آليات ردع الهجمات السيبرانية والحماية منها في الإطار القانوني الدولي والإقليمي

الدكتورة: مايا صفطلي + الباحثة: زينه عجيل – كلية الحقوق – جامعة اللاذقية

ملخص

لم تعد القوة العسكرية التقليدية فقط هي العنصر الحاكم في العلاقات الدولية في ظل التطور العلمي والتكنولوجي المتسارع وطغيان استخدام الإنترنت والحوكمة الإلكترونية في كافة مناحي الحياة. وباتت الحروب في الوقت الراهن حروبا من نوع آخر ساهمت في إحداث تغيرات جذرية بجيوش الدول وآليات عملها وبرزت فيها العديد من الاستراتيجيات العسكرية الجديدة "كالضربات من غير هجوم" أو "التعطيل الشامل دون إطلاق رصاصة واحدة". معتمدة على أحدث أنواع التكنولوجيا في جميع مراحل الهجوم والدفاع والحماية والوقاية عبر المجال الرقمي للفضاء السيبراني. وبالتوازي مع ذلك وجد المجتمع الدولي نفسه أمام ضرورة ملحة وحاجة ماسة إلى ضبط هذا المجال وتنظيمه ونقله من مرحلة الفوضى في الاستخدام إلى مرحلة التنظيم القانوني ومن مرحلة تحديد الواجبات إلى مرحلة صيانة الحقوق، في محاولة لمواجهة تنامي مخاطر وتهديدات "الهجمات السيبرانية" والتخفيف من دورها المؤثر على السلم والأمن الدوليين وتأمين الطابع السلمي والمدني للفضاء السيبراني، في ضوء إشكالية القصور التشريعي التي تحيط بهذه المسألة.

الكلمات المفتاحية: الحروب السيبرانية، الهجمات السيبرانية، الفضاء السيبراني، الأمن السيبراني، المنظمات الدولية، المنظمات الإقليمية.

Mechanisms to deter and protect against cyber attacks within international and regional legal framework

Abstract :

Traditional military power is no longer the only ruling element in international relations in light of the rapid scientific and technological development and the tyranny of the use of the Internet and electronic governance in all aspects of life. Wars have now become wars of a different kind that have contributed to radical changes in countries armies and their operating mechanisms, and many new military strategic have emerged, such as strikes without an attack or comprehensive disruption without firing a single bullet, relying on the latest types of technology in all stages of attacks, defense, protection, and prevention across the field digital cyber space. In parallel with this, the international community found itself facing an urgent necessity and urgent need to control and organize this field and move it from the stage of defining duties to the stage of preserving rights. In an attempt to confront the growing risks and threats of cyber attacks, mitigate their role affecting international peas and security, and secure the peaceful and civil character of cyber space in light of the problem of legislative deficiency surrounding this issue.

Key words: Cyber war, Cyber attacks, Cyber space, Cyber security, International organizations, Regional organizations.

مقدمة:

يعد الفضاء السيبراني مجالا حيويا للعمليات المعلوماتية وهو ما يعني بالضرورة تعامله مع بيئة يسهل اختراقها وتعطيلها وتسمح بالانتشار السريع للمعلومات، الأمر الذي مثل انعكاسات عميقة على الأمن الدولي وغير طبيعة المفاهيم التقليدية للحروب. حقيقة إن تطبيق سياسات الرد والردع بصورتها التقليدية على الهجمات السيبرانية تواجه صعوبة بالغة نظرا لاستحالة التيقن من مصدر وهوية الطرف القائم بالهجوم، لذلك تلجأ الدول إلى استهداف الطرف الذي تعتقد أنه قام بشن هجوم سيبراني ضدها لتؤكد قدرتها على اختراقه وإمكانية الإضرار به وردعه عن محاولة تنفيذ أي هجمات جديدة ضدها. وعليه فإن جوهر الردع في المجال السيبراني قد تغير عن مفهومه التقليدي الذي كان سائدا إبان الحرب الباردة وأصبح يشكل نتاج امتلاك القدرة على الهجوم فضلا عن امتلاك القدرة على الدفاع. ومع الفراغ القانوني والخلاف المستمر بين أعضاء المجتمع الدولي حول الطبيعة القانونية للهجمات السيبرانية وعدم الاتفاق على تكييفها الدقيق، لا يتضح على وجه الخصوص والتحديد السبل القانونية أو الطرق العسكرية المتاحة للتعامل مع الحالة التي تتعرض فيها دولة ما إلى هجوم سيبراني واسع النطاق منشؤه دولة أخرى استهدف بنيتها التحتية الحيوية والحرجة، وكيفية مواجهتها وإمكانية الرد عليها، سيما وأن العدوان السيبراني له طبيعته الخاصة والمتميزة عن الحروب التقليدية فهو يتصف بعدم الحركة وانعدام الطاقة الحركية المادية الناتجة عنه، الأمر الذي كان خارجا عن تصور الدول عند وضعها وتصديقها للاتفاقيات الدولية والإقليمية كميثاق الأمم المتحدة مثلا.

لذلك سيتم البحث في هذا الموضوع من خلال مطلبين:

- يتناول المطلب الاول: آليات وجهود منظمة الأمم المتحدة لردع الهجمات السيبرانية والحماية منها.
- اما المطلب الثاني: آليات المنظمات الإقليمية والوكالات العالمية المتخصصة والمجهودات الفقهية الدولية لردع الهجمات السيبرانية.

مشكلة البحث:

تتمحور النقطة الاساسية في البحث حول التساؤل الآتي:

ما هي أهم الآليات القانونية أو الوسائل العسكرية المتاحة على الصعيدين الدولي والإقليمي لردع الهجمات السيبرانية والحد من آثارها في ظل غياب إطار قانوني دولي معني بها أو اتفاقية دولية خاصة تنظمها؟

ويتفرع عن هذا التساؤل الرئيس التساؤلات الفرعية الآتية:

1- كيف واجه المجتمع الدولي التوسع في استخدام الهجمات السيبرانية العدائية خلال النزاعات المسلحة المعاصرة؟

2- ما هي الجهود الدولية المبذولة في سبيل الحفاظ على الأمن السيبراني الذي أدرج على رأس أولويات الأمن الدولي مؤخرا؟

3- ما هي أهم الجهود الدولية المبذولة في سبيل مكافحة الهجمات السيبرانية والتخفيف من دورها السلبي على السلم والأمن الدوليين؟

4- ما هي أهم الجهود الإقليمية المبذولة في سبيل مواجهة تنامي خطر الهجمات السيبرانية والتقليل من تهديداتها وتداعياتها؟

5- ما هو موقف الدول والمنظمات الدولية الحكومية وغير الحكومية من السلوك غير المسؤول وغير القانوني في الفضاء السيبراني؟

6- هل يملك مجلس الأمن الدولي صلاحيات التدخل والرد على الهجمات السيبرانية؟ وكيف يمكن أن يكون رده وردعه؟

<u>أهمية البحث واهدافه:</u>

تظهر اهمية البحث انطلاقا من اعتباره محاولة بحثية قانونية تخوض في موضوع معاصر على مستوى الدراسات القانونية في مجال القانون الدولي، حيث ازدادت أهمية الأمن السيبراني على المستوى الدولي بشكل كبير وتزايدت معها بشكل متواز نسبة المخاطر والتهديدات التي يمكن أن تشكلها الأعمال الخبيثة في الفضاء السيبراني من ضرر هائل على الهياكل الأساسية الحيوية والهياكل الأساسية المعلوماتية. وتبدي مختلف الدول حاليا قلقها إزاء التهديد المتصاعد للهجمات السيبرانية وخشيتها من تعرض أمنها القومي للخطر نتيجة لتلك الاعتداءات، خاصة مع ربط مصالحها القومية ببنيتها التحتية الرقمية، لاسيما وأن تقنية المعلومات والاتصالات قد رفعت منسوب

الخطر عبر إتاحتها مصادر جددة متشعبة ومتعددة وإمكانات هائلة لتحققه. وتتلخص اهداف البحث بالآتي:

1- معالجة موضوع يعد من أهم الموضوعات الحديثة والبالغة الأهمية في الفكر الاستراتيجي الدولي وهو الامن السيبراني الذي احتل مكانة بارزة في جدول أعمال صانعي السياسات والقادة العسكريين حول العالم وأصبح من المسائل الهامة المدرجة على أجندة الأمن الدولي والمتداولة بكثرة في مراكز صنع القرار العالمي.

2- الوقوف على أبرز الآليات القانونية الدولية والإقليمية المتاحة والهادفة إلى الحفاظ على الأمن السيبراني ومحاربة الأخطار التي تكتنفه.

3- تسليط الضوء على أبرز الجهود الدولية والإقليمية القانونية والفقهية المبذولة في سبيل مواجهة الهجمات السيبرانية والحد من آثارها وتداعياتها على الصعيدين الدولي والإقليمي.

4- بيان تأثير الهجمات السيبرانية على السلم والأمن الدوليين وما إذا كان يحق لمجلس الأمن الدولي التدخل للرد عليها وفقا لميثاق الأمم المتحدة .

5- مناقشة أهم المواقف الصادرة عن المنظمات الدولية والإقليمية الحكومية وغير الحكومية بشأن مسألة الهجمات السيبرانية وآليات مواجهتها والرد عليها.

الدراسات السابقة:

1- **الدراسة الاولى: سامي محمد عبد الحمزة: مدى مساهمة الأمم المتحدة في تشكيل القواعد الدولية الخاصة بالفضاء السيبراني، دراسة في ضوء تقرير فريق الخبراء الدولي لعام 2021، 2022.**

وهدفت الدراسة الى بيان أهمية دور الأمم المتحدة في تكوين قواعد متكاملة لما يخص التهديدات التي فرضها الفضاء السيبراني على السلم والأمن الدوليين، منذ عام 1998، إلا أن محاولاتها لم تكن موفقة لغاية عام 2021، الذي انتهت فيه إلى إقرار قواعد للفضاء السيبراني، وتوصلت إلى نتائج ومفادها أن رغم محاولات الأمم المتحدة إلا أن الصراعات السياسية والاختلاف في الإيديولوجيا والمصالح بين الدول الأعضاء مثل عائقا أمام التوافق على قواعد عامة يمكن أن تضع أساسا لاتفاقية دولية بهذا الشأن.

2- الدراسة الثانية: هاني محمد خليل ابراهيم العزازي: النظام القانوني الدولي لمكافحة المخاطر السيبرانية، 2023.

وهدفت الدراسة الى تحديد خصائص وطبيعة الهجمات السيبرانية وجرائم الإنترنت العابرة للحدود، وبينت أنه في الوقت الحالي أصبح من الضروري التصدي لتلك الاعتداءات ومواجهة أخطارها وآثارها على السلم والأمن الدوليين، عبر تسليط الضوء على الطرق القانونية التي يجب اتباعها وكذلك الجهود الدولية المبذولة لتحقيق هذه الغاية. وخلصت الى نتائج ومضمونها أن العديد من الدول قامت باعتماد استراتيجيات من شأنها دعم الجانب العسكري في الفضاء السيبراني، وأنه بات من الأهمية توحيد الجهود الدولية لوضع الأطر القانونية والتنظيمية لمواجهة المخاطر السيبرانية وآثارها، وتواجد روح التعاون بين الأنظمة القانونية الداخلية للدول.

