Journal Of the Iraqia University (74-8) December(2025)

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

# الآليات القانونية الدولية لمكافحة الهجمات السيبرانية – دراسة تحليلية في إطار القانون الدولي العام والإنساني

المشرف :الأستاذ الدكتورمصطفى فضائلي /كلية القانون / جامعة قم

حسن سامي نورالمحنا / كلية القانون / جامعة قم

# International legal mechanisms for combating cyberattacks – an analytical study within the framework of public and humanitarian international law

supervior: Dr.Mostaf Fazaeli
University : Qom University - College of Law
Rescarcher: Hasan Sami Noor Al-Mohana
hasan.iraq7777@gmail.com
fazaeli2007@gmail.com

تعد الاتفاقيات الدولية، هي اداة التشريع الرئيسية – إلى جانب مصادر أخرى – فيما يتعلق بالقانون الدولي، ولما لا وقد استطاعت هذه الاتفاقيات أن تنتزع لنفسها هذه المكانة فتصبح هي المصدر الأول للقانون الدولي بعدما احتل العرف الدولي هذه المكانة لفترة طويلة من الزمن. ولعل محكمة العدل الدولية بنظامها الأساسي قد حددت هذه المسألة بشيء من الوضوح عندما رتبت المصادر الواجب الرجوع اليها عند الرغبة في فصل في نزاع دولي، فاعترفت للاتفاقيات الدولية بهذه المكانة الخاصة .[1]فالاتفاقيات الدولية هي المرأة الحقيقية التي تعكس رغبة أعضاء الجماعة الدولية حول موضوع محدد، فعلى اساسها ومن خلالها تظهر الرغبة الحقيقة للدول في الوقوف على أمر ما، ولعل ما يمكن قوله في هذا الصدد، ان الاتفاقيات الدولية بهذه الصورة تعتبر هي الصورة المثالية والمناسبة عند الحديث عن الرغبة في حصاد مواقف الدول المختلفة تجاه موضوع محدد بذاته فكما هو معروف أن الاتفاقيات الدولية تمر بعدة مراحل تبدأ بالمفاوضات وتمر بالتوقيعات وتنتهي بالتصديقات المختلفة من الأجهزة التشريعية أو الرئاسية حسب دستور كل دولة.فعلى مستوى الأمم المتحدة فقد حرصت منذ اللحظة الأولى على عقد المزيد من المؤتمرات التي تؤكد على وجوب منع الجريمة وتحقيق العدالة الجنائية، وعلى ذلك فقد عقد المؤتمر التاسع لمنع الجريمة ومعاملة المجرمين في القاهرة بتاريخ ٢٩ مايو ١٩٩٥ ، وقد تناول المؤتمر العديد من الموضوعات منها وضع خطط لملاحقة العصابات الإجرامية عبر الوطنية والجرائم الاقتصادية من خلال تدعيم التعاون الدولي والمساعدة التقنية العملية لتعزيز سيادة القانون، وكذلك التدبير الفعالة لمكافحة غسيل الأموال. [2]وليس هذا فحسب بل تمت الدعوة إلى إنشاء اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، والتي تم اعتمادها بموجب قرار الجمعية العامة للأمم المتحدة ٥٥/٢٥ المؤرخ في ١٥ تشرين الثاني / نوفمبر ٢٠٠٠، الصك الدولي الرئيسي في مكافحة الجريمة المنظمة عبر الوطنية، وقد تم فتح باب التوقيع على الاتفاقية من قبل الدول الأعضاء في مؤتمر سياسي رفيع المستوى والذي انعقد لهذا الغرض في باليرمو، إيطاليا، في الفترة من ١٢–١٥ ديسمبر ٢٠٠٠ ودخلت الاتفاقية حيز التنفيذ في ٢٩ سبتمبر ٢٠٠٣. ٣وألحق بالاتفاقية ثلاث بروتوكولات تستهدف مجالات ومظاهر محددة للجريمة المنظمة حيث تضمن الاتي بروتوكول منع وقمع ومعاقبة الاتجار بالأشخاص، وخاصة النساء والأطفال؛ بروتوكول مكافحة تهريب المهاجرين عن طريق البر والبحر والجو، وبروتوكول مكافحة صنع الأسلحة النارية وأجزائها ومكوناتها والذخيرة والاتجار بها بصورة غير مشروعة، ولابد ان تكون البلدان أطرافا في الاتفاقية نفسها قبل أن تصبح أطرافا في أي من البروتوكولات.ومما يمكن قوله في هذا الصدد، أن أحداث الحادي عشر من سبتمبر ٢٠٠١ التي ضربت الولايات المتحدة الأمريكية كانت علامة فارقة على طريق مواجهة الجرائم السيبرانية، حيث أثبتت الحاجة الملحة إلى ضرورة مواجهة هذا الجرائم وسد كل منافذ تواجدها، خصوصا بعد استخدام مجموعة من الطائرات التجارية لتنفيذ الهجمات، ولا يخفى أن كانت أجهزة الحاسب الآلي أداة رئيسية من تلك الأدوات التي استخدمها الفاعلون في القيام بهذا الفعل، والحق يقال فقد بدأت الجهود لمواجهة هذه الجرائم

حتى قبل تاريخ هذا الهجوم.ففي شهر أكتوبر من عام ١٩٩٩ اجتمع وزراء العدل والداخلية للدول الثماني الكبار في موسكو للبحث والتشاور حول كيفية مواجهة هذه الجرائم ومحاولة وضع حد لإفلات الجناة من العقاب، بما يتضمن بحث سبل ووسائل التواصل الإليكتروني بين الجناة من أجل تنفيذ أغراضهم الإجرامية، ورغم الرغبة الشديدة في مواجهة هذه الجرائم الخطرة، الا أن نتائج المؤتمر لم تؤدي بشكل ملحوظ إلى تحقيق الأهداف المرجوة، من أجل ذلك تمت الدعوة إلى مؤتمر أخر في شهر يوليو من عام ٢٠٠٠ ولكن هذه المرة على مستوى الرؤساء الذين اصدروا توصياتهم بضرورة البدء الفعلي في اتخاذ التدابير التي تتضمن اقتفاء أثر المجرمين وتسليمهم للعدالة للمحاكمة عن الجرائم التي ارتكبوها في هذه الفترة.

الأمر الذي دفع الوزراء مرة أخرى إلى تكثيف أعمالهم من خلال عقد عدة مؤتمرات متتابعة تمت بين عدة دول مثل فرنسا والمانيا واليابان، كما تم توجيه الدعوة الى العديد من الخبراء المتخصصين والمستشارين الفنيين في مجال تكنولوجيا المعلومات من الشركات المتخصصة، وعلى ذلك فقد شارك في هذه المؤتمرات ممثلون عن أكثر من مئة شركة متخصصة في هذا المجال. [٣]ثم جاءت أحداث الحادي عشر من سبتمبر ٢٠٠١ لتضع هذه الجهود في موضع آخر، ولتثبت للجميع أن مواجهة هذه الجرائم أصبحت ضرورة لا مفر منها، خصوصا مع استخدام الفاعلون أجهزة الاتصال مثل الحاسب الآلي والتليفونات المحمولة وكذا الاستعانة برسائل البريد الإليكتروني لتنفيذ الهجمات.والحق يقال فلم يخطأ الجانب الأوروبي لا في فهم المشهد ولا في قراءة هذا الحدث، فقد كان هذ الحادث الدافع الحقيقي وراء توقيع الاتفاقية الأوروبية لمكافحة جرائم الانترنت " بودابست " بتاريخ. ٢٠٠١ / ١١ / ٢٣ويرجع الفضل الى اتفاقية بودابست في إنشائها مظلة جزائية مشتركة تضم تحتها العديد من دول العالم، فقد وقعت ٣٠ دولة على هذه الاتفاقية كان من بينها ٢٦ دولة أوروبية، كما انضمت الولايات المتحدة الأمريكية وكندا، واليابان، وجنوب افريقيا، كما امتنعت ١٧ دولة عن التوقيعكان من بينها أيرلندا والدنمارك، ودخلت هذه الاتفاقية حيز التنفيذ في يوليو ٢٠٠٤ ، [٤]وتحتوي هذه الاتفاقية على ٤٨ مادة وتقسم على أربعة فصول وتتناول موضوعات عديدة من بينها الجرائم المتصلة بالحاسب الآلي، والجرائم الخاصة بالتعدي على حقوق المؤلف والمسائل الإجرائية بما فيها تسليم المجرمين وطبيعة التعاون الدولي بين الدول الأعضاء في مواجهة هذه الظاهرة الإجرامية، وموضوعات أخرى كثيرة.وفي عام ٢٠٠٣ تم وضع بروتوكول إضافي بهدف التأكيد على مضمون اتفاقية بودابست، حيث احتوى هذا البروتوكول على ١٦ مادة، وحدد هذا البروتوكول طبيعة العلاقة بين الاتفاقية الأم والبروتوكول المكمل لها. [٥]وفي عام ٢٠٢٢ تم وضع البروتوكول الإضافي الثاني للاتفاقية المتعلقة بالجريمة الإليكترونية بشأن تعزيز التعاون والكشف عن الأدلة الإليكترونية، حيث احتوى هذا البرتوكول على ٢٥ مادة، وقد كان من ضمن أهداف هذا البروتوكول حماية ضحايا الهجمات السيبرانية المتزايدة والحرص على إنصافهم وتحقيق العدالة، وكذا التأكيد على حماية المجتمع والفرد من خلال إجراء التحقيقات الجنائية والملاحقات القضائية الفعالة. [٦]وليس هذا فحسب ففي عام ٢٠٠٠ أصدر الإتحاد الأوروبي التوجيه رقم EC/٢٠٠٠/٣١ الصادر عن البرلمان الأوروبي ومجلس أوروبا بشأن الجوانب القانونية المحددة لخدمات مجتمع المعلومات، لاسيما التجارة الإليكترونية في السوق الداخلي، وفي عام ٢٠٠٢ تم إصدار التوجيه رقم EC/٢٠٠٢/٥٨ الصادر عن البرلمان الأوروبي ومجلس أوروبا بشأن معالجة البيانات الشخصية وحماية الخصوصية في قطاع الاتصالات الإليكترونية، وفي عام ٢٠٠٦ تم إصدار التوجيه رقم EC/٢٠٠٦/٢٤ الصادر عن البرلمان الأوروبي ومجلس أوروبا بشأن الاحتفاظ بالبيانات التي تم إنشاؤها أو معالجتها فيما يتعلق بتوفير خدمات الاتصالات الإليكترونية المتاحة للجمهور أو شبكات الاتصالات العامة، وفي عام ٢٠١٠ تم إصدار المشروع التوجيهي رقم ٥١٧ (٢٠١٠) COM الصادر عن البرلمان الأوروبي ومجلس أوروبا بشأن الهجمات ضد نظم المعلومات، وفي عام ٢٠١١ تم إصدار التوجيه رقم EU/٢٠١١/٩٢ الصادر عن البرلمان الأوروبي ومجلس أوروبا بشأن مكافحة الاعتداء الجنسي واستغلال الاطفال في المواد الإباحية.[٧]وعلى مستوى الدول الأمريكية فقد تم إبرام العديد من الاتفاقيات، ففي عام ١٩٨١ تم ابرام اتفاقية البلدان الأمريكية لتسليم المجرمين، وفي عام ١٩٨٤ تم ابرام اتفاقية البلدان الأمريكية بشأن الاختصاص القضائي في المجال الدولي بشأن فعالية الأحكام الأجنبية خارج الإقليم، وفي عام ١٩٩٢ تم إبرام اتفاقية البلدان الأمريكية بشأن المساعدة المتبادلة في المسائل الجنائية، وفي عام ١٩٩٣ تم ابرام اتفاقية البلدان الأمريكية لإنفاذ الأحكام الجنائية في الخارج وفي العام نفسه تم ابرام البروتوكول الاختياري المتعلق باتفاقية البلدان الأمريكية للمساعدة المتبادلة في المسائل الجنائية، وفي عام ٢٠٠٢ تم ابرام اتفاقية البلدان الأمريكية لمكافحة الإرهاب.وعلى مستوى الإتحاد الإفريقي فقد تم إبرام اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية لعام ٢٠١٤، حيث جرى اعتمادها في الدورة العادية الثالثة والعشرون، وذلك في مالابو بغينيا الاستوائية، وقد صدرت هذه الاتفاقية بأربع لغات مختلفة هي العربية والإنجليزية والفرنسية والبرتغالية، ولهذه اللغات نفس الحجية القانونية، وقد جاءت هذه الاتفاقية في ٣٨ مادة موزعة على أربعة فصول.وتهدف اتفاقية مالابو إلى تشكيل نص قانوني استراتيجي قادر على مكافحة الجرائم الإليكترونية في القارة السمراء، حيث ركزت هذه الاتفاقية على علاج موضوعات الأمن السيبراني بتوسع شديد، كما تضمنت سبل وآليات مكافحة الجريمة السيبرانية وكذا حماية البيانات الشخصية والإشراف على المعاملات الإليكترونية، وضمان تناسق

التشريعات الوطنية للدول الاعضاء وقدرتها على مواجهة هذه الطائفة الجديدة من الجرائم مع احترامها لحقوق الإنسان. .[٨]وعلى مستوى الدول العربية فقد تم إبرام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات حيث وافق عليها مجلسا وزراء الداخلية والعدل العرب في اجتماعهما المشترك المنعقد بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة بتاريخ ٢١ / ٢١ / ٢٠١٠، وقد حررت هذه الاتفاقية باللغة العربية فقط، كما جاءت في ٤٣ مادة موزعة على خمسة فصول. وقد صدر قرار رئيس جمهورية مصر العربية رقم ٢٧٦ لسنة ٢٠١٤ بشأن الموافقة على الانضمام للاتفاقية المذكورة. [٩]

## المبحث الأول: مبدأ الدفاع عن النفس في سياق الهجمات السيبرانية

يعتبر حظر استخدام القوة أو التهديد باستخدامها بين الدول الوارد في المادة (٢)(٤) من ميثاق الأمم المتحدة مبدأ أساسيا من مبادئ القانون الدولي العام، وقد تطور هذا المبدأ ليصبح عرفا دوليا وفقا لما جاءت به محكمة العدل الدولية في حكمها في قضية النشاطات العسكرية وشبه العسكرية في وضد نيكاراغوا لعام ١٩٨٦، [١٠]حيث ينطلق فهم هذا المبدأ من المادة ٢(٤) من ميثاق الأمم المتحدة والتي تنص على أنه على جميع الأعضاء في علاقاتهم أن يتخلصوا من التهديد باستخدام أو استخدام القوة ضد سلامة الإقليم أو الاستقلال السياسي لأي دولة، أو في أي حالة أخرى تتعارض مع مبادئ الأمم المتحدة[١١]إن موقع هذه المادة من الميثاق – بمجيئها ضمن مبادئ الميثاق والتركيبة اللغوية القوية التي جاءت بها تشير إلى مركزتيها في الميثاق لغايات الوصول إلى رؤية منظمة الأمم المتحدة في تحقيق الأمن والسلم الدوليين، من خلال عدم التهديد أو استخدام القوة. واستنادا إلى ذلك أصبحت وجهة النظر السائدة حول هذه المادة أنها قد خلقت حظرا عاما على استخدام القوة أو التهديد بها في سياق العلاقات بين الدول.

