الهجمات السيبرانية
في ضوء القانون الدولي

الدكتور
عبد الله عبد الكريم علي أحمد

الملخــص

أدي التطور التكنولوجي الذي يشهده العالم حاليا الي ظهور تحديات كبيرة كان أبرزها الهجمات السيبرانية التي تمتاز بسهولة تنفيذها، وهي هجمات من نوع جديد لم يكن يعرفها العالم حتي وقت قريب، واصبحت تلك الهجمات من أخطر حروب العصر الحديث بل أنها تعتبر أكثر فتكا من المواجهات العسكرية التقليدية، حيث أن أثر تلك الهجمات لا يقتصر فقط على البيانات في أجهزة الكمبيوتر أو أنظمته بل أنها تتجاوز ذلك الأمر لتقوم بالتأثير بشكل مباشر علي العالم الحقيقي فبإمكانها أن تسيطر علي الحركة الجوية وتعطيل المصالح الحكومية والعديد من التأثيرات السلبية الأخري.

الكلمــات الافتتاحيــة: الهجمــات الســيبرانية– الفضــاء الإلكترونــي– الثــورة التكنولوجية– النزاع المسلح.

Abstract:

The technological development that the world is currently witnessing has led to the emergence of great challenges, the most prominent of which were cyber attacks that are easy to implement, which are attacks of a new type that the world did not know until recently, and these attacks have become one of the most dangerous wars in the modern era, but they are considered more deadly than traditional military confrontations, as the impact of these attacks is not limited only to data in computers or systems, but they go beyond that matter to directly affect the real world They can control air traffic, disrupt government interests and many other negative effects.

Key words: Cyber-attacks - Cyberspace - Technological revolution - Armed conflict.

المقدمة

أدي التطور التكنولوجي والانتشار الواسع لأجهزة الحاسوب واستخدام الشبكة المعلوماتية بصورة كبيرة الي احداث ثورة كبيرة في كافة المجالات، حيث أصبحت الخدمات الإنتاجية والخدمية والمعلوماتية والاجتماعية ترتكز بصورة رئيسة على الشبكة المعلوماتية، إلا أنه وبرغم الخدمات التي تقدمها الشبكة المعلوماتية وتوفرها للجميع فإن الاعتماد الكبير عليها أدي إلي زيادة المخاطر التي تتعرض لها المواقع الإلكترونية حيث أنها اصبحت عرضة للهجمات السيبرانية وذلك بسبب تطور الحواسيب والبرمجيات.

وتعتبر الهجمات السيبرانية هي إحدى الآليات التي جاءت نتيجة للتطور التكنولوجي فهي تتميز بسهولة تنفيذها وغموض مكان تنفيذها، فأصبح بإمكان أي دولة أن تقوم بشن الهجمات السيبرانية من أجل التأثير على أي دولة أخري واختراق وتعطيل الأنظمة المصرفية والأمنية والعسكرية لأي دولة أخري، وأن ما يتم تحقيقه من دمار وخسائر من خلال شن تلك الهجمات قد يقوق الآثار المتولدة عن النزاع المسلح التقليدي سواء كان ذلك في الأرواح البشرية أو في البنية التحتية.

وتظهر مخاوف الهجمات السيبرانية بصورة واضحة عندما يتخطى أثرها اختراق البيانات والمعلومات إلى خلق تأثير في العالم الحقيقي مثل القيام باختراق المواقع الحكومية الإلكترونية للسيطرة على الأماكن والمواقع الحيوية مثل: الملاحة الجوية وحركة الطائرات أو محطات الطاقة النووية أو خطوط أنابيب النفط أو اختراق القنوات التلفزيونية وبث إشاعات تخلق نوعا من الفوضى والرعب لدى المواطنين أو تؤثر على علاقات الدول ببعضها البعض.

إشكالية البحث:

تكمن إشكالية البحث في سؤال رئيس وهو إمكانية تطبيق قواعد القانون الدولي علي الهجمات السيبرانية والذي يتفرع عنه بعض الاسئلة الفرعية وهي:

١-ما المقصود بالهجمات السيبرانية؟

٢-ما هي أنواع الهجمات السيبرانية والآثار الناشئة عنها؟

٣-ما الجهود الدولية لمكافحة الهجمات السيبرانية؟

٤-ما الأخطار الناتجة عن الهجمات السيبرانية؟

٥٠-ما هي وسائل شن الهجمات السيبرانية؟

منهج البحث:

تستدعي طبيعة البحث اتباع المنهج التحليلي من خلال استعراض ماهية الهجمات السيبرانية وبيان خطورتها والآثار الناتجة عن استخدامها، وبيان وسائل مكافحتها. والتعرض للقانون الواجب التطبيق علي الهجمات السيبرانية ومدي انطباق القانون الدولي الإنساني علي تلك الهجمات.

أهداف البحث:

يهدف البحث إلي بيان خطورة الهجمات السيبرانية والجهود الدولية للحدم من تلك الهجمات وبيان الوسائل التي يتم استخدامها في شن الهجمات السيبرانية.وبيان مدي انطباق القانون الدولي الإنساني علي الهجمات السيبرانية، لاسيما أن استخدام الفضاء السيبراني لشن العمليات العسكرية غير من مفهوم النزاع المسلح، فالأهداف المقصودة من أي هجوم سيبراني سوف تكون على الأرجح مدنية كما أنها سوف تؤثر على السكان المدنيين.

خطة البحث:

المبحث الأول: ماهية الهجمات السيبرانية

المطلب الأول: تعريف الهجمات السيبرانية

المطلب الثاني: نشأة الهجمات السيبرانية وخصائصها

المطلب الثالث: أنواع الهجمات السيبرانية

المبحث الثاني:التكييف القانوني للهجمات السيبرانية والجهود الدولية في مكافحتها

المطلب الأول:التكييف القانوني للهجمات السيبرانية

المطلب الثاني:الهجمات السيبرانية في ضوء القانون الدولي الإنساني

المطلب الثالث: الجهود الدولية في مكافحة الهجمات السيبرانية

المبحث الأول
ماهية الهجمات السيبرانية

يعتبر مفهوم الهجمات السيبرانية من المفاهيم الحديثة نوعا ما، وتشير إلى أساليب الجريمة التي تعتمد بشكل أساسي على تكنولوجيا المعلومات وتستهدف الحاسبات والمواقع الإلكترونية، وتتضمن عمليات التسلل إلى أنظمة الحاسب الآلي في محاولة لجمع البيانات، أو تصديرها، أو إتلافها أو تغييرها، كما تتضمن عمليات زرع برمجيات ضارة بغرض التجسس.(١)

وتعد الهجمات السيبرانية حديثة نسبيا، لارتباطها بالثورة التكنولوجية التي عرفها المجتمع، ومع تزايد اعتماد الأفراد على وسائل التكنولوجيا والاتصال وما واكبه من تحديات كبرى. وتختلف تعريفات الهجمات السيبرانية باختلاف طبيعة كل دولة والاستراتيجية التي تعتمدها ومدي ارتباطها بالعالم الرقمي والتي تعتمد على مدى تفعيل الحكومة للنظم الإلكترونية وكيفية توظيف شبكات المعلومات ووسائل الاتصال في توصيل الخدمات للمواطنين داخل الدولة في مجالها المدني ووسائل الاتصال في توصيل الخدمات في المجالات العسكرية والنواحي الدفاعية من جهة أخرى(٢)

ويعتبر الفضاء الإلكتروني ساحة لارتكاب بعض الجرائم الأخرى التي تختلف في طبيعتها عن الهجمات السيبرانية مثل جرائم: الابتزاز الإلكتروني والاحتيال

(١) عمار ياسر محمد زهير، التحديات الأمنية المعاصرة للهجمات السيبرانية، القيادة العامة لشرطة الشارقة مركز بحوث الشرطة، المجلد ٣٠، العدد ١١٨،٢٠٢١،ص٢٧.