3- الدراسة الثالثة: ناجي محمد أسامة الشاذلي: الجوانب القانونية للحرب السيبرانية، 2023.

هدفت الدراسة الى إلقاء الضوء على الطبيعة القانونية للحروب السيبرانية التي تقع بين الدول وتكييفها الدقيق والبحث في أهم الطرق القانونية المتاحة أمام الدول للتعامل معها، وتوصلت إلى نتائج وجوهرها عدم إمكانية الإقرار بالفراغ القانوني في المجال السيبراني وأن هناك من القواعد الدولية الحالية ما يمكن الاستناد إليه في تنظيم تلك الحروب، وأنه يجب على المنظمات الدولية والإقليمية بذل المزيد من الجهود ووضع الآليات لتحقيق استجابة دولية فعالة وسد الثغرات الناتجة عن هذه المسألة.

4- الدراسة الرابعة: James Andrew Lewis: Creating Accountability for global cyber norms, 2022.

هدفت الدراسة إلى التساؤل لماذا لا يوجد نظام مساءلة دولي للحد من الهجمات السيبرانية؟ وناقشت المعايير الدولية المطبقة حاليا من منظمة الأمم المتحدة لمواجهة تلك الهجمات وأبرز التحديات التي تواجه عمليات الإسناد السياسي لها، وتوصلت إلى نتائج وقوامها ضرورة خلق نظام مساءلة دولية ملزم سياسيا لجميع الدول التي تستخدم الفضاء السيبراني لمواجهة الهجمات السيبرانية باعتبارها من أخطر القضايا الدولية المطروحة حاليا.

وتهدف هذه الدراسة موضع البحث الى استعراض أبرز الآليات القانونية المتاحة وأهم الجهود المكثفة والمبذولة من قبل هيئة الأمم المتحدة ابتداء وعبر مختلف أجهزتها الرئيسية كالجمعية العامة، مجلس الأمن الدولي و المجلس الاقتصاد والاجتماعي، مرورا بالمنظمات الإقليمية والوكالات

العالمية المتخصصة والتحالفات الدولية البارزة، وصولا إلى المساهمات والمجهودات الفقهية الدولية، في سبيل الحفاظ على الأمن السيبراني ومواجهة الهجمات السيبرانية والحد من آثارها وتداعياتها على الصعيدين الدولي والإقليمي رغم إشكالية القصور التشريعي التي ما زالت تحيط بها حتى الآن.

منهج البحث :

تم إتباع المنهج الوصفي والمنهج التحليلي كمنهجين أساسيين في البحث من خلال توصيف أبرز الآليات القانونية والوسائل العسكرية المعتمدة على الصعيدين الدولي والإقليمي والوطني في مواجهة التوسع في استخدام الهجمات السيبرانية خلال النزاعات المسلحة المعاصرة والحد من آثارها، وتحليل أهم الجهود والمواقف الدولية والإقليمية والوطنية القانونية والفقهية الصادرة حول رفض السلوك غير المسؤول وغير القانوني في الفضاء السيبراني كمحاولة لتدارك غياب الإطار القانوني الحاكم والاتفاق الدولي الملزم.

خطة البحث:

1- المطلب الاول: آليات وجهود منظمة الأمم المتحدة لردع الهجمات السيبرانية والحماية منها.
   1- الفرع الاول: دور الجمعية العامة للأمم المتحدة.
   2- الفرع الثاني: دور وصلاحيات مجلس الأمن الدولي في ردع الهجمات السيبرانية.
   3- الفرع الثالث: دور المجلس الاقتصادي والاجتماعي.

2- المطلب الثاني: آليات المنظمات الإقليمية والوكالات العالمية المتخصصة والمجهودات الفقهية الدولية.
   1- الفرع الاول: دور المنظمات الإقليمية.
   2- الفرع الثاني: دور الوكالات العالمية المتخصصة والتحالفات الدولية.
   3- الفرع الثالث: المجهودات الفقهية الدولية.

الجانب النظري للبحث:

المطلب الاول: آليات وجهود منظمة الأمم المتحدة لردع الهجمات السيبرانية والحماية منها.

يبدو أن مع تطور وسائل وأساليب الحرب المستحدثة والتهديد بها أصبح باستطاعة أي دولة أن تشن هجمات سيبرانية واسعة النطاق ضد البنية التحتية الحيوية والحرجة لدولة أخرى، لتزعزع سيادتها وأمنها وتخترق من خلالها نظام الطيران العسكري أو المدني أو أنظمة الدفاع الجوي

أو محطة نووية أو كهربائية أو مائية، مستهدفة الأعمال التدميرية والتخريبية ومعرضة حياة المدنيين للخطر[1]. لتحقيق بواعث ودوافع مختلفة قد تكون سياسية، أمنية، عسكرية، واقتصادية. خاصة وأن أنظمة أغلب الجيوش في العالم أصبحت تعتمد على أحدث أنواع التكنولوجيا ومتصلة بالإنترنت ومرتبطة بشبكات إلكترونية معقدة ومتداخلة، تفتقد عوامل الأمان بالمطلق[2]. ولما كان حفظ السلم والأمن الدوليين ومنع تهديد الاستقرار العالمي يمثلان أول وأهم الأهداف الجوهرية التي نص عليها الميثاق الأممي 1945، اتجهت الأمم المتحدة وعبر مختلف أجهزتها الرئيسية كالجمعية العامة، مجلس الأمن الدولي، والمجلس الاقتصادي والاجتماعي إلى إنفاذ آليات قانونية واتخاذ اجراءات دولية كمحاولة للحفاظ على الأمن السيبراني ومواجهة الاعتداءات السيبرانية وردع المعتدي.

الفرع الاول: دور الجمعية العامة للأمم المتحدة.

أصبح "الأمن السيبراني" أحد القضايا المحورية التي لا تزال محل تطوير وتقنين دولي. وبذلت الجمعية العامة للأمم المتحدة في سبيل الحفاظ عليه ومواجهة الهجمات السيبرانية والحد من آثارها جهودا مكثفة منذ تسعينات القرن العشرين، حيث تركزت الجهود الأممية على ضرورة تطوير قواعد القانون الدولي لتتمكن من احتواء تلك الهجمات وتضمينها من بين الأعمال العدائية التي تنطوي على استعمال القوة المحظورة بموجب المادة (2ف4) من الميثاق، وعلى تعزيز العمل المشترك بين الدول لوضع المعايير والتدابير المناسبة لبناء الثقة والتوظيف على المستوى الدولي[3]. وبهدف تحقيق ذلك عقدت ورعت العديد من المؤتمرات الدولية والقمم العالمية، وأصدرت الكثير من القرارات والتوصيات حول أمن المعلومات وجرائم أجهزة الحاسوب والاعتداءات السيبرانية، وأنشأت فريقا من الخبراء الحكوميين المعني بالتطورات في مجال المعلومات والاتصالات السلكية واللاسلكية

[1] عدنان النقيب، الحرب الإلكترونية في ضوء بروتوكولي سبع وسبعين الملحقين باتفاقيات جنيف لعام تسع وأربعين (الهجمات السيبرانية). مصر، القاهرة، المركز العربي للنشر والتوزيع، 2022، ص:35.

[2] Jeffry Carr, Inside cyber warfare: Mapping the cyber under world, ORELLY Media, (2ed), USA, 2012, p:6.

[3] فاطمة الظبيري، القانون الدولي والهجمات الإلكترونية ما دون استخدام القوة، المجلة الدولية للقانون، المجلد 11، العدد 1، دار نشر جامعة قطر، كلية القانون، جامعة قطر، 2022، ص 238.

في سياق الأمن الدولي، وناقشت مختلف هيئاتها ولجانها المعنية مسألة أمن الفضاء السيبراني وضرورة الابقاء على طابعه السلمي[1].

أولا: قرارات الجمعية العامة للأمم المتحدة بشأن استخدام تكنولوجيا المعلومات والاتصالات وأمن الفضاء السيبراني.

اتخذت الجمعية العامة للأمم المتحدة سلسلة من القرارات السنوية المتلاحقة والمتتابعة بشأن الإرهاب السيبراني وحماية أمن المعلومات والاتصالات منذ عام1998، وحاولت الجمعية العامة من خلال هذه القرارات حث الدول على الاستخدام السلمي للفضاء السيبراني، وأكدت فيها على أن سوء استخدام تقنيات المعلومات يؤثر على مصالح المجتمع الدولي بأسره، ودعت تلك القرارات الدول الأعضاء في الأمم المتحدة إلى استعراض وجهات نظرهم حول أمن المعلومات والاتصالات[2]. نذكر من هذه القرارات:

القرار رقم63/55 المتخذ في 4 كانون الأول 2000، والذي وضع الإطار القانوني بشأن مكافحة إساءة استخدام تكنولوجيا المعلومات لأغراض إجرامية. وقد أوصى القرار:

أن 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[3].

القرار رقم 121/56 المتخذ في 19 كانون الأول 2001، والذي دعا الدول الأعضاء عند وضع التشريعات الوطنية إلى مكافحة سوء استعمال تكنولوجيا المعلومات وأن تأخذ بالاعتبار توصيات عمل لجنة منع الجريمة والعدالة الجنائية الدولية[4].

---

[1] هاني محمد خليل العزازي، النظام القانوني الدولي لمكافحة المخاطر السيبرانية، مجلة مصر المعاصرة، العدد:549، يناير 2023، ص500.

[2] زينة عجيل، (2022). مدى شرعية الحرب في الفضاء الإلكتروني وفقا لقواعد القانون الدولي الإنساني والاتفاقيات الدولية، رسالة ماجستير: قسم القانون الدولي، كلية الحقوق، جامعة تشرين، اللاذقية، سورية، ص13.

[3] United Nation, General Assembly, (A/RES/63/55) 4December 2000.

[4] United Nation, General Assembly, (A/RES/56/121) 19December 2001.

[4] United Nation, General Assembly, (A/RES/57/239) 31December 2002.

وفي دورتها (56،258) المعقودة في 31 كانون الثاني 2002، تبنت الجمعية العامة للأمم المتحدة **القرار رقم 239/57** والذي دعا الى استخدام تكنولوجيا الاتصال والمعلومات من أجل التنمية. حيث جاء هذا القرار لتنبيه الرأي العام العالمي وتنمية الوعي بحجم المخاطر والأضرار الناتجة عن الهجمات السيبرانية ولإرساء ثقافة عالمية للأمن السيبراني وحماية الهياكل الأساسية الحيوية للمعلومات، وسلمت فيه بضرورة دعم الجهود الوطنية بتبادل المعلومات والتعاون في هذا المجال على كافة الصعد الوطنية والإقليمية والدولية كي يتسنى التصدي الفعال لما تتسم به الهجمات السيبرانية من طابع عابر للحدود الوطنية[1].

