دور الامن السيبرانى فى مواجهة الارهاب الالكتروني

الدكتورة / ايناس ممدوح محمد محمد سليمان

المقدمة :

فى ظل التقدم الهائل فى علم البرمجيات والتقنية المتسارعة فى النظم المعلوماتية ، ومع تزايد الاعتماد على الحواسب الآلية والشبكات المعلوماتية ظهر ما يسمى الجرائم الالكترونية والتى يطلق عليها " **الجرائم السيبرانية**" والتى تعد من أخطر التحديات التى تواجه المعاملات الالكترونية .

وبالرغم من الاثار الايجابية للتطور التكنولوجى الا ان اختراق الانترنت للحدود وظهور العوالم الافتراضية العابرة للحدود نتج عنه ما يسمى " **بالارهاب الالكترونى** "، فلم تعد الجريمة الالكترونية تتمركز فى دولة او مجتمع معين بل اصبحت تهدد امن واستقرار العديد من الدول خاصة مع صعوبة اكتشاف تلك الجرائم واثباتها ، وهو الامر الذى يتطلب معه تضافر الجهود الدولية فى التصدى لمثل هذه الجرائم .

وظهرت الثورة الرقمية، في منتصف العقد الماضي، حين انتبه الغرب إلى قضية الإرهاب الإلكتروني ومخاطره، حيث قام الرئيس الأمريكي بيل كلينتون في العام 1996 بتشكيل لجنة حماية منشآت البنية التحتية الحساسة ، وكان أول استنتاج لهذه الهيئة هو أن مصادر الطاقة الكهربائية والاتصالات إضافة إلى شبكات الكمبيوتر ضرورية بشكل قاطع لنجاة الولايات المتحدة، وبما أن هذه المنشآت تعتمد بشكل كبير على المعلومات الرقمية، فإنها ستكون الهدف الأول لأية هجمات إرهابية تستهدف أمن الولايات المتحدة .وفي أعقاب ذلك، قامت كافة الوكالات الحكومية في الولايات المتحدة، بإنشاء هيئاتها ومراكزها الخاصة، للتعامل مع احتمالات الإرهاب الإلكتروني. فقامت وكالة الاستخبارات المركزية بإنشاء مركز حروب المعلوماتية، ووظفت ألفا من خبراء أمن المعلومات، وقوة ضاربة على مدى 24 ساعة لمواجهة الإرهاب الإلكتروني . وقد اتخذت الدول الاوربية ذات النهج خاصة الدول التابعة لحلف الأطلسي، باتخاذ إجراءات مماثلة.

وقد مهدت ثورة المعلومات والقدرة على استخدام التكنولوجيا الى بروز اشكال جديدة ومتنوعة من القوة الإلكترونية ، والتي أصبح لها انعكاس مباشر على المستوى المحلي والدولي، فمن ناحية أدت إلى إعادة توزيع القوة وانتشارها بين أكبر عدد من الفاعلين،

وهذا ما جعل قدرة الدولة في السيطرة على هذا المجال موضوع شك مقارنة بالمجالات الأخرى للقوة.
ومن ناحية أخرى جعلت القوة الإلكترونية بعض الدول الأصغر في السياسة الدولية لديهم قدرة أكبر على ممارسة القوة الصلبة والناعمة عبر استراتيجية جديدة تمثل "القوة الإلكترونية" مصدرها ، وهذا ما يعني تغييراً في علاقات القوى في السياسة الدولية.
واتسمت الحروب الإلكترونية بصفة تدميرية كبرى على الامن القومى للدول لما لها من قدرة على التجسس والتسلل ثم النسف بدون دخان ولا أنقاض سواء عن طريق تدمير المواقع على الإنترنت ونسفها وقصفها بوابل من الفيروسات ، أو العمل على استخدام أسلحة الفضاء الإلكتروني المتعددة للنيل من تلك المواقع ، وهي أسلحة يسهل الحصول عليها من خلال مواقع الإنترنت أيضاً ، ولذلك فان تداعيات هذا النوع من الحروب تكون خطيرة على الامن القومى للدول.

أهمية البحث :

تكمن أهمية البحث من الموضوع كونه يبحث في العلاقة بين التطور التكنولوجي والتغيير في شكل الصراعات الدولية ، متنقلاً بذلك الى مرحلة جديدة من علاقات القوى بين وحدات النظام الدولي والتي دخلت في حالة من التسابق الدولي في تنمية وتطوير القدرات التكنولوجية في كافة المجالات. وبالرغم من حداثة قضية الأمن السيبراني كقضية ناشئة في حقل العلاقات الدولية ، الا ان هناك تاريخ طويل من البحث حول دور التكنولوجيا الرقمية في الدراسات الأمنية ، لذا يهدف البحث الى التعرف على مفهوم الامن السيبرانى ودوره فى مكافحة الارهاب الالكترونى وتأثيره على الامن القومى والاجراءات الواجب اتخاذها فى مواجهة الهجمات السيبرانية وتفعيل الدور الدولى لمواجهة هذه الظاهرة .

إشكالية البحث :

ينطلق البحث من إشكالية مفادها "ان الامن السيبرانى نقل علاقات القوى بين الوحدات الدولية والصراعات العالمية الى مرحلة جديدة ومختلفة ، حيث تطورت الجرائم السيبرانية بسرعة فائقة رغم حداثتها ترافق فى ذلك سرعة انتشار التكنولوجيا الحديثة

العابرة للحدود ، حيث اصبحت الكثير من الدول واجهزتها الامنية فى مواجهة مع انماط عديدة من الجرائم السيبرانية المستحدثة ، والتى شكلت تهديدا مباشر على الامن القومى للدول واثرت سلبا على الجانب الاقتصادى والامنى والعسكرى بشكل يوجب حتمية التدخل الدولى الحازم لمكافحة مثل هذه الجرائم ، لذا تدور تساؤلات البحث عن دور الامن السيبرانى فى مكافحة الهجمات السيبرانية والارهاب الالكترونى من خلال التوضيح النقاط الاتية :

1- ماهية الامن السيبرانى والهجمات السيبرانية
2- الطبيعة القانونية للهجمات السيبرانية
3- مدى تأثير الارهاب الالكترونى على الامن القومى والاجتماعى
4- الدور الدولى فى مواجهة تلك الهجمات
5- سبل مكافحة تلك الهجمات السيبرانية

وبناء عليه فان البحث ينطلق من فرضية مفادها" : كلما تمت الاستعانة بالعامل التكنولوجي كلما زاد من حالة عدم الاعتماد على العامل البشري في ادارة الحروب والصراعات الدولية" وبداية لحروب غير تقليدية . وعليه تم تقسيم البحث الى المباحث الاتية :

المبحث الاول : مواجهة المخاطر السيبرانية والارهاب الالكترونى

المطلب الاول : مفهوم الامن السيبرانى ومتطلبات القوة السيبرانية .

المطلب الثانى : الارهاب الالكترونى ومخاطره على الامن القومى

المبحث الثانى : تكييف الهجمات السيبرانية فى القانون الدولى

المطلب الاول: الهجمات السيبرانية فى القانون الدولى العام

المطلب الثانى : الطبيعة القانونية للهجمات السيبرانية فى القانون الدولى الانسانى

المبحث الثالث: الجهود الدولية فى التصدى للارهاب الالكترونى

المطلب الاول : جهود المنظمات الدولية

المطلب الثانى : الجهود العربية والاقليمية

المبحث الاول

مواجهة المخاطر السيبرانية والارهاب الالكترونى

- - - - - - - - - - - - - - - -

فرضت التحولات التكنولوجية واقع امنى جديد خاصة فيما يتعلق بتطور التهديدات السبرانية للبيئة الامنية الدولية ومع الانتشار المكثف للاتصالات الالكترونية عالميا واقليميا برزت تحديات أمنية متعلقة بمدى حماية امن الدول . حيث تعمل ثورة المعلومات والابتكارات التنظيمية ذات الصلة على تغيير طبيعة الصراع وأنواع الهياكل والعقائد والاستراتيجيات العسكرية فظهرت الحرب السيبرانية والحرب الشبكية. وهى حروب بعيدة عن استنزاف جيوش ضخمة كما حدث فى الحرب العالمية الأولى والثانية ،انما تقوم ثورة المعلومات إلى نشوء الحرب السيبرانية ، الفائز فيها هو الجانب الذي يعرف أكثر بالاتصالات والاستخبارات ، وسيتمتع بمزايا حاسمة ، فإن الجيوش المتصارعة تستهدف دوما ثلاثة عناصر أساسية من أجل كسب المعركة ، وهي العناصر العسكرية، والاقتصادية، والسياسية أو بكلمات أخرى إرادة الشعب. وفي عالم حروب المعلومات تجد العناصر الثلاث نفسها وعلى رأسها مراكز القيادة والتحكم العسكرية، والبنوك والمؤسسات المالية، ومؤسسات المنافع كمؤسسات المياه والكهرباء وذلك لإخضاع إرادة الشعوب .

و تشير الحرب السيبرانية إلى أنها ستتطور كمكملات للاستراتيجيات العسكرية الشاملة. قد يكون للحرب الإلكترونية دور فى الصراعات المجتمعية التي غالبًا ما ترتبط بنزاع منخفض الحدة من قبل جهات فاعلة غير حكومية ، مثل الإرهابيين أو تجار المخدرات أو ناشري أسلحة الدمار الشامل في السوق السوداء. فالنزاعات المستقبلية ستخوضها "الشبكات" و من يتقن استخدام تلك الشبكة واسرارها سيتمتع بقوة كبيرة[1]

---

(1) تقرير صادر عن معهد أبحاث الأمن القومي بمؤسسة RAND ،عن الاستعداد للصراع في عصر المعلومات ، يناير 1997 .

John Arquilla and David Ronfeld , RAND / In Athena’s Camp: Preparing for Conflict in the Information Age, eds.MR-880-OSD/RC(1997) ،

المطلب الاول

مفهوم الامن السيبرانى ومخاطره

اولا: مفهوم السبرانية :

مصطلح السيبرانية هو واحد من أكثر المصطلحات تردداً في معجم الأمن الدولي، وتشير المقاربة الإيتيمولوجية لكلمة "Cyber"إلى أنها لفظة يونانية الأصل مشتقة من كلمة "kybernetes"بمعنى الشخص الذي يدير دفة السفينة، حيث تستخدم مجازاً للتعبير عن للمتحكم ، وتجدر الإشارة إلى أن العديد من المؤرخين يرجعون أصلها إلى عالم الرياضيات الأمريكي Norbert Wieners وذلك للتعبير عن التحكم الآلي، فهو الأب الروحي المؤسس للسبرنيتيقية من خلال مؤلفه الشهير:

Cybernetics or control and communication in" the Animal and the machine .

وأشار في كتابه إلى أن السبرنتيقية هي التحكم والتواصل عند الحيوان والآلة والإنسان ، ليستبدل مصطلح الآلة بعد الحرب العالمية الثانية بالحاسوب. [1]

ويرى البعض ان السيبرانية كلمة انجليزية مشتقة من كلمة Cyber وتعنى (مرتبط بالحاسب الالى او شبكات الحاسب).[2]، وقال انها تعنى فضاء الانترنت او العالم الافتراضى [3].

---

(1) عنترة بن مرزوق ، محى الدين حرشاوى ، الامن السيبرانى كبعد جديد فى السياسة الجزائرية ،مجلة دفاتر السياسة والقانون ،العدد17 ، جامعة قاصدى مرباح ، 2017 ، ص 66

(2) عبد العزيز بن فهد ابم داود ، الجرائم السبرانية ، مجلة الاجتهاد للدراسات القانونية والاقتصادية ، المملكة العربية السعودية ، المجلد 9 العدد3 2020 ، ص 148

(3) صالح بن على بن عبد الرحمن الربيعة ، الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت، هيئة الاتصالات وتقنية المعلومات ، المملكة العربية السعودية 2018 ، ص 6

واصطلاحياً :هناك العديد من التعاريف التي قُدمت لمفهوم الأمن السيبراني، حيث يُعرّف بأنه" : مجموعة من الإجراءات المتخذة في مجال الدفاع ضد الهجمات السيبرانية ونتائجها التي تشمل تنفيذ التدابير المضادة المطلوبة."

بينما عرّفه إدوارد أمورسو استاذ علوم الكمبيوتر أنه" : وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها، وتوفير الاتصالات المشفرة

ويرتبط الأمن السيبراني بعدة مفاهيم اخرى ذات صلة به وضرورية لوجوده اهمها :

1-الفضاء السيبرانى :

الذى عرفته الوكالة الفرنسية لأمن أنظمة الإعلام ANSSI، وهي وكالة حكومية مكلفة بالدفاع السيبراني الفرنسي، بأنه" فضاء التواصل المشكّل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية ."فهو بيئة تفاعلية حديثة، تشمل عناصر مادية وغير مادية، مكوّن من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مشغلين أو مستعملين ، و هناك مَن عرّف الفضاء السيبراني بوصفه الذراع الرابعة للجيوش الحديثة

كما عرفه الاتحاد الدولى للاتصالات بانه " مجموع الادوات والسياسات والمفاهيم الامنية والضمانات الامنية والمبادىء التوجيهية والتقنيات ونهج ادارة المخاطر التى يمكن استخدامها لحماية البيئة الالكترونية وتنظيم اصول المستخدم ، تشمل توصيل اجهزة الحوسبة والموظفين والبنية التحتية والخدمات ونظم الاتصالات السلكية واللاسلكية ومجمل المعلومات المرسلة او المخزنة فى البيئة الالكترونية ."[1]

(1) الاتحاد الدولى للاتصالات ITU ، دراسة عن تأمين شبكات المعلومات والاتصالات ، قطاع تنمية الاتصالات ، فترة الدراسة (2006 -2010) متاح على موقع
https://www.Itu.Int/net/Itunews/issues/2010/9/Pdf/201009_20-ar.pdf

كما عرفه استاذ العلوم السياسية الامريكى " جو نای" بانه القدرة على استخدام الفضاء الالكترونى لخلق مزايا ، والتأثير على الاحداث فى البيئة التشغيلية الاخرى .[1]

2- الردع السيبراني

ويعرف بأنه "منع الأعمال الضارة ضد الأصول الوطنية في الفضاء والأصول التي تدعم العمليات الفضائية"، ويرتكز الردع السيبراني على ثلاث ركائز استراتيجية فى الدفاع تتمثل في :مصداقية الدفاع ، والقدرة على الانتقام ، والرغبة في الانتقام .

