الهجمة السيبرانية كجريمة دولية

الطالب/ أحمد ناجي عبد الحسين/ طالب دكتوراه في جامعة بيروت العربية

اشراف الدكتور/ جنان خوري

ahmed96iq2pac@gmail.com

ملخص الدراسة

هدف البحث الي التعرف على مدي تأثير الهجمات السيبرانية على الأمن القومي والاقتصاد العالمي، كما هدف أيضا الي معرفة أهمية تحليل الأنماط والتوجهات في الهجمات السيبرانية لتحديد الفاعلين والممارسات الشائعة، وهدف أيضا الي ابراز اهم الاستراتيجيات الفعالة للدفاع ضد الهجمات السيبرانية، بما في ذلك الوقاية والاستجابة، محاولة تعزيز آليات التعاون بين الدول لمشاركة المعلومات والتقنيات لمكافحة هذه الجرائم، كما هدف الي تحديد وتقييم المخاطر المرتبطة بالهجمات السيبرانية على المستويات المختلفة، كما اتكمن أهمية البحث الي فهم التهديدات حيث تساعد دراسة الهجمات السيبرانية على فهم طبيعة التهديدات التي تواجه الدول ومنظمات الأعمال، مما يساهم في تطوير استراتيجيات فعالة للتصدي لها، تطوير القوانين حيث تساهم هذه الدراسات في تعزيز الأطر القانونية الدولية المتعلقة بالأمن السيبراني، مما يساعد في تجريم الأنشطة السيبرانية الضارة ويعزز التعاون بين الدول، تنظيم التعاون الدولي فالهجمات السيبرانية غالبًا ما تتجاوز الحدود الوطنية، لذا فإن فهمها يساعد في تعزيز التعاون بين الدول لمكافحة هذه الجرائم، وقد تشكلت مشكلة الدراسة في التساؤل الرئيسي كيف تؤثر الهجمات السيبرانية كجريمة دولية علي الامن والسلم الدوليين؟ وقد اعتمد الباحث علي استخدم المنهج التحليلي والمنهج الاستقصائي وذلك من خلال الأبحاث والدراسات التي تناولت موضوع وصف الهجمات السيبرانية من منظور القانون الدولي، وقد تكونت فرضية الدراسة من المحتمل أن تزداد الهجمات السيبرانية بشكل ملحوظ في السنوات القادمة، مما يتطلب استجابة دولية موحدة، قد تؤدي الفجوات في التشريعات الوطنية والدولية إلى صعوبة محاسبة المهاجمين السيبرانيين، مما يسهل انتشار هذه الجرائم، من المحتمل أن يؤدي تعزيز التعاون بين الدول في مجال الأمن السيبراني إلى تقليل عدد الهجمات السيبرانية، قد تسهم التقنيات الحديثة، مثل الذكاء الاصطناعي، في زيادة فعالية الهجمات السيبرانية، مما يستدعي تطوير استراتيجيات جديدة لمواجهتها، كما توصلت الدراسة الي تؤدي الهجمات السيبرانية إلى تهديدات مباشرة للأمن الوطني للدول. يمكن أن تستهدف هذه الهجمات البنية التحتية الحيوية مثل أنظمة الطاقة والمياه والنقل، مما يؤدي إلى تعطيل الخدمات الأساسية وإحداث فوضى في المجتمع. بالإضافة إلى ذلك، قد تستخدم

مجموعة من الدول الهجمات السيبرانية كأداة للتجسس أو التأثير على السياسات الداخلية للدول المستهدفة، مما يزيد من توتر العلاقات الدولية، كما اوصت الدراسة الي يجب على الدول العمل على تعزيز التعاون الدولي في مجال مكافحة الجرائم السيبرانية. يتطلب ذلك إنشاء شبكة من الشراكات بين الدول لمشاركة المعلومات حول التهديدات السيبرانية وأساليب الهجوم.

Summary

The research aims to identify the extent of the impact of cyber attacks on national security and the global economy. It also aims to know the importance of analyzing patterns and trends in cyber attacks to identify common actors and practices. It also aims to highlight the most effective strategies for defending against cyber attacks, including prevention and response, trying to enhance cooperation mechanisms between countries to share information and technologies to combat these crimes. It also aims to identify and evaluate the risks associated with cyber attacks at different levels. The importance of the research lies in understanding the threats, as studying cyber attacks helps to understand the nature of the threats facing countries and business organizations, which contributes to developing effective strategies to address them, developing laws, as these studies contribute to strengthening international legal frameworks related to cyber security, which helps in criminalizing harmful cyber activities and enhancing cooperation between countries, and organizing international cooperation, as cyber attacks often cross national borders, so understanding them helps in enhancing cooperation between countries to combat these crimes. The problem of the study was formed in the main question: How do cyber attacks as an international crime affect international peace and security? The researcher relied on the use of the analytical and investigative approaches through research and studies that addressed the topic of describing cyber attacks from the perspective of international law. The study hypothesis was that cyber attacks are likely to increase significantly in the coming years, which requires a unified international response. Gaps in national and international legislation may make it difficult to hold cyber attackers accountable, which facilitates the spread of these crimes. Enhancing cooperation between countries in the field of cyber security is likely to reduce the number of cyber attacks. Modern technologies, such as artificial intelligence, may contribute to increasing the effectiveness of cyber attacks, which requires the development of new strategies to confront them. The study also concluded that cyber attacks pose direct threats to the national security of countries. These attacks can target vital infrastructure such as energy, water and transportation systems, disrupting basic services and causing chaos in society. In addition, a group of countries may use cyber attacks as a tool for espionage or influencing the internal policies of the targeted countries, which increases tension in international relations. The study also recommended that countries should work to enhance international cooperation in the field of

combating cyber crimes. This requires creating a network of partnerships between countries to share information on cyber threats and attack methods.

مقدمة

لقد سمح التقدم السريع في التكنولوجيا للمجتمعات بالتوسع بسرعة في جميع مجالات الحياة، ففي المجالات المدنية والعسكرية والاقتصادية والصحية والاجتماعية، على سبيل المثال، أصبحت التكنولوجيا جزءًا لا يتجزأ من الحياة، وقد يؤدي غيابها إلى اختلالات شديدة أو حتى شلل تام، وفي نهاية المطاف، يمكن تحديد مدى تطور المجتمع من خلال مقدار البنية التحتية الإلكترونية التي يستخدمها لإجراء عملياته.

مما لا شك فيه أن أقدم العمليات السيبرانية كانت تُجرى بطريقة محدودة وغير معقدة فيما يتعلق بالأعمال الإجرامية، مع أضرار أقل نسبيًا ناتجة عنها مقارنة باستخدام التكنولوجيا الإلكترونية إلى أقصى حد ممكن؛ ولقد أصبحت هذه العمليات الإلكترونية تشكل تهديداً خطيراً لأمن الأفراد والمجتمعات والدول في مختلف أنحاء العالم، وخاصة عندما بدأت تستخدم في سياق النزاعات المسلحة الدولية وغير الدولية، ومن قبل الجماعات والمنظمات الإرهابية والإجرامية، أو يتم تنفيذها في سياق الحروب الدولية، إما بمفردها أو بالتزامن مع العمليات العسكرية التقليدية التي لها عواقب مدمرة، وخاصة لأنها تعمل كمحفز وتعزيز للتفوق العسكري، واختلال هيكل القوة، وترجيح الميزان لصالح الدول التي تمتلك الأسلحة الإلكترونية على حساب الدول التي لا تمتلكها. ونتيجة لكل هذا، حذر خبراء قانونيون ومتخصصون من مختلف دول العالم من المخاطر التي تشكلها هذه العمليات الإلكترونية وأكدوا على الحاجة إلى إطار قانوني دولي ومنظمة لتنظيم ومراقبة وتيرة هذا التهديد الجديد والناشئ للسلم والأمن الدوليين. وهم ينظرون إلى هذا باعتباره تهديداً متزايداً خارج نطاق العمل القانوني[١].

إننا في حاجة إلى توضيح المبادئ الأساسية للقانون الدولي، أو الأساس الذي يقوم عليه، وذلك من أجل تقديم صورة كاملة للمتلقي، ونعني بذلك تحديد المبادئ الأساسية الأكثر أهمية التي يستند إليها القانون الدولي، ومدى انطباقه على الهجمات الإلكترونية، مع الأخذ في الاعتبار كل من تفاصيل الهجمات الإلكترونية التي تميزها عن الأسلحة التقليدية المستخدمة في النزاعات المسلحة الدولية وغير الدولية، فضلاً عن عمومية وشمولية هذه المبادئ. ويتعين علينا أولاً أن نصف طبيعة الهجمات

[١] محمد حسن سعيد دراجي، ٢٠٢٤، الهجمات السيبرانية وفقا لأحكام القانون الدولي الإنساني، مجلة علوم الشريعة والقانون، المجلد (٥١) العدد (١) ص ٢.