ثم اعتمدت القرار 60/177 لعام 2005، بشأن تشجيع التعاون الدولي لمكافحة الاعتداءات السيبرانية وتقديم المساعدة للدول الأعضاء في هذا المجال[2]. **والقرار رقم64/21 لعام 2010**، الذي دعا الدول إلى تحديث قوانينها في مجال الاعتداءات السيبرانية وحماية الخصوصية والبيانات الشخصية والتجارة والتوقيع الإلكترونيين وكذلك اعتماد اتفاقيات إقليمية بهذا الشأن[3]. وبعد ازدياد وتيرة تبادل الهجمات السيبرانية بين الدول، عبرت الجمعية العامة عن قلقها المتزايد إزاء تلك الهجمات وأصدرت في هذا الصدد مجموعة من القرارات الجديدة أدت فيها هذه المرة على أن الهجمات السيبرانية يمكن أن تستخدم في أغراض لا تتوافق مع مقتضيات الحفاظ على السلم والأمن الدوليين، وأن الاستخدام العدائي لتكنولوجيا المعلومات قد يكون له تأثير خطير على بعض الدول، **كالقرار رقم 65/41 المتخذ في 8 كانون الأول لعام 2010، والقرار66/24 المتخذ في 2 كانون الأول 2011، والقرار 67/27 المتخذ في3 كانون الأول 2012**[4].

وأخيرا، أيدت الجمعية العامة عقد "**القمة العالمية لأمن المعلومات**" والتي انعقدت على مرحلتين الأولى في جنيف2003، والثانية في تونس العاصمة 2005، حيث عهد من خلالها رؤساء

---

[2] United Nation, General Assembly, (A/RES/60/177) 2005.

[3] United Nation, General Assembly, (A/RES/64/21) 2010.

[4] United Nation, General Assembly, (A/RES/65/41) 8January2010, (A/RES/66/24) 2January 2011, (A/RES/67/26) 3January 2012.

الدول وقادة العالم إلى الاتحاد الدولي للاتصالات بوصفه وكالة عالمية متخصصة في هذا المجال بالعمل على بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات[1].

ثانيا: فريق الخبراء الحكوميين المعني بالتطورات في مجال المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي.

أدى تردد الدول في العمل على وضع تقنين دولي شامل لتنظيم السلوك في الفضاء السيبراني والحفاظ على أمنه وتأمين طابعها السلمي، وكذلك بطء اجراءات تحضير وإبرام اتفاقيات دولية معنية إلى ضرورة إيجاد وسيلة أكثر مرونة لسد الفراغ التشريعي والعملي[2]. خاصة مع خضم اللجوء المحموم لاستخدام الهجمات السيبرانية كنمط جديد من الاستراتيجيات العسكرية الحديثة وما تتميز به من خاصية عابرة للحود الإقليمية للدول، كالهجمات العدائية التي استهدفت أستونيا 2006، جورجيا 2008[3].

وعليه أنشأت الجمعية العامة فريق الخبراء الحكوميين المعني بالتطورات في مجال المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي في2 كانون الثاني 2019 على أن يعمل ضمن هيئة نزع السلاح التابعة لها، وتكون من خبراء يمثلون 25 دولة على أساس التوزيع الجغرافي العادل[4].

وبعد اجتماعات ومشاورات ومفاوضات لمدة سنتين وظهور بوادر توافق سياسي بين الدول الأطراف استطاع الفريق أن يصدر تقريره في14 تموز 2021، بالاتفاق بين جميع أعضاءه حيث تضمن للمرة الأولى معايير السلوك المسؤول في الفضاء السيبراني، ونص على أن القانون الدولي وخاصة ميثاق الأمم المتحدة قابل للتطبيق وهو ضروري للحفاظ على السلام والاستقرار والأمن في بيئة تكنولوجيا الاتصالات والمعلومات. وأكد على أن مبدأ السيادة الوطنية ينطبق على الفضاء

---

[1] United Nation, The International Telecommunication Union, Strategy for cyber security Geneva, 2008.

[2] فاطمة الزبيري، القانون الدولي والهجمات الإلكترونية، مرجع سابق، ص237.

[3] James Andriew Lewis, Creating Accountability for global cyber norms. Center for strategic and international studies(CSIS), 23/2/2022, Available at: https://www.csis.org.creating-accountability-for-global-cyber-novms/.

[4] سامر محي عبد الحمزة، مدى مساهمة الأمم المتحدة في تشكيل القواعد الدولية الخاصة بالفضاء السيبراني، دراسة في ضوء تقرير الخبراء الدولي لعام 2021، مجلة مركز دراسات الكوفة، المجلد 17، العدد 67، الجزء الأول، 2022، ص231.

السيبراني بدرجة انطباقه على الأرض نفسها، كما تم الاتفاق على قائمة مطولة من قواعد واجراءات لبناء الثقة والأمن في الفضاء السيبراني[1].

مبدئيا، يمكننا القول بأن التقرير قد شكل سابقة تتمثل في حصول إجماع دولي على بعض القواعد التي تحكم الفضاء السيبراني، على الرغم من اعتراف الفريق بعدم إمكانية الاتفاق على مسائل أخرى تخص القانون الدولي كمدى انطباق القانون الدولي الإنساني وكذلك الدفاع الشرعي ضد الهجمات السيبرانية[2]. بل وكشف التقرير عمق الخلاف حول أساسيات التعامل الدولي في الفضاء السيبراني، وبدا غير متناسب مع الهجمات التي أفرزها ذلك الفضاء وخطورة التحديات التي أصبحت تمثلها على السلم والأمن الدوليين. ويعود ذلك إلى اختلاف سياسات ومصالح الدول خاصة الكبرى منها، فلا زالت القوى العظمى تدفع المنظمة نحو سياسات تلائم مصالحها القومية، فالولايات المتحدة الأمريكية تريد التأسيس لمبدأ "الفضاء المفتوح" بما يضمن استمرار سيطرتها على البيئة السيبرانية في حين تحاول روسيا الاتحادية والصين التمسك بمبدأ "المساواة في السيادة" وإعطاء الدور الأكبر للمنظمة[3].

وبمراجعة وتحليل مبادئ السلوك السيبراني الواردة في تقرير الخبراء الدولي لعام 2021 نجد بأنها أقرت بإمكانية ازدواجية المبادئ والقواعد القابلة للتطبيق في البيئة السيبرانية المستحدثة، أي أنها انطوت على شقين من المبادئ في ذات الوقت:

1- تطبيق المبادئ التقليدية على الفضاء السيبراني.

وهي مبادئ القانون الدولي ذاتها الواردة في ميثاق الأمم المتحدة والتي استقرت بين الدول انطلاقا من أن الاعتماد على القواعد القديمة لتشمل وتغطي الحالات المستحدثة أسهل من تأسيس قواعد دولية جديدة لم يسبق وأن تم التوافق عليها. وعليه حاولت الجمعية العامة تطبيق المبادئ التقليدية التي تم الاتفاق عليها من قبل الدول الأعضاء

[1] الأمم المتحدة، الجمعية العامة، تقرير فريق الخبراء الحكوميين المعني بالتطورات في مجال المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، 14 تموز 2021، (A/68/98,15) :Doc، ص8+9.

[2] سامر محي عبد الحمزة، مدى مساهمة الأمم المتحدة في تشكيل القواعد الدولية الخاصة بالفضاء السيبراني، مرجع سابق، ص232.

[3] سامر محي عبد الحمزة، مدى مساهمة الأمم المتحدة في تشكيل القواعد الدولية الخاصة بالفضاء السيبراني، مرجع سابق، ص226.

على الفضاء السيبراني كمبدأ احترام السيادة الوطنية للدول، مبدأ حل النزاعات الدولية بالطرق السلمية، مبدأ عدم جواز استعمال القوة في العلاقات الدولية ومبدأ عدم جواز التدخل في الشؤون الداخلية للدول[1].

2- وضع قواعد تخص الفضاء السيبراني.

وضع الفريق قواعد جديدة تخص الفضاء السيبراني انطلاقا من أن القواعد التقليدية وحدها قد لا تكفي ولا تسعف المجتمع الدولي في مواجهة الأخطار والتهديدات التي فرضتها البيئة السيبرانية لذلك أضاف مبادئ جديدة فرضتها طبيعة الفضاء السيبراني كمبدأ التعاون الدولي المشترك، مبدأ التحقيق، ومبدأ احترام حقوق الإنسان في المجال السيبراني[2].

وصفت هذه المبادئ بأنها ستضع الأساس لتعامل الدول وسلوكها في الفضاء السيبراني، وقد رأى **البروفيسور** "**مايكل شميث**" أن القواعد التقليدية التي جاء بها التقرير ستتحول إلى قواعد ملزمة تقرها الدول في التعامل أما القواعد الأخرى الجديدة فستكتسب إلزاميتها من خلال تحولها بمرور الزمن الى قواعد عرفية[3].

ورغم أن التقرير غير ملزم يبقى له قيمة أدبية ومعنوية هامة لصدوره تحت مظلة الأمم المتحدة وبموافقة قوى سيبرانية عظمى على رأسها الولايات المتحدة والاتحاد الأوروبي وروسيا والصين ولكونه يمثل إجماع سياسي ودولي تاريخي حول ضرورة فهم القضايا السيبرانية ذات الأهمية الوطنية والإقليمية والدولية[4].

---

[1] سامر محي عبد الحمزة، مدى مساهمة الأمم المتحدة في تشكيل القواعد الدولية الخاصة بالفضاء السيبراني، مرجع سابق ص232.

[2] سامر محي عبد الحمزة، مدى مساهمة الأمم المتحدة في تشكيل القواعد الدولية الخاصة بالفضاء السيبراني، مرجع سابق، ص235.

[3] Michael Schmitt, The sixth United Nation GGE and International law in cyber space, Just Security center on law and security at New York university school of law, 10/6/2021, Available at: https://www.justsecurity.org./76864/the-sixth-united-nation-gge-and-international-law-in-cyber-space/.

[4] فاطمة الظبيري، القانون الدولي والهجمات الإلكترونية، مرجع سابق، ص238.

وتأكيدا على ذلك تم إنشاء فريق خبراء ثان تبعه مباشرة باقتراح قدم من روسيا الاتحادية وأطلق عليه الفريق العامل المفتوح العضوية المعني بالتطورات في ميدان الاتصالات السلكية واللاسلكية في سياق الأمن الدولي، والفرق الوحيد بين الفريقين هو أن الثاني يضم في عضويته أعضاء الجمعية العامة للأمم المتحدة، إذ بين الاقتراح الروسي أن التوافق لن يتم إلا بإشراك الدول كافة في هذا الموضوع، ولجعله أكثر ديموقراطية وشفافية ومسؤولية[1].

ثالثا: الديبلوماسية السيبرانية.

لعبت الجمعية العامة للأمم المتحدة دورا بناء ومحوريا في التأسيس "للدبلوماسية السيبرانية" والتي قادت بدورها إلى إرساء "نظام الأمن السيبراني العالمي" الذي يهدف إلى الردع السيبراني وحماية الفضاء السيبراني من كل الهجمات العدائية التي قد تطاله أو تجري عبر مجاله الرقمي. والتي تهدف عادة للوصول إلى المعلومات الحساسة واستغلالها في أفعال قد تهدد أمن الدول والأشخاص الطبيعيين أو الاعتباريين. ويشمل "نظام الأمن السيبراني" كافة القواعد والمؤسسات والاجراءات الرسمية وغير الرسمية والتي تعمل على تطوير القواعد الدولية الحاكمة للأنشطة السيبرانية[2].

