دور أجهزة الأمم المتحدة فى مكافحة القرصنة الإلكترونية

الباحث/ محمود زكريا محمود عبدالعال

باحث ماجستير في القانون الدولى العام- كلية الحقوق- جامعة اسيوط

تحت إشراف

أ.د. عصام محمد أحمد زناتى
أستاذ القانون الدولى العام- كلية الحقوق- جامعة اسيوط

أ.د. معمر رتيب محمد عبد الحافظ
أستاذ القانون الدولى العام- كلية الحقوق- جامعة اسيوط

(ISSN: 2537 - 0758)

دور أجهزة الأمم المتحدة فى مكافحة القرصنة الإلكترونية

الباحث/ محمود زكريا محمود عبد العال

ملخص:

يتناول هذا البحث دراسة دور الأمم المتحدة، كمنظمة دولية جامعة، في مواجهة التهديدات المتصاعدة للقرصنة الإلكترونية، والتي تمثل تحديًا كبيرًا للأمن السيبراني الدولي. وينقسم البحث إلى مبحثين رئيسيين، يسلطان الضوء على جهود الجمعية العامة ومجلس الأمن في وضع الأطر القانونية والسياسية لمكافحة هذا النوع من الجرائم المعقدة والعابرة للحدود.

Abstract:

This research examines the role of the United Nations, as an inclusive international organization, in confronting the growing threat of cybercrime, which represents a major challenge to international cybersecurity. The research is divided into two main sections, highlighting the efforts of the General Assembly and the Security Council in developing legal and political frameworks to combat this complex, transnational crime.

مقدمة

شهد العالم في العقود الأخيرة تحولاً جذرياً بفعل الثورة الرقمية، التي غيّرت أنماط الحياة والاتصال والتفاعل بين الأفراد والدول. ومع هذا التحول، برزت تهديدات جديدة لم تكن مألوفة في النظام القانوني التقليدي، من أبرزها القرصنة الإلكترونية التي باتت تشكل خطرًا حقيقيًا على الأمن الوطني والدولي، وتهدد استقرار المؤسسات، وسلامة البنية التحتية الحيوية، وسيادة الدول.

في ظل الطبيعة العابرة للحدود لهذه الجرائم، عجزت التشريعات الوطنية وحدها عن مواجهتها بفعالية، مما استدعى تدخلاً منظمًا من قبل المجتمع الدولي، وعلى رأسه منظمة الأمم المتحدة، باعتبارها الإطار الأوسع للتعاون الدولي وصون السلم والأمن العالميين. وقد أخذت الأمم المتحدة على عاتقها مناقشة التهديدات السيبرانية من زوايا متعددة، سواء من خلال الجمعية العامة كمنبر تشريعي ومناقشاتي عالمي، أو من خلال مجلس الأمن كجهة مسؤولة عن حفظ السلم الدولي واتخاذ الإجراءات الملزمة.

أهمية البحث:

١. مواكبة التهديدات الحديثة
٢. الفراغ القانونى الدولى
٣. تقييم فعالية الامم المتحدة
٤. تحفيز التعاون الدولى

أهداف البحث:

١. تحليل دور الأمم المتحدة في التصدي لظاهرة القرصنة الإلكترونية، من خلال استعراض جهود كل من الجمعية العامة ومجلس الأمن الدولي.
٢. تسليط الضوء على الأطر القانونية والسياسية التي وضعتها الأمم المتحدة للتعامل مع التهديدات السيبرانية، ومدى كفايتها في مواجهة الجرائم الإلكترونية المعقدة والعابرة للحدود.
٣. بيان التحديات التي تواجه الأمم المتحدة في وضع آليات دولية فعالة لمكافحة القرصنة الإلكترونية، سواء من حيث التباين في المصالح بين الدول أو من حيث غياب تعريفات موحدة ومُلزِمة.
٤. تقييم مدى فعالية التعاون الدولي في إطار المنظمة الأممية لمجابهة القرصنة الإلكترونية وتعزيز الأمن السيبراني العالمي.

إشكالية البحث:

تشكل القرصنة الإلكترونية تحديًا عالميًا متناميًا يهدد الأمن والسلم الدوليين، ويصعب التصدي له من خلال الأطر القانونية التقليدية أو الجهود الوطنية المنفردة. وفي هذا السياق، تبرز الحاجة إلى تقييم دور الأمم المتحدة كمنظمة دولية جامعة، في تنسيق الجهود الدولية لمواجهة هذا التهديد السيبراني الخطير، سواء من خلال الجمعية العامة أو مجلس الأمن الدولي.

منهجية البحث:

يعتمد هذا البحث على المنهج التحليلي الوصفي، الذي يتيح دراسة النصوص القانونية والقرارات الدولية ذات الصلة بدور الأمم المتحدة في مكافحة القرصنة الإلكترونية.

(ISSN: 2537 - 0758)

كما يُستعان بالمنهج المقارن من خلال مقارنة جهود الجمعية العامة ومجلس الأمن، وبيان الفروقات في الصلاحيات والنتائج التي تحققت على أرض الواقع، إضافة إلى استعراض تجارب دولية ذات صلة بالتعاون داخل إطار الأمم المتحدة في المجال السيبراني.

ويعتمد البحث كذلك على تحليل التقارير الرسمية، والاتفاقيات الدولية، وقرارات الأمم المتحدة، إلى جانب الأدبيات القانونية والدراسات الحديثة التي تناولت موضوع القرصنة الإلكترونية من منظور القانون الدولي العام.

الفصل الاول

دور أجهزة الأمم المتحدة فى مكافحة القرصنة الإلكترونية

تمهيد وتقسيم:

شهد العالم فى العقود الأخيرة تطوراً تكنولوجياً متسارعاً أدى إلى نشوء بيئات رقمية جديدة، كان من أبرز تجلياتها تصاعد ظاهرة القرصنة الإلكترونية بمختلف صورها وأشكالها. وقد فرضت هذه الظاهرة تحديات قانونية وأمنية غير مسبوقة على المجتمع الدولى، تطلبت تعاوناً متعدد الأطراف لمواجهتها والحد من أثارها المدمرة على الأفراد والدول والإقتصاد العالمى ككل.

وفى هذا السياق برز أجهزة الامم المتحدة بمختلف تشكيلاتها كفاعل محورى فى التصدي لظاهرة القرصنة الإلكترونية فقد سعت هذه الأجهزة كل بحسب إختصاصه إلى تطوير أطر قانونية وتنظيمية لتعزيز الامن السيبرانى الدولى كما عملت دعم جهود الدول الأعضاء فى بناء قدراتها لمكافحة الجرائم الإلكترونية، وسعت إلى ترسيخ مبادئ التعاون والتنسيق الدولى فى هذا المجال.

والأمم المتحدة هى منظمة دولية حكومية وهى أول نواة لتنظيم عالمى، وتم التوقيع على ميثاق الامم المتحدة فى ٢٦ يوليو ١٩٤٥م، ودخل حيز النفاذ فى ٢٦ أكتوبر ١٩٤٥[١]. منظمة الأمم المتحدة هيئة ذات إرادة مستقلة، تتمتع بشخصية قانونية دولية قامت على اساس اتفاق بين مجموعة من الدول ذات السيادة، وتعتبر العضوية فيها

[١] د. عصام محمد أحمد زناتى: التنظيم الدولى، دار النهضة العربية، ٢٠٠٨م، ص١٣٤

مفتوحة لكل دولة تتمتع بالسيادة، ويبلغ عدد الدول الأعضاء فيها ١٩٢ دولة ومن مبادئها[٢].

