سبل مكافحة الهجمات السيبرانية دولياً

دكتور / وسـام محمود عرفـان
دكتوراة القانون الدولي العام

المستخلص

تنامت في الأونة الأخيرة جريمة الهجمات السيبرانية العابرة للحدود، التي قد تتعرض لها الدول أعضاء المجتمع الدولي، وهو الأمر الذى بات من الأهمية بمكان إلى سعى المجتمع الدولي إلى البحث عن سُبل التصدي لها من خلال آليات تتمثل في بذل المزيد من الجهود الدولية وإتخاذ الإجراءات التي من شأنها الحد من تلك الجريمة أو منعها و ذلك بإتخاذ التدابير اللازمة للحماية، مع العمل على إطلاق المبادرات اللازمة لدعم الأمن السيبراني و الدفاع عنه، و كان لزاماً لتحقيق الغاية توحيد تلك الجهود من خلال إبرام الإتفاقيات الدولية و الإقليمية و تعزيز أطر التعاون الدولي لمواجهة تلك الهجمات التي قد تُهدد الأمن القومي للدول.

الكلمات المفتاحية: الهجمات السيبرانية، الدول، الجهود الدولية، الأمن السيبراني

.

(ISSN: 2356 - 9492)

Abstract:

The crime of cross-border cyber-attacks has increased recently, to which member states of the international community may be exposed. This has become so important that the international community seeks ways to confront it through mechanisms represented by making more international efforts and taking measures that it would reduce or prevent this crime by taking the necessary measures for protection, while working to launch the necessary initiatives to support and defend cybersecurity. To achieve this goal, it was necessary to unify these efforts by concluding international and regional agreements and strengthening international cooperation frameworks to confront these attacks. Which may threaten the national security of countries.

Keywords: cyber-attacks, countries, international efforts, cyber security

مقدمة

في ظل التطور التكنولوجي المستمر في مجال تقنية المعلومات والاتصالات إلى انتشار استخدام شبكات المعلومات لما تتميز به من سهولة ويُسر الحصول على المعلومة وهو الأمر الذى ترتب عليه أثراُ سلبياً متمثلاً فى أن الفضاء السيبراني أضحى مجالاً خصب لممارسة جرائم الكترونية قد يصعب معها تحديد مرتكبيها فضلاً عن أن هذه الجرائم قد يصعب حصرها، ومن هذه الجرائم الهجمات السيبرانية عابرة الحدود التي باتت تهدد الأمن القومي للدول وتنتهك خصوصية الفضاء السيبراني لاختراقها للنظم المعلوماتية بهدف تدمير تلك المعلومات أو الحصول عليها بالرغم من عدم مشروعية هذا الاختراق.

ومما لا شك فيه أنه قد استبان جلياً للمجتمع الدولي أنه بات من الأهمية بمكان البحث عن إيجاد كافة السبل للتصدي لهذه الجريمة نظراً لما تُشكله الجريمة من تهديد أمن الأمن القومي للدول لاسيما وأن هذه الجريمة عابرة للحدود الجغرافية بين الدول، وعلى ذلك فقد عمل المجتمع الدولي على بذل المزيد من توحيد الجهود للتصدي للهجمات السيبرانية من خلال إبرام الاتفاقيات الدولية مثل اتفاقية بودابست، واتفاقية جامعة الدول العربية، بالإضافة إلى العمل على تعزيز التعاون الدولي من خلال إطلاق مبادرات للدفاع عن الأمن السيبراني وسُبل حمايته وقد تبلور عن تلك المجهودات ما أطلقته بعض المنظمات الدولية من مبادرات لدعم الأمن السيبراني وحمايته، فعلى سبيل المثال وليس الحصر فقد أطلق الاتحاد الدولي للاتصالات مبادرة للأمن السيبراني، كما أنشأ حلف شمال الأطلنطي وحدة للدفاع السيبراني، كما أطلق الاتحاد الأوروبي مبادرة للأمن السيبراني.

(ISSN: 2356 - 9492)

أهمية البحث

تنامى الهجمات السيبرانية التي تتعرض لها الدول في الأونة الأخيرة، بات معه من الأهمية بمكان القاء الضوء تلك الجريمة وتوضيح مفهوم السيبرانية و الجرائم التي تُرتكب من خلالها، وما تمثله من تهديد للأمن القومي للدول التي تتعرض لتلك الهجمات، بالإضافة إلى ما تتكبده الدول المُعتدى عليها من خسائر إقتصادية وغير ذلك من جراء تلك الهجمات، وعلى ذلك فكان من الضرورة أيضاُ إبراز دور الإتفاقيات الدولية، والجهود الدولية المبذولة من خلال التعاون الدولي لمواجهة هذه الجريمة والحث على بذل المزيد من الجهود بما يَكفُل حماية الدول من الهجمات السيبرانية وردع مرتكبيها.

أهداف البحث

- تبيان ماهية السيبرانية والهجمات السيبرانية.
- إبراز دور المجهودات الدولية، والتعاون الدولي في مواجهة الهجمات السيبرانية.
- إبراز مدى خطورة الهجمات السيبرانية وما تلحقه من ضرر للدولة المُعتدى عليها.
- تبيان مدى فعالية المجهودات الدولية والإقليمية المبذولة من أجل مكافحة الهجمات السيبرانية.

منهج البحث

تناولت الدراسة ماهية الهجمات السيبرانية وسبل حمايتها والجهود الدولية المبذولة من أجل حمايتها، وقد تم إتباع المنهج الوصفي وعلى ذلك فستتناول الدراسة مفهوم السيبرانية ومفهوم الهجمات السيبرانية وبعض المفاهيم ذات الصلة كمفهوم الأمن السيبراني وكذلك الفضاء السيبراني، كما تتناول الدراسة الجهود الدولية المبذولة من أجل مكافحة الهجمات السيبرانية.

خطة البحث

تناولت الدراسة هذا الموضوع من خلال مبحثين وفقاً لما يلي:

- المبحث الأول: ماهية الهجمات السيبرانية.
  - المطلب الأول: مفهوم الهجمات السيبرانية
  - المطلب الثاني: مخاطر الانتهاكات السيبرانية
- المبحث الثاني: آليات التصدي للهجمات السيبرانية.
  - المطلب الأول: الجهود الدولية والإقليمية فى مكافحة الهجمات السيبرانية.
  - المطلب الثاني: دور التعاون الدولي والإقليمي فى مكافحة الهجمات السيبرانية.

المبحث الأول

(ISSN: 2356 - 9492)

ماهية الهجوم السيبراني

نشأة وتطور الجرائم الإلكترونية

مما لا ريب فيه أنه من الصعوبة بمكان تحديد تاريخ نشأة الجرائم الإلكترونية؛ ويُمكن القول أن تلك الجرائم تطورت خلال سبعينيات القرن الماضي، و رُصد بعض الحالات القليلة فى هذه الأثناء لا تتعدى خطورتها إقليم الدولة و قد ظهرت بعض التشريعات خلال تلك الفترة لتأثيم بعض الممارسات ذات الصلة باستخدام الحاسب الآلي و أفردت لها عقوبات، و تُعد دولة السويد من أوائل الدول التي سنت تشريعات تُجرم الممارسات الغير مشروعة ذات الصلة باستخدام الأنظمة الحواسيبة[1]. وفى ثمانينيات القرن الماضي كانت الجرائم ذات الصلة بإساءة استخدام الحاسب الآلي فى تزايد مستمر وهو الأمر الذي أولاه الباحثين عناية، لا سيما وأن قضايا الاختراق، والتلاعب فى أنظمة النقد، وقرصنة البرمجيات باتت تؤرق المجتمع الدولي[2].

ويرى البعض أن ثمانينيات القرن الماضي كانت بداية لظهور الهجمات السيبرانية، في عهد الرئيس الأمريكي رونالد ريجان، الذي كان يرى أن الولايات المتحدة الأمريكية قد تتعرض لخطر الهجمات السيبرانية وهو ما نتج عنه فكرة "وحدة السياسة القومية بشأن الاتصالات وأمن نظم المعلومات" وقد تطورت هذه الفكرة خلال تسعينيات القرن الماضي، وقام الجيش الأمريكي بإستخدامها في عمليات الإستشعار عن بُعد، وقد ظهرت الحاجة إليها وإلى تقنياتها خلال الحرب الأمريكية على العراق [3].

---

[1] عبد الله حسين آل حجراف القحطانى – تطوير مهارات التحقيق الجنائي فى مواجهة الجرائم المعلوماتية "دراسة تطبيقية فى هيئة التحقيق والادعاء العام بمدينة الرياض – رسالة ماجستير – المملكة العربية السعودية – الرياض – 2014 – ص 30

[2] عبد الله حسين آل حجراف القحطانى – مرجع سابق – ص 30

[3] فرد كابلان – ترجمة لؤي عبد المجيد، المنطقة المعتمة – التاريخ السري للحرب السيبرانية، عالم المعرفة، المجلس الوطني للثقافة والفنون والأدب، الكويت، 2019، ص 52

وقد سرعت الدول من وتيرة القيام باستخدام الحاسب الألى من أجل تحقيق قفزات نوعية في المجالين الأمني والعسكري وذلك في مطلع التسعينيات من القرن الماضي حيث أطلق عليها البعض مصطلح الحرب السيبرانية الباردة أو سباق التسلح السيبراني[1]. لا سيما وأن خطورة الهجمات السيبرانية تَكمُن فى سهولة اقترافها من خلال الأجهزة الإلكترونية أو الحواسيب المتصلة بالإنترنت، إذ أن تنفيذها قد يتم بشكل لحظي، وفي بعض الأحيان لا يستغرق تنفيذها سوى دقائق معدودات[2].

كما أن فقهاء القانون الدولي لم يجتمعوا على تعريف عام للهجمات السيبرانية، وكذلك قواعد القانون الدولي لم تضع تعريفاً عاماً لتلك الهجمات، وقد وردت بعض التعريفات للهجمات السيبرانية في العديد من مؤلفات فقهاء القانون، فقد عرفها جانب من الفقهاء تلك الجريمة من حيث المدلول والأركان والخصائص وأيضاً من حيث طبيعة تلك الجريمة، وقبل الخوض في تبيان مدلول الهجمات السيبرانية سنُعرج على مفهوم السيبرانية وكذلك المفاهيم المرتبطة به، ثم ننتقل إلى توضيح مفهوم الهجمات السيبرانية وما قد يتصل بها من مفاهيم قد تتشابه معها ثم أخيرا نُبرز وجه الاختلاف بين الهجمات السيبرانية والجريمة السيبرانية وهدياً على ما تقدم سنتناول ذلك من خلال هذا المطلب.

[1] Tang Lan , Zhang Xin , Harry D.Raduege , Jr.,Dmitry I. Grigoriev, pavan Duggal, and Stein Schjolberg,"Global Cyber Deterrence Views from China, the U.S., Russia, India, and NORWAY", The EastWest Institute, PRINTED in the United States, 2010, P1

[2] أميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، العدد الخامس والثلاثون، الجزء الثالث، 2020، ص 401

(ISSN: 2356 - 9492)

المطلب الأول

مفهوم الهجمات السيبرانية

لتبيان مفهوم الهجمات السيبرانية سوف نتطرق إلى مفهوم السيبرانية فى اللغة والاصطلاح وبعض التعريفات فى ضوء القانون الدولي، ثم نتطرق إلى تبيان المفاهيم ذات الصلة بالسيبرانية، ثم نُعرج بإيجاز على خصائص وبعض أنواع الهجمات السيبرانية، وذلك من خلال هذا المطلب.

الفرع الأول

مفهوم السيبرانية

تعنى السيبرانية فى اللغة أنها " علم الضبط ومصدرها (Cybernetics)[1] أى ضبط الأشياء عن بُعد والسيطرة عليها وعُرفت السيبرانية إصطلاحاً كما عرفها البعض بأنها علم القيادة والتوجيه فهي تعنى "علم الاتصالات وأنظمة التحكم الآلي في كل من الآلات والأشياء الحية"[2]، كما يرى البعض الآخر بأنها "فضاء الإنترنت أو العالم الافتراضي"[3]، فالسيبرانية وفقاً للمدلول سالف البيان تحدث في مجال الفضاء الذي هو البيئة الافتراضية التي تعمل بها المعلومات السيبرانية والتي تتصل من خلال شبكات الحاسب الآلي.

---

[1] Julia Cresswell – Oxford Dictionary of Word Origins : Cybernetics – Oxford Reference Online – Oxford University Press – 2010 – P 56

[2] منير البعلبكي – المورد قاموس إنجليزي عربي – دار العلم للملايين – بيروت – 2004 – ص243

[3] د. صالح بن على بن عبد الرحمن الربيعة – الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت – هيئة الاتصالات وتقنية المعلومات – المملكة العربية السعودية – 2018 – ص 6

وقد عرفته الوكالة الفرنسية لأمن أنظمة الإعلام "ANSSI" بأنه "فضاء التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية"[1].

كما عرفه الاتحاد الدولي للاتصالات بأنه "المجال المادي وغير المادي الذي يتكون وينتج من عناصر هي: أجهزة الكمبيوتر، الشبكات، البرمجيات، حوسبة المعلومات، المحتوى الإلكتروني، معطيات النقل والتحكم الرقمي"[2].

مفاهيم ذات صلة بالسيبرانية

أولا: الفضاء السيبراني

يُعرف الفضاء السيبراني وفقاً لما أقره الإتحاد الدولي للإتصالات والوكالة المتحدة المتخصصة فى مجال تكنولوجيا المعلومات والاتصالات بأنه "الحيز المادي وغير المادي الذي ينشأ أو يتكون من جزء أو من كل العناصر التالية حواسيب أجهزة مميكنة وشبكات ومعلومات محوسبة وبرامج ومضامين ومعطيات مرور ورقابة والذين يستخدمون كل ذلك"[3]

[1] Ebert Hannes and Maurer Tim. "Cybersecurity"– oxford bibliographies, Last Modified – 11 January 2017

[2] The International Telecommunication Union – ITU – Toolkit for cybercrime Legislation – Geneva – 2010 – p.12

[3] خالد وليد محمود، الهجمات عبر الإنترنت، ساحة الصراع الإلكتروني الجديدة، سلسلة دراسات ودراسة السياسات – المركز العربي للأبحاث، قطر، 2013، ص 4

(ISSN: 2356 - 9492)

ثانياً: الأمن السيبراني

عُرف الأمن السيبراني بأنه "مجموعة من الأدوات والاستراتيجيات الأمنية والمبادئ التوجيهية ونهج إدارة المخاطر والإجراءات والتدريب والخبرة العملية والتأمين والتكنولوجيا، والتي يمكن إستخدامها لحماية الفضاء السيبراني والتنظيم وموارد المستخدم"[1]. كما يُقصد به "أمن الشبكات والأنظمة المعلوماتية والبيانات والمعلومات والأجهزة المتصلة بالإنترنت[2].

كما عرفه البعض بأنه هو "النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الإتصالات والمعلومات ويضمن إمكانات الحد من الخسائر والأضرار التي تترتب فى حال تحقق المخاطر والتهديدات، كما يتيح إعادة الوضع إلى ما كان عليه بأسرع وقت ممكن بحيث لا تتوقف عجلة الإنتاج وبحيث لا تتحول الأضرار إلى خسائر دائمة"[3].

كما عرفه الإتحاد الدولي للإتصالات بأنه "مجموع الأدوات والسياسات والمفاهيم الأمنية والضمانات الأمنية والمبادئ التوجيهية والتقنيات ونهج إدارة المخاطر التي يُمكن إستخدامها لحماية البيئة الإلكترونية وتنظيم أصول المُستخدم وتشمل توصيات أجهزة الحوسبة، والموظفين، والبنية التحتية، والخدمات، ونظم الاتصالات السلكية واللاسلكية، ومجمل المعلومات المرسلة أو المخزنة في البيئة الإلكترونية"[4].

---

[1]Christian Agrum ,Words for Understanding Cyber Security , Enjoying a calm Internet, Edition, October 1, 2020, p. 280.