غالبا ما تسفر الهجمات السيبرانية عن إحداث نوع من التوتر والاحتقان في العلاقات الدبلوماسية بين الدول ولعل المثال الأبرز على ذلك هو تصاعد ذروة الحرب السيبرانية بين كل من روسيا الاتحادية والولايات المتحدة الأمريكية على خلفية الاتهامات التي وجهت لروسيا بالتدخل في الانتخابات الرئاسية الأمريكية لصالح دعم المرشح الجمهوري "دونالد ترامب" واختراق البريد الإلكتروني الخاص بحملة المرشح النافس الديموقراطية "هيلاري كلينتون" مما أحدث اهتزازا في شرعية نتائج الانتخابات الأمريكية. وعادة ما تلجأ الدول الى وسائل تنطوي على استخدام الأدوات الديبلوماسية التقليدية معا للاستفادة في الفضاء السيبراني بالشكل الذي يؤدي إلى احتواء الهجمات

[1] سامر محي عبد الحمزة، مدى مساهمة الأمم المتحدة، مرجع سابق، ص231+232.

[2] بالموهوب رياض، قدوج نور الدين، الردع الإلكتروني كآلية لمواجهة الهجمات السيبرانية، مذكرة مقدمة لاستكمال متطلبات نيل شهادة الماجستير في الحقوق، تخصص قانون إعلام آلي وإنترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الابراهيمي، الجزائر، 2023، ص42.

السيبرانية والحد من آثارها[1]. وظهرت بعض الأمثلة على تصاعد دور الديبلوماسية السيبرانية في احتواء التهديدات والاعتداءات المتوقعة عبر إبرام العديد من الاتفاقيات الدولية أو الثنائية السياسية والعسكرية فيما بين الدول. كالاتفاق الذي توصلت إليه الولايات المتحدة الأمريكية والصين الخاص بالحرب السيبرانية في 9 إيلول 2015 والذي يقضي بعدم شن أي هجمة سيبرانية بين الدولتين على البنية التحتية الحيوية والحرجة وشركات القطاع الخاص في حالة السلم[2].

الفرع الثاني: دور مجلس الأمن الدولي وصلاحياته.

وضع ميثاق الأمم المتحدة نظاما دقيقا لحفظ السلم والأمن الدوليين وأوكل أمر تنفيذه إلى مجلس الأمن الدولي كجهاز تنفيذي محدود العضوية يعمل بالنيابة عن أعضاء الأمم المتحدة وبموافقتهم، وزوده بالصلاحيات التي تجعله يحقق فعالية نظام الأمن الجماعي عن طريق العمل المباشر والسريع[3]. عبر منحه سلطة واسعة بموجب الفصلين السادس والسابع من الميثاق في تقدير وجود انتهاك للسلم والأمن الدوليين او تهديد لهما او عمل من أعمال العدوان[4]. وله أن يقرر ما يجب اتخاذه من التدابير القسرية كالتي لا تتطلب استخدام القوة المسلحة مثل العقوبات الاقتصادية وفقا للمادة 41 من الميثاق او التدابير التي تتطلب استخدام القوة وتتضمن الأعمال العسكرية وفقا للمادة 42 من الميثاق إذا تبين أن التدابير السلمية لم تجد نفعا في سبي لصون السلم والأمن الدوليين[5].

أولا: انتهاك الهجمات السيبرانية للسلم والأمن الدوليين.

يبدو أن السمة الرئيسية للمرحلة التي يستطيع مجلس الأمن الدولي التدخل فيها بحكم سلطته كون الفعل المجرم عملا من شأنه أن يشكل تهديدا حقيقيا للسلم والأمن الدوليين، فيعد على إثر ذلك

[1] ناجي محمد أسامة الشاذلي، الجوانب القانونية للحرب السيبرانية، دراسة في إطار القانون الدولي الإنساني، مجلة روح القوانين، العدد 103، الجزء الثاني، 2023، ص1258-1259.

[2] إيهاب خليفة، مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي، مركز المستقبل للأبحاث والدراسات المتقدمة، مصر :القاهرة، دار العربي للنشر والتوزيع، 2019، ص113.

[3] المادة 24 من ميثاق الأمم المتحدة لعام 1945.

[4] المادة39 من ميثاق الأمم المتحدة لعام1945.

[5] المادتان 41و 42 من الميثاق الأممي.

غير قانوني ومفتقد للشرعية. وعلى اعتبار أن الهجمات السيبرانية ذات طبيعة تكنولوجية وتقية متطورة، فإنها تتمتع بقدرة فائقة على إحداث أضرار مادية وخسائر محققة في الأهداف المقصودة، وتحقيق مكاسب جوهرية بأقل التكاليف على كافة الصعد للدولة المهاجمة، كما أن شنها يؤدي إلى نتائج مدمرة قد تتجاوز تلك التي تسببها الهجمات المسلحة التقليدية المحظورة كالتدمير والتعطيل الكلي أو الجزئي للبنية التحتية الحرجة والحيوية وما ينجم عن ذلك من خسائر هائلة في الأرواح أو إلحاق إصابات او إتلاف وتدمير الممتلكات والمنشآت العسكرية والمدنية في الدولة المستهدفة[1].

وبناء عليه، يمكننا القول أنه عند حدوث هجوم سيبراني ممنهج ضد إحدى الدول الأعضاء في الأمم المتحدة وتبنيها من جهة دولية معترف بها، فإنه يجب تفعيل دور مجلس الأمن الولي الذي يستطيع أن يكيف هذه الأفعال على أنها هجمات غير شرعية وغير قانونية ومن ثم أن يتدخل باتخاذ التدابير المناسبة والاجراءات الفعالة لردعها في سبيل صون السلم والأمن الدوليين بما في ذلك الوسائل العسكرية[2]. انطلاقا من أساس يقوم على أنه ليس هناك ما يمنع من عدها واحدة من أهم التهديدات الماسة بالسلم والأمن الدوليين والتي تشكل انتهاكا جسيما وخرقا صريحا لهما وبالتالي ضرورة تطبيق القواعد القانونية المنصوص عليها في القانون الدولي على تلك الهجمات.

ثانيا: التدابير التي يمكن لمجلس الأمن أن يقررها لردع الهجمات السيبرانية.

لم تطرح قضية الأمن السيبراني أمام مجلس الأمن حتى وقت قريب، وذلك مع زيادة مخاطر الأنشطة السيبرانية الخبيثة وتزايد الاعتماد على الشبكات العالمية وتطور المنافسة بين القوى العظمى[3]. وعليه أصدر مجلس الأمن الدولي أولى قراراته المتعلقة بالبيئة السيبرانية، وهو القرار ذي الرقم 2341 الصادر في 13 شباط 2017، وكان موضوعه الأخطار التي تهدد السلم والأمن الدوليين من جراء الأعمال الإرهابية، حيث تمت بموجبه دعوة الدول الأعضاء إلى معالجة التهديدات ضد البنية التحتية الحيوية بما في ذلك التهديدات الناجمة عن الإنترنت وتكنولوجيا المعلومات والتقنيات الرقمية الجديدة. وبحسب نص القرار، فقد أهاب فيه مجلس الأمن الدول الأعضاء إلى إنشاء وتعزيز الشراكات الوطنية والإقليمية والدولية مع الجهات صاحبة المصلحة من القطاعين العام

[1] عدنان النقيب، الحرب الإلكترونية في ضوء بروتوكولي سبع وسبعين الملحقين باتفاقيات جنيف لعام تسع وأربعين، مرجع سابق، ص110.

[2] زينة عجيل، مدى شرعية الحرب في الفضاء الإلكتروني، مرجع سابق، ص84.

[3] James Andriew Lewis, Creating Accountability for global cyber norms, op.cit.

والخاص حسب الاقتضاء، لتبادل المعلومات والخبرات من أجل منع الهجمات الإرهابية السيبرانية على الهياكل الأساسية الحيوية والحماية منها والتخفيف من آثارها والتعافي من أضرارها والتحقيق في مواجهتها وذلك بوسائل التدريب المشترك واستخدام أو إنشاء آليات للاتصال والإنذار في حالات الطوارئ[1]. ثم تبعه مباشرة القرار رقم 2370 لعام 2017، وفي هذا القرار حث مجلس الأمن الدول الأعضاء على العمل بصورة جماعية وفعالة لمنع الإرهابيين من حيازة الأسلحة من خلال تكنولوجيا المعلومات والاتصالات مع احترام حقوق الإنسان والحريات الأساسية والامتثال للالتزامات بموجب القانون الدولي[2].

أما بالنسبة للتدابير القسرية، فإذا ما وصف مجلس الأمن الدولي الهجمة السيبرانية بأنها تشكل تهديدا للسلم أو خرقا للسلام أو عمل عدواني فإنه بذلك يمكنه استخدام صلاحياته الواردة في الميثاق لردعها. وتشمل التدابير التي يمكن لمجلس الأمن أن يتخذها:

1- بموجب المادة 41.

وقف الصلات الاقتصادية والمواصلات الحديدية والبحرية والجوية والبرية والبريدية والبرقية واللاسلكية وغيرها من وسائل المواصلات وقفا جزئيا او كليا، وقطع العلاقات الدبلوماسية. كما يمكن له أن يفرض عقوبات إلكترونية في السياق السيبراني كالحد من الوصول للإنترنت للدولة المسؤولة عن انتهاك السلم او خرقه او القيام بعمل عدواني. وقد يطلب من الدول الأعضاء حظر دعم الدولة المهاجمة بالأجهزة والبرامج التي تسهل الاتصال بالإنترنت والتأكد من رفض الوصول الى صفحات الويب في الدولة المعتدية. وقد يطلب من الدول الأعضاء بالأمم المتحدة أيضا تبني تشريعات وطنية لتنفيذ العقوبات في نظامها القانوني المحلي، على سبيل المثال تجريم سلوك سيبراني معين او مطالبة مزودي خدمات الإنترنت الوطنيين باعتماد تدابير تقييدية[3].

2- بموجب المادة 42.

---

[1] United Nation, Security Counsel, (S/RES/2341) 13 February 2017.

[1] United Nation, Security Counsel, (S/RES/2370) 2017.

[3] زينة عجيل، مدى شرعية الحرب في الفضاء الإلكتروني، مرجع سابق، ص84+85.

[3] محمود حسين الشرقاوي، الهجمات الإلكترونية في ضوء أحكان القانون الدولي الإنساني، أطروحة دكتوراه: قسم القانون الدولي، كلية الحقوق، جامعة بني سويف، مصر، 2021،ص198+199.