- المساواة بين الدول فى السيادة.
- حل النزاعات بالطرق السليمة.
- منع استعمال القوة فى العلاقات الدولية.

وبذلت منظمة الأمم المتحدة جهوداً كبيرة فى سبيل العمل على مكافحة جرائم الإنترنت، وذلك لما تسببه هذه الجرائم من اضرار بالغة، وخسائر فادحة بالإنسانية جمعاء، وإيماناً منها بأن منع هذه الجرائم ومكافحتها يتطلبان إستجابة دولية فى ضوء الطابع والأبعاد الدولية لإساءة استخدام الكمبيوتر والجرائم المتعلقة بهذه الجهود.

أما أهدافها فتتمثل فى حفظ السلام والأمن الدوليتين وتنمية العلاقات الودية بين الدول، وتحقيق التعاون الامنى فى مواجهة الجرائم ذات البعد الدولى، وعلى رأسها الجرائم الإلكترونية بالمصادقة على العديد من الإتفاقيات الدولية ذات الصلة بالموضوع.

ولقد عملت الأمم المتحدة منذ نشأتها على رسم سياسة ناجحة فى مجال منع الجريمة وتحقيق العدالة الجنائية، عبر إقرار العديد من التوصيات، وإنشاء اللجان المتخصصة ومن بينها اللجنة الإستشارية لخبراء منع الجريمة وومعاملة المجرمين الذى عهد إليها مهمة مكافحة الجريمة وتقديم المشورة للأمين العام، وإيجاد البرامج ووضع الخطط ورسم سياسات لتدابير دولية فى مجال منع الجريمة، ومعاملة المجرمين.

ونقسم ذلك الفصل إلى مباحث حيث نتناول بالدراسة والتحليل دور أبرز أجهزة الأمم المتحدة مثل الجمعية العامة ومجلس الأمن فى الحد من مخاطر القرصنة الإلكترونية مع الإشارة إلى أبرز الإتفاقيات والمبادرات ذات الصلة. **وذلك على نحو التالى:**

المبحث الأول: دور الجمعية العامة للأمم المتحدة.

المبحث الثانى: دور مجلس الأمن الدولى فى مكافحة القرصنة الإلكترونية.

---

[٢] أ/ أمجد حسن مرشد الدعجة: استراتيجية مكافحة الجرائم المعلوماتية، رسالة ماجستير، معهد البحوث والدراسات الإستراتيجية جامعة أم درمان الإسلامية السودان ٢٠١٤م، على الموقع http://search.mandumah.com/record/٧٨٩٢٧١

(ISSN: 2537 - 0758)

المبحث الأول
دور الجمعية العامة للأمم المتحدة

تمهيد وتقسيم:

تعد الجمعية العامة للأمم المتحدة أحد الأجهزة الرئيسية فى هيكل منظمة الامم المتحدة، وتشكل منبراً دولياً فريداً يتلقى فيه جميع أعضاء المنظمة لمناقشة القضايا ذات الصلة بالسلم والأمن الدوليين والتنمية، وحقوق الإنسان وغيرها من المسائل ذات الإهتمام المشترك.

ومع تزايد الإعتماد العالمى على التكنولوجيا الرقمية وشبكات المعلومات برزت القرصنة الإلكترونية كواحدة من أخطر التحديات التى تواجه المجتمع الدولى، نظراً لما تمثله من تهديدات للأمن السيبرانى والإستقرار الإقتصادي وحماية الحقوق والحريات الأساسية وفى مواجهة هذه الظاهرة العابرة للحدود كان لابد من تدخل المنظمات الدولية، وعلى رأسها الجمعية العامة للأمم المتحدة باعتبارها الهيئة التى تضم جميع الدول الأعضاء وتعمل على مناقشة وإقرار المبادئ العامة التى تنظم العلاقات الدولة.

وفى هذا المبحث سيتم إستعراض الجهود التى بذلتها الجمعية العامة للأمم المتحدة فى هذا السياق. **وذلك على النحو التالى:**

المطلب الأول: قرار الجمعية العامة فى شأن مكافحة جريمة القرصنة الإلكترونية.

المطلب الثانى: قرار الجمعية العامة للأمم المتحدة بشأن حماية البنية التحتية الأساسية للمعلومات.

المطلب الأول
قرار الجمعية العامة فى شأن مكافحة جريمة القرصنة الإلكترونية

مع تزايد التهديدات السيبرانية التى تستهدف المؤسسة الإقتصادية والأمن القومى للدول، أولت الجمعية العامة للأمم المتحدة اهتماماً متزايداً بمسألة الجرائم الإلكترونية وعلى رأسها جريمة القرصنة الإلكترونية. وبعد إصدار الجمعية العامة للقرار رقم ٧٤/٢٤٧/ A\Res المؤرخ فى ٢٧ ديسمبر ٢٠١٩ أحد ابرز المعالم التشريعية فى هذا الإطار. إذ حتل نقطة إنطلاق نحو بلورة إتفاقية دولية شاملة لمكافحة استخدام تكنولوجيا المعلومات لأغراض إجرامية[٣].

[٣] نورة بنت ناصر بن عبد الله الهزاني، "ضوابط ومتطلبات تطبيق الأمن السيبراني لحماية البيانات". مجلة مكتبة الملك فهد الوطنية، العدد ٢٨، ذو الحجة ١٤٤٤هـ/يوليو ٢٠٢٣م، ص. ٦٤.

أولاً: **خلفية القرار ودوافعه**:

وجاء القرار نتيجة نقاشات دولية مطولة، عبرت خلالها الدول الأعضاء عند قلقها إزاء تصاعد الجريمة الإلكترونية بما فى ذلك القرصنة والتهديدات التى تشكلها على سيادة الدول وأمن الأفراد، وقد اعتبر هذا القرار استجابة مباشرة لنداءات متكررة من بعض الدول وعلى رأسها الإتحاد الروسي والصين التى دعت إلى إعتماد صك قانونى دولى جديد يعالج الفجوات القائمة فى الإتفاقيات الإقليمية وفى مقدمتها إتفاقية بودابست لعام ٢٠٠١.

ثانياً: **مضمون القرار وأهدافه**:

ينص القرار على إنشاء لجنة خبراء حكومية دولية مفتوحة العضوية تتولى وضع مشروع إتفاقية شاملة بشأن مكافحة إستخدام تكنولوجيا المعلومات والإتصالات لأغراض إجرامية. وقد حدد القرار عدد من المبادئ التى ينبغى أن تدعى فى أعمال اللجنة من **أبرزها**:

- احترام سيادة الدولة وعدم التدخل فى شئونها الداخلية.
- مراعاة التوازن بين مكافحة الجريمة وحماية حقوق الإنسان، خاصة الحق فى الخصوصية وحرية التعبير.
- ضمان مشاركة كافة الدول الأعضاء على قدم المساواة فى المفاوضات[٤].

