العدد الثاني والعشرون - الجزء الثاني - فبراير - 2025 - السنة الرابعة مجلة علمية فصلية محكمة

المجلة الأمريكية الدولية للعلوم الإنسانية والاجتماعية

American International Journal of Humanities and Social Sciences

الالكتروني (3085 - 4806) (ISSN) / الورقي (3085 - 4830) (ISSN)
رقم الايداع القانوني في المكتبة الوطنية المغربية (2025 Pe00006)
رقم الايداع القانوني في دار الكتب والوثائق العراقية (2735)

تصدر عن الأكاديمية الأمريكية الدولية للتعليم العالي والتدريب

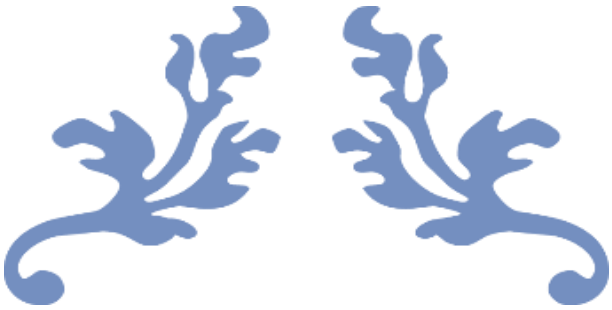
ISSUED BY AMERICAN INTERNATIONAL ACADEMY OF HIGHER EDUCATION AND TRAINING

الموقع الرسمي للمجلة / www.iajphss.us

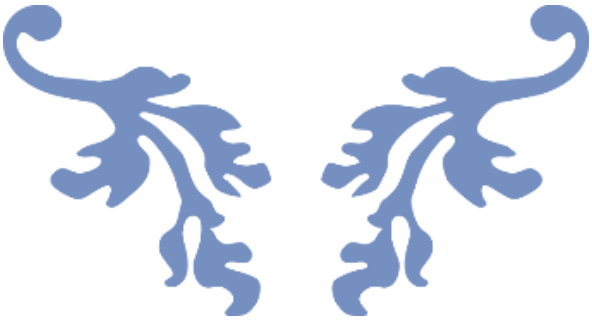

بسم الله الرحمن الرحيم

أعضاء الهيئة الاستشارية

18. أ.م.د. هلال قاسم أحمد المريسي ـ عميد الشؤون الأكاديمية الأميريكية للتعليم العالي والتدريب ـ جامعة العلوم الحديثة ـ الجمهورية اليمنية.
19. أ.د. نادية حسين العفون، كلية التربية للعلوم الصرفة- ابن الهيثم- جامعة بغداد، الجمهورية العراقية.



مقال العدد



بِسۡمِ ٱللَّهِ ٱلرَّحۡمَٰنِ ٱلرَّحِيمِ ، الحمدّ لله على فضله ونعمته ، والصلاة والسلام على رسوله الكريم وآله ، أمّا بعد

يسرّنا أن نقدم لكم العدد 22 ج2 من المجلة الأمريكية الدولية للعلوم الإنسانية والاجتماعية، الذي يضم مجموعة من البحوث العلمية المتميزة التي شارك بها باحثون من مختلف دول العالم. يشتمل هذا العدد على أعمال بحثية مقدمة في المؤتمر العلمي الدولي الثامن عشر، بالإضافة إلى مجموعة من الدراسات التي جاءت خارج نطاق المؤتمر، مما يعكس تنوعًا علميًا وثراءً في المواضيع المطروحة.

لذ دأبت هيئة التحرير على تطبيق معايير التقييم العلمية شأنها بذلك شأن المجلات الرصينة المثيلة في حقل التخصص والنشر العالمي ، فعرضت البحوث على محكمين لهم مكانتهم العلمية في فضائهم العلمي ، ويعودون لجنسيات مختلفة ، ومن جامعات متباينة ، منها الجامعات الحكومية التي ترجع بمرجعيتها إلى بلدان العالم المختلفة ، فضلا عن الاستعانة بخبراء من جامعات خاصة اثبتوا بشكل علمي أنهم أهل للتحكيم واطلاق الحكم على علمية البحث المقدم للمجلة ، وصلاحيته للنشر.

حرصت هيئة التحرير على عرض البحث المقدم من لدن كاتب البحث على محكمين اثنين ، وتقديمه لهما ، بتوقيتات زمنية محددة ، فأن اتفق المحكمان على صلاحية البحث ، تم تحويله إلى مرحلة التنضيد والنشر ، بعد التأكد من دقة تطبيق تعليمات النشر الخاصة بالمجلة . وإن اختلف المحكمان في التقييم المطلق على البحث المقدم ، حول البحث لمحكم ثالث ، فأن قبله ، تم تحويله للمرحلة الثانية التنضيد والنشر ، وإن رفضه ، عندئذ يرفع البحث من قائمة البحوث المعدة للنشر.

لم يختلف منهج هيئة التحرير في آلية قبول البحوث ، وعدّها للنشر عن غيرها من المجلات العلمية ؛ لأن الرصانة العلمية هو هدفها الذي تسعى للوصول إليه ، واعتمدت نظاما دقيقا في استقبال البحوث ، وتقديمها للمقومين ، واشعار الباحثين بقبول النشر ، وفقا لأمر إداري يصدر عن المجلة ، يعد مستندا في صحة نشر البحث في المجلة ، مع تثبيت العدد الذي نشر فيه مذيلا بإمضاء رئيس التحرير.

احتوى هذا العدد في طياته مجموعة من البحوث ، والتي تحمل موضوعات متنوعة ، ذات الطابع الإنساني والاجتماعي ، ضمن تخصص المجلة ، وكل الأفكار التي طرحت تحمل الرؤى العلمية وأبعادها ، والنظرية التي يؤمن بها أصحاب تلك الأفكار ، لذلك كانت المجلة دقيقة ؛ لأجل عرض تلك الأفكار من دون التدخل فيها ، مع متابعة كونها لا تؤدي إلى خلق الفوضى العلمية ، أو تحريض للعنف ، أو للتطرف العلمي والمجتمعي.

نحن فخورون أيضًا أن هذا العدد يصادف حدثًا مميزًا في مسيرة المجلة، حيث تم اعتمادنا من قبل المكتبة الوطنية المغربية للحصول على الاعتماد القانوني، ومنحنها التسلسل الرقمي الدولي (ISSN) للنسخة الإلكترونية وأيضًا للنسخة الورقية. هذا الإنجاز يعكس التزامنا بتقديم محتوى علمي رصين ومتنوع، ويسهم في تعزيز مكانة المجلة كمصدر مرجعي معترف به عالميًا.

28/02/2025 الرباط ـ المملكة المغربية هيئة تحرير المجلة

الملاحظة القانونية

البحوث المنشورة في المجلة لا تعبر عن وجهة نظر المجلة ، بل عن رأي كاتبها

آليات التصدي للهجمات السيبرانية في ضوء القانون الدولي

م.م. مصطفى علي حسن

كلية الحقوق _ جامعة النهرين _ العراق

mustafa.ali@nahrainuniv.edu.iq

009647717730889

الملخص -:

أن التطور الكبير في تكنولوجيا المعلومات والاتصالات بات نقمة على البشر ، فعلى الرغم من الإيجابيات الكثيرة الناجمة عن التكنلوجيا المعلوماتية ، إلا أنها أصبحت اداة فتاكة تستخدم للمساس بحقوق الإنسان ، من اخطر السلبيات الناجمة عن تلك التكنلوجيا زيادة الاعتماد عليها في عصرنا الحديث لتنفيذ الهجمات السيبرانية التي تتم في الفضاء السيبراني حيث دخلت الحروب السيبرانية بقوة في معادلات الصراع والمواجهة بين الدول الكبرى بالتالي اصبحت هذه الحروب احد عوامل مضاعفة قوة الدول وفاعليتها . وتتمثل مشكلة البحث بخطورة الهجمات السيبرانية إذ أنها تعد من اهم التحديات التي يواجهها فقهاء القانون الدولي لما لها من خطوة كبيرة على المستوى الدولي نتيجة لسهولة استخدام الاسلحة السيبرانية كالفايروسات وبرامج التجسس وسرقة المعلومات العسكرية وتدمر البنى التحتية بوقت وجيز عكس الحروب التقليدية ، وبهذا الخصوص تثار الاسئلة الاتية :

١ /هل تعد قواعد القانون الدولي كافية لصد الهجمات السيبرانية .

٢_هل بالإمكان عقد اتفاقيات ثنائية للتصدي للهجمات السيبرانية ؟

٣ _هل ان قواعد القانون الدولي كافية لتوفير الحماية للدول المتضررة من الهجوم السيبراني واثاره ؟.

و نهدف من خلال بحثنا إلى :

١ /البحث عن ماهية الهجمات السيبرانية الآثار السلبية وخصائصها لهذه الهجمات حتى يكون مفهومها واضحا.

٢ /البحث في اليات التصدي للهجمات السيبرانية على الصعيدين الدولي والفقهي لبيان الدور الذي تؤديه في مكافحة الآثار السلبية الناجمة عن الهجمات السيبرانية ودورها في تحجيم ارتكابها.

وعليه فان هيكلية بحثنا ستحدد ببحثين نخصص المبحث الاول لماهية الحرب السيبرانية نفرد المطلب الاول لمدلول الهجمات السيبرانية و نبين في المطلب الثاني آثار الحروب السيبرانية وخصائصها ، ونوظف في المبحث الثاني للبحث في اليات التصدي للهجمات السيبرانية ، نفرد المطلب الاول لآليات التصدي الدولية ، ونتناول في المطلب الثاني اليات التصدي الفقهية، ومن ثم سنختتم بحثنا بمجموعة من الاستنتاجات والمقترحات . والله ولي التوفيق

الكلمات المفتاحية -: الحروب، السيبرانية ،القانون الدولي ،الهجمات الالكترونية ،الاليات الدولية .

The mechanisms for combating cyber attacks in light of international law.

Assistant Lecturer Mustafa Ali Hassan
College of Law, Al-Nahrain University, Iraq

Abstract:-

Despite the many positives resulting from information technology, it has become a deadly tool used to harm human rights, one of the most serious negatives resulting from this technology is increased reliance on it in our modern era to carry out cyber attacks carried out in cyberspace, where cyber wars entered strongly into the equations of conflict and confrontation between major countries, thus these wars became one of the factors of doubling the strength and effectiveness of countries. The problem of research is the seriousness of cyber attacks, as they are one of the most important challenges faced by international law jurists because of their great step at the international level as a result of the ease of use of cyber weapons such as viruses and spyware and the theft of military information and the destruction of infrastructure in a short time, unlike conventional wars.

Are the rules of international law sufficient to repel cyber-attacks?

Can countries be held accountable for cyber attacks against other countries?

Are cyberattacks an attack on the sovereignty of states?

Through our research, we aim to:

Searching for what cyber warfare is and the negative effects of these wars so that their concept is clear.

Examine mechanisms to address cyberattacks at the international and internal levels to demonstrate the role they play in combating the negative effects of cyberattacks and their role in reducing their perpetration.

Therefore, the structure of our research will be determined by two types of research. We allocate the first topic to what cyber warfare is. We uniquely identify the first requirement of the meaning of cyber warfare and show the second demand for the effects of cyber warfare.

In the second topic to discuss mechanisms to address cyber attacks, we uniquely demand the first requirement for internal response mechanisms. God bless me.

Keywords:-Warfare, Cyber, International Law, Cyber Attacks, International Mechanisms.

مقدمة:-

بالتزامن مع هذا التطور الكبير في تكنولوجيا المعلومات والاتصالات اذ دخلت الحروب السيبرانية بقوة في معادلات الصراع والمواجهة بين الدول الكبرى بالتالي اصبحت هذه الحروب احد عوامل مضاعفة قوة الدول وفاعليتها حيث اصبحت الهجمات السيبرانية من اهم التحديات التي يواجهها فقهاء القانون الدولي لما لها من خطوة كبيرة على المستوى الدولي نتيجة لسهولة استخدام الاسلحة السيبرانية كالفايروسات وبرامج التجسس وسرقة المعلومات الشخصية و العسكرية وتدمير البنى التحتية بوقت وجيزعلى عكس الحروب التقليدية.

اذ أسهمت التحولات التكنولوجية والتقنية الحديثة في إحداث تطورات ملحوظة في استخدام وسائل التواصل والمنصات الرقمية، بهدف تسهيل الوصول إلى الآخرين. ومع ذلك، قد يكون هذا الوصول غير مشروع في بعض الأحيان، مما يشكل تهديدات أمنية تطال الأفراد والمؤسسات على حد سواء. وقد أدى ذلك إلى ظهور الهجمات السيبرانية بأساليب جديدة تتسم بالتعقيد وتنوع المجالات، مستغلة الفضاء الرقمي كوسيلة لتنفيذها؛ أمام هذه التحديات، حتى أصبحت المؤسسات الأمنية في مختلف الدول في حالة استنفار مستمر لتعزيز الرقمنة الأمنية، بهدف حماية المعلومات وحفظ الحقوق، سواء كانت فكرية، أومالية، أو إقليمية، ضمن إطارها الأمني ،لأن ساحات المعارك الهجومية اليوم لم تعد ساحات المعارك التقليدية كما كانت سابقآ ، بل أصبحت ساحات معارك هجومية افتراضية، مما يتطلب آليات جديدة لكشف مثل هذه الأعتداءات والتحقيق فيها، وضع خطط بديلة للتعامل معها.