3- الجريمة السيبرانية :

وهى مجموعة الأعمال الغير القانونية التي تتم عبر أجهزة إلكترونية أو شبكة الإنترنت أو تبث عبرها محتوياتها، وهي ذلك النوع من الجرائم التي تتطلب الإلمام الخاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها

ثانيا : متطلبات القوة السيبرانية

تتمثل القوة السيبرانية فى القدرة على التأثير من خلال استخدام وسائل الاتصال وشبكاته المعلوماتية بالاضافة الى العديد من العناصر والمتطلبات التى تتمثل فى الاتى :

أ : البنية التكنولوجية :

تحتاج الدولة لأجهزة ذات كفاءة وقدرة عالية وشبكات اتصال متعددة ، وكذا برمجيات متطورة بالاضافة الى العنصر البشرى المدرب من اجل البنية التحتية للقوة السيبرانية ،

([1]) Joseph .S .Nye , Cyberpower (Harvard Kennedy School ,Belfer center for science and International Affairs 2010 ,Available at:
http://www.Belfercenter.Ksg. Harvard .Edufilescyber –power ,pdf,P05

حيث تستطيع الدولة من خلالها التأثير على الاقاليم باستخدام القدرات الالكترونية من جهة وتأمين نفسها من الاخطار الممكنة من جهة اخرى [1]

ب : الفيروسات والبرامج الخبيثة :

وهى برامج مصممة من اجل تنفيذ عمليات قرصنة على اجهزة وشبكات بعض الدول وتستخدم لتعطيل البنية التحتية وتحويل عمليات الاتصال وسرقة البيانات والمعلومات بغرض التأثير على اجهزة هذه الدول .

جـ : القدرة على القيام بالعمليات الالكترونية :

وتتمثل فى اختراق الشبكات ومهاجمة أنظمة المعلومات وتسمى القدرة الهجومية اما القدرة الدفاعية فهى تتمثل فى عمليات الحماية من الهجمات المختلفة وامكانيات تشغيل الاجهزة ببرمجيات خاصة ومعينة ، اممما القدرة الاستطلاعية فهى تتمثل فى عملية الدخول فى الحواسب الالية والتجسس على الشبكات المحلية والقيام بالعمليات الاستخبارتية بغرض معرفة خطوات الخصم[2]

لذلك فان القوة السيبرانية تتطلب تحقيق اقصى درجات الامن الالكترونى من خلال تبنى سياسات دفاعية وعمليات حماية وتطوير ضد الاخطار المحتملة ومنع تعرضها للهجمات المعادية ، ويعد أبرز نمطين للقوة السيبرانية هما :

1- **نمط القوة الصلبة** : وهى استخدام المقدرات والادوات فى عمل تخريبى عبر قطع كابلات الاتصالات او تدمير انظمة الاتصالات او الاقمار الصناعية وحتى استعمال البرامج التخريبية وتنفيذ عمليات سرقة منظمة للبيانات .

---

(1) سامى محمد بوتيف ، دور الاستراتيجيات الاستباقية فى مواجهة الهجمات السيبرانية ، الردع السيبرانى نموذجاً ، المجلة الجزائرية للحقوق والعلوم السياسية ، مجلد 4 ، العدد 7 ، 2019 ص 127

(2) نسرين الشحات الصباحى ، الابعاد العسكرية للقوة السيبرانية على الامن القومى للدول ، دراسة حالة اسرائيل منذ 2010 ، المركز القومى الديمقراطى ، برلين ،2016 ، على موقع :
https://democraticac.de/?p=30962

2- **نمط القوة الناعمة :** وتتمثل فى استخدام القدرات السيبرانية فى جانب التأثير الناعم على الطرف الاخر وفق نظريات التشويش وتغيير مسارات القوة عبر التلاعب بالمعلومات وتوظيف نتائجها لخدمة المصالح المستهدفة [1]

المطلب الثانى

الارهاب الالكترونى ومخاطره على الامن القومى

اثبت الواقع العملى ان الدولة لا تستطيع بجهودها المنفردة مواجهة تلك الجرائم المستحدثة مع هذا التطور المستمر فى كافة ميادين الاتصالات وتكنولوجيا المعلومات ، ونظرا لما تشكله ظاهرة الارهاب الالكترونى من أهمية أمنية وقانونية تمس الامن القومى للدول ومواجهتها تتطلب الوقوف ضرورة الوقوف على مفهوم الارهاب الالكترونى ومخاطره وسبل مواجهتها واتخاذ كافة التدابير المضادة تجاهها .

اولا : المقصود بالارهاب الالكترونى ومخاطره :

لا يوجد مصطلح من المصطلحات أكثر استثارة للخلاف مثل مصطلح الإرهاب حيث اختلفت وجهات النظر وتباينت ، متأثرة بالمصالح الوطنية أو القومية أو الاعتبارات السياسية ، فقد ملأت قضية ما يسمى (بالإرهاب) الدنيا ، وشغلت الناس ، وأصبحت حديثًا مشتركا بكل اللغات ، وعلى اختلاف الحضارات .

وعند دراسة المفاهيم والمعاني لا بد أولاً من الرجوع إلى معاجم اللغة الأصيلة، وملاحظة تطور المعنى في المعاجم الحديثة وبالنظر في ذلك نجد في لسان العرب، ما يأتي: (رَهِبَ بمعنى خاف والاسم الرَّهَبُ، كقوله تعالى: (**مِنْ الرَّهْبِ**) أي بمعنى الرهبة،

---

(1) عادل عبد الصادق ، الفضاء الالكترونى وأسلحة الانتشار الشامل بين الردع وسباق التسلح ، مؤتمر حروب الفضاء السيبرانى ، هولندا ، مايو 2015 ، على موقع :
https://seconf.wordpress.com/2015/05/15/

ومنه: "لا رهبانية في الإسلام"... كاعتناق السلاسل، والاختصاء، وما أشبه ذلك مما كانت الرهابنة تتكلفه، وقد وضعها الله عز وجل عن أمة محمد ، وأصلها من الرهبنة: الخوف، وترك ملاذ الحياة كالنساء..). [1]

كلمة الإرهاب مشتقة من (رهِب): بالكسر، يرهب، رهبة. ورهباً -بالضم، ورهباً بالتحريك بمعنى أخاف وترهّب غيره: إذا توعّده، وأرهبه ورهّبه: أخافه وفزعه. ورهب الشيء رهباً ورهباً، ورهبه: خافه. والاسم: الرّهب، والرهبي، ورهبوت، والرهبوتي.[2]

وكلمة "إرهاب" تشتق من الفعل المزيد (أرهب)، ويقال أرهب فلانا: أي خوَّفه وفزَّعه، وهو المعنى نفسه الذي يدل عليه الفعل المضعف (رَهّبَ)، أما الفعل المجرد من المادة نفسها وهو (رَهِبَ)، يَرْهبُ رَهْبَةً فيعني خاف،. والرهبة: الخوف والفزع، أما الفعل المزيد بالتاء وهو (تَرَهَّبَ) فيعني انقطع للعبادة في صومعته، ويشتق منه الراهب والراهبة والرهبنة والرهبانية... إلخ، وكذلك يستعمل الفعل ترَهَّبَ بمعنى توعد إذا كان متعديا فيقال ترهب فلانا: أي توعده، وأرهَبَه واستَرْهَبَه: أخافَه وفزَّعه. [3]

وفي المعجم الوسيط، الإرهابيون: (وصف يطلق على الذين يسلكون سبيل العنف والإرهاب لتحقيق أهدافهم السياسية). [4]

ويعرف الارهاب فى قواميس اللغة الإنجليزية بكلمة (terror) وتعني "استعمال العنف لتحقيق أغراض سياسية" [5]

---

(1) لسان العرب لابن منظور ،أبو الفضل جمال الدين محمد بن مكرم، دار صادر بيروت، 1955م / 1374 هـ ،ج 8، ص 337، بتصرف.

(2) الصحاح، إسماعيل بن حماد الجوهري، تحقيق أحمد عبدالغفور عطار، دار العلم للملايين، بيروت، ط2، 1975م، مادة: رهب.

(3) احمد جلال الدين ، الارهاب والعنف السياسي ، دار الحرية القاهرة ، 1989 ، ص 22 ، عبد الرحيم صدقى ، الارهاب السياسى والقانون الجنائى ، دار النهضة العربية ، القاهرة ،1985 ، ص81

(4) المعجم الوسيط، مجمع اللغة العربية، ط2، القاهرة 1972م، ص 282.

(5)Longman Dictionary of English Language and Culture, London, 1993.

وقد عرفت اتفاقية جنيف لقمع الإرهاب ومعاقبته لعام 1937 المادة الأولى أن الإرهاب هو (الأعمال الإجرامية الموجهة ضد دولة ما وتستهدف خلق حالة رعب في أذهان أشخاص معينين أو مجموعة من الأشخاص أو عامة الجمهور).[1] وهذا التعريف يعتبر أن الإرهاب يكون موجه ضد الدولة وليس ضد الأفراد أو الجماعات أو حركات التحرر.

اما الارهاب الالكترونى : فينطلق تعريفه من تعريف الارهاب حيث لا يختلف كلاهما الا فى نوعية الاداة او الوسيلة المستخدمة لتحقيق العمل الارهابى .

وكانت بداية استخدام مصطلح **الإرهاب الالكتروني Cyber Terrorism** في فترة الثمانيات علي يد **باري كولين Barry Collin** [2]والتي خلص فيها إلى صعوبة تعريف شامل للإرهاب التكنولوجي. ولكنه تبنى تعريفاً للإرهاب الالكتروني مقتضاه ، بأنه "هجمة الكترونية غرضها تهديد الحكومات أو العدوان عليها، سعياً لتحقيق أهداف سياسية أو دينية أو أيديولوجية، وأن الهجمة يجب أن تكون ذات أثر مدمر وتخريبي مكافئ للأفعال المادية للإرهاب."

ويعرفه **جيمس لويس James Lewis** [3]على أنه " استخدام أدوات شبكات الحاسوب في تدمير أو تعطيل البني التحتية الوطنية المهمة مثل :الطاقة والنقل والعمليات الحكومية، أو بهدف ترهيب حكومة ما أو مدنيين"

---

(1) أمل اليازجي ، محمد عزيز شكري ، الإرهاب الدولي والنظام العالمي الراهن، دار الفكر ، دمشق ،2002 ، ط1، ص63.

(2) باري كولين ، زميل أبحاث في معهد الأمن والاستخبارات في كاليفورنيا، واول من اطلق مصطلح "الإرهاب الإلكتروني " Cyberterrorism في إشارة إلى التقاء الفضاء الإلكتروني والإرهاب.

(3) James A .Lewis, Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats, Center for Strategic and International Studies, December, 2002

أما **دورثي دينينغ Dorothy Denningg** وهى من ابرز الباحثين فى مجال الامن الالكترونى ، ترى أن الإرهاب الالكتروني هو "الهجوم القائم على مهاجمة الحاسوب، وأن التهديد به يهدف إلى الترويع أو إجبار الحكومات أو المجتمعات لتحقيق أهداف سياسية أو دينية أو عقائدية وينبغي أن يكون الهجوم مدمراً وتخريبياً ،لتوليد الخوف بحيث يكون مشابه للأفعال المادية للإرهاب.

فالارهاب الالكترونى هو احد الاستخدامات الغير سلمية للفضاء الالكترونى وهو نتيجة لتفاعل العالم المادى مع العالم الافتراضى ، لذا من الصعب الوصول الى تعريف محدد لظاهرة الارهاب الالكترونى فهو يمثل استخدام الفضاء الالكترونى كاداة لالحاق الضرر بالبنية التحتية للدول سواء كانت طاقة او خدمات حكومية او منشأت سيادية ، فهى هجمات تستخدم ضد الاقتصاد والحكومات باهداف أغلبها سياسية من اجل تدمير نظم المعلومات لدى الخصم وإفقاده القدرة على التواصل مع اعضائه عن طريق تدمير مواقعه الالكترونية واختراق شبكات معلوماته الرسمية فى الوزارات والحكومات بغرض الحصول على معلوماته السرية . [1]

ثانيا : مخاطر الارهاب الالكترونى :

يعد الفضاء الإلكتروني عنصرَ جذب مهمًّا للتنظيمات الإرهابية على اختلاف أنواعها وتباين أفكارها، نظرًا لما يتيحه لها من وسيلة إعلام عالمية هي في الوقت نفسه سلاح خطير،وتقوم هذه التنظيمات باستخدام الفضاء الالكترونى في الدعاية والتجنيد والتمويل وجمع المعلومات، وتنسيق الهجمات الإرهابية، وحشد المتعاطفين من مختلِف دول العالم. [2]

بالاضافة الى سهولة استخدام الإرهاب الإلكتروني و تنفيذه من أي مكان في العالم، ولا يلزم أن يكون الفاعل في موقع العمل الإرهابي ، بل يكفى ان تتوافر على نطاق واسع وصلات الإنترنت اللازمة لتنفيذ الهجوم باستخدام أي هاتف محمول حديث.

---

(1) صباح كزيز ، الارهاب الالكتروني وانعكاساته على الامن الاجتماعي ، مجلة التراث ، جامعة زيان عاشور، الجزائر ، العدد 28 ، 2018 ، ص 295 -296

(2) السيد عوض، الجريمة في مجتمع متغير، المكتبة المصرية،الاسكندرية،2004، ص201-202

ولا تعتمد سرعة الهجَمات الإلكترونية على سرعة وصلة الإنترنت التي يستخدمها المهاجم، بل يمكن استغلال السرعة العالية لوصلة الإنترنت التي تستخدمها الحواسيب التي تتعرض للهجوم. ذلك أن (الفيروسات) وغيرها من البرمجيات المؤذية يمكن أن تنتشر بأعلى سرعة ممكنة دون الحاجة إلى مزيد من التدخل من المهاجم.