(٢) سحر قدوري الرفاعي، الحكومة الالكترونية وسبل تطبيقها: مدخل استراتيجي، مجلة اقتصاديات شمال افريقيا، العدد السابع، جامعة حسيبة بو على،٢٠١٦،ص٣٠٨.

الإلكتروني وسرقة البيانات، كما أن الهجمات السيبرانية التي تقع على المواقع الإلكترونية قد يتم ارتكابها من داخل الدولة ومن خارجها على حد السواء، حيث تصنف جريمة الهجمات السيبرانية من الجرائم العابرة للحدود.

المطلب الأول
تعريف الهجمات السيبرانية

يعتبر مصطلح الهجمات السيبرانية مصطلح حديث الأمر الذي تطلب وضع تعريف لتلك الهجمات ليبين ماهيتها وقد ذهب الفقيه (fuertes) إلى تعريفه بأنه "هجوم يتم من خلال الإنترنت عن طريق القيام بالتسلل إلى المواقع الإلكترونية غير المرخص بالدخول إليها، وذلك من أجل القيام بتعطيل وإتلاف البيانات والمعلومات المتوفرة على تلك المواقع او الاستحواذ عليها، وتتم من خلال سلسلة من الهجمات تقوم بها دولة ضد دولة أخري ، كما ذهب شمت (schmitt) في تعريفه للهجمات السيبرانية بالقول أنها عبارة عن مجموعة من الإجراءات التي تقوم الدولة باتخاذها من أجل الهجوم على نظم المعلومات العادية في دولة أخرى، من أجل التأثير عليها والإضرار بها، وهي تعمل في الوقت نفسه على الدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة[١].

وعرفت أيضا بأنها: "عمليات قائمة على الحرب الإلكترونية والخداع النفسي، فضلا عن القيام باستهداف شبكة تواصل العدو العسكرية وعملياته الأمنية

(١) أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، منشورات زين الحقوقية، الطبعة الأولي،لبنان،٢٠١٨،ص١٦.

الإلكترونية"[١]، وتعرف أيضا بأنها:"القيام بتطويع الإمكانيات الإلكترونية العسكرية بقصد التأثير في المواقع الإلكترونية الأخرى وتعطيلها وتدميرها سواء كانت تلك المواقع مدنية أو عسكرية"[٢].

كما عرفت أيضا بأنها: " تصرف يتم في عالم افتراضي معتمدا على استعمال بيانات رقمية ووسائل اتصال تعمل إلكترونيا يقوم على تحقيق أهداف عسكرية أو أمنية ملموسة من خلال اختراق مواقع الكترونية حساسة وفي العادة تقوم بوظائف تصنف بأنها ذات أولوية مثل أنظمة الحماية الخاصة بمحطات الطاقة النووية أو الكهربائية أو المطارات ووسائل النقل الأخرى"[٣].

كما عرفت الهجمات السيبرانية ايضا بأنها " وسيلة قتالية يتم استخدامها بذاتها من أجل التسلل للأنظمة الإلكترونية المعدة من أجل حماية او تنظيم سير عمل منشآت حيوية مثل محطات توليد الطاقة النووية أو السدود أو وسائل النقل وذلك بغرض تطويعها والسيطرة عليها لتدمير ذاتها بذاتها من خلال القيام بتغذيتها بمعلومات غير صحيحة لأجهزة التحكم والحماية الإلكترونية"[٤].

---

(1)Zimet .E.and C. L. Barry," Military services Overview, Cyber power and National Security", National Defense University Press ,Washington, DC,USA,2009,P.291

(2)Marco Roscini," World Wide Warfare – Jus ad bellum and the use of Cyber Force",Max Planck Yearbook of United Nations Law, Volume 14,2010,p.91.

(3)K.Saalbach," Cyber War, Methods and Practice", Version 9.0, University of Osnabruck-17 Jun 2014. , p.6.

(٤) طلال ياسين العيسي، المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون

ونري أن الهجمات السيبرانية هي عبارة عن عمليات تتم في الفضاء الإلكتروني يقوم بارتكابها دول او أفراد من أجل إصابة الأشخاص أو تدمير أهداف خصم معين أو تعطيل الخدمات التي يتم تقديمها سواء كانت خدمات اجتماعية أو اقتصادية أو أمنية أو سياسية من خلال الدخول غير المشروع إلي النظام المعلوماتي أو مواقع الإنترنت وحذف البيانات والمعلومات داخل النظام المعلوماتي والحد من القدرة في التحكم بذلك النظام.

المطلب الثاني:

نشأة الهجمات السيبرانية وخصائصها

أولا: نشأة الهجمات السيبرانية

يعتبر البعض أن الهجمات السيبرانية بدأت في ثَمانينِيَّات القرن الماضي في عهد الرئيس الأمريكي رونالد ريغان، والذي كان يرى أنَّ بلادَه قد تتعرض لخطر تلك الهَجَمات، الأمر الذي أفرز فكرةً مميزة وسابقة لأوانها حيثُ أنتجت تلك الفكرة "وحدة السياسة القومية بشأن الاتصالات وأمن نظم المعلومات" وقد تَطورت تلك الفكرة خلال التسعينات وقام الجيش باستخدامها في عمليات الاستشعار عن بعد، وقد ظهرت الحاجة إليها وإلى تَقنياتِها خلال الحرب الأمريكية على العراق في عام ٢٠٠٣[١].

وقد كانت استراتيجية الهجمات السيبرانية الأمريكية متأثرة بالأولويات الجديدة

الدولي، مجلة الزرقا للبحوث والدراسات الإنسانية،المجلد ١٩، العدد ١، ٢٠١٩،ص٨٤

(١) فرد كابلان، ترجمة لؤي عبد المجيد، المنطقة المعتمة: التاريخ السري للحرب السيبرانية، عالم المعرفة، المجلس الوطني للثقافة والفنون والاداب،الكويت،٢٠١٩،ص٥٢.

للصناعة العسكرية الإسرائيلية والتي تصنف بأنها بالغة السرية والتي تستهدف في الأساس تباعا الصناعة النووية الإيرانية [١] والصناعات الدفاعية الأوروبية والتي يفترض أنها تعود إلى بلدان حليفة. وفي مقابل التوجهات الأمريكية كان هناك توجهات أخرى من الخصم التقليدي لأمريكا وهي روسيا والتي كانت الأسبق في مجال الاستعداد للهجمات السيبرانية[٢]وقد سرعت الدول من وتيرة القيام باستخدام الكمبيوتر من أجل تحقيق قفزات نوعية في المجالين الأمني والعسكري، وذلك في مطلع التسعينات من القرن الماضي حيث أطلق عليها البعض مصطلح الحرب السيبرانية الباردة أو سباق التسلح السيبراني[٣].

ومع ظهور تقنيات حديثة في تداول البيانات والمعلومات والتقدم الكبير في وسائل الاتصال، ودخول تكنولوجيا تقنية المعلومات كافة مناحي الحياة في مجتمعنا المعاصر، وما تفتعله فئات معينة من خلال استخدام وسائل وأدوات خاصة لتحقيق مصالحها، وذلك بتسخير تكنولوجيا المعلومات في إحداث مثل تلك الصراعات. وتكمن خطورة هذه الظاهرة في سهولة افترافها من خلال الأجهزة الإلكترونية أو

---

(١) المركز الاستشاري للدراسات والتوثيق، التحولات في العقيدة العسكرية الامريكية، دعائم الضعف السبع، اوراق استراتيجية، غير دورية، تعني بالشؤون الاستراتيجية، العدد ٢ ايلول ٢٠١٤،بيروت،ص١٧.

(2)Keir Giles, "Information Troops a Russia Cyber Command?" legal paper third international conference on Cyber Conflicts, Tallinn Estonia,2011,p.47.

(3)Tang Lan, Zhang Xin, Harry D. Raduege, Jr., Dmitry I. Grigoriev, Pavan Duggal, and Stein Schjølberg,"Global Cyber Deterrence Views from China, the U.S., Russia, India, and Norway", The EastWest Institute, Printed in the United States, 2010, p1.