ثالثاً: **الإنقسام الدولى حول القرار**:

لم يحظ القرار بالإجماع، بل عكس حالة من الإنقسام بين الدول الغربية والدول النامية. فقد أعربت عدة دول أوروبية عن تحفظها، مشيرة إلى وجود اتفاقيات قائمة بالفعل مثل إتفاقية بودابست، ورأت أن الحل لا يمكن فى إعداد صك جديد، بل فى توسيع الإنضمام للإتفاقيات القائمة وتعزيز التعاون الدولى فى إطارها. بالمقابل رأت دول اخرى أن الإتفاقيات الحالية تعانى من قصور جوهري، ولا تعكس مصالح وأولويات جميع الدول خاصة تلك التى لم تكن طرف فى إعدادها.

---

[٤] د. عبد الفتاح بيومى حجازى: الإثبات الجنائي فى جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، ٢٠٠٧، ص٣٤١

(ISSN: 2537 - 0758)

رابعاً: الأثر القانونى والسياسي للقرار:

على الرغم من الطابع غير الملزم لقرارات الجمعية العامة إلا أن قرار ٤٧/٢٤٧ A\RES يعد خطوة ذات دلالة قانونية وسياسية، كونه يشير إلى توافق عدد كبير من الدول على الحاجة لصك دولى شامل فى مجال الجريمة الإلكترونية. كما أدى القرار إلى انطلاق مفاوضات دولية فعلية فى إطار اللجنة المحدثة، والتى عقدت عدة دورات لنماقشة أبعاد الإتفاقية المقترحة، بما فى ذلك تعريف الجريمة الإلكترونية وأدوات التعاون الدولى، والضمانات الحقوقية.

وتجدر الإشارة تعمل الأمم المتحدة منذ فترة طويلة فى مجال تأمين سلامة استخدام التكنولوجيا وشبكات المعلوماتية (الإنترنت) وتشارك وكالات الأمم المتحدة المختلفة فى مختلف المفاوضات لإيجاد توافق فى الآراء بشأن عدد من القضايا، بما فى ذلك وضع معايير توفير الحماية لشبكات الإنترنت[٥].

أما أبرز قرارات الجمعية العامة للأمم المتحدة فى هذا المجال فهى:

- القرار ١٢١/٤٥ عام ١٩٩٠، وكذلك نشر دليل منع الجرائم المتصلة بأجهزة الكمبيوتر ومكافجتها فى العام ١٩٩٤.
- القرار ٧٠/ ٥٣ فى ٤ ديسمبر ١٩٩٨، القرار ٥٤/ ٤٩ فى ١ ديسمبر ١٩٩٩.
- القرار ٥٥/٢٨ فى ٢٠ نوفمبر ٢٠٠٠، القرار ١٩/٥٦ فى ٢٩ نوفمبر ٢٠٠١.
- القرار ٥٣/٥٧ فى ٢٢ نوفمبر ٢٠٠٢، القرار ٣٢/٥٨ فى ١٨ ديسمبر ٢٠٠٣ حول موضوع "التطورات فى ميدان المعلومات والإتصالات فى سياق الأمن الدولى".
- القرار ٥٥/٦٣ فى ٤ ديسمبر ٢٠٠٠، القرار ١٢/٥٦ فى ١٩ ديسمبر ٢٠٠١ بشأن "مكافحة استخدام نظم المعلومات الإدارية الجنائية لتقنية المعلومات" ويدعو هذا القرار الدول الأعضاء عند وضع التشريعات الوطنية

لمكافحة إساءة استعمل تكنولوجيا المعلومات على أن تأخذ فى الإعتبار عمل لجنة منع الجريمة والعدالة الجنائية.

---

[٥] د. سامى على حامد عياد: الجريمة المعلوماتية وإجرام الإنترنت، دار الفكر الجامعى، الإسكندرية، ٢٠٠٧م، ص٣١٢

- قرار الجمعية العامة ٥٧/ ٢٣٩ فى ٣١ يناير ٢٠٠٣، القرار ١٩٩/٥٨ فى ٣٠ يناير ٢٠٠٤ بشأن "إنشاء تفاقية عالمية للأمن السيبرانى" والذى يدعو الدول الأعضاء إلى التعاون وتعزيز ثقافة الأمن السيبرانى.

تدعو الجمعية العامة فى قراراتها المختلفة والتى غالباً ما تكون مماثلة لقرارات الإتحاد الدولى للإتصالات الدول الأعضاء، عند وضع القوانين الوطنية والسياسات العامة لمكافحة إساءة استعمال تكنولوجيا المعلومات، وأن تأخذ فى الإعتبار أعمال لجنة منع الجريمة ولجنة العدالة الجنائية وغيرها من المنظمات الدولية والإقليمية[٦].

وقد عقدت كذلك منظمة الأمم المتحدة المؤتمر الثانى عشر لمنع الجريمة والعدالة فى الفترة من ١٢-١٩ أبريل ٢٠١٠، حيث ناقشت فيه الدول الأعضاء بلجنة منع الجريمة والعدالة الجنائية وذلك بالبرازيل مختلف التطورات الأخيرة فى استخدام العلم والتكنولوجيا من جانب المجرمين والسلطات المختصة فى مكافحة الجريمة بما فى ذلك الجرائم الحاسوبية، حيث جانب المجرمين والسلطات المختصة فى مكافحة الجريمة بما فى ذلك الحاسوبية، حيث إحتل هذا النوع من الجرائم موقعاً بارزاً فى جدول أعمال مؤتمر وذلك تأكيداً على خطورتها والتحديات التى تطرحها.

وقد دعت لجنة منع الجريمة والعدالة الجنائية إلى عقد إجتماع لفريق من خبراء حكومى دولى مفتوح العضوية من أجل دراسة شاملة لمشكلة الجريمة السيبرانية وتدابير التصدى لها، ولقد ركز فريق الخبراء دراسته لهذا الموضوع على ظاهرة الجريمة السيبرانية بالتطرق إلى بعض المواضيع ومنها تحليل ظاهرة الجريمة السيبرانية، جمع المعلومات والإحصائيات المتعلقة بالجريمة السيبرانية، تحديات الجريمة السيبرانية، مدى موائمة التشريعات للظاهرة الإجرامية السيبرانية، النص على الجرائم السيبرانية، إجراءات التحقيق، التعاون الدولى، الادلة الإلكترونية، مسئولية متعهدي خدمات الإنترنت، التصدي للجريمة خارج دائرة التدابير القانونية، المساعدة التقنية الدولية، دور القطاع الخاص فى الحد من الجرمية.

---

[٦] د. جورد لبكي: المعاهدات الدولية للإنترنت: حقائق وتحديات عبر الرابط: http://groups.google.com/forum/#!topic/fayad61/pdldgy0xjm. تاريخ الزيارة ٢٠٢٥/٤/٢٠.