ويمكن إبقاء الأعمال المرتكبة عبر الشابِكة مجهولةَ المصدر، وغير قابلة لاقتفاء أثرها وتتبُّعها، عن طريق خِدْمات تجهيل المصدر وما شابهها من تقنيات التمويه ، كاستخدام حواسيب مسيطر عليها عن طريق القرصنة. ويضاف إلى ذلك أن وسائل الإثبات الرَّقْمية يمكن تزييفها عمدًا[1]. ويزيد من الإغراء بالإرهاب الإلكتروني انخفاضُ تكلفة الإنترنت، وكثرة الأهداف التي يمكن قصدها واختيار مهاجمتها، وكثير من تلك الأهداف قد لا يتمتع بحماية كافية.[2]

وفي ظل هذه المغرِيات سارعت مختلِف الجماعات الإرهابية والمتطرفة إلى امتلاك مواقع على (الإنترنت)، وبخاصة شبكات التواصل الاجتماعي، وبعضها يمتلك أكثر من موقع وبأكثر من لغة، من أجل التعريف بأهدافهم الفكرية والسياسية، ، ومهاجمة خصومهم من المفكرين والعلماء، ومن الحكومات والأجهزة الأمنية.

وتمكنت مجموعة من القراصنة التابعين لتنظيم داعش في السنوات الأخيرة من اختراق بعض المواقع لتشويهها، ونشر الدعاية المتطرفة ، مثل مواقع وزارة الصحة البريطانية، والشرطة الماليزية الملكية، والخطوط الجوية الماليزية، وشبكة التلفزيون الفرنسية TV5 والمحطات التابعة لها، والقيادة المركزية العسكرية الأمريكية.)

و نظرًا لعدم وجود تعريف دقيق ومتفق عليه لمفهوم الإرهاب الإلكتروني، يتداخل نوعان مختلفان من الإرهاب هما: الإرهاب الإلكتروني الخالص، والإرهاب الإلكتروني الهجين.

---

(1) صباح كزيز ، الارهاب الالكتروني وانعكاساته على الامن الاجتماعي ، مجلة التراث ، جامعة زيان عاشور، الجزائر ، العدد 28 ، 2018 ، ص 295

(2) Clay Wilson. Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. Congressional Research Service. (January 29, 2008). p.19

اولا : الإرهاب الإلكتروني الخالص

وهو ما يتعلق بالهجَمات المباشرة على البنية التحتية السيبرانية للضحية، مثل: الحواسيب والشبكات، والمعلومات المخزَّنة فيها ، لتحقيق أهداف مختلفة ، كإفساد وظائف أنظمة المعلومات، وإتلاف أو تدمير الأصول الافتراضية والمادية ، وحجب المواقع الإلكترونية ، وتعطيل الحياة اليومية باستهداف البنية التحتية التي تُدار بأجهزة حاسوبية ، كتلك المتعلقة بالمرافق الطبية، والبورصات، والنقل، والأنظمة المالية، وغير ذلك.

ثانيا : الإرهاب الإلكتروني الهجين:

ويتمثل فى استخدام الإرهابيين للفضاء الإلكتروني في مختلِف أنشطتهم، ومن أبرز نماذجه: [1]

1- الدعاية والحرب النفسية. على سبيل المثال: لتنظيم "داعش" سبعُ وكالات إعلامية، إضافة إلى 37 مكتبًا إعلاميًّا في بلدان مختلفة. ولتنظيم "القاعدة" ذراعٌ إعلامية باسم (سحاب Sahab)

2- التواصل الآمن. وذلك بهدف إرسال رسائلَ مشفرةٍ أو إخفاء المعلومات للمناقشات السرية، وتخطيط الهجمات والتنسيق لها، كما في حادثة مقتل كاهن فرنسي في نورماندي في يوليو 2016، حيث تلقى قتلتُه توجيهاتهم عبر شبكة الاتصال .

3- تجنيد أعضاء جدد. لاحظ تقريرٌ لمجموعة العمل المالي الدَّولية FATF عام 2015أن الشبِكة باتت الأداةَ الأكثر استخدامًا للتجنيد ودعم التنظيمات الإرهابية.

4- التدريب. بنشر أدلة التدريب التي تشرح كيفية شنِّ الهجَمات وتصنيع المتفجرات، في المواقع الخاصة بالتنظيمات.

5-جمع التبرعات .

6- جمع المعلومات عن الأهداف البشرية المحتملة.

---

(1) خلف ادريس الجبابسة ، الارهاب الالكتروني : متوفر على موقع :
http://www.lawjo.net/vb/showread.php?38805

بالاضافة الى العديد من المخاطر التى تمثل فى مضمونها قنابل الكترونية وعلى سبيل المثال : تعطيل الاتصالات والتشويش عليها، والتنصُّت على المكالمات، وبث معلومات مضللة، وتقليد الأصوات، وبخاصة أصوات القادة العسكريين لإصدار أوامر خطيرة، واستهداف شبكات الحاسوب بالتخريب عن طريق نشر (الفيروسات)، مسح الذاكرة الخاصة بالأجهزة المعادية، منع تدفق الأموال وتغيير مسار الودائع ، وايقاف محطات الكهرباء عن العمل[1]. وقد أُعدَّت لتلك المهمة قنبلةٌ إلكترونية خاصة أُطلق عليها اسمCbu 49 ، تنطلق منها عدة قنابلَ في الجوِّ تستهدف محطات الكهرباء وتؤدي إلى احتراقها وتدميرها الكامل.

وقد قدم الباحث باري كولين بحث بعنوان (مستقبل الإرهاب الإلكتروني) أُلقي في (الندوة الدَّولية السنوية الحادية عشرة لقضايا العدالة الجنائية) وتضمن البحث قائمةً بأعمال الإرهاب الإلكتروني المحتملة التي تهدد مستقبل البشرية أبرزها:[2]

- الوصول عن بُعد إلى أنظمة التحكم بمصانع الحبوب، وتغيير مستويات مكمِّلات الحديد، للإضرار بصحة المستهلكين.
- إجراء تعديلات عن بعد في معالج حليب الأطفال، للإضرار بصحة الأطفال الرضع.
- تعطيل المصارف والمعاملات المالية الدَّولية والبورصات، لإفقاد النظام الاقتصادي الثقة فيه.
- تغيير مكونات صناعة الأدوية عن بُعد لدى شركات الأدوية.
- تغيير الضغط في خطوط الغاز، وأحمال شبكات الكهرباء، مما يوقع انفجارات وحرائق مروعة.

---

(1) ربيع حسن ،سيد رفاعى ، مبادىء علمى الاجرام والعقاب ، المؤسسة الفنية للطباعة و للنشر ، القاهرة ،2001 ، ص 191-194

(2) عبد الستار عبد الرحمن ، الارهاب السبرانى – خطر يهدد العالم ، موقع التحالف الاسلامى العسكرى لمحاربة الارهاب ، فبراير ،2020 متوافر على :
https://www.imctc.org/ar/eLibrary/Articles/Pages/Articles2322020.aspx

- مهاجمة أنظمة التحكم في الحركة الجوية، وجعل طائرتين مدنيتين تتصادمان، عن طريق الولوج إلى أجهزة الاستشعار في قمرة القيادة بالطائرة، وهذا ممكن أيضًا في خطوط السكك الحديدية.

ورغم ان هذه التصورات ما زالت نظرية ، الا انه لايمكن الاستهانة بعقول الإرهابيين والاستعداد للتصدى لأى افكار قد يلجا اليها الارهابيون .[1]

وهو الامر الذى يتطلب ضرورة الاستعداد الدولى للمواجهة لمثل هذه التهديدات ، وتعود بدايات الجهود الدَّولية لمواجهة الجريمة الإلكترونية والإرهاب الرَّقْمي إلى ثلاثة عقود مضت، حين ناقش "الإنتربول" الدَّولي في عام 1981 إمكانية وضع تشريع قانوني خاص بالجريمة الإلكترونية. ومنذ ذلك الحين كان التقدم بطيئًا، لكنه أخذ في التسارع بعد انتهاء الحرب الباردة. ولعل إنشاء معهد قانون الفضاء السيبراني في جامعة جورج تاون الأمريكية عام 1995 كان مؤشرًا لإدراك المشكلة. وقد اتجهت الدول إلى تبني العديد من المبادرات على المستوى الوطني أو الثنائي أو الإقليمي أو الدَّولي، من أجل العمل على حماية البنية التحتية الكونية للمعلومات من خطر التعرض للتهديدات السيبرانية، وعملت على إيجاد أطُر تشريعية جديدة تتعامل مع تلك الظاهرة المستحدَثة بصياغة مفهوم جديد للأمن الوطني، ثم الاتجاه إلى التعاون الدَّولي.

وبدأ العالم يدرك مخاطر جرائم الإرهاب الإلكتروني ويسعى لمواجهتها والتصدي لها، بتبني إستراتيجية دَولية في مجال تأمين الفضاء الإلكتروني، عبر جملة من القوانين والمبادرات أهمها مبادرة الشراكة الدَّولية المتعددة الأطراف لمكافحة الإرهاب الإلكتروني IMPACT التي تهدف إلى حشد الجهود الدَّولية للقطاعات الحكومية والقطاع الخاص والمجتمع المدني لمواجهة التهديدات المتزايدة للإرهاب الإلكتروني، وجمع الرؤى والأفكار عن التدريب وتبادل الخبرات، وإنشاء الكثير من مواقع الإنترنت لمكافحة ذلك الإرهاب، وحماية الأمن الإلكتروني. وقد كانت تلك المواقع نقطةَ التقاء لخبراء أمن المعلومات والسياسيين؛ من أجل التباحث بشأن ماهية خطر الإرهاب الإلكتروني،

---

(1) صباح كزيز ، الارهاب الالكتروني وانعكاساته على الامن الاجتماعي ، مجلة التراث ، جامعة زيان عاشور، الجزائر ، العدد 28 ، 2018 ، ص 295 -296

وكيفية مواجهته، مثل مجموعة "SITE" للاستخبارات، التي تُعَد جهازَ استخبارات متخصصًا في رصد الإرهاب عبر الإنترنت، ودراسة المصادر الأولية للإرهابيين، ورصد أحاديثهم ومراقبة دعاياتهم.

المبحث الثانى

تكييف الهجمات السيبرانية فى القانون الدولى

ادى التوسع فى استخدام شبكات الاتصالات والتكنولوجيا المعلوماتية فى شتى المجالات وتنوع اشكال التهديدات الناجمة عنها وصورها بشكل يمثل تهديداً يواجه التنظيم الدولى المعاصر.

ولا شك ان ظهور الهجمات السيبرانية وتغيير نمط النزاع المسلح ووسائله واشخاصه قد أثار التساؤلات حول الطبيعة القانونية للهجمات السيبرانية ومدى خضوعها لمبادىء القانون الدولى العام ام القانون الدولى الانسانى ، وهو ما يستلزم فى البداية وضع تعريف محدد للهجمات السيبرانية .

عرفت الهجمات السيبرانية بانها مجموعة من الأنشطة الإلكترونية التي تتخذ من طرف سواء أكان تابعًا لدولةٍ أم يعمل لحسابها بصورةٍ مستقلة عنها في دولة ما ضد نُظم إلكترونية تابعة لدولة أخرى، يُراد منها التغلغل إلى تلك النُظم بهدف السيطرة على قوّتها الإلكترونية ومن ثم التحكم بها عن بُعد، لأجل إحداث أكبر قدر ممكن من الأضرار.

ووفقا لمبادىء (تالين) [1] بشان الحروب السيبرانية ، عرفت الهجمات السيبرانية بأنها " عمليات سيبرانية، سواء أكانت هجومية أم دفاعية، والتي يهدف من خلالها بصورةٍ معقولة التسبب بالإصابة أو وفاة الأشخاص أو الأضرار أو تدمير الأعيان والأهداف" . ووفق هذا التعريف الوارد في تلك المبادىء ، فقد اتفق معظم الفقهاء القانونيين على أنه قد يتحقق الضرر أيضًا بتوقف أحد الأعيان عن العمل ، علاوة على الضرر المادي، وليس من المهم كيف يحدث ذلك.

كما عرّفها مايكل شميت [2] على أنها" مجموعة من الإجراءات التي تتخذها الدولة للهجوم على نُظم المعلومات المعادية بهدف التأثير والإضرار بها، وفي الوقت نفسه للدفاع عن نُظم المعلومات الخاصة بالدولة المهاجمة "

وتتميز الهجمات السيبرانية بأنها تتم بواسطة شخص أو أكثر باستخدام جهاز كمبيوتر مزوّد بعددٍ كبير من الفيروسات، ويتم إرسالها إلى الهدف المراد إلحاق الضرر به، ويمكن أن يكون الضرر ماديًا أو معنويًا. وعليه، فإن الهجمات السيبرانية ليست سلاحًا تقليديًا [3]، ولا ترقى لأن تكون سلاح دمار شامل وذلك نظرًا للأضرار الناتجة عنها.

ونظرًا لأهميتها في النزاعات المسلحة، والأضرار المتوقعة من جرائها، عُقدت مباحثات بين أميركا وروسيا لوضع قيود لاستخدام هذا النوع من الأسلحة، إذ نادت أميركا بتقييده، بينما كانت روسيا مع حظره، وبالنهاية لم يتم التوصل إلى قواعد مشتركة.

---

(1) دليل تالين وهى مجموعة من المبادىء أعدها بعض الخبراء في القانون الدولي الإنساني عام 2013 أبرزهم الأستاذ مايكل شيمت بالتعاون مع حلف شمال الأطلسي، وبدعمٍ من فريق مؤلف من خبراء السيبرانية، واللجنة الدولية للصليب الأحمر والقيادة السيبرانية الأميركية الذين شاركوا في المداولات كافة

(2)Michael N Schmitt, Computer Network Attack and The Use of Force in International Law: Thoughts on a normative framework, Columbia journal of transnational law, 1998-1999, p890.

