جامعة 8 ماي 1945 قالمة

كلية الحقوق والعلوم السياسية

قسم الحقوق تخصص قانون عام

مذكرة مكملة لمتطلبات نيل شهادة الماستر في القانون

الهجمات السيبرانية وأثرها على تهديد السلم والأمن الدوليين

إعداد الطلبة:

1/ غجاتي سهيلة

2/ راهـــم أميـــرة

تحت إشراف

الدكتورة: فتيسي فوزية

تشكيل لجنة المناقشة

الرقم	الأستاذ	الجامعة	الرتبة العلمية	الصفة
1	عقابي أمال	جامعة 8 ماي 1945	أستاذ التعليم العالي	رئيساً
2	فتيسي فوزية	جامعة 8 ماي 1945	أستاذ محاضر "أ"	مشرفاً
3	مفتاح ياسين	جامعة 8 ماي 1945	أستاذ محاضر "ب"	عضواً مناقشاً

السنة الجامعية:2024/2023

شكر وتقدير

نحمد الله عز وجل الذي وفقنا في إتمام هذا البحث العلمي، والذي وهبنا الصحة والعافية والعزيمة.

قال رسول الله صلى الله عليه وسلم: **"من صنع إليكم معروفا فكافئوه، فإن لم تجدوا ما تكافئوه فادعوا له حتى تروا أنكم قد كافأتموه".**

نتقدم بجزيل الشكر والتقدير إلى الدكتورة: فتيسي فوزية على كل ما قدمته لنا من توجيهات ومعلومات قيمة ساهمت في إثراء موضوع دراستنا، وألف شكر لقلبك الطيب، وشخصك الكريم.

كما نتقدم بجزيل الشكر إلى أعضاء لجنة المناقشة الموقرة الدكتورة: عقابي أمال، والدكتور: مفتاح ياسين.

وأخيرا نتقدم بجزيل الشكر إلى كل من مدو لنا يد العون والمساعدة في إخراج هذه الدراسة على أكمل وجه نخص بالذكر الدكتورة الكريمة: وردة درارجة، والأستاذة: اسمهان بعيري بجامعة الطارف اللتان كان لهما الفضل الكبير في توفير المراجع المعتمدة في هذا البحث، وكذلك موظفي الإدارة ومكتبة جامعة 8ماي 1945 خاصة خوالدية لطيفة.

الإهداء

أهدي مجهوداتي هذا العمل المتواضع

إلى أبي روح قلبي، تعجز كلماتي عن شكرك وتقديرك على كل ما فعلته معي طوال حياتي، لو بيدي العمر لأعطيك، ومع كل هذا فحقك لن أوفيك.

إلى أمي شمعة حياتي أنت مثل نجوم السماء التي تشع بريقا في حياتنا شكرا إلى وقوفك جوارنا لتحقيق الآمال يفوق الخيال.

إلى من شجعني على مواصلة مسيرتي العلمية رفيق دربي زوجي فوزي أهديك تحياتي وأمنياتي أن تبقى رفيقي في كل أفراحي وأحزاني إلى الأبد.

إلى أحباب قلبي أولادي صغاري: ندى كان لها الفضل في كتابة هذا البحث، آمنة، أمين أتمنى الله أن يوفقكم ويرزقكم الصحة والعافية وصلاح البال ويجعلكم من النجباء.

إلى رياحين حياتي أخوتي: سامي شفاه الله عز وجل وعائلته، حسام وعائلته، وفخرالدين وفقه الله.

إلى الأخت التي لم تلدها أمي ربيعة وزوجها وأولادها.

إلى كل أهل زوجي الأم الغالية مليكة، محمد، أحمد وعائلته، حمزة وعائلته، و إلى كل أهلي كبير وصغير "غجاتي" و"زدادرة"، وإلى كل من شجعني وساعدني على إتمام هذا العمل خاصة الأخ غاني .

إلى كل من علمني حرف من الابتدائي إلى التعليم العالي، إلى كل زميلاتي وزملائي في المسار الدراسي دون استثناء.

إلى زميلات وزملاء العمل عائلتي الثانية خاصة سارة، عليمة، نادية، مديحة، سعيدة، أمال، صليحة، رجاء، حكيمة.

إلى زملائنا الفلسطيين ندعو لشهدائهم بالرحمة ولأهاليهم بالفرج والنصر.

الإهداء

أهدي ثمرة جهودي في هذا العمل المتواضع

إلى أبي الغالي، من علمني معنى العطاء والمثابرة كل الشكر والتقدير لك على كل ما فعلته معي طوال حياتي.

إلى روح أمي الزكية الطاهرة، رحمة الله عليك وجعل مثواك الفردوس الاعلى.

إلى شريك حياتي زوجي الغالي رياض أشكرك على مساعدتك ومساندتك في السراء والضراء.

إلى أحباب قلبي أولادي صغاري: أنيس قرة عيني، تسنيم، رنا أتمنى من الله أن يوفقكم ويرزقكم الصحة والعافية والنجاح في دربكم.

إلى سندي في الحياة أخوتي: فريد، وليد، حسام، منى مؤنستي في الحياة، وفقهم الله.

إلى كل الأهل والاقارب وأخص بالذكر الصديقة الوفية نسرين .

إلى كل من شجعني وساعدني على إتمام هذا العمل خاصة محافظ الدولة بالمحكمة الادارية بقالمة.

إلى كل الزميلات والزملاء بالعمل بالمحكمة الادارية بقالمة.

مقـدمـــــة

مقدمــة:

منذ ظهور الانترنت وبروز التكنولوجيا الالكترونية والمعلوماتية في فجر الألفية الثالثة، راحت المجتمعات تتغير سريعا وجذريا، أدى ذلك إلى تطور الأدوات والاختراعات والخدمات، نتج عنها نوع جديد من المعاملات يسمى بالمعاملات الالكترونية، وذلك في عصر الثورة الصناعية الرابعة التي تختلف عن الثورات السابقة في شدتها واتساع نطاقها استناد على التحول الرقمي الذي يشمل انترنت الأشياء والحوسبة السحابية وتحليلات البيانات الضخمة والذكاء الاصطناعي.

ومع تطور المجتمعات والثورة الرقمية، والتوجه نحو مجتمع المعلومات برز الفضاء الخارجي أو المجال السيبراني (cyber space) ، كمجال خامس إلى جانب البر والبحر والجو والفضاء الخارجي، هذا المجال الجديد أحدث تغييرات جذرية في العلاقات الدولية، وبالتزامن مع هذا التطور الكبير في الشبكة العنكبوتية وزيادة الاعتماد عليها ظهر ما يسمى: قراصنة المعلومات أو الهاكرز "Hakers"، وهم يملكون القدرة في المواقع المحظورة في نظم شبكات الحواسيب بمختلف أشكالها، وبهذا أصبحت الهجمات السيبرانية من أهم التحديات التي يواجهها المختصون في القانون الدولي العام، وهاجسا يخيف العالم الذي يتعرض لهذه الهجمات عبر التكنولوجيا الحديثة وبث أفكارهم عن طريق هجمات واختراعات وتسلسل داخل النظم المعلوماتية إما بغرض تدمير تلك النظم أو الحصول على معلومات سرية سواء عسكرية أو اقتصادية، الأمر الذي ينبه بوجود مخاطر على الصعيد الدولي و الوطني فلابد من إيجاد سبل للتصدي لهذه الظاهرة.

وتمثل الهجمات السيبرانية الخطر الداهم الذي يواجه المجتمع الدولي نظرا لإتساع حجم تأثيرها، حيث لا تقتصر آثار هذه الهجمات على البيانات في أجهزة الكومبيوتر، بل تؤثر أيضا على سيادة الدول ومصالحها الحيوية، وقد تتعدى آثارها إلى تهديد الأمن والسلم الدوليين.

1- أهمية الموضوع:

نظرا لتزايد الهجمات السيبرانية في الآونة الأخيرة وعدم وجود أساس قانوني ينظمها وصعوبة تحديد الجهة التي صدرت عنها هذه الهجمات، تتضح لنا أهمية البحث في موضوع الهجمات السيبرانية كونه موضوع لا يزال في طور التبلور، والذي يندرج ضمن الدراسات الأمنية والاستراتيجية، والتي برزت بعد نهاية الحرب الباردة، كما يشهد موضوع الهجمات السيبرانية أهمية من التصاعد المطرد للهجمات في الفضاء السيبراني من جهة والتداعيات السلبية لهذه الهجمات من جهة أخرى .

و تظهر أهمية هذه الدراسة في كونها تعالج مسألة التكييف القانوني للهجمات السيبرانية التي تقع بين الدول، من حيث كونها جريمة سيبرانية تحكمها اتفاقية بودابست عام 2001 المتعلقة بالجريمة السيبرانية، أم هي حرب سيبرانية تخضع لأحكام دليل تالين لعام2013، أم هي جريمة دولية ذات طابع خاص.

2- أسباب اختيار الموضوع:

تنقسم أسباب ودوافع اختيار الموضوع إلى ما هو ذاتي وما هو موضوعي:

2-1- الأسباب الذاتية: وتظهر عموما في الرغبة الشخصية بالتعمق في موضوع الهجمات السيبرانية، وتحديد تكييفها القانوني والمسؤولية الدولية الناشئة عنها ضمن التنظيم الدولي المعاصر، ومع تزايد الهجمات السيبرانية في الوقت الراهن خصوصا مع بداية- الحرب الروسية الأوكرانية- ازدادت معها الرغبة في معرفة التداعيات التي يمكن أن تحدثها هذه الهجمات على العلاقات الدولية وكذا الأمن والسلم الدوليين.

2-2- الأسباب الموضوعية: ترجع دوافع اختيار هذا الموضوع إلى مجموعة من الاعتبارات تتصدرها حداثة الموضوع وارتباطه بعدة فروع من القانون، كما أنه محل نقاش وخلاف بين المختصين في القانون الدولي العام نظرا لتنوع أشكال هذه التهديدات وتزايد آثارها وانعكاساتها على جميع الأصعدة الدولية، إن مسألة التكييف القانوني لهذه الهجمات من حيث كونها جريمة سيبرانية أم حرب سيبرانية أو أنها جريمة دولية ذات طابع خاص تستدعي الدراسة والتحليل لفهم هذه التهديدات المتنامية وتداعياتها وكذا سبل مكافحتها، ومن هنا كان لابد أن يثير هذا الموضوع الحساس بكل أبعاده وتداعياته اهتماما خاصا لدينا ويدفعنا إلى تعميق البحث فيه ورصد مستجداته في إطار تحليل علمي قانوني.

3- أهداف الدراسة:

يهدف هذا البحث إلى محاولة الوصول لتحقيق أهداف عديدة وعلى وجه الخصوص، منها ما هو علمي، ومنها ما هو عملي، فبالنسبة للأهداف العلمية فتتمثل في السعي إلى وضع إطار مفاهيمي للهجمات السيبرانية، وكذا رصد تداعياتها على مختلف المستويات الأمنية والسياسية والاقتصادية والاجتماعية، وكذا دراسة وتحليل الإطار القانوني الرادع للهجمات السيبرانية.

أما من الناحية العملية فتسعى الدراسة إلى تحقيق جملة الأهداف نجملها في النقاط التالية:

- تحديد أهم الاتجاهات التي تبناها المجتمع الدولي في تعريف الهجمات السيبرانية وتمييزها عن المفاهيم المختلفة.
- تسعى هذه الدراسة إلى القاء الضوء على أبرز أنواع الهجمات وطرق تطبيقها.
- العمل على إيجاد سبل وآليات متكاملة للحد من تداعيات الهجمات السيبرانية على الأمن والسلم الدوليين.
- البحث على مدى فاعلية وكفاية الجهود الدولية والإقليمية في الحد من تزايد التهديدات السيبرانية.

4- الدراسات السابقة:

تعد الدراسات السابقة في هذا الموضوع قليلة نوعا ما، نظرا لحداثة المصطلح والاهتمام المتأخر به، ولعل من أهم الدراسات التي لها علاقة بالموضوع نذكر:

- **الدراسة الأولى:** للطالب طلال محمد الحاج إبراهيم، الهجمات السيبرانية على شبكات الحاسوب في ضوء القانون الدولي الإنساني، رسالة دكتوراه، كلية الحقوق، جامعة دمشق، 2020، وقد تناولت الدراسة الفضاء السيبراني والهجمات السيبرانية من حيث الأهمية الاستراتيجية للفضاء السيبراني ومفهوم الهجمات السيبرانية وتداعيات هذه الهجمات على الأمن الدولي والنزاعات المسلحة، وأيضا قانون النزاعات المسلحة من حيث الانطباق على الهجمات السيبرانية وذلك من خلال الحديث عن الهجمات السيبرانية والتحول في استخدام القوة في العلاقات الدولية ومشروعية استخدام الهجمات السيبرانية في حالة النزاع المسلح وفي القسم الثاني من الدراسة تناولت المشاركة المباشرة في الهجمات السيبرانية من ناحيتين، الأولى التطرق للمسؤولية الدولية عن تصرفات المشارك المباشر في الهجمات السيبرانية والثانية المسؤولية الجنائية عن المشاركة المباشرة وأهم الجهود الدولية المبذولة في تأمين الاستخدام السلمي للقضاء السيبراني.

أما دراستنا فقد ركزت على الإطار المفاهيمي والقانوني للهجمات السيبرانية، من حيث خصائصها وتمييزها عن مختلف المفاهيم المشابهة، ومخاطر وأبعاد الهجمات السيبرانية، وكذلك تكييف الهجمات السيبرانية ومدى المسؤولية الدولية الناشئة عنها، كما تعرضت إلى تأثير الهجمات السيبرانية على السلم والأمن الدوليين وآليات مواجهتها، من خلال انعكاسات الهجمات السيبرانية على السلم والأمن الدوليين وإلى الجهود الدولية من حيث الجهود الغربية والإفريقية والعربية لمواجهة الهجمات السيبرانية.

- **الدراسة الثانية:** للطالبة زهراء عماد محمد كلنتر، المسؤولية الدولية الناشئة عن الهجمات السيبرانية، رسالة ماجستير، كلية الحقوق، جامعة الكوفة، 2016، وقد تناولت الدراسة الهجمات السيبرانية من حيث

ماهيتها، وتطور الهجمات السيبرانية وطبيعتها وسياسة الدول وموقفها ونماذج عنها، وفي القسم الثاني من الدراسة تناولت تكييف الهجمات السيبرانية والمسؤولية الدولية الناشئة عنها في ضوء أحكام القانون الدولي، من خلال بيان تكييف الهجمات السيبرانية من ناحيتين، الأولى في ظل مبدأ مسوغات الحرب، والثانية في ظل مبدأ سلوكيات الحرب، وأيضا تناولت الهجمات السيبرانية في ظل التنظيم الدولي المعاصر من حيث التنظيم القانوني بشأن المسؤولية الدولية، وبيان الجهود الدولية في تنظيم الهجمات السيبرانية.

أما دراستنا فقد ركزت على الإطار المفاهيمي والقانوني للهجمات السيبرانية، من حيث مفهوم الهجمات السيبرانية من خلال تعريفها وخصائصها وتمييزها عن مختلف المفاهيم المشابهة، ومخاطر وأبعاد الهجمات السيبرانية، كما تعرضت إلى تأثير الهجمات السيبرانية على السلم والأمن الدوليين وآليات مواجهتها، من خلال انعكاسات الهجمات السيبرانية على السلم والأمن الدوليين وإلى الآليات الدولية والإقليمية في مواجهة الهجمات السيبرانية من حيث الجهود الغربية والإفريقية والعربية لمواجهة الهجمات السيبرانية.

– **الدراسة الثالثة:** للطالبة اسمهان بعيري، الهجمات السيبرانية وأثرها على تهديد الأمن والسلم الدوليين، رسالة ماستر، تخصص قانون عام معمق، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الشاذلي بن جديد الطارف (الجزائر)، 2023، وقد تناولت الإطار المفاهيمي للهجمات السيبرانية، من حيث مفهوم الهجمات السيبرانية وتكييف الهجمات السيبرانية والمسؤولية الدولية الناشئة عنها كما تعرضت إلى مظاهر تأثير الهجمات السيبرانية على السلم والأمن الدوليين وسبل مواجهتها، من حيث التطرق إلى مظاهر تأثير الهجمات السيبرانية على السلم والأمن الدوليين، والآليات الدولية والإقليمية في مواجهة الهجمات السيبرانية.

في حين ركزت دراستنا على الإطار القانوني للهجمات السيبرانية، وخصائصها ومخاطر وأبعاد الهجمات السيبرانية، ثم كما تعرضت إلى انعكاسات الهجمات السيبرانية على الأمن، وإلى الجهود الدولية والمتمثلة في الجهود الغربية، والجهود الإفريقية والعربية لمواجهة الهجمات السيبرانية.

5- صعوبات الدراسة:

من الطبيعي أن أي بحث لا يخلو من الصعوبات ولكن حجمها يختلف من بحث لآخر، ومن أهم الصعوبات التي واجهتنا أثناء إعدادنا لهذه المذكرة ضيق الوقت بسبب التزامنا بالعمل والدراسة في أولى ماستر لم نتفرغ للمذكرة فحسب، والأهم من ذلك نقص المراجع التي تتحدث عن الهجمات السيبرانية نظرا لحداثة الموضوع وخاصة الفصل الثاني من حيث انعكاسات الهجمات السيبرانية والجهود المبذولة في مواجهة تلك الهجمات، وبالنظر لقائمة المراجع نجدها ثرية بالمراجع إلا أن كل مرجع يتناول عنصر معين وباختصار لم يقدم لنا ما نحتاجه ولم يخدمنا بالشكل الفعال، إذ اعتمدنا بشكل كبير على المراجع العامة و الإلكترونية.

6- إشكالية البحث:

باتت الهجمات السيبرانية نوع جديد من أنماط الجريمة وتتميز بأهم خاصية أنها عابرة للحدود الإقليمية للدول، مما أدى إلى توجه المجتمع الدولي للتعاون من أجل التصدي لتلك الجرائم، التي باتت تهدد سيادة الدول و أمنها وتطرح الدراسة إشكالية رئيسية مفادها:

ما مدى تأثير الهجمات السيبرانية على السلم والأمن الدوليين ؟

وتندرج تحت هذه الإشكالية الرئيسية عدة أسئلة فرعية تمثلت في:

- ما مفهوم الهجمات السيبرانية ؟ وما هي مخاطر وأبعاد الهجمات السيبرانية ؟
- ما هو تكييف الهجمات السيبرانية، وما مدى المسؤولية الدولية الناشئة عنها ؟
- ما مدى تأثير الهجمات السيبرانية على السلم والامن الدوليين ؟
- وماهي الآليات والجهود الدولية المبذولة لمواجهة الهجمات السيبرانية ؟

7- المناهج المتبعة في الدراسة:

تطلب إعداد هذه المذكرة المناهج التالية:

- **المنهج الوصفي:** حيث استدعى طبيعة البحث استعراض مفهوم الهجمات السيبرانية وأنواعها وخصائصها.
- **المنهج التحليلي:** وقد استعننا به في إطار تحليل قواعد القانون الدولي في سبيل تكييف الهجمات السيبرانية وتحديد المسؤولية الدولية الناشئة عنها، كما برز استعمال المنهج التحليلي عند تحليل بنود

مختلف الاتفاقيات والقوانين الصادرة عن المنظمات الدولية والإقليمية والتي تهدف إلى مكافحة الهجمات السيبرانية، وأبرزها اتفاقية بودابست لعام 2001.

8- الخطة (تقسيم البحث):

للإجابة عن الإشكالية المطروحة قسمنا البحث إلى فصلين، تناولنا في الفصل الأول **الإطار المفاهيمي والقانوني للهجمات السيبرانية** وقسم هذا الفصل الى مبحثين، الإطار المفاهيمي للهجمات السيبرانية (المبحث الأول)، ثم الإطار القانوني للهجمات السيبرانية (المبحث الثاني)، أما الفصل الثاني فتناولنا فيه **تأثير الهجمات السيبرانية على السلم والأمن الدوليين وسبل مواجهتها**، والذي قسم بدوره إلى مبحثين، تعرضنا في المبحث الأول إلى انعكاسات الهجمات السيبرانية على السلم والأمن الدوليين وإلى الجهود الدولية في مواجهة الهجمات السيبرانية(المبحث الثاني)، لنختم المذكرة بخاتمة احتوت على جملة من النتائج و الاقتراحات.

الفصل الأول: الإطار المفاهيمي والقانوني للهجمات السيبرانية

الفصل الأول: الإطار المفاهيمي والقانوني للهجمات السيبرانية

مع ظهور تكنولوجيا الإعلام والاتصالات أدى إلى اعتماد المجتمعات في مختلف الأبعاد السياسية والأمنية والاجتماعية والاقتصادية، على شبكات الكمبيوتر والانترنت، والتي جعلته يواجه مخاطر جديدة، ومنه ظهور الهجمات السيبرانية التي لا تقتصر آثارها على البيانات في أجهزة الكمبيوتر وأنظمته بل تتجاوز ذلك لتقوم بالتأثير على العالم الحقيقي كاختراق أنظمة الكمبيوتر للسيطرة على الحركة الجوية، وبهذا ظهرت المسؤولية الدولية عن الأضرار الجسيمة التي نجمت عن الهجوم السيبراني في العالم الافتراضي التي من خلالها يمكن مواجهة المخاطر الناشئة عنها والحفاظ على الأمن السيبراني.

وباعتبار أن امتلاك أي شخص القليل من الخبرات التقنية أن يلحق الضرر بالفضاء السيبراني لجهة أخرى، أصبح بإمكان المهاجمين السيبرانيين الهجوم على شبكات أي دولة من دون إنذار مسبق.

ولدراسة موضوع الهجمات السيبرانية، لا بد من تحديد مفهومها، وكذا الإطار القانوني الذي يحكمها، وهذا ما سنتناوله من خلال الإطار المفاهيمي للهجمات السيبرانية (المبحث الأول)، ثم الإطار القانوني للهجمات السيبرانية (المبحث الثاني).

المبحث الأول: الإطار المفاهيمي للهجمات السيبرانية

يعد المفهوم من أهم المفاتيح التي يجب التحكم فيها في البحث العلمي ذلك أن المفهوم يسمح بفحص وتحديد طبيعة الإشكالية المراد دراستها، وباعتبار أن الهجمات السيبرانية من أهم التحديات المعاصرة التي يواجهها المختصون في القانون الدولي العام، لما لها من تداعيات على الأمن القومي للدول وكذا السلم والأمن الدوليين، ومع التطور السريع في شبكة الأنترنت وزيادة الاعتماد عليها، اعتبرت هذه الهجمات أيضا تصرفات قد تكون من قبل دول ذات سيادة أو من قبل منظمات وعصابات، وقد تكون أيضا من مصادر مجهولة تشن ضد شبكات أو أنظمة معلوماتية تابعة لجهات أخرى، و ذلك من أجل تحقيق أهداف أمنية، عسكرية أو اقتصادية.

وللتفصيل في هذه المسألة سنتطرق إلى مفهوم الهجمات السيبرانية (المطلب الأول)، ثم إلى مخاطر وأبعاد الهجمات السيبرانية (المطلب الثاني).

المطلب الأول: مفهوم الهجمات السيبرانية

يعتمد مفهوم الهجمات السيبرانية أساسا على اختراق مواقع الدول في العالم أو أنظمتها المعلوماتية المتعلقة بالقطاعات الاستراتيجية كالدفاع والطاقة والاتصالات، وذلك إما عن طريق التجسس عليها أو تعطيل خدمتها أو سرقة معلوماتها.

وبذلك سنتطرق إلى الهجمات السيبرانية من خلال تعريف الهجمات السيبرانية وتمييزها عن المفاهيم الأخرى (الفرع الأول)، ثم إلى خصائص الهجمات السيبرانية وأنواعها (الفرع الثاني).

الفرع الاول: تعريف الهجمات السيبرانية وتمييزها عن المفاهيم المختلفة

من المعلوم أن الاعتماد على التقنيات الذكية والحديثة وتبني نماذج الحكومات والمدن المتطورة، فإنه يصبح أكثر انكشافا وعرضة للهجمات السيبرانية.

ولتحديد المعنى من الهجمات السيبرانية سنتطرق إلى تعريف الهجمات السيبرانية (أولا)، وتمييزها عن المفاهيم المختلفة (ثانيا).

أولا: تعريف الهجمات السيبرانية

لتحديد تعريف الهجمات السيبرانية سنتطرق إلى تعريفها اللغوي، ثم الاصطلاحي.

1- التعريف اللغوي:

تعتبر كلمة سيبرانية أو سايبر أو سيبراني لفظة يونانية الأصل"kubevav" والمشتقة من كلمة "kubeunetes" والتي تعني مدير الدقة[1].

حيث أن هذا المصطلح ورد لأول مرة في مؤلفات الخيال العالمي في أواخر عام 1948، حيث استخدمت كلمة سايبر أكاديميا لأول مرة من قبل عالم الرياضيات الأمريكي "نوربرت وينز"، وذلك للتعبير عن التحكم الآلي والسيطرة والاتصال في عالم الحيوان، والآلات الميكانيكية[2].

فلا يوجد مصطلح مقارب للسايبر"cyber" في اللغة العربية، فلقد جاء هذا المصطلح في قاموس المورد الحديث "الكمبيوتر"[3]، أو عصري جدا، كما ورد مصطلح"cyber netiees" بأنه عالم الضبط، وقد جاء في قاموس المعاني بمعنى تخيلي[4]، ومصدر"cyber netiees" يتطابق مع مفهوم الهجمات السيبرانية، أي ضبط الأشياء عن بعد والسيطرة عليها، وقد عرف قاموس مصطلحات الأمن المعلوماتي الهجوم السيبراني بأنه: "هجوم عبر الفضاء الالكتروني، يهدف إلى السيطرة على المواقع الإلكترونية، أو البنى المحمية إلكترونيا، لتعطيلها، أو تدميرها أو الإضرار بها[5].

و يعرف أيضا قاموس المصطلحات العسكرية الأمريكية بأنها: "أي فعل يستخدم عن طريق شبكات إلكترونية بهدف السيطرة أو التعطيل لبرامج إلكترونية أخرى[6].

---

(1) – زهراء عماد محمد كالنتر، المسؤولية الدولية الناشئة عن الهجمات السيبرانية، مكتبة القانون المقارن، بغداد، 2019، ص18.

(2)– نور امير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الإنسان، مذكرة ماجستير، الجامعة الافتراضية السورية، 2021، ص 9.

(3)– منير البعليكي، المورد الحديث "قاموس انجليزي– عربي"، دار للعوم للملايين، بيروت، 2019، ص307.

(4)– قاموس المعاني، معنى كلمة سايبر، تاريخ الاطلاع: 2024/02/21 على الساعة: 08:06، متوفر على موقع: https //www.almaany.com/an/dd/er/cyber.،

(5)– طلال ياسين العيسى و عدي محمد عناب، "المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر"، مجلة الزرقاء للبحوث والدراسات الإنسانية، كلية الحقوق، جامعة عجلون الوطنية، الأردن، المجلد 19، العدد 01، 2019، ص83.

(6)– عدنان النقيب، الحرب الالكترونية في ضوء بروتكولي سبع وسبعون الملحقين باتفاقيات جنيف الأربع لسنة تسع وأربعين (الهجمات السيبرانية)، المركز العربي للنشر و التوزيع القاهرة، 2022، ص 160–161.

وبالاطلاع على الوثائق الصادرة عن الأمم المتحدة باللغة العربية، ومنشورات ومقالات اللجنة الدولية للصليب الأحمر، نجدها استخدمت مصطلح الهجمات السيبرانية نفسه من جهة أخرى[1].

2- التعريف الاصطلاحي:

اعتمدنا في دراستنا على مصطلح الهجمات السيبرانية، وذلك على غرار ما درج عليه البعض من المختصون فمنهم من تبنى مصطلح الفضاء السيبراني "cyber space" وذلك بالنظر إلى المجال الذي تجري فيه العملية السيبرانية، وتبنى أخرون مصطلح الحرب السيبرانية، إلا أن مصطلح الحرب غير مرغوب به في وقتنا الراهن على المستوى الدولي، كما اتجه البعض الأخر إلى اختيار مصطلح الهجمات السيبرانية "attacks cyber" مستندين إلى أنه مصطلح يصف العالم الافتراضي "الفضاء السيبراني" المستند على استخدام البيانات الإلكترونية، كما أنه يقوم على تحقيق أهداف عسكرية وأمنية ملموسة ومباشرة وذلك من خلال عمليات الاختراق والتجسس لمواقع إلكترونية خاصة بمحطات الطاقة والماء والكهرباء وكذا وسائل النقل عامة[2].

ويقصد بالاختراق بشكل عام القدرة على الوصول لهدف معين والدخول على الأجهزة بطريقة غير مشروعة عن طريق تغيرات في نظام الحماية الخاصة بها بهدف التطفل على خصوصيات الآخرين وإلحاق الضرر بهم، ويطلق على المخترق مصطلح"hacker" وحينما يتمكن المخترق من إحداث الإضرار كحذف ملفات أو تشغيل ملفات مؤذية أو زرع فيروسات أو وضع برامج تجسسية أو أي نوع من هذه الأنواع فهو مخرب"CRACKER "[3].

ان وضع تعريف محدد للهجوم السيبراني هو أول خطوة مهمة نحو التصدي للتهديد المتزايد الناشئ عنه كمفهوم جديد وسبب حقيقي لتهديد الأمن و السلم الدوليين[4].

إلا أن معظم التعاريف التي وردت بشأن الهجمات السيبرانية تشترك في معنى متقارب وهو استهداف مواقع إلكترونية أونظام كمبيوتر أو جهاز كمبيوتر من خلال وسائل اتصال إلكترونية أخرى، هذا ما يهدد سرية أو سلامة المعلومات المخزنة عليه، وعادة ما تكون صادرة عن مصدر مجهول إما

---

[1]-نور أمير الموصلي، المرجع السابق، ص9.

[2]- عدنان النقيب، المرجع السابق، ص 17.

[3]- بشرى حسين الحمداني، القرصنة الالكترونية (أسلحة الحرب الحديثة)، دار أسامة للنشر والتوزيع، عمان، 2014، ص13.

[4]- زهراء عماد محمد كلنتر، المرجع السابق، ص22.

يسرق أو يغير أو يدمر هدفا محدد عن طريق اختراق نظام حساس[1]، وإن كان المختصون في القانون الدولي يقرون بصعوبة إيجاد تعريف شامل لمصطلح الهجمات السير الذاتية[2].

لذلك سنعرض بعض التعاريف التي اعتمدها الفقهاء و المختصون لهذه الهجمات مع إيضاح أهم الاتجاهات، الرئيسية في تعريف الهجمات السيبرانية وصولا إلى وضع تعريف راجح .

2-1- اتجاهات تعريف الهجمات السيبرانية:

هذا الموضوع عادة ما ينصب اهتمام المختصين في القانون الدولي الإنساني في وصف الوسيلة والأثر، وبعبارة أخرى التركيز على ما تحتويه وسائل و طرائق القتال نفسه[3].

إن تعريفات الهجمات السيبرانية القائمة و المفاهيم ذات الصلة واسعة جدا، إلا أن هناك اتجاهين رئيسيين مختلفين في تعريف هذا النمط من الهجمات وهما: الاتجاه الضيق والاتجاه الواسع[4].

2-1-1- الاتجاه الضيق:

هناك من يستند على المعيار الشخصي، بحيث يكون الفاعل ملم بتقنية المعلومات، ولديه دراية كافية للتعامل معها[5]، ويركز هذا الاتجاه على موضوع الهجوم، وهذا ما تبنته الولايات المتحدة الأمريكية وحلفاؤها، ومن أمثلة ذلك ما اعتمدت عليه القيادة الاستراتيجية الأمريكية عام 2007، بشأن استخدام الوسائل الالكترونية لأغراض العسكرية، وقد عرفته: "تطويع عمليات نظام الكمبيوتر بهدف منع الخصوم من الاستخدام الفعال لها، فضلا عن التسلل إلى أنظمة المعلومات وشبكات الاتصال بهدف جمع البيانات التي تحتويها وحيازتها وتحليلها"[6].

وقد عرفه البروفيسور فيورتس (Fuertes)، أستاذ في قسم الكيمياء في جامعة تكساس للتكنولوجيا إذ قال: "هجوم عبر الأنترنت يقوم على التسلل إلى مواقع الالكترونية غير مرخص بالدخول إليها،

---

(1)- نور أمير الموصلي، المرجع السابق، ص7.

(2)- محمود أحمد قرعان، الجرائم الالكترونية، دار وائل للنشر والتوزيع، عمان، 2017، ص 18- 19.

(3)- عدنان النقيب، المرجع السابق، ص 161-162.

(4)- زهراء عماد محمد كلنتر، المرجع السابق، ص23.

(5)- محمود أحمد قرعان، المرجع السابق، ص 20.

(6)- اسمهان بعيري، الهجمات السيبرانية و أثرها على تهديد الأمن والسلم الدوليين، مذكرة ماستر، قانون عام معمق، قسم الحقوق ، كلية الحقوق والعلوم السياسية، جامعة الشاذلي بن جديد، الطارف، 2022، ص 18.

بهدف تعطيل أو إتلاف البيانات أو الاستحواذ عليها وهي عبارة عن سلسلة هجمات إلكترونية تقوم بها الدول ضد أخرى"[1].

كما عرفه الأستاذ(MICHAEL N SCHMITT) بأنه:" تلك الإجراءات التي تتخذها الدولة من أجل الهجوم على نظم المعلومات، الخاصة بالدولة المهاجمة"[2].

حسب الدكتور (هربت لين) كبير العلماء في مجلس علوم الحاسوب والاتصالات السلكية و اللاسلكية التابع لمجلس البحوث الوطني الأمريكي فإنه: "يقصد بالهجوم السيبراني استخدام أنشطة متعمدة للتأثير على شبكات الحاسوب للخصم، عبر إتلافها، إضعافها، تدميرها، تعطيلها، التحكم في الأجهزة الآلات المرتبطة بها، منع مستخدميها من الولوج إلى خدمة المعلومات أو الحاسوب إتلاف بيانات ذات أهمية استراتيجية"[3]، ويعرفه كل من الأستاذ (ريشارك كلارك) والأستاذ (روبرت كناكي) بأنه:" أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكومبيوتر والشبكات التابعة لدولة أخرى بهدف تخفيض أضرار بالغة أو تعطيلها"[4].

وكما عرفه الأستاذ(SHIN) بأنه استخدام الطيف الالكتروني أو الكهرومغناطيسي لتخزين و تعديل و تبادل البيانات وجها لوجه مع أنظمة تحكم في بنى تحتية مرتبطة بها[5].

بعد تأسيس القيادة السيبرانية الأمريكية نشرت هيئة الأركان المشتركة عام 2011 تعريف رسميا بخصوص الهجوم السيبراني حيث جاء بأنه: " نشاط عدائي باستخدام الكومبيوتر أو شبكات أو الأنظمة ذات الصلة بهدف إلى تعطيل أو تدمير أنظمة الخصم السيبرانية الحرجة أو ممتلكاته أو وظائفه ، وإن النتائج الموجودة عن الهجوم السيبراني قد يفصل زمنيا أو مكانيا عن النشاط السيبراني[6].

---

[1]– أحمد عيسى نعمة الفتلاوي، الهجمات السيبراني (دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصرة)، منشورات زين الحقوقية، بيروت، 2018، ص 16.

[2]– يحي ياسين سعود، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، المجلة القانونية، كلية الحقوق، جامعة القاهرة، المجلد 04، العدد 04، 2018، ص 84.

[3]– وداد بوطلاعة و منال بوكورو ، الهجمات السيبرانية على البنية التحتية الحرجة، الإخوة منتوري قسنطينة، المجلد 07، العدد 02، 2022، ص235–236.

[4]– عبد الكريم بإسماعيل، تأثير الفضاء الافتراضي على الأمن القومي، مجلة البحوث و الدراسات، جامعة قاصدي مرباح ورقلة (الجزائر)، المجلد 19، العدد 01، 2022، ص 144.

[5]– نسيب نجيب، الحرب السيبرانية" من منظور القانون الدولي الإنساني"، المجلة النقدية للقانون والعلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة بتيزي وزو، المجلد 16، العدد 04، 2021، ص 221–222.

[6]– صلاح الدين معماش، حظر الهجمات في القانون الدولي الإنساني، مجلة السياسة، جامعة محمد بوقرة، بومرداس (الجزائر، المجلد 06 ، العدد 01، 2022، ص 623.

ومن تعريفات الاتجاه الضيق أيضا:" كل فعل غير مشروع يكون العلم بالتكنولوجيا الكومبيوتر بقدر كبير لازما من ناحية وملاحقته من ناحية أخرى"، وفي تعريف آخر:" هي التي تقع على جهاز الكومبيوتر أو داخل نظامه فقط"[1].

وعليه إن التعاريف حسب الاتجاه الضيق اعتمد على المعيار الشخصي الذي يستوجب أن يكون الفاعل ملما بتقنية المعلومات، وله دراية كافية للتعامل معها، وبهذا يجب أن يكون التعريف ملما بعناصر أخرى لتصنيف الجريمة ضمن الجرائم الالكترونية.