أهمية البحث:-

اثار الواقع الجديد العديد من التحديات التي طرأت على القانون الدولي من خلال عمليات الاقتحام للفضاء السيبراني واستعماله بطريقة أكثر فتكآ وأكثر تهديدآ للأمن والاستقرار الدوليين ، بحث اصبحت دول العالم امام منعطف خطير وهو حماية بيانتها الرقمية والشخصية من الاعتدأت السافره على السيادة الرقيمة للدول في مجال الفضاء الالكتروني.

مشكلة البحث :-

تدور إشكالية البحث في محور مهم وهو كيفية تأمين الفضاء السيبراني من الهجمات في ضل عدم وجود اتفاق دولي لفقهاء القانون على تعريف الهجمات السيبرانية وازالة الغموض من ذلك والحد من التصعيد العالمي بين الدول من خلال تقديم آليات جديدة للتعاون الدولي لحل المشكلات القانونية المرتبطة بالاعتداءات السيبرانية المتكررة واستكشاف الطرق الممكنة للتغلب عليها وبهذا الخصوص تثار الاسئلة الأتية:- 1_هل بالإمكان عقد اتفاقيات ثنائية للتصدي للهجمات السيبرانية ؟ ٢ _ هل ان قواعد القانون الدولي كافية لتوفير الحماية للدول المتضررة من الهجوم السيبراني واثاره ؟.

منهج البحث

يتطلب موضوع البحث اعتماد المنهج الوصفي التحليلي ، حيث يقوم البحث باستعراض طبيعة الهجمات السيبرانية وتحليل قواعد ومبادئ القانون الدولي لبيان مدى امكانية تطبيق هذه القواعد والمبادئ على الهجمات السيبرانية كونها اعتداءات حديثة برزت بعد صدور القانون الدولي.

الدراسات السابقة

لإعداد هذه الدراسة، قام الباحث بالاطلاع على نماذج متنوعة من الدراسات التي تناولت مواضيع قريبة من موضوع دراستنا. ونظرًا لقلة تلك الدراسات نتيجة لحداثة الموضوع، فقد سعى الباحث إلى تناول بعض جوانب الموضوع واقتربت من حدود مضمونه:

الدراسة الاولى : د. طلال محمد الحاج إبراهيم (2020) بعنوان (الهجمات السيبرانية على شبكات الحاسوب في ضوء القانون الدولي الإنساني). تناولت هذه الدراسة الفضاء السيبراني والهجمات السيبرانية من حيث الأهمية الاستراتيجية لهذا الفضاء ومفهوم الهجمات السيبرانية. كما استعرضت التداعيات المحتملة لهذه الهجمات على الأمن الدولي والنزاعات المسلحة، بالإضافة إلى المشاركة المباشرة في الهجمات السيبرانية. بينما تتناول دراستنا بيانًا أكثر تفصيلًا واستعراضاً حول ماهية الهجمات السيبرانية وتوضيح مفهومها وبيان آثارها العسكرية والاجتماعية والاقتصادية.

الدراسة الثانية : د احمد عبيس الفتلاوي (٢٠١٦) بعنوان: (الهجمات السيبرانية في ضوء التنظيم الدولي المعاصر). تناولت هذه الدراسة مفهوم الهجمات السيبرانية وإطارها القانوني، وعلاقتها بتحقيق الأمن السيبراني. بينما تتناول دراستنا مفهوم الهجمات السيبرانية من منظور أوسع وأشمل، من خلال توضيح مفهوم السيبرانية وخصائص هذه الهجمات وبيان موقف الجهود الدولية من تلك الهجمات باستعراض مفصل للأليات التصدي الدولية والفقهية لتلك الهجمات.

هيكلية البحث

لإجابة على هذه الإشكالية المطروحة حول موضوع بحثنا ، تم تقسيم البحث إلى مبحثين: المبحث الأول يتناول ماهية الهجمات السيبرانية وآثارها.اما المبحث الثاني: يتحدث عن اليات التصدي للهجمات السيبرانية الدولية والفقهية.

المبحث الاول

ماهية الهجمات السيبرانية وآثارها

تتطلب الحرب السيبرانية فهماً دقيقاً للمصطلح، خاصة في سياق قواعد القانون الدولي بالتالي يجب النظر في كيفية تطبيق القوانين والمعايير الدولية على هذه الهجمات؛ في حين أن بعض الهجمات يمكن أن تُصنَّف كأعمال حرب، إلا أنها قد تعد جرائم في الفضاء الإلكتروني.

بهذا، يتضح لنا بان الهجمات السيبرانية تمثل تهديدًا متزايدًا للأمن السيبراني، مما يتطلب وعيًا وفهمًا عميقًا لمخاطرها وآثاره. وعليه نخصص هذا المبحث في مطلبين : نتناول في المطلب الاول مفهوم الهجمات السيبرانية ونفرد في المطلب الثاني الى اثار الهجمات السيبرانية وهي كالأتي:-

المطلب الاول

مفهوم الهجمات السيبرانية

ان البحث في مفهوم الهجمات السيبرانية يتطلب منا بيان معناها وذلك من خلال الولوج في مدلولها والتعريج على خصائصها ، وهذا ما خصصنا له فرعين وكالأتي :-

التعريف بالهجمات السيبرانية :-

سنتناول مفهوم الهجمات السيبرانية، وهو موضوع ضروري للتحليل القانوني. تختلف هذه الهجمات عن المفاهيم التي تم تناولها في الدراسات القانونية السابقة، حيث يتم استخدام مصطلحات مثل "الهجوم السيبراني" (Cyber Attack)، و"الحرب السيبرانية" (Cyber Warfare)، و"الجريمة السيبرانية" (Cyber Crime) دون توضيح المعاني المقصودة منها. بالتالي يمكن أن يؤدي هذا الغموض إلى صعوبة في وضع التكييف القانوني المناسب. لذلك، سنستعرض مفهوم الهجمات السيبرانية من خلال فرعين:

الفرع الأول

مدلول الهجمات السيبرانية :

معنى كلمة "سايبر" (Cyber) في اللغة وأصلها. قبل أن تكتسب كلمة "سايبر" (Cyber) شهرتها الحالية، كانت تشير في الأصل إلى مفهوم السيبرانية أو علم الضبط، الذي نشأ في أواخر الأربعينيات من القرن العشرين. وقد أسهم في تطوير هذا المجال مجموعة متنوعة من المتخصصين من مجالات عدة، بما في ذلك علم الأحياء والهندسة والعلوم الاجتماعية. (منير البعلبكي. (2004). عربي-قاموس إنكليزي: المورد. بيروت: دار العلم للملايين. ص. 243.)

استخدم المصطلح أكاديمياً لأول مرة بواسطة "نوربرت وينر" (Norbert Wiener) في عام 1948، حيث قدم مفهوم "السيبرنتيكس" (Cybernetics). في كتابه المعروف بعنوان "السيطرة والاتصال في عالم الحيوان والآلات" (Cybernetics: Or Control and Communication in the Animal and the Machine)،

أشار وينر إلى هذا المفهوم بوصفه "آلية ذاتية التنظيم"(Norbert Wiener,"Cybernetics or control communication in the animal and the machine",M.I.T.,Press,second Edidtion, Cambridge, Massachusetts,1948.).

يمكن القول إن السيبرانية تمثل تداخلًا بين مختلف العلوم، حيث تهدف إلى فهم كيفية تنظيم الأنظمة والتفاعل بين العناصر المختلفة داخلها.

إن الاهتمام بكيفية عمل تلك الأنظمة يتطلب تسليط الضوء على أصل كلمة "سايبر" (Cyber). تعود هذه الكلمة في الأصل إلى الكلمة اليونانية "Kubernetes"(طلاس ،مصطفى، الثورة العلمية التقنية وتطور القوات المسلحة، دار طلاس للدراسات والترجمة والنشر ،دمشق،ص315 .) ، والتي تعني "مدير الدفّة". وقد ورد هذا المصطلح في بادئ الأمر في ملفات الخيال العلمي، حيث كان يشير إلى مفهوم القيادة أو التحكم عن بُعد (Jullia Cresswell , "oxford Dictionary of word origins Cybernetics" , Oxford Reference online , Oxford universitypress,2010). أما في اللغة العربية، فلا يوجد مصطلح مقارب لكلمة "سايبر" (Cyber). فمعنى هذه الكلمة في قاموس المورد الحديث يعبّر عن "الكمبيوتري" أو "عصري جداً". كما ورد معنى مصطلح "السيبرانية" (Cybernetics) بأنه "علم الضبط" (www.almaany.com).

حيث إن غياب مصطلح عربي دقيق لمفهوم "سايبر" يعكس تحديًا كبيرًا في مجال الترجمة والتعريب، خاصة في المجالات التقنية والقانونية. لذى فقد يؤدي هذا الغياب إلى سوء فهم للمفاهيم وتشويش في المعاني، كما يحد من تطور المصطلحات العربية في هذا المجال فقد كانت اتفاقية مجلس أوروبا المتعلقة

بالجريمة السيبرانية، خير مثال على ذلك والتي تمت ترجمتها إلى "الاتفاقية المتعلقة بالجريمة الإلكترونية"، مما يؤكد على غياب المصطلح العربي الجامع والمُعبّر عن المعنى الشامل لكلمة "سايبر"(احمد عبيس نعمة الفتلاوي ، الهجمات السيبرانية ومفهومها والمسؤولين الدوليين الناشئة عنها في ضوء التنظيم الدولي المعاصر ،بحث منشور في مجلة المحقق الحلي ، كلية القانون ، جامعة بابل ،2015، ص5).

وهنا تجد الاشارة الى ان الوثائق الرسمية الصادرة عن الأمم المتحدة باللغة العربية تعتمد مصطلح "السيبرانية" بدلاً من "الإلكترونية". ومن الأمثلة الدالة على ذلك القرار رقم (239/57) الذي أقرته الجمعية العامة للأمم المتحدة، والذي يركز على "إنشاء ثقافة عالمية لأمن السيبراني". كما يتضمن القرار رقم (199/58) الصادر عن الجمعية نفسها دعوة للدول الأعضاء لتعزيز التعاون في مجال الأمن السيبراني وتطوير ثقافة شاملة تضمن حماية الفضاء السيبراني (القرار رقم 57/239بتاريخ 31/كانون الثاني /يناير 2003. القرار رقم 58/199 بتاريخ 30/ كانون الثاني / يناير 2004 . مكتب الأمم المتحدة المعني بالمخدرات والجريمة ، تقرير الخبراء المعني باجراء دراسة شاملة عن الجريمة السيبرانية ، فيينا عام 2013 ، الوثيقة EG ، CCPC ، UNODC ، 2013/2/4 .

وبالنظرًا لعدم توفر مصطلح معادل لمصطلح "السيبرانية" في الوثائق الصادرة عن الأمم المتحدة باللغة العربية، تم اعتماد مصطلح "الهجمات السيبرانية" في هذه الدراسة.

الفرع الثاني

الهجمات السيبرانية اصطلاحآ

على مدى أكثر من عشر سنوات، أبدى المحللون والمختصون قلقهم حيال العواقب المحتملة التي قد تنجم عن التطورات التكنولوجية المتسارعة، والتي قد تؤدي إلى أضرار مادية واقتصادية ذات نطاق واسع. تتضمن هذه المخاوف مجموعة من السيناريوهات الكارثية، مثل انهيار السدود التي قد تسبب فيضانات مدمرة، وتعطل سوق الأسهم الذي يمكن أن يؤدي إلى أزمات مالية عالمية كبيرة . كما تشمل المخاطر ايضا إيقاف المفاعلات النووية أو حتى تفجيرها عن بُعد، مما يهدد الأمن الإقليمي والدولي (Hathaway, Oona A., Crootof, Rebecca, Levitz, Philip , Nix, Haley, Nowlan, Aileen, Perdue, William, Spiegel, Julia. (2012). The Law of Cyber-Attack. California Law Revien, 824)

ويُعد وضع تعريف دقيق ومحدد للهجوم السيبراني خطوة أساسية ومهمة للتصدي في مواجهة التهديدات المتزايدة التي تنجم عن التطور السريع للسيبرانية، وهو مفهوم حديث يتطلب اهتمامًا خاصًا نظرًا لكونه يشكل خطرًا حقيقيًا على السلم والأمن الدوليين. إن الفهم الواضح للهجوم السيبراني يساعد في تطوير استراتيجيات فعّالة للتصدي لهذه التهديدات، مما يعزز من قدرة الدول والمؤسسات على حماية بنيتها التحتية الحيوية. لذا، سنستعرض في هذا السياق مجموعة من التعريفات التي اعتمدها فقهاء ومتخصصون في مجالات الأمن السيبراني والقانون الدولي. والتي سوف تساعد في توضيح الفهم المتنوع للهجمات السيبرانية وكيفية تصنيفها.