إذا اعتبر مجلس الأمن أن التدابير المنصوص عليها في المادة 41 غير كافية او ثبت أنها غير كافية يمكن أن يأذن للدول الأعضاء بالأمم المتحدة او لقوات حفظ السلام التابعة لها بشن هجمات سيبرانية مضادة، ترقى الى مستوى استخدام القوة من أجل الرد على احتمال تهديد السلم. وبالنظر إلى الغرض الأساسي من المادة 42 والذي يتمثل بتوسيع تدابير الأمن الجماعي لتشمل كافة المجالات العسكرية المتاحة في وقت تهديد السلم والأمن الدوليين، الأمر الذي يعني أن هذه التدابير يمكن أن تشمل استخدام أي مجال مستحدث آخر، كالفضاء السيبراني والذي أفرزته بيئة تكنولوجيا المعلومات والاتصالات[1].

وبرأينا لا يوجد ما يمنع من استخدام الفضاء السيبراني باعتباره المجال الخامس المستحدث في النطاق الدولي لإيقاع التدابير القسرية المنصوص عليها في ميثاق الأمم المتحدة على الدولة المخالفة لأحكام هذا الميثاق.

الفرع الثالث: دور المجلس الاقتصادي والاجتماعي.

أصدر المجلس الاقتصادي والاجتماعي التابع لمنظمة الأمم المتحدة مجموعة من القرارات المتلاحقة **كالقرار رقم 46 لعام 2006، القرار رقم 8 لعام 2007، القرار رقم 3 لعام 2008، القرار رقم 7 لعام 2009**[2]. وهي عبارة عن قرارات أحاطت فيها اللجنة الدولية المعنية بتسخير العلم والتكنولوجيا لأغراض التنمية علما بنتائج تنفيذ مؤتمر القمة العالمي لمجتمع المعلومات استنادا إلى ما ورد في مساهمات من كيانات الأمم المتحدة ذات الصلة. وافتتح المجلس الاقتصادي والاجتماعي دورته لعام2010 بجلسة إعلامية حول التحديات التي يطرحها الأمن السيبراني فضلا عن التهديدات والمخاطر التي يتيحها الاستخدام العدائي للإنترنت الآخذ في الاتساع. وشدد المجلس من بين عدة أمور على الحاجة الملحة الى اتخاذ مبادرات دولية تكفل تبادل المعلومات وأفضل الممارسات والتدريب والبحث. وأعلن المشاركون في المناقشة أنه يتعين على الأمم المتحدة أن "توحد أدائها" بشأن هذه القضية بهدف زيادة التعاون بين الدول من جهة وبين الدول والقطاع الخاص من جهة أخرى لضمان الأمن السيبراني. وحذروا

[2] United Nation, ECOSOC, (E/RES/2006/46), (E/RES/2007/8), (E/RES/2008/3), (E/RES/2009/7).

من النطاق الدولي لحرب سيبرانية فعلية وشددوا على أن عواقبها ستكون وخيمة وسوف تحدث بشكل مؤكد إذا لم يتم تدارك الأمر. ومن ثم لابد أن يكون هناك استجابة فعالة رادعة ومنسقة بين الدول، فلم تعد تكفي استراتيجيات اعتماد حلول على أساس مخصص او تقوية الدفاع فقط[1]. ودعا المجلس الى اتباع نهج قائم على إدراك المخاطر بحيث يحاط ميع أصحاب المصلحة علما بالتهديدات والأضرار الناجمة عن الإرهاب السيبراني والاعتداءات السيبرانية والتدابير الوقائية والردود الفعالة على نحو مناسب، وطالب بإيلاء المزيد من العناية لموضوع الأمن السيبراني وضرورة إرساء ثقافة عالمية أمنية سيبرانية. ودعا الدول الأعضاء الى تقديم موجزات لمبادراتها الرئيسية بشأن الأمن السيبراني وحماية الهياكل الأساسية الحيوية للمعلومات كي يتسنى إبراز ما يتم تحقيقه من الانجازات وأفضل الممارسات في هذا الصدد، وشدد على أن الجهود الوطنية إلزامية في سبيل حماية الهياكل الأساسية الحيوية للمعلومات[2].

وفي نيسان عام 2011 عقد المجلس الاقتصاد والاجتماعي اجتماعا آخرا لمناقشة أمن الفضاء السيبراني والتنمية والقضايا والتحيات المرتبطة. واشترك فيتلك المناقشات إدارة الشؤون الاقتصادية والاجتماعية والاتحاد الدولي للاتصالات ورئيس لجنة الأمم المتحدة المعنية بتسخير العلم والتكنولوجيا لأغراض التنمية ومنظومة الأمم المتحدة والقطاعين العام والخاص إضافة الى منظمات المجتمع المدني المهتمة بمجالات الفضاء السيبراني. وتلخصت أهداف الاجتماع بأنها تتمثل في بناء وعي على مستوى السياسات الدولية عير تزويد أعضاء المجلس بصورة عن الوضع الحالي والتحديات المتعلقة بالأمن السيبراني وارتباطه بالتنمية وتحديد أفضل السياسات المتعلقة بهذا المجال والمبادرات المطبقة في مختلف أنحاء العالم لبناء ثقافة أمن الفضاء السيبراني والردع السيبراني، كما تم مناقشة الحاجة إلى إبرام اتفاقية دولية بشأن الفضاء السيبراني. وقرر **لازاروس كابامبي** رئيس المجلس الاقتصادي والاجتماعي أن أعضاء الاجتماع قد

[1] الأمم المتحدة، المجلس الاقتصادي والاجتماعي، الدورة الموضوعية لعام 2010، نيويورك، 28 حزيران-23تموز، البند: 13 (ب) من جدول الأعمال المؤقت والخاص بالمسائل الاقتصادية والبيئية: تسخير العلم والتكنولوجيا لأغراض التنمية والتقدم المحرز في تنفيذ ومتابعة نتائج مؤتمر القمة العالمي لمجتمع المعلومات على الصعيدين الدولي والإقليمي.

[2] المرجع السابق، البند:14 (ب) من جدول الأعمال المؤقت والخاص بمسائل الأوراق المالية الرقمية والنظام النقدي الرقمي.

اتفقوا على أن الأمن السيبراني قضية عالمية لا يمكن حلها إلا عبر شراكة عالمية ولا سيما من خلال الأمم المتحدة التي يمكنها استخدام قدراتها الاستراتيجية والتحليلية لمعالجة مثل هذه القضايا المستحدثة على الساحة الدولية[1].

المطلب الثاني: آليات المنظمات الإقليمية والوكالات العالمية المتخصصة والمجهودات الفقهية الدولية لردع الهجمات السيبرانية.

مع ظهور الهجمات السيبرانية كنمط جديد من الاستراتيجيات العسكرية الحديثة وما تتميز به من خاصية عابرة للحدود الإقليمية للدول وفي ضوء غياب توجه رسمي دولي موحد ولضعف الاستجابة الأممية الفعالة نحو تنظيم هذا الموضوع. وفي محاولة لمعالجة القصور التشريعي الدولي الذي يحيط بمسألة التعامل مع تلك الهجمات ولتحقيق قدر من الأمن في مجال المعاملات الإلكترونية[2]، عملت العديد من المنظمات الإقليمية والوكالات العالمية المتخصصة وبعض التحالفات الدولية البارزة باستمرار لمواكبة التطورات المتسارعة في شأن أمن الفضاء السيبراني وأسست مجموعات عمل ومبادرات ووضعت اتفاقيات لإرساء استراتيجيات ردع مضادة للاعتداءات السيبرانية الخبيثة وجرائم الإنترنت وحرب المعلومات. ووضع السياسات العامة والتدابير الأمنية والمبادئ التوجيهية وطرق إدارة المخاطر والحماية والتدريب. بالإضافة إلى مجموعة من المساهمات والمجهودات الفقهية الدولية والمرتبطة في هذا الشأن.

الفرع الأول: دور المنظمات الإقليمية.

لا شك في أن مسألة مواجهة الهجمات السيبرانية ينبغي ألا تقتصر على الجانب الدولي فقط بل يجب أن تعتمد على بعد إقليمي أيضا، لذلك كان من الضروري بناء آليات وبذل جهود إقليمية حثيثة إلى جانب الجهود الدولية المبذولة في سبيل ردع تلك الهجمات والحد من آثارها وتداعياتها. وفي هذا الصدد نشير إلى آليات أهم المنظمات الإقليمية **كجامعة الدول العربية والاتحاد الإفريقي.**

أولا: الرؤية الاستراتيجية العربية المشتركة للأمن السيبراني.

[1] الأمم المتحدة، المجلس الاقتصادي والاجتماعي، تقرير فريق الخبراء الحكومي الدولي المفتوح العضوية عن الدراسة الشاملة لمشكلة الهجمات السيبرانية وتدابير التصدي لها من جانب الدول الأعضاء والمجتمع الدولي والقطاع الخاص، فيينا، 11-15 نيسان، الوثيقة: E/CN.15/2011/19

[2] هاني محمد خليل العزازي، النظام القانوني الدولي لمكافحة المخاطر السيبرانية، مرجع سابق، ص512.

شهد موضوع أمن البيانات والمعلومات تطورات هامة على الصعيد العربي مؤخرا، حيث تم تشكيل فريق عمل عربي مشترك خلال الدورة (50) للجنة التنسيق العليا للعمل العربي المشترك في مارس 2021، بهدف وضع إطار قانوني عربي موحد لمواجهة الإرهاب السيبراني والقرصنة الإلكترونية وحماية الشبكات وأمن المعلومات. كما وتمت الدعوة إلى تنظيم منتدى عربي لمناقشة تحديات الأمن السيبراني على أن تشارك فيه كافة الدول الأعضاء ومؤسسات العمل العربي المشترك بشكل فاعل[1]. وردا على ظهور وتنامي العديد من التهديدات والتحديات فيهذا السياق والتي كانت بمعظمها ذات طبيعة عابرة للحدود الجغرافية للدول كالأخبار المزيفة وأخلاقيات الفضاء السيبراني والدبلوماسية السيبرانية والسيادة الرقمية أطلقت النسخة الأولى من الرؤية العربية للأمن السيبراني وقدمت جملة لأهم ما توصل إليه فريق الخبراء المكلف بوضع هذه الرؤية متضمنة الوضع الحالي في الدول العربية ونماذج المخاطر السيبرانية التي تواجهها كما قدمت شرحا لرؤية استراتيجية عربية مشتركة للأمن السيبراني إلى جانب مقترحات حول مسألة الأمن السيبراني في المنطقة العربية وبعض المبادرات التي يمكن تنفيذها[2]. ومن منطلق ضرورة توحيد الجهود على المستوى العربي والإقليمي لمواجهة المخاطر السيبرانية التي تتزايد يوما بعد يوم وتقديم حلول شاملة تخدم الجميع جاءت المنظمة العربية لتكنولوجيا المعلومات والاتصالات استنادا إلى قرار القمة العربية التنموية رقم 56 تاريخ 2019/1/20 للعمل على صياغة الرؤية العربية الموحدة للأمن السيبراني، في إطار المساهمة في تعزيز العمل العربي المشترك ومساعدة الدول العربية على العمل في إطار تكاملي وتشاركي لضمان الازدهار والرقي في المجال الرقمي، على أن تكون بداية لخط استراتيجيات ومبادرات عربية مشتركة في مجال الأمن السيبراني[3]. وتمثلت آليات العمل العربي المشترك في مجال الأمن السيبراني ب:

المصادقة في إطار جامعة الدول العربية على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المؤرخة في 2010/12/21 والتي دخلت حيز التنفيذ في 2014/2/6.وهدفت وفقا لما

[1] الرؤية العربية للأمن السيبراني(الواقع، التحديات، الفرص) جامعة الدول العربية، المنظمة العربية لتكنولوجيات الاتصال والمعلومات، مقتطف من كلمة السفير أحمد أبو الغيط الأمين العام لجامعة الدول العربية، خلال افتتاح اعمال الدورة (51) للجنة التنسيق العليا للعمل العربي المشترك، مصر: مدينة العلمين الجديدة، 2021/7/8.

