المسؤولية الدولية الناجمة عن الهجمات السيبرانية

بسمة صلال طه *

كلية القانون والعلوم السياسية - جامعة البيان

Article Info

Received: Oct 2023 **Accepted:** Nov 2023

Author email: Basma.s@albayan.edu.iq

Orcid: https://orcid.org/0009-0003-6247-2716

الخلاصة

الهجمات السيبرانية من التحديات الصعبة التي تواجه القائمين على تطبيق قواعد القانون الدولي العام، ويرجع ذلك إلى صعوبة تحديد طبيعتها وعناصرها، مما يؤثر سلبا على الأمن والسيادة الدولية، اذ ان التطور الالكتروني الهائل الذي نعيشه اليوم أدى الى نشوء تحديات جديدة في المجتمع الدولي ومن هذه التحديات (الهجمات السيبرانية)، فأصبح بإمكان الدول التأثير على بعضها البعض عن طريق الهجوم على البنية التحتية الأساسية بكبسة زر واحدة ورغم ذلك إحداث اثار مدمرة سواء في الحجم الدمار البشري أو المادي. أن المعالم الدقيقة للهجمات السيبرانية لا زالت غير محددة لذلك خصصنا هذه الدراسة للبحث في مفهوم الهجمات السيبرانية ومن ثم تحديد أساس المسؤولية الدولية الخاصة بالهجمات السيبرانية في المجتمع الدولي.

الكلمات المفتاحية: (المسؤولية الدولية، الهجمات السيبرانية، قانون دولي انساني).

---

international responsibility liability resulting from cyber attacks

Basma Salal Taha *

**** College of La and political science, Al Bayan University***

Abstract

Cyber-attacks have become one of the difficult challenges facing those in charge of applying the rules of public international law. This is due to the difficulty of determining their nature and elements, which in turn affects international security and sovereignty. Therefore, the research aims to identify international responsibility for cyber-attacks, in order to achieve the goal The research and solution to its problem depends on the descriptive and analytical approach, and the research reached many results, the most important of which is that the cyber-attack depends on the use of the latest advanced technical methods, meaning that it reflects the tremendous development in the technological revolution, Therefore, the keyboard and computer software have become more destructive and dangerous to the world. Therefore, cyber attacks have become low cost. Electronic or cybercrimes, as international cross-border crimes, are combated under international law. Therefore, the international community is responsible for these attacks as a result of the damage they cause to another country. The study recommended the need to reconsider international law, and add legal texts that include effective sanctions and punishments for the perpetrators of this type of crime.

Keywords:(international responsibility, cyber-attacks, international humanitarian law).

المقدمة

ساهمت تكنولوجيا المعلومات على المستوى العالمي إلى تغيير طبيعة النظرة في العديد من المجالات، فقد أصبحت معظم خدمات العالم تعتمد على الشبكة العنكبوتية بصورة جوهرية وأساسية، ومع التحول العالمي نحو تطبيق التكنولوجيا في كافة القطاعات والمجالات، أدى ذلك إلى تغيير طبيعة الحرب المستقبلية من خلال قدرتها الفائقة على التسلل لشبكة المعلومات واختراقها، ويمكن إرجاع ذلك إلى التطور المماثل في طبيعة البرمجيات والحواسيب الإلكترونية.

وفي ظل الاعتماد المتزايد على الشبكة العنكبوتية وظهور ما يسمي بقراصنة المعلومات، الذين يمتلكون القدرة والخبرة الفائقة للتعامل مع أحدث البرمجيات، التي تُمكنهم من اقتحام نُظم الاتصال، وقد يطلق عليهم (الهاكرز) فهم مجموعة مؤهلة للعمل الحاسوبي والإلكتروني. يقوموا باستهداف المواقع الإلكترونية الحيوية بالدول واختراقها والحصول على أسرارها، سواء من أجل جني المال أو التدمير[1]. وقد حذر خبراء الأسلحة من أن التقدم الكبير في تقنيات الحرب المعلوماتية ينتج عنه تطوير أسلحة ذكية يصعب السيطرة عليها. ولذلك يهتم البحث بالتعرف على المسؤولية الدولية الناتجة عن الهجمات السيبرانية.

مشكلة البحث

مع بداية الألفية الثالثة شهد العالم ثورة من التطور الهائل في المجال التقني بشكل عام، فقد رافق هذا التطور تطور مماثل في طبيعة الجريمة وانتشارها، مما أدى ذلك إلى وقوع العديد من المخاطر والتحديات، ولذلك يعد الهجوم الإلكتروني من التحديات الصعبة التي واجهت القائمين على تطبيق القانون الدولي، ويرجع ذلك لصعوبة تحديد طبيعة وعناصر هذه الجريمة، اذ يترتب عليها تبعات مسؤولية الدولة عن الأضرار التابعة بهذه الجريمة، وبناء على ما تقدم نجد أن بعض الدول تقوم بهذه الهجمات بالاعتماد على قراصنة محترفين في هذه الجرائم. وتكمن مخاطر هذه الهجمات في القدرة والسيطرة على الأنظمة والمؤسسات الدولية عن بعد. من خلال عمليات التسلل الإلكتروني واختراق الأجهزة، وبالتالي الوصول إلى المعلومات واستخدامها بما يحقق الهدف من عملية الاختراق. ولذلك أصبحت عملية[2] اختراق الأنظمة والأجهزة الدولية والوصول إلى البيانات على مستوى القطاعات كافة (الإنتاجي، الصناعي- الزراعي)، وبالتالي يمثل ذلك التحدي درجة عالية من الخطورة على الأمن والسيادة الدولية[3]. وفي ظل الانتشار الهائل لهذه الهجمات في الوقت الراهن نتيجة ارتباط العالم بالفضاء الإلكتروني، واجهت الدول العديد من المخاطر التي تمس بأمن وسيادة الدول، فلذلك تتمثل المشكلة البحثية في التعرف على مدى مسؤولية الدول عن وقوع وتنفيذ هذه الهجمات.

أهمية البحث

في العصر الحالي أصبح الهجوم الإلكتروني (السيبراني) يشكل أعلى التحديات على الأمن الوطني، من خلال تأثيرها المباشر على أمن وسيادة الدول، أذ يتم ذلك الهجوم بشكل غير مسلح، عن طريق اختراق الأجهزة الدولية وسرقة المعلومات المخزنة وتدميرها، وذلك من خلال القدرة الفائقة في المجال التقني التي يتمتع بها هؤلاء الفئة في اختراق المجال المعلوماتي للدول والقيام بعمليات التجسس والتخريب لشبكات المعلومات الدولية، مما يؤدى إلى الأضرار بمصالح الدول وتهديد آمنها واستقرارها، ومع تزايد الهجمات الإلكترونية (السيبرانية) في الآونة الأخيرة وتحولها السريع إلى نموذج حديث من الحرب، التي ظهر للمرة الأولى علناً في النزاع الدولي المسلح عام

---

[1] - حكيم، قطافي، حرب المعلومات المفهوم والتطبيق – دراسة وصفية تحليلية، رسالة ماجستير غير منشورة، جامعة الجزائر، كلية العلوم السياسية، (٢٠٠٥-٢٠٠٦)، ص ٥.

[1] - العيسي، طلال ياسين، عناب، عدي محمد، المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مجلة الزرقاء للبحوث والدراسات الإنسانية، المجلد التاسع عشر، العدد الأول، (٢٠١٩)، ص ٨٢ .

[3] - خليفة، إيهاب، مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي، القاهرة: العربي النشر والتوزيع،(٢٠١٩)، ص ١١٤- ١١٥.

(٢٠٠٨) بين جورجيا وروسيا، بالإضافة إلى استخدامها في الحرب الواقعة بين روسيا وأوكرانيا[1]، وقد أدى ذلك صعوبة تحديد الجهة المنفذة لهذه الهجمات، بسبب عدم وجود أساس قانوني لتنظيم هذه الهجمات، من هذا المنطلق تكمن أهمية البحث في كونه يساهم في تحديد المسؤولية عن هذه الهجمات، بما يفيد ذلك في توقيع الجزاء على كل المخالفين والخارجين عن مبادئ وأحكام القانون ليكون ذلك رداع خاص للحد من سرعة انتشار هذه الهجمات.