[2] حنين جميل أبو حسين، الإطار القانوني لخدمات الأمن السيبراني، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، عمان، الاردن،2021، ص 18

[3]سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، دار النهضة العربية، مصر، 2017، ص 214

[4]الإتحاد الدولي للإتصالات – دراسة تأمين شبكة المعلومات والاتصالات – قطاع تنمية الاتصال – دراسة خلال الفترة 2006– 2010 https://www.Itu.Int/net/Itunews/issues/2010/9/Pdf/201009-20-ar.pdf

ثالثاً: الجريمة الإلكترونية

عرف البعض الجريمة الإلكترونية بأنها "أى فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه والتحقيق فيه وملاحقته قضائياً"[1].

كما يعرفها البعض بأنها "نشاط غير مشروع موجه لنسخ، أو تغيير، أو حذف، أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه"[2].

ومما هو جدير بالذكر، وبعد تبيان المصطلحات والمفاهيم سالفة البيان أن ننوه على أن هناك إختلاف جوهري بين الجريمة السيبرانية وبين الهجمات السيبرانية وما يرادفها من حيث المعنى، وهو يتمثل في الباعث؛ إذ أن الباعث على الهجمات السيبرانية يتمثل في الإساس في إضعاف وظيفة شبكات الحاسوب المستهدفة في دولة أخرى لتحقيق هدف سياسي، يُضاف إلى ذلك أن القواعد القانونية التي تقرر من خلالها الهجمات السيبرانية هي قواعد القانون الدولي العام، تحديداً قواعد اللجوء إلى إستخدام القوة؛ أما الجريمة السيبرانية فتصدر عن جهة لا تمثل الدولة أو أحد مؤسساتها سواء كان شخص عادياً أو اعتبارياً سعياً وراء هدف إجرامي يتحقق عند إختراق أجهزة الكترونية معينة لأغراض شخصية، و هذا التصرف لا يرقى إلى مستوى الجريمة السيبرانية إلا إذا شكل جريمة وفقاً للقانون الجنائي الداخلي إستناداً إلى مبدأ "لا جريمة و لا عقوبة إلا بنص" و هو أحد المبادئ الأساسية التي تقوم عليها أنظمة العدالة الجنائية، فضلاً عن ذلك فالأضرار المحتملة لكل من الهجمات السيبرانية و الجريمة السيبرانية تختلف بشكل كبير

---

[1] سامي الشوا: الغش المعلوماتي كظاهرة إجرامية مستحدثة، بحث مقدم فى مؤتمر الجمعية المصرية للقانون الجنائي، القاهرة، 25:26 أكتوبر، 1993، ص 516

[2] هدى حامد قشقوش: جرائم الحاسب الإلكتروني فى التشريع المقارن، دار النهضة العربية، مصر، 1992، ص 5

(ISSN: 2356 - 9492)

على إعتبار أن الهجمة السيبرانية تهدف إلى إلحاق ضرر شامل سواء للأشخاص، أو الممتلكات في الدولة الأخرى، وهو ما يختلف جذرياً عن الجريمة السيبرانية و التي ينحصر ضررها عموماً في مستخدمين معينين"[1].

رابعاً: الجريمة السيبرانية

عُرفت الجريمة السيبرانية بأنها "كل فعل أو إمتناع عن فعل بإستعمال نظام معلوماتي معين للإضرار بمصلحة أو حق يحميه القانون من خلال جزاء جنائي، سواء كانت هذه المصالح أو الحقوق المحمية جنائياً تُمثل نماذج معلوماتية مستحدثة، أو كانت تدخل في نطاق المصالح أو الحقوق المحمية جنائياً فيما سبق بالطرق التقليدية، وسواء كان الاعتداء واقعاً داخل حدود الدولة أو يتجاوزها إلى مجموعة من الدول[2].

خامسا: القوة السيبرانية

عُرفت القوة السيبرانية بأنها " القدرة على استخدام الفضاء السيبراني لإيجاد مزايا للدولة والتأثير على الأحداث المتعلقة بالبيئات التشغيلية الأخرى وذلك عبر أدوات سيبرانية"[3].

---

[1] د. أميرة عبد العظيم محمد عبد الجواد – المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام – مجلة الشريعة والقانون – العدد الخامس والثلاثون – الجزء الثالث – 2020 – ص 394:395

[2] د. هلالي عبد اللاه أحمد – جرائم الحاسب والإنترنت بين التجريم الجنائي وآليات المواجهة – دار النهضة العربية – 2015 – ص 117

[3] Joseph S Nye , Harvard – The future of power. Press realizes – Belfer center for science and international Affairs – Kennedy Scholl – 31 JANUARY 2011

الفرع الثاني

الهجمات السيبرانية

عُرفت الهجمات السيبرانية بأنها "الأفعال الصادرة من أجهزة الحاسوب وشبكات المعلومات التابعة لدولة ما، بشكل منظم ومدروس على أجهزة حاسوب وشبكات لدولة أخرى بغرض التجسس أو التخريب[1]، أو التوجيه[2].

كما عُرف الهجوم السيبراني بأنه "تصرف يدور في عالم إفتراضى قائم على إستخدام بيانات رقمية، ووسائل إتصالات جراء إختراق مواقع الكترونية حساسة، عادة ما تقوم بوظائف تُصنف بأنها ذات أولوية كأنظمة حماية محطات الطاقة النووية أو الكهربية أو المطارات ووسائل النقل الأخرى"[3].

كما يُمكن تعريف الهجوم السيبراني من حيث وسيلة الاستخدام وأيضاً على أساس شخصي فمن حيث الوسيلة عُرف بأنه "نشاط إجرامي تُستخدم فيه التقنية الإلكترونية للحاسوب الآلي وشبكة الإنترنت بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الاعتداء الإجرامي المُستهدف"[4]، كما يُعرف التهديد السيبراني على أساس شخصي بأنه "أية سلوك يُنسب لفاعلها معرفة فنية بتقنية الحاسبات يُمَكِن من إرتكابها"[5].

---

[1] K.Saalbach,"Cyberwar, Methods and practice", version 9.o, university of Osnabruck 17 Jun 2014,p.6.

[2] د. يحي ياسين سعود، الحرب السيبرانية في ضوء القانون الدولي الإنساني، المجلة القانونية في الدراسات والبحوث القانونية، كلية الحقوق، فرع الخرطوم، المجلد الرابع، العدد الرابع، 2018، ص 58 وما بعدها.

[3] انظر مفهوم الهجمات السيبرانية والمسئولية الناشئة عنها في ضوء التنظيم الدولي المعاصر: العدد الرابع، السنة الثامنة، 2016، ص 615.

[4] د. محمد عبيد الكعبي، الجرائم الناشئة عن الإستخدام الغير مشروع لشبكة الإنترنت، دار النهضة العربية، القاهرة، بدون سنة نشر، ص 34.

[5] د. عبد الله عبد الكريم عبد الله، جرائم المعلومات والإنترنت (الجرائم الإلكترونية)، طبعة أولى منشورات الحلبي الحقوقية، لبنان، 2007، ص 16.

(ISSN: 2356 - 9492)

وقد عُرفت الهجمات السيبرانية في البروتوكول الإضافي الأول عام 1977 والملحق بإتفاقيات جنيف الأربعة عام 1949 بأنها "أعمال العنف الهجومية والدفاعية ضد الخصم بالرغم أنه لا يُشترط بالهجمات السيبرانية أن يرافقها أعمال عنف مسلح بشكل ملموس ومباشر، إلا أنه لا يمكن التسليم بأن كل عمل على شكل قرصنة سيبرانية لا يشكل عمل عنف مسلح حيث بالنظر إلى الآثار التي ترتبها تلك الأعمال السيبرانية[1]، قد تتجاوز في تأثيرها وجسامتها الهجمات العسكرية التقليدية"[2].

كما عُرفت أيضا وفقاً لمبادئ دليل تالين بأنها "عمليات سيبرانية، سواء كانت هجومية أم دفاعية، والتي يهدف من خلالها بصورة معقولة التسبب بالإصابة، أو وفاة الأشخاص، أو الأضرار، أو تدمير الأعيان والأهداف"[3].

كما عرفها مايكل شميت بأنها "مجموعة من الإجراءات التي تتخذها الدولة للهجوم على نظم المعلومات المعادية بهدف التأثير والإضرار بها وفي الوقت ذاته للدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة"[4]

أولاً: خصائص الهجوم السيبراني

[1] انظر مجلة كلية القانون الكويتية العالمية – العدد الثاني – السنة الخامسة – 5 يونية 2017 – ص 241.

[2] انظر المادة (1/49) من البروتوكول الإضافي الأول لعام 1977، الملحق بإتفاقيات جنيف الأربعة 1949.

[3] أنظر دليل تالين – مجموعة مبادئ أُعدت من قبل خبراء القانون الدولي الإنساني – 2013 – وكان مايكل شميت من أبرز المشاركين فى هذه المجموعة – صدر الدليل بالتعاون بين الخبراء وحلف شمال الأطلنطي وبدعم من فريق مؤلف من خبراء السيبرانية واللجنة الدولية للصليب الأحمر والقيادة الليبرالية الأمريكية الذين شاركوا في المداولات

[4] Michmitt – Computer Network Attack and The Use of force in international Low – Thoughts on a normative Framework – Co:ombia Journal of transnation Low – 1998-1999 – p.890

يُمكن تحديد بعض الخصائص التي يتسم بها الهجوم السيبراني بإيجاز فى النقاط الأتية [1]:

1. التحديث والتطوير بوتيرة سريعة وبصفة دائمة مما يترتب عليه زيادة فاعليتها وقدرتها التدميرية.
2. القدرة على إختراق أكثر الأنظمة حماية، وإصابة أنواعاً مختلفة من الأجهزة الإلكترونية مثل الحاسب الألى أو الخوادم الإلكترونية، وذلك على سبيل المثال وليس الحصر.
3. صعوبة تحديد هوية مرتكبيها، وأيضاً صعوبة استشعارها لعدم وجود مؤشر للتنبؤ بحدوثها.
4. التغلب على العامل الجغرافي حيث يختفي معها ولا يؤثر على اختيار الجهة المُستهدف الهجوم عليها.
5. قلة ما تتكبده من كلفة مالية مقارنة بالحروب المسلحة.

ثانياً: بعض أنواع الهجمات السيبرانية:

في حقيقة الأمر أن الدول التي تلجأ الى الهجوم السيبراني من أجل سرقة البيانات والمعلومات من المواقع التي يتم الهجوم عليها، الهدف منه هو توقف عمل القطاعات التي تعمل وفقاً لهذه البيانات، وتتنوع الهجمات السيبرانية لعدة أنواع مختلفة نذكر أهمها وأخطرها وهي:

برامج الفيروسات الخبيثة

[1] نور أمير الموصلى – الهجمات السيبرانية في ضوء القانون الدولي الإنساني – رسالة ماجستير – الجامعة الافتراضية السورية – 2021 – ص 11

(ISSN: 2356 - 9492)

تُعد هذه البرامج بمعرفة أحد المُخربين بهدف إحداث أكبر قدر من الضرر للنظام بعد أن يتم ربطه بالبرامج الأخرى، وبقدور هذا الفايروس إستهداف مواقع فى الذاكرة وكذلك برامج أخرى في الحاسب بغية تدميرها، ويقوم هذا البرنامج أيضاً بمجموعة من العمليات تؤثر بصورة مباشرة أو غير مباشرة في خصائص نظام التشغيل أو المعلومات المُخزنة .[1]

برامج القنابل المعلوماتية

تُعد هذه البرامج أكثر تقدماً من البرامج الخبيثة، وهي عبارة عن تعليمات برمجية ضارة تم تصميمها لتعمل أحداث محددة، أو تحت ظروف معينة، أو لدى تنفيذ أمر معين، بحيث تقوم بتخريب ومسح البيانات، أو تعطيل النظام وقد تظل كامنة لفترة طويلة من الزمن ثم يتم تفعيلها وقد تسبب أضراراً بالغة لجهاز الحاسب الألى المصاب مما يجعله غير صالح[2].

برامج الدودة

[1] حسن مظفر الروز: الفايروسات والحاسب الإلكتروني، المخاطر المحتملة وسبل الحد منه، المجلة العربية العلمية للفتيان، المنظمة العربية للتربية والثقافة والعلوم، المجلد الأول، العدد الثاني، 1997، ص 4

[2] طلال محمد الحاج إبراهيم: الهجمات الالكترونية والمسؤولية الجنائية للقادة، المجلة القانونية والقضائية، وزارة العدل، مركز الدراسات القانونية والقضائية، السنة 12، العدد الأول، 2018، ص 305

هي برامج تنتقل من جهاز الحاسب إلى جهاز آخر وذلك من خلال إستغلال بعض القصور فى أجهزة الحاسب الألى والشبكات، وتنتقل أيضاً من شبكات الأنظمة المعلوماتية لتعطيلها والعمل على تدمير البيانات والبرامج التي تحتوي عليها تلك الأنظمة.

المطلب الثاني

مخاطر الانتهاكات السيبرانية

فى ظل تزايد إهتمام الدول بتكنولوجيا المعلومات نظراً لما تُشكله هذه التكنولوجيا من أهمية لا سيما أثناء الحروب المتوقع حدوثها من خلال الفضاء السيبراني، وذلك من أجل الإستعداد لمواجهة هذه الحروب حال وقوعها، وقد أدت الحروب السيبرانية بين روسيا وجورجيا عام 2008 وذلك على سبيل المثال إلى دفع العديد من الدول مثل الصين وغيرها من الدول ببناء وحدات الكترونية على شبكات الإنترنت للحماية من مئات وآلاف القراصنة المحترفين[1]. وقد أولى المجتمع الدولي عناية بتحديد صور الإنتهاكات السيبرانية لما تمثله من خطورة تُهدد أمن الدول وذلك من أجل تأثيم تلك الإنتهاكات التي تُنسب للدول وإخضاعها لمبادئ القانون الدولي العام، وسوف نتناول أهم صور هذه الإنتهاكات التي تُرتكب أثناء النزاعات المسلحة، وكذلك التي لا تُرتكب أثناء النزاعات المسلحة ثم نُبين الإنتهاكات التي لا ترتكب أثناء النزاع المسلح ولا ترقى لوصف العدوان السيبراني إلا أنها تُشكل إنتهاك لمبادئ القانون الدولي، وذلك على النحو التالي:

[1] د. عباس بدران: الحرب السيبرانية – الاشتباك فى عالم المعلومات، مركز دراسات الحكومة السيبرانية، بيروت، 2010، ص 110

(ISSN: 2356 - 9492)

أولاً: الهجوم السيبراني الذي يُرتكب أثناء النزاعات المسلحة

تقوم الدولة المُعتدية بإستخدام الفضاء السيبراني لتنفيذ الهجوم السيبراني من أجل تدمير البيانات التي تحتوي عليها الأجهزة، وغير ذلك من الأسباب كنقل المعلومات للاستفادة منها للتفوق على الدولة المعتدى عليها أو لتعطيل تلك الأجهزة أو التقليل من كفاءة تشغيلها، وقد تلجأ الدول المعتدية إلى إرتكاب تلك الهجمات قبل شن الحروب على ساحة الإقتتال لإضعاف القوة العسكرية للدولة المُعتدى عليها أو يتزامن الهجوم أثناء الضربات الجوية من أجل تعطيل أجهزة الدفاع وصد هذه الضربات.

ومما لا شك فيه أنه إذا أدت الهجمات السيبرانية التي تُرتكب أثناء الحروب إلى حدوث أضرار للمدنيين دون فَتُعَد إستخداماً للقوة السيبرانية، وهذا الإستخدام يتعين ألا يخرج عن إطار الضوابط التي حددتها مبادئ القانون الدولي الإنساني. وهو ذاته القانون الذي يحدد تلك الإنتهاكات فى زمن النزاعات المسلحة كما يُحدد مدى مشروعية تلك الهجمات التي تشنها الدول، سواء العمليات السيبرانية التي تُشن كسلاح قتال مساعد للعمليات العسكرية الحركية التقليدية براً وبحراً وجواً، أو العمليات السيبرانية المستقلة التي تشن من أجل تدمير البنية التحتية للدولة المستهدفة إذا نفذت فى زمن النزاع المسلح[1].