(ISSN: 2537 - 0758)

المطلب الثانى
قرار الجمعية العامة للأمم المتحدة بشأن حماية البنية التحتية الأساسية للمعلومات

فى إطار جهود تعزيز الأمن السيبرانى الدولى أصدرت الجمعية العامة للأمم المتحدة القرار رقم A/RES /٥٨/١٩٩ بتاريخ ٢٣ ديسمبر ٢٠٠٣ بعنوان "تعزيز امن البنية التحتية الحيوية للمعلومات" وينص القرار على عدة مبادئ رئيسية، **أهمها:**

أولاً: الإعتراف بأهمية حماية البنية التحتية الحيوية للمعلومات كجزء لا يتجزأ من حماية الأمن الوطنى والدولى.

ثانياً: تشجيع الدول الأعضاء على اتخاذ التدابير اللازمة لتأمين شبكات المعلومات والإتصالات الأساسية لديها.

ثالثاً: دعوة الدول إلى تعزيز التعاون الدولى وتبادل المعلومات حول التهديدات الإلكترونية وأساليب الحماية.

رابعاً: الإشارة إلى الحاجة إلى تطوير القدرات الوزطنية لمكافحة التهديدات الإلكترونية عبر التدريب والتوعية وتعزيز التشريعات الداخلية.

خامساً: التأكد على إحترام مبادئ القانون الدولى وحقوق الإنسان وخاصة حماية الخصوصية وحرية التعبير أثناء وضع تدابير الحماية.

ويتمثل هذا القرار إعترافاً دولياً رسمياً بخطورة التهديدات السيبرانية، ويؤسس لنهج عالمى جماعى للتعامل مع الجرائم والهجمات الإلكترونية وقد شجع القرار العديد من الدول على صياغة استراتيجيات وطنية للأمن السيبرانى كما ساهم فى ظهور مبادرات دولية لاحقة مثل[٧]:

- تقرير الفريق الحكومى الدولى المعنى بالتطورات فى ميدان المعلومات والإتصالات فى سياق الأمن الدولى (GGE).
- مبادرة الأمم المتحدة لتعزيز السلم والأمن السيبرانى.

ولقد اتخذ المجلس الإقتصادي والإجتماعى التابع للأمم المتحدة توصية بأن تأخذ المنظمة الدولية على عاتقها دوراً رئيسياً فى رسم سياسة منع الجريمة وتحقيق العدالة الجنائية الدولية، وقد تحقق ذلك بموافقة الجمعية العامة للأمم المتحدة فى عام ١٩٥٠

[٧] د. عمر عباس خضير العبيدي: مرجع سابق، ص١٣٨

على التوصية التى بموجبها تم إنشاء اللجنة الإستشارية لخبراء منع الجريمة ومعاملة المجرمين التى يقع على عاتقها مهمة مكافحة الجريمة وتقديم المشورة للأمين العام وإيجاد البرامج ووضع الخطط ورسم سياسات لتدابير دولية فى مجال منع الجريمة ومعاملة المجرمين. وبعد إنعقاد مؤتمر الأمم المتحدة لمنع الجريمة ومعاملة المجرمين فى كيوتو باليابان عام ١٩٧٠، تم استبدال اللجنة الإستشارية بلجنة منع الجريمة ومكافحتها بناء على توصية للمجلس الإقتصادي والإجتماعى عام ١٩٧١.

والذى يعنينا فى هذه الدراسة هو جهود الأمم المتحدة من خلال مؤتمراتها الخاصة بنمع الجريمة ومعاملة المجرمين المتعلقة بالجرائم التقنية أو جرائم الحاسب الآلى وهنا نشير إلى أن مؤتمر الامم المتحدة السابع لمنع الجريمة ومعاملة المجرمين الذى تم انعقاده فى مدينة ميلانو بإيطاليا فى العام ١٩٨٥م.

قد انبثقت عنه مجموعة من القواعد التوجيهية والتى اكتملت صياغتها فى الأبحاث الإقليمية التحضيرية للمؤتمر الثامن الذى أجاز هذه المبادئ والذى عقد فى هافانا بكوبا فى العام ١٩٩٠.

حيث أكد المؤتمر على وجوب تطبيق التطورات الجديدة فى مجال العلم والتكنولوجيا بما أنها قد تولد أشكالاً جديدة من الجرائم فإنه ينبغى اتخاذ تدابير ملائمة ضد حالات إساءة الإستعمال لصور التكنولوجيا الحديثة، ويمكن إجمال توصيات مؤتمر هافانا للعام ١٩٩٠ وذلك طبقاً للمبادئ التالية[٨]:

١- تحديث القوانينن الجنائية الوطنية بما فى ذلك التدابير المؤسسية.

٢- تحسين أمن الحاسب الآلى والتدابير المنيعة.

٣- اعتماد إجراءات تدريب كافية للموظفين والوكالات المسئولة عن منع الجريمة الإقتصادية والجرائم المتعلقة بالحاسب الآلى والتحرى والإدعاء فيها.

٤- تلقين آداب الحاسب الآلى كجزء من مفردات مقررات الإتصالات واعتماد سياسات تعالج المشكلات المتعلقة بالمجنى عليهم فى تلك الجرائم.

٥- زيادة التعاون الدولى من أجل مكافحة هذه الجرائم.

وتجدر الإشارة أن القرار الأساسي هو ١٩٩/ ٥٨/ A/RES لسنة ٢٠٠٣ لكن يوجد أيضاً قرارات لاحقة للجمعية العامة تتعلق بتوسيع نطاق حماية البنية التحتية المعلوماتية مثل:

---

[٨] د. خالد ممدوح إبراهيم: مرجع سابق، ص٤٠٨

(ISSN: 2537 - 0758)

- القرار (٢٠٠٩) ٢١١/ ٦٤/ A/RES.
- القرار (٢٠١٣) ٦٨/١٦٧/ A/RES بشأن الحق فى الخصوصية فى العصر الرقمى.

يتضح مما سبق ان الجمعية العامة للأمم المتحدة قد أكدت مبكراً خطورة التهديدات التى تواجه البنية التحتية الأساسية للمعلومات فأصدرت قرارات تهدف إلى تعزيز أمن الفضاء السيبرانى على المستوى الدولى ولا شك أن إستمرار التطور التكنولوجي يستلزم تحديث السياسات الدولية بما يواكب المستجدات ويعزز من فاعلية الجهود الجماعية لحماية البنية التحتية المعلوماتية من المخاطر المتزايدة.

المبحث الثانى

دور مجلس الأمن الدولى فى مكافحة القرصنة الإلكترونية

تمهيد وتقسيم:

مع تصاعد وتيرة التهديدات الإلكترونية وتزايد خطورة الهجمات السيبرانية العابرة للحدود برزت الحاجة الملحة إلى تدخل المجتمع الدولى للتصدى لهذه الظاهرة[٩].

ويعد مجلس الأمن الدولى، باعتباره الجهاز الرئيسي المعنى بحفظ السلم والأمن الدوليين أحد اهم الفاعلين الدوليين الذين يقع على عاتقهم مواجهة التحديات التى تفرضها القرصنة الإلكترونية على الأمن الجماعى وقد تعامل المجلس مع الظواهر الإلكترونية باعتبارها تهديداً محتملاً للأمن والسلم العالميين لا سيما فى ضوء استخدامها فى الأعمال العدائية والجرائم المنظمة الإراهابية.