أهداف البحث

يهدف البحث إلى تحديد المسؤولية الدولية الناجمة عن الهجمات السيبرانية، ومن أجل تحقيق هدف البحث يسعى البحث إلى التعرف على طبيعة مسؤولية الدولة عن هذه الهجمات الإلكترونية.

منهج البحث

من أجل تحقيق هدف البحث يعتمد الباحث على تطبيق المنهج التحليلي الوصفي من خلال استعراض ماهية وطبيعة هذه الهجمات- تحليل مبادئ وقواعد القانون الدولي، والتعرف على مدى إمكانية تطبيقها على الهجمات الإلكترونية.

خطة البحث

ومن أجل تحقيق هدف البحث فقد تم تقسيمه إلى مبحثين رئيسيين يتمثلان في التالي:

- **المبحث الأول: الأساس النظري للهجمات الإلكترونية (السيبرانية)**
- **المبحث الثاني: أساس المسؤولية الدولية الخاصة بالهجمات السيبرانية**

المبحث الأول
الأساس النظري للهجمات (الإلكترونية) السيبرانية

على الرغم من دور ثورة المعلومات والإتصالات في احداث العديد من الآثار الإيجابية على مستوى المجالات والقطاعات كافة، إلا أنه قد صاحب هذا التطور بعض الانعكاسات والآثار السلبية من وراء استخدام وتطبيق هذه التكنولوجيا، ومن ثم فهي سلاح ذو حدين، اذ قد يتم استخدامها بطرق وأساليب غير مشروعة، مما يهدد ذلك الآمن والاستقرار الدولي، ولذلك ففي ظل هذه التكنولوجيا فقد شهد العالم نوعًا جديدًا من سباق التسلح، اذ قد تغيرت من خلاله أنماط الحروب وطبيعة النزاعات التي أصبحت تشن من خلال الهجوم الإلكتروني على قطاعات الدولة الحيوية، ومن ثم الوصول للمعلومات، والعمل على نسخها أو حذفها أو تحطيم أنظمة التشغيل، والتعدي على خصوصية المعلومات وإساءة استخدامها بما يلحق به الضرر ويمس بأمن وسيادة الدولة[2]، وفي ضوء ذلك سنتطرق في هذا المبحث الأساس القانوني للهجمات الإلكترونية(السيبرانية) من خلال مطلبين رئيسيين:

المطلب الأول
مفهوم الهجمات الإلكترونية (السيبرانية)

مصطلح الهجمات الإلكترونية أو السيبرانية من المصطلحات التي ظهرت في الأونة الأخيرة، يقابلها في الواقع العديد من المسميات (الحرب السيبرانية –الإلكترونية- الحرب الافتراضية)، من خلال هذه الهجمات يقوم القراصنة

[1] Schmitt, Michael N., The Law of Cyber Warfare: Quo Vadis? (September 4, 2013). 25 Stanford Law & Policy Review, p 270, (Available at SSRN: https://ssrn.com/abstract=2320755

[2]- **عبد اللطيف سامر مؤيد، الحرب في الفضاء الرقمي رؤية مستقبلية، مجلة رسالة الحقوق، السنة السابعة، العدد الثاني، (٢٠١٥)، ص ٩٠.**

بمهاجمة واختراق الملفات والمواقع المستهدفة من قبل هؤلاء القراصنة، بقصد تدميرها والسيطرة عليها والتحكم فيها، ومن ثم يمكن تحديد مفهومها في التالي.

الفرع الأول
معنى السيبراني في اللغة والأصطلاح

يرجع ظهور ذلك المصطلح إلى ظهور ثورة المعلومات، وسنتعرف على معنى ذلك المفهوم في اللغة والاصطلاح.

أولا: مفهوم السيبرانية في اللغة

سيبراني (Cyber هي كلمة أصلها يوناني) ظهرت في بداية الأمر في مؤلّفات الخيال العلمي، وكانت تشير إلى القيادة أو التحكم عن بعد . أما في قاموس المورد: فقد اشار إليها على أنها علم التحكم ومصدره هو علم التحكم الآلي، أذ يتوافق هذا المصدر مع مفهوم الهجوم الإلكتروني أي التحكم والسيطرة على الأشياء عن بعد[1]. ومن خلال النظر في الوثائق الصادرة عن الأمم المتحدة ، والمطبوعات والمقالات المتعلقة باللجنة الدولية للصليب الأحمر، أتضح استخدمهما مصطلح السيبرانية. ولذلك، فإن هذا المصطلح موجود في الواقع القانوني منذ فترة طويلة.[2].

ثانيا
مفهوم السيبرانية في الاصطلاح

عرفه الفقيه فيورتس على أنه: "هجوم يتم عبر الإنترنت ينفذ من التسلل حتى يتم الوصول للمواقع الإلكترونية واختراقها، الوصول للمعلومات، ومن ثم القيام بتدمير أنظمة التشغيل، والأضرار بنظام الدولة التي تمت اختراقها.[3] أدى التطور السريع في الاعتماد على الفضاء السيبراني، والاستخدام الواسع جدًا للأفراد والمنظمات والمؤسسات على مستوياتها كافة، إلى زيادة الاعتماد عليه، مما جعل الاستغناء عنه مستحيلًا. فقد أصبح الاعتماد على الأمن السيبراني والفضاء السيبراني والبنية التحتية لأي دولة، ومن ثم فإن الضرر المتعمد له يمثل تهديدًا للأمن القومي للبلد المستهدف، وهذا يفسر سبب إدراج معظم دول العالم لمسألة الأمن السيبراني كأحد أولوياتها الأمنية الوطنية ولذلك فتعد الهجمات الإلكترونية سلاح من أخطر أضخم أنواع الأسلحة المستخدمة في الحروب الدولية، نتيجة لقدرته الفائقة على اختراق شبكات المعلومات عبر الحدود الدولية، ولذلك أصبحت لوحة المفاتيح وبرمجيات الحاسب أكثر دماراً وخطراً على العالم، وبالتالي يطلق على حرب المعلومات (الحرب السيبرانية).

ثالثا: معنى الهجمات السيبرانية

ينظر للهجوم الإليكتروني (السيبراني) بأنه: (عملية إساءة استخدم أنظمة الكمبيوتر والشبكات المعتمدة على التكنولوجيا عن عمد من خلال البرمجيات الخبيثة والضارة)[4]. وينظر إليها البعض الأخر بأنها:(الإجراءات التي تتخذها بعض الدول بهدف مهاجمة أنظمة معلومات العدو ومن ثم التأثير عليها والدفاع عن أنظمة معلومات الدولة المهاجمة).[5]

---

[1] **منير البعلبكي، المورد: قاموس – انكليزي- عربي، دار العلم للملايين، بيروت، ٢٠٠٤، ص٢٤٣.**

[2] الموصلي، نور أمير، الهجمات السيبرانية في ضوء القانون الدولي الإنساني، رسالة ماجستير غير منشورة، الجامعة الافتراضية السورية،(٢٠٢١)، ص ٩ .

[3] الفتلاوي، أحمد عبيس نعمة، الهجمات السيبرانية، دراسة تحليلية بشأن تحليلية لشأن تحديات تنظيمها المعاصر، منشورات زين الحقوقية بيروت لبنان ،(٢٠١٨)، ص ١٦ .

[4] - Junaidu Bello Marshall, 2000, Cyber attacks (the legal response, International journal of international law) , Vol 01 , Is 02 , universal multidisciplinary research institute , India., P. 3 .

[5] سامية، صديقي، المسؤولية الدولية المترتبة عن الهجوم السيبراني في منظور القانون الدولي، مجلة البحوث القانونية والاقتصادية، المجلد السادس ، العدد الأول،(٢٠٢٣)، ص ٨٢٤ .

