مواجهة الهجمات السيبرانية

فى ضوء أحكام القانون الدولي

Confronting Cyber-attacks in Light of the Provisions of International Law

دكتور

إبراهيم السيد أحمد رمضان

دكتوراه في القانون الدولي العام

Dr. Ibrahim El-Sayed Ahmed Ramadan

الملخص:

مع التقدم التقني الهائل في مجال تكنولوجيا المعلومات والاتصالات عبر الإنترنت، أصبح من السهل توظيف الدول والكيانات من غير الدول لهذه التقنيات المتطورة في القيام بهجمات سيبرانية واسعة النطاق، ومن ثم تشكل الهجمات السيبرانية تحدياً جدياً خطيراً يهدد الأمن القومي للدول والمجتمع الدولي بأسره، وخصوصاً أن بعض الدول الكبري أصبحت تلجأ إلي تلك الهجمات بغرض تحقيق بعض المكاسب أو توجيه تهديدات لدول أخري.

والواقع إن التحدى الهائل الذى يواجه مسألة تنظيم إستخدام الهجمات السيبرانية هو عدم وجود إرادة دولية علي الصعيدالدولي والإقليمي، يقابله تسارع وتيرة تطوير أنظمة الكترونية قادرة علي التسلل والاختراق لأنظمة الكترونية تابعة لدولة أخرى، وإحداث الضرر بها بما يشكل هجوماً وعدواناً مفاجئاً للمنشآت الحيوية للدولة محل الهجوم السيبراني، وأدى هذا التحدي إلي إثارة التساؤل حول مدى قدرة قواعد القانون الدولي المعاصر علي مواجهة آثار استخدام الهجمات السيبرانية، وخصوصاً أن القانون الدولي الإنساني ينظم استخدام الاسحلة، في حين أن أغلب الهجمات السيبرانية تقوم علي عمليات لا تتفق والمعايير التى يهدف القانون الدولي إلي تنظيمها، وذلك لوجود مخاطر محققة بالبشر علي الصعيد الإنساني جراء استخدام الهجمات السيبرانية.

ولإلقاء الضوء علي موضوع الهجمات السيبرانية جاء بحثنا بعنوان " مواجهة الهجمات السيبرانية فى ضوء أحكام القانون الدولي"، وقمنا بتقسيمه إلي مبحث تمهيدي وثلاث مباحث رئيسية تناولنا في المبحث التمهيدي: مفهوم الهجمات السيبرانية، كما تناولنا في المبحث الأول: التكييف القانوني للهجمات السيبرانية، ثم تناولنا في المبحث الثاني: الجهود الدولية لمواجهة الهجمات السيبرانية، كما تناولنا في المبحث الثالث: المسئولية الدولية عن إستخدام الهجمات السيبرانية، ثم ختمت الدراسة بالنتائج والتوصيات.

الكلمات المفتاحية: الفضاء السيبراني– الهجمات السيبرانية– الحرب السيبرانية – المسئولية الدولية – القانون الدولي الإنساني– دليل تالين.

Abstract

Withthe tremendous technological progress in the field of information and communications technology via the Internet, it has become easy for states and non-state entities to employ these advanced technologies to carry out large-scale cyber- attacks. Thus, cyber- attacks constitute a serious and dangerous challenge that threatens the national security of states and the international community as a whole, especially since some major countries have begun to resort to these attacks in order to achieve some gains or to direct threats to other countries.

In fact, the enormous challenge facing the issue of regulating the use of cyber- attacks is the lack of international will at the international and regional levels, which is met by the accelerating pace of development of electronic systems capable of infiltrating and penetrating the electronic systems of another country, and causing damage to them, which constitutes a sudden attack and aggression against the vital facilities of the country subject to the cyber- attack. This challenge has raised questions about the ability of the rules of contemporary international law to confront the effects of the use of cyber- attacks, especially since international humanitarian law regulates the use of weapons, while most cyber- attacks are based on operations that do not conform to the standards that international law aims to regulate, due to the real risks to humans on the humanitarian level as a result of the use of cyber- attacks.

To shed light on the topic of cyber-attacks, our research was titled "Confronting Cyber-attacks in Light of the Provisions of International Law ", and we divided it into an introductory section and three main sections. In the introductory section, we discussed the concept of cyber-attacks. In the first section, we discussed the legal classification of cyber-attacks. Then, in the second section, we discussed international efforts to confront cyber-attacks. In the third section, we discussed international responsibility for the use of cyber-attacks. Then, the study concluded with results and recommendations.

Keywords: Cyberspace – Cyber-Attacks - Cyber Warfare - International Responsibility - International Humanitarian Law - Tallinn Manual.

مقدمة

لا شك أن التطور الهائل في تكنولوجيا المعلومات أدى إلي ظهور مرحلة جديدة أصبح فيها للأمن السيبراني دور رئيسي في استخدام القوة سواء من حيث طبيعتها أو أنماط استخدامها أو طبيعة الفاعلين فيها، وانعكاس ذلك علي قدرات الدول وعلاقاتها الدولية، كما دفع الدول إلي الحفاظ علي أمنها القومي لمواجهة الهجمات السيبرانية، وخاصة أن الهجمات السيبرانية قد ترتكب من داخل الدولة ومن الممكن ارتكابها من خارج الدولة، حيث تعد جريمة الهجمات السيبرانية من الجرائم العابرة للحدود، ومن السهل ارتكابها دون مراعاة حدود الزمان والمكان ولا الجهة التى تقف وراء الهجوم، سواء كانت دول أو كيانات من غير الدول كالمنظمات الإرهابية أو القراصنة([1]).

وفي هذا الإطار، تسبب الفضاء السيبراني المفتوح أمام جميع الدول والمتجاوز لحدودها السياسية في انتشار الأنشطة السيبرانية غير السلمية مثل الهجمات السيبرانية والإرهاب السيبراني والتجسس السيبراني وغيرها، وهو ما أدي إلي ظهور بعد جديد في الصراعات الدولية سمي بصراع الفضاء السيبراني، وإلي اعتبار الفضاء السيبراني ساحة حرب جديدة في القرن الحادي والعشرين. حيث بات الفضاء السيبراني المجال الخامس للحروب بعد البر والبحر والجو والفضاء، مما يشكل خطراً عالمياً متصاعداً ينذر بتحوله إلي أكبر تهديد أمني دولي، وهو ما يعني أن هجوماً سيبرانياً ناجحا يمكن أن يؤثر في مختلف عناصر قوة الدولة، مع

[1]) د. درويش سعيد،الحروب السيبرانية وأثرها علي حقوق الإنسان، دراسة علي ضوء أحكام دليل تالين، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية، المجلد (٥٤)، العدد (٥)، مارس ٢٠١٧، ص١٩٠.

صعوبة تحديد مصدر الهجوم أو الطرف المعتدي، مما أدى إلي اتساع نطاق التحدي العالمي الذى تمثله الهجمات السيبرانية([1]).

وقد ظهر بوضوح دور الفضاء السيبراني كمجال جديد في العمليات العدائية في الصراع بين إستونيا وروسيا عام ٢٠٠٧ ، وفي الحرب بين روسيا وجورجيا عام ٢٠٠٨ ، ثم جاء الهجوم السيبراني الأمريكي بفيروس "ستاكسنت" علي برنامج إيران النووي عام ٢٠١٠ ليشكل نقله مهمة في مجال تطور الأسلحة السيبرانية([2])، وفي عام ٢٠١٦ جاء الهجوم السيبراني الروسي علي الحزب الديمقراطي الأمريكي ليعيد الجدل حول خطورة الهجمات السيبرانية وطبيعتها كهجوم مسلح أو عمل من أعمال الحرب، ومن تداعيات هذا الهجوم إعلان سكرتير حلف الناتو أن بعض الهجمات السيبرانية تعد هجوماً مسلحاً وتتطلب تفعيل المادة (٥١) للدفاع الجماعي([3]).

وفى ذات الإطار، تشكل الهجمات السيبرانية إحدى أهم التحديات الراهنة التي يواجهها المجتمع الدولي، وخاصة في تحديد طبيعتها القانونية، فضلاً عن نطاق هذه الهجمات في ضوء أحكام القانون الدولي الإنساني وما يترتب عليها من تبعات المسئولية الدولية الجنائية كانت أم المدنية، وكذلك الغموض الذي يحيط بمفهوم الهجمات السيبرانية وعدم الاتفاق علي تعريف

---

[2]) عمر أحمد السعيدي، د. زياد محمد جفال، مدى اعتبار الهجمات السيبرانية انتهاكاً للحظر المفروض علي اتخدام القوة أو التهديد بها فى ضوء أحكام القانون الدولي للجوء للحرب، مجلة جامعة الإمارات للبحوث القانونية، جامعة الإمارات العربية المتحدة، كلية القانون، المجلد (٣٨)، العدد (٩٩)، سبتمبر ٢٠٢٤، ص٣٩٣.

[1]) د. عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، سلسة أوراق، العدد الثالث والعشرين، وحدة الدراسات المستقبلية،مكتبة الإسكندرية، ٢٠١٦، ص١١.

2) Carl Fitz,"All is Fair in Love and Cyber war: International Law and Cyber Attacks", Houston Journal of International Law, Vol. 1, No, 2017, p8.

محدد لها، يمكن الاستناد في إطاره لتنظيم استخدام الهجمات السيبرانية بالحظر أو التقييد لمواجهة عواقبها الجسيمة علي الصعيد الدولي الإنساني([1]).

- **أهمية موضوع الدراسة:**

ترجع أهمية هذه الدراسة إلي حداثة الموضوع محل الدراسة، وتعقده البالغ في ذات الوقت، إذ أن تحدي الهجمات السيبرانية علي وجه الخصوص دون غيرها من باقي التحديات التى شهدها الفقه القانوني الدولي والممارسة الدولية، تشكل تحدياً هائلاً لقواعد القانون الدولي العرفي الثابتة لمبدأ سيادة الدول وحق الدفاع الشرعي والمسئولية الدولية بل لباقي فروع االقانون الدولي ذات الصلة، وهو الأمر الذى يدفع بدوره لممارسة دولية جديدة ومتطورة تماماً لمواجهة الهجمات السيبرانية المسلحة.

- **أهداف الدراسة:**

يعد موضوع الهجمات السيبرانية من الموضوعات التي تحتل مرتبة متقدمة في الفقة القانوني الدولي، لما تثيرة من إشكاليات وتحديات هائلة بشأن استخدام التكنولوجيا الالكترونية في المجال العسكري والأمني وتحديد آثارها المستقبلية علي السلم والأمن الدوليين، وبالتالي تهدف الدراسة إلي ما يلي:-

- بيان مفهوم الهجمات السيبرانية والتكييف القانوني لها ومدى إمكانية تصنيف الهجمات السيبرانية ضمن أساليب ووسائل القتال وإذا كانت كذلك هل ستنطبق عليها أحكام الاتفاقيات الدولية والقواعد العرفية ذات الصلة بسير العمليات العدائية وكيفية تعامل المجتمع الدولي مع

---

[3] Oona` A.Hathway , Rebecca Crootof , Philip Levtiz , aley Nix, Aileen Nowlan ,William Perdue and Julia Spiegel, "The Law of Cyber –Attack", California Law Review, 2012 ,p7.

مشكلة الفراغ القانوني الذي يشهده موضوع التنظيم الدولي للهجمات السيبرانية، ومدي مشروعية اللجوء إليها في ضوء أحكام القانون الدولي.

- بيان الجهود الدولية المبذولة لمواجهة الهجمات السيبرانية.
- بيان المسئولية الدولية عن الهجمات السيبرانية.

- **إشكالية الدراسة:**

أثارت ظاهرة الهجمات السيبرانية جدلاً واسعاً في فقه القانون الدولي، عما إذا كانت القواعد القانونية الحالية تكفي لمواجهة هذه الأشكال الجديدة من الهجمات المسلحة أم الأمر يقتضي تأسيس قواعد قانونية جديدة تكون أكثر ملاءمة مع هذا التطور في شكل الهجمات السيبرانية ولا سيما مع تزايد أهمية الأمن السيبراني في القطاعات الحكومية والعسكرية والاقتصادية وأصبحت حماية الفضاء السيبراني عنصراً جوهرياً لاستراتيجية الأمن القومي للدول([1]).

وبالتالي تتمثل إشكالية البحث في بيان موقف القانون الدولي من الهجمات السيبرانية، والتكييف القانوني للهجمات السيبرانية من حيث مدى اعتبار الهجمات السيبرانية التى تؤدي إلي ضحايا بشرية وخسائر مادية جسيمة – استخداما للقوة المسلحة بموجب قواعد القانون الدولي والتى يمكن للدول المتضررة اللجوء لاستخدام القوة المسلحة في الرد علي هذه الهجمات استناداً لحق الدفاع الشرعي عن النفس وفقاً للمادة (٥١) من الميثاق، ومدى فعالية قواعد القانون الدولي الحالية وكفايتها للتعامل مع تحدى الهجمات السيبرانية.

- **منهج الدراسة:**

لما كان الهدف الرئيسي من الدراسة هو إبراز مفهوم الهجمات السيبرانية والتكييف القانوني لها وبيان المسئولية الدولية عن الهجمات السيبرانية، وبشكل خاص الوقوف علي مدى التزام الدول

---

[1] Matthew C.Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)",The Yale Journal of International Law, Vol. 36,2011,p431.

بقواعد القانون الدولي عند إستخدام الهجمات السيبرانية، والجهود الدولية المبذولة لمواجهة الهجمات السيبرانية، لقد وجدنا في المنهج الوصفي التحليلي أنه السبيل الأمثل لطرح كافة جوانب موضوع الدراسة، كما اعتمدنا في هذه الدراسة علي استخدام الأسلوب الوثائقي لجمع المعلومات من خلال الكتب والأبحاث ذات الصلة بموضوع الدراسة.

- **خطة الدراسة:**

لعل الإحاطة بكافة جوانب موضوع مواجهة الهجمات السيبرانية فى ضوء أحكام القانون الدولي تقتضي تناول دراسة هذا الموضوع وفقاً للخطة الآتية:

المبحث التمهيدي: مفهوم الهجمات السيبرانية.

المطلب الأول: تعريف الهجمات السيبرانية وتمييزها عن مصطلحات مشابهة.

المطلب الثاني: وسائل وأساليب تنفيذ الهجمات السيبرانية.

المطلب الثالث: تهديدات الهجمات السيبرانية ومخاطرها.

المبحث الأول: التكييف القانوني للهجمات السيبرانية.

المطلب الأول: تكييف الهجمات السيبرانية وفقاً لمبادئ الأمم المتحدة.

المطلب الثاني: تكييف الهجمات السيبرانية وفقاً لمبادئ القانون الدولي الإنساني.

المطلب الثالث: مدى إمكانية تطبيق قواعد القانون الدولي الحالية علي الهجمات السيبرانية.

المبحث الثاني:الجهود الدولية لمواجهة الهجمات السيبرانية.

المطلب الأول: إتفاقية مجلس أوروبا "بودابست" بشأن الجريمة السيبرانية لعام ٢٠٠١.

المطلب الثاني: دليل تالين وإعلان إيريتشي.

المطلب الثالث: جهود الأجهزة الرئيسية للأمم المتحدة ووكالاتها المتخصصة بشأن مواجهة الهجمات السيبرانية.

المبحث الثالث:المسئولية الدولية عن إستخدام الهجمات السيبرانية.

المطلب الأول: مفهوم المسئولية الدولية فى ضوء الهجمات السيبرانية.

المطلب الثاني: الإشكاليات القانونية بشأن المسئولية الدولية عن إرتكاب الهجمات السيبرانية.

المبحث التمهيدي

مفهوم الهجمات السيبرانية

أدى التطور الإلكتروني الهائل إلي نشوء تحديات جديدة في المجتمع الدولي، وتعد الهجمات السيرانية أحد صور هذه التحديات والتى تتميز بسهولة تنفيذها، حيث أصبح بإمكان الدول التأثير علي بعضها البعض من خلال الهجوم على أمن البنية التحتية الكونية للمعلومات وإحداث آثار مدمرة علي الأمن القومي للدول([1]).

وفى هذا الإطار، تهدف قواعد القانون الدولي الإنساني إلي توفير الحماية الضرورية لضحايا النزاعات المسلحة، وذلك من خلال وضع قواعد قانونية تهدف إلي تحقيق التوازن بين المتطلبات الإنسانية والاعتبارات العسكرية والتى تطبق في إطار النزاع المسلح، وسوف نوضح فى هذا المبحث تعريف الهجمات السيبرانية وتمييزها عن مصطلحات مشابهة ووسائل وأساليب تنفيذ الهجمات السيبرانية، وكذلك تهديدات الهجمات السيبرانية ومخاطرها، وذلك في ثلاث مطالب علي النحو التالي:

المطلب الأول: تعريف الهجمات السيبرانية وتمييزها عن مصطلحات مشابهة.

المطلب الثاني: وسائل وأساليب تنفيذ الهجمات السيبرانية.

المطلب الثالث: تهديدات الهجمات السيبرانية ومخاطرها.

المطلب الأول

تعريف الهجمات السيبرانية وتمييزها عن مصطلحات مشابهة

أولا: تعريف الهجمات السيبرانية:

---

[1]) د. إيهاب خليفة، القوة الإلكترونية .. كيف يمكن أن تدير الدول شؤونها في عصر الإنترنت؟ "الولايات المتحدة نموذجاً"، الطبعة الأولي، العربي للنشر والتوزيع، القاهرة، ٢٠١٧، ص٢٠.

من الملاحظ عدم إتفاق الفقه الدولي علي تعريف قانوني للهجمات السيبرانية، حيث تعددت تعريفات الهجمات السيبرانية، وتتراوح هذه التعريفات بين من يعد السيبرانية بمثابة أداة للهجوم وآخر يعدها هدفاً له، وثالث يركز علي الآثار الناتجة عنه.

حيث قصر جانب من الفقه تعريف الهجمات السيبرانية علي الأداة المستخدمة في الهجوم، ومن ذلك:عرفها البعض بأنها" هجوم عبر الفضاء السيبراني، يهدف إلي السيطرة علي مواقع الكترونية، أو بنى تحتية محمية الكترونياً لتعطيلها أو تدميرها أو الأضرار بها"([1]). وعرفها آخرون بأنها" تلك الإجراءات التي تتخذها الدولة من أجل الهجوم علي نظم المعلومات للعدو وبهدف التأثير والإضرار بها، وفي الوقت نفسه للدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة"([2]). وحددها البعض الآخر بأنها:" تلك الإجراءت التى تتخذها الأطراف في نزاع مسلح لكسب الميزة على خصومهم في فضاء السايبر بإستخدام مختلف الوسائل التكنولوجية والأشخاص التقنيين، ويحصل علي المزايا من جراء تلك الهجمات وذلك بإتلاف أو تدمير أو تعطيل أو الاستيلاء علي أنظمة الحاسوب للعدو والحصول علي معلومات سرية"([3]) كما بين البعض بأنها:"استخدام البيانات والأكواد الضارة أو الخبيثة لتغيير بيانات وأكواد الحواسيب، مما

---

[2] Richard Kissel,"Glassory of Key Information Security Terms", National Institute of Standards and technology, U.S Department of Commerce ", Revision, 2, May, 2013, p.57.

[1] Schmitt, M.N, "Computer network attack and the use of force in international law": thoughts on a normative framework. In the Use of Force in International Law, 2017, Vol.27, No. 379-431, p.7.

[2] د. يحيي ياسين سعود، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، المجلة القانونية، كلية الحقوق جامعة القاهرة (فرع الخرطوم)، المجلد (٤)، العدد (٤)، ٢٠١٨،ص٨٥، راجع حول ذلك بالتفصيل:

-Herbert Lin, Cyber conflict and international humanitarian law, International review of the red cross, 2012, Vol. 94, N886, P515.

يؤدي إلي عواقب وخيمة تتراوح ما بين تعريض سلامة هذه البيانات للخطر أو سرقة المعلومات والبيانات الشخصية والهويات"([1]).

وتوسع جانب آخر من الفقه في تعريف مفهوم الهجمات السيبرانية إستناداً إلي الغرض أو الهدف من الهجمات بدلاً من الوسائل المستخدمة، حيث قرر البعض بأنها:" إستخدام إجراءات متعمدة لتغيير أو تعطيل أو خداع أو إضعاف أو تدمير أنظمة أو شبكات كمبيوتر الخصم، أو المعلومات والبرامج الموجودة في هذه الأنظمة أو الشبكات"([2])، وحددها البعض الآخر بأنها"الاستغلال غير المشروع لأنظمة الحاسوب، والشبكات، والمنظمات التى تعتمد علي تقنية المعلومات والاتصالات الرقمية بهدف إحداث أضرار أو تعطيل أو تشفير أو تدمير نظم البنية التحتية المعلوماتية"([3]) كما بين البعض بأنها:" كل فعل يقوض من قدرات ووظائف شبكة الكمبيوتر لأغراض سياسية أو ماسة بالأمن القومي، من خلال استغلال نقطة ضعف معينة تمكن المهاجم من التلاعب بالنظام"([4]). وأورد البعض الآخر بأنها:" هجوم عبر الانترنت يقوم علي التسلل إلي مواقع إلكترونية غير مرخص بالدخول إليها بغرض تعطيل البيانات المخزنة

---

[3]) د. أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، كلية القانون جامعة بابل، العراق، العدد الرابع،السنة الثامنة، ٢٠١٦،ص٦١٦.

[4]) د. شريف نسيم قلته بخيت،الهجمات الإلكترونية وحق الدفاع الشرعي للدول في القانون الدولي، رسالة دكتوراه، كلية الإقتصاد والعلوم السياسية، جامعة القاهرة،٢٠٢٣،ص١٩-٢٠، راجع حول ذلك بالتفصيل:

-Lisa Nevala, What Can be Qualified as an Armed Attack in Cyber Operations under the Article 51 of the UN Charter under the Energy Sector in Finland?, Master Thesis, Tallinn University of Technology,2022,p9

[5]) د. أبو بكر محمد الديب، المسئولية الدولية تجاه استخدام الأسلحة الحديثة في النزاعات، مجلة السياسة الدولية، المجلد ٥٨، العدد ٢٣٤، أكتوبر ٢٠٢٣، ص٤١.

[1]) Cyber-Attacks and the Use of Force: Matthew C. Waxman, Back to the Future of Article 2(4), The Yale Journal of International, Vol. 36, 2011, P.423.

عليها أو إتلافها أو الاستيلاء عليها وهى عبارة عن سلسلة هجمات سيبرانية تقوم بها دولة ضد أخري"([1]).

ويري أصحاب هذا الاتجاه أن الاعتماد علي الغرض في تعريف الهجمات السيبرانية أفضل لسببين رئيسيين هما: أن تعريف الهجوم السيراني نظراً للغرض وليس الوسيلة هو أكثر منطقية فإستخدام شبكة الكمبيوتر لتشغيل طائرة مقاتلة بدون طيار لتنفيذ هجوم معين ليس هجوماً سيبرانياً بل إنه استخدام للتكنولوجيا الحديثة في الحرب التقليدية، بينما استخدام متفجرات منتظمة لقطع كابلات الشبكة في البحار التى تحمل حزم المعلومات والبيانات هو هجوم سيبراني لأن الهدف المقصود هو تعطيل أو تدمير البنية التحتية الحيوية، كما يتجنب هذا الرأي المخاطر الجسيمة التى يشكلها التعريف القائم علي الوسائل والذى من شأنه فرض قيود علي حرية التعبير والخطاب والمعارضة السياسية علي الإنترنت.

وعلى الرغم من وجاهة هذا الرأى ومحاولته تقديم تعريف محدد للهجمات السيبرانية، إلا أنه يؤخذ عليه عدم تقديمه تمييزاً كافياً بين مفهوم الهجوم السيبراني ومفهوم الجرائم السيبرانية السياسية أو الأمنية، كما أنه لا يمكن قبول الرأي القائل إن الهجوم السيبراني يتم تحديده بصرف النظر عن الوسيلة المستخدمة التى قد تكون أسلحة تقليدية أو إلكترونية، وبالتالي فإن هذا الرأى يؤدي إلي خلط واسع النطاق بين الهجمات السيبرانية والهجمات التقليدية، وخاصة أن أهم ما يميز الهجمات السيبرانية هو استخدامها كوسيلة للقيام بالهجمات واستغلال خصائصها المميزة لتنفيذ هذه الهجمات([2]).

وذهب جانب ثالث من الفقه إلي تعريف مفهوم الهجمات السيبرانية إستناداً إلي الآثار التى يمكن أن تترتب عليها، ومن ذلك: عرفها البعض بأنها"أي تصرف دفاعياً كان أم هجومياً، يتوقع منه وعلي نحو معقول في التسبب بجرح أو قتل شخص أو إلحاق أضرار مادية أو دمار

[2)]Micheal S.Fuertes, "Cyber warfare, Unjust Actins in a just War ", FloridaInternational University, Full 2013, P.1.

[3]) د. محمود حسين الشرقاوي، الهجمات الإلكترونية في ضوء أحكام القانون الدولي الإنساني، رسالة دكتوراه، كلية الحقوق، جامعة بني سويف،٢٠٢١، ص ٤٩-٥٠.

بالهدف المهاجم"([1]) وهو التعريف الذي يقرب الهجمات السيبرانية من أن تعد بمثابة هجمات مسلحة وفقاً لقواعد القانون الدولي الإنساني، والتى قد تشن ضد دولة ما بصرف النظر عمن يقوم بها، والأداة المستخدمة فيها وسواء أكانت للدفاع عن النفس ضد هجمات تقليدية أم سيبرانية أو ذات طابع هجومي، كما بين البعض بأنها:" عمليات لإيقاع الفوضي في المعلومات التى يتم تخزينها في أجهزة أو شبكات الحاسوب أو الأجهزة أو الشبكات نفسها أو نفيها أو الانتقاص منها أو تدميرها، وبصرف النظر عن الإطار الذى تجرى فيه الهجمات، وتعتمد هذه الهجمات علي عدد هائل من البيانات الإلكترونية لتنفيذ الهجوم، وقد تصل هذه الهجمات إلي مستوى حرب المعلومات ويمكن اللجوء إليها وقت السلم"([2])، وأورد البعض الآخر بأنها:" الهجمات التى تقوم علي إستخدام أنشطة الكترونية متعددة بغرض إضعاف أو تدمير أنشطة الحاسوب أو إتلافها أو إرسال معلومات من خلالها، أثناء استخدام شبكات الحاسب الآلي التابعة للخصم" وكذلك عرفها بعضهم بأنها"قيام دولة أو كيانات من غير الدول بشن هجوم إلكتروني في إطار متبادل، أو من قبل طرف واحد"([3])، وحددها البعض بأنها"العمليات العدائية التى تستهدف شبكات الحاسوب والمنشآت المرتبطة بها لغرض تحقيق إصابات أو أضرار مادية في المعلومات المخزنة في الحواسيب والبنية التحتية من خلال استخدام الفضاء السيبراني

---

[4] Micheal N.Schmitt,"Tallinn Manual on the International Law Applicable to Cyber Warfare", Cambridge University press, first publishes 2013.p.92.

[1] د. أميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة البحوث الفقهية والقانونية، كلية الشريعة والقانون بدمنهور، جامعة الأزهر، العدد الخامس والثلاثون، الجزء الثالث، ٢٠٢٠،ص٣٩٤.

[2] د. عادل عبد الصادق، أنماط الحرب السيبرانية وتداعياتها علي الأمن العالمي، مجلة السياسة الدولية، ملحق اتجاهات نظرية، الصراع السيبراني، مركز الأهرام للدراسات الاستراتيجية، القاهرة، العدد ٢٠٨،ابريل ٢٠١٧،ص٣١-٣٢.

وتنفيذ الهجمات داخله، والتى قد تصل إلي الموت أو التدمير الكلي للبنية التحتية"([1])، كما بين البعض بأنها:" أى عملية إلكترونية تقوم بها دولة ضد دولة أخري، يكون هدفها تعطيل المعلومات الموجودة علي شبكات الكمبيوتر أو إتلافها، لتعريض الدولة لخطر ما، أو السيطرة علي بعض المجالات داخل الدولة"([2]).

وبتحليل العرض السابق يمكننا استخلاص أن الهجوم السيبراني يشمل أى عمل عدائي يقع في زمن السلم تقوم به الدول أو كيانات تابعة لها ضد دول أخري، ويتم بإستخدام وسائل تكنولوجية يوفرها الفضاء السيبراني بهدف تدمير أو تعطيل أو التشويش علي شبكات الكمبيوتر التى تتحكم أساساً بالبنية التحتية الحيوية، المدنية أو العسكرية، لتلك الدول لأغراض سياسية أو أمنية أو إقتصادية أو غيرها.

وفى ذات الإطار، عرفت القيادة الإستراتيجية الأمريكية عام ٢٠٠٧، الهجمات السيبرانية بأنها:" تطويع عمليات نظام الكمبيوتر بهدف منع الخصوم من الإستخدام الفعال لها، فضلاً عن التسلل إلي أنظمة المعلومات وشبكات الإتصال بغرض جمع البيانات التى تحتويها وحيازتها وتحليلها"([3]). وعرفها دليل قيادة إدارة الأمن السيبراني بالولايات المتحدة الأمريكية لعام ٢٠١١، بأنها تشمل أى:" عمل عدائي بإستخدام الكمبيوتر أو الشبكات أو الأنظمة السيبرانية ذات الصلة، ويهدف إلي تعطيل أو تدمير أو التلاعب بأنظمة الإنترنت لدولة، أو المعلومات المخزنة علي الحاسبات الآلية لها، أو الأصول أو الوظائف الحيوية لتلك الأجهزة، وتتم هذه

---

[3]) د. محمد صلاح عبد اللاه ربيع، الهجمات السيبرانية بين مشروعيتها كوسيلة للدفاع الشرعي وادانتها كاعتداء غير مشروع: دراسة تحليلية فى ضوء القانون الدولي، مجلة الدراسات القانونية والاقتصادية، كلية الحقوق جامعة مدينة السادات، المجلد (١٠)، العدد (١)، مارس ٢٠٢٤.ص٤١٦٤.

[4]) د. سامي محمد عبد العال، الدفاع الشرعي ضد الهجمات السيبرانية، المجلة المصرية للقانون الدولي، الجمعية المصرية للقانون الدولي، المجلد التاسع والسبعون، العدد ٧٩ لسنة ٢٠٢٣،ص٣٠.

[1])K.Saalbach," Cyber War, Methods and Practice", Version 9.0, University of Osnabruck-17 Jun 2013, p.8.

الهجمات بوسائل متعددة منها المراسلات الإلكترونية المزيفة، أو الرسائل المفخخة، وتتميز هذه الهجمات بأن آثارها عادة ما تكون منفصلة من الناحية الجغرافية عن نقطة إنطلاقها"([1]).

كما عرفتها اللجنة الدولية للصليب الأحمر بأنها:"عمليات تشن ضد أو عبر نظام حاسوب من خلال تدفق البيانات، وتهدف هذه العمليات إلي تحقيق أغراض مختلفة ومنها اختراق نظام معين وجمع أو نقل أو تدمير أو تغيير أو تشفير البيانات أو إجراء تعديل للعمليات التى يتحكم بها جهاز الحاسب الآلي المخترق أو التلاعب بها ويمكن إعتبار تلك العمليات في بعض الظروف – هجمات وفقاً للتعريف الوارد في القانون الدولي الإنساني وتحديداً نص الفقرة (٢) من المادة (٤٩) من البروتوكول الإضافي الأول لعام ١٩٧٧([2]).

وعرفها دليل تالين "١" لعام ٢٠١٣ (القاعدة رقم ٣٠) وكذلك دليل تالين"٢"لعام ٢٠١٧ (القاعدة رقم ٩٢)، بأنها:"عملية سيبرانية، سواء كانت هجومية دفاعلية، والتى يهدف من خلالها بصورة معقولة التسبب الاصابة أو وفاة الأشخاص أو الاضرار أو تدمير الأعيان أو الأهداف"([3])، ويعد هذا التعريف من أفضل التعريفات التى قدمت في في هذا الشأن، حيث يجمع بين الوسيلة المستخدمة وكذلك الهدف من الهجوم، فمن ناحية الوسيلة يجب أن يتم الهجوم بإستخدام الوسائل التكنولوجية عن طريق الفضاء السيبراني، ومن ناحية الهدف يجب أن تؤدي أو يحتمل بشكل معقول أن تؤدي الهجمات السيبرانية إلي خسائر مادية مماثلة للخسائر التى تحدثها الهجمات التقليدية، من إصابات أو وفاة أو تدمير للمنشآت أو الممتلكات.

---

[2] Joint Terminology for Cyberspace Operations, The Vice Chairman of The Joint Chiefs of Staff, Department of efense, Washington, D.C., 2011, available at:

https://info.publicintelligence.net/DOD-JointCyberTerms.pdf.

[3] د. أحمد عبيس نعمة الفتلاوي، د. أزهر عبد الأمير الفتلاوي، المسؤولية الناشئة عن إستخدام وسائل القتال الفتاكة في نشر الأوبئة (الهجمات السيبرانية في مقابل جائحة كورونا أنموذجا)، مجلة الحقوق الجامعة المستنصرية – كلية القانون، المجلد (١٣)، العدد(٤١)،٢٠٢١،ص٦٠.

[1] T. HERR, P. ROSENZWEIG, Cyber Weapons and Export Control: Incorporating Dual Use with the Prep Model, 8 J. NAT'L SEC. L. & POL'Y, 2015, P. 301.

وترتيباً علي ما سبق، يمكننا المساهمة بتعريف للهجمات السيبرانية بإعتبارها:" عمليات سيبرانية عدائية تتم في الفضاء السيبراني تقوم بإرتكابها دول أو كيانات من غير الدول(أفراد أو مجموعات مسلحة) سواء كانت هجومية أو دفاعية وينتج عنها أضراراً مباشرة للأنظمة الإلكترونية والبنية التحتية للدولة ضحية الهجوم السيبراني، ومن أمثلتها تعطيل الأنظمة الالكترونية للمؤسسات الطبية مما قد يؤدي إلي حدوث وفيات أو تدمير أنظمة شبكات الكهرباء وأنظمة تشغيل السدود مما يتسبب في حدوث فيضانات، وغالباً ما يتم استخدام الهجمات السيبرانية لتحقيق أهداف سياسية أوأمنية أو اقتصادية أو أى أهداف مماثلة".

ثانيا:- تمييز الهجمات السيبرانية عن مصطلحات مشابهة

فى ضوء تشابه الممارسات السيبرانية باعتبارها تتم الكترونياً ومن خلال الفضاء السيبراني، وكذلك ما قد ينتج عنه أضراراً أو ربما يرقي لتهديد أمن الدول واستقرارها، مثل الهجمات السيرانية والحرب السيبرانية والإرهاب السيبراني والتجسس السيبراني، إلا أنها ليست متماثلة فكل منها خصائص مميزة، وقد يؤدي الخلط بينها إلي صعوبات عملية وتشريعية، حيث تقوم معظم الدول بتنظيم العمليات السيبرانية في تشريعاتها الوطنية، بإعتبارها نوع واحد فقط، وهو الجريمة السيبرانية ذات الطبيعة الجنائية كالنصب والسرقة وتزوير التوقيع الالكتروني وغيرها، ولا تخصص هذه التشريعات مساحة لباقي العمليات السيبرانية، والتى تستهدف تعطيل أو تدمير البني التحتية والأنظمة المعلوماتية لمؤسسات الدول، والتى قد تكافئ آثارها ما ينتج عن الهجوم المسلح التقليدي، ويستلزم الأمر تناول كل منها بنصوص تتفق مع طبيعتها وخصائصها وآثارها المحتملة([١])، ولأغراض الدراسة، سوف نتناول التمييز بين هذه الممارسات، وعلي النحو التالي:-

---

[٢]) د. محمد عادل محمد عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق علي ممارسة التجسس وقت السلم: دراسة علي ضوء دليل "تالين" بشأن القانون الدولي المطبق علي العمليات السيبرانية ٢٠١٣-٢٠١٧، مجلة البحوث القانونية والاقتصادية، كلية الحقوق جامعة بني سويف، المجلد (٣٣)، العدد (١)، يناير ٢٠٢١، ص٢٦٨.

١- التمييز بين الهجمات السيبرانية والحرب السيبرانية:

تعرف الحرب السيبرانية بأنها:" أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخري بغرض تحقيق أضرار بالغة أو تعطيلها"، ويعرفها البعض بأنها:" الهجمات التى تتم بواسطة استخدام الكمبيوتر أو الشبكات أو الأنظمة ذات الشأن، وتهدف إلي تعطيل أو تدمير أنظمة الإنترنت، أو الممتلكات أو الوظائف الحاسوبية الخاصة بالخصم"([١])، كما تعرف بأنها" استخدامات معينة لتكنولوجيا المعلومات والاتصالات ضمن استراتيجية عسكرية هجومية أو دفاعية مدروسة داخل الفضاء الإلكتروني بهدف التعطيل الفوري أو السيطرة علي موارد العدو"([٢]).