الحواسيب المتصلة بالإنترنت، حيث إن تنفيذها قد يتم بشكل لحظي، وفي بعض الأحيان لا يستغرق تنفيذها سوى دقائق معدودات[١]، لذلك فإنه من الملاحظ أن العديد من الدول في الوقت الحاضر تقوم بصرف المليارات من أجل تطوير الأنشطة السيبرانية الخاصة بها من أجل صد أي هجوم سيبراني يحاول القيان باستهداف مواقعها الإلكترونية.

ولعل من أبرز الهجمات السيبرانية الهجمات التي قامت بها الولايات المتحدة الأمريكية قاصدة به منظومة التحكم الآلي صناعيا في أنبوب النفط (Chelyabinsk) التابع للاتحاد السوفيتي، إلا أن الاتحاد السوفيتي قد قتام بنفي تلك الهجمات آنذاك[٢]، كما يعتبر هجوم (Stucksnet) الذي شنته الولايات المتحدة الأمريكية واسرائيل علي إيران من ابر ز الهجمات وقد كان ذلك الهجوم جزء من هجمات أكبر عرفت باسم Operation Olympic Games ، وقد هدف ذلك الهجوم إلي تخريب برنامج إيران النووي حيث تم إنزال فيروس على برنامج التشغيل الإلكتروني الذي يدير عملية تخصيب اليورانيوم في موقع "ناتانز" النووي، وتسبب ذلك في إتلاف عدد كبير من وحدات الطرد المركزي، وكان ذلك الهجوم متطورا، بالنظر لقدرته على اتخاذ قرارات مستقلة في البيئة المستهدفة بدون التواصل مع

(١) أميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، العدد الخامس والثلاثون، الجزء الثالث،٢٠٢٠، ص٤٠١ .

(2)Diego Rafael Canabarro and Thiago Borne," Reflection on the fog of Cyber War", National Center for Digital Government, Policy working Paper No.13:001, March 1, 2013, footnote 11, p.10.

الطرف منفذ الهجوم[١].

ثانيا: خصائص الهجمات السيبرانية

تتسم الهجمات السيبرانية بمجموعة من الخصائص يمكن تحديدها على النحو الآتي[٢]:

١- سهولة تنفيذها واستخدامها لتوفرها على نطاق واسع، ما يمكن مرتكبيها من القيام بهجمات متعددة تتجاوز مستوى قدراتهم الحقيقية.

٢- خضوعها لعمليات التحديث والتطوير بوتيرة سريعة وبشكل دائم، الأمر الذي يترتب عليه زيادة فاعليتها وقدرتها التدميرية.

٣- قدرتها على اختراق أكثر أنظمة الحماية تعقيدا، وإصابة أنواع مختلفة بالإضافة إلى قدرة تلك الهجمات على اصابة انواع مختلفة من الأجهزة الإلكترونية سواء كانت أجهزة حاسب آلي أو خوادم إلكترونية أو أي جهاز متصل بشبكة إلكترونية.

٤- صعوبة تحديد مصدرها بسبب غياب الدليل الفيزيائي في ذلك النوع من الهجمات، وفي أغلب الأحيان تظل مجهولة المصدر ما لم يعلن عنها مرتكبها أو تتبناها جهة محددة، كما أن الكشف عن مصدر تلك الهجمات يستلزم أساليبا أمنية عالية التقنية.

---

(١) شادي منصور، حروب الجيل الخامس، أساليب التفجير من الداخل على الساحة الدولية، دار المنهل، ٢٠١٩، ص٩٩.

(٢) نور أمير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الإنساني، رسالة ماجستير، الجامعة الافتراضية السورية،٢٠٢١، ص١١.

٥- اختفاء العامل الجغرافي في الهجمات السيبرانية، بحيث يصبح أي مركز أو منشأة بغض النظر عن مكان تواجده الفعلي هدفا لتلك الهجمات. ولا يقتصر التهديد بالهجمات السيبرانية على نطاق الكرة الأرضية فحسب، بل قد يصل إلى الفضاء من خلال إرسال القراصنة فايروسات إلى الأقمار الصناعية بهدف تعطيلها أو سرقة البيانات والمعلومات الموجودة فيها.

٦- قلة الكلفة المادية للهجمات السيبرانية مقارنة بالحروب التقليدية، بل تعتبر تلك الهجمات عاملا مساعدا فيها، وأداة مؤثرة في السياسة والاقتصاد على الصعيد الدولي، ويرجع السبب في ذلك إلى انتقال جزء كبير من الصراعات بين الدول إلى الفضاء الإلكتروني مع تزايد ارتباط العالم بثورة تقنية المعلومات وتزامنا مع تراجع دور الدولة في ظل العولمة، وانسحابها من بعض القطاعات الاستراتيجية لمصلحة القطاع الخاص. هذا بالإضافة إلى تصاعد أدوار الشركات متعددة الجنسيات لا سيما الشركات المتخصصة في مجال التكنولوجيا.

٧- يترتب على الهجمات السيبرانية خسائر مالية ضخمة كما أنها قد تؤدي إلى خسائر في الأرواح في حالة استهداف تلك الهجمات قطاعات حساسة مثل أنظمة المستشفيات وأنظمة التبريد في المفاعلات النووية.

٨- صعوبة استشعار الهجمات السيبرانية لعدم وجود أي دلائل أو مؤشرات تفيد التنبؤ بحدوثها، إذ أنها قد تحدث في أي مكان وأي وقت وبسرعة فائقة.

المطلب الثالث

أنواع الهجمات السيبرانية

تقوم الدول أو الأفراد بشن الهجمات السيبرانية من أجل إيقاف المواقع الإلكترونية عن العمل أو اختراقها وسرقة البيانات والمعلومات التي تحتوي عليها تلك المواقع، الأمر الذي قد يترتب عليه توقف الحياة في تلك الدول لما لتلك الهجمات من أثر علي القطاعات المختلفة داخل الدولة، وتلك الهجمات التي يتم شنها لها أنواع مختلفة وهي علي النحو الآتي:

أولا: هجوم الحرمان من الخدمة

ويتضح من أسم ذلك النوع من الهجمات أنه يهدف إلي أن يتم حرمان المستخدمين من بعض الخدمات المعينة أو التأثير عليها، ويطلق علي أسم ذلك النوع من الهجوم (DDOS - DISTRIBUTED DENIAL OF SERVICE) ويعني رفض الخدمة الموزعة، ويتم شن هجوم الحرمان من الخدمة علي شبكة معلوماتية فيتم بتحميلها بما يفوق طاقتها، ومن ثم نقص الموارد المتاحة، ومنع المستخدم الشرعي من الاستفادة من تلك الموارد.

ومن ابرز تلك الهجمات، الهجمات التي شنتها روسيا في عام ٢٠٠٧ على استونيا بسبب نقل تمثال يخلد تضحيات جنود روس في الحرب العالمية الثانية، فبدأت روسيا بإطلاق سلسلة من هجمات الحرمان من الخدمة ،والتي تسببت في عرقلة المواطنين في الدخول الي بعض المواقع، ولم يعد المواطنين قادرين علي إجراء معاملاتهم البنكية الإلكترونية أو التواصل مع بعضهم بالبريد الإلكتروني لأيام عديدة، كما تم تعطيل البنية التحتية للاقتصاد الرقمي الاستواني.

ثانيا: الفايروسات البرامج الخبيثة

تعد الفايروسات برامجا مثلها مثل أية برامج أخرى إلا أنه تم تصميمها من قبل أحد المخربين بهدف إحداث أكبر قدر من الضرر للنظام بعد أن يتم ربطه بالبرامج الأخرى، ويمتلك الفايروس القدرة على تكرار نفسه حتي يبدو وكأنه يتوالد ذاتيا مما يمنحه القدرة على القيام باستهداف برامج أخرى في الحاسب ومواقع أخرى في الذاكرة من أجل العمل على تدميرها، وتضاف الفايروسات إلى أحد البرمجيات أو إلى أنظمة تشغيل الحاسب الآلي، حيث يقوم ذلك البرنامج الدخيل بمجموعة من العمليات التي تؤثر بصورة مباشرة أو غير مباشرة في خصائص نظام التشغيل أو المعلومات المخزَّنة (١).