2-1-2 – الاتجاه الواسع:

على النقيض من الاتجاه الضيق الذي تبنته الولايات المتحدة رسميا، فقد تبنت منظمة شنغهاي[2] للتعاون نهجا أكثر توسعا بشأن الهجمات السيبرانية حيث أعربت هذه المنظمة عن قلقها بشأن التهديدات التي تشكلها إمكانية استخدام وسائل المعلومات والاتصالات الحديثة وتقنياتها لأغراض تتنافى مع ضمان الأمن والاستقرار الدوليين على الصعيدين العسكري و المدني[3].

كما عرف فقهاء هذا الاتجاه الهجوم السيبراني على أنه: "تصرف يدور في فضاء إلكتروني ينطوي على التسبب إلى مواقع الكترونية عبر مرخص بالدخول لها ، يهدف إلى تعطيل أو إتلاف البيانات، واختراق مواقع الكترونية حساسة"[4].

كما جاء في دليل تالين[5]، أن الهجمات السيبرانية هي: "عمليات الكترونية سواء كانت هجومية أو دفاعية من المتوقع بشكل معقول أن تتسبب في إصابة الأشخاص أو موتهم أو إلحاق الضرر أو تدمير الأشياء[6].

---

[1]– خالد حسن أحمد لطفي، الإرهاب الالكتروني (آفة العصر الحديث و الآليات القانونية للمواجهة)، دار الفكر الجامعي، كلية الحقوق، الإسكندرية، 2019، ص 91.

[2]– تأسست في مدينة شنغهاي بتاريخ: 15حزيران 2001 وأصبحت منظمة رسمية حسب مبادئ القانون الدولي في عام 2002 وتتألف من الصين، روسيا ومعظم جمهوريات الاتحاد السوفياتي السابق في اسيا الوسطى ....من أهدافها مكافحة الإرهاب، ومواجهة التطرف والحركات الانفصالية والتصدي لتجارة الأسلحة إلا أن بعضهم يرى إنها حلف عسكري لمواجهة حلف الشمال الأطلسي (NATO)، ينظر: عبد الحق الرحمن، التحالف الشرقي المقبل "منظمة شنغهاي للتعاون والتوجه نحو العالمية"، مجلة سياسات عربية، العدد 12، جانفي 2015، ص4.

[3]– اسمهان بعيري، المرجع السابق، ص 19.

[4]– أحمد عيسى نعمة الفتلاوي، المرجع السابق، ص 212.

[5]– دليل تالين جهد اكاديمي مميز من الخبراء في القانون الدولي و المسائل التكنولوجية المعاصرة، انظر: يحي ياسين، المرجع السابق، ص 94.

[6]– وداد بوطلاعة و منال بوكورو، المرجع السابق، ص 326.

ينظر مؤيدو هذا الاتجاه إلى نشر المعلومات الضارة للأنظمة السياسية والاجتماعية والاقتصادية فضلا عن المجالات الروحية والأخلاقية والثقافية للدول الأخرى، بوصفها أيضا من التهديدات الرئيسية للأمن السيبراني. إن الهجوم السيبراني تصرف في عالم رقمي قائم على استخدام بيانات رقمية ووسائل اتصال تعمل الكترونيا، ومن ثم تطور ليتضمن مفهوما أوسع يقوم على تحقيق أهداف عسكرية أو أمنية ملموسة ومباشرة جراء اختراق مواقع الكترونية حساسة، كأنظمة حماية محطات الطاقة النووية أو الكهربائية أو المطارات ووسائل النقل الأخرى[1].

وقد عرف التقرير الحادي و الثلاثون للجنة الدولية للصليب الأحمر العمليات السيبرانية "المعلوماتية " بأنها: "عمليات تشن ضد أو عبر حاسوب أو نظام حاسوبي بواسطة بيانات أخرى مخصصة للغرض، وقد تهدف هذه العمليات إلى تحقيق أغراض مختلفة تضم على سبيل المثال اختراق نظام معين وجمع أو نقل تدمير أو تغيير أو تشفير البيانات، أو إجراء أو تعديل العمليات التي يتحكم بها الجهاز الحاسوبي المخترق أو التلاعب بهذه العمليات، ويمكن بالتالي استخدام هذه الوسائل لتدمير، أو تعديل أو تعطيل مجموعة متنوعة من الأهداف في العالم الحقيقي كالصناعات والبنى الأساسية والاتصالات المالية "[2].

من خلال هذه التعاريف نجد أن العنصر البشري لعب دور أساسي لتنفيذ هذه الهجمات، كما تقاربت في تركيزها على الوسيلة الالكترونية و الهدف أو المحل الالكتروني (حواسيب) وكل ما يتصل بها، أيضا ركزت في مجملها على الآثار و الأضرار التي تنتج عنها، واتسع التعريف الذي قدمه الخبراء في دليل تالين ليشمل الهجمات السيبرانية الدفاعية و الهجومية في رغبة من الفقه في احتواء أكبر قدر من الوقائع بمفهوم الهجمات السيبرانية[3].

وعليه فإن الاتجاه الموسع اعتمد على السلوك الإجرامي الذي يتم بمساعدة الكمبيوتر أو كل جريمة تتم في محيط أجهزة الكمبيوتر.

2-2 – تعريف الهجمات السيبرانية من خلال الأمن القومي:

تظهر المستجدات العديدة في مجال التكنولوجيا، بأن الحرب السيبرانية تعد تحديا للمفاهيم السائدة حول الأمن القومي أو برتب إيلاء قضية الدفاع عن البنى التحتية الحيوية للدولة أهمية قصوى، لاسيما

---

[1]– زهراء عماد محمد كلنتر، المرجع نفسه، ص 28 .

[2]– علي سنوسي، "الهجمات السيبرانية في ضوء أحكام قواعد القانون الدولي الإنساني والاتفاقيات الدولية"، مجلة الحقوق والعلوم السياسية، كلية الحقوق، جامعة بن خلدون، تيارت، المجلد 10، العدد 02، 2023، ص 249.

[3]– وداد بوطلاعة و منال بوكورو، المرجع السابق، ص 326.

في مجالات الطاقة والمياه و الحوسبة، والاتصالات، والمواصلات، والاقتصاد في القطاعيين المدني و الأمني، لذلك تجد أن الركائز الثلاث لمفهوم الأمن القومي، تتمثل فيما يلي:

أ – الردع: إن القدرات السيبرانية المتطورة يمكن أي دولة من ردع أعدائها، فقديما كان من السهل تقييم قدرات الدول و إمكاناتها، وقياس قوتها لكن عبر مضي القرون، و ازدهار التكنولوجيا و تطورها، تغيرت مصادر القوة، و أشكال الردع، و أصبحت القوة الالكترونية من أهم أدوات الردع التي تستهدفها الدول في التنافس و التصارع مع بعضها بعضا، ومثال ذلك التغطية الإعلامية الواسعة التي حظي بها فيروس "ساكنت" الذي استخدم لتخريب أنظمة الكومبيوتر التي تتحكم بمرافق تخصيب اليورانيوم في إيران المنسوب إلى الولايات المتحدة و إسرائيل، والذي شكل قفزة نوعية في كل ما يتعلق بالقدرة الهجومية السيبرانية للدول، و قوتها، و نفوذها؛

ب – الإنذار المبكر: إن القدرات السيبرانية الهائلة للدولة ستمكنها من جمع معلومات كثيرة عن أعدائها، وفي الوقت ذاته ستمنع هؤلاء من الوصول إلى قاعدة بياناتها، وهذا يشكل بالنسبة للدولة إنذارا فعالا بشأن نية أعدائها؛

ج – الحسم: فالدول الرائدة في العالم من حيث قدراتها السيبرانية، تكون متفوقة في المعركة من خلال استخدام أدوات سيبرانية متقدمة بهدف حسم المعركة، فالواضح اليوم أن التفوق السيبراني المتكامل مع قدرات حركية متقدمة، أصبح من شأنه أن يحسم المعارك[1].

ومن هذا المنطلق فإن الهجمات السيبرانية ميدانها الفضاء السيبراني وهي غير محدودة المجال وتكون غامضة الاهداف لأنها تتحرك عبر شبكات المعلومات والاتصالات المتعدية للحدود الدولية، فضلا عن اعتمادها على أسلحة الكترونية ذكية ومتطورة تلائم مع عصر المعلومات، او يتم توجيهها ضد المنشآت الحيوية أو دسها عن طريق عملاء لأجهزة الاستخبارات.

ثانيا: تمييز الهجمات السيبرانية عن المفاهيم المختلفة

تختلف الهجمات السيبرانية عن العديد من المفاهيم الاخرى القريبة منها، سنحاول من خلال هذا العنصر إبداء أوجه التمييز بين المصطلحات المختلفة كالاتي:

1- التمييز بين الهجمات السيبرانية والجريمة السيبرانية: يعد الهجوم السيبراني كما ذكرنا سابقا عبارة عن تصرفات إلكترونية تتسبب في قتل أو دمار أو أضرار مادية تقوم بها دولة أو مجموعة مسلحة ضد

[1]- طلال ياسين العيسى وعدي محمد عناب، المرجع نفسه، ص 84.

دولة أخرى، بينما الجريمة السيبرانية تشمل مجالا أوسع بكثير من ذلك أي تتضمن كل النشاطات الالكترونية غير القانونية بما في ذلك استخدام الوسائل المعتمدة على الكومبيوتر[1].

إن الحداثة التي تتميز بها الجريمة السيبرانية، و اختلاف النظم القانونية و الثقافية بين الدول أدت الى صعوبة وضع نظام لتضييق الجرائم السيبرانية وكذا عدم الاتفاق على تعريف موحد لهذا النمط من الجرائم، وذلك تخوف من حصرها في المجال ضيق[2].

وقد عرفت بأنها " كل فعل صار بالآخرين عبر استعمال الوسائط الإلكترونية مثل الحواسيب أجهزة الموبايل، شبكات الاتصالات الهاتفية شبكات نقل المعلومات، شبكة الانترنت أو الاستخدامات غير القانونية للبيانات الحاسوبية أو الالكترونية عموما"، ويعرفها آخرون بأنها: "نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود"[3].

إن الجرائم السيبرانية والهجمات السيبرانية يشتركان في البنية التي يحدثان فيها، أي الفضاء السيبراني، إلا أنهما يختلفان من ناحية القانونية، حيث لا يمكن و صف أي اعتداء جريمة سيبرانية في غياب نص قانوني يصفها و يحدد عناصرها، بينما يمكن وصف أي اعتداء أنه هجوم سيبراني و ذلك بمجرد وقوعه خارج الوصف القانوني[4].

ويكمن التباين أيضا من حيث الأشخاص و الأهداف، فالجريمة السيبرانية غالبا ما ترتكب من قبل أفراد و توجه ضد مؤسسات مالية أو شركات و حتي أفراد داخل أو خارج إقليم الدولة أما الهجمات السيبرانية فعادة ما ترتكب من قبل دولة أو منظمات حكومية أو غير حكومية ضد دولة أخرى[5].

أما من ناحية الهدف فالجرائم السيبرانية غايتها التعلم والتي يتم استخدام الكمبيوتر والامكانيات المستحدثة لنظم المعلومات على أمل الربح وروح الكسب التي تدفع إلى التعدي على نظم المعلومات بالإضافة إلى الدوافع الشخصية والمؤثرات الخارجية التي قد تكون سببا في ارتكاب الجريمة

---

[1]– زهراء عماد محمد كلنتر، المرجع السابق، ص 30.

[2]– اسمهان بعيري، المرجع السابق، ص20.

[3]– وفاء لطفي، الجهود الدولية في مجال مكافحة جرائم الإرهاب السيبراني، التجربة الماليزية نموذجا، تاريخ الاطلاع (2024/02/18، على 21:9)، متوفر على الرابط: http ://jpsa.journals.ekb.eg/article.

[4]–بلقاسم بن صابر و محمد حيدرة، "الهجمات السيبرانية ومواجهتها في ضوء القانون الدولي المعاصر"، مجلة حقوق الإنسان والحريات العامة، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم، العدد 4، جوان 2017، ص90.

[5]– اسمهان بعيري، المرجع السابق، ص20.

المعلوماتية[1]، خلاف للهجمات السيبرانية التي تهدف إلى المساس بسيادة الدولة وتهديد استقرارها وذلك بزعزعت الأمن القومي والسياسي للدولة، وكذا تحطيم البنى التحتية الكونية للدولة، وتعريض مصالحها للخطر في شتى المجالات[2].

2- التميز بين الهجمات السيبرانية والحرب السيبرانية:

يقصد بالحرب السيبرانية أساليب الحرب ووسائلها التي تعتمد على تكنولوجيا المعلومات وتستخدم في سياق نزاع مسلح، أي هي الهجمات والعمليات التي ترتكب ضد أو بواسطة شبكات الحواسيب و أنظمة البيانات بين الدول أو الجماعات المسلحة المنظمة في سياق نزاع مسلح، أو سياسات الردع المتبادل، وتعد الحروب السيبرانية ميدان رابع من ميادين الحروب فهي حروب خفية تقتحم الأنظمة الإلكترونية وتسبق العمل العسكري، وتستهدف الأنظمة العسكرية والبنية التحتية الحيوية للدولة فضلا عن الشبكات الذكية وشبكات المراقبة الإشرافية وحيازة البيانات (SCADA)التي تسمح لها بالعمل والدفاع عن نفسها[3]، إن الحرب السيبرانية و إن كانت تتفق كثيرا مع الهجمات السيبرانية إلا أن ذلك لا يعني عدم وجود ما يميزها عن بعض، فالحرب السيبرانية هي نوع أو جزء من الهجمات السيبرانية التي تحدث أثناء النزاع المسلح، خلافا للهجمات السيبرانية التي تعتبر في النشاط إلكتروني ضار بالدول الأخرى سواء كان وقت السلم أو أثناء النزاع المسلح، كذلك بالنسبة للآثار التي ترتبها الحروب السيبرانية هي عبارة عن آثار مادية " آثار حركية"، بينما الهجمات السيبرانية قد ينتج عنها المساس بالأنظمة الرقمية، وذلك لأغراض أمنية و عسكرية أو زعزعت نظام وعمل حكومة دولة ما[4].

3- التمييز بين الهجمات السيبرانية و الإرهاب السيبراني:

في ثمانينات القرن العشرين كان أول ظهور لمفهوم الإرهاب السيبراني (cyber Terrorism)، فقد عرفه باري كولين (Barry collin) بأنه:" هجمة الكترونية غرضها تهديد الحكومات أو العدوان عليها، سعيا لتحقيق أهداف سياسية أو دينية أو إيديولوجية، وأن الهجمة يجب أن تكون ذات أثر مدمر و تخريب مكافئ للأفعال المادية للإرهاب"، ويعتبر الإرهاب السيبراني حسب الموسوعة السياسية أنه: "استخدام

---

[1]- عبد العال الديربي ومحمد صادق إسماعيل، الجرائم الالكترونية "دراسة قانونية قضائية مقارنة"، المركز القومي للإصدارات القانونية، القاهرة، 2012، ص47-48.

[2]- سامية صديقي، المسؤولية الدولية المترتبة عن الهجوم السيبراني في منظور القانون الدولي، مجلة البحوث القانونية والاقتصادية، جامعة محمد البشير الابراهيمي برج بوعريريج، الجزائر، المجلد 06، العدد 01، 2023، ص822.

[3]- وفاء لطفي، المرجع السابق، ص8.

[4]- سالم محمد عبود، أساسيات الأمن السيبراني، دار الدكتور للعلوم الإدارية و الاقتصادية، بغداد، 2022، ص 64.

العنف غير القانوني أو التهديد به بأشكاله المختلفة كالاغتيال والتشويه والتعذيب والتخريب بغية تحقيق هدف سياسي معين مثل: كسر روح المقاومة والتقيد عند الأفراد،

ونقض المعنويات عند الهيئات والمؤسسات، أو كسبيل للحصول على المعلومات أو مال، وبشكل عام هو استخدام الإكراه لإخضاع طرف مضاد لمشيئة الجهة الإرهابية"، والإرهاب السيبراني كما عرفه دروثي دينينغ (Dorothy Denningg) على أنه: " الهجوم القائم على مهاجمة الحاسوب، وأن التهديد به يهدف إلى الترويج أو إجبار الحكومات أو المجتمعات لتحقيق أهداف سياسية أو دينية أو عقائدية وينبغي أن يكون الهجوم مدمرا و مخربا لتوليد الخوف شبيها للأفعال المادية للإرهاب"، ويعرف أيضا على أنه: نقطة التقاء الفضاء الالكتروني والإرهاب وهو يشير إلى الهجمات والتهديدات غير القانونية بالهجوم على أجهزة الكومبيوتر و الشبكات والمعلومات المخزنة فيها عندما يتم ذلك لتخويف أو إكراه حكومة أو شعبها لتحقيق أهداف سياسية أو اجتماعية؛ وهو التهديد أو الهجوم غير القانوني بشن هجمات على أجهزة الكومبيوتر و أنظمة المعلومات، والبرامج، والبيانات، بهدف ترهيب و إكراه الحكومات تحقيقا لمختلف الأهداف[1].

إن الإرهاب الإلكتروني يشير إلى عنصرين أساسين هما: الفضاء الافتراضي(cyber space) والإرهاب (Terrorism)، إضافة إلى ذلك هناك كلمة أخرى تشير إلى الفضاء الإلكتروني وهي العالم الافتراضي (Virtualworld)، والذي يشير إلى التمثيل الرمزي والزائف للمعلومات، إن خطورة الإرهاب الالكتروني تزداد في الدول المتقدمة والتي تؤدي إلى تدمير البنية التحتية بالحاسوب الآلية والشبكات المعلوماتية، وذلك بشن هجوم إرهاب مدمر لإغلاق المواقع الحيوية وإلحاق الشلل بأنظمة القيادة والسيطرة والاتصالات[2].

4- التمييز بين الجريمة المعلوماتية و الجريمة الالكترونية:

نتيجة ازدياد استخدام شبكة الأنترنيت في كثير من المعاملات الإلكترونية أصبحت مجالا خصبا لكثير من الأفعال الإجرامية والتي أطلق عليها الجريمة الالكترونية(cyber crime) تتميز لها عن الجريمة المعلوماتية، بحيث باشرت الجريمة الإلكترونية في الانتشار مع ظهور مناهج قياس درجات الأمان في أنظمة الكومبيوتر، حيث تم استخدام هذه البرامج لاستقبال المعلومات والتلاعب بأنظمة الكومبيوتر التي تحتوي عليها و ذلك لأغراض غير مشروعة، ولا تتباين الجريمة الالكترونية عن الجريمة المعلوماتية في كثير من الأحوال، باستثناء أنها تتم عن طريق جهازين كومبيوتر أو أكثر متصلين فيما بينهم عبر شبكة

---

[1]- وفاء لطفي، المرجع السابق، ص6- 7.

[2]- رفد عيادة الهاشمي، الإرهاب الالكتروني، دار أمجد للنشر و التوزيع، 2019، ص 18.

الانترنت وإن كانت الثانية تجد مكانها في الفضاء الافتراضي (cyber sace) عبر شبكة الانترنيت[1]، والفضاء الافتراضي هو الفضاء السيبراني "cyber space" الذي يسعى إلى ضم العالم بأسره، ويختلف عن الفضاء الحقيقي وتوجد فيه العديد من المجتمعات الموزعة على نحو غير متساو باستخدام بيئة تقنية– الأنترنت في المقام الأول– حيث يستفيد المواطنون و المؤسسات من تكنولوجيا المعلومات و الاتصالات في تفاعلاتهم[2].

5– تمييز الهجمات السيبرانية عن الأمن السيبراني و الجيش السيبراني:

صار مصطلح الأمن السيبراني يستخدم لتلخيص السياسيات العامة والتدابير الأمنية والمبادئ التوجيهية و طرق إدارة المخاطر والحماية و التدريب ومختلف التقنيات و الأدلة التي يمكن استخدامها و الاعتماد عليها لحماية أجهزة الحاسوب و شبكات الانترنت والبيانات المخزنة و المتداولة عبرها[3].

والأمن السيبراني هو ممارسة حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية، وعادة ما تهدف هذه الالكترونية إلى الوصول إلى المعلومات الحساسة أو تغييرها أو تدميرها، ابتزاز المال من المستخدمين، أو مقاطعة العمليات التجارية العادية[4]،

ويعرف الأمن السيبراني بأنه العملية التي تهدف إلى حماية أنظمة وشبكات الكومبيوتر المتصلة بالأنترنت من الهجمات الرقمية و الاختراقات أو التدمير أو التعطيل، وتطرح في هذا الصدد مسألة الفرق بين الأمن السيبراني **والذكاء الاصطناعي** الذي يعد أحد فروع علوم الكومبيوتر[5]، مهمته هي إنشاء آلات تستطيع القيام بالمهام التي تحتاج إلى ذكاء بشريا مثل فهم اللغة الطبيعية والتعرف على الصور واتخاذ القرارات، يتعامل الذكاء الاصطناعي مع تجميع البيانات وتصنيفها عالجتها وتصنيفها وإدارتها، وهناك علاقة وثيقة بين الذكاء الاصطناعي والأمن الالكتروني أو السيبراني إذ يتم تطوير أنظمة الذكاء الاصطناعي التي يمكن استخدمها لتعزيز الأمن السيبراني، إلى جانب تنفيذ تدابير أمنية لحماية أنظمة الذكاء الاصطناعي حتى الاختراق أو التلاعب، فبعد تزايد الجرائم الالكترونية مثل سرقة البيانات،

---

(1)– خالد ممدوح إبراهيم، أمن الجريمة الالكترونية، الدار الجامعية، الإسكندرية، 2008، ص 56.

(2)– الهجمات السيبرانية (الالكترونية والتأمين)، تاريخ الاطلاع (2024/02/18 على الساعة: 21:05)، متوفر على الموقع: نشرة الاتحاد المصري للتامين .https://www.infegypt.org /News Details.aspx، ص13.

(3)– أحمد عمرو، ما بعد الإنسانية العوالم الافتراضية و أثرها على الإنسان، شركة أفاق المعرفة للنشر و التوزيع، المملكة العربية السعودية، الرياض، 2022، ص 239.

(4)– وفاء لطفي، المرجع السابق، ص 8.

(5)– تحديات الأمن السيبراني في عصر الذكاء الاصطناعي، تاريخ الاطلاع (2024/03/06، على الساعة 22:11)، متاح على موقع Bakkah.

والتصدي الاحتيالي لجأت المنظمات إلى عدة وسائل لمكافحة تلك التهديدات، فاستعانت بفرق الأمن، السيبراني المؤهلة بأحدث التقنيات ومنها تقنية الذكاء الاصطناعي، التي تساعد على الكشف السريع عن الأنشطة الضارة ومواجهاتها، وتحمي الشبكات من الهجمات الالكترونية[1].

ويستخدم الذكاء الاصطناعي في الأمن السيبراني لتحليل البيانات الكبيرة وتحديد الأنماط والسلوكيات غير العادية التي قد تشير الهجمات المحتملة، وباستخدام الذكاء الاصطناعي في أمن الأنترنت، يمكن تعزيز المنظمات لمواجهة التهديدات السيبرانية وحماية البيانات والمعلومات الحساسة[2].

ولعل انتشار الانترنت "انترنت الأشياء" كإفراز من إفرازات الذكاء الاصطناعي وتطبيقاتها، أدى إلى تفاقم المخاطر المهددة للأفراد والدول وحتى للمنظمات وخاصة الأجهزة، التي باتت موجودة في مختلف القطاعات الحساسة، وهذا من شأنه أن يعطي أبعاد أخرى للحرب السيبرانية، وفي مقال نشرته (آرني بركار) نائبة رئيس القسم الأمني لدى شركة (أي ب أم) على الموقع الالكتروني لمجلة فاست كومباني تحت عنوان" مستقبل الأمن مرتبط بالذكاء الاصطناعي وليس بكلمة المرور "إعادة تصميم الأنظمة الأمنية، بحيث لا تعتمد الطرف التقليدية للمصادقة مثل كلمات المرور إنما تلجأ إلى الذكاء الاصطناعي للتحقق من الهويات والسلوكيات الرقمية مشيرة إلى أن عملية تسجيل الدخول يجب ألا يتم بعد ذلك دون أن تثار حولها الشكوك"[3].

وهناك العديد من الفوائد لاستخدام أدوات و أنظمة الأمن السيبراني التي تعمل بالذكاء الاصطناعي فيما يلي:

1-التعامل مع الكثير من البيانات: يجد موظفو الأمن السيبراني صعوبة كبيرة في مراجعة جميع الأنشطة يدويا بحثا عن التهديدات المحتملة وهنا تتجلى فائدة الذكاء الاصطناعي الذي يقوم تلقائيا بمسح وتحديد التهديدات و يسهل من عملية الكشف عنها و يعزز من الحماية ضدها؛

---

[1]- تحديات الأمن السيبراني في عصر الذكاء الاصطناعي موقع Bakkah، تاريخ الاطلاع(2024/03/06، على الساعة 22:11).

[2]- محمد دحماني، "الذكاء الاصطناعي كآلية لتعزيز الأمن السيبراني"، مجلة الفكر القانوني والسياسي، جامعة عمار ثليجي، الأغواط، المجلد 07، العدد 02، 2023، ص 607.

[3]-خليلي سعيدي ومرزوق بن مهيدي، "الذكاء الاصطناعي كتوجه حتمي في حماية الامن السيبراني"، دراسات في حقوق الانسان، جامعة العربي التبسي تبسة، الجزائر، المجلد 06، العدد 01، جوان 2022، ص 35.

2- تقليل العمليات المزدوجة: قدرة الذكاء الاصطناعي على الكشف عن التهديدات الأمنية الأساسية بانتظام ومنها إضافة إلى دوره في التحليل الشامل من تنفيذ أفضل ممارسات أمن الشبكة دون التعرض لخطر الخطأ البشري أو الملل الذي يصيب موظفي فرق الأمن السيبراني؛

3- تسريع أوقات الكشف والاستجابة: عند قيام الشركات بدمج الذكاء الاصطناعي مع الأمن السيبراني، فهي تضمن الكشف السريع عن التهديدات الأمنية و الاستجابة لها لأن الذكاء الاصطناعي يقوم بمسح النظام بالكامل و يحدد التهديدات مبكرا، ويسهل من المهام الأمنية؛

4- محاربة الروبوتات الضارة: هناك الكثير من الروبوتات التي تستخدم في الأنشطة الضارة مثل نشر البرامج الضارة وسرقة البيانات، ويمتلك الذكاء الاصطناعي القدرة من تحديد أنماط تلك الروبوتات والتعرف عليها و حظرها؛

5- تأمين المصادقة: يوفر الذكاء الاصطناعي العديد من الأدوات مثل ماسحات بصمات الأصابع والتعرف على الوجه، وهي الأدوات المطلوبة لتأمين المصادقة أثناء محاولاته تسجيل الدخول على المواقع التي تحتوي على معلومات حساسة وتتطلب طبقة أمان إضافية للحماية، وتساعد ذلك الأدوات على اكتشاف محاولات تسجيل الدخول الاحتيالية و الهجمات الالكترونية التي تهدف إلى سرقة البيانات؛

6- تحسين الدقة والكفاءة: توفر أنظمة الأمن السيبراني القائمة على الذكاء الاصطناعي دقة وكفاءة أفضل مقارنة بالحلول الأمنية التقليدية، كما تمتلك خوارزميات الذكاء الاصطناعي القدرة على الأنماط التي تستطيع العين البشرية اكتشافها، وهو ما يزيد من دقة اكتشاف الأنشطة الضارة[1].

أما الجيش السيبراني فيعبر عنه بعض الباحثين " بالقوة الرابعة"، باعتبار أن الجيش جوي، و بري، وبحري، بينما الجيش السيبراني هو الرابع وقد أنشأت كل القوى الكبرى في العالم إدارات متخصصة لهذا الغرض وعلى سبيل المثال لا الحصر ففي الولايات المتحدة نجد أن وزارة الدفاع مسؤولة عن الدفاع، والهجوم السيبراني في المجال العسكري وعن تقديم المساعدة للهجمات المدنية في نفس المجال، ولهذا الغرض أنشئت القيادة السيبرانية للولايات المتحدة (United states cyber command) بوصفها جزءا من القيادة الاستراتيجية في وزارة الدفاع، ونجد إدارات مناظرة أو مشابهة في بقية الدول الكبرى[2].

---

[1]- تحديات الأمن السيبراني في عصر الذكاء الاصطناعي موقع Bakkah، تاريخ الاطلاع(2024/03/06على الساعة 22:11)، المرجع السابق.

[2]- أحمد عمور، المرجع السابق، ص 243.

وبالتالي لا بد من اعادة النظر في مختلف المفاهيم التي فرضتها هذه الحرب السيبرانية خاصة في هذا العصر الذي يسيطر عليه الذكاء الاصطناعي، والتعامل بحذر امام المخاطر والهجومات غير المرتقبة، أمام بروز الديبلوماسية السيبرانية، الذي يتطلب فرض عقوبات في إطار دولي.

الفرع الثاني: خصائص الهجمات السيبرانية و أنواعها

تعتبر الهجمات الإلكترونية من الجرائم المستحدثة و السريعة في التغيير والتطور ووليدة ثورة المعلومات الهائلة فهي تتميز بجملة من الخصائص تميزها عن الجرائم العادية التقليدية ولدراسة هذا الاختلاف سنتناول خصائص الهجمات السيبرانية (أولا)، ثم أنواع الهجمات السيبرانية (ثانيا).

أولا: خصائص الهجمات السيبرانية

تتسم الهجمات السيبرانية بجملة من الخصائص من أهمها:

- **الهجمات السيبرانية ذات طبيعة تقنية،** ومتطورة تعكس التطور الحاصل في مجال البرمجيات و الحواسيب والاتصالات؛

- **التكلفة المتدنية نسبيا،** مقارنة مع الميزانيات الضخمة التي تخصص لإنتاج أسلحة تقليدية كالغواصات و المقاتلات المتطورة[1].

- **سرعة التنفيذ،** هذه الجريمة لا تتطلب الإعداد قبل التنفيذ أو استخدام معدات وبرامج معينة، فيكفي فقط ضغطة واحدة على لوحة المفاتيح، أو أن يتم التنفيذ عبر الهاتف[2].

- **جريمة مستمرة في معظم أحوالها،** كما في حالة التطرف الديني و تغذية المواقع ببعض العقائد الفيديوهات المتطرفة، ما لم يتم ضبط الفاعل والتدخل الفني لإنهاء الجريمة[3].

- **تتسم بسمات مخصوصة تستهدف معنويات وليست ماديات محسوسة،** وتثير في هذا النطاق مشكلات الاعتراف بحماية المال المعلوماتي إن جاز التعبير[4].

- **الجريمة المعلوماتية جريمة عابرة للحدود،** وتتسم غالبا بالطابع الدولي ذلك لأن الطابع العالمي لشبكة الانترنت وما يرتبه من جعل معظم دول العالم في حالة اتصال دائم على الخط (on line)، يسهل ارتكاب الجريمة من دولة إلى دولة أخرى، فهي جريمة عابرة للقارات، وهي من نوع الجرائم التي يتم ارتكابها عبر

---

(1)- بوطلاعة وداد و بوكورو منال، المرجع السابق، ص 237.

(2)- خالد حسن أحمد لطفي، المرجع السابق، ص 95.

(3)- منال محمد عباس، الإرهاب الالكتروني و الأمن الاجتماعي، دار المعرفة الجامعية، كلية الآداب، جامعة الإسكندرية، 2019، ص 120.

(4)- نسرين عبد الحميد نبيه، الجريمة المعلوماتية و المجرم المعلوماتي، منشأة المعارف جلال حزي و شركاه، 2008، ص 132.

المسافات حيث لا يتواجد الفاعل على مسرح الجريمة بل يرتكب جريمته عن بعد[1]، وعلاوة على ذلك فهي غير محدودة الأهداف والنتائج، إذ قد تتعدى مخاطرها ميادين القتال التقليدية لتصل بدمارها إلى أكثر المواقع السيادية والحساسة تحصينا وبعدا عن دائرة القتال[2].

– **صعوبة الإثبات و الاكتشاف،** حيث تعتبر جريمة صعبة الإثبات، و أنها لا تترك في الغالب أثرا ماديا ظاهرا يمكن ضبطه، وسهولة محو الدليل أو تدميره في زمن قصير، يضاف إلى ذلك نقص خبرة الشرطة، والنظام العدلي، وعدم كفاية القوانين القائمة، كما أنها جرائم مخفية، لا يمكن أن تلاحظ آثارها، والتخمين بوقوعها؛

– **جرائم ذات جاذبية،** نظرا لما تمثله سوق الكومبيوتر والانترنت من ثروة كبيرة للمجرمين أو الإجرام المنظم، فقد غدت أكثر جذبا لاستثمار الأموال وغسلها وتوظيف الكثير منها في تطوير تقنيات وأساليب تمكن من الدخول إلى الشبكات وسرقة المعلومات وبيعها أو سرقة البنوك أو اعتراض العمليات المالية وتحويل مسارها أو استخدام أرقام البطاقات وغيرها[3].

– **عالمية الجريمة،** نظر الارتباط المجتمع الدولي الكترونيا، فقد أصبح مجتمعنا تخيليا مما أدى إلى إن تكون ساحة المجتمع الدولي بكافة دوله ومجتمعاته مكانا لارتكاب الجريمة من كل مكان ، والأمر الذي استدعى أن تكون القوانين ذات صبغة عالمية؛

– **جرائم ناعمة،** بمعنى لا تتطلب عنفا، فنقل بيانات من كمبيوتر إلى آخر أو السطو الالكتروني على أرصدة بنك ما لا يتطلب أي عنف أو تبادل إطلاق نار مع رجال الأمن؛

– **الفساد الثقافي،** لا يتوقف تأثير الجرائم المتصلة بالكمبيوتر عند الأثر المادي الناجم عنها، وإنما يتعدى ذلك ليهدد نظام القيم والنظام الأخلاقي خاصة في المجتمعات المحافظة والمغلقة[4].

– **مرتكب الجريمة الالكترونية يكون عادة مخترق ومدرب على كيفية التعامل مع البيانات،** والإنترنت وإرسالها بشكل لا يثير الشبهات في بعض الحالات[5]، إن المجرم المعلوماتي ذو مهارات تقنية عالية وإلمام بتكنولوجيا النظم المعلوماتية[6].

---

(1)– خالد ممدوح إبراهيم، المرجع السابق، ص 44.

(2)– نور أمير الموصلي، المرجع السابق، ص 11.

(3)– خالد حسن أحمد لطفي، المرجع السابق، ص 95.

(4)– المرجع نفسه، ص 96-97.

(5)– منال محمد عباس، المرجع السابق، ص119.

(6)– خالد ممدوح إبراهيم، المرجع السابق، ص47.

– **وقوع الجريمة المعلوماتية أثناء المعالجة الآلية للبيانات**، في أي مرحلة من المراحل الأساسية لتشغيل ضام المعالجة الآلية للبيانات سواء عند مرحلة إدخال البيانات أو أثناء مرحلة إخراج المعلومات[1].

– **جريمة مستحدثة**، تعد الجريمة الالكترونية من الجرائم المستحدثة، حيث أن التقدم التكنولوجي الذي تحقق خلال السنوات القليلة جعل العالم بمثابة قرية صغيرة، بحيث يتجاوز هذا التقدم بقدراته و إمكاناته أجهزة الدولة الرقابية، بل أنه أضعف من قدراتها في تطبيق قوانينها بالشكل الذي أصبح يهدد أمنها و أمن مواطنيها[2].

– **عدم الإبلاغ عن جرائم الانترنت**، وذلك بسبب عدم اكتشاف الفاعل أو الخوف من التشهير، وعليه نجد أن معظم جرائم الانترنت ثم اكتشافها بالمصادفة، وبعد وقت طويل من ارتكابها، و الجرائم التي لم تكشف هي أكثر بكثير من تلك التي كشف عنها الستار[3].

– **تعدد الأوصاف القانونية لمحل الجريمة الالكتروني**، إذ قد يكون محل الجريمة مادي أو معنوي، كما هو الحال بالنسبة للمعلومات، فقد تكون في حالة انتقال أو موجودة في ذاكرة النظام الالكتروني أي أنها في حالة غير مادية، و الشكل الأخر أن تكون المعلومات متجسدة في صورة مادية بتخزينها على دعامة الالكترونية، حتى أن المعلومات غير المادية بطبيعتها يمكن أن تخضع لأكثر من نص قانوني[4].

وعليه فالهجوم السيبراني من الافعال الاجرامية خاصة مع التطور التكنولوجي المتسارع، والتي تسمح للمخترقين من الاختراق بسهولة وذلك بإخفاء ومحو الدليل او تدميره في وقت وجيز بمجرد كبسة زر بحيث لا تتمكن سلطات البحث والتحقيق من كشف جرمه واقامة الدليل ضده فهو لا يحتاج الى جهد عضلي بل يعتمد على الذكاء الذهني المحكم والتفكير العلمي المدروس القائم على معرفة تقنية ممتازة للحاسب الالي والتعامل السليم للشبكة.