(3) يحيى ياسين سعود ، الحرب السيبرانية في ضوء قواعد القانون الدولي الانساني ، المجلة القانونية ، جامعة القاهرة ، كلية الحقوق فرع الخرطوم ، نوفمبر 2018 ، ص 85 ،86

وهى عبارة عن هجوم يتم شنه من أحد أجهزة الكمبيوتر او مجموعة من الاجهزة على جهاز كمبيوتر اخر او عدة أجهزة كمبيوتر او شبكات .
ويمكن تقسيم الهجمات السيبرانية الى نوعين هجمات يكمن الهدف من ورائها الى تعطيل جهاز الكمبيوتر المستهدف، او هجمات يكون الغرض منها الوصول الى بيانات جهاز الكمبيوتر المستهدف وربما الحصول على امتيازات المسئول عنه.

المطلب الاول

الهجمات السيبرانية فى القانون الدولى العام

- - - - - - - - - - - -

الأصل في القانون الدولي العام, هو حظر إستخدام القوة وفقا لنص المادة 2 الفقرة الرابعة من ميثاق الأمم المتحدة, والإستثناء الوارد عليها فى حق الدفاع الشرعي وفقا لنص المادة 51 من نفس الميثاق، إ ذ يعد هذا الحق من أسباب الإباحة وهو ذا طبيعة موضوعية ينصرف أثرها إلى نفي الصفة غير المشروعة عن الفعل، فتنتقل من دائرة التجريم إلى مجال الإباحة. ومعرفة ذلك تتطلب تكييف الهجمات السيبرانية فى ظل قانون الحرب ، وقانون الحرب يبحث فى الظروف التى يمكن للدول فيها اللجوء الى النزاع المسلح او استخدام القوة بشكل عام [1]،وقد اكد ميثاق الامم المتحدة على تسوية النزاعات بطرق سلمية وحظر اعمال العدوان او منع التهديد باستخدام القوة ضد اى دولة [2]

---

(1) احمد عبيس الفتلاوى ، زهراء عماد محمد ، تكييف الهجمات السيبرانية فى ضوء القانون الدولى ، مجلة الكوفة للعلوم القانونية والسياسية ، كلية القانون جامعة الكوفة ، مجلد 13 ، العدد44 ، 2020 ، ص 56

(2) ميثاق الامم المتحدة ، الفصل الاول ، المادة 2 على موقع :
www.un.org. charter-united-nation

وتشكل الهجمات السيبرانية تهديدا لمبادىء القانون الدولى التى تقوم على احترام سيادة الدول لما فيها من اختراق لمعلومات امنية وعسكرية تصنف بالسرية ، وتقوض واجبا اساسيا وهو الامتناع عن استخدام القوة او التهديد بها وذلك لاضرارها البالغة على سير عمل الحكومة او تقديم الخدمات فى الدولة التى تتعرض لمثل هذه الهجمات ، وهو ما يؤثر على فكرة سيادة الدولة ونطاقها ، فالسيادة بمعناها التقليدى هو تمتع الدولة بمباشرة سلطاتهاعلى اقليمها وتنفرد فيه باصدار القرارات السياسية والقدرة على الاحتكار الشرعى لادوات القمع فى الداخل ورفض الامتثال لأى سلطة اجنبية اخرى. [1]

وتعد الهجمات السيبرانية هى احدى التحديات الراهنة امام سيادة الدولة ، فالتغيرات التكنولوجية المتسارعة فى علوم الاتصالات والتى اصبحت لاتعترف بحدود جغرافية خلقت فضاء جديد وهو الفضاء السيبرانى [2] الذى باتت الاطراف الدولية تتنازع وتتسابق على استغلاله لمصلحتها والقيام بتطوير قدراتها الهجومية والدفاعية ضمن شكل جديد من اشكال سباقات التسلح [3]

ومع هذا التغير التكنولوجى تغير المفهوم التقليدى للسيادة من خلال ظهور مفاهيم جديدة منها ما يعرف بالسيادة الرقمية والتى تعنى" بسط الدولة سيطرتها وولايتها القضائية على الفضاء الرقمى المتمثل فى شبكات الانترنت التى تجتاز حدود الدولة وينشىء مجموعة اشخاص إفتراضية ضمن شبكات إلكترونية بعيدا عن الانتماء الوطنى " [4]

---

(1) محمد طلعت الغنيمى، الوسيط فى قانون السلام، منشأة المعارف، الاسكندرية،1993، ص317

(2) مصطفى عصام عنوس ، سيادة الدولة فى الفضاء الالكترونى ، مجلة الشريعة والقانون ، كلية الحقوق ،جامعة الامارات العربية المتحدة ، السنة 26 ، العدد51 ، يوليو 2012 ، ص 128، انظر ايضا : عمر بن يونس، المجتمع المعلوماتي ، الدار العربية للموسوعات ، بيروت ،2010 ، ص 13

(3) روبرت كناكى ، حوكمة الانترنت فى عصر انعدام الامن الالكترونى ، سلسلة الدراسات عالمية ، مركز الامارات للدراسات والبحوث الاستراتيجية ، ابوظبى ، العدد95 ،2011 ، ص 13

(4) سراب ثامر احمد ، الهجمات على شبكات الحاسوب فى القانون الدولى الانسانى ، رسالة دكتوراه ، كلية الحقوق ، جامعة النهرين ، العراق ، 2015 ، ص 101

وهنا يظهر تحدى حقيقى ، حيث لا تستطيع الدولة فرض سيطرتها على مواطنيها عن طريق الجنسية مثلاً او الاحاطة بالمفاهيم الجغرافية التقليدية بل يمتد ليشمل تغييب الهوية الوطنية .[1]ولهذا قد نجد ان مستخدمى الانترنت اى افراد الفضاء السيبرانى قد يكونوا منتمين الى مجتمعات سياسية متعددة وفى حال ارتكاب اى جريمة ضمن هذا الفضاء وقيام الدولة بتتبع مصدر الجريمة قد تنتهك فى سبيل ذلك مفهوم السيادة الوطنية اذا كان مصدر الجريمة ينتمى الى نطاق سيادة دولة اخرى[2]

ويتسم الإجرام السيبراني بالنظر لطبيعتها بطابع دولي ، لكن اختلاف التشريعات في تأسيس اختصاصها الجنائي نتيجة تعدد الأسس التي يقوم عليها هذا الاختصاص قد يؤدي إلى تنازع الاختصاص بين الدول ، فقد يحدث أن ترتكب الجريمة المعلوماتية في دول معينة ، و يكون المجرم المعلوماتي مرتكب هذه الجريمة أجنبياً ، فتخضع هذه الجريمة للاختصاص الجنائي للدولة الأولى استناداً إلى مبدأ الاقليمية ، وتخضع كذلك لاختصاص الدول الثانية على أساس مبدأ الاختصاص الشخصي في جانبه الايجابي[3] و قد تكون الجريمة المرتكبة على اقليم الدولة من الجرائم التي تهدد أمن و سلامة دولة أخرى ، فتخضع للاختصاص الجنائي الاقليمي من جهة ، و تخضع لاختصاص الدولة المجني عليها استناداً إلى مبدأ الاختصاص العيني من جهة أخرى.

وبذلك بدأت تتأثر سيادة الدول والانتماءات الوطنية فى ظل الفضاء السيبرانى ولتلافى المخاطر المستقبلية لذلك بدأت العديد من الدول فى تطوير التشريعات الوطنية لاستيعاب الجرائم التى تحدث فى نطاق إقليمها والتنسيق مع الدول الاخرى عن طريق إبرام الاتفاقيات الدولية لتنظيم الجرائم السيبرانية وتحديد الآليات الواجب اتباعها فى حال حدوث تلك الجرائم كالتوصية الصادرة من مجلس اوروبا بشان المشاكل الاجرائية

---

(1) نبيل على ، فادية حجازى ، الفجوة الرقمية رؤية عربية لمجتمع المعرفة ، سلسلة عالم المعرفة ، المجلس الوطنى للثقافة والفنون والاداب ، الكويت العدد 318 ، 2005 ص 12

(2) مصطفى عصام عنوس، سيادة الدولة فى الفضاء الالكترونى ، مرجع سابق ، ص 136-139

(3) جميل عبد الباقي الصغير ، الجوانب الاجرائية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، القاهرة ،2002 ، ص 73

المرتبطة بتكنولوجيا المعلومات واتفاقية بودابست عام 2001 [1]وبورتوكول ستراسبورغ عام 2013 والاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010 .

ويرى خبراء الامن السيبرانى فى حلف الشمال الاطلسى وجوب منع الدول من استخدام البنية التحتية السيبرانية الواقعة فى اقليمها او التى تخضع لسيطرتها الكاملة فى نشاطات تمس الحقوق السيادية للدول الاخرى .

كما تتضمن مبادىء القانون الدولى ما يبرر مسئولية بعض الدول عن الافعال الغير مشروعة دوليا بصفة استثنائية باعتبار اتخاذها يعد من قبيل التدابير المضادة التى يلجأ اليها قسراً عندما تتسبب دولة بضرر فى حق دولة اخرى ، وتستخدمها الدولة المتضررة من اجل حث الاخيرة على احترام التزاماتها ووقف السلوك الغير مشروع دولياً ، بل ويمكن لأى دولة كانت ان تتخذ تلك التدابير القانونية ضد دولة تقوم بانتهاكات من نوع خاص كانتهاكات حقوق الانسان او التزامات تجاه المجتمع الدولى وذلك ضمانا لوقف الخرق وجبراً تناله الدولة المتضررة او المستفيدة من الالتزام الذى خرق ، مع الاخذ فى الاعتبار ان المادة الثانية من ميثاق الامم المتحدة تتضمن فى الفقرة الرابعة منها على ان يمتنع على اعضاء الهيئة جميعا فى علاقاتهم الدولية من التهديد باستخدام القوة او استخدامها ضد سلامة الاراضى او الاستقلال السياسى لأية دولة او على اى وجه أخر لا يتفق مع مقاصد الامم المتحدة ، كذلك يشمل الحظر قاعدة عدم التدخل الواردة فى القانون الدولى العرفى التى تحظر من التدخل فى الشئون الداخلية للدول الاخرى .

كما اكدت محكمة العدل الدولية (ICJ) فى قضية الانشطة العسكرية وشبه العسكرية (نيكارجوا ضد الولايات المتحدة) بانه متى ما اتخذ التدخل شكل استخدام او تهديد باستخدام القوة ن فان قاعدة عدم التدخل الواردة فى القانون الدولى العرفى تتطابق مع المادة 2/ 4 من ميثاق الامم المتحدة .[2]

---

(1) اتفاقية مجلس اوروبا المتعلقة بالجريمة الالكترونية ، مجموعة المعاهدات الاوربية رقم 185 بودابست 2001

(2) تحدد المادة 51 من ميثاق الامم المتحدة ان حق الدفاع مرتبط بوجود هجوم عسكرى كشرط لتفعيل استخدام هذا الحق ، وقد استخدم هذا الحق امام محكمة العدل الدولية فى قضية نيكارجوا :

الا ان حظر استخدام القوة الوارد فى المادة 51 المشار اليها يرد عليه استثنائين **الاول** : اذا كان متعلق بموضوع السلم والامن الدوليين الواردين فى المادة 39 من الميثاق والتى تمنح مجلس الامن السلطة فى تقرير وقوع اى عمل عدائى وتحديد اذا كان هذا العمل يمثل تهديد او خرق للسلم ومن ثم يقرر الاجراءات الواجب اتخاذها لاستعادة السلم والامن الدوليين .

اما الاستثناء **الثانى** :- ويتمثل فى حق الدفاع الشرعى الواردة فى المادة 51 من الميثاق، فحق الدفاع الشرعي في القانون الدولي ينطلق من فكرة حق الدولة التي تدافع عن وجودها وإستمراريتها فى البقاء ضد كل عدوان.

وليس فى هذا الميثاق ما يضعف او ينقص من الحق الطبيعى للدول فرادى او جماعات فى الدفاع عن انفسهم اذا ما اعتدت قوة مسلحة على احد اعضاء الامم المتحدة وذلك الى ان يتخذ مجلس الامن التدابير اللازمة لحفظ السلم والامن الدوليين ، وبالتالى تشترط هذه المادة ان تكون الدول تعرضت لاعتداء مسلح ، لكن اذا اخذ الاعتداء شكل اخر من اشكال القوة فلا يكون له الحق فى الدفاع الشرعى .

ونخلص من ذلك ان طبيعة الحق في الدفاع الشرعي تتجاذب بين إتجاهان: الأول : بأن هذا الحق لم يطرأ عليه تغيير في ظل ميثاق الأمم المتحدة, فهذا الحق إرتبط في ظل القانون الدولي التقليدي بفكرة المصالح الحيوية للدول إذا ما تعارضت مع مصالح غيرها من الدول، ولو إقتضى الأمر الإعتداء على مصالح الدول الأخرى, وذلك في إطار المحافظة على حق الدولة في البقاء بإستعمال وسائل وقائية، وهنا لم يختلف نص المادة 51 من الميثاق بإقراره أنه حق طبيعي متأصل, مما يعني عدم تقييد هذا الحق فيما ذهب إتجاه آخر إلى أن هذا الحق قد تغير في ظل الميثاق الذي كرس

ICJ, Military and Paramilitary Activities in and against Nicaragua (Nicaragua. v. United States of America) icj.14(june 27) ,1986 ,p209

حظر إستخدام القوة أو التهديد بها في العلاقات الدولية، حظرا شاملا على نحو يصبح حق الدفاع الشرعي مجرد إستثناء فقط[1] ، ولا يجوز التوسيع في تفسيره.