ومن الأمثلة علي ذلك ما قامت به مجموعة من الهاكرز من روسيا بزراعة برنامج خبيث في نظام تابع لشركة solar winds، وعندما قامت الشركة بعمل تحديث لبرنامجها الذي يتم استخدامه من قبل أكثر من ٣٠٠٠٠٠ عميل حول العالم قامت الشركة بإرسال التحديث إليهم محملا بالفايروس الذي زرعه الهاكرز داخل النظام، وقد فتح هذا الفايروس بابا خفيا في أنظمة الجهات التي استقبلت التحديث، وقد استغل الهاكرز هذه الثغرات لتركيب برمجيات إضافية علي الأجهزة والأنظمة التي أصيبت بذلك الفايروس الذي تم تحميله مع التحديث، ما سمح للهاكرز بالتجسس علي أنظمة الجهات المستقبلة، وقد أعلنت شركة solar winds أن هناك أكثر من ١٨٠٠٠ عميل قاموا بتحميل التحديث علي أنظمتهم وهي عرضة

---

(١) حسن مظفر الرزو، الفايروسات والحاسب الإلكتروني: المخاطر المحتملة وسبل الحد منه، المجلة العربية العلمية للفتيان، المنظمة العربية للتربية والثقافة والعلوم، المجلد الاول، العدد الثاني،١٩٩٧،ص٤ .

للاختراق[١].

ثالثا: برامج القنابل المعلوماتية

تعتبر برامج القنابل المعلوماتية اكثر تقدما من البرامج الخبيثة ، وهي عبارة عن تعليمات برمجية ضارة تم تصميمها لتعمل خلال أحداث محددة أو تحت ظروف معينة أو لدى تنفيذ أمر معين، بحيث تقوم بتخريب ومسح البيانات أو تعطيل النظام، وقد تظل كامنة لفترة طويلة من الزمن ثم يتم تفعيلها وقد تسبب أضرارا بالغة لجهاز الحاسب الآلي المصاب مما يجعله غير صالح للاستعمال[٢].

ويتم استخدام القنابل المعلوماتية للعمل علي القيام بتدمير المعلومات من أجل تدمير المعلومات والبيانات وتغيير برامجَ ومعلوماتِ النظام كما أنه يمكن استخدامها لغرض حماية بعض برامج الملكية من خطر الاختراق، ويظهر ذلك بصورة واضحة في الحَملات الاعلانية كما هو الشأن في المجلاَّت التي يوزَّع معها بعض الأقراص كهديّة وتحتوي على برامجَ خبيثة، بالإضافة إلى وجود تلك البرامج في عددٍ من مواقع الإنترنت. كما أنَّه من الممكن أن تظهر في بعض البرامج المؤجرة والتي لا يفقد مالكها حقوق الملكية الواردة عليها، وفي تلك الأحوال إذا توقف المستأجر عن دفع القيمة الإيجارية التي تم الاتفاق عليها فيما فيما بينهم، فيقوم المالك بإرسال قنابلَ البرامج المعلوماتيّة أو تفعيل البرامج التي قد تكون موجودة أصلاً في البرامج

(١) عمار ياسر محمد زهير البابلي، التحديات الأمنية المعاصرة للهجمات السيبرانية ، المرجع السابق، ص٣٩-٤٠

(٢) طلال محمد الحاج ابراهيم، الهجمات الالكترونية والمسؤولية الجنائية للقادة، المجلة القانونية والقضائية، وزارة العدل-مركز الدراسات القانونية والقضائية، السنة ١٢، العدد الأول،٢٠١٨،ص٣٠٥.

المستأجرة ولا يقوم المالك فيما بعد بإرسال ما يوقف انفجارها [١].

ومن الأمثلة على الهجمات باستخدام برامج القنابل المعلوماتية، الهجوم الإلكتروني الذي حدث في العام ٢٠١٦ واستهدف الهيئة العامة للطيران السعودي وعددا من المؤسسات الحكومية، وكان عبارة عن برنامج قنبلة إلكترونية موقوتة، تم زرعها مسبقا، وبدأت البرمجيات الخبيثة بمحو البيانات المخزنة في أجهزة الكمبيوتر، ثم سيطرت هذه البرمجيات على سجل تمهيد الأجهزة ومنعت إعادة تشغيلها[٢].

رابعا: برامج الدودة

يقصد ببرامج الدودة تلك البرامج التي تستفيد من الثغرات الموجودة في أنظمة تشغيل الحاسب الآلي والتي تنتقل من جهاز إلى آخر، الأمر الذي يترتب عليه احتلال الشبكة بالكامل والتسبب في آثار مدمرة. وبفضل الوصلات التي تربط تلك الحواسب ببعضها البعض، تتمكن تلك البرامج من الانتقال من شبكة إلى أخرى بهدف شغل أكبر قدر من سعة الشبكة، وبالتالي العمل على تعطيل أو خفض كفاءة تلك الشبكات. وقد تتعدى أهداف برامج الدودة ذلك لتبدأ التكاثر والانتشار وتقوم بالتخريب الفعلي للملفات والبرامج وأنظمة التشغيل وبروتوكولات الاتصال.

ومن أكثر الطرق وضوحا لنشر برامج الدودة هي مرفقات البريد الإلكتروني المصابة والتنزيلات التلقائية التي تحدث عند القيام بزيارة بعض المواقع على الإنترنت أو التسلل عبر الثغرات الأمنية في أنظمة التشغيل أو برامج الحماية كما انه

---

(١) عمار ياسر محمد، التحديات الأمنية المعاصرة للهجمات السيبرانية ، المرجع السابق،ص١٤٤.

(٢) نور أمير الموصلي، المرجع السابق،ص١٨ .

تتجلي اضرار برامج الدودة في أنها تسمح للمهاجم باستخدام الحاسب الآلي المصاب في مهاجمة مواقع الإنترنت، أو إرسال بريد إلكتروني يحتوي على تلك البرامج أو القيام بتنزيل برامج ضارة إليه[١].

(١) عمار عباس الحسيني، ،المرجع السابق،ص١٤٥.

المبحث الثاني

التكييف القانوني للهجمات السيبرانية والجهود الدولية في مكافحتها

أسهمت الهجمات السيبرانية في توجيه العمليات العسكرية، كما أنها سهلت عمل القوات العسكرية التقليدية، فيعتبر طريقة قتالية كالطائرات بدون طيار التي يتم القيام بتوجيهها لتحديد الأهداف العسكرية والقيام بتدميرها، أو القيام باستخدام الهجوم السيبراني لقطع الاتصالات في المطارات العسكرية والمدنية، وقد اصبحت تلك الهجمات مصدر قلق لكافة دول العالم سواء علي مستوي الحكومات أو حتي الأفراد، بعد أن اصبحت شبكة الإنترنت ساحة لاستعراض القوة الإلكترونية من خلال الاختراق المتبادل للعديد من المواقع الحيوية على مستوي العالم.

وقد اضحت الهجمات السيبرانية حربا مكتملة الأركان تفرض تحديات كبيرة لاسيما على الدول الأقل تقدما والتي ليس لديها القدرة على القيام بحماية البنية الأساسية لديها من الاختراق وتعزيز دور التكنولوجيا في مواجهة الهجمات السيبرانية، وقد دفعت تلك الهجمات الدول على القيام بتعزيز بيئتها الرقمية وتحقيق الأمن السيبراني للمنشآت المهمة والحيوية من أجل العمل على تقليل المخاطر التي قد تتعرض لها.