وهناك من عرفها بأنها:" أى تصرف الكتروني دفاعياً كان أم هجومياً يتوقع منه التسبب بجرح أو قتل شخص أو إلحاق أضرار مادية أو دمار بالهدف المهاجم"وبالتالي يعد الهجوم السيبراني" تصرف ينفذ في عالم رقمي قائم علي إستخدام بيانات رقمية ووسائل إتصال تعمل الكترونياً بهدف تحقيق أهداف عسكرية أو أمنية ملموسة ومباشرة نتيجة إختراق مواقع الكترونية حساسة ذات أولوية كأنظمة حماية محطات الطاقة النووية أو الكهربائية أو المطارات ووسائل النقل الأخري"([٣]).

كما تعد الحرب السيبرانية أحد مصادر تهديد الأمن الدولي، ويقصد بها "أساليب الحرب ووسائلها التى تعتمد علي تكنولوجيا المعلومات وتستخدم في إطار نزاع مسلح بخلاف العمليات العسكرية التقليدية، وذلك لأهداف متنوعة من بينها التسلل إلي نظام الحاسوب وجمع البيانات المخزنة به أو سرقتها أو إتلافها أو تبديلها أو التلاعب بها بعد أن تصبح تحت سيطرة مدبر

---

[١]) د. شريف نسيم قلته بخيت، الهجمات الإلكترونية وحق الدفاع الشرعي للدول في القانون الدولي، مرجع سابق،ص٢٢.

[2]) Michael Robinson and others, "Cyber Warfare: Issues and Challenges", Computers and Security, No.49, 2015, pp73-76.

[٣]) د. أحمد عبيس نعمة الفتلاوي، زهراء عماد محمد كلنتر، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مجلة الكوفة للعلوم القانونية والسياسية، العراق، المجلد (١٣)، العدد(٤٤)،٢٠٢٠،ص٥١-٥٢.

الهجوم"([١]).وبالتالي يتشابة مفهوم الحرب السيبرانية إلي حد كبير مع مفهوم الهجمات السيبرانية، فيما عدا الإشارة إلي هدف تحقيق الأهداف العسكرية وعلانية حالة الحرب السيبرانية من جانب الدولة المعتدية وأن يتم إستخدام الحرب السيبرانية لخوض هذه الحرب في الفضاء السيبراني والتى ترقي إلي مستوى النزاع المسلح([٢])، وتتميز الهجمات السيبرانية كأسلوب للحرب بالسرعة الهائلة في التنفيذ وتعد من أدوات الحرب الشاملة نظراً لما تسببه من آثار إنسانية جسيمة، ومثال ذلك: عندما يتم تنفيذ هجمة سيبرانية للسيطرة علي أنظمة التحكم في المطارات والحركة الجوية أو محطات الطاقة النووية وهو ما قد ينتج عنه آثار كارثية محتملة من تصادم الطائرات أو تسرب إشاعات نووية([٣]).

٢- التمييز بين الهجمات السيبرانية والإرهاب السيبراني:

أصبحت التكنولوجيا أحد أبرز أسلحة التنظيمات الإرهابية، وقد أسهمت هذه التطورات التكنولوجية فى ظهور أنماط جديدة من الإرهاب لم تكن موجودة من قبل، منها الإرهاب السيبراني([٤])، وهو إحدى صور الجرائم السيبرانية العابرة للحدود الوطنية، تمس على نحو مباشر أمن الدول، إذ تستخدم التنظيمات الإرهابية الإنترنت للقيام بعمليات الدعوة والتجنيد وجمع التمويل اللازم لتنفيذ عملياتها الإرهابية، وكذلك إختراق الموقع الإلكترونية، وصفحات

---

[٤]) د.هالة أحمد الرشيدي، الإرهاب السيبراني، ماهيته وجهود مكافحته في ضوء التشريعات والقوانين الوطنية والدولية، دار النهضة العربية،القاهرة، ٢٠٢١، ص٤٢.

[١]) د. عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، سلسة أوراق، العدد الثالث والعشرين، وحدة الدراسات المستقبلية،مكتبة الإسكندرية،٢٠١٦، ص٥٥.

[٢]) د. سلوي يوسف الاكيابي، مدي انطباق القانون الدولي الإنساني علي الهجمات السيبرانية، مجلة روح القوانين، كلية الحقوق جامعة طنطا، المجلد (٣٥)، العدد (١٠١)، يناير- الجزء الثاني ٢٠٢٣، ص ١٢٩٠- ١٢٩٤.

[٣]) د. وسام محمود عرفان مصطفي، سبل مكافحة الهجمات السيبرانية دولياً، مجلة الدراسات القانونية والاقتصادية، كلية الحقوق جامعة مدينة السادات، المجلد (١٠)، العدد (٣)، سبتمبر ٢٠٢٤، ص٣٠٠٠.

التواصل الاجتماعى للضحايا للتأثير فيها معنوياً، فضلاً عن إختراق الحواسب الآلية للمؤسسات والمرافق الحيوية العسكرية والاقتصادية والثقافية للدول المستهدفة، كالبنوك والبورصات العالمية والمطارات والموانئ وغيرها، والإطلاع على بياناتها المخزنة والتجسس عليها وتدميرها وإرسال رسائل تدمير للحكومة لقبول مطالبها، على نحو يهدد أمن الدول العسكرى والإقتصادى([1]).

ويعرف الإرهاب السيبراني بأنه:" إستخدام أدوات شبكات الحاسوب في تدمير أو تعطيل البني التحتية الوطنية المهمة، كالطاقة والنقل والعمليات الحكومية، أو بغرض ترهيب حكومة ما أو مدنيين"،وهناك من عرفه بأنه"هجمة إلكترونية غرضها تهديد الحكومات أو العدوان عليها، سعياً لتحقيق أهداف سياسية أو دينية أو أيديولوجية، وأن الهجمة يجب أن تكون ذات أثر مدمر وتخريبي مكافئ للأفعال المادية للإرهاب"([2]).

ويتميز الإرهاب السيبراني بالطابع العابر للحدود، ليس فقط من حيث آثارها وأضرارها، بل أيضاً من حيث مراحل إعداده وتنفيذه. فقد يتم التخطيط للجريمة الإرهابية بدولة، ويتم جمع التمويل اللازم لتنفيذها ورصده بدولة أخرى، ويتم التنفيذ بدولة ثالثة. وبالتالي، يدخل الإرهاب السيبراني ضمن طائفة الجرائم المنظمة غير الوطنية([3]).

وقد اهتمت بعض الدول بسن تشريعات وطنية وإتخاذ ما يلزم من تدابير تشريعية وإجرائية ومؤسسية لمكافحة الإرهاب السيبراني، بالنظر إلى أخطاره الجسيمة التى أصبحت تهدد أمن

---

[4]) د. رغدة البهي، الإرهاب السيبراني: المفهوم والسمات والأنماط، المركز المصري للفكر والدراسات الاستراتيجية، ٣٠ سبتمبر ٢٠١٩، متاح علي الرابط التالي:

https://www.ecsstudies.com/7414

[1]) بن صابر بلقاسم، د. حيدرة محمد، الهجمات السيبرانية ومواجهتها في ضوء القانون الدولي المعاصر، مجلة حقوق الإنسان والحريات العامة، الجزائر،العدد الرابع، يونيو ٢٠١٧، ص ١٩٤.

[2]) د. مايا حسن خاطر، الإطار القانوني لجريمة الإرهاب السيبراني، مجلة جامعة الناصر، العدد الخامس، المجلد الأول، يناير– يونيو ٢٠١٥، ص١٣٨.

الدول والمجتمعات بشكل دائم. ولجأت بعض الدول الأخرى إلى استخدام القوانين الجنائية العامة أو التشريعات المتعلقة بمكافحة الإرهاب أو الجرائم السيبرانية أو مزيج مما سبق لتجريم هذه الأعمال وملاحقة مرتكبيها قضائياً. فى المقابل، جرم عدد من الدول بعض جوانب استخدام شبكة الإنترنت ووسائل تكنولوجيا المعلومات والاتصالات المتاحة لتحقيق أغراض إرهابية، ضمن مكافحتها لجرائم دولية أخرى. فجرم التشريع السعودى تمويل الإرهاب عبر شبكة الإنترنت ضمن جرائم غسل الأموال. وجرمت بعض الدول الهجوم على البنية التحتية المعلوماتية للمرافق الحيوية للدولة ضمن قوانين أمن المعلومات. كما جرمت بعض الدول التحريض على الإرهاب والدعاية إلى العنف والتطرف عبر شبكة الإنترنت ضمن جهودها لتنظيم حرية الاتصالات والمعلومات([1]). ورغم جهود بعض الدول فى إطار مكافحة ظاهرة الإرهاب السيبراني، فإنها تظل غير كافية بذاتها لمواجهة الإرهاب السيبراني ومكافحته.

وترتيباً علي ما تقدم، يعد الإرهاب السيبراني شكل من أشكال الهجمات السيبرانية، لكن هناك بعض الصفات المميزة له، وذلك استناداً إلي الهدف الرئيسي للإرهاب السيبراني ونمط منفذيه وهم الفواعل من غير الدول مثل الهاكرز أو المتسللين، كما أن أهدافه الرئيسية فهي أما سياسية أو أيديولوجية أو دينية، كما أن المستهدفين من الإرهاب السيبراني هم غالباً السكان المدنيين بهدف إرهابهم أو إضغاف معنوياتهم وثقتهم في الحكومات والمثال علي ذلك أحداث الحادي عشر من سبتمبر ٢٠٠١ والتى استهدفت المدنيين وبرجي التجارة العالمية للتأثير علي صورة ومكانة الولايات المتحدة الأمريكية داخلياً وعالمياً([2]).

---

[3]) د. منى الأشقر جبور، الأمن السيبراني: التحديات ومستلزمات المواجهة، دراسة مقدمة إلى اللقاء السنوى الأول للمختصين فى أمن وسلامة الفضاء السيبراني، بيروت: المركز العربي للبحوث القانونية والقضائية، ٢٧-٢٨ أغسطس ٢٠١٢، ص٩.

[1]) د. شريف نسيم قلته بخيت،الهجمات الإلكترونية وحق الدفاع الشرعي للدول في القانون الدولي، مرجع سابق،ص٢٣.

٣- التمييز بين الهجمات السيبرانية والتجسس السيبراني:

يعرف التجسس السيبراني بأنه:" القيام باختراق شبكة أو جهاز إلكتروني بغرض سرقة المعلومات المخزنة فيه، والتي عادة ما تكون على درجة كبيرة من الأهمية لدى الحكومات، سواء أكانت معلومات عسكرية، أم اقتصادية، أم صناعية، أم تجارية، أم غيرها، وهو ما يترتب عليه آثار إستراتيجية فادحة في الطرف المستهدف"([١]).

وهناك من عرفه بأنه:" قيام دولة أو جهاز تابع لها أو وكيل عنها، بالإطلاع علي، أو نسخ البيانات السرية غير المتاحة للجمهور والمحفوظة علي أنظمة تكنولوجيا المعلومات أو شبكات الحاسوب الموجودة في منطقة خاضعة لولاية دولة أخرى، بواسطة عمليات سرية وباستخدام مظاهر مزيفة أو كاذبة وبدون ترخيص أو موافقة من مالكي أو مشغلي هذه الأنظمة أو شبكات الحاسوب المستهدفة، أو الدولة المستهدفة"([٢]).

وعرف دليل تالين التجسس السيبراني وقت النزاعات المسلحة بأنه:" أى عمل يتم تنفيذه سراً، أو تحت ادعاءات كاذبة، بواسطة قدرات الكترونية، بهدف جمع معلومات لإبلاغها إلي الطرف العدو" وتضمن القاعدة (٦٦) من دليل تالين "١" بعنوات التجسس السيبراني: أ- التجسس السيبراني وغيرها من صور جمع المعلومات الموجهة ضد العدو أثناء النزاع المسلح لا تنتهك قانون النزاعات المسحلة. ب- عضو القوات المسلحة الذى ينخرط في عمليات التجسس السيبراني في الأراضي التى يسيطر عليها العدو يفقد الحق في أن يتمتع بمركز أسير حرب،

---

[٢]) طلال ياسين العيسي، عدى محمد عناب،المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مجلة الزرقاء للبحوث والدراسات الإنسانية، الأردن، المجلد التاسع عشر، العدد الأول، إبريل ٢٠١٩، ص٨٥.

[3]) K ZIOLKOWSKI, Peacetime Cyber Espionage, New Tendencies in Public International Law, in K. ZIOLKOWSKI (ed), Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy, 1st edn., NATO CCD COE Publication, Tallinn 1, 2013, P. 429..

ويمكن أن يعامل كجاسوس عند القبض عليه وذلك قبل الانضمام مجدداً للقوات المسلحة التى ينتمي إليها"([1]).

وبالتالي فإن عمليات التجسس السيبراني لا ترقي إلي مستوى الهجمات السيبرانية أو كقوة بالمعني الوارد في المادة ٢ (٤) من الميثاق، وأنها تعد إنتهاكاً لمبدأ عدم التدخل وسيادة الدول وليس انتهاكاً لمبدأ حظر استخدام القوة([2]).

ومن خلال التمييز بين الانتهاكات السيبرانية، يتضح لنا وجود علاقة بين المفاهيم المختلفة للعمليات السيبرانية، سواء الحرب السيبرانية أو الهجوم السيبراني أو الإرهاب السيبراني أو التجسس السيبراني، من حيث أن كل منها يتم بإستخدام وسائل معلوماتية وتقنية خاصة بالشبكات والحاسبات، وأن أي انتهاك منها يبدأ بقيام المهاجم بالتسلل إلي الموقع المستهدف، ثم يتنوع هدف المتسلل بعد ذلك، إما أن يلي التسلل مجرد الاطلاع علي معلومات سرية من الموقع أو نسخها ونقلها، دون محاولة السيطرة علي هذا الموقع أو التحكم فيه، وهنا نكون بصدد تجسس سيبراني([3])، أما إذا أعقب التسلل السيبراني التحكم في البيانات الموجودة علي الموقع المستهدف والسيطرة عليها واستخدام ذلك في تعطيل البنية التحتية والمرافق الأساسية للدولة المستهدفة أو تخريبها أو تعطيلها، فهنا نكون بصدد هجمات سيبرانية، أما الحرب السيبرانية فإنها تتمثل في شن عدة هجمات سيبرانية سواء أكانت دفعة واحدة أو علي عدة

---

[4]) د. محمد عادل محمد عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق علي ممارسة التجسس وقت السلم: دراسة علي ضوء دليل "تالين" بشأن القانون الدولي المطبق علي العمليات السيبرانية ٢٠١٣-٢٠١٧، مرجع سابق، ص٢٧٧-٢٧٨.

[1])David Weissbrodt, "Cyber-Conflict, Cyber-Crime, and Cyber-Espionage", Minnesota Journal of International Law, Vol.22, No.2, 2013, pp 371-372.

[2]) د. وسام محمود عرفان مصطفي، سبل مكافحة الهجمات السيبرانية دولياً، مرجع سابق، ص٢٩٩٨-٢٩٩٩.

مراحل بهدف تقويض وظائف شبكة الحاسوب التابعة لمؤسسة عسكرية وحكومية للدولة محل الهجوم وبالتالي فإنها أوسع نطاقاً من الهجمات السيبرانية([1]).

المطلب الثاني

وسائل وأساليب تنفيذ الهجمات السيبرانية

أدى التطور الهائل في مجال التكنولوجيا منذ منتصف القرن العشرين، إلي استغلال الإنسان لبيئة الفضاء السيبراني وتحول كافة المعاملات إلي الاعتماد علي شبكة الإنترنت، وأصبح هذا النمط هو جوهر إدارة أنظمة الأمن القومي للدول وتشغيل البني التحتية للنظم الاقتصادية والسياسية والعسكرية، وقد شكلت تلك التعاملات السيبرانية عدد من الإشكاليات المتعلقة بكيفية استغلالها من قبل الدول، كإستغلالها للقيام بهجمات سيبرانية، والتى قد تصل الآثار الناتجة عنها إلي آثار مماثلة للنزاعات المسلحة التقليدية، أو تهدد أمن واستقرار الدول.

وفى هذا الإطار، أوردت إستراتيجية المملكة المتحدة السيبرانية، ثلاثة صور للهجمات السيبرانية، وهي التلاعب بآليات تبادل المعلومات إلكترونياً وكذلك اعتراض الموجات اللاسلكية وأيضا تعطيل الاتصالات الالكترونية، حيث تحقق الهجمات السيبرانية أهدافاً تخريبية، من خلال برامج الكترونية ضارة "فيروسات خبيثة"، لديها القدرة علي تقويض نظم تشغيل الحاسبات الآلية، والتحكم فيها، وينظر إلي تلك الأنظمة المعرضة لهذا الهجوم علي أنها تعمل بشكل سليم، ولا يتم اكتشاف ما أصابها من خلل بسهولة، مع استمرارها في إعطاء نتائج مضللة([2]).

ووفقاً لدليل الجيس الأمريكي للعمليات السيبرانية والإرهاب السيبراني لعام ٢٠٠٥، فإن الهجمات السيبرانية تهدف إلي تحقيق أربعة أهداف أساسية، وهي التلاعب بحقيقة المعلومات وما يتعلق بأمانتها وذلك بتعديلها لتصبح غير صحيحة وبلا قيمة، وأيضا إخفاء المعلومات

---

[2]) د. محمد عادل محمد عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق علي ممارسة التجسس وقت السلم: دراسة علي ضوء دليل "تالين" بشأن القانون الدولي المطبق علي العمليات السيبرانية ٢٠١٣-٢٠١٧، مرجع سابق، ص٢٧٩.

[1]) D. PUN, Rethinking Espionage in the Modern Era, Chicago Journal of International Law, Volume 18, Number 1, 2017, P. 353.

وجعلها غير متاحة للمستخدمين المصرح بهم بإستخدامها، كما تهدف إلي إفشاء سرية المعلومات وكشفها، وجعلها متاحة للمستخدمين الغير مصرح لهم بالاطلاع عليها، وكذلك تدمير أو محو أو إتلاف البنية التحتية المادية المرتبطة بتشغيل واستخدام النظم الالكترونية أو المعلومات ذات الصلة([1]).

وفي إطار تصنيف الهجمات السيبرانية وفقاً لمعيار التوجية، فتنقسم إلي طائفتين، أولها الهجمات الموجهة أو المستهدفة، وتتطلب تلك الهجمات عملية تخطيط تفصيلية ومتقنة، ويستخدم فيها المهاجم أدوات وتقنيات متخصصة، وغير مألوفة، وتتميز هذه الهجمات بضرورة توافر قدرات فنية وتقنية متطورة للمهاجم، وقدرتها علي استغلال واستهداف نقاط الضعف الموجودة بالأنظمة التكنولوجية، ومن ثم صعوبة التعامل معها أو مواجهتها، وكذلك تأثيراتها الجسيمة علي الدولة بأسرها في حالة ما إذا كان القطاع المستهدف يتسم بقدر من الأهمية والحساسية، أو كان المهاجم يتسم بقدر كبيرة من العدائية([2])، وتتمثل الطائفة الثانية في الهجمات غير الموجهة أو غير المستهدفة وهي تلك الهجمات التى لا تستهدف جهة أو قطاع بعينه، بل تستهدف الإضرار بنظام تكنولوجيا المعلومات أو أنظمة تكنولوجيا التشغيل، وعادة ما تتم عن طريق رسائل البريد الإلكتروني([3]).

وفى ذات الإطار، تأخذ الوسائل والأساليب المستخدمة في تنفيذ الهجمات السيبرانية، أحد شكلين وهما أولاً استهداف البيانات المخزنة عبر أجهزة الحاسوب والشبكات المرتبطة بها

---

[2]) US Army Training & Doctrine Command, DCSINT Handbook No. 1.02, Critical Infrastructure Threats and Terrorism: Cyber Operations and Cyber Terrorism Handbook, 2006, at VII-2

[3]) Joe Franscella, "Targeted Attack Vs. Untargeted Attack", The Anomali Blog, Available at: https://www.anomali.com/blog/targeted-attack-vs-untargeted-attack-knowing-the-difference.

[4]) Pierre Jeanne and Olivier Jamart, "Report on Cyber Threats to Operational Technologies in the Energy Sector", GE Steam Power & Thales, 2020. P.18, Available at: https://www.ge.com/content/dam/gepower-new/global/en_US/downloads/steam-new-site/services/automation-controls/ge-thales-cybersecurity-report-2020.pdf.

بغرض سرقتها أو تخزينها وإتلافها، أما الشكل الآخر فهو استهداف أنظمة التحكم في البني التحتية الحيوية كشبكات الكهرباء والمياه وأنظمة النقل والمنشأت الطبية والمالية، وينتج عنها آثار كارثية تهدد أمن المجتمع الدولي أو الدولة محل الهجوم السيبراني، وبالتالي تأخذ الهجمات السيبرانية أساليب متنوعة لتنفيذها، وتستخدم وسائل مختلفة علي النحو التالي:-

أولاً:- هجمات الحرمان من الخدمة وتعطيلها:

تتنوع الأساليب التى تستخدم في تنفيذ هجمات الحرمان من الخدمة وتعطيلها لتشمل بصفة خاصة، الأساليب والوسائل التالية:

١- هجمات الحرمان من الخدمة الموزع (DDOS).

يقوم المهاجم في هذا النمط من الهجمات بإستخدام برامج خبيثة أو فيروسات تسمي (Bots) لاختراق المئات أو الآلاف من أجهزة الحاسوب وربطها ببعضها البعض([١])، ثم يقوم بعد ذلك بتسجيل الدخول فى ذات الوقت على الموقع المستهدف عبر هذا العدد الهائل من أجهزة الحاسوب المخترقة، مما يتسبب في حدوث خلل كبير في الموقع المستهدف جراء هذا الدخول المكثف للموقع، وهو ما يؤدي إلي تعطيل عمل الموقع تماماً وإيقافه مؤقتاً([٢])، وتعد الهجمات السيبرانية على إستونيا عام ٢٠٠٧ المثال الأبرز الذى تم فيه استخدام هذا النمط من الهجمات علي مواقع المؤسسات الحكومية والمالية والإعلامية لإستونيا([٣]).

٢- هجمات الحرمان من الخدمة (DOS) .

وهو أحد أنواع الهجوم السيبراني الموجه للشركات بشكل أساسي، إذ يستهدف المتسللون مهاجمة الأنظمة والخوادم والشبكات وذلك من خلال غمرها بالبيانات والحركات بهدف تشتيتها،

---

[١]) د. سلوي يوسف الاكيابي، مدي انطباق القانون الدولي الإنساني علي الهجمات السيبرانية، مرجع سابق، ص ١٣٤٣.

[٢]) د. رغدة البهي، الحرب السيبرانية وتحديات الدفاع الجوي، مجلة السياسة الدولية، المجلد (٥٩)، العدد (٢٣٥)، يناير ٢٠٢٤، ص٢٩٤- ٢٩٥.

[3]) Peter Margulies, " Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility ", Melbourne Journal of International Law, Vol.14, 2013, P 6.

واستنفاذ مواردها، بما يحول دون قدرتها علي تلبية الطلبات الواردة إليها، مما يؤدي إلي غلق الموقع الإلكتروني الذي يستضيفه أو إبطائه([1]). وبالتالي يقوم المهاجم في هذا النمط من الهجمات بإغراق الموقع المستهدف بعدد هائل من البيانات والطلبات التى لا قيمة لها، مما يؤدي إلي حدوث بطء شديد للموقع أو تعطيله لأيام في بعض الأوقات، ويحرم المستخدمين من الخدمة أو الوصول إلي الموقع، بالإضافة إلي الخسائر التى تتكبدها المؤسسة صاحبة الخدمة، ومع إستخدام المهاجم تقنيات الإخفاء مع كثافة الهجمات، فإنه من الصعب معرفة هوية ومصدر هذه الهجمات([2]).

٣- استخدام برامج قنابل البريد الإلكتروني:

يقوم المهاجم في هذا النمط من الهجمات بإستخدام رسائل البريد الإلكتروني الهائلة لجعل الخوادم المستهدفة مكتظة، علي الرغم من أن البريد الإلكتروني ذاته ليس ضاراً، إلا أن أنظمة الاتصال القائمة علي الحاسوب قد لا تعمل بشكل صحيح عند اقتحامها من قبل أعداد كبيرة من رسائل البريد الإلكتروني([3]). ويعرف كذلك بإسم هجوم التنصت أو التجسس علي ما تحتوية المراسلات الإلكترونية من بيانات ومعلومات، ويتمكن من خلاله المهاجم من التنصت علي المراسلات الإلكترونية بين المستخدمين، بحيث يمكنه ذلك سرقة البيانات والمعلومات، والتلاعب بها([4]).

---

[4]) "What is a denial of service attack (DOS)?", Paloalto networks, Available at: https://www.paloaltonetworks.com /cyberpedia/what-is-a-denial-of-service-attack-dos.

[1]) د. شريف نسيم قلته بخيت،الهجمات الإلكترونية وحق الدفاع الشرعي للدول في القانون الدولي، مرجع سابق،ص ٢١.

[2]) د.هالة أحمد الرشيدي، الإرهاب السيبراني، ماهيته وجهود مكافحته في ضوء التشريعات والقوانين الوطنية والدولية، مرجع سابق، ص ٧٠.

[3]) Andrew Magnusson, "Man-in-the-Middle (MITM) Attack: Definition, Examples & More", Strongdm, 12 February 2023, Available at:https://www.strongdm.com/blog/man-in-the-middle-attack.

ثانياً:- هجمات اختراق المواقع وتدميرها:

تتنوع الأساليب التى تستخدم في تنفيذ هجمات اختراق المواقع الإلكترونية أو تدميرها لتشمل بعض الأساليب والوسائل التالية:-

١- استخدام البرمجيات الخبيثة وفيروسات الكمبيوتر وشبكة الإنترنت:

تعد الأكثر شيوعاً بين كافة أنواع الهجمات السيبرانية، وهي عبارة عن مجموعة من البرامج الضارة، تضم الفيروسات المتنقلة وبرامج التجسس، وبرامج الفدية، وبرامج الإعلانات المتسللة، وتقوم هذه البرامج بإختراق شبكات الإتصالات والمعلومات عبر ثغرات أمنية عند قيام المستخدم بالنقر علي رابط خطر أو تحميل ملفات مرفقة في بريد إلكتروني أو عند استخدام ناقل بيانات مصاب([١]).

وفى هذا النوع من الهجوم السيبراني يقوم المهاجمون باختراق شبكات التشغيل وتعطيلها أو إحداث شلل بها لفترة زمنية معينة، ثم المطالبة بالحصول علي فدية أو أموال مقابل إعادة تشغيل هذه الشبكات([٢])، وهذا النمط هو الشائع في الوقت الحالي نظراً للتطورات التكنولوجية الهائلة وخاصة مع انتشار العملات الإلكترونية التى لا يمكن تتبع مسارها([٣])، ففي عام ٢٠١٧ أثر هجوم الفدية علي مئات الآلاف من أجهزة الحاسوب حول العالم، وكان من تصميم وتنفيذ قراصنة من كوريا الشمالية، وتأثرت به بصفة خاصة المؤسسات الصحية في بريطانيا، حيث استغل الفيروس ثغرة في بعض أنظمة التشغيل وسمح للمهاجم بالتحكم بالأجهزة المخترقة،

---

[٤]) د. أحمد زكريا الباسوسي، الجهود الدولية لمكافحة الهجمات السيبرانية علي قطاع الطاقة: حالات مختارة، مجلة كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، المجلد (٢٤)، العدد (٤) أكتوبر ٢٠٢٣، ص١٥٦.

[٥]) د. إيمان أحمد علام، الهجمات السيبرانية "الحرب الإلكترونية" واستخدام القوة المسلحة في القانون الدولي العام: الاستغلال السيبراني، مجلة الدراسات القانونية والاقتصادية، كلية الحقوق جامعة مدينة السادات، المجلد (٩)، العدد (٤)، ديسمبر ٢٠٢٣،ص٤٥٥.

[١]) د. سلوي يوسف الاكيابي، مدي انطباق القانون الدولي الإنساني علي الهجمات السيبرانية، مرجع سابق، ص ١٣٣٨.

وتشفير الملفات المخزنة عليها، ثم طلب دفع فدية كشرط لإزالة التشفير، وإعادة الملفات مرة أخري قابلة للاستخدام([1]).

٢- استخدام برامج الدودة([2]):

يقوم المهاجم في هذا النمط من الهجمات بإستغلال أية فجوات في نظم تشغيل الحاسب، وتنتقل هذه البرامج من حاسب إلي آخر، لتغطي شبكة بأكلمها، وتحدث آثاراً تخريبية للملفات والبرامج ونظم التشغيل وبروتوكولات الاتصال([3]). كما يقوم المهاجم بإستغلال وجود ثغرة أمنية في الشبكة أو التطبيق، قبل أن يستطيع المطورون التعامل معها أو حلها، وهو ما يجعل عملية سرقة هويات المستخدمين أمر وارد، ويجعلهم ضحايا محتملين لأشكال متعددة من الجرائم ذات الطبيعة السيبرانية([4]).

٣- هجمات التصيد الاحتيالي:

يقوم المهاجم بانتحال صفة جهة موثوق منها، ثم يقوم بإرسال رسائل بريدية مزيفة للضحية، وفور فتح الرسالة والنقر علي الرابط الضار المرفق، يتمكن المتسلل من الوصول إلي المعلومات السرية، والبيانات الخاصة بالحساب، إضافة إلي إمكانية تثبيت برامج ضارة علي شبكة الاتصالات والمعلومات([5]).

---

[2]) D. TRENIN, Information is a Potent Weapon in the New Cold War, the Guardian (Sept. 17, 2016), available at: https://perma.cc/QPT4-4B8T. 15/2/2020.

[3]) د. سلوي يوسف الاكيابي، مدي انطباق القانون الدولي الإنساني علي الهجمات السيبرانية، مرجع سابق، ص ١٣٤٠.

[4]) د. وسام محمود عرفان مصطفي، سبل مكافحة الهجمات السيبرانية دولياً، مرجع سابق، ص٢٩٩١-٢٩٩٢.

[5]) طلال ياسين العيسي، عدى محمد عناب،المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مرجع سابق، ص٨٦.

[6]) Shruti M., 10 Types of cyber-attacks you should be aware in 2023, 8 February 2023, Available at: https://www.simplilearn.com/tutorials/cyber-security-tutorial/types-of-cyber-attacks

وقد يتم الهجوم السيبراني بهدف سياسي، حيث يقوم فيه مهاجمون لهم أغراض سياسية محددة (دول أو جماعات أو أفراد يعملون لحساب وتوجيهات من مسئولين في دول) بالضغط علي دول أخري لتحقيق مصالح بلادهم، كما قد يتم الهجوم السيبراني بهدف التجسس، حيث يقوم فيه المهاجمون باختراق أنظمة الحاسوب بغرض الحصول علي معلومات والتجسس علي الخصوم السياسيين([1]).

المطلب الثالث

تهديدات الهجمات السيبرانية ومخاطرها

أدى التطور السريع في مجال تقنية المعلومات والاتصالات وشبكات الإنترنت إلي ظهور أنماط جديدة من الجرائم جاءت عن طريق الاستغلال السيئ للتكنولوجيا، مما ترتب عليه خلق ظاهرة إجرامية جديدة تتم بواسطة هجمات سيبرانية واختراقات وتسلل داخل النظم المعلوماتية إما بهدف تدمير تلك النظم أو الحصول علي معلومات سرية سواء عسكرية أو اقتصادية، الأمر الذى ينذر بوجود مخاطر علي الصعيد الدولي والإقليمي، وضروة إيجاد سبل للتصدي لهذه الظاهرة، حيث تتسم الهجمات السيبرانية بطابع سرية الهوية وعدم ترك سوى القليل من الاثر، إضافة إلي ذلك لا تقف أمام الهجمات السيبرانية أى قيود إقليمية أو زمنية، وقد تسبب أضراراً فورية لعدد لا يحصي من الضحايا([2]).

والواضح، أنه من التحديات الكبري التى تواجه المجتمع الدولي، هو استخدام تكنولوجيا المعلومات لأغراض عسكرية ليس من قبل الدول فقط، بل من كيانات من غير الدول، بقصد إلحاق الأضرار الجسيمة بالبني التحتية لحياة الإنسان،مما يجعل أى تنظيم دولي لهذه المسألة قاصراً، وتتطلب تضافر جهود دولية تشارك فيها الدول والمنظمات الدولية لتنظيم مسألة

---

[1]) د. أحمد زكريا الباسوسي، الجهود الدولية لمكافحة الهجمات السيبرانية علي قطاع الطاقة: حالات مختارة، مرجع سابق، ص١٦٨.

[2]) د. وفاء لطفي، الجهود الدولية في مجال مكافحة جرائم الارهاب السيبراني: التجربة الماليزية نموذجا، مجلة كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، المجلد الثالث والعشرون، العدد الأول، يناير ٢٠٢٢، ص ١٦٣.

استخدام تكنولوجيا المعلومات في المجال العسكري والأمني، وبالتالي تصنف الهجمات السيبرانية ضمن أبرز المخاطر التى تحيط بالدول، حيث زادت حجم الهجمات السيبرانية بين الدول في الفترة الحالية، لذلك قامت الدول بتخصيص وحدات إلكترونية خاصة بالأمن السيبراني وزادت من حجم صلاحيتها.

وفى هذا الإطار، تعد الهجمات السيبرانية من أبرز معالم الصراعات السياسية والتجارية بين الدول، والتى تستهدف البني التحتية أو المنشآت والمؤسسات الحكومية والشبكات المعلوماتية، وهي قادرة علي تعطيل تشغيل البنية التحتية الحيوية للدولة محل الهجوم، بهدف تحقيق أضرار مادية في المعلومات المخزنة عليها والبني التحتية من خلال إستخدام الفضاء السيبراني وتنفيذ الهجمات داخله، والتى قد تصل إلي الموت أو التدمير الكامل للبني التحتية، وبالتالي فإن الهجوم السيبراني يقوم علي التسلسل ومن ثم السيطرة وأخيراً التحكم عن بعد لتتحول الأوامر الرقمية إلي نشاط مادى لغرض التعطيل أو التدمير في الأهداف أو الأعيان المدنية المستهدفة من الهجوم بشرط أن تكون محمية بواسطة برنامج الكتروني([1]).

وفي الإطار ذاته، تتمثل أهم مخاطر الهجمات السيبرانية، في تهديد البني التحتية الحيوية للدولة ضحية الهجوم السيبراني، حيث تنفذ الهجمات السيبرانية من خلال مجموعة من الإجراءات تتخذها الدولة للهجوم علي نظم المعلومات المعادية بهدف التأثير والإضرار بها، أو للدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة، ومن الآثار الناجمة عن الهجمات السيبرانية، التحكم في أنظمة تشغيل مؤسسات الدولة الحيوية، أو البني التحتية لها أو تدميرها أو تعطيلها، ومن ذلك تعطيل أو إتلاف النظم السيبرانية الخاصة بتشغيل أجهزة مؤسسات صحية مما يتسبب في حدوث وفيات أو تفاقم في درجة الإصابات، أو تعطيل أو إتلاف نظم إدارة شبكات توزيع الكهرباء أو محطات تنقية مياة الشرب، بحيث تتكبد الدولة المستهدفة

[1]) د. أحمد عبيس نعمة الفتلاوي، د. أزهر عبد الأمير الفتلاوي، المسؤولية الناشئة عن إستخدام وسائل القتال الفتاكة في نشر الأوبئة (الهجمات السيبرانية في مقابل جائحة كورونا أنموذجا)، مرجع سابق، ص٦١.

خسائر فادحة في الأوراح أو الممتلكات([1]). كما تتسبب الهجمات السيبرانية في تعطيل عمل المؤسسات الحيوية للدولة محل الهجوم، بما في ذلك المنشآت العسكرية والأمنية، ووفقاً لتقرير وكالة الأمن السيبراني وأمن البنية التحتية الأمريكية فإن هدف الهجمات السيبرانية إضعاف أو تعطيل أو تدمير البني التحتية لدولة أخري، والمثال علي ذلك عطل هجوم سيبراني عام ٢٠١٩ عمليات منشأة لخفر السواحل الأمريكية لمدة ٣٠ ساعة([2]).

كما أكد تقرير المخاطر العالمية الصادر عن المنتدي الاقتصادي العالمي عام ٢٠١٩، عن مخاطر عميقة للهجمات السيبرانية، حيث أنها لها صلة وثيقة بانهيار البنية التحتية للمعلومات الهامة، وتهدف إلي إلحاق أضرار بشرية أو مادية واسعة النطاق. وقد تتعدد طرق الهجمات السيبرانية ومنها استخدام البرامج التخريبية الخبيثة (فيروسات) والبرامج، وحجب الخدمات وغيرها([3]).

وكذلك من مخاطر الهجمات السيبرانية، المخاطر الإقتصادية حيث تشكل الهجمات السيبرانية وخاصة برامج الفدية، خطرا هائلاً علي الأمن القومي للدول، حيث يقوم المتسللون باختراق أنظمة الحاسوب عن بعد ويطلبون فدية مقابل استعادة البيانات أو عدم كشفها، مما يؤدي إلي عواقب إقتصادية جسيمة، حيث تتعرض الشركات الخاصة لخسائر تقدر بملايين الدولارات كل عام جراء الهجمات السيبرانية، وأيضا قد تتتسبب الهجمات السيبرانية في مخاطر علي الصحة العامة، حيث تعد المنشآت الطبية من مستشفيات ومراكز طبية، هدفاً للهجمات السيبرانية، ففي عام ٢٠٢٠ تعرضت ٥٦٠ منشأة رعاية طبية لهجمات سيبرانية في الولايات المتحدة، ونتج عنها خسائر مادية قدرت بملايين الدولارات ، كما أدت إلي تأخر علاج المرضي وموت

---

[2]) د. ياسر إسماعيل الدفراوي، دور القانون الدولي في ضبط استخدام التكنولوجيا في الفضاء الخارجي، مجلة الشريعة والقانون بالقاهرة، جامعة الأزهر، المجلد (٤٢)، العدد (٤٢)، أكتوبر ٢٠٢٣، ص١٥٢٤.