ثانيا: أنواع الهجمات السيبرانية

تعددت الهجمات السيبرانية من خلال الغاية منها، إذ تختلف من الغابة في كل هجوم وتختلف باختلاف التي وجدت من أجلها، ولكن عموما يمكن تقسيمها إلى هجمات فعالة وأخرى غير فعالة، وسنتعرض لبعض النماذج منها:

---

[1]–خالد ممدوح إبراهيم، المرجع السابق، ص 49–50.

[2]– المرجع نفسه، ص 51.

[3]– خالد حسن أحمد لطفي، المرجع السابق، ص 97.

[4]– المرجع نفسه، ص 100.

1- الهجمات الفعالة:

يركز المهاجمون على إيجاد الثغرات الأمنية والأبواب الخلفية لهذه البرامج والنظم ومن بين هذه الهجمات ما يلي:

1-1- هجمات الحرمان من الخدمة(DOS):

و تعتبر من أخطر الهجمات، حيث يقوم المهاجم بإطلاق برنامج خبيث يؤدي إلى زيادة قبول البرنامج، وبالتالي يمنع الاستخدام الحقيقي من الوصول إلى الخدمات التي تتوفر عليها البرامج[1]، وبمعنى أخر هو إيقاف قدرة الهدف على تقديم الخدمات المعتادة أو المفترض تقديمها، إذا فالهدف الرئيسي من هجمات الحرمان من الخدمة هو إجبار النظام الإلكتروني المستهدف على الاستجابة لعدد معتبر من الطلبات والأوامر الخدماتية بشكل يفوق قدرته، مما يمنعه عن تقديم الخدمات المطلوب منه تقديمها[2].

1-2- فيروسات الحاسوب: وهي برنامج مثل أي برنامج تطبيق آخر، لكنه مصمم من قبل أحد المخربين لإحداث أكبر قدر ممكن من الضرر للنظام بعد ربطه بالبرامج الأخرى، ولديه القدرة على تكرار نفسه حتى يبدو و كأنه يتوالد ذاتيا، والفيروسات كما حددها التقرير الصادر عن المركز القومي للحاسبات في الولايات المتحدة الأمريكية هي:" برامج مهاجمة تصيب أنظمة الحاسب بأسلوب يماثل إلى حد كبير الفيروسات الحيوية التي تصيب الإنسان"[3]، وبسبب وجود عدد كبير من البرامج التي تقوم بكشف الفيروسات والقضاء عليها، تم تطوير نوع أخر من الفيروسات يسمى بالفيروس متعدد الأشكال (polymophic virus) هذا النوع من الفيروسات يقوم بتغيير نفسه في كل مرة يتم تكراره فيها أو تفعيله ومن يصعب اكتشافه او القضاء عليه[4].

1-3- أحصنة طروادة: وهو شفرة أو برنامج تغيير مختبئ في برنامج كبير من البرامج ذات الشعبية المالية، وهو مبرمج بمهارة عالية، حيث يقوم بالمهام الخفية مثل: نشر دودة أو فيروس، ومن الصعوبة اكتشافه إذ يعمل دائما على مسح آثاره التي تحمل صنعة تخريبية، ويقوم بإضعاف قوة الدفاع للمستهدف

---

[1]- سالم محمد عبود، المرجع السابق، ص91.

[2]- نوران شفيق، أثر التهديدات الالكترونية على العلاقات الدولية" دراسة في أبعاد الأمن الإلكتروني"، المركز العربي للمعارف، القاهرة، 2016، ص21.

[3]- نور أمير الموصلي، المرجع السابق، ص 17.

[4]- نوران شفيق، المرجع السابق، ص26.

و سهولة اختراق و سرقة بياناته[1]، فضلا عن وجود هذه البرامج الخبيثة "القنابل" في عدد من مواقع الأنترنت التي تتضمن مثل هذه البرامج[2].

1-4 – برامج الدودة: تعرف برامج الدودة بالبرامج التي تستفيد من الثغرات الموجودة في نظام تشغيل الكومبيوتر للانتقال من كومبيوتر إلى آخر، مما يؤدي إلى احتلال الشبكة بالكامل والتسبب في نهاية بآثار مدمرة، وبفضل الوصلات التي تربط الشبكات بعضها ببعض، يمكنهم الانتقال من شبكة لأخرى و التكاثر مثل البكتيريا في عملية النقل، ومن أهداف تلك البرامج شغل أكبر قدر ممكن من سعة الشبكة ومن ثم تقليل أو خفض كفاءتها[3]، وهي أيضا برامج قادرة على إعادة إنتاج نفسها، ولكن بعكس الفيروسات فهي برامج قائمة بذاتها بمعنى لا تحتاج إلى مضيف(host) ولا إلى فعل البشر بل تقوم بتفعيل نفسها تلقائيا، ويمكن تكرار نفسها والانتشار إلى جهة أخرى[4].

1-5- الأبواب الخلفية: وهي ثغرة تترك عن عمد من مصمم النظام للتسلل إليه عند الحاجة، والجدير بالذكر أن الكثير من البرامج و النظم التي تطورها الولايات المتحدة الأمريكية تحتوي على أبواب خلفية تستخدمها عند الحاجة مما يسمح لها بالتجول الحر داخل نظام أي دولة أجنبية[5].

1-6 – الاختناق المروري الالكتروني: ويعني هذا سد وخنق قنوات الاتصال لدى المستهدف بحيث لا يمكنه تبادل المعلومات، أو استبدالها وهي في الطريق بين المرسل و المستقبل بمعلومات مضللة؛

1-7 – القصف الالكتروني: وهذا يعني الهجوم على شبكة المعلومات عن طريق توجيه مئات الآلاف من الرسائل الالكترونية إلى مواقع هذه الشبكات وبالتالي تسبب ضغط كبير على هذه المواقع، وتفقدها قدرتها على استقبال الرسائل من العملاء، ويؤدي ذلك إلى التوقف عن العمل تماما؛

1-8 – الهاكرز: وهم أفراد عاديين لديهم قدرات ومهارات عالية في استخدام الكومبيوتر لتحقيق أهدافهم أيا كانت سياسية أو غيره و يرغبوا في اثبات قدرتهم وبالتالي يتم ذلك بطرق غير شرعية، وتتم فيه عملية الاختراق و التدمير[6].

---

(1)–أقوى هجمات سيبرانية استهدفت روسيا، تاريخ الاطلاع(2024/02/25 على الساعة 21:00)، العربية، متوفر على الموقع :http://www.arabic.com.

(2)– نور أمير الموصلي، المرجع السابق، ص 17.

(3)– المرجع نفسه، ص 18.

(4)– نوران شفيق، المرجع السابق، ص26.

(5)– خالد حسن أحمد لطفي، المرجع السابق، ص 65.

(6)– المرجع نفسه، ص66.

2 – الهجمات الغير فعالة: وتتمثل في ما يلي:

2-1- برامج التجسس: وهي عبارة عن برامج تثبت خلسة على أجهزة الحاسوب بالتجسس و السيطرة عليها من دون علم المستخدم، و بإمكان هذه البرامج السيطرة على الحاسوب، وتركيب برامج إضافية وإعادة توجيه لمواقع الكترونية ضارة، والتسبب بمزيد من الفيروسات وتغيير إعدادات الحاسبات و إلحاق الضرر، كما حصل مع الكثير من الشركات العالمية الكبرى، مثل: شركة أمازون الأمريكية[1]، وبالتالي هو القيام باختراق شبكة أو جهاز الكتروني، بهدف سرقة المعلومات المخزنة فيه، والتي عادة ما تكون على درجة كبيرة من الأهمية، سواء كانت معلومات عسكرية، أم اقتصادية، أم صناعية، أم تجارية، أم غيرها، و يوصف هذا المستوى بأنه تجاوز لحدود الخصوصية الالكترونية الفردية[2].

2-2- التصيد: ويعرف أيضا بالخداع الالكتروني، إذ يخدع المستخدمون ليشاركوا بياناته الشخصية، مثل: تفاصيل بطاقات الائتمان وكلمات المرور، مما يسهل وصول المحترفين إلى أجهزتهم، وهي أكثر جرائم الاختراق شيوعا، وتتم عن طريق تقنيات التواصل الاجتماعي مثل رسائل البريد الالكتروني، والرسائل النصية SMS [3].

2-3- راصد لوحة المفاتيح: وهو أحد أشهر برامج التجسس، ومن أقدم أشكال التهديد السيبراني، يسرق المعلومات الشخصية أو المالية مثل التفاصيل المصرفية إذ يجمع المعلومات ويرسلها إلى طرف ثالث عن طريق برنامج مخفي يرسل عبر الايمايل، حيث سجل هذا البرنامج ضغطات المفاتيح التي يقوم بها المستخدم مثل سرقة كلمات السر، والمعلومات الأخرى المهمة التي تخص الأفراد أو المنظمات أو أرقام بطاقات الائتمان[4].

2 – نماذج عن الهجمات السيبرانية:

إن للهجمات السيبرانية انعكاسات على جميع الأصعدة، سواء على الصعيد السياسي أو الاستخباراتي أو حتى الاقتصادي والثقافي، يمكن إن لهذه الهجمات مجال واسع للتطبيق، فقط تتم وقت

---

(1)- عبد الحميد بن بادة، جريمة التجسس الالكتروني نمط جديد من التهديدات السيبرانية الماسة بآمن دول المنطقة، ورقة بحث قدمت ضمن فعليات الملتقى الدولي الأول الموسم "بآمن المعلومات في الفضاء السيبراني"، المنظم من قبل كلية الحقوق و العلوم السياسية، جامعة غرداية، (يومي17و18 فيفري2020)، ص 9-10.

(2)- حياة حسين، "الفضاء الالكتروني و تحديات الآمن العالمي"، مجلة العلوم القانونية والسياسية، مخبر الرقمنة والقانون في الجزائر، جامعة البليدة 02، المجلد 12، العدد 01، أفريل2021، ص 1069.

(3)- حياة حسين، المرجع السابق، ص 1069.

(4)- هاجر ختال، "الوضع القانوني للحرب السيبرانية على ضوء القانون الدولي"، مجلة التواصل في الاقتصاد و الادارة و القانون، كلية الحقوق و العلوم السياسية، جامعة باجي مختار، عنابة، المجلد 25، العدد 03، سبتمر2019، ص 161.

السلم أو أثناء الحرب، وفي هذا الصدد سوف تطرح نماذج عن تلك الهجمات في كلا الحالتين أي أثناء السلم أو إثناء النزاع المسلح؛

2-1- السيبرانية أثناء النزاع المسلح:

لقد أجمع المختصون في القانون الدولي الإنساني على أنه ليس جميع العمليات الالكترونية أو ما يطلق عليها "بالهجمات السيبرانية" تنطبق عليها أحكام القانون الدولي الانساني، فالقانون الدولي الإنساني لا ينظم العمليات التي تقع خارج السياق النزاع المسلح[1].

2-1-1 – النزاع المسلح في كوسوفو عام 1999: يرى بعضهم أن الهجمات السيبرانية قد تعنت لأول مرة في أثناء حرب كوسوفو عام 1995، حيث استهدفت سلاح الجو التابع لحلف الشمال الأطلسي لشبكات التي يوغسلافيا السابقة، أدت هذه الهجمات إلى توقف الاتصالات فجأة من خلال استخدام سلاح يعمل على تعطيل شبكات الاتصالات الخاصة بالجيش، وهذا ما حدث مع الجيش اليوغسلافي، الذي تعطل نظام الكمبيوتر الأساسي الخاص به[2].

2-1-2 – الهجوم الاسرائيلي على سوريا عام 2007: في هذا العام قام سلاح الجو الإسرائيلي بتنفيذ هجوم سيبراني استهدف أنظمة الاتصالات والرادارات السورية، مما أدى إلى تعطيلها بالكامل، وذلك تمهيدا لغارة جوية تنفذها إسرائيل على مناطق في سوريا[3].

2-2- الهجمات السيبرانية خارج النزاع المسلح:

مع تطور أجهزة الكمبيوتر والاعتماد الشامل على شبكات الاتصال أصبح تمكن تطبيق الهجمات السيبرانية في جميع الأوقات فقد تستخدم الهجمات وقت الحرب والسلم أيضا، ومن أمثلة الهجمات السيبرانية التي وقعت وقت السلم ما يلي:

2-2-1- الصراع السيبراني بين الصين والولايات المتحدة الأمريكية: يعد الصراع الالكتروني الدائر بين الصين والولايات المتحدة الأمريكية، أحد أكبر الاختراعات الإلكترونية القائمة في العالم، وهذا الصراع ناتج عن تنافس البلدين على القوة العسكرية والمالية والتجارية.

ومن أمثلة سلسلة هذه الهجمات، قيام عدد من المهاجمين الصينيين بمهاجمة مواقع الكترونية أمريكية، نجم عنها خسائر كبيرة عقب قيام الولايات المتحدة باستهداف مواقع الكترونية عسكرية واستحواذ على معلومات بشان تطوير مقاتلات صينية[4].

---

(1)- أحمد عبيس نعمة الفتلاوي، المرجع السابق، ص 266.

(2)- اسمهان بعيري، المرجع السابق، ص 28-29.

(3)- عدنان النقيب، المرجع السابق، ص83.

(4)- أحمد عبيس نعمة الفتلاوي، المرجع السابق، ص 247.

2-2-2- الهجوم السيبراني ضد موقع Google : منذ دخول شركة جوجل إلى الصين في 2006 والصراعات قائمة بينها وبين الحكومة الصينية، بسبب أن محرك جوجل هو ثاني أكبر محرك بحثي في الصين، والأقل تعرضا للرقابة. فقد حاولت شركة جوجل أن تتعامل مع قوانين الرقابة الصينية بأن حددت خدمتها فقط كمحرك بحثي، دون تقديم خدمات البريد الإلكتروني. كما أنها كانت تعلم المستخدم الصيني بوجود المعلومة وأنه لن يستطيع الوصول إليها بسبب سياسات الحكومة، كشفت شركة جوجل عن هجوم الكتروني تعرضت له ضمن 33 شركة أخرى في عام 2009 في إطار عملية فجر، والتي تم فيها اختراق الأجهزة الالكترونية التابعة للشركة لسرقة المعلومات الموجودة عليها فضلا عن اختراق حسابات (Gmail)[1]، وحسب ما أفاده المسؤولون عن محرك البحث العملاق جوجل أن الهجوم كان متطورا جدا وكان أساسه من الصين، ومن الجدير بالذكر أن شركة قوقل لم تصرح بالهجوم إلا في سنة 2010 [2].

المطلب الثاني: مخاطر وأبعاد الهجمات السيبرانية

يمثل استخدام شبكة الأنترنت إحدى سمات عصر الفضاء الإلكتروني في العصر الحالي نظرا للمميزات العديدة التي وفرتها تلك التقنية والثورة التكنولوجية على العالم أجمع، ولكن مع هذه المميزات لم يخلو المجتمع من المخاطر الجمة التي ترتبط بكيفية استخدام الأنترنت، وعليه سنتعرض لأهم هذه المخاطر التي تنتج عن استخدام شبكة الانترنت بشكل غير قانوني داخل المجتمع، وذلك من خلال مخاطر الهجمات السيبرانية (الفرع الأول)، ثم أبعاد الهجمات السيبرانية (الفرع الثاني).

الفرع الأول: مخاطر الهجمات السيبرانية

أولا: المخاطر السياسية والأمنية

1- المخاطر السياسية:

من أهم المخاطر السياسية التي تسعى التنظيمات الارهابية إلى تحقيقها من خلال منظومة الإرهاب الالكتروني:

1- تهدد شخصيات سياسية بارزة في المجتمع بالقتل.

2- القيام بتفجير منشآت وطنية، أو بنشر فيروسات من أجل إلحاق الضرر والدمار بالشبكات المعلوماتية والأنظمة الالكترونية.

---

[1]- نوران شفيق، المرجع السابق، ص157.

[2]- عدنان النقيب، المرجع السابق، ص85.

3 – اختراق البريد الالكتروني لرؤساء الدول وكبار الشخصيات السياسية وهتك أسرارهم و الاطلاع على معلوماتهم و بياناتهم و التجسس عليها لمعرفة مراسلاتهم و مخاطباتهم و الاستفادة منها في عملياتهم الإرهابية أو تهديدهم لحملهم على إثبات أفعال معينة يخططون لاقترافها؛

ومن الأمثلة عن ذلك:

في عام 2010 ظهر ما يعرف " بإعصار ويكيليكس" إذ تم استغلال شبكة الانترنت العالمية في تسريب وثائق تحوي معلومات سرية للغاية متداولة بين الإدارة الأمريكية و قنصلياتها الخارجية بدول العالم.

ـ في مارس 2014 هاجمت مجموعة" سايبر بيركوت" الاوكرانية المواقع الالكترونية لحلف الناتو، ما أدى إلى تعطيل مواقع الحلف لعدة ساعات، كما أكدت صحيفة نيويورك تايمز في تقرير لها في 26 أبريل 2015 أن قراصنة روسيين أطلعوا على رسائل الكترونية للرئيس الأمريكي باراك أوباما العام الماضي، بعدما تمكنوا من اختراق الشبكة الالكترونية غير السرية للبيت الأبيض[1]،

واطلعوا على أرشيف الرسائل الالكترونية لموظفين في البيت الأبيض يتواصلون يوميا مع أوباما، ومن خلال هذا الأرشيف تمكن القراصنة من قراءة رسائل تلقاها أوباما، وهذا ما يهدد الأمن القومي الأمريكي؛

2: المخاطر الأمنية:

من أهم المخاطر الأمنية التي تسعى التنظيمات الإرهابية إلى تحقيقها من خلال منظومة الإرهاب الالكتروني ما يلي:

1 – إلحاق الشلل بأنظمة القيادة والسيطرة والاتصالات، أو قطع شبكات الاتصال بين الوحدات و القيادات المركزية، أو تعطيل أنظمة الدفاع الجوي، أو اخراج الصواريخ عن مسارها، مما يهدد أمن الدول.

2 – الاختراق الالكتروني إلى الأنظمة الأمنية في دولة ما، وفك الشفرات السرية للتحكم بتشغيل منصات إطلاق الصواريخ الاستراتيجية، والأسلحة الفتاكة، وتعطيل مراكز القيادة والسيطرة العسكرية ووسائل الاتصال للجيوش بهدف عزلها عن قواتها، والنفاذ إلى النظم العسكرية واستخدامها لتوجيه الجنود إلى نقطة غير آمنة قبل قصفها أو تفجيرها[2].

ثانيا: المخاطر الاقتصادية والاجتماعية والثقافية

1– المخاطر الاقتصادية:

---

[1]– خالد حسن أحمد لطفي، المرجع السابق، ص74.

[2]– المرجع نفسه، ص 75.

بظهور العولمة والثورة التكنولوجية أصبح المجتمع يعاني من الكثير من المشكلات الاقتصادية الكبيرة، التي ارتبطت بالتنمية الاقتصادية والتي لها أثار إيجابية وأخرى سلبية، ومن هذه السلبية وجود جيوش جرارة من المتعطلين عن العمل والراغبين فيه من الشباب والمراهقين، يسلكون مسلكا غير شرعي مناقض للقانون والعرف السائد في المجتمع، ومن نتائج اللجوء إلى الانترنت الانغماس في عالم الفضاء الالكتروني والحصول على المال بعدة طرق مختلفة، كالنصب والاحتيال والسرقات والتلاعب في البورصة، واللجوء بجمع التبرعات الوهمية بقصد القيام بأعمال خيرية وكلها تمثل جرائم اقتصادية قد يقوم بها فرد أو جماعة(عصابة)، وكذلك الشراء عبر الانترنت بالبطاقة الائتمانية، ما حول المجتمع إلى استهلاكي لا إنتاجي، وأصبحت القدرة الشرائية تسترق الأموال وتبددها بسلع قد لا يستفاد منها بالطريقة المثلى[1].

ولعل من أهم المخاطر الاقتصادية التي تتحقق من خلال التنظيمات الإرهابية:

1-اختراق النظام المصرفي والحاق الضرر بأعمال البنوك وأسواق المال العالمية .

2-تعطيل عمليات التحويل المالي، مما يلحق الأذى بالاستثمار الأجنبي وبالثقة بالاستثمار عامة، وإلحاق الأذى بالاقتصادي الوطني[2].

2- المخاطر الاجتماعية والثقافية:

رغم التقدم الكبير الذي أحرزته الثورة التكنولوجية و الفضاء الإلكتروني حول العالم في التقارب الزماني و المكاني، و جعلت العالم قرية صغيرة ترتبط بعضها البعض من خلال هذه التكنولوجيا الجديدة، إلا أن هناك العديد من المخاطر التي أثرت على العديد من النواحي سواء كانت الاجتماعية أو الثقافية أو الاقتصادية أو البيئية...الخ، وأصبحت تتجلى بصورة مجسدة تتناول حياة الأفراد وتمس أسلوب معيشتهم مباشرة، فالمخاطر المرتبطة بالمنظومة الثقافية تتضح بوضوح من خلال ما سعت إليه الدول الكبرى من غرس و تحريك الولاء والانتماء لما يسمى بالمجتمع الكوني الجديد، الذي تترابط أطرافه بفضل تكنولوجيا الاتصالات الحديثة، وإلى طمس الهوية الوطنية و سحق الثقافة و الحضارة المحلية

وإيجاد حالة من الاغتراب ما بين الانسان وتاريخه الوطني وموروثاته الثقافية والحضارية، والتي تسيطر عليه الثقافة الأمريكية والتي تتباين مع ثقافات كثيرة لاسيما ثقافات الدول النامية، فالعولمة وما جاءت به

---

[1]- منال محمد عباس، المرجع السابق، ص61- 62.

[2]- خالد حسن أحمد لطفي، المرجع نفسه، ص 76.

من ثورة تكنولوجية و معلوماتية بمعناها الثقافي تعني فرض ثقافة الكسي السريع و السهل وتمكين الروح الاستهلاكية لدى الدول الفقيرة، ومن ثم طمس ثقافتها التقليدية و أعرافها و موروثاتها[1].

وعليه تظهر صعوبة في تقييم المخاطر بشكل عام، يرجع ذلك إلى طبيعة الفضاء الالكتروني تضفي عليها صعوبة إضافية لان نقاط الضعف التي يهاجمها الخصم لا يعلمها إلا هو ولا تكون الدولة على علم مسبق بها إلا بعد وقوع الجريمة، وهذا ما يبرر وجوب التدخل التشريعي بسن قانون خاص بالجريمة المعلوماتية.

الفرع الثاني: أبعاد الهجمات السيبرانية

أولا: البعد العسكري والسياسي

1- البعد العسكري:

لقد كانت بدايات الانترنت في بيئة عسكرية، بشكل أساسي، لتنتقل فيما بعد إلى الأوساط العلمية والأكاديمية، تمثلت في أبحاث تخدم القدرات العسكرية وتطورها، والانجازات العلمية، التي تساهم في تفوق بلد على أخر، حيث كان التنافس بين الاتحاد السوفياتي، والولايات المتحدة الأمريكية، في مجال الوصول إلى الفضاء الخارجي، وتطوير الأسلحة النووية.

ومن أمثلة ذلك: ما حصل في جورجيا، وإستونيا، وكوريا الجنوبية، وإيران، وتعتبر هجمات واختراقات مادية، سواء باندلاع صراع مسلح لاحق كذلك الذي وقع بين روسيا و جورجيا، أو بانقطاع الاتصال بالأنترنت في إستونيا بين الدول والمواطنين، والتشويش على الادارات الحكومية، كذلك اختراقات أنظمة المنشآت النووية، في إيران وتحقق إمكانات التلاعب بها، مع ما يعنيه هذا من تعرض الامن القومي للدولة المعنية؛

وفي هذا السياق وجه خبراء أميركيون خطابا مفتوحا للرئيس الأمريكي "جورج بوش" في 2007 محذرين إياه من خطر الهجمات السيبرانية على البنية التحتية الأمريكية، التي تضم إلى الدفاع إمدادات الطاقة الكهربائية، والمياه، الاتصالات السلكية واللاسلكية، والخدمات الصحية، والنقل، والانترنت[2].

ويتجلى ذلك من خلال ربط البيئة العسكرية ببعضها عبر العالم الافتراضي، وهذا ما يسهل عملية تبادل المعلومات من أجل تحقيق الأهداف العسكرية و حماية القدرات الدفاعية و حتى الهجومية للدولة،

---

[1]- منال محمد عباس، المرجع السابق، ص58-59.

[2]- سمير بارة، الأمن السيبراني (cyber Security) في الجزائر: السياسات والمؤسسات، المجلة الجزائرية للأمن الانساني جامعة قاصدي مرباح، ورقلة، العدد 04، جويلية 2017، ص260.

والترسانة العسكرية والنووية للدولة من خلال مجموعة لبرامج التقنية والتكنولوجية، وبالتالي ربط القوة العسكرية بالتطور التكنولوجي[1]،

إن عدم استغلال هذه التقنية والتسلح بها أو تأمينها من أي اختراق خارجي، سيؤدي بالضرورة الى شن هجمات الكترونية مضادة على شبكات القوات العسكرية، وثم تدمير قواعد البيانات، وما يلحقه من مخاطر[2].

كما يجب أن يوفر الأمن السيبراني للقوات العسكرية التواصل وتبادل المعلومات والأوامر عن بعد بشكل آمن مع وجوب القدرة على صد أي محاولة اختراق تؤدي إلى تدمير البيانات العسكرية لدولة العدو، بحيث يمس الأمن القومي مثلما حدث في إيران عند اختراق المنشآت النووية[3].

2- البعد السياسي:

تشكل السياسة عصب الحياة لدى الدول والمجتمعات ما يجعل الكثير من الصراعات السياسية الحاصلة في ارض الواقع تتحول إلى صراعات افتراضية تخلق نوع من الحروب، خاصة في السنوات الاخيرة أن أصبح توظيف القوة السيبرانية سلاح مهم للتغلب على خصم السياسة[4].

وبذلك يشكل الأمن السيبراني وسيلة حماية للمعلومات والوثائق الاساسية الحساسة لعمل قطاعات الدولة، وعليه لا يمكن تحقيقه حتى لا تخلق خلافات دبلوماسيا بين الدول ونذكر كمثال الحرب الروسية الاوكرانية 2022 التي كانت جراء اختراق الامن السياسي[5]،

وكذلك وجود أمثلة اخرى كثيرة تدفع للاهتمام بالبعد السياسي للأمن السيبراني، كالتسريبات المختلفة للوثائق الحساسة، التي تؤدي إلى مشكلات عويصة جدا، على المستوى الخارجي والدولي، كما أنه لا ينكر الدور لمتعاظم لشبكات التواصل الاجتماعي، على المستوى السياسي(حملات انتخابية)، تظاهرات افتراضية، حركات احتجاجية إلكترونية كما يتم استغلال هذه المواقع من طرف العديد من الحكومات لتمرير سياستها؛

---

(1)- سمير قلاع الضروس، الأمن السيبراني الوطني "قراءة في أهم الاستراتيجيات الامنية والتقنية لمواجهة الجريمة الإلكترونية بالجزائر"، مجلة الرواق للدراسات الاجتماعية والإنسانية، جامعة غرداية (الجزائر)، المجلد 08، العدد 02، 2022، ص255- 256.

(2)- سمير بارة، المرجع السابق، ص261.

(3)- جلالي شويرب و فائزة مراد، "مفهوم الحروب السيبرانية الأمن السيبراني"، مجلة الحقوق والحريات، جامعة عمار ثليجي الأغواط، كلية الحقوق والعلوم السياسية، المجلد 11، العدد 01، 2023، ص166.

(4)- سمير قلاع الضروس، المرجع السابق، ص256.

(5)- جلالي شويرب و فائزة مراد، المرجع السابق، ص167.

وفي سياق أخر يجب أن لا ننسى استخدام هذه المواقع من طرف الحركات الإرهابية لتجنيد أفرادها وجمع التمويل لعملياتها، وآلية للاتصال بينها كأفراد وكجماعات، وهو ما استوجب على الدول لعمل على حماية أمنها من التهديدات والمخاطر لتي قد تتعرض لها من خلال شبكة الانترنت[1].

ثانيا: البعد الاقتصادي والاجتماعي والقانوني

1- البعد الاقتصادي:

لقد أصبح الفضاء الالكتروني جاذبا لقطاعات المجتمع كافة، وباتت المعرفة محرك الإنتاج والنمو الاقتصادي، عرف الجميع أن التركيز على المعلومات والتكنولوجيا يعد عاملا من العوامل الأساسية للنهوض بالاقتصاد، وهذا ما دفع بالدول لزيادة الاستثمار في المعرفة، أصبحت عصرنة الاقتصاد مرتبطة بالتحكم في الاقتصاد الرقمي من طرف مختلف الفاعلين الاقتصاديين والاجتماعيين. كما أن استخدام الحاسوب وشبكة الأنترنت في تطوير الصناعات وتحريك الاقتصاد، ومعالجة كل المعاملات الاقتصادية والمالية، زاد من أهمية ضرورة توفير الأمن السيبراني لضمان حماية المعلومات[2]،

فالأمن السيبراني يرتبط بالاقتصاد ارتباطا وثيقا فاعتماد اقتصاد المعرفة يتصل اتصالا وثيقا بتقنيات المعلومات[3]، وبهذا ينتظر أهمية الأمن السيبراني بشكل أوسع وأكبر في المجال الاقتصادي لأن الفضاء الإلكتروني أصبح أساس للتعاملات التجارية والمالية والاقتصادية، كما أصبح الحاسوب أداة لتسيير الصناعة والاقتصاد ولهذا يستدعي الحرص على تحقيقه[4].

2- البعد الاجتماعي:

يرتبط الأمن السيبراني بالخصوص بشبكات التواصل الاجتماعي التي تسمح وتتيح جمع المعلومات المتعلقة بالأفراد والتي تسمى "الهندسة الاجتماعية" من خلال معرفة تطلعاتهم السياسية والاجتماعية واستغلالها[5]، كما تعتبر مواقع التواصل الاجتماعي أداة اتصال عالمية بين البشر، ولكنها عرضت أخلاق المجتمع للخطر إذ تمس هوية الأشخاص وتهدد السلم الاجتماعي،

---

(1)- سمير بارة، المرجع السابق، ص263.

(2)-سمير بارة، المرجع السابق، ص 261.

(3)- حسين ربيعي ومحمود ووسمر، الحروب السيبرانية "المخاطر واستراتيجيات تحقيق الأمن السيبراني الدولي والداخلي"، المجلة الجزائرية للأمن الانساني، جامعة الإخوة منتوري، قسنطينة، المجلد 07، العدد 02، 2022، ص179.

(4)- جلالي شويرب و فائزة مراد، المرجع السابق، ص166.

(5)- حسين ربيعي ومحمود ووسمر، المرجع السابق، ص180.

وعليه لا بد من العمل أولا على تكريس مفهوم الأمن السيبراني ثم توعية الأفراد بمخاطر اختراقه[1]. فبات من الضروري تعميم المفهوم الصحيح والسليم للأمن الى كل المشتركين في الشبكة الدولية للمعلومات، إذ تعتبر من الخطوات الأساسية التي تقوي مستوى الأمن إذا ما صيغت بطريق جيدة وواضحة وعرفت ونفذت بذكاء، لذا أصبح من الضروري توفير التثقيف والتدريب على تكنولوجيات المعلومات والاتصال[2].

3- البعد القانوني:

يمثل القانون أداة ضبط المجتمعات وهو يحمل نفس الوظيفة بالنسبة للفضاء الإلكتروني، إذ لابد أن تحدد الدول تشريعات خاصة وأطر قانونية تبنى على ما هو قانوني وغير قانوني، لأن الشيء الملحوظ أن الجريمة القانونية تفتقر للصرامة في التعامل معها سيما التشريعات الجنائية، كما أصبح الأمن الالكتروني حقا جماعيا من الحقوق الحديثة وتفرعت منه عدة حقوق كحق النفاذ إلى الشبكة العالمية للمعلومات وحق إنشاء المدونات الالكترونية بإبلاغ عن مخالفات وجرائم خاصة، وكل هذا يتطلب وجود قوانين تواكب التطور[3]، كذلك الحق في حماية البرامج المعلوماتية ويقابلها مجموع التزامات مثل: الالتزام العلاقة المستقبلية في الطبيعة التبادلية بين التطور التكنولوجي وتطور النظام القانوني والتشريعي[4].

وبالتالي يمكن القول بأن هذه الابعاد الاستراتيجية السالفة الذكر وجب التركيز عليها والاهتمام بها بشكل دقيق خاصة البعدين العسكري الذي يعتبر الواجهة الأمنية للدولة، والبعد الاقتصادي من خلال تعزيز نظام التأمين للحفاظ على المعلومات الخاصة بالدولة وبعيدا عن أي خطر للاختراق، وقصد تمكين هذه الابعاد وجب تكوين وخلق جيل رقمي يفهم ويستوعب المخاطر الأمنية الناتجة عن الجرائم الالكترونية.

---

[1]- جلالي شويرب و فائزة مراد، المرجع السابق، ص167.

[2]- سمير بارة، المرجع السابق، ص262.

[3]- سمير بارة، المرجع السابق، ص 167.

[4]- حسين ربيعي ومحمود ووسمر، المرجع السابق، ص180.

المبحث الثاني: الإطار القانوني للهجمات السيبرانية

تعد الهجمات السيبرانية نوع من الأنواع الإجرامية المستحدثة حيث أصبحت حقيقة يومية خاصة مع التطور التكنولوجي المتسارع والتي اعتمدت الدول من خلاله اجراءات تتخذها من أجل الهجوم على النظم المعلوماتية للعدو وبهدف التأثير فيها والدفاع عن نظم المعلومات الخاصة بالدولة .

ومن هذا المنطلق كانت هناك صعوبة في تكييف هذه الهجمات في ظل قانون الحرب أو في ظل النزاعات المسلحة وتحديد القانون الواجب التطبيق بين القانون الدولي الذي يحكم العلاقات بين الدول والقانون الانساني والاتفاقيات الدولية بناءا على المسؤولية الدولية الناشئة على الهجمات السيبرانية.

وسنتطرق إلى تكييف الهجمات السيبرانية والقانون الواجب التطبيق (المطلب الأول)، ثم إلى المسؤولية الدولية الناشئة عن الهجمات السيبرانية (المطلب الثاني).

المطلب الأول: تكييف الهجمات السيبرانية والقانون الواجب التطبيق

حصيلة لظهور الهجمات أصبح الفضاء السيبراني يمثل تحديات المجتمع الدولي، وفي هذا الإطار صدرت الجمعية العامة للأمم المتحدة عدة قرارات تؤكد فيها على خطورة استخدام تقنيات السيبرانية على الأمن والسلم الدوليين.

كما أن توسع الهجمات السيبرانية وانتشارها بشكل كبير ورهيب، وما ينتج عنها من آثار مضرة بالإنسانية، هذا ما جعل مسألة البحث عن التكييف القانوني لهذه الهجمات مع تحديد القانون الواجب التطبيق عليها مسألة صورية.

ومن هذا المنطلق سنتطرق إلى تكييف الهجمات السيبرانية (الفرع الأول)، ثم إلى القانون الواجب التطبيق على الهجمات السيبرانية (الفرع الثاني).

الفرع الأول : تكييف الهجمات السيبرانية

يعد تكييف الهجمات السيبرانية بعد استخدام شبكة المعلومات والاتصال وتنوع أشكال التهديدات الناجمة عنها بشكل تحديا كبيرا يواجه النظام الدولي المعاصر، وعليه لابد من تكييف الهجمات السيبرانية في ضل كل من القانون الحرب الذي يوجد بين ثنايا القانون الدولي العام، والقانون الدولي الإنساني هذا الذي يهدف إلى حماية ضحايا النزاعات المسلحة بغض النظر عن انتمائهم لأطراف النزاع ومدى شرعية النزاع[1]، وذلك خلافا لقانون الحرب الذي يبحث في مدى شرعية النزاع المسلح ويسعى إلى تقييد اللجوء فيما بين الدولة وهذا هو السبب في استغلال قانون الحرب عن القانون الدولي الإنساني[2].

---

[1]– نور أمير الموصلي، المرجع السابق، ص 15.

[2]– عدنان النقيب، المرجع السابق، ص 170.

لا توجد قواعد واتفاقيات دولية وقانون إنساني تتعامل بشكل مباشر مع الهجمات الالكترونية لأن هذه الأخيرة– الهجمات السيبرانية– والعمليات الالكترونية غير منظمة في المنازعات المسلحة، إضافة إلى أن تطوير الهجمات الالكترونية حصل في فترة لاحقة على إعداد صكوك القانون الدولي الإنساني، كما أن هذا القانون وضعت قواعده لتنظيم وسائل أساليب القتال ذات طبيعة المتحركة التي تنتج عنها آثار مادية غير متوفرة في الهجمات السيبرانية، وبالتي فان الهجمات السيبرانية تكون خارج نطاق قانون الدولي الإنساني، أي بعبارة أخرى أن القانون الدولي الإنساني يطبق أثناء النزاعات المسلحة، والهجمات السيبرانية ليست مسلحة ولكن يمكن طبق شرط مارتينز على الهجمات السيبرانية[1].