وبعد ذلك، سنقدم التعريف الذي يتضمن الأنشطة والأعمال التي تؤدي إلى تصنيف الهجمات السيبرانية، مع الأخذ في الاعتبار العوامل التقنية والقانونية والأخلاقية. وسنسعى جاهدين للوصول إلى

التعريف الأكثر قبولًا وموثوقية، والذي يعكس تعقيدات هذا المجال ويتيح لنا إدارة المخاطر المرتبطة به بشكل أكثر فعالية.

منما شك تتنوع التعريفات المتعلقة بمصطلح الهجوم السيبراني بشكل كبير، وذلك بسبب اختلاف طبيعة الدول وتباين ظروفها السياسية والاقتصادية. بالإضافة إلى ذلك، تلعب الاستراتيجيات المعتمدة في كل دولة دورًا حاسمًا في كيفية فهم هذا المصطلح وتفسيره

فقد عرف فيورتس (Fuertes) الهجوم السيبراني بأنه "هجوم عبر الإنترنت يستند إلى الوصول إلى مواقع إلكترونية غير مرخصة، بهدف تدمير أو إتلاف المعلومات الموجودة فيها أو الاستحواذ عليها. وتُعد هذه الهجمات نوعًا من الهجمات الإلكترونية التي تنفذها دولة ضد دولة أخرى".

أما شميت (Schmitt) فقد عرفه بأنه "مجموعة من الإجراءات التي تتخذها الدولة للهجوم على نظم المعلومات المعادية، بهدف التأثير عليها وإضعافها، مع العمل في الوقت نفسه على حماية نظم المعلومات الخاصة بها"(الفتلاوي، أحمد عبيس نعمة. (2018). الهجمات السيبرانية: دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصرة. الطبعة الأولى، منشورات زين الحقوقية، بيروت، لبنان، ص 16).وفيما يتعلق باللجنة الدولية للصليب الأحمر، فقد عرفت الهجوم السيبراني بأنه "استخدام أنشطة متعمدة لتخريب أو إفساد أو خداع أو إضعاف أو تدمير أنظمة الحاسوب أو شبكات الحاسوب الخاصة بالخصوم، بالإضافة إلى المعلومات والبرامج الموجودة في هذه الأنظمة أو التي تمر عبرها.

كما يمكن أن تؤثر هذه الأنشطة أيضًا على الكيانات المرتبطة بهذه الأنظمة والشبكات.وايضا يمكن أن يُستخدم الهجوم السيبراني في هجمات الحرمان من الخدمة، حيث يتم منع المستخدمين المرخص لهم من الوصول إلى الحاسوب أو خدمة المعلومات. كما قد يستهدف تدمير الآلات التي يتحكم فيها الحاسوب، مثل الهجمات التي تستخدم الفيروسات، أو تدمير أو تخريب بيانات حيوية، مثل الجداول الزمنية المستخدمة في العمليات اللوجستية(لين، هربرت. (2012). "النزاع السيبراني والقانون الدولي الإنساني". مجلة اللجنة الدولية للصليب الأحمر، مجلد 94(886)، صيف، 515-531، 518-519. متاح على الرابط: https://cutt.ly/RkoansD[ ).(https://cutt.ly/RkoansD) .

استنادًا إلى ما سبق، نجد أن التعريف الذي قدمه "شميت"، المتخصص في القانون الدولي الإنساني والعضو البارز في مركز الدفاع السيبراني التعاوني التابع لحلف الشمال الأطلسي (NATO)، في دليل تالين يُعتبر الأكثر دقة في وصف مفهوم الهجمات السيبرانية. حيث أشار شميت إلى أن الهجوم السيبراني يُعرّف بأنه "أي تصرف إلكتروني، سواء كان دفاعيًا أو هجوميًا، يُتوقع منه بشكل معقول أن يُسبب جروحًا أو وفاة شخص، أو يلحق أضرارًا مادية أو دمارًا بالهدف المستهدف"(Schmit, Michael N. (2013)."Tallinn Manual on the International Law Applicable to Cyber Warfare." Cambridge University Press.First published.p.92)

ان هذا التعريف يسلط الضوء على الأبعاد القانونية والأخلاقية للهجمات السيبرانية، وبالتالي يتناغم هذا التعريف مع ما جاء في اتفاقية مجلس أوروبا الخاصة بالجريمة السيبرانية لعام 2001. حيث أوضحت المادة الخامسة (5) من الاتفاقية أنه ينبغي على كل دولة طرف اتخاذ جميع التدابير التشريعية والتدابير الأخرى اللازمة لتجريم الهجمات السيبرانية في إطار نظامها القانوني: "الإعاقة الخطيرة لعمل منظومة الكمبيوتر عن بُعد، إذا ما ارتكبت عمدًا". وتشمل أساليب التعامل مع بيانات الكمبيوتر مجموعة متنوعة من الإجراءات، مثل إدخال البيانات، إرسالها، إتلافها، محوها، تغييرها، تبديلها، وتدميرها. كل من هذه الطرق

تلعب دورًا هامًا في إدارة البيانات وضمان سلامتها وأمانها(مجلس أوروبا، "اتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية، مجموعة المعاهدات الأوروبية رقم 185، بودابست، عام 2001 – المادة رقم (5)).

المطلب الثاني

خصائص الهجمات السيبرانية و اثارها

الهجمات السيبرانية تمثل تهديدًا متزايدًا للأفراد والشركات والحكومات على حد سواء. ولفهم ذلك سوف نستعرض في الفرع الاول عدة خصائص لتلك الهجمات .

تتميز الهجمات السيبرانية بمجموعة من الخصائص خصصنا لبيانها الفقرات الاتية :-

الفرع الاول

خصائص الهجمات السيبرانية

اولآ: تتميز الأسلحة والوسائل المستخدمة في الهجمات السيبرانية بسهولة الاستخدام وإمكانية التطوير المستمر، مما يعزز من قدرتها التدميرية. كما أنها تتسم بدقة عالية وقدرة فعالة على اختراق الأنظمة والأجهزة الإلكترونية الحساسة.(العيسى، طلال ياسين، وعنب، عدي محمد. (2019). المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر. مجلة الزرقاء للبحوث والدراسات الإنسانية، 2019. https://doi.org/10.12816/0054788)

ثانياً: تعتبر الهجمات السيبرانية من الأعمال التي تهدف إلى زعزعة استقرار الوظائف الأساسية للشبكات وأنظمة الكمبيوتر المعتمدة، مما يسفر عن تعطيل أو تدمير هذه الأنظمة بشكل فعّال. مما يترتب على ذلك تأثيرات مباشرة على العمليات الحيوية للمنشآت الحيوية، مثل السدود ومحطات توليد الطاقة وغيرها من البنى التحتية. حيث تهدف هذه الهجمات، من خلال التدمير والإتلاف، إلى تحقيق أهداف استراتيجية تتعلق بالسياسة والأمن العسكري.(نادين جميل سلمان هارون،المسؤولية الدولية عن الهجمات السيب ارنية في ظل القانون الدولي الانساني،رسالة ماجستير ، جامعة العلوم التطبيقية الخاصة ، الاردن ،عمان، 2023)

ثالثآ: تتميز الهجمات السيبرانية بعدم وجود حدود جغرافية أو نطاق محدد، حيث يتم تنفيذها ضمن فضاء سيبراني غير ملموس وغير محدود. وتُستخدم في هذه الهجمات أدوات وأساليب غير تقليدية، مما يمكنها من التمتع بقدرة تدميرية واسعة النطاق،و يجعلها تمثل تهديدًا خطيرًا على الأمن السيبراني والبنى التحتية الحيوية. (عبد الله بن سعيد بن البلوشي، مشروعية أسلحة الدمار الشامل وقواعد القانون الدولي، الطبعة الأولى، منشورات الحلبي الحقوقية، 2007)

رابعآ: الهجمات السيبرانية تتميز بشكل عام بغياب الوضوح حول هوية مرتكبيها، مما يخلق تحديات كبيرة في تحديد الجهات الفاعلة أو المصادر الجغرافية التي تنطلق منها هذه الهجمات. ويُعد هذا الغموض عاملًا رئيسيًا يعيق عملية الإسناد القانوني، مما يصعّب تحديد المسؤولية الدولية وفقًا لأطر القانون الدولي. وعلى الرغم من أن هذه الخصائص تُعزز من فعالية الأسلحة السيبرانية وقدرتها على التخفي، إلا أنها تشكل في الوقت ذاته عقبةً أمام تطوير آليات واضحة وفعالة لتحميل الأطراف المسؤولية القانونية، مما يؤثر سلبًا على إمكانية إرساء قواعد قانونية دولية متفق عليها في مجال الفضاء السيبراني. (Clarke, R., & Nick, R.

Cyber Warfare. 1st Edition. Abu Dhabi: Emirates Center for Strategic Studies and Research, 2012, p. 28)

خامساً: وتتميزايضا الهجمات السيبرانية بعدم اشتراط الوجود المادي للمنفذين في ساحة المعركة، حيث يتم تنفيذها عبر الفضاء السيبراني باستخدام وسائل اتصال متقدمة يصعب تعقبها أو تحديد هوية مستخدميها. كما تُعد هذه الهجمات ذات تكلفة مادية منخفضة مقارنةً بالوسائل العسكرية التقليدية، مما يجعلها في متناول مجموعة واسعة من الفاعلين، بما في ذلك الجهات غير الحكومية مثل الجماعات المسلحة، والمرتزقة، والمليشيات، والشركات الأمنية الخاصة، والتنظيمات ذات الأهداف السياسية أو الاقتصادية. هذا التنوع في الجهات الفاعلة يزيد من تعقيد التحديات الأمنية والقانونية المرتبطة بمكافحة هذه الهجمات.(راضي، عمار مزاحم مهدي، مبادئ التحقيق الجنائي في الجرائم الإلكترونية والمعلوماتية عبر الإنترنت وسبل معالجتها، الطبعة الأولى، منشورات مكتبة بغداد القانونية، 2022، ص 63)

سادساً: يُعتبر التفاعل في الفضاء السيبراني من المميزات الأساسية التي تميزه، حيث يتيح التواصل بين الأفراد عبر منصات رقمية افتراضية يمكنها استيعاب عدد غير محدود من المستخدمين ضمن إطار واحد. وهذا يوفر مستوىً عالٍ من الانفتاح العالمي الغيرمسبوق. بالتالي يتمتع الفضاء السيبراني بالقدرة على تجاوز الحدود الجغرافية، مما يسمح بالتفاعل بين الأفراد من خلال شبكات افتراضية تدمج مختلف الشبكات في فضاء موحد، وهو ما يميزه عن الفضاء المادي أو الواقعي. وهذا مايوضح لنا ان السمة الفريدة لهذا الفضاء تكمن في قدرته على جمع الأفراد والبيئات الرقمية المتنوعة في مكان واحد، مما يسهم في خلق بيئة تفاعلية غير مقيدة بالحدود التقليدية. (Choucri, Nazli.*Cyberpolitics in International Relations*. London: The MIT Press, 2012, p. 4. Library of Congress.)

الفرع الثاني

اثار الهجمات السيبرانية

أذ لا تقتصر اثار الهجمات السيبرانية على حدود معينة ، بل تمتد لتشمل العديد من الجوانب الحيوية والمؤثرة في حياتنا اليومية. بالتالي يمكن لهذه الهجمات أن تتسبب في انفجارات كبيرة داخل مخازن الوقود والمحطات النووية، مما يهدد الأرواح والبنية التحتية. إضافة إلى ذلك، قد تؤدي إلى تغيير مسارات الرحلات الجوية أو تعطيلها بشكل كامل، مما يتسبب في فوضى داخل قطاع النقل الجوي.و هذا التأثير قد يمتد ليشمل أنظمة الطاقة، حيث يمكنها ايضا إيقاف تشغيلها بشكل كامل، وقطع الكهرباء عن مدن بأكملها، مما يؤدي إلى شلل في كافة الأنشطة اليومية والاقتصادية.

ومن جهة أخرى ،يمتد اثر الهجمات ليشمل تعطيل أنظمة التحكم والتشويش على الصواريخ والطائرات، مما يؤثر على دقة مسارها أو يتسبب في فشلها التام. كما أنها قد تضعف أنظمة الدفاع وتخترق أجهزة الحواسيب المسؤولة عن أمن المعلومات، مما يحد من قدراتها التشغيلية ويعرضها للخطر.وسوف نقوم بتوضيح أبرز الآثار القانونية والعمليّة الناشئة عن الهجمات السيبرانية في عدة مجالات، مع التركيز على الجوانب التي تمس الأمن القومي ،ان هذه الآثار تشكل تحديات كبيرة للنظم القانونية الحالية (غيث، علاوى. "الهجمات السيبرانية.. أكبر من حرب نووية: توسع التهديدات الإلكترونية". موقع متخصص في

الشؤون الإيرانية. متاح على الرابط: [https://jadehiran.com/archives/16835] (https://jadehiran.com/archives/16835) :

اولآ: اثر الهجمات السيبرانية على المجال العسكري .

