

١٧) تقرير الخبراء رفيع المستوى المعني بالأمن السيبراني عام ٢٠٠٨ قرار الجمعية العامة رقم ٢٤٧/ ٧٤ بشأن مكافحة إستخدام تكنولوجيا الإتصالات والمعلومات لأغراض خبيثة

١٨) قرار الجمعية العامة للأمم المتحدة رقم ٧٤/١٧٣ بشأن تعزيز المساعدة التقنية وبناء القدرات لتعزيز التدابير الوطنية والتعاون الدولي

١٩) قرار الجمعية العامة للأمم المتحدة في ٢٩-٣-٢٠١٢ – وثائق الأمم المتحدة (L /20 13)

٢٠) الجمعية العامة للأمم المتحدة – فريق الخبراء الحكوميين – المعني بتعزيز السلوك السيبراني في سياق الأمن الدولي مارس،٧٥/٦٠١٤/ A

٢١) الفصل السادس من ميثاق الأمم المتحدة والنظام الأساسي لمحكمة العدل الدولية

٢٢) مذكرة الأمين العام للأمم المتحدة في ٢٠٢١/٧/١٤ الوثيقة (A/76/135)

٢٣) الإتحاد الدولي للإتصالات، المؤشرات الأساسية لتكنولوجيا المعلومات والإتصالات ٢٠١٠، جنيف – مكتب تنمية الإتصالات

٢٤) تقرير الأمين العام للأمم المتحدة حول متابعة نتائج مؤتمر القمة العالمي لمجتمع المعلومات على الصعيد الإقليمي والعالمي القرار رقم ١٣٠ في دبي ٢٠١٨ لمؤتمر المندوبين المفوضين، البرنامج العالمي للأمن السيبراني الوثيقة C20/3,٦C20/inf/11
٢٥) الجمعية العامة للأمم المتحدة – فريق الخبراء الحكوميين المعني بالتطورات في مجال تكنولوجيا المعلومات والإتصالات في سياق التعاون الدولي الأمني، الفقرة ١٠ يوليو ٢٠١٥، A/174.22
٢٦) تقارير الإتحاد الدولي للإتصالات حول الأمن السيبراني لسنوات ٢٠١٥، ٢٠١٧، ٢٠١٨ على الموقع https:/www.itu
٢٧) تقرير فريق الخبراء رفيع المستوى المعني بالأمن السيبراني عام ٢٠٠٨
٢٨) قرار الجمعية العامة للأمم المتحدة رقم ٦٥/٢٣٠ الخاص بالجرائم الإلكترونية