الإلكترونية ومدى إمكانية خضوعها للقانون الدولي الإنساني، لأننا سنتحدث عن الدرجة التي يمكن بها استخدام التكنولوجيا الرقمية كسلاح أو أداة في النزاعات المسلحة الدولية وغير الدولية، ومن أجل تحقيق هذه الغاية، فالمبادئ الأساسية للقانون الدولي التي تتناول الحق في استخدام القوة في زمن الحرب ومدى انطباقها على الهجمات الإلكترونية في سياق العلاقات بين الدول[٢].

في العقدين الأخيرين، أصبح الفضاء السيبراني ساحة معركة جديدة تتنافس فيها الدول، الجماعات، والأفراد، حيث تشكل الهجمات السيبرانية تهديدًا متزايدًا للأمن القومي والاقتصادي، حيث تتنوع أهدافها بين التجسس، التخريب، وسرقة المعلومات. هذه الأنشطة لم تعد مقتصرة على الأفراد أو الجماعات الصغيرة، بل أصبحت تمثل تحديات كبيرة للحكومات على مستوى العالم. لذا، فإن الهجمة السيبرانية تُعتبر جريمة دولية تتطلب استجابة قانونية وتنظيمية شاملة.

حيث تتعدد أشكال الهجمات السيبرانية، بدءًا من البرمجيات الخبيثة التي تستهدف الأجهزة الخاصة، وصولًا إلى الهجمات المعقدة التي تستهدف البنية التحتية الحيوية للدول. تعكس هذه الأنشطة تطور التكنولوجيا وتزايد الاعتماد على الشبكات الرقمية، مما يزيد من خطورة التهديدات السيبرانية. في هذا السياق، تُظهر الدراسات أن الهجمات السيبرانية يمكن أن تؤدي إلى خسائر مالية ضخمة، فضلاً عن تأثيرها على سمعة الدول والشركات.

ومن الناحية القانونية، تُعاني الجرائم السيبرانية من نقص في التوجيهات الموحدة على المستوى الدولي. تختلف القوانين من دولة إلى أخرى، مما يصعب ملاحقة الجناة عبر الحدود. هذا التباين في التشريعات يخلق ثغرات يمكن أن تُستغل من قبل المهاجمين، مما يجعل من الضروري تطوير أطر قانونية دولية تتناول هذه الجرائم بفعالية.

حيث تتطلب مواجهة الهجمات السيبرانية تعاونًا دوليًا متكاملًا، حيث يجب على الدول تبادل المعلومات والتقنيات لتعزيز الأمن السيبراني. كما ينبغي أن تشمل هذه الجهود تعزيز الوعي العام حول المخاطر السيبرانية وتطبيق استراتيجيات وقائية

[٢] وفاء لطفي، ٢٠٢٢، الجهود الدولية في مجال مكافحة جرائم الارهاب السيبراني: التجربة الماليزية نموذجا، مجلة كلية الاقتصاد والعلوم السياسية، المجلد (٢٣) العدد (١)، ص ١٥٣.

فعالة. إن فهم الهجمات السيبرانية كجرائم دولية يتطلب تضافر الجهود بين الحكومات، القطاع الخاص، والمجتمع المدني، لتحقيق بيئة سيبرانية أكثر أمانًا[٣].

مشكلة الدراسة

إن طبيعة الجرائم الإلكترونية ومداها ووسائلها وأدلتها تختلف كثيراً عن الجرائم العادية، حيث تتطور تكنولوجيا المعلومات بوتيرة سريعة، مما أدى إلى إساءة استخدام التكنولوجيا وظهور ظاهرة إجرامية جديدة، فبفضل الاتصالات والإنترنت ظهرت أنواع جديدة من الجرائم، وترتكب هذه الجرائم من خلال الاختراق والهجوم والتسلل داخل أنظمة المعلومات، بقصد تدمير تلك الأنظمة أو الحصول على بيانات حساسة، مثل الأسرار العسكرية أو المالية، والتي تنبه السلطات إلى التهديدات المحتملة على المستوى الوطني والدولي. ولابد أن نتوصل إلى كيفية التعامل مع هذه الظاهرة.

إن سرية الهوية والأدلة الضئيلة على الجريمة هي السمات المميزة للجرائم الإلكترونية، فضلاً عن أن الجرائم الإلكترونية يمكن أن تلحق الضرر بعدد لا نهائي من الضحايا في الحال ولا تقتصر على وقت أو مكان، ومن الجدير بالذكر أن فكرة أمن المعلومات توسعت إلى ما هو أبعد من جذورها التقنية لتشمل الجوانب الأمنية والدفاعية والاستراتيجية، كما أصبحت عنصراً حاسماً في مواثيق الدفاع للتحالفات العسكرية واستراتيجيات الأمن الوطني.

تتمثل القضية الرئيسية التي تتناولها الدراسة في الطبيعة الناشئة للهجمات الإلكترونية ودمجها القسري في سباق التسلح كسلاح أو أداة في النزاعات المسلحة، مع ما يترتب على ذلك من عواقب قانونية وعملية كبيرة، وينطبق هذا بشكل خاص في ضوء الفجوة في مجموعة القانون الدولي التي تحكم قواعد الهجمات الإلكترونية وبالتالي، فإن القضية الرئيسية التي تتناولها الدراسة تتمحور حول مدى إمكانية تغطية الهجمات الإلكترونية بالقانون الإنساني الدولي، ومن هنا فقد تشكلت مشكلة الدراسة في التساؤل الرئيسي التالي" كيف تؤثر الهجمات السيبرانية كجريمة دولية علي الامن والسلم الدوليين؟ ويندرج من هذا التساؤل الرئيسي عدة أسئلة فرعية حيث تشكلت في الاتي:

١. هل عالجت الاتفاقيات الدولية الهجمة السيبرانية من ناحية إطار القانون الدولي.
٢. ما هي الطبيعة القانونية للحروب والنزاعات السيبرانية.

[٣] يحي ياسين سعود، ٢٠٢٠، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، المجلة القانونية، ص ٨٢.

٣. ما مدى إمكانية تطبيق المسؤولية الدولية عن أضرار التي يخلفها الهجوم السيبراني؟

٤. هل تتطبق مبادئ القانون الدولي على الهجمات السيبرانية؟

أهمية الدراسة

هناك جانبان رئيسيان لهذا الموضوع، الأول علمي بطبيعته؛ إذ ينص على أن الكتابات القانونية التي تنظم الفضاء الإلكتروني، وتحل النزاعات، وتضع حدًا للحروب والهجمات السيبرانية الإلكترونية، وتحمي الدول من الخروقات التي تضر بالعلاقات الدولية، وتتجاوز القانون الدولي، وتحافظ على السلام والأمن السيبراني الدوليين، كما تفتقر إلى المعرفة العلمية، ولأن العالم السيبراني هو انعكاس للنظام الدولي، اما الثاني فهو تطبيق القوانين الدولية فمن المهم تطبيق القوانين الدولية، وفي حالات الصراع والحرب حيث لا توجد وثيقة قانونية تحمي الأطراف بسبب حداثتها، من الضروري تكييف القانون الدولي مع المجال الرقمي وإنشاء قوانين جديدة.

حيث نكمن أهمية الدراسة لأنها تسلط الضوء على القيود التي تفرضها الصكوك القانونية الدولية الحالية وتسلط الضوء على الحاجة إلى حماية المدنيين من الهجمات السيبرانية الدولية وغير الدولية مع الالتزام بمبادئ القانون الدولي، كما إن توضيح مدى وقوع الهجمات الإلكترونية ضمن نطاق القانون الدولي وضمان مواجهة المسؤولين عن الهجمات الإلكترونية في سياق النزاعات كما تعد هذه الدراسة هي إضافة بسيطة ولكنها مهمة ستساعد في فهم بعض التفاصيل الغامضة المحيطة بالتخطيط للهجمات الإلكترونية وتقنينها في ضوء القانون الإنساني الدولي. كما ستتيح للعلماء والخبراء فهم كيفية استخدام الهجمات الإلكترونية في النزاعات المسلحة، وتتشكل أهمية الدراسة في النقاط التالي:

١. فهم التهديدات حيث تساعد دراسة الهجمات السيبرانية على فهم طبيعة التهديدات التي تواجه الدول ومنظمات الأعمال، مما يساهم في تطوير استراتيجيات فعالة للتصدي لها.
٢. تطوير القوانين حيث تساهم هذه الدراسات في تعزيز الأطر القانونية الدولية المتعلقة بالأمن السيبراني، مما يساعد في تجريم الأنشطة السيبرانية الضارة ويعزز التعاون بين الدول.
٣. تنظيم التعاون الدولي فالهجمات السيبرانية غالبًا ما تتجاوز الحدود الوطنية، لذا فإن فهمها يساعد في تعزيز التعاون بين الدول لمكافحة هذه الجرائم.

٤. حماية البنية التحتية فدراسة الهجمات السيبرانية تساهم في حماية البنية التحتية الحرجة، مثل الشبكات الكهربائية والاتصالات، مما يقلل من المخاطر الاقتصادية والاجتماعية.
٥. توعية المجتمع حيث تساعد في رفع الوعي حول المخاطر المرتبطة بالأمن السيبراني، مما يعزز من ثقافة الأمن السيبراني في المجتمع.