والثانى: إذا كانت المنظمة الدولية هي التي تتولى ممثلة في مجلس الأمن إتخاذ إجراءات الأمن الجماعي لمواجهة حالات الإستخدام غير المشروع للقوة، فإن حق الدفاع الشرعي ينبغي أن ينظر إليه على أنه مكمل لنظام الأمن الجماعي، ذلك أنه إذا كان نظام الأمن الجماعي لا يستطيع منع الإعتداء أو حالات الإستخدام غير المشروع للقوة من قبل دولة ما ضد دولة أخرى فإنه لا يقبل أن يلزم الميثاق الدولة المعتدى عليها بعدم رد الإعتداء وإنتظار إجراءات الأمن الجماعي التي تتخذها المنظمة الدولية خاصة في الفترة ما بين وقوع الإعتداء وإتخاذ إجراءات القسر الجماعية وهي فترة كفيلة لإنزال الضرر بالدولة المعتدى عليها, لذا فإن حق الدفاع الشرعي أضحى في ظل الأمم المتحدة إستثناء على المبدأ العام، مما يتعين معه ألا يلجأ إليه إلا في حالة الضرورة المتمثلة في دفع الأضرار التي تترتب على الإعتداء في الفترة ما بين تحقق وقوعه فعلا وإتخاذ إجراءات الأمن الجماعي، حيث أن الضرورة تقدر بقدرها.

ومع انتشار الانشطة السيبرانية وتنوعها اثير التساؤل حول مدى امكانية استخدام الحق فى الدفاع الشرعى للدول فى مواجهة الهجمات السيبرانية او الارهاب الالكترونى فى ضوء المادة 51 من ميثاق الامم المتحدة ومتى يعد الهجوم السيبرانى هجوما مسلحا يستوجب الدفاع ؟

هناك ثلاث معايير بشأن الاعتداد بالهجوم السيبرانى كعمل مسلح :

اولا: معيار الوسيلة :

حيث تبنى انصار هذه الاتجاه معيار الوسيلة المستخدمة فى الهجوم ، وبموجب هذا النهج فان الهجوم السيبرانى بمفرده يفتقد معنى الهجوم المسلح الذى يستوجب الدفاع الشرعى الوارد فى المادة 51 من ميثاق الامم المتحدة لانه يفتقر الى الخصائص

---

(1) سامي جاد عبد الرحمن، إرهاب الدولة في إطار قواعد القانون الدولي العام، دار النهضة العربية، القاهرة، 2004, ص 202 ،203

الفيزيائية المرتبطة بالاكراه العسكرى ولا يشتمل على الاسلحة التقليدية ، وقد حددت المادة 39 من ميثاق الامم المتحدة تعريف العدوان والاعمال التى ترد عليه وان كانت على سبيل المثال وليس الحصر ، ومع ذلك يحق لمجلس الامن ان يعتبر فعل ما عدواناً حتى ولو لم يرد شكل هذا العدوان ضمن الاعمال المذكورة فى الفقرة الثالثة من المادة 39 من الميثاق .[1]

وعلى الرغم من سهولة تطبيق هذا المعيار نظراً لسهولة تحديد الاسلحة والقوة العسكرية الا ان هذا المعيار تغاضى عن الهجمات السيبرانية ذات القدرة الهائلة على احداث اضرار دون استخدام الاسلحة التقليدية .

ثانيا : معيار الاهداف :

ويذهب انصار هذا المعيار الى ان تصنيف الهجوم يتوقف على تحقيق الاهداف منه، حيث يكفى ان يهدف الهجوم السيبرانى نظاماً الكترونيا مهما للغاية لكى يصنف هجوماً مسلحاً وعلى سبيل المثال الهجوم على البنية التحتية لدولة ما للسيطرة على النظم المصرفية فيها .

وقد انتقد هذا المعيار بسبب تجاهله لمفهوم البنية التحتية المتعددة الاغراض .

ثالثا : معيار الاثار الناجمة :

ويذهب انصار هذا المعيار الى تصنيف الهجوم السيبرانى على اساس خطورة اثاره ويروا ان كل نشاط مشبوه يمكن معاقبته وفقا لاثاره على الدول الاخرى ، فالتأثير على نظم الملاحة فى دولة ما قد يسبب حوادث طيران فبذلك يعد هجوما مسلحاً .

وتأسيسا على ما تقدم فان الهجمات السيبرانية متى كانت اثارها شبيهة بأثار الهجوم المسلح التقليدى من حيث الاصابات والاضرار المادية والمعنوية فانه يتم تكييفها كاستخدام للقوة المسلحة وبالتالى للدول المتضررة اللجوء الى استخدام حقها فى الدفاع عن أمنها.

---

(1) بدر محمد هلال ، جريمة العدوان في القانون الدولي ، كلية الدراسات العليا ، جامعة ال البيت ، الاردن ، 2012 ،ص 12

اما عن تكييف الهجمات السيبرانية اثناء الحروب ، عن طريق استخدام تلك الهجمات فى استفزاز الطرف الاخر او لتمهيد الطريق للهجوم التقليدى بهدف تحقيق التفوق والميزة العسكرية [1] فقد افادت اللجنة الدولية للصليب الاحمر عام 2011 الى ان توظيف الهجمات السيبرانية فى النزاع المسلح لابد ان يتوافق مع جميع مبادىء القانون الدولى الانسانى وقواعده ، كما هو الحال مع اى سلاح او وسيلة تقليدية ، وايدت ذلك محكمة العدل الدولية بان مبادىء وقواعد القانون الدولى الانسانى المنطبق على النزاعات المسلحة تنطبق كذلك على جميع اشكال الحروب وعلى جميع الاسلحة بما فى ذلك المستقبلية.

المطلب الثانى

الطبيعة القانونية للهجمات السيبرانية فى القانون الدولى الانسانى

ترتب الفجوة التكنولوجية والتقنية المتزايدة تحديات كبيرة بين مختلف الدول وبخاصةٍ على صعيد القانون الدولي الإنساني، من حيث الطبيعة القانونية للهجمات السيبرانية في هذا القانون، ومدى إمكانية تطبيق مبادئه وقواعده على هذا الشكل الجديد من الحروب في ظل وجود فراغ قانوني وعدم وجود قواعد قانونية محددة تُنظّم الهجمات السيبرانية

وتطور وسائل وأساليب الحروب الجديدة امر لم يكن بعيد عن التوقع ، فالمادة 36 من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف نصت على ما يأتي " يلتزم أي طرف سامٍ متعاقد، عند دراسة سلاح جديد أو تطويره أو اقتنائه أو أداة حرب أو اتّباع أسلوب للحرب، بأن يتحقق مما إذا كان ذلك محظورًا في الأحوال كافة أو في بعضها بمقتضى هذا الملحق البروتوكول أو أي قاعدة أخرى من قواعد القانون الدولي

---

(1) مايكل .ن.شميث ، الحرب بواسطة شبكات الاتصال ، الهجوم على شبكات الحاسوب ، القانون فى الحرب ، المجلة الدولية للصليب الاحمر ، مختارات من الاعداد 2002 ، ص90-94

التي يلتزم بها ذلك الطرف السامي المتعاقد». وبالتالي، تضع هذه المادة الإطار العام لاستخدام وسائل وأساليب قتال جديدة في النزاعات المسلحة.

وتبين أحكام هذه المادة أنه على ضوء قانون الحرب، يتعيّن على الدول التي تقتني أسلحة حديثة أو تطوّرها أن تحدد مشروعية استعمالها. كما يفيد هذا النص ضمنيًا أن كل قواعد قانون الحرب تكون قابلة للتطبيق على وسائل القتال الحديثة وأساليبها، ففي حال غياب النص الخاص يطبّق النص العام، هذا من حيث المبدأ. وفي المقابل، فإن المادة 36 من البروتوكول الإضافي الأول لا تحرّم تطوير، أو اقتناء أسلحة حديثة أو حتى حيازة أسلحة أو اعتماد أساليب جديدة غير منظمة بقواعد القانون الدولي الإنساني [1]، ومن هذا المنطلق فإن أحكام هذه المادة لا توقف حق الدول في ذلك، وإنما تنص على ضرورة المراجعة القانونية عند اقتناء أسلحة من نوع جديد أو تطويرها أو أسلوب حديث أو ما يعرف بالمطابقة القانونية مع قواعد القانون الدولي وذلك قبل استعمالها، ومن ثم لا يعد هذا النص قانونًا جديدًا ولكنه يقنّن القاعدة القانونية العرفية في التزام الدول بتطبيق معاهدة أو قاعدة عرفية بنيّةٍ حسنة

ويعتبر اللجوء المتزايد للدول في استخدام الفضاء الإلكتروني لشن هجمات سيبرانية ، جعل مبادئ القانون الدولي الإنساني وقواعده أمام اختبار حقيقي ومعقد حول إمكانية تطبيق قواعده على هذا النوع الجديد من الحروب، ذلك لأن الفترة التي جرى فيها تقنين قواعد قانونية ذات الصلة بوسائل القتال وأساليبه، لا سيما اتفاقيات لاهاي لعام 1899-1907، واتفاقيات جنيف الأربعة لعام 1949 والبروتوكولان الإضافيان لعام 1977، حينها لم يكن للهجمات السيبرانية عند إبرامها أي وجود يُذكر، ما يعني أنها لم تُقنّن بأحكامٍ خاصة تنظّم استعمالها من الناحية القانونية.

وفي إطار تطبيق مبدأ التمييز بين المقاتلين والمدنيين على الهجمات السيبرانية او الحروب الالكترونية فقد أشارت مبادىء تالين، على الرغم من عدم إلزامية قواعده،

---

(1) محمد عبد الحق شربال ، الاسلحة الحديثة والقانون الدولي الانساني، رسالة ماجستير، كلية الحقوق ،جامعة بن يوسف ، الجزائر ،2012 ، ص 14

بأنه لا يجوز أن تكون الأعيان المدنية هدفًا للهجمات السيبرانية ، فلا يجوز على سبيل المثال توجيه الهجمات السيبرانية التي من شأنها تدمير الأنظمة المدنية والبنية التحتية، ما لم تعد هذه الأنظمة من قبيل الأهداف العسكرية التي يجوز استهدافها وفق الظروف السائدة[1]

لكن فى حقيقة الامر ان تطبيق مبدأ التمييز بين المقاتلين والمدنيين على الهجمات السيبرانية هو أمر في غاية التعقيد، إذ إن المهاجم في الأغلب يكون بعيدًا عن مكان الهجوم ما يجعل التأكد من الالتزام به أمرًا غاية في الصعوبة.[2]

ويرى خبراء الامن انه من الصعب توجيه هجوم سيبراني الى هدف عسكري فى دولة ما دون ان يمتد اثره على كافة جوانب الامن القومى لهذه الدولة ،حيث يتميز الفضاء السيبراني بالارتباط بين نُظم الحواسيب، ويتألف هذا الفضاء من عدد لا يحصى من نُظم الحواسيب المتصلة بعضها ببعض في أرجاء العالم. وغالبًا ما يبدو أن نُظم الحواسيب العسكرية تتصل بالنُظم التجارية والمدنية وتعتمد عليها كليًا أو جزئيًا. وبالتالي, قد يكون من المستحيل شن هجوم سيبراني على بنية تحتية عسكرية وجعل الآثار تقتصر على هدف عسكري فحسب. فإذا تم توجيه هجمات سيبرانية ضد بنية تحتية تُستخدم للاستعمال المزدوج المدني و العسكري وعن بُعد، فلا يبدو أن الميزة العسكرية الملموسة والمباشرة ستكون واضحة، ما يجعل تطبيق مبدأ التناسب في أثناء الهجمات السيبرانية أمرًا معقدًا عمليًا[3]. ومن المسلّم به أن أيًا من الأعيان المدنية التي

---

(1)مايكل شميدت، الحرب بواسطة شبكات الاتصال- الهجوم على شبكات الكمبيوتر والقانون في الحرب، المجلة الدولية للصليب الأحمر، 2002، ص 105.

(2) أحمد عبيس الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، جامعة بابل – كلية القانون العدد الرابع، السنة الثامنة، 2016، ص 642 .

(3) احمد الانور ، قواعد وسلوك القتال ، دراسات في القانون الدولي الانساني ،دار المستقبل العربى، القاهرة ، 2000 ، ص 319

تُستخدم لأغراضٍ عسكرية تصبح هدفًا عسكريًا، وبالتالي لا تتوافر لها الحماية بموجب القانون الدولي الإنساني.

وتكمن المشكلة بوجود العديد من البنى التحتية الإلكترونية الحالية ذات استخدام مزدوج بطبيعتها، ولن يتغير هذا في المستقبل. على سبيل المثال، يمكن مد شبكة الاتصالات العسكرية جزئيًا عبر الكابلات مع وسائط أخرى تُستخدم أيضًا لحركة المرور المدنية. غالبًا ما تعتمد الأسلحة على البيانات الناتجة عن نظام تحديد المواقع العالمي GPS، والذي يخدم أغراضًا مدنية مثل الملاحة. كما أنه تم استخدام وسائل التواصل الاجتماعي كمنصات للهجوم على الدول او لاستخدامها فى الارهاب الالكترونى او للحشد والتجنيد او لاثارة الفوضى .

ومع يتزايد الاعتماد العسكري على البنية التحتية الإلكترونية المدنية، وذلك للحفاظ على القوات التابعة لدولةٍ ما وقدراتها العسكرية في مواجهة تراجع الميزانيات. سيكون من الصعب تمويل صيانة شبكات إلكترونية منفصلة أو شراء منتجات مصممة خصيصًا للأغراض العسكرية. هذا الواقع سيضع الدول أمام مشكلة فمن ناحية، سيرغبون في حرمان أعدائهم من استخدام البنية التحتية الإلكترونية ذات الاستخدام المزدوج، ومن ناحية أخرى، سترغب الدول في تحصين البنية التحتية الإلكترونية التي يعتمد عليها سكانها المدنيون وأنشطتها. [1]

وبناء على ذلك فان القانون الدولى الانسانى ينطبق على الهجمات السيبرانية التى تحدث اثناء نزاع مسلح قائم .