[3]) د. رغدة البهي، الحرب السيبرانية وتحديات الدفاع الجوي، مرجع سابق، ص٢٩٤.

[4]) د. وفاء لطفي، الجهود الدولية في مجال مكافحة جرائم الارهاب السيبراني: التجربة الماليزية نموذجا، مرجع سابق، ص ١٦٢.

البعض الآخر([1]).وتشمل صور مخاطر الهجمات السيبرانية علي أمن واستقرار الدول ومواطنيها، علي سبيل المثال، ما يلي:-

* التسلل إلي الأنظمة الأمنية للدولة محل الهجوم وشلها وتعطيل أنظمة الاتصال بين القيادة والوحدات المركزية أو بين الأجهزة السيادية بالدولة وبعضها البعض.

* اختراق منظومة الأسلحة الاستراتيجة ونظم الدفاع الجوي الخاصة بالدولة محل الهجوم، وفك شفرات التحكم بتشغيل منصات إطلاق الصواريخ والأسلحة النووية وغيرها من الأسلحة الفتاكة([2]).

* استهداف محطات توليد الكهرباء والمياه، وشل نظم الحواسيب والشبكات المعلوماتية المنوط بها التحكم في شبكات توزيع الكهرباء والمياه بالدولة محل الهجوم، الأمر الذى ينتج عنه تعطيل العديد من المرافق الحيوية، وشل الحركة في كافة أنحاء الدولة المستهدفة.

* تعطيل أنظمة التحكم بخطوط الملاحة الجوية والبحرية والبرية وإحداث خلل ببرامج هبوط الطائرات وإقلاعها أو حدوث تصادم بين القطارات وما يستتبعه ذلك من آثار بالغة وخسائر جسيمة بالأوراح والممتلكات.

* إحداث خلل واسع في نظم الشبكات التى تتحكم في النظام المصرفي والبورصة للدولة محل الهجوم، وما يستتبعه ذلك من تعطيل التجارة الدولية والحركة الإقتصادية بالدولة المستهدفة.

* مهاجمة شبكات المعلومات الطبية واختراقها والتلاعب بها، لإعطاء المرضي أدوية مميتة مثلا أو التلاعب في نسب الأدوية المقررة لهم، وما يستتبعه ذلك من خسائر في أرواح المدنيين([3]).

---

[1]) د.إسراء أحمد إسماعيل، الحروب السيبرانية.. تهديد لأمن الدول بدون اشتباكات عسكرية، مجلة السياسة الدولية، ملحق تحولات استراتيجية، التكنولوجيا وتحولات الحروب، المجلد ٥٧، العدد ٢٢٨، أبريل ٢٠٢٢، ص١٠.

[2]) د. رغدة البهي، الحرب السيبرانية وتحديات الدفاع الجوي، مرجع سابق، ص٢٩٥.

[3]) د.هالة أحمد الرشيدي، الإرهاب السيبراني، ماهيته وجهود مكافحته في ضوء التشريعات والقوانين الوطنية والدولية،مرجع سابق، ص٣٧.

وقد يكون من اللازم، ونحن بصدد الحديث عن مخاطر الهجمات السيبرانية، أن نلقي الضوء علي بعض الهجمات السيبرانية التى حدثت في مختلف أنحاء العالم، وذلك علي النحو التالي:-

١- **الهجمات الروسية علي دولة إستونيا عام ٢٠١٧:** حيث وجهت روسيا الاتحاديه هجوماً سيبرانياً استهدف تعطيل شبكات الاتصالات الالكترونية في إستونيا وكانت المواقع الرسمية الحساسة هى الأكثر استهدافاً مثل موقع رئيس الوزراء ورئيس البرلمان فضلاً عن تعطيل بعض الخدمات الضرورية كالإطفاء والإسعاف([1]). وقد تم توجيه اتهامات للحكومة الروسية بإعتبارها مسئولة عن هذا الهجوم، إلا أن إستونيا لم توجه اتهام رسمي حتى الآن لروسيا بسبب عدم قدرتها علي توفير دلائل إسناد كافية وقانونية علي خلفية تحديات الإسناد المتعلقة بتحديد هوية أو مكان القائم بالهجوم والتى هى من خصائص الهجمات السيبرانية([2]).

٢- **الهجمات السيبرانية الروسية علي جورجيا عام ٢٠٠٨:** وذلك بالتزامن مع شن عملبات عسكرية تقليدية في النزاع المسلح بين روسيا وجورجيا، مع شن روسيا هجوم سيبراني علي دولة جورجيا استهدف البني التحتية المرتبطة بشبكة الإنترنت واستهدفت البني التحتية المهمة للإتصالات والمعلومات([3]). كما تمكنت من الاستيلاء علي (٥٤) موقع إخباري لجورجيا وموقع رسمي لوزارة الدفاع وموقع مالي لأحد البنوك، كما قامت بقطع خدمة الإنترنت عن جورجيا لمدة ست ساعات، مما تسبب في توقف نسبة ٣٥٪ من المؤسسات الحيوية بجورجيا المعتمدة علي شبكات الإتصالات والمعلومات، ومنها البنك الوطني الذى

---

[1] Scott J. Shackelford, From Nuclear War to Net War: Analogizing Cyber Attacks in International Law, Berkeley Journal of International Law, 2009, Vol. 27, Issue 1, p193.

[2] د. شريف نسيم قلته بخيت، الهجمات الإلكترونية وحق الدفاع الشرعي للدول في القانون الدولي، مرجع سابق، ص٣.

[3] د. حسام عبد الأمير خلف، البعد الجديد – الخامس– في النزاعات المسلحة – الفضاء الالكتروني، مجلة كلية الحقوق، جامعة النهرين، العدد الأول، يناير، ٢٠١٦، ص١٢٦.

اضطر إلي وقف جميع خدمات الإلكترونية في الفترة من ٨ إلي ١٩ أغسطس، كما قام موقع الكتروني روسي بتحميل قائمة بأنظمة جورجيا الالكترونية المستهدفة وكذلك البرامج التى يمكن من خلالها اختراق هذه الأنظمة، وأتاح الوصول إلي هذا القائمة والبرامج، لأى شخص مهتم بالمشاركة في الهجوم، وبالفعل اشترك الآلاف من الروس في هذا الهجوم([1]).

٣- **الهجوم السيبراني الذي قامت به إسرائيل عام ٢٠٠٧ ضد سوريا:** والذى نتج عنه توقف أجهزة الرادار وباقي منظومات الاتصال في المطارات العسكرية والمدنية عن العمل، في أثناء الهجوم الذي نفذه سلاح الجو التابع لها علي مواقع سورية زعمت إسرائيل أنها منشآت لمفاعل نووي([2]).

٤- **الهجمات السيبرانية الأمريكية علي إيران:** ففي عام ٢٠١٠ تم شن هجوم سيبراني علي المرافق النووية الأيرانية، حيث تعرضت إليه محطة نطنز النووية الإيرانية لهجوم سيبراني بإستخدام برنامجاً ويدعي ستوكسنت "Stuxnet"([3])واستمر لمدة تسعة أشهر وإستهدف نظم التحكم الإشرافي والحصول علي البيانات والسيطرة الالكترونية المختصة بتشغيل أجهزة الطرد المركزي التى تعمل علي تخصيب اليورانيوم مما أدى إلي إتلاف ألف جهاز طرد مركزي واستبعادها من الخدمة، وهو ما يمكن معه إعتبار هذا الهجوم سابقة في

---

[4]) د. محمد عادل محمد عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق علي ممارسة التجسس وقت السلم: دراسة علي ضوء دليل "تالين" بشأن القانون الدولي المطبق علي العمليات السيبرانية ٢٠١٣-٢٠١٧، مرجع سابق، ص ٢٦٣.

[1]) د. أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مرجع سابق، ص٦١٩.

[2]) د. سلوي يوسف الاكيابي، مدي انطباق القانون الدولي الإنساني علي الهجمات السيبرانية، مرجع سابق، ص ١٢٧١.

مجال الهجمات السيبرانية([١]). وتكررت الهجمات مرة أخري في فبراير ٢٠٢٠، والذى أدى إلي إنقطاع الانترنت بنسة ٧٥٪ فى عموم إيران وتعطيل شبكات الاتصالات الإيرانية عدة ساعات وحجب شبكة الانترنت لتتمكن إيران من صد الهجمات السيبرانية والحفاظ علي أمن البنية التحتية([٢]). وفي أبريل ٢٠٢١ أعلنت السلطات الإيرانية عن تعرض شبكة الطاقة الكهربائية بمنشأة ناتنز النووية لهجوم سيبراني أدى إلي شلل جزئي، كما تكررت الهجمات مرة أخري في أكتوبر ٢٠٢٢، عندما أعلنت منظمة الطاقة الذرية الإيرانية عن تعرضها لهجوم سيبراني وذلك باختراق خادم البريد الإلكتروني بمنشأة بوشهر للطاقة النووية([٣]).

٥- **الهجمات السيبرانية بين الولايات المتحدة الأمريكية وروسيا:** ففى عام ٢٠١٦ زعمت وكالة الاستخبارات المركزية الأمريكية أن موسكو أثرت بشكل مباشر في نتيجة الانتخابات الرئاسية لعام ٢٠١٦، وذلك من خلال قيام روسيا بالهجوم السيبراني للتلاعب بنتائج الانتخابات الأمريكية، حيث أعلنت المخابرات الأمريكية بأنها علي ثقة بأن الحكومة الروسية متورطة في هذا الاختراق، بهدف التأثير علي نتائج الانتخابات لصالح "دونالد ترامب" وأن عملاء روس قاموا بإختراق أنظمة المعلومات والإتصالات التابعة للجنة الوطنية الديمقراطية، وحصلوا علي كل تقاريرها، وتسريب ٦٠ ألف رسالة بريد إلكتروني من الحساب الخاص لمدير حملة المرشحة الديمقراطية المنافسة له (هيلارى كلينتون)، وتم التلاعب بالمعلومات والبيانات الخاصة باللجنة لصالح دونالد ترامب"([٤]).وكذلك تعرض

---

[3] Micheal Gervais,"Cyber Attacks and the Laws of War", Berkeley Journal of International Law", Vol: 30, Issue .2, Article 6, 2012, p.46.

[٤] د. أحمد عبيس نعمة الفتلاوي، د. أزهر عبد الأمير الفتلاوي، المسؤولية الناشئة عن إستخدام وسائل القتال الفتاكة في نشر الأوبئة (الهجمات السيبرانية في مقابل جائحة كورونا أنموذجا)، مرجع سابق،ص٦٥.

[5] Apurva Venkat, "Iran's nuclear energy agency confirms email server hacked", 24 October 2023, available at: https://www.csoonline.com/article/3677849/irans-unclear-energy-agency-confirms-email-server-hacked.html.

[١] د.إسراء أحمد إسماعيل، الحروب السيبرانية.. تهديد لأمن الدول بدون اشتباكات عسكرية، مرجع

خط أنابيب كولونيال الأمريكي في ٧ مايو ٢٠٢١ لهجوم سيبراني وهو أكبر خط من قبل مجموعة إجرامية تقيم داخل الحدود الروسية تحمل الاسم الرمزى "دارك سايد"، وذلك عن طريق برامج الفدية، حيث قام المهاجمون بسرقة ما يقارب ١٠٠ جيجا من البيانات قبل إغلاق أجهزة الكمبيوتر، وطلب الفدية التى قدرت ما يقارب ٤,٤ مليون دولاء بالعملة الرقمية (بيتكوين)، وفي ١٣ مايو ٢٠٢١ قامت شركة كولونيال بدفع الفدية للمهاجمين مما أدي إلي إعادة تشغيل الخط مرة أخري([1]).كما نفذت الولايات المتحدة الأمريكية العديد من الهجمات السيبرانية ضد روسيا، وفي المقابل قامت روسيا بتوجيه عدة هجمات سيبرانية علي وزارة الدفاع الأمريكية وغيرها من الوزارات والمصالح الأمريكية، ونتج عنها خسائر جسيمة للولايات المتحدة الأمريكية، كما تم توزيع برامج خبيثة لعرقلة شبكة الكهرباء الأمريكية، واستهدفت هذه البرامج شبكات الحاسوب والبنية التحتية والبنوك والقوات العسكرية الأمريكية والتى نتج عنها إصابات وخسائر في الأرواح والممتلكات([2]).

٦- **الهجمات السيبرانية الروسية الموجهة ضد أوكرانيا:**حيث شهدت الفترة ما بعد عام ٢٠١٤ وتحديداً بعد ضم روسيا لجزيرة القرم كثافة شديدة للهجمات السيبرانية الروسية الموجهة ضد أوكرانيا، وخصوصاً ضد قطاع الطاقة الأوكراني([3])، ومن أمثلة ذلك الهجوم السيبراني الذى وقع خلال عامي ٢٠١٥-٢٠١٦ والذى استهدف شبكة الكهرباء الأوكرانية

سابق، ص١١.

[2]) William Turton and Kartikay Mehrotra, "Hackers Breached Colonial Pipeline Using Compromised Password", Bloomberg, 4 June 2021, Available at: https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password?leadSource=uverify%20wall.

[3]) James Andrew Lewis: Aux Armes, Citoyens: Cyber Security and Regulation in the United States (pre-print version of article published in Elsevier's Telecommunications Policy, fall 2005, p. 8.

[4]) د. سلوي يوسف الاكيابي، مدي انطباق القانون الدولي الإنساني علي الهجمات السيبرانية، مرجع سابق، ص١٢٦٩.

مما تسبب في إنقطاع التيار الكهربائى عن مائتي ألف عميل، كما زادت حده تلك الهجمات بعد الغزو الروسي لأوكرانيا مع بدايات عام ٢٠٢٢، وكانت أغلب الهجمات السيبرانية الروسية ضد أوكرانيا علي شبكات الكهرباء، وذلك بهدف شل حركة الدولة وإظهار فشل الحكومة الأوكرانية وأنها غير قادرة علي مواجهة التهديدات الخارجية([1]).

المبحث الأول

التكييف القانوني للهجمات السيبرانية

تمثل الهجمات السيبرانية إحدى التحديات الراهنة لسيادة الدول، والتى سارعت الدول إلي إستغلالها لمصلحتها والقيام بتطوير قدراتها الهجومية والدفاعية بإعتبارها صورة جديدة من صور سباقات التسلح([2]).

ومن الجدير بالذكر، أن المادة (٣٦) من البروتوكول الإضافي الأول لإتفاقيات جنيف لعام ١٩٧٧، توقعت حدوث تطورات مستقبلية في وسائل وأساليب الحرب "الأسلحة الجديدة"، وذلك بالنص أنه علي الأطراف المتحاربة التحقق مما إذا كانت هذه التطورات محظورة بمقتضي البروتوكول، أم بموجب قواعد القانون الدولي، ومن ثم فهل تدخل الهجمات السيبرانية ضمن فئة الأسلحة الجديدة، رغم عدم النص عليها بشكل صريح، وتضمن مبدأ شرط مارتنز، بإعتباره المبدأ الذي يعالج القضايا الدولية المستحدثة وغير المنظمة صراحة وفقاً لأحكام القانون الدولي العام، النص علي أن:" يظل السكان المدنيون والمقاتلون تحت حماية وسلطان مبادئ قانون الأمم الناتجة عن العادات والتقاليد الراسخة بين الشعوب المتحضرة وقوانين الإنسانية، وما يميلة الضمير العام". وأكد بعض الفقة الدولي بأن مبدأ شرط مارتنز يعد الأنسب للتطبيق علي

---

[1]) د. أحمد زكريا الباسوسي، الجهود الدولية لمكافحة الهجمات السيبرانية علي قطاع الطاقة: حالات مختارة، مرجع سابق، ص١٦٧.

[2]) د. أميرة عبد العظيم محمد عبد الجواد، الدفاع الشرعي وإشكاليات الرد علي الهجمات السيبرانية في ضوء ميثاق الأمم المتحدة، مجلة روح القوانين، كلية الحقوق جامعة طنطا، المجلد (٣٥)، العدد (١٠٢)، عدد خاص– المؤتمر العلمي الدولي الثامن – التكنولوجيا والقانون– مايو ٢٠٢٣، ص٨٨٥.

الهجمات السيبرانية، وذلك لكونه يشمل أوضاعاً غير منظمة في الاتفاقيات الدولية، ولا يكون ذلك ممكناً إلا باللجوء للقانون الدولي العرفي، وهو المصدر الذى أشارت إليه أحكام المادة (٣٨) من النظام الأساسي لمحكمة العدل الدولية([٣]).

والواضح أن ظهور تحدى الهجمات السيبرانية وتغيير شكل النزاع المسلح ومجاله وأشخاصه وآثاره، يثير الكثير من التساؤلات، عن مدى إعتبار الهجوم السيبراني إستخداماً للقوة؟وهل يشكل خرقاً لسيادة الدول؟ ومدى إنطباق أحكام ومبادئ القانون الدولي الإنساني علي الهجوم السيبراني، وهو ما سنحاول بيانه علي النحو التالي:-

المطلب الأول: تكييف الهجمات السيبرانية وفقاً لمبادئ الأمم المتحدة.

المطلب الثاني: تكييف الهجمات السيبرانية وفقاً لمبادئ القانون الدولي الإنساني.

المطلب الثالث: مدى إمكانية تطبيق قواعد القانون الدولي الحالية علي الهجمات السيبرانية.

المطلب الأول

تكييف الهجمات السيبرانية وفقاً لمبادئ الأمم المتحدة

إن تكييف الهجمات السيبرانية يشكل تحدياً كبيراً يواجه القانون الدولي المعاصر، وخصوصاً بعد تزايد إستخدام شبكة المعلومات والإتصالات في مختلف المجالات وتنوع أشكال التهديدات الناجمة عنها، حيث أكد ميثاق الأمم المتحدة علي ضرورة تسوية النزاعات الدولية بالطرق السلمية وحظر إستخدام القوة أو التهديد بإستخدامها في العلاقات الدولية.

وفى هذا الإطار، تمثل الهجمات السيبرانية تهديداً للمبادئ الأساسية في القانون الدولي التى تقوم علي مبدأ إحترام سيادة الدول، لما تمثله من اختراق للأمن السيبراني للدولة من خلال اختراق معلومات استراتيجية وأمنية وعسكرية ذات طبيعة سرية، كما تتعارض مع مبدأ حظر إستخدام القوة أو التهديد بإستخدامها في العلاقات الدولية، نظراً إلي أضرارها الجسيمة علي

---

[٣]) د. محمد ربيع أحمد حسين، الهجمات السيبرانية واستخدام القوة في القانون الدولي المعاصر، مجلة العلوم القانونية والاقتصادية، كلية الحقوق جامعة عين شمس، المجلد (٦٥)، العدد (١)، يناير ٢٠٢٣، ص ٣٠٣-٣٠٤.

سير الخدمات في الدولة التى تتعرض لهذه الهجمات، فالهجمات السيبرانية التى تتعرض لها الدولة تؤثر علي سيادتها وإستقلالها السياسي في إتخاذ القرارات ونطاقها، وهو ما سنحاول بيانه في التعرض لمبدأ السيادة ومبدأ حظر إستخدام القوة أو التهديد بإستخدامها في العلاقات الدولية، علي النحو التالي:

أولاً:مبدأ السيادة.

يعد مبدأ السيادة من المبادئ المعترف بها في ميثاق الأمم المتحدة والإتفاقيات الدولية ذات الصلة، وتضمنت الفقرة الأولي من المادة الثانية من ميثاق الأمم المتحدة النص علي هذا المبدأ وذلك بأن:" تقوم الهيئة علي مبدأ المساواة في السيادة بين جميع أعضائها"([1]).

وتعد الهجمات السيبرانية من التحديات الواضحة أمام مبدأ سيادة الدولة ونطاقه، فالتغييرات التكنولوجية الهائلة وتطورات إستخدام شبكات الإتصال والفضاء السيبراني، دفعت الأطراف الدولية إلي التنازع والتسابق علي إستغلاله لمصلحتها والقيام بتطوير قدراتها الهجومية والدفاعية بإعتباره شكل جديد من أشكال سباقات التسلح([2]).

وفى ظل وجود وسائل الإتصال الإلكترونية والتغيير التكنولوجي الهائل، فقد تغير المفهوم التقليدي للسيادة، وبدأت تتناقص سيادة الدولة التقليدية ومقوماتها التى تؤثر علي نطاق سيادة الدولة في الفضاء السيبراني، ولقد سارعت الدول إلي تطوير تشريعاتها الوطنية لإستيعاب الجرائم التى تحدث في نطاق إقليمها وذلك بالتنسيق مع الدول الأخرى عن طريق إبرام إتفاقيات منظمة للجرائم السيبرانية وحل مشكلة السيادة من خلال الإتفاق علي آليات تتبع مصادر الجريمة والقوانين واجبة التطبيق في حال وقوعها كالتوصية الصادرة من مجلس أوروبا بشأن المشاكل الإجرائية المتعلقة بتكنولوجيا المعلومات، واتفاقية بودابست لعام ٢٠٠١، وبروتوكول

---

[1]) د. أحمد عبيس نعمة الفتلاوي، زهراء عماد محمد كلنتر، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مرجع سابق،ص٥٧.

[2]) د. سراب ثامر أحمد، الهجمات علي شبكات الحاسوب في القانون الدولي الإنساني، أطروحه دكتوراه، كلية الحقوق جامعة النهرين، بغداد، العراق، ٢٠١٥، ص١٠١.

ستراسبورغ في ٢٨ يناير ٢٠٠٣ (البروتوكول الإضافي لاتفاقية الجريمة الإلكترونية) والإتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام ٢٠١٠([1]).

بالتالي فإن مبدأ السيادة الإقليمية للدولة ينطبق علي الفضاء السيبراني ويشمل البنية التحتية السيبرانية، فيحق للدولة أن تمارس الرقابة علي أنشطة البنية التحتية السيبرانية كنظم الحواسيب وشبكات الإتصال والمعلوماتية وقطاعات الطاقة والنقل في تلك المناطق، وتخضع ممارسة تلك السيادة لقواعد القانون الدولي، ويتعين علي الدول منع إستخدام البني التحتية السيبرانية – الواقعة في إقليمها أو التى تخضع لسيطرتها بشكل كامل– فى أنشطة تمس الحقوق السيادية للدول الأخري([2]).

وترتيباً علي ما تقدم، فإن الهجمات السيبرانية التى توجه من قبل دولة ضد البني التحتية السيبرانية التابعة لدولة أخري، يمكن أن تشكل خرقاً لسيادة دولة الإقليم وخصوصاً إذا تسببت تلك الهجمات في إحداث آثار مدمرة للدولة ضحية الهجوم السيبراني([3]).

ثانياً: مبدأ حظر إستخدام القوة أو التهديد بإستخدامها في العلاقات الدولية:

نصت الفقرة الرابعة من المادة الثانية من ميثاق الأمم المتحدة علي أنه:" يمتنع أعضاء الهيئة جميعاً في علاقاتهم الدولية عن التهديد باستخدام القوة أو استخدامها ضد سلامة الأراضي أو الإستقلال السياسي لأية دولة، أو علي أي وجه آخر لا يتفق ومقاصد الأمم المتحدة"([4]). ويرتبط هذا الحظر بقاعدة عدم التدخل في الشئون الداخلية للدول الأخري".

---

[1]) مصطفي عصام نعوس، سيادة الدولة في الفضاء الالكتروني، مجلة الشريعة والقانون، جامعة الإمارات العربية المتحدة – كلية القانون، المجلد (٢٦)، العدد (٥١)، يوليو ٢٠١٢، ص١٣٦-١٣٩.

[2]) د. أحمد عبيس نعمة الفتلاوي، زهراء عماد محمد كلنتر، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مرجع سابق،ص٥٨.

[3]) د. سراب ثامر أحمد، الهجمات علي شبكات الحاسوب في القانون الدولي الإنساني، مرجع سابق، ص١١٨.

وفي هذا الإطار، أكدت محكمة العدل الدولية في قضية الأنشطة العسكرية وشبه العسكرية (نيكاراغوا ضد الولايات المتحدة الأمريكية) لعام ١٩٨٦([١])"بأنه متى إتخذ التدخل شكل إستخدام أو التهديد بإستخدام القوة فإن قاعدة عدم التدخل الواردة في القانون الدولي تتطابق مع المادة (٤/٢) من ميثاق الأمم المتحدة"([٢]). فالهجمات السيبرانية عادة ما تستهدف استقرار الدول وأنظمتها السياسية، وقد تصل في حالة استخدام الهجمات السيبرانية إلي التهديد المباشر للسيادة والأمن الداخلي للدول، وذلك من خلال استهداف شبكات الاتصال الالكترونية، والبنى التحتية الضرورية لحياة المواطنين، كمحطات توليد الكهرباء، والبنى التحتية العسكرية أو المدنية([٣]).

بالتالي فإن حظر استخدام القوة الوارد في المادة (٤/٢) يخضع لإستثناءين وهما([٤]):-

---

[٤]) د. إيمان أحمد علام، الهجمات السيبرانية "الحرب الإلكترونية" واستخدام القوة المسلحة في القانون الدولي العام: الاستغلال السيبراني، مجلة الدراسات القانونية والاقتصادية، كلية الحقوق جامعة مدينة السادات، المجلد (٩)، العدد (٤)، ديسمبر ٢٠٢٣،ص٤٤٩.

[1]) Papastavridis, E. Judgment of the International Court of Justice in Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), 1986. In Latin America and the International Court of Justice, 2016, pp. 233-244.

[٢]) د. أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مرجع سابق،ص٦٢٩-٦٣٢.

[3]) Scoot J Shackleford," State Responsibility for Cyber Attacks: Competing Standards for Growing Problem", CCD COE Publications, C.Czosseck and K. Podins Eds, Tallinn, Estonia, 2010, pp.200-202.

[٤]) د. أحمد عبيس نعمة الفتلاوي، زهراء عماد محمد كلنتر، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مرجع سابق،ص٥٩.

١- السلم والأمن الدوليين وفقاً للمادة (٣٩) من الميثاق:- والتى تمنح مجلس الأمن السلطة في تحديد وجود أى تهديد أو خرق للسلم او عمل من أعمال العدوان، ومن ثم يتخذ الإجراءات اللازمة للحفاظ علي السلم والأمن الدوليين وإعادته إلي نصابه.

٢- حق الدفاع الشرعيوفقاً للمادة (٥١) من الميثاق والتى نصت علي أنه:" ليس فى هذا الميثاق ما ينقص أو يضعف من الحق الطبيعي للدول، بشكل فردى أو جماعي، في الدفاع عن النفس إذا أعتدت قوة مسلحة علي أحد أعضاء الأمم المتحدة، وذلك إلي أن يتخذ مجلس الأمن التدابير اللازمة لحفظ السلم والأمن الدوليين".

ووفقاً لهذه المادة يتطلب لإستخدام الدول حق الدفاع الشرعي أن تكون قد تعرضت لإعتداء مسلح، ومن ثم فإن الأشكال الأخري من إستخدام القوة التى لا تشكل هجوم مسلح لا تعطي الحق للدول في الدفاع الشرعي([٥]).

وفي ضوء هذه الإستثناءات، يتوقف جواز إستخدام القوة المسلحة علي وقوع العدوان، والذى يعني إستخدام القوة المسلحة بواسطة دولة ضد السيادة أو السلامة الإقليمية أو الإستقلال السياسي لدولة أخري أو بأي شكل آخر لا يتفق مع مبادئ الأمم المتحدة ذات الصلة.

وترتيباً علي ما تقدم، يثور التساؤل: هل تشكل الهجمات السيبرانية هجوماً مسلحاً أم شكل آخر من أشكال القوة؟ وهل تعرض دولة ما لهجوم سيبراني يمنحها الحق في الدفاع الشرعي؟ ومدى إمكانية ممارسة الدول حق الدفاع الشرعي عن النفس المنصوص عليه في المادة (٥١) من الميثاق رداً علي الهجمات السيبرانية: حيث برز أتجاهان فقهيان بشأن مدى إمكانية إدراج الهجمات السيبرانية ضمن نطاق المادة (٥١) ومدى تكييف الهجمات السيبرانية كهجمات مسلحة وفقاً للمادة (٥١) من الميثاق وذلك علي النحو التالي:-

الاتجاه الأول: وهذا الاتجاه مؤيد تماماً لإمكانية إدراج الهجمات السيبرانية ضمن نطاق المادة (٥١) من الميثاق وحق الدفاع الشرعي للدول في مواجهة الهجمات السيبرانية، واستند أنصار

---

[٥]) رزق أحمد سمودي، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام، مجلة جامعة الشارقة للعلوم القانونية، الإمارات العربية المتحدة، المجلد (١٥)، العدد (٢)، ديسمبر ٢٠١٨، ص٣٤٠.

هذا الاتجاه إلي الطبيعة المرنة والمتطورة للمادة (٥١) من الميثاق والقابلة لإعادة تفسير واسع ومقبول في مواجهة أية مستجدات أو تحديات دولية جديدة، والممارسة الدولية لهذا الحق بعد أحداث ١١ سبتمبر ٢٠٠١، حيث أصبح بإمكانية الدول التذرع بحق الدفاع الشرعي في مواجهة الهجمات السيبرانية سواء من قبل الدول أو الكيانات من غير الدول أو الجماعات الإرهابية([1]). كما أن التطور الهائل في صور وأشكال الهجمات السيبرانية وتأثيراتها، يتطلب إعادة صياغة مفهوم الهجوم المسلح، ويتخذ هذا الاتجاه وجهة النظر المؤيدة لإمكانية تكييف الهجوم السيبراني كهجوم مسلح، ويستند إلي أمرين:

١- الفتوى الصادرة من محكمة العدل الدولية والمتعلقة بمشروعية التهديد أو استخدام السلاح النووى، والتى أكدت علي الضرر وليس نوع السلاح المستخدم، استناداً إلي أن الميثاق حظر استخدام القوة دون أن يشير إلى نوع السلاح المستخدم، وبالتالي يمكن اعتبار الهجوم السيبراني المسلح كاستخدام للقوة، وحكم محكمة العدل الدولية فى قضية نيكاراجوا للتمييز بين الهجوم المسلح وغيره من إستخدام القوة، والذى أكد علي معيار الجسامة لتحديد نطاق الهجوم السيبراني بالتأثيرات والأضرار المادية الجسيمة التى يحدثها للدولة، أو المماثلة للأضرار التى يحدثها الهجوم العسكري التقليدي(تدمير منشآت، أو إصابة أو موت أشخاص).

٢- قرار مجلس الأمن الدولي بإعتبار هجمات ١١ سبتمبر ٢٠٠١ هجوم مسلح وفقاً للمادة (٥١) من الميثاق، وبالتالي فإن المعيار الرئيسي لتكييف الهجوم السيبراني كهجوم مسلح هو معيار الضرر الجسيم الناتج وليس نوع السلاح المستخدم أو طبيعة منفذه، كما أن هناك قيود تتعلق بإستخدام القوة بغرض الدفاع الشرعي ضد الهجمات السيبرانية، فإذا كان مصدر أومنفذ الهجوم معلوم علي الفور أو يعلن منفذ الهجوم مسئوليته عن الهجوم، فإنه

[1] Iréne Couzigou, "The Challenges Posed by Cyber Attacks to the Law on Self-Defence", ESIL Conference Paper Series. Vol. 4, No.16, European Society of International Law, 2014, p4-6.

يلزم مراعاة الضرورة والتناسب في إستخدام القوة فالغرض هو إيقاف الهجوم وليس الانتقام([1]).

وفى ذات الإطار، ذهب البعض إلي عرض نظريتين لتناول هذه المسألة علي النحو التالي:

الأولي: تبنت المفهوم الضيق للهجوم المسلح وفقاً للمادة (٥١) أى تضييق نطاق الهجوم المسلح على الضرر المادي الجسيم الناتج عن استخدام الأسلحة العسكرية التقليدية فقط، وبالتالي فإن الهجمات السيبرانية وفقاً لهذا المفهوم لا يمكن أن ترقي إلي مستوى الهجوم المسلح، وهذا الاتجاه محل انتقاد واسع لتجاهله الرأى الاستشاري لمحكمة العدل الدولية بشأن مشروعية استخدام السلاح النووى، وإجماع الفقه الدولي علي أن استخدام الأسلحة غير التقليدية يعد استخداماً للقوة، والعبرة بالتأثير والضرر وليس بنوع السلاح المستخدم([2]).

وتبنت النظرية الثانية المفهوم الواسع للهجوم المسلح وفقاً للمادة (٥١)، وبالتالي فإن تكييف الهجوم السيبراني كهجوم مسلح وفقا للمادة (٥١)، يكون بناء علي تأثيراته أو أضراره الجسيمة، وليس بنوع السلاح المستخدم، وأن حق الدفاع الشرعي في مواجهة الهجمات السيبرانية يكون النتيجة المباشرة لذلك الهجوم الذى تسبب في أضرار مادية جسيمة للدولة([3]).

بالتالي وفقاً لهذا الاتجاه، ينشأ حق الدفاع الشرعي للدول في مواجهة الهجمات السيبرانية في حالة واحدة فقط إذا تعرضت لهجوم مسلح ذات أضرار مادية جسيمة، أو مماثلة للأضرار التى يحدثها الهجوم العسكري التقليدي، حيث يتميز القانون الدولي بالمرونة والقدرة علي استيعاب

---

[1]) Marco Roscini, "World Wide Warfare – Jus ad bellum and the Use of Cyber Force", Max Planck Yearbook of United Nations Law, Vol. 14, 2010, p10.

[2]) د. سلوي يوسف الاكيابي، مدي انطباق القانون الدولي الإنساني علي الهجمات السيبرانية، مرجع سابق، ص ١٣٠٨.

[3]) Matthew C.Waxman, "Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions", International Law Studies, Vol. 89, 2013, p9.

أية ظواهر جديدة في العلاقات الدولية، وإمكانية تكييف الهجمات السيبرانية ذات الأضرار المادية الجسيمة كهجوم مسلح وفقاً للمادة (٥١) من الميثاق([1]).

وخلاصة القول، فإن الهجمات السيبرانية متى كانت آثارها مماثلة لآثار الهجوم المسلح التقليدي بشأن الإصابات الجسدية والأضرار المادية فإنها تكيف كإستخدام للقوة المسحلة المعروفة، وبالتالي للدولة ضحية الهجوم السيبراني اللجوء إلي إستخدام حقها في الدفاع الشرعي عن النفس، كما أن المادة (٤/٢) من الميثاق لم تحظر إستخدام القوة المسلحة فقط، بل حظرت كذلك التهديد بإستخدامها ضد الدول الأخري، ووفقاً لما قررته محكمة العدل الدولية في رأيها الإستشاري بشأن شرعية إستخدام الأسلحة النووية أو التهديد بإستخدامها في الفقرة (٤٧) بأن مفهوما التهديد بالقوة وإستعمال القوة وفقاً للفقرة الرابعة من المادة الثانية من ميثاق الأمم المتحدة متلازمان من حيث أنه إذا كان إستخدام القوة في حالة ما غير مشروع لأي سبب من الأسباب فإن التهديد بإستخدام هذه القوة هو أيضاً غير مشروع، ومن ثم فإن التهديد بإستخدام الهجوم السيبراني يكون مرتبطاً في شرعيته بمدى شرعية الهجوم السيبراني ذاته([2]).

الاتجاه الثاني: ذهب جانب من الفقة الدولي إلي القول بأنه من الصعب علي الدول ممارسة حق الدفاع الشرعي في مواجهة الهجمات السيبرانية والتى قد تحدث أضرار مادية جسيمة مماثلة للأضرار التى يحدثها الهجوم العسكري التقليدي، ويرجع ذلك إلي صعوبة تحديد المسئولية أو معرفة مصدر الهجوم السيبراني أو منفذه، ما لم يعلن منفذه مسئوليته المباشرة عنه، ومن هذه الصعوبات، الأساليب المتطورة المستخدمة لإخفاء هوية مرتكب الهجوم السيبراني، وإمكانية إنطلاق الهجمات السيبرانية من وعبر أجهزة حاسوب متفرقة حول العالم أو من دول مختلفة، وأيضا تنفيذ الهجمات السيبرانية يتم في لمح البصر، مما يستلزم وقتاً طويلاً

---

[4] Michael N. Schmitt, "Attack" as a Term of Art in International Law: The Cyber Operations Context", NATO CCD COE Publications, International Conference on Cyber Conflict, Tallinn, 2012, p5.

[1]) د. أحمد عبيس نعمة الفتلاوي، زهراء عماد محمد كلنتر، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مرجع سابق،ص٦٠-٦١.

لتحديد مصدرها، وكذلك صعوبة وجود أدلة إثبات وإسناد كافية وراسخة وقانونية للهجوم السيبراني([1]).