ومع ذلك، فإن الاعتماد المفرط على التكنولوجيا الرقمية في المجال العسكري يُعَد بمثابة "سلاح ذو حدين". ففي حال تعرض الشبكات السيبرانية العسكرية لهجمات إلكترونية، قد تتحول هذه الميزة التكنولوجية إلى نقطة ضعف خطيرة. لهجمات السيبرانية على البنى التحتية العسكرية يمكن أن تؤدي إلى السيطرة على الأنظمة العسكرية، وتعطيل الاتصالات، وحتى توجيه الأسلحة بشكل خاطئ، مما قد يتسبب في خسائر بشرية بين صفوف العسكريين والمدنيين على حد سواء. بالإضافة إلى ذلك،بالتالي قد تؤدي هذه الهجمات إلى زعزعة الاستقرار الأمني وتهديد السلام الدولي، خاصة إذا فيما لو تم استهداف الأنظمة الدفاعية الحيوية أو أنظمة التحكم في الأسلحة الاستراتيجية.

من الناحية القانونية، تُعد الهجمات السيبرانية على الأنظمة العسكرية انتهاكًا صارخًا لمبادئ القانون الدولي الإنساني، وخاصة المبادئ التي تحكم استخدام القوة في النزاعات المسلحة. وفقًا لـدليل تالين ، يمكن اعتبار الهجمات السيبرانية التي تسبب أضرارًا جسيمة تعادل تلك الناجمة عن الهجمات العسكرية التقليدية بمثابة استخدام غير مشروع للقوة، مما قد يؤدي إلى إثارة المسؤولية الدولية للدولة المعتدية.

كما أن هذه الهجمات قد تشكل انتهاكًا لـميثاق الأمم المتحدة، خاصة ما جاء في المادة (٤/٢) من ميثاق الأمم المتحدة ما نصه: "**يمتنع أعضاء الهيئة جميعاً في علاقاتهم الدولية عن التهديد باستخدام القوة، أو باستخدامها، ضد سلامة الأراضي أو الاستقلال السياسي لأي دولة، أو بأي وجه آخر لا يتفق ومقاصد الأمم المتحدة**." التي تحظر استخدام القوة في العلاقات الدولية.(خليفة، إيهاب . "ما هو موقف ميثاق الأمم المتحدة من استخدام القوة السيبرانية في التفاعلات الدولية؟" موقع المستقبل للأبحاث والدراسات المتقدمة.[رابط المقال](https://cutt.ly/jQ3rkpu))(المادة (2/4)ميثاق الامم المتحدة)

ثانيآ: اثر الهجمات السيبرانية على المجال الاقتصادي:-

تُعد ثورة تكنولوجيا المعلومات والاتصالات عنصرًا أساسيًا في دفع عجلة التنمية الاقتصادية للعديد من الدول حيث توفر أدوات فعالة تساعد صانعي القرار في اتخاذ قرارات استثمارية مدروسة وشفافة وقد أسهم هذا التحول الرقمي بشكل كبير في تعزيز معدلات النمو الاقتصادي وتحسين الكفاءة التشغيلية ، مما يجعل تنوع تطبيقات التكنولوجيا في المجال الاقتصادي ومنها الإعلان عن المنتجات الجديدة بطرق مبتكرة وتوفير الأخبار الصحفية المتعلقة بالشركات والمنتجات وتقديم معلومات ترويجية دقيقة حول مبيعات محددة وعرض دراسات شامله للسوق التي تسهم في فهم الاتجاهات الاقتصادية وإجراء أبحاث العملاء لجمع بيانات قيمة حول سلوك المستهلكين وتجميع المعلومات المتعلقة بخدمات العملاء لتحسين تجربتهم وتطبيق استراتيجيات التسويق الإلكتروني لتعزيز الوصول إلى الأسواق .إلا أن الهجمات السيبرانية على هذا القطاع تشكل تهديدًا كبيرًا حيث يمكن أن تترتب عليها آثار سلبية خطيرة فقد يفقد المدنيون فرص عملهم وقد تتعطل العمليات الاقتصادية بين المناطق المختلفة داخل الدولة مما يؤدي إلى حالة من عدم الاستقرار بالإضافة إلى ذلك فإن عمليات الاحتيال في تحويل الأموال عبر الوسائل السيبرانية وسرقة الأرصدة قد تسهم في تفاقم الأزمات الاقتصادية بتالي تبرز الحاجة الملحة إلى تعزيز الأطر القانونية والتنظيمية لحماية هذا القطاع الحيوي والحفاظ على استقراره. (العتيبي، عبد الرحمن بجاد شاهر. "دور الأمن السيبراني في تعزيز الأمن

الإنساني." جامعة نايف العربية للعلوم الأمنية، كلية العلوم الاستراتيجية (قسم الأمن الإنساني)، رسالة ماجستير ، إشراف الدكتور: جارق محمد سليمان، 2017، ص62.)

ثالثآ: اثر الهجمات السيبرانية على المجال السياسي

تستند الأبعاد السياسية للأمن السيبراني إلى ضرورة حماية النظام السياسي للدولة وكيانها المؤسسي. في هذا السياق، يمكن أن تُستخدم التقنيات الرقمية لنشر معلومات وبيانات قد تؤدي إلى زعزعة استقرار الأمن الوطني. تُتيح هذه التقنيات إمكانية وصول المعلومات بسرعة فائقة إلى شريحة واسعة من المواطنين، مما يثير القلق بشأن دقة وموثوقية البيانات المتداولة. وبالتالي،فإن التدخل السيبراني لروسيا في الانتخابات الأمريكية هو أهم دليل على الحاجة إلى الأمن السيبراني وأهميته في البعد السياسي مما يصعب التحديات التي تطرحها هذه الظاهرة والتي تتطلب استراتيجيات فعّالة للتصدي للمعلومات المضللة وتعزيز الأمن السيبراني لحماية استقرار الدولة ومؤسساتها.(السمحان، مني عبدالله ،متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية ، جامعة المنصورة ، العدد 111، يوليو2020.)

رابعآ: اثر الهجمات السيبرانية على البعد الاجتماعي

تشير الإحصائيات إلى أن هناك أكثر من 4 مليارات مستخدم للإنترنت على مستوى العالم، مع استخدام أكثر من 2.6 مليار شخص لمواقع الشبكات الاجتماعية. وتُعد هذه المنصات من بين أعلى وسائل التفاعل البشري، مما يوفر فرصًا كبيرة لتبادل الأفكار والتجارب الناجحة. ومع ذلك، فإنها تكشف أيضًا عن أخلاقيات الأفراد وسلوكياتهم.

وتُعَدّ صعوبة الرقابة على محتوى الإنترنت تهديدًا ليس فقط للمجتمعات، بل أنها تعرض المعلومات الشخصية لخطر الاستخدام غير مشروع من قِبل الجهات الخارجية. بالتالي فان هذا الوضع يهدد السلم الاجتماعي في البلدان، ويعكس صورة فقدان الأمن السيبراني الاجتماعي، لذا، تسعى الدول خصوصا في هذا المجال الى حماية البيانات الشخصية وضمان سلامة المعلومات للحفاظ على استقرار المجتمعات وأمنها.(دور الذكاء الاصطناعي في تعزيز الأمن السيبراني: رؤى نظرية رابط www.mecsj.com)

خامسآ: الاثار الناشئة عن الهجمات السيبرانية في المجال البيئي

تُعتبر الهجمات السيبرانية تهديدًا جسيمًا للبيئة، حيث تُستخدم أنظمة الاستشعار عن بُعد ونظم المعلومات الجغرافية كأدوات حيوية في حماية البيئة. حيث تؤدي هذه الأنظمة دورًا مركزيًا في دراسة تلوث المياه والهواء وسطح الأرض من خلال تحليل صور الأقمار الصناعية المعالجة بواسطة أجهزة الكمبيوتر.

وتقدم هذه التقنيات في تحديد مصادر التلوث ومراقبة انتشاره، خصوصًا خلال حدوث تلوث محددة. كما تتيح دراسة تركيز التلوث وسرعة جريانه وتدفقه، مما يتيح تفاعلًا سريعًا مع الأحداث البيئية. إضافةً إلى ذلك، فإن أجهزة قياس الإشعاع المتناهي الدقة تُعزز القدرة على الكشف عن تسرب النفط والبقع الزيتية، مما يُساعد في تنفيذ استراتيجيات فعّالة للتقليل من الأضرار.

إن أهمية التكنولوجيا في حماية البيئة من التلوث وضمان استدامتها تتجلى بوضوح. ومع ذلك، فإن أي هجوم سيبراني على هذه الأنظمة يمكن أن يؤدي إلى آثار مدمرة، مما يُعرض سلامة النظام البيئي للخطر

ويستدعي الحاجة الملحة لتعزيز الأطر القانونية والتنظيمية اللازمة لحماية هذه الأنظمة الحيوية.(العتيبي، عبد الرحمن بجاد. "دور الأمن السيبراني في تعزيز الأمن الإنساني."مرجع سابق،ص66.)

وفي ضوء ماتقدم نرى بضرورة تفعيل البرامج الالكترونية المخصصه لصد الهجمات السيبرانية للحفاظ على امن واستقرار المجتمعات من جهة ولتقدير السلام الدولي من جهة اخرى ، ولا سيما وان المجتمع الدولي يشهد حرب سيبرانية خطيرة وكبيرة والتي تتطلب على اقل تقدير التصدي لها عبر البرامج والوسائل السيبرانية ومن النوع ذاته ،للحد من الاثار السلبية الناجمة عن تلك الحروب الفتاكة والمروعة .

المبحث الثاني

اليات التصدي للهجمات السيبرانية

تُعد الهجمات السيبرانية في الوقت الراهن إحدى الجرائم ذات الطابع العابر للحدود، والتي تشكّل تهديدًا جسيمًا لأمن وسلامة المجتمع الدولي. مما يستدعي تعزيز التعاون الدولي وتبني إطار قانوني متين لمواجهتها بشكل فعال. وعليه، تعمل الدول على تكثيف الجهود الرامية إلى مكافحة هذه الظاهرة، من خلال وضع استراتيجيات دولية شاملة ومتكاملة لضمان الحد من انتشارها وتأثيراتها السلبية.

وتتمثل هذه الجهود في إبرام الاتفاقيات والمعاهدات الدولية والإقليمية التي يتم التفاوض عليها وإقرارها تحت إشراف المنظمات الدولية المختصة.

وسوف نوضح اليات الدولية في هذا الشأن، بالإضافة إلى المساهمات الفقهية بشأن المخاطر السيبرانية، وذلك من خلال مبحثين على النحو التالي:

المطلب الأول: اليات التصدي الدولية بشأن تنظيم العمليات السيبرانية.

المطلب الثاني: الاليات الفقهية لمواجهة المخاطر السيبرانية.

المطلب الاول

آليات التصدي الدولية لمواجهة الهجمات السيبرانية

يواجه المجتمع الدولي تحديات متزايدة في مجال الأمن السيبراني، حيث تتطور الهجمات الإلكترونية وتزداد تعقيدًا. لذلك، تتضافر الجهود الدولية لمكافحة هذه المخاطر وحماية الأفراد والمؤسسات من التهديدات السيبرانية.

منظمة الامم المتحدة

تضطلع العديد من المنظمات، وعلى رأسها منظمة الأمم المتحدة، بدور محوري في تعزيز التعاون الدولي، وذلك في إطار مواجهة التحديات المرتبطة بالجرائم المعلوماتية والمخاطر السيبرانية. وفي هذا السياق، قامت الأمم المتحدة بتنظيم سلسلة من المؤتمرات الهامة، بدءًا من المؤتمر السابع الذي عُقد في ميلانو عام 1985، وانتهاءً بالمؤتمر الثاني عشر الذي انعقد في عام 2010. كما شهد عام 1994 انعقاد المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات تحت إشراف المنظمة، مما أتاح منصة لمناقشة القضايا القانونية المتعلقة بالجرائم المعلوماتية.

حيث أسفرت هذه المؤتمرات عن إصدار مجموعة من التوصيات ذات الصلة بجرائم المعلومات، وتناولت بعض هذه التوصيات الأفعال التي تُصنف ضمن الإجرام المعلوماتي، بينما تمحورت توصيات أخرى حول الإجراءات الواجب اتباعها لتطبيق القواعد الموضوعية بشكل فعّال (د. هاني محمد خليل العزازي - النظام القانوني الدولي لمكافحة الجرائم السيبرانية ،مصر المعاصرة ، عدد 549،يناير 2023)

علاوة على ذلك، أصدرت منظمة الأمم المتحدة عدة قرارات وتوصيات تتعلق بالعمليات السيبرانية، كما قامت بتشكيل فرق من الخبراء الحكوميين المتخصصين في هذا المجال. بالإضافة إلى ذلك، ناقشت هيئات الأمم المتحدة قضايا أمن الفضاء السيبراني. والتي سنبينها في ثلاثة فروع وكالاتي :-

الفرع الاول

قرارات ووثائق الجمعية العامة للأمم المتحدة المتعلقة بالإرهاب السيبراني.