[2] المرجع السابق، مقتطف من كلمة أحمد البياتي رئيس المجلس التنفيذي لجامعة الدول العربية.

[3] المرجع السابق، مقتطف من كلمة المهندس محمد بن عمر المدير العام للمنظمة العربية لتكنولوجيات الاتصال والمعلومات.

نصت عليه مادتها الأولى إلى مكافحة الجرائم التي تعتمد على تقنيات المعلومات مع وضع إطار قانوني للتحقيق فيها وملاحقة مرتكبيها بالإضافة إلى تعزيز التعاون وتدعيمه بين الدول العربية في مواجهة إساءة استخدام تقنية المعلومات والاعتداءات السيبرانية لدرء أخطارها حفاظا على أمن الدول العربية ومصالحها وسلامتها وسلامة كياناتها وأفرادها[1]، وتضمنت مجموعة من الالتزامات التي تهدف إلى توحيد الاجراءات الخاصة بجرائم تقنية المعلومات والجرائم المرتبطة بالبيئة السيبرانية[2]. إضافة إلى اتخاذ بعض المبادرات التشريعية العربية المشتركة والتي اتخذت شكل القوانين الارشادية سواء في مجال الأمن السيبراني ككل، أو في مجال مكافحة الهجمات السيبرانية، أو فيبعض المجالات الأخرى كالقانون الارشادي للإثبات بالتقنيات الحديثة والقانون الارشادي للمعاملات التجارية والمصرفية الإلكترونية والتوقيع الرقمي. حيث تم وضعها في إطار أشغال المركز العربي للبحوث القانونية والقضائية التابع لجامعة الدول العربية والذي يعمل تحت اشراف وزراء العدل العرب. الذي بدوره أعد مسودة الاتفاقية العربية لحماية الفضاء السيبراني لعام 2018 بمبادرة من مجلس وزراء العدل العرب بجامعة الدول العربية. وأخيرا المبادرة حديثة العهد في إطار أشغال لجنة التنسيق العليا للعمل العربي المشترك في دورتها (50) 2021 والتي تم تقديمها من الأكاديمية العربية للعلوم والتكنولوجيا والنقل البحري والمنظمة العربية لتكنولوجيا الاتصال والمعلومات، والتي يمكن أن تشكل الإطار القانوني الجديد لمواجهة الإرهاب السيبراني والقرصنة الإلكترونية وحماية الشبكات وأمن المعلومات لمؤسسات ومنظمات العمل العربي المشترك[3].

ثانيا: اتفاقية الاتحاد الإفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية.

شهدت القارة الإفريقية موجة من الهجمات السيبرانية والتي استهدفت أنظمة مفوضية الاتحاد الإفريقي وأنظمة بيانات الحكومة الكينية والبنية التحتية للانتخابات النيجيرية وغيرها. ويبدو أن هذه الهجمات كانت بمثابة جرس إنذار للقارة، مما دفع مجلس السلام والأن التابع للاتحاد الإفريقي إلى جعل الأمن السيبراني نقطة رئيسية على جدول الأعمال في القمة الأعمال في القمة الإفريقية التي

[1] المادة الأولى من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010.

[2] الرؤية العربية للأمن السيبراني(الواقع والفرص والتحديات) جامعة الدول العربية، المنظمة العربية لتكنولوجيات الاتصال والمعلومات، تونس، مرجع سابق 2021/10/21، ص15.

[3] الرؤية العربية للأمن السيبراني(الواقع والفرص والتحديات) جامعة الدول العربية، المنظمة العربية لتكنولوجيات الاتصال والمعلومات، تونس، 2021/10/21،مرجع السابق، ص16.

عقدت مؤخرا في أديس أبابا، كما تم اعتماد سياسة قارية لحماية الأطفال على شبكة الإنترنت، وتم الاتفاق على موقف إفريقي مشترك خلال القمة بشأن تطبيق القانون الدولي في الفضاء السيبراني[1]. كما سبق وأن أنشأ الاتحاد الإفريقي استراتيجية التحول الرقمي لإفريقيا في شباط2020. إلا أن الآلية الأبرز تمثلت باتفاقية الاتحاد الإفريقي بشأن الأمن السيبراني وحماية البيانات ذات الطابع الشخصي أو ما تعرف اختصارا باتفاقية مالابو والتي تضمنت 38 مادة.

طرح المشروع الأولي للاتفاقية عام 2013،وكان معنونا باتفاقية الاتحاد الإفريقي حول الثقة والأمان في الفضاء السيبراني وكان نتاج تعاون بين مفوضية الاتحاد الإفريقي ولجنة الأمم المتحدة الاقتصادية لإفريقيا (CEA)وبالفعل اعتمده رؤساء الدول والحكومات المجتمعين في مالابو بغينيا الاستوائية خلال الدورة العامة رقم 23 لمؤتمر الاتحاد الإفريقي يومي 26-27 حزيران 2014. وعليه أصبح المشروع اتفاقية إقليمية مفتوحة للمصادقة عليها مع تعديل تسميتها لتصبح "اتفاقية الاتحاد الإفريقي حول الأمن السيبراني وحماية البيانات ذات الطابع الشخصي"[2].

صورت اتفاقية مالابو إفريقيا على أنها قارة مستعدة لمعالجة الأمن السيبراني من خلال اجراءات جادة وموحدة وجعلتها المنطقة الوحيدة في العالم التي لديها اتفاق قاري يجمع بين الأمن السيبراني وأمن المعلومات وأن المعاملات الإلكترونية وحماية البيانات الشخصية في معاهدة واحدة. وعلى الرغم من تلك الأهمية إلا أنها لم تدخل حيز التنفيذ حتى 2014/6/2 بسبب التأخيرات في التصديق عليها من قبل الدول الأعضاء في الاتحاد الإفريقي حيث لم يصادق عليها حتى الآن سوى 15 دولة من أصل الدول 55 الأعضاء، ولا تزال غير موقعة من قبل معظم الدول الإفريقية الكبرى بما فيذلك مصر والجزائر وجنوب إفريقيا وكينيا والمغرب وأثيوبيا[3].

الفرع الثاني: دور الوكالات العالمية المتخصصة والتحالفات الدولية.

لعب الاتحاد الدولي للاتصالات بوصفه أحد الوكالات العالمية المتخصصة في شأن البيئة الرقمية وتكنولوجيا الاتصالات والمعلومات وحماية الأمن السيبراني دورا محوريا وهاما في مواجهة

[1] الاتحاد الإفريقي، اللجنة الفنية المتخصصة للاتصال وتكنولوجيا المعلومات والاتصالات، تقرير اجتماع الخبراء، أديس أبابا، أثيوبيا، 20-22 تشرين الثاني 2017، الوثيقة: .AV/CCICT-2/EXP/RPT

[2] مريم لوكال، قراءة في اتفاقية الاتحاد الإفريقي حول الأمن السيبراني وحماية المعطيات ذات الطابع الشخصي لعام 2014، مجلة الدراسات القانونية والاقتصادية المجلد 4، العدد3، 2021، ص660.

[3] المرجع السابق، ص670.

الاعتداءات السيبرانية الخبيثة على المستوى الدولي، كما لا يمكن إغفال دور حلف شمال الأطلسي في هذا الصدد والذي يعد أبرز التحالفات الدولية حيث كان من السباقين في تبني استراتيجية جديدة للأمن والدفاع السيبراني.

أولا: الاتحاد الدولي للاتصالات.

يوصف الاتحاد الدولي للاتصالات (ITU) بأنه أحد الوكالات المتخصصة في عمل الاتصالات والمنضوية تحت لواء الأمم المتحدة، وأصبح بمثابة ملتقى دولي رئيسي لهذه الأنشطة. ويتكون من 192 دولة و700 شركة من القطاع الخاص والمؤسسات الأكاديمية ويعتبر منبرا استراتيجيا للتعاون بين أعضاءه ويعمل على مساعدة الحكومات في الاتفاق على مبادئ مشتركة تفيدها والانفاق على الصناعات التي تعتمد على تكنولوجيا المعلومات والبنية التحتية للاتصالات[1]. وبغية معالجة مسألة الأمن السيبراني المتنامية قام الاتحاد بإنشاء فريق متخصص معني بالشبكات الذكية من أجل جمع وتوفير المعلومات والمفاهيم التي تكون مفيدة بهدف إعداد توصيات لدعم تلك الشبكات من منظور الاتصالات. وكان أحد الأدوار الرئيسية التي أنيطت بالاتحاد في أعقاب القمة العالمية لمجتمع المعلومات ومؤتمر المندوبين المفوضين لعام 2006 يتمثل في بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات. وإثر قيام رؤساء الدول والحكومات وقادة العالم المشاركين في القمة العالمية لمجتمع المعلومات وكذلك الدول الأعضاء في الاتحاد بتكليف الأخير باتخاذ خطوات ملموسة للحد من التهديدات وانعدام الأمن فيما يتصل بمجتمع المعلومات، وأطلق "**حمدون توريه**" الأمين العام للاتحاد الدولي للاتصالات برنامج الأمن السيبراني العالمي في2007 ليشكل إطارا للتعاون الدولي. وهكذا أعلن الأمين العام للاتحاد الدولي للاتصالات اطلاق مبادرة أجندة شاملة للأمن السيبراني تتضمن التوصل إلى إطار أو بروتوكول لتنسيق جهود مواجهة الهجمات السيبرانية. حيث اشتملت على خمس ركائز ومجالات واستراتيجيات عمل وهي: التدابير القانونية، التدابير التقنية والاجرائية، الهياكل التنظيمية، بناء القدرات وتعزيز التعاون الدولي[2]. وادراكا منه للمخاطر والتهديدات المتنامية للهجمات السيبرانية اقترح الأمين العام للاتحاد الدولي للاتصالات

[1] هاني محمد خليل العزازي، النظام القانوني الدولي لمكافحة الأخطار السيبرانية، مرجع سابق، ص512.

[2] United Nation, The International Telecommunication Union, Strategy for cyber security Geneva, 2008, op,cit.

مجموعة من القيم الجوهرية التي من شأنها إحلال السلام والاستقرار في الفضاء السيبراني مع تحديد التزامات واجراءات محددة، وتنص هذه المبادئ على ما يلي:[1]

1- أن تلتزم كل حكومة بإتاحة نفاذ شعبها على الاتصالات.
2- أن تلتزم كل حكومة بتأمين الحماية لشعبها في الفضاء السيبراني.
3- أن يلتزم كل بلد لعدم إيواء الإرهابيين والمجرمين السيبرانيين على أراضيه.
4- أن يلتزم كل بلد بألا يكون الطرف الذي يبدأ شن هجوم سيبراني على غيره من البلدان.
5- أن يلتزم كل بلد بالتعاون مع غيره ضمن إطار دولي للتعاون لضمان السلام والاستقرار في الفضاء السيبراني.