اهداف الدراسة

تسعي الدراسة الي تحقيق العديد من الأهداف ومن اهما ما يلي:

١. التعرف على مدي تأثير الهجمات السيبرانية على الأمن القومي والاقتصاد العالمي.
٢. معرفة أهمية تحليل الأنماط والتوجهات في الهجمات السيبرانية لتحديد الفاعلين والممارسات الشائعة.
٣. ابراز اهم الاستراتيجيات الفعالة للدفاع ضد الهجمات السيبرانية، بما في ذلك الوقاية والاستجابة.
٤. محاولة تعزيز آليات التعاون بين الدول لمشاركة المعلومات والتقنيات لمكافحة هذه الجرائم.
٥. تحديد وتقييم المخاطر المرتبطة بالهجمات السيبرانية على المستويات المختلفة.

منهجية الدراسة

اعتمد الباحث علي استخدم المنهج التحليلي والمنهج الاستقصائي وذلك من خلال الأبحاث والدراسات التي تناولت موضوع وصف الهجمات السيبرانية من منظور القانون الدولي.

فرضيات الدراسة

١. من المحتمل أن تزداد الهجمات السيبرانية بشكل ملحوظ في السنوات القادمة، مما يتطلب استجابة دولية موحدة.
٢. قد تؤدي الفجوات في التشريعات الوطنية والدولية إلى صعوبة محاسبة المهاجمين السيبرانيين، مما يسهل انتشار هذه الجرائم.
٣. من المحتمل أن يؤدي تعزيز التعاون بين الدول في مجال الأمن السيبراني إلى تقليل عدد الهجمات السيبرانية.

٤. قد تسهم التقنيات الحديثة، مثل الذكاء الاصطناعي، في زيادة فعالية الهجمات السيبرانية، مما يستدعي تطوير استراتيجيات جديدة لمواجهتها.
٥. من المحتمل أن تكون الدوافع الاقتصادية والسياسية هي المحرك الرئيسي وراء معظم الهجمات السيبرانية، مما يجعل من الضروري فهم هذه الدوافع لتحسين استراتيجيات الدفاع.
٦. قد تزداد الهجمات السيبرانية على البنية التحتية الحيوية للدول، مما يستدعي وضع سياسات وقائية أكثر صرامة.
٧. من الممكن أن تؤثر الهجمات السيبرانية على حقوق الإنسان، مثل الخصوصية وحرية التعبير، مما يبرز الحاجة إلى حماية هذه الحقوق في سياق الأمن السيبراني.
٨. قد تتطور الهجمات السيبرانية إلى شكل من أشكال الجريمة المنظمة، حيث تتعاون عدة جهات لتحقيق أهداف مشتركة.

هيكلة الدراسة

المبحث الأول: الهجمات السيبرانية وأثرها على تهديد الامن والسلم الدوليين.

المطلب الأول: الوصف الدلالي للهجمات السيبرانية.

المطلب الثاني: الهجمات السيبرانية وانعكاساتها على السلم والامن الدوليين.

المبحث الثاني: موقف المنظمات الدولية والجهود الدولية لمواجهة الهجمات السيبرانية.

المطلب الأول: دور الأمم المتحدة في تقنين الهجمات السيبرانية.

المطلب الثاني: الاتفاقيات الدولية في مجال مكافحة الهجمات السيبرانية .

المبحث الأول: الهجمات السيبرانية وأثرها على تهديد الامن والسلم الدوليين.

تُعتبر الهجمات السيبرانية من أخطر التهديدات التي تواجه العالم الرقمي اليوم، حيث تتضمن هذه الهجمات أساليب متعددة تستهدف الأنظمة والشبكات المعلوماتية بهدف السرقة، التخريب، أو التجسس، حيث تتراوح هذه الهجمات بين

الفيروسات، والبرمجيات الخبيثة، والهجمات الموزعة على الخدمات (DDoS)، مما يؤدي إلى فقدان البيانات وتعطيل الأعمال.

وعلى مر السنوات، شهدت الهجمات السيبرانية تطوراً ملحوظاً في تعقيدها وتأثيرها. في الماضي، كانت هذه الهجمات تتم من قبل أفراد أو مجموعات صغيرة، لكن اليوم نجد أنها تُنفذ من قبل دول ومنظمات متقدمة تكنولوجياً. هذا التغير يعكس مدى أهمية الأمن السيبراني ويظهر الحاجة الملحة للتصدي لمثل هذه التهديدات على مستوى دولي.

حيث تُعتبر الهجمات السيبرانية جريمة دولية تتجاوز الحدود الوطنية، مما يجعلها تحدياً قانونياً معقداً. فالقوانين الحالية، رغم تطورها، لا تزال تواجه صعوبات في محاسبة المهاجمين الذين يتخذون من الفضاء الإلكتروني ساحة لنشاطاتهم الإجرامية. لذا، تتطلب هذه القضية جهوداً منسقة بين الدول لتطوير أطر قانونية فعالة تعزز من مكافحة هذه الجرائم[٤].

حيث تؤدي الهجمات السيبرانية إلى تأثيرات اقتصادية واجتماعية جسيمة. فقد تكبدت الشركات خسائر مالية ضخمة نتيجة لهذه الهجمات، كما أن ثقة المستهلكين في الخدمات الرقمية تتأثر سلباً. بالإضافة إلى ذلك، تساهم هذه الهجمات في زيادة القلق الاجتماعي حول الخصوصية والأمان الشخصي، مما يستدعي استجابة فعالة من الحكومات والمجتمعات.

كما تتطلب مكافحة الهجمات السيبرانية تعاوناً دولياً شاملاً، يجب على الدول تبادل المعلومات والتقنيات، وتطوير استراتيجيات مشتركة لمواجهة التهديدات المتزايدة، إن بناء شراكات بين القطاعين العام والخاص، بالإضافة إلى تعزيز التعليم والتوعية حول الأمن السيبراني، يعد خطوة أساسية في مواجهة هذا التحدي العالمي[٥].

المطلب الأول: الوصف الدلالي للهجمات السيبرانية.

تشير الهجمات السيبرانية إلى الأنشطة الضارة التي تستهدف الأنظمة والشبكات الحاسوبية بهدف سرقة المعلومات، تخريب البيانات، أو تعطيل الخدمات. تشمل هذه الهجمات مجموعة متنوعة من الأساليب، مثل البرمجيات الخبيثة، هجمات الحرمان من الخدمة (DDoS)، والاحتيال الإلكتروني. يُستخدم مصطلح "هجوم سيبراني" بشكل عام للإشارة إلى أي نشاط

[٤] عادل عبد الصادق، ٢٠١٦، أسلحة الفضاؤ الالكتروني في ضوء القانون الدولي الإنساني، مكتبة المستقبلية، مصر، ص ١٦.

[٥] احمد عبيس نعمة الفتلاوي، ٢٠١٦، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، جامعة بابل، كلية القانون، المجلد (٨) العدد (٤)، ص ٦٨٧-٦١٠.

ينطوي على استغلال الثغرات في الأنظمة الحاسوبية. تتنوع الهجمات السيبرانية بشكل كبير، مما يجعل من الصعب تحديد نوع واحد منها. يمكن تقسيم هذه الهجمات إلى عدة فئات، منها الهجمات الموجهة التي تستهدف أهدافًا معينة، والهجمات العشوائية التي تستهدف مجموعة واسعة من الأهداف. ومن بين الأنواع الشائعة: الفيروسات، الديدان، أحصنة طروادة، وهجمات التصيد. كل نوع له خصائصه وآثاره الخاصة على الأنظمة المستهدفة.

تتعدد الأسباب التي تدفع الأفراد أو المجموعات لتنفيذ الهجمات السيبرانية. يمكن أن تكون دوافع سياسية، اقتصادية، أو حتى شخصية. تسعى بعض الجماعات إلى تحقيق أهداف سياسية من خلال زعزعة استقرار الحكومات، بينما يهدف آخرون إلى الحصول على المال من خلال سرقة المعلومات المالية أو الابتزاز. تعتبر الدوافع النفسية والاجتماعية أيضًا عوامل مهمة تسهم في انتشار هذه الهجمات، تترك الهجمات السيبرانية آثارًا سلبية كبيرة على الأفراد والدول. يمكن أن تؤدي إلى فقدان المعلومات الحساسة، تضرر البنية التحتية الحيوية، وزعزعة الثقة بين الحكومات والمواطنين. بالإضافة إلى ذلك، قد تؤثر هذه الهجمات على الاقتصاد العالمي وتؤدي إلى تكاليف مالية ضخمة. تتطلب هذه التأثيرات استجابة سريعة وفعالة من قبل الحكومات والمؤسسات.