وعليه سنتناول تكييف الهجمات السيبرانية في ظل قانون الحرب (أولا)، ثم تكييف الهجمات السيبرانية في ظل النزاعات المسلحة (ثانيا).

أولا: تكييف الهجمات السيبرانية في ظل قانون الحرب

يعتبر قانون الحرب يشير إلى الظروف التي تمكن الدول فيها اللجوء إلى النزاع المسلح أو استخدام القوة المسلحة بشكل عام، أي بعبارة أخرى في مشروعية اللجوء إلى استخدام القوة المسلحة، ومن أجل بناء عالم يسوده السلام نص ميثاق الأمم المتحدة على تسوية النزاعات بالطريقة السلمية وحظر أعمال العدوان ومنع التهديد باستخدام القوة ضد أي دولة [2].

كما أن الهجمات السيبرانية تشكل تهديدا للمبادئ الرئيسية في القانون الدولي، كذلك احترام سيادة الدولة ومنع استخدام القوة والتهديد باستخدامها، وذلك في ظل غياب نصوص قانونية خاصة في قانون الدولي حول هذه الهجمات، لذلك نجدها استندت في ذلك على المبادئ والتي سنفصل فيها فيما يلي:

1– مبدأ السيادة:

ويرجع مفهوم السيادة بشكل عام إلى معاهدة وستفاليا لعام 1648، والتي كانت أول من أرسى هذا المبدأ ويقصد به (أن تقوم الدولة بإدارة شؤونها دون تدخل من أي دولة أخرى) [3].

---

[1] -Marco Roscini ,World Warfare, Jus ad bellum and the Use of cyber Farce, Max Planck Yearbook of united Law.VOL 14.2014, p.95.

[2]– اسمهان بعيري، المرجع السابق، ص 31.

[3]– إسراء نادر كيطان، المسؤولية الدولية عن الأضرار التي تحدثها الهجمات الالكترونية في الفضاء الافتراضي، ماجيستر، الجزء الثاني، المجلد 03، العدد خاص لبحوث التدريسيين مع طلبة الدراسات العليا، 2021، ص 339، تاريخ الاطلاع (2024/04/15 على الساعة 14:37)، متوفر على الموقع: Esraamader 743@gmail.com-lumam529@ gmail.com

إن المفهوم التقليدي للسيادة لم يعد كما هو، إنما طرأ عليه تغيير بسبب التطور التكنولوجي وظهور الفضاء الافتراضي، فبرز ما يسمى بالسيادة السيبرانية [1]، هذا ما دفع دول العالم لفرض الرقابة عليها فهي مفهوم جديد مشتق من مصطلح الأمن السيبراني الذي يتعلق بحماية البنى التحتية الرقمية والتقنيات والمحتويات الرقمية والاتصالات، وكل ما يمكن أن يرتبط بالفضاء السيبراني[2].

ومن بين التحديات الراهنة أمام سيادة الدولة، انتشار الهجمات السيبرانية وتطور استخدام الحاسوب وشبكات الاتصال وظهور الفضاء السيبراني كمجال ثاني إلى جانب المجال البحري والجوي والفضاء الخارجي، وظهور مفهوم السيادة السيبرانية والتي تعرف بأنها "بسط الدولة لسيطرتها وولايتها القضائية على الفضاء الرقمي المتمثل بالأنترنت الذي يجتاز حدود الدولة وينشأ مجموعة أشخاص افتراضية ضمن شبكات الكترونية ما وراء أي انتماء وطني"[3].

هذا وواجهت السيادة تحدي جديد وهو الهجمات الالكترونية، والتي تقوم عبر شبكات الانترنت لانتهاك السيادة الوطنية لدولة ما، وذلك عندما يكون الهجوم دفع ضمن سيادة دولة أخرى، وبهذا يكون مفهوم السيادة التقليدي بدء يتقلص بسب وسائل الاتصال الالكترونية التي جعلت الحدود الإقليمية تتضاءل شيئا فشيئا في الفضاء الافتراضي، وما ينتج عنه من مخاطر لذلك قامت الدول بتطوير تشريعاتها الوطنية استبعاد هذه الجرائم والمخاطر[4].

كما أن الهجمات السيبرانية تشكل تهديدا حقيقيا بالسيادة السيبرانية للدول، فالدولة لها حق سيادي في إدارة شبكة الانترانت الخاصة بها، والتي يجب أن تعمل بشكل مستقبل ودون الخضوع لدولة أخرى، وأي مساس بالبنية التحتية الإلكترونية الأساسية وغيرها هو انتهاك لسيادتها، كما أن سيادة الدولة لا تكون علي البنية التحتية للإلكترونية الموجودة على إقليمها فحسب وإنما تمتد إلى البنى التحتية التي تحت سيطرتها والموجودة على إقليم دولة أخرى [5].

ومن خلال ما تقدم فان الهجمات الالكترونية التي تقوم بما دولة ضد دولة أخرى تكون خرقا لسيادة تلك الدولة، ومن ثم ينطبق مبدأ السيادة في الفضاء السيبراني، لكن ليس بشكل الذي ينطق فيه بالعالم

---

[1]– هناك من استعمل مصطلح السيادة الرقمية بدل السيادة السيبرانية .

[2]– إسراء نادر كيطان، المرجع السابق، ص 340.

[3]– اسمهان بعيري، المرجع السابق، ص 32.

[4]– إسراء نادر كيطان، المرجع السابق، ص 340.

[5]– منى الأشقر جبور، المرجع السابق، ص 30.

الواقعي، لأن الفضاء الافتراضي لا يعرف الحدود، وعلى الرغم من ذلك أقرت السيادة للدولة في هذا الفضاء لأن أثار الهجمات الالكترونية قد تكون خطرة [1].

2-مبدأ حظر استخدام القوة والتهديد باستخدامه:

إن المادة الثانية (2) من ميثاق الأمم المتحدة تنص في الفترة الرابعة منها على أنه" يمتنع أعضاء الهيئة جميعا في علاقاتهم الدولية عن التهديد باستخدام القوة أو استخدامها ضد الأراضي أو الاستقلال السياسي لأية دولة أو على أي وجود لا يتفق ومقاصد الأمم المتحدة "[2].

ويتم هذا بقاعدة أخرى في ميثاق، وهي قاعدة عدم التدخل في الشؤون الداخلية أو الخارجية لدولة أخرى، وهو ما أكدته محكمة العدل الدولية في عدة قضايا ومن بينها قضية الأنشطة العسكرية وشبه العسكرية "نيكاراغو"، حيث نص بأنه متى ما اتخذ تدخل شكل استخدام أو التهديد باستخدام القوة فان قاعدة عدم التدخل الواردة في القانون العرفي تتطابق مع المادة (2/ف4) من ميثاق الأمم المتحدة [3].

ولقد نصت الفقرة الرابعة من المادة الثانية للميثاق علي المصطلح القوة دون اقترانه بأي مصطلح آخر، أي دون تحديد نوع القوة، وذلك خلافا لمواد اخرى من الميثاق التي نصت على القوة المسلحة، كما ورد في الديباجة والمادة (44) من الميثاق، وعليه مفهوم القوة لا ينحصر فقط على القوة العسكرية، فقد التدخل مالي، أو اقتصادي أو السياسي[4].

كما أدت التطورات في المجال الإلكتروني إلى ظهور بعد جديد للقوة، وهي القوة السيبرانية، إلا انه يجب التمييز بين القوة السيبرانية التي تتوافق في تداعياتها مع القوة العسكرية وتلك القوة السيبرانية التي لها تأثير إعلامي أو اقتصادي أو سياسي[5].

إن القوة السيبرانية التي تدخل ضمن مفهوم الفقرة 4 من المادة (2) من ميثاق الأمم المتحدة، هي تلك التي تتوافق في تداعياتها مع القوة العسكرية التقليدية من قتل على نطاق واسع وتدمير الطبيعة والبيئة التحتية للدولة، أما مجموعة الخبراء في دليل تالين الذي أعدته اللجنة الدولية التابعة لحلف شمال

---

[1]- إسراء نادر كيطان، المرجع السابق، ص 340.

[2]- المادة 2/ف4 من ميثاق الأمم المتحدة لعام 1945

[3]- محكمة العدل الدولية، قضية الأنشطة العسكرية وشبه العسكرية في نيكاراغوا ضد الولايات المتحدة الأمريكية، 27 جوان 1986، موجز الأحكام والفتاوى الصادرة من محكمة العدل الدولية 1948-1991، منشورات الأمم المتحدة نيويورك ،1999، ص212، تاريخ الاطلاع (2024/04/17 على الساعة 11:30) متوفر على الموقع:
.https://www.icj.cij.org/or

[4]- اسمهان بعيري، المرجع السابق، ص 33-34.

[5]- يحي ياسين مسعود، المرجع السابق، ص 87.

الأطلسي، والمكونة من خبراء قانونيين وعسكريين سنة 2013، اعتبرت أن "أي هجوم سيبراني يكون باستخدام

أو تهديدا باستخدام القوة ضد السلامة الإقليمية والاستقلال السياسي لأي دولة أو أي شكل من الأشكال يتعارض مع مقاصد الأمم بعد عملا غير مشروع" [1].

3-مبدأ الدفاع الشرعي:

لقد نص في ميثاق الأمم المتحدة على أن المجلس الأمن هو من يقرر ما إذا كان قد وقع تهديد للسلم أو إخلال به لو كان ما وقع عملا من أعمال العدوان، ويقدم في ذلك توصياته يقرر ما يجب اتخاذه من التدابير، طبقا لأحكام المادتين (41) و(42) لحفظ السلم والأمن الدولي أو إعادته إلى نصابه [2].

ونصت المادة (51) من ميثاق الأمم المتحدة لعام 1945 على حق الدفاع الشرعي للدولة في حال تعرضت لأي اعتداء وهذا ما جاء في نصها" ليس في هذا الميثاق ما يضعف أو ينقص الحق الطبيعي للدول، فرادى أو جماعات، في الدفاع عن أنفسهم إذا اعتمدت قوة مسلحة على أحد أعضاء الأمم المتحدة وذلك إلى أن يتخذ مجلس الأمن للتدابير اللازمة لحفظ السلم والأمن الدوليين والتدابير التي اتخذها الأعضاء استعمالا لحق الدفاع عن النفس تبلغ إلى المجلس فورا، ولا تؤثر تلك التدابير بأي حال فيما للمجلس لمقتضى سلطة ومسؤوليات المستمرة من أحكام الميثاق من الحق في أن يتخذ في أي وقت ما يرى ضرورة لاتخاذه من الأعمال لحفظ السلم والأمن الدولي أو إعادته إلى نصابه".

ومن خلال هذين المادتين يطرح التساؤل إذا كان نص هذين المادتين يطلق على الهجمات التقليدية واستخدام القوة المجال الواقعي، وكذلك إمكانية تطبيقها علي الهجمات الالكترونية في الفضاء الافتراضي، وما إذا كان للدول التي تتعرض للهجوم السيبراني حق الدفاع عن نفسها، وفي هذا الصدد سنتطرق إلى ثلاث نظريات فيما يلي:

3-1-نظرية النهج القائم على الوسيلة:

وتستند هذه النظرية على الوسيلة التي تستخدم في الهجوم، إذا تؤكد على أن الهجوم السيبراني وحدة لا تكون هجوم صلح ومن ثم لا يكون للدول حق الدفاع عن نفسها وقف للمادة (51) من ميثاق لأمم المتحدة سالفة الذكر لأن هذا الهجوم ليس فيه الخصائص الفيزيائية التي ترتبط بالإكراه العسكري وبتعبير آخر فهو لا يحتوي على الطاقة الحركة كما في الأسلحة التقليدية[3].

---

[1]- زهراء عماد محمد كلنتر، المرجع السابق، ص 112.

[2]- إسراء نادر كيطان، المرجع السابق، ص 340.

[3]- المرجع نفسه، ص341.

3-2- نظرية النهج القائم على حماية البنية التحتية:

وتشيد هذه النظرية إلى حق الدول في الدفاع عن النفس ومثال على ذلك استهداف البنى التحتية لدول هجوما مسلحا وقفا لهذه النظرية، لكن هذه النظرية انتقدت لأنها تجاهلت مفهوم البنى التحتية الحرجة وجسامة الهجوم السيبراني وأثاره[1].

3-3- نظرية النهج القائم على الآثار:

تعد هذه النظرية وسط بين النظرتين السابقتين، وهي تقوم على خطورة أثار الهجوم، لها بعد الهجوم الالكتروني مسلحا إذا كانت آثاره خطيرة، مثال ذلك الهجوم ضد نظام مراقبة الملاحة الجوية والتسبب بحوادث للطائرات، فبعد هذا الهجوم مسلحا، لأنه من المتوقع أن بتسبب خسائر في الأموال والأرواح، ومن هذا النطق يمكن القول أن هذا الاتجاه هو الأكثر قبولا إلا أنها تطبق على مجموعة صغيرة من الهجمات الالكترونية الضارة والتي تكون لها أثار تشبه أثار الأسلحة التقليدية[2].

ومما تقدم ذكره يمكن أن تثبت أن الهجوم السيبراني متى كانت أثاره ضارة يكون بمثابة هجوم مسلح واستخدام للقوة ضد دولة ما، فيكون لهذه الأخيرة حق الدفاع عن نفسها فيطبق الاستثناء الوارد في المادة (51) من الميثاق وهو حق الدفاع الشرعي، وهو ما ذهب إليه(دانيل سيلفر) المستشار العام السابق لوكالة الاستخبارات المركزية ووكالة الأمن القومي الأمريكية إلى القول بأن: "الهجوم السيبراني سينوع الدفاع الشرعي إذا كانت النتيجة المتوقعة إحداث إصابات جسدية أو أضرار مادية تماثل النتائج المرتبطة بالإكراه المسلح[3].

ولقد أيد ماركو روسي هذا التوجه بقول" من الممكن عد الهجمات السرية بمثابة خرق واضح بأحكام الفقرة 04 من المادة (02) من ميثاق الأمم المتحدة، شريطة أن تثبيت بتعطيل أو دمار واسع للبني التحتية الضرورية للإنسان، وفيما لتحقق ذلك فالدولة المتعدي عليها، الحق في اللجوء إلى استخدام القوة بموجب المادة(51) من الميثاق نفسه، والتي نصت على الحق في الدفاع عن النفس[4].

ومما سبق يمكن القول أن أحكام ميثاق الأمم المتحدة أعطت الحق للدولة المعتدى عليها في إطار الهجمات السيبرانية متى ما تسببت هذه الأخيرة في آثار كبيرة على البنية التحتية للدولة المتضررة، إذ يحق لها أن ترد على هذا الاعتداء تحت ما يسمي بالدفاع عن النفس.

---

[1]- إسراء نادر كيطان، المرجع السابق، ص 342.

[2]- المرجع نفسه، ص.342

[3]- اسمهان بعيري، المرجع السابق، ص 35.

[4]- المرجع نفسه، ص 35.

ثانيا: تكييف الهجمات السيبرانية في ظل النزاعات المسلحة

على الرغم من أن الهجوم السيبراني لا يتشكل بذاته نزاعا مسلحا إلا أن الهجمات السيبرانية قد تشكل جزاء من النزاع بهدف لتحقيق غاية عسكرية، وبالتالي يثير الموضوع الخاص بهذه الجزئية مسألة تتعلق بوصف الهجمات السيبرانية كجزء من نزاع مسلح [1].

ومن المتفق عليه أن القانون الدولي الإنساني ينطبق علي الهجمات السيبرانية التي تحدث في سياق نزاع مسلح قائم بالفعل فيجب علي الدول أن تحترم قواعد القانون الدولي الإنساني عندما تشن هجمات سيبرانية في إطار نزاع مسلح بغض النظر عما إذا كان الفضاء السيبراني معترفا به كميدان قتال اصطناعي جديد يضاف إلى الميادين الطبيعية للحرب، المتمثل في البر والجو البحر والفضاء الخارجي ويرتبط بجميع هذه الميادين الطبيعية، أم لم يعتبر ميدانا للحرب في حد ذاته [2].

كما أن الخبراء في الأمم المتحدة علي انطباق المبادئ القانونية كمبادئ الإنسانية والضرورة العسكرية والتناسب في استخدام القوة والتمييز بين المدنيين والمقاتلين على الهجمات السيبرانية التي تقع أثناء النزاع المسلح[3].

وسنتعرض إلى أربعة مبادئ أساسية لمعرفة مدى انطباق مبادئ القانون الدولي الإنساني على الهجمات السيبرانية كمبدأ الضرورة العسكرية والتناسب في استخدام القوة والتمييز بين المدنيين والمقاتلين وأخيرا مبدأ مارتينز.

1- مبدأ الضرورة العسكرية:

وهو المبدأ الذي يسمح فقط باستخدام النوع والدرجة من القوة غير المحظورة، والتي تكون لازمة لتحقيق الهدف المقصود والمشروع من النزاع المسلح وهو إخضاع العدو بصورة كاملة أو جزئية و بأقل قدر ممكن من التضحية في الأرواح والموار، وبالتالي لمنع في هدا الخصوص تدمير ممتلكات العدو أو حجزها إلا إذا كانت ضرورات الحرب تقتضي حتما هذا التدمير والحجز [4].

وتجدر الإشارة إلى أن مبدأ الضرورة العسكرية تم ذكره في صكوك دولية عدة من بينها ديباجة إعلان بيان بيترسبورغ لعام 1928، والذي نص على: "الهدف المشروع الوحيد الذي يجب أن تسعى إليه الدول في أثناء الحرب هو إضعاف القوات العسكرية للعدو" وفي نفس السياق أشارت المادة (52) من

---

[1]- يحي ياسين مسعود، المرجع السابق، ص 87.

[2] - نور أمير الموصلي، المرجع السابق، ص55.

[3]- يحي ياسين سعود، المرجع السابق، ص 87.

[4]- المرجع نفسه، ص 92.

البروتوكول الإضافي الأول لعام1977 في الفقرة الثانية إلى أن" تقتصر الهجمات على الأهداف العسكرية فحسب "والتي يحقق تدمير كلي أو جزئي أو الاستيلاء عليها أو تعطيلها، في الظروف السائدة حينا ذاك ميزة عسكرية أكيدة" [1].

فمبدأ الضرورة العسكرية بعد من المواضيع المهمة في القانون الدولي الإنساني، إذا يقوم أساسا على الموازنة بين متطلبات الضرورة العسكرية والاعتبارات الإنسانية وذلك الضرورة تتطلب استخداما للقوة العسكرية المتاحة لتحقيق تفوق أو ميزة عسكرية، بينما الاعتبارات الإنسانية وتقتضي تقيد استخدام هذه القوة لتحقيق الميزة العسكرية المبتغاة بأقل الخسائر في الأرواح والأعيان وسائل وأساليب قتالية إنسانية، ولأهمية هذا المبدأ يمكن تعريفه بأنه " تلك تدابير التي لا غنى عنها لتحقيق غايات الحرب، على أن تكون هده التدابير مشروعة وفقا لأعراف وقوانين الحرب، وبتعبير آخر أن الضرورة العسكرية هي الملاذ الأخير الذي يبرر كل التدابير التي لا غنى عنها لضمان التقدم على العدو، بشرط أن لا يتعارض مع قانون النزاعات المسلحة" [2].

2- مبدأ التناسب في استخدام القوة:

إن مبدأ التناسب في استخدام القوة العسكرية في النزاع المسلح قد أكدت عدة صكوك دولية على واجب مراعاتها، منها ما ورد في البروتوكول الإضافي الأول لعام 1977في الفترة 15من المادة (51) إذ نصت "إن الهجوم الذي يتوقع منه إحداث خسائر عرضة في الأرواح المدنيين وإصابة المدنيين الإضرار بالأعيان المدنية أو مزيجا منها الذي يكون مفرط فيها يتعلق بالميزة العسكرية المباشرة والملموسة المرتقبة، وتثير تطبيق مبدأ التناسب على الهجمات السيبرانية بعض الصعوبات، ذلك أن الأضرار أمر لا مجال بسبب عدم وجود الفاعل في كثير من الأحيان بين الفضاء السيبراني موضع استخدام المدنيين وبين ذلك الفضاء الذي يستخدم من قبل القوات والجماعات المسلحة والمدنيين المشاركين في العمل العدواني[3].

إن تحقيق التناسب في الهجمات السيبرانية قد يكون مستحيلا وذلك لأن تكنولوجيا المعلومات غير متساوية في الدول، ومن ثم قد تكون الدولة الضحية غير متطور من ناحية التكنولوجيا الهجمات السيبرانية، مما يجعل تطبيق مبدأ التناسب على الهجمات تقسيم بصعوبة بالغة [4].

---

[1]- اللجنة الدولية للصليب الاحمر، القانون الدولي المتعلق بسير العمليات العسكرية، مجموعة اتفاقيات لاهاي وبعض المعاهدات الاخرى، الطبعة الثانية، جنيف، سبتمبر 2001، ص 129.

[2]- إسراء نادر كيطان، المرجع السابق، ص 343.

[3]- يحي ياسين سعود، المرجع السابق، ص 94.

[4]- زهراء عماد محمد كلنتر، المرجع السابق، ص 148.

3- مبدأ التميز بين المدنيين والمقاتلين:

ولقد وردت الإشارة إلى مبدأ التميز بين المقاتلين والمدنيين لأول مرة في ميثاق إعلان سان بطرسبورغ لعام 1868، عندما نص على أن: "الهدف المشروع الوحيد الذي يتعين علي الدول أن تسعى إلى تحقيقه أثناء الحرب هو إضعاف القوات العسكرية للعدو، وقد جري تعين هذا المبدأ في البروتوكول الإضافي الأول المشار إليه أعلاه، وأيضا تطالب المادة (51) من البروتوكول الإضافي الأول بضمان الحماية العامة للمدنيين المهاجمين من لأخطار الناشئة عن العلميات العسكرية، أما بالنسبة للمدنيين الذين يشاركون بشكل مباشر في الأعمال العدائية فإنهم لا يتمتعون بالحماية بحكم المشاركة، كما أشرنا سابقا والجدير بالذكر أن النظام الأساسي للمحكمة الجنائية الدولة ونص علي هذا المبدأ حيث اعتبر أن تعمد توجيه هجمات ضد السكان المدنيين بصفتهم هذه، أو ضد أفراد مدنين لا يشاركون مباشرة في الأعمال الحربية على أنه جريمة حرب" [1].

ولقد نصت المادة (48) من البروتوكول الإضافي الأول لعام 1977على أن: "تقتصر الهجمات علي الأهداف العسكرية فحسب وتنحصر الأهداف العسكرية فيما يتعلق بالأعيان علي ذلك التي تسهم مساهمة فعالة في العمل العسكري، سواء كان ذلك بطبيعتها أم بموقعها أو بغايتها أم باستخدامها والتي تحقق تدميرها التام والجزئي أو الاستيلاء عليها أو تعطيلها في الظروف السائدة حينا ذاك ميزة عسكرية كبيرة"

واستثناء لنص المادة أعلاه وجب على أطراف النزاع المسلح التميز بين المدنيين والمقاتلين، وبين الأعيان المدنية والأهداف العسكرية دون غيرها.

4- مبدأ مارتينز:

سمي بمبدأ "مارتينز" نسبة إلى الدبلوماسي الروسي في" فيدور فيودوفج مارتينز" أحد مندوبي روسيا في مؤتمر السلام لعام 1899، والذي صرح فيه:" في الحالات الغير مشمولة بالأحكام يظل السكان المتحاربون تحث حماية للسلطان مبادئ قانون الأمم المتحدة كما جاءت من تقاليد استقر عليها بين الشعوب المتمدنة والقوانين الإنسانية ومقتضيات الضمير العام"[2].

ويعني ذلك أنه في غياب، نص صريح بحضر الهجمات السيبرانية على البنية التحتية الحرجة فإنها محمية بموجب المبادئ العامة والضمير الإنساني، وما استقر عليه العرف الدولي؛

---

[1]- نور أمير الموصلي، المرجع السابق، ص 45.

[2]- زهراء عماد محمد كلنتر، المرجع السابق، ص 149.

للإشارة فإن هذا المبدأ له أهمية كبرى، فهو القاعدة الخلفية أو الاحتياطية التي تلجأ إليها كلما فشلت أو انعدمت القواعد الاتفاقية والعرفية في معالجة المسائل التي تهم البشرية وتمسها في كيانها، كما تتجلى أهميته في إمكانية اتخاذه أساسا للمسؤولية الدولية المزدوجة المدنية عن الأضرار التي تلحق بالدول ومصالحها والتعويض عما لحق بها، والجنائية الفردية للقادة ومرؤوسيهم في حال وقوع ضحايا [1].

وأخيرا يمكن اعتبار شرط مارتينز صار الأمان الذي يمنع الدول وغيرها من الأطراف المتنازعة من استخدام واستحداث وسائل قتال جديدة كما يقطع الطريق أمام الدولة التي تتهرب من المسؤولية بحجة عدم وجود القواعد القانونية تحكم الوسائل والأساليب الجديدة التي لم يتطرق إليها القانون الدولي الإنساني[2].

الفرع الثاني: القانون الواجب التطبيق علي الهجمات السيبرانية

تعد مسألة تحديد القانون الواجب التطبيق على الهجمات السيبرانية من المسائل المهمة، لذا سنحاول تحديد القواعد التي تخضع لها هذه الهجمات، وذلك من خلال التطرق إلى خضوع الهجمات السيبرانية للقانون الدولي التي تحكم العلاقات بين الدول (أولا)، ثم خضوع الهجمات السيبرانية للقانون الدولي الإنساني (ثانيا)، وأخيرا خضوع الهجمات السيبرانية للاتفاقيات الدولية الخاصة بالحروب السيبرانية (ثالثا).

أولا: خضوع الهجمات السيبرانية لقواعد القانون الدولي التي تحكم العلاقات بين الدول

تأتي في مقدمة هذه القواعد نصوص ميثاق الأمم المتحدة، لاسيما الأحكام المتعلقة بخطر استخدام القوة في العلاقات الدولية، وخطر اللجوء إلى العدوان، وكذا مبدأ احترام سيادة الدولة، واستقلالها السياسي، بالإضافة إلى أحكام اتفاقية فينا لقانون المعاهدات لعام 1969، كما تجدر الإشارة إلى أن قواعد دليل تالين الخاصة بالحروب السيبرانية جاءت موافقة لما نص عليه ميثاق الأمم المتحدة فلقد تضمنت المادة الأولى منه مسألة سيادة الدولة بالإضافة إلى أحكام ميثاق الأمم المتحدة فلقد أكدت الجمعية العامة للأمم المتحدة أن حقوق الأشخاص خارج الفضاء السيبراني وداخله يجب أن يحظى بالحماية الكاملة، حيث طلبت الجمعية العامة من المفوضية السامية لحقوق الإنسان إعداد تقرير عن الخصوصية في الحق الرقمي، إذ تناول التقرير "حماية الحق في الخصوصية وتعزيز في سياق المراقبة الداخلية والخارجية للاتصالات الرقمية أو اعتراضها وجمع البيانات الشخصية [3].

---

[1]– وداد بوطلاعة ومنال بوكورو، المرجع السابق، ص 337.

[2]– أحمد عبيس نعمة الفتلاوي، المرجع السابق ، ص 36 .

[3]– اسمهان بعيري، المرجع نفسه، ص 41.

ثانيا: خضوع الهجمات السيبرانية لمبادئ القانون الدولي الإنساني

تخضع الهجمات السيبرانية التي تنفذ في إطار النزاع المسلح لقواعد القانون الدولي الإنساني، لاسيما القواعد التي تحكم سير العمليات العدائية، وكما جاء في تقرير اللجنة الدولة للصليب الأحمر عام 2011، يجب أن يتوافق توظيف الهجمات السيبرانية في إطار النزاع المسلح مع جميع مبادئ القانون الدولي الإنساني وقواعده، كما هو الحال مع أي سلاح أو وسيلة أو أسلوب حرب آخر جديد أو قديم، وما يؤيد ذلك أنه أشارت إليه محكمة العدل الدولية أن "مبادئ وقواعد القانون الدولي الإنساني المنطبق في النزاع المسلح، تنطبق على جميع أشكال الحروب وعلى جميع أنواع الأسلحة بما في ذلك تلك المستقبلية"[1]، ولقد استثنت اللجنة الدولية للصليب الأحمر في تقريرها عام 2015 عمليات التجسس من انطباق القانون الدولي الإنساني عليها، ولكنها استدركت على هامش التحرير أنه من الممكن أن يشملها القانون الدولي الإنساني، وذلك للاختراقات التي تنتج عنها الأضرار، حيث أن أغلب العمليات السيبرانية تتم في بدايتها عن طريق التجسس والحصول على البيانات عن طريق اختراقها للأجهزة والحواسيب، أما الاستثناء الثاني فيتعلق بتشويش الاتصالات اللاسلكية والبث التليفزيوني فلم يتم اعتباره من قبل الهجوم الوارد في القانون الدولي الإنساني[2].

ويواجه انطباق القانون الدولي الإنساني على الهجمات السيبرانية تحديات عدة فلا يتضمن القانون الدولي الإنساني على أي قواعد صريحة بشأن الهجمات السيبرانية في السيبراني، والسبب في هذا أنها تكون خطة للهجمات الحركية، أي ليست هجمات مسلحة بالمعنى التقليدي، إلا أنه وبالنظر إلى الهدف الأساسي للقانون الدولي الإنساني المتمثل في حماية المدنيين من ويلات الحرب، يصبح القانون الدولي الإنساني منطبقا وتندرج الهجمات ضمن قواعده إذا كان هدفها تعويض الأشخاص المحميين للخطر[3].

ثالثا: خضوع الهجمات السيبرانية للاتفاقيات الدولية الخاصة بالحروب السيبرانية

نظرا للتطور الحاصل في تكنولوجيا المعلومات، وظهور مجال خاص وهو الفضاء السيبراني، وانتشار تهديدات التي أصبحت تشكل خطرا دائما يهدد الأمن والسلم الدوليين، سعي المجتمع الدولي إلى عقد العديد من الاتفاقيات الدولية التي من شأنها تنظيم و وضع إطار قانوني يحكم مثل هذه الهجمات ومن أهم هذه الاتفاقيات نجد اتفاقية بودابست لسنة 2001، المتعلقة بالجريمة السيبرانية، وكذلك دليل تالين الصادر في عام 2013، الخاص بالحروب السيبرانية، وسنتعرض لهما فيما يأتي :

---

[1]– نور أمير الموصلي، المرجع السابق، ص 44.

[2]– اسمهان بعيري، المرجع نفسه، ص 40.

[3]– نور أمير الموصلي، المرجع السابق، ص 54.

1- اتفاقية بودابست لعام 2001 الخاص بالجريمة السيبرانية:

لقد تم إبرام هذه الاتفاقية نتيجة التغيرات المتتالية التي نجمت عن طريق الرقمنة وعن التقارب الرقمي والعولمة، وكذا إدراك الدول الأطراف للمخاطر التي قد تنجم عن استخدام شبكات الحاسوب[1].

ويعاب على هذه الاتفاقية أنها تنفذ من قبل الأفراد وضد الأفراد، دون التطرق إلى الهجمات السيبرانية التي تنشئها الدول ضد بعضهما البعض[2].

إضافة إلى اتفاقية بودابست لعام 2001 تم الاتفاق بين الدول على إصدار قانون (الأونيسترال) النموذجي وذلك يتطلب استجابة ديناميكية في ضوء الطابع الدولي لإساءة استخدام الكومبيوتر والجرائم المتعلقة به، إذ تم صياغة قانون (الأونيسترال) النموذجي بشأن التجارة الإلكترونية، وقانون آخر بشأن التوقعات الإلكترونية عام 2001 [3].

2- أحكام دليل تالين لعام 2013 الخاص بالحرب السيبرانية:

أعد هذا الدليل من قبل مجموعة من الخبراء في القانون الدولي بدعوة من منظمة حلف شمال الأطلسي بحضور لجنة الصليب الأحمر الدولي، ويشمل هذا الدليل على (95) قاعدة استمدت مجملها من أحكام القانون الدولي[4].

ولقد ورد في القاعدة (71) من هذا الدليل النص الثاني " للدولة التي تكون موضوع هجوم سيبراني تصل إلى حد الهجوم المسلح أن تمارس حقها الطبيعي في الدفاع عن النفس يعتمد ما إذا كانت العملية تشكل هجوما مسلحا على حجمها وأثرها".

ويستند دليل تالين على مؤشرين هذا حجم الهجوم وأثره، فإذا بلغ الهجوم السيبراني من الشدة والتدمير ما يعادل الهجوم المسلح الحركي فهنا تقوم قواعد في الدفاع عن نفسها[5].

وجاء دليل تالين ببعض النقص الذي تضمه القانون الدولي في مجال الحرب السيبرانية، وتم إبرامه كصك قانوني وحيد يمكن اللجوء إليه عند الضرورة ولكن يعاب على هذا الدليل أنه نظم الهجمات السيبرانية التي تحدث في إطار النزاع المسلح التقليدي، وفقا للمادة (20) من الدليل.

حيث نصت على أن كل نشاط سيبراني يجب أن يخضع لقواعد النزاعات المسلحة لكنها اشترطت أن يتم ذلك في سياق نزاع مسلح، إضافة إلى ذلك فقواعد هذا الدليل لا ترقى إلى مستوى الاتفاقيات

---

(1)- سليمان قطاف و عبد الحليم بوقرين، المرجع السابق، ص80.

(2)- نور أمير الموصلي، المرجع السابق، ص 168.

(3)- طلال ياسين العيسى وعدي محمد عناب، المرجع السابق، ص90.

(4)- وداد بوطلاعة ومنال بوكورو، المرجع السابق، ص 341.

(5)- المرجع نفسه، ص 348.

الدولية فهي ليست ملزمة فضلا عن معارضة بعض الدول الحاكمة كروسيا والصين على اعتبار أنهما لم تشاركا في إعداده.

المطلب الثاني: المسؤولية الدولية الناشئة عن الهجمات السيبرانية

تعد المسؤولية الدولية من أهم العلاقات موضوعات القانون الدولي في الوقت الراهن فعند النظر إلى التطورات العملية الحديثة التي أثرت تأثيرا بالغا على العلاقات الدولية نجد أنه ظهرت مشكلات جديدة لم تتناولها قواعد القانون الدولي بالتنظيم، مما أدى إلى ضرورة معالجة هذه المشكلات بطريقة جديدة تتلاءم مع طبيعتها إضافة إلى ذلك فإن قواعد المسؤولية يعبر بها عن عدم الوضوح بشكل عام، وخاصة فيما يتعلق بالهجمات السيبرانية[1].

والمسؤولية الدولية بصفة عامة لا يمكن أن تثار في مواجهة دولة ما لم تتوافر على شروطها وأركانها وذلك من خلال أركان المسؤولية على الهجمات السيبرانية (الفرع الأول)، ثم أساس المسؤولية الدولية عن الأضرار التي يسببها الهجوم السيبراني (الفرع الثاني).

الفرع الأول: أركان المسؤولية علي الهجمات السيبرانية

هناك تشابه كبير بين النظام القانوني الداخلي والنظام القانون الدولي لا يتعلق بقواعد المسؤولية [2]، فإذا كان نظام القانون الداخلي الفرد، فان النظام القانوني الدولي له أشخاص الخاصون ومنهم الدول، الدولة التي تقوم بأي فعل من شأنها إحداث الضرر يتبع بقيام المسؤولية الدولية، والهجمات السيبرانية تهديدا تتسبب في أضرار لأفراد المجتمع الدولي، وبالتالي تستوفي شروط قيام المسؤولية الدولة التي سوف يتم عرضها [3].

وذلك بالتطرق إلى نسبة الفعل إلى الدولة (أولا)، ثم أن يكون الفعل غير مشروع دوليا (ثانيا)، وأخيرا الضرر (ثالثا).

أولا: نسبة الفعل إلى الدولة

لا يكفي لقيام المسؤولية الدولية وجود الضرر، بل يجب إسناد الفعل إلى الدولة، ففي التشريعات الداخلية يشترط القانون إسناد الفعل إلى شخص ما لا مكان لقيام المسؤولية، ويستوجب في الدولة المسند

---

[1]– وداد بوطلاعة ومنال بوكورو، المرجع السابق، ص 341.

[2]– زهرة عماد محمد كنتر، المرجع السابق، ص 98.

[3]– المرجع نفسه، ص 157.

إليها المسؤولية أن تكون كاملة السيادة، وبالتالي فإن الدولة المنظمة إلى الدولة الاتحادية لا تسأل عن أعمالها، لأنه لم تعد من أشخاص القانون الدولي[1].

وفي حالة الهجمات السيبرانية، نجد أن الضرر يتحقق بمجرد إطلاق تلك الهجمات، خاصة وأن تلك الهجمات تستهدف البنى التحتية للدولة قد يخلق أضرار كثيرة وأن من يقوم بهذه الهجمات هي الدول المتقدمة التي تملك القوة الإلكترونية الكبيرة، بالإضافة إلى الدول كاملة السيادة يمكن أن تقوم الدول القومية أو حتى المنظمات الحكومية، وفي بعض الأحيان يمتد إلى الأفراد[2].