ثانياً: العدوان السيبراني

[1] انظر: حسن فياض: الهجمات السيبرانية من منظور القانون الدولي الإنساني، الموقع الرسمي للجيش اللبناني، 2020، ص 4

هو الهجمات السيبرانية التي لا تُرتكب أثناء الحروب إلا أن نتائجها ترقى لمستوى العدوان، ويرى البعض[1] أنه يُمكن تحديد مفهوم العدوان السيبراني من خلال تطبيق مفهوم العدوان التقليدي الوارد فى الفقرة الأولى من المادة الثامنة مكرر من النظام الأساسي للمحكمة الجنائية الدولية. وترتيباً على ذلك يكون العدوان السيبراني يتمثل فى أن يُنسب لدولة ما بشن هجوم سيبراني على دولة أخرى تُشكل بما لها من خطورة وخصائص انتهاكاً لميثاق الأمم المتحدة؛ ويتفق البعض مع هذا المفهوم والذي يرى[2] أن الأعمال العدوانية تستند فى الأساس على انتهاك ميثاق الأمم المتحدة وأن هذا الانتهاك يمثل الفعل المادي للعدوان من عدمه يُحَدد من خلال الوقوف على خصائص الفعل ونطاقه ومدى خطورته.

ويرى جانب من فقهاء القانون الدولي – الغالبية – أنه وإن كان العدوان الإلكتروني يمثل أحد أخطر صور العدوان إلا أن هذا الأمر لم يلق استجابة على أرض الواقع من منظمة الأمم المتحدة أو المحكمة الجنائية الدولية لمحاولة تحديد الإطار القانوني لمحاكمة مرتكبي جريمة العدوان السيبراني[3].

كما يرى رأى آخر[4] أن المحكمة الجنائية الدولية يُمكنها مكافحة العدوان السيبراني من خلال تفسيرها لنص المادة الثامنة مكرر التي اضيفت فى كمبالا دون الحاجة إلى إدخال تعديلات على النظام الأساسي بالإضافة إلى أن مجلس

[1] Gianpiero Greco – Cyber-Attacks as aggression crimes in cyberspace in the context of international law-O.P p 43

[2] Jonathan A.OPHARD,"Cyber warfare and the crime of aggression:the Need for individual Accountability on tomorrow Battlefield, Duke law and technology" O.P , P1

[3] Albi Kociblli, Aggression, from Cyber-Attacks To ISIS:Why International low Struggles to Adapt,2017 vol39

[4] Kevin L. Miller, The Kampala Compromise and Cyberattacks: Can there Be an international Crime of

(ISSN: 2356 - 9492)

الأمن بمقدوره مكافحة العدوان السيبراني بما يملكه من سلطات واسعة فى تحديد ما إذا كان أى فعل تقترفه الدول يمثل عدوان من عدمه وذلك بالاستناد على ما يمثله ذلك الفعل من تهديد للسلم والأمن الدولي.

ثالثاً: الهجوم السيبراني الذي لا يُرتكب أثناء الحروب ولا يرقى لمستوى العدوان إلا أنه يُمَثل إنتهاكاً لمبادئ القانون الدولي

كما سبق و أسلفنا بأن هناك هجمات سيبرانية تُرتكب أثناء النزاعات المسلحة و أيضاً هناك العدوان السيبراني الذى لا يُرتكب أثناء النزاعات المسلحة، فيوجد أيضاً عمليات سيبرانية لا تُرتكب أثناء النزاعات المسلحة، و أيضاً لا ترقى لمستوى العدوان السيبراني، مثال ذلك عمليات إختراق وكالات الأنباء و أيضاً الاختراق من أجل الحصول على بيانات سرية مُخزنة بغية تدميرها أو إفشاء تلك البيانات و إن كان هذا الفعل غير مشروع دولياً لتسببه فى الحاق ضرر بالدولة المُستهدفة، إلا أن هذه العمليات لا ترقى إلى نعتها بالعدوان السيبراني من حيث درجة خطورتها و ترتيباً على ذلك لا تقع تحت طائلة القانون الدولي الإنساني.

الفرع الأول

المخاطر السيبرانية

Cyber-Aggression? Southern California interdisciplinary law Journal, 2014, vol.23, p.217

قبل الخوض فى تبيان المخاطر السيبرانية ينبغي أن نُعرج على طبيعة تلك المخاطر وهو ما سنتناوله أولاً ثم نتناول صور تلك المخاطر وفقاً لمبادئ القانون الدولي.

اولاً: طبيعة المخاطر السيبرانية

المخاطر السيبرانية لا تتغير إنما ما يتغير هو سماتها نظرا لتطور الوسائل الالكترونية المستخدمة ولذلك تتجه الدول إلى الإهتمام بتكنولوجيا المعلومات لتعاظم دورها فى الحروب والصراعات وسمة التكنولوجيا أنها فى تطور دائم ومستمر لذا أولت الدول عناية فى بناء وحدات الكترونية على شبكات الإنترنت للحماية من القراصنة[1]. ويرى جانب من الفقهاء أن الحروب السيبرانية باتت بديلاً عن الحروب التقليدية التي تستخدم الجيوش العسكرية، فلا تعتمد الحروب السيبرانية على الجيوش إنما تعتمد فى الأساس على القرصنة ونشر الفيروسات الإلكترونية التي تنتشر فى شبكات الحاسب الآلي بعد إختراقها وذلك فى سرية تامة وكفاءة عالية، بالإضافة إلى أن الصراعات السيبرانية تتميز بأن ما تحدثه من تدمير وتجسس وغير ذلك دون إحداث خسائر بشرية كما يحدث فى الصراعات العسكرية.

والصراعات السيبرانية يُمكن أن تكون لأسباب سياسية، ويأخذ شكلاً عسكرياً ويتم فيه استخدام قدرات هجومية ودفاعية عبر الفضاء الإلكتروني، ويُمكن أيضاً أن يكون الصراع السيبراني ذو طبيعة ناعمة عن طريق شن الحروب

[1] فى هذا المعنى انظر د. عباس بدران: الحرب السيبرانية – الاشتباك فى عالم المعلومات، مركز دراسات الحكومة السيبرانية، بيروت، 2010، ص 110

(ISSN: 2356 - 9492)

النفسية والإعلامية والحصول على المعلومات لتسريبها بما يؤثر على طبيعة العلاقات الدولية[1]؛ كما يُمكن أيضاً أن يكون الصراع داخل الدولة على أساس طائفي أو اقتصادي أو دينى[2].

ثانياً: بعض صور المخاطر السيبرانية

الهجوم السيبراني يستند فى الأساس على استخدام التقنيات الحديثة والمتطورة للحاسب الآلي من أجل الهجوم على نظم المعلومات بغية تدميرها لغاية تُريد الدولة المعتدية أن تُحققها، ومن أهم الصور التي يُمكن أن يترتب عليها مخاطر سيبرانية هي التجسس، والقرصنة، والإرهاب وهو ما سنتناوله بإيجاز.

1- التجسس السيبراني

ذهب جانب من الفقه إلى تعريف التجسس السيبراني بأنه "استخدام القدرات السيبرانية لإجراء عمليات رصد، أو مراقبة، أو التقاط، أو تسريب الاتصالات الإلكترونية، أو المخزنة، أو البيانات المخزنة، أو معلومات أخرى"[3].

---

[1] د. عادل عبد الصادق – موقع ويكليكس وتحدى عالم الاستخبارات الأمريكي – ملف الأهرام الإستراتيجي – مركز الاهرام للدراسات السياسية والإستراتيجية – اكتوبر 2012

[2] د. عادل عبد الصادق – القوة الالكترونية اسلحة الدمار الشامل فى عصر الفضاء الإلكتروني – المركز العربي لأبحاث الفضاء الإلكتروني – قضايا إستراتيجية – 2012

[3] Michael N.Schmitt& Liis Vihul, Tallinn Manual 2.0 on the International Law Applicable to Cyber, pretations, Cambridge University press, 2017, note 13, Rule 32, p.168

كما ذهب جانب آخر إلى أنه "عبارة عن الطرق المستخدمة لاختراق المواقع الإلكترونية ومن ثم سرقة بعض المعلومات والتي قد تكون فائقة الأهمية والخطورة للطرف المتلقي والمسروق منه، وقد انتشرت فى الألفية الجديدة بانتشار طرق الاختراق، وأحياناً قد يكون الاختراق من أشخاص عابثين ليس إلا، وأحياناً بغرض سرقة معلومات"[1].

وقد بذلت الدول جهوداً على المستوى التقني من أجل مكافحة هذه الجريمة بحماية المعلومات التي تتعرض للتجسس السيبراني وذلك بالعمل على تشفير البيانات وإخفائها، ومن آليات الحماية الإحتفاظ بسرية المعلومات قبل الجميع باستثناء الذين لهم صلاحية للاطلاع عليه، وأيضاً التيقن من أن المعلومات لم تتغير من قِبَل أشخاص غير مخولين لذلك، والتحقق من الشخصية، ويُطلق على هذه الآلية تكامل البيانات[2]. ومما هو جدير بالذكر أن هذه الجرائم قد تستهدف التجسس على المعلومات الثقافية والتعليمية وقد يكون الحصول أيضاً على معلومات إقتصادية أو تجارية أو صناعية.

[1] د. عصام فاعور ملكاوي – الفضاء الإلكتروني ساحة حرب دولية مفترضة – أربد للبحوث والدراسات – القانون – جامعة إربد الأهلية – عمادة البحث العلمي والدراسات العليا – مجموعة 18 – ع2 – تموز 2015 – ص 120

[2] د. مصطفى جاد: مستقبل الإرهاب السيبراني – مقال، ندوة المركز الدولي للدراسات المستقبلية والإستراتيجية، 11 إبريل 2012، جريدة السياسة الدولية، مؤسسة الأهرام المصرية، إعداد شريهان نشأت المنيرى، انظر http:/www.siyassa.org.eg//news Content/6/51/2450

(ISSN: 2356 - 9492)

2- الاختراق السيبراني

تُعد القرصنة أحد صور المخاطر السيبرانية إن كان هدفها تعطيل نظم المعلومات فعلى سبيل المثال فاختراق قواعد البيانات للإستيلاء عليها أو تعديلها أو حذفها أو تدميرها يُمكن اعتباره صورة من صور الاختراقات السيبرانية؛ وينشط دور القرصنة فى التعبير عن المواقف السياسية وقد تم استخدام هذه الاختراقات فى الفضاء السيبراني فى إطار الصراعات بين الدول كما حدث بين استونيا وروسيا فى عام 2007 و الاختراقات المتبادلة بين الصين و الولايات المتحدة الأمريكية أو ما بين كوريا الجنوبية[1].

3- الارهاب السيبراني

عرفه جانب من الفقهاء بأنه "نشاط إجرامي مُخطط ومُنظم مُخالف للقانون، يقوم به التنظيم الإرهابي من خلال التقنية الإلكترونية الرقمية بغية تحقيق غرض معين تحت تغطية"[2].

كما عرفه جانب آخر من الفقهاء بأنه "كل نشاط إجرامي يتم من خلال شبكة الإنترنت بغية بث الأفكار المتطرفة سواء كانت سياسية أو عنصرية أو دينية من أجل إفساد عقيدة أو إستغلال معاناة الأفراد فى تحقيق مآرب خاصة تتعارض مع مصالح المجتمع"[3].

ويُعد من أشكال الإرهاب الإلكتروني، التجنيد السيبراني من خلال ما يُطلق عليه "التلقين السيبراني" وأخيراً "التهديد والترويع السيبراني"[4].

---

[1] يراجع د. عادل عبد الصادق: اسلحة الفضاء السيبراني فى ضوء القانون الدولي الإنساني، وحدة الدراسات المستقبلية، ص 43

[2] انظر: د. مصطفى محمد موسى: الإرهاب الإلكتروني، بدون دار نشر، طبعة أولى،2009، ص 173

[3] انظر: د. حسين المحمدي بوادي: الإرهاب الدولي بين التجريم والمكافحة، دار الفكر العربي، 2006، ص 54

[4] د. عبد الله بن عبد العزيز بن فهد: بحث بعنوان "الإرهاب الإلكتروني فى عصر المعلومات" ، مقدم إلى المؤتمر الدولي الأول حول

الفرع الثاني

التكييف القانوني للهجمات السيبرانية

يُعد مبدأ إحترام السيادة من أهم مبادئ القانون الدولي بموجب نص الفقرة الرابعة من المادة الثانية من ميثاق الأمم المتحدة، و بالنظر إلى الهجمات السيبرانية و ما قد يلحق عنها من الإضرار بالأمن القومي للدولة المُعتدى عليها، أو ما قد تلحقه أيضاً بالإضرار بالمدنيين حال أن توجه الهجمة بهدف قطع الخدمات الحيوية التي تؤثر على الحياة المعيشية لهم مثل قطع الإتصالات بأنواعها أو قطع الخدمة عن مرفق حيوي مثل الكهرباء و غير ذلك؛ و لذا فقد ذهب جانب من الفقه إلى أن هذه الهجمات يُمكن أن يكون القانون الدولي سنداً قانونياً لتجريمها إذ أنه فى بعض الأحيان لا يُمكن إثبات وقوعها لعدم توافر الدليل المادي لارتكابها و من ثم لم تَثبُت الجريمة، و أحياناً أخرى قد يتوافر هذا الدليل الدال على ثبوتها. وعلى ذلك فيكون المعيار فى تكييف الهجوم هو إن كان هذا الهجوم تصرف عدواني على دولة أم رد لعدوان موجه من دولة أخرى، واستند هذا الجانب من الفقهاء على صحة إتخاذ هذا المعيار بما ورد بنص المادة 51 من ميثاق الأمم المتحدة الذي أباح للدولة المُعتدى عليها حق الدفاع عن النفس وإتخاذ التدابير اللازمة حيال هذا الحق.

"حماية أمن المعلومات والخصوصية فى قانون الإنترنت" المنعقد بالقاهرة فى الفترة من 4:2 يونيو 2008

(ISSN: 2356 - 9492)

المبحث الثاني

أليات مواجهة المجتمع الدولي للهجمات السيبرانية

باتت الهجمات السيبرانية إبان العصر الحالي جريمة تؤرق المجتمع الدولي، و هو الأمر الذى بات معه من الأهمية بمكان التصدي لها و مكافحتها دولياً، و على ذلك فقد بذلت تلك الدول و لا تزال تبذل جهود من أجل التصدي لتلك الهجمات، و ذلك فى إطار إبرام الإتفاقيات دولياً و إقليمياً، و على قمة هذه الجهود هي جهود المنظمات الدولية و الإقليمية و المنظمات الدولية المتخصصة بالإضافة إلى إدراك الدول أعضاء المجتمع الدولي أهمية تكريس سُبل التعاون الدولي لمكافحتها و كيفية التصدي لها حرصاً منها على ضرورة تأثيم تلك الجريمة وملاحقة مرتكبيها وإفراد عقوبات على من يَثبُت إرتكابها فى حقه، وهدياً على ذلك سنتناول هذا المبحث فى مطلبين أولهما نتناول فيه الجهود الدولية والإقليمية لمكافحة الهجمات السيبرانية، ثم نتناول سُبل التعاون الدولي فى مكافحة الهجمات السيبرانية.

المطلب الأول

الجهود الدولية والإقليمية فى مكافحة الهجمات السيبرانية

تسعى المنظمات الدولية و الإقليمية إلى بذل جهود من أجل مكافحة الهجمات السيبرانية لما تلحقه من ضرر يُهدد الأمن القومي، و الاقتصادي و غير ذلك، بالدول الأعضاء المُعتدى عليها من جراء هذا الهجوم، وذلك من خلال إبرام الإتفاقيات الدولية و الإقليمية التي من شأنها مكافحة هذه الجريمة والتصدي لها، أو الحد من إرتكابها، كما أولت الدول أعضاء المجتمع الدولي عناية بإتخاذ ما يلزم من إجراءات وتدابير من أجل الحماية من ما يلحق بها من أضرار، وما تتكبده من خسائر من جراء استهدافها بالهجمات السيبرانية بوجه خاص والجرائم الإلكترونية بوجه عام،

ويُعد من أهم سُبل تحقيق هذا الغرض عضوية هذه الدول فى المنظمات الدولية و الإقليمية، التي يُبرم تحت مظلتها المُعاهدات والاتفاقيات التي من شأنها مكافحة تلك الجرائم، وهدياً على ذلك سنتناول فى هذا المطلب جهود منظمة الأمم المتحدة وكذلك جهود بعض المنظمات الدولية والإقليمية، والمُنظمات الدولية المتخصصة فى مكافحة الهجمات السيبرانية، ثم نذكر بعض الإتفاقيات الدولية المُبرمة من أجل مكافحة الهجمات السيبرانية.