### المطلب الأول: شروط ممارسة حق الدفاع عن النفس

طبقا لميثاق الأمم المتحدة جاءت القاعدة العامة تؤكد على حظر استخدام القوة، وهذه القاعدة ورد عليها استثناء يتمثل في حق الدفاع الشرعي طبقا لنص المادة (٥١) من ميثاق الأمم المتحدة، وهذا الحق لا يتوافر إلا إذا اعتدت قوة مسلحة على إحدى دول أعضاء الأمم المتحدة[١٢]وتضمنت المادة (٥١) من ميثاق الأمم المتحدة على أنه لا يوجد في هذا الميثاق ما ينقص أو يضعف الحق الطبيعي للدول في الدفاع عن نفسها عند تعرضها لاعتداء مسلح، ولكي تنطبق حالة الدفاع الشرعي لابد من وجود اعتداء مسلح ، وذلك حسب ما ورد في المادة (٥١) من ميثاق الأمم المتحدة، وكذلك عند استخدام القوة أو التهديد حسب ما ورد في المادة (٤٢) من ميثاق الأمم المتحدة[١٣]ومما يجب ملاحظته أن المادة (٥١) من ميثاق الأمم المتحدة استخدمت مصطلح الاعتداء المسلح، والمادة (٢/ ٤) من هذا الميثاق استخدمت مصطلح القوة، وهذا يعنى أن المادة (٥١) من هذا الميثاق أعطت الدولة المعتدى عليها حق الرد بدون استخدام القوة[١٤]

**البند الأول: وجود هجوم غير مشروع** يحظر استخدام القوة طبقا للمادة (٢) (٤) من ميثاق الأمم المتحدة، وهذا مبدأ أساسي من مبادئ القانون الدولي العام إلا أنه يطبق في الحالات التي يقرها مجلس الأمن لحفظ السلم والأمن الدوليين، ومنها: حالة الدفاع الشرعي طبقا لميثاق الأمم المتحدة[١٥]وقد تطور هذا الأمر وأصبح عرفا دوليا وفقا لما جاء عن محكمة العدل الدولية في القضية المعروفة بـ النشاطات العسكرية وشبه العسكرية في قضية نيكاراغوا ١٩٨٦م.[١٦]واختلف الفقهاء بشأن المقصود به القوة الوارد في المادة (٢/٤) من ميثاق الأمم المتحدة إلى اتجاهين:الاتجاه الأول:يأخذ بالتفسير الضيق لهذه المادة، وهو أن المقصود بالقوة هذا هي القوة العسكرية فقط دون التهديد بها، وأن المقصود من نص المادة سالفة الذكر يجب أن تكون في حدود ديباجية الميثاق ونصوصه، ولكن غالبا ما يصطحب لفظ القوة في ميثاق الأمم المتحدة مصطلح المسلحة التي تم ذكرها في الديباجية في المادة (٤٤) من الميثاق، ويستند أنصار هذا الاتجاه إلى الاقتراح المقدم من البرازيل في مؤتمر سان فرانسوا بخصوص الضغط السياسي بحيث يكون من قبل الاستخدام غير المشروع للقوة، ولكن هذا المقترح قوبل بالرفض[١٧]الاتجاه الثاني:يأخذ أنصار هذا الاتجاه بالمفهوم الواسع للمادة سالفة الذكر، وبموجبه تشمل القوة العسكرية كل أنواع التهديد؛ لأن المادة (٢/٤) من هذا الميثاق جاءت مرنة بلفظ القوة أو التهديد به، وأن للهجوم السيبراني آثار مشابهة لمفهوم القوة العسكرية، كما أن الكود الضار أو الفيروسات لها خصائص ضارة يمكن أن تكون أداة للدمار، مثلها مثل السلاح الحربي واستدلوا أنصار هذا الاتجاه بأن ما صدر من محكمة العدل الدولية في الفتوى المتعلقة بشأن الأسلحة الدولية لا تشير إلى أسلحة محدودة، ومن ثم فإن ذلك ينطبق على الأسلحة السيبرانية أو على أنها قوة أيضا وذهب فريق آخر إلى أن المقصود بالقوة هو جميع صور استخدام القوة المسلحة ليس هذا فحسب، بل يشمل المصطلح أي صور أخرى يكون لها تأثير أو انتهاك واضح للأمن القومي للدولة وقد لعب الفضاء الإلكتروني دورا أساسيا في هذه الحرب حيث أصبح التفوق في هذا المجال عنصرا حيويا لهذه الهجمات التي يتم تنفيذها على الأرض أو الجو أو البحر من خلال التحكم والسيطرة التكنولوجية العالية الأمر الذي يستدعي بالضرورة تغيير مفهوم القوة[١٨]وإذا نظرنا إلى ما ورد

في دليل تالين تجد أنه يوجد نزاع مسلح دولي عندما تكون هناك أعمال عدائية، والتي قد تشمل أو تقتصر على العمليات السيبرانية، التي تحدث بين دولتين أو أكثر[١٩]والدليل على ذلك ما جاء في النسخة الأولى من دليل تالين ٢٠١١م في القاعدة ١١ منه، وهي التي تؤكد على أن العمليات الإلكترونية تعد استخداما للقوة عندما يكون مستواها وتأثيرها متقاربا مع العمليات غير الإلكترونية وتم إعداد النص من قبل مجموعة من الخبراء استندت إلى معيار الحجم والتأثير Effect and Scale لتحديد ما إذا كانت الهجمات الإلكترونية ترقى إلى الاستخدام غير المشروع للقوة – باستثناء ما ورد في المادة (٢/٤) من ميثاق الأمم المتحدة وفيما إذا كان ذلك بعد هجوما عسكريا يبرر الدفاع عن النفس طبقا للمادة ٥١ من ميثاق الأمم المتحدة وهذان المعيارات نفسهما – في الحجم والتأثير – هما اللذان استندت إليهما محكمة العدل الدولية في قضية نيكاراغوا )وتصدت أيضا محكمة العدل الدولية لهذه الإشكالية في قضية نيكاراغوا حيث تبين أن مبدأ استخدام القوة أو التهديد به يتحول إلى قاعدة عرفية دولية تلتزم به جميع الدول وهذا يتفق مع مبادئ الأمم المتحدة – ولا يجوز لأي دولة أن تخالفه [٢٠]وقد اعتبرت كل من محكمة العدل الدولية ومجموعة لجنة الخبراء لدليل تالين أن الاعتداء على الدولة بأي شكل من أشكال الاعتداء بما فيها الهجمات السيبرانية يشكل انتهاكا لسيادة الدولة طالما وصل حجم الاعتناء أو الهجوم إلى مستوى معين وعلى ذلك بعد إرسال قوة نظامية أو غير نظامية خارج حدود الدولة أو أي وسيلة أخرى بمثابة هجوم مسلح، وهذا خروج واضح للمحكمة عن النهج المعروف لفهم استخدام القوة، والذي يتمثل في صدور قرار صريح من الدولة باستخدام القوة المسلحة.[٢١]وتم التأكيد على ذلك عند صياغة المادة (٤ / ٢) من ميثاق الأمم المتحدة على أن أيه تهديد أو استخدام للقوة من قبل دولة بعد ذلك خرقا لهذه المادة يبرر حق الدفاع عن النفس [٢٢]وأما القول بأن الميثاق اشترط استخدام القوة وأن الهجمات السيبرانية لا يتوافر فيها ذلك فهذا القول يتنافى مع مقاصد الأمم المتحدة الذي حظر في الفقرة الرابعة من المادة الثانية اللجوء إلى الحرب أو التهديد باستعمال القوة أو استخدامه ضد سلامة الأراضي أو على أية وجه آخر لا يتفق مع مقاصد الأمم المتحدة ونجد أن ميثاق الأمم المتحدة ترك الأمر المجلس الأمن ليقرر كل حالة على حدة تبعا للظروف المحيطة بها[٢٣]وتم تجريم الهجمات التي ترتكب بشكل مباشر، ويكون لها تأثير مباشر أيضا مستندين إلى مبدأ التأثيرات، لكون أن هذه الأفعال يترتب عليها أضرار بالغة تلحق بالدولة وبعد إرسال القوات من الدولة أو بالنيابة عنها سواء كانت هذه القوات على شكل مجموعات نظامية أو غير نظامية مخالفاً للمادة (٤ / ٢) من الميثاق، ويمكن لمثل هذا التصرف أن يعد هجوما مسلحا طبقا لحجم القوة والتأثير .وذهب كل من شين، ورسيني إلى أنه من الممكن أن تكون الهجمات بمثابة خرق واضح لأحكام الفقرة الرابعة من المادة الثانية من ميثاق الأمم المتحدة شريطة أن تتسبب هذه الهجمات في دمار واسع المدى أو تعطيل للبنية التحتية وذهب لوارن جبريل[٢٤] إلى أن القانون الدولي الإنساني لا ينطبق على كافة الهجمات السيبرانية التي تقع خارج النطاق المسلح، ولكن ما جاء في اتفاقية جنيف الرابعة من استبدال مصطلح الحرب بمصطلح النزاع المسلح بهدف توسيع النطاق المادي لهذه الاتفاقيات لتطبيقها على هذه الهجمات، وجعل القانون الدولي الإنساني أيضا قابلا للتطبيق بناء على كل حالة على حدة".[٢٥]

ولكن قد تحدث الهجمات السيبرانية خارج نطاق النزاع المسلح، ولكنها ترتقى إلى مستوى الهجوم المسلح، وينتج عنها أضرار مادية وخسائر في الأرواح والممتلكات، ويمكن إثباتها أو نسبها لدولة معينة، فعندئذ يمكن تطبيق قواعد القانون الدولي الإنساني، بخلاف ما إذا كان لا تستطيع الدولة نسب هذا الهجوم إلى دولة معينة فهذا يمكن تطبيق القانون الدولي لحقوق الإنسان بالإضافة إلى تطبيق القانون المحلي للدولة المعنية وقد فرقت محكمة العدل الدولية في قضية نيكاراغوا بين الأشكال الأكثر خطراً والأقل خطورة واعتبرت الأشكال الأكثر خطرا هي التي تبيح استخدام حق الدفاع عن النفس وفقا لنص المادة (٥١) من ميثاق الأمم المتحدة، بخلاف الأقل خطورة [٢٦]خلاصة القول: إن الدعم غير العسكري قد يشكل انتهاكاً للمادة من ميثاق الأمم المتحدة، كما إن الاستخدام غير المشروع والاستغلال قد يشكل خطورة شديدة تضاهي في الحجم والأثر القوة العسكرية خاصة إذا كانت متعلقة بإصابات أو خسائر في أرواح المدنيين وفي هذه الحالة يمكن القول بأن ما ينطبق على الجرائم العسكرية ينطبق عليها باعتبارها جرائم لا تقل كثيرا عن الجرائم العسكرية.**البند الثاني: ضرورة الدفاع عن النفس** تنص المادة ٥١ على أنه لا يوجد في هذا الميثاق ما ينقص أو يضعف الحق الطبيعي للدول، بشكل فردي أو جماعي، في الدفاع عن النفس في الحالة التي تتعرض بها إلى اعتداء مسلح ...»[٢٧]إن أبرز الشروط التي أوردتها هذه المادة – في حدود غرض هذا البحث يتمثل في وقوع اعتداء مسلح على دولة ما حتى تتمكن هذه الأخيرة من استخدام القوة كرد على هذا الاعتداء [٢٨]إن أول ما يجب أن يثار في هذا السياق يتمثل في الاختلاف حول المصطلح المستخدم في المادة ٥١، وهو شرط الاعتداء المسلح لتفعيل الحق في الدفاع عن النفس ومصطلح استخدام القوة أو التهديد بها حسب المادة ٢(٤)ويلاحظ أن هاتين المادتين استخدمتا مصطلحات مختلفة كل منها يؤدي إلى خيارات قانونية متباينة أمام الدولة المعتدى عليها، ف الاعتداء المسلح» يضع الدولة المعتدى عليها امام خيار استخدام القوة، حيث يقرأ استخدام القوة هذا في سياق الدفاع عن النفس الذي قد يكون فرديا أو جماعيا حسب المادة ٥١، أما استخدام القوة أو التهديد بها» والذي لا يرقى إلى كونه اعتداء مسلحا، فيضع الدولة المعتدى عليها أمام خيارات قانونية أخرى ابرزها الإجراء المضاد والذي يعطي الدولة المتضررة

القدرة للرد على الاعتداء بطرق ما دون استخدام القوة [٢٩]الجدير ذكره أن فكرة الإجراء المضاد كخيار أمام الدولة المعتدى عليها والتي جاء النص عليها في المادة ٢٢ من مشروع مواد مسؤولية الدول عن الأفعال غير المشروعة ٢٠٠١ قد جاء مقيدا بمجموعة من الشروط أهمها شرط التناسب بين الخرق والخرق المقابل وهذا ما أكدت عليه محكمة العدل الدولية في قضية كوبسكوفو للعام١٩٩٧ [٣٠]وقد جاءت هذه التفرقة على اعتبار أن القانون الدولي قد وفر بعض الحماية للدولة التي تستخدم القوة في مواجهة دولة أخرى، عندما لا يرقى استخدام للقوة هذا إلى مستوى الاعتداء المسلح الفعلي[٣١] وبالرغم من وضوح هذا الفرق في التعبيرات ونتائجه القانونية يبرز التعقيد عند رسم الخط الفاصل بين استخدام القوة والاعتداء المسلح، والذي قد يكون في كثير من الحالات ضبابيا غير واضح المعالم، خاصة وأن ميثاق الأمم المتحدة ذاته قد خلا من أي نص يوضح هذه الفرق، وبالرغم من ذلك، يمكن الاستهداء إلى معالم هذا الخط الفاصل من خلال العودة إلى قرار محكمة العدل الدولية في قضية نيكاراغوا، حين وصفت «الاعتداء المسلح» بأنه اخطر شكل من أشكال استخدام القوة، وفي هذا الخصوص، بينت المحكمة في هذا القرار أن المناوشات المسلحة على الحدود – مثلا – لا ترقى إلى مرتبة الاعتداء المسلح الذي من شأنه تفعيل خيار الدفاع عن النفس وفقا للمادة ٥١ [٣٢]وكررت محكمة العدل الدولية هذا الموقف في عام ٢٠٠٣ في قضية منصات النفط بين إيران والولايات المتحدة، والتي تمحورت حول حادثة قيام الولايات المتحدة بتدمير مجموعة من منصات النفط الإيرانية في منطقة الخليج لعام ١٩٨٧ وفيما إذا كانت الولايات المتحدة مسؤولة عن هذا التصرف في ضوء اتفاقية الصداقة الموقعة بين البلدين في العام ١٩٥٥[٣٣]وفي ضوء ذلك يمكن لنا أن نتصور أن استخدام للقوة من قبل دولة معينة لا يرقى إلى اعتداء مسلح، مثل إطلاق النار على الحدود من دولة باتجاه دولة أخرى أو الاعتداء على المناطق المائية لدولة معينة، حيث إن هذه الأعمال تنطوي على استخدام للقوة، ولكنها لا ترقى إلى حالة الهجوم المسلح الذي يجيز الدفاع عن النفس وفقا للمادة ٥١.إلى جانب ذلك جاء قرار الجمعية العامة للأمم المتحدة رقم ٣٣١٤ لعام ١٩٧٤ الخاص بتعريف العدوان مشترطا الخطورة الكافية (Sufficient Gravity) كأحد متطلبات الهجوم العسكري[٣٤]، أما الفقه الدولي فقد كانت له اليد الطولى في تحديد هذا الخط الفاصل، وذلك يتجلى في مساهمات الفقيه الدولي Jean–Pictet» حين جاء بمجموعة من المعايير أو المتطلبات لاعتبار الاعتداء هجوم عسكريا وهي النطاق والشدة والمدة الزمنية[٣٥]، ويلاحظ أن هنالك عاملا مشتركا بين مجمل هذه التعريفات للهجوم العسكري وهو – باعتقادي الغموض، إذ من الصعوبة بمكان في كثير من الحالات بناء على هذه التعاريف تحديد ما إذا كان استخدام معين للقوة يرقى إلى حد الهجوم المسلح. ولكن بالرغم من هذا الغموض إلا أن هذه التعاريف تقود إلى نتيجة مفادها أن كل اعتداء مسلح في ضوء المادة ٥١ يعد في الوقت ذاته استخداما للقوة ولكن العكس غير صحيح فالهجوم بالأسلحة الفتاكة مثلا يعد استخداما للقوة وهجوما مسلحا في آن واحد، وبالتالي يجيز تفعيل المادة ٥١ لأنها قد حققت الشرط الوارد في المادة.وتجدر الإشارة إلى أن تفعيل المادة ٥١ واللجوء إلى الدفاع عن النفس في مواجهة هجوم مسلح لا يعني بأية حال أن الدولة التي تدافع عن نفسها غير مقيدة في طريقة رد الهجوم، بل على العكس من ذلك، لقد تضمنت قواعد العرف الدولي، إلى جانب المادة ٥١ من ميثاق الأمم المتحدة مجموعة من الشروط الواجب توافرها حتى يبقى التصرف متوافقا مع أحكام المادة، وهذه الشروط هي أولا: الضرورة، وثانيا: التناسب، وثالثا: الفورية [٣٦]أما شرط الضرورة فيقصد به الحالة التي تجبر فيها الدولة على اللجوء للدفاع عن النفس باستخدام القوة، حيث لم يعد اللجوء إلى الطرق السلمية لفض النزاع بحسب الفصل السادس من الميثاق [٣٧]خيارا، أو أن هذه الطرق قد تم اللجوء إليها ولكنها أثبتت عدم فعاليتها في مواجهة الدولة الأخرى [٣٨] ، ويضاف إلى ذلك أن شرط الضرورة قد جاء كمساحة إضافية للتأكد من نية الدولة المهاجمة والظروف التي تحيط بالهجوم، إذ خلال هذه المساحة الزمنية تعطى الدولة المعتدية فرصة إضافية يمكن أن تثبت خلالها مثلا – أن الاعتداء لم يكن مقصودا وأنها لا تسعى إلى حرب مع الدولة الأخرى.وأما التناسب فإن معناه يتجسد في مصطلح «الدفاع»، والذي يعني اتخاذ الإجراءات اللازمة والضرورية لرد الاعتداء وعدم تجاوزها، وهذا يتحقق في شبه التماثل بين الاعتداء والإجراءات المتخذة لرده من لدن الدولة المعتدى عليها، أو أن لا تتجاوز الإجراءات المتخذة الهدف التي يجب أن تسعى وراءه الدولة المعتدى عليها، وهو تحقيق الأمن والسلم الدوليين[٣٩] ، أما شرط الفورية فيقصد به أساسا أن لا تفوت الدولة المعتدى عليها فترة زمنية طويلة على الاعتداء قبل أن تقوم باتخاذ إجراءات الدفاع عن النفس، لأنه في هذه الحالة سوف ينتفي المنطق من إعطاء الدولة الحق في الدفاع عن نفسها دون اللجوء إلى مجلس الأمن صاحب السلطة الأساسية في حفظ الأمن والسلم الدوليين[٤٠]. بالرغم من ذلك يمكن لهذه الفترة الزمنية أن تمتد بصورة معقولة، وفي هذا تحقيق الشرط الضرورة أنف الذكر، والذي يوجب على الدولة المعتدى عليها التحقق من نية الدولة المعتدية وتجدر الملاحظة أن شرط الفورية ينظر إليه بنوع من الخصوصية في سياق الهجمات الإلكترونية، حيث يمكن لهذه الفترة الزمنية أن تمتد، آخذين بعين الاعتبار خاصية جوهرية للهجمات الإلكترونية تتمثل في التعقيد الذي يكتنف عملية التحقق من مصدر الاعتداء[٤١]