لمواجهة التهديدات السيبرانية، يجب على الدول والمؤسسات تعزيز قدراتها الأمنية. يتضمن ذلك تطوير أنظمة أمان متقدمة، تدريب الموظفين على الوعي الأمني، وإقامة شراكات دولية لتبادل المعلومات حول التهديدات. بالإضافة إلى ذلك، يجب على الحكومات وضع تشريعات فعالة لمكافحة الجرائم السيبرانية، وتطوير استراتيجيات للتعامل مع الحوادث الأمنية.

من الممكن أن يكون الجميع قد لاحظوا انتشار المصطلحات والقوانين التي لم تكن موجودة في أوائل القرن الحادي والعشرين، مثل القوانين المتعلقة بالهجمات والجرائم الإلكترونية، والخصوصية الرقمية، والفضاء الإلكتروني، إلى جانب تقديم أفكار جديدة مثل الحوكمة الإلكترونية، والفضاء الإلكتروني، والعلاقات الدولية الإلكترونية، والتجارة والاستثمار عبر الإنترنت، تعود كلمة "cyber " إلى الكلمة اليونانية "Kybernetes "[٦]، والتي تعني في الأصل "التحكم عن بعد"، وفي وقت لاحق، أصبح قانون تكنولوجيا المعلومات، المعروف أيضًا باسم "قانون الإنترنت"، يُفهم على أنه إطار قانوني يتناول المسائل المتعلقة

[6] Andreea bendovschi, 2015, cyber -attacks - trends, patterns and security counter measures, procedia economics and finance, Elsevier, Vol .28, p. 3.

بالكمبيوتر، والإنترنت، والفضاء الإلكتروني، والمخاوف القانونية ذات الصلة. بعبارة أخرى، فإن إنشاء "قوانين ورقية" لحكم "عالم بلا ورق" هو طريقة مناسبة لوصف قانون الإنترنت[٧].

لا شك أن العالم بعد فيروس كورونا شهد تحولاً نوعياً نحو الفضاء الإلكتروني، مع ارتفاع عدد الحروب والصراعات الإلكترونية، وقد بدأ البحث عن تعريف متفق عليه للهجمات والحروب والصراعات الإلكترونية بين علماء القانون الدولي للباحثين والمتخصصين والمهتمين، وقد عرفها بعض الفقهاء بأنها الاستخدام العمدي لأنظمة شبكات الإنترنت لنقل برامج خبيثة، كما عرفها بأنها سلوك عدواني يتم تنفيذه إلكترونياً بقصد إلحاق الضرر بالآخرين، وبأنها أفعال تتخذها الدولة لمهاجمة أنظمة معلومات العدو في محاولة للتأثير عليها وحماية أنظمة معلومات الدولة المهاجمة[٨].

وهنا نلاحظ توازياً بين الهجوم السيبراني والهجوم التقليدي، ففي كلتا الحالتين، يكون لدى المهاجم سبب لتنفيذ الهجوم، وقد يكون الهدف فرداً حقيقياً أو افتراضياً، ولكن أداة الهجوم وموقع الهجوم يظهران مدى الاختلاف بينهما، إذ تُستخدم أداة تكنولوجية متقدمة في الهجوم الإلكتروني، وبما أن الهجوم يتم عن بعد عبر شبكات وخطوط اتصال تربط المهاجم بالمنطقة المستهدفة، فإن الجاني لا يحتاج إلى الانتقال إلى مكان آخر، فالهجمات السيبرانية لا يقوم بها أشخاص عاديون، بل عصابة من قراصنة الكمبيوتر المهرة الذين يتعاونون عبر شبكات إلكترونية[٩].

[٧] اللجنة الدولية، ٢٠١٥، القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة، ص٥٧.

[٨] احمد عبيس نعمة الفتلاوي، ٢٠١٦، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، جامعة بابل، كلية القانون، العدد ٤، ٦١٤.

[9] Heather Harrison Dinniss, 2018, The status and use of computer network attacks in international law, Phd thesis, London school of a economics and Political science, p. 33.

من الواضح أن ضعف سياسات الدفاع السيبراني الوطنية وانتشار الجهات الفاعلة غير الحكومية في الفضاء الإلكتروني، والتي يصعب تنظيمها ويصعب إضفاء الشرعية عليها بسبب براعتها التكنولوجية المتفوقة، هي الأسباب الرئيسية للحروب والصراعات السيبرانية، يمكن للاختراق السيبراني العدواني الاستفادة من التهديد المرتفع مقابل الأمن المتراخي[١٠].

في الختام، يُظهر الوصف الدلالي للهجمات السيبرانية مدى تعقيد هذا المجال وأهميته في عصر التكنولوجيا. من خلال فهم الأنواع، الأسباب، والتأثيرات، يمكن للدول والمؤسسات العمل بشكل أفضل لتطوير استراتيجيات فعالة للتصدي لهذه الظاهرة المتزايدة. يتطلب الأمر تعاونًا دوليًا وتطوير وعي شامل لضمان أمن المعلومات وحماية المجتمعات من التهديدات السيبرانية.

المطلب الثاني: الهجمات السيبرانية وانعكاساتها على السلم والامن الدوليين.

تعتبر الهجمات السيبرانية من أبرز التحديات التي تواجه العالم في العصر الرقمي الحالي، حيث تزايدت وتيرتها بشكل ملحوظ في السنوات الأخيرة. تتنوع هذه الهجمات بين الاختراقات البسيطة والتهديدات المعقدة التي تستهدف الأنظمة الحيوية للدول، مما يطرح تساؤلات حول تأثيراتها على السلم والأمن الدوليين. فمع ازدياد الاعتماد على التكنولوجيا في جميع جوانب الحياة، أصبحت هذه الهجمات تمثل خطرًا حقيقيًا يهدد استقرار الدول والأمن العالمي.

تتسم الهجمات السيبرانية بتعقيدها وسرعتها، حيث يمكن أن تؤدي إلى تعطيل الخدمات الحيوية مثل الكهرباء والماء والرعاية الصحية. كما يمكن أن تستهدف البنية التحتية الحيوية للدول، مما يؤدي إلى عواقب وخيمة على المواطنين والاقتصاد. لذلك، فإن فهم هذه الهجمات وكيفية التصدي لها يعد أمرًا ضروريًا لضمان حماية السلم والأمن الدوليين، تتأثر العلاقات الدولية بشكل كبير بالهجمات السيبرانية، حيث يمكن أن تؤدي إلى تصعيد النزاعات بين الدول. هذه الهجمات قد تُعتبر أعمالًا عدائية، مما يزيد من التوترات السياسية ويؤثر على التعاون الدولي. وبالتالي، تتطلب هذه الظاهرة وضع استراتيجيات فعالة للتصدي لها، بما في ذلك تعزيز التعاون بين الدول وتبادل المعلومات[١١].

---

[10] Jeffrey T. G Kelsey, 2018, Hacking in to international humanitarian law: The principles of distinction and neutrality in the age of cyber warfare, Michigan law review, Vol. 106, No.7, p.1437.

[١١] عادل عبد الصادق، ٢٠١٦، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، مكتبة المستقبلية، مصر، ص٩٦.

علاوة على ذلك، تلعب الحكومات والشركات دورًا حيويًا في حماية المعلومات الحساسة وتطوير أنظمة أمنية متقدمة. إن الاستثمارات في التكنولوجيا والأمن السيبراني تمثل أولوية قصوى للدول لتحقيق الأمن والاستقرار. لذا فإن تعزيز الوعي العام حول الهجمات السيبرانية يعد خطوة مهمة في بناء مجتمع أكثر أمانًا، الهجمات السيبرانية تمثل تحديًا كبيرًا للسلم والأمن الدوليين، وتتطلب استجابة جماعية من المجتمع الدولي. من خلال فهم طبيعة هذه الهجمات وآثارها، يمكن للدول العمل معًا لتعزيز الأمن السيبراني وضمان حماية مصالحهم المشتركة[١٢].

لا شك أن انتشار الهجمات الإلكترونية المدمرة والضارة في مختلف أنحاء العالم بعد عام ٢٠١١ كان نتيجة لضعف أطر الأمن الإلكتروني في العديد من الدول. وقد أدى هذا إلى جعل التهديد للسلام والأمن العالميين حاضرا على الدوام، كما يتضح من الحالات العديدة لهذه الهجمات، والتي تشمل ثورات الربيع العربي في إستونيا وإيران. كما ساهم الصراع الروسي الأوكراني، وتسريب أوراق بنما، واختراق وكالة أبحاث الإنترنت الروسية، والتقارير الإعلامية التي تكشف تفاصيل إقامة الرئيس الروسي فلاديمير بوتن، في نمو هذه الهجمات. ومع انتشار هذه الهجمات على نطاق أوسع، برز السؤال حول سبب عدم وجود إطار عالمي للمساءلة أو هيكل للمساءلة للسيطرة على هذه الهجمات الإلكترونية.