لذلك يتناول هذا المبحث دور مجلس الأمن الدولى فى وضع الأطر القانونية والسياسية اللازمة لمكافحة القرصنة الإلكترونية. مع بيان أهم القرارات والمبادرات التى إعتمدها فى هذا السياق ومدى فعاليته فى معالجة هذه الظاهرة المستجدة على الساحة الدولية. **وعلى هذا الأساس نقسم ذلك المبحث إلى المطلبين التاليين:**

المطلب الأول: قرار مجلس الأمن رقم ٢/٢٩ لسنة ٢٠١٣ بشأن الإرهاب الإلكترونى.

المطلب الثانى: دور مجلس الأمن الدولي في مكافحة القرصنة الإلكترونية.

---

[٩] د. عبد العزيز حسن الحمادى: مرجع سابق، ص٣٥٤

المطلب الأول

قرار مجلس الأمن رقم ٢/٢٩ لسنة ٢٠١٣ بشأن الإرهاب الإلكترونى

فى ظل تزايد إستخدام الفضاء السيبرانى كوسيلة لتنفيذ أنشطة إرهابية، سواء عبر التخطيط أو التمويل أو تنفيذ الهجمات الإلكترونية إتخذ مجلس الأمن الدولى عدة خطوات لمواجهة هذا التهديد المستجد وقد جاء القرار رقم ٢/٢٩ لسنة ٢٠١٣ كجزء من الجهود الدولية الرامية إلى تعزيز مكافحة الإرهاب بما يشمل التهديدات الإلكترونية التى تشكل تحدياً متنامياً للسلم والأمن الدوليين.

ولقد صدر القرار رقم ١/٢٩ بتاريخ ١٧ ديسمبر ٢٠١٣ وتمحور بشكل رئيسي حول[١٠]:

- تعزيز دور لجنة مكافحة الإرهاب CTC ودعم وحدتها التنفيذيية TEO التوسيع ولايتها بحيث تشمل التهديدات الإرهابية المرتبطة بتكنولوجيا المعلومات والإتصالات.
- التأكيد على أهمية التعاون الدولى فى مكافحة إستخدام الإنترنت لأغراض إرهابية.
- حث الدول الأعضاء على اتخاذ التدابير القانونية والعملية اللازمة لمنع الجماعات الإرهابية من استغلال الفضاء السيبرانى لنشر دعايتها أو تجنيد الأفراد أو التخطيط للعمليات الإرهابية.
- دعوة الدول إلى تطور تشريعاتها الوطنية فى مجال مكافحة الجرائم الإلكترونية ذات الطابع الإرهابي بما يتماشي مع إلتزاماتها بموجب القانون الدولة ٢/٢٩.

وتجدر الإشارة إلى ان القرار يمثل نقطة تحول فى تعامل مجلس الأمن مع الفضاء السيبرانى حيث إعترف صراحة بالدور المحورى الذى باتت تلعبه التقنيات الحديثة فى دعم الإرهاب الدولى ولقد وسع من نطاق مكافحة الإرهاب التقليدي ليشمل الإرهاب الإلكترونى بصورة صريحة.

ولقد أرسى أسساً للتعاون بين الدول، وأكد ضرورة تبادل الخبرات والمعلومات حول اساليب التصدي للهجمات الإلكترونية الإرهابية.

---

[١٠] د. طارق إبراهيم الدسوقى: الأمن المعلوماتى، النظام القانونى للحماية المعلوماتية، مرجع سابق، ص٥٩٩

(ISSN: 2537 - 0758)

كما شدد على إحترام الإنسان خاصة فيما يتعلق بحرية التعبير والخصوصية أثناء اتخاذ التدابير لمكافحة الإرهاب عبر الإنترنت.

المطلب الثانى

دور مجلس الأمن الدولي في مكافحة القرصنة الإلكترونية

شهد العالم خلال العقود الأخيرة تطورًا غير مسبوق في تكنولوجيا المعلومات والاتصالات، مما أدى إلى نشوء تحديات أمنية جديدة، من أبرزها القرصنة الإلكترونية أو ما يعرف بالهجمات السيبرانية. فقد أصبحت هذه الظاهرة تهدد الأمن القومي للدول، وتؤثر على استقرار البنى التحتية الحيوية والأنظمة الاقتصادية والمالية، بل وتمتد لتطال العمليات الانتخابية والديمقراطية في بعض البلدان. وفي هذا السياق، برز تساؤل قانوني وسياسي هام حول مدى إمكانية تدخل مجلس الأمن الدولي، بصفته الجهاز المسؤول عن حفظ السلم والأمن الدوليين، لمواجهة هذه التحديات المعاصرة.

في ضوء ذلك، يصبح التساؤل المطروح هو: هل يمكن اعتبار القرصنة الإلكترونية تهديدًا للسلم والأمن الدوليين يستوجب تدخل مجلس الأمن؟

خلال العقود الماضية، توسع مجلس الأمن في تفسير مفهوم "تهديد السلم والأمن الدوليين" ليشمل قضايا لم تكن تُعد تقليديًا من هذا القبيل، مثل الإرهاب الدولي، انتشار الأسلحة النووية، الأوبئة العالمية كفيروس الإيبولا وكوفيد-١٩، بل وحتى التغير المناخي في بعض المناقشات الأخيرة [١١].

في ضوء هذا التوسع، يصبح من المنطقي إدراج القرصنة الإلكترونية ضمن هذه التهديدات، لا سيما وأن بعض الهجمات السيبرانية قد شلت أنظمة حيوية في دول متقدمة، وأثّرت على العلاقات بين الدول، مثلما حدث في الهجوم السيبراني المعروف بـ Stuxnet الذي استهدف منشآت نووية إيرانية، أو الهجمات التي نُسبت إلى روسيا في الانتخابات الأمريكية عام ٢٠١٦.

ورغم إدراك مجلس الأمن لخطورة التهديدات السيبرانية، إلا أن استجابته لا تزال محدودة نسبيًا مقارنة بتهديدات أخرى كالإرهاب. إلا أن هناك بعض الإشارات التي تُعد مؤشرات أولية على اهتمام المجلس بالمسألة السيبرانية، **منها:**

---

[١١] منى عبد العليم، "الحروب السيبرانية كأداة صراع في العلاقات الدولية"، المجلة المصرية للعلوم السياسية، العدد ١١٧، ٢٠٢٢، ص. ٤٥.

١. البيانات الرئاسية والقرارات غير الملزمة: ففي جلسة لمجلس الأمن عام ٢٠١٧، تم التأكيد على أهمية تعزيز التعاون الدولي في مواجهة التهديدات السيبرانية، لا سيما المرتبطة بالجماعات الإرهابية، إلا أن البيان لم يصدر على شكل قرار ملزم[١٢].
٢. ربط الهجمات السيبرانية بالإرهاب: لجأ المجلس إلى إدراج القرصنة الإلكترونية ضمن وسائل تمويل أو تنفيذ العمليات الإرهابية، مما يُمكّنه من التدخل بموجب قرارات سابقة مثل القرار ١٣٧٣ لعام ٢٠٠١، الذي يُلزم الدول بمنع استخدام أراضيها لأي نشاط إرهابي، بما في ذلك الأنشطة الإلكترونية ذات الصلة[١٣].
٣. دعوة الدول إلى سن تشريعات وطنية: في عدة مناسبات، شجع مجلس الأمن الدول على تطوير أنظمتها القانونية الداخلية لمكافحة الجرائم السيبرانية وتبادل المعلومات في هذا الشأن.