ثانيا: أن يكون الفعل غير مشروع دوليا

لقد عرف العمل الغير مشروع بأنه مجرد انتهاك دولة لواجب دولي أو عدم تنفيذها للالتزام الذي تفرضه قواعد القانون الدولي، كما عرف بأنه مخالفة الدول لقيامها أو امتناعها لعمل لا يجيزه القانون كما عرف بأنه هو سلوك مخالف لالتزامات قانونية دولية، أو هو الخروج على قاعدة من قواعد القانون لا يتأثر القانون الدولي بأية أوصاف يصفها القانون الوطني[3].

وقد أجمع الفقه الدولي بأن الفعل الغير مشروع دوليا وهو ذلك الفعل الذي يعد انتهاكا لأحكام القانون الدولي، أي يعني مخالفة الدول لأحكام ومبادئ القانون العام، ويتمثل أساسا في القيام بفعل أو امتناع عن القيام بفعل، يشكل مخالف لأخذ التزاماتها الدولية، فمعيار عدم المشروعية هو معيار دولي موضوعي، لا عبرة فيه لمنشأ الالتزام، لام المخالفة أي لالتزام دولي، أيا كان مصدره تولد المسؤولية دون النظر لوصف الفعل في القانون الداخلي، كما لا يعتمد بالوسيلة التي يتحقق بها انتهاك القانون الدولي، سواء كان ذلك بفعل أم امتناع عن فعل، أو إهمال [4].

وبتطبيقها على الهجمات السيبرانية، نجد أنها مخالفة لقواعد القانون الدولي، لأنها قد تسبب أضرار مادية وبشرية كبيرة، وهذا مخالف لمقاصد الأمم المتحدة، والقانون الدولي الإنساني، وغيرها من قواعد القانون الدولي ككل .

---

[1]– زهرة عماد محمد كنتر، المرجع نفسه، ص 155–160.

[2]– المرجع نفسه، ص 167.

[3]– عبد العزيز العشاوي، محاضرات في المسؤولية الدولية، دار هومة، الجزائر، 2007، ص28–29.

[4]– طلال ياسين العيسى وعدي محمد عناب، المرجع السابق، ص89.

ثالثا: الضرر

عنصر الضرر يعد أهم عنصر من عناصر المسؤولية، لأنه إذا انعدم الضرر انعدمت المسؤولية وللضرر أنواع وبالنظر لمصلحة المعتدي عليه، أو الجهة التي لحقها الضرر ومن ثمة فان أنواع الضرر بالنظر إلى الجهة التي لحقها الضرر ينقسم إلى (ضرر مباشر، وضرر غير مباشر) ومن حيث مصلحة المتعدي عليه ينقسم إلى (الضرر المادي، والضرر المعنوي).

ويعد الضرر المادي كل مساس بحق من حقوق الشخص القانوني الدولي المادية أو بحقوق رعاياه، مما يترتب عليه أثر ملموس ظاهر للعيان، ويكون مباشرا أما الضرر المعنوي فهو كل مساس بشرف أو اعتبار الشخص الدولي أو بأخذ رعاياه، أي أن الضرر المعنوي هو كل اعتداء على حق من حقوق الأشخاص الدوليين أو رعاياهم، وتترتب عنه أثار غير ملموسة[1].

وتطبيقا على الهجمات السيبرانية، نجد أن الضرر بكافة أشكاله يتحقق من تلك الهجمات، سواء كان الفاعل دولا قومية، كما حصل في الهجوم الفيروسي على البرامج النووي الإيراني، أو تقوم به منظمات إجرامية تلحق أضرارا فادحة بالآخرين، خاصة في الهجمات التي تهدف لسرقة المعلومات إذا اخترق حسابات بنكية وسرقة أرقام بطاقات الائتمان، ورغم أن أركان المسؤولية الدولية في الهجمات السيبرانية متوفرة إلا أن الفاعلين ومراقبتهم وتتبعهم من أجل محاكمتهم، أمر بالغ الصعوبة لما يتمتع به هذا الفضاء من قابلية التخفي[2].

الفرع الثاني: أساس المسؤولية الدولية عن الأضرار التي يتسبب بها الهجوم السيبراني

إن المسؤولية الدولية للهجوم السيبراني بالمعني الدقيق تنبعث من القانون الدولي العرفي، والمواثيق الدولية باعتبارها تمس القيم الأساسية للمجتمع الدولي، حيث أصبحت شبكة الانترنيت تشكل قوة اجتماعية واقتصادية وسياسية مؤثرة في العالم، ويمكن أن تستخدم لزيادة حدة سباق التسلح، وقمع حركات التحرر الوطني، وحرمان الأفراد والشعوب من حقوقهم الإنسانية وحرياتهم الإنسانية، كما أن المنجزات العملية التكنولوجية يمكن أن تعرض لأخطار الحقوق المدنية السياسية للفرد أو الجماعة، والكرامة البشرية، وتمس بكيان الدولة واستقلالها[3].

---

[1]– طلال ياسين العيسى وعدي محمد عناب، المرجع السابق، ص 89.

[2]– سامية صديقي، المسؤولية الدولية المترتبة عن الهجوم السيبراني في منظور القانون الدولي، مجلة البحوث القانونية والاقتصادية، جامعة محمد البشير الإبراهيمي، برج بوعريريج، الجزائر، المجلد 06، العدد 01، 2023، ص829.

[3]– المرجع نفسه، ص829.

وسنتناولها في المسؤولية عن الهجمات السيبرانية على أساس عمل غير مشروع (أولا)، والمسؤولية عن الهجمات السيبرانية استنادا إلى نظرية المخاطر(ثانيا).

أولا: المسؤولية عن الهجمات السيبرانية على أساس عمل غير مشروع

مما لاشك فيه أن المسؤولية الدولية من المواضيع المتشبعة والمهمة وهي أهم ضمانة لكفالة تطبيق القانون الدولي بسبب غياب سلطة عليا مستقلة عن الدول تمتلك السلطة الشرعية لتحديد نظام المسؤولية، وفرض احترامه كما هو الحال في القانون الوطني[1].

تنطوي نظرية الفعل غير المشروع أن كل إخلال بالتزام دولي من قبل دولة ما يستوجب مسؤولية هذه الدولة سواء كان هذا الإخلال صادر من سلطتها التشريعية أو التنفيذية أو القضائية والحق ضررا بأحد الأجانب في شخصية أو أمواله وكان متواجدا بأرضيها، ويعتبر الفقيه انزيلوتي من تبني نظرية الفعل غير مشروع[2].

ويرى الفقيه انزيلوتي أنه من حق الدولة المضرورة المطالبة بإصلاح الضرر وتقديم ضمانات للمستقبل، وأن العلاقة القانونية التي تنشأ بها الروابط بين الدولة نتيجة الإخلال بالحقوق نفس ملامح الرئيسة التي تتسم بها الروابط في قانون الالتزامات وتظهر في أعقاب تصرف غير مشروع هو بصورة عامة انتهاك لالتزام دولي ينشأ علاقة قانونية جديدة بين الدولة صاحبة التصرف، والدولة التي وقع الإخلال في مواجهتها، فتلتزم بالتعويض ويحق للثانية إن تقتضي هذا التعويض تلك هي النتيجة الوحيدة التي تمكن إن تلصقها القواعد الدولية المعبرة عن الالتزامات المتبادلة بين الدول بالعمل المخالف للقانون، كما نجد الفقيه بول روتر يعتر أيضا العمل غير مشروع أساس للمسؤولية الدولية بل الشرط الأهم لقيامها[3].

تعتبر الهجمات الدولية عمل غير مشروع، وتخضع للمسؤولية الدولية على هذا الأساس إذا توفر معيار الصفة الدولية، والمتمثل في صدور هذه الهجمات من قبل الدولة تخضع لها هذه الدول حتى يتم إلحاقها بالمسؤولية الدولية، أما المعيار الثاني أن تكون هذه الهجمات الالكترونية الدولية خارقة لمعاهدة أو عرف أو ميثاق دولي، وبتوضيح أكثر لهذا العنصر يجب أن يترتب على هذه الهجمات الأضرار بمصالح الدولة المعتدى عليها الاقتصادية والسياسية والاستراتيجية، أو تمس بأحد المبادئ التي كرستها الأمم المتحدة من أجل حفظ السلم والأمن الدوليين والمحافظة عليهما من أي اختراق أو تدخل يضر

---

[1]–عبد العزيز العشاوي، المرجع السابق، ص18.

[2]– المرجع نفسه، ص18.

[3]– سامية صديقي، المرجع السابق، ص 830.

بمصالح الدولة الأساسية، التي لا يجوز انتهاكها، كما يمكن إسناد مسؤولية الدولة عن الهجمات السيبرانية، التي تعتبر أعمال غير مشروعة إلى نص المادة (19) من مشروع تقنين مسؤولية الدولة، التي أكدت على أن عمل الدولة الذي يتشكل مخالفة الالتزام الدولي، يعد عملا جائزا دوليا بغض النظر عن موضوع الالتزام الذي تمت مخالفته، كانتهاك جسيم للالتزام الدولي ذي أهمية أساسية في الحفاظ علي السلم والأمن الدوليين منح ذلك تلك التي تحصر العدوان.[1]

إن إسناد المسؤولية للدولة عن الأضرار الناتجة عن الهجمات السيبرانية يمكن أن تشير مشكلة تتمثل في صعوبة تحديد ما إذا كان هذا العمل منسوبا للدولة فعلا، وهذا مرتبط بالقدرة التكنولوجية المتنامية، والتي يمكن أن تكون الدولة منشأ التصرف أن تطمس هوية الفاعل الحقيقي.[2]

إضافة إلى ذلك فإن عملية نسبة العمل الدولية تزداد تعقيدا في الحالة التي لا تكون الشبكات السيبرانية هي الوسط الذي تمت من خلاله هذه الهجمات كإرسال فيروسات توضح مباشرة في أجهزة الحاسوب الخاصة بالدولة المستهدفة أو في الحالة التي تستخدم فيها إقليم دولة أخرى لتنفيذ هذه الهجمات، كما أن التحقيقات بشأن الهجمات السيبرانية قد تجمع بين المبادئ الأساسية لعمل أجهزة الاستخبارات بوصفها عملا ماديا طبيعيا وبين الإلكتروني العابر للشبكات والحدود الدولية، لكن المحققين في أجهزة الاستخبارات الدولية قد لا يستطيعون الولوج للدول الأخرى لأنه يشكل مساسا وانتهاكا بسيادتها.[3]

ولقد لخص الفقيه" تونكين" هذه النظرية تغيرا منه الفقه السوفياتي آنذاك فذكر بأن العمل الدولي غير مشروع ينقسم إلى قسمين، إما غير مشروعة تمس السلم الدولي، وهناك أفعال غير مشروعة أخرى تكون أقل درجة، كما أن الممارسة السوفياتية أظهرت أن الحكومة الاتحادية السوفياتية نفسها تتعامل مع هذه النظرية رسميا، وهذا حينما أرسلت في عام 1957 إلى أعضاء الأمم المتحدة بهذه النظرية، معتبرة أن الحق في السلم هو حق شخصي لكل دولة ويتمثل في عدم استعمال القوة[4].

---

[1]– سامية صديقي، المرجع السابق، ص 830.

[2]– رزق أحمد سمودي، حق الدفاع عن النفس نتيجة الهجمات الالكترونية في ضوء قواعد القانون الدولي العام، مجلة جامعة الشارقة للعلوم القانونية، المجلد 15، العدد 02، 2018، ص338.

[3]– سامية صديقي، المرجع السابق، ص 831.

[4]– لخضر زازة، أحكام المسؤولية الدولية في ضوء قواعد القانون الدولي العام، دراسة مدعمة بالأمثلة والسوابق القضائية وأعمال لجنة القانون الدولي، دار هومة، جامعة الاغواط، 2011.

ثانيا: المسؤولية عن الهجمات السيبرانية استنادا إلى نظرية المخاطر

جاءت نظرية المخاطر كنظرية حديثة نتيجة الانتقادات التي وجهت لنظرية الفعل غير المشروع، التي أصبحت عاجزة عن مواكبة التطور التكنولوجي والعلمي وكان نتاج هذا التطور العالم الافتراضي الذي أصبح مسرحا لإدارة شؤون الدول في شتى المجالات سواء سياسية أو اجتماعية أو اقتصادية، وتقوم نظرية المخاطر على أساس مساءلة الشخص القانون الدولي الذي يقوم بارتكاب سلوك مخالف للقانون الدولي يكون على درجة الخطورة، بحيث ينتج عنه إضرار بالدول أخرى، فالعبرة بحدوث الضرر لأنه وحده من يرتب المسؤولية الدولية في حق الدولة التي تباشر نشاطا دوليا مشروعا، ويؤكد أنصار هذه النظرية على أن المخاطر تقوم على فكرة تحمل نتائج التي تترتب على النشاطات الخطرة وليس على أساس الخطأ[1].

ومن أهم الاتفاقيات الدولية التي أخذت بنظرية المخاطر نجد الاتفاقيات الخاصة بالطاقة الذرية، التي تلزم الدولة التي تقوم بأي نشاط ذري وقت السلم بتعويض الأضرار الناجمة عن هذه النشاط على أساس المسؤولية المطلقة المتجردة عن نسبة أي خطأ للدولة، كاتفاقية باريس المتعلقة بالمسؤولية الدولية قبل الغير في ميدان الطاقة النووية لسنة 1960،

والمسؤولية بموجب اتفاقية باريس لسنة 1960 مطلقة تقع على عاتق المستغل القائم بإدارة المنشأة النووية، فهو المسؤول عن أي خسارة أو ضرر للأشخاص أو الممتلكات، عما يقع خارج المنشأة ولا تنتفي المسؤولية إلا في حالة وقوع حادث ابن النزاعات المسلحة أو كارثة طبيعية أو غزو، وإلا عليه أن يدفع التعويض اللازم[2].

إن أغلب الأضرار تصيب دولا أخرى تكون نتيجة أعمال غير مشروعة للدول المتسببة فيها أو عن أنشطة مشروعة وفقا لمعايير القانون الدولي، ورغم ذلك تعذر إثبات عدم مشروعيتها أو يتعذر إثباتها بصفة عامة، لذلك أقيمت المسؤولية على أساس توفر ركن الضرر والعلاقة السببية بين الضرر وبين النشاط الذي تقوم به الدولة، وعلى هذا الأساس يجب أن نبين ما إذا كانت شروط المسؤولية الموضوعية تنطبق على الفضاء السيبراني وهما شرطان، الشرط الأول، هو وجود نشاط خطر، أما الشرط الثاني هو الضرر العابر الحدود، أما بالنسبة للشرط الأول والمتمثل في وجود نشاط خطر باعتبار أن الهجمات السيبرانية فالأنشطة الضارة في الفضاء السيبراني تسبب ضررا عابر للحدود يمس البنية التحتية للدول والأمن والسلم الدولي، فان الهجمات السيبرانية والأنشطة الضارة التي تقوم بها الدول في العالم

---

[1]– سامية صديقي، المرجع السابق، ص 832.

[2]–عبد العزيز العشاوي، المرجع السابق، ص 174.

الافتراضي، تكيف على أنها نشاطات خطرة نظرا لما ينتج عنها من أثار وخيمة على الأمن القومي والدولي، أما الشرط الثاني والمتعلق بالضرر العابر للحدود وهنا لا يمكن أن ننكر أن الهجمات السيبرانية والأنشطة الضارة التي تمارسها الدولة في الفضاء الالكتروني لإلحاق أضرار بالدولة، إذ أن تبني الدول الحكومة الإلكترونية في تسيير شؤونها واتساع نطاق مستخدمي وسائل الاتصال وتكنولوجيا المعلومات في العالم جعل قواعد البيانات القومية غير سرية مما عرضها إلى مخاطر هجمات الفضاء الالكتروني[1]، وقيام المسؤولية الموضوعية تشترط وجود علاقة سببية بين النشاط الخطر والأضرار الناتجة عنها[2].

لذلك يجب إثبات أن الأضرار التي لحقت الدول ومست أمنها القومي ناتج عن الهجمات السيبرانية التي قامت بها دولة أخرى ومن هنا يمكن القول أن نظرية المخاطر يمكن أن تصلح كأساس المسؤولية الموضوعية في العالم الخارجي[3].

وبالتالي فان المسؤولية الدولية عن الهجمات السيبرانية في مجال القواعد الدولية للقانون الدولي العام قد لا تحقق أهدافها وأغراضها ويرجع ذلك إلى صعوبة تحديد هوية المهاجم السيبراني وكذلك صعوبة ملاحقته قضائيا وإكمال إجراءات المتابعة القضائية، وهذا ما يجعلنا أمام عائق يحول دون تحقيق أهداف القانون الدولي باعتباره ينظم قواعد المسؤولية المتعلقة بانتهاكات القانون الدولي الإنساني والقانون الدولي العام.

---

[1]– سامية صديقي، المرجع نفسه، ص 833.

[2]– محمد حيدر، المسؤولية عن الأضرار البيئية في القانون المدني الجزائري، مداخلة مقدمة في ملتقى الوطني حول آليات الوقاية من الأخطار الطبيعية والتكنولوجية الكبرى في القانون الجزائري والقوانين المقارن، كلية الحقوق والعلوم السياسية، جامعة حسيبة بن بوعلي، الشلف، (يومي 01 و02 ديسمبر 2014).

[3]– سامية صديقي، المرجع السابق، ص 834.

خلاصة الفصل الأول:

نخلص مما سبق في هذا الفصل إلى أن الهجمات السيبرانية هي من أهم التحديات المعاصر التي تواجه المجتمع الدولي، وذلك نظرا لتأثيرها الكبير عليه كما أن موضوع الهجمات السيبرانية محل خلاف ودراسات لدى المختصين في القانون الدولي فيما يتعلق بمفهومها وتكييفها في ظل قانون الحرب و في ظل النزاعات المسلحة.

أما بالنسبة للأحكام القانونية التي تخضع لها الهجمات السيبرانية فهي موزعة بين القانون الدولي التي تحكم العلاقات بين الدول و القانون الدولي الإنساني وأيضا الاتفاقيات الدولية الخاصة بالحروب السيبرانية.

وسعيا من المجتمع الدولي لتنظيم هذه التهديدات وضعت العديد من الصكوك الدولية المتعلقة بالحروب والجرائم السيبرانية مثل اتفاقية بودابست لعام 2001 وأحكام دليل تالين لعام 2013 الخاص بالحرب السيبرانية.

الفصل الثاني:

تأثير الهجمات السيبرانية على السلم والأمن الدوليين وسبل مواجهتها

الفصل الثاني: تأثير الهجمات السيبرانية على السلم و الأمن الدوليين و سبل مواجهتها

لقد عرف التاريخ البشري صراعات وحدود عدة بين الدول وكان ميدانيا الرئيس على أرض الواقع ولها حدود معينة وتدار بأدوات معروفة تتناسب مع هذا الصراع ولكل طرف في هذا الصراع أدواته للهجوم والردع والدفاع بمعني أنها يمكن أن تحدد العدو والصديق مسبقا وأهدافها عن دخولها في الصراع إلا أنه ومع نهاية القرن الثاني ودخول القرن لثالث ويفضل الثورة المعلوماتية والثورة التكنولوجية أصبح هناك مسرح آخر وقضاء آخر تدار عليه الصراعات بكل أنواعها وقد أدى هذا التطور التكنولوجي لاعتماد الدول على هذه التكنولوجيات في التنمية الاقتصادية والاجتماعية وبروز الفضاء السيبراني كعنصر مؤثر في النظام الدولي، والكشف عن أنماط جديدة من المخاطر والتهديدات السيبرانية الذي أصبح يشكل المهدد الرئيسي للأمن والسلم الدوليين، مما حتم على دول العالم على اختلاف مستوياتها الاقتصادية والاجتماعية للتعاون في سبيل البحث عن استراتيجيات وميكانيزمات فعالة كفيلة بالتصدي لهذا النوع من التهديدات وذلك عن طريق وضع العديد من الاتفاقيات الدولية والقوانين للتصدي لهذه الظواهر الإجرامية.

وبناءا على ما تقدم سوف نتطرق من خلال هذا الفصل الى انعكاسات الهجمات السيبرانية على السلم والأمن الدوليين ضمن (المبحث الاول)، ثم الجهود الدولية لمواجهة الهجمات السيبرانية (المبحث الثاني)

المبحث الأول: انعكاسات الهجمات السيبرانية على السلم والأمن الدوليين

شهد العقد الأخير من القرن الماضي تطورات معتبرة على مستوي تكنولوجيا المعلومات والاتصالات وشبكات الانترنيت على اختلاف استعمالاتها، صاحب ذلك تطور ملحوظ في نشاطات الجريمة الالكترونية والتهديدات الأمنية التي تستهدف المجال السيبراني ضمن القضاء الإلكتروني، وبعد أن كان تهديد السلم والأمن الدوليين يقتصر على العدوان الفعلي فقد تطور اليوم ليشمل تهديدات وتحديات جديدة أكتر وأشد تعقيدا تعرف بالهجمات السيبرانية.

سنتطرق إلى دراسة انعكاسات الهجمات السيبرانية على السلم والأمن الدوليين من خلال التطرق إلى تأثير الهجمات السيبرانية على الأمن بوجه عام (المطلب الأول)، ثم تأثير الهجمات السيبرانية على سيادة الدول والعلاقات الدولية (المطلب الثاني).

المطلب الأول: تأثير الهجمات السيبرانية على الأمن

ليس للهجمات السيبرانية حدود فبإمكانها التسبب في العديد من الآثار الخاصة كانفجار في مخازن الوقود أو تغيير مسار الرحلات أو تعطيل أنظمة الطاقة وقطع الكهرباء من مدن بأكملها وتعد الهجمات السيبرانية التي وقعت في السنوات الأخيرة تهديدا حقيقيا للسلم والأمن الدوليين وبمستوي لا يقل جسامة عن أخطر التهديدات المعروفة دوليا مثل الخلافات السياسية والنزاعات المسلحة وغيرها.

وسنحاول الخوض في هذه المسألة من خلال دراسة تداعيات الهجوم السيبراني على الأمن العالمي والأمن القومي (الفرع الأول)، ثم تداعيات الهجوم السيبراني على الأمن الإنساني وحقوق الإنسان (الفرع الثاني).

الفرع الأول: تداعيات الهجوم السيبراني على الأمن العالمي والأمن القومي

لقد تطور مفهوم الأمن فلم يعد مقصورا فقط على أمن الدولة القومية، وإنما ظهر مفهوم الأمن العالمي ليضم الدول وغيرها من الفواعل على الساحة الدولة، ومن الواضح أن هذا التطور في مفهوم الأمن قد اقترن بالتطور في مفهوم القوة والفواعل والقضايا والآليات الدولية، وذلك في إطار التطور العلمي خلال النصف الثاني من القرن العشرين، ولقد انعكست هذه التغيرات في مستوى الحركة على الجانب التنظيري في العلاقات الدولية،

أولا: تداعيات الهجوم السيبراني على الأمن العالمي

تكمن خطورة الهجمات السيبرانية على الأمن العالمي بكونها وسيلة قتالية قادرة على التسلل إلى أنظمة الكمبيوتر معدة لحماية سير عمل إنشاءات حيوية لتنظيمها كمحطات توليد الطاقة النووية أو

السدود أو وسائل نقل الطائرات بهدف تطويعها والسيطرة عليها ولتدمير ذاتها بذاتها من خلال تزويدها بمعلومات خاطئة لأجهزة التحكم والحماية الالكترونية [1].

لقد عرف الأمن الدولي في تجربة عصبة الأمم وثم عاود الظهور في ميثاق الأمم المتحدة ولقد تحول الأمن الوطني إلى مفهوم الأمن الجماعي في التسعينيات بالأخص مع بداية القرن الواحد والعشرون مع تجذر لعملية العولمة واستثمار الفجوة الكبيرة من القوة العسكرية التي تفصلها عن بقية دول العالم لكي تطبق أجندتها إلى عملية أمريكية سياسية وأمنية للعالم وهنا يقفز الفهم الأمريكي الأمن العالمي بقوة ويفرض نفسه على الجميع [2].

والهجمات الالكترونية تتمثل في سرقة أو تغيير معلومات أو تدمير النظام أو إيقاف عمل الشبكات وباستخدام الشفرات الخبيثة أو تعطيل الوظائف أو إيقاف عمل الشبكات وباستخدام هذه الوسائل يمكن للقائمين بالهجوم الإضرار بالمؤسسات الحكومية والمستشفيات وغيرة من الكيانات التي تعتمد بشكل كبير على أجهزة الحاسب الآلي في القيام بأعمالها الرئيسة وهو ما يترتب عليه تعطيل المحركات الرئيسة لاقتصاد الدولة والأضرار بمواطنيها وتهديد أمنها القومي بشكل عام ولذلك تكون التداعيات الدولية لتلك الهجمات خطيرة وواسعة النطاق وتتخطي حير الدولة لتؤثر في الأمن العالمي ككل[3].

ولقد أدى التزايد في درجة تعقيد وتشابك أنظمة التحتية في عديد من الدول وتزايد في اعتمادها على أجهزة الحاسب الآلي إلى زيادات قابلية تعرضها للهجمات الالكترونية واتساع نطاق التأثيرات المحتملة المرتبة علي هذه الهجمات فعلى سبيل المثال إذا أسفرت الهجمات السيبرانية أو الالكترونية علي توقيف الطاقة الكهربائية أو الاتصالات قد يودي ذلك إلي تأثيرات متتالية علي البنوك والمؤسسات الحكومية [4]، يجري في الوقت الراهن سباق بين الدون الدول الغنية لتطوير برمجيات من شأنها امتلاك قدرات هجومية وأخرى دفاعية قادرة علي التصدي للهجمات السيبرانية وعلى سبيل المثال ما بذلته الولايات المتحدة الأمريكية من جهود كبيرة لتطوير أنظمة الدفاع يحتوي لتحمي شبكتها من القراصنة والخدمات الإلكترونية المدمرة من جانب الحكومات الأجنبية [5].

---

(1)– اسمهان بعيري، المرجع السابق، ص51.

(2)– مصطفي علوي، مفاهيم الأسس العلمية للمعرف –الأمن الإقليمي بين الأمن الوطني والأمن العالمي، المركز الدولي للدراسات المستقبلية و الاستراتيجية، القاهرة، العدد السنة الأولى، ابريل 2005، ص26.

(3)– نوران شقيق، المرجع السابق، ص56.

(4)– المرجع نفسه، ص56–57.

(5)– اسمهان بعيري، المرجع السابق ،51.

ثانيا: تداعيات الهجوم السيبراني على الأمن القومي

سبب الحروب السيبرانية جملة من المخاطر والتداعيات على تفاعلات سياسة الدولية يمكن طرح أبرزها على النحو الآتي :

1- تصاعد المخاطر السيبرانية:

خاصة مع قابلية المنشآت الحيوية (مدنية وعسكرية) في الدول للهجوم الأمر الذي يؤثر في وظائف تلك المنشآت وبالتالي فان التحكم في تنفيذ هذا الهجوم بعد أداة سيطرة استراتيجية[1].

2- تعزيز القوة وانتشارها:

عمل القضاء السيبراني على إعادة تشكيل قوة الأفراد المؤثرة، وأدى إلى عملية انتشار القوة بين الفاعلين[2]، حيث تجري الولايات المتحدة الأمريكية سنويا محاكاة التعرض لحرب الكترونية فيما يطلق عليه عاصفة الحواسيب" cyber Storm" كما تتبع روسيا أساليب مختلفة كالتجسس السيبراني للاستخبارات لخدع التظليل تنظيم الاتصالات وأنظمة دعم الملاحة لضغوط النفسية، الدعاية تجاه خصومها كأكرانيا وغيرها من الدول، ما يجعل الخطوط الفاصلة بين الحرب والسلام متآكلة في الفضاء السيبراني؛

3- عسكرة الفضاء السيبراني:

برز في هذا الإطار عدة اتجاهات مثل التطور في مجال سياسات الدفاع والأمن السيبراني، دفاعية القدرات في سباق التسلح السيبراني، وتبقي سياسيات دفاعية سيبرانية لدي الأجهزة المعنية بالدفاع والأمن في الدول وتزايد الاستثمار في مجال تطوير أدوات الحرب السيبرانية داخل الجيوش الحديثة [3]، فقد كان لازما على الدول التحول الشامل نحو دمج الفضاء السيبراني في إطار العقائد العسكرية للجيوش باعتباره مجالا للتفاعل الدفاعي والهجومي يشمل بالحماية ويخضع لسيادة الدولة بأهمية هذا الفضاء بالنسبة لحلف الناتو مثلا تكمن في عدة عناصر وهي: حماية البيانات العسكرية، من تلاعب حماية القادة عسكريين من التجسس، حماية البنية التحتية من التدمير، ودعم العمليات الاستخباراتية، دعم وحدات الحرب التقليدية، تحقق الردع السيبراني و تحقيق الأمن السيبراني للدول الأعضاء ؛

---

[1]- لامية طالة، التهديدات والجرائم السيبرانية: تأثيرها على الأمن القومي لدول واستراتيجيات مكافحتها، مجلة معالم الدراسات القانونية والسياسية، المجلد 04، العدد 02، 2000، ص 50.

[2]-لامية طالة، المرجع السابق، ص 59.

[3]- وداد بوطلاعة و منال بوكور، صراع الفضاء السيبراني و تأثيره على السلم و الامن والاجتماعية، المجلد 07، العدد 04، ديسمبر 2022، ص818.

4- إدماج الفضاء السيبراني ضمن الأمن القومي للدول:

ويتم ذلك عبر تحديث الجيوش، وتشكيل وحدات متخصصة في الحروب السيبرانية، وإقامة هيئات وطنية للأمن والدفاع السيبراني، والقيام بالتدريب، وإجراء المناورات لتعزيز الدفاعات السيبرانية [1].

ومثال على ذلك وفي ظل هذا السباق السيبراني الدولي المفتوح، وفي إطار التحول الرقمي المتزايد في دولة الإمارات، وما واكبه من تنامي التهديدات الالكترونية، بصورها وأشكالها العديدة والمتنوعة، على الدولة والمجتمع، وبنيتها التحتية الحيوية، اتخذت الحكومة الإماراتية من الإجراءات والتدابير والمبادرات لتعزيز أمنها السيبراني وتأمين فضائها الإلكتروني، ومن أهم هذه الجهود شبكة إلكترونية اتحادية (FedNet) تسمح بالتوصيل البيئي، وتبادل البيانات بين جميع الجهات المحلية والاتحادية في الدولة، وتعزيز قنوات التواصل فيها بينها باستخدام بنية تكنولوجية موجودة وآمنة، كما أسست مركز الاستجابة الوطني لطوارئ الحاسب الآلي (ae CERT) الذي يهدف إلى تحسين معايير أمن المعلومات وممارساتها وحماية البنى التحتية لقطاع الاتصالات وتقنية المعلومات من مخاطر شبكة الانترنت واختراقاتها[2].

واتخذت مبادرات عدة في السلامة الإلكترونية، مثل مبادرة سالم التوعوية، وسفراء الإمارات للأمن الإلكتروني، ومبادرة الابتزاز الإلكتروني، ومبادرة " النبض السيبراني"، " cyber pulse" وتأتي المبادرة الأخيرة لمواكبة الجهود التي باشرتها دولة الإمارات في مجال السلامة السيبرانية، وتهدف إلى ضمان تحول رقمي أمني واستخدام منجزات التكنولوجيا الرقمية في بيئة أقل تهديدا، ورفع مستوى الوعي بالممارسات الجيدة للأمن السيبراني، وتحفيز الاهتمام العام بالتعريف على الأمان والأمن السيبراني عبر مختلف الفئات العمرية في دولة الإمارات[3].

5- الاستعداد لحروب المستقبل:

تبني العديد من الدول استراتيجية حرب المعلومات باعتبارها حربا للمستقبل، وترى الدول الكبرى أن من يحدد مثير تلك المعركة المستقبلية ليس من يملك القوة فقط، وإنما القادر على القوة، والتشويش على المعلومة[4].

ولقد دفع التطور في مجال الفضاء الالكتروني خاصة في نهاية القرن العشرين وبداية القرن الحادي والعشرين، الدول على تعزيز دفاعاتها ضد خطر التعرض للهجمات الالكترونية، ولكنها اتجهت إلى

---

[1]- لامية طالة، المرجع السابق، ص59.

[2]- محمد الكويتي، الامن السيبراني في 2023، تحولات وتحديات عصر الذكاء الاصطناعي، تريندز للبحوث والاستثمارات، 2023، ص 02.

[3]- محمد الكويتي، المرجع نفسه، ص 02.

[4]- لامية طالة، المرجع السابق، ص 59.

التحول من اتخاذ إجراءات وقائية ذات في طياته مخاطر عسكرية الفضاء الالكتروني، خاصة وان القدرة على السيطرة على مثل هدا النوع من الأسلحة ضئيلة بالمقارنة مع الأسلحة التقليدية، وهناك مسالة صعوبة تحديد الأسلحة التي يمتلكها الآخرون ومن ثم يتعذر على المجتمع الدولي القدرة على التدخل لاحتواء التقدم في مثل هكذا أسلحة[1].

مما سبق يمكن القول أن مفهوم الأمن القومي قد طرأ. عليه الكثير من التعديل والتغير على مستوي التهديدات، الفاعلين القطاعات، حيث خلق فضاء جديد للتفاعل، هو الفضاء السيبراني بدا واضحا أن الدولة تتجه نحو عسكرة الفضاء السيبراني، مما نتج عنه ظهور تهديدات جديدة تتزايد في الحجم والشدة، وتشكل تهديدا خطيرا للأمن القومي فكلما زادت التشابك، زادت التهديدات السيبرانية على الأمن القومي[2].

الفرع الثاني: تداعيات الهجوم السيبراني على الأمن الإنساني وحقوق الإنسان

إن أثر الهجمات على حقوق الإنسان يكون له تأثيرين أحدهما مباشر والثاني يكون غير مباشر وقبل التطرق إلى ذلك وجب علينا تعريف الأمن الوطني والأمن الإنساني ومهددات الأمن الإنساني.

أولا: الآثار المباشرة للهجمات السيبرانية على الأمن الإنساني

يعرف الأمن الوطني بمدى الاستقرار الاجتماعي والسياسي والاقتصادي وبمقدرة الدولة على الحفاظ على الأمن الداخلي وحماية حدود البلاد واستقلالها، وتحقيق التنمية وإرساء دولة المؤسسات والقانون، أما الأمن الإنساني وهو أمن الإنسان من الخوف والجوع وحفظ كرامته الإنسانية من خلال حياة آمنة مستقرة ومستمرة، أما مهددات الأمن الإنساني فهو تغيير في عمل مجموعة المتغيرات والعوامل الإنسانية وإدارتها عن مسارها الصحيح، وتؤدي إلى إضعاف النظام الأمني المعمول به[3].

إن الفضاء السيبراني أصبح ساحة جديدة يستخدم في شتي مظاهر الحياة في الدولة السياسية، الأمنية، الاقتصادية والتجارية، كما أن البنية التحتية الالكترونية المدنية غالبا ما ترتبط بنظيرتها العسكرية عن طريق شبكة الانترنيت[4].

كما تواجه منظمات حقوق الإنسان والمجتمع المدني بالإضافة إلى نشطاء الحقوق مجموعة متزايدة من الهجمات الالكترونية من هجمات للتصعيد الالكتروني وهجمات لرفض الخدمة وذلك بهدف ممارسة

---

[1]– علي عبد الرحيم العبودي، المرجع السابق، ص 96.

[2]– لامية طالة، المرجع السابق، ص 59–60.

[3]–حسن عبد الله الدعجة، مهددات الامن الإنساني، مجلة الجزائرية للأمن الإنساني، العدد الرابع، جويلية 2017، السعودية، ص130.

[4]– رمضان محمد حمدان، الإرهاب الدولي وتداعياته على الامن والسلم العالمي دراسة تحليلية من منظور اجتماعي، مجلة ابحاث التربية الأساسية، جامعة الموصل، العراق، المجلد 11، 2011، ص56.

انتقام منهم بسبب أعمالهم الحقوقية أو إجبارهم علي السكوت عن انتهاكات الحقوقية المختلفة، وهذا يضر جملة من الحقوق المدنية والسياسية المنصوص عليها في العهد الدولي الخاص بالحقوق السياسية والمدنية والتي من بينها الحق في تكوين المجتمعات المنصوص عليه في المادة (22) من العهد سابق الذكر، هذا بالإضافة إلى الاعتداء على الحق في خصوصية حرية الرأي والتعبير[1].

ومن ثمة فاستهداف نظم المواصلات وشبكات الكهرباء والسدود والمستشفيات الكيميائية أو النووية من أهم الآثار السلبية التي تديرها الهجمات السيبرانية، وبالتالي فإن احتمال اختراق المنظومة الالكترونية للمفاعلات النووية قد يتسبب في كوارث مروعة بحيث يصعب التحكم في أثارها البشرية[2].