وأشار هذا الاتجاه إلي القيود المرتبطة بإستخدام القوة لحق الدفاع الشرعي في مواجهة الهجمات السيبرانية، وأولها شرط تحديد مصدر الهجوم أو منفذه، وهذا أكبر تحدى يواجه تأسيس حق الدفاع الشرعي، بسبب التكنولوجيا الحديثة التى تمكن منفذ الهجوم من إخفاء هويته بسهولة، وحتى مع معرفة مصدر الهجوم فإن التقييم الكامل للهجوم السيبراني والخسائر المترتبة عليه تحتاج لوقت طويل.

وفيما يتعلق بشرط الضرورة فإنه حتى مع معرفة مصدر الهجوم أو منفذه، فهذا ليس دليل كاف على ممارسة حق الدفاع الشرعي لأن منفذه قد يكون مجموعة من الأفراد، وحتى مع تورط الدولة فيمكنها أن تنفي مسئوليتها عن هذا الهجوم.

وفيما يتعلق بشرط التناسب، فإنه من الصعب تحقيقه أيضا حتى مع معرفة مصدر الهجوم أو منفذه، والمثال على ذلك إذا تورط أفراد أو فاعلين من غير الدول في هجوم سيبراني، فكيف ستوازن الدولة بين مقدار ما تعرضت له من خسائر وأضرار ومقدار القوة المستخدمة، ويؤدي في ذات الوقت لحدوث خسائر أخرى بين المدنيين، وأكد دليل تالين علي أن المعيار الرئيسي لاستخدام القوة هو التناسب وليس نوع السلاح المستخدم، فالرد علي الهجوم السيبراني قد يكون تقليدي أو إلكتروني والعكس صحيح([2]).

بالتالي تفرض هذه الصعوبات أمام الدولة الضحية لهجوم سيبراني مسلح تحديات كبيرة في سبيل إستيفاء شروط ومتطلبات ممارسة حق الدفاع الشرعي، وانتهى أصحاب هذا الاتجاه إلي ضرورة تأسيس قواعد دولية جديدة وخصوصاً علي مستوى مسئولية الدولة في الفضاء السيبراني، لا تمنح حق الدفاع الشرعي للدول ضد الهجمات السيبرانية فحسب، بل تساير التطور الهائل

---

[2] Nicholas Tsagourias, "Cyber Attacks, Self-Defence and the Problem of Attribution", Journal of Conflict and Security Law, 2012, p5.

[1] Elin Jansson Holmberg, Armed Attacks In Cybersapce: Do They Exist and Can They Trigger The Right to Self-Defence?, Thesis dissertation, Faculty of Law, Stockholm University,2015,p8.

والخطير في أشكال وأنماط الصراعات الجديدة في العلاقات الدولية، معللين ذلك بأن المادة (٥١) من الميثاق وقواعد الدفاع الشرعي التى تم إقرارها مع نشأة الأمم المتحدة عام ١٩٤٥، غير ملائمة لمواكبة هذا التطور، والفضاء السيبراني علي وجه الخصوص كساحة جديدة للصراع الدولي، له طبيعة خاصة وأسلحة مختلفة غير تقليدية، يصعب أن تندرج في إطار قواعد الدفاع الشرعي الحالية([1]).

وترتيباً علي ما تقدم، يلاحظ أن هناك شبه إجماع على تكييف الهجوم السيبراني ذات التأثيرات المادية الجسيمة المشابهة لتأثيرات الهجوم المسلح التقليدي، كهجوم مسلح وفقاً للمادة (٥١) من ميثاق الأمم المتحدة، كما أن هناك إجماع علي أن شرط تحديد مصدر الهجوم و منفذه أو قاعدة الإسناد و تحديد المسئولية عن الهجوم تشكل التحدي الرئيسي أمام ممارسة هذا الحق رداً علي الهجمات السيبرانية([2]).

المطلب الثاني

تكييف الهجمات السيبرانية وفقاً لمبادئ القانون الدولي الإنساني

تمثل الهجمات السيبرانية أحدي التحديات الجديدة أمام القانون الدولي الإنساني ومدى إنطباق أحكام ومبادئ هذا القانون عليها، كمبدأ الضرورة العسكرية ومبدأ التناسب ومبدأ التمييز بين المقاتلين والمدنيين، وهذه المبادئ تم النص عليها صراحة في اتفاقيات القانون الدولي الإنساني وتبدو أهمية المبادئ العامة للقانون في تزويد القانون الدولي الإنساني بالقواعد القانونية اللازمة لمواجهة الأشكال الجديدة من الصراعات المسلحة والتى حدثت في السنوات الأخيرة، وأنه بالرجوع إلي المبادئ العامة المنصوص عليها في الاتفاقيات أو المستمدة من النظم القانونية،

---

[2] Gonzalo J.Arias, "Are The Rules For The Right to Self-Defence Outdated to Address Current Conflicts?" The Law Journal, Vol.6. No.11, University of Chile's Law School, 2017, pp 16-17.

[٣]) د. سلوي يوسف الاكيابي، مدي انطباق القانون الدولي الإنساني علي الهجمات السيبرانية، مرجع سابق، ص ١٣٠٨.

يمكن إيجاد حل لمثل هذه الظواهر الجديدة والوصول إلي المبادئ التى يمكن تطبيقها علي هذه التحديات الجديدة([1]).

ومن الجدير بالذكر، إن قواعد القانون الدولي الإنساني لم تفرد نصوصاً خاصة لتنظيم استخدام الأطراف المتنازعة للهجمات السيبرانية كأسلوب للحرب، ولكن ليس من المقبول القول إن هذه الهجمات لا تخضع لقواعد القانون الدولي الإنساني ذات الصلة، لأن هذه الهجمات تندرج أولاً وأخيراً ورغم حداثتها ضمن أساليب الحرب ووسائل القتال بصفة عامة، التى نظمت قواعد هذا القانون ضوابط اللجوء إليها أثناء النزاعات المسلحة ضماناً لحماية المدنيين وإعمالاً للمبادئ الرئيسية المنظمة له، وخاصة مبادئ الضرورة العسكرية والتناسب والتمييز بين المدنيين والمقاتلين من جانب والأهداف المدنية والأهداف العسكرية من جانب آخر، وهو ما سنحاول بيانه علي النحو التالي:

أولاً: مبدأ الضرورة العسكرية:

وهذا المبدأ يجد أساسه في قواعد القانون الدولي الإنساني العرفي والتى تطبق في النزاعات المسلحة الدولية وغير الدولية([2])، والذى يسمح فقط بإستخدام النوع والدرجة من القوة العسكرية غير المحظورة والتى تكون لازمة لتحقيق الغرض المقصود من النزاع المسلح وهو إضعاف القوة العسكرية للعدو بصورة كاملة أو جزئية وبأقل قدر ممكن من الخسائر في الأرواح والممتلكات، وبالتالي يحظر في هذا الخصوص تدمير ممتلكات العدو أو حجزها، إلا إذا كانت ضرورات الحرب تستلزم هذا التدمير أو الحجز([3]).

---

[1]) د. سعيد سالم جويلي، المدخل لدراسة القانون الدولي الإنساني، دار النهضة العربية، القاهرة، ٢٠٠٢-٢٠٠٣،ص٢٠٣-٢٠٤.

[2]) د. شريف عبد الحميد حسن رمضان، الحرب السيبرانية ومدى ملائمتها مع القانون الدولي الإنساني، مجلة كلية الشريعة والقانون بتفهنا الأشراف – دقهلية، جامعة الأزهر، المجلد (٢٣)، العدد (٤)، يونيو ٢٠٢١، ص٣٠٩١.

[3]) د. يحيي ياسين سعود، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، مرجع سابق، ص٩٢.

فى هذا السياق، تمت الإشارة إلي مبدأ الضرورة العسكرية في عدة وثائق دولية منها إعلان سان بيترسبورغ لعام ١٨٦٨ والذى نص في ديباجته علي أن:" الهدف المشروع الوحيد الذى يجب أن تسعي إليه الدول في أثناء الحرب هو إضعاف القوة العسكرية للعدو". كما أكدت لجنة القانون الدولي، علي عدم جواز اللجوء إلي الضرورة العسكرية إلا إذا لم تستطيع الدولة بلوغ أهدافها العسكرية المشروعة إلا بالقيام بعمل طارئ وضرورى لتحقيق ذلك الغرض وهو حماية مصالحها العليا([1]).

وفى السياق ذاته، أشارت الفقرة (٢/ز) من المادة (٢٣) من اتفاقية لاهاي بشأن الحرب البرية لعام ١٩٠٧، بأنه:" يمنع تدمير ممتلكات العدو أو حجزها، إلا إذا كانت ضرورات الحرب تتطلب حتماً هذا التدمير أو الحجز"، كما تضمنت الفقرة (٢) من المادة (٥٢) من البروتوكول الإضافي الأول لعام ١٩٧٧، أنه:" تقتصر الهجمات علي الأهداف العسكرية، وتنحصر الأهداف العسكرية فيما يتعلق بالأعيان التي تسهم مساهمة فعلية في العمل العسكري، سواء كان ذلك بطبيعتها أم بموقعها أم بغايتها أم باستخدامها، والتي يحقق تدميرها التام أو الجزئي أو الاستيلاء عليها أو تعطيلها، ميزة عسكرية أكيدة"([2]).

ومن الواضح، أنه إذا كان من الممكن التمييز بين الأهداف العسكرية والأهداف المدنية في النزاعات المسلحة التقليدية، فالأمر ليس بالإمكان بالنسبة للهجمات السيبرانية التي من الجائز أن تستهدف منشآت تقدم خدمة للجهد العسكري وفي الوقت نفسه للمدنيين وخاصة في ضوء عدم تحديد معايير منظمة لاستخدام الهجمات السيبرانية للإغراض العسكرية الهجومية،

---

[٤]) د. أحمد عبيس نعمة الفتلاوي، زهراء عماد محمد كلنتر، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مرجع سابق،ص٦٢.

[1]) د. أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مرجع سابق، ص٦٣٤-٦٣٥.

وإمكانية اللجوء إليها بداعي الضرورة العسكرية([1])، وهو ما نجده واضحاً في تصريحات متبادلة بين الولايات المتحدة وروسيا([2]).

وفي هذا الإطار، أشار دليل تالين إلي ضرورة مراعاة تطبيق مبدأ الضرورة العسكرية، وذلك في الحالات التى يكون الخيار ممكناً بين عدة أهداف عسكرية للحصول علي ميزة عسكرية مماثلة، فالهدف الذي يتم اختياره للهجوم السيبراني، هو ذلك الهدف الذى يتوقع منه أن يسبب خطراً أقل علي المدنيين والأعيان المدنية، وفي حالة وجود العديد من أهداف إلا أن احداها يحقق ميزة عسكرية أفضل من غيرها، فإنه يحق للخصم توجيه الهجمات السيبرانية المباشرة ضد الهدف العسكري الذى يحقق أفضل ميزة عسكرية ممكنة في إطار النزاع المسلح، مع مراعاة الضرر الذى تسببه الهجمات السيبرانية بالمنشآت والبنية التحتية الهامة بالنسبة للمدنيين تطبيقاً لمبدأ الضرورة العسكرية([3]).

وخلاصة القول، فإن اللجوء إلي استخدام الهجمات السيبرانية يجب أن يكون ضرورياً وحتمياً لتحقيق الهدف العسكري المشروع، وبشأن مسألة تحديد الأهداف والمنشآت العسكرية عند استخدام الهجمات السيبرانية، فإنها تشكل تحدياً كبيراً أمام المجتمع الدولي فى ضوء عدم وجود معايير محددة لإستخدام الفضاء السيبراني في الأغراض العسكرية، وبالتالي فإن الهجمات السيبرانية تشكل تحدياً واضحاً أمام تطبيق مبدأ الضرورة العسكرية ولابد من بذل الجهود الدولية لتحديد ما يمكن وصفه بهدف فى هذا الصدد([4]).

---

[2]) د. إيمان أحمد علام، الهجمات السيبرانية "الحرب الإلكترونية" واستخدام القوة المسلحة في القانون الدولي العام: الاستغلال السيبراني، مرجع سابق، ص٤٧٣.

[3]) د. سلوي يوسف الاكيابي، مدي انطباق القانون الدولي الإنساني علي الهجمات السيبرانية، مرجع سابق، ص ١٣٧٩-١٣٨٠.

[4]) د. يحيي ياسين سعود، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، مرجع سابق، ص٩٤.

[1]) د. عبد الله عبد الكريم علي أحمد، الهجمات السيبرانية في ضوء القانون الدولي، المجلة المصرية للقانون الدولي، المجلد السابع والسبعون، العدد ٧٧ لسنة ٢٠٢١،ص٢٣.

ثانياً: مبدأ التناسب:

يعد مبدأ التناسب من أهم المبادئ المنظمة للحماية الدولية للمدنيين أثناء النزاعات المسلحة، ويقصد بهذا المبدأ ضرورة مراعاة التوازن بين ضرورات الحرب والنزاع المسلح وبين متطلبات الحفاظ علي الإنسانية([١])، وبالتالي يتعين أن يكون العمل العسكري متناسباً مع النتائج المتوقعة من ورائه، أى مراعاة التناسب ما بين الضرر الذى قد يلحق بالخصم والمزايا العسكرية الممكن تحقيقها نتيجة لاستخدام القوة أثناء سير عملياتها العسكرية([٢]).

فى هذا الإطار، تمت الإشارة إلي مبدأ التناسب في العديد من المواثيق الدولية وأكدت ضرورة مراعاته([٣])، ومن أهمها ما جاء في الفقرة (٥/ب) من المادة (٥١) من البروتوكول الإضافي الأول لاتفاقيات جنيف لعام ١٩٧٧ على أن:" يحظر الهجوم الذي يمكن أن يتوقع منه أن يسبب خسارة في أرواح المدنيين أو إصابة بهم، أو أضرارا بالأعيان المدنية أو أن يحدث مزيجاً من هذه الخسائر والأضرار، ويكون مفرطاً فيما يتعلق بالميزة العسكرية الملموسة والمباشرة"([٤]).

---

[٢]) د. سلوي يوسف الاكيابي، مدي انطباق القانون الدولي الإنساني علي الهجمات السيبرانية، مرجع سابق، ص ١٤٠١.

[٣]) د.هالة أحمد الرشيدي، الإرهاب السيبراني، ماهيته وجهود مكافحته في ضوء التشريعات والقوانين الوطنية والدولية، مرجع سابق، ص٤٧.

[٤]) د. إيمان أحمد علام، الهجمات السيبرانية "الحرب الإلكترونية" واستخدام القوة المسلحة في القانون الدولي العام: الاستغلال السيبراني، مرجع سابق، ص٤٧٤.

[٥]) د. أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مرجع سابق،ص٦٣٧-٦٣٨.

وفى ذات الإطار، أكدت الفقرة (ب/٢) من المادة (٥٧) من البروتوكول الإضافي الأول لعام ١٩٧٧([1])، بالنص علي:" يلغي أو يعلق أي هجوم، إذا تبين أن الهدف المقصود منه ليس هدفاً عسكرياً، أو أنه مشمول بحماية خاصة، أو أن الهجوم قد يتوقع منه أن يحدث خسائر في أرواح المدنيين أو إلحاق الإصابة بهم، أو الأضرار بالأعيان المدنية أو أن يحدث خلطاً من هذه الخسائر أو الأضرار وذلك بصفة عرضية، تفرط في تجاوز ما ينتظر أن يسفر عنه ذلك الهجوم من ميزة عسكرية مباشرة"([2]).

كما أكدت القاعدة (٥٠) من دليل تالين"١" لعام ٢٠١٣ علي حظر الهجمات السيبرانية التى تعامل عدداً من الأهداف العسكرية السيبرانية المميزة والمفصولة بشكل واضح، بصورة مماثلة باعتبارها هدفاً واحداً، في البنية التحتية السيبرانية التى تستخدم في المقام الأول للأغراض المدنية، إذا كان من شأن ذلك أن يضر الأشخاص والأعيان المحميين"([3])، كما حظرت الهجمات السيبرانية التى يتوقع منها أو من شأنها أن تسبب أضراراً عرضية في أرواح المدنيين، أو الإصابة في صفوف المدنيين، أو الاضرار بالأعيان المدنية، أو أن يحدث مزيجاً من ذلك، والتى من شأنها أن تكون مفرطة بالنسبة للميزة العسكرية الملموسة والمباشرة المتوقعة من ذلك الهجوم([4]).

أما بشأن كيفية ضمان مبدأ التناسب في الرد علي استخدام الهجمات السيبرانية، فإنه بالنظر إلي الطبيعة الخاصة للضرر الذى تسببه تلك الهجمات، فإن تطبيق مبدأ التناسب بشأن هذه الهجمات يشكل تحدياً كبيراً أمام التنظيم الدولي وذلك لأن آثار الهجمات السيبرانية غالباً ما

---

[٦]) د. شريف عبد الحميد حسن رمضان، الحرب السيبرانية ومدى ملائمتها مع القانون الدولي الإنساني، مرجع سابق، ص٣٠٩٣.

[1]) د. عبد الله عبد الكريم علي أحمد، الهجمات السيبرانية في ضوء القانون الدولي، مرجع سابق،ص٢٤.

[2]) Tallinn Manual 1.0, definition of cyber attack, Rule 50. Para.2.

[3]) Tallinn Manual 1.0, definition of cyber attack, Rule 51. Para.2.

تكون آثار غير مباشرة([1]). المثال على ذلك الهجوم السيبراني الذى يمنع تدفق المعلومات عبر الإنترنت فإنه سيؤدي إلي عدم قدرة المستشفيات علي نقل المعلومات الحيوية ومن ثم يؤدي إلي خسائر بالأوراح وإصابات جسيمة، وأيضا إذا تم توجيه هجمات سيبرانية ضد بنى تحتية ثنائية الاستخدام "مدنية وعسكرية" مما يصعب تحديد الميزة العسكرية، مما يجعل تطبيق مبدأ التناسب عند استخدام الهجمات السيبرانية أمراً غاية في الصعوبة([2]).

وفى الإطار ذاته، أكد دليل تالين على ضرورة الحد من التكلفة الإنسانية للهجمات السيبرانية متى حدثت في إطار النزاعات المسلحة، واستند في ذلك إلي نص المادة (٣٦) من البروتوكول الإضافي الأول الملحق بإتفاقيات جنيف لعام ١٩٤٩ والصادر في عام ١٩٧٧، والتى نصت بأنه:" يلزم أي طرف متعاقد عند دراسة أو تطوير أو اقتناء سلاح جديد أو أداة للحرب أو إتباع أسلوب للحرب، أن يتحقق فيما إذا كان ذلك محظوراً في جميع الأحوال بمقتضي هذا الملحق (البروتوكول) أو أية قواعد أخري من قواعد القانون الدولي، التي يلتزم بها الطرف السامي المتعاقد، وبالتالي يتعين إلتزام الدول بالإمتثال لتقييم مشروعية أي أسلحة جديدة تقوم بنشرها أو تدرس مسألة استخدامها في ضوء قواعد القانون الدولي الإنساني([3])، وهو ما أكدته القادة (٤٨) من دليل تالين"١" لعام ٢٠١٣ علي ضروة مراجعة الأسلحة وذلك بأنه" أ- على جميع الدول التأكد من أن الوسائل السيبرانية التى يستخدمونها تمتثل لقواعد النزاع المسلح التى تلزم الدولة، ب- على الدول التى تكون طرفاً في البروتوكول الإضافي الأول عند تقوم بدراسة، تطوير، إستحداث، أو اعتماد وسائل أو أساليب جديدة للحرب السيبرانية، أن تحدد ما إذا كان من شأن

---

[4]) طلال ياسين العيسي، عدى محمد عناب، المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مرجع سابق، ص٦٣.

[5]) د. أحمد عبيس نعمة الفتلاوي، زهراء عماد محمد كلنتر، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مرجع سابق، ص٦٢-٦٣.

[1]) د. سلوي يوسف الاكيابي، مدي انطباق القانون الدولي الإنساني علي الهجمات السيبرانية، مرجع سابق، ص ١٣٥٠.

إستخدامها (تشغيلها)، في بعض أو جميع الظروف، أن تكون محظورة بموجب هذا البروتوكول أو من قبل أي قاعدة أخري من قواعد القانون الدولي ذات الصلة الملزمة لها"([1]).

ثالثاً: مبدأ التمييز بين المدنيين والمقاتلين:

نظراً للتطور الهائل في وسائل الحرب والتسلح على النحو الذى أصبح معه بالإمكان إلحاق الضرر بالخصم في كل مكان ولو كان ذلك خارج نطاق العمليات العسكرية، الأمر الذى يستلزم وضع القواعد والأحكام التى تضمن حماية المدنيين والأعيان المدنية ضد أخطار الحروب وأضرارها وذلك من خلال وضع القيود والضوابط التى يتعين الاستعانة بها في التمييز بين الأهداف المدنية من جانب المقاتلين والأهداف العسكرية من جانب آخر، بما يكفل ضمان احترام وحماية السكان المدنيين والأعيان المدنية وتوجيه العمليات العسكرية ضد الأهداف العسكرية دون غيرها([2]).

فى هذا السياق، تمت الإشارة إلي مبدأ التمييز بين المدنيين والمقاتلين في المادة (٤٨) من البروتوكول الإضافي الأول لاتفاقيات جنيف لعام ١٩٧٧ علي ما يلي:" تعمل أطراف النزاع علي التمييز بين السكان المدنيين والمقاتلين وبين الأعيان المدنية والأهداف العسكرية وتوجيه عملياتها ضد الأهداف العسكرية دون غيرها، وذلك من أجل حماية السكان المدنيين والأعيان المدنية"([3]).كما نصت الفقرة (٢) من المادة (٥١) من ذات البروتوكول علي أنه:" لا يجوز أن يكون السكان المدنيون بوصفهم هذا، وكذا الأشخاص المدنيون محلاً للهجوم وتحظر أعمال العنف أو التهديد به الرامية إلي بث الخوف بين السكان المدنيين"". وقد أكدت محكمة العدل الدولية علي هذا المبدأ، بشأن شرعية التهديد باستعمال أو استعمال الأسلحة النووية عام ١٩٩٦، بإعتباره قاعدة آمرة من القواعد الأساسية للقانون الدولي الإنساني وتمثل أحد مبادئ

---

[2] Tallinn Manual 1.0, definition of cyber attack, Rule 48. Para.2.

[٣]) د.هالة أحمد الرشيدي، الإرهاب السيبراني، ماهيته وجهود مكافحته في ضوء التشريعات والقوانين الوطنية والدولية، مرجع سابق، ص٤٤.

[٤]) د.أبو الخير أحمد عطية، حماية السكان المدنيين والأعيان المدنية إبان النزاعات المسحلة، دار النهضة العربية، ١٩٩٨، ص٥٦-٥٧.

القانون الدولي العرفي غير القابلة للانتهاك، كما أكدت المحكمة الجنائية الدولية الخاصة ليوغسلافيا السابقة لعام ١٩٩٣ علي هذا المبدأ والواجب تطبيقه علي كافة النزاعات المسلحة([1]).

كما أكدت القاعدة (٣١) من دليل تالين"١" لعام ٢٠١٣، والقاعدة (٩٣) من دليل تالين "٢" لعام ٢٠١٧ علي أن مبدأ التمييز ينطبق علي الهجمات السيبرانية، كما حظرت القاعدة (٤٩) من دليل تالين"١"، والقاعدة (١٠٥) من دليل تالين "٢" الهجمات العشوائية، وبالتالي تعد محظورة الهجمات السيبرانية التى لا توجه نحو هدف مشروع، والتى يكون من شأنها أن تصيب الأهداف المشروعة والمدنيين والأعيان المدنية من دون أى تمييز" كما حظرت القاعدة (٣٢)،(٣٣) من دليل تالين "١" الهجمات السيبرانية علي السكان المدنيين بصفتهم هذه وكذلك الأفراد المدنيين ينبغي أن لا يكونوا هدفاً للهجمات السيبرانية، وفي حالة الشك في ما إذا كان شخصاً ما مدنياً أم لا يجب أن يعتبر ذلك الشخص مدنيا"([2])، كما أكدت القاعدة (٣٧)،(٣٨) من دليل تالين"١" علي "حظر الهجمات السيبرانية علي الأعيان المدنية وهى كافة الأعيان التى ليست أهدافاً عسكرية، والأهداف العسكرية هى تلك الأعيان التى بحكم طبيعتها، موقعها، غرضها، أو إستخدامها تقدم مساهمة فعالة في العمل العسكري، والتى وفق الظروف السائدة فى ذلك الوقت يشكل تدميرها الكلي أو الجزئي أو الاستيلاء عليها أو تعطيلها ميزة عسكرية أكيدة، ومن الممكن أن تشكل الأهداف العسكري الحواسيب، شبكات الحاسوب، والبنية التحتية السيبرانية"([3]).

كذلك حظرت قواعد القانون الدولي الإنساني الهجمات العشوائية، وهى الهجمات التى من طبيعتها أن تصيب الأهداف العسكرية والأعيان المدنية والمدنيين دون تمييز، كما حظرت

---

[1]) د.داليا أحمد فؤاد، مبدأ التمييز في القانون الدولى بين المقاتلين والمدنيين في النزاعات المسلحة، مجلة السياسة الدولية، العدد ٢١٨، أكتوبر ٢٠١٩، المجلد ٥٤، ص ٦٢-٦٣.

[2]) Tallinn Manual 1.0, definition of cyber attack, Rule 32-33. Para.2.

[3]) Tallinn Manual 1.0, definition of cyber attack, Rule 37-38. Para.2.

قواعد القانون الدولي الإنساني علي الأطراف المتحاربة اللجوء إلي أساليب القتال التى يكون من شأنها تعريض حياة المدنيين للخطر أو مهاجمة الأعيان التى لا غني عنها لبقاء السكان المدنيين علي الحياة، أو شن هجمات الردع أو الهجوم علي المباني أو المنشآت التى تحتوي علي قوى خطرة وهى السدود، الجسور ومحطات توليد الكهرباء النووية، فضلاً عن المنشآت الواقعة في جوارها، من أجل تجنب إطلاق قوى خطرة تتسبب بخسائر فادحة بين السكان المدنيين وأضرار فادحة بالبشرية([1]). كما أكدت القاعدة (٤٩) من دليل تالين"١" علي أن تعد محظورة الهجمات السيبرانية العشوائية التى لا توجه نحو هدف مشروع، وبالتالي يكون من شأنها أن تصيب الأهداف المشروعة والمدنيين والأعيان المدنية من دون أى تمييز([2]).

وفى هذا الإطار، يتطلب مبدأ التمييز بين المقاتلين والمدنيين، من أطراف النزاع المسلح التمييز بين الأشخاص المدنيين والمقاتلين وتوجيه الهجمات السيبرانية للأهداف العسكرية دون المدنية، وهو ما يشكل تحدياً واضحاً أمام القانون الدولي، فوفقاً لهذا المبدأ يتعين علي القادة العسكريين استخدام الوسائل التى يمكنها الاستهداف المحدد للتمييز بين السكان المدنيين والمقاتلين وكذلك التمييز بين الأعيان المدنية والأهداف العسكرية، وبالتالي يحظر علي أطراف النزاع توجيه هجمات سيبرانية ضد أهداف غير عسكرية يقصد بها أو يتوقع منها أن تتسبب بالموت أو الإصابة أو التلف أو الدمار([3]).

وترتيباً علي ما تقدم، فإن التحدي الصعب في تطبيق مبدأ التمييز علي الهجمات السيبرانية، هو كيفية تمييز المدنيين عن المقاتلين، وخاصة أن الهجمات السيبرانية – علي عكس الهجمات التقليدية– غالبا ما يتم تنفيذها عن طريق أشخاص قد يبعدون عن المكان محل

---

[4]) د.هالة أحمد الرشيدي، الإرهاب السيبراني، ماهيته وجهود مكافحته في ضوء التشريعات والقوانين الوطنية والدولية، مرجع سابق، ص٤٥.

[1]) Tallinn Manual 1.0, definition of cyber attack, Rule 49. Para.2.

[2]) د. أحمد عبيس نعمة الفتلاوي، زهراء كلنتر، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مرجع سابق،ص٦٣–٦٤.

الهجوم مسافات قد تتجاوز مئات الأميال، وهذا ما يجعل التمييز بين المدنيين والمقاتلين أمراً غاية في الصعوبة([1]).

وفى هذا السياق، فإذا كان القانون الدولي الإنساني ينطبق علي حالات استخدام الهجمات السيبرانية في إطار النزاعات المسلحة أيا كانت أطرافها، فإن الهجمات السيبرانية غير العسكرية أو التى ترتكب خارج إطار النزاعات المسلحة ، تتمتع بحماية قانونية يحظر اللجوء إليها كأسلوب لإدارة التفاعلات الدولية وذلك وفقاً لنص المادة ٤/٢ من ميثاق الأمم المتحدة والتى تحظر استخدام القوة المسحلة أو التهديد بإستخدامها في العلاقات الدولية، كما استقر الفقة والممارسة الدولية علي أن مفهوم القوة لا يقتصر علي القوة العسكرية وحدها بل يشكل كافة مظاهر التهديد ووسائل الإكراه التى يكون من شأن استخدامها تهديد أمن الدول واستقرارها وسلامتها، والتى تماثل في خطورتها التهديدات العسكرية، وبالتالي فإن الهجمات السيبرانية ذات الطبيعة غير العسكرية وما تحدثه من أضرار اقتصادية جسيمة بالدولة الضحية للهجوم السيبراني تماثل في أثرها الأضرار الجسيمة الناتجة عن استخدام الهجمات السيبرانية ذات الطبيعة العسكرية، واستقر الفقه الدولي علي تكييف استخدام هذه الهجمات خارج إطار النزاعات المسلحة محظوراً في ضوء ما تفرضه قواعد القانون الدولي العام من قواعد وضوابط تتعلق بإستخدام القوة في العلاقات الدولية([2]).

المطلب الثالث

مدى إمكانية تطبيق قواعد القانون الدولي الحالية علي الهجمات السيبرانية

إن التحدى الهائل الذى يواجه مسألة تنظيم إستخدام الهجمات السيبرانية هو عدم وجود إرادة دولية علي المستويين الدبلوماسي والقانوني، يقابله تسارع وتيرة تطوير أنظمة الكترونية قادرة علي التسلل والاختراق لأنظمة الكترونية تابعة لدولة أخرى، وإحداث الضرر بها بما يشكل

---

[2]) د. عبد الله عبد الكريم علي أحمد، الهجمات السيبرانية في ضوء القانون الدولي، مرجع سابق،ص٢٥.

[1]) د. يحيي ياسين سعود، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، مرجع سابق، ص٨٧-٩٠، وكذا د.هالة أحمد الرشيدي، الإرهاب السيبراني، ماهيته وجهود مكافحته في ضوء التشريعات والقوانين الوطنية والدولية، مرجع سابق، ص٥٠-٥١.

هجوماً وعدواناً مفاجئاً للمنشآت الحيوية للدولة الضحية للهجوم السيبراني، وأدى هذا التحدي إلي إثارة التساؤل حول مدى قدرة القانون الدولي العام والإنساني خاصة علي مواجهة آثار الهجمات السيبرانية، وخصوصاً أن القانون الدولي الإنساني ينظم استخدام الاسحلة، في حين أن أغلب الهجمات السيبرانية تقوم علي عمليات لا تتفق والمعايير التى يهدف القانون الدولي إلي تنظيمها، وذلك لوجود مخاطر محققة بالبشر علي الصعيد الإنساني جراء استخدام الهجمات السيبرانية([1]).

فى هذا الإطار، يثور الجدل الفقهي حول السؤال الأتي: هل القواعد الحالية للقانون الدولي تنطبق علي استخدام الهجمات السيبرانية أم أن هناك حاجة إلي قواعد عرفية جديدة وحاجة المجتمع الدولي إلي التوصل لإبرام إتفاقية دولية متعددة الأطراف تحظر أو تقيد استخدام الهجمات السيبرانية؟ حيث اختلف الفقة الدولي في هذه المسألة إلي اتجاهين علي النحو التالي([2]):

ويرى الاتجاه الأول أن القواعد الحالية ومواد الميثاق تنطبق علي الهجمات السيبرانية، إذ هى كافية وعلى قدر كبير من المرونة بحيث يمكن من خلالها تطوير قواعد عرفية جديدة لاستخدام الهجمات السيبرانية، ويستند هذا الاتجاه إلى أن الفضاء السيبراني والتفاعلات داخله لا تشكل في حد ذاتها موضوعات جديدة، بل تحدى للقواعد الحالية للقانون الدولي، كما أن الميثاق قد أقر بأن المعاهدات والقوانين يجب أن تفسر في سياقها التى تعمل فيه، وبالتالي قد أقر بالطبيعة المرنة والمتطورة لمواد الميثاق، كما أن تأسيس قواعد جديدة لتتلاءم مع ظاهرة جديدة

---

[2]) Vida M.Antolin- Jenkins, "Defining the parameters of cyber war operations: Looking for law in all the wrong places", Naval Law Review No.51., 2005, p.134.

[3]) د. شريف عبد الحميد حسن رمضان، الحرب السيبرانية ومدى ملائمتها مع القانون الدولي الإنساني، مرجع سابق، ص٣٠٨٣.

أمر غير منطقي، لأننا سنكون بحاجة إلي تأسيس قواعد جديدة كل يوم لمواكبة التطورات الهائلة في أنماط وطبيعة الصراعات الدولية([1]).

كما أكد جانب من الفقه الدولي، علي أن قواعد القانون الدولي الحالية تنطبق بشكل عام على الفضاء السيبراني، وأن قواعد القانون الدولي قابلة للتكيف مع الظواهر الجديدة دون الحاجة إلي إعادة اختراع إطار تنظيمي كامل فى كل تحدى، والمثال علي ذلك، أنه تم الانتهاء من ميثاق الأمم المتحدة عندما كان اختراع الأسلحة النووية لا يزال سراً، فالقوة المقصودة في الميثاق هي القوة العسكرية الملموسة، ومع ذلك لم تجد محكمة العدل الدولية صعوبة في إصدار رأيها الاستشاري بشأن الأسلحة النووية الذى صدر بعد سنوات من تأسيس الميثاق، وبالتالي فإن أحكام الميثاق تنطبق علي أي استخدام للقوة بصرف النظر علي نوعية السلام المستخدم، وتأسيساً على ذلك يجب أن تخضع الهجمات السيبرانية علي قدم المساواة لقواعد القانون الدولي الخاصة باستخدام القوة([2]).

وعلي الجانب الآخر، يرى الاتجاه الثاني ضرورة تأسيس قواعد جديدة شاملة وذلك لعدة أسباب، أهمها طبيعة الفضاء السيبراني كمجال جديد له أدوات ونطاق مختلف عن المجالات الأخري، وكذلك عدم ملاءمة قواعد الميثاق التى تم تأسيسها عام ١٩٤٥ مع طبيعة وأدوات الصراع في الفضاء السيبراني، وأخيرا حالة الغموض بشأن موقف الدول من استخدام الهجمات السيبرانية، وعدم الإجماع بين الدول الكبري بسبب التحديات الجديدة التى يفرضها تحدى الهجمات السيبرانية علي القوانين والمفاهيم السائة في القانون الدولي، ومنها المسئولية في الفضاء

---

[1]) د. شريف نسيم قلته بخيت،الهجمات الإلكترونية وحق الدفاع الشرعي للدول في القانون الدولي، مرجع سابق،ص١٦٨-١٧٠.

[2]) Kubo Macak, "From Cyber Norms to Cyber Rules: Re-engaging States as Law-Makers", Leiden Journal of International Law, Vol. 30. No. 4,2017, available at:

https://doi.org/10.1017/S092215617000358.

السيبراني ومدى تعلقها بمبدأ سيادة الدولة ومفهوم الهجوم السيبراني وإختلاف مفهوم ومنظور الدول لتهديد السلم والأمن الدوليين([١]).

والواضح أن الدول تعمدت تأييد الاتجاه الأول وإنطباق القواعد الحالية للقانون الدولي والميثاق علي استخدام الهجمات السيبرانية وذلك للحفاظ علي مستويات عالية من الحركة والمرونة داخل الفضاء السيبراني دون التقيد بقوانين وكذلك الرغبة في إسناد الهجمات السيبرانية العدائية علنا إلي دول أخري دون التقيد بقواعد القانون الدولي الحالية([٢]).

ورغم تأييد أغلب الفقه الدولي والدول لانطباق القواعد الحالية وقواعد الميثاق علي الهجمات السيبرانية إلا أنهم اختلفوا حول تفسير القواعد الحالية للقانون الدولي بشأن الهجمات السيبرانية، حيث يواجه التطبيق العملي للكثير من تلك القواعد العرفية وليكن قانون استخدام القوة وحق الدفاع الشرعي ومسألة السيادة – العديد من الصعوبات بالقدر الذي يستلزم التكييف المرن للغاية لتلك القواعد أو استبدالها بقواعد عرفية جديدة لتتلاءم مع قواعد القانون الدولي الحالية وميثاق الأمم المتحدة، كما أن إخضاع الهجمات السيبرانية للقانون الدولي الإنساني مسألة في غاية الصعوبة([٣]).