ومن هنا، فإن أهمية قوانين الهجمات السيبرانية تكمن في أنها تضع المبادئ التوجيهية لاستخدامها وتتبع ردود الفعل العامة في الفضاء الإلكتروني؛ وهي تعزز الأمن والحماية للمعاملات عبر الإنترنت؛ وتخضع جميع الأنشطة عبر الإنترنت لمراقبة مسؤولي قانون الفضاء الإلكتروني؛ وهي تحمي جميع المعلومات الشخصية والممتلكات الحكومية؛ وتساعد في الحد من الأنشطة الإلكترونية غير المشروعة من خلال توفير الرقابة والعناية الواجبة من قبل المؤسسات الحكومية المختصة؛ وتختلف الآثار القانونية لردود الفعل العامة المقاسة في الفضاء الإلكتروني تبعًا لطبيعتها، سواء كانت مرتبطة بالتجارة أو الخدمات أو الأمن من مختلف الأنواع. كما أن وجود قوانين الفضاء الإلكتروني يعني وجود اتفاقيات دولية في هذا المجال. وهي تجعل من الممكن تتبع جميع السجلات الإلكترونية من خلال التعاون العالمي في مكافحة الجريمة المنظمة. كما أنها تساعد في إنشاء حوكمة إلكترونية، وتحسين حياة أولئك الذين يستخدمون خدمات الحكومة الإلكترونية[١٣].

---

[12] Herbert Lin, 2012,Cyber conflict and international humanitarian law International review of the red cross, Vol. 94, N886, p.515.

[١٣] رزق أحمد سمودي، ٢٠١٨، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية، ص ٣٣٨.

إن الهجمات السيبرانية تشتمل على عدد هائل من أنظمة الكمبيوتر المترابطة عالمياً، ويبدو أن أنظمة الكمبيوتر العسكرية غالباً ما ترتبط بأنظمة تجارية ومدنية وتعتمد عليها، إما كلياً أو جزئياً. ونتيجة لهذا، يكاد يكون من الصعب شن هجوم إلكتروني على البنية الأساسية العسكرية وتقييد عواقبه بهدف عسكري حصرياً. على سبيل المثال، فإن استخدام دودة تنتشر بسرعة، ولا يمكن السيطرة عليها، وتلحق أضراراً جسيمة بالبنية الأساسية التي يستخدمها المدنيون يشكل مخالفة للقانون الإنساني الدولي. وخلافاً للهجمات التقليدية، حيث يكون المهاجم غالباً على بعد مئات الكيلومترات، فإن تطبيق فكرة التمييز بين المقاتلين والمدنيين على الهجمات الإلكترونية يشكل مشكلة بالغة الصعوبة، ربما يكون من الصعب، إن لم يكن من المستحيل، الوصول إلى مسافة بين المقاتلين والمدنيين. وقد يكون من الصعب التمييز بين الأهداف العسكرية والمدنية في الهجمات الإلكترونية، خاصة وأن أنظمة الكمبيوتر العسكرية غالباً ما ترتبط بأنظمة تجارية ومدنية وتعتمد عليها، إما كلياً أو جزئياً، وقد يكون هناك حتى تداخل بينهما. والفضاء الإلكتروني هو الوسيلة والشبكة الوحيدة التي تتصل بها التطبيقات العسكرية والمدنية. لذلك، من دون تعريض الأشخاص والمرافق المدنية للخطر، من المستحيل شن هجوم إلكتروني على البنية التحتية العسكرية وتقييد عواقبه على هدف عسكري فقط[١٤].

المبحث الثاني: موقف المنظمات الدولية والجهود الدولية لمواجهة الهجمات السيبرانية.

إن التكيف القانوني لهذه القضية من حيث الشرعية أو عدم الشرعية الهجمات السيبرانية في ضوء استخدام القوة في العلاقات الدولية يشكل شرطاً مسبقاً لأي بحث في إمكانية تطبيق قواعد القانون الدولي على الهجمات السيبرانية. وسوف يكون هناك دائماً صراع في العلاقة بين الحق في استخدام القوة وقانون الحرب، إن استخدام القوة محظور بموجب القانون الدولي الحديث، باستثناء حق الدول في الدفاع عن النفس سواء بشكل فردي أو جماعي، أو عندما يستخدم مجلس الأمن تدابير إنفاذ القانون. ويتعين على المنظمات الدولية مثل الأمم المتحدة أن تتخذ موقفاً بشأن هذه القضية وأن تفرض القانون الدولي ضد أولئك الذين ينخرطون في سلوك عدواني سيبراني.

[١٤] مايكل شميت، ٢٠١٢، الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكومبيوتر والقانون في الحرب، المجلة الدولية للصليب الأحمر، ص٩١٥.

تُعتبر الهجمات السيبرانية من التهديدات المتزايدة التي تواجه الأفراد والدول على حد سواء. ومع تزايد الاعتماد على التكنولوجيا والإنترنت، أصبحت هذه الهجمات تشكل خطراً كبيراً على الأمن القومي والاقتصادي. في هذا السياق، تلعب المنظمات الدولية دوراً حيوياً في تنسيق الجهود لمواجهة هذه التهديدات وتعزيز الأمن السيبراني.

تعتبر منظمة التعاون والتنمية الاقتصادية من الجهات الفاعلة المهمة في مجال الأمن السيبراني. تعمل المنظمة على تطوير سياسات فعالة لمواجهة التهديدات السيبرانية وتعزيز التعاون بين الدول الأعضاء. كما تقدم توصيات وإرشادات لتعزيز الأمان السيبراني في مختلف القطاعات، بما في ذلك القطاعين العام والخاص[١٥].

رغم الجهود المبذولة، تواجه المنظمات الدولية تحديات كبيرة في مواجهة الهجمات السيبرانية، مثل تطور الأساليب المستخدمة من قبل المهاجمين وزيادة تعقيد الهجمات. يتطلب ذلك استمرار التعاون الدولي وتبادل المعلومات والخبرات بين الدول لتطوير استراتيجيات فعالة للتصدي لهذه التهديدات، تتطلب مواجهة الهجمات السيبرانية جهوداً منسقة بين الدول ومنظمات المجتمع الدولي. يجب أن تركز هذه الجهود على تعزيز التعاون وتبادل المعرفة والتقنيات، لضمان حماية الأمن السيبراني على المستوى العالمي.

المطلب الأول: دور الأمم المتحدة في تقنين الهجمات السيبرانية.

وتشير تقديرات الأمم المتحدة إلى أن عدد سكان العالم يبلغ ٧,٩ مليار نسمة، وأن أكثر من نصفهم يستخدمون الإنترنت. وبالإضافة إلى ذلك، يتلقى محرك البحث جوجل وحده ما معدله ٣,٥ مليار عملية بحث يوميا، وفي غضون سنوات قليلة، سيكون هناك ٥٠ مليار جهاز متصل بالإنترنت. وبالإضافة إلى ذلك، يستخدم أكثر من ١,٩ مليار شخص موقع فيسبوك يوميا، وأكثر من ٢,٩ مليار مستخدم شهريا. ولا تأخذ هذه الإحصائيات في الحسبان ارتفاع الهجمات والصراعات والحروب الإلكترونية وغيرها من الأعمال العدوانية التي تقوم على الكراهية والابتزاز والتجارة الإلكترونية غير القانونية في الفضاء الإلكتروني.

وقد دفع هذا الأمم المتحدة إلى صياغة مبادئ توجيهية محددة في عام ٢٠١٥ لمواجهة الهجمات الإلكترونية، ووافق جميع أعضاء الأمم المتحدة بالإجماع على هذه المبادئ التوجيهية في عام ٢٠٢١ لإنشاء إطار ملزم قانونًا لجميع الدول التي تستخدم

[١٥] عبد الصادق، ٢٠١٦، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، مكتبة المستقبلية، مصر، ص١٠٠.

الفضاء الإلكتروني. ومن بين هذه المتطلبات أن تتعهد الدول بعدم السماح باستغلال أراضيها عمدًا في أنشطة غير مشروعة، أو السماح باستخدام شبكات الإنترنت في أعمال تعرض السلم والأمن الدوليين للخطر أو تضر بهما[١٦].

لقد أثبتت التجربة الدولية أن تحقيق الأمن السيبراني يتطلب أكثر من مجرد الاتفاق على المعايير واللوائح السيبرانية الدولية. وبدلاً من ذلك، يجب إنشاء خطة دبلوماسية منسقة لمراقبة كيفية اتباع هذه المبادئ التوجيهية وتطبيق العقوبات عندما لا يتم ذلك. ولتفعيل النظام القانوني في الفضاء الإلكتروني، يجب أن يكون هناك حركة في السياسة الدولية. إن المبادئ التوجيهية للأمم المتحدة بها بعض العيوب، أحدها عدم قدرتها على محاسبة المهاجمين السيبرانيين المعادين إن المجتمع العالمي، الذي يتصرف من خلال مجلس الأمن التابع للأمم المتحدة، مسؤول نظريًا عن اتخاذ أي إجراء حقيقي. لكن الأدلة تشير إلى أن التوصل إلى إجماع داخل الأمم المتحدة لمعالجة الإجراءات السيبرانية غير المشروعة التي تتعارض مع الشرعية الدولية والتي توصف بأنها عدوانية أمر نادر للغاية، حيث لا يتخذ المجتمع الدولي إجراءات إلا في حالات استخدام القوة وهو شيء لا تمتلكه الهجمات السيبرانية. لم يمت أحد قط نتيجة لهجوم سيبراني.