أصدرت الجمعية العامة للأمم المتحدة عدة قرارات بشأن جرائم الإرهاب السيبراني. من بين هذه القرارات القرار رقم 55/63 الذي صدر في الرابع من ديسمبر عام 2000 والقرار رقم 56/121 الذي صدر في التاسع عشر من ديسمبر عام 2001 والمتعلق بمكافحة سوء استخدام تكنولوجيا المعلومات.

أوصى القرار الأول بأن تضمن الدول في قوانينها وممارساتها عدم توفير ملاذات آمنة لمن يسيء استخدام تكنولوجيا المعلومات. كما دعا إلى ضرورة حماية سرية المعلومات وسلامة أنظمة الحاسوب ضد أي اعتداء غير مشروع مع تقرير عقوبة على هذا الفعل. أما القرار 56/121 فقد دعا الدول الأعضاء عند وضع التشريعات الوطنية لمكافحة إساءة استعمال تكنولوجيا المعلومات إلى أخذ بعين الاعتبار عمل لجنة منع الجريمة والعدالة الجنائية.(56/121 قرار الجمعية العامة الأمم المتحدة 2001)

وفي عام 2002، أصدرت الأمم المتحدة القرار رقم 57/239 بشأن إرساء ثقافة عالمية للأمن السيبراني، حيث اعتمدت فيه قراراً يتعلق بالأمن السيبراني الذي أكد على ضرورة دعم الجهود الوطنية من خلال تبادل المعلومات والتعاون في هذا المجال على الأصعدة الوطنية والإقليمية والدولية.(57/239 ، الأمم المتحدة ،ثقافة الامن السيبراني 2002)

يهدف هذا التعاون إلى التصدي الفعال للتهديدات السيبرانية التي تتسم بطابع عابر للحدود الوطنية. كما يعكس هذا القرار التزام العالم بإنشاء ثقافة عالمية للأمن السيبراني. وأكد القرار على أن الأمن السيبراني للهيكل الأساسي الحيوي للمعلومات هو مسؤولية ملقاة على عاتق الحكومات، ويجب عليها أن تحمل لواء الصدارة وطنياً بالتنسيق مع أصحاب المصلحة ذوي الشأن.

وفي عام 2005، أصدرت الأمم المتحدة القرار رقم 177/60. الذي دعا إلى تعزيز التعاون الدولي في مجال مكافحة الجرائم الإلكترونية، وتقديم الدعم والمساعدة التقنية للدول الأعضاء لتعزيز قدراتها في هذا المجال. كما أكد القرار على أهمية تبادل الخبرات والمعلومات بين الدول لمواجهة التحديات المتزايدة الناجمة عن الجرائم الإلكترونية.

واستمراراً لتلك الجهود ففي عام 2010، أصدرت الأمم المتحدة القرار رقم 211/64، الذي حث الدول الأعضاء على تحديث تشريعاتها الوطنية في مجالات الجرائم الإلكترونية، وحماية الخصوصية،

وإدارة البيانات الشخصية، والتوقيع الإلكتروني. كما شجع القرار الدول على اعتماد اتفاقيات إقليمية ودولية لتعزيز الأطر القانونية والتعاون في مواجهة التهديدات الإلكترونية العابرة للحدود.

وقد جاءت هذه القرارات في إطار الجهود الدولية المستمرة لتعزيز الأمن السيبراني، ومواكبة التطورات التكنولوجية السريعة، وضمان توافق التشريعات الوطنية مع المعايير الدولية في مجال مكافحة الجرائم الإلكترونية وحماية حقوق الأفراد والشركات في الفضاء الرقمي.(Schjolberg, S. (2008). The Global History of Cybercrime Legislation: Harmonization Efforts. Available at: (http://www.cybercrimelaw.net) www.cybercrimelaw.net)

الفرع الثاني

توصيات المجلس الاقتصادي والاجتماعي.

قام المجلس الاقتصادي والاجتماعي بافتتاح دورته لعام 2010 بجلسة إعلامية تناولت التحديات التي يفرضها الأمن السيبراني، وكذلك التهديدات والفرص التي يوفرها الاستخدام المتزايد للإنترنت. وقد أكد المجلس، ضمن عدة نقاط، على ضرورة تبني مبادرات دولية تهدف إلى تعزيز تبادل المعلومات، ونشر أفضل الممارسات، وتنظيم برامج تدريبية، ودعم الأبحاث في هذا المجال.

كما أشار المشاركون في المناقشة إلى أن على الأمم المتحدة أن تعزز من أدائها وتنسيق جهودها فيما يتعلق بقضية الأمن السيبراني، مما سيسهم حتمًا في تعزيز التعاون ليس فقط بين الدول، بل أيضًا بين الحكومات والقطاع الخاص. وتم التأكيد على أن هذا التعاون يُعد أمرًا وجوبياً لضمان تحقيق الأمن السيبراني الفعال على المستوى العالمي.(المجلس الاقتصادي والاجتماعي، الدورة الموضوعية لعام 2010، نيويورك، 28 يونيو - 23 يوليو 2010، البند 13 (ب) من جدول الأعمال المؤقت، المسائل الاقتصادية والبيئية: تسخير العلم والتكنولوجيا لأغراض التنمية والتقدم المحرز في تنفيذ ومتابعة نتائج مؤتمر القمة العالمي لمجتمع المعلومات على الصعيدين الإقليمي والدولي.)

وفي ضوء التحذيرات من النطاق الدولي للحرب السيبرانية، يجب الإشارة إلى العواقب الوخيمة التي قد تترتب على هذا التهديد، والتي قد تؤثر بشكل خطير على الأمن والاستقرار العالمي. لذا، يتعين أن تكون هناك استجابة منسقة بين الدول لمواجهة هذه التحديات. إذا لم يتم تدارك الأمر بشكل عاجل، فإن الاعتماد على استراتيجيات مخصصة وحلول فردية لن يكون كافيًا. فمن الضروري تعزيز تدابير الدفاع السيبراني وتطوير آليات فعالة للتعاون الدولي في هذا المجال؛ لضمان حماية الأمن السيبراني على المستوى العالمي. (المصدر نفسه: مناقشة "الأوراق المالية الرقمية" أو النظام النقدي الرقمي المستخدم في البلدان الإفريقية)

كما دعا القرار الالتزام من دول الأعضاء باعتماد نهج قائم على إدراك المخاطر، وذلك لضمان إحاطة جميع أصحاب المصلحة بالمخاطر ذات الصلة، والتدابير الوقائية، والاستجابات الفعالة، كلٌ وفقًا للدور المنوط به. ويؤكد القرار على أن الجهود الوطنية يجب أن تُوجَّه بشكل إلزامي نحو حماية البنية التحتية الحيوية للمعلومات، مع ضرورة إجراء تقييم دوري لقياس التقدم المحرز في تنفيذ هذه الجهود.

وطالب القرار الدول ببذل المزيد من العناية بموضوع الأمن الإلكتروني، حيث يدعو الدول الأعضاء إلى تقديم التقارير الموجزة عن مبادراتها الرئيسية في مجال الأمن السيبراني وحماية البنية التحتية الحيوية للمعلومات. وذلك بهدف إبراز الإنجازات المحققة، وأفضل الممارسات، والدروس ذات الفائدة، والإجراءات التي تتطلب تعزيزًا إضافيًا على المستوى الوطني. ويشجع القرار على إجراء تقييم ذاتي طوعي للأمن الإلكتروني الوطني، باعتباره أداة فعالة لمساعدة الدول على مراجعة الجهود الوطنية المبذولة في مجال الأمن السيبراني وحماية البنية التحتية الحيوية للمعلومات. (عبد الجواد، أميرة عبد العظيم محمد. 2020. المخاطر السيبرانية و سبل مواجهتها في القانون الدولي العام. مجلة البحوث الفقهية و القانونية،مج. 2020)

بتالي اصحبت الحاجة ملحه الى عقد اجتماع باقصى سرعة ففي سبتمبر عام 2011، وقد تتبع عن عقد المجلس الاقتصادي والاجتماعي للأمم المتحدة اجتماعًا لمناقشة أمن الفضاء الإلكتروني والتنمية، بالإضافة إلى القضايا والتحديات ذات الصلة. وقد شاركت هذه المناقشات في إدارة الشؤون الاقتصادية والاجتماعية، والاتحاد الدولي للاتصالات، ورئيس لجنة الأمم المتحدة المعنية بتسخير العلم والتكنولوجيا لأغراض التنمية، إلى جانب ممثلين عن منظمة الأمم المتحدة والقطاعين العام والخاص، بالإضافة إلى تفعيل التعاون مع منظمات المجتمع المدني المهتمة بمجالات الفضاء السيبراني والهجمات الإلكترونية على مستوى السياسات الدولية.

وقد خلص الاجتماع الى تحديد أهدافًا رئيسية تتمثل في تزويد أعضاء المجلس بصورة شاملة عن الوضع الحالي والتحديات المتعلقة بأمن الفضاء الإلكتروني، وارتباط ذلك بالتنمية المستدامة. كما تم التركيز على تحديد أفضل السياسات المتعلقة بهذا المجال، والمبادرات المطبقة في مختلف أنحاء العالم، بهدف بناء ثقافة أمن الفضاء السيبراني، واستكشاف خيارات للاستجابة العالمية تجاه تزايد معدلات الهجمات السيبرانية.

وكذلك فقد قرر"زاروس كابامبي"، رئيس المجلس الاقتصادي والاجتماعي، أن أعضاء الاجتماع قد اتفقوا على أن الأمن السيبراني يمثل قضية عالمية لا يمكن معالجتها إلا من خلال شراكة دولية فعالة، ولا سيما عبر الأمم المتحدة، التي يمكنها استخدام قدراتها الاستراتيجية والتحليلية لمعالجة مثل هذه القضايا المعقدة.(د. محمد عادل محمد عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسس وقت السلم: دراسة على ضوء دليل "تالين" بشأن القانون الدولي المطبق على العمليات السيبرانية 2013-2017، 2020م، ص: 63.)

الفرع الثالث

تأسيس مجموعة من الخبراء الحكوميين المختصين في العمليات السيبرانية.

في عام 2004، أنشأت الجمعية العامة للأمم المتحدة مجموعة من الخبراء الحكوميين بهدف دراسة تأثير التطورات في تكنولوجيا المعلومات والاتصالات على الأمن القومي والشؤون العسكرية للدول. واختتم المؤتمر أعماله بإصدار تقرير شامل تضمن مجموعة من التوصيات الهامة في هذا الصدد.

وقد واصل الفريق عقد اجتماعاته بشكل سنوي، حيث ناقش خلالها القضايا المتعلقة بالتهديدات السيبرانية التي تواجه الأمن والاستقرار الدوليين. وفي عام 2010، أصدر الفريق تقريرًا سلط فيه الضوء

على المخاطر الناجمة عن عدم وجود توجيه دولي موحد بشأن العمليات السيبرانية للدول، مؤكدًا أن هذا النقص قد يؤدي إلى أضرار كبيرة. كما تضمن التقرير مجموعة من التوصيات، أهمها:

1_مواصلة تعزيز الحوار بين الدول:

فقد اوصى المجلس بمواصلة عقد الحوارات بين الدول لبحث ودراسة المعايير الدولية المتعلقة باستخدام تكنولوجيا المعلومات والاتصالات، وذلك بهدف الحد من المخاطر الناجمة عن سوء استخدام هذه التكنولوجيا، وحماية البنية التحتية الإلكترونية للدول من التهديدات السيبرانية.

٢_تعزيز تدابير بناء الثقة. اذ انه اوصى بالسعي نحو تطبيق تدابير فعالة لبناء الثقة بين الدول في مجال تقليل المخاطر المرتبطة باستخدام تكنولوجيا المعلومات والاتصالات. وذلك من خلال تشجيع تبادل الآراء والخبرات الوطنية بين الدول حول أفضل الممارسات والضوابط المتعلقة باستخدام هذه التكنولوجيا، بما يعزز الشفافية والتعاون الدولي.

٣_يُعتبر تبادل المعلومات المتعلقة بالتشريعات الوطنية والبيانات السيادية، فضلاً عن الاستراتيجيات والتقنيات والسياسات المعنية بأمن الاتصالات، إلى جانب أفضل الممارسات المعتمدة في هذا المجال، من العناصر الجوهرية التي تسهم في تعزيز منظومة الأمن السيبراني. مما يعزز لنا ان هذا التبادل بمثابة ركيزة أساسية لتعزيز التعاون بين الأطراف المعنية، بما يكفل تحقيق أعلى معايير الحماية للأصول الرقمية والبنى التحتية المعلوماتية، وذلك في إطار الالتزام بالقوانين والأنظمة الوطنية والدولية ذات الصلة.

٤_كما يجب تحديد تدابير واضحة لدعم تطوير القدرات في الدول الأقل نمواً، بما يشمل توفير التدريب والموارد اللازمة، لضمان قدرتها على مواجهة التحديات السيبرانية بشكل فعّال.