أما علي صعيد موقف الدول بشأن القانون الدولي الواجب التطبيق علي الهجمات السيبرانية، فأكدت الولايات المتحدة الأمريكية أن مبادئ وقواعد القانون الدولي تنطبق علي الفضاء السيبراني، وأن مطالبة البعض بتأسيس قواعد عرفية جديدة تماما لمواكبة التحديات الصعبة التى يفرضها الفضاء السيبراني محل تشكيك كبير ولا تعكس الإجماع العالمي، وهذه ليست

---

[3]) Iliasse Sdiqui, "Challenges of Regulation: Cyberspace and International Law", November 28, 2016, available at:

http://delma.io/en/draft/challenges-of-regulation-cyberspace-and-international-law.

[4]) Michael N. Schmitt, " International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed", Harvard International Law Journal, Vlo.54, December 2012, pp15-18.

[١]) د. شريف عبد الحميد حسن رمضان، الحرب السيبرانية ومدى ملائمتها مع القانون الدولي الإنساني، مرجع سابق، ص٣٠٩٢.

المرة الأولي التى تواجه القواعد الحالية ومبادئ الميثاق بتحديات تكنولوجية، لكن هذا لا يمنع من أن ما تفرضه ظاهرة الهجمات السيبرانية من تطورات خطيرة متلاحقة يشكل تحديدا لقانون استخدام القوة المسلحة والقانون الدولي الانساني بصفة خاصة، مما يتطلب ضرورة الإجماع دولي حول كيفية تطبيق وإعادة تقييم القواعد الحالية لاسيما قواعد الصراعات المسلحة على الفضاء السيبراني([١]).

وبخصوص الموقف الدولي من إبرام إتفاقية دولية تنظم مسألة استخدام الهجمات السيبرانية، فإن أغلبية الاتفاقيات الدولية المتعلقة بتنظيم استخدام أساليب ووسائل القتال، تم ابرامها في وقت لم يكن معروفاً وقتها استخدام وسائل الإتصالات والمعلومات الإلكترونية كما هو الحال في وقتنا الحالي، ومن المنطقي عدم وجود تنظيماً قانونياً لاستخدام الهجمات السيبرانية بشكل صريح وواضح([٢]). الأمر الذى يتطلب وجود قواعد دولية عرفية لتنظيمها وعلي سبيل المثال حظر استخدام أسلحة الليزر المسببة للعمي عام ١٩٩٥ في البروتوكول الرابع الملحق باتفاقية الأمم المتحدة لحظر أو تقييد استعمال أسلحة تقليدية معينة يمكن اعتبارها مفرطة الضرر أو عشوائية الأثر لعام ١٩٨٠ وذلك وفقاً لمبادئ دولية مقننة وأخرى عرفية أكدت علي عدم شرعية استخدامها، لكونها أسلحة عمياء لا تميز بين الأهداف المدنية والعسكرية، وهو ما يمكن تطبيقه علي الهجمات السيبرانية([٣]).

وفى ذات الإطار، يمكن التأسيس علي ما أصدرته محكمة العدل الدولية عام ١٩٩٦ من رأيها الاستشاري بشأن شرعية التهديد أو استخدام الأسلحة النووية وفقاً للمبادئ الدولية، كمبدا أن

---

[2]) Carrielyn D. Gumon (Ed), Digest of United States Practice in International Law 2012, Office of the Legal Adviser United States Department of State, 2011, available at:

https://2009-2017.state.gov/documents/organization/211955.pdf.

[3]) Rex Hughes, "A treaty for cyberspace", The Royal Institute of International Affairs, International Affairs Journal No.86, Blackwell publishing Ltd, 2010, p.533.

[١]) د. أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مرجع سابق،ص٦٤٨.

حق أطراف النزاع المسلح في اختيار أساليب ووسائل القتال ليس حقاً مطلقاً، وهو ما يعني أن الفرصة متاحة أمام المجتمع لتنظيم مسألة استخدام الهجمات السيبرانية بالاستناد إلي ذات المبادئ والاستعانة بالاتفاقيات الدولية والتشريعات الداخلية التى نظمت مسألة مكافحة الجرائم السيبرانية، وعلي جانب آخر يري البعض أن الاختلاف في وجهات النظر حول حظر تكنولوجيا المعلومات للأغراض العسكرية هى ذاتها القائمة بين الدول الحائزة للأسلحة النووية، وما زال الغموض يتضمن موقف المجتمع الدولي من حظرها أو تقييدها علي مستوى اتفاقية متعددة الأطراف([1]).

وبناء علي ما تقدم، نرى أن التقدم الذى تتمتع به بعض الدول الكبري كالولايات المتحدة الأمريكية وروسيا الاتحادية في مجال المعلومات والبرامج والأنظمة الإلكترونية للأغراض العسكرية والمستحوذة علي الصعيد العالمي، أدخل موضوع استخدام الهجمات السيبرانية ضمن دائرة المصالح والصراعات بين هذه الدول بهدف تحقيق كل منهما مكاسب محددة دون النظر في تنظيم إشكالية وتحدى الهجمات السيبرانية في إطار إتفاقية دولية متعددة الأطراف.

وما يمكن استخلاصه مما سبق، أن موقف الفقة الدولي والدول علي حد سواء قد عكس بالفعل تأييد انطباق القواعد الحالية وقواعد الميثاق علي الهجمات السيبرانية مع التأكيد علي الحاجة إلي بذل المزيد من الجهود نحو بناء التفاهمات والآراء ومحاولة التوافق والإجماع بشأن كيفية تطبيق وتفسير القواعد الحالية للقانون الدولي علي استخدام الهجمات السيبرانية.

المبحث الثاني

الجهود الدولية لمواجهة الهجمات السيبرانية

لا شك أن ظهور الهجمات السيبرانية كأحد مصادر تهديد الأمن الدولي، دفع المجتمع الدولي إلي تعزيز الجهود الرامية لمواجهة الخطورة التى يشكلها هذا الإجرام المستحدث علي الأمن القومي للدول، حيث أصبحت هذه الهجمات من أدوات الحرب الشاملة، كما يعد القضاء علي

---

[2]) Scott J. Shackelford,"State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem", University of Cambridge, Dept of politicos and International STUDIES, Cambridge, UK, 2010.p.216.

الهجمات السيبرانية أمراً معقداً، ولا يمكن تحقيقه إلا من خلال تفعيل سبل التعاون الدولي، وهو أمر من الصعب تحقيقه في ضوء إستمرار القوى العظمي في دعم وتأييد الهجمات السيبرانية ضد بعضها بعضاً، بينما ترفض الهجمات الموجهة إليها، ومع ذلك يجب بذل المزيد من الجهود لعزيز التعاون الدولي، وتقليل الفرص الآمنة للمتسللين والمتورطين في الهجمات السيبرانية، وملاءمة المعايير الدولية، وتفعيل أحكام وقواعد القانون الدولي ذات الصلة([1]).

ولبيان الجهود الدولية لمواجهة استخدام الهجمات السيبرانية، سنتطرق لإتفاقية مجلس أوروبا "بودابست" بشأن الجريمة السيبرانية لعام ٢٠٠١، ثم نتناول وثيقتين بشأن الهجمات السيبرانية وهما دليل تالين وإعلان إيريتشي، وبيان جهود الأجهزة الرئيسية للأمم المتحدة ووكالاتها المتخصصة بشأن الهجمات السيبرانية، وهو ما سنحاول بيانه من خلال ثلاث مطالب علي النحو التالي:

المطلب الأول: إتفاقية مجلس أوروبا "بودابست" بشأن الجريمة السيبرانية لعام ٢٠٠١.

المطلب الثاني: دليل تالين وإعلان إيريتشي.

المطلب الثالث: جهود الأجهزة الرئيسية للأمم المتحدة ووكالاتها المتخصصة بشأن مواجهة الهجمات السيبرانية.

المطلب الأول

إتفاقية مجلس أوروبا "بودابست" بشأن الجريمة السيبرانية لعام ٢٠٠١

لقد أدى ظهور الجرائم السيبرانية كنمط جديد من أنماط الجريمة، وما تتميز به من خاصية عابرة للحدود الإقليمية للدول، إلى توجه المجتمع الدولي للتعاون من أجل التصدي ومكافحة تلك الجرائم التى لها بالغ الأثر السلبي على الأمن القومي للدول في جميع النواحي الإقتصادية منها والعسكرية والاجتماعية. كما سعت دول إلى إتخاذ إجراءات مشتركة للتصدي لتلك الجرائم، من خلال إبرام اتفاقيات ومواثيق دولية لمواجهة تلك الجرائم والعمل على محاربتها، ومنها اتفاقية بودابست لمكافحة الجرائم المعلوماتية لعام ٢٠٠١، وكذلك الاتفاقيات الثنائية

---

[1]) د.إسراء أحمد إسماعيل، الحروب السيبرانية.. تهديد لأمن الدول بدون اشتباكات عسكرية، مرجع سابق، ص١٠-١٤.

والمتعددة لتسليم المجرمين، التي تعد من أهم وسائل مكافحة تلك الجرائم نظراً لكونها عابرة للحدود([1]).

ويعد الهدف من إبرام اتفاقية بودابست المتعلقة بالجريمة السيبرانية([2])هو القيام باستكمال المعاهدات أو الترتيبات الثنائية أو المتعددة الأطراف فيما بين الدول ومنها الاتفاقية الأوروبية المتعلقة بتسليم المجرمين والتى فتح التوقيع عليها في باريس بتاريخ ١٣ ديسمبر عام ١٩٥٧، والاتفاقية الأوروبية المتعلقة بالمساعدة المتبادلة بين الدول في المسائل الجنائية والتى فتح التوقيع عليها في بستراسبورغ بتاريخ ٢٠ ابريل عام١٩٥٢، والبروتوكول الاضافي للاتفاقية الأوروبية بشأن المساعدة المتبادلة في المسائل الجنائية والتى فتح التوقيع عليها في بستراسبورغ بتاريخ ١٧ مارس ١٩٧٨([3]).

وفي هذا الإطار، تعد إتفاقية بوادبست أول معاهدة دولية بشأن جرائم الإنترنت وشبكات الحاسوب الأخري، حيث وقعت هذه الاتفاقية في العاصمة المجرية بودابست في ٢٣ نوفمبر ٢٠٠١، بهدف التعاون والتضامن الدولي في مكافحة الجرائم السيبرانية([4])، حيث وقعت (٢٦) دولة أوروبية علي هذه الإتفاقية بالإضافة إلي الولايات المتحدة الأمريكية، وكندا واليابان وجنوب أفريقيا، وبالرغم من أن هذه الاتفاقية أوروبية المنشأ، إلا أن عضويتها مفتوحة لجميع الدول التى تريد الانضمان إليها، وهى تركز علي تنظيم الجرائم ذات الصبغة الجنائية، مثل

---

[2]) د. إبراهيم السيد رمضان، استجابة الأطر القانونية للقضايا العابرة للحدود، مجلة السياسة الدولية، المجلد ٥٧، العدد ٢٢٨، أبريل ٢٠٢٢، ص٢١٨-٢١٩.

[1]) مجلس أوروبا، إتفاقية مجلس أوروبا المتعلقة بالجريمة الإلكترونية، مجموعة المعاهدات الأوربية رقم ١٨٥، بودابست، عام ٢٠٠١.

[2]) د. عبد الله عبد الكريم علي أحمد، الهجمات السيبرانية في ضوء القانون الدولي، مرجع سابق،ص٣٠-٣١.

[3]) د. وفاء لطفي، الجهود الدولية في مجال مكافحة جرائم الارهاب السيبراني: التجربة الماليزية نموذجا، مجلة كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، المجلد الثالث والعشرون، العدد الأول، يناير ٢٠٢٢، ص ١٦٣.

انتهاكات حق المؤلف، والاحتيال الالكتروني، والتصوير الإباحي للأطفال، وانتهاك أمن الشبكات المعلوماتية، ودخلت حيز النفاذ في ٢٠٠٤/٧/١، من خلال خمسة تصديقات بما فيها ثلاث دول أعضاء في مجلس أوروبا وتوقيعات خمسة وخمسون دولة حتى تاريخ ٢٠٢٠/٧/٢٩([1]).

وفى الإطار ذاته، نصت المادة الخامسة من اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية لعام ٢٠٠١، علي أن:" تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمداً وبغير حق: الإعاقة الخطيرة لاشتغال نظام الكمبيوتر عن طريق إدخال بيانات حاسوبية، إرسالها، إتلافها، حذفها، إفسادها، تغييرها أو تدميرها"([2]).

وكذلك تهدف إتفاقية بودابست بشأن الجريمة السيبرانية إلي تحقيق ثلاثة أهداف رئيسية، وهي علي النحو التالي([3]):

١- مواءمة عناصر القانون الجنائي الوطني مع الأحكام المتصلة بمكافحة الجرائم السيبرانية.

٢- النص علي صلاحيات القانون الإجرائي الجنائي الداخلي اللازمة للتحقيق في هذه الجرائم ومتابعتها قضائياً، إضافة إلي الجرائم الأخري المرتكبة عن طريق نظام الكمبيوتر أو التى تكون الأدلة المتصلة بها الكترونية.

---

[4]) د. هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية للجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في ٢٣ نوفمبر ٢٠٠١، دار النهضة العربية، القاهرة، ط١، ٢٠٠٣، ص٢٩. راجع حول ذلك بالتفصيل:

https://rm.coe.int/budapest-convention-in-arabic/1680739173.

[1]) د. أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مرجع سابق، ص٦١٧.

[2]) د.هالة أحمد الرشيدي، الإرهاب السيبراني، ماهيته وجهود مكافحته في ضوء التشريعات والقوانين الوطنية والدولية، مرجع سابق، ص١٨٤-١٨٦.

٣- إنشاء نظام سريع وفعال للتعاون الدولي والحفاظ السريع علي البيانات المخزنة علي أجهزة الكمبيوتر وحفظها وعدم الإفصاح الجزئي عن حركة هذه البيانات المخزنة علي الكمبيوتر.

وقد صنفت إتفاقية بودابست الجرائم السيبرانية إلي أربع طوائف مختلفة علي النحو التالي([1]):

١- الجرائم المرتكبة ضد سلامة المعلومات وخصوصيتها، وتشمل جرائم الدخول غير المشروع (القرصنة)، التجسس علي البيانات والمعلومات، الاعتراض غير القانوني، التدخل في البيانات والمعلومات، التدخل في أنظمة الكمبيوتر وبرامجه.

٢- الجرائم المتصلة بالكمبيوتر، وتشمل جرائم استخدام الكمبيوتر في التزوير والأفعال الاحتيالية.

٣- الجرائم المتعلقة بالمحتوى والمضمون، وتشمل جرائم وجود مضمون جنسي أو إباحي والتحريض علي العنصرية الكراهية والتعرض للأديان والألعاب علي الإنترنت والتشهير والمعلومات المضللة والبريد المزعج.

٤- الجرائم المتصلة بحقوق الطبع والنشر والعلامات التجارية، وتشمل جرائم إستخدام العلامات التجارية في أنشطة إجرامية بهدف التضليل والجرائم ذات الصلة بإسم المواقع الإلكترونية([2]).

وكذلك تناولت الاتفاقية الجرائم التى تعتبر من أكثر الجرائم شيوعاً علي مستوي العالم، مثل الإرهاب السيبراني، الحرب الإلكترونية، غسل الأموال السيبراني، الخداع، عمليات تزوير بطاقات الائتمان.كما تضمنت الإتفاقية المبادئ العامة المتعلقة بمسائل التعاون الدولي، كتسليم المجرمين والمساعدات المتبادلة، وإجراءات طلب المساعدات المتبادلة في غياب الاتفاقيات الدولية واجبة التطبيق، إعطاء المعلومات بصورة آلية والولاية القضائية، التدابير المؤقتة

---

[3]) بن صابر بلقاسم، د. حيدرة محمد، الهجمات السيبرانية ومواجهتها في ضوء القانون الدولي المعاصر، مرجع سابق، ص٢٠٦.

[4]) د. وسام محمود عرفان مصطفي، سبل مكافحة الهجمات السيبرانية دولياً، مرجع سابق، ص٣٠١٢-٣٠١٣.

والمساعدات المتبادلة فيما يتعلق بسلطات التحقيق ومكافحة استخدام شبكة الإنترنت لارتكاب جرائم سيبرانية([1]).

مما سبق، يتضح أن اتفاقية بودابست تعد محاولة من المشرع الدولي لتحديد القانون الواجب التطبيق علي الهجمات السيبرانية، ووضع قواعد قانونية منظمة لهذا النوع من الهجمات، حيث جاء في ديباجة الاتفاقية أن إبرامها جاء نتيجة التغيرات التى أحدثتها الرقمية والتقارب والعولمة المستمرة للشبكات المعلوماتية، وأن هناك سمة بارزة في تكنولوجيا المعلومات تتمثل في الآثار الناشئة عن تطور التكنولوجياالسيبرانية ومخاطر استخدام هذه التكنولوجيا في ارتكاب أفعال تعد من قبيل الجرائم الدولية، حيث حاولت الإتفاقية إيجاد نظام فعال للتعاون الدولي في مجال مواجهة الهجمات السيبرانية، كما حاولت الدول الأطراف في الاتفاقية الوصول إلي صيغة تشريعية عامة لمواجهة الهجمات السيبرانية والحد من آثارها، ويعاب علي هذه الاتفاقية عدم الالتفات إلي الهجمات السيبرانية التى تقوم بها الدول في إطار رسمي، حيث تناولت فقط النص علي الهجوم السيبراني الذى يشنه الأشخاص ضد بعضهم البعض، واقتصر اهتمامها علي الطابع التجريمي للهجمات السيبرانية([2]).

المطلب الثاني

دليل تالين وإعلان إيريتشي

أولاً:- دليل تالين بشأن القانون الدولي المطبق علي الهجمات السيبرانية:

منذ تصاعد خطورة هذه الأنماط الجديدة من الهجمات السيبرانية عام ٢٠٠٧ وفي ظل غياب دور الأمم المتحدة والأجهزة والهيئات التابعة لها وخصوصاً مجلس الأمن ولجنة القانون

---

[1]) د. هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية للجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في ٢٣ نوفمبر ٢٠٠١، مرجع سابق، ص٣٠.

[2]) د. إسلام رمضان هديب، مفهوم الحرب السيبرانية في ظل القانون الدولي وتحديد خصائصها والنتائج المترتبة عليها، مجلة البحوث القانونية والاقتصادية، كلية الحقوق جامعة بني سويف، المجلد (٣٦)، العدد (١)، يناير ٢٠٢٤، ص١٥٢.

الدولي، بشأن الصراع في الفضاء السيبراني، والهجمات السيرانية وكيفية مواجهتها وفقاً لقواعد وأحكام القانون الدولي، ففي عام ٢٠٠٩ دعا مركز التميز للدفاع الإلكتروني التعاوني التابع لحلف الناتو والذى مقره مدينة "تالين" عاصمة "إستونيا"، مجموعة من أبرز الخبراء العسكريين والقانونيين بمشاركة اللجنة الدولية للصليب الأحمر بصفتها مراقب، لمناقشة كيفية تطبيق القواعد القانونية الدولية الحالية علي الهجمات السيبرانية، وإصدار دليلاً لدراسة تداعيات الحروب والهجمات السيبرانية والقواعد المنظمة لها، عرف بإسم "دليل تالين" وذلك تأكيداً منهم على ضرورة الحد من التكلفة الإنسانية للهجمات السيبرانية متى حدثت في إطار النزاعات المسلحة([1]).

ونشر الإصدار الأول منه عام ٢٠١٣ كأهم استجابة دولية بشأن تكييف هذه الأنماط الجديدة من الحروب، ومواجهتها وفقاً لأحكام وقواعد القانون الدولي وميثاق الأمم المتحدة، ويحتوى هذا الدليل على (٩٥) قاعدة لسلوك الدول في سياق الهجمات السيبرانية وكيفية تعامل الدول في الفضاء السيبراني، وكيفية تطبيق قواعد القانون الدولي الحالية وأحكام الميثاق في الفضاء السيبراني، وعلى الهجمات السيبرانية، في حين نشر الإصدار الثاني من دليل تالين عام ٢٠١٧ متضمناً (١٥٤) قاعدة تشكل مستوى أكثر توسعاً بشأن معالجة العمليات السيبرانية، مع تعليقات علي كل قاعدة، وبيان حقوق والتزامات الدول في الفضاء السيبراني وانتهى الدليل إلي أن القواعد الدولية السارية فاعلة إلي حد كبير، ويمكن تطبيقها علي العمليات السيبرانية، كما تناول الدليل بعض التحديات القانونية في الفضاء السيبراني كسيادة الدول، وقواعد ممارسة الاختصاص القضائي وقانون مسئولية الدول ومبدأ العناية الواجبة في الفضاء السيبراني، بالإضافة إلي قانون الفضاء والقانون الدولي لحقوق الإنسان وقانون البحار والقانون الدبلوماسي

---

[1]) د. شريف نسيم قلته بخيت،الهجمات الإلكترونية وحق الدفاع الشرعي للدول في القانون الدولي، مرجع سابق،ص١-٢، راجع حول ذلك بالتفصيل:

-Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press. 2013, pp 1-11, and Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press. 2017, pp 1-7.

والقنصلي، إضافة إلي تقديم مراجعة وتقييم وتعديلات لبعض قواعد " تالين١" وذلك في ضوء مواقف الدول وتطور الممارسة الدولية([١]).

وفي هذا الإطار، يشكل دليل تالين أول محاولة دولية لكيفية التعامل مع هذا التطور التكنولوجي والبحث في التكييف القانوني للهجمات السيبرانية، بإصدارية الأول عام ٢٠١٣، والثاني عام ٢٠١٧، حيث أكدت قواعد دليل تالين علي أن بعض أحكام القانون الدولي المعاصر يمكن تطبيقها في مجال الفضاء السيبراني([٢]).

وقد ساهم دليل تالين([٣]) بشكل واضح في المناقشات بين الدول حول تحدى الهجمات السيبرانية وكيفية تفسير وتطبيق أحكام وقواعد القانون الدولي علي أنشطة الدول والكيانات من غير الدول في الفضاء السيبراني، ويقرر دليل تالين أن الهجمات السيبرانية قد تشكل نزاعات مسلحة، وذلك بالنظر للآثار الجسيمة والمدمرة لتلك الهجمات، ويتناول دليل تالين تعريف الهجمات السيبرانية بالقاعدة رقم (٣٠) من دليل تالين "١" بأنها" عمليات سيبرانية، سواء كانت هجومية أو دفاعية، والتى يهدف من خلالها بصورة معقولة التسبب بالاصابة أو وفاة الأشخاص أو الاضرار أو تدمير الأعيان أو الأهداف"([٤]).

وفى ذات الإطار، تناول دليل تالين تعريف الهجمات السيبرانية الإجراءات التى قد تتخذها الدول للرد علي الهجمات السيبرانية بالقاعدة رقم (١٣) من دليل تالين "١" الدفاع عن النفس

---

[٢]) د. محمد عادل محمد عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق علي ممارسة التجسس وقت السلم: دراسة علي ضوء دليل "تالين" بشأن القانون الدولي المطبق علي العمليات السيبرانية ٢٠١٣-٢٠١٧، مرجع سابق، ص ٣١١-٣١٢.

[٣]) د. محمد ربيع أحمد حسين، الهجمات السيبرانية واستخدام القوة في القانون الدولي المعاصر، مرجع سابق.ص ٣٠٣-٣٠٤.

[1]) R. Buchan & I. Navarrete. "Cyber espionage and international law". In Research Handbook on International Law and Cyberspace. Edward Elgar Publishing, 2021, pp. 231-252.

[٢]) د. وسام محمود عرفان مصطفي، سبل مكافحة الهجمات السيبرانية دولياً، مرجع سابق، ص٣٠٢٤.

ضد هجوم مسلح والتى نصت علي أنه"يجوز للدولة التى تكون هدفاً للعمليات السيبرانية التى تصل لمستوى الهجوم المسلح بالمعني المفهوم في المادة (٥١) من ميثاق الأمم المتحدة، أن تمارس حقها الطبيعي في الدفاع عن النفس، وتعتبر العملية السيبرانية هجوماً مسلحاً بالاعتماد علي حجمها وآثارها المادية الجسيمة"([1]) وقرر خبراء دليل تالين أنه يعد استخداماً غير مشروع للقوة، قيام دولة بتزويد قوات أو أفراد بأجهزة وتدريبهم لشن هجمات سيبرانية ضد دولة أخرى([2]).

وقد طبق هذا المفهوم بصورة واضحة في عملية استخدام الهجمات السيبرانية في الحرب بين جورجيا وروسيا في أغسطس ٢٠٠٨، وفي الهجمة السيبرانية العالمية (فيروس الفدية) التى طالت أكثر من ٦٠ دولة علي مستوى العالم في ٢٧ يونيو ٢٠١٧، وهو ما أدى إلي ظهور الهجمات السيبرانية بشكل علني وواضح في الصراع الدولي المسلح، وثار الجدل حول مدى اعتبار الهجمات السيبرانية المسلحة عملاً من أعمال الحرب، وخاصة مع تماثل نتائج الهجمات السيبرانية مع الهجمات التقليدية، مما أدى إلي وجود حرب مفتوحة ومن الصعب تحديد أطرافها، لذا تسعي الدول إلي تطوير أساليب جديدة في الحروب المستقبلية([3])، وقد وضع دليل تالين مجموعة من الصفات التى يجب أن تتسم بها الهجمات السيبرانية، حتى ترقي إلي درجة الهجوم المسلح، وبالتالي تعطي الدولة المعرضة لهجوم سيبراني حق الدفاع الشرعي وتفعيل المادة (٥١) من الميثاق([4]).

---

[3]) د. سامي محمد عبد العال، الدفاع الشرعي ضد الهجمات السيبرانية، مرجع سابق، ص٧٦-٧٧.

[4]) Michael N. Schmitt:" Peacetime Cyber Responses and wartime Cyber Operations inder International Law: An Analytical Vade Mecum", Harvard National Security Journal, Vol.8, 2017, p.245.

[5]) د. هانى محمد خليل العزازي، النظام القانوني الدولي لمكافحة المخاطر السيبرانية، مجلة مصر المعاصرة، الجمعية المصرية للإقتصاد السياسي والإحصاء والتشريع، القاهرة، العدد ٥٤٩، يناير ٢٠٢٣،ص٥١٩-٥٢٠.

[1]) رزق أحمد سمودي، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام، مرجع سابق، ص٣٥١-٣٥٣.

ومن أهم المعايير وفقاً لدليل تالين والتى يجب الاستناد إليها في تحديد المستوى المطلوب لوصول الهجمات السيبرانية إلي درجة الهجوم المسلح، يتمثل في جسامة هذا الهجوم وحدته ومدى تأثيره علي الدولة المعتدي عليها، وأن يكون هناك ضرر مادى حال وآنى علي الأفراد والممتلكات في الدولة المعتدي عليها بهجوم سيبراني، فالهجمات السيبرانية يمكن لها أن تنتج مثل الضرر المصاحب للهجمات العسكرية التقليدية أو يفوقه كما لو حدث اعتداء سيبراني علي شبكات الإتصالات والمعلومات الخاصة بمطار إحدى الدول، مما أدى إلي مقتل الآلاف بسبب الخلل الذى أحدثته الهجمة، وأدى إلي تصادم الطائرات هبوطا وصعودا، ففي مثل هذه الحالة يعد الهجوم السيبراني هجوماً عسكرياً(١).

وفي الإطار ذاته، أكد دليل تالين أن أحكام ميثاق الأمم المتحدة قابلة للتطبيق علي الهجمات السيبرانية، كما يطالب الدول ألا تعامل الفضاء السيبراني علي أنه فراغ قانوني لا تنطبق عليه المبادئ القانونية المطبقة في الفضاءات المادية، ويجب علي المجتمع الدولي الاستجابة والالتزام بأحكام وقواعد القانون الدولي عند استخدام الهجمات السيبرانية، إضافة إلي ذلك لا يعد هذا الدليل صكاً دولياً رسمياً أو ملزماً، وأنه يعد وثيقة رائدة في مجال العمليات السيبرانية وخطوة مهمة لنتظيم الفضاء السيبراني، وإن كانت غير كافية ويلزم أن تتبعها خطوات أخري(٢) ومن الإنتقادات التى وجهت لدليل تالين هو تطبيق نصوصه فقط علي الحالات التى تتم خلال نزاع مسلح، وهذا ما أشارت إليه القاعدة (٢٠) من دليل تالين "١" المتعلقة بتطبيق قانون النزاعات المسلحة علي الهجمات السيبرانية التى تنفذ في سياق النزاع المسلح(٣).

---

٢) د. أميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مرجع سابق، ص٥٠٦.

3) M. D. CAVELTY, The Militarisation of Cyberspace: Why Less May Be Better‘in C. CZOSSECK, R. OTTIS, K. ZIOLKOWSKI (eds.), 4th International Conference on CyberConflict, NATO CCD COE, 2012, P. 141.

٤) د. إسلام رمضان هديب، مفهوم الحرب السيبرانية في ظل القانون الدولي وتحديد خصائصها والنتائج المترتبة عليها، مرجع سابق، ص١٥٣-١٥٤.

ثانياً:- إعلان إيريتشي بشأن مبادئ الاستقرار السيبراني والسلام السيبراني:

أعد إعلان إيريتشي بشأن مبادئ الاستقرار السيبراني والسلام السيبراني بواسطة فريق الرصد الدائم المعني بأمن المعلومات التابع للاتحاد العالمي للعلماء (WFS)، واعتمدته الجلسة العامة للاتحاد العالمي للعلماء في الدورة الثانية والأربعين للحلقات الدراسية الدولية بشأن الطوارئ العالمية، في إريتشي (صقلية) في ٢٠ أغسطس ٢٠٠٩([1]).

ويؤكد هذا الإعلان أن تحقيق الاستقرار السيبراني وتحقيق السلام السيبراني أمران متدخلان تداخلاً وثيقاً، ويتميز الإعلان بالإيجاز ويركز علي المبادئ التالية لتحقيق الاستقرار والسلام السيبراني وحفظهما، وذلك علي النحو التالي([2]):

١- يجب علي جميع الحكومات الاعتراف بأن القانون الدولي يضمن للأفراد التدفق الحر للمعلومات والأفكار، وتنطبق هذه الضمانات أيضاً على الفضاء السيبراني. ويجب عدم فرض القيود إلا عند الاقتضاء، على أن تخضع لعملية مراجعة قانونية.

٣- يجب علي جميع البلدان العمل معاً لوضع مدونة مشتركة للسلوك السيبراني وإطار قانوني عالمي منسق، بما في ذلك أحكام إجرائية تتعلق بالمساعدة في التحقيق والتعاون بما يكفل احترام الخصوصية وحقوق الإنسان. ويجب علي جميع الحكومات ومزودي الخدمات والمستعملين دعم الجهود المبذولة في سبيل إنفاذ القانون الدولي ضد مرتكبي الجرائم السيبرانية([3]).

---

[1]) د. هانى محمد خليل العزازي، النظام القانوني الدولي لمكافحة المخاطر السيبرانية، مرجع سابق،ص٥٢١-٥٢٢.

[2]) د. أميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مرجع سابق،ص٥١٢.

[3]) د. وسام محمود عرفان مصطفي، سبل مكافحة الهجمات السيبرانية دولياً، مرجع سابق، ص٣٠٢٨.

٣- يجب علي جميع المستعملين ومزودي الخدمات والحكومات العمل معاً لضمان ألا يستخدم الفضاء السيبراني بأي شكل من شأنه أن يؤدي إلى استغلال المستعملين، وخاصة الشباب والمستضعفين منهم، من خلال العنف أو الإذلال.

٤- يجب عليالحكومات والمنظمات والقطاع الخاص بما في ذلك الأفراد، تنفيذ برامج شاملة للأمن وتحديثها وفقاًلأفضل الممارسات والمعايير المقبولة دولياً واستخدام تكنولوجيات حماية الخصوصية والأمن.

٥- يجب علي مطوري البرمجيات والمعدات السعي إلى تطوير تكنولوجيات آمنة تدعم القدرة على التصدي ومقاومة نقاط الضعف.

٦- يجب علي الحكومات أن تشارك بفعالية في جهود الأمم المتحدة الرامية إلى النهوض بالأمن السيبراني والسلام السيبراني في العالم وأن تتفادى استخدام الفضاء السيبراني من أجل النزاعات المسلحة([1]).

وترتيباً علي ما تقدم، فإنه لابد من السعي إلي السلام السيبراني، وذلك فى ضوء القدرات الهائلة للهجمات السيبرانية العدوانية التى تقوم بها الدول أو جهات فاعلة من غير الدول، وقد دعا الاتحاد العالمي للعلماء إلي العمل من أجل وضع قانون عالمي للفضاء السيبراني تحت رعاية الأمم المتحدة، وخصوصا في مجال الاستخدامات العسكرية والعدوانية للفضاء السيبراني، فضلاً عن ضرورة تحديد إطار قانوني لتعريف ما الذي يشكل خرقاً للسلام، وقد اقترح الأمين العام للاتحاد الدولي للاتصالات، بأنه يتعين علي الدول أن تتعهد في هذا الإطار بألا تبدأ بالهجوم السيبراني ضد دولة أخر (عدم المبادأة) ويتعين أن تلتزم بعدم حماية الإرهابيين السيبرانيين والمهاجمين في بلدانها دون أن تعاقبهم([2]).

---

[1]) د. سامي محمد عبد العال، الدفاع الشرعي ضد الهجمات السيبرانية، مرجع سابق،ص٨١-٨٢.

[2]) د. أميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مرجع سابق،ص٥١٧.

المطلب الثالث

جهود الأجهزة الرئيسية للأمم المتحدة ووكالاتها المتخصصة بشأن الهجمات السيبرانية

أولاً: الجمعية العامة للأمم المتحدة.

أصدرت الجمعية العامة للأمم المتحدة العديد من القرارات والتوصيات فى هذا المجال، طالبت من خلالها الدول باستخدام تكنولوجيا الاتصالات والمعلومات استخداما سلميا، وتعزيز التعاون الدولي فيما بينها لتحقيق أمن الفضاء السيبراني، ومكافحة إساءة استخدامه في أعمال إجرامية فى ضوء ارتفاع معدلات الجرائم المرتكبة في العالم الرقمي وازدياد تنوعها، وإزاء تأثير هذه الجرائم على استقرار البني التحتية الحيوية للدول والمؤسسات، وشددت علي ضرورة تعزيز التنسيق والتعاون بين الدول في مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية، بما فى ذلك من خلال تقديم المساعدة التقنية إلي البلدان النامية بناء علي طلبها من أجل تحسين التشريعات الوطنية وبناء قدرات السلطات الوطنية بهدف التصدى لذلك الاستخدام بكل أشكاله، بما يشمل منعه والكشف عنه والتحقيق فيه وملاحقة مرتكبيه قضائياً، وأهمية الصكوك الدولية والإقليمية في مجال مكافحة الجريمة السيبرانية والجهود الرامية إلي بحث الخيارات المتاحة لتعزيز التدابير القانونية أوغيرها من التدابير القائمة علي الصعيدين الوطني والدولي للتصدي لاستخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية، واقتراح تدابير جديدة في هذا الشأن، كما أكدت علي الدور الذى تؤديه الأمم المتحدة وبالأخص لجنة منع الجريمة والعدالة الجنائية، وأهمية احترام حقوق الإنسان والحريات الأساسية في استخدام تكنولوجيا المعلومات والإتصالات، ومن أهم القرارات التى أصدرتها الجمعية العامة للأمم المتحدة في هذا الخصوص، ما يلي:

١- القرار رقم A/RES/55/28، الصادر في ٢٠ نوفمبر ٢٠٠٠، بشأن التطور في مجال المعلومات والإتصالات([1]).

---

[1]) د. محمد عادل محمد عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق علي ممارسة التجسس وقت السلم: دراسة علي ضوء دليل "تالين" بشأن القانون الدولي المطبق علي العمليات السيبرانية ٢٠١٣-٢٠١٧، مرجع سابق، ص ٣٠٢-٣٠٣.

٢- القرار رقم A/RES/55/63، الصادر في ٤ ديسمبر ٢٠٠٠، بشأن محاربة استخدام تكنولوجيا المعلومات للأغراض الإجرامية([1]).

٣- القرار رقم A/RES/56/19، الصادر في ٢٩ نوفمبر ٢٠٠١، والمتعلق بمكافحة إساءة استعمال تكنولوجيا المعلومات والاتصالات لأغراض إجرامية، وأوصي القرار بأن تضمن الدول فى قوانينها وممارساتها عدم توفير ملاذات آمنة لكل من يسئ استخدام تكنولوجيا المعلومات لأغراض إجرامية، وضمان حماية سرية المعلومات وسلامة أنظمة الحاسوب، ضد أي اعتداء غير مشروع مع تقرير عقوبة على ذلك الفعل".

٤- القرار رقم A/RES/56/121، الصادر في ١٩ ديسمبر ٢٠٠١، والمتعلق بمكافحة إساءة استعمال تكنولوجيا المعلومات والاتصالات لأغراض إجرامية، ويدعو هذا القرار الدول الأعضاء، عند وضع التشريعات الوطنية لمكافحة إساءة استعمال تكنولوجيا المعلومات، أن تأخذ بالاعتبار عمل لجنة منع الجريمة والعدالة الجنائية في هذا الخصوص([2]).