الفرع الأول

جهود منظمة الأمم المتحدة

تُباشر منظمة الأمم المتحدة دورا هاما فى الحد من انتشار الجرائم السيبرانية، ومواجهة الآثار المُترتبة عليها، ومن أجل تحقيق ذلك نظمت العديد من المؤتمرات نذكر منها المؤتمر السابع الذي عقد في ميلانو 1985 حتى المؤتمر الثاني عشر في ٢٠١٠ بالإضافة إلى المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات والذى عقد تحت إشراف الأمم المتحدة في عام ١٩٩٤، وأسفر عن إصدار عدة توصيات ذات صلة بجرائم المعلومات بعضها تناول الأفعال التي تقع تحت طائلة الإجرام المعلوماتي، والبعض الآخر يتمثل في الإجراءات الواجب اتباعها لتطبيق القواعد الموضوعية وذلك من اجل الحد من انتشار الجرائم المعلوماتية ومواجهه المخاطر.

وهكذا أصدرت منظمة الأمم المتحدة عدة قرارات وتوصيات بشأن العمليات السيبرانية، كما أنشأت فرقا من الخبراء الحكوميين المعنيين بهذه العمليات، وناقشت هيئاتها أمن الفضاء السيبراني.

(ISSN: 2356 - 9492)

اولاً: قرارات ووثائق الجمعية العامة للأمم المتحدة بشأن الإرهاب السيبراني

أصدرت الجمعية العامة للأمم المتحدة عدة قرارات بشأن جرائم الإرهاب السيبراني نذكر منها على سبيل المثال بعض القرارات وهي:

القرار رقم 63/55 في ٤ ديسمبر ٢٠٠٠م الذي اصدار التوصية بأن تضمن الدول في قوانينها وممارساتها عدم توفير ملاذات آمنة لكل من يسيء استخدام تكنولوجيا المعلومات، وضمان حماية سرية المعلومات وسلامة أنظمة الحاسوب، ضد أي اعتداء غير مشروع، مع تقرير عقوبة على ذلك الفعل.

القرار رقم 121/56 في ١٩ ديسمبر ٢٠٠١، بشأن مكافحة سوء استخدام تكنولوجيا المعلومات، والذي دعا الدول الأعضاء عند وضع التشريعات الوطنية لمكافحة إساءة استعمال تكنولوجيا المعلومات أن تأخذ بالاعتبار عمل لجنة منع الجريمة والعدالة الجنائية.

القرار رقم 239/57، الصادر عام 2002، بشأن إرساء ثقافة عالمية للأمن السيبراني، الذي اعتمدت فيه قرارًا بشأن الأمن السيبراني والذي أكدت فيه على ضرورة دعم الجهود الوطنية بتبادل المعلومات والتعاون فى هذا الشأن وطنياً واقليمياً ودولياً بما يكفل التصدي للتهديدات السيبرانية بصفة، التي تتسم بطابع عابر للحدود الوطنية.

القرار 60/177، الصادر عام 2005، بشأن تشجيع التعاون الدولي لمكافحة الجرائم الإلكترونية، وتقديم المساعدة للدول الأعضاء في هذا المجال.

القرار رقم 64/211 الصادر عام 2010، الذي يدعو الدول إلى تحديث تشريعاتها بشأن الجرائم الإلكترونية، والخصوصية، والبيانات الشخصية، ونحو ذلك وأيضاً اعتماد اتفاقيات إقليمية بهذا الشأن[1].

القرار رقم 41/65 والذي صادقت عليه الجمعية العامة للأمم المتحدة فى يناير ٢٠١١، الذي دعا فيه على تقرير فريق الخبراء الحكوميين في مجال المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي. وتضمنت استنتاجات فريق الخبراء من بينها ما ذكرته من أن هناك دول تستحدث تكنولوجيا المعلومات والاتصال كوسائل للحرب والاستخبارات، وتلفت اللجنة الدولية في هذا الصدد انتباه الدول إلى عواقب الحرب السيبرانية، وهي مجموعة من الهجمات على شبكة الحواسيب خلال حالات النزاع المسلح، وقد تشمل هذه العواقب سيناريوهات كارثية مثل: التشويش على نظم مراقبة الملاحة الجوية، والتسبب بتصادم الطائرات، أو تحطمها، أو قطع إمدادات الكهرباء، أو الماء على السكان المدنيين، أو إلحاق أضرار بالمرافق الكيميائية أو النووية. وتُذكر اللجنة الدولية بضرورة التزام كل الأطراف في النزاعات المسلحة باحترام قواعد القانون الدولي الإنساني إذا لجأت إلى وسائل وأساليب الحرب الإلكترونية ومن هذه القواعد مبادئ التمييز والتناسبية والحيطة[2].

---

[1] انظر

SSCHJOLBERG, The History of Global Harmonication on Cybercrime Legislation, 2008, available at: https://www.cybercrimelaw.net/Cybercrimelaw.html

[2] بيان اللجنة الدولية للصليب الأحمر للأمم المتحدة ٢٠١١ بشأن المناقشات العامة لكافة بنود جدول الأعمال فيما يتعلق بنزع السلاح والأمن الجمعية العامة للأمم المتحدة الدورة 11 اللجنة الأولى البندان ٨٧ و١٠٦ من جدول الأعمال بيان اللجنة الدولية للصليب الأحمر، نيويورك، ١١ أكتوبر ٢٠١١

(ISSN: 2356 - 9492)

ثانياً: قرارات المجلس الاقتصادي والاجتماعي

افتتح المجلس الاقتصادي والاجتماعي دورته لعام ٢٠١٠ مُعلناً عن التحديات التي يطرحها الأمن السيبراني، و كذلك التهديدات والفرص التي يتيحها استخدام الإنترنت الآخذ في الاتساع، وقد شدد المجلس من بين عدة أمور على الحاجة إلى اتخاذ مبادرات دولية تكفل تبادل المعلومات وأفضل الممارسات التدريب والبحث، وإضافة إلى ذلك، أعلن المشاركون في المناقشة أنه يتعين على الأمم المتحدة أن توحد أداءها ، بشأن هذه القضية، مما سيؤدي حتما إلى زيادة التعاون بين البلدان بل وبين الدول والقطاع الخاص أيضا لضمان الأمن السيبراني [1] وحذروا من النطاق الدولي لحرب سيبرانية فعلية وعواقبها وخيمة سوف تحدث بشكل خطير إن لم يتم تدارك الأمر، ومن ثم لا بد أن تكون هناك استجابة منشقة بين الدول : ولا تكفي الآن إستراتيجيات اعتماد حلول على أساس مخصص وتقوية الدفاع [2] .

وقد دعا القرار أيضًا إلى اتباع نهج قائم على إدراك المخاطر، وإحاطة أصحاب المصلحة علما بالمخاطر ذات الصلة والتدابير الوقائية والردود الفعالة على نحو مناسب، كل في إطار الدور المنوط به. وطالب القرار بمزيد من العناية لموضوع الأمن الإلكتروني، حيث دعا الدول الأعضاء إلى تقديم موجزات لمبادراتها الرئيسية بشأن الأمن السيبراني وحماية الهياكل الأساسية الحيوية للمعلومات كي يتسنى إبراز ما يتم تحقيقه من الإنجازات وأفضل الممارسات والدروس المكتسبة والإجمالات التي تتطلب مزيدًا من التدابير على الصعيد الوطني، وقدم استقصاء

[1] المجلس الاقتصادي والاجتماعي الدورة الموضوعية لعام ٢٠١٠ نيويورك، ٢٨ يونية – ٢٢ يوليه ٢٠١٠ البند 13 (ب) من جدول الأعمال المؤقت المسائل الاقتصادية والبيئية تسخير العلم والتكنولوجيا لأغراض التنمية والتقدم المحرز في تنفيذ ومتابعة نتائج مؤتمر القمة العالمي لمجتمع المعلومات على الصعيد بن الإقليمي والدولي.

[2] المرجع نفسه (مناقشة الأوراق المالية الرقمية أو النظام النقدي الرقمي المستخدم في البلدان الإفريقية).

طوعيًا في شكل تقييم ذاتي للأمن الإلكتروني الوطني باعتباره أداة يمكن أن تساعد البلدان على استعراض الجهود الوطنية المبذولة في مجال الأمن السيبراني وحماية الهياكل الأساسية الحيوية للمعلومات[1].

وفي سبتمبر عام ٢٠١١ عقد المجلس الاقتصادي والاجتماعي للأمم المتحدة اجتماعا لمناقشة أمن الفضاء الإلكتروني والتنمية والقضايا والتحديات ذات الصلة، وحُددت أهداف الاجتماع بأنها تتمثل في بناء وعي على مستوى السياسات الدولية عبر تزويد أعضاء المجلس الاقتصادي والاجتماعي بالوضع والتحديات المتعلقة بأمن الفضاء الإلكتروني.

كما ناقش الاجتماع الفوارق الاقتصادية بين الدول، وعدم قدرة الدول النامية منها على مكافحة الجرائم السيبرانية، وكذلك افتقاد الشراكة بينها وبين الدول الصناعية، مما يؤدي إلى خلق ملاذ آمن لمهاجمي الفضاء السيبراني لارتكاب جرائمهم. كما تم مناقشة الحاجة إلى إبرام اتفاقية دولية بشأن الفضاء الإلكتروني بما يشمل احتمال البناء على اتفاقية بودابست باعتبارها تنسيقا بين الدول بشأن بعض الجرائم السيبرانية كالتعدي على حق المؤلف، والغش، واستغلال الأطفال في المواد الإباحية، وجرائم الكراهية، وانتهاكات أمن الشبكات. وقرر" لازاروس كابامبي" رئيس المجلس الاقتصادي والاجتماعي، أن أعضاء الاجتماع قد اتفقوا على أن الأمن السيبراني قضية عالمية، لا يمكن حلها إلا

[1] د. أميرة عبد العظيم محمد عبد الجواد المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، العدد الخامس والثلاثون، الجزء الثالث، 2020، ص ١٨٧.

(ISSN: 2356 - 9492)

عبر شراكة عالمية، لا سيما من خلال الأمم المتحدة التي يمكنها استخدام قدراتها الإستراتيجية والتحليلية لمعالجة مثل هذه القضايا[1].

ثالثاً: مؤتمر الأمم المتحدة الثامن لمنع الجريمة هافانا - كوبا ١٩٩٠ بشأن الجرائم ذات الصلة بالكمبيوتر

أكد المؤتمر على أنه ينبغي اتخاذ تدابير ملائمة ضد حالات إساءة الاستعمال المخلة لهذه التكنولوجيا، وأشار إلى مسألة الخصوصية التي يمكن أن تخترق عن طريق الاطلاع على البيانات الشخصية المخزنة داخل نظم الحسابات الآلية والتي تشكل انتهاكا لحقوق الإنسان، كما أكد عبر قواعده التوجيهية على ضرورة تشجيع اصدار التشريعات الحديثة التي تجرم وتتناول جرائم الحاسب الآلي باعتبارها نمطا من أنماط الجريمة المنظمة كغسيل الأموال والاحتيال المنظم وفتح حسابات وتشغيلها بأسماء وهمية، وقد أكد مؤتمر هافانا ١٩٩٠ عدة مبادئ أهمها: تحديث القوانين الجنائية الوطنية بما في ذلك التدابير المؤسساتية، وتحسين أمن الحاسب الآلي والتدبير الفنية، واعتماد إجراءات تدريب كافية للموظفين والوكالات المسئولة عن منع الجريمة الاقتصادية والجرائم المتعلقة بالحاسب الآلي والتحري والادعاء فيها، تلقين آداب الحاسب الآلي كجزء من مفردات مقررات الاتصالات والمعلومات، وزيادة التعاون الدولي من أجل مكافحة هذه الجرائم.

[1] د. محمد عادل محمد عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسس وقت السلم، دراسة على ضوء دليل، تالين، بشأن القانون الدولي المطبق على العمليات السيبرانية ٢٠١٢،٢٠١٧، ٢٠٢٠م، ص ١٢.

كما حث المؤتمر الدول الأعضاء على مضاعفة الأنشطة التي تبذلها على الصعيد الدولي من أجل مكافحة الجرائم المتصلة بالكمبيوتر بما في ذلك دخولها كأطراف في المعاهدات المتعلقة بتسليم المجرمين وتبادل المساعدة في المسائل الخاصة المرتبطة بهذه الجريمة، ونصح هذا القرار الدول الأعضاء بالعمل على أن تكون تشريعاتها ذات العلاقة بتسليم المجرمين وتبادل المساعدة في المسائل الجنائية تنطبق بشكل تام على الأشكال الجديدة للإجرام مثل الجرائم السيبرانية، وأن تتخذ خطوات محددة نحو مكافحة الجرائم المتصلة بالحاسب الآلي و الانترنت كما تكمل الأمم المتحدة رؤيتها بشأن الجريمة السيبرانية بصفة عامة بضرورة وضع أو تطوير[1] معايير دولية لأمن المعالجة الآلية للبيانات، و اتخاذ تدابير ملائمة لحل إشكاليات الاختصاص القضائي التي تثيرها الجرائم السيبرانية العابرة للحدود أو ذات الطبيعة الدولية، و إبرام اتفاقيات دولية تنطوي على نصوص تنظيم وإجراءات التفتيش والضبط المباشر الواقع عبر الحدود على الأنظمة الإلكترونية المتصلة فيما بينها والأشكال الأخرى للمساعدة المتبادلة بما يكفل حماية الافراد وسيادة الدولة.

[1] د. عبد الفتاح حجازي، الإثبات الجنائي في جرائم الكمبيوتر والإنترنت المرجع السابق، ص ١٩٠.

(ISSN: 2356 - 9492)

رابعاً: إنشاء فريق من الخبراء الحكوميين المعنيين بالعمليات السيبرانية

في عام ٢٠٠٤، أنشأت الجمعية العامة للأمم المتحدة مجموعة للخبراء الحكوميين لدراسة تأثير تطورات تكنولوجيا المعلومات والاتصالات على الأمن القومي والشئون العسكرية للدول، وقد أختتم المؤتمر أعماله بإصدار تقرير تضمن التوصيات من أهمها:

1. مواصلة الحوار بين الدول لمناقشة المعايير المتعلقة باستخدام تكنولوجيا المعلومات والاتصالات للحد من مخاطرها، وحماية البنى التحتية الإلكترونية للدول.
2. السعي لتحقيق تدابير بناء الثقة في مجال الحد من أخطار استخدام الدول لتكنولوجيا المعلومات والاتصالات، بما في ذلك تبادل الآراء الوطنية بشأن استخدامها.
3. تبادل المعلومات بشأن التشريعات الوطنية والمعلومات الوطنية واستراتيجيات وتقنيات وسياسات أمن الاتصال وأفضل الممارسات.
4. تحديد تدابير لدعم بناء القدرات في أقل البلدان نموا.

الفرع الثاني

الاتفاقيات الدولية في مجال مكافحة الهجوم السيبراني

تعد الاتفاقيات والمعاهدات الدولية من أهم صور التعاون الدولي بصفة عامة، وفي مجال مكافحة الجرائم الناتجة عن الهجوم السيبراني بصفة خاصة ومن بين المعاهدات والاتفاقيات التي تعمل على مكافحة الجرائم السيبرانية معاهدة بودابست لمكافحة جرائم الإنترنت، وتوصيات المجلس الأوروبي بشأن مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات.

اولاً: معاهدة بودابست لمكافحة جرائم الإنترنت

تعد معاهدة بودابست لمكافحة جرائم الإنترنت أولى المعاهدات المتعلقة بتلك الجرائم، والتي تمت في العاصمة المجرية بودابست في ٢٠٠١/١١/٢٣، والتي تبرز التعاون والتضامن الدولي في محاربة الجرائم السيبرانية، ويعد التوقيع على تلك المعاهدة الدولية الخطوة الأولى في مجال تكوين التضامن الدولي ضد تلك الجرائم التي تتم عبر شبكة الإنترنت والاستخدام السيء لها[1].

