النظام القانوني الدولي لمُكافحة المَخاطر السيبرانية

د . هاني محمد خليل إبراهيم العزازي

دكتوراة فى القانون الدولي العام – كلية الحقوق – جامعة الزقازيق

المُقدِّمة

موضوع البحث:

شهد المجتمع الدولي خلال العقد الأخير مَوجة انتشار واسعة لتكنولوجيا الأجهزة الحاسوبية والشبكة المعلوماتية التي أحدثت ثورة فى الطريقة التي نعيش بها فى حياتنا، كالمرونة فى الحصول على المعلومات، واعتماد العديد من الخدمات والبِنَى التحتية الأساسية عليهم.

هذا وقد أدَّى التطوُّر السريع فى مجال تقنية المعلومات والاتصالات وشبكة الإنترنت فى العالم كلِّه إلى ظهور أنماط جديدة من الجرائم، جاءت عن طريق الاستغلال السيِّء للتكنولوجيا، ممَّا ترتَّب معه خلق ظاهرة إجرامية جديدة، وهي الجرائم المُتعلِّقة بالحاسب الآلي والإنترنت، والتي تتمُّ عن طريق هجمات واختراقات وتسلُّل داخل النظم المعلوماتية، والتي تُعرَف بالهجمات من خلال الفضاء السيبراني، إذ أصبح الفضاء السيبراني عُرْضة للانتهاكات من قِبَل مُخترِقي الشبكات، سواء أكانوا دُولًا أو غيرها ممَّن يَملكون هذه التقنيات المعلوماتية؛ بغرض إمَّا تدمير تلك النظم أو الحصول على معلومات سِرِّيَّة، سواء عسكرية أو اقتصادية، الأمر الذي يُنبِّه بوجود مخاطر على الصعيد الدولي إذا لم يتمَّ تدارُك هذه الظاهرة التي سوف ينشأ عنها -إذا ما تُركت- خسائر هائلة على المستوى العسكري والاقتصادي والاجتماعي لجميع دول العالم، ممَّا يَستوجب معه -والحال كذلك- إيجاد سبيل للتصدِّي لهذه الظاهرة.

لذا قامت العديد من الدول باعتماد إستراتيجيات من شأنها دعم الجانب العسكري فى الفضاء السيبراني، ليس فقط ضدَّ الهجمات التي قد يقوم بها الأفراد والقراصنة بل أيضًا ضدَّ احتمال استخدام الدول لمثل هذا المجال الجديد فى الصراع، ولذلك بات من الضروري توحيد الجهود الدولية لوضع الأطر القانونية والتنظيمية لمُواجهة المخاطر السيبرانية، وآثارها على المستوى الدولي.

أهَمِّيَّة البحث:

إنَّ مُكافحة الهجوم السيبراني وجرائم الإنترنت أصبح من الأهَمِّيَّة بمكان بأن نبحث فى السبل التي يجب اتِّباعها للتصدِّي لتلك الجرائم العابرة للحدود، والتي تستلزم تحديد ماهيتها وخصائصها وطبيعتها وخصائص مُرتكبيها. كذلك لا بُدَّ أن نبحث المخاطر السيبرانية وأثرها على تهديد السِّلْم والأمن الدوليين، وكذا الجهود الدولية لمُواجهة الهجوم السيبراني.

بناءً على ما سبق فإنَّ الحدَّ من الهجوم السيبراني ومُكافحة الجريمة السيبرانية على المستوى الدولي لا بُدَّ له من تواجُد روح التعاون بين الأنظمة القانونية الداخلية للدول.

إشكالية البحث:

الإشكالية التي يُثيرها هذا البحث والتي تقتضي البحث لها عن إجابة هي: ما هي الجرائم السيبرانية؟ وما هي صورها؟ وما هي الطبيعة القانونية للمخاطر السيبرانية؟ وكيف تُؤثِّر المخاطر السيبرانية على السِّلْم والأمن الدوليين؟ وما هي الجهود الدولية لمُواجهة المخاطر السيبرانية؟

منهج البحث:

إنَّ إشكالية البحث لها دورٌ رئيس فى اختيار المنهج الذي يجب اتِّباعه فى تناول موضوع البحث، وعلى ذلك اتَّبعنا المنهج التحليلي والاستقصائي، وذلك من خلال تحليل الموضوع من أمَّهات الكتُب والمراجع ذات العلاقة، والأبحاث والدراسات التي تناولت الموضوع، مع بيان رأي الفِقه فى تلك المسألة.

خُطَّة البحث:

تناولت الدراسة هذا الموضوع فى ثلاثة فصول، فى محاولة من الباحث للإحاطة بجميع جوانب الموضوع دون الخروج عنه، فجاءت الخُطَّة كالآتي:

الفصل الأوَّل: ماهية المَخاطر السيبرانية وصورها:

المبحث الأوَّل: ماهية المَخاطر السيبرانية والمفاهيم المُرتبطة بها.

المبحث الثاني: صور المَخاطر السيبرانية.

الفصل الثاني: المَخاطر السيبرانية وأثرها على تهديد السِّلْم والأمن الدوليين:

المبحث الأوَّل: المَخاطر السيبرانية وحقُّ الدفاع الشرعي وفق المادة ٥١ من ميثاق الأمم المتحدة من استخدام القوَّة السيبرانية.

المبحث الثاني: المَخاطر السيبرانية والقانون الدولي الإنساني.

الفصل الثالث: الجهود الدولية لمُواجهة المَخاطر السيبرانية:

المبحث الأوَّل: بعض جهود التعاوُن الدولي بشأن تنظيم العمليات السيبرانية.

المبحث الثاني: المجهودات الفقهية لمُواجهة المَخاطر السيبرانية.

الفصل الأوَّل
ماهية المَخاطر السيبرانية وصورها

تمهيد وتقسيم:

لقد ساعد التطوُّر العلمي التكنولوجي على ازدياد الجرائم السيبرانية، فالثورات العلمية والتكنولوجية هيَّأت المجال الخصب لإحداث تغييرات متنوِّعة على كافة المستويات وفي كافة المجالات، كما ساعد فى ارتكاب الجرائم السيبرانية الطبيعة الخاصَّة لجرائم التقنية الحديثة، واختلافها عن الجرائم التقليدية فى سهولة ارتكابها على الأجهزة الإلكترونية أو بواسطتها، كما يَسهل ارتكابها عبر الحدود، وأنَّ تنفيذها لا يستغرق إلا دقائق مَعدودة، وأحيانًا يتمُّ فى ثواني مَعدودة، كذلك صعوبة الرقابة على الإنترنت أو المُحاسبة على ما يُنشر فيه؛ ممَّا جعل الإنترنت مقرًا للإرهابيين، ويهدف الإرهابيون للقيام بهذه العمليات إلى زعزعة الأمن والإخلال بالنظام، والاستيلاء على الأموال العامة والخاصة، وإلحاق الضرر بالمَرافق العامة والاتِّصال والمواصلات.

لذا فإنَّ إدراك ماهية المَخاطر السيبرانية، وتحديد الطبيعة الخاصة لهذه المَخاطر يتَّخِذ أهَمِّيَّة بالغة لسلامة التعامُل مع هذه الظاهرة، ونطاق مَخاطرها الاقتصادية والأمنية والاجتماعية والثقافية، وهذا ما سأتناوله فى هذا الفصل من خلال المباحث التالية:

المبحث الأوَّل: التعريف بمصطلح المَخاطر السيبرانية والمفاهيم المُرتبطة به.

المبحث الثاني: طبيعة المَخاطر السيبرانية وسماتها.

المبحث الثالث: صور المَخاطر السيبرانية.

المبحث الأوَّل

التعريف بمُصطلح المَخاطر السيبرانية والمفاهيم المُرتبطة به

يتعيَّن لتحديد ماهية المَخاطر السيبرانية أن نتعرَّض لتعريفها، ثم نُبيِّن المفاهيم المُرتبطة بها. ومن ثَمَّ سوف نُقسِّم المبحث إلى مطلبين على النحو التالي:

المطلب الأوَّل: التعريف بمصطلح المَخاطر السيبرانية.

المطلب الثاني: المفاهيم المُرتبطة بالمَخاطر السيبرانية.