كما يلاحظ إن التهديدات الالكترونية لا تستهدف الإضرار بالبشر بصورة مباشرة، وإنما التأثير على الفضاء الالكتروني الذي بات بشكل مكونا رئيسيا في صار حياتهم، فهي تؤثر على الأنظمة والشبكات والأجهزة التي يستخدمها الأفراد وتعتمد عليها الدول، ومن ثم تؤثر على الأسلوب الحياة ذاتها بشكل يهدد امن الدول ككل، ولكنها لا توجه ضد بشر كما هو الحال في الأسلحة التقليدية التي قد تستخدم للقتل المباشر [3].

وفي هذا الصدد قد عبرت اللجنة الدولية عن قلقها بشأن الحرب السيبرانية بسبب ضعف الشبكات الالكترونية والتكلفة الإنسانية المحتملة من جراء الهجمات السيبرانية فقد تتعرض الحواسيب أو الشبكات التابعة لدولة ما هجوم أو اختراق أو إعاقة تدل يجعل هذا الأمر المدنيين عرضة لخطر الحرمان من الاحتياطات الأساسية، مثل مياه الشرب والرعاية الطبية والكهرباء وإذا تعطلت أنظمة تحديد المواقع GPS عن العمل قد تحدث إصابات في صفوف المدنيين من خلاف تعطيل عمليات إقلاع مروحيات الإنقاذ على سبيل المثال[4].

ثانيا: الآثار غير مباشرة للهجمات السيبرانية على الأمن الإنساني

إن التأثير غير المباشر للهجمات السيبرانية يمكن ملامسته من خلال الإجراءات الوقائية التي تتخذها الحكومات والأجهزة الأمنية من خلال المراقبة، وأيضا من خلال إجراءات إنفاذ القانون فبالنسبة

---

(1)– العربية " التهديدات السيبرانية واثرها علي حماية البنى التحتية والخدمات الحيوية ، ماعت السلام والتنمية وحقوق الانسان، الموقع الإلكتروني .maatpeace; https اخر زيارة (5.05.2004 الساعة16:00).

(2)– رمضان محمد حمدان، المرجع السابق، ص57–58.

(3)– نوران شفيق، المرجع السابق، ص20–40.

(4)– إسمان بعيري، المرجع السابق، ص52.

لهذه الأخيرة، فتجري المراقبة تحث هذه الذريعة على نطاق واسع من خلال تقنيات ترشيح الانترنيت[1] مثلا وكذلك القدرة على الاتصال والحصول على أسماء المستخدمين وغير ذلك من الإجراءات ،مما يزيد من احتمال تعرض الأفراد لانتهاك حقوق الإنسان المكفولة لهم [2].

ومن جهة أخرى لا تقف تأثير هذه الإجراءات على المستوى الوطني بل من الممكن أن تتخذ هذه الإجراءات أثارا خارج نطاق الأصابع يسمح بكشف المجرمين والتعرف عليهم، وفي نفس الوقت يسمح بالاطلاع على جميع جوانب الحياة الخاصة [3].

وتبقى الإجراءات والقوانين التي تفرض القيود على حقوق الإنسان محكومة بعدة عناصر أساسية وهي الضرورة والتناسب فقد قضت المحكمة الأوروبية لحقوق الإنسان بان صلاحية المراقبة السرية للموظفين يوازي ما تفعله الدولة البوليسية تعتبر مقبولة بموجب الاتفاقية الأوروبية لحقوق الإنسان والحريات الأساسية بقدر الضرورة القصوى فقط وبقصد حماية المؤسسات الديمقراطية[4].

المطلب الثاني: تأثير الهجمات السيبرانية على سيادة الدول وعلاقاتها الخارجية

توجه ثلاث حقائق مرتبطة بعناصر الدولة لا يمكن التقاضي عنها، أول هذه الحقائق أن الفضاء السيبراني مفتوح على كل دول العالم، ثانيا أن أي تهديد يصدر من خلاله من الممكن أن يعبر الحدود بلا مراجع والمستخدمين فيه مختلفين فلا توجد هوية تعريفية تحدد مواطنة بل أن عدم الكشف عن الهوية حق للمستخدم، وثالثا الفضاء السيبراني غير مملوك لأحد بالرغم من عالمية النشاط، وعملية فقد أدت هذه الحقائق إلى تعاظم التهديد المحتمل على الدول وسيادتها وعلاقاتها الخارجية خصوصا أن الفضاء السيبراني يحمل عدة أوجه من التهديدات قد تشكل خرقا لسيادة الدول وسلامة إقليمها[5]، وعلى ضوء ما نقدم ذكره سنتطرق في هذا المطلب إلى اثر الهجمات السيبرانية على سيادة الدول (الفرع الأول)، ثم إلى اثر الهجمات السيبرانية على العلاقات الدولية (الفرع الثاني).

---

(1)– ترشيح الانترنت: يعني الرصد الالي او اليدوي لما تحتويه الانترنت من مواقع شبكية ومدونات ومصادر اعلامية وبريد الكتروني ،للاطلاع اكثر انظر: زهراء عماد محمد كلنتر، المرجع السابق، ص188.

(2)– زهراء عماد محمد كلنتر، المرجع نفسه، ص 188.

(3)– المرجع نفسه، ص190.

(4)– اسمهان بعيري، المرجع السابق، ص53.

(5)– إبراهيم مسلم نبراس، "الجرائم السيبرانية وأثرها على الأمن السيبراني"، مجلة القادسية للقانون و العلوم السياسية، كلية الحقوق، جامعة بغداد، العراق، العدد 01، المجلد 12، 2021، ص381.

الفرع الأول: أثر الهجمات السيبرانية على سيادة الدول

لقد سعت الدولة على مر التاريخ إلى محاولة إثبات سيادتها أما في مقابل مواطنيها محليا من خلال ممارستها للسلطة على عموم الشعب من دون أن تكون هناك أي هيئة أو قوة أو سلطة أخرى موازية لها تنازعها سلطاتها، مع ضرورة الإقرار بالاختلاف في نمط ممارسة السلطة بين الدولة وأخرى، أو في مقابل دون أخرى من خلال تأكيدها على حدودها الإقليمية السيادية المعلومة وغير القابلة للتنازل، ولأجل ذلك كان تعريف الفقه السياسي والقانون لا دولة السيدة باعتبارها دولة كاملة الصلاحية في ممارسة سلطاتها ولا تعلوها أي سلطة، وتكون قراراتها نافذة على إقليمها، وأمام التغيرات التي شهدها الواقع الدولي، ومن صمنها التغير في أنماط التهديد وصولا إلى التهديدات السيبرانية –الافتراضية–، والتي كان لها تداعيات عميقة على العديد من المفاهيم المسلم بقدرتها علي التحليل في مرحلة من المراحل، ولقد ارتبط مفهوم السيادة الرقمية بالتغيرات الثورية التي أجرتها عصر التكنولوجيا الرقمية على واقع المجتمعات والدول والسيادة الإقليمية[1].

ومن هذا المنطلق يمكن التعرض من خلال هذا الفرع إلى نوعين من التهديدات للسيادة السيبرانية وهما :

أولا: التهديدات الداخلية

أدى التطور التكنولوجي، كانتشار الانترنيت والحواسيب، والأجهزة النقالة، وتوافر الحزمة العريضة الانترنيت غبر الأجهزة النقالة وتدني كلفتها، إلى ارتفاع إعداد مستخدمي الانترنيت وتزايد اعتماد الدول على هذه التكنولوجيات في الاقتصادية والاجتماعية، إلا أن الانفتاح الذي يميز شبكة الانترنيت والفضاء السيبراني عموما جعلها عرضة للتعديات والأنشطة الغير سليمة، فصار مستخدمو الفضاء السيبراني من الدول وعبر الدول عرضة للانتهاكات والتهديد لمنظوماتها الالكترونية إذ لا يمكن لأي حكومة، أو إدارة، سواء كانت من العالم الثالث، أم في الدول الأكثر تقدما أن تنأى بنفسها عن الهم الذي يمثل اختراق الشبكات وتهديد أمنها ومصالحها[2].

فقد كانت الدولة بحلول منتصف القرن العشرين كانت الدولة تسيطر على إقليمها بشكل مباشر، إذ أنها كانت تحدد السلطة في استخدامها الشرعي للقوة غير أن الفضاء السيبراني غير من أسلوب وتأثير ارتكاب الجريمة إذ أنها أخذت طابعا غير مرئيا ومسرح الجريمة إختلف أيضا، كما أصبح يقع على الدول واجب استقلال وسيادة الدول الأخرى ويمنع الاعتداء عليها، ضمن المبادئ الراسخة في القانون الدولي

---

[1]– عبد الغاني شرقي، التهديدات السيبرانية العالمية، المجلد 07، العدد 02، 2023، ص278.

[2]– م م علي عبد الرحيم العبودي، هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين، جامعة بغداد–كلية العلوم السياسية، ص 107.

فان الدولة ملزمة بمنح استخدام أرضيها في أعمال إجرامية لتهدد سلامة دولة أخرى أو شعبها، وهذا المبدأ انعكس في العديد من الإعلانات والمبادئ والآراء[1].

وكذلك تداعيات الإرهاب الدولي الاعتداء على الدول والتدخل في شؤونها الداخلية والخارجية بما أن القوانين الدولية أقرت حق الدول في استقلالها وسيادتها الداخلية والخارجية ومنعت الدول من التدخل في شؤون بعضها البعض ولكن ليس إلا حبر على ورق فالقوي الكبرى والعظمي لا يحلوها بين الحين والأخر، إلا أن تتدخل في شؤون الدول الضعيفة والصغرى تحت ذرائع ومسميات مختلفة خصوصا ما يتعلق منها بالحفاظ على الأمن والسلم الدوليين والحفاظ على حقوق الإنسان ونشر الديمقراطية والتعددية السياسية والقضاء على الأنظمة الشريرة والفاسدة ....الخ [2].

ولقد أكد العرف الدولي على قاعدين أساسيتين: الأولى تتمثل بواجب الدولة الإيجابي لمنع الجهات الفاعلة غير الحكومية داخل حدودها من ارتكاب هجمات ضد دولة أخرى والثانية التسامح بشأن هذه الهجمات[3].

وكذلك يمكن القول أن تعزيز الهجمات المطبقة داخل إقليم الدولة ذات أثر مباشر على الأمن القومي للدولة نفسها كما تؤثر بطريقة غير مباشرة على مواطنيها وعلى الأشخاص داخل الحدود الإقليمية.

ثانيا: التهديدات الخارجية

أغلب التهديدات التي تستهدف الدول في الأصل خارجية، يختلف مداها وأثارها ودوافعها وتتوقف على المهاجمين وأدواتهم، وقد أصبح الأمر متخلفا بعد ظهور الفضاء السيبراني، فالشبكة العنكبوتية ليس لها مقر في دولة معينة، ولا تخضع للرقابة ولا لسيطرة دولة ما عليها، ولا يوجد قانونا جنائي موحد نافذ فيها[4].

ويعتبر الكمبيوتر والانترنيت أحد أهم مصادر التهديد التي يوفرها الفضاء السيبراني، وذلك لقدراتها الإنسانية في اختراق الشبكات الويب بشكل يسمح بالاطلاع على أسرار المؤسسات والدوائر السيادية في الدولة المراد اختراقها، ويمكن كذلك تعطيلها، ما يجعل الدولة المستهدفة في حرج تقني وفي فراغ أمني[5].

---

(1)– إبراهيم مسلم نبراس، المرجع السابق، ص 383.

(2)– حمدان رمضان محمد، المرجع السابق، ص285.

(3)– إبراهيم مسلم نبراس، المرجع السابق، ص383.

(4)– اسمهان بعيري، المرجع السابق، ص56.

(5)– عبد الكريم بإسماعيل، تأثير الفضاء الافتراضي على الأمن القومي مجلة البحوث والدراسات، المجلد19، العدد 01، 2022، ص 147.

بالتالي أصبح موضوع تامين الشبكات العنكبوتية أمرا غاية في الأهمية ، من أجل حماية مؤسسات وسيادة الدولة، حيث أضحى ممكنا جدا إرسال فيروسات تقوم بتحطيم الشبكة الأمنية لدولة معينة، وليسهل بذلك احتلالها أو الحصول علب معلومات سرية وسيادية منها، من أجل الهجوم على بعض الدول وابتزازها وتدمير مؤسساتها يتم تطوير عدة برامج خبيثة وفيروسات يتم إرسالها عن طريق الانترنيت وشبكات الكمبيوتر[1].

ويقع على الدولة واجب مؤكد للحفاظ على سيادتها اتجاه التهديدات السيبرانية، وهو منع التهديدات من المساس بإقليمها وبإقليم دولة أخرى، إذ يجب أن تلتزم الدولة بمنع الهجمات والجرائم السيبرانية من خلال العمل على تشريع نصوص جزائية صارمة، وإجراءات تحقيقها ملائمة في مجال إنفاذ القانون وملاحقة المتهمين والتعاون مع الدولة الضحية للجرائم أو الهجمات، وهذا الالتزام ينبع من مصادر ثلاثة للقانون الدولي العرفي، وهي الاتفاقيات الدولية، والعرف الدولي ومبادئ القانون العامة[2].

الفرع الثاني: أثر الهجمات السيبرانية على العلاقات الدولية

كانت ثورة المعلومات و ظهور الانترنت إعلانا ببروز العصر الإلكتروني، وخلق بيئة جديدة هي الفضاء الإلكتروني (cyber space) الذي يمثل بعدا خامسا للحرب والإرهاب إلى جانب الأبعاد الأربعة مع بروز شكل جديد من القوة وهي القوة الالكترونية (Cabet power) التي توزعت وانتشرت بين عدد أكبر من الفاعلين على المستوى الدولي والمحلي، ما جعل الفضاء الإلكتروني مجالا جديدا للصراع بين الدول[3].

كما كشف استخدام الفضاء السيبراني عن حال التعارض الحقيقي أو المتخيل للاحتياجات والقيم والمصالح بين العديد من الجهات سواء كانت دولة أو أفراد أو جماعات أو شركات، مما ساعد على بلورة أساليب الصراع الدولي ذات الطابع الفقهي والتجاري والاقتصادي والعسكري إلى جانب ظهور طرائق بديلة عن الحرب المباشرة بين الدول أو بين الخصوم عبر شبكات الاتصال والمعلومات، وبالتالي أصبح الفضاء السيبراني ساحة جديدة للصراع بشكله، التقليدي ولكنه ذو طابع سيبراني بعكس النزاعات التي تخوضها الدول أو الفاعلين من عبر الدول على خلفيات دينية أو عرقية أو إيديولوجية أو اقتصادية أو سياسية، ويتمدد الصراع السيبراني بداخل شبكات الاتصال والمعلومات متجاوزا الحدود التقليدية وسيادة الدول[4].

---

[1]– عبد الكريم إسماعيل، المرجع السابق، ص 147-148.

[2]– إبراهيم مسلم نبراس، المرجع السابق، ص 383.

[3]– محمود علي عبد الرحمان، "الفضاء الالكتروني وأثره على مفاهيم القوة والأمن والصراع في العلاقات الدولية"، مجلة كلية السياسية والاقتصاد، جامعة بني سويف، المجلد 16، العدد 15، 2022 ، ص427.

[4]– لامية طالة، المرجع السابق، ص57.

كما أن التطورات التكنولوجية والرقمية أحد إفرازات العولمة التي تم الاستعانة بها في الصراعات الدولية، من خلال التوظيف الفعال لمختلف الأسلحة المتطورة[1].

نماذج عن أكبر تهديدات الهجمات السيبرانية

أولا: تنظيم "داعش"

لقد مثل تنظيم "داعش" أكبر تهديد لسلامة شبكة الأنترنت العالمية، وبالتالي فإن أهم مظاهر هذه التهديدات السيبرانية للأمن الدولي والأمن القومي للدول تتمثل:

- استخدام نظم المعلومات في الدعاية والتجنيد والتمويل وجمع المعلومات.
- تنسيق الهجمات الإرهابية وحشد المتعاطفين ونشر أفكار التطرق في وسط، ففي هذا الإطار حدد "أبو بكر ناجي" في كتابه "إدارة التوحش" أساليب توظيف الاعلام الجهادي لتنظيم داعش من خلال:
- فئة الشعوب: وذلك بالعمل على دمج تكبر عدد منهم في صفوف الجهاد ودعمها.
- جنود العدو: بالتركيز على الفئات الهشة والموظفين ذوي الدخل الضعيف للزج بهم في صفوف الجهاد[2].

ثانيا: الصراع الالكتروني ذو الطبيعة الناعمة لموقع ويكيليكس

حيث قام موقع ويكيليكس والذي يعرف بـ " صراع الكتروني ذو طبيعة ناعمة" وذلك ما أدى إلى صراع دولي الكتروني من أجل الحصول على معلومات والتأثير في الأفكار وشحن الأفراد إعلاميا من خلال تسريب المعلومات بما يوثر على طبيعة العلاقات الدولية، ويعد من أثار الهجمات السيبرانية التأثير على مستوي العلاقات الدبلوماسية من خلال جمع المعلومات والتنصت والتجسس وتسهيل النشاطات السرية في العلاقات الدولية، مثل عمليات الاغتيال التي مست الممثلين الدبلوماسيين للدول[3].

ويتضح مما سبق وتقدم أن على المجتمع الدولي بذل المزيد من الجهود لمكافحة الجرائم السيبرانية بما لها من أثار كبيرة على المجتمع الدولي ككل لما لهذه الجرائم من أثار والتهديدات والتداعيات التي تمس الأمن والسلم الدوليين.

---

[1]– سمير باي، التهديدات الأمنية السيبرانية: دراسة في انعكاسات الحرب الالكترونية على الأمن القومي للدول واستراتيجيات المقاومة، مجلة الرسالة للدراسات والبحوث الإنسانية، المجلد 08، العدد 02، 2023، ص196.

[2]– المرجع نفسه، ص 196–197.

[3]– اسمهان بعيري، المرجع السابق، ص57.

المبحث الثاني: الجهود الدولية لمواجهة الهجمات السيبرانية

إن مواجهة الهجمات السيبرانية تتطلب اتخاذ جهود و تدابير صارمة في كافة الجوانب و يمكن تقسيم أساليب مواجهة التهديدات السيبرانية العابرة للحدود و إلى أسلوب يركز على التقنيات الرقمية من برامج مضادة للفيروسات أو برامج جدران النار أو برامج التشفير، وتستعمل هذه التقنيات من طرف الدول من أجل تقوية قوتها السيبرانية و تحصين قضائها السيبراني، أما الأسلوب الثاني فيركز على المواجهة التشريعية سواء على المستوي الدولي أو الإقليمي أو الوطني بمعنى المواجهة الإجرائية العملية.

وسنحاول التطرق إلى ذلك من خلال الجهود العالمية في مواجهة الهجمات السيبرانية (المطلب الأول والجهود الإقليمية في مواجهة الهجمات السيبرانية (المطلب الثاني).

المطلب الأول: جهود العالمية في مواجهة الهجمات السيبرانية

على الرغم من تزايد الهجمات السيبرانية و الخطورة الناشئة عنها، إلا أن المجتمع الدولي سيسعى إلى وضع إطار قانوني ينظم هذه التهديدات وذلك من خلال النص على أطر قانونية مشتركة واتفاقات عامة خاصة بالجرائم السيبرانية، وسنتناول ذلك من خلال جهود المنظمات العامة في مواجهة الهجمات السيبرانية (الفرع الأول)، والجهود الاقليمية لمواجهة الهجمات السيبرانية (الفرع الثاني).

الفرع الاول: جهود المنظمات العامة في مواجهة الهجمات السيبرانية

سنحاول تسليط الضوء على الجهود الدولية الرامية بالأساس الى تنظيم موضوع الهجمات السيبرانية، وفقا لما استقر في القانون الدولي التعاهدي أو العرفي وذلك من خلال التركيز على جهود منظمة الأمم المتحدة في مواجهة الهجمات السيبرانية (أولا)، ثم ثانيا جهود المنظمات الاخرى لمواجهة الجريمة السيبرانية (ثانيا).

أولا: جهود منظمة الأمم المتحدة في مواجهة الهجمات السيبرانية

لقد سعت الأمم متحدة إلى تأمين سلامة استخدام التكنولوجيا ، وشبكات المعلوماتية بشكل عام و تشارك كلا من الجمعية العامة ومجلس الأمن ومكتب مكافحة الإرهاب التابع للأمم المتحدة[1] في مختلف المفاوضات لاتحاد توافق في الآراء[2]، من أجل وضع معايير توفر الحماية لشبكات الانترنت، وسوف نبين ذلك فيما يلي:

---

[1]– الأمم المتحدة تعتبر المنبر العالمي لترجمة هذه الجهود و استثمارها الأمثل في هذه المواجهة لما تتمتع بهذه الاخيرة من مصداقية في مجال تعزيز التعاون الدولي لتحقيق مقاصدها في ضمان الأمن و السلم الدوليين في مواجهة مختلف التهديدات العالمية ضمها خطر الإرهاب الدولي، أنظر خالد حسن أحمد لطفي، المرجع السابق، ص166.

[2]– نور أمير الموصلي، المرجع السابق، ص21.

1- الجمعية العامة:

توصلت الجمعية العام للأمم المتحدة نتيجة جهودها على المسار القانوني والتنفيذي إلى اعتماد استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب عام[1] 2006.

فلقد قامت الجمعية العامة للأمم المتحدة بإصدار بعض التوصيات والقرارات ذات الصلة بالأمن الإلكتروني، كان لها دور كبير في دفع الدول الأعضاء لإدراك أهميته وما يرتبط به من تحديات تتطلب جهودا تعاونية مشتركة لمواجهتها. كما ظهر الاهتمام بالبعد الإلكتروني في أغلب الأجهزة التابعة للأمم المتحدة وأبرزها المجلس الاقتصادي والاجتماعي، وجهاز مكافحة الجرائم[2].

و من أمثلة قرارات الجمعية العامة للأمم المتحدة:

- القرارين 55/63، 56/121 اللذان يضعان الإطار القانوني بشأن" مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية."
- القرار 57/239 المتعلق بإنشاء ثقافة أمنية عالمية للقضاء الحاسوبي.
- القرار 58/199 المتعلق بإرساء ثقافة عالمية لأمن القضاء الحاسوبي وحماية الهياكل الاساسية الحيوية للمعلومات.
- القرار 73/187 المتعلق بمكافحة استخدام تكنولوجيا المعلومات والاتصالات لأغراض الجرمية.
- القرار 74/174 المتعلق بتعزيز المساعدة التقنية و بناء القدرات لتدعيم التدابير الوطنية والتعاون الدولي في مجال مكافحة الجريمة السيبرانية بما يسمح تبادل المعلومات[3].

كذلك القرارات رقم 64/211 الصادر عام 2010 والمتعلق بإرساء ثقافة عالمية للأمن السيبراني ويدعو البلدان إلى استعراض وتحديث الهيئات والقوانين المتعلقة بالجرائم السيبرانية، وعند متابعة قرارات الجمعية العامة تجدها غالبا ما تدعو إلى المزيد من المحادثات والمناقشات بشأن الأمن المعلوماتي وقضايا الأمن المعلوماتي الدولي، وبالتالي العمل على الوصول إلى طرح مشروع اتفاقية دولية تفيد وتحضر باستخدام الهجمات السيبرانية، إلى أن الأمر يعتبر صعبا نوعا ما نظرا للتفوق الكبير بين الدول في مجال الفضاء السيبراني والأنظمة المعلوماتية[4].

---

[1]- خالد حسن أحمد لطفي، المرجع السابق، ص149.

[2]- نوران شفيق، المرجع السابق، ص107-108.

[3]- نور أمير الموصلي، المرجع السابق، ص22.

[4]- اسمهان بعيري، المرجع السابق، ص63.

2- مجلس الأمن:

1-القرار 2341(2017)، الذي يهيب فيه الدول الأعضاء إلى إنشاء أو تعزيز الشراكات الوطنية والإقليمية والدولية مع الجهات صاحبة المصلحة من القطاعين العام والخاص، لتبادل المعلومات والخبرات من أجل منع الهجمات الإرهابية على الهياكل الأساسية ومواجهتها من أضرارها.

2- والقرار 2370(2017)، الذي يحث فيه الدول الأعضاء على العمل بصورة تعاونية لمنع الإرهابيين من حيازة الأسلحة، من خلال تكنولوجيا المعلومات والاتصالات، مع احترام حقوق الأساس والحريات الأساسية والامتثال للالتزامات بموجب القانون الدولي؛

2- مكتب مكافحة الإرهاب:

لقد اتخذ مكتب الأمم المتحدة لمكافحة الإرهاب عدة مبادرات في مجال التكنولوجيات الجديدة منها برنامج أمن الفضاء الالكتروني والذي يهدف الى:

1-تعزيز قدرات الدول الأعضاء والمنظمات الخاصة على منع إساءة استعمال الإرهابيين والمتطرفين العنيفين التطورات التكنولوجية، والتصدي لخطر الهجمات السيبرانية التي تشنها الجهات الفاعلة الإرهابية على البني التحتية الحيوية.

2-تخفيف أثار الهجمات السيبرانية واستعادة وإصلاح النظم المستهدفة في حالة حدوث تلك الهجمات.

3- تطوير استخدام وسائط التواصل الاجتماعي لمكافحة الإرهاب والتطرف العنيف على الانترنت في ظل احترام حقوق الإنسان[1].

4- تعزيز الحوار والتسامح والتفاهم بين الحضارات والثقافات والشعوب والأديان وتعزيز الاحترام المتبادل للأديان والقيم والمعتقدات الدينية والثقافات والأديان ومنع التشهير له.

5- التصميم على تحقيق الأهداف والغايات الإنمائية في المؤتمرات الرئيسية التي تعقدها الأمم المتحدة،

6- ترويج ثقافة السلامة والعدالة والتنمية البشرية والتسامح العرقي والوطني والديني[2].

ثانيا: جهود المنظمات الاخرى في مواجهة الهجومات السيبرانية

فضلا عن جهود المنظمات العامة السالفة الذكر، والتي تهدف الى تنظيم الهجمات السيبرانية، هناك صكوك قانونية أخرى قد تنطبق بشكل غير مباشر فهي لا تنظم أو تحظر الهجمات السيبرانية صراحة سوف نتطرق إلى أهمها فيما يلي :

---

[1]- نور أمير الموصلي، المرجع السابق، ص23.

[2]- خالد حسن أحمد لطفي، المرجع السابق، ص152.

1- حلف شمال الأطلسي (الناتو):

أدت تداعيات الهجمات السيبرانية التي استهدفت البنية التحتية الرقمية لاستونياعام2007 وأيضا منه جورجينا خلال نزاعها المسلح مع روسيا عام 2008، إلى سعي حلف شمال الأطلسي (الناتو) للتصدي لتلك الهجمات و ذلك من خلال نشر دليل يعرف باسم "دليل تالين" (Manuel de tallinn) الذي يعتبر وثيقة غير ملزمة تنظم قواعد الاشتباك عبر الانترنت و قد تم صدور إصدارين له:

- **الإصدار الأول عام 2013:** ويتكون من 95 قاعدة قانونية ويركز على أشد الهجمات السيبرانية خطورة ويطبق عليها قواعد القانون الدولي الإنساني .

- **الإصدار الثاني عام 2017:** المعروف باسم "Tallinn20" ويتكون من 154 قاعدة قانونية ويركز على الوضع القانوني لمختلف أنواع القرصنة والهجمات السيبرانية الأخرى التي تحدث يوميا وقت السلم[1].

ويوضح دليل تالين، قوانين الدولة التي يمكن تطبيقها على الحرب السيبرانية و هو سيمثل على كل من مبدأ حق اللجوء إلى الحرب و مبدأ سلوكيات الحرب، لما يعالج هذا الدليل كلا من النزاعات المسلحة الدولية وغير الدولية ويجمع الفقهاء في ضوء دليل تالين، بأن النزاع المسلح الدولي يحصل متى ما قامت دولة ذات سيطرة لحاملة على مجموعة من الأفراد بتوجيه تلك المجموعة لتنفيذ هجمات سيبرانية ضد دولة، أما إذا كانت لا تملك إلا سيطرة فعالة على تلك المجموعة فعندئذ تلك الهجمات لا تبلغ مستوى النزاع المسلح الدولي[2].

2- المنظمة العالمية للملكية الفكرية:

يمكن إبراز الإطار القانوني لحماية برامج الحاسوب الالي وبنوك المعلومات ضمن اتفاقية برن سنة1971، وكذا الاتفاقية المتعلقة بالجوانب المتصلة بالتجارة من حقوق الملكية الفكرية المسماة(التريبلس) كأهم محور وكذلك المعاهدة الخاصة بالمنظمة العالمية للملكية الفردية(الوايبوwipo) حول حقوق المؤلف والحقوق المجاورة والتي مرت بمراحل، أوفي اتفاقية باريس لحماية الملكية الصناعية التي أبرمت في 20 مارس 1883، وعدلت بتاريخ 1900 ببروكسل، و1911 بواشنطن، و1934 بلندن[3]، وكذلك وضع عقوبات على كل أعمال تزوير في العلامات التجارية لقرصنة المعتمدة والمرتكبة في إطار تجاري[4].

---

[1]- نور أمير الموصلي، المرجع السابق، ص24.

[2]- زهراء عماد محمد كلنتر، المرجع السابق، ص105.

[3]- زيبحة زيدان، الجريمة المعلوماتية في التشريع الجزائري و الدولي، دار الهدى، عين مليلة، الجزائر، 2011، ص17.

[4]- بن علية بن جدو، المرجع السابق، ص 310.

تأثير تقنية المعلومات على الحقوق المعنوية" تشريعات الملكية الفكرية فيما يتعلق بحماية حقوق المؤلف على البرمجيات وقواعد المعلومات والدوائر المتكاملة والنشر الالكتروني وعناوين المواقع في بيئة الانترنت"[1]، وفقا لاتفاقية إنشاء هذه المنظمة يتضح لنا أن من أهم أدوارها دعم الملكية الفردية في جميع أنحاء العالم يجمع صورها المصنفات الأدبية والفنية والعلمية والاختراعات[2].

3- الاتحاد الدولي للاتصالات (ITU):

يقوم الاتحاد بالاشتراك مع الوكالة الأوروبية لأمن الشبكات والمعلومات، شبه خريطة الطريق المتعلقة بمعايير الأمن في مجال تكنولوجيا المعلومات و الاتصالات كما تعاون الاتحاد الدولي مع المجلس أوروبا لإنجاز الاتفاقية الأوروبية حول الجريمة الالكترونية من أجل الاستعانة بها في عملية إطار قانوني دولي[3]، وهو يضم 193 عضوا من القطاعين الخاص والعام[4].

اعتمد المؤتمر العالمي لتنمية الاتصالات لعام 2006 القرار رقم 45، الذي دعا فيه مدير مكتب تنمية الاتصالات إلى تنظيم اجتماع بشأن الأمن المعلومات ومكافحة الرسائل الاقتصادية، وتقديم تقرير يتضمن نتائج الاجتماع إلى مؤتمر المندوبين المفوضية العام 2006[5]،

و في عام 2007 تم تبني مجموعة من التوصيات في مجال الأمن المعلوماتي الرسائل الاقتحامية، وهو ما يعرف ب" الاجندة العالمية للأمن الإلكتروني" والتي تضع إطارا للتنسيق ما بين الجهود الدولية لمواجهة التهديدات الإلكترونية وبناء الثقة ما بين مختلف الاطراف، وذلك إلى جانب تطوير انظمة للإنذار المبكر، كما أطلق الأمين العام للاتحاد في ايار 2007 جدول أعمال الأمن المعلوماتي العالمي لوضع إطار لمواجهة التحديات المتزايدة لأمن الانترنت[6] .

أما في عام 2008 تم عقد المؤتمر الإقليمي حول الأمن الالكتروني بالتعاون مع الاتحاد الدولي للاتصال في قطر و فيه دعوة جميع الدول لوضع وتنفيذ إطار وطني للأمن الالكتروني وحماية البنية التحتية الحرجة للمعلومات، والتي تعد أول خطوة في سبيل التحدي للتحديات التي تواجهها جراء اتصالها

---

(1)- نسرين عبد الحميد نبيه، المرجع السابق، ص 200.

(2)- خالد حسن أحمد لطفي، المرجع السابق، ص 175.

(3)- المرجع نفسه، ص 172.

(4)- نوران شفيق، المرجع السابق، ص109.

(5)- سليمان قطاف و عبد الحليم بوقرين، "مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية"، مجلد البحوث القانونية و الاقتصادية، جامعة عمار تليجي الأغواط، الجزائر، المجلد 03، العدد 02، 2022، ص76.

(6)- المرجع نفسه، ص76.

بتكنولوجيا المعلومات و الاتصال، وتم لهذا الغرض تعيين فريق خبراء لإسداء المشورة إلى الأمين العام للاتحاد بشأن المسائل المعقدة التي تكشف موضوع الامن السيبراني[1].

و تسمح اتفاقية الاتحاد الدولي للاتصالات[2]، للدول الأعضاء بقطع أي اتصالات سلكية أولا سلكية التي قد تظهر بأنها قد تشكل خطرا على أمن أي دولة طرف في الاتفاقية، و إضافة إلى ذلك، يحق للدول تعليق جميع خدمات الاتصالات الدولية لمدة غير محدودة لأسباب تتعلق بالأمن الوطني شريطة إذ تقوم على الفور بإخطار الأمين العام للأمم المتحدة، و على الرغم من القيود المذكورة أعلاه إلا أن اتفاقية الاتحاد الدولي للاتصالات لا تحظر على وجه التحديد استخدام الاتصالات، للأغراض العسكرية ما دامت تتخذ جميع الخطوات الازمة لمنع أي تدخل ضار[3].

الفرع الثاني: الاتفاقيات والالتزامات الدولية في مواجهة الهجمات السيبرانية

سنتطرق إلى دراسة الاتفاقيات والالتزامات الدولية في مواجهة الهجمات السيبرانية وفقا لما استقر في القانون الدولي أو العرفي وذلك من خلال التركيز على الاتفاقيات الدولية في مواجهة الهجمات السيبرانية (أولا)، ثم ثانيا الالتزامات الدولية في مواجهة الجريمة السيبرانية (ثانيا).

أولا: الاتفاقيات الدولية في مواجهة الهجمات السيبرانية

سنحاول الحديث عن الاتفاقيات العامة ذات الصلة بالتعاون الدولي في مواجهة الهجمات السيبرانية، ثم الاتفاقيات الدولية الاخرى من خلال ما يلي:

1- الاتفاقيات العامة ذات الصلة بالتعاون الدولي في مواجهة الهجمات السيبرانية:

إن القانون الدولي يحتوي على إرشادات و قواعد قانونية يبن الكثير من الالتزامات التي تقع على عاتق الدول قيما يتعلق بالتعاون الدولي لمكافحة الجريمة، ومنها الاتفاقيات العامة في اتفاقية بودابست لعام 2001، وكذلك دليل تالين الذي سنتناولهما فيما يلي:

1-1- اتفاقية بودابست لعام2001:

تعد هذه الاتفاقية هي أولى الاتفاقيات العالمية المتعلقة بجرائم الانترنت وقعت الاتفاقية في العاصمة المجرية بودابست في 23 نوفمبر 2001، بهدف التعاون و التضامن الدولي في محاربة الجرائم الالكترونية[4].

---

[1]- خالد حسن أحمد لطفي، المرجع السابق، ص173.

[2]- الاتحاد الدولي للاتصالات ITU هو وكالة متخصصة في مجال تكنولوجيا الاتصالات والمعلومات تابع للأمم المتحدة، الموقع الرسميhttps://www.itn. Int/Ar/ pages default.aspx.

[3]- نور أمير الموصلي، المرجع السابق، ص27.

[4]- وفاء لطفي، المرجع السابق، ص9.

إن مجلس أوروبا أول من اتخذ الخطوات مباشرة في تنظيم الهجمات السيبرانية فقد قام بعقد هذه الاتفاقية المتعلقة بالجريمة السيبرانية عام 2001 في بودابست هذه الاتفاقية عبارة عن سياسة مشتركة تهدف إلى حماية المجتمع من الجرائم السيبرانية من خلال التعاون بين الدول الأطراف[1].

قد وقعت 26 دولة أوروبية على هذه الاتفاقية بالإضافة إلى الولايات المتحدة الأمريكية، اليابان وجنوب افريقيا [2].

و تعرف اتفاقية بودابست عام 2001 باتفاقية الجرائم الالكترونية و التي حددت قائمة الحد الأدنى من صور الجرائم الالكترونية والمتعين تجريمها وتضمنت قواعد في الميدان إجراءات الضبط والتفتيش، والدليل الالكتروني والتعاون الدولي في تتبع هذه الجرائم وملاحقة المجرمين[3].

تضمنت هذه الاتفاقية (48) مادة، وقد أكدت على الحاجة الى اتخاذ تدابير تشريعية لمكافحة جرائم الكمبيوتر ومخاطرها على الدول، كما تضمنت عدة توصيات للدول الأعضاء لمكافحة الجريمة السيبرانية، ولغة اعتبرت مرجعا لا يستهان به في مجال محاربة المجرمين السيبرانيين[4].