المطلب الأول

التكييف القانوني للهجمات السيبرانية

تمثل الهجمات السيبرانية تهديدا لأحد أهم المبادئ الرئيسة في القانون الدولي وهو مبدأ احترام سيادة الدولة بوصفه واجبا اساسيا، وهو واجب عدم التدخل، والذي تم النص عليه في الفقرة الرابعة من المادة الثانية من ميثاق الأمم الامم المتحدة، لما تقوم به تلك الهجمات من تسريب للبيانات والمعلومات الأمنية والسرية التي تحتويها المواقع الالكترونية ، كما أن الأمر لا يقف عند هذا الحد حيث أن تلك الهجمات تتسبب في ضرر للمدنيين لما تقوم به الهجمات السيبرانية من قطع للخدمات الحيوية.

وقد اختلفت الاراء الفقهية حول التكييف القانوني للهجمات السيبرانية، حيث ذهب جانب من الفقه الي القول بأن المدة التي جري فيها تقنين القواعد القانونية التي لها صلة باستخدام وسائل القتال وطرقه، لم يكن آنذاك لاستخدام الأنظمة الإلكترونية للأغراض العسكرية أي وجود بمعني أن تلك الوسائل غير مقننة في الأصل، وقد أشار ذلك الرأي إلي مدة إبرام الاتفاقيات، وذلك في منتصف القرن الثامن عشر وما بعدها، والمتمثلة في اتفاقية لاهاي واتفاقيات جنيف الأربع لعام ١٩٤٩ والبروتوكولين الاضافيين لعام ١٩٧٧، حيث لم يكن للهجمات السيبرانية أي ذكر [(١)].

وذهب جانب آخر من الفقه إلي القول بأن الهجمات السيبرانية يمكن تكييفها في ظل أحكام القانون الدولي العام على أساس أن الصورة الأولية تظهر أن تلك

(١) طلال ياسين العيسي، المرجع السابق، ص٨٧

الهجمات من الممكن أن يتم ارتكابها أثناء النزاعات المسلحة الدولية أو غير الدولية وفي أوقات السلم، وأن تكييف استخدام الهجمات السيبرانية يدور حول فرضيتين وهما علي النحو الآتي:

الفرضية الأولي: عدم إمكانية إثبات الدليل المادي الناجم عن استخدام الهجمات السيبرانية، ويعتبر ذلك الأمر هو العقبة التي تواجه المتخصصين، وذلك بخلاف وسائل القتال الأخرى التي تترك أثر مادي عند استخدامها.

الفرضية الثانية: إذا ثبت أن الهجمات السيبرانية يترتب عليها أثر مادي ملموس علي المستويات الاقتصادية والأمنية والعسكرية فهنا يكون المعيار في تكييف الهجمات السيبرانية، فيما إذا كانت من قبيل التصرف العدائي، أو كونها تصرف من أجل رد العدوان، حيث تعتمد بصورة أساسية علي القواعد القانونية ذات الصلة، وبالذات حكم الفقرة الرابعة من المادة الثانية من ميثاق الأمم المتحدة والتي نصت على أنه " يمتنع أعضاء الهيئة جميعاً في علاقاتهم الدولية عن التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو على أي وجه آخر لا يتفق ومقاصد "الأمم المتحدة."، والمادة ٥١ من ميثاق الأمم المتحدة التي نصت علي أنه " ليس في هذا الميثاق ما يضعف أو ينتقص الحق الطبيعي للدول، فرادى أو جماعات، في الدفاع عن أنفسهم إذا اعتدت قوة مسلحة على أحد أعضاء "الأمم المتحدة" وذلك إلى أن يتخذ مجلس الأمن التدابير اللازمة لحفظ السلم والأمن الدولي، والتدابير التي اتخذها الأعضاء استعمالاً لحق الدفاع عن النفس تبلغ إلى المجلس فورا، ولا تؤثر تلك التدابير بأي حال فيما للمجلس – بمقتضى سلطته ومسؤولياته المستمرة من أحكام هذا الميثاق – من

الحق في أن يتخذ في أي وقت ما يرى ضرورة لاتخاذه من الأعمال لحفظ السلم والأمن الدولي أو إعادته إلى نصابه." وتلك المواد ترتب آثار قانونية عند اللجوء إلي الهجمات السيبرانية.

المطلب الثاني

الهجمات السيبرانية في ضوء القانون الدولي الإنساني

نصت الفقرة الأولي من المادة ٣٥ من البروتوكول الإضافي الأول عام ١٩٧٧ علي " إن حق أطراف أي نزاع في اختيار أساليب ووسائل القتال ليس حقا لا تقيده قيود"، كما أنه يمكن الرجوع الي شروط مارتنز كأساس يتم من خلاله تفسير معاهدات القانون الدولي الإنساني كلما ثارت الشكوك حول معني بعض الأحكام الواردة فيه، وطبقا لتلك القاعدة فإنه يمكن القول أن كل ما يقع أثناء المنازعات فإنه يخضع لمباديء القانون الدولي الإنساني،، الأمر الذي يعني عدم خلو الهجمات السيبرانية من القانون أثناء النزاع المسلح، وهو الأمر الذي أكدته محكمة العدل الدولية في رأيها الاستشاري بشأن مشروعية التهديد بالأسلحة النووية أو استخدامها، حيث أشارت المحكمة إلي أن مباديء وقواعد القانون الدولي الإنساني المستقرة يتم تطبيقها على كافة أشكال الحروب وعلي كافة أنواع الأسلحة بما في ذلك تلك المستقبلية.

وطبقا لذلك فإن القانون الدولي الإنساني ينطبق علي الهجمات السيبرانية التي تحدث أثناء نزاع مسلح، وتثير الهجمات السيبرانية تحدي أما القانون الدولي الإنساني من حيث مدي إنطباق مباديء القانون الدولي الإنساني علي الهجمات السيبرانية وتلك المباديء علي النحو الآتي:

أولا: مبدأ الضرورة العسكرية

تحتل الضرورة الحربية موقعًا بارزًا فى مواثيق القانون الدولى الإنسانى، وفى ديباجة إعلان سان بيترسبورغ تمت الإشارة إلى ضرورات الحرب التى يجب أن تتوقف أمام مقتضيات الإنسانية(١).

وكذلك أكدت الفقرة الثانية من ديباجة اتفاقية لاهاى الرابعة لسنة ١٩٠٧ " مصالح الإنسانية "، واشارت الفقرة الخامسة من الديباجة نفسها إلى الحد من الحرب حسب ما تسمح به الضرورات العسكرية، ونجد أن اتفاقية جنيف وبروتوكولها الإضافى الأول بالخصوص أوردت موادًا محددة ورد فيها ذكر الضرورات الحربية، أو ما يرادفها مثل: عبارة " المقتضيات العسكرية الحتمية".

ويدور هذا المبدأ حول إطار فكرة قوامها أن: استعمال أساليب العنف والقوة والخداع فى الحرب تقف عند حد قهر العدو، وتحقيق الهدف من الحرب.

---

(١) فالهدف الوحيد الذى ينبغى للدول أن تسعى إلى تحقيقه أثناء الحرب حسب ما جاء فى إعلان سان بيترسبورع لعام ١٨٦٨ هو: " إضعاف القوة العسكرية للعدو، وإحدى الوسائل التى قد يلجأ إليها طرف محارب لتحقيق هذا الهدف القضاء على الأشياء التى يجوز اعتبارها أهدافًا عسكرية بأضيق معانى هذه الكلمة وأكثرها حرفية، أى وحدات القوة المسلحة للعدو، وعرباته المدرعة، ومدفعياته المتحركة، ومنشآته العسكرية، ومستودعات الذخيرة، فكون جميع هذه الأشياء جميعًا تمثل أهدافًا عسكرية هو أمر لا يحتمل الشك".

انظر فى ذلك: فريست كالهوفت، ليزابيث تسغفلد، ضوابط تحكم خوص الحرب، مدخل القانون الدولى الإنسانى، ترجمة أحمد عبد العليم، اللجنة الدولية للصليب الأحمر، ٢٠٠٤، ص ٥٢.