المطلب الأوَّل

التعريف بمصطلح المَخاطر السيبرانية

كلمة السيبرانية، مُشتقَّة من الكلمة اللاتينية « سايبر Cyber » ومعناها تخيُّلي أو افتراضي، والسايبر كلمة يَجري استخدامها لوصف الفضاء الذي يضمُّ الشبكات العنكبوتية المُحوسَبة، ومنظومات الاتصال والمعلومات، وأنظمة التحكُّم عن بُعد. وتعني: كلَّ ما يتعلَّق أو يرتبط بالحواسيب وتكنولوجيا المعلومات والواقع الافتراضي، ومنها اشتُقَّت صفة السيبرانية والسيبراني Cybernetics وتعني: عِلم التحكُّم الأوتوماتيكي، أو علم الضبط. وتعني أيضًا: القيادة والتوجيه، والذي يعني: « علم الاتصالات وأنظمة التحكُّم الآلي فى كلٍّ من الآلات والأشياء الحية »[١]. ويرى البعض أنَّ السيبرانية تعني: فضاء الإنترنت أو العالم الافتراضي[٢]. فالسيبرانية هي حرب تخيُّلية تقع فى الفضاء الشبكي غير الملموس، تُحاكي الواقع بشكل تام، إذ تتلخَّص وسائل الصراع فيها بالمُواجهات الرقمية، والبرمجيات التقنية، والجنود الافتراضيون، وطلقات من لوحات المفاتيح، ونقرات المُبرمجين، فى بيئة افتراضية تصل آثارها إلى ملامح الحياة المادية، إذ هي حربٌ بلا دماء، فهي عمليات تُشَنُّ ضدَّ أو عبر حاسوب أو نظام حاسوبي بواسطة تيار البيانات الرقمية.

ولبيان المقصود بالمَخاطر السيبرانية لا بُدَّ أن نعرف البيئة التي تحدث فيها المَخاطر، وهي الفضاء السيبراني:

(١) منير البعلبكي « المورد: قاموس إنكليزي - عربي »، دار العلم للملايين، بيروت ٢٠٠٤، ص: ٢٤٣.
(٢) د. صالح بن علي بن عبد الرحمن الربيعة، الأمن الرقمي وحماية المستخدم من مَخاطر الإنترنت، هيئة الاتصالات وتقنية المعلومات، المملكة العربية السعودية، ٢٠١٨، ص: ٦.

ويُعرف الفضاء السيبراني بأنَّه: مجال افتراضي من صُنع الإنسان، يعتمد على نُظُم الكمبيوتر وشبكات الإنترنت، وكم هائل من البيانات والمعلومات والأجهزة، وقد عرَّف الاتحاد الدولي للاتصالات الفضاء السيبراني على أنَّه: «المجال المادي وغير المادي الذي يتكوَّن وينتج عن عناصر هي: أجهزة الكمبيوتر، الشبكات، البرمجيات، حوسبة المعلومات، المحتوى الإلكتروني، مُعطيات النقل والتحكُّم الرقمي»(١). فى حين ركَّز البعض الآخر فى تعريفه للفضاء السيبراني على المنظور العسكري، وأكَّد على أنَّ الفضاء السيبراني هو الذراع الرابعة للجيوش الحديثة(٢). وعرَّفته الوكالة الفرنسية لأمن أنظمة الإعلام (ANSSI)، وهي وكالة حكومية مُكلَّفة بالدفاع السيبراني الفرنسي، بأنَّه: «فضاء التواصُل المشكل من خلال الربط البيني العالمي لمُعدَّات المُعالجة الآلية للمُعطيات الرقمية»(٣). فهو بيئة تفاعلية حديثة، تشمل عناصر مادية وغير مادية، مكوَّنة من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات، والمُستخدمين، سواء مُشغلين أو مُستعملين.

كما عرَّفه أستاذ العلوم السياسية الأمريكي «جو ناي» بأنَّه: القُدرة على استخدام الفضاء الإلكتروني لخلق مزايا، والتأثير على الأحداث فى البيئة التشغيلية الأخرى(٤).

فالفضاء السيبراني هو تلك البيئة الافتراضية التي تعمل بها المعلومات السيبرانية والتي تتصل عن طريق شبكات الكمبيوتر، وكما يُعرَّف أيضًا بأنَّه: المجال الكهرومغناطيسي لتخزين وتعديل أو تغيير البيانات المتَّصِلة والمُرتبطة بشبكة البنية التحتية الطبيعية، ويتضمَّن عملية الاندماج ما بين الإنترنت والمحمول وأجهزة الاتصالات والأقمار الصناعية، والفضاء الإلكتروني أكبر من الإنترنت؛ لما يحتويه من قُدرات توجيهية للطاقة التي تُوجد فى جزءٍ من الموجات الكهرومغناطيسية»(٥).

(١) انظر في ذلك:

The International Telecommunication Union , ITU Toolkit for Cybercrime Legislation , Geneva , 2010,p.12.

(٢) د. عباس بدران، الحروب الإلكترونية، الاشتباك في عالم متغيّر، مركز دراسات الحكومة الإلكترونية، بيروت، لبنان، ٢٠١٠، ص: ٤.

(٣) انظر في ذلك:

Ebert Hannes and Maurer Tim." Cyber Security " oxford bibliographies , Last Modified : 11 January,2017.

(٤) انظر:

Joseph . S. Nye , Cyberpower (Haward Kennedy School , Belfer center for science and International Affairs 2010 ,Available at :

http://www.Belfercenter.Ksg. Harvard .Edufilescyber –power ,pdf,P05

(٥) انظر: د. عادل عبد الصادق، الفضاء الإلكتروني والرأي العام، تغيُّر المجتمع والأدوات والتأثير، المركز العربي لبحوث الفضاء الإلكتروني: قضايا إستراتيجية، ٢٠١٣، ص: ٣٩.

ويُعدُّ الفضاء السيبراني فى وقتنا الراهن وحسب المفهوم الأمريكي، البُعد الخامس بعد حروب البرِّ والبحر والجو والفضاء، كما أعلنت حكومة المملكة المتحدة أنَّ إستراتيجيتها للحرب السيبرانية أخذت منحًى أبعد من مجرَّد تأمين المملكة المتحدة ضدَّ الهجمات الإلكترونية، لتُصبح فى الواقع إستراتيجية تسعى لتطوير الأسلحة الإلكترونية لاستخدامات المستقبل.

وتُعرَّف المَخاطر بأنَّها: عبارة عن الضرر الذي يُهدِّد أمن الأفراد والبيئة والجماعات البشرية، لكنَّه يُوشك أن يحدث- أو حدث فعلًا - ويُمكن احتواؤه إن لم يتفاقم. فالمَخاطر تشتمل على كلِّ تهديد يستهدف مؤسَّسات الدولة باستخدام الأيدلوجيات أو استخدام مُكوّنات القُدرة لدولة ضدَّ دولة أخرى، حيث يمكن أن يكون إقليم الدولة أو استقلالها أو أمنها مهدَّدًا بضرر، ويُمكن أن تأتي التهديدات من الخارج أو من داخل الدولة[1].

المطلب الثاني
المفاهيم المُرتبطة بالمَخاطر السيبرانية

هناك العديد من المفاهيم المُرتبطة بالمَخاطر السيبرانية، ومن أهمِّها ما يلي:

الأمن السيبراني: هو مجموعة من العمليات التقنية الحديثة والمُمارسات التي تحمي الشبكات وأجهزة الكمبيوتر والبيانات من الهجمات والأضرار والوصول غير المُصرَّح به. وفي ضوء التقنيات الحديثة، عُرِّف الأمن السيبراني والأمن المادي بأنَّه: مجموعة من الأدوات والإستراتيجيات الأمنية والمبادئ التوجيهية ونهج إدارة المخاطر والإجراءات والتدريب والخبرة العملية والتأمين والتكنولوجيا، والتي يُمكن استخدامها لحماية الفضاء السيبراني والتنظيم وموارد المُستخدِم [2].

كما عرَّفه الاتحاد الدولي للاتصالات بأنَّه: «مجموع الأدوات والسياسات والمفاهيم الأمنية والضمانات الأمنية والمبادئ التوجيهية والتقنيات ونهج إدارة المَخاطر التي يُمكن استخدامها لحماية البيئة الإلكترونية وتنظيم أصول المُستخدِم،

(١) تيري ديبيل، إستراتيجية الشئون الخارجية منطق الحكم الأمريكي، ترجمة: وليد شحادة، دار الكتب العربية، مؤسَّسة محمد بن راشد آل مكتوم، بيروت، ٢٠٠٩، ص: ٢٥٨.

(٢) انظر:

Christian Agrum, Words for Understanding Cyber Security: Enjoying a Calm Internet, Edition, October, 1, 2010, p.280.