٥- القرار A/RES/57/53، الصادرفي ٢٢ نوفمبر ٢٠٠٢، والمتعلق بمكافحة إساءة استعمال تكنولوجيا المعلومات والاتصالات لأغراض إجرامية، ودعا القرار الدول الأعضاء عند وضع التشريعات الوطنية لمكافحة إساءة استعمال تكنولوجيا المعلومات، الأخذ بعين الاعتبار عمل لجنة منع الجريمة والعدالة الجنائية.

٦- القرار A/RES/57/239، الصادرفي ٢٠ ديسمبر ٢٠٠٢، والمتعلق بإرساء ثقافة عالمية للأمن السيبراني، وضرورة دعم الجهود الوطنية بتبادل المعلومات والتعاون في هذا المجال علي الأصعدة الوطنية والإقليمية والدولية، حتى يتسني التصدى الفعال لما تتميز به التهديدات السيبرانية بشكل متزايد من طابع عابر للحدود الوطنية، كما أكد القرار علي أن الأمن السيبراني للهياكل الأساسية الحيوية للمعلومات مسئولية ملقاة علي عاتق الحكومات

---

[2]) Resolution adopted by the General Assembly [on the report of the Third Committee (A/55/593)], General Assembly, United Nations, Fifty-fifth session Agenda item 105, 22 January 2001, p. 2.

[3]) Resolution adopted by the General Assembly [on the report of the Third Committee (A/56/574)], General Assembly, United Nations, Fifty-sixth session Agenda item 110, 23 January 2002, p.2.

ومجال يجب أن تحمل فيه عنصر الصدارة وطنياً، بالتنسيق مع أصحاب المصلحة ذوى الشأن([1]).

٧- القرار رقم A/RES/58/32، الصادر في ٨ ديسمبر ٢٠٠٣، بشأن إنشاء ثقافة أمنية عالمية للفضاء الحاسوبي وحماية الهياكل الأساسية الحيوية للمعلومات([2]).

٨- القرار رقم A/RES/58/199، الصادر في ٣٠ يناير ٢٠٠٤، والمتعلق بإرساء ثقافة أمنية عالمية للأمن السيبراني وحماية البنية التحتية الأساسية الحيوية للمعلومات.

٩- القرار رقم A/RES/59/61، الصادر في ٣ ديسمبر ٢٠٠٤، والمتعلق بدعوة الدول إلي تحديث قوانينها في مجال مكافحة الجرائم الإلكترونية، وكذلك اعتماد إتفاقيات إقليمية في هذا الشأن([3]).

١٠- القراررقم A/RES/60/45، الصادر في ٨ ديسمبر ٢٠٠٥، والمتعلق بالتقدم في المعلومات والاتصالات في سياق الأمن الدولي، ودعا القرار إلي ضرورة تشجيع التعاون الدولي لمكافحة الجرائم الإلكترونية، وتقديم المساعدة للدول الأعضاء في هذا المجال.

١١- القرار رقم A/RES/60/175، الصادر في ١٦ ديسمبر ٢٠٠٥، والمتعلق بتعزيز برنامج الأمم المتحدة لمنع الجريمة والعدالة الجنائية، ولا سيما قدراته في مجال التعاون التقني([4]).

---

[1] Resolution adopted by the General Assembly [on the report of the e Second Committee (A/57/529/Add.3)], General Assembly, United Nations, Fifty-seventh session Agenda item 84 (c) , 31 January 2003, p.2-3.

[2] د. أميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مرجع سابق،ص٤٨٣-٤٨٤.

[3] د. عبد الله عبد الكريم علي أحمد، الهجمات السيبرانية في ضوء القانون الدولي، مرجع سابق،ص٢٩.

[4] Resolution adopted by the General Assembly [on the report of the Third Committee (A/60/510 and Corr.1)], General Assembly, United Nations, Sixtieth session Agenda item 106 , 20 March 2006, p.1

١٢- القرار رقم A/RES/64/211، الصادر في ٢١ ديسمبر ٢٠٠٩، بشأن إرسال ثقافة عالمية تكفل أمن الفضاء الإلكتروني وتقييم الجهود الوطنية الرامية إلي حماية الهياكل الأساسية الحيوية للمعلومات، ويدعو القرار الدول إلي وضع التشريعات الضرورية للتحقيق في جرائم الفضاء الإلكتروني ومحاكمة مرتكبيها، مع ملاحظة الأطر القائمة، مثل قرارات الجمعية العامة ٦٣/٥٥ و ١٢١/٥٦ و٢٣٩/٥٧ و ١٩٩/٥٨ بشأن مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، والمبادرات الإقليمية، بما فى ذلك اتفاقية مجلس أوروبا المتعلقة بجرائم الفضاء الإلكتروني، والتعاون مع الجهات الدولية النظيرة للتحقيق في جرائم الفضاء الإلكتروني العابرة للحدود الوطنية في الحالات التى تكون فيها الهياكل الأساسية واقعة في أراضي دولة أو التى يكون فيها الجناة مقيمين في تلك الأراضي، في حين يقيم الضحايا في أراضي دولة أخري([1]).

١٣- القرارات أرقام ٦١/٥٤ و ٦٢/١٧ و٦٣/٣٧ و ٦٤/٢٥ و ٦٥/٤١ و٦٦/٢٤ و ٦٧/٢٧ و ٦٨/٢٣٧ و٧١/٢٨ والمتعلقين بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وضرورة منع استخدام مصادر أو تكنولوجيات المعلومات في تحقيق أغراض إجرامية أو إرهابية، ولفت انتباه الدول إلي عواقب الحرب السيبرانية وهى مجموعة من الهجمات علي شبكة الحاسوب خلال حالات النزاع المسلح، وتشمل هذه العواقب مخاطر كارثية ومنها التشويش علي نظم مراقبة الملاحة الجوية والتسبب في تصادم الطائرات أو تحطمها أو قطع إمدادات الكهرباء أو المياة على السكان المدنيين أو إلحاق الضرر بالمرافقة الكيمائية أو النووية، وضرورة التزام كل الأطراف في النزاعات المسحلة بإحترام قواعد القانون الدولي الإنساني إذا لجأت إلي وسائل وأساليب الحرب السيبرانية ومن هذه القواعد مبادئ الضرورة العسكرية والتمييز والتناسب والحيطة([2]).

---

[1]) د. سامي محمد عبد العال، الدفاع الشرعي ضد الهجمات السيبرانية، مرجع سابق، ص٨٤-٨٥.

[2]) انظر نص قرارات الجمعية العامة للأمم المتحدة بشأن الهجمات السيبرانية في:

١٤- القرار رقم A/RES/66/181، الصادر في ١٩ ديسمبر ٢٠١١، بشأن تعزيز برنامج الأمم المتحدة لمنع الجريمة والعدالة الجنائية، ولا سيما قدراته في مجال التعاون التقني.

١٥- القرار رقم A/RES/68/193، الصادر في ١٨ ديسمبر ٢٠١٣، بشأن تعزيز برنامج الأمم المتحدة لمنع الجريمة والعدالة الجنائية، ولا سيما قدراته في مجال التعاون التقني، وتحديداً قراري لجنة منع الجريمة والعدالة الجنائية التابعة للمجلس الاقتصادي والاجتماعي رقمي ٧/٢٢ المؤرخ ٢٦ أبريل ٢٠١٣ بشأن" تعزيز التعاون الدولي علي مكافحة الجريمة السيبرانية" و٨/٢٢ المؤرخ ٢٦ أبريل ٢٠١٣ بشأن "الترويج للمساعدة التقنية وبناء القدرات بغية تعزيز التدابير الوطنية والتعاون الدولي لمكافحة الجريمة السيبرانية"([1]).

١٦- القرار رقم A/RES/72/28، الصادر في ٤ ديسمبر ٢٠١٧، والمتعلق بدور العلم والتكنولوجيا في سياق الأمن الدولي ونزع السلاح، وضرورة اهتمام المجتمع الدولي بتوجيه التطورات العلمية والتكنولوجية لتحقيق أغراض مفيدة.

١٧- القرار رقم A/RES/73/187، الصادر في ١٧ ديسمبر ٢٠١٨، والمتعلق بمكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية.

١٨- القرار رقم A/RES/74/173، الصادر في ١٨ ديسمبر ٢٠١٩، والمتعلق بتعزيز المساعدة التقنية وبناء القدرات لتدعيم التدابير الوطنية والتعاون الدولي في مجال مكافحة الجريمة السيبرانية، بما يشمل تبادل المعلومات.

١٩- القرار رقم A/RES/75/240، الصادر في ٣١ ديسمبر ٢٠٢٠، والمتعلق بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وضرورة استخدام تكنولوجيات المعلومات والاتصالات في الأغراض السلمية في سبيل تحقيق

- A/RES/61/54 of 6 December 2006, A/RES/62/17 of 5 December 2007, A/RES/63/37 of 2 December 2008, A/RES/64/25 of 2 December 2009, A/RES/65/41 of 8 December 2010, A/RES/66/24 of 2 December 2011,A/RES/67/27 of 3 December 2012, - A/RES/68/243 of 27 December 2013, A/RES/69/28 of 2 December 2014, A/RES/70/237 of 23 December 2015,A/RES/71/28 of 5 December 2016.

[1]) د. وسام محمود عرفان مصطفي، سبل مكافحة الهجمات السيبرانية دولياً، مرجع سابق، ص ٣٠٠٤-٣٠٠٥.

الصالح العام للبشرية في الفضاء الإلكتروني، ومصلحة جميع الدول في منع نشوب النزاعات الناشئة عن استخدام هذه التكنولوجيات.

٢٠- القرار رقم A/RES/75/282، الصادر في ٢٦ مايو ٢٠٢١، والمتعلق بمكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية.

٢١- القرار رقم A/RES/76/19، الصادر في ٦ ديسمبر ٢٠٢١، والمتعلق بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي، وتعزيز السلوك المسؤول من جانب الدول في استخدام تكنولوجيات المعلومات والاتصالات، وضرورة منع استخدام موارد أو تكنولوجيات المعلومات لأغراض إجرامية أو إرهابية.

٢٢- القرار رقم A/RES/77/37، الصادر في ٧ ديسمبر ٢٠٢٢، والمتعلق ببرنامج العمل للارتقاء بسلوك الدول المسؤول في استخدام تكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي.

٢٣- القرار رقم A/RES/78/16، الصادر في ٤ ديسمبر ٢٠٢٣، والمتعلق بالتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية وبرنامج العمل للارتقاء بسلوك الدول المسؤول في استخدام تكنولوجيات المعلومات والاتصالات في سياق الأمن الدولي، والتأكيد علي أن المعايير الطوعية وغير الملزمة لسلوك الدول المسؤول في استخدام تكنولوجيا المعلومات والاتصالات يمكن أن تحد من المخاطر التى تهدد السلام والأمن والاستقرار على الصعيد الدولي([1]).

وفي عام ٢٠٠٤، أنشأت الجمعية العامة للأمم المتحدة، مجموعة للخبراء الحكوميين (GGE) لدراسة تأثير تطورات تكنولجيا المعلومات والاتصالات علي الأمن القومي والعسكري للدول، وفي عام ٢٠٠٩ قامت الأمم المتحدة في إطار جهودها لمواجهة الهجمات السيبرانية بإنشاء ما يطلق عليه "الشراكة التعددية ضد الهجمات السيبرانية"Impact وفي أبريل ٢٠١٠ قامت لجنة

[1]) د. هانى محمد خليل العزازي، النظام القانوني الدولي لمكافحة المخاطر السيبرانية، مرجع سابق،ص٥٠١-٥٠٢.

الأمم المتحدة لمنع الجريمة والعدالة الجنائية بتكوين فريق دولي من الخبراء الحكوميين مهمته بحث مشاكل استخدام الهجمات السيبرانية، وكيفية التعامل معها([1]).

وفي عام ٢٠١٠ قدمت مجموعة(GGE) تقريراً بشأن التهديدات التى تشكلها العمليات السيبرانية للسلم والاستقرار الدوليين، وأن الافتقار إلي توجيه دولي بشأنها قد يتسبب في أضرار جسيمة، وقد تضمن التقرير التوصيات التالية:

١-مواصلة التعاون بين الدول لمناقشة المعايير المتعلقة باستخدام تكنولوجيا المعلومات والاتصالات، وذلك بهدف الحد من مخاطرها وحماية البني التحتية السيبرانية للدول.

٢-تبادل الآراء الوطنية وبناء الثقة في مجال الحد من مخاطر استخدام الدول لتكنولوجيا المعلومات والإتصالات.

٣-تبادل المعلومات بشأن التشريعات الوطنية واستراتيجيات وسياسات أمن الاتصالات وأفضل الممارسات الدولية.

٤-تحديد التدابير اللازمة لدعم بناء القدرات في الدول النامية([2]).

وكذلك في عام ٢٠١٥ قدمت مجموعة (GGE) تقريراً تضمن عدة توصيات وأهمها ضرورة تطبيق قواعد وأحكام القانون الدولي علي الفضاء السيبراني وعدم استهداف البني التحتية السيبرانية للدول، أو دعم الأنشطة ذات الصلة، واعتبار أى دولة مسئولة عن الهجمات السيبرانية التى تنطلق من أراضيها.

وفى ذات الإطار، اعتمدت الجمعية العامة في ٢٨ ديسمبر ٢٠١٩، قراراً ببدء صياغة معاهدة دولية لمكافحة استخدام تكنولوجيا الاتصالات والمعلومات لأغراض إجرامية، وذلك من خلال

---

[1]) د. أحمد زكريا الباسوسي، الجهود الدولية لمكافحة الهجمات السيبرانية علي قطاع الطاقة: حالات مختارة، مجلة كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، المجلد (٢٤)، العدد (٤) أكتوبر ٢٠٢٣، ص ١٧١.

[2]) د. محمد عادل محمد عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق علي ممارسة التجسس وقت السلم: دراسة علي ضوء دليل "تالين" بشأن القانون الدولي المطبق علي العمليات السيبرانية ٢٠١٣-٢٠١٧، مرجع سابق، ص ٣٠٣.

لجنة دولية من عدد من الخبراء الحكوميين، ورغم اختلاف مواقف القوي الدولية من هذا القرار ومن الحاجة لصياغة معاهدة دولية جديدة فى هذا الشأن، إلا أنه يعكس الاهتمام الدولي بمكافحة خطورة الهجمات السيبرانية وضرورة مكافخة كافة صور الاستخدام غير الآمن للفضاء السيبراني، علي غرار ما تم تحقيقه بإعتماد إتفاقية بودابست لعام ٢٠٠١ في هذا الصدد([1]).

ثانياً: مجلس الأمن.

١-القرار رقم S/RES/1963(2010)، الصادر عن مجلس الأمن والذي أعرب فيه عن القلق إزاء إستخدام الإرهابيين للتكنولوجيا الجديدة للمعلومات والاتصالات، خاصة الإنترنت لأغراض التجنيد والتحريض، إضافة إلى تمويل أنشطتهم وتخطيطها وإعدادها. كما أكد المجلس أهمية التعاون بين الدول الأعضاء لمنع الإرهابيين من حيازة الأسلحة من خلال تكنولوجيا المعلومات والاتصالات، مع احترام حقوق الانسان وحرياته الأساسية والامتثال للالتزامات بموجب القانون الدولي، وأنه لا يمكن هزيمة الإرهاب بالقوة العسكرية وتدابير إنفاذ القانون والعمليات الاستخباراتية وحدها([2]).

٢-القرار رقم S/RES/2341(2017)، الصادر في ١٣ فبراير ٢٠١٧ عن مجلس الأمن والذى يهيب فيه مجلس الأمن بالدول الأعضاء إلي إنشاء أوتعزيز الشراكات الوطنية والإقليمية والدولية مع الجهات صاحبة المصلحة من القطاعين العام والخاص، حسب الاقتضاء، لتبادل المعلومات والخبرات من أجل منع الهجمات الإرهابية علي الهياكل الأساسية الحيوية والحماية منها والتخفيف من آثارها والتحقيق فيها ومواجهتها والتعافي من أضرارها، وذلك بوسائل منها التدريب المشترك واستخدام أو إنشاء شبكات ملائمة للاتصال والإنذار في حالات الطوارئ، وذلك بما يتفق والتزامات الدول الأعضاء ذات الصلة بكفالة احترام حقوق الإنسان وسيادة القانون، كما أكد ضرورة اتخاذ ما يلزم من تدابير لاسيما عن طريق حرمان الإرهابيين من

---

[3]) د.هالة أحمد الرشيدي، الطابع التشريعى لقرارات مجلس الأمن: دراسة حالة قرارات مكافحة الإرهاب، المجلة المصرية للقانون الدولى، العدد ٦٩، ٢٠١٣، ص١٥٨-١٥٩.

[1]) انظر نص القرار علي الرابط التالي:

https://undocs.org/ar/S/RES/1963 (2010)

الوصول لوسائل تنفيذ هجماتهم، بما فى ذلك تعزيز أمن الهياكل الأساسية الحيوية التى يسهل استهدافها([1]).

٣-القرار رقم S/RES/2370(2017)، الصادر في ٢ أغسطس ٢٠١٧ عن مجلس الأمن والذى يدعو فيه الدول الأعضاء إلي العمل بصورة تعاونية لمنع الإرهابين والمتطرفين من حيازة الأسلحة، من خلال تكنولوجيا المعلومات والإتصالات، مع كفالة احترام حقوق الإنسان وحرياته الأساسية والامتثال للالتزامات الدولية بموجب قواعد القانون الدولي ذات الصلة([2]).

وفي هذا الإطار، اتخذ مكتب الأمم المتحدة لمكافحة الإرهاب العديد من المبادرات في مجال التكنولوجيا الجديدة، ومنها برنامج أمن الفضاء الإلكتروني والتقنيات الحديثة علي وجه الخصوص والذي يهدف إلي تعزيز قدرات الدول الأعضاء والمنظمات الخاصة علي منع الهجمات السيبرانية التى تقوم بها الجهات الفاعلة الإرهابية ضد البنية التحتية الحيوية، كما يهدف البرنامج إلي تخفيف آثار الهجمات السيبرانية واستعادة وإصلاح الأنظمة المستهدفة في حالة حدوث تلك الهجمات([3]).

ثالثاً: المجلس الاقتصادي والاجتماعي.

في التاسع من سبتمبر عام ٢٠١١ عقد المجلس الاقتصادي والاجتماعي التابع للأمم المتحدة، اجتماعاً لمناقشة أمن الفضاء السيبراني والتنمية، والقضايا والتحديات ذات الصلة، وحددت أهداف الإجتماع فى النقاط التالية:

---

[2] SC. Res. 2341, UN. Doc. No, S/RES/2341(2017) (February, 13, 2017), Available At:
https://undocs.org/ar/S/RES/2341(2017)

[3]) SC. Res. 2370, UN. Doc. No, S/RES/2370(2017) (August, 2, 2017), Available At:
https://digitallibrary.un.org/record/1298189?ln=ar

[1]) د.هالة أحمد الرشيدي، الإرهاب السيبراني، ماهيته وجهود مكافحته في ضوء التشريعات والقوانين الوطنية والدولية، مرجع سابق، انظر نص القرار علي الربط التالي:

https://www.un.org/counterterrorism/ar/cybersecurity

١-بناء وعى على مستوى السياسات الدولية، من خلال تزويد أعضاء المجلي الاقتصادي والاجتماعي، بصورة عن الوضع الحالي والتحديات المتعلقة بأمن الفضاء السيبراني وارتباطاته بالتنمية.

٢-تحديد أفضل السياسات المتعلقة بهذا المجال، والمبادرات المطبقة في مختلف دول العالم بهدف بناء ثقافة أمن الفضاء السيبراني.

٣-مدى الاستجابة الدولية بشأن تزايد معدلات الجريمة السيبرانية([١]).

كما تناول الاجتماع الفوارق الاقتصادية بين الدول وعدم قدرة الدول النامية علي مكافحة الهجمات السيبرانية، وكذلك افتقاد الشراكة بينها وبين الدول الكبري، وهو ما يؤدي إلي خلق ملاذ آمن لمهاجمي الفضاء السيبراني لارتكاب جرائمهم، كما تناول الاجتماع الحاجة إلي ابرام اتفاقية دولية بشأن الهجمات السيبراني، وذلك علي غرار إتفاقية بودابست بإعتبارها تنسيقاً بين الدول بخصوص بعض الجرائم السيبرانية، وخلص الاجتماع إلي أن الأمن السيبراني قضية عالمية لا يمكن حلها إلا من خلال شراكة عالمية وخاصة من خلال الأمم المتحدة لما تملكه من قدرات إستراتيجية وتحليلية يمكن استخدامها لمعالجة هذه التحديات([٢]).

بالتالي فإن قرارات الأمم المتحدة ممثلة في أجهزتها كالجمعية العامة ومجلس الأمن والمجلس الاقتصادي والاجتماعي لم تتناول معالجة مسألة تنظيم استخدام الهجمات السيبرانية في الأغراض العسكرية، وأن قراراتها اقتصرت علي المناشدة أو الدعوة أو الطلب من الدول إتخاذ إجراءات الحيطة ووضع التشريعات اللازمة لمواجهة الهجمات السيبرانية، رغم ما تشكله الهجمات السيبرانية من تهديد واضح وصريح للسلم والأمن الدوليين، إكتفاءً بدعوة الدول الأعضاء في قراراتها المختلفة، إلي إرساء ثقافة أمنية عالمية للأمن السيبراني وحماية البنية التحتية الأساسية الحيوية للمعلومات وكذلك وضع القوانين الوطنية والسياسات العامة لمكافحة

---

[٢]) د. هانى محمد خليل العزازي، النظام القانوني الدولي لمكافحة المخاطر السيبرانية، مرجع سابق،ص٥٠٣.

[٣]) د. وسام محمود عرفان مصطفي، سبل مكافحة الهجمات السيبرانية دولياً، مرجع سابق، ص٣٠٠٦.

إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية أو إرهابية، وأن تأخذ في اعتبارها عواقب الهجمات السيبرانية([1]).

رابعاً: الاتحاد الدولي للاتصالات:

يؤدي الاتحاد الدولى للاتصالات دوراً عالمياً فريداً لمناقشة مسألة الأمن السيبراني، حيث يعمل الاتحاد على مساعدة حكومات الدول الأعضاء في الاتفاق على مبادئ مشتركة حول ضوابط الاعتماد على تكنولوجيا المعلومات والبنية التحتية للاتصالات.

وفي مايو ٢٠٠٧ أعلن الأمين العام للاتحاد الدولي للاتصالات إطلاق برنامج الأمن السيبراني العالمي(GCA) لتوفير إطار يمكن من خلاله لجميع أصحاب المصلحة تنسيق استجابة دولية للتحديات الهائلة التي يطرحها الأمن السيبراني. ويقوم برنامج الأمن السيبراني العالمي على التعاون الدولي ويهدف إلى التوصل إلي إطار أو بروتوكول لتنسيق جهود مكافحة الجرائم السيبرانية، ومساهمة جميع أصحاب المصلحة المعنيين في جهود لبناء الثقة والأمن في مجتمع المعلومات، وبما يشمل تدابير قانونية وتقنية وإجرائية وتنظيمية وتعاون دولي([2]).

وقد وضع الاتحاد الدولي مخططاً لتعزيز برنامج الأمن السيبراني العالمي لعام ٢٠٠٩، يتكون من سبعة أهداف استراتيجية رئيسية، وهي علي النحو التالي([3]):

١- وضع استراتيجيات لاستحداث تشريع نموذجي لمكافحة الجريمة السيبرانية يكون قابلاً للتطبيق محلياً وعالمياً بالتوازي مع التدابير القانونية الوطنية والدولية المعتمدة.

٢- وضع استراتيجيات عالمية لإيجاد الهياكل التنظيمية والسياسات العامة بشأن الجريمة السيبرانية المناسبة لوضع الهيكليات التنظيمية علي الصعيدين الوطني والإقليمي.

---

[1]) د. سامي محمد عبد العال، الدفاع الشرعي ضد الهجمات السيبرانية، مرجع سابق،ص٨٦-٨٧.

[2]) د. محمد عادل محمد عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق علي ممارسة التجسس وقت السلم: دراسة علي ضوء دليل "تالين" بشأن القانون الدولي المطبق علي العمليات السيبرانية ٢٠١٣-٢٠١٧، مرجع سابق، ص ٣٠٨.

[3]) د. وسام محمود عرفان مصطفي، سبل مكافحة الهجمات السيبرانية دولياً، مرجع سابق،ص ٣٠١٨-٣٠١٩.

٣- وضع استراتيجية لتحديد الحد الأدني المقبول عالمياً في موضوع المعايير الأمنية ونظم تطبيقات البرمجيات والأنظمة.

٤- وضع استراتيجيات لإيجاد إطار عالمي للرصد والمراقبة والإنذار والرد المبكر لضمان التنسيق عبر الحدود بين المبادرات الجديدة والقائمة.

٥- وضع استراتيجيات عالمية لإنشاء وإقرار نظام هوية رقمي عام عالمي وتطبيقه، وتحديد الهيكليات التنظيمية اللازمة لضمان الاعتراف بالوثائق الرقمية للأفراد عبر الحدود الجغرافية.

٦- وضع استراتيجية عالمية لتسهيل بناء القدرات البشرية والمؤسسية لتعزيز المعرفة والمهارات في مختلف القطاعات وفي كافة المجالات المعلوماتية.

٧- وضع مقترحات بشأن إمكانية اعتماد إطار لاستراتيجية عالمية لأصحاب المصلحة المتعددين من أجل التعاون الدولي والحوار والتنسيق على الصعيد الدولي في جميع المجالات التى سبق ذكرها ([1]).

وفى الإطار ذاته، وضع الاتحاد الدولي للاتصالات عدة تشريعات في مجال الجرائم السيبرانية عام ٢٠١٠، لتعزيز التقارب فيما بين التشريعات الوطنية بشأن هذه الجرائم والتى تتناول المسائل المتعلقة بالأمن السيبراني، وقدمت أحكاماً نموذجية لتجريم بعض الهجمات السيبرانية الإرهابية التى تستخدم فيها الإنترنت، ومنها الدخول غير المصرح به إلي برامج أو بيانات حاسوبية لأغراض إرهابية، أو نقل برمجيات خبيثة ضارة بقصد دعم الإرهاب، أو الحصول علي برامج حاسوبية بغرض التحضير لارتكاب أعمال إرهابية([2])، كما اتجهت العديد من الدول

---

[1]) انظر الاتحاد الدولي للاتصالات، التقرير السنوى للاتحاد لعام ٢٠٠٩، جنيف، ص٢٠، متاح علي الرابط:

https://www.itu.int/dms_pub/itu-s/opb/conf/S-CONF-AREP-2009-PDF-A.pdf

[2]) د.هالة أحمد الرشيدي، الإرهاب السيبراني، ماهيته وجهود مكافحته في ضوء التشريعات والقوانين الوطنية والدولية، مرجع سابق، ص١٦٧، وكذلك د. أميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مرجع سابق، ص٤٩٤-٤٩٦.

لتبني العديد من المبادرات على المستويات الوطنية والثنائية والإقليمية والدولية، للعمل على حماية البنية التحتية للمعلومات من خطر التعرض للهجمات السيبرانية، والعمل على إيجاد أطر تشريعية جديدة تتعامل مع تلك الظاهرة المستحدثة وتبني إجراءات قانونية وأمنية صارمة بإمكانها الوقاية والتصدى للتهديدات المتزايدة التى تمثلها الهجات السيبرانية الإرهابية([1]).

المبحث الثالث

المسئولية الدولية عن إستخدام الهجمات السيبرانية

أصبحت الهجمات السيبرانية من أهم التحديات التى تواجه المجتمع الدولي، نظراً لما يترتب علي تلك الهجمات من تبعات المسئولية الجنائية والمدنية، وخصوصاً أن بعض الدول أصبحت تلجأ إلي تلك الهجمات، بهدف تحقيق بعض المكاسب أو توجيه تهديدات لدول أخري، الأمر الذى يستلزم تناول عنصر المساءلة بوصفها عنصراً أساسياً من عناصر القانون الدولي الإنساني، كما أثيرت شكوك حول إمكانية المحافظة علي معايير المساءلة([2])والمسئولية عن استخدام القوة وآثاره عند استخدام الهجمات السيبرانية المسلحة ويرجع ذلك إلي صعوبة تحديد المسئولية أو معرفة مصدر الهجوم السيبراني أو منفذه وصعوبة وجود أدلة إثبات وإسناد كافية وراسخة وقانونية للهجوم السيبراني، مما يثير إشكالية الإفلات من العقاب، والوقوف علي مدى امتثال الهجمات السيبرانية لقواعد وأحكام القانون الدولي الإنساني، وتحديد المسئولية الدولية المترتبة علي الأضرار التى تصيب المستهدفين بالهجمات السيبرانية وحماية المجتمع الدولي مما تهدده من مخاطر جسيمة.

---

[3]) Adam Peake, Internet governance and the World Summit on the Information Society (WSIS)- Report for the Association for Progressive Communications (APC), June 2004, P: 3.

[1]) د. محمد صافي يوسف،القانون الدولي العام، دار النهضة العربية، القاهرة، ٢٠١٩، ص٤٠٥.

وفى ضوء عدم وضوح المفاهيم التقليدية لمسئولية الدولية في إطار التكنولوجيا الحديثة، مثل صعوبة أو استحالة إثبات (إسناد) الهجمات السيبرانية لمصدر محدد، وذلك لتنفيذها في سرية وسرعة فائقة، ويتم توجيهها عبر عدة أجهزة حاسوب، ومن دول مختلفة، وصعوبة التحقق من مصدر الهجوم أو هوية المهاجم، الأمر الذى يستلزم التعرض لهذه الإشكاليات القانونية بشأن المسئولية الدولية سواء فيما يتعلق بالدول أو الكيانات الأخري التى تقوم بتلك الهجمات، وخصوصاً في حالة وجود صلة بين الدول وهذه الكيانات، وذلك في إطار مشروع لجنة القانون الدولي بشأن مسئولية الدول لعام ٢٠٠١، وأيضا دليل تالين "١" لعام ٢٠١٣، ودليل تالين "٢" لعام ٢٠١٧ بشأن القانون الدولي المطبق علي الحروب السيبرانية.

ولبيان أبعاد المسئولية الدولية الناتجة عن الهجمات السيبرانية، سنتطرق لبيان مفهوم المسئولية الدولية فى ضوء الهجمات السيبرانية، ثم بيانالإشكاليات القانونية بشأن المسئولية الدولية عن إرتكاب الهجمات السيبرانية، وهو ما سنحاول بيانه علي النحو التالي:

المطلب الأول: مفهوم المسئولية الدولية فى ضوء الهجمات السيبرانية.

المطلب الثاني: الإشكاليات القانونية بشأن المسئولية الدولية عن إرتكاب الهجمات السيبرانية.

المطلب الأول

مفهوم المسئولية الدولية فى ضوء الهجمات السيبرانية

تعرف المسئولية الدولية بأنها" الجزاء القانوني الذي يرتبه القانون الدولي العام على عدم احترام أحد أشخاص هذا القانون لالتزاماته الدولية"([1])، وعرفت كذلك بأنها" النظام القانوني الذي بمقتضاه تلتزم الدولة التي نسب إليها عملا غير مشروع طبقا للقانون الدولي، بأن تعوض الدولة التي ارتكب ضدها هذا العمل"([2]).

بالتالي تترتب المسئولية الدولية على مخالفة الدولة لالتزاماتها الدولية المقررة في القانون الدولي وذلك نتيجة لقيامها بعمل أو بامتناع عن عمل لا يجيزه لها القانون الدولي، أو يترتب عليه

---

[1]) د. عبد العزيز محمد سرحان، القانون الدولي العام ، المجتمع الدولي – المصادر– نظرية الدولة، دار النهضة العربية، القاهرة ،١٩٨٦، ص ٣٨٥.

[2]) د. الشافعي بشير، القانون الدولي العام في السلم والحرب ،منشأة المعارف بالإسكندرية، ١٩٧٤، ص ٧٩.

المساس بالحقوق التي قررها ذلك القانون لأشخاص القانون الدولي الآخرين. فمناط المسئولية الدولية إذن هو ارتكاب مخالفة لأحكام القانون الدولي تحدث ضرراً بالدول الأخرى([١]).

وعرفت لجنة القانون الدوليفي مشروعها بشأن مسئولية الدول لعام ٢٠٠١المسئولية الدولية بأنها:" كل فعل غير مشروع دولياً تقوم به الدولة يستتبع مسئوليتها الدولية"، حيث أشارت إلى أن أساس المسئولية الدولية طبقا لنظرية الفعل غير المشروع دوليا يأتي موسعا لنطاق المسئولية الدولية([٢]).وبالتالي لا يمكن قيام المسئولية الدولية إلا إذا ثبت أن السلوك كان مخالفاً لأحكام القانون الدولي العرفية أو التعاهدية، ولكن لم تشترط هذه المادة وقوع الضرر لإثارة المسئولية الدولية، ولا يعني ذلك أن الضرر ليس له دور في إطار المسئولية الدولية، فيعد الضرر في أغلب الحالات العنصر الأساسي لتحديد آثار هذه المسئولية، ولكن مجرد وقوعه لا يكفي كقاعدة لتقرير المسئولية ابتداء ويلزم تحقق انتهاك التزام دولي([٣]).

وفى إطار جهود لجنة القانون الدولي نحو تطوير قواعد المسئولية الدولية عن الأفعال الضارة العابرة للحدود والتى لا يحظرها القانون الدولي وذلك نظراً للتطور الهائل في مجال التكنولوجيا والمجال التقني، حيث تم إدراج المسئولية الدولية عن النتائج الضارة الناشئة عن أفعال لا يحظرها القانون الدولي ضمن أنشطتها المقدم من لجنة القانون الدولي في دورتها الأربعين عام ١٩٨٨، ودورتها التاسعة والأربعين عام ١٩٩٧ بعنوان (منع الضرر العابر للحدود الناشئ عن

---

[٣]) د. محمد حافظ غانم، المسئولية الدولية، دراسة لأحكام القانون الدولي ولتطبيقاتها التي تهم الدول العربية ، محاضرات ألقاها على طلاب الدراسات القانونية ، معهد الدراسات العربية العالية، جامعة الدول العربية، بدون ناشر ، ١٩٦٢، ص٤١.

[٤]) د. أيمن عبد العزيز سلامة ، المسئولية الدولية عن ارتكاب جريمة الإبادة الجماعية، رسالة دكتوراه، كلية الحقوق ، جامعة الإسكندرية، ٢٠٠٥، ص٣٣١- ٣٣٢.

[٥]) د. أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مرجع سابق، ص٦٤١.

أنشطة خطرة) والتى قررت بأن تنشأ المسئولية على الأنشطة التي تنطوي على مخاطر إيقاع ضرر ملموس عابر للحدود([1]).

ويلاحظ أن قيام المسئولية الموضوعية على الأفعال التي تنطوي على مخاطر إيقاع ضرر ملموس عابر للحدود يعد اتجاها شديدا نحو العدالة في أسمى صورها، وترجمة حقيقية لكافة التطورات الاقتصادية والعلمية الحديثة، الأمر الذي يؤدى غالبا إلى استقرار المراكز القانونية لأطراف المسئولية الدولية([2]). بالتالي تؤكد نظرية المخاطر أن الدولة التى تقوم بأي نشاط تكنولوجي ترافقه مخاطر تصيب دولة أخري، فإنها تتحمل المسئولية الناشئة عن ذلك النشاط بالتعويض عن أي ضرر دون النظر إلي الخطأ كأساس لقيام المسئولية الدولية([3]).

وفى هذا الإطار، أكد دليل تالين بإصدارية الأول عام ٢٠١٣، والثاني عام ٢٠١٧، علي تقرير أحكام المسئولية الدولية عن الهجمات السيبرانية، بإعتبار أنه وإن كانت بعض هذه الهجمات لا تنتهك القانون الدولي في حد ذاتها، إلا أن الطريقة التى تنفذ بها قد تمثل فعلاً غير مشروع دولياً، كانتهاك سيادة الدول، وحظر التدخل في شئونها، مع تحمل الدولة المسئولية الدولية عن الهجمات السيبرانية التى تنسب إليها، وتشكل خرقاً لإلتزام دولي، وأيضاً تقرير المسئولية الجنائية الفردية، والمسئولية الجنائية للقادة والرؤساء، عن إصدار أوامر بشن هجمات سيبرانية تشكل جرائم حرب([4]).

---

[1]) د. أمجد هيكل، المسئولية الجنائية الفردية الدولية أمام القضاء الجنائي الدولي، دار النهضة العربية، القاهرة، ٢٠٠٩، ط٢، ص٧٦.

[2]) د. صلاح الدين عبد العظيم محمد خليل، المسئولية الموضوعية في القانون الدولي العام، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ٢٠٠٢، ص ٣١.

[3]) د. محسن عبدالحميد أفكيرين، النظرية العامة للمسئولية الدولية عن النتائج الضارة عن أفعال لا يحظرها القانون الدولى ، دار النهضة العربية ، القاهرة ، ١٩٩٩، ص ٣١.