وبسبب هذا، لم يتم طرح قضية الأمن السيبراني أمام مجلس الأمن التابع للأمم المتحدة حتى عام ٢٠٢٠، حيث اعتبرت معظم الدول الأعضاء التي لا تشارك بشكل مباشر في الصراع السيبراني هذه القضية قضية غير خطيرة. ومع ذلك، مع تزايد التهديدات المتمثلة في النشاط السيبراني غير القانوني، والاعتماد المتزايد على الشبكات الدولية، وظهور المنافسة بين القوى العظمى، بدأ هذا الموقف يتغير. ولأن الهجمات السيبرانية تشكل مصدر قلق كبير، يعتقد صناع القرار في الأمم المتحدة أنه من أجل معالجة هذه القضية، يجب اتخاذ بعض الإجراءات التي تتوافق مع القانون والمعايير الدولية الراسخة من أجل إرساء المساءلة الدولية.

إن الصعوبة تكمن في أن تفويض مسائل الأمن السيبراني إلى منظمة منفصلة مرتبطة بطرف ثالث لن يحظى بالدعم الدولي. ورغم أنه ثبت من خلال المناقشات أن النظر في قوى سيبرانية كبرى مثل الصين أو الولايات المتحدة أمر صعب، إلا أنها مع ذلك ذكرت أنها ستكون على استعداد للنظر في عدد قليل من الدول الضعيفة، مثل كوريا الشمالية، أو المجرمين السيبرانيين، شريطة أن يكون من الممكن إثبات أنهم لا يتصرفون نيابة عن دولة. إحدى القضايا المتعلقة بالمبادئ التوجيهية لعام ٢٠١٥

[١٦] السيد محمد السيد احمد، ٢٠٢٢، القانون في الفضاء السيبراني، المنصة القانونية على الرابط: http://www.sajplus.com.

هي أنها تتطلب من جميع الدول المشاركة في التحقيق المطلوب لتوضيح تفاصيل الهجوم السيبراني، مما يعقد عملية الإسناد لأنه في حالة وقوع كارثة سيبرانية، من المتوقع أن تعترض الدول على هذا التدخل، وستكون ملزمة بالكشف عن جميع الحقائق ذات الصلة بالحدث. سيكون هناك حد أقصى لقدرة الحكومات على الاعتراض إذا تم ربط حادث سيبراني أو اتهامه بدولة معينة، وفقًا للاقتراح الروسي الذي تم طرحه. بطبيعة الحال، سوف تدحض الصين وروسيا أو ربما أي قوة سيبرانية أخرى هذه المزاعم، ولكن الهدف هو إقناع السلطات الوطنية وعامة الناس في جميع أنحاء العالم، وليس إقناعهم بالاعتراف بالحقيقة. وفيما يتعلق بالشركات الخاصة مثل FireEye أو Cloudstrike، فإنها تستطيع حاليًا تحديد أصل الهجوم الإلكتروني المعادي، ومع ذلك، نظرًا لأن الحكومات لا تستطيع الاتفاق على درجة الإسناد اللازمة للعمل التعاوني، فإن هذا التقدم في تحديد المصدر لا يعترف به المجتمع الدولي[١٧].

إن الرأي الاستشاري لمحكمة العدل الدولية بشأن مشروعية التهديد باستخدام الأسلحة النووية أو استخدامها، والذي نص على أن القواعد والمبادئ الراسخة للقانون الإنساني الدولي المرنطبقة في النزاعات المسلحة تنطبق "على جميع أشكال الحرب وجميع أنواع النزاعات المسلحة"، يشكل حجة قوية لصالح هذا الاستنتاج. ووفقًا للجنة الدولية للصليب الأحمر، فإن استخدام العمليات السيبرانية في النزاعات المسلحة مشمول بهذا الاستنتاج. وبالتالي، يجب على مرتكب الهجوم اتخاذ جميع الخطوات المعقولة لمنع أو تقليل الأضرار العرضية للبنية التحتية المدنية أو الأذى للمدنيين. وهذا يتطلب تحديد نوع الأنظمة التي يتم مهاجمتها والأضرار المحتملة التي قد يلحقها الهجوم؛ بعبارة أخرى، يجب وقف الهجوم بمجرد أن يصبح من الواضح أنه قد يؤدي إلى إصابات أو أضرار غير مقصودة بين المدنيين.

كما تسعى الأمم المتحدة لتعزيز التعاون الدولي في مجال الأمن السيبراني من خلال مجموعة من المبادرات والاتفاقيات. تعمل المنظمة على إنشاء إطار عمل شامل يهدف إلى حماية الدول من الهجمات السيبرانية، ويشمل ذلك تنظيم ورش عمل وتقديم الدعم الفني للدول النامية لتعزيز قدراتها السيبرانية[١٨].

---

[17] James Andrew Lewis, ٢٠٢٢, Creating Accountability for Global Cyber Norms, Op. Cit,p5-8.

[١٨] مايكل شميت، ٢٠١٢، الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكومبيوتر والقانون في الحرب، المجلة الدولية للصليب الأحمر، ص٩١٥.

تعتبر الهجمات السيبرانية من التحديات الكبرى التي تواجه العالم اليوم، حيث تشمل مجموعة واسعة من الأنشطة الضارة التي تستهدف الأنظمة المعلوماتية، في ظل هذا التهديد المتزايد، تلعب الأمم المتحدة دورًا حيويًا في وضع الأطر القانونية والسياسات الدولية لمواجهة هذه التحديات، كما عملت الأمم المتحدة على تطوير إطار قانوني دولي لمواجهة الهجمات السيبرانية. من خلال اللجان والمنتديات، قامت الأمم المتحدة بتعزيز الفهم العام للمسؤوليات القانونية للدول في الفضاء السيبراني، مما يساعد على تحديد قواعد السلوك المقبولة دوليًا، تعمل الأمم المتحدة أيضًا على تعزيز قدرات الدول النامية في مجال الأمن السيبراني. من خلال التدريب وتوفير الموارد، تساعد الأمم المتحدة هذه الدول على تحسين بنيتها التحتية السيبرانية وتطوير استراتيجيات فعالة لمواجهة الهجمات.

تُعزز الأمم المتحدة الوعي حول أهمية الأمن السيبراني من خلال حملات التوعية والتثقيف. تهدف هذه الحملات إلى زيادة الفهم حول المخاطر السيبرانية وكيفية التصدي لها، مما يسهم في بناء مجتمع أكثر أمانًا، رغم الجهود المبذولة، لا تزال أمام الأمم المتحدة تحديات كبيرة في تقنين الهجمات السيبرانية. تشمل هذه التحديات تنامي التكنولوجيا وتطور أساليب الهجوم، مما يتطلب تحديثًا مستمرًا للأطر القانونية والسياسات المعمول بها لمواكبة هذه التغيرات[١٩].

وهنا نستنتج إمكانية تطبيق المبادئ التقليدية على الفضاء الإلكتروني، مثل مبادئ الحفاظ على السيادة في الفضاء الإلكتروني، والامتناع عن استخدام القوة في العلاقات الدولية في الفضاء الإلكتروني، وحل النزاعات في الفضاء الإلكتروني سلمياً، والامتناع عن التدخل في الشؤون الداخلية في الفضاء الإلكتروني. ومن المبادئ التقليدية الأخرى التي يمكن تطبيقها على الفضاء الإلكتروني وضع مبادئ توجيهية للفضاء الإلكتروني الدولي، والتعاون الدولي في الفضاء الإلكتروني، والتحقيق في القضايا الإلكترونية، واحترام حقوق الإنسان في الفضاء الإلكتروني.

المطلب الثاني: الاتفاقيات الدولية في مجال مكافحة الهجمات السيبرانية

الاتفاقيات الدولية المتعلقة بالدفاع ضد الهجمات الإلكترونية من بين أهم أشكال التعاون الدولي بشكل عام وفي مجال منع الجرائم الناجمة عن الهجمات الإلكترونية بشكل خاص الاتفاقيات والمعاهدات الدولية. اتفاقية بودابست لمكافحة الجرائم

[19] James Andrew Lewis, ٢٠٢٢, Creating Accountability for Global Cyber Norms, Center for Strategic and International Studies (CSIS, p1-5.

الإلكترونية ومقترحات المجلس الأوروبي بشأن قضايا الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات هما اثنتان من المعاهدات والاتفاقات التي تهدف إلى مكافحة الجرائم الإلكترونية.