وتشمل توصيل أجهزة الحوسبة، والمُوظَّفين، والبنية التحتية، والخدمات، ونُظُم الاتصالات السلكية واللاسلكية، ومُجمل المعلومات المُرسَلة أو المُخزَّنة فى البيئة الإلكترونية»[١].

كما يُمكن تعريف الأمن السيبراني انطلاقًا من أهدافه بأنَّه النشاط الذي يُؤمِّن حماية الموارد البشرية والمالية المُرتبطة بتقنيات الاتصالات والمعلومات، ويضمن إمكانات الحدِّ من الخسائر والأضرار، التي تترتَّب فى حال تحقُّق المَخاطر والتهديدات؛ علَّها تُتيح إعادة التوسُّع إلى ما كان عليه، بأسرع وقت مُمكن، بحيث لا تتوقَّف عجلة الإنتاج، وبحيث لا تتحوَّل الأضرار إلى خسائر دائمة. فهو النشاط أو العملية والقُدرة أو نُظُم المعلومات واتصالات الدولة، حيث تكون المعلومات الواردة فيه محميَّة من أيِّ دافع من التلف والاستخدام غير المُصرَّح به أو التحليل أو الاستغلال. فهو عبارة عن مجموع الوسائل التقنية والتنظيمية والإدارية التي يتمُّ استخدامها لمنع الاستخدام غير المُصرَّح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونُظُم الاتصالات والمعلومات التي تحتويها وذلك بهدف ضمان توافر واستمرار عمل نُظُم المعلومات وتعزيز حماية سِرِّيَّة البيانات الشخصية وخصوصيتها، واتخاذ جميع التدابير اللازمة لحماية المُواطنين والمُستهلكين من المَخاطر فى الفضاء السيبراني، فالأمن السيبراني هو سلاح إستراتيجي بيد الحكومات والأفراد، لا سيَّما أنَّ الحرب السيبرانية أصبحت جزءًا لا يتجزَّأ من التكتيكات الحديثة للحروب والهجمات بين الدول، ويشمل الأمن السيبراني أمن المعلومات على أجهزة وشبكات الحاسوب الآلي، بما فى ذلك العمليات والآليات التي يتمُّ من خلالها حماية مُعدَّات الحاسوب الآلي والمعلومات والخدمات من أيِّ تدخُّل غير مقصود أو غير مُصرَّح به أو تغيير أو إتلاف قد يحدث[٢].

فالأمن السيبراني إذًا هو سلاح إستراتيجي بيد الحكومات والأفراد، ويشمل مجموعة من الممارسات التي ترمي إلى حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية أيًّا كان نوعها. وهذه الممارسات متنوِّعة إلى تدابير احتياطية استباقية قبل وقوع الخلل، وعلاجية تكون بعد وقوع الخلل.

(١) الاتحاد الدولي للاتصالات ITU دراسة عن تأمين شبكة المعلومات والاتصالات، قطاع تنمية الاتصال، فترة الدراسة (٢٠٠٦-٢٠١٠) متاح على الموقع الإلكتروني التالي:

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

(٢) د. لامية طالة، الإرهاب السيبراني والأمن القومي: قراءة في تحوُّلات الإستراتيجية الدفاعية، حوليات جامعة الجزائر ١، المجلد ٣٥، العدد ٤، ٢٠٢١م، ص٣٥٦.

والأمن السيبراني أمر حتميٌّ لتحقيق رحلة تحوُّل رقمي آمنة فى الدول على الرغم من التحديات التي فرضها وباء فيروس كورونا إلا أنَّها فى الوقت نفسه أظهرت حقائق عديدة، وكشفت عن فُرص جديدة غيَّرت من مجريات حياتنا اليومية، يُعدُّ أمن الفضاء السيبراني الركيزة الأساسية لأيِّ تحوُّل رقمي، حيث تستند إليه المصداقية الرقمية للشركات والمؤسَّسات(١).

ويشمل هذا المجال الحمائي الحيوي مجموع الأُطُر والسياسات والإستراتيجيات والأنشطة والأنظمة والنُّظُم والتدابير والسُّبُل والتوجُّهات والاحتياطات الدفاعية الشاملة، التي تهدف إلى تحقيق أمن وأمان وسلامة البيئة الافتراضية الإلكترونية بكافة عناصرها وقِيَمها ومُشتملاتها من منظور وأبعاد الأمن القومي، والمصالح والقِيَم الحيوية ذات الأهَمِّيَّة(٢).

والقوَّة السيبرانية: هي القدرة على الحصول على النتائج المرجوَّة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني؛ أي: أنَّها القُدرة على استخدام الفضاء السيبراني لإيجاد مزايا للدولة، والتأثير على الأحداث المتعلِّقة بالبيئات التشغيلية الأخرى وذلك عبر أدوات سيبرانية(٣).

ومصطلح القوَّة السيبرانية أكثر شمولًا من مصطلح الحرب السيبرانية، فمفهوم القوَّة السيبرانية «cyber power» يتضمَّن كافة مجالات القوَّة التي تندرج تحت إطار الصراع السيبراني بشكل يختلف عن مُسمَّى الحرب السيبرانية «cyber war» والذي يُشير إلى القوَّة العسكرية للفضاء السيبراني، ويتمُّ الإشارة إليه بالهجوم السيبراني عندما يتمُّ اعتباره نمطًا من الهجوم يتمُّ شنُّه من قِبَل الدولة أو الفاعلين من غير الدول، والتي يكون لها تداعيات على الأمن القومي للدول والأمن العالمي.

والجريمة السيبرانية: هي مجموعة من الأعمال غير القانونية التي تتمُّ عبر أجهزة إلكترونية أو شبكة الإنترنت أو تُبَثُّ عبر محتوياتها، وهي ذلك النوع من

(١) د. كلاوس شواب، الثورة الصناعية الرابعة، ملخَّصات لكتُب عالمية، تصدر عن مؤسَّسة محمد بن زايد للمعرفة، دبي، الإمارات، ٢٠٢٠، ص: ٢.

(٢) د. حازم حسن أحمد الجمل، الحماية الجنائية للأمن السيبراني في ضوء المملكة ٢٠٣٠، مجلة البحوث الأمنية، كلية الملك فهد الأمنية، مركز الدراسات والبحوث، مج ٣٠، ع٧٧، أغسطس ٢٠٢٠، ص: ٢٥٣-٢٥٤.

(٣) انظر:

Harvard , Joseph S. Nye : The future of power .press realise , Belfer center for Science and international Affairs , Kennedy Scholl, 31 january 2011.

الجرائم التي تتطلَّب الإلمام الخاص بتقنيات الحاسب الآلي ونُظُم المعلومات لارتكابها أو التحقيق فيها ومُقاضاة فاعليها.

ولقد عرَّفها البعض بأنَّها هي: « كلُّ فعل أو امتناع عن فعل باستعمال نظام معلوماتي معيَّن للإضرار بمصلحة أو حقٍّ يحميه القانون من خلال جزاء جنائي، سواء كانت هذه المصالح أو الحقوق المحميَّة جنائيًا تُمثِّل نماذج معلوماتية مُستحدَثة، أو كانت تدخل فى نطاق المصالح أو الحقوق المحميَّة جنائيًا فيما سبق بالطرُق التقليدية، وسواء كان الاعتداء واقعًا داخل حدود الدولة أو يتجاوزها إلى مجموعة من الدول »[١].

وأمَّا الهجمات السيبرانية: ووفقًا لمبادئ (تالين) [٢] بشأن الحروب السيبرانية، فقد عُرفت الهجمات السيبرانية بأنَّها: « عمليات سيبرانية، سواء أكانت هجومية أم دفاعية، والتي يهدف من خلالها بصورة مَعقولة التسبُّب بالإصابة أو وفاة الأشخاص أو الأضرار أو تدمير الأعيان والأهداف »، ووفق هذا التعريف الوارد فى تلك المبادئ، فقد اتَّفق مُعظم الفُقهاء القانونيين على أنَّه قد يتحقَّق الضرر أيضًا بتوقُّف أحد الأعيان عن العمل، علاوة على الضرر المادي، وليس من المهم كيف يحدث ذلك.

كما عرَّفها مايكل شميت [٣] على أنَّها: « مجموعة من الإجراءات التي تتَّخِذها الدولة للهجوم على نُظُم المعلومات المعادية؛ بهدف التأثير والإضرار بها، وفي الوقت نفسه للدفاع عن نُظُم المعلومات الخاصة بالدولة المهاجمة ».