([1])Michael N.Schmidt, The Law of Cyber Warfare, Stanford Law & Policy Review, Vol. 25:269,p.29

المبحث الثالث

الجهود الدولية في التصدى للارهاب الالكترونى

- - - - - - - - - - -

ادركت الدول والمنظمات الدولية اهمية التعاون الدولى فى صد الهجمت الالكترونية وجرائمها فعمدت الى عقد الكثير من الاتفاقيات لتسهيل مهمة التحقيق فى الهجمات السيبرانية والارهاب الالكترونى. [1]

وتعمل عدد من المنظمات الدولية باستمرار لمواكبة التطورات في شأن أمن الفضاء الإلكتروني وقد أسّست مجموعات عمل لوضع استراتيجيات لمكافحة جرائم الإنترنت. ويستخدم مصطلح «الأمن السيبراني» لتلخيص أنشطة مختلفة كجمع المعلومات ووضع السياسات العامة والتدابير الأمنية، والمبادئ التوجيهية، وطرق إدارة المخاطر، والحماية، والتدريب، ودليل لأفضل الممارسات المهنية، ومختلف التقنيات التي يمكن استخدامها لحماية شبكة الإنترنت. وتشمل هذه السياسات المعلومات وأجهزة الكمبيوتر، والأفراد، والبنية التحتية، وبرامج المعلوماتية، والخدمات، ونظم الاتصالات السلكية واللاسلكية، ومجمل المعلومات المنقولة أو المخزنة في الاجهزة الإلكترونية وذلك لضمان تحقيق سلامة المؤسسات والأفراد في مواجهة المخاطر الأمنية وكل ما يتعلق بشبكة الانترنت [2]

وقد اعربت الدول الأعضاء فى منظمة الامم المتحدة ، في الاستعراض السادس للاستراتيجية العالمية لمكافحة الإرهاب (A/RES/72/284)، عن قلقها إزاء تزايد استخدام الإرهابيين تكنولوجيات المعلومات والاتصالات، وبخاصة شبكة الإنترنت وغيرها من الوسائط، واستخدام هذه التكنولوجيات لارتكاب الأعمال الإرهابية أو

---

(1) محمد الأمين البشرى ، التحقيق في جرائم الحاسب الالى ، ورقة بحثية فى مؤتمر " القانون والكمبيوتر والانترنت، كلية الشريعة والقانون ، الامارات، خلال الفترة 1-3 مايو 2000، ص 1078

(2) United Nations Conference on Trade and Development, Information Economy Report 2005 ,UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at :http://www.unctad.org

التحريض عليها أو التجنيد لها أو تمويلها أو التخطيط لها. ولاحظت الدول الأعضاء كذلك أهمية التعاون بين أصحاب المصلحة في تنفيذ الاستراتيجية، بما في ذلك التعاون بين الدول الأعضاء والمنظمات الدولية والإقليمية ودون الإقليمية والقطاع الخاص والمجتمع المدني.

كما اهاب مجلس الامن فى القرار رقم 2341 لسنة 2017 بالدول الأعضاء إلى "إنشاء أو تعزيز الشراكات الوطنية والإقليمية والدولية مع الجهات صاحبة المصلحة من القطاعين العام والخاص، حسب الاقتضاء، لتبادل المعلومات والخبرات من أجل منع الهجمات الإرهابية على الهياكل الأساسية الحيوية والحماية منها والتخفيف من آثارها والتحقيق فيها ومواجهتها والتعافي من أضرارها، وذلك بوسائل منها التدريب المشترك واستخدام أو إنشاء شبكات ملائمة للاتصال والإنذار في حالات الطوارئ". لذلك عمدت الكثير من المنظمات الدولية الى عقد الاتفاقيات لمواجهة تلك التحديات والممارسات العدائية .

المطلب الاول

جهود المنظمات الدولية

مع هذا التطور التكنولوجى الهائل فى كافة المجالات كان لابد من التعاون الدولى فى تنظيم التشريعات والاجراءات الوطنية فى مواجهة الهجمات الالكترونية و إيجاد آلية عمل محددة والزامية تتناسب مع الاطار الدولى العام لذا أسست منظمات وهيئات دولية تهدف الى وضع مخطاطات لتعزيز الأمن السيبراني العالمي

اولا : منظمة الأمم المتحدة :

تلعب العديد من المنظمات وعلى رأسهم منظمة الامم المتحدة دورا هاما فى تعزيز العمل المشترك بين الدول للحد من انتشار الجرائم المعلوماتية ومواجهة الارهاب الالكترونى وعقدت فى سبيل ذلك العديد من المؤتمرات بداية من المؤتمر السابع الذى عقد فى ميلانو 1985 حتى المؤتمر الثانى عشر فى 2010 بالاضافة الى المؤتمر

الخامس عشر للجمعية الدولية لقانون العقوبات والذى عقد تحت اشراف الامم المتحدة فى عام 1994 ونتج عنه عدة توصيات ذات صلة بجرائم المعلومات بعضها تناول الافعال التى تقع تحت طائلة الاجرام المعلوماتى ، والبعض الاخر اجرائى يتمثل فى الاجراءات الواجب اتباعها لتطبيق القواعد الموضوعية

ويعتبر مؤتمر الأمم المتحدة السابع لمنع الجريمة ومعاملة المجرمين الذي تم انعقاده مدين ميلانو بإيطاليا في سنة 1985 م، والذى كلف الخبراء العشرين بدراسة موضوع حماية نظم المعالجة الآلية والاعتداء على الحاسب الآلى واعداد تقرير عن ذلك.

وقد انبثق عن هذا المؤتمر مجموعة من القواعد التوجيهية والتي توجت بالمصادقة على هذه المبادئ في المؤتمر الثانى بهافانا بكوبا عام 1990[1] فقد أكد هذا المؤتمر على وجوب تطبيق التطورات الجديدة في مجال العلم والتكنولوجيا فى كل مكان لصالح الشعوب ، وبالتالي لمنع الجريمة على نحو فعال ، كما أكد على أن التكنولوجيا بما أنها قد تولد أشكالا جديدة من الجريمة فإنه ينبغي اتخاذ تدابير ملائمة ضد حالات إساءة استعمال المخلة لهذه التكنولوجيا، وأشاروا إلى مسألة الخصوصية التي يمكن أن تخترق عن طريق الإطلاع على البيانات الشخصية المخزنة داخل نظم الحسابات الآلية والتي تشكل انتهاكا لحقوق الإنسان واعتداء على حرمة الحياة الخاصة ، كما أكد المؤتمر على وجوب اعتماد ضمانات ملائمة لحفظ السرية ، كذلك أكد المؤتمر عبر قواعده التوجيهية على ضرورة تشجيع التشريعات الحديثة التي تجرم وتتناول جرائم الحاسب الآلي باعتبارها نمطا من أنماط الجريمة المنظمة كغسيل الأموال والاحتيال المنظم وفتح حسابات وتشغيلها بأسماء وهمية ، وقد اقر مؤتمر هافانا 1990 عدة مبادىء اهمها تحديث القوانين الجنائية الوطنية بما في ذلك التدابير المؤسساتية ، وتحسين أمن الحاسب الآلي والتدابير الفنية اعتماد إجراءات تدريب كافية للموظفين والوكالات المسئولة عن منع الجريمة الاقتصادية والجرائم المتعلقة بالحاسب الآلي

---

(1) محمد الأمين ، محسن عبد الحميد أحمد ، معايير الأمم المتحدة في مجال العدالة الجنائية ومنع الجريمة ، أكاديمية نايف العربية للعلوم الأمنية ، الرياض، الطبعة الأولى 1998، ص 19.

والتحري والإدعاء فيها، تلقين آداب الحاسب الآلي كجزء من مفردات مقررات الاتصالات والمعلومات ، وزيادة التعاون الدولي من أجل مكافحة هذه الجرائم .

وتواصلت جهود الأمم المتحدة عبر عقد عدة مؤتمرات أهمها المؤتمر التاسع لمنع الجريمة ومعاملة المجرمين والذي عقد في القاهرة عام 1995 ، والذى اوصى بضرورة حماية حياة الإنسان الخاصة وملكيته الفكرية في مواجهة مخاطر التكنولوجيا ، والعمل على التنسيق وتعزيز التعاون بين أعضاء المجتمع الدولي لاتخاذ الإجراءات المناسبة للحد منها. كذلك اوصى المؤتمر العاشر المنعقد فى بودابست فى عام 2000 بوجوب العمل الجاد من اجل الحد من جرائم تقنية المعلومات المتزايدة والتى اعتبرت نمطا من الجرائم المستحدثة والعمل على اتخاذ التدابير المناسبة للحد من عمليات القرصنة .

ثانيا : المنظمة العالمية للملكية الفكرية :

تأسست المنظمة العالمية للملكية الفكرية " WIPO بموجب اتفاقية تم التوقيع عليها في استكهولم في 14 يوليو 1967 تحت عنوان اتفاقية "إنشاء المنظمة العالمية للملكية الفكرية ، وتعتبر هذه المنظمة إحدى الوكالات المتخصصة للأمم المتحدة ابتداء من 1974 وتدعم حماية الملكية الفكرية في كل أنحاء العالم بفضل التعاون الدولي بين أعضائها وقد شكلت بهدف دراسة الاساليب المناسبة لحماية برامج الاسب الالى من خلال اعضائها لقوانين حماية المؤلف ، ومن خلال خلقها لنصوص قانونية خاصة بحماية برامج الحاسب الالى [1]

ثالثا : الاتحاد الدولى للاتصالات :

يوفّر الاتحاد الدولي للاتصالات الذي يضم 192 دولة و700 شركة من القطاع الخاص والمؤسسات الأكاديمية منبرًا «استراتيجيا» للتعاون بين أعضائه باعتباره وكالة متخصصة داخل الأمم المتحدة. ويعمل الاتحاد على مساعدة الحكومات في الاتفاق على مبادئ مشتركة تفيد الحكومات والصناعات التي تعتمد على تكنولوجيا المعلومات

---

(1) نعيم سعدانى ، أليات البحث والتحرى عن الجريمة المعلوماتية فى القانون الجزائرى ، رسالة ماجستير ، كلية الحقوق ، جامعة حاج لخضر باتنة ، 2013 ، ص 125

والبنية التحتية للاتصالات. وقد وضع الاتحاد الدولي للاتصالات مخططًا «لتعزيز الأمن السيبراني العالمي يتكوّن من سبعة أهداف رئيسة، والأهداف السبعة هي:

- وضع استراتيجيات لتطوير نموذج التشريعات السيبرانية يكون قابلاً للتطبيق محليًا وعالميًا بالتوازي مع التدابير القانونية الوطنية والدولية المعتمدة.
- وضع استراتيجيات لتهيئة الأرضية الوطنية والإقليمية المناسبة لوضع الهيكليات التنظيمية والسياسات المتعلّقة بجرائم الانترنت.
- وضع استراتيجية لتحديد الحد الأدنى المقبول عالميًا في موضوع معايير الأمن ونظم تطبيقات البرامج والأنظمة.
- وضع استراتيجيات لوضع آلية عالمية للمراقبة والإنذار والرد المبكر مع ضمان قيام التنسيق عبر الحدود.
- وضع استراتيجيات لإنشاء نظام هوية رقمي عالمي وتطبيقه، وتحديد الهيكليات التنظيمية اللازمة لضمان الاعتراف بالوثائق الرقمية للأفراد عبر الحدود الجغرافية.
- تطوير استراتيجية عالمية لتسهيل بناء القدرات البشرية والمؤسسية لتعزيز المعرفة والدراية في مختلف القطاعات وفي جميع المجالات المعلوماتية.
- تقديم المشورة بشأن إمكانية اعتماد إطار استراتيجي عالمي لأصحاب المصلحة من أجل التعاون الدولي والحوار والتعاون والتنسيق في جميع المجالات التي سبق ذكرها[1]

(1)Schjolberg and Hubbard, «Harmonizing National Legal Approaches on Cybercrime», 2005, page 5. available at: http://www.itu.int

المطلب الثانى

الجهود العربية والاقليمية

اولا : اتفاقية المجلس الأوروبي بشأن جرائم الإنترنت

إعتمد المجلس الأوروبي الطابع الدولي لجرائم الكمبيوتر منذ العام 1976 ، وفي العام 1996، أنشأت اللجنة الأوروبية لمشاكل الجريمة (CDPC) لجنة خبراء للتعامل مع مشكلة الجريمة السيبرانية. عملت اللجنة بين العامين 1997 و2000 على مشروع الاتفاقية التي اعتمدها البرلمان الأوروبي في الجزء الثاني من جلسته العامة في شهر نيسان/أبريل 2001. وتم التصديق على الاتفاقية من قبل 30 دولة بحلول العام 2010.

إن إتفاقية جرائم الانترنت هي المعاهدة الدولية الأولى التي تسعى لمعالجة الجرائم المتعلقة بالكمبيوتر والإنترنت عبر التنسيق بين القوانين الوطنية وقوانين الدول الأخرى. وتهدف الاتفاقية إلى:[1]

- توحيد عناصر القانون الجزائي المحلي مع الأحكام المتعلقة بالجرائم الإلكترونية.
- توفير الاجراءات القانونية اللازمة للتحري وملاحقة الجرائم المرتكبة الكترونيًا بواسطة الكمبيوتر.
- تعيين نظام سريع وفعال للتعاون الدولي.
- الحفاظ بشكل سريع على البيانات المخزّنة على أجهزة الكمبيوتر وحفظها والإفصاح الجزئي عن حركة هذه البيانات المخزنة على الكمبيوتر.
- جمع معلومات عن حركة البيانات وعن إمكان وجود تدخّل في محتواها.

---

(1) كرستينا سكولمان ، الاجراءات الوقائية والتعاون الدولى لمحاربة الجريمة الالكترونية ، ورقة بحثية فى الندوة الاقليمية عن الجرائم المتعلقة بالكمبيوتر ، المغرب ، 2007 ، ص 119 ،120 ،

- تتضمن أيضًا الاتفاقية المبادئ العامة المتعلّقة بالتعاون الدولي في المواضيع التالية: تسليم المجرمين، المساعدة الدولية المتبادلة، إعطاء المعلومات بصورة آلية، وإنشاء الولاية القضائية على أي جريمة.
- المساعدة المتبادلة في جمع حركة المعلومات واعتراضها.
- الإجراءات المتعلقة بطلبات المساعدة المتبادلة في غياب الاتفاقات الدولية.