[1] د. منير محمد الجهيني، د. ممدوح محمد الجهيني جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر العربي الإسكندرية، ط ٢٠٠٤، ص: ٩٦

(ISSN: 2356 - 9492)

وقد وقعت على تلك المعاهدة ٢٦ دولة أوروبية بالإضافة إلى كندا واليابان، وجنوب أفريقيا والولايات المتحدة الأمريكية، وتضمنت ٤٨ مادة مُقسمة على أربعة فصول كالآتي:[1]

الفصل الأول تضمن تعريفات خاصة ببعض التعريفات الفنية، والثاني: يتضمن الإجراءات اللازم اتخاذها على المستوى المحلي لكل دولة وتنقسم إلى قسمين:

أولهما: يتعلق بالنصوص الجنائية الموضوعية على النحو التالي:

1. بشأن الجرائم ضد الخصوصية وسلامة وتواجد معلومات الحاسب ونظم الحاسب، ويشمل وصفا لأنواع متعددة من الجرائم.
2. الجرائم المتصلة بالحاسب شاملة استخدام الكمبيوتر في التزوير والأفعال الاحتيالية.
3. الجرائم المتعلقة بالمحتوى والمضمون.
4. الجرائم المتصلة بالتعدي على حقوق المؤلف.

و ثانيهما : القانون الإجرائي فيما يتصل بالإجراءات الجنائية شاملة الحفاظ على المعلومات المخزنة والأوامر الخاصة بتسليم الأدلة، وتتضمن كذلك تفتيش وضبط بيانات الحاسب المخزنة.

[1] د. هلالي عبد اللاه أحمد: الجوانب الموضوعية والإجرائية للجرائم المعلوماتية على ضوء اتفاقية بودابست 2001، دار النهضة العربية، ط1، ٢٠٠١.

كما تضمن الفصل الثالث: مسائل التعاون الدولي وتسليم الجناة والمساندة المشتركة والتعاون في التحريات وجمع بيانات المرور والحركة الخاصة بالبيانات،و الفصل الرابع: يتعلق بالانضمام والانسحاب من تعديل المعاهدة وفض المنازعات والتشاور بين الأعضاء.

وعلى الرغم من أن هذه الاتفاقية أوروبية المنشأ، إلا أنها مفتوحة للدول الأخرى لطلب الانضمام إليها لتعم الفائدة. وتتضمن الاتفاقية التعاون والعمل المشترك ما بين الدول الأعضاء وأعضاء القطاعات وأصحاب المصلحة ذوي الصلة، وهما ضروريان لبناء ثقافة للأمن السيبراني وفي الحفاظ عليها، وسبل مكافحة الجرائم السيبرانية، إذ تقرر:[1]

1. مواصلة اعتبار الأمن السيبراني في صدارة أنشطة الاتحاد ذات الأولوية والاستمرار في إطار مجالات اختصاصاته الرئيسية بدراسة مسألة توفير الأمن وبناء الثقة في استعمال الاتصالات تكنولوجيا المعلومات والاتصالات من خلال إذكاء الوعي، وتحديد أفضل الممارسات، وتطوير مواد التدريس المناسبة لتعزيز ثقافة الأمن الإلكتروني.
2. تعزيز العمل والتعاون وتبادل المعلومات مع جميع المنظمات الدولية والإقليمية ذات الصلة فيما يتعلق بالمبادرات المتصلة بالأمن السيبراني في مجالات اختصاصاتها، مع مراعاة احتياجات مساعدة البلدان النامية.

[1] وتعود أهمية توقيع هذه الاتفاقية إلى رغبة المجتمع الدولي لإيجاد صيغة دولية لمكافحة ومواجهة هذا الإجرام المستحدث وعلى ذلك بذلت الجهود الدولية لتحقيق هذه الرغبة، فبتاريخ ٢٠ نوفمبر تقدمت اللجنة الأوروبية لمشكلات الجريمة CDBC ولجنة الخبراء في حقل جرائم التقنية CYBER CRIME PC-CU ((بمشروع اتفاقية جرائم الكمبيوتر، وخضعت مواد الاتفاقية المقترحة للمناقشة وتبادل الآراء خلال الفترة من إصدار مشروعها الأول وحتى إعداد مسودتها النهائية التي أقرت لاحقا في بودابست وتعرف باتفاقية بودابست ٢٠٠١) اتفاقية الجرائم السيبرانية - سايبر كرايم) ، ولا شك في أن الاتفاقية قد بذل فيها جهد واسع ومميز يذكر للاتحاد الأوروبي ومجلس أوروبا ولا سيما في المسائل المتعلقة بجرائم الكمبيوتر وأغراضها منذ أواخر القرن الواحد والعشرين. للمزيد انظر د. هلالي عبد اللاه أحمد، اتفاقية بودابست 2001 لمكافحة جرائم المعلوماتية (معقبا عليها) ، دار النهضة العربية ، ط3، ٢٠١١ ص 130 و ما بعدها

(ISSN: 2356 - 9492)

3. تعيين نظام سريع وفعال للتعاون الدولي، والحفاظ بشكل سريع على البيانات المخزنة على أجهزة الكمبيوتر وحفظها والإفصاح الجزئي عن حركة هذه البيانات المخزنة على الكمبيوتر.[1]

وقد تناولت المعاهدة الجرائم التي تعتبر من أكثر الجرائم شيوعًا على مستوى العالم مثل الإرهاب السيبراني وعمليات تزوير بطاقات الائتمان ودعارة الأطفال. كما حددت المعاهدة الطرق الواجب اتباعها في التحقيق في جرائم الإنترنت، وتعهدت الدول الموقعة بالتعاون من أجل محاربتها، كما حاولت المعاهدة إقامة التوازن بين الاقتراحات التي تقدمت بها أجهزة الشرطة، وما عبرت عنه المنظمات المدافعة عن حقوق الإنسان ومزودي خدمات الإنترنت من قلق، حيث تخشى منظمات حقوق الإنسان من أن تحد المعاهدة من حرية الأفراد، وأن تؤدي الرقابة إلى انتهاك حقوق مستخدمي الإنترنت[2].

وفي عام ٢٠١٦ أصدرت لجنة اتفاقية الجرائم السيبرانية مذكرة توجيهية تتعلق بجوانب الإرهاب السيبراني بموجب اتفاقية بودابست، تعلن فيها أن الجرائم الموضوعية في الاتفاقية قد تكون أيضا أعمالا إرهابية على النحو المحدد في القانون المعمول به، وجاءت هذه المذكرة الإضافية بموجب الاتفاقية في الوقت المناسب لتسلط المذكرة الضوء على

[1] انظر https://www.itu.int/ar/mediacentre

[2] د. هلالي عبد اللاه أحمد: الجوانب الموضوعية والإجرائية للجرائم المعلوماتية على ضوء اتفاقية بودابست، دار النهضة العربية، ط1، ٢٠٠١.

أن هذه الاتفاقية ليست معاهدة مختصة بالإرهاب، إلا إنه يمكن القول: أن الجرائم الموضوعية في الاتفاقية يمكن أن تنفذ على أنها أعمال إرهابية، لتسهيل الإرهاب ولدعم الإرهاب، ومن ذلك الجانب التمويلي، أو الأعمال التحضيرية [1]

ثانياً: توصيات المجلس الأوروبي [2]

أصدر المجلس الأوروبي التوصية رقم ١٣/٩٥ في ١١/٩/١٩٩٥ في شأن مشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات، وحث الدول الأعضاء بمراجعة قوانين الإجراءات الجنائية الوطنية لكي تتلاءم مع التطور فى هذا المجال، ومن أهم ما ورد بها:

1. أن توضح القوانين إجراءات تفتيش أجهزة الكمبيوتر وضبط المعلومات التي تحويها ومراقبة المعلومات أثناء انتقالها.
2. أن تسمح الإجراءات الجنائية الوطنية لجهات التفتيش بضبط برامج الكمبيوتر والمعلومات الموجودة بالأجهزة وفقا لذات الشروط الخاصة بإجراءات التفتيش العادية، ويتعين إخطار الشخص القائم على الأجهزة بأن النظام كان

[1] د. منير محمد الجهيني، د. ممدوح محمد الجهيني جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر العربي الإسكندرية، ط ٢٠٠٤، ص: ٩٦

[2] د. مدحت رمضان جرائم الاعتداء على الأشخاص والإنترنت دار النهضة العربية، ط ٢٠٠٠، ص: ٨٠ وما بعدها.

(ISSN: 2356 - 9492)

محلا للتفتيش مع بيان المعلومات التي تم ضبطها، ويسمح باتخاذ إجراءات الطعن العادية في قرارات الضبط والتفتيش.

3. أن يسمح أثناء عملية التفتيش للجهات القائمة بالتنفيذ ومع احترام الضمانات المقررة بعد التفتيش إلى أنظمة الكمبيوتر الأخرى فى دائرة اختصاصهم والتي تكون متصلة بالنظام محل التفتيش، وضبط ما بها من معلومات، بشرط أن يكون هذا الإجراء ضروريا.
4. أن يوضح قانون الإجراءات الجنائية أن الإجراءات الخاصة بالوثائق التقليدية تنطبق في شأن المعلومات الموجود بأجهزة الكمبيوتر.
5. تطبق إجراءات المراقبة والتسجيل في مجال التحقيق الجنائي في حالة الضرورة فى مجال تكنولوجيا المعلومات، ويتعين توفير السرية والاحترام للمعلومات التي يفرض القانون لها حماية خاصة.
6. يجب إلزام العاملين بالمؤسسات الحكومية والخاصة التي توفر خدمات الاتصال بالتعاون مع سلطة التحقيق لإجراء المراقبة والتسجيل.
7. يتعين تعديل القوانين الإجرائية بإصدار أوامر لمن يحوز معلومات، سواء أكانت برامج، أم قواعد، أم بيانات تتعلق بأجهزة الكمبيوتر بتسليمها للكشف عن الحقيقة.
8. يتعين إعطاء سلطات التحقيق سلطة توجيه أوامر لمن يكون لديه معلومات خاصة للدخول على نظام من أنظمة المعلومات أو الدخول على ما يحويه من معلومات باتخاذ اللازم للسماح لرجال التحقيق بالاطلاع عليها. وأن تخول سلطات التحقيق بإصدار أوامر مماثلة لأي شخص لديه معلومات عن طريق التشغيل والمحافظة على المعلومات.

9. يجب تطوير وتوحيد أنظمة التعامل مع الأدلة الإلكترونية، وحتى يتم الاعتراف بها بين الدول المختلفة، ويتعين أيضا تطبيق النصوص الإجرائية الخاصة بالأدلة التقليدية على الأدلة الإلكترونية.

10. يجب تشكيل وحدات خاصة لمكافحة جرائم الكمبيوتر وإعداد برامج خاصة لتأهيل العاملين في مجال العدالة الجنائية لتطوير معلوماتهم في مجال تكنولوجيا المعلومات.

11. قد تتطلب إجراءات التحقيق من الإجراءات إلى أنظمة كمبيوتر أخرى قد تكون موجودة خارج الدولة، وتفترض التدخل السريع، وحتى لا يُمثل هذا الأمر اعتداء على سيادة الدولة والقانون الدولي، يجب وضع قاعدة قانونية صريحة تسمح بمثل هذا الإجراء، ولذلك كانت الحاجة إلى عمل اتفاقيات تنظم وقت وكيفية اتخاذ مثل هذه الإجراءات.

12. يجب أن تكون هناك إجراءات سريعة ومتناسبة ونظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهة أجنبية لجمع أدلة معينة، ويتعين عندئذ أن تسمح السلطة الأخيرة بإجراءات التفتيش والضبط. ويتعين كذلك السماح لهذه السلطة بإجراء تسجيلات للتعاملات الجارية، وتحديد مصدرها، ولذلك يتعين تطوير اتفاقيات التعاون الدولي القائمة.

الفرع الثالث

(ISSN: 2356 - 9492)

جهود بعض المنظمات العالمية المتخصصة والتحالفات الدولية

في مكافحة الإرهاب السيبراني

كان للمنظمات العلمية المتخصصة دوراً هاماً بشأن التعامل مع العمليات السيبرانية بأنواعها المختلفة، وتحقيق قدراً من الأمن في مجال المعاملات الإلكترونية ومن أبرز هذه المنظمات الاتحاد الدولي للاتصالات والمنظمة العالمية للملكية الفكرية، ومنظمة حلف شمال الأطلسي، وسوف نتناول بإيجاز جهود تلك المنظمات.

اولاً: الاتحاد الدولي للاتصالات

نشأ الاتحاد الدولي للاتصالات بموجب اتفاقية باريس عام ١٨٦٥ تحت اسم (اتحاد التلغراف الدولي)، ثم عدل الاسم ليصبح الاتحاد الدولي للاتصالات السلكية واللاسلكية، ثم في عام ١٩٤٧ انضم الاتحاد إلى هيئة الأمم المتحدة، وبات إحدى الوكالات المتخصصة في عمل الاتصالات تحت مظلة الأمم المتحدة.

يهدف الإتحاد إلى تعزيز التعاون الدولي للخدمات الهاتفية والسلكية واللاسلكية وتوسيع استخدامها بواسطة الجمهور وتطوير إمكانات الاتصالات السلكية واللاسلكية وتوزيع الموجات اللاسلكية، كما يقوم الاتحاد بتقديم التوصيات الخاصة والدراسات الفنية المتخصصة في الاتصالات اللاسلكية وجمع المعلومات ونشرها من أجل بناء قدرات الدول الأعضاء – ولاسيما البلدان النامية لتنسيق الإستراتيجيات الوطنية وحماية البنية التحتية للشبكات ضد المخاطر من خلال التوعية، والتقييم الذاتي، وبناء القدرات، وتوسيع نطاق المراقبة، والإنذار وقدرات الاستجابة للحوادث للدول والجهات المعنية، ويعمل الاتحاد بصورة وثيقة مع المنظمات الأخرى المعنية على (وضع المعايير المتعلقة بالأمن المعلوماتي؛ إذ يقوم الاتحاد بالاشتراك مع الوكالة الأوروبية لأمن الشبكات والمعلومات بنشر خريطة الطريق المتعلقة

بمعايير الأمن في مجال تكنولوجيا المعلومات والاتصالات، كما تعاون الاتحاد الدولي مع مجلس أوروبا لإنجاز الاتفاقية الأوروبية حول الجريمة الإلكترونية من أجل الاستعانة بها في عملية وضع إطار قانوني دولي[1].

وقد قام الاتحاد الدولي للاتصالات بإنشاء فريق متخصص معني بالشبكات الذكية من أجل جمع وتوثيق المعلومات والمفاهيم التي ستكون مفيدة من أجل إعداد توصيات لدعم تلك الشبكات من منظور الاتصالات [2]، وكان أحد الأدوار الأساسية التي أنيطت بالاتحاد الدولي للاتصالات في أعقاب القمة العالمية لمجتمع المعلومات ومؤتمر المندوبين المفوضين العام ٢٠٠٦ يتمثل في بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات فقد قام رؤساء الدول والحكومات وغيرهم من قادة العالم المشاركين في القمة العالمية لمجتمع المعلومات، وكذلك الدول الأعضاء في الاتحاد ، بتكليف الاتحاد باتخاذ خطوات ملموسة للحد من التهديدات وانعدام الأمن فيما يتصل بمجتمع المعلومات، ولتحقيق هذه الولاية أطلق الأمين العام للاتحاد برنامج الأمن السيبراني العالمي في عام ٢٠٠٧ ليكون إطارا للتعاون الدولي[3].

---

[1] د. خالد محمد نور عبد الحميد الطباخ المواجهة القانونية للإرهاب الإلكتروني الدولي، مجلة الدراسات القانونية والاقتصادية، جامعة مدينة السادات كلية الحقوق، مج ٣، ١٤، ٢٠١٧، ص ٢٣

[2] الفرق المتخصصة هي أداة من أدوات الاتحاد التي تعزز برنامج عمل لجان الدراسات من خلال توفير بيئة عمل بديلة لتطوير المواصفات بسرعة في مجالات عملها، مما يجعلها مثالية للتكنولوجيات المتغيرة والمتطورة بسرعة مثل الشبكات الذكية، ويتألف الفريق المتخصص بالشبكة الذكية من ممثلين من مختلف الدول الأعضاء، وسيقوم بالتعاون مع مجتمعات الشبكة الذكية في جميع أنحاء العالم (مثل: معاهد البحوث والمنديات والأوساط الأكاديمية)

[3] د. أميرة عبد العظيم محمد عبد الجواد المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام المرجع السابق، ص ٤٩٣

(ISSN: 2356 - 9492)

وقد أعلن الأمين العام للاتحاد الدولي للاتصالات عام ٢٠٠٧ عن إطلاق مبادرة أجندة شاملة بشأن الأمن السيبراني، تتضمن التوصل إلى إطار أو بروتوكول لتنسيق جهود مكافحة الجرائم السيبرانية، وبما يشمل تدابير قانونية، وتقنية، وإجرائية وتنظيمية، وتعاون دولي[1].