-للمزيد أنظر: د/ زحل محمد الأمين، دور القانون الدولي الإنساني في تعزيز حماية حقوق الإنسان، دار النهضة،٢٠١٨،ص١٩٣

ويمكن القول أن اللجوء إلي الهجمات السيبرانية يجب أن يكون ضروريا لتحقيق الهدف العسكري المشروع، وأما مسألة تحديد الأهداف والمنشآت العسكرية في الفضاء الإلكتروني تثير تحديا كبيرا أمام الدول وذلك لأن المنشآت التي تقدم خدماتها للجهد العسكري الضرورة هي في الوقت نفسه قد تخدم القطاع المدني، وأن عدم القيام بتحديد معايير منظمة لاستخدام تلك الهجمات سيعني إمكانية اللجوء لاستخدامها بداعي الضرورة العسكرية، لذلك فإن الأمر يتطلب تحديد وبيان ما يمكن اعتباره هدفا للهجوم السيبراني.

ثانيا : مبدأ التناسب

أكدت العديد من الاتفاقيات الدولية علي ضرورة مراعاة مبدأ التناسب في استخدام القوة في النزاع المسلح، منها ما تم النص عليه في البروتوكول الإضافي الأول لعام ١٩٧٧ حيث نصت الفقرة ٥/ب من المادة ٥١ من ذلك البروتوكول على أنه " الهجوم الذي يتوقع منه إحداث خسائر عرضية في أرواح المدنيين، إصابة المدنيين، الإضرار بالأعيان المدنية أو مزيجا منها الذي سيكون مفرطا فيما يتعلق بالميزة العسكرية المباشرة والملموسة المرتقبة"، أما بالنسبة للهجمات السيبرانية فنظرا لطبيعة الضرر الذي تحدثه تلك الهجمات فإن تحقق مبدأ التناسب يشكل فيها تحديا فريدا من نوعه أمام التنظيم الدولي وذلك لأن الآثار التي تحدثها الهجمات السيبرانية عادة ما تكون غير مباشرة.

وتحقيق مبدأ التناسب في الهجمات السيبرانية قد يكون أمر من الصعوبة بمكان تحققه والعلة في ذلك الأمر ترجع إلي أن تكنولوجيا المعلومات والاتصالات غير متساوية في الدول، ومن ثم تكون الدولة الضحية غير متطورة من ناحية تكنولوجيا الهجوم السيبراني لرد تلك الهجمات وتحقيق الأمن السيبراني، ويتطلب

تطبيق مبدأ التناسب توقع النتائج المحتملة للنشاط العدائي، وفيما يخص الهجمات السيبرانية والغموض الذي يكتنف تلك الهجمات والآثار التي تتسبب فيها، يجعل تطبيق مبدأ التناسب يتسم بالصعوبة بالنسبة للقادة العسكريين الذي عليهم في سياق الهجمات السيبرانية مواجهة المزيد من الشكوك والغموض بشأن شرعية الهجمات التي سينفذونها[١].

ثالثا: مبدأ التفرقة بين المقاتلين وغير المقاتلين[٢]

تم النص في البرتوكول الأول الإضافى إلى اتفاقيات جنيف لسنة ١٩٤٩ والصادر عام ١٩٧٧، في مادته ٤٨ على هذا المبدأ: " تعمل أطراف النزاع على التمييز بين السكان المدنيين والمقاتلين وبين الأعيان المدنية والأهداف العسكرية؛ ومن ثم توجه أعمالها ضد الأهداف العسكرية دون غيرها. "

---

(١) طلال ياسين العيسي، المرجع السابق،ص٦٣.

(٢) برغم ان ذلك المبدأ لم يستقر في أوروبا إلا في أواخر القرن التاسع عشر، إلا أن الشريعة الإسلامية الغراء قد عرفت ذلك المبدأ وأقرته منذ أربعة عشر قرنا من الزمان، فقد أقر النظام الإسلامي واجب حماية الأفراد المدنيين المسالمين والمنشأت المدنية. يتضح ذلك جليا من حديث الرسول الكريم _صلي الله عليه وسلم_ عندما قال لجيش أرسله:(انطلقوا باسم الله وعلي بركة رسول الله، لاتقتلوا شيخا فانيا، ولا طفلا، ولا صغيرا، ولا امرأة، ولا تغلوا، وضعوا غنائمكم، وأصلحوا، وأحسنوا؛ إن الله يحب المحسنين)، وفي حديث أخر يقول الرسول الكريم _صلي الله عليه وسلم_ (سيروا باسم الله وعلي بركة رسول الله وفي سبيل الله، قاتلوا أعداء الله، ولاتغلوا، ولاتغدروا، ولاتنفروا، ولاتمثلوا ولاتقتلوا وليدا)، ويقول لخالد بن الوليد في حديث أخر: (لاتقتل ذرية ولا عسيفا).

انظر في ذلك د/ أبوالخير احمد عطية، حماية السكان المدنيين والأعيان المدنية إبان النزاعات المسلحة، دار النهضة العربية، ١٩٩٨، ص٥٦، ٥٧.

وهذه القاعدة هى أساس قوانين الحرب وأعرافها، وفى صياغتها بوضوح وإدراجها فى معاهدة دولية تأكيد لأهميتها أيا كانت ظروف النزاعات المسلحة، ومن الملاحظ أن فئة غير المقاتلين أشمل من المدنيين، فالقوات المسلحة نفسها تتكون من مقاتلين وغير مقاتلين كأفراد الخدمات الطبية، والطوائف الدينية.

وتقتضى قاعدة التمييز بين المقاتلين، وغير المقاتلين من جهة والأهداف العسكرية والأعيان من جهة أخرى عدم استهداف المدنيين بالعمليات الحربية ومن أصبح غير قادر على أعمال القتال أى الجرحى والمرضى والغرقى وأسرى الحرب، وأى شخص هابط بمظلة بعد أن أصيبت طائرته، كما لا يستهدف بالعمليات الحربية أفراد الخدمات الطبية والدينية سواء كانوا مدنيين أم عسكريين، أو أفراد الدفاع المدنى، وأفراد منظمات الإغاثة الدوليين والمحليين المرخص لهم بتلك المهام[١].

وبالنسبة للهجمات السيبرانية فإن التحدي الأصعب الذي تواجهه تلك الهجمات هو التمييز بين المقاتلين وغير المقاتلين، وذلك الأمر يرجع إلي عدة أسباب منها إن الهجوم السيبراني في أغلب الأحوال ما يتم من خلال أشخاص قد يبعدون عن محل الهجوم لمسافات تتجاوز مئات الأميال وهو الأمر الذي يجعل التمييز بين المقاتلين وغير المقاتلين أمر غاية في الصعوبة.

---

(1)1-Gary D.Solis, The Law of Armed Conflict International Humanitrain Law in War, Campridge University Press ،2010, New York, p 251.

انظر أيضًا : د/ محمد عبد الكريم حسن ، مسئولية المقاتل عن انتهاك القانون الدولى الانسانى ، مركز الدراسات العربية للنشر والتوزيع ، ٢٠١٨.

– أنظر أيضًا : أزهر عبد عبد الامير الفتلاوى ، العمليات العدائية طبقا لقواعد القانون الدولى الانسانى ، مركز الدراسات العربية للنشر والتوزيع ، ٢٠١٨.

المطلب الثالث

الجهود الدولية في مكافحة الهجمات السيبرانية

يعتبر التعاون الدولي هو الوسيلة التي يمكن من خلالها مكافحة جريمة الهجمات السيبرانية إلا أن هذا التعاون يستلزم أن يتم التخفيف من غلو الفوارق بين الأنظمة العقابية الداخلية وذلك لأن هذا التباعد بين الأنظمة يجعل المجرم يقوم بالبحث عن الأنظمة الأكثر تسامحا، ولذلك تم إبرام العديد من الاتفاقيات الدولية في مجال التعاون الدولي من أجل مكافحة ذلك النوع من الجرائم، وتظهر معالم هذا التقارب في قبول حالات تفويض الاختصاص في اتخاذ إجراءات البحث والتحري والتفتيش والملاحقة وجمع الأدلة والاعتراف بالأحكام الجنائية.