وتتميَّز الهجمات بأنَّها تتمُّ بواسطة شخص أو أكثر باستخدام جهاز كمبيوتر مزوَّد بعدد كبير من الفيروسات، ويتمُّ إرسالها إلى الهدف المراد إلحاق الضرر به، ويمكن أن يكون الضرر مادِّيًا أو مَعنويًا. وعليه فإنَّ الهجمات السيبرانية ليست سلاحًا تقليديًا[٤]، ولا ترقى لأن تكون سلاح دمار شامل؛ وذلك نظرًا للأضرار الناتجة عنها.

---

(١) د. هلالي عبداللاه أحمد، جرائم الحاسب والإنترنت بين التجريم الجنائي وآليات المواجهة دار النهضة العربية، ٢٠١٥، ص: ١١٧.

(٢) دليل تالين، وهو مجموعة من المبادئ أعدَّها بعض الخبراء في القانون الدولي الإنساني عام ٢٠١٣ أبرزهم الأستاذ مايكل شميت بالتعاون مع حلف شمال الأطلنطي، ويدعم من فريق مؤلف من خبراء السيبرالية، واللجنة الدولية للصليب الأحمر والقيادة السيبرالية الأمريكية الذين شاركوا في المداولات كافة.

(٣) انظر:

Michael N Schmitt, Computer Network Attack and The Use of Force in International Law : Thoughts on a normative framework , Co;ombia Journal of transnation law , 1998-1999,p.890.

(٤) د. يحيى ياسين سعود، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، المجلة القانونية، جامعة القاهرة، كلية الحقوق فرع الخرطوم، نوفمبر ٢٠١٨، ص: ٨٥-٨٦.

وتجدر الإشارة إلى أنَّ هناك فروقًا جوهرية بين الجريمة السيبرانية والهجمات السيبرانية (الحرب أو القوَّة السيبرانية) والذي يتمثَّل فى الباعث، حيث إنَّ الباعث على الهجمات السيبرانية يتمثَّل أساسًا فى إضعاف وظيفة شبكات الحاسوب المستهدَفة فى دولة أخرى لتحقيق هدف سياسي، يُضاف إلى ذلك أنَّ القواعد القانونية التي تُقرَّر من خلالها الهجمات السيبرانية هي قواعد القانون الدولي العام، تحديدًا قواعد اللجوء إلى استخدام القوَّة. أمَّا الجريمة السيبرانية فتصدر عن جهة لا تُمثِّل الدولة أو أحد مؤسّساتها سواء كان شخصًا عاديًا أو اعتباريًا، سعيًا وراء هدف إجرامي يتحقَّق عند اختراق أجهزة إلكترونية معينة لأغراض شخصية، وهذا التصرُّف لا يرقى إلى مستوى الجريمة السيبرانية إلا إذا شكَّل جريمة وفقًا للقانون الجنائي الداخلي استنادًا إلى مبدأ « لا جريمة ولا عقوبة إلا بنصٍّ »، وهو أحد المبادئ الأساسية التي تقوم عليها أنظمة العدالة الجنائية. فضلًا عن ذلك فالأضرار المحتملة لكلٍّ من الهجمات السيبرانية والجريمة السيبرانية تختلف بشكل كبير على اعتبار أنَّ الهجمة السيبرانية تهدف إلى إلحاق ضرر شامل سواء للأشخاص أو الممتلكات فى الدولة الأخرى، وهو ما يختلف جذريًا عن الجريمة السيبرانية والتي ينحصر ضررها عمومًا فى مُستخدمين معينين[1] .

(١) د. أميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسُبل مواجهتها في القانون الدولي العام ، مجلة الشريعة والقانون، العدد الخامس والثلاثون، الجزء الثالث، ٢٠٢٠م، ص: ٣٩٤-٣٩٥.

المبحث الثاني

طبيعة المخاطر السيبرانية وسماتها

المخاطر فى حدِّ ذاتها لا تتغيَّر ولكنَّ سماتها هي التي تتغيَّر مع تطوُّر الأدوار والوسائل المستخدَمة، فقد أصبحت الدول تهتمُّ بتكنولوجيا المعلومات ودورها فى الصراعات والحروب المستقبلية استعدادًا لمواجهة ما ينشأ عنها من مخاطر، والتي يتوقَّع الكثير حدوثها فى الفضاء السيبراني، ولذا نجد أنَّ هناك مناورات يتمُّ إجراؤها للتدريب على هذا النوع الجديد من الصراع، وكيف يمكن مواجهته والاستعداد له. وبات من الصعب تخيُّل صراعٍ عسكريٍّ اليوم دون أن يكون لهذا الصراع أبعادٌ سيبرانية، وأصبحت فى صلب اهتمامات الأنظمة الدفاعية لأيِّ صراع يمكن أن يحدث فى المستقبل، فالحرب التي تَمَّ شنُّها ما بين روسيا واستونيا عام ٢٠٠٧، وبين جورجيا وروسيا عام ٢٠٠٨، دفع العديدُ من الدول مثل الولايات المتحدة الأمريكية وغيرها من الدول الأخرى مثل الصين - على الرغم من التقدُّم التكنولوجي لها - ببناء وحدات إلكترونية على شبكات الإنترنت للحماية من مئات وآلاف القراصنة المحترفين[١].

بل يرى البعض أنَّ الحروب السيبرانية أصبحت بديلًا لتلك الحروب التقليدية التي كانت تعتمد على جيوش عسكرية وأسلحة قتالية، فالحرب السيبرانية بالرغم من أنَّها حرب من دون نار أو قصف ولكن لها جانبًا عنيفًا من حيث الاختراقات والقرصنة ونشر الفيروسات وغيرها من الأساليب، وبالرغم من فداحة الخسائر، فإنَّ الأسلحة بسيطة لا تتعدَّى فى أغلب الأحوال « الكيلو بايتس» والتي تتمثَّل فى فيروسات إلكترونية تخترق شبكة الحاسب الآلي، وتنتشر بسرعة بين الأجهزة، وتبدأ عملها فى سِرِّيَّة تامَّة وبكفاءة عالية. وتتميَّز هذه الحروب بالسرعة والدقة فى تنفيذ العمليات العسكرية، وتُعتبر من أدوات الحرب الشاملة[٢].

ويتميَّز الصراع السيبراني بأنَّ به تدميرًا لا تُصاحبه دماء وأشلاء بالضرورة، بل يتضمَّن التجسُّس والتسلُّل ثم النسف، لكن لا دخان ولا أنقاض، ويتميَّز أطرافه بعدم الوضوح، وتكون تداعياته خطيرة، سواء عن طريق تدمير المواقع على الإنترنت ونسفها وقصفها بوابل من الفيروسات، أو العمل على استخدام أسلحة الفضاء

(١) د. عباس بدران، الحرب السيبرانية، الاشتباك في عالم المعلومات، مركز دراسات الحكومة السيبرانية، بيروت، ٢٠١٠، ص: ١١٠.
(٢) د. جمال محمد غيطاس، الحرب وتكنولوجيا المعلومات، الطبعة الأولى، دار النهضة العربية، ٢٠٠٦.

السيبراني المتعدِّدة للنيل من سلامة تلك المواقع، وهي أسلحة يسهل الحصول عليها من خلال مواقع الإنترنت وتعلُّم كيفية استخدامها، كما أنَّ انتشار الفضاء السيبراني وسهولة الدخول إليه يمكن أن يُوسِّع دائرة استهداف المواقع بالإضافة إلى زيادة عدد المهاجمين[١] . وهناك صراع سيبراني تُحرِّكه دوافع سياسية ويأخذ شكلًا عسكريًا، ويتمُّ فيه استخدام قُدرات هجومية ودفاعية عبر الفضاء الإلكتروني؛ وذلك بهدف إفساد النظم المعلوماتية والشبكات والبنية التحتية، وبما يتضمَّن استخدام أسلحة وأدوات إلكترونية من قِبَل الفاعلين داخل المجتمع المعلوماتي أو من خلال التعاون ما بين قُوى أخرى لتحقيق أهداف سياسية. ويُوجد صراع ذو طبيعة ناعمة عن طريق الصراع حول الحصول على المعلومات والتأثير فى المشاعر والأفكار وشنّ حرب نفسية وإعلامية، ويتمُّ أيضًا من خلال تسريب المعلومات واستخدامها عبر منصَّات إعلامية بما يُؤثِّر على طبيعة العلاقات الدولية كالدور الذي لعبه موقع ويكيليكس فى الدبلوماسية الدولية[٢] .