وبالرغم من أن هذه الاتفاقية أوروبية المنشأ إلا أن عضويتها مفتوحة لجميع الدول التي تريد الانضمام اليها لتعم الفائدة[5]، وتنظم الجرائم السيبرانية ومع أنها البيان التوضيحي المصاحب لها يذهب إلى هذه الاتفاقية تترك مجالا بسيطا لا تتأثر به الحكومة كأحكام الحفاظ على النظام العام **أو** حماية الأمن القومي[6].

وعليه تعد اتفاقية بودابست الاتفاقية القانونية الوحيدة الملزمة التي توفر إطارا للتعاون الدولي في مكافحة الجرائم السيبرانية.

1-2-دليل تالين لعام 2013:

ان استبعاد قواعد اتفاقية بودابست من التطبيق في حالة الهجمات السيبرانية التي تقع بين الدول، يجعلنا نبحث عن أساس قانوني أخر يمكننا الاعتماد عليه، ومن أبرز هذه النصوص قواعد دليل

---

(1)- فيصل بدري، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة دكتوراه، تخصص قانون عام، كلية الحقوق، جامعة الجزائر، 2018، ص29-30.

(2)- وفاء لطفي، المرجع السابق، ص9.

(3)- نسرين عبد الحميد بنية، المرجع السابق، ص255.

(4)- منى الأشقر جبور، السيبرانية هاجس العصر، ط2، المركز العربي للبحوث القانونية القاهرة، 2016، ص105.

(5)- وفاء لطفي، المرجع السابق، ص9.

(6)- فيصل بدري، المرجع السابق، ص32.

تالين(lemanuel de tallinn) لعام 2013 المتعلقة بقواعد القانون الدولي المطبقة على الحروب السيبرانية[1].

بعد الهجمات السيبرانية المتتالية التي مست كل من استونيا عام 2007، وعلى إيران عن طريق برنامج ستاكس نت عام 2010 بدأ الاهتمام الدولي يركز على الهجمات السيبرانية، حث على أثر ذلك عقد حلف الشمال الأطلس مجموعة من المؤتمرات، وأهم ما تمخض عنها هو تقديم دليل بشأن الحرب السيبرانية عام[2]2013، (OTAN) أعد هذا الدليل من مجموعة خبراء في القانون الدولي بدعوة من منظمة حلف شمال الأطلسي (CICR)، ويتكون من (95) قاعدة استمدت في مجملها من أحكام القانون الدولي المختلفة كميثاق الأمم المتحدة وقواعد القانون الدولي الإنساني .....وغيرها[3].

إن دليل تالين هو وثيقة قانونية أعدها مجموعة من الخبراء تحت إشراف منظمة حلف الشمال الأطلسي و بمساعدة اللجنة الدولية للصليب الأحمر تضمن هذا الدليل قواعد يمكن تطبيقها على الحرب السيبرانية سواء وقت الحرب أو السلم[4].

و تجدر الاشارة أن اللجنة الدولية للصليب الأحمر[5]، كان لها دور كبير في إعداد هذا الدليل وذلك سبب تخوفها من التحديات التي أفرزتها التكنولوجيا العسكرية، لا سيما مع الاسلحة السيبرانية لذلك كانت من بين المشاركين الفاعلين في إعداد هذا الصك الدولي المنظم للهجمات السيبرانية[6].

جاء دليل تالين نظر لقصور القانون الدولي في مجال الحرب في مجال الحرب السيبرانية، ولذلك تم إبرامه كصك قانوني وحيد يكتب أن يلجأ إليه، لكن ما يعاب عليه هو تطبيقه في الحالات التي تتم خلال تنزع مسلح تقليدي وهذا ما كرسته القاعدة 20 من الدليل، المتعلقة بتطبيق قانون النزاع المسلح بحيث

---

(1)– رابح منزر، سعيد درويش الطبعة القانونية للهجمات السيبرانية التي تقع بين الدول، مجلة صوت القانون، المجلد 08، العدد 01، 2021، ص547.

(2)– اسمهان بعيري، المرجع السابق، ص59.

(3)– رابح منزر و سعيد درويش، المرجع السابق، ص547.

(4)– سعيد درويش، الحروب السيبرانية و أثرها على حقوق الإنسان، دراسة على ضوء أحكام تالين، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية كلية الحقوق، جامعة محمد بوقرة بومرداس، 2016، ص185.

(5)– اللجنة الدولية للصليب الأحمر هي عبارة عن منظمة دولية غير حكومية تأسيس في بداية الأمر بموجب المادة 60 من القانون المدني السويسري عام 1864 انظر: فيصل المقدم دور اللجنة الولية للصليب الأحمر في الرقابة على مدى تنقيذ القانون الدولي الانساني ابان الثورة الجزائرية، المجلة الاكاديمية للبحث القانوني، كلية الحقوق و العلوم السياسية ،جامعة تيزي وزو، 15000 الجزائري، المجلة 13، العدد 01، 2016، ص369–370.

(6)– سعيد درويش، المرجع السابق، ص186.

تشترط أن يكون النزاع مسلح سواء كان دولي أو كان داخل الحدود الجغرافية للدولة[1]، بالإضافة الى أنه عبارة عن وثيقة غير ملزمة قانونيا[2]، إذ لا يرقى إلى مستوى الاتفاقية الدولية فضلا عن معارضة بعض الدول لأحكامه كروسيا والصين على اعتبار أنهما لم يتشاركا في إعداده[3].

2- الاتفاقيات الدولية الاخرى في مواجهة الهجمات السيبرانية:

إن الاهتمام المتزايد لمعالجة الهجمات السيبرانية من خلال أطر قانونية مشتركة، جعل أغلب المنظمات الدولية تسعى الى وضع تنظيم قانوني يحكم الهجمات السيبرانية وسوف نبين أبرز هذه الجهود فيما يلي:

2-1- قانون الطيران:

يحتوي قانون الطيران المدني على ثلاثة صكوك رئيسية يمكن أن تنطبق على الهجمات السيبرانية.

2-1-1- اتفاقية شيكاغو لعام 1944 للطيران المدني الدولي: حيث تتعهد الدول الأعضاء في الاتفاقية عند إصدار اللوائح الخاصة بطائرتها الحكومية بمراعاة سلامة ملاحة الطائرات المدنية، بالتالي الهجوم السيبراني الذي يستهدف الرحلات الجوية المدنية، إذا وجه من دولة ما ضد طائرات مدنية تابعة لدولة أخرى، يمكن أن يتعارض مع ضمانات هذه الاتفاقية[4].

2-1-2- اتفاقية مونتريال لعام 1971 لقمع الأعمال غير مشروعة ضد الطيران المدني: حددت الاتفاقية مجموعة من الأفعال غير المشروعة الموجهة ضد سلامة الطائرة و التي ترتكب عن بعد فتجعلها غير صالحة للطيران أو تعرض سلامتها للخطر، فالهجوم السيبراني يتمثل في التدخل في نظام تشغيل الطائرة أو تعريض سلامتها للخطر أثناء الطيران، و كذلك التدخل في اتصالات مراقبة الحركة الجوية أو جوانب أخرى من الملاحة الجوية، فإنه يدخل في نطاق هذه الاتفاقية، أما خارج ذلك لا يتدخل ضمن الاتفاقية[5].

2-1-3- بروتكول مونتريال لعام 1988 لفهم أعمال العنف غير المشروعة في المطارات التي تخدم الطيران المدني الدولي: وسع البروتوكول الإطار القانوني لقمع أعمال العنف غير المشروعة في المطارات التي تستخدم الطيران المدني الدولي ليشمل أعمال العنف التي تعرض للخطر أو من المحتمل

---

(1)- رابح منزر، سعيد درويش، المرجع السابق، ص547.

(2)- الياس الصديقي، المرجع السابق.

(3)- رابح منزر، سعيد درويش، المرجع السابق، ص548.

(4)- نور أمير الموصلي، المرجع السابق، ص28.

(5)- نور أمير الموصلي، المرجع السابق، ص 28-29.

أن تعرض سلامة الأشخاص في المطارات للخطر و بالتالي يحظر هذا البروتكول أي هجمات سيبرانية مثل العبث بقوائم حظر الطيران أو بيانات الركاب أو نظام شبكة الكمبيوتر في المطار[1].

2-2- قانون الفضاء الخارجي:

يحتوي قانون الفضاء على قواعد قانونية قابلة للتطبيق على هجمات السيبرانية ذلك أن الشبكات العالمية، و الجوانب الرئيسية لتكنولوجيا المعلوماتية الحديثة يعتمد على منصات قضائية متعددة تدور حول الأمن من أجل دعم المحطات الأرضية، و فضلا من ذلك تعتبر هذه المنصات الفضائية في غاية الأهمية للهجمات السيبرانية و ذلك بسبب اعتبار هذه المنصات من العناصر الأكثر ضعفا في نظام المعلومات لأنه يستحيل ضد أي هجوم قد يقع عليه و بالإضافة إلى ذلك لأنها تتمثل القوة الأكثر حيوية و مقدرة لأي دولة تريد القيام بالهجمات السيبرانية بشكل ناجح، وبالتالي ستكون هذه المنصات الفضائية مشتركة[2] .

وكذلك تؤكد أنظمة الأقمار الصناعية كاتفاقية الاتصالات الفضائية لعام 1971 على" الغرض السلمي" في استخدام الأقمار الصناعية، ولكن على الرغم من أن هذه التنظيمات، لها دور جزئي في تنظيم الهجمات السيبرانية إلا أنها غير كافية[3].

2-3- قانون البحار:

يحتوي اتفاقية الأمم المتحدة لقانون البحار لعام 1982 على عدة قواعد قانونية يمكن أن ينطبق بشكل ثانوي على أنشطة الهجمات السيبرانية، فقد نصت الاتفاقية على حق المرور الكبرى للسفن طالما أنشطتها لا تضر بالسلام و حسن النظام وأمن الدولة الساحلية، وقد عددت الأنشطة المحظورة مثل أي نشاط يهدف الى جمع المعلومات للمساس بأمن أو دفاع الدولة الساحلية أو نشر المعلومات و الإشاعات بهدف التأثير على أمن أو دفاع الدولة الساحلية أو أي نشاط الى التدخل في أنظمة الاتصالات[4]، وبالتالي قد تؤدي هذه الأنشطة المحظورة إلى منع الهجمات السيبرانية التي تستخدم أنظمة الاتصالات والكمية الموجودة على متن السفن في البحار[5].

وفي حقيقة الامر وفي ظل غياب اتفاقيات دولية تنظم انتشار واستخدام الاسلحة الرقمية، فالقانون السائد يسير وفق قاعدة "البقاء للأقوى".

---

(1)- زهراء عماد محمد كلنتر، المرجع السابق، ص110.

(2)- مصطفى نعوس، "حقوق و التزامات الدول في الحرب المعلوماتية"، مجلة دار علوم الشريعة والقانون الجامعة الأردنية، المجلد 40، ملحق 01، 2013، ص84.

(3)- زهراء عماد محمد كلنتر، المرجع السابق، ص111.

(4)- المادة (19) من اتفاقية الأمم المتحدة لقانون البحار لعام 1982.

(5)- زهراء عماد محمد كلنتر، المرجع السابق، ص112.

ثانيا: الالتزامات الدولية في مواجهة الهجمات السيبرانية

سنتناول من خلال الالتزامات الدولية في مواجهة الجرائم السيبرانية ما يتعلق بإدراج الالتزامات الدولية في التشريعات الوطنية (أولا)، ثم الالتزام بتسليم المجرمين وملاحقتهم (ثانيا)، والالتزامات الدولية الاخرى ذات الصلة بالتعاون الدولي (ثالثا).

1- إدراج الالتزامات الدولية في التشريعات الوطنية:

إن الانضمام لأي معاهدة أو اتفاقية دولية تتعلق بالتهديدات، السيبرانية يلزم الدولة المصادقة ان تختار إلية مناسبة لتنفيذ بنود المعاهدة[1]، وذلك بإحدى الوسائل التالية :

1-1- الإضافة، وذلك من خلال إضافة باب خاص بالمواد التي تجرم التهديدات السيبرانية، وهو خيار جيد للدولة التي ترغب بإجراء إصلاحات واسعة في قانونها الجنائي[2].

1-2- التعديل، من خلال تعديل بعض المواد القانونية التي يحتويها القانون الجنائي بما يتلاءم وتجريم الأفعال وفقا لما هو منصوص عليه في الاتفاقية المصادق عليها[3].

1-3- النص الرئيسي، وذلك من خلال اعتماد قانون قائم بذاته يتضمن جميع العناصر الموضوعية والإجرائية التي تضمنتها الاتفاقيات الدولية[4].

2- الالتزام بتسليم المجرمين أو ملاحقتهم:

المعنى من تسليم المجرمين هو:" تخلي الدولة عن شخص موجود على إقليمها إلى دولة أخرى بناء على طلبها، لتحاكمه عن جريمة يعاقب عليها قانونا أو تنفذ فيه حكما صادرا عليه من إحدى محاكمها"[5].

إن الأساس القانوني لهذه الالتزامات نجده في العديد من الصكوك الدولية و هو مبدأ يقضي بأن كل دولة ملزمة أما بتسليم من ارتكب الجريمة أو محاكمة[6]، وبعد تسليم أو استرداد المجرمين هو إجراء من إجراءات التعاون القضائي الدولي وليشترط لصحة هذا الإجراء: التجريم المزدوج للفعل سبب المطالبة

---

(1)- اسمهان بعيري، المرجع السابق، ص60.

(2)- عزيز حسن كاميران، الجهود الدولية في مواجهة الجرائم السيبرانية، بغداد،2021، ص140.

(3)- مروى السيد السيد الحصاوي، السياسات الجنائية في مواجهة التقنيات الرقمية، ط2، المركز القومي للإصدارات القانونية، القاهرة، 2016، ص102.

(4)- عزيز حسن كاميران، المرجع السابق، ص142.

(5)- نادية دردار، الجهود الدولية لمكافحة الجريمة، المركز القومي للإصدارات القانونية، القاهرة،2017، ص19.

(6)- بلقاسم باريشي ومحمد سي ناصر، "التعاون الدولي في مجال تسليم المجرمين دراسة تحليلية على ضوء الاتفاقيات الدولية"، مجلة المستقبل للدراسات القانونية والسياسية، كلية الحقوق والعلوم المركز الجامعي أفلو، المجلد 04، العدد 01، جوان 2020، ص89.

بالتسليم مع ضرورة قيام معاهدة تسليم بين الطرفين العلاقة التعاونية – كأفضل عام – و توافر درجة معينة من الخطورة في الوقائع سبب المطالبة[1].

يمكن أن يستند التسليم إلى اتفاقيات إقليمية متعددة الأطراف مثل الاتفاقية الأوروبية لتسليم المجرمين لعام 1957، واتفاقية تسليم المجرمين بين الدول العربية واتفاقية الرياض العربية للتعاون القضائي، وغيرها[2].

وكذلك تقرر هذا المبدأ في اتفاقية بودابست في المادة (24/ فقرة 06) تحديدا فقد ورد فيها أنه رفض طلب التسليم المجرم بالنسبة للجرائم من المادة (2–11) من هذه الاتفاقية، كون المجرم من رعايا الدولة المطلوب منها التسليم أو ترى الدولة بأنها مختصة بالنظر في القضية، فإنه يجب على الطرف الآخر أن يحيل القضية إلى سلطاته لإجراء التحقيقات اللازمة[3]، كما تجدر الإشارة أن هذا المبدأ قد وجد أساسه أيضا، ضمن المادة (31) من اتفاقية العربية لمكافحة جرائم تقنية المعلومات[4].

3–الالتزامات الدولية الأخرى ذات الصلة بالتعاون الدولي:

من خلال تحليل نصوص اتفاقية بودابست نجد أن هناك عدة التزامات تقع على عاتقه الدول و من بينها:

3–1– الالتزام باحترام حقوق الإنسان: ولقد ورد هذا في المادة (15) المتعلقة بالشروط والضامنات الخاصة بالأحكام الإجرائية ونصت على سعي الدول لضمان خضوع وتنفيذ وتطبيق السلطات والإجراءات المنصوص عليها في هذه الاتفاقية لقانونها الوطني والذي يجب أن يوفر الملائمة لحقوق الإنسان[5]، ولقد جاء نص هذه المادة للتأكيد على أهمية حقوق الانسان عند قيام السلطة المختصة بالإجراءات المتعلقة بالكشف عن المجرمين وملاحقتهم كضبط وتفتيش الحاسوب ومكونات إذ يجب مراعاة حق الخصوصية[6].

---

(1)– فيصل بدري، المرجع السابق، ص545.

(2)– نادية دردار، المرجع السابق، ص30.

(3)– هلالي عبد الله أحمد، "الجريمة المعلوماتية"، مجلة جامعة بليل، العلوم الإنسانية، المجلد 14، العدد 02، 2007، ص89.

(4)– المادة (31) من اتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

(5)– المادة (15)من اتفاقية بودابست لمكافحة الجرائم السيبرانية لعام2001.

(6)– اسمهان بعيري، المرجع السابق، ص62.

3-2- احترام مبدأ التجريم المزدوج للوقائع: يعتبر شرط التجريم المزدوج قيد على الدولة طالبة التسليم والمطالبة كذلك باستلزام أن يكون الفعل محل التسليم معاقبا عليه كلا الدولتين كما أنه بعد كذلك ضمانة للشخص المطلوب تسليمه[1].

لقد نصت الفقرة الأولى من المادة السادسة عشر(16/ف1)من اتفاقية باليرمو على:" تطبيق هذه المادة على الجرائم المشمولة بهذه الاتفاقية شريطة أن يكون الجرم يلتمس بشأنه التسليم معاقبا عليه بمقتضي القانون الداخلي لكل من الدولة الطرف الطالبة و الدولة الطرف متلقية الطلب"، كما نصت عليه الفقرة الأولى من المادة السادسة (6/ف1)من اتفاقية الأمم المتحدة فيينا على شرط التجريم المزدوج بقولها: "تطبق هذه المادة على الجرائم التي تقررها الأطراف وفقا للفقرة 1 من المادة(3)".

و يجد التجريم المزدوج أثره في المادة (24) من اتفاقية بودابست، إذ ورد النص على انطباق هذه المادة على تسليم المجرمين بين الدول الأطراف في الأفعال المجرمة وفقا للاتفاقية شريطة أن يعاقب غلى هذه الجرائم قوانين كلا الطرفين المعنيين بعقوبة سالبة للحرية[2].

3-3- المساعدة القضائية المتبادلة: تعد المساعدة القضائية المتبادلة واحدة من أهم آليات التعاون الدولي في مجال القضائي، وتعني تقديم الدول الأطراف لبعضها البعض، على قدر أكبر من المساعدة من المساعدة القانونية في التحقيقات القضائية، وقد تظهر هذه الآلية في شكل إنابات قضائية دولية[3]، وقد تظهر في شكل تدابير إنقاذ الأحكام القضائية الجزائية الأجنبية، واكسابها الصيغة التنفيذية على الأقاليم الوطنية، وكذلك نقل المحكوم عليهم، ومصادرة العائدات المتأنية من الأنشطة غير المشروعة، وغيرها[4].

ورد هذا النص في المادة (25/ف1) من اتفاقية بودابست لعام2001، والتي بينت أن المساعدة المتبادلة تخضع لشروط الدولة المطلوب منها المساعدة، أو المعاهدات المساعدة القانونية المتبادلة بين

---

(1)- نادية دردار، المرجع السابق، ص47.

(2)- المادة 24 من اتفاقية بودابست لمكافحة الجرائم السيبرانية لعام 2001.

(3)- الإنابة القضائية الدولية في نقل إجراءات الملاحقة الجنائية بصدد جريمة من جرائم من الدولة الى أخرى، حتى كان ذلك في مصلحة حسن سير العدالة، و الغالب أن تنظم هذه الإنابة، بموجب اتفاقية دولية خاصة إذا تعلق الأمر بأكثر من ولاية قضائية، انظر: نادية دردار، المرجع السابق، ص74-75.

(4)- فيصل بدري، المرجع السابق، ص545.

الطرفين إلا أنه لا يجوز للدولة، الطرف أن ترفض تقديم المساعدة المتبادلة قيما يتعلق بالجرائم المشار إليها في الاتفاقية بحجة أن الدولة تعتبر هذه الجريمة مالية[1].

وعليه أصبح من الضروري إيجاد الوسائل المناسبة لتشجيع التعاون الدولي لمواجهة الهجمات السيبرانية، والعمل على التوفيق بين التشريعات الخاصة التي احتوت تلك الهجمات، فيجب أن يشمل هذا التعاون تبادل المعلومات، تسليم المجرمين، المساعدة القضائية المتبادلة ومكافحة الجرائم الناتجة عن تلك الهجمات، وتعد الوسيلة المثلى للتعاون الدولي في هذا الخصوص هو إبرام الاتفاقيات الدولية.

المطلب الثاني: الجهود الإقليمية في مواجهة الهجمات السيبرانية

تتميز الجهود الإقليمية في مواجهة الهجمات السيبرانية بالوضوح وذلك للحيز الجغرافي المحدود من الدول وقرب المسافة ووحدة التهديدات والتحديات بين مختلف الدول التي تملك حدود جغرافية موحدة، سنتناول الجهود الغربية في مواجهة الهجمات السيبرانية (الفرع الأول)، ثم الجهود الافريقية والعربية في مواجهة الجرائم السيبرانية (الفرع الثاني).

الفرع الأول: الجهود الغربية في مواجهة الجرائم السيبرانية

تقوم المنظمات الدولية بدورهم على الصعيد العالمي، فضلا عن عدد من المنظمات الإقليمية التي تركز فيعملها على مناطق محدودة، وهذه المنظمات لها جهود دولية مباشرة وأخرى جهود غير مباشرة سنطرق لها في ما يلي:

أولا: الجهود الاوروبية في مواجهة الجرائم السيبرانية

إن الاهتمام المتزايد لمعالجة الهجمات السيبرانية من خلال أطر قانونية مشتركة، جعل أغلب المنظمات الدولية تسعى الى وضع تنظيم قانوني بحكم الهجمات السيبرانية وسوف نبين أبرز هذه الجهود فيما يلي:

1- مجلس أوروبا:

يعد مجلس أوروبا[2] أول من اتخذ خطوات جدية و مباشرة لتنظيم جزء من الأمن السيبراني لأي منظمة دولية أو إقليمية أخرى، فقد قام بإنشاء اتفاقية بودابست المتعلقة بالجريمة السيبرانية[3]، لقد دعت

---

[1]- يوسف برقوق، "المساعدة القضائية المتبادلة لمواجهة الجرائم الكترونية"، مجلة البصائر للدراسات القانونية والاقتصادية، كلية الحقوق والعلوم السياسية جامعة جيلالي الياسي، سيدي بلعباس، الجزائر، المجلد 01، العدد 01، 2021، ص96.

[2]- مجلس أوروبا هو منظمة دولية معنية بالدفاع عن حقوق الانسان في القرة الأوروبية، موقعه الرسمي https://www.coe .Int /en/web/portal /home

[3]- نور أمير الموصلي، المرجع السابق، ص25.

ثلاثون دولة إلى التوقيع على أول اتفاقية دولية لمكافحة الإجرام السيبراني في العاصمة المجرية بودابست 2001، عقب الهجمات الإرهابية التي لها الولايات المتحدة الأمريكية في 11سبتمبر من العام نفسه، وتعد هذه الاتفاقية بمثابة المصدر القانوني الدولي الأول لكل الاتفاقيات الدولية والإقليمي والتشريعيات الوطنية ذات الصلة بالإرهاب الالكتروني، ونظرا لأهميتها انظم إليها العديد من الدول خارج مجلس أوروبا كالولايات المتحدة الأمريكية، اليابان، كندا وجنوب إفريقيا[1].

يتطرق نص الاتفاقية إلى تجريم الأفعال التي تمس سرية وسلامة الأنظمة المعلوماتية، كالدخول غير القانوني المتعمد (القرصنة)[2]، والاعتراض على سلامة البيانات[3]، وعرقلة الاستخدام الشرعي لنظام المعلومات[4]، وإساءة استخدام أجهزة الحاسوب[5]، نستنتج أن اتفاقية بودابست قد وضعت الإطار القانوني الدولي الأكثر تطور الذي ينظم الهجمات السيبرانية إلا أنها لا تتناول سوى جزء من التحدي العام، ومع ذلك فإنها توفر نقطة انطلاق لتصميم إطار دولي شامل لتنظيم الهجمات السيبرانية غير القانونية[6].

1- منظمة التعاون الاقتصادي و التنمية(OECD):

وهي المنظمة التي اهتمت بشكل عملي بحماية الخصوصية عبر الحدود، وقد تبلور هذا الاهتمام على شكل قواعد ارشادية وليست الزامية من الناحية القانونية، تم تبنيها رسميا من قبل مجلس لمنظمة في ايلول 1980، عرفت باسم قواعد (OECD) الإرشادية بشأن حماية الخصوصية ونقل وتدفق البيانات الشخصية[7].

وقد بدأت هذه المنظمة الاهتمام بالجرائم المرتكبة عبر الانترنت منذ عام1978 حيث وعت مجموعة أدلة وقواعد ارشادية تتصل بتقنية المعلومات أصدرت هذه المنظمة تقرير عام 1983 بعنوان الجرائم المرتبطة بالحاسوب وتحليل السياسة القانونية الجنائية[8]، وتعتبر هذه المنظمة أول منظمات التي

---

(1)– بلقاسم بن صابر و محمد حيدرة، "الهجمات السيبرانية و مواجهتها في ضوء القانون الدولي المعاصر"، مجلة حقوق الانسان و الحريات العامة، جامعة عبد الحميد بن باديس– مستغانم–، العدد 04، جوان 2017، ص205–206.

(2)– المادة (2) من اتفاقية بودابست لسنة 2001.

(3)– المادة (4) من ذات الاتفاقية.

(4)– المادة (5) من ذات الاتفاقية

(5)– المادة (6) من ذات الاتفاقية.

(6)– نور أمير الموصلي، المرجع السابق، ص26.

(7)– محمد أمين شوابكة، المرجع السابق، ص75.

(8)– بن عيلة بن جدو، المرجع السابق، ص309.

تطلق تحقيقا شاملا بشأن مشاكل الجرائم السيبرانية في الساحة الدولية، وترتكز هذه المنظمة شكل أكبر على الأمن السيبراني وتعزيز الثقة بين الدول في القضاء السيبراني[1].

وفي عام 1992 وضعت المنظمة توصيات إرشادية خاصة بأمن أنظمة المعلومات وقد تمخضت جهود المنظمة من أجل معالجة الجرائم المرتكبة عبر الانترنت بالتوصية بضرورة أن تعطي التشريعات الجنائية للدول الادعاء الافعال التالية:

- نقل البيانات بطريقة غير مشروعة والمعالجة الآلية بما في ذلك محوها.
- التجسس المعلوماتي ويتمثل في الحصول، أو الاقتناء أو الاستعمال غير المشروع للمعطيات.
- التخريب المعلوماتي ويكون من خلال الاستخدام غير المشروع، أو سرقة وقت الحاسب.
- قرصنة البرامج واعتراض استخدام المعطيات أو نقلها.
- الدخول غير المشروع على البيانات أو نقلها[2].

ثانيا: الجهود الأمريكية في مواجهة الهجمات السيبرانية:

عملت منظمة الدول الأمريكية[3]، منذ مطلع الألفية الثالثة على معادلة قضية الجريمة الالكترونية داخل المنطقة التي تعنى بها[4]، حيث وقع في الاجتماع الاستثنائي الذي عقدته لجنة مكافحة الإرهاب في نيويورك عام 2003، تعهد المنظمات الإقليمية في جميع المناطق، وخصوصا منظمة الدول الأمريكية، من حيث تقاسم خبراتها في إطار التعاون الإقليمي لمكافحة الأنشطة الإرهابية، كما عملت على إذكاء الوعي في مكافحة الإرهاب على الصعيدين الإقليمي والقطري وذلك بالتعاون مع منظمة الطيران المدني الدولي، والمنظمة الدولية للشرطة الجنائية (الإنتربول)، والمنظمة البحرية الدولية، ومفوض الأمم المتحدة السامي لشؤون اللاجئين، ومنظمة الجمارك العالمية.

وفي أثناء الاجتماع الخاص للجنة مكافحة الإرهاب ومنظمة الدول الأميركية، لجنة البلدان الأميركية لمناهضة الإرهاب الذي عقد في واشنطن، في2003، أقرت الدول الأعضاء التعاون الإقليمي، سواء بمعناه السياسي والتضامني أم على المستوى التنفيذي.

---

(1)– اسمهان بعيري، المرجع السابق، ص66.

(2)– بن عيلة بن جدو، المرجع السابق، ص310.

(3)– منظمة الدول الامريكية (AOS)هي منظمة دولية إقليمية تأسست عام 1984، في يوغوتا، ويقع مقرها في واشنطن يبلغ عدد الاعضاء المنظمة 35 عضوا من البلدان المستقلة في أمريكا الشمالية الجنوبية وتهدف المنظمة إلى تحقيق الامن والسلامة والعدالة، وتعزيز تضامنهم و الدفاع عن سيادة واستقلال أراضي وتلك البلدان، للمزيد أنظر:

http //www oas.org /en /defanlt.asp.

(4)– رامي وحيد منصور، المرجع السابق، ص107.

وفي سياق مكافحة تمويل الجماعات الارهابية داخل أميركا وخارجها، تعهدت الولايات المتحدة تقديم الدعم الفني لدول المنظمة الأمريكية، ومراقبة أنشطة المنظمات الارهابية المالية داخل وخارج أميركا، وتجميد أرصدتها وأصولها الثابتة، وقد قررت المنظمة التعاون الدولي لمكافحة تمويل الارهاب، وتمت صياغة سبع توصيات خاصة بتمويل الارهاب، أضيف إلى التوصيات ال 40 الموجودة حاليا لمكافحة غسيل الأموال، وذلك في إطار مجموعة العمل المالي الدولية وفريق العمل للشؤون المالية[1].

إن تهديد الهجمات السيبرانية والحرب السيبرانية كبير جدا بالنسبة للولايات المتحدة لدرجة أن مكتب التحقيقات الفيدرالي اعتبرها التهديد الأول للأمن القومي الأمريكي[2].

وعليه هناك ارتفاع هائل في الدول الغربية، الأوروبية منها والأمريكية من حيث الجرائم المعلوماتية وهو الامر الذي دفع هذه الدول إلى الاهتمام بسن قوانين وطنية لمكافحتها.

الفرع الثاني: الجهود الإفريقية و العربية في مواجهة الجرائم السيبرانية

على الصعيد الإفريقي والعربي، بذلت جهود كبيرة في مكافحة الجرائم السيبرانية والالكترونية أسفرت عن الجهود الإفريقية لمواجهة الهجمات السيبرانية (أولا)، ثم الجهود العربية في مواجهة الهجمات السيبرانية (ثانيا).

أولا: الجهود الإفريقية في مواجهة الهجمات السيبرانية

أطلقت قمة الاتحاد الإفريقي في عام 2007، المنعقد في بوتسوانا مبادرة في إطار الاتحاد تهدف إلى المساعدة في استكمال تطوير البنية التحتية في إفريقيا، وقد اعتمدت دول الاتحاد قانونا لمكافحة الإرهاب و الجرائم المتصلة بالحاسوب لقمع الأنشطة التي ترتكب من خلال أنظمة الحاسوب و تسهيل جمع الأدلة الرقمية وذلك على 2007، كما نص الاتحاد الإفريقي على اتفاقية تخص أمن الفضاء الالكتروني وحماية البيانات ذات الطابع الشخصي عام 2014 تهدف هذه الاتفاقية إلى تنظيم مجال تكنولوجيا متطور وإلى تعزيز الأمن السيبراني للدول الأطراف إذ تحدد هذه الاتفاقية القواعد الضرورية لإنشاء فضاء رقمي موثوق به المعاملات الالكترونية وحماية البيانات الشخصية ومكافحة التهديدات السيبرانية[3]،

---

[1]– خالد حسن أحمد لطفي، المرجع السابق، ص 162.

[2]-Tshepo Tlhacoane , cyber attacks « The latest threat to international peace and how international law can respond », Master of laws,sepcialising in international law, p.9.

[3]– اسمهان بعيري، المرجع السابق، ص71.

كما أن هذه الاتفاقية ركزت على وضع قواعد أساسية متعلقة بالتجارة الالكترونية في المنطقة الإفريقية فضلا عن القواعد المتعلقة بالتعاون الدولي والتنسيق بين الدول بغية المساعدة القانونية المتبادلة وتبادل المعلومات [1]، ومن أمثلة الجهود الإفريقية:

1- الجزائر في مواجهة الحروب السيبرانية:

تشهد الجزائر شكلا جديدا من الصراع و التحدي الأمني، تدور وقائعه ضمن الفضاء السيبراني تستهدف أساسا الأمن القومي و الوحدة الوطنية بالذات من قبل عديد من الفواعل الدولية في صورة دول أو منظمات أو أفراد[2]، وفي الجزائر يبدو أن هناك محاولات جادة لتطوير المنظومة القانونية وإصدار تشريعات تواكب التطور الحاصل في المجال التكنولوجي خاصة ما تعلق منها بتكنولوجيا الإعلام والاتصال ثم تغيير حتى اسم الوزارة المعنية لتأخذ اسم وزارة البريد وتكنولوجيا الإعلام والاتصال، إن الجزائر لا تزال متأخرة في هذا الميدان وهي تحتل المرتبة 121 ضمن البلدان الأعضاء في منظمة الأمم المتحدة التي شملها المسح و البالغ عددها 192 دولة[3]، هذا فضلا عن مشروع إنجاز بطاقة التعريف الالكترونية[4].

وكذلك تطوير النظام المصرفي الذي أدى إلى عدة تعديلات، أبرزها ما أورده الأمر رقم 03-05 الصادر في 2003/07/19 و المتعلق بحقوق المؤلف والحقوق المجاورة والتي أدرجت برنامج الحاسوب ضمن المؤلفات مضمونة الحماية، ويضاف إلى ذلك ما جاء به الأمر رقم 03-06 الصادر في 2003/07/19 المتعلق بالعلامات والأمر رقم 03-07 الصادر في: 2003/07/19 والمتعلق براءة الاختراع[5].

ومن الواضح أن كل ذلك يهدف إلى جعل القوانين الوطنية تنسجم مع التشريعات الدولية بعد انضمام الجزائر إلى الاتفاقيات الدولية الخاصة المتعلقة بالملكية الفكرية ذات العلاقة بالتجارة والمسماة تريبس، ومما يجب تأكيده أن الجريمة الالكترونية كظاهرة حديثة و خطيرة لم تعد الجزائر بمأمن عنها ولم تعد خفية، ومن الأمثلة عنها تعرض حقوق الإنسان للقرصنة عن طريق الانترنت، كذلك تعرض بعض المواطنين إلى عمليات النصب والاحتيال عن طريق البريد الالكتروني(e-Mail)[6].

---

[1]- مريم عبد اللطيف المسلماني، المرجع السابق، ص 24.

[2]- حسين ربيعي و محمود وسمر، "الحروب السيبرانية المخاطر و استراتيجيات تحقيق الامن السيبراني الدولي والداخلي"، المجلة الجزائرية للأمن الانساني، جامعة الاخوة المنتوري، قسنطينة، المجلد 07، العدد 02، 2022، ص185.

[3]- زيبحة زيدان، المرجع السابق، ص 20.

[4]- جريدة الخبر اليومية 12 مارس 2008.

[5]- زيبحة زيدان، المرجع السابق، ص 21.

[6]- المرجع نفسه، ص24-25.

وقد أكد التقرير السنوي لسنة 2020 لمخبر الأمن السيبراني(KASPERSKY)أن الجزائر تحتل المركز الثاني من حيث العتاد الالكتروني المستهدف بواسطة هجمات إلكترونية[1].

كخطوة أولى للحكومة الجزائرية لمواجهة ما يعرف بالجريمة الالكترونية صدر سنة 2009 القانون رقم 09-04 المؤرخ في 05 غشت2009، والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحاتها، إلا أن تجسيد بنوده على أرض الواقع ضعيف إلى حد الساعة، بعدما أهملت الجوانب التقنية الكفيلة بتصنيف هذه الجرائم وتحديد العقوبة المناسبة في حق مرتكبيها: كما أن هذا القانون أكد في فصله الأخير على مبدأ التعاون والمساعدة القضائية الدولية من إطار مبدأ المعاملة بالمثل، دعا رئيس الكتلة البرلمانية لجبهة العدالة والتنمية، الحكومة إلى ضرورة مراجعة موقفها تجاه هذا القانون، وقال لابد من ايلائه أهمية أكبر في ظل دخول الشارع الجزائري نفق الإدمان، والاعتماد الرهيب على شبكة الانترنت وما يصاحبها من آليات وخدمات الكترونية، مشددا في السياق ذاته على ضرورة تشريع قوانين جديدة تكرس العقاب الصارم لكبح مثل هذه الجرائم التي وصفها بالخطيرة و المدمرة[2].