**المطلب الثاني: مبادئ التناسب والضرورة في الهجمات السيبرانية**

**البند الأول: مبدأ التناسب** مبدأ التناسب هو أحد المبادئ الرئيسية للقانون الدولي الإنساني وينطبق على جميع النزاعات المسلحة الدولية وغير الدولية. ومبدأ التناسب مبدأ عملي وميداني يحظر الهجمات المسلحة التي من المحتمل أن تلحق أضراراً جانبية بحياة المدنيين أو الممتلكات أو الأعيان المدنية أو البنية التحتية. وهذا المبدأ معترف به في المادتين ٥١ و٥٧ من البروتوكول الإضافي لاتفاقيات جنيف لعام ١٩٧٧.إن تطبيق هذا المبدأ فيما يتعلق بالطبيعة المحددة للهجمات السيبرانية عندما تكون سلاحاً أو وسيلة عسكرية في سياق النزاع المسلح، فيما يتعلق بعدم القدرة على الفصل بين الفضاء السيبراني المستخدم لأغراض مدنية أو من قبل المدنيين وبين الفضاء السيبراني المستخدم لأغراض عسكرية، هو صعوبات عند استخدامه من قبل أطراف النزاع. وينطوي مبدأ التناسب على تحقيق التوازن بين المعاناة والتدمير في مقابل المصالح العسكرية المنشودة، إذ لا توجد معايير واضحة لتقييم ما يشكل درجة مقبولة من المعاناة الإنسانية عند تدمير المرافق المدنية التي توفر الخدمات الأساسية للسكان وتضمن استمرار توفيرها.[٤٢]

**البند الثاني: مبدأ الضرورة** يتمحور مبدأ الضرورة في إطار القانون الدولي الإنساني حول فكرة مؤداها أن استعمال أساليب العنف والقوة في الحرب تقف عند حد قهر العدو وتحقيق الهدف من الحرب، وهو هزيمته وكسر شوكته وتحقيق النصر[٤٣] فإذا ما تحقق هذا الهدف وتم هزيمة العدو وإخضاعه أو استسلامه أمتنع على الطرف المنتصر التمادي في توجيه الأعمال العدائية ضد الطرف الآخر[٤٤]وقد ترتب على هيمنة مبدأ الضرورة في القانون الدولي الإنساني عدة قواعد أهمها : تقييد استخدام الأسلحة وحصرها في النطاق والقدر الضروري لحسم الحرب دون تجاوز ، فالضرورة تقدر بقدرها ، ولذلك تم التوصل إلى اتفاقيات تحرم استخدام أسلحة معينة مثل اتفاقية حظر استحداث وإنتاج الأسلحة البكتريولوجية والبيولوجية والتكسينية وتدمير هذه الأسلحة والملحق الخاص بها المؤرخة في ١٠ نيسان ١٩٧٢ ، واتفاقية حظر استخدام تقنيات التغيير في البيئة الأغراض عسكرية أو لأية أغراض عدائية المؤرخة في ١٠ كانون الأول ١٩٧٦ ، واتفاقية حظر أو تقييد استعمال أسلحة تقليدية معينة يمكن اعتبارها مفرطة الضرر أو عشوائية الأثر الموقعة في جنيف في ١٠ تشرين الأول ١٩٨٠ ، وبروتوكول بشأن الشظايا التي لا يمكن الكشف عنها المؤرخة في ١٠ تشرين الأول ١٩٨٠ ، والبروتوكولين الأول والثاني المتعلقين بحظر أو تقييد استعمال الألغام والإشراك الخداعية والنباتط الأخرى المؤرخين في ٣ أيار ١٩٩٦ ، وبروتوكول حظر أو تقييد استعمال الأسلحة المحرقة والبروتوكول الثالث جنيف ١٠ تشرين الأول ١٩٨٠وعلى الرغم من تلك النتائج فقد حذر بعض الفقهاء من الأخذ بوجه آخر لمبدأ الضرورة يكمن في اتخاذ حالة الضرورة كمبرر لخرق قواعد وأعراف الحرب ذاتها ، ولذلك رفض هذا الجانب الأخذ بحالة الضرورة ، وذهب بعض أنصار هذا الجانب إلى رفض المبدأ من أساسه في قانون الحرب ، فلا يمكن تبرير خرق مبدأ تحريم الأسلحة تحت مسمى الضرورة بمعنى إباحة استخدامها في حالة الخوف من زوال كيان الدولة ووجودها[٤٥]وعلى ذلك ، يجب حصر معنى الضرورة في إطار القانون الدولي الإنساني في حدود ما يخدم مبادئه وقواعده وليست ستار لخرق قواعد وأعراف الحرب التي غدت أمرا غير مشروعا، أما إذا اتخذت الضرورة كمبرر لحماية فئات القانون الدولي الإنساني فيجب إعمالها وتطبيقها ، ومثال ذلك لا يمكن تبرير قصف المدارس والمستشفيات والمناطق الآهلة بالسكان بدعوى اختباء العناصر المسلحة بها وأن هناك ضرورة عسكرية تبرر ذلك ، وإنما يمكن الاستناد إلى الضرورة لتبرير تقييد استخدام الأسلحة التقليدية من دبابات وطائرات ومدفعية وهي أسلحة مباحة أصلا في الحرب ( إذا كان من شأنها إبادة المدنيين مع المتمردين حيث ينبغي أن يقتصر القتال على الأسلحة الخفيفة لتجنب الخسائر والأضرار العشوائية والمفرطة[٤٦]

## المبحث الثاني: التعاون الدولي لمكافحة الهجمات السيبرانية

يُعدُّ التعاون الدولي لمكافحة الهجمات السيبرانية أمرًا بالغ الأهمية في عصر تكنولوجيا المعلومات والاتصالات. تتزايد التهديدات السيبرانية بشكل مستمر، مما يستدعي تضافر الجهود بين الدول لمواجهة هذه التحديات. يشمل التعاون تبادل المعلومات والخبرات بين الدول، مما يساعد في الكشف المبكر عن الهجمات وتطوير استراتيجيات فعالة للتصدي لها. كما تسهم المنظمات الدولية في تعزيز هذا التعاون من خلال وضع معايير وأطر عمل مشتركة، مما يسهل التنسيق بين مختلف الأطراف المعنية وعلاوة على ذلك، يتطلب النجاح في مكافحة الهجمات السيبرانية التزامًا من الحكومات والشركات والمجتمعات. يجب أن تتبنى الدول سياسات أمنية متكاملة وتستثمر في التعليم والتدريب لتعزيز القدرات المحلية. بالإضافة إلى ذلك، يعدّ تطوير تقنيات جديدة لمواجهة التهديدات السيبرانية ضرورة ملحة، مما يجعل الابتكار جزءًا لا يتجزأ من الاستجابة العالمية. من خلال التعاون الدولي، يمكن للدول تعزيز الأمن السيبراني وبناء عالم رقمي أكثر أمانًا للجميع.

### المطلب الأول: إنشاء الأطر القانونية الدولية

تعد الاتفاقيات والمعاهدات الدولية من أهم صور التعاون الدولي بصفة عامة، وفي مجال مكافحة الجرائم الناتجة عن الهجوم السيبراني بصفة خاصة ومن بين المعاهدات والاتفاقيات التي تعمل على مكافحة الجرائم السيبرانية معاهدة بودابست لمكافحة جرائم الإنترنت، وتوصيات المجلس

الأوروبي بشأن مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات **البند الأول: المعاهدات الدولية ذات الصلة** معاهدة بودابست لمكافحة جرائم الإنترنت تعد معاهدة بودابست لمكافحة جرائم الإنترنت أولى المعاهدات المتعلقة بتلك الجرائم، والتي تمت في العاصمة المجرية بودابست في ٢٣/١١/٢٠٠١، والتي تبرز التعاون والتضامن الدولي في محاربة الجرائم السيبرانية، ويعد التوقيع على تلك المعاهدة الدولية الخطوة الأولى فى مجال تكوين التضامن الدولي ضد تلك الجرائم التي تتم عبر شبكة الإنترنت والاستخدام السيء لها[٤٧] وقد وقعت على تلك المعاهدة ٢٦ دولة أوروبية بالإضافة إلى كندا واليابان، وجنوب أفريقيا والولايات المتحدة الأمريكية، وتوفر المعاهدة أسس الأمن العام، وتتضمن ٤٨ مادة على أربعة فصول كالاتي الفصل الأول : تعريفات خاصة ببعض التعريفات الفنية.الفصل الثاني يتضمن الإجراءات اللازم اتخاذها على المستوى المحلي لكل دولة وتنقسم إلى قسمين:القسم الأول: يتعلق بالنصوص الجنائية الموضوعية على النحو التالي:بشأن الجرائم ضد الخصوصية وسلامة وتواجد معلومات الحاسب ونظم الحاسب، ويشمل وصفا لأنواع متعددة من الجرائم.الجرائم المتصلة بالحاسب شاملة استخدام الكمبيوتر في التزوير والأفعال الاحتيالية. الجرائم المتعلقة بالمحتوى والمضمون الجرائم المتصلة بالتعدي على حقوق المؤلف.القسم الثاني: القانون الإجرائي فيما يتصل بالإجراءات الجنائية شاملة الحفاظ على المعلومات المخزنة والأوامر الخاصة بتسليم الأدلة، وتتضمن كذلك تفتيش وضبط بيانات الحاسب المخزنة.الفصل الثالث مسائل التعاون الدولي وتسليم الجناة والمساندة المشتركة والتعاون في التحريات وجمع بيانات المرور والحركة الخاصة بالبيانات.الفصل الرابع: يتعلق بالانضمام والانسحاب من تعديل المعاهدة وفض المنازعات والتشاور بين الأعضاء.وعلى الرغم من أن هذه الاتفاقية أوروبية المنشأ، إلا أنها مفتوحة للدول الأخرى لطلب الانضمام إليها لتعم الفائدة. وتتضمن الاتفاقية التعاون والعمل المشترك ما بين الدول الأعضاء وأعضاء القطاعات وأصحاب المصلحة ذوي الصلة، وهما ضروريان لبناء ثقافة للأمن السيبراني وفي الحفاظ عليها، وسبل مكافحة الجرائم السيبرانية، إذ تقرر [٤٨]مواصلة اعتبار الأمن السيبراني في صدارة أنشطة الاتحاد ذات الأولوية. والاستمرار فى إطار مجالات اختصاصاته الرئيسية بدراسة مسألة توفير الأمن وبناء الثقة في استعمال الاتصالات تكنولوجيا المعلومات والاتصالات من خلال إذكاء الوعي، وتحديد أفضل الممارسات، وتطوير مواد التدريس المناسبة لتعزيز ثقافة الأمن الإلكتروني.تعزيز العمل والتعاون وتبادل المعلومات مع جميع المنظمات الدولية والإقليمية ذات الصلة فيما يتعلق بالمبادرات المتصلة بالأمن السيبراني في مجالات اختصاصاتها، مع مراعاة احتياجات مساعدة البلدان النامية.تعيين نظام سريع وفعال للتعاون الدولي، والحفاظ بشكل سريع على البيانات المخزنة على أجهزة الكمبيوتر وحفظها والإفصاح الجزئي عن حركة هذه البيانات المخزنة على الكمبيوتر[٤٩]هذا وقد تناولت المعاهدة الجرائم التي تعتبر من أكثر الجرائم شيوعا على مستوى العالم مثل الإرهاب السيبراني وعمليات تزوير بطاقات الائتمان ودعارة الأطفال. كما حددت المعاهدة الطرق الواجب اتباعها في التحقيق في جرائم الإنترنت، وتعهدت الدول الموقعة بالتعاون من أجل محاربتها، كما حاولت المعاهدة إقامة التوازن بين الاقتراحات التي تقدمت بها أجهزة الشرطة، وما عبرت عنه المنظمات المدافعة عن حقوق الإنسان ومزودي خدمات الإنترنت من قلق، حيث تخشى منظمات حقوق الإنسان من أن تحد المعاهدة من حرية الأفراد، وأن تؤدي الرقابة إلى انتهاك حقوق مستخدمي الإنترنت[٥٠].وفي عام ٢٠١٦ أصدرت لجنة اتفاقية الجرائم السيبرانية مذكرة توجيهية تتعلق بجوانب الإرهاب السيبراني بموجب اتفاقية بودابست، تعلن فيها أن الجرائم الموضوعية في الاتفاقية قد تكون أيضا أعمالا إرهابية على النحو المحدد في القانون المعمول به .. وجاءت هذه المذكرة الإضافية بموجب الاتفاقية في الوقت المناسب التسلط المذكرة الضوء على أن هذه الاتفاقية ليست معاهدة مختصة بالإرهاب، إلا إنه يمكن القول: أن الجرائم الموضوعية في الاتفاقية يمكن أن تنفذ على أنها أعمال إرهابية، لتسهيل الإرهاب ولدعم الإرهاب، ومن ذلك الجانب التمويلي، أو الأعمال التحضيرية .[٥١]**البند الثاني: القواعد العرفية الدولية** وعلى الرغم من تزايد وتيرة الهجمات السيرانية والمخاطر المصاحبة لها، هناك غياب ملحوظ الإطار القانوني دولي شامل التنظيم هذه الأنشطة ومع ذلك، فإن هذا لا يعني النقص المطلق في المجهود الدولية المعالجة قضايا الأمن السيبراني، لقد كانت هناك مبادرات مهمة من قبل المنظمات الدولية والإقليمية مثل الأمم المتحدة وحلف العمال الأطلسي ومجلس أوروبا الهدف إلى التخفيف من هذه التهديدات بالإضافة إلى ذلك، التحدت كيانات عالمية مختلفة تدابير تساهم بشكل غير مباشر في إدارة منهجيات المهجمات السيوانية التي يمكن تكييفها لمكافحة الأنشطة السيوانية الضارة. على سبيل المثال، قد تقدم اللوائح التي وضعها الاتحاد الدولي للاتصالات منذ عام ١٩٤٧ إلى جانب القوانين التي تحكم الجو والبحر والقضاء أدوارا ذات صلة في معالجة الجوانب المتعلقة بالأمن السيراني (٩٠)واستنادا إلى مبادئ القانون الدولي الإنساني، فإن شرط مارتنز ( la clause de Martens) وهي وسيلة فعالة المواجهة التطورات التقنية في وسائل وأساليب القتال كما وردت لأول مرة في القافية لاهاي الثانية العام ١٨٩٩ والذي ينص على في الحالات التي لا تنطبق فيها المعاهدات أو القانون العربي، يتمتع المدنيون والعسكريون بالحماية بموجب مبادئ القانون الدولي المستمدة من الأعراف الراسخة، ومن المبادئ الإنسانية، ومن ما عليه الضمير العام"، وانطلاقاً من هذا المعنى، يمكن حظر الأسلحة التي يكرهها الضمير العام [٥٢]