ويمكن أن يُستخدم الفضاء السيبراني كوسيلة من وسائل الصراع داخل الدولة، بين مكوِّناتها على أساس طائفي أو اقتصادي أو ديني، وهو ما يُساعد على كشف ديناميكات التفاعُل الداخلي إلى الخارج؛ بما يُسهِّل من عملية الاختراق الخارجي عبر شبكة الاتصال بدعم أحد أطراف الصراع بأدوات غير قتالية[٣] .

(١) انظر:

Jennie M. Williamson "Information Operations : computer U.S.Army , PA, Carlisle Barracks , Network Attack in the 21 st century" war college, 2002,p.15.

(٢) د. عادل عبد الصادق، موقع ويكيليكس وتحدّي عالم الاستخبارات الأمريكي، ملف الأهرام الإستراتيجي، مركز الأهرام للدراسات السياسية والإستراتيجية، أكتوبر، ٢٠١٠.

(٣) د. عادل عبد الصادق، القوة الإلكترونية «أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني»، المركز العربي لأبحاث الفضاء الإلكتروني، قضايا إستراتيجية، ٢٠١٢.

المبحث الثالث

صور المخاطر السيبرانية

يتمثَّل الصراع السيبراني فى استخدام تقنيات الحاسوب لتخريب أو تهديد نشاطات دولة أو منظَّمة دولية، وبخاصة الهجوم على نُظُم المعلومات الخاصَّة، وذلك لغايات إستراتيجية أو عسكرية؛ وفيما يلي نُبيِّن أهمَّ الصور التي يمكن أن تُشكِّل مخاطر سيبرانية، وذلك من خلال ثلاث مَطالب وعلى النحو التالي:

المطلب الأوَّل: الاختراقات السيبرانية.

المطلب الثاني: التجسُّس السيبراني.

المطلب الثالث: الإرهاب السيبراني.

المطلب الأوَّل

الاختراقات السيبرانية

لم تَعد القرصنة تتمُّ بصورتها التقليدية، بل استفاد القراصنة من وسائل وتقنيات المعلومات؛ حيث أصبح الجُناة بفضل تلك التقنيات يرتكبون جرائم القرصنة بصور مُستحدثة من خلال العثور على مواقع الإنترنت لترويج البرامج المقرصنة مجانًا أو بمقابل مبلغ رمزي، مما ألحق العديد من الخسائر المادية الباهظة بالشركات المتخصِّصة فى صناعة البرامج، ودعا هذه الشركات إلى إنشاء منظَّمة خاصة لمراقبة وتحليل ما يُعرَف بسوق البرمجيات، ومنها منظمة اتحاد برمجيات الأعمال التي تُجري دراسات حول هذا، وتبنِّي الحلول المناسبة[١].

والقرصنة مصطلح عام يُشير إلى جميع أشكال الوصول غير المصرَّح به إلى أجهزة الكمبيوتر والشبكات، والبيانات، وإلحاق الأضرار بها، وقد تظهر القرصنة فى العديد من أشكال السلوك الإجرامي بما فى ذلك الجرائم السيبرانية[٢].

(١) د. أميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسَبُل مواجهتها في القانون الدولي العام، المرجع السابق، ص: ٤٠٨.

(٢) انظر:

Rohas Nagpal, Cyber terrorism in the context of globalization, Paper presented at II World Congress on Informatics and Law, Madrid, Spain, September 2002 ,p.4 , available at : http://www.asianlaws.org/aboutus/spain.pdf

وتُعتبر القرصنة أحد صور المخاطر السيبرانية إذا كان القصد منها تعطيل أو إصابة نُظُم المعلومات، أو البنية التحتية الحيوية المدارة عبر الشبكات، أو قتل الأشخاص، أو إصابتهم لغرَض سياسي أو أيدلوجي أو مادي أو غيره.

ويمكن أن تتَّخِذ الاختراقات السيبرانية إحدى الصور الآتية:

١- اختراق المواقع والصفحات السيبرانية على الإنترنت وتدميرها، أو إلغائها، أو إتلافها، أو التعديل والعبث بالبيانات والمعلومات المتوفِّرة عليها.

٢- شغل العنوان (الرابط) السيبراني للموقع أو تحويله لعنوان موقع آخر على الإنترنت.

٣- اختراق قواعد البيانات وحذف أو تعديل المعلومات الموجودة عليها، أو الاستيلاء على المعلومات الموفَّرة عليها كأسماء المستخدِمين وأرقامهم السرية وعناوين الاتصال الخاصة بهم، واستخدامها لأغراض غير مشروعة، أو بيعها إلى جهات مُستفيدة (جهات اقتصادية وتجارية، أو سياسية، أو أمنية).

ويَنشط دور القرصنة فى التعبير عن المواقف السياسية بقيامها بمهمات على مواقع حكومية مثل جماعة ويكيليكس وأنونيموس والتي أصبحت تُهدِّد شركات ودولًا بالاختراق. وقد تَمَّ استخدام هذه الاختراقات فى الفضاء السيبراني فى إطار الصراعات بين الدول، كما حدث بين إستونيا وروسيا فى عام ٢٠٠٧، والاختراقات المتبادلة بين الصين والولايات المتحدة أو ما بين كوريا الجنوبية [١].

وخلال الفترة من أبريل ١٩٩٠ إلى مايو ١٩٩١ نجحت مجموعة من القراصنة الهولنديين فى الوصول إلى أسرار عسكرية أمريكية بالغة الحساسية عن تحرُّكات القوات الأمريكية - إبان حرب الخليج- ومواقعها وأسلحتها، وتحرُّكات الطائرات المقاتلة، وسعوا إلى بيع هذه المعلومات إلى السُّلطات العراقية، إلا أنَّ الشرطة الهولندية قبضت عليهم [٢].

(١) للمزيد انظر: د. عادل عبد الصادق، أسلحة الفضاء الإلكتروني في ضوء القانون الدولي الإنساني، وحدة الدراسات المستقبلية، المرجع السابق، ص: ٤٣.

(٢) انظر:

See Jack L. Brock, Computer Security: Hackers Penetrate DOD Computer System (Washington DC: General Accounting Office , 1991) Full Text available online at: http://www.globalsecurity.org/security/library/report/gao/145327.pdf

وهناك العديد من الوسائل التكنولوجية التي تُسهِّل عمليات القرصنة، وأهمُّها ما يجري عبر التقاط حزم البيانات المارة بالشبكات، وهجوم العاصفة، وكسر كلمة السر، وتجاوُز المخزون المؤقَّت [١].

المطلب الثاني

التجسُّس السيبراني

بالرغم من أنَّ التجسُّس السيبراني ظاهرة جديدة نسبيًّا، فإنَّ التجسُّس ليس بالتأكيد كذلك؛ إذ تَمَّ ممارسته منذ فجر التاريخ. ويصف التجسُّس فى مفهومه التقليدي الممارسة التي يتمُّ بموجبها إرسال الدولة وكيلًا عنها إلى أراضي دولة أخرى؛ من أجل الوصول إلى المعلومات السرية والحصول عليها. ومع ذلك، فقد استغلَّت الدول التطوُّرات التي حدثت فى مجال التكنولوجيا من أجل ابتكار طُرُق أكثر فعالية يمكن من خلالها إجراء التجسُّس. ومع اكتشاف السفن والطائرات والأجرام السماوية، بدَت البحار والسماء والفضاء الخارجي كنطاقات يمكن استغلالها كمنصَّات للتجسُّس عن بُعد. ولذلك، فإنَّه ليس من المستغرب تسخير الفضاء السيبراني أيضًا كوسيلة يمكن من خلالها ارتكاب التجسُّس[٢].

ويكمن التجسُّس السيبراني فى الحصول على المعلومات السرية دون إذن من صاحبها، سواء كانوا أشخاصًا، أو شركات، أو حكومات؛ تحقيقًا لميزة اقتصادية أو سياسية، أو عسكرية باستخدام وسائل غير مشروعة عبر الإنترنت، أو الشبكات، أو أجهزة الكمبيوتر. كما يمكن أن يتمَّ من خلال القرصنة أو البرمجيات الخبيثة مثل أحصنة طروادة وبرامج التجسُّس[٣].

وقد ذهب رأيٌ إلى أنَّ التجسُّس السيبراني هو: « عبارة عن الطُرق المستخدَمة لاختراق المواقع الإلكترونية، ومن ثَمَّ سرقة بعض المعلومات والتي قد تكون فائقة

(١) انظر:

Rohas Nagpal, Cyber terrorism in the context of globalization , Paper presented at II World Congress on Informatics and Law, Madrid, Spain, September 2002, p.4, available at : http://www.asianlaws.org/aboutus/spain.pdf

(٢) انظر:

see, Ruseell Buchan, "Cyber espionage and international law", in: Nicholas Tsagourias and Russell Buchan (eds), Research .Handbook on International law Cyberspace, (Edward Elgar Publishing 2015),p.170.