2- مصر في مواجهة الحروب السيبرانية:

في اطار الجهود الدولية لدعم الأمن القومي وتنمية المجتمع المصري، ومع تزايد التهديدات والتحديات المستقبلية في المجال السيبراني والمجتمع الرقمي ولرصد ومجابهة المخاطر والتهديدات المتزايدة، قام المجلس الأعلى للأمن السيبراني بوضع الاستراتيجية الوطنية للأمن السيبراني(2017-2021)[3].

حيث تم في مصر لأول مرة انشاء إدارة عامة لمكافحة جرائم الحاسب الآلي وشبكة المعلومات، فرجال الشرطة يتلقون تكوينا في مجال مكافحة الجريمة المعلوماتية والتي أفشلت عدة محاولات لسرقة بطاقة الائتمان عن طريق الانترنت، التي قام بها شاب جامعي وكذا تم القبض على مهندس قام بتشويه سمعة بنت رجل مصري مهم عن طريق الانترنت[4].

وعليه يضعف الاستقرار الإقليمي بسبب غياب الهياكل والمؤسسات الأمنية، الامر الذي يهدد بدوره يجعل منطقة الشرق الأوسط وشمال افريقيا عرضة للصراع الدائم، بما في ذلك في الفضاء السيبراني.

---

(1)- حسين ربيعي و محمود وسيم، المرجع السابق، ص185.

(2)- أحمد بن خليفة و حفوظة الأمير عبد القادر، "الجريمة الالكترونية و اليات التصدي لها"، مجلة الامتياز لبحوث الاقتصاد و الإدارة، جامعة حمه لخضر، الوادي، المجلد 01، العدد 01، جوان 2017، ص 165-166.

(3)- الهجمات السيبرانية (الالكترونية و التأمين)، تاريخ الاطلاع (2024/02/18 على الساعة : 21:05)، متوفر على الموقع: نشرة الاتحاد المصري للتامين، المرجع السابق، ص14.

(4)- فاطمة الزهراء نسيسة، الجريمة الالكترونية واثرها على الفرد والمجتمع "دراسة سيسيولوجية"، الفا للوثائق، جامعة خميس مليانة ، الجزائر، 2019، ص127.

ثانيا: الجهود العربية في مواجهة الهجمات السيبرانية

أسفرت الجهود العربية لوضع اتفاقية عربية لمكافحة جرائم تقنية المعلومات2010، وكذا قانون الامارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات لعام 2003، وكذا وثيقة الرياض للنظام الموحد لمكافحة جرائم تقنية المعلومات في دول مجلس التعاون لدول الخليج العربي 2013 إضافة إلى الجهود الإقليمية الأخرى و المتمثلة، والتي سنتناولها فيما يلي:

1- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010:

جاءت هذه الاتفاقية من خلال الاجتماع المشترك لمجلس وزراء الداخلية والعدل العرب، الذي عقد بمقر الأمانة العامة لجامعة الدول العربية في عام 2010، بهدف تعزيز التعاون بين الدول العربية في مكافحة جرائم تقنية المعلومات، والجرائم السيبرانية التي تهدد أمنها و مصالحها و سلامة مجتمعاتها، وتلبية الحاجة إلى تبني سياسية جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد جرائم تقنية المعلومات، وقد أسفرت هذه الاتفاقية من منطق الالتزام بالمعاهدات والمواثيق العربية والدولية المتعلقة بهذا الشأن[1].

ودعا المجلس، الدول العربية المصدقة على هذه الاتفاقية بموافاة الأمانة الفنية للمجلس باتخاذ الاجراءات الملائمة لتشريعاتها مع أحكام الاتفاقية وتجريم الصور المستحدثة من الهجمات لمنع الإرهابيين من استخدام الانترنت وتعزيز التعاون مع المنظمات الدولية والإقليمية المعنية بمواجهة تلك الهجمات السيبرانية.

كما دعا المجلس الدول العربية إلى التعاون لمنع الإرهابيين من استغلال تكنولوجيا المعلومات والاتصالات والانترنت للتحريض على دعم أعمالهم الإرهابية وتمويل أنشطتهم والتخطيط والإعداد لها[2].

وتعتبر من أهم الجهود التي رصدها في هذا الشأن، اعتماد مجلس وزراء العدل العرب للقانون الجزائي العربي الموحد كقانون نموذجي بموجب القرار رقم 229 لسنة 1996، الذي تضمن فصلا خاصا بالاعتداء على حقوق الأشخاص الناتج عم المعالجات المعلوماتية مع النص بموجب المواد(461-463) حثه على وجوب حماية الحياة الخاصة وأسرار الأفراد من خطر المعالجة الآلية وكيفية جمع المعلومات والاطلاع عليها، وعقوبة من يقوم بالدخول بطريقة احتيالية إلى نظام المعالجة الآلية لمعلومات، وإفساد نظام التشغيل أو تغير المعلومات داخل النظام وتزوير وثائق المعالجة الآلية وسرقة المعلومات[3]،

---

[1]- طلال ياسين العيسى و عدي محمد عناب، المرجع السابق، ص 90.

[2]- سليمان قطاف و عبد الحليم بوقرين، المرجع السابق، ص 81.

[3]- خالد حسن أحمد لطفي، المرجع السابق، ص 177.

وهذه الاتفاقيات التي تم المصادقة عليها جاءت مطابقة لاتفاقية بودابست خاصة على المستوى الإجرامي من جهة وعلى ما يرتبط بالتعاون الدولي القانوني و القضائي (خاصة تسلم المجرمين من جهة أخرى[1].

2- قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات لعام 2003:

تم في عام 2003 مناقشة مشروعين أحدهما لمكافحة الجرائم السيبرانية و الأخر يخص التجارة الالكترونية، وما يهمنا بهذا الخصوص القانون العربي الاسترشادي "النموذجي" لمكافحة جرائم تقنية المعلومات إذ تم إفراره من قبل مجلس الوزراء العدل العرب في دورته 19، ومجلس وزراء الداخلية العرب في دورته الحادية و العشرون[2].

وبذلك تعد كل هذه الجهود العربية ترجمت في إصدار القانون العربي الاسترشادي، بصيغته المرفقة بعد تعديل تسميته ليصبح" قانون الإمارات العربي لاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها 2004" وطلب الأمانة العامة تعميمه على وزارة الداخلية في الدول العربي، هذا الأخير الذي جاء بسياسة تجريمية و عقابية في مضمونه[3].

بحيث تنص المادة (3) من القانون أعلاه:" حيث أنه عاقب كل من دخل عمدا وبغير وجه حق موقعا أو نظاما معلوماتيا يعاقب بالحبس و الغرامة أو بإحدى هاتين العقوبتين.."

3- وثيقة الرياض للنظام الموحد لمكافحة تقنية المعلومات في دول مجلس التعاون لدول الخليج العربي 2013:

أقر المجلس الأعلى لمجلس التعاون لدول العربية المنعقد في البحرين عام 2012، النظام الموحد لمكافحة جرائم تقنية المعلومات لدول مجلس التعاون هذا القانون يأتي في إطار سلسلة من القوانين والأنظمة الاستشارية في مسائل التعاون العدلي والقضائي بين دول المجلس الخليجي، وإذ يتجدد هذا النظام كل أربع سنوات تلقائيا في حال عدم ورود ملاحظات عليه، وتهدف وثيقة الرياض إلى محاربة الجرائم السيبرانية وفرض العقوبة على مرتكبيها ثم تحديد الأفعال المعاقب عليها في هذه الوثيقة أما العقوبات فتركت للسلطة التقديرية للأعضاء[4].

---

[1]- عبد الفتاح الطاهري، الجريمة المعلوماتية بين ثبات النص وتطوير الجريمة، مجلة القانون والأعمال الدولية، جامعة الحسن الاول، 2018.

[2]- اسمهان بعيري، المرجع السابق، ص69.

[3]- عبد الفتاح الطاهري، المرجع السابق.

[4]- عزيز حسن كاميران، المرجع السابق، ص142.

وعليه فالدول العربية ليست ببعيدة عن مرمى الهجمات السيبرانية، مما يجعل ضرورة لمواجهة تلك الهجمات، ووضع قانون للأنترنت يشتمل في أحد جوانبه على جرائم الانترنت بشقيها الموضوعي والإجرائي، فضلا عن ضرورة إنشاء منظمة عربية وتشجيع قيام اتحادات عربية تسعى للتصدي لمثل هذه الهجمات، وكذلك تفعيل دور المنظمات والإدارات والحكومات العربية في مواجهة تلك الجرائم عبر نظام الأمن الوقائي، كما يجب أن تمتد الجهود لتشمل التعاون العربي والدولي للقضاء على تلك الهجمات.

خلاصة الفصل الثاني:

نخلص مما سبق أن الهجمات السيبرانية تثير العديد من الاشكالات والتساؤلات الصعبة وذلك يرجع إلى تقنية الفضاء الإلكتروني الذي أصبح يشكل البعد الجديد في النزاعات المسلحة، وهو ما قد يدفع بالدول والجهات الفاعلة من غير الدول (الجماعات الإرهابية) خاصة إلى تطوير وشن مثل هذه الهجمات في المستقبل المنظور، مما يجعل ضرورة تطوير قواعد القانون الدولي المعاصر من أجل التكيف مع الاستخدام المتطور لهذه الهجمات.

وللقضاء على التأثيرات السلبية لهذه الهجمات على السلم و الأمن الدوليين سعى المجتمع الدولي لوضع آليات دولية من أجل التصدي لتلك الهجمات السيبرانية، إذا ما تركت على الأمن القومي للدول، وذلك عن طريق إبرام اتفاقيات ومواثيق دولية لمواجهة تلك الهجمات والعمل على محاربتها خاصة في إطار الأمم المتحدة، منها اتفاقية بودابست لمكافحة الهجمات السيبرانية، واتفاقية جامعة الدول العربية وكذلك الاتفاقيات الثنائية والمتعددة لتسليم المجرمين، والتي تعد من أهم أساليب مكافحة تلك الجرائم لما تتمتع به تلك الهجمات من خاصية اللاحدودية.

خـــاتمـــة

خاتمة:

إن ظهور الهجمات السيبرانية كانت نتيجة التطور الحاصل في تقنيات الحاسوب نتيجة الثورة التكنولوجية في العالم، وهو سلوك غير مشروع يهدد أمن الدول وسلامة مواطنيها وبنيتها التحتية الحيوية، ويتسبب في تعطيل استخدام الدولة لآليات الكترونية في إدارة شؤونها الداخلية، كما يمس بالسلم والأمن الدوليين، ما يستلزم مساءلة الدولة التي تشن هجمات سيبرانية ضد دولة أخرى ونتج عنها أضرار لحقت بها.

وتعتبر الهجمات السيبرانية واحدة من أهم التحديات المعاصرة التي تواجه المجتمع الدولي، لما لها من تداعيات على الأمن والسلم الدوليين، فقد أصبح الفضاء السيبراني جزءا لا يتجزأ من التفاعلات الدولية التي تبذل الأمم المتحدة والمجتمع الدولي الجهود لضبط الأمن فيه، خاصة وأن التهديدات في تزايد سريع ومستمر وفرص الحرب السيبرانية تتوسع باستمرار بشكل كبير والأطراف المشاركة فيها تزداد يوما بعد يوم، لاسيما مع انتشار الذكاء الاصطناعي، الأجهزة الإلكترونية وأنترنت الأشياء، ما يؤدي إلى ظهور كتل وتحالفات جديدة تتوحد بفضل المعلومة والتكنولوجيا والقوة السيبرانية، وهي بوادر الخريطة الجديدة للعالم الافتراضي.

ولهذا حاولنا من خلال هذه الدراسة البحث في مفهوم هذه الهجمات و المسؤولية القائمة بشأنها وكذا مظاهر تأثيرها على السلم و الأمن الدوليين والعلاقات الدولية لتصل في نهاية هذه الدراسة لعرض الجهود الدولية في مكافحة الهجمات السيبرانية، حيث توصلنا الى مجموعة من النتائج مرفوقة بجملة من الاقتراحات نراعي من خلالها مبدأ التدرج الذي ارتكزت عليه الدراسة، نوردها على النحو التالي:

أولا: النتائج

1- إن الهجمات السيبرانية ما زالت من المفاهيم الحديثة التي لا يوجد اتفاق دولي بشأن تعريفها، أدى إلى صعوبة تكييفها و تحديد المسؤولية الدولية القائمة بشأنها.

2- يكفل القانون الدولي بشتى مصادره الحماية القانونية للبنية التحتية ضد الهجمات السيبرانية مع تسجيل قصور في بعض هذه القواعد.

3- جاء المجال الخامس وهو الفضاء السيبراني ليشكل مجالا دوليا جديدا يمثل امتدادا لنشاط الإنسان ذي الطابع المدني أو العسكري، ويوازي ما يقوم به الإنسان في المجالات والفضاءات الدولية الأخرى، المجال البري والبحري والجوي والفضاء الخارجي.

4- تكمن الميزة النسبية للهجمات السيبرانية في انخفاض تكاليفها وسهولة اللجوء إليها، إذ لا تتطلب حشودا من المقاتلين العسكريين والآلاف حتى الأسلحة والوسائل، كالنزاعات المسلحة الحركية التقليدية، بل يكفي لتنفيذها شخص أو مجموعة صغيرة ممن لديهم الخبرة والمهارة في التكنولوجيا السيبرانية و ثغرات البرامج لاستخدامها ضد الدولة أو دولة أخرى.

5- إجماع الفقهاء الدوليين على خضوع الهجمات السيبرانية التي تحدث في سياق النزاع المسلح الحركي للقانون الدولي الإنساني، إلا أن التحدي الأكبر هو تلك الهجمات التي خارج سياق النزاع المسلح الحركي ومدى إمكانية عدها نزاع مسلح وإثبات نسبة الهجوم لدولة معينة وبالتالي إمكانية تطبيق القانون الدولي الإنساني عليها أيضا.

6- صعوبة تطبيق بعض مبادئ القانون الدولي الانساني، كمبدأ التناسب لضرورة في الإطار السيبراني لعدم وجود معايير ضابطة لمفهوم التناسب والضرورة.

7- تطرح المسؤولية الدولية للهجمات السيبرانية عدة إشكالات لا تزال محل بحث و نقاش بين الخبراء في القانون الدولي الذين يناشدون بتجاوز المفهوم التقليدي للمسؤولية الدولية، والأخذ بعين الاعتبار الطبيعة التقنية للفضاء السيبراني والتحديات التي أفرزها في مسألة كشف هوية المعتدي.

8- الأهمية الكبيرة التي يكتسبها مبدأ الانسانية أو مبدأ مارتينز في معالجة المسائل المعاصرة التي تهم البشرية وكأساس لتوقيع المسؤولية الدولية.

9- تكمن خطورة الهجمات السيبرانية على السلم والأمن الدوليين بكونها وسيلة قتال قادرة على التسلل إلى أنظمة إلكترونية معدة لحماية سير منشئات حيوية وحساسية لدول أخرى كمحافظة الطاقة النووية والسدود والمطارات..... وذلك بهدف تخريبها والسيطرة عليها.

10- إن الهجمات السيبرانية تؤثر على مجرى العلاقات الدولية وذلك من خلال تجنيد الارهاب عبر الشبكة الدولية للمعلومات وتحريضهم ضد الدول تحت مسمى الإرهاب السيبراني، وكل هذه الأفعال تؤثر و تهدد أمن المجتمع الدولي ككل.

11- هناك جهود دولية في سبيل تنظيم الأنشطة السيبرانية كاتفاقية بودابست ودليل تالين والقرارات الصادرة عن الأمم المتحدة، كما أن هناك قوانين وإن كانت سابقة لظهور الهجمات السيبرانية، إلا أنها تنظم وسائل و أدوات قد تستخدم في تنفيذها، مما يمكن الرجوع إليها، ومع ذلك هذه الجهود لم ترق الى مستوى تنظيم شامل لهذه الهجمات.

12- الإقرار بأنه تكمن صعوبة الهجمات السيبرانية من ناحيتين الأولى في عدم وجود خط محدد وواضح بين الأعيان العسكرية والمدنية بسبب الاستخدام المزدوج للأنترنت، أما الثاني في صعوبة إثبات نسبة الهجوم السيبراني في حال تم تكييفه على أنه هجوم الدولة أو جهة معينة.

ثانيا- الإقتراحات

1- العمل على الاتفاق بوضع معايير محددة لمعرفة المقصود بالهجمات السيبرانية، كونها الأساس لأي صك دولي ينظم الهجمات السيبرانية مستقبلا.

2- سعي الدول لاعتماد اتفاقية دولية لتنظيم الهجمات السيبرانية وإن كان هذا الأمر بعيد المنال في الوقت الحالي، وقد يستغرق وقت طويل من الزمن، كما يمكن وكحل سريع القيام بإصدار "بروتكول إضافي رابع" ملحق باتفاقيات جنيف الأربعة لعام 1949 بغرض تنظيم الهجمات السيبرانية وتجريم استخدامها على البنى التحتية الحيوية التي يمكن أن تعرض السكان المدنيين للخطر.

3- أهمية دور المجتمع الدولي في رفع الوعي بمخاطر الاستخدامات غير السليمة للتكنولوجيا، على الصحة والاقتصاد والأمن العالمي وذلك بتنظيم حملات توعية لمستعملي الوسائط الإلكترونية (الحاسوب، الانترنت، الهواتف الذكية...، تعريفهم بحجم الخطورة التي تترصدهم في حالة عدم اتخاذ الاحتياطات الوقائية اللازمة عند استعمالهم لها.

4- تعزيز الحوار والتنسيق وتبادل المعلومات بين الدول والمنظمات الدولية والإقليمية في إطار مكافحة إساءة استخدام تكنولوجيا المعلومات والاتصالات.

5- النهوض بالذكاء الاصطناعي واستخدامه بشكل مسؤول، وفقا للقوانين والأخلاقيات وجعله آلية فعالة لتحقيق الأمن السيبراني وفضاء رقمي أكثر أمانا.

6- على الدول أفرادا أو جماعات أن تعمل على دعم الجهود الدولية لمكافحة وتطويق الهجمات التي مصدرها الجهات الفاعلة من غير الدول سواء كانت شبكات إرهابية أو جماعات إجرامية، كما ينبغي على الحكومات توفير التقنيات اللازمة للتصدي لها، وإنشاء مراكز مخصصة لمكافحة الإرهاب السيبراني، وذلك للحد من احتمالات نجاح التهديدات السيبرانية المنظمة من قبل شبكات إرهابية.

7- اتخاذ تدابير من شأنها الحفاظ على سرية المعلومات الخاصة بالحسابات البنكية وبطاقات الائتمان، و غيرها من تبادل المعلومات.

8- التحديث المستمر لبرامج حماية الحواسب من الفيروسات.

9- التدريب والتكوين المستمر للكوادر البشرية العاملة في مجال مكافحة الهجمات السيبرانية واستحداث شهادات عليا متخصصة في المجالات التقنية والقانونية، المتعلقة بمكافحة الجرائم المعلوماتية، وحث الجامعات، من خلال تكثيف الندوات و الملتقيات والأيام الدراسية حول هذا الموضوع.

قائمة المصادر والمراجع

قائمة المصادر والمراجع:

أولا: المصادر

1- الاتفاقيات الدولية:

1-ميثاق الأمم المتحدة لعام 1945 .

2-البروتكول الاضافي الاول لعام 1977 الملحق باتفاقيات جنيف الاربعة لعام 1949.

3-اتفاقية بودابست لمكافحة الجرائم السيبرانية لعام2001.

4-الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010.

5-دليل تالين 2013، بشأن القانون الدولي المطبق على الحروب السيبرانية.

2- المعاجم اللغوية:

1- منير البعليكي، المورد الحديث "قاموس انجليزي- عربي"، دار للعوم للملايين، بيروت، 2019.

2- قاموس المعاني، معنى كلمة سايبر، تاريخ الاطلاع(2024/02/21 على الساعة: 08:06)، متوفر على موقع:.https //www. almaany.com/an/dd/er/cyber،

ثانيا: المراجع

1-باللغة العربية:

1- 1-الكتب:

1- أحمد عمرو، ما بعد الإنسانية العوالم الافتراضية وأثرها على الإنسان، شركة أفاق المعرفة للنشر والتوزيع، المملكة العربية السعودية، الرياض، 2022.

2- أحمد عيسى نعمة الفتلاوي، الهجمات السيبرانية (دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصرة)، منشورات زين الحقوقية ، بيروت، 2018.

3- بشرى حسين الحمداني، القرصنة الالكترونية (أسلحة الحرب الحديثة)، دار أسامة للنشر والتوزيع، عمان، 2014.

4- خالد حسن أحمد لطفي، الإرهاب الالكتروني (آفة العصر الحديث والآليات القانونية للمواجهة)، دار الفكر الجامعي، كلية الحقوق، الإسكندرية، 2019.

5- خالد ممدوح إبراهيم، أمن الجريمة الالكترونية، الدار الجامعية، الإسكندرية، 2008.

6- رفد عيادة الهاشمي، الإرهاب الالكتروني، دار أمجد للنشر والتوزيع، 2019.

7- زهراء عماد محمد كلنتر، المسؤولية الدولية الناشئة عن الهجمات السيبرانية، مكتبة القانون المقارن، بغداد، 2019.

8- زيبحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة، الجزائر، 2011.

9- سالم محمد عبود، أساسيات الأمن السيبراني، دار الدكتور للعلوم الإدارية والاقتصادية، بغداد، 2022.

10- عبد العزيز العشاوي، محاضرات في المسؤولية الدولية، دار هومة ، الجزائر ، 2007

11- عبد الغاني شرقي، " التهديدات السيبرانية العالمية، المجلد 07، العدد 02، 2023،

12- عدنان النقيب، الحرب الالكترونية في ضوء بروتكولي سبع وسبعون الملحقين باتفاقيات جنيف الأربع لسنة تسع وأربعين (الهجمات السيبرانية)، المركز العربي للنشر والتوزيع، القاهرة، 2022.

13- فاطمة الزهراء نسيسة، الجريمة الالكترونية واثرها على الفرد والمجتمع "دراسة سيسيولوجية"، الفا للوثائق، جامعة خميس مليانة، الجزائر،2019.

14- لخضر زازة، أحكام المسؤولية الدولية في ضوء قواعد القانون الدولي العام، دراسة مدعمة بالأمثلة والسوابق القضائية وأعمال لجنة القانون الدولي، دار هومة، جامعة الاغواط، 2011.

15- م م علي عبد الرحيم العبودي، هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين، جامعة بغداد-كلية العلوم السياسية

16- محمد الكويتي، الامن السيبراني في 2023، تحولات عصر الذكاء الاصطناعي، ترينذز للبحوث والاستثمارات، 2023/04/01.

17- محمود أحمد قرعان، الجرائم الالكترونية، دار وائل للنشر والتوزيع، عمان، 2017.

18- مروى السيد السيد الحصاوي، السياسات الجنائية في مواجهة التقنيات الرقمية، ط2، المركز القومي للإصدارات القانونية، القاهرة، 2016.

19- مصطفي علوي، مفاهيم الأسس العلمية للمعرف "الامن الإقليمي بين الامن الوطني والامن العالمي"، المركز الدولي للدراسات المستقبلية و الاستراتيجية، القاهرة، العدد السنة الاولي، أبريل 2005

20- منال محمد عباس، الإرهاب الالكتروني والأمن الاجتماعي، دار المعرفة الجامعية، كلية الآداب، جامعة الإسكندرية، 2019.

21- منى الأشقر جبور، السيبرانية هاجس العصر، ط2، المركز العربي للبحوث القانونية، القاهرة، 2016.

22- نادية دردار، الجهود الدولية لمكافحة الجريمة، المركز القومي للإصدارات القانونية، القاهرة، 2017.

23- نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف جلال حزي وشركاه، 2008.

24- نوران شفيق، أثر التهديدات الالكترونية على العلاقات الدولية" دراسة في أبعاد الأمن الإلكتروني"، المركز العربي للمعارف، القاهرة، 2016.

1-2-المقالات:

1- إبراهيم مسلم نبراس، "الجرائم السيبرانية وأثرها على الأمن السيبراني" مجلة القادسية للقانون و العلوم السياسية، كلية الحقوق، جامعة بغداد، العراق، العدد 01،المجلد 12، 2021.

2- أحمد بن خليفة و حفوظة الأمير عبد القادر، الجريمة الالكترونية وآليات التصدي لها، مجلة الامتياز لبحوث الاقتصاد والإدارة، جامعة حمه لخضر، الوادي، المجلد 01، العدد 01، جوان 2017.

3- بلقاسم باريشي و محمد سي ناصر، "التعاون الدولي في مجال تسليم المجرمين دراسة تحليلية على ضوء الاتفاقيات الدولية"، مجلة المستقبل للدراسات القانونية والسياسية، كلية الحقوق و العلوم المركز الجامعي افلو، المجلد 04، العدد 01، جوان 2020.

4- بلقاسم بن صابر و محمد حيدرة ، الهجمات السيبرانية ومواجهتها في ضوء القانون الدولي المعاصر، مجلة حقوق الإنسان والحريات العامة، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم، العدد 04، جوان 2017.

5- بوطلاعة وداد و بوكورو منال، الهجمات السيبرانية على البنية التحتية الحرجة، الإخوة منتوري قسنطينة، المجلد 07، العدد 02، 2022.

6- جلالي شويرب و فائزة مراد، مفهوم الحروب السيبرانية الأمن السيبراني، مجلة الحقوق والحريات، جامعة عمار ثليجي الأغواط، كلية الحقوق والعلوم السياسية، المجلد 11، العدد 01، 2023.

7- حسن عبد الله الدعجة، مهددات الامن الإنساني، مجلة الجزائرية للأمن الإنساني، العدد الرابع، جويلية 2017، ص130.

8- حسين ربيعي و محمود و وسمر، الحروب السيبرانية، المخاطر و استراتيجيات تحقيق الامن السيبراني الدولي والداخلي، المجلة الجزائرية للأمن الانساني، جامعة الاخوة المنتوري، قسنطينة، المجلد 07، العدد 02، 2022.

9- حسين ربيعي ومحمود وسمر، الحروب السيبرانية، المخاطر واستراتيجيات تحقيق الامن السيبراني الدولي والداخلي، المجلة الجزائرية للأمن الانساني، جامعة الاخوة المنتوري، قسنطينة، المجلد 07، العدد 02، 2022.

10- حياة حسين، الفضاء الالكتروني و تحديات الآمن العالمي، مجلة العلوم القانونية والسياسية، مخبر الرقمنة والقانون في الجزائر، جامعة البليدة 02، المجلد12، العدد 01، أفريل2021.

11- خليلي سعيدي ومرزوق بن مهيدي، الذكاء الاصطناعي كتوجه حتمي في حماية الامن السيبراني، دراسات في حقوق الانسان، جامعة العربي التبسي تبسة، الجزائر، المجلد 06، العدد 01، جوان 2022.

12- رابح منزر و سعيد درويش، الطبعة القانونية للهجمات السيبرانية التي تقع بين الدول، مجلة صوت القانون، المجلد 08، العدد 01، 2021.

13- رزق أحمد سمودي، حق الدفاع عن النفس نتيجة الهجمات الالكترونية في ضوء قواعد القانون الدولي العام مجلة جامعة الشارقة للعلوم القانونية، المجلد 15، العدد 02، 2018.

14- رمضان محمد حمدان، الإرهاب الدولي وتداعياته على الأمن والسلم العالمي دراسة تحليلية من منظور اجتماعي، مجلة أبحاث التربية الأساسية، جامعة الموصل، العراق، المجلد 11، 2011.

15- سعيد درويش، الحروب السيبرانية وأثرها على حقوق الإنسان، دراسة على ضوء أحكام تالين، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية كلية الحقوق، جامعة محمد بوقرة بومرداس، 2016

16- سليمان قطاف و عبد الحليم بوقرين، مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية، مجلد البحوث القانونية والاقتصادية، جامعة عمار تليجي الأغواط، الجزائر، المجلد 03، العدد 02، 2022.

17- سمير باي، التهديدات الأمنية السيبرانية: دراسة في انعكاسات الحرب الالكترونية على الامن القومي للدول واستراتيجيات المقاومة، مجلة الرسالة للدراسات والبحوث الإنسانية، المجلد 08، العدد 02، 2023.

18- سمير قلاع الضروس، الأمن السيبراني الوطني "قراءة في أهم الاستراتيجيات الأمنية والتقنية لمواجهة الجريمة الإلكترونية بالجزائر"، مجلة الرواق للدراسات الاجتماعية والإنسانية، جامعة غرداية (الجزائر)، المجلد 08، العدد 02، 2022.

19- صلاح الدين معماش، حظر الهجمات في القانون الدولي الإنساني، مجلة السياسة، جامعة محمد بوقرة، بومرداس (الجزائر)، المجلد 06، العدد 01، 2022.

20- طلال ياسين العيسى و عدي محمد عناب، "المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر"، مجلة الزرقاء للبحوث والدراسات الإنسانية، كلية الحقوق، جامعة عجلون الوطنية، الأردن، المجلد 19، العدد 01، 2019.

21- عبد الفتاح الطاهري، الجريمة المعلوماتية بين ثبات النص وتطوير الجريمة، مجلة القانون و الأعمال، 2018.

22- عبد الكريم بإسماعيل، تأثير الفضاء الافتراضي على الأمن القومي، مجلة البحوث والدراسات، جامعة قاصدي مرباح ورقلة (الجزائر)، المجلد 19، العدد 01، 2022.

23- علي سنوسي، الهجمات السيبرانية في ضوء أحكام قواعد القانون الدولي الإنساني والاتفاقيات الدولية، مجلة الحقوق والعلوم السياسية، كلية الحقوق، جامعة بن خلدون، تيارت، المجلد 10، العدد 02، 2023.

24- لامية طالة، التهديدات والجرائم السيبرانية: تأثيرها على الامن القومي لدول واستراتيجيات مكافحتها، مجلة معالم الدراسات القانونية والسياسية، المجلد 4، العدد، 02السنة 2000.

25- محمد دحماني، الذكاء الاصطناعي كآلية لتعزيز الأمن السيبراني، مجلة الفكر القانوني والسياسي، جامعة عمار ثليجي، الأغواط، المجلد 07، العدد 02، 2023.

26- مصطفى نعوس، حقوق و التزامات الدول في الحرب المعلوماتية، مجلة دار علوم الشريعة و القانون الجامعة الاردنية المجلد 40، ملحق 01، 2013.

27- نسيب نجيب، الحرب السيبرانية، من منظور القانون الدولي الإنساني، المجلة النقدية للقانون والعلوم السياسية، كلية الحقوق والعلوم السياسية ، جامعة بتيزي وزو، المجلد 16، العدد 04، 2021.

28- هاجر ختال، الوضع القانوني للحرب السيبرانية على ضوء القانون الدولي، مجلة التواصل في الاقتصاد والادارة والقانون، كلية الحقوق و العلوم السياسية، جامعة باجي مختار، عنابة، المجلد25، العدد 03، سبتمر 2019.

29- هلالي عبد الله أحمد، الجريمة المعلوماتية، مجلة جامعة بليل، العلوم الإنسانية، المجلد 14، العدد 02، 2007.

30- يحي ياسين سعود، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، المجلة القانونية، كلية الحقوق، جامعة القاهرة، المجلد 04، العدد 04، 2018.

31- يوسف برقوق، "المساعدة القضائية المتبادلة لمواجهة الجرائم الكترونية"، مجلة البصائر للدراسات القانونية والاقتصادية، كلية الحقوق والعلوم السياسية جامعة جيلالي الياسي، سيدي بلعباس، الجزائر المجلد 01، العدد 01، 2021.

1-3- المذكرات والرسائل الجامعية:

1-فيصل بدري، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي أطروحة مقدمة لنيل شهادة الدكتوراه، علوم تخصص قانون عام، كلية الحقوق، جامعة الجزائر، 2018.

2-نور أمير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الإنسان، مذكرة ماجستير، الجامعة الافتراضية السورية، 2021.

3-اسمهان بعيري، الهجمات السيبرانية وأثرها على تهديد الأمن والسلم الدوليين، مذكرة ماستر، قانون عام معمق، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الشاذلي بن جديد، الطارف، 2022.

1-4- المداخـلات:

1-عبد الحميد بن بادة، جريمة التجسس الالكتروني نمط جديد من التهديدات السيبرانية الماسة بآمن دول المنطقة، ورقة بحث قدمت ضمن فعليات الملتقى الدولي الأول الموسم "بآمن المعلومات في الفضاء السيبراني"، المنظم من قبل كلية الحقوق والعلوم السياسية، جامعة غرداية، (يومي17و18 فيفري2020).

2-محمد حيدر، المسؤولية عن الأضرار البيئية في القانون المدني الجزائري، مداخلة مقدمة في ملتقى الوطني حول آليات الوقاية من الأخطار الطبيعية والتكنولوجية الكبرى في القانون الجزائري والقوانين المقارن، كلية الحقوق والعلوم السياسية، جامعة حسيبة بن بوعلي ، الشلف، (يومي 01 و02 ديسمبر 2014).

1-5- المقالات الإلكترونية:

1- إسراء نادر كيطان، المسؤولية الدولية عن الأضرار التي تحدثها الهجمات الالكترونية في الفضاء الافتراضي، ماجستير، الجزء الثاني، المجلد 03، العدد خاص لبحوث المدرسيين مع طلبة الدراسات

العليا،2021، ص 339. تاريخ الاطلاع (2024/04/15 على الساعة 14:37)، متوفر على الموقع: Esraamader 743@gmail.com-lumam529@ gmail.com

2- محكمة العدل الدولية ، قضية الأنشطة العسكرية وشبه العسكرية في نيكاراغوا ضد الولايات المتحدة الأمريكية ، 27 جوان 1986، موجز الأحكام والفتاوى الصادرة من محكمة العدل الدولية 1948-1991 ، منشورات الامم المتحدة نيويورك ،1999، ص 212، تاريخ الاطلاع (2024/04/17 على الساعة 11:30)، متوفر على الموقع : https://www.icj.cij.org/or.

3- وفاء لطفي، الجهود الدولية في مجال مكافحة جرائم الإرهاب السيبراني، التجربة الماليزية نموذجا، متوفر على الرابط:http ://jpsa.journals.ekb.eg/article، تاريخ الاطلاع (2024/02/18، على الساعة 21:09).

4- الهجمات السيبرانية (الالكترونية والتأمين)، تاريخ الاطلاع (2024/02/18 على الساعة: 21:05)، متوفر على الموقع: https://www.infegypt.org /News Details.aspx

5- تحديات الأمن السيبراني في عصر الذكاء الاصطناعي، تاريخ الاطلاع (2024/03/06، على الساعة 22:11)، متوفر على موقع Bakkah.

6- أقوى هجمات سيبرانية استهدفت روسيا، تاريخ الاطلاع(2024/02/25، على الساعة 21:00)، العربية، متوفر على الموقع :http://www.arabic.com.

7- العربية " التهديدات السيبرانية واثرها علي حماية البنى التحتية والخدمات الحيوية ، ماعت السلام والتنمية وحقوق الانسان، الموقع الإلكتروني .https ;maatpeace اخر زيارة(5.05.2004 0 الساعة 16:00).

2-باللغة الأجنبية

2-1-الكتب

1-Marco Roscini ,World Warfare, Jus ad bellum and the Use of cyber Farce, Max Planck Yearbook of united Law.VOL 14.2014, p.95.

2-2-المقالات

1-Tshepo Tlhacoane , cyber attacks « The latest threat to international peace and how international law can respond », Master of laws,sepcialising in international law,.

فهرس المحتويات

فهرس المحتويات

الملخص:

تشكل الهجمات السيبرانية تهديدا حقيقيا للبنية التحتية للدول وأمنها القومي، في ظل الانتشار الواسع لتكنولوجيا الأجهزة الحاسوبية والشبكة المعلوماتية ومع تطور الذكاء الاصطناعي، هذا ما جعل المجتمع الدولي يواجه مخاطر جديدة مواكبة لهذا التطور، عرفت بالهجمات السيبرانية والتي لا تقتصر أثارها على البيانات في أجهزة الكمبيوتر وأنظمته، بل تمتد لتهديد كل من الأمن والسلم الدوليين، ولما يشكله من مجال مفتوح لتصاعد التهديدات الأمنية وانعدام الاستقرار.

في هذا السياق نبحث عن مدى تأثير الهجمات السيبرانية على السلم والأمن الدوليين والجهود الدولية المبذولة في مواجهة تلك الهجمات وذلك في ظل غياب قانون دولي سيبراني متخصص ودقيق، حيث أصبح لا بد أن نبحث في السبل التي يجب إتباعها للتصدي لتلك الهجمات العابرة للحدود.

Abstract :

Cyber-attacks constitute a real threat to the infrastructure of countries and their national, in light of the widespread spread of computer technology and the information network, and with the development, known as cyber attaks, the effects of wich are not limited to the data in computers and systems, rather, it extends to the threat of international peace and security, and what it poses an open field for escalating security threats and instability.

In this context, we examine the extent cyber attaks affect international peace and security and effort, the international efforts made to confront these attaks in the absence of specialized and precise international cyber law, it has become necessary to look into the methods that must be followed to confront these cross-border attaks.