في ضوء ماتقدم تعدهذه الجهود جزءاً من التزام عالمي نحو تعزيز الأمن السيبراني وبناء بيئة رقمية آمنة ومستدامة.

وهنا تجدر الاشارة الى جهود مجموعة الخبراء الحكومية (GGE) حول تقريرها لعام 2015 والذي تضمن (11) توصية رئيسية تهدف إلى تعزيز الأمن والاستقرار في الفضاء السيبراني. ومن أبرز هذه التوصيات:

1_تطبيق القانون الدولي على الفضاء السيبراني:-

أكدت التوصيات على ضرورة تطبيق مبادئ القانون الدولي، بما في ذلك مبادئ سيادة الدول وعدم التدخل في الشؤون الداخلية، على الأنشطة التي تتم في الفضاء السيبراني.

2_حماية البنية التحتية الإلكترونية:- فقد شددت التوصيات على أهمية تجنب استهداف البنية التحتية الإلكترونية للدول أو دعم أي أنشطة مرتبطة بذلك، مع التأكيد على أن مثل هذه الأعمال تُعد انتهاكًا للقواعد الدولية.

٣_مسؤولية الدول عن الهجمات السيبرانية:- أقرت التوصيات بمسؤولية الدول عن الهجمات السيبرانية التي تنطلق من أراضيها، ودعت إلى اتخاذ التدابير اللازمة لمنع ومعالجة مثل هذه الحوادث.

على الرغم من أن التوصيات ذات طبيعة طوعية وغير ملزمة قانونيًا، إلا أنها تُعتبر خطوة مهمة نحو تطوير إطار معياري دولي متفق عليه لتنظيم الفضاء السيبراني وتعزيز التعاون بين الدول في هذا المجال.(د. محمد عادل محمد عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسس وقت السلم: دراسة على ضوء دليل "تالين" بشأن القانون الدولي المطبق على الهجمات السيبرانية ،مصدر سبق ذكره .)

المطلب الثاني

الاليات الفقهية لمواجهة المخاطر السيبرانية

ظهرت اجتهادات فقهية حديثة تهدف إلى معالجة إشكالية الهجمات السيبرانية، ومن أبرزها "إعلان ريتشي" الذي صدر عن الاتحاد العالمي للعلماء، والذي يضع مبادئ أساسية لتحقيق الاستقرار السيبراني والسلم السيبراني. بالإضافة إلى ذلك، يُعد "دليل تالين" للقانون الدولي المنطبق على الفضاء السيبراني مرجعًا مهمًا في العمليات السيبرانية، حيث يساهم في تطوير إطار قانوني متكامل لمواجهة التحديات الناشئة عن الهجمات السيبرانية.

حيث سنستعرض بعض من نماذج الاليات الفقهية التي بُذلت لمعالجة إشكالية الهجمات السيبرانية، وذلك من خلال ثلاثة فروع الاول نستعرض به. **إعلان ريتشي"** بشأن مبادئ الاستقرار السيبراني والسلم السيبراني، الذي صدر عن الاتحاد العالمي للعلماء. وكذلك ،سنبين في الفرع الثاني **"دليل تالين"** للقانون الدولي المنطبق على الفضاء السيبراني.و نخصص في الفرع الثالث **" لمبدأ مارتنز"** والذي جاء بخصوص الحالات التي لا تغطيها القوانين أو الاتفاقيات الدولية.

الفرع الاول

اعلان ريتشي

أصدر فريق الرصد الدائم المعني بأمن المعلومات التابع للاتحاد العالمي للعلماء، إعلانًا اعتمدته الجلسة العامة للاتحاد خلال الدورة الثانية والأربعين للحلقات الدراسية الدولية بشأن الطوارئ العالمية في إيريتشي (صقلية) بتاريخ 20 أغسطس 2009. وقد نشر فريق الرصد العديد من الأوراق المتعلقة بالأمن السيبراني والحرب السيبرانية، حيث يتناول بانتظام قضايا أمن المعلومات كموضوع من الموضوعات ذات الأولوية خلال الدورات العامة للاتحاد التي تعقد سنويًا في أغسطس بإيريتشي.(في عام 1973، قام مجموعة من العلماء البارزين بإنشاء الاتحاد العالمي للعلماء في إيريتشي بجزيرة صقلية. منذ ذلك الحين، انضم عدد كبير من العلماء الآخرين إلى الاتحاد، الذي شهد نموًا ملحوظًا ليضم أكثر من 1000 عالم من 110 دول. يتقاسم الأعضاء الأهداف والمبادئ، ويسهمون طواعية في الدفاع عنها، كما يشجع الاتحاد على التعاون الدولي في مجالات العلم والتكنولوجيا بين العلماء والباحثين من مختلف أنحاء العالم.يهدف الاتحاد وأعضاؤه إلى تحقيق حرية تبادل المعلومات كهدف مثالي، بحيث لا تقتصر الاكتشافات والتقدمات العلمية على قلة مختارة. يسعى الاتحاد إلى توزيع هذه المعارف بين شعوب جميع الدول، لتمكين الجميع من فوائد تقدم العلم.تم إنشاء الاتحاد بفضل مركز الثقافة العلمية الذي يحمل اسم "جامعة إيتوري مايورانا"، والذي يُعرف أيضًا بمؤسسة إيتوري مايورانا ومركز الثقافة العلمية. منذ تأسيسه في عام 1963، أصبح هذا

المركز قوة تعليمية عالمية، حيث نظم 123 مدرسة و1497 دورة دراسية، حضرها أكثر من 484 ألف مشارك، من بينهم 125 من الحاصلين على جائزة نوبل، من 923 جامعة ومختبرًا في 140 دولة.)

ويؤكد هذا الإعلان على أن تحقيق الاستقرار السيبراني والسلام السيبراني هما مسألتان متداخلتان بشكل وثيق، ويستعرض بشكل موجز العناصر التشغيلية الأساسية التي تعزز السلام السيبراني للفضاء الالكتروني وهي مفصلة في النقاط التالية:-

١_ ينبغي على جميع الحكومات الاعتراف بأن القانون الدولي يضمن للأفراد حق التدفق الحر للمعلومات والأفكار، حيث تنطبق هذه الضمانات بشكل كامل على الفضاء السيبراني. ويجب ايضا ان لا تُفرض أي قيود على هذا الحق إلا في حالات الضرورة القصوى، شريطة أن تكون هذه القيود محددة، وأن تخضع لعملية مراجعة قضائية وقانونية تضمن احترام المبادئ ، بما يتوافق مع المعايير الدولية لحقوق الإنسان.

٢_ ينبغي على جميع الدول التعاون من أجل وضع مدونة سلوك سيبراني مشتركة، وإيطار قانوني دولي منسق، يشمل أحكامًا إجرائية تتعلق بالتحقيق والتعاون في مجال الأمن السيبراني، مع ضمان احترام الخصوصية وحقوق الإنسان. كما يتعين على جميع الحكومات دعم الجهود الرامية إلى إنفاذ القانون الدولي، وتوفير الحماية اللازمة لمقدمي الخدمات والمستخدمين، ومكافحة الجرائم السيبرانية بشكل فعال.

٣_ من الضروي على جميع المستخدمين ومقدمي الخدمات والحكومات أن يتعاونوا بشكل فعال لضمان ألا يُستخدم الفضاء السيبراني بأي شكل من الأشكال والتي تفضي إلى استغلال المستخدمين، وخاصة الفئات الأكثر عرضة للخطر مثل الشباب والأفراد المستضعفين، سواء من خلال ممارسات العنف أو الإذلال أو أي انتهاكات أخرى لحقوقهم.

٤_ يجب على الحكومات المشاركة الفاعلة في جهود الأمم المتحدة لتعزيز الأمن والسلم السيبراني على المستوى الدولي، وذلك من خلال دعم المبادرات والآليات التي تهدف إلى منع استخدام الفضاء السيبراني كوسيلة لتصعيد النزاعات أو التهديدات الدولية.

٥_ يتعين على مطوري البرمجيات ومصنعي المعدات السعي إلى تصميم وتطوير تكنولوجيات آمنة تكون قادرة على مقاومة نقاط الضعف والتصدي للتهديدات السيبرانية بشكل فعال، بما يضمن تعزيز الأمن والحماية في الفضاء السيبراني.

٦_ من الملزم على الحكومات والمنظمات والقطاع الخاص، بما في ذلك الأفراد، الالتزام بتنفيذ برامج شاملة للأمن السيبراني وتحديثها بشكل دوري، بما يتماشى مع أفضل الممارسات الدولية والمعايير المتعارف عليها عالمياً. يتعين أيضًا استخدام تكنولوجيات حماية الخصوصية وتعزيز تدابير الأمن لضمان سلامة البيانات والمعلومات وحمايتها من المخاطر المحتملة.

وقد اوصى الاتحاد العالمي للعلماء منذ عام 2002 إلى العمل على وضع قانون عالمي للفضاء السيبراني، مع التأكيد على أن يكون هذا القانون تحت رعاية الأمم المتحدة، وذلك لضمان تنظيم استخدام الفضاء السيبراني بشكل عادل وفعال، وخاصة في ما يتعلق بالاستخدامات العدوانية والعسكرية التي قد تشكل تهديدًا للسلم والأمن الدوليين.(Toward a Universal order of Cyberspace managing Threats from Cybercrime of Cyberya

تقرير وتوصيات فريق الرصد الدائم المعني بمجتمع المعلومات والتابع التحاد العلماء العالمي، ١٩ نوفمبر ٢٠٠٢، تقرير مقدم إلى القمة العالمية لمجتمع المعلومات http://www.itu.int/dms/pub/itu-s/md./pdf

الفرع الثاني

دليل تالين

تم إعداد هذا الدليل من قبل مجموعة من خبراء القانون الدولي عام ٢٠١٣، بدعوة من منظمة حلف شمال الأطلسي (الناتو)، وبحضور اللجنة الدولية للصليب الأحمر (CICR). يتألف هذا الدليل من وثيقة موحدة تحكم هذه الاعتداءات التي تتم بين الدول، حيث اعتبرت وثيقة قانونية غير ملزمة تنظم قواعد الاشتباك عبر الإنترنت(نسيم ،شريف ،دليل "تالين":الهجمات الإلكترونية وحظر استخدام القوة فى القانون الدولي ،المركز العربي للابحاث الفضاء الالكتروني ،جامعة القاهرة ،2017 .) وقد صدرت منها نسختان :

_**النسخة الاولى كانت في عام(2013)** :والتي تتكون من **95 قاعدة قانونية**، ويركز على الهجمات السيبرانية، مسلطًا الضوء على خطورة تلك الهجمات التي تنتهك حظر استخدام القوة في العلاقات الدولية. كما يخول الدول ممارسة حق الدفاع عن النفس، ويتعلق بالهجمات التي تحدث أثناء النزاع المسلح، حيث تطبق عليها قواعد القانون الدولي الإنساني.

_**اما النسخة الثانية كانت في عام (2017)**، المعروف باسم (Tallinn 2.0): يتكون من **154 قاعدة قانونية**، ويركز على الوضع القانوني لمختلف أنواع القرصنة والهجمات السيبرانية الأخرى التي تحدث يوميًا في وقت السلم، والتي تقل عن عتبة استخدام القوة أو النزاع المسلح. ويتناول القضايا التي تعتبر فيها الهجمات انتهاكًا للقانون الدولي في الفضاء السيبراني. (خليل، بشار. "ما هي الحرب السيبرانية؟ مستقبل مخيف للصراع الرقمي." مجلة المعلوماتية، العدد 154، شهر آب، الجمعية السورية للمعلوماتية، 2020. متاح على الرابط: http://www.scs.org.sy/?q=scs/)

حيث تجسَّد هذا المفهوم بوضوح في توظيف الهجمات السيبرانية كأداة للصراع المسلح، كما حدث خلال النزاع بين جورجيا وروسيا في أغسطس 2008، وكذلك في الهجوم السيبراني العالمي المعروف بـ"فيروس الفدية"، الذي استهدف في 27 يونيو أكثر من 60 دولة، من بينها المملكة المتحدة، ومصر، وروسيا، وأوكرانيا، وألمانيا، والمكسيك، وإسبانيا. وقد أدى ذلك إلى بروز الفضاء السيبراني كساحة جديدة للنزاعات الدولية، مما أثار تساؤلات قانونية حول مدى إمكانية تصنيف هذه الهجمات كأعمال عدائية تدخل ضمن مفهوم النزاع المسلح بموجب القانون الدولي.

وبالنظر إلى أن الهجمات السيبرانية قد تسفر عن أضرار تماثل تلك الناجمة عن الهجمات التقليدية، رغم اختلاف الأدوات وطرائق التنفيذ، فإن ذلك يساهم في نشوء نمط من الحروب غير التقليدية، التي قد يكون من الصعب تحديد الفاعلين المسؤولين عنها بدقة. واستجابة لهذه التحديات، تسعى الدول والمنظمات الدولية إلى تطوير أطر قانونية ومعايير تقنية لتصنيف الهجمات السيبرانية، وتحديد الظروف التي يمكن أن ترفعها إلى مستوى "الهجوم المسلح"، على نحو يستوجب تطبيق أحكام المادة 51 من ميثاق الأمم المتحدة، والتي تكرّس الحق في الدفاع الشرعي عن النفس في حال وقوع عدوان مسلح. (د. محمد عادل محمد عسكر،

وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسس وقت السلم، المرجع السابق،ص٧١.)