ومن خلال ما تقدم، يمكن وصف الهجمات الإلكترونية على أنها: (عبارة عن تصرف فعلي أو واقعي يدور في عالم غير واقعي يتم افتراضه قائم على استخدام البيانات الرقمية ووسائل اتصال تعمل بشكل إلكتروني، يستهدف اختراق المواقع الحيوية والحساسة على مستوى القطاعات كافة)، من أجل تحقيق أهداف مختلفة قد تكون أمنية أو عسكرية ملموسة، وذلك عن طريق القراصنة[1]. ولذلك نرى بأن تلك الهجمات هو محاولة متعمدة لاختراق أنظمة المعلومات الخاصة بفرد أو مؤسسة أو دولة، بهدف الحصول على مكاسب أو تعطيل الشبكة، وذلك عن طريق إنشاء نظـامٍ أو برنـامجٍ إلكتروني يسعى إلى القيام باستغلال معلومات الخصم وتدميرها، بخلاف إتلاف الأجهزة الإلكترونية الخاصة به. ومن خلال عرض وتحليل بعض المفاهيم الخاصة بالهجمات السيبرانية يمكن تحديد خصائصها على النحو التالي:

- تتسم تلك الهجمات بأنها هجمات تعتمد على استخدام أحدث الأساليب التقنية المتطورة، ومن ثم فهي عكست التطور الهائل في الثورة التكنولوجيا.
- أدت تلك الهجمات إلى تغيير أساليب ووسائل القتال المعروفة[2]، اذ تخترق شبكات المعلومات عبر الحدود الدولية، ومن خلالها أصبحت لوحة المفاتيح وبرمجيات الحاسب أكثر دماراً وخطراً على العالم. ويرجع ذلك إلى أنها ذات تكلفة متدنية.
- أن الهجمات الإلكترونية تدار عن بعد، اذ أنها تتسم بأهدافها المتعددة، كما يقوم الهدف من ذلك الهجوم إيقاف شبكة المعلومات المستهدفة وذلك خلال وقت قصير، مما يؤدي إلى تعطيل ومنع الدولة المستهدفة من الاستفادة من الشبكة[3].

الفرع الثاني
نشأة وتطور الهجوم الإلكتروني (السيبراني)

ساهم ظهور ثورة المعلومات في نشأة العديد من المتغيرات على مستوى المجالات كافة بصفة عامة، والمجال الأمني والعسكري بصفة خاصة، فقد أحدث استخدامها في الأغراض العسكرية والحروب الحديثة تطور هائل في إدارة الصراع وتحقيق الأهداف[4]. ولعل من أهم هذه المتغيرات ظهور مصطلح الهجمات أو الحرب السيبرانية، اذ أصبحت تمثل جانب من جوانب الثورة في الشؤون العسكرية، ومن ثم غيرت في طبيعة الحرب المستقبلية من خلال قدرتها الفائقة على اختراق المجال المعلوماتي للدول والأضرار بها، عن طريق عمليات التسلل والتخريب على الشبكات الدولية[5]، وبذلك يمكن القول بأن ثورة المعلومات غيرت في أنماط وطبيعة الحروب والصراعات، وأن التغلب عليها يرجع إلى مدى الاعتماد الدولي على التطور التقني في وسائل وأساليب تكنولوجيا المعلومات والاتصالات فأن امتلاك هذه الأساليب يحقق التفوق والسيطرة في ميادين الحروب .

ولذلك فأن ظهور التطور التقني كانت من العوامل الرئيسية التي ساعدت ظهور الجرائم الإلكترونية، بخلاف قصور القواعد القانونية التي تعالج الجرائم الإلكترونية في القانون الدولي، مما ساهم ذلك بدوره في نشأة وتطور الحرب الإليكترونية[6] .

المطلب الثاني
التكييف القانوني للهجمات السيبرانية

---

[1] العيسي، طلال ياسين، عناب، عدي محمد، مرجع سابق ذكره، ص ٨٣ – ٨٤ .

[2] سعود، يحيي ياسين،(الحرب السيبرانية في ضوء قواعد القانون الدولي الانساني)، المجلة القانونية في البحوث والدراسات القانونية،(٢٠١٩)، ص٨٢.

[3] : John Richardson , Stuxnet as cyberwarfare : Applying the law of war to the Virtual attlefield ,JMR Portfolio Intelligence,2011,p9. Available at www.assrn.com/abstract=1892888

[4] - عبد اللطيف سامر مؤيد، مرجع سابق ذكره، ص ٧٤.

[5] - حكيم، قطافي، حرب المعلومات المفهوم والتطبيق – دراسة وصفية تحليلية، رسالة ماجستير غير منشورة، جامعة الجزائر، كلية العلوم السياسية،(٢٠٠٥-٢٠٠٦)، ص ٥.

[6] علي سنوسي، الهجمات السيبرانية في ضوء أحكام قواعد القانون الدولي الإنساني والاتفاقيات الدولية، مجلة الحقوق للعلوم السياسية جعة خنشلة، المجلد الأول، العدد الثاني، (٢٠٢٣)، ص ٢٤٩ .

أثار الهجوم الإلكتروني (السيبراني) العديد من الجدل ويرجع ذلك إلى جسامة وخطورة الهجوم على المستوى الدولي، ومدى قدرته الفائقة على المساس بالأمن القومي والسيادة الدولية[1]، ولذلك أصبحت تلك الهجمات أحد وسائل الصراعات الحديثة بين الدول نتيجة إلى زيادة سرعتها وقلة تكلفتها، اذ يمكن لأي دولة من خلالها القيام بتعطيل منشآت الدولة الحيوية وبنيتها التحتية على نطاق واسع وفي ثواني معدودة، لأن طبيعتها لا تحتاج إلى ميدان قتال، ولا إعلان للحرب، بل تحتاج إلى قدرة على عملية الاختراق لأنظمة المعلومات المتعلقة بمؤسسات وهيئات الدول وفرض السيطرة عليها عن بعد، ولذلك تعد الجرائم السيبرانية لا أرض ولا وطن لها. ومن ثم نناقش تكييف هذه الهجمات وفقاً للمبادئ الأساسية للقانون الدولي على النحو التالي.

الفرع الأول
الوصف القانوني للهجمات السيبرانية

شكلت الهجمات الإلكترونية تهديداً وتحدياً خطيراً لأحد المبادئ الرئيسة في القانون الدولي، وهو العمل على احترام سيادة الدول على اعتبار أن ذلك الأمر يمثل واجب أساسي وهو "عدم التدخل" ولذلك نص الميثاق الخاص بالأمم المتحدة (المادة الثانية / الفقرة ٤) بمنع التهديد باستعمال القوة أو استخدامها ضد سلامة الأراض، ولذلك يعد وضع الهجوم الإلكتروني أو السيبراني ضمن الإطار القانوني الدولي أمر صعب للغاية، ويمكن أن يعزى ذلك إلى الطبيعة الخاصة للمخاطر القانونية. فضلا عن عدم وجود نظام قانوني رسمي يتعلق بشأن هذا الموضوع الحديث[2] .

ولذلك غالباً ما يكون الهدف الرئيسي من الهجوم السيبراني بين الدول وبعضها البعض بسبب خلاف سياسي أو بهدف سرقة المعلومات الاستراتيجية والتعرف على كيف يفكر الخصم، وغالباً ما يستهدف الهجوم الإلكتروني (السيبراني) البنية الأساسية للدول، مما يؤدي إلى تعطيل مرافق الحياة وأحداث الفوضى[3]، وتدمير أنظمة التشغيل الدولية ، ومن أمثلة ذلك ما حدث في عام (٢٠١٠) في دولة إيران اذ تم أستهدف محطة الطاقة النووية وذلك من خلال فيروس "ستاكسنت" (Stuxnet) الذي ساهم في تعطيل العديد من أجهزة الطرد المركزي الذي يصل عددهم نحو الألف، وذلك في منشأة تخصيب اليورانيوم في مفاعل ناتانز، بخلاف ما حدث في شهر (تشرين الثاني) لعام (٢٠١٤) في كوريا الجنوبية فقد تم القيام بهجوم إلكتروني على أنظمة الكمبيوتر للشركة الخاصة بالطاقة النووية والمائية التي تديرها الدولة، وفي البرازيل في (٢٠٠٨) تمكن القراصنة من الدخول إلى الموقع الشبكي للحكومة والسيطرة عليه لمدة تزيد عن أسبوع، كما نذكر في عام (٢٠٢٠) تم شن هجوم على المفاعل الإيراني ناتانز، وقد نسب هذا الاختراق إلى جهات أمريكية و"إسرائيلية"، وهناك العديد من تلك الهجمات التي استهدفت البنية التحية للدول، مما أدى إلى التأثير على أمن وسيادة الدول.