ورغم الأهمية المتزايدة للتهديدات السيبرانية، يواجه مجلس الأمن عدة عوائق تحد من فعالية تدخله، **ومنها:**

غياب التوافق الدولي: تتباين مواقف الدول الأعضاء الدائمين في مجلس الأمن بشأن ما يُعد تهديدًا سيبرانيًا، وتختلف رؤاهم حول حرية الإنترنت، السيادة السيبرانية، والمسؤولية الدولية، ما يجعل إصدار قرارات ملزمة بشأن القرصنة الإلكترونية أمرًا صعبًا. فمثلًا، تُعارض روسيا والصين المعايير الغربية في حرية الفضاء الإلكتروني، وتطالب بوضع قواعد تنظم استخدامه وفقًا لمبدأ سيادة الدولة[١٤].

صعوبة تحديد مصدر الهجمات: الطبيعة اللامادية وغير المحددة للفضاء الإلكتروني تعيق إمكانية تحديد المسؤول عن الهجوم، وهو ما يُضعف من إمكانية مساءلة الدول أو الجماعات أمام مجلس الأمن، إذ يتطلب الفصل السابع وجود فاعل واضح ومحدد مسؤول عن التهديد.

انعدام آليات التحقيق الدولية: لا توجد حتى الآن آليات دولية معترف بها للتحقيق في الهجمات السيبرانية وتحديد المسؤولية عنها، كما هو الحال في الجرائم الإرهابية أو النزاعات المسلحة، ما يفتح المجال للاتهامات المتبادلة دون أدلة دامغة.

---

[١٢] بيان رئيس مجلس الأمن حول الإرهاب والفضاء السيبراني، جلسة ٢٨ يونيو ٢٠١٧.

[١٣] قرار مجلس الأمن رقم ١٣٧٣ لعام ٢٠٠١ بشأن مكافحة الإرهاب.

[١٤] أحمد فوزي، "الفضاء الإلكتروني بين السيادة والحرية: قراءة في مواقف القوى الكبرى"، السياسة الدولية، العدد ٢٢٤، ٢٠٢١، ص ٨٩.

(ISSN: 2537 - 0758)

ويمكن لمجلس الأمن اتخاذ عدد من الخطوات لتعزيز دوره في مكافحة القرصنة الإلكترونية:

إصدار قرارات ملزمة:

ينبغي لمجلس الأمن إصدار قرار ملزم يعترف رسميًا بالقرصنة الإلكترونية كتهديد للسلم والأمن الدوليين، وهو ما يفتح الباب لتفعيل آليات الفصل السابع ضد الدول أو الكيانات التي تقوم أو تدعم مثل هذه الهجمات[١٥].

إنشاء لجنة فرعية للتهديدات السيبرانية:

يمكن للمجلس إنشاء لجنة دائمة تُعنى بمتابعة التهديدات الإلكترونية، تضم خبراء تقنيين وقانونيين، مهمتها تقييم المخاطر، والتحقيق في الحوادث الكبرى، ورفع تقارير دورية للمجلس.

دعم المعايير الدولية:

تشجيع الدول الأعضاء على تبني "مدونة قواعد سلوك دولية في الفضاء السيبراني"، ووضع اتفاقية دولية شاملة تحظى بدعم واسع، تُحدّد القواعد التي تحكم السلوك السيبراني، والمسؤولية الدولية المترتبة على مخالفتها.

من بين الوسائل غير القسرية التي اعتمدها مجلس الأمن في معالجة التهديدات السيبرانية، تشجيع الدول على التعاون التقني وتبادل الخبرات في مجال الأمن السيبرانى، وقد وردت إشارات واضحة في تقارير اللجان الفرعية التابعة للمجلس، تؤكد على ضرورة تعزيز بناء القدرات في الدول النامية لمواجهة الاختراقات الإلكترونية، لا سيما في ظل اعتماد البنى التحتية فيها على أنظمة تشغيل قديمة أو ضعيفة الحماية[١٦].

وعلى الرغم من أن هذا التوجه لا يتخذ شكل قرارات ملزمة، إلا أن التنسيق مع وكالات الأمم المتحدة، مثل الاتحاد الدولي للاتصالات (ITU) وبرنامج الأمم المتحدة الإنمائي (UNDP)، يُظهر إمكانية خلق شراكة تكاملية بين مجلس الأمن والأجهزة الأممية التقنية لتعزيز الأمن الرقمي.

---

[١٥] د. عبد الله على سعيد بن ساحوه: العدالة الجنائية مفهومها نظمها وتطبيقات دولة الإمارات العربية المتحدة، مركز بحوث الشرطة الشارقة، الطبعة الأولى، ٢٠١٣م، ص١٧٣

[١٦] المجلس الاقتصادي والاجتماعي، تقرير لجنة العلوم والتكنولوجيا لأغراض التنمية، الأمم المتحدة، ٢٠١٩.

وتجدر الإشارة إلى أنه في السنوات الأخيرة، بدأ مجلس الأمن في دمج موضوع الأمن السيبراني ضمن مناقشاته العامة المتعلقة بحفظ السلم والأمن الدوليين. وقد برز هذا الاتجاه بشكل خاص منذ عام ٢٠١٥، حينما أدرجت الهيئة الفرعية التابعة للجمعية العامة المعنية بتطورات الفضاء المعلوماتي في السياق الأمني تقارير حول التهديدات السيبرانية رفعتها إلى مجلس الأمن عبر الأمانة العامة، وهو ما اعتُبر محاولة أولى لتنسيق المواقف الدولية تجاه استخدامات الفضاء السيبراني للأغراض العدوانية[١٧].

كما انعقدت جلسات غير رسمية داخل مجلس الأمن تحت ما يُعرف بـ"صيغة آريا" (Arria Formula)، وهي لقاءات غير رسمية تُعقد لمناقشة قضايا مهمة لا تحظى بتوافق واسع داخل المجلس. وتم تخصيص بعض هذه الجلسات لموضوع التهديدات الإلكترونية العابرة للحدود، مما يدل على إدراك تدريجي لخطورة الظاهرة وأثرها المتصاعد على استقرار الدول.

وتعد أداة العقوبات هي من أبرز الوسائل التي يمتلكها مجلس الأمن بموجب الفصل السابع من الميثاق. ومع أن المجلس لم يفرض بعد عقوبات صريحة ومباشرة بسبب هجوم إلكتروني بحت، إلا أنه استند إلى نشاطات إلكترونية ضمن سياقات أوسع في بعض قراراته، لا سيما في المسائل المتعلقة بالإرهاب، أو برامج الأسلحة النووية التي تعتمد في تنفيذها على تقنيات القرصنة وجمع المعلومات عبر الهجمات السيبرانية[١٨].

ويُتوقع أن تتطور آليات العقوبات في المستقبل لتشمل الكيانات الحكومية أو الخاصة التي تُثبت التحقيقات الأممية تورطها في عمليات قرصنة ممنهجة تهدد البنى التحتية أو الانتخابات في دول أخرى، وذلك على غرار العقوبات التي تفرضها بعض الدول بشكل أحادي حاليًا، مثل الولايات المتحدة أو الاتحاد الأوروبي.