ومن الجدير بالذكر أن هذا الدليل يعكس رؤية الخبراء المستقلين الذين قاموا بصياغته بصفتهم الشخصية. ورغم ذلك، فإنه يُعد وثيقة رائدة في مجال العمليات السيبرانية وخطوة مهمة نحو تنظيم الفضاء السيبراني، وإن كانت غير كافية، مما يستلزم اتخاذ مزيد من الخطوات لاستكمال هذا التنظيم.(د.هاني محمد خليل العزازي - النظام القانوني الدولي لمكافحة المخاطر السيبرانية ،مرجع سابق.)

الفرع الثالث

مبدأ مارتنز

تعود تسمية "مارتنز" إلى الدبلوماسي الروسي فيدور فيودو وفيتش مارتنز، الذي كان أحد الممثلين الروس في مؤتمر السلام المنعقد عام 1899. وقد أدلى مارتنز ببيان مهم خلال هذا المؤتمر، **حيث أشار إلى أنه في الحالات التي تفتقر إلى أحكام قانونية واضحة، فإن السكان المتحاربين يظلون تحت حماية وسلطة مبادئ قانون الأمم**. هذه المبادئ، استقرت في تقاليد الشعوب المتحضرة، وتُعد جزءًا من متطلبات الضمير والقوانين الانسانية .

وبناءً عليه، يعكس هذا التصريح أهمية الالتزام بمبادئ العدالة الإنسانية في سياق النزاعات المسلحة، ويؤكد على ضرورة حماية الحقوق الأساسية للأفراد، حتى في غياب نصوص قانونية محددة. (زهراء عماد محمد كلنتر ،المسؤولية الدولية الناشئة عن الهجمات السيبرانية،رسالة ماجستير ،جامعة الكوفة ،٢٠١٦،ص٧٧.)

وقد ورد هذا المبدأ في مقدمات اتفاقيات لاهاي لعامي 1899 و1907، المتعلقة بقواعد وأعراف الحرب البرية، كما تم تضمينه في اتفاقيات جنيف لعام 1949، بالإضافة إلى إدراجه في البروتوكول الإضافي الأول لعام 1977. حيث نصت الفقرة الثانية من المادة الأولى من البروتوكول الإضافي الأول على أن: "يظل المدنيون والمقاتلون في الحالات التي لا ينص عليها في هذا البروتوكول، أو أي اتفاق دولي آخر، تحت حماية وسلطان مبادئ القانون الدولي، كما استقر عليها العرف، ومبادئ الإنسانية، وما يمليه الضمير العام." (نفس المصدر السابق، ص٧٨)

أما في سياق الهجمات السيبرانية، فيمكن الاستناد إلى ما أورده القاضي شهاب الدين في الرأي الاستشاري الصادر عن محكمة العدل الدولية عام 1996 بشأن استخدام الأسلحة النووية وشرعية التهديد بها، إذ أكد على أن "مبدأ مارتنز يمنح سلطةً قانونيةً لمعالجة مبادئ القانون الإنساني وما يمليه الضمير العام باعتبارهما جزءاً لا يتجزأ من مبادئ القانون الدولي، مع ترك تحديد معيار التطبيق لمبادئ القانون الدولي في ضوء المحتوى الدقيق للظروف المتغيرة، بما في ذلك التطورات في وسائل وطرق الحرب، فضلاً عن التغيرات في مستويات تطور المجتمع الدولي وقيمه الأخلاقية والتسامح السائد فيه. كما أشارت المحكمة في رأيها الاستشاري إلى أن **"مبدأ مارتنز قد أثبت فعاليته كأداة قانونية قادرة على مواجهة التطورات السريعة والمتلاحقة في مجال التكنولوجيا العسكرية**، مما يجعله آليةً حيويةً في تفسير وتطبيق قواعد القانون الدولي الإنساني، خاصةً في ظل التحديات المعاصرة التي تفرضها الوسائل الحديثة للحرب، بما فيها الهجمات السيبرانية، والتي تتطلب مواءمةً مستمرةً بين المبادئ القانونية الراسخة والمستجدات التكنولوجية. (نفس المصدر السابق)

وفي السياق ذاته ، يؤكد إيركي كودار، وكيل وزارة الدفاع للشؤون القانونية والإدارية في جمهورية إستونيا، والمساهم في صياغة دستورها، على أن **"مبدأ مارتنز ينص على أنه في حالة عدم وجود نصوص واضحة في الاتفاقيات الدولية المعاصرة أو في العرف الدولي، تبقى المبادئ التقييدية التي يعتمد عليها قانون النزاعات المسلحة سارية المفعول في هذه الحالات.**(Kodar, Erki. "Applying the Law of Armed Conflict to Cyber Attacks: From the Martens Clause to Additional Protocol I." ENDC

Proceedings, vol. 15, 2012, p. 110.)

اذ تكمن الأهمية الجوهرية للصياغة المرنة لمبدأمارتنز في أنه لايعد مجرد آلية قانونية تم وضعها لسد الثغرات الناشئة عن الحالات التي لم يتم التنظيم الصريح لها في الاتفاقيات الدولية السابقة. بل إن هذا الشرط يُعد بمثابة ركيزة أساسية لفرضية قانونية راسخة، تهدف إلى ضمان تقييد أو منع استخدام الوسائل والأساليب العسكرية الحديثة التي قد تظهر في سياق النزاعات المسلحة، بما في ذلك تلك التي لم تكن متوقعة أو مُنظمة سابقاً. ويتم ذلك من خلال الاستناد إلى المبادئ الراسخة للقانون الدولي الإنساني،

والتي تشمل حماية القيم الإنسانية الأساسية والحفاظ على الضمير الإنساني الجماعي، مما يضمن استمرارية تطبيق هذه المبادئ في مواجهة التطورات التكنولوجية والمتغيرات المعاصرة في طبيعة وسائل وأساليب الحرب.(رسل علاء داود العكيدي، حيدر ادهم الطائي، أثر شرط مارتنز في التفسير التطوري للتكنولوجيا العسكرية الحديثة"دراسة تحليلية"،

المجلد ،14 العدد1، 2013 ،ص 105.)

ومن الامثلة على مبدأ مارتنز:-

1_حرب العراق عام 2003: استخدم مبدأ مارتنز للدعوة إلى معاملة الأسرى والمدنيين وفقًا لمبادئ الإنسانية، حتى في غياب اتفاقيات واضحة تحظر بعض الافعال العدوانية، مما يعكس أهمية هذا المبدأ في تعزيز الحماية الإنسانية.

٢_ **الهجمات السيبرانية**: في ظل التحديات الجديدة التي تطرحها الهجمات السيبرانية، يُستند إلى مبدأ مارتنز لتأكيد ضرورة حماية المدنيين والبنية التحتية الحيوية، رغم عدم وجود تنظيمات قانونية واضحة في هذا المجال.(https://sherloc.unodc.org/cld/en/education/tertiary/terrorism/module-6/index.html?lf_id=)

وخلاصة قولنا ،يُعد مبدأ مارتنز مبدأً احتياطيًا يُستند إليه في حال عدم وجود قاعدة تعاهدية صريحة تحظر استخدام أسلحة معينة، حيث يتماشى هذا المبدأ مع الأسس الراسخة للقانون الدولي الإنساني، ويعمل كآلية توجيهية تُطبق في الأوضاع الدولية التي تنشأ بشأن حظر أو تقييد استخدام الأسلحة التي لم يتم تنظيمها بشكل محدد في الاتفاقيات الدولية. وقد تم إقرار هذا الشرط بهدف سد الثغرات والعيوب التشريعية التي قد تظهر في الاتفاقيات الدولية المتعلقة بتنظيم استخدام الأسلحة، مما يوفر إطارًا قانونيًا يسمح بحظر أو تقييد استعمال أي سلاح يتنافى مع المبادئ الإنسانية العامة أو ما يفرضه الضمير الإنساني الجماعي.

وبذلك، يُشكل مبدأ مارتنز أداة قانونية جوهرية تُعزز من حماية القيم الإنسانية في سياقات النزاعات المسلحة، حيث يُسهم في تحقيق التوازن بين متطلبات الأمن القومي والدولي من جهة، وضرورة احترام المبادئ الإنسانية وحماية المدنيين من جهة أخرى. ويظل هذا المبدأ بمثابة ضمانة قانونية تُعزز التزام الدول

بمبادئ القانون الدولي الإنساني، حتى في ظل التطورات التكنولوجية والعسكرية التي قد تفرض تحديات جديدة على الساحة الدولية.

مما يتطلب ضمان احترام مبدأ مارتنز جهودًا متواصلة من الدول والمنظمات الدولية والمجتمع المدني.

الخاتمة

وبعد... ينتهي بنا المطاف في شأن بحثنا اليات التصدي للهجمات السيبرانية في ضوء القانون الدولي هذا الموضوع يشغل بال المهتمين بالهجمات السيبرانية، خاصة مع ظهور خطر جديد يهدد العالم بأسره في عصر تزايدت فيه المخاطر السيبرانية في جميع النواحي .

وقد خلصنا في نهاية دراستنا الى جملة من النتائج والتوصيات نسردها بالتفصيل التالي :-

النتائج:-

١_ تواجه بعض الدول الأعضاء في المجتمع الدولي، وبشكل خاص الدول النامية، مجموعة من المعوقات والصعوبات التي تضعف فعاليتها في التصدي للانتهاكات السيبرانية. لذا، يتعين على هذه الدول أن تُظهر إرادة ورغبة قوية في مواجهة هذه الانتهاكات والتصدي لها بفعالية.

2_ تُعد الهجمات السيبرانية من المفاهيم الحديثة التي لم يتم التوصل إلى تعريف دولي متفق عليه بشأنها حتى الوقت الراهن، مما يُصعّب عملية تكييفها وتحديد المسؤولية الدولية المتعلقة بها.

3_ تقع خطورة الهجمات السيبرانية على السلم والأمن الدوليين في كونها وسيلة قتال قادرة على التسلل إلى الأنظمة الإلكترونية المصممة لحماية المنشآت الحيوية والحساسة لدول أخرى، مثل محطات الطاقة النووية والسدود والمطارات. ويهدف ذلك إلى تخريب هذه الأنظمة والسيطرة عليها.

٤_ هناك جهود دولية في سبيل تنظيم الأنشطة السيبرانية كدليل تالين واعلان ريتشي ومبدأ مارتنز الا ان هذه الجهود ، لم تصل إلى مستوى تنظيم شامل لمواجهة هذه الهجمات.

5_ لقد أحدث الفضاء السيبراني تغييرات جذرية في مختلف الجوانب الاقتصادية والاجتماعية والحياتية. ومع تزايد المنافع الناتجة عنه، ظهرت مخاطر متعددة تتطلب تبني مقاربة جديدة لحماية مستخدمي الإنترنت من التهديدات السيبرانية السلبية.

التوصيات :-

١_ تتمثل الخطوة الأولى من التوصيات في إيجاد تعريف قانوني دولي متفق عليه للهجمات السيبرانية. حيث إن غياب مصطلح عربي دقيق يعكس هذا المفهوم قد يؤدي إلى سوء فهم للمفاهيم وتشويش في المعاني، مما يستدعي ضرورة وضع تعريف واضح ومحدد يسهم في تعزيز الفهم القانوني ويعزز التعاون الدولي في مواجهة التهديدات السيبرانية.

٢_ تتطلب مكافحة مخاطر الفضاء السيبراني دورًا محددًا وواضحًا من الأمم المتحدة، مع ضرورة تحقيق توازن بين حرية الاستخدام وأمن الفضاء السيبراني. يمكن تحقيق ذلك من خلال إنشاء منظمة دولية متخصصة في الأمن السيبراني، أو من خلال إبرام اتفاقية دولية جديدة تتعلق بالفضاء السيبراني، أو عبر تأسيس منظمة عالمية مستقلة عن هيئة الأمم المتحدة تُعنى بشؤون الفضاء السيبراني. يتعين على هذه الهيئة

وضع القوانين المنظمة لاستخدام الفضاء السيبراني، حيث يستدعي الواقع الحالي الإسراع في تطوير نظام قانوني يساهم في تقليص مستويات التهديدات في هذا الفضاء الحيوي والخطير.

٣_يجب صياغة نصوص قانونية رادعة ضد مرتكبي الجرائم الإلكترونية، مع التركيز على سد الفراغ التشريعي في مجال مكافحة هذه الجرائم.اذ يتعين أن تتضمن هذه النصوص عرضًا مفصلًا للقواعد الموضوعية والإجرائية، مع تحديد طبيعة الجرائم المرتكبة على شبكات الاتصال والتواصل الاجتماعي والبريد الإلكتروني. كما ينبغي أن تتناول هذه النصوص العقوبات المناسبة والإجراءات اللازمة للتحقيق والملاحقة، بما يسهم في تعزيز الحماية القانونية ويحد من انتشار الجرائم الإلكترونية.