الفرع الثاني
أساس تكييف الهجوم الإلكتروني أو السيبراني

في الوقت الحالي أصبح المستوي الدولي يواجه تحدي كبير ودرجة عالية من الخطورة نتيجة التصرفات الغير قانونية التي تمس بالأمن والاستقرار القومي للدول، ولذلك أصبحت الهجمات السيبرانية من المشكلات والتحديات الكبيرة نتيجة درجة تعقدها وخطورتها، التي وصلت إلى القيام بتدمير البنية التحتية لدول بأكملها، والتأثير على الأمن والسيادة الدولية، ومن ثم يتم البحث في الطبيعة القانونية لتكييف هذه الهجمات[4] .

أولاً: تكييف الهجمات الإلكترونية أو السيبرانية مع مبدأ سيادة الدولة

---

[1] رابح منزر، سعيد درويش، الطبيعة القانونية للهجمات السيبرانية التي تقع بين الدول، مجلة صوت القانون، المجلد الثامن ، العدد الأول،(٢٠٢١)، ص ٥٤٣ .

[2] العيسي، طلال ياسين، عناب، عدي محمد ، مرجع سابق ذكره، ص ٨٧ .

[3] - عبد الجواد، أميرة عبد العظيم محمد، "المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام"، مجلة الشريعة والقانون، الجزء الثالث، العدد الخامس والثلاثون، (٢٠٢٢)، ص ٤٣١.

[4] الموصلي، نور أمير، مرجع سابق ذكره ، ص ١٦ .

من سبل انتشار وتطور الهجمات الإليكترونية (السيبرانية) يرجع إلى أن القانون الدولي لم ينظم هذه الهجمات بشكل صريح سواء في أوقات الحرب أو السلم، اذ يرجع ذلك إلى الحداثة النسبية لشبكات الإنترنت والاعتماد الكامل عليها في الفترة الأخيرة، فضلا عن القصور النسبي في القانون الدولي، الذي يرجع تاريخه إلى ما قبل الفضاء الإلكتروني، من ثم ظهرت العديد من الصكوك التي تنظم الأسس لهذه الهجمات ومنها معاهدة (ستقاليا) لسنة (١٦٤٨) فهي أول صك دولي وضع الأسس لهذا المفهوم، الذي عرف عدة تطورات للتكييف مع الأوضاع الجديدة الناتجة عن التطور، ولذلك فتقليداً كانت السيادة ذات مدلول سياسي، اذ يعني به السلطة العليا للدولة في الداخل واستقلالها عن غيرها من الخارج، كما يعني به قانوناً الأهلية القانونية التي تتمتع بها الدولة على اعتبار أن ذلك يميزها عن غيرها من الدول، بما يسمح ذلك بقيام الدولة بممارسة اختصاصاتها على الصعيدين الداخلي والدولي على حد السواء[1] .

وبناء على ما تقدم، يمكن القول أن مفهوم السيادة لم يعد مقتصر على المفهوم التقليدي بل تطور مع تطور الثورة التكنولوجية، ولذلك فقد بدء يظهر مفهوم السيادة السيبرانية، مما يعني قيام الدولة بفرض الهيمنة والسيطرة والولاية القضائية على الفضاء الرقمي، ومن ثم القيام بفرض الحماية على الأمن القومي من أي مخاطر أو تهديدات جديدة مرتبطة بالفضاء السيبراني[2]. ولذلك ترتبط السيادة الدولية بمفهوم الأمن السيبراني باعتبار أنه مجموعة من الآليات والأساليب التقنية والإدارية التي يعتمد عليها ويتم تطبيقها لمنع الاستخدام الغير مصرح به، ولذلك فالحرب السيبرانية تمثل أعلى تحديات الأمن الوطني، وأن ذلك الموضوع يشكل أعلى درجات الخطورة على المجتمعات الدولية بشكل عام، نتيجة لتأثيره على أمن وسيادة الدول. ويرجع ذلك إلى تصاعد الهجوم الإلكتروني واستهداف البنية الأساسية للدول والقيام بعمليات تخريبية قد تصل درجة خطورتها إلى التحكم والسيطرة على القطاعات الحيوية، فقد وصل الأمر في بعض الحالات إلى إخراج بعض منظمات الأسلحة عن سير القيادة المركزية، أو القيام بإعادة توجيه هذه المنظمات نحو أطراف داخلية أو ضد دول صديقة، بخلاف مدى القدرة على السيطرة على طائرات بدون طيار، أو التحكم والسيطرة على غواصات في أعماق البحار، فضلا عن قدرتها على السيطرة على بعض الأقمار الصناعية، وبالتالي إخراجها عن سيطرة الدولة التابعة لها، بخلاف القيام بتعطيل أو إتلاف شبكات الدفاع العسكرية عن بعد، وبالتالي يمكن القول بأن ذلك التحدي يمثل درجة عالية من الخطورة على الأمن والسيادة الدولية[3] .في ضوء ذلك تم إبرام اتفاقية (بودابست) في عام (٢٠٠١) المتعلقة بشأن الجرائم الإلكترونية، والتي نصت في مادتها رقم (١٢) على تحديد مسؤولية (الأشخاص المعنوية)، مع النص على دور الدول الأطراف في القيام بوضع نصوص أو مواد قانونية يرتب على أساسها تحديد المسؤولية حول منفذي أي جريمة سيبرانية[4] .

- **ثانياً: الهجوم السيبراني ذات طابع خاص**

يعد الهجوم الإلكتروني (السيبراني) ذو طبيعة خاصة عند تكييفه في كثير من الأحيان، اذ ينظر البعض على أن تلك الهجمات جرائم ذات طبيعة خاصة، نتيجة إلى تعدد عدد الفاعلين أو الأطراف التي يمكن أن تقوم بشن هذه الهجمات، اذ تختلف هذه الأطراف ما بين دول لمنظمات إجرامية، وكذا الأفراد من قراصنة الأنترنت،

---

[1] سفيان، خلافي، تكييف الهجمات السيبرانية في ضوء أحكام القانون الدولي، المجلة الأكاديمية للبحث القانوني، المجلد ١٣، العدد الثاني، (٢٠٢٢)، ص ٣٠٨ . [1] العيسي، طلال ياسين، عناب، عدي محمد ، مرجع سابق ذكره، ص ٨٧ .

[1] - عبد الجواد، أميرة عبد العظيم محمد، "المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام"، مجلة الشريعة والقانون، الجزء الثالث، العدد الخامس والثلاثون، (٢٠٢٢)، ص ٤٣١.

[2] الدليمي، حسام جاسم محمد أحمد ، التطور التكنولوجي وأثره في سيادة الدول، رسالة ماجستير غير منشورة، جامعة الأنبار العراق ،٢٠١٨، ص ١١٤

[3] - خليفة، إيهاب، مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي، القاهرة: العربي النشر والتوزيع،(٢٠١٩)، ص ١١٤- ١١٥.

[4] رابح منزر، سعيد درويش، الطبيعة ا لقانونية للهجمات السيبرانية التي تقع بين الدول، مجلة صوت القانون، العدد الأول، المجلد الثامن ، (٢٠٢١)، ص ٥٤٣ .

مما يجعل تكييفها أمر صعب، ومن ثم يمكن وصفها بالجريمة السيبرانية، كما يمكن تكييفها على أنها حرب سيبرانية، وفي ضوء ما تقدم يمكن القول أن طبيعة تلك الجريمة خاصة اذ تتسم بأن بيئة الهجوم الخاصة بها غير تقليدية، تقع خارج الاطار الواقعي، اذ تتم عملية الهجوم من خلال الحاسب والشبكات، مما يجعل أمر ملاحقتها وتكييفها أمر معقد[1]، كما ينظر إليها البعض على أنها هجمات ذات طبيعة قانونية خاصة يحكمها قواعد القانون الدولي المتعلق بتنظيم طبيعة العلاقات بين الدول وبعضها البعض.