**أولا التعاون الدولي في مواجهة المحجوم الإلكتروني (السيران)**إن مسألة مواجهة الهجمات الإلكترونية (السيرانية) عند تناولها بشكل عام، قد كبير وتفرح عن عدة مواضيع بحكم ارتباطها لهما، ومواجهتها في الجانب الفني على أساس أن الهجوم السيبراني كجريمة في إحدى الجرائم التي لا يمكن أن يرتكبها إلا شخص متخصص تقنيا في تفاصيل وخفايا تكنولوجيا المعلومات وشبكات المعلومات، بالإضافة إلى الجانب القانوني في مواجهة الآثار وانتهاكات الحقوق الناجمة عن هذه الجرائم، وكذلك على المستوى القانوني تجد أن الرد القانوني قد يكون على المستوى الوطني أو المحلي للدول، ويكون ويمكن أن تكون على المستوى الدولي على أساس أن هذه الجريمة في حرية عابرة للحدود ولها طبيعة عابرة للحدود الوطنية والدولية[٥٣] من الممكن أن يشارك أكثر من شخص في أكثر من دولة في ارتكاب جريمة واحدة يصبح ضحيتها عدة أفراد مقيمين في دول متعددة، ومما يزيد الأمر صعوبة هو اختلاف البيئات والعادات والتقاليد والثقافات والأديان بين الدول المتصلة بالأنترنت مما يؤدي إلى اختلاف التشريعات المتعلقة بالقضايا الأساسية بين الدول الشرق والغرب والعالم الإسلامي قد يتم بت معلومات أو صور على الإنترنت، وقد تكون هذه المعلومات قانونية في البلد الأصلي، ولكنها قد تكون غير قانونية في بلد آخر. كما أن اختلاف التشريعات في تجديد اختصاصها الحالي بسبب تعدد الأسس التي يقوم عليها هذا الاختصاص قد يؤدي إلى ... تضارب الاختصاص بين الدول فيما يتعلق بالجرائم الإلكترونية العابرة للحدود، قد يحدث أن ترتكب جريمة على أراضي دولة معينة ويكون مرتكب الجريمة شخصا أجنبيا، ومن ثم فإن هذه الجريمة تخضع للولاية الجنائية للدولة الأولى على أساس مبدأ الإقليمية، كما تخضع أيضا للولاية القضائية الدولة الثانية على أساس مبدأ الاختصاص الشخصي في جانبه الإيجابي[٥٤]وتنشأ فكرة تنازع الاختصاص القضائي أيضا في حال قيام الاختصاص على مبدأ الإقليمية، كأن يقوم مرتكب الجريمة بين معلومات غير قانونية أو صور إباحية من أراضي دولة معينة وتم مشاهدتها في دولة أخرى، ووفقاً لمبدأ الإقليمية، يتم تجديد الولاية القضائية الجنائية والقضائية لكل دولة من البلدان. المتضررة من الجريمة وسواء وقع فعل الإذاعة أو الذي وقع نتيجة الفعل، فهنا نجد أن الأمر سيترتب عليه المخالفة مبدأ عدم جواز محاكمة الشخص على الفعل الواحد أكثر من مرة، وهو واحد للمبادئ الأساسية التي يقوم عليها القانون الجنائي [٥٥]

أولاً: التعاون الدولي بين الأجهزة الشرطية:أدى التطور الكبير في وسائل النقل بشكل عام وشبكة المعلومات بشكل خاص إلى انتقال المجرمين من دولة إلى أخرى لقد أدرك المجتمع الدولي أنه أصبح من المستحيل على أي دولة القضاء على الجرائم العابرة للحدود، لأن الإجراءات العامة الأجهزة الشرطة في كل دولة لا تجعل أجهزتها الأمنية تتعقب المعرفين وتتابعهم إذا تجاوزوا حدود الدولة، وعليه لا بد من تعاون الأجهزة الشرطية بين الدول وتنسيق العمل فيما بينها الملاحقة المجرمين. ومن أبرز مظاهر التعاون إنشاء المنظمة الدولية للشرطة الجنائية "الإنتربول" والظهور العديد من أشكال وأشكال ووسائل التعاون بين الأجهزة الشرطية. وهذه الصور والطرق في كما يلي[٥٦]

ثانيا ربط شبكات الاتصالات والمعلومات يتم الاتصال بين وكالات العدالة الجنائية الوطنية بشكل عام وأجهزة الشرطة بشكل خاص، وبين تلك الأجهزة في البلدان الأخرى من خلال السلك الدبلوماسي، وبما أن الاتصالات الشرطية تحتاج إلى الصالات خاصة لتحقيق السرعة المطلوبة، فقد حاولت منظمة الشرطة الجنائية الدولية (الإنتربول) وكذلك العديد من الدول تطوير أنظمة الاتصال وتبادل المعلومات فيما بينها، بحيث يمكن الوصول إلى المجرمين وملاحقتهم في أسرع وقت حيث يغادرون البلد الذي ارتكبت فيه الجريمة، التسارع أجهزة شرطة البلد الصحية إلى الاتصال بأجهزة الأمن في البلد الذي انفقوا معه على الأمن للقيام بملاحقة المحرمين داخل حدود بلدهم الذي قرارهم[٥٧]

ثالثا المنظمة الدولية للشرطة الجنائية (الإنتربول) بعد الإنتربول أهم آلية المتعاون الشرطي الدولي لمكافحة الجرائم العالمية العابرة للحدود الوطنية بشكل عام والجرائم الإلكترونية بشكل خاص مهمة الإنتربول الأساسية في تفعيل التعاون بين الأجهزة الشرطية في الدول الأعضاء في المنظمة من خلال توحيد إجراءات تسليم المجرمين، ومن خلال تنسيق العمل الشرطي وجمع البيانات وتبادل المعلومات التسهيل أجهزة التحقيق لضبطهم ... ملاحقة المجرمين الحارين وتسليمهم إلى الجهات الأمنية الدولة التي تطلب تسليمهم، وإنشاء وتطوير كافة الأنظمة القادرة على المساهمة بفعالية في منع جرائم القانون العام والمعافية عليها [٥٨] تسند هذه المهمة إلى المكاتب المركزية والوطنية في كل دولة عضو وإلى عينة دائمة تعريتها السلطات الحكومية الوطنية، وتساعدها فرق الإنتربول للعمل في الأحداث التي يمكن أن تسهل مجموعة من خدمات التحقيق والتحليل في موقع الموقع الحفل بالتنسيق مع الأمانة العامة. يقوم الإنتربول بتعميم التحذيرات والتنبيهات المضمنة المعلومات الاستخباراتية والإحاطات والمنشورة التحليلية والفنية بشأن المخاطر الإجرامية المحتملة، ويستخدم الإنتربول أدواته الخاصة، مثل نظام النشرات الدولية بمختلف أنواعها، والتحقيق في قواعد البيانات، وتقديم الحوات والدورات التدريبية في مجال مكافحة الجرائم الإلكترونية. المساعدة تحية من الخبراء الدوليين والمختبرات الدولية على المستوى العالمي، وتسهيل تبادل البيانات الجمالية وتحليلها وتعريبها وتقوم المنظمة بتزويد شرطة الدول الأطراف بأدلة إرشادية حول الجرائم

الإلكترونية وكيفية التدريب على مكافحتها والتحقيق فيها وبعد الجرائم المالية المرتبطة بالتكنولوجيا المتقدمة إحدى الجرائم التي يركز عليها الإنتربول [٥٩]

**رابعا تبادل المعاونة لمواجهة الكوارث والأزمات** في حالة الأزمات وفي المواقف الحرجة، يعتبر عنصر الوقت أحد الأمور الحاسمة في مواجهة تلك الأزمة أو الكارثة، الأمر الذي يتطلب تكثيف وزيادة الجهود والخبرات والإمكانات، وهو ما لا يتأتى إلا بتركيز الجهود الدولية في التجاه واحد طريق على سبيل المثال: مشاركة قوات الإنقاذ والدفاع المدني للدول المنكوبة بالزلازل والأعاصير والفيضانات أو المشاركة مع خواه أو توفير معدات متطورة، وكذلك المشاركة بقوات خاصة أو خبراء أو معدات في تحرير الرهائن المحتجزين أو احتلال المباني المهمة، أو طائرات أو سفن المختطفة [٦٠]

**خامسا مظاهر القيام ببعض عمليات شرطية دولية مشتركة**

١- شرطة الويب الدولية .تأسست هذه المنظمة في الولايات المتحدة الأمريكية عام ١٩٨٦ تتلقي الشكاوي من مستخدمي الشبكة وملاحقة الجناة والمتسللين إلكترونيا والبحث عن الأدلة ضدهم وتقديمهم للمحاكمة، ويضم فريق العمل في علم المنظمة متخصصين من جهات إنفاذ القانون والمؤسسات الحكومية وضباط الشرطة والمتطوعين الفنيين من ٦١ دولة حول العالم، ونظراً لاتساع نطاق نشاط على المنظمة، إن التنظيم والإجراءات التي تتخذها بالتعاون مع أجهزة المعاد القانون في الدول الأعضاء تسهل على فريق العمل تتبع الأنشطة الإجرامية المرتكبة عبر شبكة الإنترنت في جميع أنحاء العالم، وفي إطار مسألة الضوابط القانونية التي تحكم حركة المعلومات عبر الإنترنت، هناك من يرى أنه من الضروري وضع ضوابط وقواعد لا تؤدي إلى المساس بالحريات العامة في تبادل المعلومات وحقوق الإنسان على حد سواء من ناحية، وعدم استخدام الشبكة الأغراض إجرامية أو نشر مواد إباحية نظر المجتمع من ناحية أخرى

**سادسا مركز بلاغات احتيالات الإنترنت** تأسس هذا المركز في الولايات المتحدة الأمريكية عام ٢٠٠٠ للتعاون مع مكتب التحقيقات الفيدرالي FBI والمركز القومي الجرائم ذوي الياقات البيضاء National white collier crime center وذلك بهدف تلقي البلاغات وتتبع الجرائم وعمليات الاحتيال المرتكبة عبر الإنترنت بالتنسيق مع الجهات الرقابية والرقابية المعنية داخل وخارج الولايات المتحدة الأمريكية من خلال الموقع الإلكتروني للمركز على الشبكة الدولية.ومن أجل تشديد الرقابة على شبكة الإنترنت، طبقت دولة الإمارات العربية المتحدة ما يعرف بنظام الرقيب Proxy والذي يستعرض جودة الخدمات المقدمة عبر الإنترنت عندما يطلب أحد المشتركين موقعا على الشبكة الرئيسية، تصل الإشارة إلى الرقيب الذي بدوره يعرض الموضوع على قائمة كبيرة جدا من المواقع المحظورة، فإذا تبين له أن الموقع المطلوب يقع ضمن هذه القائمة المحظورة

ثانياً: تعاون السلطات القضائية للدول:ويوازن التعاون القضائي الدولي بين استقلال الدولة في ممارسة اختصاصها الحالي داخل حدود إقليمها، وضرورة ممارسة حقها في العقاب، ولا يمكن لهذا التعاون، من الناحية العملية، أن ينشئ حقه في العقاب، ومع ذلك، فإن التعاون الدولي ضروري لسين السبب الأول: تلتزم الدولة بحدودها الإقليمية ويجوز أن يعتد قانون العقوبات في نطاق تطبيقه إلى ما يتجاوز حدود إقليم الدولة إلا أنه لا يمكن البدء بإجراءات خارج التراب الوطني لأن ممارستها تنتهك سيادة الدول الأجنبية الأخرى.السبب الثاني: ولا يجوز تطبيق قانون العقوبات دون قانون الإجراءات الجزائية تعدد الإجراءات الجزائية الوسيلة اللازمة لتطبيق قانون العقوبات ونقله من حالة السكون إلى الحركة. ولذلك، إذا كان تطبيق قانون العقوبات يقتضي توجيه بعض الإجراءات الجزائية خارج حدود الإقليم الدولة، فلا يجب أن العظيم مشكلة الحدود الإقليمية بين الدول ولا بد من اللجوء إلى التعاون القضائي للتغلب على هذه الصعوبة، ويتمثل هذا التعاون في مجموعة من الوسائل التي من خلالها تقوم إحدى الدول المساعدة بإخضاع سلطاتها العامة أو مؤسساتها الفضائية السلطة التحقيق أو الحكم أو التنفيذ في دولة أخرى [٦١] تحمد المساعدة القانونية عدة أشكال:

١- تبادل المعلومات يتمثل ذلك في تقديم المعلومات والمستندات التي تطلبها جهة فضائية أجنبية بشأن جريمة ما بشأن الاتهامات الموجهة ضد رعايتها في الخارج والإجراءات المتحدة ضدهم كما أن هناك جانب آخر التبادل المعلومات، وهو ما يتعلق بالسوابق القضائية للجناة، والتي من خلالها تعرف السلطة القضائية بدقة على الماضي الإجرامي للفرد الحال إليها، كما تساعد في تنفيذ الأحكام المتعلقة بالعودة، ووقف الجريمة تنفيذ الحكم، وفقدان الأهلية

٢- نقل الإجراءات نقل الإجراءات يعني أن تقوم الدولة، بناء على اتفاق، باتخاذ الإجراءات الجمالية فيما يتعلق بجريمة ارتكبت في إقليم دولة أخرى والصالح هذه الدولة إذا توافرت الشروط التالية:أن يكون الفعل المنسوب إلى الشخص يشكل حريفة في الدولة الطالبة والدولة المطلوب منها.

يجوز لأي طرف متعاقد أن يطلب من أي طرف آخر اتخاذ الإجراءات الجنائية في أي من الحالات التالية:إذا كان المتهم محكوماً عليه أو سوف يحكم عليه بعقوبة مقيدة للحرية في الدولة الطالبة.. إذا كانت الإجراءات المطلوب اتخاذها منصوص عليها في قانون الدولة المطلوب إليها بالنسبة النفس الجريمة. أن تؤدي الإجراءات المطلوب اتخاذها إلى الوصول إلى الحقيقة مثل وجود أدلة على الحريمة في الدولة المطلوب منها إذا كان تنفيذ العقوبة في الدولة المطلوب إليها تحقق التأهيل الاجتماعي للمحكوم عليه.إذا كمال حضور المتهم في الجلسة غير مضمون في الدولة الطالبة بينما حضوره مضمون في الدولة الطالبة بينما حضوره مضمون في الدولة المطلوبة ويجوز الدولة المطلوب إليها أن ترفض نقل الإجراءات في الحالات الآتية:إذا كان طلب نقل الإجراءات غير مبرر بأن الأسباب التي ذكرتها الدولة الطالبة لا تستدعي اتخاذ مثل هذه الإجراءات.إذا ثبت أن الدافع وراء طلب نقل الإجراءات هو الاعتبارات عنصرية أو دينية أو سياسية.إذا كانت الدولة المطلوب إليها قد طبقت قانونها على الجريمة قبل استلامها من الدولة الطالبة وكان الإجراء الذي تم اتخاذه سابقاً وفقا للقانون.. إن كانت الإجراءات التي تطلبها الدولة الطالبة تخالف الواجبات التي تقوم بها الدولة الطالبة.. إذا كانت الإجراءات المطلوبة تخالف للمبادئ الأساسية للنظام القانوني في الدولة المطلوبة إلا أن هناك رأيا يعتقد بحق أن تطبيق هذه الآليات التقليدية للاتفاقيات يثير بعض الإشكاليات، مثل وجود معوقات خاصة بالجرائم المرتكبة عند الإنترنت، ورغم أن هذه العقبات موجودة على المستوى المحلي أو الوطني، فإنها تنشأ أيضا على المستوى الدولي الإنابة القضائية الدولية:بعد الإنابة القضائية أحمد أشكال المساعدة القضائية للتعاون الجزائي الدولي، حيث تمكن دولة ما من الاستفادة من السلطات العامة لدولة أخرى إذا كانت الحدود الإقليمية تمنع إنفاذ قانونها عند المحرم [٦٢]والمقصود بالتفويض القضائي الدولي هو طلب اتخاذ إجراء فضائي من إجراءات الدعوى الجزائية المقدمة من الدولة الطالبة إلى الدولة المطلوب إليها الضرورة ذلك للبت في أمر معروض على السلطة القضائية في الدولة الطالبة وما يستحيل عليه أن يفعله بنفسه وعليه فإن الإنابة القضائية هي إجراء التسهيل الإجراءات الجنائية بين الدول الضمان إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة، والتغلب على علية السيادة الإقليمية التي تمنع الدول الأجنبية من ممارسة بعض الأعمال القضائية داخل الإقليم من بلدان أخرى، ومن الأمثلة على ذلك سماع الشهود وإجراءات القامة الدعاوى الجنائية وتتم الإنابة القضائية بين الدول من خلال اتفاقيات تتضمن شروط وطرق تنفيذ الإنابة القضائية، وغالباً ما تتضمن شرط استبعاد تنفيذ الأحكام في المحالات السياسية والضريبية والعسكرية، أو إذا قدرت الدولة المطلوب إليها أن التنفيذ المطلوب من شأنه الإخلال سيادة الدولة أو النظام العام أو المصباح الأساسية مما يترك للدولة سلطة تقديرية في تنفيذ أو عدم تنفيذ ما يطلب منها خوفاً من تحميلها المسؤولية الدولية عن إعمالها، وفي حالة عدم الاتفاق، لا الجوز تنفيذ الإنابة القضائية إلا بموافقة الدولة المطلوب إليها ذلك وفقاً للإجراءات والشروط المنصوص عليها في قانونها الداخلي [٦٣]