وقد ادركت الدول العربية انه من الضروري ان يتم تقريب التشريعات الجزائية في الدول العربية من بعضها البعض، والتمكين من استخدام وسائل وتدابير فعالة من اجل التحقيق في ذلك النوع من الجرائم فبادرت بعقد اتفاقية فيما بينها تم التوقيع عليها في عام ٢٠١٠ ،وسمية تلك الاتفاقية بالاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وقد تضمنت تلك الاتفاقية مجموعة من الالتزامات تهدف الي توحيد الاجراءات الخاصة بجرائم تقنية المعلومات والجرائم المرتبطة بتلك التقنية[١].

وتعتبر تلك الاتفاقية من اهم الاتفاقيات التي تم ابرامها في مجال مكافحة الجريمة التقنية من اجل منع الجريمة والتحقيق فيها وملاحقة مرتكبيها مثل الاعتداء

---

(١) احمد خيدل، اجراءات جمع الادلة الرقمية طبقا للاتفاقية العربية لمكافحة جرائم تقنية المعلومات، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المركز الجامعي ،معهد الحقوق والعلوم السياسية، المجلد ١١، العدد الاول،٢٠٢٢ ،ص٢٣٣

علي سلامة البيانات وجرائم اساءة استخدام وسائل التقنية والتزوير والاحتيال والاباحية والاعتداء علي حرمة الحياة الخاصة والجرائم المتعلقة بالارهاب والمرتكبة من خلال تقنية المعلومات مثل القيام بنشر افكار جماعات ارهابية وتمويل العمليات الارهابية، وقد دعت الاتفاقية الدول الاطراف الي اقرار مجموعة من التدابير او الاجراءات التي لا تطبق الا علي المعلومات المخزنة داخل تقنية المعلومات ولكي تعد المعلومات مخزنة فإنه يجب ان تكون موجودة بالفعل(١).

ولقد كان الهدف من تلك الاتفاقية وفق ما نصت عليه المادة الاولي منها هو تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات لدرء اخطار هذه الجرائم حفاظا علي امن الدول العربية ومصالحها وسلامة مجتمعاتها وافرادها(٢).

كما سعت الأمم المتحدة إلي تأمين سلامة استخدام التكنولوجيا والشبكات المعلوماتية بشكل عام، فأصدرت من خلال الجمعية العامة ومجلس الأمن العديد من القرارات ومن تلك القرارات الآتي:

١-القرارين ٥٥/٦٣ و ٥٦/١٢١ عن الجمعية العامة واللذين يضعان الإطار القانوني بشأن مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية

٢-القرار ٥٧/٢٣٩ عن الجمعية العامة المتعلق بإنشاء ثقافة أمنية عالمية للفضاء السيبراني

(١) احمد خيدل المرجع السابق،ص٣٧٣

(٢) ينظر المادة الاولي من الاتفاقية

٣-القرار رقم ٥٨/١٩٩ عن الجمعية العامة المتعلق بإرسال ثقافة عالمية لأمن الفضاء الحاسوبي وحماية الهياكل الأساسية الحيوية للمعلومات.

٤- القرار رقم ٢٣٤١ لسنة ٢٠١٧ الصادر عن مجلس الأمن والذي يهيب فيه الدول الأعضاء إلي إنشاء أو تعزيز 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 ملائمة للاتصال والإنذار في حالات الطواريء

٥-القرار رقم ٢٣٧٠ لسنة ٢٠١٧ الصادر عن مجلس الأمن، وفي ذلك القرار حث مجلس الأمن الدول الأعضاء على العمل بصورة تعاونية لمنع الإرهابيين من حيازة الأسلحة من خلال تكنولوجيا المعلومات والاتصالات، مع احترام حقوق الإنسان والحريات الأساسية والامتثال للالتزامات بموجب القانون الدولي.

وفي ظل عدم وجود تشريع دولي ملزم للدول يمكن من خلاله مكافحة جرائم تقنية المعلومات بصفة عامة فقد فتح مجلس اوروبا باب التوقيع علي اتفاقية بودابست الدولية وذلك في ٢٠٠١/١١/٢٣ ودخلت حيز التنفيذ في ٢٠٠٤/٧/١ ،والتي تعتبر الصك الدولي الاول الذي اتجه لتجريم كافة اشكال الجريمة الالكترونية[١]،وادراكا من الدول الاعضاء بمجلس اوروبا والدول غير

(١) ايمن عبد الحفيظ،حدود مشروعية دور أجهزة الشرطة في مواجهة الجرائم المعلوماتية،مجلة مركز بحوث الشرطة بأكاديمية مبارك،العدد٢٥، يناير ٢٠٠٤ ،ص٣٨٩

الاعضاء والموقعة علي الاتفاقية لعمق التعييرات التي احدثتها الرقمية والتقارب والعولمة المستمرة للشبكات المعلوماتية،فقد بينت المذكرة التفسيرية لتلك الاتفاقية ان هناك سمة بارزة في تكنولوجيا المعلومات تتمثل في الاثر المترتب علي تطور التكنولوجيا والاتصالات.(١)

وقد تضمنت اتفاقية بودابست الاوروبية لعام ٢٠٠١ ثمان واربعين مادة، فجاء الباب الاول من الاتفاقية ليبين المصطلحات المستخدمة في تلك الاتفاقية، وتعتبر تلك الاتفاقية من اوائل الاتفاقيات التي تصدت للاستخدام غير المشروع للحاسبات وشبكات المعلومات، وقد تبين ذلك فيما ورد بالقسم الاول من الباب الثاني نت الاتفاقية في المادة الثانية منها حتي المادة الحادية عشر، بالاضافة الي تحديد معيار مشترك لوضع الحد الأدنى لذي يسمح باعتبار بعض التصرفات من قبيل الجرائم الجنائية الامر الذي يفرض وجود تجانس علي المستويين القومي والدولي، وعلي ذلك الاساس يمكن التوافق التشريعي الداخلي بين الدول من اجل مقاومة التصرفات غير المشروعة لاسيما الدول التي اتخذت تشريعاتها الداخلية معيار اقل صرامة من الاتفاقية(٢).

ويعد الغرض من ابرام اتفاقية بودابست لمكافحة الجرائم الالكترونية هو القيام باستكمال المعاهدات او الترتيبات ثنائية او متعددة الاطراف فيما بين الاطراف خاصة في الاتي:

---

(١) هلالي عبد اللاه احمد،اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها،دار النهضة العربية،القاهرة،الطبعة الثامنة،٢٠١١، ص٥

(٢) هند نجيب السيد مطر، الاثبات في الجرائم الالكترونية،رسالة دكتوراة،كلية الحقوق،جامعة القاهرة،٢٠١٦،ص٥٩

-الاتفاقية الاوروبية المتعلقة بتسليم المجرمين والتي فتحت للتوقيع في باريس بتاريخ ١٣ ديسمبر عام ١٩٥٧.

-الاتفاقية الاوروبية المتعلقة بالمساعدة المتبادلة بين الدول في المسائل الجنائية والتي فتح التوقيع عليها في بستراسبورغ في ٢٠ ابريل عام ١٩٥٢.

-البروتوكول الاضافي للاتفاقية الاوروبية المتعلقة بشأن المساعدة المتبادلة في المسائل الجنائية والتي فتح التوقيع عليها بستراسبورغ في ١٧ مارس عام ١٩٧٨[١]

(١) ينظر المادة ٣٩ الفقرة الاولي من اتفاقية بودابست الاوروبية المتعلقة بالجرائم الالكترونية

الخاتمة

تعتبر الهجمات السيبرانية نتيجة للتطور التكنولوجي الرهيب الذي يشهده العالم، وهي جريمة من الجرائم المعلوماتية التي ترتبط بالحاسب الآلي، وتعتبر تلك الهجمات واحدة من أهم التحديات المعاصرة التي تواجه كافة دول العالم، لما لتلك الهجمات من تداعيات على الأمن القومي للدول، لما يترتب عليها من خطر اختراق البيانات والمعلومات وبث إشاعات تخلق الفوضي والرعب لدي المواطنين، كما تؤثر تلك الهجمات على العلاقات الدولية الأمر الذي اصبح معه من الضروري بمكان أن يتم مواجهة تلك الهجمات والتصدي لها.