ومن ثم يمكن القول أن الهجوم الإلكتروني أو السيبراني على أي مجتمع يمثل أعلى تحديات الأمن الوطني في القرن الواحد والعشرين، وأن ذلك الموضوع يشكل أعلى درجات الخطورة على المجتمعات الدولية بشكل عام، اذ أثر على أمن وسيادة الدول، فبالتالي أن ذلك الموضوع يحتاج إلى التدخل من الدول كافة حول البحث عن حل جذري يتناسب مع هذه المشكلة الدولية، يساعد في الحفاظ على تحقيق الأمن الوطني والتكنولوجي للدول، بالإضافة الى المساعدة في الإنذار والكشف المبكر عن تلك الهجمات قبل وقوعها أو في وقتها الحقيقي، ففي ظل غياب منظومة قانونية تهدف لتوفير الحماية والوقاية من هذه الجرائم، والنص على جزاءات رادعة في وجه مخترقي تلك الأجهزة، لذلك فإن ذلك القصور بمثابة تحفيز وتشجيع على ارتكاب وتنفيذ تلك الجرائم، ولذلك سنتطرق الى تحديد مدى المسؤولية الدولية الخاصة بالهجوم السيبراني .

المبحث الثاني
اساس المسؤولية الدولية الخاصة بالهجمات السيبرانية

تبعث المسؤولية عن الهجوم السيبراني من القانون الدولي العرفي، فضلا عن المواثيق الدولية على اعتبار أنها تمس بالقيم الأساسية للمجتمع الدولي، لذلك ينظر إلى موضوع المسؤولية في الوقت الحاضر بأنه من أهم موضوعات القانون الدولي. ففي ظل التطورات العلمية الحديثة التي كان لها أثر كبير على العلاقات الدولية، ساهم في ظهور العديد من المشكلات التي تتناول القانون الدولي قواعد تنظيمها ولكن بشكل غير مباشر أو صريح. ويرجع ذلك إلى حداثة ظهور هذه الهجمات التي ظهرت بعد وضع القانون الدولي، مما أدى ذلك عدم وضوح قواعد مسؤولية الدول عن تنفيذ تلك الهجمات، وما ينتج عنها من خطورة وتضرر للغير، ولذلك تشير بالمسؤولية الدولية على أنه تمثل الالتزام المفروض من القانون الدولي على منتهكي القواعد المنظمة لحظر استخدام الأسلحة أو تقييده، القيام بإصلاح الضرر الناشئ عن تلك الانتهاك، ومن هذا المنطلق سنتطرق إلى المسؤولية فيما يخص تلك الهجمات.

المطلب الأول
أساس المسؤولية عن الأضرار الناتجة عن الهجوم السيبراني

شكلت شبكة الإنترنت العالمية قوة مؤثرة على العالم، فقد تم استخدامها لقمع حركة التحرر الوطني، ومن ثم فإن التطور التقني صاحبه العديد من الأضرار التي مست بكيان الدولة واستقلالها[2]، ولذلك فإن طبيعة المسؤولية الدولية المتعلقة بالهجمات الإلكترونية ترجع إلى مصدر القانون الدولي العرفي، حتى وإن تضمنتها اتفاقيات دولية. لذلك لابد من النص على إن مسؤولية الدول عن هذه الهجمات، تتمتع بطبيعة وطنية مصدر تجريمها هو القانون الدولي، حتى لو القانون يعد تطبيق لاتفاقية دولية تستند إلى عرف دولي[3]، وعلى الرغم من أن اتفاقيات القانون الدولي لا تشير بشكل واضح وصريح على الهجوم السيبراني، إلا أن القانون الإنساني الدولي بمبادئه وقواعده يمكن تطبيقه على إي نزاع، ولذلك يشير مفهوم المسؤولية الدولية أنها" نظام قانوني بموجبه تلتزم الدول المدعى عليها بالقيام بإصلاح أو التعويض عن الضرر الذي يقع على دولة أخرى بصفتها، أو بأحد مواطنيها نتيجة قيامها بعمل غير

---

[1] الراوي، رعد فجر، القصور التشريعي في مواجهة الهجمات السيبرانية، مجلة كلية القانون للعلوم القانونية والسياسية، المجلد العاشر، العدد ٣٩، (٢٠٢١)، ص ١٩٤ .

[2] صديقي، سامية، مرجع سابق ذكره، ص ٨٢٩ .

[3] الراوي، رعد فجر، مرجع سابق ذكره، ص ١٨٩ .

قانوني أو الامتناع عن تصرف قانوني وفقا للأحكام والقواعد المحددة بموجب القانون[1] ، وينظر الفقيه (كلسن) إلى تلك المسؤولية بأنها "المبدأ الذي ينشئ التزاماً بإصلاح أي انتهاك للقانون الدولي الذي ارتكبته دولة مسؤولة ويرتب ضرراً" [2] .

كما أشار (مارتينز) على الشرط التي يمثل أحد المبادئ الأساسية والراسخة في القانون الدولي، أنه عند وجود حالة لا يغطيها اتفاقية دولية، فيتم الرجوع إلى مبادئ وأحكام القانون الدولي الإنساني، اذ يتوافر فيه قواعد حماية راسخة تطبق على جميع الحالات، فلذلك يمكن القول بأن قواعد القانون الدولي تطبق على الهجمات السيبرانية .

الفرع الأول: المسؤولية الدولية عن الهجمات السيبرانية على أساس الأعمال الغير مشروعة

تحظى المسؤولية الدولية بجانب كبير من الأهمية ويرجع ذلك الاهتمام الى المدى الذي يمكن من خلاله القيام بتوفير الحماية القانونية لكافة أطراف المعاملة الدولية، وبالتالي فأن المسؤولية الدولية كانت ومازالت محور اهتمام رجال الفقه والقضاء وذلك من أجل البحث لإيجاد الحلول التي تلاءم التطور واستجابة للمقتضيات المجتمعية العصرية[3]. ومن هذا المنطلق تعد المسؤولية الدولية هي أحد الضمانات الأساسية والفعالة لكفالة القيام بتطبيق القانون الدولي، وذلك في ظل وجود سلطة عليا مستقلة تتسم بامتلاكها للسلطة الشرعية لتحديد نظام المسؤولية، ومن هذا المنطلق نجد نظرية الفعل الغير مشروع تقوم على كل إخلال بالتزام دولي من قبل دولة مما يستوجب ذلك الأمر ضرورة تحديد المسؤولية الدولية ، ولكي تتحقق المسؤولية لابد من وجود ضرر يقع من أحد الأطراف على الطرف الآخر يتطلب تعويض الواقع عليه ومن ثم تقديم ضمانات للمستقبل .

تكمن أهمية المسؤولية الدولية في القانون الدولي العام باعتبارها جزءًا أساسيًا من كل نظام قانوني، ففعالية هذا النظام تتوقف على مدى نضج قواعد المسؤولية ونموها باعتبارها أداة تطور بما تكفله من ضمانات ضد التعسف الدولي، ولذلك يعد البعض قواعد المسؤولية تمثل مفتاح لكل نظام قانوني، بدونها لا يكون تأثير أو أهمية لقواعد القانون الدولي. ولذلك يتميز النظام القانوني الفعال على مدى نضج قواعد تلك المسؤولية.[4]ولكي تتحدد المسؤولية عن الفعل أو التصرفات الغير مشروعة يستوجب ذلك القيام بتحديد أركان المسؤولية الدولية.