[4]) د. محمد عادل محمد عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق علي ممارسة التجسس وقت السلم: دراسة علي ضوء دليل "تالين" بشأن القانون الدولي المطبق علي العمليات السيبرانية ٢٠١٣-٢٠١٧، مرجع سابق، ص ٢٦٦.

وفيما يتعلق بمفهوم المسئولية الدولية عن الهجمات السيبرانية، وسواء أكان اللجوء إلي الهجمات السيبرانية محظوراً أم مقيداً وفقاً لأحكام القانون الدولي العام بصفة عامة والقانون الدولي الإنساني بصفة خاصة، فإن معظم أحكام الاتفاقيات والقواعد العرفية الدولية حددت المسئولية التى تقع علي الدولة سواء ارتكب التصرف من مؤسسات الدولة الرسمية أو غير الرسمية، بشرط أن يكون لديها السيطرة الكاملة علي ضبط تصرفات أجهزتها الحكومية أو أحد موظفيها أو الجماعات التى تدعمها الدولة([1]).

وقد عالج القانون الدولي مسألة استخدام الهجمات السيبرانية، بإعتبارها أحد أخطر التهديدات السيبرانية فيما يتعلق بالتأثير علي العلاقات الودية بين الدول، وبالتالي فإن المسئولية الدولية الناشئة على ذلك ستكون فى إطار تطبيق مبادئ ومفاهيم القانون الدولي الإنساني([2]) علي الهجمات السيبرانية، كمبدأ التمييزبين المقاتلين والمدنيين، والضرورة العسكرية والتناسب في استخدام القوة العسكرية، مع اعتبارأن بعض هذه الهجمات قد ترقي إلي مستوى هجوم مسلح تقليدي، أو استخداماً للقوة العسكرية، وتدخل ضمن نطاق الأسلحة الجديدة المنصوص عليها في المادة (٣٦) من البروتوكول الإضافي الأول لعام ١٩٧٧ الملحق باتفاقيات جنيف لعام ١٩٤٩، إذا كانت الآثار الناتجة عن استخدام الهجمات السيبرانية جسيمة كموت أشخاص أو إتلاف أو تدمير ممتلكات([3]).

وكذلك ينبغي تطبيق مبدأ حظر إستخدام وسائل وأساليب الحرب السيبرانية التى من شأنها أن تسبب أضراراً زائدة أو آلاماً لا مبرر لها، وذلك نظراً للتطور الهائل في أنظمة التسلح وأساليب القتال وما نتج عن استخدام الأسلحة الحديثة من خسائر وأضرار جسيمة على البشرية، حيث أصبح من الضرورى إخضاع الأطراف المتحاربة لنوع من القيود والضوابط في اختيار أساليب

---

[1]) طلال ياسين العيسي، عدى محمد عناب،المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مرجع سابق، ص٨٨.

[2]) د. سعيد سالم جويلي، المدخل لدراسة القانون الدولي الإنساني، مرجع سابق،ص١٣٧-١٣٨.

[3]) E. Shoshan, Applicability of international Law on Cyber espionage intrusions, Faculty of Law, Stockholm University Press, 2015, PP. 31: 32.

ووسائل القتال، بما يكفل التخفيف من المعاناة الإنسانية التى تسفر عنها الحروب والنزاعات المسلحة، وهذا ما نصت عليه المادة (٢٢) من اتفاقية لاهاي لعام ١٩٠٧ بأنه:" ليس للمتحاربين حق مطلق في اختيار وسائل إلحاق الضرر بالعدو". كما تضمنت المادة (٥٣) من البروتوكول الإضافي الأول لاتفاقيات جنيف لعام ١٩٧٧ علي أن حق الأطراف المتحاربة في اختيار أساليب ووسائل القتال ليس مطلقاً، ويحظر عليهم استخدام أى وسائل أو أساليبللقتال يكون من شأنها إحداث إصابات لا مبرر لها، أو إلحاق أضرار جسيمة على البشرية([1]).

وعلي جانب آخر، وهو القيام بهجمات سيبرانية في أوقات السلم كالتجسس السيبراني، فتقوم المسئولية الدولية في هذه الحالة بناء علي إنتهاك مبدأ عدم جواز التدخل فى الشئون الداخلية للدول([2]).

المطلب الثاني

الإشكاليات القانونية بشأن المسئولية الدولية عن إرتكاب هجمات سيبرانية

من الثابت في تحديد مسئولية الدول عن مشاركتها في النزاعات المسلحة التقليدية قد يكون أكثر يسراً، بالاستناد إلي معياري السيطرة الكاملة أو الفعالة، للتحقيق في هجمات قامت بها مجموعات مسلحة عابرة للحدود استخدمت أسلحة تقليدية أو غير تقليدية كالأسلحة الكيميائية، إلا أن الأمر يكون صعباً للغاية في إثبات المسئولية الدولية عن الهجمات السيبرانية، والتى تتم في الفضاء السيبراني لكونها تصرفات غير مادية ولا يمكن إثباتها بالطرق العادية، وهو ما يقف عائقاً أمام التنظيم الدولي المتعلق بإستخدام الهجمات السيبرانية([3]).

---

[4]) د.هالة أحمد الرشيدي، الإرهاب السيبراني، ماهيته وجهود مكافحته في ضوء التشريعات والقوانين الوطنية والدولية، مرجع سابق، ص١٦٣-١٦٤.

[1]) د. أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مرجع سابق، ص٦٤٣.

[2]) د. محمد صلاح عبد اللاه ربيع، الهجمات السيبرانية بين مشروعيتها كوسيلة للدفاع الشرعي وادانتها كاعتداء غير مشروع: دراسة تحليلية فى ضوء القانون الدولي، مرجع سابق، ص٤٢٠٨-٤٢٠٩.

وفى هذا الإطار، يثور التساؤل عن مدى إمكانية توجيه المسئولية الدولية ضد دولة أو مجموعة من الأفراد أو الكيانات من غير الدول، نسبت إليها تهم بإرتكاب هجمات سيبرانية، وذلك علي التالي بيانه:

أولاً: مسئولية الدول عن الهجمات السيبرانية:

أكدت المادة (٨) من مشروع مواد لجنة القانون الدولي بشأن مسئولية الدول لعام ٢٠٠١ علي مسئولية الدولة عن تصرفاتها إضافة إلي مسئوليتها عن تصرفات المجموعات التى تنتمي لها والمسيطرة عليها، وبالتالي فإن التصرفات التي تصدر عن أحد أجهزة الدولة التشريعية أو التنفيذية أو القضائية توجب مسئولية الدولة عن التصرفات الخاصة التى تصدر عنها والتى ينتج عنها أضرار جسيمة تصيب رعايا أو مصالح دولة أخري، أى أن الأساس في تحمل الدولة المسئولية الدولية هو معيار سيطرة الدولة علي التصرفات التى تصدر من أجهزتها أو الكيانات التى تدعمها الدولة([٣]).

وفى ذات الإطار، أقرت القاعدة رقم (٦) من دليل تالين"١" لعام ٢٠١٣، والقاعدة رقم (١٤) من دليل تالين "٢" بعنوان المسئولية القانونية للدول، بأن" تتحمل الدولة المسئولية القانونية الدولية للعمليات السيبرانية التى تنسب إليها والتى تشكل خرقاً لالتزام دولي"، وبالتالي فإن مفهوم الدولة المسئولة ينصرف إلي الدولة التى تنتهك التزاماً دولياً تجاه دولة أخري (الدولة المضرورة أو الضحية لهجوم سيبراني)، وتتحمل الدولة المسئولية الدولية عن الهجمات السيبرانية التى تنسب إليها وتشكل خرقاً لالتزام دولي، ويعد إسناد الفعل غير المشروع إلي الدول هو أساس تقرير المسئولية، وهو ما أكدته المادة (١) من مشروع مواد لجنة القانون الدولي بشأن مسئولية الدول لعام ٢٠٠١، وأن الدولة تتحمل المسئولية عن أفعالها غير

---

[٣]) د. أبو بكر محمد الديب، المسئولية الدولية تجاه استخدام الأسلحة الحديثة في النزاعات، مرجع سابق، ص٤٥.

المشروعة دولياً والتى تشكل خرقاً لالتزام دولي مع نسبته إليها وفقاً لأحكام القانون الدولي([1]).وتتمثل شروط المسئولية الدولية في مجال الهجمات السيبرانية فى التالي([2]):

(أ) ارتكاب الدولة فعلا غير مشروع دولياً:

ويقصد به أن تخالف الدولة التزاما دوليا مقرراً عليها، والذى قد يتمثل طبقاً للمادة (٣٨) من النظام الأساسي لمحكمة العدل الدولية، في التزام تعاهدى (اتفاقية دولية) أو قاعدة عرفية دولية أو أحد المبادئ العامة للقانون، وبالتالي تتحمل الدولة المسئولية الدولية إذا ارتكبت فعلا غير مشروع دوليا وذلك وفقاً لما تقضي به قواعد القانون الدولي حتى ولو كان القانون الداخلي يصف الفعل نفسه بأنه مشروع([3]).

وفى إطار الهجمات السيبرانية، قد يتمثل الفعل غير المشروع دولياً في قيام سفينة بهجمات سيبرانية ضد دولة ساحلية من داخل بحرها الإقليمي أو شن هجمات سيبرانية علي أهداف مدنية أثناء نزاع مسلح، أو إتاحة دولة بنيتهاالتحتية المعلوماتية لدول أو كيانات من غير الدول أو أفراد مما يتسبب في الإضرار بدول أخري([4]).

---

[1]) د. محمد عادل محمد عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق علي ممارسة التجسس وقت السلم: دراسة علي ضوء دليل "تالين" بشأن القانون الدولي المطبق علي العمليات السيبرانية ٢٠١٣-٢٠١٧، مرجع سابق، ص ٤٢١..

[2]) بن صابر بلقاسم، د. حيدرة محمد، الهجمات السيبرانية ومواجهتها في ضوء القانون الدولي المعاصر، مرجع سابق، ص٢٠٣.

[3]) د. أحمد أبو الوفا، المسئولية الدولية للدول واضعة الألغام في الأراضي المصرية،دراسة في إطار القواعد المنظمة للمسئولية الدولية وللألغام البرية، دار النهضة العربية،القاهرة، ٢٠٠٣، ص١٦-١٨.

[4]) M. J. SKLEROV, Solving the Dilemma of State Responses to Cyber-attacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent, Mil. L. Rev. 201, 2009, PP. 38:39.

(ب) نسبة التصرف إلي الدولة:

أكدته المواد من (٤:١٩) من مشروع مواد لجنة القانون الدولي بشأن مسئولية الدول لعام ٢٠٠١، إلي أن الشرط الثاني لتقرير المسئولية الدولية، بعد تحقق الفعل غير المشروع دولياً، هو إسناد هذا الفعل إلي الدولة، ويتحقق ذلك بصدور الفعل من السلطة التشريعية أو القضائية أو التنفيذية أو من أفراد عاديين، باعتبار أن هذه الفئات تمثل أجهزة الدولة أو تتصرف نيابة عنها، حتى لو تجاوزت تصرفاتها حدود ما رسمه القانون الداخلي أو خالفته، حيث تسأل الدولة عن الخطأ الذى يرتكبه موظفوها خلال مارستهم لأعمالهم، إذا كانوا مخولين سلطة تنفيذ أوامرها، كما تفترض مسئوليتها إذا كانت مخطئة في اختيارهم، وفي الرقابة عليهم، وفي التعليمات الصادرة إليهم([1]).

ومن الملاحظ أن العديد من الهجمات السيبرانية، تنفذ من قبل كيانات خاصة أو أفراد تستخدمهم الدول لهذا الغرض، وبالتالي فإن إسناد هذه الهجمات يواجه صعوبات، تتعلق بإشكالية تطبيق المعايير التقليدية لإثبات الصلة بين تلك الكيانات وشخص القانون الدولي، ومن اعتبارهم من أجهزة الدولة، أو أنهم قاموا بالعمل غير المشروع تحت سيطرة الدولة ورقابتها([2]).

١- المسئولية الدولية في حالة وجود علاقة قانونية بين القائم بالهجوم السيبراني والدولة:

وفقاً لنص المادة (١/٤) من مشروع مواد لجنة القانون الدولي بشأن مسئولية الدول لعام ٢٠٠١، بشأن مسئولية الدول عن قيام أحد الأجهزة التابعة لها بهجمات سيبرانية، والمتضمنة أنه "يعد تصرف أي جهاز من أجهزة الدولة فعلاً صادراً عن هذه الدولة بمقتضي القانون الدولي، سواء أكان الجهاز يمارس وظائف تشريعية أم تنفيذية أم قضائية أم أية وظائف أخري،

---

[1]) د. أحمد أبو الوفا، القانون الدولي والعلاقات الدولية، دار النهضة العربية،القاهرة، ٢٠٠٦، ص٥٠٨-٥٠٩.

[2]) د. محمد ربيع أحمد حسين، الهجمات السيبرانية واستخدام القوة في القانون الدولي المعاصر، مرجع سابق،ص ٣١٠-٣١١.

وأياً كان المركز الذي يشغله في تنظيم الدولة، وسواء أكانت صفته أنه جهاز من أجهزة الحكومة المركزية أم جهاز من أجهزة وحدة إقليمية من وحدات الدولة" وهو ذات الاتجاه الذى تضمنته القاعدة رقم (١٥) من دليل تالين "٢" بعنوان إسناد العمليات السيبرانية من قبل أجهزة الدولة، بأن العمليات السيبرانية التى تجريها أجهزة الدولة تسند إلي الدولة" ورغم الطبيعة السرية للهجمات السيبرانية، إلا أنه في بعض الحالات يكون من الواضح أن جهازً معيناً يضطلع بهجمات سيبرانية حكومية وعلي سبيل المثال وحدات الحرب الالكترونية للدول، ففى هذه الحالة يعد ما يصدر عن ذلك الجهاز من أفعال، صادراً عن الدولة وينسب إليها وإذا شكلت هذه الأفعال عملاً غير مشروع دولياً فإن الدولة هى التى تتحمل المسئولية الدولية([1]).

وفى هذا الإطار، أشارت القاعدة رقم (٧) من دليل تالين "١" بعنوان العمليات السيبرانية التى انطلقت من البنية التحتية السيبرانية الحكومية، بأنه "مجرد حقيقة أن عملية سيبرانية أنطلقت أو أنشئت من البنية التحتية السيبرانية الحكومية لا يكون دليلاً كافياً لاسناد العملية لتلك الدولة، بل هي إشارة إلي إرتباط الدولة المعنية بالعملية" كما قررت القاعدة رقم (٨) من دليل تالين "١" بعنوان العمليات السيبرانية التى توجه من خلال الدولة، بأن "حقيقة أن العملية السيبرانية وجهت من خلال البنية التحتية السيبرانية الواقعة في دولة (ما) لا يعد دليلاً كافياً لاسناد العملية لتلك الدولة". وهذا يعني أنه قد تسيطر دولة أو فرد أو كيان بخلاف الدولة علي بنية تحتية سيبرانية حكومية ويتم إستغلالها للقيام بهجمات سيبرانية، والمثال على ذلك أنه خلال عام ٢٠١٣ تم شن هجمات سيبرانية عدائية أسفرت عن تخريب مواقع الكترونية للحكومة الأوكرانية، وظهر أنها تنطلق من مركز الدفاع السيبراني لحلف الناتو، ثم قام المهاجم بتوجيه

[1]) د. أحمد أبو الوفا، المسئولية الدولية للدول واضعة الألغام في الأراضي المصرية، دراسة في إطار القواعد المنظمة للمسئولية الدولية وللألغام البرية، مرجع سابق، ص٢٠.

جزء من ذات الهجمات ضد موقع حلف الناتو، وجعل الأمر يظهر كما لو أن الحكومة الأوكرانية هي التى قامت به، وبالتالي يواجه الإسناد في مثل هذه الحالات إشكالية كبيرة([1]).

٢- المسئولية الدولية عن قيام كيانات أو أشخاص بخلاف أجهزتها بهجمات سيبرانية:

وفقاً لنص المادة (٥) من مشروع مواد لجنة القانون الدولي بشأن مسئولية الدول لعام ٢٠٠١ بشأن مسئولية الدول عن تصرفات الأشخاص أو الكيانات التى تمارس بعض اختصاصات السلطة الحكومية، والمتضمنة أنه" يعتبر فعلاً صادراً عن الدولة بمقتضي الدولي تصرف شخص أو كيان لا يشكل جهازاً من أجهزة الدولة بمقتضي المادة (٤) ولكن يخوله قانون تلك الدولة صلاحية ممارسة بعض اختصاصات السلطة الحكومية، بشرط أن يكون الشخص أو الكيان قد تصرف بهذه الصفة في الحالة المعنية"، وكذلك ما قررته القاعدة رقم (١٥) من دليل تالين "٢" بأن (العمليات السيبرانية التى يضطلع بها أشخاص أو كيانات مخولة بموجب القانون الوطني لممارسة عناصر السلطة الحكومية، تسند إلي الدولة). وبالتالي فإن تعاقد دولة مع شخص أو شركة خاصة وفقاً لتشريعاتها الداخلية، للقيام بهجمات سيبرانية عسكرية، فتسند الأفعال غير المشروعة دولياً التى قد تقع جراء هذه الهجمات إلي الدولة([2]).

وفقاً لنص المادة (٧) من مشروع مواد لجنة القانون الدولي بشأن مسئولية الدول لعام ٢٠٠١ بشأن حالة تجاوز هؤلاء الأشخاص أو الكيانات حدود السلطة أو مخالفة التعليمات التى كلفوا بها فإن الدولة تتحمل المسئولية أيضاً عن أفعالهم، والمتضمنة أنه" يعتبر فعلاً صادراً عن الدولة بمقتضي الدولي تصرف جهاز من أجهزتها أو شخص أو كيان مخول صلاحية ممارسة بعض اختصاصات السلطة الحكومية إذا كان الجهاز أو الشخص أو الكيان يتصرف بهذه

---

[1]) د. محمد عادل محمد عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق علي ممارسة التجسس وقت السلم: دراسة علي ضوء دليل "تالين" بشأن القانون الدولي المطبق علي العمليات السيبرانية ٢٠١٣-٢٠١٧، مرجع سابق، ص ٤٢٥-٤٢٦.

[2]) د. محمد ربيع أحمد حسين، الهجمات السيبرانية واستخدام القوة في القانون الدولي المعاصر، مرجع سابق،ص ٣١٣.

الصفة، حتى ولو تجاوز حدود سلطته أو خالف التعليمات".وبالتالي فإن إسناد إحدى الدول مهمة الدفع عن بنيتها السيبرانية إلي شركة خاصة فإذا تجاوزت الشركة في الدفاع باستخدام القرصنة أو المبادرة بالهجوم علي شبكات دول أخري، فإن هذه الأفعال تنسب إلي الدولة([1]).

وكذلك وفقاً لنص المادة (٩) من مشروع مواد لجنة القانون الدولي بشأن مسئولية الدول لعام ٢٠٠١ بشأن التصرفات التى يتم القيام بها في غياب السلطات الرسمية أو في حالة عدم قيامها بمهامها، والمتضمنة" يعتبر فعلاً صادراً عن الدولة بمقتضي القانون الدولي تصرف شخص أو مجموعة أشخاص إذا كان الشخص أو مجموعة الأشخاص يمارسون في الواقع بعض اختصاصات السلطة الحكومية في غياب السلطات الرسمية أو في حالة عدم قيامها بمهامها وفي ظروف تستدعي ممارسة تلك الاختصاصات"([2]).

٢- المسئولية الدولية في حالة خضوع القائم بالهجوم السيبراني للسيطرة الفعلية للدولة:

وفقاً لنص المادة (٨) من مشروع مواد لجنة القانون الدولي بشأن مسئولية الدول لعام ٢٠٠١، بشأن التصرفات التى يتم القيام بها بناء علي توجيهات الدولة أو تحت رقابتها، والمتضمنة أنه" يعد فعلاً صادراً عن الدولة بمقتضي القانون الدولي تصرف شخص أو مجموعة أشخاص إذا كان الشخص أو مجموعة الأشخاص يتصرفون في الواقع بناء علي تعليمات تلك الدولة أو بتوجيهات منها أو تحت رقابتها لدى القيام بذلك التصرف". وكذلك ما قررته القاعدة رقم (١٧) من دليل تالين "٢" بعنوان معيار السيطرة الفعلية بشأن الإسناد، بأنه" تسند الهجمات السيبرانية

---

[3]) د. أبو بكر محمد الديب، المسئولية الدولية تجاه استخدام الأسلحة الحديثة في النزاعات، مرجع سابق، ص٤٦.

[1]) المادة (٩) من مشروع مواد لجنة القانون الدولي بشأن مسئولية الدول عن الأفعال غير المشروعة دولياً لعام ٢٠٠١. راجع وثيقة:

-(GA Res 56/83 annex, UN Doc. A/RES/56/83, December 12, 2001.)

التى يقوم بها فاعل من غير الدول، إلي الدولة في حالتين وهما: المشاركة بموجب تعليماتها أو تحت توجيهها أو سيطرتها، وأن تعترف الدولة بالهجمات وتعتمدها بصفتها الآمرة بها([1]).

وفى هذا الإطار، أقرت محكمة العدل الدولية في قضية نيكاراجوا عام ١٩٨٦، معيار السيطرة الفعلية كأساس للإسناد، عند يتعلق الأمر بأفعال أشخاص مرتبطين بالدول، وأشارت إلي أن الولايات المتحدة الأمريكية تعد مسئولة عن بعض الأفعال التى قام بها مقاتلوا الكونترا، لقيامها بالتخطيط والتوجيه والدعم لهذه الأفعال، وباشرت من الناحية الفعلية درجة من الرقابة والسيطرة، تكفي لتبرير اعتبار هؤلاء المقاتلين قد تصرفوا بالنيابة عنها([2]). وبالتالي في حالة السيطرة الفعلية لدولة علي هجمات سيبرانية تقوم بها كيانات من غير الدول، فإن الدولة تكون مسئولة عن نتائج تلك الهجمات من أفعال غير مشروعة دولياً، بإعتبار أن هذه الكياناتتتصرف وفقاً لتعليمات الدولة وبإشرافها وتحت سيطرتها، ويعتبر هذا المعيار ضمانة لتجنب الحالات التى قد تلجأ فيها بعض الدول للتعاقد مع كيانات خاصة أو أفراد للقيام بهجمات سيبرانية وذلك لتجنب تقرير مسئوليتها الدولية عن تلك الهجمات، والمثال علي السيطرة الفعالة في مجال الهجمات السيبرانية، عندما تخطط دولة وتشرف من خلال شركة وطنية، علي إنتاج تحديثات ضارة لبرامج إلكترونية تتسبب في إتلاف البرامج المحملة علي أجهزة الحاسوب الحكومية لدولة أخرى، أو عندما تتعاقد دولة مع شركة خاصة لدعم قواتها المسحلة ثم إصدار أوامر لهذه الشركة للقيام بهجمات سيبرانية تجاه دولة أخرى، وذلك بتوجيه برامج ضارة لتدمير بعض النظم الإلكترونية لهذه الدولة، وفي الحالتين تسند أفعال الشركة إلي الدولة المسيطرة([3]).

---

[2]) طلال ياسين العيسي، عدى محمد عناب،المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مرجع سابق، ص٨٩.

[3]) د. أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مرجع سابق، ص٦٤٤.

[1]) د. أبو بكر محمد الديب، المسئولية الدولية تجاه استخدام الأسلحة الحديثة في النزاعات، مرجع سابق، ص٤٧.

وفيما يتعلق بإسناد الهجمات السيبرانية للدولة، في حالة اعترافها بالهجمات واعتمادها بصفتها، وفقاً للقاعدة (١٧) من دليل تالين "٢" فهو تأكيد ما تضمنته المادة (١١) من مشروع مواد لجنة القانون الدولي بشأن مسئولية الدول لعام ٢٠٠١، بشأن التصرفات التى تعترف بها الدولة وتعتبرها صادرة عنها، والمتضمنة أن" التصرف الذى لا ينسب إلي الدولة بموجب المواد السابقة يعتبر مع ذلك فعلاً صادراً عن هذه الدولة بمقتضي القانون الدولي إذا اعترفت هذه الدولة بذلك التصرف واعتبرته صادراً عنها وبقدر هذا الاعتراف والاعتبار"([1]).

وقد أقرت القاعدة رقم (٩) من دليل تالين "١" بعنوان التدابير المضادة([2])، أنه "يجوز للدولة التى أصيبت بفعل غير مشروع دولياً اللجوء إلي إتخاذ التدابير المضادة المتناسبة، بما في ذلك التدابير المضادة السيبرانية، ضد الدولة المسئولة". وبالتالي فإن آثار الهجمات السيبرانية العرضية، تعد عملاً يرتب المسئولية الدولية فيما لو أدت إلي إلحاق ضرر بالدولة المستهدفة، وهذا بدوره يجعل الدولة المضرورة قادرة علي اتخاذ أي تدابير من شأنها رد الهجوم القائم ضدها حتى لو لجأت إلي التدابير المضادة السيبرانية، وتنحضر الممارسة الدولية العملية في خيار رد السيئة بالمثل وتعرف مسودة مسئولية الدول عن الأعمال غير المشروعة دولياً، أعمل رد السيئة بالمثل بالأعمال غير الودية، التى لا تتعارض مع أى التزام دولي تجاه الدولة المستهدفة بها حتى وإن كانت رداً علي فعل غير مشروع دولياً، وقد تشمل أعمال رد السيئة بالمثل حظر أو تقييد العلاقات الدبلوماسية أو الاتصالات أو سحب برامج المساعدة الطوعية.

ومن الممارسة الدولية لأعمال رد السئية بالمثل، ما قامت به الولايات المتحدة الأمريكية ضد روسيا في ديسمبر ٢٠١٦، علي خلفية تدخل روسيا في الانتخابات الأمريكية، حيث أصدر الرئيس أوباما مرسوماً تنفيذياً تضمن فرض عقوبات ضد ثمانية كيانات وأشخاص روسية

---

[2]) د. محمد عادل محمد عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق علي ممارسة التجسس وقت السلم: دراسة علي ضوء دليل "تالين" بشأن القانون الدولي المطبق علي العمليات السيبرانية ٢٠١٣-٢٠١٧، مرجع سابق، ص٤٣٠.

[3]) د. محسن عبدالحميد أفكيرين، النظرية العامة للمسئولية الدولية عن النتائج الضارة عن أفعال لا يحظرها القانون الدولى، مرجع سابق، ص ٤٥.

متهمة في الهجمات السيبرانية التى استهدفت التأثير علي الانتخابات الأمريكية، وفي مارس ٢٠١٨ أعلنت وزارة الخزانة الأمريكية عن فرض عقوبات علي خمسة كيانات روسية وتجميد أصول ١٩ مواطناً روسيا بموجب قانون مكافحة خصوم أمريكا (CAATSA) علي خلفية اتهامهم في الهجمات السيبرانية عليى الحزب الديمقراطي الأمريكي ٢٠١٦ واتهامهم أيضاً في الهجوم السيبراني علي نوتبيتيا (NotPetya) في فبراير ٢٠١٨ والذى تسبب في إحداث خسائر جسيمة تقدر بمليارات الدولارات في آسيا وأوروبا والولايات المتحدة، كما تسبب في تعطيل حركة الشحن العالمي والتجارة العالمية([1]).

وفي الإطار ذاته، أشارت محكمة عدل الاتحاد الأوروبي بمناسبة حكمها الصادر في ١١ مارس ٢٠٠٣، بأن التدابير والإجراءات الضرورية لحماية الأمن القومي هى تدابير متنوعة ويصعب حصرها، ومن الممكن أن تكون ذات طبيعة عسكرية حينما تدافع الدولة عن استقلالها السياسي وسيادتها وسلامة أراضيها ضد العدوان المسلح أو ضد العمليات الإرهابية المعرضة لها، وقد تكون تدابير اقتصادية كوقف أو تقييد الصادرات المصدرة إلي الخارج أو الواردات القادمة منه، وتدابير أخري تتعلق بحقوق الإنسان وحرياته الأساسية وغيرها من المصالح الأساسية أو الحيوية الأخري، كما أكدت محكمة العدل الدولي في حكمها الصادر في ٢٧ يونيو ١٩٨٦ بشان قضية الأنشطة العسكرية وشبه العسكرية في نيكارجوا وضدها، علي المفهوم الواسع للأمن القومي وللتدابير الضرورية لحمايته، عندما أشارت إلي أنه يصعب المنازعة في أن الدفاع الشرعي ضد العدوان المسلح يعد من التدابير الضرورية لحماية المصالح الحيوية في مجال الأمن القومي للدولة، ولكن مفهوم هذه المصالح أوسع بالتأكيد من مفهوم العدوان المسلح([2]).

---

[1]) د. شريف نسيم قلته بخيت،الهجمات الإلكترونية وحق الدفاع الشرعي للدول في القانون الدولي، مرجع سابق، ص١٩٥-١٩٦.

[2]) د. محمد صافي يوسف، تدابير حماية الأمن القومي كاستثناء علي تطبيق قواعد القانون الدولي العام،، المجلة المصرية للقانون الدولي، الجمعية المصرية للقانون الدولي، المجلد السادس والستون، العدد ٢٠١٠،٦٦، ص١٦٩-١٧٠.

وترتيباً علي ما تقدم، يمكن القول أنه لا يمكن أن يتوافر إسناد قاطع في مجال الهجمات السيبرانية أو أدلة كافية علي تورط دولة ما، ولا يتبقي أمام الدولة الضحية لهجوم سيبراني، في أغلب الأحيان، إلا اللجو إلي اعتماد تدابير أمنية محكمة للنظم السيبرانية، ومطالبة الدولة التى انطلق منها الهجوم بإجراء تحقيقات ومحاكمة مرتكبي الهجمات السيبرانية، أو إعمال قواعد المسئولية المفترضة، التى أقرتها اتفاقية مجلس أوروبا (بودابست) لعام ٢٠٠١، بشأن الجرائم الإلكترونية، والتى تقضي بإسناد الهجمات السيبرانية إلي الدولة التى تنطلق منها، بصرف النظر عما إذا هناك تموية أو خداع بشأن هذا المكان، وذلك استناداً إلي إخفاق الدولة في الالتزام بواجب منع استخدام أراضيها لمهاجمة الدول الأخري أو فشلها في التأكد من ذلك أو ملاحقة المهاجمين([1]).

ثانياً: المسئولية الفردية عن الهجمات السيبرانية:

يعتبر ترسيخ مبدأ المسئولية الجنائية الفردية عن الانتهاكات الجسيمة لقواعد القانون الدولي الإنساني من أهم التطورات التي لحقت بهذا القانون([2])، كما يعد النظام الأساسي للمحكمة الجنائية الدولية الوثيقة الدولية الأولي التي دونت المبادئ العامة لقواعد المسئولية الدولية الجنائية وهذا في إطار معاهدة متعددة الأطراف حيث تظهر المسئولية الشخصية الجنائية عند ارتكاب الأفعال الموصوفة كجرائم دولية في المادة (٥) من النظام الأساسي([3]).

وقد أقرت المادة (٢٥) من النظام الأساسي للمحكمة الجنائية الدولية، مبدأ المسئولية الجنائة الفردية، أى مسئولية الأفراد عن الجرائم التى تدخل في اختصاص المحكمة، وللمحكمة اختصاص على الأشخاص الطبيعيين، وهى بهذا أخذت بالرأي السائد في الفقه والقضاء

---

[1] V. J. PROULX, Babysitting Terrorists: Should States Be Strictly Liable for Failing To .Prevent Transborder Attacks?. In International Law, 2018, PP. 406- 447.

[2] بن صابر بلقاسم، د. حيدرة محمد، الهجمات السيبرانية ومواجهتها في ضوء القانون الدولي المعاصر، مرجع سابق، ص٢٠٤.

[3] د. محمود شريف بسيوني، المحكمة الجنائية الدولية، نشأتها ونظامها الأساسي، ط١، مطابع روز اليوسف الجديدة، القاهرة، ٢٠٠١، ص١٦١.

الدوليين بأن الفرد وحده هو محل المسئولية الجنائية لأنه القادر على خرق القانون وارتكاب الجرائم التي تكون سبب للمسئولية الجنائية([1]).

والواضح من خلال نص المادة (٢٥) أن المحكمة تختص بمحاكمة الأشخاص الطبيعيين فالشخص الطبيعي يقع على عاتقه المسئولية بصفة فردية عن الجرائم المرتكبة والداخلة في اختصاص المحكمة، كما أن النظام الأساسي سعياً منه لعدم إفلات المجرمين من العقاب نص على المساهمة الجنائية، وهي الأمر أو الحث وحتى الإغراء على ارتكاب إحدى الجرائم الداخلة في اختصاص المحكمة، وتظهر المساهمة الجنائية في حالة تقديم العون أو التحريض أو المساعدة بأي شكل لتسهيل ارتكاب الجريمة الدولية([2]).

كما أكدت دائرة الاستئناف للمحكمة الجنائية الدولية ليوغسلافيا السابقة علي ذات المبدأ، عندما أقرت مسئولية الفرد الجنائية عن التعذيب، مع عدم اشتراط كونه موظفاً عاماً([3]).

وفيما يتعلق بالهجمات السيبرانية، فقد تناولت القاعدة (٨٤) من دليل تالين "٢" المسئولية الجنائية الفردية، عن الهجمات السيبرانية التى قد تشكل جرائم حرب، أو انتهاكات جسيمة لقانون النزاعات المسلحة، وأن هذه الجرائم تجسد الانتهاكات الجسيمة، وكذلك المادة (٨٥) من البروتوكول الإضافي الأول لعام ١٩٧٧ بشأن جرائم الحرب، والمادة (٨) من نظام روما الأساسي، بإعتبار أن الأفعال التى ترتكب بوسائل إلكترونية يمكن اعتبارها جرائم حرب، لأن قانون النزاعات المسلحة ينطبق علي أساليب ووسائل الحرب الجديدة، حتى التى لم تكن قد ظهرت وقت صياغة هذا القانون([4]).

---

[4]) د.عمر محمود المخزومي، القانون الدولي الإنساني في ضوء المحكمة الجنائية الدولية، دار الثقافة للنشر والتوزيع، عمان، الأردن، ٢٠٠٩، ص٢٥٩-٢٦٠.

[5]) د. أمجد هيكل ، المسئولية الجنائية الفردية الدولية أمام القضاء الجنائي الدولي، مرجع سابق ، ص٥٣٠.

[6] ICTY, Prosecutor v. Kunarac, Kovac and Vukovic, Case IT-96-23 & IT-96-23/1-A, Judgment (Appeals Chamber), 12 June 2002, para. 148.

[1]) د. محمد عادل محمد عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق علي ممارسة التجسس وقت السلم: دراسة علي ضوء دليل "تالين" بشأن القانون الدولي المطبق علي العمليات السيبرانية ٢٠١٣-٢٠١٧، مرجع سابق، ص ٤٣٣-٤٣٤.

ثالثاً: المسئولية الجنائية للقادة والرؤساء عن الهجمات السيبرانية:

تعد مسئولية القادة والرؤساء من أهم قواعد المسئولية الجنائية الفردية الدولية، واستقرت أحكام القضاء الجنائي الدولي على التأكيد على مبدأ عدم الاعتداد بالحصانة كسبب للإفلات من العقاب عن الجرائم الدولية ولعل المبادئ التي أسستها محكمة نورمبرج كانت الأولي في هذا الصدد، إذ نصت المادة السابعة من النظام الأساسي لمحكمة نورمبرج" إن المركز الرسمي للمتهمين سواء بصفة رؤساء دول أم بصفة موظفين كبار لن يؤخذ بعين الاعتبار كعذر أو كسبب مخفف للعقوبة"([1]).

وقد قررت المادة (٢/٨٦) من البروتوكول الإضافي الأول لعام ١٩٧٧، مبدأ المسئولية الجنائية الفردية للرؤساء عن أى خرق لأحكام هذه الاتفاقيات من قبل مرؤوسيهم، إذا كان هؤلاء الرؤساء يعلمون أو توافرت لديهم معلومات فى ذلك الوقت، وفشلوا في اتخاذ التدابير الممكنة لمنع هذا الانتهاك، كما وسعت أحكام المادة (١/٨٧) من البروتوكول، من مسئولية الرؤساء لتشمل الأشخاص الآخرين الخاضعين لسيطرتهم([2]).وقد نص النظام الأساسي للمحكمة الجنائية الدولية علي قواعد هذه المسئولية في المادتين (٢٧-٢٨) منه، فجاءت المادة (٢٧) بعنوان " عدم الاعتداد بالصفة الرسميةلدفع المسئولية، في حين جاءت المادة (٢٨) بعنوان "مسئولية القادة والرؤساء الآخرين"([3]).

١- القاعدة العامة: عدم الاعتداد بالصفة الرسمية لدفع المسئولية.

نصت الفقرة الأولي من المادة (٢٧) من النظام الأساسي للمحكمة الجنائية الدولية علي أنه:" يطبق هذا النظام الأساسي على جميع الأشخاص بصورة متساوية دون تمييز بسبب الصفة الرسمية وبوجه خاص فإن الصفة الرسمية للشخص سواء كان رئيسا لدولة أو لحكومة أو عضو في حكومة أو برلمان أو ممثلا منتخباً أو موظفاً حكومياً لا تعفيه بأي حال من الأحوال

---

[2]) د. عبدالفتاح بيومي حجازي، قواعد أساسية في نظام محكمة الجزاء الدولية، دار الكتب القانونية، مصر، ٢٠٠٧، ص١٤٠-١٤١.