ويقترح الأمين العام للاتحاد الدولي للاتصالات خمسة مبادئ توجيهية الإحلال السلام وحفظه في العالم السيبراني الناشئ إدراكا منه للخطر المتنامي للهجوم السيبراني، وقد أعدت لوائح الاتصالات الدولية كإطار تنظيمي لمعالجة القضايا الناشئة والتحديات التي تصاحب عالم الاتصالات الجديد الذي تجسد في أواخر ثمانينات القرن الماضي، وقد صيغت هذه اللوائح لتعزيز الكفاءة والتنمية الدوليين، فضلا عن أنها تبرز تركيز الاتحاد على حماية الحق في الاتصال وفي الوقت نفسه إلحاق الضرر بالمرافق[2].

وعلى غرار ذلك، تتضمن المبادئ الخمسة التي اقترحها الأمين العام للاتحاد الدولي للاتصالات فيما يتعلق بالسلام السيبراني هذه القيم الجوهرية مع تحديد إجراءات والتزامات محددة من شأنها أن تضمن السلام والاستقرار في الفضاء السيبراني، وتنص هذه المبادئ على ما يلي[3]:

1- أن تلتزم كل حكومة بإتاحة نفاذ شعبها على الاتصالات.

---

[1] د. محمد عادل محمد عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسس وقت السلم دراسة على ضوء دليل تالين، بشأن القانون الدولي المطبق على العمليات السيبرانية ٢٠١٢-٢٠١٧، ٢٠٢٠م، ص: ٢٠٨

[2] د. أميرة عبد العظيم محمد عبد الجواد المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام المرجع السابق، ص: ١٩٤.

[3] 17) المرفوعة إلى عناية مؤتمر المندوبين المفوضين، مؤتمر المندوبين wtdc قرارات المؤتمر العالمي لتنمية الاتصالات لعام ٢٠١٧ (دبي، ٢٩ أكتوبر ١٦ نوفمبر ٢٠١٨، الاتحاد الدولي للاتصالات.-ppالمفوضين (١٨

2- أن تلتزم كل حكومة بتأمين الحماية لشعبها في الفضاء السيبراني.

3- أن يلتزم كل بلد بعدم إيواء الإرهابيين / المجرمين في أراضيه.

4- أن يلتزم كل بلد بألا من البلدان يكون الطرف الذي يبدأ شن هجوم سيبراني على غيره من البلدان.

5- أن يلتزم كل بلد بالتعاون مع غيره ضمن إطار دولي للتعاون لضمان السلام في الفضاء السيبراني.

وفي مسعى أكثر شمولا، تم في المؤتمر الإقليمي حول الأمن السيبراني بالتعاون مع الاتحاد الدولي للاتصالات في قطر عام ٢٠٠٨، دعوة جميع الدول لوضع وتنفيذ إطار وطني للأمن السيبراني وحماية البنية التحتية الحرجة للمعلومات والتي تعد بمثابة خطوة أولى في سبيل التصدي للتحديات التي تواجهها جراء اتصالها بتكنولوجيا المعلومات والاتصالات [1]: وفي نفس العام وقع الاتحاد الدولي للاتصالات والشراكة الدولية المتعددة الأطراف لمكافحة التهديدات السيبرانية (إمباكت) (IMPACT) مذكرة تفاهم رسميًا، بعدها أصبح مقر شراكة إمباكت في سايبر جايا بماليزيا، الذي يضم أحدث ما توصلت إليه التكنولوجيا، المقر الفعلي للبرنامج[2].

[1] د. خالد محمد نور عبد الحميد الطباخ المواجهة القانونية للإرهاب الإلكتروني الدولي، مجلة الدراسات القانونية والاقتصادية – كليه الحقوق – جامعة السادات – مجموعه 3ع1-2017، ص: ٣٤

[2] إمباكت هي مبادرة دولية مشتركة بين القطاعين العام والخاص لتعزيز قدرة المجتمع الدولية على منع الهجمات السيبرانية والدفاع ضدها والتصدي لها. ويوفر هذا التعاون للدول الأعضاء في الاتحاد البالغ عددها ١٩٢ دولة وغيرها من الجهات الخبرات الفنية والتسهيلات والموارد اللازمة لتعزيز قدرات المجتمع العالمي تعزيزاً فعالاً، وزيادة القدرة على منع الهجمات السيبرانية، والدفاع ضدها والتصدي لها، وقد جذب هذا البرنامج منذ إطلاقه دعم واعتراف الزعماء وخبراء الأمن السيبراني في أنحاء العالم. انظر، د. أميرة عبد العظيم محمد عبد الجواد المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام المرجع السابق، ص ٤٩٦

(ISSN: 2356 - 9492)

ثانياً: المنظمة العالمية للملكية الفكرية

إبان عام ١٩٦٧ تم التوقيع في ستوكهولم بالسويد على اتفاقية المنظمة العالمية للملكية الفكرية، وأصبحت هذه المنظمة إحدى الوكالات المتخصصة التابعة للأمم المتحدة اعتبارا من السابع عشر من ديسمبر عام ١٩٧٤، والتي من أهدافها حماية الملكية الفكرية في شتى أنحاء العالم عن طريق التعاون بين الدول الأعضاء والمنظمات الدولية الأخرى، وتعمل المنظمة على متابعة تنفيذ الاتفاقيات المتعلقة بالتصميمات الصناعية وتصنيف السلع التجارية وحماية الأعمال الإدارية والفنية وحقوق الإنتاج. كما تشجع المنظمة كذلك على توقيع معاهدات دولية جديدة وتقوم بالتنسيق بين التشريعات الوطنية، وتقديم المساعدات القانونية والفنية للدول النامية بهدف حماية الملكية الفكرية وتنميتها وتغطية بعض أوجه القصور في مجال التوثيق العلمي ونقل التقنية الحديثة[1].

وبالرجوع إلى اتفاقية إنشاء هذه المنظمة تتضح غايات هذه المنظمة في دعم الملكية الفكرية في جميع أنحاء العالم بجميع صورها المصنفات الأدبية والفنية والعلمية والاختراعات، ومع تزايد الحاجة العالمية لحماية البرامج شكلت هذه المنظمة مجموعة عمل تضم عددًا من الخبراء بهدف حماية برامج الحاسب الآلي، وبعد سلسلة من الاجتماعات والدراسات حول الأساليب المثلى لحماية برامج الحاسوب، ساد الاتجاه لدى أغلب الدول إلى الميل إلى خضوع برامج الحاسوب لقوانين حماية حق المؤلف. وقد جاءت منظمة التجارة العالمية عام ١٩٩٤ لتؤيد هذا التوجه وتستكمل طريقها من خلال إبرام اتفاقية تريبس (TRIPS) المتعلقة بمواصفات التجارة المرتبطة بحقوق الملكية الفكرية وما

[1] د. طارق عزت رخاء المنظمات الدولية المعاصرة، دار النهضة العربية القاهرة، ٢٠٠٦، ص: ٢١٤.

تفرضه من التزامات على الدول الأعضاء الفرض إجراءات تنفيذية وعقوبات جنائية لمواجهة أي اعتداء على حق المؤلف وخاصة القراصنة.[1]

ثالثاً: منظمة حلف شمال الأطلسي

دفع عجز حلف الناتو في مواجهة الهجمات السيبرانية على إستونيا عام ٢٠٠٧ وجورجيا عام ٢٠٠٨ إلى تكوين وحدة للدفاع السيبراني، مقرها تالين عاصمة إستونيا، وعمل على تطوير المفهوم الإستراتيجي للحلف بحيث أصبح الفضاء السيبراني منطقة لعمليات الحلف، وأن عليه أن يطور قدراته الدفاعية السيبرانية بما يشمل مساندة ودعم حلفائه الذين يتعرضون لهجمات سيبرانية، وأنه وفقا لذلك فإن أي هجوم يتم على أوروبا أو أمريكا الشمالية يعتبر هجومًا ضد الجميع[2].

ولذا نفذت الناتو السياسة الخاصة بها في مجال الدفاع السيبراني في ٢٠٠٨؛ من أجل حماية مواردها التكنولوجية وتلك الخاصة بالدول الأعضاء[3] وكجزء من هذه السياسة، أنشأ الحلف هيئة معينة بإدارة الدفاع السيبراني، وفريقا للاستجابة للحوادث الحاسوبية، يكفل إرسال فرق الدعم السريع إلى فرادى البلدان الأعضاء، ومركزا للتميز من أجل الدفاع السيبراني التعاوني [4]، ويضم هذا المركز الذي يوجد مقره في إستونيا خبراء يضطلعون بالبحث والتدريب في مجال الأمن السيبراني.

---

[1] د. عبد الصبور عبد القوي الجريمة الإلكترونية، دار العلوم للنشر والتوزيع القاهرة، ٢٠٠٨، ص ١٥٩-١٦٣

[2] تقرير التوازن العسكري ٢٠١١ الذي يصدر سنويا عن المعهد الدولي للدراسات الإستراتيجية هو تقرير مستقل وشامل يعرض للقدرات العسكرية العالمية واقتصاديات الدفاع لنحو ٧٠ دولة حول العالم. يشير للتطور العسكري العالمي والقضايا الأمنية الراهنة.

[3] الدفاع ضد الهجمات السيبرانية.. الناتو
https://www.nato.int/cps/en/natohq

[4] انظر
https://www.nato.int/cps/en/natolive/official_texts

(ISSN: 2356 - 9492)

وتضم البلدان التي ترعى هذا المركز: إستونيا ولاتفيا وليتوانيا وألمانيا وإيطاليا والجمهورية السلوفاكية وإسبانيا[1]. ووقعت الناتو مذكرة تفاهم بشأن الأمن السيبراني مع إستونيا والولايات المتحدة الأمريكية والمملكة المتحدة وتركيا سلوفاكيا[2]

الفرع الرابع

المجهودات الفقهية لمواجهة المخاطر السيبرانية

ظهرت بعض الاجتهادات الفقهية لمعالجة اشكالية الهجمات السيبرانية، و قد كان دليل تالين للقانون الدولي المنطبق على الحرب الإلكترونية، دوراً هاما في العمل على معالجة إشكالية الهجمات السيبرانية؛ و كذلك المبادئ الواردة في إعلان ريتشي بشأن مبادئ الاستقرار السيبراني والسلام السيبراني والذي أعده فريق الرصد الدائم المعني بأمن المعلومات التابع للاتحاد العالمي للعلماء (WFS)، و سوف نتناول بعض نماذج هذه المجهودات باستعراض دليل تالين والهجمات السيبرانية، و إعلان إيريتشي بشأن مبادئ الاستقرار السيبراني والسلام السيبراني (الصادر عن الاتحاد العالمي للعلماء).

اولاً: دليل تالين والهجمات السيبرانية

تبنى (NATO) إعداد دليل تالين، بشأن القانون الدولي المطبق على الحرب السيبرانية، بإصداريه عامي ٢٠١٣، ٢٠١٧، وهو غير ملزم بشأن القواعد الدولية التي تحكم العمليات السيبرانية، حيث استضاف المركز التعاوني للدفاع

[1] مركز التميز للدفاع السيبراني التعاوني

WWW.ccdcoe.org

[2] أبريل ٢٠١٠nato–news أبرمت الناتو واستونيا اتفاقا بشأن الدفاع السيبراني

https://www.nato.int/cps/en/natolive/news_62894.htm

في مدينة تالين عاصمة إستونيا، و تم صياغته في الفترة من عام ٢٠٠٩ وحتى ٢٠١٧، بجهود فريق خبراء قانونيين دوليين (IGE) برئاسة البروفيسور Michael N.Schmitt[1]

وقد عرف خبراء تالين العمليات السيبرانية بأنها: تلك التي تتضمن استخدام القوة أو التهديد بها ضد سلامة الأراضي أو الاستقلال السياسي لأي دولة أو على وجه آخر لا يتفق ومقاصد الأمم المتحدة؛ وأن العملية السيبرانية تشكل استخداما للقوة عندما يكون حجمها وأثرها قابلا للمقارنة مع العمليات غير السيبرانية التي تصل لمستوى استخدام القوة[2].

وقد ظهر الإصدار الأول من الدليل عام ٢٠١٣، وتضمن (٩٥) قاعدة السلوك الدول في سياق الحرب السيبرانية، مع تعليقات على كل قاعدة، وفي عام ٢٠١٧ ظهر الإصدار الثاني، وتضمن (١٥٤) قاعدة، تشكل مستوى أكثر عمقا بشأن معالجة العمليات السيبرانية، مع تعليقات على كل قاعدة، تبين النقاش الذي دار بشأنها، وأن أي وجهة نظر قبلت بالأغلبية، وموقف الأقلية إن وجد، وكذلك حالات الإجماع. وانتهى الدليل إلى أن القواعد الدولية السارية فاعلة إلى حد كبير، ويمكن تطبيقها على العمليات السيبرانية، وتعرض الدليل لبعض الإشكاليات القانونية في المجال

[1] د. محمد عادل محمد عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسس وقت السلم – دراسة على ضوء دليل تالين بشأن القانون الدولى المطبق على العمليات السيبرانية – 2013 – 2017 – 2020 – المرجع السابق، ص 69

[2] القاعدة (١١) من دليل تالين والمعنونة بـ تعريف استخدام القوة ...

(ISSN: 2356 - 9492)

السيبراني، كسيادة الدول، وقواعد ممارسة الاختصاص، وقانون مسئولية الدول إضافة إلى قانون حقوق الإنسان، وقانون البحار، والقانون الدبلوماسي، والقنصلي[1].

واستناداً لدليل تالين فإن العمليات السيبرانية تُعد استخداما للقوة عندما يكون مستواها وتأثيرها متقاربين مع العمليات غير السيبرانية، وذلك اعتمادا على معيار النطاق والأثر في تحديد الدرجة التي يجب أن يصل إليها الهجوم السيبراني كاستخدام للقوة أو هجوم مسلح، وعليه يمكن اعتبار هجوم سيراني كهجوم مسلح إذا أحدث ضررا، أو يصل إلى درجة الشدة، والمقصود بذلك أن يحدث أضرارا مادية جسيمة، واستند خبراء تالين في اعتماد هذا الاختبار على رأي محكمة العدل الدولية في قضية نيكاراجوا ، على أساس أنه الأنسب لتحديد الدرجة المناسبة للأعمال التي تصل إلى حد استخدام القوة والهجمات المسلحة، وبالقياس على الهجمات السيبرانية، اتفق خبراء دليل تالين في الإصدار الثاني، على أن قيام دولة بتزويد قوات أو أفراد بأجهزة وتدريبهم لشن هجمات سيبرانية ضد دولة أخرى يعد ذلك استخداما غير مشروع للقوة[2] .