ويجدر بنا نشير في هذا الصدد إلى أنه في عدد من المناقشات رفيعة المستوى، دعت بعض الدول الأعضاء في مجلس الأمن إلى ضرورة وضع معاهدة دولية ملزمة تنظم استخدام الفضاء السيبراني، تُشبه في أهدافها اتفاقيات حظر الأسلحة النووية أو

---

[١٧] تقرير مجموعة الخبراء الحكومية حول الأمن المعلوماتي، الجمعية العامة للأمم المتحدة، الدورة السبعون، الوثيقة A/٧٠/١٧٤ ٢٠١٥.

[١٨] لجنة العقوبات التابعة لمجلس الأمن بشأن كوريا الشمالية، تقرير عام ٢٠٢٠ حول استخدام الوسائل السيبرانية لتمويل البرنامج النووي.

(ISSN: 2537 - 0758)

البيولوجية. ورغم أن هذه الدعوات لم تثمر بعد عن وثيقة دولية ملزمة، إلا أنها تشير إلى اهتمام حقيقي من قبل المجلس بضرورة ضبط المجال السيبراني ضمن قواعد القانون الدولي الإنساني والقانون الدولي العام[١٩].

كما دعمت بعض الدول، كفرنسا وألمانيا، فكرة "الفضاء السيبراني كمجال مشترك للسلام"، وطرحت مقترحات لتأسيس آلية دولية محايدة للتحقيق في الهجمات السيبرانية، وتحديد المسؤوليات القانونية، بما يُمكّن مجلس الأمن من التحرك بصورة أكثر فاعلية عند وجود تهديد حقيقي.

وأخيراً يمكننا القول أنه في ظل تعاظم التهديدات السيبرانية، بات من الضروري أن يواكب مجلس الأمن التطورات التكنولوجية المتسارعة، وأن يُفعّل أدواته القانونية والدبلوماسية لمكافحة القرصنة الإلكترونية، باعتبارها من أخطر التحديات العابرة للحدود. فالمسؤولية الأخلاقية والقانونية تحتم على المجلس أن لا يظل أسيرًا للانقسامات السياسية بين أعضائه الدائمين، وأن يسعى جاهدًا لوضع إطار قانوني دولي يكفل الأمن والاستقرار في الفضاء الرقمي.

خاتمة

في خضم التوسع الهائل في استخدام تكنولوجيا المعلومات والاتصالات، أصبحت القرصنة الإلكترونية من أبرز التهديدات التي تواجه المجتمع الدولي، نظرًا لما تسببه من أضرار اقتصادية وأمنية وسيادية جسيمة. وقد تبين من خلال هذا البحث أن الأمم المتحدة، رغم كونها الإطار الأوسع للتعاون الدولي، لا تزال تواجه تحديات كبيرة في التصدي الفعّال لهذه الظاهرة المتنامية.

فالجمعية العامة أدّت دورًا مهمًا في إثارة النقاشات ووضع قواعد سلوك غير ملزمة، في حين أن مجلس الأمن لم يُفعّل بعد صلاحياته الكاملة في هذا المجال، رغم الاعتراف المتزايد بالطبيعة المهددة للسلم التي قد تتسم بها بعض الهجمات السيبرانية.

لقد خلص البحث إلى أن هناك فجوة تشريعية ومؤسسية في المنظومة الدولية لمواجهة القرصنة الإلكترونية، وهو ما يستدعي تحركًا أمميًا منسقًا لإقرار اتفاقية دولية ملزمة، وتوسيع التعاون بين الدول، وتفعيل آليات الردع والمساءلة. إن مواجهة التحديات

[١٩] مركز جنيف للسياسات الأمنية، تقرير "نحو اتفاقية دولية للفضاء السيبراني"، ٢٠٢٢، ص ١١–١٤.

السيبرانية لم تعد خيارًا، بل ضرورة ملحة لضمان استقرار وأمن النظام الدولي في العصر الرقمي.

نتائج البحث:

توصل البحث إلى مجموعة من النتائج المهمة، يمكن تلخيصها فيما يلي:

١. غياب إطار قانوني دولي ملزم: رغم الجهود المتعددة التي تبذلها أجهزة الأمم المتحدة، لا يزال المجتمع الدولي يفتقر إلى اتفاقية شاملة وملزمة تنظم مكافحة القرصنة الإلكترونية وتحدد مسؤوليات الدولية

٢. دور الجمعية العامة إرشادي وغير ملزم: تساهم الجمعية العامة في رفع الوعي وتطوير قواعد السلوك في الفضاء الإلكتروني، إلا أن قراراتها تظل ذات طابع توصوي وغير ملزمة، مما يحد من أثرها الفعلي في التصدي للقرصنة الإلكترونية.

٣. صلاحيات محدودة لمجلس الأمن: على الرغم من أن مجلس الأمن يملك صلاحيات واسعة بموجب الفصل السابع، إلا أن تدخله في القضايا السيبرانية لا يزال محدودًا ولم يُفعّل بشكل واضح ومباشر ضد الجرائم الإلكترونية.

٤. تحديات سياسية تحول دون التعاون الدولي: الانقسامات السياسية بين الدول الكبرى، وتباين المفاهيم حول سيادة الدول في الفضاء السيبراني، تشكل عقبة أمام تبني مواقف موحدة داخل أجهزة الأمم المتحدة.

٥. الحاجة إلى تطوير آليات جديدة: يبرز البحث ضرورة تطوير آليات أممية أكثر فاعلية، تشمل تعزيز تبادل المعلومات، وبناء القدرات التقنية، وصياغة معايير دولية واضحة للسلوك المسؤول في الفضاء السيبراني.

توصيات البحث:

في ضوء النتائج التي توصل إليها البحث، يمكن تقديم مجموعة من التوصيات التي قد تسهم في تعزيز دور الأمم المتحدة في مكافحة القرصنة الإلكترونية، **وهي:**

١. الدعوة إلى إعداد اتفاقية دولية شاملة وملزمة تحت مظلة الأمم المتحدة، تتناول بشكل دقيق الجرائم الإلكترونية وعلى رأسها القرصنة، وتحدد المسؤوليات القانونية للدول والجهات الفاعلة.

٢. تعزيز دور الجمعية العامة من خلال دعم مبادراتها المتعلقة بوضع قواعد السلوك السيبراني، وتوسيع نطاق مشاركة الدول النامية في فرق الخبراء الحكومية المتخصصة في هذا المجال.

(ISSN: 2537 - 0758)

٣. تشجيع مجلس الأمن على إدراج التهديدات السيبرانية ضمن جدول أعماله بشكل منهجي، خاصة عندما تُهدد هذه الهجمات السلم والأمن الدوليين أو تستهدف البنى التحتية الحيوية للدول.
٤. إقامة آلية تنسيق دولي داخل الأمم المتحدة لتبادل المعلومات حول الحوادث السيبرانية، وتوفير الدعم الفني للدول الأقل قدرة على التصدي للقرصنة الإلكترونية.
٥. تفعيل الشراكات الدولية والإقليمية بالتوازي مع جهود الأمم المتحدة، من خلال دعم التعاون مع منظمات مثل الإنتربول، والاتحاد الدولي للاتصالات (ITU)، والمنظمات الإقليمية المختصة بالأمن السيبراني.