وبالتعاون مع الاتحاد الدولي للاتصالات عقد في دولة قطر عام2008 المؤتمر الإقليمي حول الأمن السيبراني حيث تمت دعوة دول المنطقة لوضع وتنفيذ إطار وطني للأمن السيبراني وحماية البنية التحتية الحرجة للمعلومات والتي تعد بمثابة خطوة أولى في سبيل التصدي للتحديات التي تواجهها عند إساءة استخدام تكنولوجيا المعلومات والاتصالات. وأخيرا قام الاتحاد الدولي للاتصالات بتوقيع مذكرة تفاهم رسمية عام 2008 مع الشراكة الدولية المتعددة الأطراف لمكافحة التهديدات السيبرانية "إمباكت" (IMPACT) وعلى إثر ذلك أصبحت "سايبرجايا" بماليزيا والتي تضم أحدث ما توصلت إليه التكنولوجيا المقر الفعلي لبرامج شركة إمباكت[2].

ثانيا: استراتيجية حلف شمال الأطلسي للأمن والدفاع السيبراني.

دفع عجز حلف شمال الأطلسي (NATO) في مواجهة الهجمات السيبرانية التي استهدفت استونيا 2007 ثم جورجيا 2008 إلى تكوين وحدة للدفاع السيبراني مقرها مدينة تالين عاصمة استونيا. ومن حينها عمد الحلف الى تطوير المفهوم العسكري الاستراتيجي الخاص به بالاعتماد على تطوير قدراته الدفاعية السيبرانية بما يشمل مساندة ودعم حلفائه الذين يتعرضون لهجمات سيبرانية،

[1] الأمم المتحدة، الاتحاد الدولي للاتصالات، قرارات المؤتمر العالمي لتنمية الاتصالات عام 2017 المرفوعة إلى مؤتمر المندوبين المفوضين(17wtdc), مؤتمر المندوبين المفوضين (18pp) ، دبي 29 تشرين الأول-16 تشرين الثاني 2018.

[2] United Nation, The International Telecommunication Union, Strategy for cyber security Geneva, 2008, op,cit.

وأقر وفقا لذلك بأن أي هجوم يتم على أوروبا وأمريكا الشمالية سيعد هجوما ضد الجميع[1]. وتبنى الحلف السياسة الخاصة به في مجال الدفاع السيبراني عام 2008 من أجل حماية موارده التكنولوجية والموارد الخاصة بالدول الأعضاء، وكجزء من تنفيذ هذه السياسة أنشأ الحلف هيئة معنية بإدارة الدفاع السيبراني وفريقا للاستجابة للحوادث الحاسوبية ويكفل ارسال فرق الدعم السريع الى الدول الأعضاء، وأنشأ مركزا للتميز من أجل الدفاع السيبراني التعاوني ومقره استونيا، ويضم خبراء يضطلعون في البحث والتدريب والمتابعة والحماية في مال الأمن السيبراني، ومن الدول الأطلسية التي دعمت هذا المركز ورعته: استونيا، لاتفيا، ليتوانيا، ألمانيا، إيطاليا، اسبانيا وسلوفاكيا[2]. وفي العام 2010 تبنى حلف الناتو المفهوم الاستراتيجي الجديد والذي أشار إلى أن التهديدات السيبرانية أصبحت أكثر تواترا وتنظيما وأكثر تكلفة من حيث الضرر الذي يمكن أن تتسبب به ، حيث يمكن أن تصل إلى درجة تهديد القومية الأوروبية الأطلسية وأمنها واستقرارها، وإثر ذلك تم تغيير العقيدة العسكرية للحلف لتتلاءم مع المتغير المستحدث، ولتشمل وتغطي "الحرب في الفضاء السيبراني[3]. وفي قمة وارسو في بولندا لعام 2016 وافق وزراء دفاع دول الحلف على ترقية الفضاء السيبراني الى المجال التشغيلي وجعله منطقة لعمليات الحلف الامر الذي منحه نفس أهمية البر والبحر والجو. وقد اعتبر الأمين العام لحلف شمال الأطلسي "نيس ستولتنبورغ" الفضاء السيبراني جزء من منظومة الدفاع الجماعي للحلف[4].

الفرع الثالث: دور المجهودات الفقهية الدولية.

ظهرت العديد من المجهودات والمساهمات الفقهية على المستوى الدولي بهدف معالجة مسألة الهجمات السيبرانية ومواجهتها في ظل إشكالية القصور التشريعي والفراغ القانوني التي تحيط بها. وتمثلت الاستجابة الأهم والأبرز في هذا الإطار "بدليل تالين" للقانون الدولي المطبق على الحرب السيبرانية والذي قام بإعداده مجموعة من أبرز فقهاء القانون الدولي، بالإضافة إلى "إعلان

[1] هاني محمد خليل العزازي، النظام القانوني لمكافحة المخاطر السيبرانية، مرجع سابق، ص517.

[2] رغدة البهي، كيف استجاب حلف شمال الأطلسي للدفاع السيبراني؟ كراسات استراتيجية، مركز الأهرام للدراسات السياسية والاستراتيجية، العدد 334، المجلد 31، 2022، ص27.

[1] NATO, Active Engagment, Modern Defence, Strategy concept for the defecce and security for the members of the north atlantic treaty organization, November 2010.

[2] North Atlantic treaty organization, NATO, strategy for cyber defence, Warsaw, 2016.

[3] هاني محمد خليل العزازي، النظام القانوني الدولي لمكافحة المخاطر السيبرانية، مرجع سابق، ص 518.

إيريتشي" بشأن مبادئ الاستقرار والسلام السيبراني والذي أعده فريق الرصد الدائم المعني بأمن المعلومات التابع للاتحاد العالمي للعلماء[1].

أولا: دليل تالين للقانون الدولي المطبق على الحرب السيبرانية.

يمثل دليل تالين آلية قانونية لملائمة المبادئ الأساسية للقانون الدولي مع الحرب السيبرانية وهو توجه فقهي غير ملزم بشأن القواعد الدولية الحاكمة للعمليات السيبرانية. حيث تقرر قواعد الدليل من حيث المبدأ أن أحكام ميثاق الأمم المتحدة قابلة للتطبيق في البيئة السيبرانية. ويناشد الدول بألا تتعامل مع الفضاء السيبراني على أنه منطقة فراغ قانوني لا تنطبق عليه المبادئ القانونية المعمول بها فيغيره من الفضاءات المادية، ويحث المجتمع الدولي على الاستجابة والاستعداد لردع تلك الهجمات والالتزام بمتطلبات القانون الدولي[2]. استضاف المركز التعاوني للدفاع السيبراني التابع لحلف شمال الأطلسي بمقره في مدينة تالين عاصمة استونيا صياغة هذا الدليل في الفترة الممتدة بين عامي 2009–2017 بجهود فريق خبراء قانونيين دوليين (ICE) برئاسة البروفيسور مايكل شميث ، وانتهى إلى أن القواعد الدولية السارية فاعلة إلى حد كبير ويمكن تطبيقها على الهجمات السيبرانية. كما تعرض إلى الإشكاليات القانونية المثارة في المجال السيبراني كسيادة الدول، وقواعد ممارسة الاختصاص وقانون مسؤولية الدول، إضافة إلى قانون حقوق الإنسان وقانون البحار والقانون الدبلوماسي والقنصلي. وقد انطوى على 154 قاعدة تم تحديثها لأكثر من مرة حسب اقتضاء الحاجة والتطور في المجال السيبراني[3]. لا يعد دليل تالين صكا دوليا رسميا او ملزما، ولا يمكن القول بأنه يمثل وجهة نظر حلف الناتو الرسمية او الدول التي شارك خبراء من جنسيتها في وضعه وإنما يمكن عده من قبيل رؤية الخبراء المستقلين الذين صاغوه بصفاتهم الشخصية الفقهية. ومع ذلك وعلى الرغم من أن القواعد الواردة فيه ذات طبيعة استرشادية غير رسمية ولا ملزمة إلا أنها تتمتع بمكانة هامة بين الدول الأعضاء في الحلف على اعتباره وثيقة رائدة في مجال العمليات السيبرانية وخطوة مهمة بشأن تطوير واعتماد إطار معياري موحد ومتفق عليه[4].

---

[2] ناجي محمد أسامة الشاذلي، الجوانب القانونية للحرب السيبرانية، مرجع سابق، ص1271.

[3] هاني محمد خليل العزازي، النظام القانوني الدولي، مرجع سابق، ص518.

[4] هاني محمد خليل العزازي، النظام القانوني الدولي، مرجع السابق، ص520.

ثانيا: إعلان إيريتشي بشأن مبادئ الاستقرار والسلام السيبراني.

أعد إعلان إيريتشي بشأن مبادئ الاستقرار والسلام السيبراني بواسطة فريق الرصد الدائم المعني بأمن المعلومات التابع للاتحاد العالمي للعلماء (WFS) حيث اعتمدته الجلسة العامة للاتحاد العالمي للعلماء في الدورة الثانية والأربعين للحلقات الدراسية الدولية بشأن الطوارئ العالمية في إيريتشي (صقلية) في 20 آب 2009. وتناول قضايا أمن المعلومات باعتبارها موضوعا من موضوعات الطوارئ الحرجة وبين أن الاستقرار السيبراني والسلام السيبراني أمران متداخلان تداخلا وثيقا، وركز على العناصر التشغيلية الأساسية للسلام السيبراني:[1]

1- ينبغي لجميع الحكومات الاعتراف بأن القانون الدولي يضمن للأفراد التدفق الحر للمعلومات والأفكار وتنطبق هذه الضمانات أيضا على الفضاء السيبراني، وينبغي عدم فرض القيود إلا عند الاقتضاء على أن تخضع لعملية مراجعة قانونية.

2- ينبغي على جميع الدول العمل معا لوضع مدونة مشتركة للسلوك السيبراني وإطار قانوني عالمي منسق بما في ذلك أحكام إجرائية تتعلق بالمساعدة في التحقيق والتعاون بما يكفل احترام الخصوصية وحقوق الإنسان.

3- ينبغي على جميع الحكومات ومزودي الخدمات والمستعملين دعم الجهود المبذولة في سبيل إنفاذ القانون الدول يضد مرتكبي الهجمات السيبرانية.

4- ينبغي للحكومات أن تشارك بفعالية في جهود الأمم المتحدة الرامية الى النهوض بالأمن السيبراني والسلام السيبراني في العالم وان تتفادى استعمال الفضاء السيبراني من أجل النزاعات.

وقد دعا الاتحاد العالمي للعلماء منذ عام 2003 إلى العمل على وضع قانون عالمي للفضاء السيبراني وأنه من الأفضل أن يكون تحت رعاية الأمم المتحدة خاصة في مجال الاستخدامات العدائية العسكرية والخبيثة للفضاء السيبراني[2].