[1] د. محمد عادل محمد عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسس وقت السلم المرجع السابق، ص ٧٠

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

وطبق هذا المعنى بصورة واضحة فى الهجمة السيبرانية العالمية– فيروس الفدية – التي تأثر بها العديد من الدول و ذلك فى ٢٧ يونيو ٢٠١٧ مثل بريطانيا ومصر على سبيل المثال، و قد أُثير الجدل حول مدى اعتبار تلك الهجمات عملا من أعمال الحرب، وقد وضعت اللجنة مجموعة من الصفات التي يجب أن تتسم بها الهجمات السيبرانية حتى ترقى إلى درجة الهجوم المسلح، وبالتالي تعطي الدولة المعتدى عليها حق الدفاع الشرعي وتفعيل المادة ٥١ من الميثاق

حيث اعتبرت اللجنة أن أهم المعايير التي يجب الاستناد إليها في تحديد المستوى المطلوب لوصول العمليات السيبرانية إلى درجة الهجوم المسلح يتمثل في جسامة هذا التصرف أو حدته، ومدى تأثيره على الدولة المعتدى عليها، وأن يكون هناك ضرر مادي حالا على الأفراد والممتلكات في الدولة المعتدى عليها بهجوم سيبراني، وفي سبيل ذلك قامت اللجنة بالمقارنة بين أثر الهجمات العسكرية التقليدية والهجمات السيبرانية استنادا إلى قياس نتائج الأخيرة، وفيما إذا كانت منتجة لأضرار مماثلة للهجمات العسكرية التقليدية أم لا : فالهجمات السيبرانية يمكن لها أن تنتج مثل هذا الضرر المماثل للهجمات العسكرية التقليدية أو يفوقه كما لو حدث اعتداء سيبراني على شبكات الكمبيوتر الخاصة بمطار إحدى الدول؛ مما أدى إلى مقتل الآلاف بسبب الخلل الذي أحدثته الهجمة، وأدى إلى تصادم الطائرات هبوطا وصعودا، ففي مثل هذه الحالة تعتبر العملية السيبرانية هجومًا عسكريا، أما تلك التصرفات التي لا تلحق مثل هذا

(ISSN: 2356 - 9492)

النوع من الضرر فتخرج حسب اللجنة من دائرة الهجوم العسكري، إلا في الحالة التي تضر فيها هذه العمليات السيبرانية بمصلحة وطنية حساسة للدولة المعتدى عليها دون أن تتصل بضرر مادي محسوس [1] .

وتجدر الإشارة إلى أن هذا الدليل ليس أصلا دوليا رسميا أو ملزما، أو يمثل وجهة نظر (NATO)، أو الدول التي شارك خبراء من جنسيتها في وضع الدليل، وإنما هو رؤية الخبراء المستقلين الذين صاغوه بصفاتهم الشخصية، ومع ذلك، فإن أهميته كبيرة، كوثيقة رائدة في مجال العمليات السيبرانية، وخطوة مهمة لتنظيم الفضاء السيبراني، وإن كانت غير كافية ويلزم أن تتبعها خطوات أخرى[2].

ثانياً: إعلان ايريتشى بشأن مبادئ الاستقرار السيبراني والسلام السيبراني (الصادر عن الاتحاد العالمي للعلماء)

صدر إعلان إيريتشي بشأن مبادئ الاستقرار السيبراني والسلام السيبراني بواسطة فريق الرصد الدائم المعني بأمن المعلومات التابع للاتحاد العالمي للعلماء (WFS)[3] ، حيث اعتمدته الجلسة العامة للاتحاد العالمي للعلماء في الدورة الثانية والأربعين للحلقات الدراسية الدولية بشأن الطوارئ العالمية وفي إيريتشي (صقلية) في ٢٠ أغسطس ٢٠٠٩ ؛ وقد نشر فريق الرصد ورقات عديدة بشأن الأمن السيبراني والحرب السيبرانية، ويتناول بانتظام قضايا أمن المعلومات

[1] د. أميرة عبد العظيم محمد عبد الجواد المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام المرجع السابق، ص: ٥٠٦

[2] د. محمد عادل محمد عسكر وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسس وقت السلم المرجع السابق، ص ٧٠

[3] تم إنشاء الاتحاد العالمي للعلماء عام 1972، في إيرتشه – جزيرة صقلية، ويهدف إلى التعاون الدولي في مجالات العلم والتكنولوجيا.

باعتبارها موضوعا من موضوعات الطوارئ الحرجة أثناء الدورات العامة للاتحاد العالمي للعلماء التي تنعقد في شهر أغسطس من كل عام في إيريتشي، و قد ابرز بعض العناصر التشغيلية الأساسية للسلام السيبراني، وهي تخلص فى:

1- اعتراف الحكومات بأن القانون الدولي يضمن للأفراد التدفق الحر للمعلومات والأفكار وتنطبق هذه الضمانات أيضا على الفضاء السيبراني وينبغي عدم فرض القيود إلا عند الاقتضاء، على أن تخضع لعملية مراجعة قانونية.

2- العمل لوضع مدونة مشتركة بين الحكومات لتنظيم السلوك السيبراني دولياً، بما في ذلك أحكام إجرائية تتعلق بالمساعدة في التحقيق بما يكفل احترام الخصوصية وحقوق الإنسان، ودعم الجهود المبذولة في سبيل إنفاذ القانون الدولي وإطار والتعاون ضد مرتكبي الجرائم السيبرانية.

3- عدم استخدم الفضاء السيبراني بأي شكل من شأنه التي من شأنها استغلال المستعملين.

4- ينبغي للحكومات والمنظمات والقطاع الخاص بما في ذلك الأفراد، تنفيذ برامج شاملة للأمن وتحديثها بناء على أفضل الممارسات والمعايير المقبولة دوليا، واستعمال تكنولوجيات حماية الخصوصية والأمن.

5- تطوير تكنولوجيات آمنة تعزز القدرة على التصدي وتقاوم نقاط الضعف.

6- مشاركة الحكومات فى جهود الأمم المتحدة بما يكفل النهوض بالأمن والسلام السيبراني دولياً، وتفادى استعمال الفضاء السيبراني من أجل النزاعات.

(ISSN: 2356 - 9492)

وقد دعا الاتحاد العالمي للعلماء منذ سنة ٢٠٠٢ إلى العمل على وضع قانون عالمي للفضاء السيبراني – وأنه من الأفضل أن يكون تحت رعاية الأمم المتحدة [1] – خاصة في مجال الاستخدامات العدوانية والعسكرية للفضاء السيبراني.

المطلب الثاني

سُبل التعاون الدولي والإقليمي فى مكافحة الهجمات السيبرانية

يُعد التعاون الدولي والإقليمي من أهم وسائل مكافحة الهجمات السيبرانية والأمر الذي بات معه من الأهمية بمكان إلى تعاون الدول أطراف المجتمع الدولي من أجل مكافحة هذه الجريمة وذلك فى إطار إبرام الإتفاقيات الثنائية ومتعددة الأطراف فى مجال التعاون الدولي من حيث جمع الأدلة والتحري وملاحقة الجاني والإختصاص، وذلك على سبيل المثال وليس الحصر، وهو ما لجأت إليه تلك الدول وعلى ذلك سنلقى الضوء بإيجاز على بعض هذه الصور من خلال هذا المطلب.

---

[1] انظر

Toward a Universal order of Cyberspace managing Threats from Cybercrime of Cyberya

تقرير وتوصيات فريق الرصد الدائم المعني بمجتمع المعلومات والتابع لاتحاد العلماء العالمي، ١٩ نوفمبر ٢٠٠٢، تقرير مقدم إلى القمة العالمية لمجتمع المعلومات

http://www.itu.int/dms/pub/itu-s/md./pdf

الفرع الأول

التعاون القضائي فى مكافحة الهجوم السيبراني

يُعد التعاون القضائي من أهم صور التعاون بين الدول من أجل مكافحة الهجمات السيبرانية، ومن هذه الصور تبادل المعلومات، ونقل الإجراءات، والإنابة القضائية الدولية، وتسليم المجرمين.

أولاً: الإنابة القضائية الدولية

يُقصد بها "تكليف جهة قضائية من الدولة لجهة قضائية في دولة أخرى بإتخاذ إجراء قضائي نيابة عنها طبقاً لمعاهدة أو اتفاق بين دولتين"[1]. والغاية منها تيسير الإجراءات القضائية التي تُتخذ من أجل التحقيق في الجريمة، واحترام مبدأ السيادة الذي يُشكل فى كثير من الأحيان عقبة أمام الإجراءات حال أن تكون الجريمة عابرة للحدود مما يصعب معه سماع الشهود أو التفتيش أو التحقيق، فلا سبيل لإتمام تلك الإجراءات بدون التعاون بين الدول في هذا المجال.

ثانياً: تسليم المجرمين

عرفه البعض بأنه " نظام في علاقات الدول من مقتضاه أن تتخلى دولة عن شخص موجود على اقليمها لدولة أخرى بناء على طلبها لتتولى محاكمته عن جريمة منسوب إليه ارتكابها أو لتنفيذ حكم صادراً من محاكمها وذلك باعتبارها

[1] د. رعد فجر الراوي: شرح قانون أصول المحاكمات الجزائية، الجزء الثاني، طبعة أولى، الهاشمي للكتاب الجامعي، بغداد، 2016، ص 244

(ISSN: 2356 - 9492)

صاحبة الإختصاص"[1]؛ ونظم القانون الدولي هذا النظام بأن يكون من خلال اتفاق دولي أو إقليمي بين الدول فعلى سبيل المثال نظمته المادة (24) من اتفاقية بودابست عام 2001[2].

وهذه الصورة تُعد آلية لتسليم مرتكبي الجرائم الهاربين إلى دولة أخرى تفادياً لتنفيذ العقوبة وقد نظمت إتفاقية بودابست لمكافحة الجرائم الإلكترونية عام 2001 ضوابط تسليم المجرمين.

ثالثاً: نقل الإجراءات

هو إجراء يهدف إلى نقل الإجراءات الجنائية المتعلقة بالتحقيق فى الجريمة السيبرانية التي تقوم بها الدولة الى دولة أخرى وذلك لتحقيق مصلحة من نقل الإجراءات، شريطة أن يمون هذا الفعل مؤثم لدى الدولة المُقدم لها طلب نقل الإجراءات، ويكون إتمام هذا الإجراء بموجب معاهدة جماعية أو اتفاقيات ثنائية.

رابعاً: تبادل المعلومات

يُعد تبادل المعلومات بين الدول سعياً لمكافحة الجريمة من أهم صور التعاون الدولي ويُقصد به أن يكون التعاون قائم بين أطراف المعاهدة أو الاتفاقية من أجل توفير المعلومات الموثقة الصحيحة التي من شأنها التحقق من صحة الفعل

[1] د. على حسين الخلف، د. سلطان عبد القادر الشناوي: المبادئ العامة في قانون العقوبات، الطبعة الثانية، العاتق لصناعة الكتاب، 2010، ص 120، مُشار اليه د. رعد فجر الراوي – القصور التشريعي في مواجهة الهجمات السيبرانية، مجلة كلية القانون للعلوم القانونية والسياسة، مجلد 10، عدد 39، العراق، 2021، ص 204

[2] انظر: اتفاقية بودابست لمكافحة الجرائم الالكترونية، عام 2001

السيبراني المؤاثم جنائياً وتعقب وملاحقة مُرتكبيه وهو الأمر الذي يقتضي تبادل الوثائق والمعلومات التي يتم طلبها من سلطات خارج الحدود الإقليمية للدولة للمساعدة في التحقق من الجريمة السيبرانية التي هي بصدد التحقق من عدم مشروعيتها.

الفرع الثاني

التعاون التقني فى مكافحة الهجوم السيبراني

ومما هو جدير بالذكر أن التعاون القضائي ليس كافياً أما التطور التقني المستمر في المجال السيبراني واستخدام الحاسب إذ أن الجريمة السيبرانية بوجه عام والهجوم السيبراني بوجه خاص ليس لها وسائل محددة وأيضاً يسهل إخفائها مما يتطلب أن يكون المحقق في تلك الجريمة على دراية كافية بالوسائل والأدوات الإلكترونية لكشف الجريمة وأن يكون عالماً بأحدث الوسائل التقنية المتعلقة بالجريمة التي هو بصدد التحقق منها، وهو ما يتطلب أن يكون التعاون التقني بين الدول متماشياً جنباً إلى جنب والتعاون القضائي ومُكملاً له وهذا الأمر يقتضى تقديم برامج تدريبية من الدول ذات الخبرات في هذا المجال إلى الدول النامية ونقل الخبرات إليها والمساهمة في إعداد كوادر مؤهلة تقنياً للعمل على مكافحة تلك الجرائم تكون على علم بمخاطر الجرائم السيبرانية وكيفية إختراق شبكات نظم المعلومات من خلال الفضاء السيبراني وغير ذلك من المناهج التدريبية.

كما تجدر الإشارة، بعد العرض الموجز للجهود الدولية و التعاون الدولي في مكافحة الجرائم السيبرانية بوجه عام و الهجمات السيبرانية بوجه خاص و هي الجريمة التي تعنى بها الدراسة، أن ما تبذله المنظمات الدولية و الإقليمية من

(ISSN: 2356 - 9492)

جهود لمكافحة الهجمات السيبرانية، و ما أدركته الدول أطراف المجتمع الدولي من أهمية التعاون الدولي لمكافحة تلك الهجمات، قد يكون يُقابله بعض الأمور التي تقف حائلاً أمام تحقيق الغاية المرجوة مُتمثلة فى مكافحة الهجوم مما يدعو إلى الحاجة إلى بذل المزيد من الجهود والسعي وراء مزيد من التعاون، ومن هذه الصعوبات نذكر أن الفعل الإجرامي ليس مُحدد على سبيل الحصر من حيث كيفية إرتكابه وتعريفه، إضافة إلى ذلك أن استخدام الحاسب الآلي والإنترنت فى تطور دائم و مستمر وهو ما يحد من مجابهة التشريعات التي تُسن من أجل مكافحة الهجوم السيبراني لما ما يقتضيه الأمر من ضرورة مُسايرة التشريعات للتطور التقني للوسائل المُستخدمة فى الهجوم وهو ما يتطلب تدخل تشريعي بتعديل وسن التشريعات بصفة مُستمرة لمواكبة التطور التقني، يُضاف إلى ذلك أنه بات من الأهمية بمكان التنسيق بين الجهات المعنية بالدول أعضاء المجتمع الدولي فيما يتعلق بمكافحة الهجوم السيبراني، فى مجالات تعقب الهجوم والتحقق من إن كان مُرتكب فى إقليم خارج حدود الدولة وكذلك ملاحقة الجاني، و هذا يقتضى مزيداً من التنسيق وينبغي أن يكون هذا التنسيق فى إطار إتفاقيات ثُنائية تَهدِف إلى تحقيق الغاية من إبرامها للتغلب على العقبات التي تواجه الدول فى مكافحة الهجوم كالاختصاص على سبيل المثال كما ينبغي مواجهة كافة الصعوبات التي تقف حائلاً أمام مكافحة جرائم الهجوم بإجراءات تُصاغ فى إتفاقيات مُلزمة لأطرافها بما يَكفُل إتخاذ الإجراءات اللازمة تجاه هذا الهجوم وردع مُرتكبيه و فى سبيل ذلك ينبغي أن يكون مجال تبادل المعلومات و إجراءات التحقق والتحري والملاحقة مُلزم لأطراف الإتفاق كما ينبغي أن لا يكون هناك مُقاربات فى تعاريف الجرائم المعلوماتية وصورها ووسائل إرتكابها حتى لا يكون الإختلاف ثغرة تتسبب فى إفلات المُعتدى من إنزال العقوبة وردعه.

الخاتمة

مما لا ريب فيه أن التطور التكنولوجي المستمر في مجال تقنية المعلومات والاتصالات بات يُشكل إساءة استخدامه من قبل البعض اثراً سلبياً يتمثل في صورة ارتكاب جرائم الكترونية، ومن هذه الجرائم الهجمات السيبرانية عابرة الحدود التي تنتهك خصوصية الفضاء السيبراني بهدف تدمير معلومات أو الحصول عليها بما يُلحق ضرراً بالغاً بالدولة المُعتدى عليها.

ومما لا شك أنه بات من الأهمية بمكان أن تتعاون الدول أعضاء المجتمع الدولي من أجل التصدي لهذه الجريمة و العمل على توحيد الجهود للتصدي لها و ذلك من خلال إبرام الاتفاقيات الدولية لدعم الأمن السيبراني و قد تناول هذا البحث إبراز المفاهيم المتعلقة بالسيبرانية و الجرائم التي يُنتهك بها الفضاء السيبراني بوجه عام و الهجمات السيبرانية بوجه خاص، و كذلك المفاهيم ذات الصلة، ثم تناول دور التعاون الدولي من أجل التصدي للجرائم التي تنتهك الفضاء السيبراني، من أجل القاء الضوء على السيبرانية و ما يتعلق بها من مفاهيم و أيضاُ ما يتعرض له الفضاء السيبراني من إنتهاكات قد تُشكل جرائم عابرة للحدود، و استنباط ما شاب آليات مواجهة الانتهاكات السيبرانية من قصور ينبغي العمل على معالجته من أجل التصدي للجرائم السيبرانية و تعقب مرتكبيها و تحديد الجاني و ردعه، و قد أسفر البحث عن بعض النتائج التي تم التوصل إليها، و عرض ما إنتهى إليه من توصيات.