- **أركان المسؤولية الدولية عن الهجمات السيبرانية**

يتسم النظام القانوني الدولي بأنه يترتب عليه حقوق والتزامات على أشخاصه، اذ أن الدول التي تقوم بتصرفات غير مشروعة يترتب الأضرار لدول أخرى، فمن ثم تكون الدولة مكلفة بتحمل أحداث ذلك الضرر، تبعاً للمسؤولية عن الفعل، وبالتالي فالهجمات الإلكترونية (السيبرانية) يقوم بها أشخاص يخضعون للقانون الدولي، ولكي تثبت المسؤولية عن تلك الأفعال، فلابد أن يكون الأفعال مستوفية الشروط، ولذلك يمكن تحديد الأركان الخاصة بتلك المسؤولية، اذ تتمثل في ثلاث أركان رئيسة (نسبة الفعل الضار – عدم مشروعية الفعل – وقوع الضرر)، وسوف نوضح كل هذه الأركان على النحو التالي [5]

---

[1] سلامة، أحمد عبد الكريم سلامه, نظرات في الحماية الدبلوماسية ودور فكرة الجنسية في المسؤولية الدولية عن الأضرار البيئية ,كلية الحقوق جامعة البحرين , ج(٢) , (٢٠١٥)، ص١١

[2] - Kelsen , State Responsibility and the Abnormally Dangerous Activity , Columbig jolumbig journal of lntrrnational Law , vol(2) , 1972 , P . 198

[3] جبر نبرأس ظاهر، المسؤولية المدنية الناشئة عن إخلال الغير بالعقد: دراسة مقارنة، مجلة المحقق الحلى للعلوم القانوني والسياسية، المجلد العاشر، العدد الأول، ص ٤٠٥.

[4] أتوبه، محمد جبار, المسؤولية الدولية عن التلوث البيئي في العراق , رسالة ماجستير , كلية الحقوق والعلوم السياسية , جامعة بيروت العربية ،(٢٠١١)، ص٥٩

[5] العيسي، طلال ياسين، عناب، عدي محمد ، مرجع سابق ذكره، ص ٨٨ .

- **نسبة الفعل إلى الدولة**: يمثل ذلك الفعل الركن الأول من أركان مسؤولية الدولة عن الهجوم الإلكتروني أو السيبراني، ففي حالة تصرف الدولة بتصرفات غير مشروعة وغير قانونية، ينتج عنها الحاق الضرر بدولة أخرى، يستوجب ذلك ضرورة تعويض هذا الضرر، ولذلك يشترط القانون ضرورة القيام بإسناد الفعل الغير مشروع إلى دولة ما، فضلا عن القانون الدولي أشترط أن تكون الدولة صاحب الفعل أو التصرف الغير مشروع تامة السيادة والأهلية، أي مسؤولة عن أعمالها نتيجة استقلال سلطاتها الثلاثة المتمثلة في (التنفيذية –التشريعية – القضائية)، فضلا عن بعض الحالات التي تسأل الدولة فيها عن أفعال الأشخاص العاديين أو الموظفين الرسميين المفوضة لهم القيام بالأعمال.

ولذلك ففي حالة الهجوم الإلكتروني أو السيبراني فأن فعل الضرر يقع بمجرد القيام بتنفيذ الهجمات، وبالأخص فيما يتعلق بتدمير القطاعات الأساسية، وقد ينتج عنها العديد من المخاطر والأضرار، ومن ثم يتم تنفيذ ذلك الهجوم عن طريق دول ذات القدرة الفائقة في تطبيق التطور التقتني، ومن منطلق مسؤولية الدول عن رعاياها فتكون الدولة مسؤولة عن تصرفات هؤلاء الأفراد .

- **أن يكون الفعل أو التصرف تم تجريمه دولياً:** يشير عدم مشروعية التصرف أو الفعل بأنه الركن الثاني للمسؤولية. اذ تقوم فكرة الفعل الغير القانوني على الإخلال بالتزام دولي من قبل الدولة مما يستوجب مسؤوليتها عنه، سواء كان التصرف ناتج عن إحدى السلطات الرئيسة (التنفيذية أو التشريعية أو القضائية)[1] .

وبناء على ما تقدم تعد الهجمات الدولية عمل غير مشروع يمكن إخضاعها لقواعد المسؤولية الدولية، ومن ثم يتمثل معيار الصفة الدولية في صدور التصرفات أو الأفعال الغير قانونية من قبل الدولة، ولذلك فأن تنفيذ هذه الأفعال يتم إلحاقها بقواعد المسؤولية الدولية[2]، فبالرجوع إلى طبيعة الهجمات يتضح بأنها مخالفة لقواعد القانون الدولي، وذلك نتيجة إلى المخاطر الناجمة عنها والمسببة لوقوع العديد من الأضرار سواء على المستوى المادي أو البشري. فمن هذا المنطلق ينظر إلى الهجوم الإلكتروني على أنه عمل غير مشروع، نتيجة لانتهاكها أحكام وقواعد القانون الدولي، واختراق أسرار ووثائق الدول، واستهداف مصالحها الكبرى.

- **الضرر:** يمثل الركن الأخير من أركان المسؤولية، كما يعد تعويض الضرر الوظيفة الأساسية للمسؤولية[3] ولكي يتحقق الضرر فأن الأمر مشروط بالوقوع الفعلي للضرر، أو يكون قد وقع بشكل حتمي، ولذلك فحكم التعويض مشروط بأن يكون الضرر الذي وقع ساعد على الإخلال بمصلحة المتضرر المالية. وبالتالي يعد احتمال وقوع الضرر في المستقبل لا يستوجب الحكم بالتعويض. وبالتالي ظهور تلك الهجمات واختراق أنظمتها، والوصول إلى المعلومات، وتعرضها للسرقة والإتلاف والتدمير، بمثابة ضربة قاضية لاقتصاد أي دولة، وبالتالي إلحاق الضرر بالقطاع الذي تم اختراقه[4].

وبناء على ما تقدم، لكي تترتب مسؤولية الدولة عن تلك الهجمات لابد من وقوع المخاطر والأضرار التي تضر بالدول الأخرى، كوقوع ضحايا في صفوف المدنيين والمقاتلين، وتهديد الأمن والسلم الدولي . ولذلك فالضرر بأشكاله كافة يتحقق من جراء القيام بتلك الهجمات, سواء الفاعل فرد أو دولاً قومية، تؤي إلى وقوع الضرر، ومن أمثلة ذلك نذكر الاختراق أو الهجوم الإلكتروني الذي تم على دولة العراق في عام (٢٠١٩)، الذي وقع على يد

---

[1] عبد العزيز العيشاوي، محاضرات في المسؤولية الدولية ،دار هومة للنشر والتوزيع، الجزائر، (٢٠٠٧)، ص ١٨ .
[2] صديقي، سامية، مرجع سابق ذكره، ص٨٣٠ .
[3] دبش، عمرو أحمد عبد المنعم، مجلة العلوم القانونية والاجتماعية، المجلد الرابع، العدد الثاني،(٢٠١٩)،ص٣٠.
[4] كلاع، شريفة، الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني، مجلة الحقوق والعلوم الإنسانية، المجلد الخامس عشر، العدد الأول، (٢٠٢٢)، ص ٢٩٩.

مجموعة من القراصنة قد طال ذلك حوالى (٣٠) موقع حكومي، ومن أبرز هذه المواقع نذكر موقع وزارة الدفاع والأمن الوطني والصحة، وقد وقع ذلك عن طريق قيام بعض المهاجمين باستغلال الثغرات والتعامل مع بيانات مواقع البحث، التي تقوم بتوجيه المستخدمين لصفحة البحث مختلفة، وعلى الرغم من نجاح الحكومة العراقية في الاستعادة السريعة لبعض المواقع، إلا أن استرجاع بعض المواقع احتاج مزيداً من الوقت، لأن المهاجمين كانوا قد تمكنوا من الوصول لأجهزة الحاسب الحكومية، واختراق قواعد البيانات والحصول على البيانات، التي تستوجب الحماية بشكل جيد[1] .مما أدى ذلك إلى تعطيل مرافق الحياة وأحدث الفوضى[2].

وبالاعتماد على ما تقدم فالمسؤولية الدولية تنشأ نتيجة قيام الشخص أو الدولة بعمل غير قانوني، مما يؤدي إلى وقوع الضرر على فرد أو مؤسسة أو دولة، ولذلك يستلزم الأمر القيام بتحمل المسؤولية عن ذلك الضرر، وجبر الضرر بالتعويض، فعند توافر الشروط المتعلقة بالمسؤولية الدولية يتم مساءلة الدولة أو الشخص صاحب هذه الهجمات وتوقيع الجزاءات المنصوص عليها نتيجة هذه الأفعال.