## المطلب الثاني: دور المنظمات الدولية في الأمن السيبراني

حاولت الدول حماية مصالحها من التضرر بسبب استهدافها بعمليات سيبرانية مختلفة، أو استهداف الشركات الخاصة بها ومواطنيها، فسعت من خلال عضويتها في منظمات دولية، أو من خلال تشريعاتها الوطنية، إلى محاولة تنظيم هذه العمليات، كما شاركت في بعض المؤتمرات لنفس الغرض، وتعرض لبعض هذه الممارسات من خلال:**البند الأول: الأمم المتحدة** تلعب العديد من المنظمات وعلى رأسها منظمة الأمم المتحدة دورا هاما في تعزيز العمل المشترك بين الدول للحد من انتشار الجرائم المعلوماتية، ومواجهة المخاطر السيبرانية، وعقدت في سبيل ذلك العديد من المؤتمرات بداية من المؤتمر السابع الذي عقد في ميلانو ١٩٨٥ حتى المؤتمر الثاني عشر فى ٢٠١٠ بالإضافة إلى المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات والذي عقد تحت إشراف الأمم المتحدة في عام ١٩٩٤ ، ونتج عنه عدة توصيات ذات صلة بجرائم المعلومات بعضها تناول الأفعال التي تقع تحت طائلة الإجرام المعلوماتي، والبعض الآخر يتمثل في الإجراءات الواجب اتباعها لتطبيق القواعد الموضوعية. وهكذا أصدرت منظمة الأمم المتحدة عدة قرارات وتوصيات بشأن العمليات السيبرانية، كما أنشأت فرقا من الخبراء الحكوميين المعنيين بهذه العمليات، وناقشت هيئاتها أمن الفضاء السيبراني، وفيما يلي بيان ذلك **قرارات ووثائق الجمعية العامة للأمم المتحدة بشأن الإرهاب السيبراني**

أصدرت الجمعية العامة للأمم المتحدة عدة قرارات بشأن جرائم الإرهاب السيبراني، منها القرار رقم ٥٥/٦٣ في ٤ ديسمبر ٢٠٠٠م، والقرار رقم ٥٦/١٢١ في ١٩ ديسمبر ٢٠٠١، بشأن مكافحة سوء استخدام تكنولوجيا المعلومات، وقد أوصى القرار الأول بأن تضمن الدول في قوانينها وممارساتها عدم توفير ملاذات آمنة لكل من يسيء استخدام تكنولوجيا المعلومات، وضمان حماية سرية المعلومات وسلامة أنظمة الحاسوب، ضد أي اعتداء غير مشروع، مع تقرير عقوبة على ذلك الفعل. ودعا القرار ٥٦/١٢١، الدول الأعضاء عند وضع التشريعات الوطنية لمكافحة إساءة استعمال تكنولوجيا المعلومات، على أن تأخذ بالاعتبار عمل لجنة منع الجريمة والعدالة الجنائية. وفي عام ٢٠٠٢ أصدرت الأمم المتحدة القرار رقم ٥٧/٢٣٩، بشأن إرساء ثقافة عالمية للأمن السيبراني، حيث اعتمدت فيه قرارا بشأن الأمن السيبراني والذي سلمت فيه بضرورة دعم الجهود

الوطنية بتبادل المعلومات والتعاون في هذا المجال على الصعد الوطنية والإقليمية والدولية كي يتسنى التصدي الفعال لما تتسم به هذه التهديدات السيبرانية بصفة متزايدة من طابع عابر للحدود الوطنية. ويشهد هذا القرار على التزام العالم بإنشاء ثقافة عالمية للأمن السيبراني، وأهم ما في القرار أنه يؤكد أن الأمن السيبراني للهياكل الأساسية الحيوية للمعلومات مسئولية ملقاة على عاتق الحكومات، ومجال يجب عليها أن تحمل فيه لواء الصدارة وطنيا، بالتنسيق مع أصحاب المصلحة ذوي الشأن.وفي عام ٢٠٠٥ أصدرت الأمم المتحدة القرار ١٧٧/٦٠، بشأن تشجيع التعاون الدولي لمكافحة الجرائم الإلكترونية، وتقديم المساعدة للدول الأعضاء في هذا المجال، كما أصدرت في عام ٢٠١٠ ، القرار رقم ٢١١/٦٤ الذي يدعو الدول إلى تحديث قوانينها فى مجال الجرائم الإلكترونية، والخصوصية، والبيانات الشخصية، والتجارة والتوقيع الإلكترونيين، وكذلك اعتماد اتفاقيات إقليمية بهذا الشأن .[٦٤]ودعا القرار رقم ٦٥/٤١ والذي صادقت الجمعية العامة للأمم المتحدة عليه في يناير ٢٠١١ على تقرير فريق الخبراء الحكوميين في مجال المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي. وتضمنت استنتاجات فريق الخبراء من بينها ما ذكرته من أن هناك دول تستحدث تكنولوجيا المعلومات والاتصال كوسائل للحرب والاستخبارات، وتلفت اللجنة الدولية في هذا الصدد انتباه الدول إلى عواقب الحرب السيبرانية، وهي مجموعة من الهجمات على شبكة الحواسيب خلال حالات النزاع المسلح، وقد تشمل هذه العواقب سيناريوهات كارثية مثل: التشويش على نظم مراقبة الملاحة الجوية، والتسبب بتصادم الطائرات أو تحطمها، أو قطع إمدادات الكهرباء أو الماء على السكان المدنيين، أو إلحاق أضرار بالمرافق الكيميائية أو النووية. وتذكر اللجنة الدولية بضرورة التزام كل الأطراف في النزاعات المسلحة باحترام قواعد القانون الدولي الإنساني إذا لجأت إلى وسائل وأساليب الحرب الإلكترونية ومن هذه القواعد مبادئ التمييز والتناسبية والحيطة ).[٦٥]**قرارات المجلس الاقتصادي والاجتماعي** قرارات المجلس الاقتصادي والاجتماعي ٢٠٠٦/٢٠٠٧٠٤٦/٢٠٠٨.٨/٢٠٠٩،٢/٧ هي التي أحاطت فيها اللجنة المعنية بتسخير العلم والتكنولوجيا لأغراض التنمية علما بنتائج تنفيذ مؤتمر القمة العالمي لمجتمع المعلومات استنادا إلى ما ورد من مساهمات من كيانات الأمم المتحدة ذات الصلة وغيرها من الكيانات، حسب الاقتضاء. فضلا عن ذلك افتتح المجلس الاقتصادي والاجتماعي دورته لعام ٢٠١٠ بجلسة إعلامية عن التحديات التي يطرحها الأمن السيبراني، فضلا عن التهديدات والفرص التي يتيحها استخدام الإنترنت الآخذ في الاتساع، وقد شدد المجلس من بين عدة أمور على الحاجة إلى اتخاذ مبادرات دولية تكفل تبادل المعلومات وأفضل الممارسات والتدريب والبحث، وإضافة إلى ذلك، أعلن المشاركون في المناقشة أنه يتعين على الأمم المتحدة أن توحد أداءها ، بشأن هذه القضية، مما سيؤدي حتما إلى زيادة التعاون بين البلدان بل وبين الدول والقطاع الخاص أيضا الضمان الأمن السيبراني[٦٦] وحذروا من النطاق الدولي لحرب سيبرانية فعلية وعواقبها وخيمة سوف تحدث بشكل خطير إن لم يتم تدارك الأمر، ومن ثم لا بد أن تكون هناك استجابة منسقة بين الدول ولا تكفي الآن إستراتيجيات اعتماد حلول على أساس مخصص وتقوية الدفاع [٦٧] ودعا القرار أيضا إلى اتباع نهج قائم على إدراك المخاطر، بحيث يحاط جميع أصحاب المصلحة علما بالمخاطر ذات الصلة والتدابير الوقائية والردود الفعالة على نحو مناسب، كل في إطار الدور المنوط به. وأشار القرار إلى أن الجهود الوطنية إلزامية إلى حماية الهياكل الأساسية الحيوية للمعلومات التي تستفيد من التقييم الدوري للتقدم الذي تحرزه هذه الجهود. وطالب القرار بمزيد من العناية الموضوع الأمن الإلكتروني، حيث دعا الدول الأعضاء إلى تقديم موجزات المبادراتها الرئيسية بشأن الأمن السيبراني وحماية الهياكل الأساسية الحيوية للمعلومات كي يتسنى إبراز ما يتم تحقيقه من الإنجازات وأفضل الممارسات والدروس المكتسبة والإجمالات التي تتطلب مزيدا من التدابير على الصعيد الوطني.. وقدم استقصاء طوعيا في شكل تقييم ذاتي للأمن الإلكتروني الوطني باعتباره أداة يمكن أن تساعد البلدان على استعراض الجهود الوطنية المبذولة في مجال الأمن السيبراني وحماية الهياكل الأساسية الحيوية للمعلومات[٦٨] وفي سبتمبر عام ٢٠١١ عقد المجلس الاقتصادي والاجتماعي للأمم المتحدة اجتماعا لمناقشة أمن الفضاء الإلكتروني والتنمية والقضايا والتحديات ذات الصلة، واشترك فى المناقشات إدارة الشئون الاقتصادية والاجتماعية، والاتحاد الدولي للاتصالات، ورئيس لجنة الأمم المتحدة المعنية بتسخير العلم والتكنولوجيا الأغراض التنمية، ومنظومة الأمم المتحدة، والقطاعين العام والخاص، بالإضافة إلى منظمات المجتمع المدني المهتمة بمجالات الفضاء السيبراني والجرائم الإلكترونية وحددت أهداف الاجتماع بأنها تتمثل في بناء وعي على مستوى السياسات الدولية عبر تزويد أعضاء المجلس الاقتصادي والاجتماعي بصورة عن الوضع الحالي والتحديات المتعلقة بأمن الفضاء الإلكتروني، وارتباطه بالتنمية وتحديد أفضل السياسات المتعلقة بهذا المجال، والمبادرات المطبقة في مختلف أنحاء العالم لبناء ثقافة أمن الفضاء السيبراني، وكذا استكشاف خيارات للاستجابة العالمية بشأن تزايد معدلات الجريمة السيبرانية.كما ناقش الاجتماع الفوارق الاقتصادية بين الدول، وعدم قدرة الدول النامية منها على مكافحة الجرائم السيبرانية، وكذلك افتقاد الشراكة بينها وبين الدول الصناعية، مما يؤدي إلى خلق ملاذ امن لمهاجمي الفضاء السيبراني لارتكاب جرائمهم. كما تم مناقشة الحاجة إلى إبرام اتفاقية دولية بشأن الفضاء الإلكتروني بما يشمل احتمال البناء على اتفاقية بودابست، باعتبارها تنسيقا بين الدول بشأن بعض الجرائم السيبرانية، كالتعدي على حق المؤلف والغش، واستغلال

الأطفال في المواد الإباحية، وجرائم الكراهية، وانتهاكات أمن الشبكات وقرر لازاروس كابامبي. رئيس المجلس الاقتصادي والاجتماعي، أن أعضاء الاجتماع قد اتفقوا على أن الأمن السيبراني قضية عالمية، لا يمكن حلها إلا عبر شراكة عالمية، لا سيما من خلال الأمم المتحدة التي يمكنها استخدام قدراتها الإستراتيجية والتحليلية لمعالجة مثل هذه القضايا.[٦٩]**البند الثاني: المنظمات الإقليمية والدولية الأخرى** كان للمنظمات العلمية المتخصصة دوراً هاماً بشأن التعامل مع العمليات السيبرانية بأنواعها المختلفة، وتحقيق قدراً من الأمن في مجال المعاملات الإلكترونية ومن أبرز هذه المنظمات الاتحاد الدولي للاتصالات والمنظمة العالمية للملكية الفكرية، ومنظمة حلف شمال الأطلسي، وسوف نتناول بإيجاز جهود تلك المنظمات.

**اولاً: الاتحاد الدولي للاتصالات** نشأ الاتحاد الدولي للاتصالات بموجب اتفاقية باريس عام ١٨٦٥ تحت اسم (اتحاد التلغراف الدولي)، ثم عدل الاسم ليصبح الاتحاد الدولي للاتصالات السلكية واللاسلكية، ثم في عام ١٩٤٧ انضم الاتحاد إلى هيئة الأمم المتحدة، وبات إحدى الوكالات المتخصصة في عمل الاتصالات تحت مظلة الأمم المتحدة.يهدف الإتحاد إلى تعزيز التعاون الدولي للخدمات الهاتفية والسلكية واللاسلكية وتوسيع استخدامها بواسطة الجمهور وتطوير إمكانات الاتصالات السلكية واللاسلكية وتوزيع الموجات اللاسلكية، كما يقوم الاتحاد بتقديم التوصيات الخاصة والدراسات الفنية المتخصصة في الاتصالات اللاسلكية وجمع المعلومات ونشرها من أجل بناء قدرات الدول الأعضاء – ولاسيما البلدان النامية لتنسيق الإستراتيجيات الوطنية وحماية البنية التحتية للشبكات ضد المخاطر من خلال التوعية، والتقييم الذاتي، وبناء القدرات، وتوسيع نطاق المراقبة، والإنذار وقدرات الاستجابة للحوادث للدول والجهات المعنية، ويعمل الاتحاد بصورة وثيقة مع المنظمات الأخرى المعنية على وضع المعايير المتعلقة بالأمن المعلوماتي إذ يقوم الاتحاد بالاشتراك مع الوكالة الأوروبية لأمن الشبكات والمعلومات بنشر خريطة الطريق المتعلقة بمعايير الأمن في مجال تكنولوجيا المعلومات والاتصالات، كما تعاون الاتحاد الدولي مع مجلس أوروبا الإنجاز الاتفاقية الأوروبية حول الجريمة الإلكترونية من أجل الاستعانة بها في عملية وضع إطار قانوني دولي.[٧٠]وقد قام الاتحاد الدولي للاتصالات بإنشاء فريق متخصص معني بالشبكات الذكية من أجل جمع وتوثيق المعلومات والمفاهيم التي ستكون مفيدة من أجل إعداد توصيات لدعم تلك الشبكات من منظور الاتصالات ،[٧١] وكان أحد الأدوار الأساسية التي أنيطت بالاتحاد الدولي للاتصالات في أعقاب القمة العالمية لمجتمع المعلومات ومؤتمر المندوبين المفوضين العام ٢٠٠٦ يتمثل في بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات فقد قام رؤساء الدول والحكومات وغيرهم من قادة العالم المشاركين في القمة العالمية المجتمع المعلومات، وكذلك الدول الأعضاء في الاتحاد ، بتكليف الاتحاد باتخاذ خطوات ملموسة للحد من التهديدات وانعدام الأمن فيما يتصل بمجتمع المعلومات ولتحقيق هذه الولاية أطلق الأمين العام للاتحاد برنامج الأمن السيبراني العالمي في عام ٢٠٠٧ ليكون إطارا للتعاون الدولي .[٧٢] وقد أعلن الأمين العام للاتحاد الدولي للاتصالات عام ٢٠٠٧ عن إطلاق مبادرة أجندة شاملة بشأن الأمن السيبراني تتضمن التوصل إلى إطار أو بروتوكول لتنسيق جهود مكافحة الجرائم السيبرانية، وبما يشمل تدابير قانونية، وتقنية، وإجرائية وتنظيمية، وتعاون دولي .[٧٣]ويقترح الأمين العام للاتحاد الدولي للاتصالات خمسة مبادئ توجيهية الإحلال السلام وحفظه في العالم السيبراني الناشئ إدراكا منه للخطر المتنامي للهجوم السيبراني، وقد أعدت لوائح الاتصالات الدولية كإطار تنظيمي المعالجة القضايا الناشئة والتحديات التي تصاحب عالم الاتصالات الجديد الذي تجسد في أواخر ثمانينات القرن الماضي، وقد صيغت هذه اللوائح لتعزيز الكفاءة والتنمية الدوليين، فضلا عن أنها تبرز تركيز الاتحاد على حماية الحق في الاتصال وفي الوقت نفسه إلحاق الضرر بالمرافق .[٧٤]وعلى غرار ذلك، تتضمن المبادئ الخمسة التي اقترحها الأمين العام للاتحاد الدولي للاتصالات فيما يتعلق بالسلام السيبراني هذه القيم الجوهرية مع تحديد إجراءات والتزامات محددة من شأنها أن تضمن السلام والاستقرار في الفضاء السيبراني، وتنص هذه المبادئ على ما يلي :[٧٥]

-١- أن تلتزم كل حكومة بإتاحة نفاذ شعبها على الاتصالات.

٢- أن تلتزم كل حكومة بتأمين الحماية الشعبها في الفضاء السيبراني.

٣ أن يلتزم كل بلد بعدم إيواء الإرهابيين / المجرمين في أراضيه.