(٣) انظر:

Fahad Ullah Khan , States rather than criminals pose a greater threat to global cyber security: a critical analysis, the Institute of Strategic Islamabad ISSI ..olume xxxi, no3, Autumm 2011, p.93, available at: http://issi.org.pk/wp-content/uploads/2014/06/1328592265_ 43276030.pdf

الأهَمِّيَّة والخطورة للطرَف المتلقِّي والمسروق منه، وقد انتشرت فى الألفية الجديدة بانتشار طرُق الاختراق، وأحيانًا قد يكون الاختراق من أشخاص عابثين ليس إلا، وأحيانًا بغرض سرقة معلومات» [١] . فى حين ذهب رأيٌ ثان إلى أنَّه: «هو استخدام القُدرات السيبرانية لإجراء عمليات رصد، أو مُراقبة، أو التقاط، أو تسريب الاتصالات الإلكترونية، أو المخزَّنة، أو البيانات المخزَّنة، أو معلومات أخرى» [٢] .

نستخلص مما سبق أنَّ التجسُّس السيبراني يمكن أن يكون شكلًا من أشكال الإرهاب السيبراني، إذا اعتمد على استخدام التكنولوجيا بشكل سلبي؛ من أجل إحداث آثار مدَمِّرة وأضرار بالغة وكبيرة لمحطات التحكُّم وأجهزة الكمبيوتر وشبكات الاتصال [٣] . فمن الممكن استخدام التجسُّس السيبراني للاستطلاع واستكشاف النقاط شديدة الضعف فى البنية التحتية لأنظمة الكمبيوتر، ومن ثَمَّ تصميم برامج تستغلُّ هذه الثغرات؛ لتنفيذ هجمات الإرهاب السيبراني فى المستقبل [٤] .

فالتجسُّس السيبراني ينطوي على الوصول إلى أنظمة الكمبيوتر المستهدَفة سِرًا من أجل جمع المعلومات الحسَّاسة عنها، وهو ما يتمُّ عادة عبر تقنية التخفِّي، كما يمكن أيضًا أن يتمَّ من خلال أشخاص داخل المؤسَّسة يقومون خلسة بتثبيت كود التجسُّس السيبراني داخل نُظُم الكمبيوتر المحمية. ومن ثَمَّ يتمُ جمع المعلومات الضرورية لمساعدة المجموعة الإرهابية على تحديد نقاط الضعف داخل النظام المستهدَف؛ وعليه قد يستخدم الإرهابيون المعلومات التي تَمَّ جمعها لزيادة فعالية هجوم مُستقبلي. فبمجرد التثبيت، قد يرسل الرمز الخبيث معلومات حسَّاسة إلى نقطة تجميع مركزية عن بُعد، وفي وقت لاحق، قد يتمُّ إرسال أمر لإصدار تعليمات برمجية ضارَّة لبدء الهجوم الإرهابي على الإنترنت، وقد تُعطي التفاصيل التي تَمَّ جمعها بواسطة الشفرة الخبيثة القُدرة على إغلاق صمامات التحكُّم المحدَّدة فى مرفق أساسي من مرافق البنية التحتية، أو يكون من نتائجها إصدار تعليمات غير صحيحة قد تُؤدِّي فى النهاية إلى تدمير معدَّات محدَّدة فى موقع حسَّاس [٥] .

(١) د. عصام فاعور ملكاوي، الفضاء الإلكتروني ساحة حرب دولية مُفترضة، إربد للبحوث والدراسات - القانون، جامعة إربد الأهلية - عمادة البحث العلمي والدراسات العليا، مج ١٨، ع ٢، تموز ٢٠١٥، ص: ١٢٠.

(٢) انظر:

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.

(٣) انظر:

.Near this concerned, Irving Lachow, Cyber Terrorism: Menace or Myth ? ..., op.cit,p.439

(٤) انظر:

see , Clay Wilson , Cyber Threats ...,op.cit, p.129.

(٥) انظر:

see , Clay Wilson , Cyber Threats ...,op.cit, p.129.

وقد تَمَّ رصد بعض حالات التجسُّس الدولي من طرَف وكالة الأمن القومي الأمريكي « NSA »، والكشف عن شبكة دولية ضخمة للتجسُّس بإدارة كندا وبريطانيا وأستراليا ونيوزيلندا لرصد المكالمات الهاتفية والرسائل بمختلف أنواعها ويُطلَق على هذه الشبكة اسم (ECHELOW).

ومن الجهود التي بُذِلت لمكافحة هذا النوع من الإجرام - على الصعيد التقني - ولحماية المعلومات التي تتعرَّض لأعمال التجسُّس السيبراني: العمل على تشفير البيانات وإخفائها، والاهتمام ببروتوكولات الحماية، ونُظُم منع المتطفِّلين، وتُشير تلك الجهود أيضًا إلى أنَّ أهداف وطرُق الحماية تتمثَّل فى أمرين:

الأوَّل: هو «الوثوقية» بمعنى: الاحتفاظ بسرية المعلومات قبل الجميع، باستثناء الذين لهم صلاحية للاطلاع عليها.

الثاني: هو «تكامل البيانات» بمعنى: التأكُّد من أنَّ المعلومات لم تتغيَّر من قِبَل أشخاص غير مخوَّلين لذلك، والتحقُّق من الشخصية [١] .

ومن أهمِّ ما يندرج تحت مُسمَّى جرائم التجسُّس السيبراني [٢] ما يلي:

١- جرائم التجسُّس الاقتصادية والتجارية: وهي جرائم التجسُّس التي يكون الهدف منها الحصول على معلومات اقتصادية وتجارية. ويُعدُّ التجسُّس الصناعي نوعًا من التجسُّس الذي يُنفَّذ لأغراض تجارية، وتقوم به بعض الشركات والمؤسَّسات التجارية؛ بهدف الحصول على أسرار صناعية من الشركات المنافسة، وهذا النوع من التجسُّس غالبًا ما يرتبط بالصناعات التقنية، مثل البرمجيات والتقنية الحيوية، وتقنيات الفضاء والاتصالات والمواد والطاقة.

٢- جرائم التجسُّس الثقافية والتعليمية: وهي جرائم التجسُّس التي يكون الهدف منها الحصول على معلومات ثقافية وتعليمية. ومن أمثلتها التجسُّس على الأبحاث والمخترَعات والدراسات العلمية والتعاون الثقافي والتعليمي بين الدول.

---

(١) د. مصطفى جاد، مقال بعنوان « مستقبل الإرهاب السيبراني »، في ندوة نظمها المركز الدولي للدراسات المستقبلية والإستراتيجية في ١١ أبريل ٢٠١٢، جريدة السياسة الدولية التابعة لمؤسسة الأهرام، إعداد / شريهات نشأت المنيري، على الموقع السيبراني:
http://www.siyassa.org.eg//newsContent/6/51/2450

(٢) د. ممدوح عبد الحميد عبد المطلب، جرائم استخدام شبكة المعلومات، الجريمة عبر الإنترنت، بحث مقدَّم لمؤتمر القانون والكمبيوتر، كلية الشريعة والقانون، جامعة الإمارات، ٢٠٠٠، ص: ٢٠.

المطلب الثالث

الإرهاب السيبراني

الإرهاب السيبراني هو اعتداء غير مشروع أو التهديد بالاعتداء على أجهزة الكمبيوتر والشبكات المعلوماتية المخزَّنة فيها؛ بهدف إرهاب الحكومة أو المواطنين لتحقيق أهداف سياسية أو اجتماعية أو أيدلوجية، وينبغي أن يكون الهجوم مدمِّرًا وتخريبيًا؛ لتوليد الخوف والرعب، ويكون مشابهًا للأفعال المادية للإرهاب (١).

وذهب البعض الآخر إلى تعريفه بأنَّه: «هو كلُّ نشاط إجرامي يتمُّ من خلال شبكة الإنترنت؛ بهدف بثِّ الأفكار المتطرِّفة، سواء كانت سياسية أو دينية أو عنصرية للسيطرة على وجدان الأفراد، وإفساد عقائدهم، وإذكاء تمرُّدهم، واستغلال معاناتهم فى تحقيق مآرب خاصة تتعارض مع مصالح المجتمع (٢).