[3]) د. محمد عبد المنعم عبد الغني، القانون الدولي الجنائي دراسة في النظرية العامة للجريمة الدولية، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٨، ص٢١٤.

[4]) د. أمجد هيكل، المسئولية الجنائية الفردية الدولية أمام القضاء الجنائي الدولي، مرجع سابق، ص٥٣٦.

من المسئولية الجنائية بموجب هذا النظام الأساسي كما أنها لا تشكل في حد ذاتها سببا لتخفيف العقوبة".

كما نصت الفقرة الثانية من المادة (٢٧) علي أنه" لا تحول الحصانات أو القواعد الإجرائية الخاصة التي قد ترتبط بالصفة الرسمية للشخص سواء كانت في إطار القوانين الوطنية أو الدولية دون ممارسة المحكمة اختصاصها على هذا الشخص"([1]).

٢- أحكام مسئولية القادة العسكريين والرؤساء المدنيين:

نصت المادة (١/٢٨) من النظام الأساسي للمحكمة الجنائية الدولية، علي مسئولية القادة العسكريين بأنه:" يكون القائد العسكري أو الشخص القائم فعلاً باعمال القائد العسكري مسئولا مسئولية جنائية عن الجرائم التى تدخل في اختصاص المحكمة والمرتكبة من جانب قوات تخضع لسلطته وسيطرته الفعليتين، نتيجة لعدم ممارسة القائد العسكري أو الشخص سيطرته علي هذه القوات ممارسة صحيحة:

أ-إذا كان القائد العسكري أو الشخص قد علم أو يفترض أن يكون قد علم بسبب الظروف االسائدة، بأن القوات ترتكب أو علي وشك ارتكاب هذه الجرائم.

ب-إذا لم يتخذ القائد العسكري أو الشخص جميع التدابير اللازمة في حدود سلطته لمنع أو قمع ارتكاب هذه الجرائم أو لعرض المسألة علي السلطات المختصة للتحقيق والمقاضاة".

وبالتالي فرضت هذه المادة مسئولية القائد العسكري عن الجرائم التى ترتكبها القوات التى تحت سيطرته الفعلية([2]).

أما بشأن مسئولية الرؤساء المدنيين، فنصت المادة (١/٢٨) من النظام الأساسي للمحكمة الجنائية الدولية، على أن: " يسأل الرئيس عن جرائم مرؤوسيه الخاضعين لسلطته وسيطرته الفعليين، في الحالات التالية:

---

[1]) د.حازم محمد عتلم، المحكمة الجنائية الدولية الخاصة بلبنان مقارنة بالمحاكم الجنائية الدولية والمدولة والمختلطة الأخرى مع دراسة خاصة لمسئولية القادة، المجلة المصرية للقانون الدولي، العدد ٧١، ٢٠١٥، ص٣٨.

[2]) د. أمجد هيكل، المسئولية الجنائية الفردية الدولية أمام القضاء الجنائي الدولي، مرجع سابق، ص٥٣٨-٥٤٠.

أ–إذا كان قد علم أو تجاهل عن وعي أية معلومات تبين بوضوح أن مرؤوسيه يرتكبون أو علي وشك أن يرتكبوا هذه الجرائم.

ب– إذا تعلقت الجرائم بأنشطة تتدرج في إطار المسئولية والسيطرة الفعليتين للرئيس.

ج– إذا لم يتخذ جميع التدابير اللازمة والمعقولة في حدود سلطته لمنع أو قمع ارتكاب هذه الجرائم أو لعرض المسألة علي السلطات المختصة للتحقيق والمقاضاة([1]).

وفيما يتعلق بالهجمات السيبرانية، فقد تناولت القاعدة رقم (٢٤) من دليل تالين "١"، والقاعدة رقم (٨٥) من دليل تالين "٢" بعنوان المسئولية الجنائية للقادة والرؤساء، أنه:

أ–يتحمل القادة والرؤساء الآخرون المسئولية الجنائية لإصدار الأوامر بشن العمليات السيبرانية التى تشكل جرائم حرب.

ب–كذلك يكون القادة مسؤولين في حالة علمهم أو وجوب علمهم بسبب الظروف السائدة في ذلك الوقت، بأن مرؤوسيهم كانوا يرتكبون، أو علي وشك إرتكاب، أو أرتكبوا جرائم حرب، وفشل القائد في إتخاذ جميع التدابير المعقولة والمتاحة لمنع إرتكاب هذه الجرائم أو معاقبة المسؤولين عنها([2]).

وترتيباً علي ما تقدم، فإنه إذا توافرت شروط المسئولية الدولية، فلابد أن تترتب عليها بعض الآثار في حق الدولة المنسوب إليها الفعل غير المشروع دولياً، وتتمثل هذه الآثار، في إصلاح الضرر والترضية، وإصلاح الضرر يكون بإعادة الحال إلي ما كانت عليه قبل ارتكاب الفعل غير المشروع دولياً أو، إذا تعذر ذلك، يكون عن طريق التعويض بدفع مبلغ يساوى التنفيذ العيني ودفع التعويضات عن الأضرار التى قد لا يغطيها التنفيذ العيني أو المبلغ الذى يحل محله، ويتم اللجوء إلي الترضية في الأحوال التى يصيب الدولة فيها ضرر معنوى أو أدبي،

---

[1]) Van Sliedregt, E.: The criminal responsibility of individuals for violations of international humanitarian law, The Hague: T.M.C. Asser Press, 2003, pp186-189.

[2]) د. محمد عادل محمد عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق علي ممارسة التجسس وقت السلم: دراسة علي ضوء دليل "تالين" بشأن القانون الدولي المطبق علي العمليات السيبرانية ٢٠١٣–٢٠١٧، مرجع سابق، ص ٤٣٥.

فتحاول الدولة الأخري التى نسب إليها الفعل غير المشروع إصلاح خطئها عن طريق وسيلة أو أكثر من الوسائل التالية وهي: قيام الدولة المسئولة بتقديم اعتذار رسمي، أو إرسال مذكرات دبلوماسية للإعتراف بالانتهاك أو التعبير عن الأسف، وقد طبقت محكمة العدل الدولية وسيلة الترضية في قضية مضيق كورفو عام ١٩٤٩، حينما ذهبت إلي القول بأن الفعل الذى قامت به بريطانيا في مياه ألبانيا دون موافقة هذه الأخيرة، يعتبر مخالفة أو انتهاكاً لسيادة ألبانيا، وتضيف المحكمة أن هذه الملاحظة تشكل في حد ذاتها ترضية ملائمة لحكومة ألبانيا، وهذا يعني أن الترضية تتم لمجرد أن أعلي هيئة قضائية دولية أكدت علي وجود انتهاك للسيادة الألبانية([1]).

[1]) د. أحمد أبو الوفا، المسئولية الدولية للدول واضعة الألغام في الأراضي المصرية، دراسة في إطار القواعد المنظمة للمسئولية الدولية وللألغام البرية، مرجع سابق، ص٢٤-٢٥، وكذلك د. وائل أحمد علام، مركز الفرد في النظام القانوني للمسئولية الدولية، دار النهضة العربية، القاهرة،٢٠٠١، ص٣٧.

الخاتمة

علي الرغم من التطور الهائل لثورة تكنولوجيا المعلومات والاتصالات، إلا أنها في ذات الوقت جعلت المجتمع الدولي يواجه تحديات جديدة مرتبطة بهذا التطور، فقد ظهرت الهجمات السيبرانية كأحد أهم هذه التحديات، لما تشكله من تداعيات خطيرة علي الأمن القومي للدول حول العالم وتهديداً للسلم والأمن الدوليين، وخصوصاً أن عملية التعاون الدولي لمواجهة الهجمات السيبرانية تقابلها العديد من الإشكاليات، من أبرزها: تضارب المصالح وعدم وجود تنسيق قانوني كاف بين مختلف الدول، وقيام بعضها بإستخدام الهجمات السيبرانية كسلاح ضد البعض الآخر لاسيما في أوقات النزاعات المسحلة، وعدم وجود استراتيجية دولية شاملة أو إتفاقاً دولياً ملزماً لكافة الدول لمكافحة الهجمات السيبرانية علي الصعيد العالمي، وكذلك ضعف البنية التشريعية الداخلية في العديد من الدول لمواجهة الهجمات السيبرانية، وهو ما أدى إلي اتساع نطاق التحدى العالمي الذى تمثله الهجمات السيبرانية، والخلاف حول مدى إمكانية تطبيق قواعد القانون الدولي عليها.

وكما توصلنا من خلال هذه الدراسة إلي أن الهجمات السيبرانية تعد واحدة من أهم التحديات المعاصرة التى تواجه المجتمع الدولي، فالتطورات التكنولوجية المختلفة تتطلب مواكبة التشريعات القانونية لها، سواء علي المستوى الداخلي للدول أو علي المستوى الدولي، إلا أن الهجمات السيبرانية تفتقر إلي الأطر القانونية الصارمة للتعامل معها، والتنظيمات والقوانين الدولية المعاصرة وإن كانت تنطبق علي استخدام الهجمات السيبرانية إلا أنها لا تغطي كل أشكال وتحديات الهجمات السيبرانية، وانتهيت من خلال هذه الدراسة إلي عدد من النتائج والتوصيات، وذلك على النحو التالي:

أولا: النتائج:

١- أن السبب الحقيقي وراء عدم التوصل لإتفاقية دولية تنظم مسألة الهجمات السيبرانية، يرجع إلي المصالح الدولية للدول العظمي الرائدة في مجال أمن الفضاء السيبراني، الأمر الذى يستلزم ضرورة تضافر جهود المجتمع الدولي لإنجاز إتفاقية دولية ملزمة، تنظم مسألة

استخدام الهجمات السيبرانية، من حيث التكييف القانوني لها وصورها والمسئولية الدولية الناشئة عن الهجمات السيبرانية.

٢- تشكل تحديات وصعوبات الإسناد وخصوصية الهجمات السيبرانية، عائقاً كبيراً أمام إمكانية ممارسة حق الدفاع الشرعي رداً علي الهجمات السيبرانية التى تتم في وقت السلم بواسطة كيانات من غير الدول، بإعتبارها هجوماً مسلحاً أو إعتبارها خرقاً لمبدأ عدم التدخل في الشئون الداخلية للدول والذى يسمح فقط بإستخدام التدابير المضادة والوسائل السلمية الأخري في مواجهتها.

٣- عدم إمكانية تطبيق العديد من قواعد القانون الدولي الحالية ومبادئ الأمم المتحدة ذات الصلة علي الهجمات السيبرانية، وذلك في ضوء ما يواجهه التطبيق العملي للكثير من تلك القواعد العرفية وليكن قانون استخدام القوة وحق الدفاع الشرعي ومسألة السيادة – العديد من الصعوبات بالقدر الذي يستلزم التكييف المرن للغاية لتلك القواعد أو استبدالها بقواعد عرفية جديدة لتتلاءم مع قواعد القانون الدولي الحالية وميثاق الأمم المتحدة، كما أن إخضاع الهجمات السيبرانية للقانون الدولي الإنساني مسألة في غاية الصعوبة.

٤- يعد استيفاء مبادئ الضرورة العسكرية والتناسب والتمييز في إطار ممارسة حق الدفاع الشرعي رداً علي الهجوم السيبراني، من أكثر الإشكاليات التى تواجه ممارسة هذا الحق ومن الصعب إيجاد حل ملائم له، وهو أمر متروك للممارسة الدولية رغم التداعيات الخطيرة الناتجة عن استخدام القوة دون توافر وسائل الإثبات الكافية.

٥- إن الحاجة إلي التعاون الدولي بين الدول والمنظمات الدولية والإقليمية والكيانات الأخري، يعد أمراً بالغ الضرورة في مواجهة الهجمات السيبرانية، وخاصة أن الحكومات تحتاج إلي ضمان حماية بنيتها السيبرانية التحتية بشكل جيد ضد الهجمات السيبرانية، وأن الأطر القانونية والسياسية تسمح لها بمنع الهجمات السيبرانية المحتملة وردعها والتخفيف من حدتها بشكل فعال.

ثانيا: التوصيات:

١- يجب أن تنظر لجنة القانون الدولي التابعة للأمم المتحدة في إمكانية تأسيس اتفاقية دولية للفضاء السيبراني أو بروتوكول للأمم المتحدة بشأن الأمن السيبراني ومكافحة الهجمات

السيبرانية، وضرورة تحديد استراتيجيات وطنية ودولية تحتوى علي قواعد ومبادئ قانونية كافية للتصدي للإشكاليات والتحديات القانونية الهائلة الناتجة عن استخدام الهجمات السيبرانية، وكذلك النظر في التدابير الاستباقية التى يجب اتخاذها قبل الهجوم السيبراني وتجنب الانتهاكات الأمنية، وضمان ممارسة دولية مشروعة وسلمية في الفضاء السيبراني، قائمة علي التحديد الصريح للحقوق والإلتزامات في الفضاء السيبراني.

٢- يجب أن تنشئ الأمم المتحدة جهازاً خاصاً بحالات استخدام الهجمات السيبرانية التى تتم في إطار العلاقات الدولية بين الدول، ويختص هذا الجهاز بتطبيق القواعد القانونية علي هذه النزاعات، وتتضمن إجراءات وآليات واضحة للتعاون والتنسيق وتبادل المعلومات ذات الصلة بالتهديدات السيبرانية وذلك بالتنسيق مع مجلس الأمن الدولي، وكذلك مراقبة الهجمات التى تحدث في الفضاء السيبراني، ومساعدة الدول النامية علي التصدي لتلك الهجمات، كالإخطار بحدوث هجوم معين أو أن هجوماً علي وشك الوقوع بما يحقق تعاوناً دولياً فعالاً لمواجهة تلك الهجمات، وكذلك بالتعاون مع الاتحاد الدولي للإتصالات بإعتباره أحد وكالات الأمم المتحدة المتخصصة في مجال تكنولوجيا المعلومات والإتصالات، بغرض حماية المجتمع الدولي من العواقب الإنسانية الجسيمة لهذه الهجمات.

٣- يجب أن يتم تطوير ومراجعة إتفاقيات وقواعد القانون الدولي الإنساني الحالية أو وضع قواعد عرفية جديدة قابلة للتطبيق علي حالات استخدام الهجمات السيبرانية في النزاعات المسلحة الدولية وغير الدولية بما يناسب الطبيعة التقنية الخاصة لهذه الهجمات، وإدخال الهجوم السيبراني العدواني ضمن صور العدوان بهدف التغلب علي التحديات القانونية الصعبة في الفضاء السيبراني كإشكالية السيادة، وإشكالية تطبيق مبادئ التمييز والتناسب والاحتياطات أثناء الهجوم والتى تسبب الضرر للمدنيين والأعيان المدنية دون تمييز، والحفاظ علي الأمن القومي للدول، وتحقيق السلم والأمن الدوليين.

٤- ضرورة الحاجة إلي خلق ثقافة عالمية للأمن السيبراني، والإقرار بالمسئولية الدولية الجنائية الفردية عن الجرائم المرتكبة بواسطة استخدام الهجمات السيبرانية لما تشكله من تهديد مباشر للسلم والأمن الدوليين، وذلك بهدف حماية السكان المدنيين من مخاطر الهجمات

السيبرانية وخاصة إذا ما نظرنا إلي آثار هذه الهجمات وتبعاتها علي السكان المدنيين والبيئة فيما لو تم تنفيذها علي منشأة نووية أو مصادر الطاقة كشبكة الكهرباء والمياه.

٥- ضرورة اضطلاع مجلس الأمن بدوره الرئيسي في تحديد موقفه من استخدام الهجمات السيبرانية المسلحة ومدى اعتبارها تهديداً للسلم والأمن الدوليين أو كأحد أعمال العدوان، بإعتبار أن تلك الخطوة تعد استرشادية بشأن تكييف الهجوم السيبراني المسلح، وتحديد مدى مشروعية ممارسة حق الدفاع الشرعي ضد الهجمات السيبرانية.

٦- يجب على المجتمع الدولي التأكيد علي انطباق أحكام وقواعد القانون الدولي الإنساني علي استخدام الهجمات السيبرانية خلال النزاعات المسلحة الدولية وغير الدولية، ويظل أى لجوء من الدول إلي القوة (الهجمات السيبرانية) محكوماً بميثاق الأمم المتحدة وقواعد القانون الدولي العرفي ذات الصلة، وذلك إعمالاً لمبدأ حظر استخدام القوة أو التهديد بإستخدامها في العلاقات الدولية.

قائمة المراجع

أولاً: المراجع العربية:

١) د. إبراهيم السيد رمضان، استجابة الأطر القانونية للقضايا العابرة للحدود، مجلة السياسة الدولية، المجلد ٥٧، العدد ٢٢٨، أبريل ٢٠٢٢.

٢) د. أبو بكر محمد الديب، المسئولية الدولية تجاه استخدام الأسلحة الحديثة في النزاعات، مجلة السياسة الدولية، المجلد ٥٨، العدد ٢٣٤، أكتوبر ٢٠٢٣ .

٣) د. أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، كلية القانون جامعة بابل، العراق، العدد الرابع،السنة الثامنة، ٢٠١٦.

٤) د. أحمد عبيس نعمة الفتلاوي، د. أزهر عبد الأمير الفتلاوي، المسؤولية الناشئة عن إستخدام وسائل القتال الفتاكة في نشر الأوبئة (الهجمات السيبرانية في مقابل جائحة كورونا أنموذجا)، مجلة الحقوق الجامعة المستنصرية – كلية القانون، المجلد (١٣)، العدد(٤١)،٢٠٢١.

٥) د. أحمد عبيس نعمة الفتلاوي، زهراء عماد محمد كلنتر، تكييف الهجمات السيبرانية في ضوء القانون الدولي، مجلة الكوفة للعلوم القانونية والسياسية، العراق، المجلد (١٣)، العدد(٤٤)،٢٠٢٠.

٦) د. أحمد زكريا الباسوسي، الجهود الدولية لمكافحة الهجمات السيبرانية علي قطاع الطاقة: حالات مختارة، مجلة كلية الاقتصاد والعلوم السياسية، جامعة القاهرة، المجلد (٢٤)، العدد (٤) أكتوبر ٢٠٢٣ .

٧) د. أحمد أبو الوفا، المسئولية الدولية للدول واضعة الألغام في الأراضي المصرية،دراسة في إطار القواعد المنظمة للمسئولية الدولية وللألغام البرية، دار النهضة العربية،القاهرة، ٢٠٠٣.

٨) د. أميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة البحوث الفقهية والقانونية، كلية الشريعة والقانون بدمنهور، جامعة الأزهر، العدد الخامس والثلاثون، الجزء الثالث،٢٠٢٠.

٩) د. أمجد هيكل، المسئولية الجنائية الفردية الدولية أمام القضاء الجنائي الدولي، دار النهضة العربية، القاهرة، ط٢،٢٠٠٩.

١٠) د.أبو الخير أحمد عطية، حماية السكان المدنيين والأعيان المدنية إبان النزاعات المسلحة، دار النهضة العربية، ١٩٩٨.

١١) د. إيهاب خليفة، القوة الإلكترونية .. كيف يمكن أن تدير الدول شؤونها في عصر الإنترنت؟ "الولايات المتحدة نموذجاً"، الطبعة الأولي، العربي للنشر والتوزيع، القاهرة، ٢٠١٧ .

١٢) د. إيمان أحمد علام، الهجمات السيبرانية "الحرب الإلكترونية" واستخدام القوة المسلحة في القانون الدولي العام: الاستغلال السيبراني، مجلة الدراسات القانونية والاقتصادية، كلية الحقوق جامعة مدينة السادات، المجلد (٩)، العدد (٤)، ديسمبر ٢٠٢٣.

١٣) د.إسراء أحمد إسماعيل، الحروب السيبرانية.. تهديد لأمن الدول بدون اشتباكات عسكرية، مجلة السياسة الدولية، ملحق تحولات استراتيجية،التكنولوجيا وتحولات الحروب، المجلد ٥٧، العدد ٢٢٨، أبريل ٢٠٢٢.

١٤) د. إسلام رمضان هديب، مفهوم الحرب السيبرانية في ظل القانون الدولي وتحديد خصائصها والنتائج المترتبة عليها، مجلة البحوث القانونية والاقتصادية، كلية الحقوق جامعة بني سويف، المجلد (٣٦)، العدد (١)، يناير ٢٠٢٤.

١٥) بن صابر بلقاسم، د. حيدرة محمد، الهجمات السيبرانية ومواجهتها في ضوء القانون الدولي المعاصر، مجلة حقوق الإنسان والحريات العامة، الجزائر، العدد الرابع، يونيو ٢٠١٧.

١٦) د. درويش سعيد،الحروب السيبرانية وأثرها علي حقوق الإنسان، دراسة علي ضوء أحكام دليل تالين، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية، المجلد (٥٤)، العدد (٥).

١٧) د.داليا أحمد فؤاد، مبدأ التمييز في القانون الدولى بين المقاتلين والمدنيين في النزاعات المسلحة، مجلة السياسة الدولية، المجلد ٥٤،العدد ٢١٨، أكتوبر ٢٠١٩.

١٨) د. هالة أحمد الرشيدي، الإرهاب السيبراني، ماهيته وجهود مكافحته في ضوء التشريعات والقوانين الوطنية والدولية، دار النهضة العربية، القاهرة، ٢٠٢١.

١٩) د. هلالي عبداللاه أحمد، الجوانب الموضوعية والإجرائية للجرائم المعلوماتية على ضوء إتفاقية بودابست الموقعة في ٢٣ نوفمبر ٢٠٠١ ، دار النهضة العربية، القاهرة، ط١ ، ٢٠٠٣.

٢٠) د. هاني محمد خليل العزازي، النظام القانوني الدولي لمكافحة المخاطر السيبرانية، مجلة مصر المعاصرة، الجمعية المصرية للإقتصاد السياسي والإحصاء والتشريع، القاهرة، العدد ٥٤٩، يناير ٢٠٢٣.

٢١) د. وائل أحمد علام ، مركز الفرد في النظام القانوني للمسئولية الدولية، دار النهضة العربية، القاهرة، ٢٠٠١.

٢٢) د. وفاء لطفي، الجهود الدولية في مجال مكافحة جرائم الارهاب السيبراني: التجربة الماليزية نموذجا، مجلة كلية الاقتصاد والعلوم السياسية، جامعة القاهرة ، المجلد الثالث والعشرون، العدد الأول، يناير ٢٠٢٢.

٢٣) د. وسام محمود عرفان مصطفي، سبل مكافحة الهجمات السيبرانية دولياً، مجلة الدراسات القانونية والاقتصادية، كلية الحقوق جامعة مدينة السادات، المجلد (١٠)، العدد (٣)، سبتمبر ٢٠٢٤.

٢٤) د. حازم محمد عتلم، المحكمة الجنائية الدولية الخاصة بلبنان مقارنة بالمحاكم الجنائية الدولية والمدولة والمختلطة الأخرى مع دراسة خاصة لمسئولية القادة، المجلة المصرية للقانون الدولي، العدد ٧١، ٢٠١٥.

٢٥) د. حسام عبد الأمير خلف، البعد الجديد – الخامس– في النزاعات المسلحة – الفضاء الالكتروني، مجلة كلية الحقوق، جامعة النهرين، العدد الأول، يناير، ٢٠١٦.

٢٦) طلال ياسين العيسي، عدى محمد عناب، المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مجلة الزرقاء للبحوث والدراسات الإنسانية، الأردن، المجلد التاسع عشر، العدد الأول، إبريل ٢٠١٩.

٢٧) د. ياسر إسماعيل الدفراوي، دور القانون الدولي في ضبط استخدام التكنولوجيا في الفضاء الخارجي، مجلة الشريعة والقانون بالقاهرة، جامعة الأزهر، المجلد (٤٢)، العدد (٤٢)، أكتوبر ٢٠٢٣.

٢٨) د. يحيي ياسين سعود، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، المجلة القانونية، كلية الحقوق جامعة القاهرة (فرع الخرطوم)، المجلد (٤)، العدد (٤)، ٢٠١٨ .

٢٩) د. مايا حسن خاطر ، الإطار القانوني لجريمة الإرهاب السيبراني، مجلة جامعة الناصر، العدد الخامس، المجلد الأول، يناير– يونيو ٢٠١٥.

٣٠) د. منى الأشقر جبور، الأمن السيبراني: التحديات ومستلزمات المواجهة، دراسة مقدمة إلى اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني، بيروت: المركز العربي للبحوث القانونية والقضائية، ٢٧–٢٨ أغسطس٢٠١٢ .

٣١) د. محمد صلاح عبد اللاه ربيع، الهجمات السيبرانية بين مشروعيتها كوسيلة للدفاع الشرعي وادانتها كاعتداء غير مشروع: دراسة تحليلية في ضوء القانون الدولي، مجلة الدراسات القانونية والاقتصادية، كلية الحقوق جامعة مدينة السادات، المجلد (١٠)، العدد (١)، مارس ٢٠٢٤ .

٣٢) د. محمد عادل محمد عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق علي ممارسة التجسس وقت السلم: دراسة علي ضوء دليل "تالين" بشأن القانون الدولي المطبق علي العمليات السيبرانية ٢٠١٣-٢٠١٧، مجلة البحوث القانونية والاقتصادية، كلية الحقوق جامعة بني سويف، المجلد (٣٣)، العدد (١)، يناير ٢٠٢١ .

٣٣) مصطفي عصام نعوس، سيادة الدولة في الفضاء الالكتروني، مجلة الشريعة والقانون، جامعة الإمارات العربية المتحدة – كلية القانون، المجلد (٢٦)، العدد (٥١)، يوليو ٢٠١٢.

٣٤) د. محمد صافي يوسف ،القانون الدولي العام، دار النهضة العربية، القاهرة، ٢٠١٩.

ـــــــــــــ، تدابير حماية الأمن القومي كاستثناء علي تطبيق قواعد القانون الدولي العام ، المجلة المصرية للقانون الدولي، الجمعية المصرية للقانون الدولي، المجلد السادس والستون ، العدد ٦٦ ، ٢٠١٠.

٣٥) د. محمد عبد المنعم عبد الغني، القانون الدولي الجنائي دراسة في النظرية العامة للجريمة الدولية، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٨.

٣٦) د. محمود حسين الشرقاوي، الهجمات الإلكترونية في ضوء أحكام القانون الدولي الإنساني، رسالة دكتوراه، كلية الحقوق، جامعة بني سويف،٢٠٢١.

٣٧) د. محمود شريف بسيوني، المحكمة الجنائية الدولية، نشأتها ونظامها الأساسي، ط١، مطابع روز اليوسف الجديدة، القاهرة،٢٠٠١.

٣٨) د. محمد ربيع أحمد حسين، الهجمات السيبرانية واستخدام القوة في القانون الدولي المعاصر، مجلة العلوم القانونية والاقتصادية، كلية الحقوق جامعة عين شمس، المجلد (٦٥)، العدد (١)، يناير ٢٠٢٣.

٣٩) د. محسن عبدالحميد أفكيرين، النظرية العامة للمسئولية الدولية عن النتائج الضارة عن أفعال لا يحظرها القانون الدولى ، دار النهضة العربية، القاهرة، ١٩٩٩.

٤٠) د. سامي محمد عبد العال، الدفاع الشرعي ضد الهجمات السيبرانية، المجلة المصرية للقانون الدولي، الجمعية المصرية للقانون الدولي، المجلد التاسع والسبعون، العدد ٧٩ لسنة ٢٠٢٣ .

٤١) د. سلوي يوسف الاكيابي، مدي انطباق القانون الدولي الإنساني علي الهجمات السيبرانية، مجلة روح القوانين، كلية الحقوق جامعة طنطا، المجلد (٣٥)، العدد (١٠١)، يناير– الجزء الثاني ٢٠٢٣ .

٤٢) د. سراب ثامر أحمد، الهجمات علي شبكات الحاسوب في القانون الدولي الإنساني، أطروحة دكتوراه، كلية الحقوق جامعة النهرين، بغداد، العراق، ٢٠١٥.

٤٣) د. سعيد سالم جويلي، المدخل لدراسة القانون الدولي الإنساني، دار النهضة العربية، القاهرة، ٢٠٠٢–٢٠٠٣ .

٤٤) د. عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، سلسة أوراق، العدد الثالث والعشرين، وحدة الدراسات المستقبلية، مكتبة الإسكندرية،٢٠١٦.

ـــــــــــــ ، أنماط الحرب السيبرانية وتداعياتها علي الأمن العالمي، مجلة السياسة الدولية، ملحق اتجاهات نظرية، الصراع السيبراني، مركز الأهرام للدراسات الاستراتيجية، القاهرة، العدد ٢٠٨، ابريل ٢٠١٧ .

٤٥) د. عبد الله عبد الكريم علي أحمد، الهجمات السيبرانية في ضوء القانون الدولي، المجلة المصرية للقانون الدولي، المجلد السابع والسبعون، العدد ٧٧ لسنة ، ٢٠٢١ .

٤٦) عمر أحمد السعيدي، د. زياد محمد جفال، مدى اعتبار الهجمات السيبرانية انتهاكاً للحظر المفروض علي اتخدام القوة أو التهديد بها فى ضوء أحكام القانون الدولي للجوء للحرب، مجلة جامعة الإمارات للبحوث القانونية، جامعة الإمارات العربية المتحدة، كلية القانون، المجلد (٣٨)، العدد (٩٩)، سبتمبر ٢٠٢٤ .

٤٧) رزق أحمد سمودي، حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام، مجلة جامعة الشارقة للعلوم القانونية، الإمارات العربية المتحدة، المجلد (١٥)، العدد (٢)، ديسمبر ٢٠١٨.

٤٨) د. رغدة البهي، الحرب السيبرانية وتحديات الدفاع الجوي، مجلة السياسة الدولية، المجلد (٥٩)، العدد (٢٣٥)، يناير ٢٠٢٤.

ـــــــــ ، الإرهاب السيبراني: المفهوم والسمات والأنماط، المركز المصري للفكر والدراسات الاستراتيجية، ٣٠ سبتمبر ٢٠١٩.

٤٩) د. شريف نسيم قلته بخيت ،الهجمات الإلكترونية وحق الدفاع الشرعي للدول في القانون الدولي، رسالة دكتوراه، كلية الاقتصاد والعلوم السياسية، جامعة القاهرة ،٢٠٢٣ .

٥٠) د. شريف عبد الحميد حسن رمضان، الحرب السيبرانية ومدى ملائمتها مع القانون الدولي الإنساني، مجلة كلية الشريعة والقانون بتفهنا الأشراف – دقهلية، جامعة الأزهر، المجلد (٢٣)، العدد (٤)، يونيو ٢٠٢١.

ثانياً: المراجع الأجنبية:

1) Arias, G. J. (2017). Are the rules for the right to self-defense outdated to address current conflicts like attacks from non-state actors and cyber-attacks?. Revista Tribuna Internacional, 6(11).

2) Antolin-Jenkins, V. M. (2005). Defining the parameters of cyber war operations: looking for law in all the wrong places. Naval L. Rev., 51, 132.

3) Buchan, R., & Navarrete, I. (2021). Cyber espionage and international law. In Research Handbook on International Law and Cyberspace (pp. 231-252). Edward Elgar Publishing.

4) Cavelty, M. D. (2012, June). The militarisation of cyberspace: Why less may be better. In 2012 4th international conference on cyber conflict (CYCON 2012) (pp. 1-13). IEEE.

5) Couzigou, I. (2014, September). The Challenges Posed by Cyber Attacks to the Law on Self-Defence. In EUROPEAN SOCIETY OF INTERNATIONAL LAW, 10th Anniversary Conference, Vienna (pp. 4-6).

6) Czosseck, C., & Podins, K. (2010). State responsibility for Cyber-attacks: Competing standards for a Growing Problem. In Conference on Cyber Conflict (p. 197).

7) Fitz, C. (2017). All Is Fair In Love And Cyberwar: International Law And Cyber-Attacks. Houston Journal Of Internatıonal Law, 1(1).

8) Gervais, M. (2012). Cyber attacks and the laws of war. Journal of Law & Cyber Warfare, 1(1), 8-98.

9) Guymon, C. D. (Ed.). (2011). Digest of United States practice in international law. International Law Institute.

10) Hathaway, O. A., Crootof, R., Levitz, P., & Nix, H. (2012). The law of cyber-attack. Calif. L. Rev., 100, 817.

11) Herr, T., & Rosenzweig, P. (2015). Cyber weapons and export control: Incorporating dual use with the prep model. J. Nat'l Sec. L. & Pol'y, 8, 301.

12) Hughes, R. (2010). A treaty for cyberspace. International Affairs, 86(2), 523-541.

13) Jansson Holmberg, E. (2015). Armed attacks in cyberspace: do they exist and can they trigger the right to self-defence?.

14) Kissel, R. (2013). Glossary of Key Information Security terms: National Institute of Standards and Technology. US Department of Commerce Revision, 2.

15) Lewis, J. A. (2005). Aux armes, citoyens: Cyber security and regulation in the United States. Telecommunications Policy, 29(11), 821-830.

16) Lin, H. (2012). Cyber conflict and international humanitarian law. International review of the Red Cross, 94(886), 515-531.

17) Magnusson, A. (2023). Man-in-the-middle (mitm) attack: Definition examples more—strongdm. Available at: https://www.strongdm.com/blog/man-in-the-middle-attack.

18) Mačák, K. (2017). From cyber norms to cyber rules: re-engaging states as law-makers. Leiden Journal of International Law, 30(4), 877-899.

19) Margulies, P. (2013). Sovereignty and cyber- attacks: Technology's challenge to the law of state responsibility. Melbourne Journal of International Law, 14(2), 496-519.

20) Nevala, L. What can be qualified as an armed attack in cyber operations under the Article 51 of the UN Charter under the energy sector in Finland?.

21) Papastavridis, E. (2016). Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), 1986.

In Latin America and the International Court of Justice (pp. 233-244). Routledge.

22) Peake, A. (2004). Internet governance and the World Summit on the Information Society (WSIS). Report for the Association for Progressive Communications, URL (consulted June 2005): http://rights. Acpc. Org/documents/governance. pdf.

23) Proulx, V. J. (2018). Babysitting Terrorists: Should States Be Strictly Liable for Failing to Prevent Transborder Attacks?. In International Law (pp. 406-447). Routledge.

24) Pun, D. (2017). Rethinking espionage in the modern era. Chi. J. Int'l L., 18, 353.

25) Robinson, M., Jones, K., & Janicke, H. (2015). Cyber warfare: Issues and challenges. Computers & security, 49, 70-94.

26) Roscini, M. (2010). World wide warfare-'jus ad bellum'and the use of cyber force. Max Planck Yearbook of United Nations Law, 14, 85-130.

27) Saalbach, K. (2013). Cyber war methods and practice. Universitat Osnabruck [Online], Aug.

28) Schmitt, M. N. (2012, June). "Attack" as a term of art in international law: The cyber operations context. In 2012 4th international conference on cyber conflict (CYCON 2012) (pp. 1-11). IEEE.

———————. (2012). International Law in Cyberspace: The Koh Speech and the Tallinn Manual Juxtaposed.

———————. (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare (Vol. 32). Cambridge University Press.

———————. (2017). Peacetime cyber responses and wartime cyber operations under international law: An analytical vade mecum. Harv. Nat'l Sec. J., 8, 239.

29) Schmitt, M. (2017). Computer network attack and the use of force in international law: thoughts on a normative framework. In The Use of Force in International Law, Vol.27, (No. 379-431).

30) Shruti, M. (10). Types of Cyber Attacks You Should Be Aware in 2023.

31) Shackelford, S. J. (2009). From nuclear war to net war: analogizing cyber attacks in international law. Berkeley J. Int'l Law, 27, 192.

32) Shackelford, S. J., & Andres, R. B. (2010). State responsibility for cyber- attacks: competing standards for a growing problem. Geo. J. Int'l L., 42, 971.

33) Shoshan, E. (2015). Applicability of international law on cyber espionage intrusions.

34) Sklerov, M. J. (2009). Solving the dilemma of sate responses to cyber-attacks: a justification for the use of active defenses against states who neglect their duty to prevent. Mil. L. Rev., 201, 1.

35) Trenin, D. (2016). Information is a potent weapon in the new cold war., available at: https://perma.cc/QPT4-4B8T. 15/2/2020.

36) Tsagourias, N. (2012). Cyber attacks, self-defence and the problem of attribution. Journal of conflict and security law, 17(2), 229-244.

37) Van Sliedregt, E. (2003). The criminal responsibility of individuals for violations of international humanitarian law (Vol. 46). The Hague: TMC Asser Press.

38) Waxman, M. C. (2011). Cyber-attacks and the use of force: Back to the future of article 2 (4). Yale J. Int'l L., 36, 421.

———————. (2013). Self-defensive force against cyber- attacks: legal, strategic and political dimensions. International Law Studies, 89.

39) Weissbrodt, D. (2013). Cyber-conflict, cyber-crime, and cyber-espionage. Minn. J. Int'l L., 22, 347.

40) Ziolkowski, K. (2013). Peacetime regime for state activities in cyberspace. Tallinn: NATO CCD COE Publications.