٤- أن يلتزم كل بلد بألا من البلدان يكون الطرف الذي يبدأ شن هجوم سيبراني على غيره من البلدان.أن يلتزم كل بلد بالتعاون مع غيره ضمن إطار دولي للتعاون لضمان السلام في الفضاء السيبراني.وفي مسعى أكثر شمولا، تم في المؤتمر الإقليمي حول الأمن السيبراني بالتعاون مع الاتحاد الدولي للاتصالات في قطر عام ٢٠٠٨، دعوة جميع الدول لوضع وتنفيذ إطار وطني للأمن السيبراني وحماية البنية التحتية الحرجة للمعلومات والتي تعد بمثابة خطوة أولى في سبيل التصدي للتحديات التي تواجهها جراء اتصالها بتكنولوجيا.المعلومات والاتصالات [٧٦]: وفي نفس العام وقع

الاتحاد الدولي للاتصالات والشراكة الدولية المتعددة الأطراف المكافحة التهديدات السيبرانية (إمباكت) (IMPACT) مذكرة تفاهم رسميا، بعدها أصبح مقر شراكة إمباكت في سايبر جايا بماليزيا، الذي يضم أحدث ما توصلت إليه التكنولوجيا، المقر الفعلي للبرنامج.[٧٧]

**ثانيا: المنظمة العالمية للملكية الفكرية** إبان عام ١٩٦٧ تم التوقيع في ستوكهولم بالسويد على اتفاقية المنظمة العالمية للملكية الفكرية، وأصبحت هذه المنظمة إحدى الوكالات المتخصصة التابعة للأمم المتحدة اعتبارا من السابع عشر من ديسمبر عام ١٩٧٤، والتي من أهدافها حماية الملكية الفكرية في شتى أنحاء العالم عن طريق التعاون بين الدول الأعضاء والمنظمات الدولية الأخرى، وتعمل المنظمة على متابعة تنفيذ الاتفاقيات المتعلقة بالتصميمات الصناعية وتصنيف السلع التجارية وحماية الأعمال الإدارية والفنية وحقوق الإنتاج، كما تشجع المنظمة كذلك على توقيع معاهدات دولية جديدة وتقوم بالتنسيق بين التشريعات الوطنية، وتقديم المساعدات القانونية والفنية للدول النامية بهدف حماية الملكية الفكرية وتنميتها وتغطية بعض أوجه القصور في مجال التوثيق العلمي ونقل التقنية الحديثة.[٧٨]وبالرجوع إلى اتفاقية إنشاء هذه المنظمة تتضح غايات هذه المنظمة في دعم الملكية الفكرية في جميع أنحاء العالم بجميع صورها المصنفات الأدبية والفنية والعلمية والاختراعات، ومع تزايد الحاجة العالمية لحماية البرامج شكلت هذه المنظمة مجموعة عمل تضم عددًا من الخبراء بهدف حماية برامج الحاسب الآلي، وبعد سلسلة من الاجتماعات والدراسات حول الأساليب المثلى لحماية برامج الحاسوب، ساد الاتجاه لدى أغلب الدول إلى الميل إلى خضوع برامج الحاسوب القوانين حماية حق المؤلف. وقد جاءت منظمة التجارة العالمية عام ١٩٩٤ لتؤيد هذا التوجه وتستكمل طريقها من خلال إبرام اتفاقية تربيس (TRIPS) المتعلقة بمواصفات التجارة المرتبطة بحقوق الملكية الفكرية وما تفرضه من التزامات على الدول الأعضاء الفرض إجراءات تنفيذية وعقوبات جنائية لمواجهة أي اعتداء على حق المؤلف وخاصة القراصنة[٧٩]

## المطلب الثالث: التحديات في تطبيق التعاون الدولي

تواجه الدول تحديات كبيرة في تطبيق التعاون الدولي لمواجهة الهجمات السيبرانية، حيث تزداد تعقيدات التهديدات السيبرانية بسرعة. من بين هذه التحديات، عدم وجود إطار قانوني موحد يحدد كيفية التعامل مع الجرائم السيبرانية عبر الحدود. تختلف القوانين والتشريعات من دولة لأخرى، مما يعيق التنسيق الفعال بين الدول. هذا الاختلاف يجعل من الصعب تبادل المعلومات والبيانات المتعلقة بالهجمات، ويزيد من فرص الإفلات من العقاب للجناة وعلاوة على ذلك، تتطلب مكافحة الهجمات السيبرانية تعاونًا بين الحكومات والقطاع الخاص، وهو ما يمثل تحديًا آخر.[٨٠] غالبًا ما تتجاهل الشركات الكبرى التهديدات السيبرانية، مما يؤدي إلى نقص في المعلومات والموارد اللازمة لمكافحة هذه الهجمات. كما أن الشركات قد تكون reluctant للمشاركة في تبادل المعلومات حول الهجمات لأسباب تتعلق بالخصوصية أو السمعة، مما يحد من فعالية الجهود الدولية حيث تتسم الهجمات السيبرانية بتطورها السريع، مما يتطلب استجابة فورية وفعالة من الدول. ومع ذلك، فإن التباين في القدرات التكنولوجية بين الدول يخلق فجوة كبيرة في الاستجابة. الدول النامية قد تفتقر إلى الموارد التقنية أو البشرية اللازمة لمواجهة التهديدات، مما يزيد من صعوبة تحقيق تعاون دولي فعّال. هذه التحديات مجتمعة تعيق الجهود المبذولة لمواجهة الهجمات السيبرانية بشكل منسق وشامل[81].

**البند الأول: صعوبة تحديد الجهة المسؤولة عن الهجمات السيبرانية**تُعتبر صعوبة تحديد الجهة المسؤولة عن الهجمات السيبرانية من أبرز التحديات التي تواجه التعاون الدولي في مجال الأمن السيبراني. تتسم هذه الهجمات بالتعقيد والغموض، مما يجعل من الصعب في كثير من الأحيان تحديد الفاعل بدقة. تحتل هذه القضية مكانة مركزية في النقاشات حول كيفية التعامل مع هذه التهديدات على الصعيد الدولي كما تتعدد الأسباب التي تجعل عملية تحديد الجهة المسؤولة معقدة. أولاً، يمكن للمهاجمين استخدام تقنيات التمويه والتخفي، مثل الشبكات الافتراضية الخاصة (VPN) أو خدمات الوكيل، لإخفاء هويتهم وموقعهم. هذه الأساليب تجعل من الصعب تتبع مصدر الهجوم، مما يزيد من صعوبة تحميل أي جهة المسؤولية. قد تكون هذه الجهات دولاً معينة، مجموعات إجرامية، أو حتى أفراد يعملون بشكل مستقل[82].ثانيًا، تتنوع الأهداف وراء الهجمات السيبرانية. قد تستهدف الهجمات مؤسسات حكومية، شركات خاصة، أو حتى الأفراد. هذه التنوع في الأهداف يزيد من تعقيد المسألة، حيث قد يكون من الصعب معرفة من يستفيد من الهجوم. في بعض الحالات، قد تكون الدوافع سياسية أو اقتصادية أو حتى اجتماعية، مما يستدعي فهماً عميقاً للسياقات المختلفة كما تتطلب الهجمات السيبرانية في كثير من الأحيان تعاونًا دوليًا فعّالًا لتحديد الجهة المسؤولة. لكن، بسبب عدم وجود إطار قانوني موحد، تواجه الدول صعوبة في تبادل المعلومات اللازمة. كل دولة تتبنى سياسات وقوانين مختلفة في مجال الأمن السيبراني، مما يعيق التنسيق الفعّال. هذا التباين يمكن أن يؤدي إلى حواجز قانونية تحول دون تحقيق العدالة[83].علاوة على ذلك، تسهم الفجوة التكنولوجية بين الدول في تعقيد الأمور. الدول المتقدمة تمتلك موارد وتقنيات متطورة تمكنها من تحليل الهجمات بشكل أفضل، بينما الدول النامية قد تفتقر إلى هذه القدرات. هذا التفاوت يجعل من الصعب تحقيق تعاون متكافئ بين الدول، مما يزيد من فرص الإفلات من العقاب ويمكن أن تؤدي الهجمات السيبرانية أيضًا إلى توترات

سياسية بين الدول. عندما يتم اتهام دولة ما بدعم أو تنفيذ هجوم سيبراني، قد تتصاعد التوترات بشكل كبير. هذا الوضع يجعل من الصعب على الدول التعاون في مواجهة هذه التهديدات، حيث يكون هناك خوف من ردود الفعل السياسية السلبية[84].تتطلب مواجهة هذه التحديات جهودًا مستمرة من جميع الدول المعنية. يجب على الدول أن تعمل على تعزيز التعاون وتبادل المعلومات على مستويات متعددة، بما في ذلك الحكومات والقطاع الخاص. كما ينبغي تعزيز البحث والتطوير في مجال الأمن السيبراني لتقليل الفجوات التكنولوجية بين الدول ومن المهم أيضًا أن يتم تطوير استراتيجيات شاملة لتحديد الجهة المسؤولة عن الهجمات السيبرانية. يمكن أن تشمل هذه الاستراتيجيات استخدام تقنيات متقدمة في تحليل البيانات، بما في ذلك الذكاء الاصطناعي والتعلم الآلي، لتعزيز القدرة على التنبؤ بالهجمات وتحليلها. كذلك، ينبغي أن يتم تعزيز التعاون الدولي في مجال التعليم والتدريب لتطوير مهارات الأفراد في مجال الأمن السيبراني[85].تستخدم بعض الدول استراتيجيات دبلوماسية لتحقيق التعاون في هذا المجال. يتضمن ذلك تشكيل تحالفات دولية لمواجهة التهديدات السيبرانية بشكل جماعي. هذه التحالفات يمكن أن تسهم في تعزيز تبادل المعلومات والخبرات، مما يزيد من فعالية الجهود المبذولة ومع ذلك، يجب أن تكون هناك جهود متواصلة لتطوير إطار قانوني دولي ينظم التعامل مع الهجمات السيبرانية. هذا الإطار ينبغي أن يحدد المعايير والممارسات المثلى لتحديد الجهة المسؤولة عن الهجمات، مما يسهل التعاون بين الدول. من خلال إنشاء قواعد واضحة، يمكن للدول أن تعمل معًا بشكل أكثر فعالية.تتطلب التحديات المرتبطة بتحديد الجهة المسؤولة عن الهجمات السيبرانية أيضًا تعزيز الوعي العام. يجب على الحكومات والمؤسسات التعليمية تعزيز الثقافة السيبرانية لدى الأفراد والمجتمعات. هذا الوعي يمكن أن يسهم في توفير معلومات قيمة حول كيفية حماية البيانات والمعلومات من الهجمات، مما يقلل من تأثير هذه التهديدات[86].في النهاية، يتضح أن صعوبة تحديد الجهة المسؤولة عن الهجمات السيبرانية تمثل تحديًا كبيرًا أمام التعاون الدولي. يتطلب التصدي لهذه التحديات جهودًا منسقة وشاملة على المستويات الحكومية والخاصة. يجب أن يعمل المجتمع الدولي على تعزيز التعاون وتبادل المعلومات، مع التركيز على تطوير استراتيجيات قانونية وتكنولوجية فعالة. فقط من خلال هذا التعاون المستدام يمكن تحقيق الأمن السيبراني الفعال والعمل على تقليل الآثار السلبية للهجمات السيبرانية[87].

**البند الثاني: الاختلافات في القوانين الوطنية المتعلقة بالجرائم الإلكترونية** تُعتبر الاختلافات في القوانين الوطنية المتعلقة بالجرائم الإلكترونية من أبرز التحديات التي تواجه التعاون الدولي في مكافحة الهجمات السيبرانية. حيث تتباين التشريعات من دولة إلى أخرى، مما يعيق التنسيق الفعّال بين الدول. يتطلب الأمر فهمًا عميقًا لهذه الاختلافات لتحديد كيفية تجاوزها وتعزيز التعاون حيث تُظهر القوانين الوطنية تباينًا واضحًا في التعريفات المتعلقة بالجرائم الإلكترونية. فبعض الدول قد تعرّف الجريمة الإلكترونية بشكل ضيق يقتصر على بعض الأفعال مثل اختراق الأنظمة، بينما قد تشمل دول أخرى مجموعة أوسع من الأنشطة، بما في ذلك الاحتيال الإلكتروني، والاعتداء على البيانات. هذا الاختلاف في التعريفات يخلق تحديًا في مواءمة الجهود الدولية[88].كما أن العقوبات المفروضة على الجرائم الإلكترونية تختلف بشكل كبير بين الدول. في حين قد تفرض دولة ما عقوبات صارمة تشمل السجن لفترات طويلة، قد تكتفي دول أخرى بعقوبات خفيفة أو غرامات مالية. هذا التباين في العقوبات يمكن أن يؤدي إلى عدم التجانس في تطبيق العدالة، مما يجعل من الصعب محاسبة المجرمين الدوليين.تتضمن بعض القوانين الوطنية أيضًا مواد تتعلق بحماية الخصوصية وحقوق الأفراد، وهو ما قد يتعارض مع الجهود المبذولة لمكافحة الجرائم الإلكترونية. فعلى سبيل المثال، قد تمنع قوانين الخصوصية تبادل المعلومات بين الدول، مما يعيق التحقيقات في الجرائم السيبرانية. هذا الأمر يتطلب تحقيق توازن بين حماية الخصوصية وضرورة التحقيق في الجرائم وتعد القوانين المتعلقة بالجرائم السيبرانية حديثة نسبيًا، مما يعني أنه لا تزال هناك فجوات في بعض التشريعات. بعض الدول لم تقم بتحديث قوانينها لتواكب التطورات السريعة في التكنولوجيا، مما يجعلها عرضة للاستغلال. هذه الفجوات تُعتبر بيئة خصبة للمجرمين السيبرانيين، مما يتطلب جهودًا موحدة لتحسين الأطر القانونية[89].من ناحية أخرى، تواجه الدول صعوبة في تطبيق القوانين الوطنية في حالات الجرائم السيبرانية العابرة للحدود. قد يكون من الصعب تحديد الجهة المسؤولة عن الهجوم، مما يؤدي إلى صعوبة في تطبيق القوانين. هذا التحدي يتطلب تطوير آليات تعزز من التعاون بين الدول في مجالات التحقيق والمقاضاة كما تتطلب الجرائم الإلكترونية في كثير من الأحيان جمع الأدلة من عدة دول، وهو ما قد يكون معقدًا بسبب الاختلافات في القوانين. على سبيل المثال، قد تحتاج إحدى الدول إلى الحصول على إذن قانوني لجمع الأدلة من دولة أخرى، مما يعيق التحقيقات. لذا، فإن توفير آليات قانونية واضحة وسهلة الاستخدام يعد أمرًا ضروريًا[90].تسهم الفجوة في فهم القوانين بين الدول في تعقيد الأمور. بعض الدول قد تكون لديها قدرات قانونية متطورة، بينما تفتقر أخرى إلى المعرفة الكافية حول كيفية التعامل مع الجرائم الإلكترونية. هذه الفجوة في الفهم يمكن أن تعرقل التعاون، حيث قد لا تكون بعض الدول على دراية بكيفية تقديم المساعدة القانونية كما تتطلب معالجة هذه التحديات تعاونًا دوليًا شاملًا. يجب على الدول العمل على تطوير معاهدات دولية تهدف إلى مواءمة القوانين المتعلقة بالجرائم الإلكترونية. يمكن أن تشمل هذه المعاهدات تحديد تعريفات موحدة للجريمة الإلكترونية، وتوحيد العقوبات، وتسهيل تبادل المعلومات وتُعتبر مبادرات التعاون الإقليمي أيضًا

خطوة مهمة نحو تحقيق هذا الهدف. من خلال تشكيل تحالفات إقليمية، يمكن للدول تبادل المعرفة والخبرات وتعزيز التنسيق في مجال مكافحة الجرائم الإلكترونية. هذه التحالفات يمكن أن تسهم في تطوير استراتيجيات قانونية مشتركة[91].علاوة على ذلك، ينبغي أن يتم تعزيز الوعي القانوني بين الدول. يمكن أن تشمل هذه الجهود تنظيم ورش عمل ودورات تدريبية لتعزيز فهم القوانين الوطنية والدولية المتعلقة بالجرائم الإلكترونية. هذا النوع من التعليم يمكن أن يساهم في تحسين التعاون الدولي في هذا المجال حيث تعد التكنولوجيا أداة حيوية في مكافحة الجرائم الإلكترونية، لكن يجب أن تكون القوانين مرنة بما يكفي لتواكب التطورات. من المهم أن تتضمن التشريعات نصوصًا تسمح بتبني تقنيات جديدة لمكافحة الجرائم، مما يسهل عملية التعاون. يجب أن تكون هناك استجابة سريعة للتغيرات في مشهد التهديدات السيبرانية.تواجه الدول أيضًا تحديات تتعلق بتطبيق القوانين في بيئات متعددة اللغات. قد تتطلب التحقيقات ترجمة الوثائق القانونية، مما يضيف طبقة من التعقيد. لذا، يجب أن يتم تطوير آليات لتسهيل الترجمة والتواصل بين الدول وتُعتبر السياسات الحكومية أيضًا عنصرًا حاسمًا في تحقيق التعاون الدولي. يجب أن تلتزم الحكومات بتطوير استراتيجيات وطنية تتماشى مع الأهداف الدولية لمكافحة الجرائم الإلكترونية. هذه السياسات يجب أن تشمل تعزيز التعاون مع القطاع الخاص والمجتمع المدني[92].تمثل الجرائم السيبرانية تهديدًا عالميًا، لذا يجب أن يكون هناك اهتمام دولي مشترك لمواجهتها. يتطلب ذلك من الدول أن تتجاوز الحدود الوطنية وتعمل معًا بشكل منسق. تعزيز التعاون هو المفتاح للتغلب على التحديات الناجمة عن الاختلافات القانونية ويتضح أن الاختلافات في القوانين الوطنية المتعلقة بالجرائم الإلكترونية تشكل تحديًا كبيرًا أمام التعاون الدولي. تحتاج الدول إلى تعزيز الجهود المشتركة لتطوير أطر قانونية موحدة، وتسهيل تبادل المعلومات، وتعزيز الوعي القانوني. فقط من خلال هذا التعاون المستدام يمكن مواجهتها بفعالية وتحقيق الأمن السيبراني للجميع[93].