النتائج

(ISSN: 2356 - 9492)

1- عدم فعالية الإتفاقيات الدولية والإقليمية فى تحقيق الأهداف المرجوة من إبرامها فى التصدي للجرائم السيبرانية بوجه عام والهجوم السيبراني بوجه خاص.

2- تواجه بعض الدول أعضاء المجتمع الدولي بوجه عام والدول النامية منها بوجه خاص بعض المعوقات والصعوبات التي قد تقف حائلاً أمام التصدي للإنتهاكات السيبرانية مما ينبغي على هذه الدول أن يتوافر لديها الرغبة والإرادة في التصدي لتلك الإنتهاكات.

3- لا تزال المنظمات الدولية والإقليمية في حاجة إلى بذل مزيد الجهد لمكافحة الهجمات السيبرانية.

4- أليات مكافحة بعض الدول للإنتهاكات السيبرانية بإعتبارها من الجرائم العابرة للحدود ليست كافية لتحقيق الحد الأدنى من حماية الأمن السيبراني، لعد إمتلاكهم للقوة البشرية المواكبة للتطور التكنولوجي المستمر مما يترتب عليه إفلات مرتكبي تلك الانتهاكات من العقوبة وبالتالي لا يتحقق الردع العام والخاص.

التوصيات

1- بات من الأهمية بمكان إبرام إتفاقية دولية وإقليمية وثنائية تكون مُلزمة لإطرافها لتنظيم إستخدامات الدول للفضاء السيبراني وتجريم الإعتداء عليه مع إقرار عقوبات رادعة وملاحقة الدول المُعتدية من أجل تحقيق الأمن السيبراني.

2- بذل الدول أعضاء المجتمع الدولي مزيد من السعي من أجل انشاء هيئات متخصصة فى تقنية تتبع مصدر الهجمات السيبرانية وتحديده.

3- تطوير وسائل ترقب الهجوم السيبراني والإنذار من إحتمالية وقوعه بما يكفل تحقيق فعالية حماية الأمن السيبراني.

4- تدريب كوادر فنية متخصصة والحاقهم ببرامج تدريبية متطورة وفق أحدث التقنيات التكنولوجية لتتبع مصادر الانتهاكات السيبرانية وتحديد مرتكبيها.

5- سعى واستمرار الدول لسن وتعديل تشريعاتها الداخلية بما يتناسب والتطور التقني الدائم و المستمر لتكنولوجيا الشبكات و الإنترنت.

6- السعي لتكثيف التعاون الدولي بين الدول من أجل حماية الأمن السيبراني من الانتهاكات التي قد تتعرض له تلك الدول للحد والتصدي للمخاطر المترتبة على تلك الانتهاكات.

المراجع

المراجع العربي:

1. اتفاقية بودابست لمكافحة الجرائم الالكترونية، عام 2001
2. أميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام، مجلة الشريعة والقانون، العدد الخامس والثلاثون، الجزء الثالث، 2020
3. القاعدة (١١) من دليل تالين والمعنونة بـ تعريف استخدام القوة
4. الإتحاد الدولي للإتصالات – دراسة تأمين شبكة المعلومات والاتصالات – قطاع تنمية الاتصال – دراسة خلال الفترة 2006- 2010

(ISSN: 2356 - 9492)

https://www.Itu.Int/net/Itunews/issues/2010/9/Pdf/201009-20-ar.pdf

5. المجلس الاقتصادي والاجتماعي الدورة الموضوعية لعام ٢٠١٠ نيويورك، ٢٨ يونية – ٢٢ يوليه ٢٠١٠ البند 13 (ب) من جدول الأعمال المؤقت المسائل الاقتصادية والبيئية تسخير العلم والتكنولوجيا لأغراض التنمية والتقدم المحرز في تنفيذ ومتابعة نتائج مؤتمر القمة العالمي لمجتمع المعلومات على الصعيد بن الإقليمي والدولي.

6. المادة (1/49) من البروتوكول الإضافي الأول لعام 1977، الملحق بإتفاقيات جنيف الأربعة 1949.
7. بيان اللجنة الدولية للصليب الأحمر للأمم المتحدة ٢٠١١ بشأن المناقشات العامة لكافة بنود جدول الأعمال فيما يتعلق بنزع السلاح والأمن الجمعية العامة للأمم المتحدة الدورة 11 اللجنة الأولى البندان ٨٧ و١٠٦ من جدول الأعمال بيان اللجنة الدولية للصليب الأحمر، نيويورك، ١١ أكتوبر ٢٠١١
8. تقرير التوازن العسكري ٢٠١١ الذي يصدر سنويا عن المعهد الدولي للدراسات الإستراتيجية هو تقرير مستقل وشامل يعرض للقدرات العسكرية العالمية واقتصاديات الدفاع لنحو ٧٠ دولة حول العالم. يشير للتطور العسكري العالمي والقضايا الأمنية الراهنة
9. دليل تالين – مجموعة مبادئ أُعدت من قبل خبراء القانون الدولي الإنساني – 2013 – وكان مايكل شميت من أبرز المشاركين فى هذه المجموعة – صدر الدليل بالتعاون بين الخبراء وحلف شمال الأطلنطي وبدعم من فريق مؤلف من خبراء السيبرانية واللجنة الدولية للصليب الأحمر والقيادة الليبرالية الأمريكية الذين شاركوا في المداولات
10. حسن فياض: الهجمات السيبرانية من منظور القانون الدولي الإنساني، الموقع الرسمي للجيش اللبناني، 2020

11. حسن مظفر الروز: الفايروسات والحاسب الإلكتروني، المخاطر المحتملة وسبل الحد منه، المجلة العربية العلمية للفتيان، المنظمة العربية للتربية والثقافة والعلوم، المجلد الأول، العدد الثاني، 1997

12. حسين المحمدي بوادي: الإرهاب الدولي بين التجريم والمكافحة، دار الفكر العربي، 2006

13. حنين جميل أبو حسين، الإطار القانوني لخدمات الأمن السيبراني، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، عمان، الاردن،2021

14. خالد وليد محمود، الهجمات عبر الإنترنت، ساحة الصراع الإلكتروني الجديدة، سلسلة دراسات ودراسة السياسات – المركز العربي للأبحاث، قطر، 2013

15. خالد محمد نور عبد الحميد الطباخ المواجهة القانونية للإرهاب الإلكتروني الدولي، مجلة الدراسات القانونية والاقتصادية – كليه الحقوق – جامعة السادات – مجموعه 3ع1–2017

16. رعد فجر الراوي: شرح قانون أصول المحاكمات الجزائية، الجزء الثاني، طبعة أولى، الهاشمي للكتاب الجامعي، بغداد، 2016

17. سامي الشوا: الغش المعلوماتي كظاهرة إجرامية مستحدثة، بحث مقدم فى مؤتمر الجمعية المصرية للقانون الجنائي، القاهرة، 25:26 أكتوبر، 1993

18. سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، دار النهضة العربية، مصر، 2017

19. صالح بن على بن عبد الرحمن الربيعة – الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت – هيئة الاتصالات وتقنية المعلومات – المملكة العربية السعودية، 2018

(ISSN: 2356 - 9492)

20. طارق عزت رخاء المنظمات الدولية المعاصرة، دار النهضة العربية القاهرة، ٢٠٠٦

21. طلال محمد الحاج إبراهيم: الهجمات الالكترونية والمسؤولية الجنائية للقادة، المجلة القانونية والقضائية، وزارة العدل، مركز الدراسات القانونية والقضائية، السنة 12، العدد الأول، 2018

22. عادل عبد الصادق: اسلحة الفضاء السيبراني فى ضوء القانون الدولي الإنساني، وحدة الدراسات المستقبلية

23. عادل عبد الصادق: القوة الالكترونية اسلحة الدمار الشامل فى عصر الفضاء الإلكتروني، المركز العربي لأبحاث الفضاء الإلكتروني، قضايا إستراتيجية، 2012

24. عادل عبد الصادق: موقع ويكليكس وتحدى عالم الاستخبارات الأمريكي، ملف الأهرام الإستراتيجي، مركز الاهرام للدراسات السياسية والإستراتيجية، اكتوبر 2012

25. عباس بدران: الحرب السيبرانية – الاشتباك فى عالم المعلومات، مركز دراسات الحكومة السيبرانية، بيروت، 2010

26. عبد الصبور عبد القوي الجريمة الإلكترونية، دار العلوم للنشر والتوزيع القاهرة، ٢٠٠٨

27. عبد الله حسين آل حجراف القحطانى – تطوير مهارات التحقيق الجنائي فى مواجهة الجرائم المعلوماتية "دراسة تطبيقية فى هيئة التحقيق والادعاء العام بمدينة الرياض، رسالة ماجستير، المملكة العربية السعودية، الرياض، 2014

28. عبد الله بن عبد العزيز بن فهد: بحث بعنوان "الإرهاب الإلكتروني فى عصر المعلومات" ، مقدم إلى المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية فى قانون الإنترنت" المنعقد بالقاهرة فى الفترة من 4:2 يونيو 2008

29. عبد الله عبد الكريم عبد الله، جرائم المعلومات والإنترنت (الجرائم الإلكترونية)، طبعة أولى منشورات الحلبي الحقوقية، لبنان، 2007

30. على حسين الخلف، د. سلطان عبد القادر الشناوي: المبادئ العامة في قانون العقوبات، الطبعة الثانية، العاتق لصناعة الكتاب، 2010، ص 120، مُشار اليه د. رعد فجر الراوي – القصور التشريعي في مواجهة الهجمات السيبرانية، مجلة كلية القانون للعلوم القانونية والسياسة، مجلد 10، عدد 39، العراق، 2021

31. عصام فاعور ملكاوي: الفضاء الإلكتروني ساحة حرب دولية مفترضة، أربد للبحوث والدراسات القانون، جامعة إربد الأهلية، عمادة البحث العلمي والدراسات العليا، مجموعة 18 – ع2، تموز 2015

32. فرد كابلان – ترجمة لؤي عبد المجيد، المنطقة المعتمة – التاريخ السري للحرب السيبرانية، عالم المعرفة، المجلس الوطني للثقافة والفنون والأدب، الكويت، 2019

33.قرارات المؤتمر العالمي لتنمية الاتصالات لعام ٢٠١٧ (17wtdc) المرفوعة إلى عناية مؤتمر المندوبين المفوضين، مؤتمر المندوبين المفوضين (١٨ –pp) دبي، ٢٩ أكتوبر ١٦ نوفمبر ٢٠١٨، الاتحاد الدولي للاتصالات.

34. مجلة كلية القانون الكويتية العالمية، العدد الثاني، السنة الخامسة، 5 يونية 2017

35. محمد عادل محمد عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسس وقت السلم، دراسة على ضوء دليل، تالين، بشأن القانون الدولي المطبق على العمليات السيبرانية ٢٠١٢،٢٠١٧، ٢٠٢٠م.

(ISSN: 2356 - 9492)

36. محمد عبيد الكعبي، الجرائم الناشئة عن الإستخدام الغير مشروع لشبكة الإنترنت، دار النهضة العربية، القاهرة، بدون سنة نشر

37. مدحت رمضان جرائم الاعتداء على الأشخاص والإنترنت دار النهضة العربية، ط ٢٠٠٠

38. مصطفى جاد: مستقبل الإرهاب السيبراني – مقال، ندوة المركز الدولي للدراسات المستقبلية والإستراتيجية، 11 إبريل 2012، جريدة السياسة الدولية، مؤسسة الأهرام المصرية، إعداد شريهان نشأت المنيرى، انظر http:/www.siyassa.org.eg//news Content/6/51/2450

39. مصطفى محمد موسى: الإرهاب الإلكتروني، بدون دار نشر، طبعة أولى،2009

40. مفهوم الهجمات السيبرانية والمسئولية الناشئة عنها في ضوء التنظيم الدولي المعاصر: العدد الرابع، السنة الثامنة، 2016

41. منير البعلبكي – المورد قاموس إنجليزي عربي، دار العلم للملايين، بيروت، 2004

42. منير محمد الجهيني، د. ممدوح محمد الجهيني جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر العربي الإسكندرية، ط1، ٢٠٠٤

43. نور أمير الموصلى – الهجمات السيبرانية في ضوء القانون الدولي الإنساني – رسالة ماجستير، الجامعة الافتراضية السورية، 2021

44. هدى حامد قشقوش: جرائم الحاسب الإلكتروني فى التشريع المقارن، دار النهضة العربية، مصر، 1992

45. هلالي عبد اللاه أحمد: الجوانب الموضوعية والإجرائية للجرائم المعلوماتية على ضوء اتفاقية بودابست، دار النهضة العربية، ط1، ٢٠٠١.

46. هلالي عبد اللاه أحمد: جرائم الحاسب والإنترنت بين التجريم الجنائي وآليات المواجهة، دار النهضة العربية، 2015

47. يحي ياسين سعود، الحرب السيبرانية في ضوء القانون الدولي الإنساني، المجلة القانونية في الدراسات والبحوث القانونية، كلية الحقوق، فرع الخرطوم، المجلد الرابع، العدد الرابع، 2018

المراجع الأجنبي:

1. Albi Kociblli, Aggression, from Cyber-Attacks To ISIS:Why International low Struggles to Adapt,2017 voI39
2. Christian Agrum ,Words for Understanding Cyber Security , Enjoying a calm Internet, Edition, October 1, 2020, p. 280
3. Ebert Hannes and Maurer Tim. ”Cybersecurity”- oxford bibliographies, Last Modified - 11 January 2017
4. Gianpiero Greco - Cyber-Attacks as aggression crimes in cyberspace in the context of international law-O.P p 43
5. Belfer center for - The future of power. Press realizes -Harvard , Joseph S Nye 31 JANUARY 2011 - Kennedy Scholl -Science and international Affairs
6. Jonathan A.OPHARD,"Cyber warfare and the crime of aggression:the Need for individual Accountability on tomorrow Battlefield, Duke law and technology" O.P , P1
7. Julia Cresswell – Oxford Dictionary of Word Origins : Cybernetics – Oxford Reference Online – Oxford University Press – 2010 – P 56

(ISSN: 2356 - 9492)

8. Kevin L. Miller, The Kampala Compromise and Cyberattacks: Can there Be an international Crime of Cyber-Aggression? Southern California interdisciplinary law Journal, 2014, vol.23, p.217

9. K.Saalbach,"Cyberwar, Methods and practice", version 9.o, university of Osnabruck 17 Jun 2014,p.6.

10. Michael N.Schmitt& Liis Vihul, Tallinn Manual 2.0 on the International Law Applicable to Cyber, pretations, Cambridge University press, 2017, note 13, Rule 32, p.168

11. Michael N. Schmitt, "Peacetime Cyber Responses and wartime Cyber Operations inder International Law: An Analytical Vade Mecum", Harvard National Security Journal, Vol.8, 2017

12. Michmitt – Computer Network Attack and The Use of force in international Low – Thoughts on a normative Framework – Co:ombia Journal of transnation Low – 1998-1999 – p.890

13. SSCHJOLBERG, The History of Global Harmonication on Cybercrime Legislation, 2008, available at: https://www.cybercrimelaw.net/Cybercrimelaw.html

14. Tang Lan , Zhang Xin , Harry D.Raduege , Jr.,Dmitry I. Grigoriev, pavan Duggal, and Stein Schjolberg,"Global Cyber Deterrence Views from China, the U.S., Russia, India, and NORWAY", The EastWest Institute, PRINTED in the United States, 2010, P1

15. The International Telecommunication Union - ITU - Toolkit for cybercrime Legislation - Geneva - 2010 - p.12

المواقع الالكترونية

1. https://www.itu.int/ar/mediacentre

أبرمت الناتو واستونيا اتفاقا بشأن الدفاع السيبراني nato-news أبريل ٢٠١٠

2. https://www.nato.int/cps/en/natolive/news_62894.htm
3. WWW.ccdcoe.org
4. https://www.nato.int/cps/en/natolive/official_texts

الدفاع ضد الهجمات السيبرانية.. الناتو

5. https://www.nato.int/cps/en/natohq