قائمة المراجع

أولاً: الكتب

١. د. عصام محمد أحمد زناتى: التنظيم الدولى، دار النهضة العربية، ٢٠٠٨م، ص١٣٤.
٢. أ/ أمجد حسن مرشد الدعجة: استراتيجية مكافحة الجرائم المعلوماتية، رسالة ماجستير، معهد البحوث والدراسات الإستراتيجية جامعة أم درمان الإسلامية السودان ٢٠١٤م، على الموقعhttp://search.mandumah.com/record/789271
٣. نورة بنت ناصر بن عبد الله الهزاني، "ضوابط ومتطلبات تطبيق الأمن السيبراني لحماية البيانات". مجلة مكتبة الملك فهد الوطنية، العدد ٢٨، ذو الحجة ١٤٤٤هـ/ يوليو ٢٠٢٣م، ص ٦٤.
٤. د. عبد الفتاح بيومى حجازى: الإثبات الجنائي فى جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، ٢٠٠٧، ص٣٤١.
٥. د. سامى على حامد عياد: الجريمة المعلوماتية وإجرام الإنترنت، دار الفكر الجامعى، الإسكندرية، ٢٠٠٧م، ص٣١٢.
٦. د. جورد لبكي: المعاهدات الدولية للإنترنت: حقائق وتحديات عبر الرابط: تاريخ الزيارة ٢٠٢٥/٤/٢٠.
٧. د. طارق إبراهيم الدسوقى: الأمن المعلوماتى، النظام القانونى للحماية المعلوماتية، مرجع سابق، ص٥٩٩.

٨. منى عبد العليم، "الحروب السيبرانية كأداة صراع في العلاقات الدولية"، المجلة المصرية للعلوم السياسية، العدد ١١٧، ٢٠٢٢، ص ٤٥.
٩. بيان رئيس مجلس الأمن حول الإرهاب والفضاء السيبراني، جلسة ٢٨ يونيو ٢٠١٧.
١٠. قرار مجلس الأمن رقم ١٣٧٣ لعام ٢٠٠١ بشأن مكافحة الإرهاب.
١١. أحمد فوزي، "الفضاء الإلكتروني بين السيادة والحرية: قراءة في مواقف القوى الكبرى"، السياسة الدولية، العدد ٢٢٤، ٢٠٢١، ص ٨٩.
١٢. د. عبد الله على سعيد بن ساحوه: العدالة الجنائية مفهومها نظمها وتطبيقات دولة الإمارات العربية المتحدة، مركز بحوث الشرطة الشارقة، الطبعة الأولى، ٢٠١٣م، ص١٧٣.
١٣. المجلس الاقتصادي والاجتماعي، تقرير لجنة العلوم والتكنولوجيا لأغراض التنمية، الأمم المتحدة، ٢٠١٩.
١٤. تقرير مجموعة الخبراء الحكومية حول الأمن المعلوماتي، الجمعية العامة للأمم المتحدة، الدورة السبعون، الوثيقةA/70/174 2015
١٥. لجنة العقوبات التابعة لمجلس الأمن بشأن كوريا الشمالية، تقرير عام ٢٠٢٠ حول استخدام الوسائل السيبرانية لتمويل البرنامج النووي .
١٦. مركز جنيف للسياسات الأمنية، تقرير "نحو اتفاقية دولية للفضاء السيبراني"، ٢٠٢٢، ص. ١١-١٤.

ثانياً: وثائق صادرة عن الجمعية العامة للأمم المتحدة

١. ميثاق الأمم المتحدة.
٢. قرار الجمعية العامة رقم ١٢١/٤٥ (١٩٩٠).
٣. دليل منع الجرائم المتصلة بأجهزة الكمبيوتر ومكافحتها (١٩٩٤).
٤. القرار ٥٣/٧٠ بتاريخ ٤ ديسمبر ١٩٩٨.
٥. القرار ٤٩/٥٤ بتاريخ ١ ديسمبر ١٩٩٩.
٦. القرار ٥٥/٢٨ بتاريخ ٢٠ نوفمبر ٢٠٠٠.
٧. القرار ١٩/٥٦ بتاريخ ٢٩ نوفمبر ٢٠٠١.
٨. القرار ١٢/٥٦ بتاريخ ١٩ ديسمبر ٢٠٠١ بشأن "مكافحة استخدام نظم المعلومات الإدارية الجنائية لتقنية المعلومات".
٩. القرار ٥٣/٥٧ بتاريخ ٢٢ نوفمبر ٢٠٠٢.

(ISSN: 2537 - 0758)

١٠. قرار الجمعية العامة رقم ٢٣٩/٥٧ بتاريخ ٣١ يناير ٢٠٠٣.
١١. القرار ٣٢/٥٨ بتاريخ ١٨ ديسمبر ٢٠٠٣ حول موضوع "التطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي".
١٢. قرار الجمعية العامة رقم A/RES/٥٨/١٩٩ بتاريخ ٢٣ ديسمبر ٢٠٠٣ بعنوان "تعزيز أمن البنية التحتية الحيوية للمعلومات".
١٣. القرار ١٩٩/٥٨ بتاريخ ٣٠ يناير ٢٠٠٤ بشأن "إنشاء اتفاقية عالمية للأمن السيبراني".
١٤. القرار ٥٥/٦٣ بتاريخ ٤ ديسمبر ٢٠٠٠.
١٥. قرار الجمعية العامة رقم A/RES/٢٤٧/٧٤ المؤرخ في ٢٧ ديسمبر ٢٠١٩.
١٦. القرار ٢١١/٦٤ (٢٠٠٩).
١٧. القرار ١٦٧/٦٨ (٢٠١٣) بشأن الحق في الخصوصية في العصر الرقمي.

ثالثاً: قرارات صادرة عن مجلس الأمن

١. القرار ١٣٧٣ لعام ٢٠٠١.
٢. قرار مجلس الأمن رقم ٢/٢٩ لسنة ٢٠١٣ بشأن الإرهاب الإلكتروني.
٣. القرار رقم ١/٢٩ بتاريخ ١٧ ديسمبر ٢٠١٣

رابعاً: مؤتمرات دولية تحت إشراف الأمم المتحدة

١. مؤتمر الأمم المتحدة السابع لمنع الجريمة ومعاملة المجرمين– ميلانو، إيطاليا (١٩٨٥).
٢. المؤتمر الثامن لمنع الجريمة ومعاملة المجرمين– هافانا، كوبا (١٩٩٠).

خامساً: تقارير ومبادرات

١. تقرير الفريق الحكومي الدولي المعني بالتطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي (GGE).
٢. مبادرة الأمم المتحدة لتعزيز السلم والأمن السيبراني.
٣. تقارير اللجان الفرعية التابعة لمجلس الأمن.
٤. الهيئة الفرعية التابعة للجمعية العامة المعنية بتطورات الفضاء المعلوماتي في السياق الأمني– تقارير حول التهديدات السيبرانية.
٥. جلسات غير رسمية داخل مجلس الأمن تحت "صيغة آريا" (Arria Formula).