معاهدة بودابست لمكافحة جرائم الانترنت

إن أول معاهدة تتعلق بهذه الجرائم هي اتفاقية بودابست لمكافحة الجرائم الإلكترونية والتي تم التوقيع عليها في ٢٠٠١/١١/٢٣ في بودابست عاصمة المجر، وهي تؤكد على التعاون والتضامن الدولي في مكافحة الجرائم الإلكترونية. والخطوة الأولى نحو بناء وحدة دولية ضد هذه الجرائم المرتكبة عبر الإنترنت وإساءة استخدامها هي التوقيع على هذه الاتفاقية الدولية. بالإضافة إلى الولايات المتحدة الأمريكية وكندا واليابان وجنوب إفريقيا، فقد وافقت على هذه الاتفاقية ٢٦ دولة أوروبية. وتتناول الاتفاقية التي تحتوي على ٤٨ بندًا الأمن العام. وكانت الفصول الأربعة التالية بمثابة الأساس لها[٢٠].

تعتبر معاهدة بودابست لمكافحة جرائم الإنترنت واحدة من أبرز الاتفاقيات الدولية التي تم توقيعها لمواجهة التهديدات المتزايدة التي تطرأ نتيجة استخدام التكنولوجيا الحديثة. تم اعتماد هذه المعاهدة في عام ٢٠٠١ في بودابست، عاصمة المجر، وتستهدف تعزيز التعاون الدولي في مجال مكافحة الجرائم الإلكترونية، تتضمن المعاهدة مجموعة من القوانين والإجراءات التي تهدف إلى مكافحة مجموعة واسعة من الجرائم، مثل اختراق الأنظمة المعلوماتية، والجرائم المتعلقة بالبيانات الشخصية، والجرائم المالية عبر الإنترنت. كما تسعى المعاهدة إلى توفير إطار قانوني يمكن الدول من تبادل المعلومات والتعاون في التحقيقات الجنائية.

تعتبر معاهدة بودابست خطوة هامة في إطار تعزيز الأمن السيبراني، حيث تساهم في تطوير آليات فعالة لمواجهة التهديدات الناجمة عن الجرائم الإلكترونية. إن التنسيق بين الدول في هذا المجال أصبح أمرًا ضروريًا نظرًا للطبيعة العالمية للإنترنت، مما يستدعي استجابة عالمية موحدة، تسعى المعاهدة أيضًا إلى تعزيز الوعي المجتمعي حول مخاطر الجرائم الإلكترونية وسبل الحماية منها. من خلال تنظيم ورش عمل ودورات تدريبية، تُساهم في نشر المعرفة حول الأمان السيبراني وكيفية التصدي للهجمات الإلكترونية، تظل معاهدة بودابست لمكافحة جرائم الإنترنت ركيزة أساسية في الجهود الدولية لمواجهة التحديات التي فرضتها

[٢٠] منير محمد الجهيني، ٢٠١٩، جرائم الانترنت والحاسب الالي ووسائل مكافحتها، دار الفكر العربي، الإسكندرية، ص ٩٦.

التكنولوجيا الحديثة. ومع تزايد الاعتماد على الإنترنت في مختلف مجالات الحياة، يبقى الالتزام بتطبيق بنود هذه المعاهدة ضرورة ملحة لضمان سلامة الفضاء الرقمي.

توصيات المجلس الأوروبي

يعتبر المجلس الأوروبي من المؤسسات الرائدة في تعزيز الأمن السيبراني على مستوى القارة. وقد قدم مجموعة من التوصيات لمكافحة الهجمات السيبرانية، بهدف تعزيز التعاون بين الدول الأعضاء وتحسين استجابتها لهذه التهديدات المتزايدة. تتضمن هذه التوصيات استراتيجيات شاملة تهدف إلى حماية البنية التحتية الحيوية والمعلومات الحساسة، تسعى التوصيات إلى تعزيز تبادل المعلومات بين الدول الأعضاء حول الهجمات السيبرانية وأساليب التصدي لها. يعتبر هذا التعاون ضروريًا لمواجهة التهديدات العابرة للحدود، حيث أن الكثير من الهجمات لا تتوقف عند حدود الدول. من خلال تبادل البيانات والخبرات، يمكن للدول تعزيز قدراتها في التعرف على الهجمات والرد عليها بشكل أسرع وأكثر فعالية.

كما تركز التوصيات على أهمية تعزيز القدرات الوطنية في مجال الأمن السيبراني. يتعين على الدول تطوير استراتيجيات وطنية واضحة تتضمن التدريب والتوعية، بالإضافة إلى إنشاء وحدات متخصصة للتعامل مع الحوادث السيبرانية. إن الاستثمار في التعليم والتدريب في هذا المجال يعد خطوة حيوية لضمان وجود كوادر قادرة على التصدي للهجمات، تشدد التوصيات أيضًا على ضرورة تعزيز الشراكة بين القطاعين العام والخاص. يجب أن تعمل الحكومات مع الشركات الخاصة لتطوير حلول أمنية فعالة، حيث أن الكثير من الهجمات تستهدف المؤسسات التجارية. يمكن أن تسهم الشراكات في تطوير تقنيات جديدة وتعزيز البحث والتطوير في مجال الأمن السيبراني[٢١].

أصدر المجلس الأوروبي التوصية رقم ١٣/٩٥ بتاريخ ١٩٩٥/١١/٩م بشأن قضايا الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات، وحثت التوصية الدول الأعضاء على مراجعة قوانين الإجراءات الجنائية الوطنية لديها لمواكبة التطور في هذا المجال

[٢١] خالد محمد نولا عبد الحميد الطباخ، ٢٠١٧، المواجهة القانونية للإرهاب الالكتروني الدولي، مجلة الدراسات القانونية والاقتصادية، جامعة السادات، مجلد (٣)، عدد (١) ص ٣٢.

بسبب التقدم السريع في تكنولوجيا الكمبيوتر والإنترنت، فضلاً عن وعي الدول الأوروبية بأهمية مراجعة الإجراءات الجنائية في هذا المجال، وفيما يلي بعض أهم البنود في توصية المجلس الأوروبي[٢٢]:

١. ستوضح القوانين كيفية تفتيش أجهزة الكمبيوتر، وما هي المعلومات التي يمكن مصادرتها منها، وكيف تتم مراقبة المعلومات أثناء نقلها.
٢. موجب نفس شروط عمليات التفتيش العادية، ستمكن الإجراءات الجنائية الوطنية سلطات التفتيش من مصادرة برامج الكمبيوتر والبيانات من الأجهزة. إن إخطار الشخص الذي يتحكم في الأجهزة بأن النظام كان خاضعًا للتفتيش، وتحديد المعلومات التي تم مصادرتها، وتوفير إجراءات استئناف متكررة ضد القرارات المتخذة بشأن مصادرة وفحص البيانات كلها ضرورية.
٣. يجوز لسلطات التنفيذ فحص أنظمة كمبيوتر إضافية تحت سيطرتها ومتصلة بالنظام قيد التفتيش وأخذ المعلومات منها أثناء عملية التفتيش، طالما أنها تلتزم بالضمانات المحددة.
٤. سيوضح قانون الإجراءات الجنائية أن بيانات الكمبيوتر تخضع لنفس الإجراءات التي تخضع لها معلومات المستندات التقليدية.
٥. في حالة الحاجة إلى استخدام وسائل المراقبة والتسجيل باستخدام تكنولوجيا المعلومات، فيجب استخدامها في مجال التحقيق الجنائي، بالإضافة إلى ذلك، يجب التعامل مع المعلومات الخاضعة لحماية قانونية خاصة بسرية واحترام.

في الختام، تبرز توصيات المجلس الأوروبي كخطوة استراتيجية لمواجهة التحديات المتزايدة في مجال الأمن السيبراني، إن الالتزام بتنفيذ هذه التوصيات سيساهم في تعزيز القدرات الدفاعية للدول الأعضاء ويعزز من الاستقرار الرقمي في المنطقة الأوروبية.

النتائج

١. تؤدي الهجمات السيبرانية إلى تهديدات مباشرة للأمن الوطني للدول. يمكن أن تستهدف هذه الهجمات البنية التحتية الحيوية مثل أنظمة الطاقة والمياه والنقل، مما يؤدي إلى تعطيل الخدمات الأساسية وإحداث فوضى في المجتمع.

[٢٢] محمد عادل محمد عسكر، ٢٠١٧، وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسس وقت السلم، ص ٣٠٨.

بالإضافة إلى ذلك، قد تستخدم مجموعة من الدول الهجمات السيبرانية كأداة للتجسس أو التأثير على السياسات الداخلية للدول المستهدفة، مما يزيد من توتر العلاقات الدولية.

٢. تؤدي الهجمات السيبرانية إلى تآكل الثقة في الأنظمة الرقمية، مما يؤثر على الأفراد والشركات على حد سواء. عندما تتعرض البيانات الشخصية أو المعلومات الحساسة للاختراق، يشعر الأفراد بعدم الأمان في استخدام الإنترنت، مما قد يؤدي إلى تقليل الاعتماد على الحلول الرقمية. هذا التدهور في الثقة يمكن أن يؤثر أيضًا على الابتكار والنمو الاقتصادي، حيث تتجنب الشركات الاستثمار في تكنولوجيا جديدة بسبب المخاطر المحتملة.