**البند الثالث: قلة الموارد المتاحة لمكافحة الهجمات السيبرانية** تُعد قلة الموارد المتاحة لمكافحة الهجمات السيبرانية من التحديات التي تواجه الدول في تعزيز التعاون الدولي في هذا المجال. يتطلب التصدي لهذه التهديدات استثمارات كبيرة في التكنولوجيا، والتدريب، والبحث، وهو ما قد يكون غير متاح للكثير من الدول، خاصة تلك التي تعاني من أزمات اقتصادية. هذا النقص في الموارد يمكن أن يعيق فعالية الاستجابة للهجمات فتواجه الدول النامية تحديات إضافية في هذا السياق. غالباً ما تكون هذه الدول غير قادرة على تخصيص ميزانيات كافية للأمن السيبراني، مما يجعلها عرضة للهجمات.[٩٤] في كثير من الحالات، قد تفتقر الحكومات إلى الخبرة الفنية اللازمة لتطوير استراتيجيات فعالة لمواجهة الجرائم السيبرانية، مما يزيد من تعقيد الوضع وتتطلب مكافحة الهجمات السيبرانية أيضًا تحسين القدرات البشرية. فالتدريب والتطوير المهني للكوادر العاملة في مجال الأمن السيبراني يعد أمرًا ضروريًا. ومع ذلك، قد لا تتوفر الموارد اللازمة لتوفير التدريب المتخصص، مما يؤدي إلى نقص في المهارات والخبرات في هذا المجال. هذه الفجوة تؤثر على قدرة الدول على التعاون بشكل فعّال[95].تتطلب تقنيات الأمن السيبراني الحديثة استثمارات كبيرة في البنية التحتية التكنولوجية. فالكثير من الدول تفتقر إلى الأنظمة المتطورة التي تتيح لها الكشف عن الهجمات وتحليلها بشكل فعال. هذا النقص في التكنولوجيا يجعل من الصعب تبادل المعلومات والخبرات بين الدول، مما يعيق التعاون الدولي حتى الدول التي تمتلك ميزانيات أكبر قد تواجه صعوبة في توجيه الموارد بشكل فعّال. إذ يمكن أن تكون هناك أولويات أخرى تتطلب التمويل ، مما يؤدي إلى نقص التمويل المخصص للأمن السيبراني. هذا الأمر يتطلب من الحكومات أن تعيد تقييم أولوياتها وتخصيص المزيد من الموارد لمواجهة التهديدات السيبرانية تتطلب مكافحة الجرائم السيبرانية أيضًا تعاونًا بين القطاعين العام والخاص. ومع ذلك، قد تكون هناك حواجز تمنع هذا التعاون، مثل عدم الثقة أو قلة الفهم حول كيفية العمل معًا. قد تشعر الشركات الخاصة بأنها لا تملك الموارد الكافية للتعاون مع الحكومات، مما يعيق تبادل المعلومات والخبرات وتعتبر المبادرات الدولية لمكافحة الهجمات السيبرانية مهمة، لكنها غالبًا ما تكون محدودة بسبب نقص الموارد. تحتاج هذه المبادرات إلى دعم مالي وتقني من الدول الأعضاء، وهو ما قد يكون غير متاح في بعض الحالات. هذا النقص في الدعم يمكن أن يقوض فعالية هذه المبادرات [96].كما أن نقص البيانات والمعلومات حول الهجمات السيبرانية يعد تحديًا آخر. فالدول التي تفتقر إلى الموارد قد تجد صعوبة في جمع وتحليل البيانات المتعلقة بالتهديدات. هذا النقص في المعلومات يمنع الدول من اتخاذ قرارات مستنيرة بشأن كيفية التصدي للهجمات، مما يزيد من تعقيد الوضع وتُعتبر الأبحاث والدراسات في مجال الأمن السيبراني ضرورية لتطوير استراتيجيات فعالة. ومع ذلك، فإن قلة الموارد قد تعني أن العديد من الدول لا تستطيع تمويل الأبحاث اللازمة. هذا النقص في الأبحاث يحد من قدرة الدول على فهم التهديدات بشكل أفضل وتطوير حلول مبتكرة لمواجهتها وتُعتبر الدول التي تتمتع بموارد أكبر في مجال الأمن السيبراني قادرة على جذب أفضل المواهب. بينما قد تجد الدول النامية نفسها غير قادرة على المنافسة في هذا المجال، مما يؤدي إلى فقدان الكفاءات. هذه الفجوة في القدرات البشرية تؤثر سلبًا على الجهود المبذولة لمكافحة الجرائم السيبرانية وتتطلب الجرائم السيبرانية أيضًا استجابة منسقة على المستوى الدولي. لكن نقص الموارد قد يعني أن بعض الدول غير قادرة على المشاركة بفعالية

في الجهود الدولية. هذا الأمر يعيق تحقيق أهداف التعاون الدولي في مجال الأمن السيبراني[97].تُعتبر التهديدات السيبرانية عابرة للحدود، مما يتطلب من الدول التعاون بشكل فعّال. ومع ذلك، فإن قلة الموارد يمكن أن تؤدي إلى عدم قدرة بعض الدول على الانخراط في هذا التعاون. هذا الوضع يضعف الجهود العالمية لمواجهة هذه التهديدات على ان يجب أن تعمل الدول على تعزيز تبادل المعلومات والخبرات بشكل يراعي قلة الموارد. يمكن أن يتم ذلك من خلال تطوير شراكات استراتيجية بين الدول ذات القدرات المختلفة، مما يتيح للدول الأضعف الاستفادة من الخبرات والموارد كما تتطلب مواجهة التهديدات السيبرانية أيضًا الابتكار في استخدام الموارد المتاحة. يجب على الدول أن تبحث عن حلول مبتكرة لتقليل التكاليف، مثل استخدام التكنولوجيا السحابية أو التعاون مع الشركات الناشئة في مجال الأمن السيبراني. هذه الابتكارات يمكن أن تعزز من فعالية الجهود المبذولة[98].يجب أن تتضمن الاستراتيجيات الوطنية لمكافحة الجرائم السيبرانية أيضًا خططًا لتوسيع نطاق الموارد المتاحة. يمكن أن تشمل هذه الخطط التعاون مع المنظمات الدولية لتأمين الدعم المالي والتقني. هذا التعاون يمكن أن يسهم في تعزيز القدرات المحلية لمواجهة التهديدات حيث تعتبر التوعية والتعليم أيضًا جزءًا مهمًا من مكافحة الجرائم السيبرانية. يجب أن تعمل الدول على تعزيز الثقافة السيبرانية بين المواطنين، مما يساهم في تقليل المخاطر. لكن، قلة الموارد قد تعني أن هذه الجهود لا تحظى بالاهتمام الكافي، مما يعوق التقدم في هذا المجال.يتطلب تحقيق الأمن السيبراني الفعّال تعاونًا دوليًا وشراكات قوية بين الدول. ومع ذلك، فإن قلة الموارد تعني أن بعض الدول قد لا تتمكن من المشاركة بفعالية في هذه الشراكات. هذا الأمر يمكن أن يؤدي إلى تفاقم الفجوة بين الدول في مجال الأمن السيبراني ويتضح أن قلة الموارد المتاحة لمكافحة الهجمات السيبرانية تمثل تحديًا كبيرًا أمام التعاون الدولي. يتطلب التصدي لهذه التحديات جهودًا منسقة ومبتكرة لتعزيز القدرات المحلية والدولية. من خلال العمل معًا وتبادل الموارد والخبرات، يمكن تحقيق الأمن السيبراني وتعزيز التعاون الدولي في مواجهة التهديدات[99].**ملخص الفصل** تُعتبر الآليات القانونية الدولية لمكافحة الهجمات السيبرانية عنصرًا حيويًا في تعزيز الأمن السيبراني على مستوى العالم. مع تزايد التهديدات السيبرانية وتطور أساليب الهجوم، أصبح من الضروري وجود إطار قانوني يحدد المسؤوليات والالتزامات بين الدول. هذه الآليات تساعد في تحديد كيفية التعامل مع الجرائم السيبرانية عبر الحدود، مما يسهل تبادل المعلومات والتعاون بين الدول وتعمل الآليات القانونية الدولية على توفير إطار موحد يساهم في تعزيز التنسيق بين الدول. من خلال المعاهدات والاتفاقيات، يمكن للدول تطوير استراتيجيات مشتركة لمواجهة التهديدات السيبرانية. هذه الاستراتيجيات تشمل تبادل المعلومات حول الهجمات والتهديدات، مما يساعد الدول على الاستجابة بشكل أسرع وأكثر فعالية.ومع ذلك، لا تزال هناك تحديات كبيرة تواجه تطبيق هذه الآليات. تختلف القوانين الوطنية من دولة إلى أخرى، مما قد يؤدي إلى تعقيدات في تنفيذ الاتفاقيات الدولية. هذا التباين يمكن أن يعيق جهود التعاون ويجعل من الصعب تحميل الجناة المسؤولية عن أفعالهم. لذا، يجب العمل على مواءمة القوانين الوطنية مع المعايير الدولية لتعزيز الفعالية حيث تتطلب الآليات القانونية الدولية أيضًا تطوير آليات فعالة لرصد وتقييم الأداء. يجب أن تتضمن هذه الآليات آليات للمتابعة والتقارير، لضمان التزام الدول بالتزاماتها القانونية. من خلال هذه المراقبة، يمكن تحسين استراتيجيات الأمن السيبراني وتحديد الفجوات التي تحتاج إلى معالجة وعليه تُعد الآليات القانونية الدولية لمكافحة الهجمات السيبرانية ضرورة ملحة في عالم متزايد الاتصال. يجب أن تستمر الدول في تعزيز التعاون وتبادل المعرفة والخبرات، مع التركيز على تطوير إطار قانوني مرن وفعال من خلال هذه الجهود المشتركة، يمكن تحقيق الأمن السيبراني وتعزيز الاستجابة العالمية للتحديات المتزايدة في هذا المجال.

## هوامش البحث

[1] تنص المادة ٣٨ من النظام الأساسي لمحكمة العدل الدولية على انه " . تطبق المحكمة، التي تتمثل مهمتها في الفصل وفقا للقانون الدولي، في النزاعات المعروضة عليها الاتفاقيات الدولية، سواء كانت عامة أو خاصة، التي تحدد القواعد المعترف بها صراحة من قبل الدول المتنازعة العرف الدولي، كدليل على ممارسة عامة مقبولة كقانون : المبادئ العامة للقانون المعترف به من قبل الدول المتحضرة مع مراعاة أحكام المادة ٥٩ والقرارات القضائية وتعاليم أمهر الدعاة من الدول المختلفة كوسائل فرعية لتقرير أحكام القانون."

[2] تقرير الأمين العام للأمم المتحدة، مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية، خمسون سنة من مؤتمرات الأمم المتحدة لمنع الجريمة والعدالة الجنائية : انجازات الماضي وآفاق المستقبل، بانكوك، ٢٠٠٥ ،ص١

[3] هند نجيب التعاون القضائي الدولي في مجال الجرائم الاليكترونية، المجلة الجنائية القومية، العدد ٢، ٢٠١٦، ص١٠٦

[4] قطايف سليمان، بوقرين عبد الحليم الآليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل اتفاقية بودابست والتشريع الجزائري المجلة الأكاديمية للبحوث القانونية والسياسية، العدد ١ المجلد ٦ ٢٠٢٢، ص ٣٣٧

[٥] سلسلة معاهدات مجلس أوروبا، البروتوكول الاضافي لاتفاقية الجريمة الاليكترونية بشأن تجريم الأفعال المرتبطة بالتمييز العنصري وكراهية الاجانب التي ترتكب عن طريق انظمة الكمبيوتر، ٢٠٠٣

[٦] سلسلة معاهدات مجلس أوروبا، البروتوكول الاضافي الثاني للاتفاقية المتعلقة بالجريمة الاليكترونية بشأن تعزيز التعاون والكشف عن الأدلة الاليكترونية، ٢٠٢٢

[٧] دراسة شاملة عن الجريمة السيبرانية، منشورات مكتب الامم المتحدة المعني بالمخدرات والجريمة، فيينا ٢٠١٣

[٨] مريم لوكال، قراءة في اتفاقية الاتحاد الأفريقي حول الأمن السيبراني وحماية المعطيات ذات الطابع الشخصي لسنة مجلة الدراسات القانونية والاقتصادية، المجلد ٤ العدد ٢، ٢٠٢، ص٦٦١

[٩] رئيس الجمهورية رقم ٢٧٦ الصادر بتاريخ ١٩ / ٨ / على انضمام مصر إلى الاتفاقية العربية المكافحة جرائم تقنية المعلومات، وقد نشر هذا القرار بتاريخ ١٣ / ١١ / ٢٠١٤، وبدأ العمل به بتاريخ ٨ / ١٠ / ٢٠١٤

[10] Judgment of the International Court of Justice in Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States), 1986, L.C.J. 14, 96-97; See also, Malcolm Shaw, International Law, (7th edition, 2014), Cambridge University Press; Yoram Dinstein, War, Aggression and Self-defence (3ed edition 2011).

[١١] ميثاق الأمم المتحدة ١٩٤٥، المادة(٢،٤)

[١٢] فليح غزلان التدخل العسكري المعاصر بين القانون الدولي والممارسة الدولية – العدوان المقنع مجلة العلوم القانونية والاجتماعية جامعة زيان عاشور بالحلقة الجزائر، المجلد الرابع العدد الثالث سبتمبر ٢٠١٩م، ص ١٣٤

[١٣] بودربالة صلاح الدين استخدام القوة المسلحة في إطار أحكام ميثاق الأمم المتحدة، رسالة دكتوراه (غير منشورة)، جامعة الجزائر، كلية الحقوق، ٢٠١٠م، من ٤٦.

[١٤] إبراهيم رمضان عطاء الجريمة الإلكترونية وسول مواجهتها في الشريعة الإسلامية والأنظمة الدولية، العدد الثلاثون – الجزء الثاني (دراسة تحليلية تطبيقية ٢٠١٥م، ص ٣٣٠، ٤٠٤، ص ٣٦٠

https://mksq.journals.ekb.eg/article 7802 486775c9046bdacb05a5dc3a52784c0.pdf

[15] Sara Pangrazzi (MLaw), op. cit., p. 7. See: Anna C. Mourlam: op. cit., p. 24.

[16] See: Matthew Borton, Samuel Liles, Sydney Liles: op. cit., p. 314.

[17] See: Matthew Borton, Samuel Liles, Sydney Liles: op. cit., p. 315.

[١٨] ويمكن تعريف القوة بأنها مجموعة من الوسائل والطاقات والامكانات المادية وغير المادية المنظورة وغير المنظورة التي بحوزة الدولة ويستخدمها صانعي القرار في فعل مؤثر يحق مصالح الدولة ويؤثر في ملوك الوحدات السياسية الأخرى

[١٩] هربرت اين النزاع السيبراني والقانون الدولي الإنساني مختارات من المجلة الدولية للصليب الأحمر المجلد ١٤ (٨٨٦) ٢٠١٢ ي ص٨٨٦

[٢٠] أميرة عبد العظيم محمد عبد الجواد المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام مجلة الشريعة والقانون، العدد ٥٣، الجزء ٣. ٢٠٢٠م، من ٤٤٤.

[٢١] سلامة طارق الشالان: تكييف استخدام الحرب الإلكترونية في النزاعات المسلحة وفقا للقانون الدولي الإنساني، هذه الكوفة للعلوم القانونية والسياسية العدد ٢٦، ٢٠١٦، ص ١٢٥

See also: Matthew Borton, Samuel Liles, Sydney Liles: op. cit., p. 310, 314.

[22] Sara Pangrazzi (MLaw): op. cit., p. 7. Kamal Ahmad Khan: Use of Force and Human Rights under International Law, op. cit., p. 142.

[٢٣] عمر محمود أعمر: مرجع سابق، ص ١٣٨ انظر: د. بودربالة صلاح الدين استخدام القوة المسلحة في إطار أحكام ميثاق الأمم المتحدة ( رسالة دكتوراه (غير منشورة)، جامعة الجزائر، كلية الحقوق، ٢٠١٠م، ص ٤٨.

[٢٤] المستشار القانوني للجنة الدولية للصليب الاحمر

[٢٥] نور أمير الموصلي مرجع سابق، ص ١١، ١٧ انظر : CRC : اللجنة الدولية الصليب الأحمر، ما هي القيود التي يفرضها قانون الحرب على الهجمات السيبرانية ، مقال منشورة للجنة ٢٨/٦/٢٠١٣م

https://www.icrc.org/ar/doc/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm

[26] Matthew C. Waxman: Self-Defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions, Vol. 89, 2013, p. 109. See: Sara Pangrazzi (MLaw): op. cit., p. 4.