---

[1] إعلان إيريتشي، مبادئ الاستقرار السيبراني والسلام السيبراني، فريق الرصد الدائم لأمن المعلومات، الاتحاد العالمي للعلماء(WFS) جنيف، الجلسة العامة للاتحاد، الدورة الثانية والأربعين، الحلقات الدراسية الدولية للطوارئ العالمية، إريتشي، صقلية، 20 آب، 2009.

[2] تقرير وتوصيات فريق الرصد الدائم المعني بجمع المعلومات التابع لاتحاد العلماء العالمي، 19 نوفمبر 2003، تقرير قدم إلى القمة العالمية لمجتمع المعلومات، سويسرا، جنيف، 2003.

الاستنتاجات والتوصيات:

1-الاستنتاجات:

1- أصبح الفضاء السيبراني جزءا لا يتجزأ من المنظومة الشاملة للمجتمع الدولي وشكل عاملا مهما من عوامل القوة والتأثير في العلاقات الدولية، الأمر الذي خلق حاجة ماسة وضرورة ملحة لتأمينه من الهجمات السيبرانية منعا من عسكرته وتحوله لساحة للصراع الدولي وخوفا من تعرض المصالح الاستراتيجية السيبرانية للأخطار والتهديدات.

2- تمثل الهجمات السيبرانية خطرا حقيقيا على السلم والأمن الدوليين خاصة إذا ما صنفت بأنها واسعة النطاق شديدة الأثر وطويلة الأمد، وذلك لخرقها سيادة الدول الوطنية وإقليمها البري والبحري والجوي وانتهاكها لميثاق الأمم المتحدة وقواعد القانون الدولي الإنساني والقانون الدولي لحقوق الإنسان وغيرها من الانتهاكات الجسيمة التي تشرع تدخل مجلس المن الدولي لمواجهتها لصون السلم والأمن الدوليين.

3- أظهرت التجربة الدولية أن الاتفاق على المعايير والقواعد لا يكفي في حد ذاته لإرساء الأمن السيبراني والحفاظ عليه بل يجب تطوير استراتيجية ديبلوماسية جماعية لمراقبة تنفيذ هذه المعايير وفرض العقوبات عند تجاوزها.

4- يؤخذ على معظم الآليات الدولية والإقليمية المتبعة في مواجهة الهجمات السيبرانية أنها افتقرت إلى القدرة على المساءلة الدولية عن تلك الهجمات وإسنادها إلى الدولة المعتدية وإثارة المسؤولية الدولية القانونية والجنائية والمدنية ضدهم ومعاقبتهم.

5- يشير الواقع الدولي الى أن إمكانية التوصل الى توافق سياسي داخل الأمم المتحدة لمواجهة الأنشطة السيبرانية أمرا محدودا للغاية، وذلك لأن المجتمع الدولي يتحرك فقط عند استخدام القوة وهو أمر غير متوفر في سياق الهجمات السيبرانية حتى الآن.

6- عدم جواز التذرع بمسألة القصور التشريعي بهدف تسهيل واستهداف البنية التحتية الإلكترونية للدول، فبالرغم من أن ميثاق الأمم المتحدة لم ينص صراحة على تحريم الهجمات السيبرانية أو لم يعدها من قبيل استخدام القوة المحظورة إلا أن روح الميثاق ومقاصده يتفقان على تحريم استخدامها بوصفها تمثل انتهاكا لما ورد فيه.

7- القانون الدولي ليس لديه سوى القليل من الآليات والتدابير التي تسمح للدولة بالرد بفعالية على الهجمات السيبرانية مجرد وقوعها مقارنة بالتدابير والاجراءات التي يمكن أن تتخذها في حالة تعرضها لهجوم تقليدي حيث يسمح للدولة حينها باستخدام القوة للدفاع الشرعي عن النفس ضد الدولة المعتدية.

8- إن إطار القانون الدولي الحالي يوفر القليل من الحماية الفعالة للدول ضد هذا النوع من الهجمات المستحدثة، بل وأثبت فشله وعجزه عن تعزيز سبل الحماية المتاحة ففي سياق التدابير الاحترازية المضادة، إن القانون الدولي يسمح باتخاذ فئة واسعة من التدابير المؤقتة التي تهدف إلى حث الدولة على وقف تصرفاتها غير المشروعة بموجب أحكامه في ظروف معينة، ولكن في سياق الهجمات السيبرانية يبقى تفعيل هذه الاجراءات والوسائل محدود الاستخدام والفعالية والنتائج.

2- التوصيات:

1- ضرورة العمل على إيجاد إطار قانوني دولي موحد لحماية الأمن السيبراني وإعداد قائمة من الاجراءات والتدابير المتسقة مع القانون الدولي والمعايير المتفق عليها من أجل حماية الهياكل الأساسية للمعلومات ومنع استهداف البنية التحتية الحيوية والحرجة للدول.

2- ضرورة بناء آليات مساءلة دولية فعالة عن لهجمات السيبرانية واعتبار أي دولة مسؤولة عن الهجمات التي تصدر من أراضيها.

3- ضرورة أن تنتقل جهود كافة المنظمات الدولية والإقليمية في مجال مواجهة الهجمات السيبرانية من مرحلة الشجب والتحذير غير المنتظم بنسق وإطار محدد وبطيء الى مرحلة التأطير القانوني الفعال ووضع الاستراتيجيات الدولية والإقليمية لمواجهة هذا التهديد.

4- التواصل والتنسيق مع خبراء معلوماتيين وتقنيين وتكنولوجيين لإيجاد برمجة معينة تقوم بفصل البنية التحتية والشبكات السيبرانية العسكرية عن المدنية بهدف حماية السكان المدنيين من مخاطر الهجمات السيبرانية.

5- ضرورة التعجيل بالتفاوض على صك دولي بشأن مواجهة الهجمات السيبرانية في إطار الأمم المتحدة يستند إلى القواعد الدولية السارية لاسيما القانون الدولي الإنساني وقواعد دليل تالين والتب تعتبر أكثر ملائمة لهذا المجال.

6- إيجاد منظومة قانونية متخصصة تحت مظلة الأمم المتحدة تهدف إلى توحيد جهود الدول في مواجهة الهجمات السيبرانية ويتفرع منها لجنة أو هيئة محايدة تتولى التحقيق في تلك الهجمات ويكون لها سلطة الأمر بإسنادها الى الدول المعتدية ومن ثم تقرير ترتب مسؤوليتها الدولية القانونية والجنائية والمدنية ومعاقبتها.

References:

Books:

1. Carr, J. Inside cyber warfare: Mapping the cyber under world. OREILLY Media, (2ed), USA, 2012, 314.

2. Khaleefah, E. Post-Information Society: The Impact of The fourth industrial revolution on national security. Future Center for Advanced Research and Studies, Egypt, Cairo: Dar Al- Arabi for publishing and distribution, 2019, 181.

3- AlNnakeeb, A. Electronic War in the light of the seventy-seven protocols attached to the Geneva Conventions for the year forty-nine (Cyber attacks). Egypt, Cairo, the Arab Center for Publishing and Distribution, 2022, 392.

Scientific Theses:

1. ALSharkawy, H, M. Electronic attacks in light of the provisions of international humanitarian law. Doctoral thesis, Egypt, Beni suef University, faculty of law, dpartment of international law, 2021, 419.

2. Ojel, Z. The extent of the legitimacy of war in cyber space according to the rules of international humanitarian law and international conventions. Masters thesis . Syria ,Tishreen University , faculty of law , department of international law, 2022. 142.

3.Riyadh, B, Noor Aldeen, K. Electronic deterrence as a mechanism to confront cyber attacks. Amemorandun submitted to complete the requirements for obtaining a professional masters degree in law, specializing in media an internet law, Algeria, Mohammad Bashir Ebrahimi University, Faculty of law and political science, 2023, 70.

Articals:

1. Schmitt, M. The sixth United Nation GGE and international law in cyber space. Just Security Center on law and security at New York University School of law, 10/6/2021.

2. Lewis, A,J. Creating Accountability for global cyber norms. Center for strategy and international studies (CSIS), 23/2/2022.

Journals:

1.Lockal, M. A reading of the African Union Agreement on cyber security and the protection of personal data for the year 2014. Journal of legal and economic studies, Vol:4, No:3, 2021, 657-673 .

2.AlZobairy, F, International law and electronic attacks without the use of force. International Journal of law, Qatar University press, college of law, Qatar University, Vol:11, No:1, 2022, 227-249.

3. Abd-AlHamaah, M,S. The extent of the United Nation contribution to shaping international rules related to cyber space, A study in light of the report of the international expert group for the year 2021. Journal of the Kufah studies center, Vol:17, No:67, 2022, 325-350.

4.AlBahiy, R. How has NATO responded to cyber defense? Strategic brochures ,Al-Ahram center for political and strategic studies, Vol:31, No:334, 2022,20-35.

5.Al-Azzazy, E,KH,M,H. The international legal system to combat cyber risks. Contemporary Egypt Journal, No:549, 2023, 534-465.

6.AlShazely, O,M,N, The legal aspects of cyber warfare: A study within the framework of international humanitarian law. Spirit of laws Journal, No:103, part two, 2023, 1229-1286.

International Resolutions:

***1.General Assembly**:*

A/RES/63/55/2000.

A/RES/56/121/2001.

A/RES/57/239/2002.

A/RES/66/177/2005.

A/RES/64/21/2010.

A/RES/65/41/2010.

A/RES/66/24/2011.

A/RES/67/27/2012.

2.Security Counsel:

S/RES/2341/2017.

S/RES/2370/2017.

3.ECOSOC:

E/RES/2006/46.

E/RES/2007/8.

E/RES/2008/3.

E/RES/2009/7.

4.United Nation, International Telecommunication Union Resolutions of the world telecommunication development conference 2017.

<u>International Documents, Reports and Conferences:</u>

1.Report and Recommendations of the permanent monitoring group on information collection of the world Union of Scientists to the world summit on the information society, Switzerland, Geneva, November 2003.

2.United Nation ,ECOSOC, 2010 substantive session, New York, 28 June-23July 2010.

3.United Nation ,ECOSOC, Report of the open-ended intergovernment group of experts on the comprehensive study of the problems of cyber attacks, Austeria, Vienna, 11-15 April 2011, Doc: E/CN.15/2011/19.

4.African Union specialized technical committee on communication and ICT, Report of the expert meeting, Addis Ababa, Ethiopia, 20-22 November, 2017,Doc: AU/CCICT-2/EXP/RP.

5.The Arab Vision for Cyber Security, League of Arab states, Arab Organization for communication and information technology, Tunisia, Tunisia, 2021

6.Report of the Intergovernmental Group of Experts on Development in information and telecommunication in the context of international security, 14/7/2021, Doc: A/68/98,15.

International Conventions:

1.Charter of the United Nation 1945.

2.The International Telecommunication Union, Strategy for cyber security 2008.

3.Erice Declaration for cyber peace and stability 2009.

4.The Arab convention to combat information technology crimes 2010.

5. North Atlantic Treaty Organization (NATO), Active Engagment, Modern Defence, Strategy concept for the defence and security of the members of NATO, 2010 .

6.North Atlantic Treaty Organization (NATO), Strategy for cyber defence,2016.