٣. تتسبب الهجمات السيبرانية في تكاليف اقتصادية باهظة للدول والشركات. تشمل هذه التكاليف فقدان الإيرادات بسبب تعطيل العمليات، وتكاليف استعادة البيانات المتضررة، ونفقات التحقيق في الحوادث. وفقًا للتقديرات، قد تصل الخسائر الناتجة عن الهجمات السيبرانية إلى مليارات الدولارات سنويًا، مما يؤثر على الاستقرار المالي للدول والشركات ويزيد من العبء على الموارد العامة.

٤. تنبه الهجمات السيبرانية الدول إلى ضرورة تعزيز التشريعات المتعلقة بالأمن السيبراني وتطوير استراتيجيات مشتركة لمواجهتها. يتطلب ذلك إنشاء أطر قانونية واضحة وموحدة لمكافحة الجرائم السيبرانية، وتعزيز التعاون بين الدول في مجال تبادل المعلومات والتنسيق في التحقيقات. هذه الحاجة الملحة للتعاون الدولي تدفع الدول إلى العمل معًا لبناء استجابة شاملة وفعالة لمواجهة التهديدات السيبرانية المتزايدة.

توصيات

١. يجب على الدول العمل على تعزيز التعاون الدولي في مجال مكافحة الجرائم السيبرانية. يتطلب ذلك إنشاء شبكة من الشراكات بين الدول لمشاركة المعلومات حول التهديدات السيبرانية وأساليب الهجوم. يمكن أن تشمل هذه الشراكات تبادل البيانات الاستخباراتية، وتنسيق الجهود في التحقيقات، وتطوير استراتيجيات مشتركة لمكافحة الجريمة. كما ينبغي تأسيس منتديات دولية للتباحث حول التحديات السيبرانية وتنسيق الردود عليها.

٢. من الضروري أن تعمل الدول على تطوير إطار قانوني موحد لمكافحة الهجمات السيبرانية. ينبغي أن يتضمن هذا الإطار تعريفات واضحة للجرائم السيبرانية، وعقوبات رادعة للجناة، وآليات للتعاون القضائي بين الدول. بالإضافة

إلى ذلك، يجب أن تُعزز القوانين المحلية لتتوافق مع المعايير الدولية، مما يسهل عملية التحقيق والمقاضاة للأفراد أو الجماعات المتورطة في الجرائم السيبرانية.

٣. يجب أن تُبذل جهود كبيرة لزيادة الوعي حول مخاطر الهجمات السيبرانية، سواء على مستوى الأفراد أو المؤسسات. يمكن تحقيق ذلك من خلال حملات توعية وتدريب متخصص. يجب على المؤسسات الحكومية والخاصة تنظيم ورش عمل ودورات تدريبية لتعليم الموظفين كيفية التعرف على التهديدات السيبرانية وطرق الحماية منها. كما يجب دعم التعليم الأكاديمي في مجالات الأمن السيبراني لتخريج كوادر مؤهلة لمواجهة هذه التحديات.

٤. يتطلب حماية البنية التحتية الحيوية للدول استثمارات كبيرة في الأمن السيبراني. ينبغي أن تُعد خطط طوارئ شاملة للتصدي للهجمات المحتملة، بالإضافة إلى تنفيذ تقنيات متقدمة للكشف عن التهديدات والاستجابة السريعة. يجب أن تشمل هذه الخطط التعاون بين القطاعين العام والخاص لضمان تنفيذ معايير أمان عالية، وتبادل المعلومات حول نقاط الضعف، مما يسهم في تعزيز مستوى الأمان العام.

الخاتمة

تعتبر الهجمات السيبرانية من أبرز التحديات التي تواجه المجتمع الدولي في العصر الرقمي. حيث تندرج هذه الهجمات تحت فئة الجرائم الدولية، نظرًا لتأثيراتها العابرة للحدود وقدرتها على الإضرار بالأمن القومي والاقتصادي للدول. إن الطبيعة العالمية للإنترنت تجعل من الصعب تحديد مصدر الهجوم أو محاسبة الجناة، مما يستدعي تعاونًا دوليًا فعالًا لمواجهة هذه الظاهرة.

يتطلب التصدي للهجمات السيبرانية وضع استراتيجيات شاملة تشمل تعزيز التعاون بين الدول وتبادل المعلومات حول التهديدات وأساليب التصدي لها. كما يجب على الدول تطوير إطار قانوني متكامل يتيح لها التعامل مع الجرائم السيبرانية بفعالية، وتوفير التدريب والموارد اللازمة للأجهزة الأمنية لمواجهة هذه التحديات. إن تعزيز القدرات التقنية والرقابية يعد أمرًا حيويًا لضمان حماية المعلومات والبنية التحتية الحيوية.

إن القضية الرئيسية التي تطرحها هذه الدراسة تتلخص في حداثة الهجمات السيبرانية ودخولها القسري في سباق التسلح كسلاح أو إحدى أدوات الصراعات المسلحة، مع ما يترتب على ذلك من عواقب قانونية وعملية كبيرة، خاصة في ظل الفجوة في النظام القانوني للقانون الإنساني الدولي الذي يحكم الهجمات السيبرانية. وبالتالي، فإن القضية الرئيسية للدراسة تتركز حول مدى إمكانية تغطية الهجمات السيبرانية من قبل القانون الإنساني الدولي.

في النهاية، يجب أن يكون التصدي للهجمات السيبرانية أولوية عالمية، مع تزايد الاعتماد على التكنولوجيا في جميع جوانب الحياة، يصبح من الضروري وضع تدابير فعالة لحماية الفضاء السيبراني. من خلال التعاون الدولي وتبادل الخبرات، يمكن أن نحقق تقدمًا كبيرًا في مواجهة هذه الجرائم، مما يسهم في تعزيز الأمن السيبراني واستقرار المجتمعات على مستوى العالم.

المراجع

١. احمد عبيس نعمة الفتلاوي، ٢٠١٦، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، جامعة بابل، كلية القانون، المجلد (٨) العدد (٤)، ص ٦٨٧-٦١٠.

٢. خالد محمد نولا عبد الحميد الطباخ، ٢٠١٧، المواجهة القانونية للإرهاب الالكتروني الدولي، مجلة الدراسات القانونية والاقتصادية، جامعة السادات، مجلد (٣)، عدد (١) ص ٣٢.

٣. زق أحمد سمودي، ٢٠١٨، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية، ص ٣٣٨.

٤. السيد محمد السيد احمد، ٢٠٢٢، القانون في الفضاء السيبراني، المنصة القانونية على الرابط: http://www.sajplus.com.

٥. عادل عبد الصادق، ٢٠١٦، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، مكتبة المستقبلية، مصر، ص٩٦.

٦. عبد الصادق، ٢٠١٦، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، مكتبة المستقبلية، مصر، ص١٠٠.

٧. اللجنة الدولية، ٢٠١٥، القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة، ص٥٧.

٨. مايكل شميت، ٢٠١٢، الحرب بواسطة شبكات الاتصال: الهجوم على شبكات الكومبيوتر والقانون في الحرب، المجلة الدولية للصليب الأحمر، ص٩١٥.

٩. محمد حسن سعيد دراجي، ٢٠٢٤، الهجمات السيبرانية وفقا لأحكام القانون الدولي الإنساني، مجلة علوم الشريعة والقانون، المجلد (٥١) العدد (١) ص ٢.

١٠. محمد عادل محمد عسكر، ٢٠١٧، وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسس وقت السلم، ص ٣٠٨.

١١. منير محمد الجهيني، ٢٠١٩، جرائم الانترنت والحاسب الالي ووسائل مكافحتها، دار الفكر العربي، الإسكندرية، ص ٩٦.

١٢. وفاء لطفي، ٢٠٢٢، الجهود الدولية في مجال مكافحة جرائم الارهاب السيبراني: التجربة الماليزية نموذجا، مجلة كلية الاقتصاد والعلوم السياسية، المجلد (٢٣) العدد (١)، ص ١٥٣.

١٣. يحي ياسين سعود، ٢٠٢٠، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، المجلة القانونية، ص ٨٢.

المراجع الأجنبية

1. Heather Harrison Dinniss, 2018, The status and use of computer network attacks in international law, Phd thesis, London school of a economics and Political science, p. 33.
2. Herbert Lin, 2012,Cyber conflict and international humanitarian law International review of the red cross, Vol. 94, N886, p.515.
3. James Andrew Lewis, ٢٠٢٢, Creating Accountability for Global Cyber Norms, Op. Cit,p5-8.
4. James Andrew Lewis, ٢٠٢٢, Creating Accountability for Global Cyber Norms, Center for Strategic and International Studies (CSIS, p1-5.
5. Jeffrey T. G Kelsey, 2018, Hacking in to international humanitarian law: The principles of distinction and neutrality in the age of cyber warfare, Michigan law review, Vol. 106, No.7, p.1437.

6. Andreea bendovschi, 2015, cyber –attacks – trends, patterns and security counter measures, procedia economics and finance, Elsevier, Vol .28, p. 3.