النتائج:

١-برزت مخاطر الهجمات السيبرانية كواحدة من المخاطر التي تواجه الدول لاسيما الدول التي لا تمتلك قدر كافي من التكنولوجيا يساعدها في التصدي لتلك الهجمات الأمر الذي يعرضها لاختراق بياناتها والتأثير على الخدمات الأمنية والسياسية والاقتصادية والاجتماعية داخل الدول.

٢-لا تتطلب الهجمات السيبرانية حشودا من المقاتلين العسكريين والآلاف من الأسلحة كالنزاعات المسلحة التقليدية، بل أنه يكفي شخص واحد يمتلك الخبرة الكافية والمهارة اللازمة لشن تلك الهجمات

٣-أجمع الفقهاء على أن الهجمات السيبرانية التي يتم حدوثها أثناء النزاع المسلح التقليدي تخضع للقانون الدولي الإنساني.

٤-يلعب التعاون الدولي دور كبير في الحد من الهجمات السيبرانية بوصف أن تلك الجريمة تعتبر من الجرائم العابرة للحدود.

٥-هناك جهود دولية وإقليمية لمكافحة جريمة الهجمات السيبرانية تبدو من خلال الاتفاقيات الدولية والقرارات الصادرة عن الأمم المتحدة من خلال الجمعية العامة للأمم المتحدة ومجلس الأمن.

التوصيات:

١-ضرورة العمل على تدريب الكوادر البشرية علي أبرز تطورات وأنواع تكنولوجيا المعلومات من أجل مواجهة الهجمات السيبرانية التي قد تتعرض لها الدولة والعمل على حماية الأنظمة المعلوماتية الأمنية.

٢-ضرورة رفع الوعي لدي المجتمع الدولي بمخاطر الاستخدامات غير السلمية للتكنولوجيا علي الخدمات الاجتماعية والاقتصادية والأمنية والسياسية ، لما تقوم به تلك الهجمات من تعطيل لتلك الخدمات.

٣-ضرورة سعي كافة الدول لاسيما الدول النامية إلي تطوير أمنها السيبراني والاستفادة من خبرات الدول المتقدمة في هذا الشأن.

٤-ضرورة السعي نحو اعتماد اتفاقية دولية يتم من خلالها تنظيم الهجمات السيبرانية، وتجريم تلك الاتفاقيات بصورة واضحة وإقرار عقوبة دولية في حالة القيام بارتكاب الهجمات السيبرانية.

قائمة المراجع

أولا: الكتب

١- أبوالخير احمد عطية، حماية السكان المدنيين والأعيان المدنية إبان النزاعات المسلحة، دار النهضة العربية، ١٩٩٨.

٢- أحمد عبيس نعمة الفتلاوي، الهجمات السيبرانية دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، منشورات زين الحقوقية، الطبعة الأولي،لبنان،٢٠١٨.

٣- أزهر عبد عبد الامير الفتلاوى ، العمليات العدائية طبقا لقواعد القانون الدولى الانسانى ، مركز الدراسات العربية للنشر والتوزيع ، ٢٠١٨.

٤- زحل محمد الأمين، دور القانون الدولي الإنساني في تعزيز حماية حقوق الإنسان، دار النهضة،٢٠١٨.

٥- شادي منصور، حروب الجيل الخامس، أساليب التفجير من الداخل على الساحة الدولية، دار المنهل، ٢٠١٩.

٦- فرد كابلان، ترجمة لؤي عبد المجيد، المنطقة المعتمة: التاريخ السري للحرب السيبرانية، عالم المعرفة، المجلس الوطني للثقافة والفنون والاداب،الكويت،٢٠١٩.

٧- فريست كالهوفت، ليزابيث تسغفلد، ضوابط تحكم خوص الحرب، مدخل القانون الدولى الإنسانى، ترجمة أحمد عبد العليم، اللجنة الدولية للصليب الأحمر، ٢٠٠٤.

٨- محمد عبد الكريم حسن ، مسئولية المقاتل عن انتهاك القانون الدولى الانسانى ، مركز الدراسات العربية للنشر والتوزيع ، ٢٠١٨.

٩- هلالي عبد اللاه احمد،اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقا عليها،دار النهضة العربية،القاهرة،الطبعة الثامنة،٢٠١١.

ثانيا: الرسائل

١- نور أمير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الإنساني، رسالة ماجستير، الجامعة الافتراضية السورية،٢٠٢١.

٢- هند نجيب السيد مطر، الاثبات في الجرائم الالكترونية،رسالة دكتوراة،كلية الحقوق،جامعة القاهرة،٢٠١٦.

ثالثا: الدوريات

٣- احمد خيدل، اجراءات جمع الادلة الرقمية طبقا للاتفاقية العربية لمكافحة جرائم تقنية المعلومات، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المركز الجامعي ،معهد الحقوق والعلوم السياسية، المجلد ١١، العدد الاول،٢٠٢٢.

٤- أميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، العدد الخامس والثلاثون، الجزء الثالث،٢٠٢٠.

٥- ايمن عبد الحفيظ،حدود مشروعية دور أجهزة الشرطة في مواجهة الجرائم المعلوماتية،مجلة مركز بحوث الشرطة بأكاديمية مبارك،العدد٢٥، يناير ٢٠٠٤.

٦- حسن مظفر الرزو، الفايروسات والحاسب الإلكتروني: المخاطر المحتملة وسبل الحد منه، المجلة العربية العلمية للفتيان، المنظمة العربية للتربية والثقافة والعلوم، المجلد الاول، العدد الثاني،١٩٩٧.

٧- سحر قدوري الرفاعي، الحكومة الالكترونية وسبل تطبيقها: مدخل استراتيجي، مجلة اقتصاديات شمال افريقيا، العدد السابع، جامعة حسيبة بو على،٢٠١٦.

٨- طلال محمد الحاج ابراهيم، الهجمات الالكترونية والمسؤولية الجنائية للقادة، المجلة القانونية والقضائية، وزارة العدل–مركز الدراسات القانونية والقضائية، السنة ١٢، العدد الأول،٢٠١٨.

٩- طلال ياسين العيسي، المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي، مجلة الزرقا للبحوث والدراسات الإنسانية،المجلد ١٩، العدد ١، ٢٠١٩.

١٠-عمار ياسر محمد زهير، التحديات الأمنية المعاصرة للهجمات السيبرانية، القيادة العامة لشرطة الشارقة مركز بحوث الشرطة، المجلد ٣٠، العدد١١٨،٢٠٢١.

١١– المركز الاستشاري للدراسات والتوثيق، التحولات في العقيدة العسكرية الامريكية، دعائم الضعف السبع، اوراق استراتيجية، غير دورية، تعني بالشؤون الاستراتيجية، العدد ٢ ايلول ٢٠١٤،بيروت.

رابعا: المراجع الأجنبية

1- Diego Rafael Canabarro and Thiago Borne," Reflection on the fog of Cyber War", National Center for Digital Government, Policy working Paper No.13:001, March 1, 2013, footnote 11

2- Gary D.Solis, The Law of Armed Conflict International Humanitrain Law in War, Campridge University Press,New York,2010

3- Marco Roscini," World Wide Warfare – Jus ad bellum and the use of Cyber Force",Max Planck Yearbook of United Nations Law, Volume 14,2010.

4- Tang Lan, Zhang Xin, Harry D. Raduege, Jr., Dmitry I. Grigoriev, Pavan Duggal, and Stein Schjølberg,"Global Cyber Deterrence Views from China, the U.S., Russia, India, and Norway", The EastWest Institute, Printed in the United States, 2010.

5- Zimet .E.and C. L. Barry," Military services Overview, Cyber power and National Security", National Defense University Press ,Washington, DC,USA,2009.