الفرع الثاني
المسؤولية الدولية عن وقوع الهجوم الإلكتروني أو السيبراني بالإستناد على نظرية المخاطر

ظهرت هذه النظرية لمعالجة الانتقادات الموجه إلى نظرية الفعل أو التصرف الغير قانوني، وذلك نتيجة عدم قدرتها على مواكبة التطورات الحديثة، المعتمدة على العالم الافتراضي في إدارة شؤون القطاعات والمجالات كافة على المستوى الدولي. ومن هذا المنطلق فأن نظرية المخاطر تقوم على مساءلة الشخص أو الدولة صاحبة التصرفات الغير قانونية الضارة بالآخرين، اذ ترى هذه النظرية أن فعل الضرر هو الذي ينشأ المسؤولية الدولية تجاه الدولة التي تمارس تصرفات غير مشروعة. ويؤكد مؤيدي تلك النظرية على أنها تقوم على تحمل النتائج التي تنجم عن التصرفات الغير قانونية وليس على أساس الخطأ[3] . ونجد أن اتفاقية الطاقة الدولية اعتمدت هذه النظرية، من خلال جعل إلزام الدولة صاحبة النشاط النووي وقت السلم بتعويض الأضرار الناجمة عن أنشطتها. بغض النظر عن نسبته. وانطلاقاً من هذه المسؤولية فيقع على عاتق المسؤول عن إدارة المحطة القيام بتعويض الأضرار التي تلحق بالآخرين[4].

المطلب الثاني
التحقيق في مجال الهجوم السيبراني

يستوجب تحديد مدى مسؤولية الدول عن الهجمات السيبرانية ضرورة القيام بإجراء التحقيقات لكي يتم الوصول إلى مرتكبي هذه الهجمات وتقديمهما للمحاكمة، وإقامة الدعوي الجزائية ضدهم بما يساهم ذلك في تحقيق مبدأ العدالة الاجتماعية وتحقيق سيادة الدولة والقانون، ومن ثم تشير عملية التحقيق إلى جمع البراهين والأدلة التي تؤكد وتثبت المسؤولية عن التصرفات المخالفة والغير مشروعة[5] .

أولاً : التحقيق

---

[1] الشمري، مصطفى إبراهيم سلمان،" الأمن السيبراني وأثره في الأمن الوطني العراقي"، مجلة العلوم القانونية والسياسية، المجلد العاشر، العدد الأول،(٢٠٢١)، ص ١٧٤.

[2] عبد الجواد، أميرة عبد العظيم محمد، "المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام"، مجلة الشريعة والقانون، الجزء الثالث، العدد الخامس والثلاثون، (٢٠٢٠)، ص ٤٣١.

[3] صديقي، سامية، مرجع سابق ذكره، ص٨٣٢ .

[4] صباح العشاوي،المسؤولية الدولية عن حماية البيئة، دار الخلدونية للنشر والتوزيع، الجزائر، الطبعة الأولي، ص ١٧٤ : نقلاً عن المرجع السابق..

[5] الراوي، رعد فجر، مرجع سابق ذكره، ص ١٩٧ .

يتمثل دور المحقق عند القيام بالتحقيق في الجرائم الإليكترونية إلى تطبيق واتباع الإجراءات القانونية التي تساهم في أثبات المسئولية عن تلك الهجمات، وذلك عن طريق اتباع إجراءات التحقيق المنصوص عليها قانونياً، ولذلك فإن الهدف دور المحقق هو الوصول إلى الأدلة الإلكترونية، ولذلك يتم تشكيل فريق تحقيق يتكون من قاضي التحقيق فضلا عن خبراء من أجل القدرة على كشف تلك الهجمات. [1]

ثانياً: إجراءات التحقيق

تتسم الجرائم السيبرانية بأنها جرائم ذات طبيعة خاصة من حيث درجة التعقيد التي يتميز بها عالم الإنترنت، مما يتطلب ذلك القيام بتطوير أساليب التحقيق وإجراءاته بما يتناسب مع التطور في ساحة الجرائم، وبالتالي تمكين المحقق من أثبات المسؤولية عن ذلك النوع من الجرائم، اذ يستوجب ذلك القيام بالإجراءات التالية.

- تدريب الكوادر والاستعانة بالخبراء الفنيين: أي لابد أن يكون فريق التحقيق الخاص بتلك المهمة ذات درجة عالية من المعرفة والخبرة في المجال التكنولوجي، بالإضافة إلى قدرته على تطبيق المعالجات الإلكترونية مع دراسة حالات تطبيقية. مما يؤدي ذلك إلى تحسين إداء العمل .

- المعاينة : اذ يقصد بذلك القيام بالمشاهدة والمعاينة لمكان الحدث وما يتعلق به لكي يتم الوصول إلى الدليل المادي الذي يثبت مسؤولية مرتكبي تلك الجريمة، ففي ظل الهجوم الإلكتروني أو (السيبراني) تتمثل صور المعاينة في التفتيش من خلال تصوير الأجهزة المستخدمة تنفيذ تلك الجريمة، مع اتخاذ الاحتياطات اللازمة لحمايتها والحفاظ عليها من التلف، سواء كانت مستندات مادية أو ورقية لكي يتم القيام برفع البصمات[2] .

- التفتيش والضبط : يعد هذا الإجراء أحد الضمانات الرئيسة في اكتشاف الحقيقة وتحقيق العدالة، اذ يتم التنفيش من خلال البحث في الكيانات المنطقية الخاصة بالحاسب وعمليات الدخول في النظام، ومفاتيح فك الشفرة، حتى يتم الوصول إلى البراهين والأدلة التي تؤكد المسؤولية عن تلك الجريمة .

ولذلك يتبين أن الثورة المعلوماتية ساعدت على أحداث التطورات العديدة في المجالات كافة، ومن ثم قد أنتجت تصوراً جديداً في المجال الأمني، حيث غيرت ميدان النزاعات والصراعات، فقد أصبحت فكرة الحروب مرتبطة بالشبكات وأنظمة المعلومات، اذ تدار هذه الحروب من خلال أسلحة مختلفة عن الأسلحة التقليدية شكلاً ومضموناً، فقد سميت (بالحرب السيبرانية) ولذلك أصبحت تلك النوع من الحروب حقيقة واقعة لا مفر منها، أصبحت الأساليب المستخدمة تهدد المجتمع الدولي بصفة عامة دون أي استثناءات، وبالتالي يعد ذلك النوع من الحروب هو الذي يقود العالم في المستقبل فعلى المجتمع الدولي من ضرورة التعاون والتكاتف من أجل العمل على الحماية الدولية من خطورة هذه الحرب.

الخاتمة

شكل الهجوم السيبراني أعلى تحديات الأمن الوطني في القرن الواحد والعشرين، وأن ذلك الموضوع يشكل أعلى درجات الخطورة على المجتمعات الدولية بشكل عام، من خلال تأثيره المباشر على أمن وسيادة الدول، يتم من خلال اختراق الأجهزة الدولية وسرقة المعلومات المخزنة وتدميرها، اذ تدار هذه الحروب من خلال أسلحة مختلفة تماماً شكلاً ومضموناً عن الأسلحة التقليدية، فقد سميت (بالحرب السيبرانية) ولذلك هذه الحروب حقيقة واقعة لا

[1] محمد حجازي، جرائم الحاسبة والإنترنت، الجرائم المعلوماتية، (بدون دار نشر) ، (٢٠٠٥)، ص.١٨.
[2] عبد اللطيف ، براء منذر كمال، : شرح قانون أصول المحاكمات الجزائية، ط،٢ مكتبة السنهوري، بغداد، ص ٢٠٦ .

مفر منها، أصبحت هذه الهجمات تهدد المجتمع الدولي بصفة عامة دون أي استثناءات، لذلك استوجب الأمر تحديد المسؤولية عن هذه الجرائم.