بينما عرَّفه البعض الآخر بأنَّه: «نشاط إجرامي مخطَّط ومنظَّم مخالِف للقانون، يقوم به التنظيم الإرهابي بواسطة التقنية الإلكترونية الرقمية؛ لتحقيق غرض معين تحت تغطية (٣). وذهب البعض الآخر إلى القول بأنَّ المناط فى تحقيق الإرهاب السيبراني يكمن فى استخدام الإنترنت فى تنفيذ هجمات إلكترونية ضد البنية التحتية للنُّظُم المعلوماتية بالدولة (٤).

فى حين ذهب البعض الآخر إلى تعريفه بأنَّه: «هو العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول أو الجماعات أو الأفراد على الإنسان فى دِينه أو نفسه أو عِرضه، أو عقله، أو ماله، أو بشتَّى صور العدوان والإفساد، وذلك باستخدام الموارد المعلوماتية والوسائل الإلكترونية (٥).

---

(١) انظر:

Dorothy E. Denning, Activism, Hacktivism and cyber terrorism, the internet as a tool for influencing Foreign policy in: Arquilla & D. Ronfold (eds), Networks and net wars, the future of terror crime and miletences, National Defense Research Institute, 2001, pp.239-288.

(٢) د. حسين المحمدي بوادي، الرهاب الدولي بين التجريم والمكافحة، دار الفكر العربي، ٢٠٠٦، ص: ٥٤.

(٣) د. مصطفى محمد موسى، الإرهاب الإلكتروني، بدون دار نشر، الطبعة الأولى، ٢٠٠٩، ص: ١٧٣.

(٤) انظر:

Maura Conway, Terrorism and new media : the cyber-battl espace in : Forest, James F., (eds.), Countering terrorism and insurgency in the 21st century, Greenwood Publishing Group, Inc., Westport. CT, 2007,PP.363-384.

(٥) د. عبد الله عبد العزيز العجلان، الإرهاب الإلكتروني في عصر المعلومات، بحث مقدَّم إلى المؤتمر الدولي الأوَّل لحماية أمن المعلومات والخصوصية في قانون الإنترنت والمنعقد بالقاهرة في الفترة ٢-٤ يونيو ٢٠٠٨ متاح على الرابط التالي:

http://www.shaimaaatalla.com/vb/

ومن أشكال الإرهاب الإلكتروني، التجنيد السيبراني من خلال ما يُطلق عليه «التلقين السيبراني» وأخيرًا «التهديد والترويع السيبراني»[١].

وقد تمكَّنت الجماعات الإرهابية من خلال استخدام الإنترنت من التواصُل مع بعضها البعض عبر القارات، وهو الأمر الذي كان يستغرق شهورًا فى الماضي؛ ومن ثَمَّ تحدث هجمات سيبرانية إرهابية مدمِّرة على المواقع الحيوية على الشبكة المعلوماتية وإلحاق الضرر بأنظمة القيادة والسيطرة والاتصالات ومحطات الطاقة الدولية وأسواق المال وإطفاء مصابيح ممرَّات هبوط الطائرات وغيرها، بحيث يُؤدِّي توقُّفها أو العبث بأنظمتها إلى حدوث آثار تدميرية تفوق ما تُحدِثه القنابل والمتفجِّرات، كما قد يحدث هجوم إلكتروني على المواقع السيبرانية بقصد الاستيلاء على محتوياتها، كشنِّ هجوم على المصارف المالية للاستيلاء على ما بها من أموال؛ من أجل تمويل التنظيم[٢].

الفصل الثاني

المخاطر السيبرانية وأثرها على تهديد السِّلْم والأمن الدوليين

يتضمَّن القانون الدولي العام نوعين من القواعد التي تُنظِّم استخدام الدول للقوَّة؛ يتعلَّق الأوَّل بمشروعية استخدامها قبل نشوب الأعمال العدائية، ويُنظِّم النوع الثاني استخدامها أثناء النزاعات المسلَّحة «قانون الحرب»، حيث تعني بتطبيق مبادئ الإنسانية، والاستخدام المشروع للأسلحة، والأهداف المشروعة، وحماية بعض الفئات والأماكن والأشياء. ولم يتعرَّض أيٌّ من النوعين صراحة للعمليات السيبرانية، بالنظر إلى أنَّ هذه القواعد قد أُبرِمت فى وقت لم تكن فيه هذه العمليات شائعة أو ربما حتى متصوَّرة، فتمَّ التركيز على تنظيم وسائل وأساليب استخدام القوَّة المادية أو «الحركية»، والتي تختلف فى طبيعتها وخصائصها عمَّا قد يتمُّ فى مجال الفضاء السيبراني من عمليات؛ وإذا كانت قواعد القانون الدولي الإنساني لم تتطرَّق مباشرة إلى تنظيم أو ضبط العمليات السيبرانية، إلا أنَّ بعض النصوص الدولية، والاتجاهات

(١) د. عبد بن عبد العزيز بن فهد، بحث بعنوان «الإرهاب الإلكتروني في عصر المعلومات»، مقدَّم إلى المؤتمر الدولي الأوَّل حول «حماية أمن المعلومات والخصوصية في قانون الإنترنت» المنعقد بالقاهرة في الفترة من ٢-٤ يونيو ٢٠٠٨م.

(٢) يتمُّ التدمير السيبراني أو نظم المعلومات عن طريق الدخول غير المشروع على نقطة ارتباط أساسية أو فرعية متصلة بالشبكة المعلوماتية من خلال نظام آلي أو مجموعة نُظُم مترابطة شبكيًا؛ بهدف تخريب نقطة الاتصال أو النظام. وللمزيد من التفصيل حول طرق تدمير وإتلاف المواقع السيبرانية راجع: د. عادل عبد الصادق، هل يُمثِّل الإرهاب الإلكتروني شكلًا جديدًا من أشكال الصراع الدولي ، ملف الأهرام الإستراتيجي، مركز الدراسات السياسية والإستراتيجية بالأهرام ، العدد ١٥٦، ديسمبر ٢٠٠٧.

الفقهية، والأحكام القضائية الدولية تدعم رؤية مفادها إمكان تطبيق تلك القواعد، وكذلك مبادئ القانون الدولي الإنساني على العمليات السيبرانية [١] . وعليه سوف نتناول هذا الفصل من خلال مبحثين على النحو التالي:

المبحث الأوَّل: المخاطر السيبرانية وحقُّ الدفاع الشرعي وفقًا للمادة ٥١ من ميثاق الأمم المتحدة.

المبحث الثاني: تطبيق مفاهيم ومبادئ وقواعد القانون الدولي الإنساني على العمليات السيبرانية.

المبحث الأوَّل
المخاطر السيبرانية وحقُّ الدفاع الشرعي وفقًا للمادة ٥١ من ميثاق الأمم المتحدة

حظر ميثاق الأمم المتحدة فى مادته رقم (٤/٢) على جميع أعضاء المنظَّمة، استخدام القوَّة أو التهديد باستخدامها فى العلاقات الدولية، ثم أورد الميثاق بعض الاستثناءات على هذا المبدأ، منها ما ورد بالمادة رقم (٥١) منه، بشأن حقِّ الدول فى الدفاع عن نفسها عند التعرُّض لهجوم مسلح، وتبنَّت محكمة العدل الدولية تفسيرًا ضيِّقًا للمادة (٥١)، بالتأكيد على جواز حقِّ الدفاع فقط فى حالة الهجوم المسلَّح من قِبَل دولة ضدَّ دولة أخرى، وأوردت المحكمة فى قضية «منصَّات النفط» عام ٢٠٠٣ أمثلة لهذا الهجوم، حيث اعتبرت أنَّ استهداف منصَّة عسكرية، أو منشأة عسكرية قد يرقى إلى مستوى الهجوم المسلَّح [٢] .

وكانت محكمة العدل الدولية قد قرَّرت فى قضية «نيكاراجوا» عام ١٩٨٦، استبعادها ما وصفته بمجرَّد حادثة حدودية من نطاق الهجوم المسلَّح(٣)، كما أوضحت القاضية « Rosalyn Higgins »، فى رأيها الانفرادي فى قضية «الجدار العازل» التي نظرتها المحكمة عام ٢٠٠٤، أنَّها غير مُقتنعة بأنَّ عدم استخدام القوَّة، أو التدابير غير القسرية -كبناء جدار- يمكن أن تقع ضمن نطاق الدفاع عن النفس بموجب المادة

(١) د. محمد عادل محمد عسكر، المرجع السابق، ص: ٣٨.
(٢) حكم محكمة العدل الدولية في قضية (Oil Platforms)، ٢٠٠٣، الفقرات (٥٧: ٦١).
(٣) حكم محكمة العدل الدولية في قضية (Nicaragua v. USA)، ٢٧ يونيو ١٩٨٦، الفقرة ١٩٥.