ثانيا : الجهود العربية فى مكافحة الجرائم السيبرانية :

تم تأسيس المركز الاقليمى للامن السيبرانى من قبل الاتحاد الدولى للاتصالات وسلطنة عمان فى ديسمبر 2012 ، ويسعى المركز نحو انشاء بيئة اقليمية اكثر تعاوناً وامناً فى مجال الامن السيبرانى تماشياً مع اهداف الاتحاد الدولى فى تعزيز الثقة والامن فى الاستخدام التكنولوجى وتنسيق المبادرات الامنية فى مجال الامن السيبرانى فى المنطقة العربية .

كما اتجهت الدول العربية الى ارساء سبل التعاون فى مجال مكافحة جرائم الانترنت ، حيث تم وقعت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات فى القاهرة 2010 ، وتهدف الى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات ، لدرء أخطار هذه الجرائم حفاظا على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها ونصت المادة الرابعة منها على احترام سيادة الدولة والتزام كل دولة طرف وفقا لنظمها الأساسية أو لمبادئها الدستورية بتنفيذ التزاماتها الناشئة عن تطبيق هذه الاتفاقية على نحو يتفق مع مبدأي المساواة في السيادة الإقليمية للدول وعدم التدخل في الشؤون الداخلية للدول الأخرى. [1]

كذلك ليس في هذه الاتفاقية ما يبيح لدولة طرف أن تقوم في إقليم دولة أخرى بممارسة الولاية القضائية وأداء الوظائف التي يناط أداؤها حصرا بسلطات تلك الدولة الأخرى بمقتضى قانونها الداخلي .

وفى فبراير 2014 عقدت جامعة الدول العربية ورشة عمل عن التعاون الدولى فى مكافحة الجريمة المنظمة العبرة للحدود الوطنية ، واكدت على ضروة التعاون على

---

(1) صباح كزيز ، الارهاب الالكتروني وانعكساته على الامن الاجتماعي ، مرجع سابق ، ص 303

المستوى الاقليمى لمواجهة خطورة الجريمة المنظمة لارتباطها بعمليات تمويل الارهاب ، كذلك ضرورة تفعيل قرار قمة بغداد 2012 الخاص بإنشاء شبكة تعاون قضائى عربى فى مكافحة الارهاب والجريمة المنظمة لتعزيز التعاون الدولى والاقليمى فى المجال القضائى.

ثالثا : الموقف المصرى فى مكافحة الجرائم السيبرانية :

شهدت مصر حراك قوى فى مجال الامن السيبرانى والذى تجسد فى انضمامها الى الاتفاقية العربية لمكافحة جرائم الانترنت والارهاب الالكترونى ، كما قامت مصر بإنشاء المجلس الاعلى للامن السيبرانى للحد من اثار اختراق امن المعلومات على الامن القومى للدول وتأمين الخدمات الالكترونية ومواجهة مخاطر استهداف البنية التحتية للجهات الحكومية .

ولقد نص دستور 2014 فى المادة 31 منه على ان " أمن الفضاء المعلوماتى جزء اساسى من منظومة الاقتصاد والامن القومى ،وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه وعلى النحو الذى ينظمه القانون "

ولقد بدأت مصر بإتباع بعض الأليات لتقليص مخاطر الهجمات السيبرانية ، فأطلقت استراتيجية موحدة فى مجال الامن السيبرانى بعنوان "الامن السيبرانى أفاق وتحديات " وذلك على هامش المؤتمر السنوى لتطوير الصناعة فى 2015 ن وركزت الاستراتيجية على سبل تامين شبكات البنية التحتية وتطبيقات التحكم الصناعى وتامين الخدمات الالكترونية .[1] هذا وقد تم تشكيل المجلس الاعلى للامن السيبرانى فى مصر فى ديسمبر 2014 لحماية البيانات والمعلومات لدى الجهات الحكومية والتاكد من توفير التمويل اللازم لضمان تنفيذ منظومة حماية الامن السيبرانى .

كما نظمت مصر المؤتمر الاقليمى الخامس للامن السيبرانى الذى انعقد فى شرم الشيخ نوفمبر 2016 ونظمه المركز العربى الاقليمى للامن السيبرانى تحت شعار (تعاون

---

(1) احمد جلال محمود ، اثر التهديدات الغير تقليدية للامن على العلاقات الدولية المعاصرة ، مؤتمر الامن السيبرانى فى الشرق الاوسط ، مركز بحوث الشرق الاوسط والدراسات المستقبلية ، جامعة عين شمس ، 2020 ، ص 70 ،71

بلا حدود) بهدف تعزيز التعاون الاقليمى فى هذا المجال ، كما استضافت مصر منتدى فرست الاقليمى للمنطقة العربية والافريقية فى 2016 للتاكيد على اهمية تبادل الخبرات والتعاون مع المنظمات الدولية ذات الصلة لمواجهة الاخطار السيبرانية

وقد وقعت مصر فى 2017 اتفاقية التعاون بين المعهد القومى للاتصالات التابع لوزارة الاتصالات وتكنولوجيا المعلومات وشركة سيسكو العالمية بهدف اطلاق اول اكاديمية للامن السيبرانى تهدف الى تثقيف وتطبيق المهارات اللازمة لمواجهة تحديات الامن السيبرانى .

ونخلص من ذلك اتجاه مصر نحو تحقيق الامن السيبرانى من خلال التنسيق والتعاون مع الجهات الاقليمية والدولية ومن خلال انضمامها للاتفاقيات الدولية فى مجال التصدى لجرائم الارهاب الالكترونى وذلك للاستفادة من الخبرات الدولية فى مجال الامن السيبرانى .

كما شاركت مصر فى مؤتمر المنطقة المركزية للاتصالات بواشنطن فى ابريل 2017 عن الاستجابة للحوادث التى تهدد الامن السيبرانى .

ومما تقدم يمكن التوصل الى النتائج الاتية :

1- ان الجريمة السيبرانية تتمثل فى الافعال الغير قانونية باستخدام الحاسب الالى كوسيلة او هدف .
2- الجريمة السيبرانية خطر يتعين التصدى له بتوعية وتثقيف الافراد عن الفضاء السيبرانى وبالتدابير الوقائية الكفيلة بتقليل خطر الوقوع فى مسار الجريمة الالكترونية .
3- الهجمات السيبرانية ساحة جديدة للحروب بعيداً عن المواجهات العسكرية والتقليدية .
4- تطور مفهوم الامن القومى تجاه التهديدات المستحدثة والغير تقليدية واتساع مجاله ليمتد الى المجال العسكرى .
5- اوجد الانترنت فضاءً عاماً جديدا يتجاوز الحدود الجغرافية وساحة لدعم الارهاب والتجنيد والتمويل .

6- عدم اعتراف بعض الدول علانياً بوجود الحروب السيبرانية خشية ان يتطلب الاعتراف اتخاذ مواقف انتقامية او اجراءات متصاعدة الرد.
7- بعض العمليات السيبرانية المعادية لاتعد ضمن العمليات العسكرية المعادية بوصفها المذكور فى المادة 51 من ميثاق الامم المتحدة .
8- لابد من مراعاة مبدا التناسب عند استخدام حق الدفاع الشرعى

وبناء على ما سبق يوصى البحث بما يلى :

1- ضرورة تشديد اجراءات الرقابة على مستعملى الفضاء الالكترونى واتخاذ اجراءات ردعية وفرض قوانين صارمة علي مستخدميها .
2- ضرورة ادراج مجال الفضاء السيبرانى ضمن مناهج التعليم فى جميع مراحله للتوعية بخطورة الاستخدام الخاطىء لوسائل الاتصالات وتكنولوجيا المعلومات.
3- ضرورة عقد دورات تدريبية لتوعية الافراد و العاملين بالمؤسسات الحكومية لقواعد استخدام المعلومات والبيانات وتنمية مهاراتهم الاحترافية .
4- عقد بروتوكولات تعاون بين المؤسسات الحكومية داخل الدولة وتبادل الخبرات بين الخبراء المدنيين و العسكريين لمتابعة المستجدات على الفضاء السيبرانى والاستعدادت الوقائية لمواجهة كل ماهو جديد فى هذا المجال .

الخاتمة :

مع تطور التكنولوجيا في وسائل القتال وأساليبه، وبخاصةٍ المستعملة في النموذج الجديد من الحروب كالحرب السيبرانية، التي حلت في صدارة الدراسات القانونية المتخصصة، مقارنة مع القضايا الدولية الأخرى المهددة للسلم والأمن الدوليَين، برزت تحديات كبيرة على صعيد القانون الدولي العام وعلى صعيد القانون الدولي الإنساني خصوصًا، باعتباره القانون الذي يُنظّم وسائل القتال وأساليبه خلال النزاعات المسلحة.

وحيث ان مفهوم الهجمات السيبرانية في النظام القانوني الدولي، لا يزال غير متفق عليه دوليًا، ما يستدعي تعاون الجهود الفقهية لتحديده باعتباره الركيزة الأساسية لأي اتفاقية تقنّن استخدامه مستقبلًا أو تنظّمه. أما أبرز المعضلات التي تؤخّر الجهود الدولية من تقنين هذا النوع الجديد من وسائل القتال وأساليبه، هو انعدام الثقة بين الدول ، إلا أن إبرام الاتفاقية في هذا الشأن في المستقبل، سيعني تحريك المسؤولية الجنائية الفردية عن دعم أي مجموعات مسلحة يمكن أن تستخدم الوسائل الإلكترونية للأغراض غير العسكرية تجاه دول أخرى أو تدريبها أو تمويلها.

ونظرًا لأن الأنشطة السيبرانية أصبحت مركزية أكثر من أي وقت مضى في تنظيم المجتمعات الحديثة، من المرجح أن تتكيّف هذه الأنشطة مع القانون من خلال تقنينها في اتفاقية خاصة لمنحه حماية أكبر لهذه المجتمعات، إذ ستفرض التزامات على الدول للتصرف بصفتها مسئولة عن حماية الفضاء السيبراني، وتقليل النقطة التي تنتهك فيها العمليات الإلكترونية الحظر المفروض على استخدام القوة ، والسماح للدول بالرد بقوةٍ على بعض العمليات السيبرانية غير المدمرة، وتعزيز حماية البنية التحتية السيبرانية والبيانات والأنشطة خلال النزاعات المسلحة لذا فان المصالح الوطنية. تقتضى اتخاذ التدابير الوقائية لحماية وصولها الآمن إلى الفضاء السيبراني والخدمات التي يمنحها.

الملخص:

فى ظل التقدم الهائل فى علم البرمجيات والتقنية المتسارعة فى النظم المعلوماتية ، ومع تزايد الاعتماد على الحواسب الآلية والشبكات المعلوماتية ظهر ما يسمى الجرائم الالكترونية والتى يطلق عليها " **الجرائم السيبرانية**" والتى تعد من أخطر التحديات التى تواجه المعاملات الالكترونية .

وبالرغم من الاثار الايجابية للتطور التكنولوجى الا ان اختراق الانترنت للحدود وظهور العوالم الافتراضية العابرة للحدود نتج عنه ما يسمى " **بالارهاب الالكترونى** "، فلم تعد الجريمة الالكترونية تتمركز فى دولة او مجتمع معين بل اصبحت تهدد امن واستقرار العديد من الدول خاصة مع صعوبة اكتشاف تلك الجرائم واثباتها ، وهو الامر الذى يتطلب معه تضافر الجهود الدولية فى التصدى لمثل هذه الجرائم .

وقد مهدت ثورة المعلومات والقدرة على استخدام التكنولوجيا الى بروز اشكال جديدة ومتنوعة من القوة الإلكترونية ، والتي أصبح لها انعكاس مباشر على المستوى المحلي والدولي، فمن ناحية أدت إلى إعادة توزيع القوة وانتشارها بين أكبر عدد من الفاعلين، وهذا ما جعل قدرة الدولة في السيطرة على هذا المجال موضوع شك مقارنة بالمجالات الأخرى للقوة.

ومن ناحية أخرى جعلت القوة الإلكترونية بعض الدول الأصغر في السياسة الدولية لديهم قدرة أكبر على ممارسة القوة الصلبة والناعمة عبر استراتيجية جديدة تمثل "القوة الإلكترونية" مصدرها ، وهذا ما يعني تغييراً في علاقات القوى في السياسة الدولية.

واتسمت الحروب الإلكترونية بصفة تدميرية كبرى على الامن القومى للدول لما لها من قدرة على التجسس والتسلل ثم النسف بدون دخان ولا أنقاض سواء عن طريق تدمير المواقع على الإنترنت ونسفها وقصفها بوابل من الفيروسات ، أو العمل على استخدام أسلحة الفضاء الإلكتروني المتعددة للنيل من تلك المواقع ، وهي أسلحة يسهل الحصول عليها من خلال مواقع الإنترنت أيضاً ، ولذلك فان تداعيات هذا النوع من الحروب تكون خطيرة على الامن القومى للدول .

اثبت الواقع العملى ان الدولة لا تستطيع بجهودها المنفردة مواجهة تلك الجرائم المستحدثة مع هذا التطور المستمر فى كافة ميادين الاتصالات وتكنولوجيا المعلومات ، ونظرا لما تشكله ظاهرة الارهاب الالكترونى من أهمية أمنية وقانونية تمس الامن القومى للدول ومواجهتها تتطلب الوقوف ضرورة الوقوف على مفهوم الارهاب الالكترونى ومخاطره وسبل مواجهتها واتخاذ كافة التدابير المضادة تجاهها .

وهو الامر الذى يتطلب ضرورة الاستعداد الدولى للمواجهة لمثل هذه التهديدات ، وتعود بدايات الجهود الدَّولية لمواجهة الجريمة الإلكترونية والإرهاب الرَّقْمي إلى ثلاثة عقود مضت، حين ناقش "الإنتربول" الدَّولي في عام 1981 إمكانية وضع تشريع قانوني خاص بالجريمة الإلكترونية. ومنذ ذلك الحين كان التقدم بطيئًا، لكنه أخذ في التسارع بعد انتهاء الحرب الباردة. ولعل إنشاء معهد قانون الفضاء السيبراني في جامعة جورج تاون الأمريكية عام 1995 كان مؤشرًا لإدراك المشكلة. وقد اتجهت الدول إلى تبني العديد من المبادرات على المستوى الوطني أو الثنائي أو الإقليمي أو الدَّولي، من أجل العمل على حماية البنية التحتية الكونية للمعلومات من خطر التعرض للتهديدات السيبرانية، وعملت على إيجاد أطُر تشريعية جديدة تتعامل مع تلك الظاهرة المستحدَثة بصياغة مفهوم جديد للأمن الوطني، ثم الاتجاه إلى التعاون الدَّولي.