٤_يجب التواصل مع خبراء المعلوماتية لتطوير برمجة محددة تهدف إلى فصل البنية التحتية والشبكات السيبرانية العسكرية عن المدنية. يهدف هذا الإجراء إلى حماية السكان المدنيين من مخاطر الحروب السيبرانية، مما يستدعي وضع إطار قانوني ينظم هذا الفصل ويحدد المعايير اللازمة لضمان سلامة البيانات والبنية التحتية المدنية في ظل التهديدات السيبرانية المتزايدة.

لهذا فأكتفي بما قد كتبته لأن المجال لا يتسع للاستفاضة في التفاصيل والوقت لا يسعفني للإسهاب في الحديث، أختتم موضوعي حتى لا أُطيل عليكم والسلام.

المصادر والمراجع

اولاً: الكتب

1- طلاس ،مصطفى، الثورة العلمية التقنية وتطور القوات المسلحة، دار طلاس للدراسات والترجمة والنشر ،دمشق،ص315

2- عبد الله بن سعيد بن البلوشي، مشروعية أسلحة الدمار الشامل وقواعد القانون الدولي، الطبعة الأولى، منشورات الحلبي الحقوقية، 2007.

3- راضي، عمار مزاحم مهدي، مبادئ التحقيق الجنائي في الجرائم الإلكترونية والمعلوماتية عبر الإنترنت وسبل معالجتها، الطبعة الأولى، منشورات مكتبة بغداد القانونية، 2022، ص 63.

4- منير البعلبكي. (2004). عربي-قاموس إنكليزي: المورد. بيروت: دار العلم للملايين. ص. 243.

ثانياً: الأبحاث والمقالات

1- احمد عبيس نعمة الفتلاوي ، الهجمات السيبرانية ومفهومها والمسؤولين الدوليين الناشئة عنها في ضوء التنظيم الدولي المعاصر ،بحث منشور في مجلة المحقق الحلي ، كلية القانون ، جامعة بابل ،2015، ص5.

2- العيسى، طلال ياسين، وعنب، عدي محمد. (2019). المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر. مجلة الزرقاء للبحوث والدراسات الإنسانية، 2019.

3- غيث، علاوى. "الهجمات السيبرانية.. أكبر من حرب نووية: توسع التهديدات الإلكترونية". موقع متخصص في الشؤون الإيرانية.

4- خليفة، إيهاب . "ما هو موقف ميثاق الأمم المتحدة من استخدام القوة السيبرانية في التفاعلات الدولية؟" موقع المستقبل للأبحاث والدراسات المتقدمة

5- السمحان، مني عبدالله ،متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية ، جامعة المنصورة ، العدد 111، يوليو2020.

6- د. هاني محمد خليل العزازي - النظام القانوني الدولي لمكافحة الجرائم السيبرانية ،مصر المعاصرة ، عدد 549،يناير 2023

7- عبد الجواد، أميرة عبد العظيم محمد. 2020. المخاطر السيبرانية و سبل مواجهتها في القانون الدولي العام. مجلة البحوث الفقهية و القانونية،مج. 2020

8- د. محمد عادل محمد عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسس وقت السلم: دراسة على ضوء دليل "تالين" بشأن القانون الدولي المطبق على العمليات السيبرانية 2013-2017، 2020م، ص: 63

9- نسيم ،شريف ،دليل "تالين":الهجمات الإلكترونية وحظر استخدام القوة فى القانون الدولي ،المركز العربي للابحاث الفضاء الالكتروني ،جامعة القاهرة ،2017 .

10- خليل، بشار. "ما هي الحرب السيبرانية؟ مستقبل مخيف للصراع الرقمي." مجلة المعلوماتية، العدد 154، شهر آب، الجمعية السورية للمعلوماتية، 2020. متاح على الرابط: http://www.scs.org.sy/?q=scs/ (تاريخ زيارة 2025/1/1

11- رسل علاء داود العكيدي، حيدر ادهم الطائي، أثر شرط مارتنز في التفسير التطوري للتكنولوجيا العسكرية الحديثة"دراسة تحليلية"، المجلد ،14 العدد1، 2013 ،ص 105

ثالثاً: القرارات والمواثيق الدولية

1- القرار رقم 57/239بتاريخ 31/كانون الثاني /يناير 2003. القرار رقم 58/199 بتاريخ 30/ كانون الثاني / يناير 2004 . مكتب الأمم المتحدة المعني بالمخدرات والجريمة ، تقرير الخبراء المعني باجراء دراسة شاملة عن الجريمة السيبرانية ، فيينا عام 2013 ، الوثيقة EG ، CCPC ، UNODC ، 2013/2/4 .

2- مجلس أوروبا، "اتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية، مجموعة المعاهدات الأوروبية رقم 185، بودابست، عام 2001 – المادة رقم (5).

3- (المادة (2/4)ميثاق الامم المتحدة)

4- (56/121 قرار الجمعية العامة الأمم المتحدة 2001)

5- (57/239 ، الأمم المتحدة ،ثقافة الامن السيبراني 2002)

6- المجلس الاقتصادي والاجتماعي، الدورة الموضوعية لعام 2010، نيويورك، 28 يونيو - 23 يوليو 2010، البند 13 (ب) من جدول الأعمال المؤقت، المسائل الاقتصادية والبيئية: تسخير العلم والتكنولوجيا لأغراض التنمية والتقدم المحرز في تنفيذ ومتابعة نتائج مؤتمر القمة العالمي لمجتمع المعلومات على الصعيدين الإقليمي والدولي.

7- في عام 1973، قام مجموعة من العلماء البارزين بإنشاء الاتحاد العالمي للعلماء في إيريتشي بجزيرة صقلية. منذ ذلك الحين، انضم عدد كبير من العلماء الآخرين إلى الاتحاد، الذي شهد نموًا ملحوظًا ليضم أكثر من 1000 عالم من 110 دول. يتقاسم الأعضاء الأهداف والمبادئ، ويسهمون طواعية في الدفاع عنها، كما يشجع الاتحاد على التعاون الدولي في مجالات العلم والتكنولوجيا بين العلماء والباحثين من مختلف أنحاء العالم.يهدف الاتحاد وأعضاؤه إلى تحقيق حرية تبادل المعلومات كهدف مثالي، بحيث لا تقتصر الاكتشافات والتقدمات العلمية على قلة مختارة. يسعى الاتحاد إلى توزيع هذه المعارف بين شعوب جميع الدول، لتمكين الجميع من فوائد تقدم العلم.تم إنشاء الاتحاد بفضل مركز الثقافة العلمية الذي يحمل اسم "جامعة إيتوري مايورانا"، والذي يُعرف أيضًا بمؤسسة إيتوري مايورانا ومركز الثقافة العلمية. منذ تأسيسه في عام 1963، أصبح هذا المركز قوة تعليمية عالمية، حيث نظم 123 مدرسة و1497 دورة دراسية، حضرها أكثر من 484 ألف مشارك، من بينهم 125 من الحاصلين على جائزة نوبل، من 923 جامعة ومختبرًا في 140 دولة.

رابعاً: الرسائل والاطاريح

1- نادين جميل سلمان هارون،المسؤولية الدولية عن الهجمات السيب ارنية في ظل القانون الدولي الانساني،رسالة ماجستير ، جامعة العلوم التطبيقية الخاصة ، الاردن ،عمان، 2023)

2- العتيبي، عبد الرحمن بجاد شاهر. "دور الأمن السيبراني في تعزيز الأمن الإنساني." جامعة نايف العربية للعلوم الأمنية، كلية العلوم الاستراتيجية (قسم الأمن الإنساني)، رسالة ماجستير ، إشراف الدكتور: جارق محمد سليمان، 2017، ص62.

3- زهراء عماد محمد كلنتر ،المسؤولية الدولية الناشئة عن الهجمات السيبرانية،رسالة ماجستير ،جامعة الكوفة ،٢٠١٦،ص٧٧.

خامساً: الروابط الالكترونية

1-www.almaany.com تاريخ الزيارة 2025/1/26

2-https://cutt.ly/RkoansD،(https://cutt.ly/RkoansD) تاريخ الزيارة 2025/1/28

3-https://doi.org/10.12816/0054788 تاريخ الزيارة 2025/1/29

4-https://jadehiran.com/archives/16835(تاريخ الزيارة 2025/1/5

8- (https://cutt.ly/jQ3rkpu تاريخ الزيارة 2025/1/10

9- دور الذكاء الاصطناعي في تعزيز الأمن السيبراني: رؤى نظرية رابط www.mecsj.com تاريخ الزيارة 2025/1/18)

10- http://www.cybercrimelaw.net() www.cybercrimelaw.net_ تاريخ الزيارة 2025/1/20

11- تقرير مقدم الى القمة العالمية لمجتمع المعلومات http://www.itu.int/dms/pub/itu-s/md./pdf تاريخ الزيارة 2025/2/1

12- https://sherloc.unodc.org/cld/en/education/tertiary/terrorism/module-6/index.html?lf_id= تاريخ الزيارة 2025/1/12

سادساً: مصادر إنكليزية

1- Norbert Wiener," Cybernetics or control communication in the animal and the machine", M.I.T., Press, Second Edition, Cambridge, Massachusetts,1948.

2- Julia Cresswell, "Oxford Dictionary of Word Origins Cybernetics", Oxford Reference Online, Oxford University Press,2010.

3- Hathaway, Oona A., Crootof, Rebecca, Levitz, Philip, Nix, Haley, Nowlan, Aileen, Perdue, William, Spiegel, Julia. (2012). The Law of Cyber-Attack. California Law Review, 824

4- Schmit, Michael N. (2013)."Tallinn Manual on the International Law Applicable to Cyber Warfare." Cambridge University Press.First published.p.92)

5- Clarke, R., & Nick, R. *Cyber Warfare*. 1st Edition. Abu Dhabi: Emirates Center for Strategic Studies and Research, 2012, p. 28

6- Choucri, Nazli.*Cyberpolitics in International Relations*. London: The MIT Press, 2012, p. 4. Library of Congress.

7- Schjolberg, S. (2008). The Global History of Cybercrime Legislation: Harmonization Efforts.

8- Toward a Universal order of Cyberspace managing Threats from Cybercrime of Cyberya

القمة العالمية لمجتمع المعلومات http://www.itu.int/dms/pub/itu-s/md./pdf

9- Kodar, Erki. "Applying the Law of Armed Conflict to Cyber Attacks: From the Martens Clause to Additional Protocol I." ENDC

Proceedings , vol. 15, 2012, p. 110.

Issue - N0. 22 - Part II - February - Year 4 Refereed Quarterly Scientific Journal

American International Journal of Humanities and Social Sciences

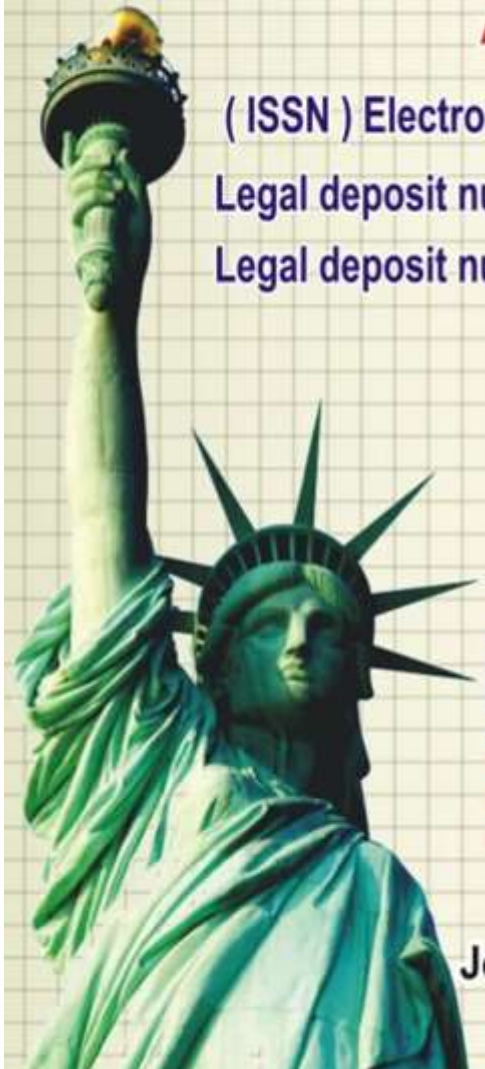
ISSUED BY AMERICAN INTERNATIONAL ACADEMY FOR HIGHER EDUCATION AND TRAINING

QUARTERLY JOURNAL ON HUMANITARIAN AND SOCIAL AFFAIRS

(ISSN) Electronic (4806 - 3085) / (ISSN) Paper (4830 - 3085)

Legal deposit number in the Moroccan National Library (2025PE00006)

Legal deposit number in the Iraq National Library and Archives (2735)



Journal Website : https://iajphss.us/