[٢٧] ميثاق الأمم المتحدة ١٩٤٥، المادة ٥١

[٢٨] تجدر الإشارة إلى أن هنالك شروط أخرى تضمنتها المادة من اجل مباشرة حق الدفاع عن النفس وفقا للمادة منها شرط الضرورة والتناسب والفورية أكدت على هذه الشروط محكمة العدل الدولية في قرارها في قضية نيكاراغوا ١٩٨٦ وأيضا في رأيها الاستشاري في قضية التهديد باستخدام أو استخدام الأسلحة النووية ١٩٩٦.

[29] See, Omer Elegab, The Legality of Non-forcible Counter-measures in International Law (Oxford Monographs in International Law), 1988.

[30] See, Omer Elegab, The Legality of Non-forcible Counter-measures in International Law (Oxford Monographs in International Law), 1988.

ICJ, Case Concerning Gabčíkovo-Nagymaros Project (HUNGARYISLOVAKIA), 1997, paragraph 71

[31] A. Randelzhofer, Article 51, in The Charter of the United Nations: A Commentary 661, 664 (B. Simma ed.) 1995.

[32] ICJ, case concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States), Reports 1986, para. 191.

[33] (1) ICJ, case concerning Oil Platforms, (Islamic Republic of Iran v. United States of America), Reports 2003, para. 51.

[34] UN General Assembly Res. 3314 (XXIX), Definition of Aggression, Adopted 14 December 1974.

[35] Cited in: Jeffry Car, Inside Cyber Warfare, O'Reilly Media, Inc., 2011, p.114.

[٣٦] أكدت على هذه الشروط محكمة العدل الدولية في قرارها في قضية نيكاراغوا ١٩٨٦ وأيضا في رأيها الاستشاري في قضية الأسلحة النووية ١٩٩٦.

[٣٧] تحديدا المادة ٣٣ والتي حددت أن هذه الطرق تشمل المفاوضات والتحقيق والوساطة والتوفيق والتحكيم والوسائل القضائية بالإضافة إلى الوكالات الإقليمية.

[38] Lee Stuesser, Active Defense: State Military Response to International Terrorism, 17, California Western International Law Journal, 1987, p.31

[39] Micheal Newton & Larry May, Proportionality in International Law, Oxford University Press, 2014; Arbitral Award in the Naulilaa Case 1928, 2 Reports of the International Arbitral Awards 1011-1028.

[40] Yoram Dinstein, Computer Network Attacks and Self-Defense, 76 U.S. Naval War College of International Law Studies (2002).

[٤١] انظر في الأقسام الأخرى من هذه المساهمة حيث تم التعريج على هذه الخاصية والإفرازات القانونية الناتجة عنها

[٤٢] صلاح عبد الرحمن الحديثي، التفصيل الشامل لتطور القواعد القانونية الخاصة بالحرب السيبرانية، ط١، مصر ، منشورات المجموعة العلمية للطباعة والنشر والتوزيع، ٢٠٢١، ص١٣٢

[٤٣] فؤاد ، مصطفى احمد (دت) فكرة الضرورة في القانون الدولي العام، الإسكندرية منشأة المعارف، من ٣٦ وما بعدها.

[٤٤] منصور على على (١٩٧١)، الشريعة الإسلامية والقانون الدولي العام، إصدارات المجلس الأعلى للشؤون الإسلامية، القاهرة . ٤٧ من

[٤٥]ولذلك لا يقبل من الكيان الصهيوني ( إسرائيل ) التهديد باستخدام الأسلحة النووية ضد المدن العربية حيث هدد بقصف القاهرة و الرياض و دمشق وبغداد والكويت والرباط إذا ما تعرض وجوده و كياته لخطر حقيقي

[٤٦] ولذلك أصدر مجلس الأمن قرارا في تشرين الأول ٢٠٠٩ يحظر على سيريلانكا استخدام الأسلحة الثقيلة الناء هجومها على المتمردين التاميل الذين اخليتوا في المدن التاميلية.

[٤٧] منير محمد الجهيني د. ممدوح محمد الجهيني جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر العربي الإسكندرية – ٢٠٠٤ ص ٩٦

[٤٨] تعود أهمية توقيع هذه الاتفاقية إلى رغبة المجتمع الدولي لايجاد صيغة دولية لمكافحة ومواجهة هذا الإجرام المستحدث. وعلى ذلك بذلت الجهود الدولية لتحقيق هذه الرغبة في تاريخ ٢٠ نوفمبر تقدمت اللجنة الأوروبية المشكلات الجريمة CIRC ولجنة الخبراء في حقل جرائم التقنية ( CYREIME بمشروع اتفاقية جرائم الكمبيوتر، وخضعت مواد الاتفاقية المقترحة للمناقشة وتبادل الآراء خلال الفترة من إصدار مشروعها الأول وحتى إعداد مسودتها النهائية التي أقرت لاحقا في بودابست ٢٠٠١ وتعرف باتفاقية بودابست (٢٠٠١) اتفاقية الجرائم السيبرانية سايبر كريم ) . ولا شك في أن الاتفاقية قد بذل فيها جهد واسع ومميز يذكر للاتحاد الأوروبي ومجلس أوروبا ولا سيما في المسائل المتعلقة بجرائم الكمبيوتر وأغراضها منذ أواخر القرن الواحد والعشرين. للمزيد د. هلالي عبد الله أحمد اتفاقية بودابست لمكافحة جرائم المعلوماتية ( معلبا عليها ) . دار النهضة العربية ، ط١ : ٢٠١١

[٤٩]/ttp://www.itu.int/ar/mediacentre

[٥٠] هلالي عبد الله احمد الجوانب الموضوعية والإجرائية للجرائم المعلوماتية المرجع السابق، ص ٢٠ وما بعدها

[٥١] منير محمد الجهيني، د. ممدوح محمد الجهيني، جرائم الإنترنت والمحاسب الآلي ووسائل مكافحتها، المرجع السابق، من ٢٦.

[٥٢] دوسولت لويز، وتويين بك وأنا (٢٠٠٠) الأسلحة الحديثة والقانون الدولي الإنساني، ندوة علمية حول القانون الدولي الإنساني: الواقع والطموح، اللجنة الدولية للصليب الأحمر، جامعة دمشق كلية الحقوق، من ١٥٨

[٥٣] الزهراني، شيخة حسين (٢٠٢٠٠) التعاون الدولي في مواجهة الهجوم السيبراني، محملة جامعة الشارقة للعلوم القانونية، مع ١٧، ج١، ص ٧٤٣

[٥٤] الصغير، جميل عبد الباقي (٢٠٠١) الجوانب الإجرائية الجرائم المتعلقة بالإنترنت، دار النهضة العربية من ٧٢، فضل، سليمان أحمد (٢٠٠٧) المواجهة التشريعية والأمنية الجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، مصر، من ٤١١ ٣٣

[٥٥] الأحول، سالم محمد سليمان (١٩٩٧) أحكام المسئولية الجمالية عن الجرائم الدولية في التشريعات الوطنية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، من ٤١٩

[٥٦] الزهراني، شيخة حسين، مرجع سابق، من ٧٤٤

[٥٧] الأجولى، سالم محمد سليمان، مرجع سابق، من ٤٢١، شحاتة علاء الدين (٢٠٠٠) التعاون الدول في مجال مكافحة الجريمة، دين القاهرة من ١١٠، فضل، سليمان أحمد، مرجع سابق، من ٤١٤، داود، عيسى سليم (٢٠١٧) جرائم القرصنة الإلكترونية رسالة ماجستير، جامعة الإسكندرية، من ١٣٤

[٥٨] العازمي، فهد عبد الله العبيد (٢٠١٦) الإجراءات الجنائية للمعلوماتية، دار الجامعة الجديدة، مصر، من ٦٥١.

[٥٩] معلومات عن الإنتربول، لهجة: https://www.interpol.int/ar/interne عامة، الموقع الرحمى المنظمة الشرطة الجنائية الدولية، على لموقع الإلكترون

[٦٠] يوسف، حسن يوسف (٢٠١١): الجرائم الدولية للإنترنت المركز القومي للاتصالات القانونية، القاهرة، ط١، من ١٤٨، الشمري، عالم مرضى (٢٠١٦) الجرائم المعلوماتية دار الثقافة، الأردن، من ٩٨)

[٦١] عبيد حسين صالح (١٩٧٧) القضاء الجنائي الدولي (تاريخة – تطبيقاته – مشروعاته)، دار النهضة العربية القاهرة، من ٩٩ – ١٠٠

[٦٢] صدقى عبد الرحيم (١٩٨٣) التعاون الدول في الفكر المعاصرة مجلة القانون والاقتصاد، جامعة القاهرة، من ٢٤٩

[٦٣] الصغير، جميل عبد الباقي (٢٠٠١) الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية ، ص٨٥

[64] SCHIOLBERG, The History of Global Harmonication on Cybercrime Legislation, 2008, available at httpa//www.cybercrimelane.net/Cybercrimelochtml

[٦٥] بيان اللجنة الدولية للصليب الأحمر للأمم المتحدة ٢٠١١ بشأن المناقشات العامة لكافة بنود جدول الأعمال في ما يتعلق بتزع السلاح والأمن الجمعية العامة للأمم المتحدة الدورة ١٧ اللجنة الأولى البندان و ١٠٦ من جدول الأعمال بيان اللجنة الدولية. للصليب الأحمر نيويورك، ١١ اكتوبر ٢٠١١

[٦٦] المجلس الاقتصادي والاجتماعي الدورة الموضوعية العام ٢٠١٠ نيويورك ، ٢٨ يونيه ٢٢٠ يوليه ٢٠١٠ البلد ١٣ (ب) من جدول الأعمال المؤقت المسائل الاقتصادية والبيئية، تسخير العلم والتكنولوجيا لأغراض التنمية والتقدم المحرز في تنفيذ ومتابعة نتائج مؤتمر القمة العالمي المجتمع المعلومات على الصعيدين الاقليمي والدولي.

[٦٧] المرجع نفسه (مناقشة الأوراق المالية الرقمية، أو النظام النقدي الرقمي المستخدم في البلدان الإفريقية.

[٦٨] أميرة عبد العظيم محمد عبد الجواد المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام المرجع السابق من ١٨٧

[٦٩] محمد عادل محمد عسكر وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسس وقت السلم، دراسة على ضوء دليل تالين بشأن القانون الدولي المطبق على العمليات السيبرانية ٢٠١٢-٢٠١٧ ،ص ١٢

[٧٠] خالد محمد نور عبد الحميد الطباخ المواجهة القانونية للإرهاب الإلكتروني الدولي، مجلة الدراسات القانونية والاقتصادية، جامعة ) مدينة السادات كلية الحقوق، مع ٣، ١٤، ٢٠١٧، ص ٢٣

[٧١] الفرق المتخصصة هي أداة من أدوات الاتحاد التي تعزز برنامج عمل لجان الدراسات من خلال توفير بيئة عمل بديلة التطوير المواصفات بسرعة في مجالات عملها، مما يجعلها مثالية للتكنولوجيات المتغيرة والمتطورة بسرعة مثل الشبكات الذكية، ويتألف الفريق المتخصص بالشبكة الذكية من ممثلين من مختلف الدول الأعضاء، وسيقوم بالتعاون مع مجتمعات الشبكة الذكية في جميع أنحاء العالم (مثل: معاهد البحوث والمنديات والأوساط الأكاديمية)

[٧٢] أميرة عبد العظيم محمد عبد الجواد المخاطر السيبرانية وسجل مواجهتها في القانون الدولي العام المرجع السابق، ص ٤٩٣

[٧٣] محمد عادل محمد عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسس وقت السلم دراسة على ضوء دليل تالين، بشأن القانون الدولي المطبق على العمليات السيبرانية ٢٠١٧-٢٠١٢، ٢٠٢٠ ، ص: ٢٠٨

[٧٤] أميرة عبد العظيم محمد عبد الجواد المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام المرجع السابق، ص: ١٩٤

[٧٥] المرفوعة إلى عناية مؤتمر المندوبين المفوضين، مؤتمر المندوبين wide قرارات المؤتمر العالمي لتنمية الاتصالات لعام ٢٠١٧ ) دبي، ٢٩ أكتوبر ١٦ نوفمبر ٢٠١٨، الاتحاد الدولي للاتصالات – pp المفوضين (١٨)

[٧٦] خالد محمد نور عبد الحميد الطباخ المواجهة القانونية للإرهاب الإلكتروني الدولي، مجلة الدراسات القانونية والاقتصادية – كليه " الحقوق – جامعة السادات – مجموعه ٣ ع ١-٢٠١٧، ص: ٣٤

[٧٧] إمباكت في مبادرة دولية مشتركة بين القطاعين العام والخاص لتعزيز قدرة المجتمع الدولية على منع الهجمات السيبرانية والدفاع ضدها : والتصدي لها، ويوفر هذا التعاون للدول الأعضاء في الاتحاد البالغ عددها ١٩٢ دولة وغيرها من الجهات الخبرات الفنية والتسهيلات والموارد اللازمة لتعزيز قدرات المجتمع العالمي تعزيزاً فعالاً، وزيادة القدرة على منع الهجمات السيبرانية، والدفاع ضدها والتصدي لها، وقد جذب هذا البرنامج منذ إطلاقه دعم واعتراف الزعماء وخبراء الأمن السيبراني في أنحاء العالم، انظر... أميرة عبد العظيم محمد عبد الجواد المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام المرجع السابق، ص ٤٩٦

[٧٨] طارق عزت رخاء المنظمات الدولية المعاصرة، دار النهضة العربية القاهرة، ٢٠٠٦، ص: ١٠٢١٤

[٧٩] عبد الصبور عبد القوي، الجريمة الالكترونية، دار العلوم للنشر والتوزيع، القاهرة، ٢٠٠٨، ص١٥٩

[80] Allison Peters & Amy Jordan, Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime, Journal of national security law, policy, Vol. 10:487, 2020

[81] Juan Ignacio Alcaide, Critical infrastructure cybersecurity and the marine security, University of Cadiz, Spain, 2020

[82] Joint Standing Committee on Foreign Affairs, Defense and Trade Inquiry into Australia's Relationship with ASEAN, 2008

[83] Juan Ignacio Alcaide, Critical infrastructure cybersecurity and the marine security, University of Cadiz, Spain, 2020

[84] William M. Stahl, the uncharted water of cyberspace; applying the principles of international maritime law to the problem of cybersecurity, University of Georgia, 2010

[85] Dora Arifi, Cybercrime: a challenge to law enforcement, SEEU Review Volume 15 Issue 2, Macedonia, 2020

[86] Allison Peters & Amy Jordan, Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime, Journal of national security law, policy, Vol. 10:487, 2020

[87] Pallavi Kapila, Cyber Crimes and Cyber Laws in India: An Overview, MCM DAV College for Women, Chandigarh, India, 2020

[88] Attila Tanzi and others, international law and cyberspace, Ministry of Foreign Affairs, Italy, 2021

[89] The United Nations, Cyberspace and International Peace and Security, Responding to Complexity in the 21st Century, UNIDIR, 2017 , P21

[90] Abdelmonem Mohamed Magdy, Overcoming the conflict of jurisdiction in cybercrime, Master thesis, American University in Cairo, 2020

[91] عماد الدين محمد كامل، الجرائم السيبرانية في زمن كورونا وآثارها على الامن القومي الاقتصادي : دراسة للتحديات القانونية والاقتصادية واستراتيجية المواجهة، بنك دبي الاسلامي، العدد ٥، ٢٠٢٢ ، ص٣٢

[92] صالح سعود، الانتربول ودوره في التعاون الامني الدولي، مجلة المنارة للدراسات القانونية والادارية، العدد ٢١، ٢٠١٧، ص٣

[93] هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، ١٩٩٤ ، ص٤٣

[٩٤] قطاف سليمان، بوقرين عبد الحليم، الاليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل اتفاقية بودابست والتشريع الجزائري، المجلة الاكاديمية للبحوث القانونية والسياسية، العدد ١، المجلد ٦، ٢٠٢٢

[95] شيخة حسين الزهراني، التعاون الدولي في مواجهة الهجوم السيبراني، مجلة جامعة الشارقة للعلوم القانونية، العدد١، ٢٠٢٠

[96] سامر محيي حمزة، مدى مساهمة الامم المتحدة في تشكيل القواعد الدولية الخاصة بالفضاء السيبراني : دراسة في ضوء تقرير فريق الخبراء الدولي لعام ٢٠٢١، مجلة مركز دراسات الكوفة، العدد ٧٦، ٢٠٢٢، ص٣١

[97] محمد محمود فياله، النظام القانوني للسفن غير المأهولة في ضوء القانون الدولي للبحار، مجلة كلية الحقوق، جامعة الاسكندرية، العدد ١، ٢٠٢٣، ص١٢

[98] حاتم احمد بطيخ، تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات، مجلة الدراسات القانونية والاقتصادية، جامعة السادات، العدد١، ٢٠٢١، ص٢٥

[99] مريم لوكال، قراءة في اتفاقية الاتحاد الافريقي حول الامن السيبراني وحماية المعطيات ذات الطابع الشخصي لسنة ٢٠١٤، مجلة الدراسات القانونية والاقتصادية، المجلد ٤، العدد ٢، ٢٠٢١، ص٣١