حيث تشكل الهجمات السيبرانية تهديدا لمبادىء القانون الدولى التى تقوم على احترام سيادة الدول لما فيها من اختراق لمعلومات امنية وعسكرية تصنف بالسرية ، وتقوض واجبا اساسيا وهو الامتناع عن استخدام القوة او التهديد بها وذلك لاضرارها البالغة على سير عمل الحكومة او تقديم الخدمات فى الدولة التى تتعرض لمثل هذه الهجمات ، وهو ما يؤثر على فكرة سيادة الدولة ونطاقها ، فالسيادة بمعناها التقليدى هو تمتع الدولة بمباشرة سلطاتها على اقليمها وتنفرد فيه باصدار القرارات السياسية والقدرة على الاحتكار الشرعى لادوات القمع فى الداخل ورفض الامتثال لأى سلطة اجنبية اخرى . ولهذا تعمل المنظمات الدولية على مواكبة التطورات في شأن أمن الفضاء الإلكتروني

وقد أسّست مجموعات عمل لوضع استراتيجيات لمكافحة جرائم الإنترنت ووضع السياسات العامة والتدابير الأمنية، والمبادئ التوجيهية، وطرق إدارة المخاطر ومختلف التقنيات التي يمكن استخدامها لحماية شبكة الإنترنت. وتشمل هذه السياسات المعلومات وأجهزة الكمبيوتر، والأفراد، والبنية التحتية، وبرامج المعلوماتية، والخدمات، ونظم الاتصالات السلكية واللاسلكية، ومجمل المعلومات المنقولة أو المخزنة في الاجهزة الإلكترونية وذلك لضمان تحقيق سلامة المؤسسات والأفراد في مواجهة المخاطر الأمنية وكل ما يتعلق بشبكة الانترنت

المراجع :

1. ابن منظور ،أبو الفضل جمال الدين محمد بن مكرم، لسان العرب ،دار صادر بيروت، 1955م / 1374 هـ
2. المعجم الوسيط، مجمع اللغة العربية، ط2، القاهرة 1972م
3. احمد الانور ، قواعد وسلوك القتال ، دراسات فى القانون الدولى الانسانى ،دار المستقبل العربى، القاهرة ، 2000
4. احمد جلال الدين ، الارهاب والعنف السياسى ، دار الحرية القاهرة ، 1989
5. احمد عبيس الفتلاوى ، زهراء عماد محمد ، تكييف الهجمات السيبرانية فى ضوء القانون الدولى ، مجلة الكوفة للعلوم القانونية والسياسية ، كلية القانون جامعة الكوفة ، مجلد 13 ، العدد44 ، 2020
6. أمل اليازجي ، محمد عزيز شكري ، الإرهاب الدولي والنظام العالمي الراهن، دار الفكر ، دمشق ،2002
7. السيد عوض ، الجريمة فى مجتمع متغير ، المكتبة المصرية ، الاسكندرية ،2004
8. الصحاح، إسماعيل بن حماد الجوهري، تحقيق أحمد عبدالغفور عطار، دار العلم للملايين، بيروت، ط2، 1975م، مادة: رهب

9. بدر محمد هلال ، جريمة العدوان فى القانون الدولى ، كلية الدراسات العليا ، جامعة ال البيت ، الاردن ، 2012
10. جميل عبد الباقي الصغير ، الجوانب الاجرائية للجرائم المتعلقة بالأنترنت، دار النهضة العربية، القاهرة ،2002
11. خلف ادريس الجبابسة ، الارهاب الالكترونى : متوفر على موقع : http://www.lawjo.net/vb/showread.php?38805
12. ربيع حسن ،سيد رفاعى ، مبادىء علمى الاجرام والعقاب ، المؤسسة الفنية للطباعة و للنشر ، القاهرة ،2001
13. روبرت كناكى ، حوكمة الانترنت فى عصر انعدام الامن الالكترونى ، سلسلة الدراسات عالمية ، مركز الامارات للدراسات والبحوث الاستراتيجية ، ابوظبى ، العدد95 ،2011
14. سامي جاد عبد الرحمن، إرهاب الدولة في إطار قواعد القانون الدولي العام، دار النهضة العربية، القاهرة، 2004
15. سامى محمد بوتيف ، دور الاستراتيجيات الاستباقية فى مواجهة الهجمات السيبرانية ، الردع السيبرانى نموذجاً ، المجلة الجزائرية للحقوق والعلوم السياسية ، مجلد 4 ، العدد 7 ، 2019
16. سراب ثامر احمد ، الهجمات على شبكات الحاسوب فى القانون الدولى الانسانى ، دكتوراه ، كلية الحقوق ، جامعة النهرين ، العراق ، 2015
17. صالح بن على بن عبد الرحمن ، الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت، هيئة الاتصالات وتقنية المعلومات ، المملكة العربية السعودية 2018
18. صباح كزيز ، الارهاب الالكترونى وانعكاساته على الامن الاجتماعى ، مجلة التراث ، جامعة زيان عاشور، الجزائر ، العدد 28 ، 2018
19. عادل عبد الصادق ، الفضاء الالكترونى وأسلحة الانتشار الشامل بين الردع وسباق التسلح ، مؤتمر حروب الفضاء السيبرانى ، هولندا ، مايو 2015 ، على موقع : https://seconf.wordpress.com/2015/05/15

20. عبد العزيز بن فهد ابم داود ، الجرائم السبرانية ، مجلة الاجتهاد للدراسات القانونية والاقتصادية ، المملكة العربية السعودية ، المجلد 9 العدد3 2020
21. عبد الرحيم صدقى ، الارهاب السياسى والقانون الجنائى ، دار النهضة العربية ، القاهرة ،1985
22. عبد الستار عبد الرحمن ، الارهاب السبرانى – خطر يهدد العالم ، موقع التحالف الاسلامى العسكرى لمحاربة الارهاب ، فبراير ،2020 متوافر على : https://www.imctc.org/ar/eLibrary/Articles/Pages/Articles2322020.aspx
23. عمر بن يونس ، المجتمع المعلوماتى ، الدار العربية للموسوعات ، بيروت ،2010
24. عنترة بن مرزوق ، محى الدين حرشاوى ، الامن السيبرانى كبعد جديد فى السياسة الجزائرية ،مجلة دفاتر السياسة والقانون ،العدد17 ،جامعة قاصدى مرباح ، 2017
25. كرستينا سكولمان ، الاجراءات الوقائية والتعاون الدولى لمحاربة الجريمة الالكترونية ، ورقة بحثية فى الندوة الاقليمية عن الجرائم المتعلقة بالكمبيوتر ، المغرب ، 2007
26. مايكل .ن.شميث ، الحرب بواسطة شبكات الاتصال ، الهجوم على شبكات الحاسوب ، القانون فى الحرب ، المجلة الدولية للصليب الاحمر ، مختارات من الاعداد 2002
27. محمد الأمين ، محسن عبد الحميد أحمد ، معايير الأمم المتحدة في مجال العدالة الجنائية ومنع الجريمة ، أكاديمية نايف العربية للعلوم الأمنية ، الرياض، الطبعة الأولى 1998
28. محمد الأمين البشرى ، التحقيق فى جرائم الحاسب الالى ، ورقة بحثية فى مؤتمر " القانون والكمبيوتر والانترنت ، كلية الشريعة والقانون ، الامارات ، خلال الفترة من 1-3 مايو 2000

29. محمد طلعت الغنيمى ، الوسيط فى قانون السلام ، منشأة المعارف ، الاسكندرية ، 1993
30. محمد عبد الحق شربال ، الاسلحة الحديثة والقانون الدولى الانسانى،ماجستير، كلية الحقوق ،جامعة بن يوسف ، الجزائر ،2012
31. محمد على رعايت ، الحرب السيبرانية وتهديد الامن القومى لجمهورية ايران الاسلامية ، دكتوراه ، كلية الاداب للعلوم الانسانية ، جامعة ازاد اسلامى ، ايران ، 2012
32. مصطفى عصام عنوس ، سيادة الدولة فى الفضاء الالكترونى ، مجلة الشريعة والقانون ، كلية الحقوق ،جامعة الامارات العربية المتحدة ، السنة 26 ، العدد51 ، يوليو 2012
33. نسرين الشحات الصباحى ، الابعاد العسكرية للقوة السيبرانية على الامن القومى للدول ، دراسة حالة اسرائيل منذ 2010 ، المركز القومى الديمقراطى ، برلين ،2016 ، على موقع :
https://democraticac.de/?p=30962
34. نعيم سعدانى ، أليات البحث والتحرى عن الجريمة المعلوماتية فى القانون الجزائرى ، ماجستير ، كلية الحقوق ، جامعة حاج لخضر باتنة ، 2013
35. يحيى ياسين سعود ، الحرب السيبرانية فى ضوء قواعد القانون الدولى الانسانى ، المجلة القانونية ، جامعة القاهرة ، كلية الحقوق فرع الخرطوم ، نوفمبر 2018
36. Clay Wilson. Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. Congressional Research Service. (January 29, 2008
37. ICJ, Military and Paramilitary Activities in and against Nicaragua (Nicaragua. v. United States of America) icj.14(june 27) ,1986 ,p209

38. James A .Lewis, Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats, Center for Strategic and International Studies, December, 2002
39. John Arquilla and David Ronfeld, RAND / In Athena's Camp: Preparing for Conflict in the Information Age ،eds.MR-880-OSD/RC(1997).
40. Joseph .S .Nye , Cyberpower (Harvard Kennedy School ,Belfer center for science and International Affairs 2010 ,Available at: http://www.Belfercenter.Ksg. Harvard .edufilescyber –power , PDF, P05
41. Longman Dictionary of English Language and Culture, London, 1993
42. Michael N Schmitt, computer network attack and the use of force in international law: Thoughts on a normative framework, Columbia journal of transnational law, 1998-1999, p890.
43. Michael N.Schmidt, the law of cyber warfare, Sanford Lw & Policy Review, Vol. 25:269,p.29
44. Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)
45. Schjolberg and Hubbard, «Harmonizing National Legal Approaches on Cybercrime», 2005, page 5. available at: http://www.itu.int
46. United Nations Conference on Trade and Development, Information Economy Report 2005 ,unctad/sdte/ecb/2005/1, 2005, Chapter 6, page 233, available at :http://www.unctad.org
47. www.un.org.>charter-united-nation

48. https://www.Itu.Int/net/Itunews/issues/2010/9/Pdf/201009_20-ar.pdf

Abstract

With the tremendous progress in software science and accelerated technology in information systems, and with the increasing reliance on computers and information networks, the so-called Cybercrime has emerged, which is called "Cybercrime", which is one of the most serious challenges facing electronic transactions. Despite the positive effects of technological development, internet penetration of borders and the emergence of virtual cross-border worlds resulted in what is called "electronic terrorism". Cybercrime is no longer concentrated in a specific country or society, but rather threatens the security and stability of many countries, especially with the difficulty of discovering and proving these crimes. Which requires concerted international efforts to deal with such crimes? The information revolution and the ability to use technology have paved the way for the emergence of new and diverse forms of electronic power, which have a direct reflection at the local and international level, on the one hand it led to the redistribution and spread of power among the largest number of actors, and this is what made the state’s ability to control this The field is in doubt compared to other fields of strength.

On the other hand, cyber power has made some smaller countries in international politics have a greater ability to exercise hard and soft power through a new strategy of "electronic power" as its source, and this means a change in power relations in international politics. Electronic wars have been characterized by a major destructive characteristic to the national security of countries because of their ability to spy, infiltrate, and then blow up without smoke and rubble, whether by destroying websites, blowing them up and bombing them with a barrage of viruses, or working to use multiple cyber weapons to undermine those sites, which are Weapons are also easy to obtain through Internet sites, and therefore the repercussions of this type of war are dangerous for the national security of countries. The practical reality has proven that the state cannot, through its single efforts, confront these new crimes with this continuous development in all fields of communication and information technology, and given the security and legal significance of the phenomenon of electronic terrorism that affects the national security of countries and confronting them requires standing up the necessity of standing on the concept of electronic terrorism, its dangers and ways to confront it And to take all countermeasures towards it.

This requires the necessity of international preparedness to confront such threats. The beginnings of international efforts to confront Cybercrime and digital terrorism go back three decades, when the international "Interpol" discussed in 1981 the possibility

of developing legal legislation on Cybercrime. Since then, progress has been slow, but accelerated after the end of the Cold War. Perhaps the establishment of the Cyberspace Law Institute at Georgetown University in 1995 was an indicator of awareness of the problem. Countries have adopted many initiatives at the national, bilateral, regional or international level, in order to work to protect the global information infrastructure from the risk of exposure to cyber threats, and have worked to create new legislative frameworks that deal with this new phenomenon by formulating a new concept of national security, Then the trend towards international cooperation. Whereas, cyber attacks constitute a threat to the principles of international law, which are based on respect for the sovereignty of states, because of the breach of security and military information that is classified as confidential, and undermines a basic duty which is to refrain from the use or threat of force due to its severe damage to the functioning of the government or the provision of services in the country that is subjected to such.

These attacks, which affect the idea of the state's sovereignty and its scope. Sovereignty in the traditional sense is the state's enjoyment of exercising its powers over its territory and the exclusivity in it by issuing political decisions and the ability to legitimately monopolize the tools of repression at home and refuse to comply with any other foreign authority. That is why international organizations are working to keep abreast of

developments in the matter of cybersecurity and have established working groups to develop strategies to combat Cybercrime and to develop general policies, security measures, guidelines, risk management methods and various technologies that can be used to protect the Internet. These policies include information, computers, individuals, infrastructure, informational programs, services, wired and wireless communication systems, and the entirety of information transmitted or stored in electronic devices in order to ensure the safety of institutions and individuals in the face of security risks and everything related to the Internet