أولاً: النتائج

- تعد الهجمات السيبرانية محاولة متعمدة من قبل فرد أو منظمة لاختراق نظام المعلومات الخاص بفرد آخر أو مؤسسة أو دولة، وذلك من أجل الحصول على مكاسب أو تعطيل الشبكة .
- يعتمد الهجوم الإلكتروني على استخدام أحدث الأساليب والآليات التكنولوجية المتطورة، اذ عكست التطور الهائل في الثورة التكنولوجيا. وغيرت وسائل وأساليب الحرب التقليدية .فقد أصبحت لوحة المفاتيح وبرمجيات الحاسب أكثر دماراً وخطراً على العالم.
- نتيجة الطبيعة الخاصة بالهجمات الإلكترونية (السيبرانية)، يصعب وضعها في إطار قانوني دولي، نتيجة عدم وجود نظام قانوني موحد خاص بتلك الهجمات .
- إن الجريمة السيبرانية بوصفها جرائم دولية، يستوجب مكافحتها والاعتماد على القانون الدولي.
- تقع المسؤولية الدولية عن الهجمات السيبرانية نتيجة ما تقوم به الدولة من هجمات تلحق الضرر بدولة أخرى.

ثانياً: المقترحات

- تقترح الدراسة بضرورة إجراء مزيد من الدراسات والبحوث في ترتبط التعاون الدولي للحد من الجريمة السيبرانية .
- تقترح الدراسة بإعادة النظر في القانون الدولي، ومن ثم إضافة نصوص قانونية تتضمن تحديد عقوبات وجزاءات فعالة لمرتكبي هذه الجرائم .
- تقترح الدراسة بضرورة إعادة النظر في القوانين الوطنية وتفعيلها بما يتناسب مع طبيعة التطور في الجرائم الدولية، ومن ثم النص على جزاءات وعقوبات تكون رادعة لمرتكبي الجرائم السيبرانية.
- تقترح الدراسة بضرورة التعاون الفني عن طريق تدريب الكوادر الفنية من أجل الاستفادة من خبراتهما ومهاراتهما في مكافحة الجريمة .

تقترح الدراسة بتوفير الحماية القانونية للفضاء السيبراني من خلال العمل على وضع تشريعات داخلية تتناسب مع التطور القني في ثورة تكنولوجيا المعلومات والاتصالات.

المصادر والمراجع

القران الكريم

اولا/ المعاجم اللغوية:

- منير البعلبكي، المورد: قاموس – انكليزي- عربي، دار العلم للملايين، بيروت، ٢٠٠٤.

ثانيا/ الكتب:

1- الفتلاوي، أحمد عبيس نعمة، الهجمات السيبرانية، دراسة تحليلية بشأن تحليلية لشأن تحديات تنظيمها المعاصر، منشورات زين الحقوقية بيروت لبنان ،(٢٠١٨).

٢ - خليفة، إيهاب، مجتمع ما بعد المعلومات: تأثير الثورة الصناعية الرابعة على الأمن القومي، القاهرة: العربي النشر والتوزيع،(٢٠١٩).

٣- صباح العشاوي،المسؤولية الدولية عن حماية البيئة، دار الخلدونية للنشر والتوزيع، الجزائر، الطبعة الأولى.

٤- عبد العزيز العيشاوي، محاضرات في المسؤولية الدولية ،دار هومة للنشر والتوزيع، الجزائر، (٢٠٠٧).

٥- عبد اللطيف ، براء منذر كمال، : شرح قانون أصول المحاكمات الجزائية، ط،٢ مكتبة السنهوري، بغداد، ص ٢٠٦ .

٦- محمد حجازي، جرائم الحاسبة والإنترنت، الجرائم المعلوماتية، (بدون دار نشر) ، (٢٠٠٥).

ثالثا/ البحوث:
١- الراوي، رعد فجر، القصور التشريعي في مواجهة الهجمات السيبرانية، مجلة كلية القانون للعلوم القانونية والسياسية، المجلد العاشر، العدد ٣٩، (٢٠٢١).
٢- الشمري، مصطفى إبراهيم سلمان،" الأمن السيبراني وأثره في الأمن الوطني العراقي"، مجلة العلوم القانونية والسياسية، المجلد العاشر، العدد الأول،(٢٠٢١).
٣- العيسي، طلال ياسين، عناب، عدي محمد، المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مجلة الزرقاء للبحوث والدراسات الإنسانية، المجلد التاسع عشر، العدد الأول، (٢٠١٩).
٤- جبر نبرأس ظاهر، المسؤولية المدنية الناشئة عن إخلال الغير بالعقد: دراسة مقارنة، مجلة المحقق الحلى للعلوم القانوني والسياسية، المجلد العاشر، العدد الأول.
٥- دبش، عمرو أحمد عبد المنعم، مجلة العلوم القانونية والاجتماعية، المجلد الرابع، العدد الثاني،(٢٠١٩).
٦- سامية، صديقي، المسؤولية الدولية المترتبة عن الهجوم السيبراني في منظور القانون الدولي، مجلة البحوث القانونية والاقتصادية، المجلد السادس ، العدد الأول،(٢٠٢٣).
٧- سعود، يحيي ياسين،(الحرب السيبرانية في ضوء قواعد القانون الدولي الانساني)، المجلة القانونية في البحوث والدراسات القانونية،(٢٠١٩).
٨- سفيان، خلافي، تكييف الهجمات السيبرانية في ضوء أحكام القانون الدولي، المجلة الأكاديمية للبحث القانوني، المجلد ١٣، العدد الثاني، (٢٠٢٢).
٩- سلامة، أحمد عبد الكريم سلامه, نظرات في الحماية الدبلوماسية ودور فكرة الجنسية في المسؤولية الدولية عن الأضرار البيئية ,كلية الحقوق جامعة البحرين , ج(٢) , (٢٠١٥).
١٠- رابح منزر، سعيد درويش، الطبيعة القانونية للهجمات السيبرانية التي تقع بين الدول، مجلة صوت القانون، المجلد الثامن ، العدد الأول،(٢٠٢١).
١١- عبد الجواد، أميرة عبد العظيم محمد، "المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام"، مجلة الشريعة والقانون، الجزء الثالث، العدد الخامس والثلاثون، (٢٠٢٢).
١٢- عبد اللطيف سامر مؤيد، الحرب في الفضاء الرقمي رؤية مستقبلية، مجلة رسالة الحقوق، السنة السابعة، العدد الثاني، (٢٠١٥).
١٣- علي سنوسي، الهجمات السيبرانية في ضوء أحكام قواعد القانون الدولي الإنساني والاتفاقيات الدولية، مجلة الحقو ق للعلوم السياسية جعة خنشلة، المجلد الأول، العدد الثاني، (٢٠٢٣).
١٤- كلاع، شريفة، الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني، مجلة الحقوق والعلوم الإنسانية، المجلد الخامس عشر، العدد الأول، (٢٠٢٢).

رابعا/ الرسائل والاطاريح :
1 - أتوبه، محمد جبار, المسؤولية الدولية عن التلوث البيئي في العراق , رسالة ماجستير , كلية الحقوق والعلوم السياسية , جامعة بيروت العربية ،(٢٠١١).
٢ - الدليمي، حسام جاسم محمد أحمد ، التطور التكنولوجي وأثره في سيادة الدول، رسالة ماجستير غير منشورة، جامعة الأنبار العراق ،٢٠١٨
٣- الموصلي، نور أمير، الهجمات السيبرانية في ضوء القانون الدولي الإنساني، رسالة ماجستير غير منشورة، الجامعة الافتراضية السورية،(٢٠٢١).
٤- حكيم، قطافي، حرب المعلومات المفهوم والتطبيق – دراسة وصفية تحليلية، رسالة ماجستير غير منشورة، جامعة الجزائر، كلية العلوم السياسية، (٢٠٠٥-٢٠٠٦).

خامسا/ المراجع الاجنبية:
1- Kelsen, State Responsibility and the Abnormally Dangerous Activity, Columbig jolumbig journal of lntrrnational Law, vol (2), 1972
2- Junaidu Bello Marshall, 2000, Cyber-attacks (the legal response, international journal of international law), Vol 01, Is 02, universal multidisciplinary research

institute, India.
3- John Richardson, Stuxnet as cyberwarfare: Applying the law of war to the Virtual attlefield, JMR Portfolio Intelligence,2011, p9. Available at www.assrn.com/abstract=1892888.