(٥١) من ميثاق الأمم المتحدة، حيث يجب لإعمال مضمون الحُكم أن تُواجه الدولة قوَّة مسلَّحة [١].

ووفقًا لهذا يكفل القانون الدولي للدول حقَّ الدفاع عن نفسها عبر ممارسات فردية أو جماعية، ويعني ذلك أنَّ لكلِّ دولة الحقَّ فى أن تتصرَّف لنفسها على أيِّ نحو يكفل لها بقاءها، ويضمن استقرارها، ويترتَّب على ذلك أن يكون من حقِّها أن تتخذ ما تراه مناسبًا من الوسائل الدفاعية ضدَّ الأخطار- داخلية أو خارجية - التي تهدِّد أمنها ومصالحها العليا [٢]؛ نظرًا لأنَّ تلك الهجمات السيبرانية يمكن أن يكون لها أبعادٌ دولية خارج حدود السيادة الوطنية للدولة، لذا يلزم لمواجهتها تكاتُف وتعاون دولي لتحقيق السِّلم والأمن الدوليين.

لذا يرى البعض أنَّ ما قامت به دولة « إسبانيا » فى مواجهة إقليم « كتالونيا » للاستقلال هو دفاعٌ شرعي عن أمن واستقرار الدولة، وقد حصلت على دعم دولي فى مواجهة تلك المحاولة، وأكَّد غالبية الدول أنَّ ما يحدث شأنٌ داخلي لا يمكنُ التدخُّل فيه، وما تفعله «إسبانيا» يُعدُّ من مظاهر السيادة الوطنية احترامًا لدستورها وتشريعاتها الداخلية؛ مما أضعف من قوة تلك المحاولة البائسة للانفصال من جانب إقليم « كتالونيا » [٣].

ولعلَّ الاستناد إلى معيار درجة الخطورة لتصنيف العمليات السيبرانية كهجوم مسلَّح، يُثير إشكالية تتعلَّق بكيفية تقدير أو تقييم هذه الخطورة، إلا أنَّه يمكن الاعتماد على تقييم مدى تأثير العملية على الدولة المضرورة، وعلى سبيل المثال، عند تعطيل أو إعاقة مؤسَّسات الدولة عن أداء وظائفها، وحدوث أضرار يتعذَّر تداركها، كتخريب الأجهزة التي تعتمد عليها مُنشآت طبية، مما ينتج عنه وفيات، فإنَّ مثل هذه العمليات تُكافئ استخدام القوَّة، ويكون للدول حقُّ الردِّ عليها بموجب المادة (٥١) من الميثاق [٤].

(١) انظر:

Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory , Advisory Opinion, 2004, JCJ Rep 136, para 35, Separate opinion of Judge Higgins.

(٢) د. إسماعيل صبري مقلد، أصول العلاقات الدولية في إطار عام، دار النهضة العربية، الطبعة الأولى، ٢٠٠٧، ص: ٦-٢٠.

(٣) انظر:

in The Charter of the United Nations: Article 51, A. Randelzhofer .664 (B.Simma ed.) 1995 , A Commentary 661.

(٤) انظر:

N .TSAGOURLAS , Cyber Attacks, Self-defence and the Problem of Artibution, J.Conflict & Sec L.Vol.17, no 2 , 2012, pp.229-244.

وعلى المستوى الوطني، تبنَّت بعض الدول معيار درجة الخطورة، لتصنيف العمليات السيبرانية، وما إذا كانت تُكافئ الهجوم المسلَّح، وتتأهَّل للردِّ عليها وفقًا للمادة (٥١) من ميثاق الأمم المتحدة، ومنها الولايات المتحدة الأمريكية، التي أكَّدت فى تقرير قدَّمته إلى الأمم المتحدة عام ٢٠١١، أنَّه فى بعض الظروف تُشكِّل الأنشطة التخريبية فى الفضاء السيبراني هجومًا مسلَّحًا، ويكون من الملائم ألا يقتصر الردُّ عليها بشنِّ هجوم إلكتروني مضاد فحسب، وإنما يتطلَّب هجومًا بالوسائل العسكرية التقليدية [١].

أمَّا الفقه الدولي فقد كان واضحًا فى تحديد هذا الخط الفاصل، وذلك يتجلَّى فى مساهمات الفقيه الدولي «JEAN- PICLET» حين جاء بمجموعة من المعايير أو المتطلَّبات لاعتبار الاعتداء هجومًا عسكريًا، وهي: النطاق والشدَّة والمدَّة الزمنية [٢].

وتجدر الإشارة إلى أنَّ تفعيل المادة ٥١ واللجوء إلى الدفاع عن النفس فى مواجهة هجوم مسلَّح لا يعني بأيَّة حال أنَّ الدولة التي تُدافع عن نفسها غير مقيَّدة فى طريقة ردِّ الهجوم، بل على العكس من ذلك، لقد تضمَّنت قواعد العُرف الدولي، إلى جانب المادة ٥١ من ميثاق الأمم المتحدة مجموعة من الشروط الواجب توافرها حتى يبقى التصرُّف متوافقًا مع أحكام المادة، وهذه الشروط هي: أوَّلًا: الضرورة، وثانيًا: التناسُب، وثالثًا: الفورية [٣].

(١) انظر:

United Nation, General Assembly, Development in the field of information and telecommunications in the context of international security, Report, Sixty-sixth session, 15 July 2011, (UN DOC.A/66/152).

(٢) انظر:

Cited in : Jeffry car, Inside Cyber Warfare , O Reiily Media , Inc.,2011,p.114.

(٣) أكَّدت على هذه الشروط محكمة العدل الدولية في قرارها في قضية نيكاراغوا ١٩٨٦ وأيضًا في رأيها الاستشاري في قضية الأسلحة النووية ١٩٩٦.

المبحث الثاني
تطبيق مفاهيم ومبادئ وقواعد القانون الدولي الإنساني على العمليات السيبرانية

تمهيد وتقسيم:

إنَّ البحث فى إمكانية تطبيق قواعد القانون الدولي الإنساني على الحرب السيبرانية قد يستلزم ابتداءً التكييف القانوني لتلك المسألة من حيث شرعية وعدم شرعية الحرب السيبرانية فى ضوء استخدام القوَّة فى العلاقات الدولية، فالعلاقة بين حقِّ اللجوء إلى الحرب وقانون الحرب تتَّسِم بأنَّها علاقة توتُّر لا بُدَّ منه، فالقواعد المعاصرة للقانون الدولي تحظر استخدام القوة، باستثناء حقِّ الدول فُرادى أو جماعات فى الدفاع عن نفسها[١]، أو بمقتضى استخدام تدابير إنفاذ القانون التي يتَّخِذها مجلس الأمن[٢]، أمَّا قانون الحرب فهدفه التوفيق بين ضرورات الحرب وقوانين الإنسانية من خلال فرض قيود واضحة على سير العمليات العسكرية، وبخلاف ما تَمَّ الإشارة إليه، فإنَّ استخدام القوَّة فى العلاقات الدولية يُعدُّ عملًا غير مشروع وفقًا لميثاق الأمم المتحدة؛ حيث نصَّ على ما يلي: (يمتنع أعضاء المنظمة جميعًا فى علاقاتهم الدولية عن التهديد باستعمال القوَّة أو استخدامها ضدَّ سلامة الأراضي أو الاستقلال السياسي لأيِّ دولة أو أيِّ وجه آخر لا يتَّفِق ومقاصد الأمم المتحدة)[٣]، ومع ذلك فإنَّ الحرب ظاهرة موجودة - ولا يمكن إغفالها، ولهذا فإنَّ المجتمع الدولي قام بوضع قواعد وضوابط لتقييم الحرب وسلوكيات المتحاربين؛ وذلك لغرض التخفيف من آثار الحرب، طالما أنَّ المجتمع الدولي غير قادر على التخلُّص منها نهائيًا. والقانون الدولي الإنساني لا يعني بحقِّ الحرب ومدى مشروعيتها، وإنَّما حماية الأشخاص والأعيان أثناء النزاع المسلَّح[٤].

وعليه سوف نتناول هذا المبحث من خلال مطلبين على النحو التالي:

---

(١) المادة (٥١) من ميثاق لأمم المتحدة.
(٢) الفقرة (٩) من المادة (٤٢) من ميثاق الأمم المتحدة.
(٣) الفقرة (٤) من المادة (٢) من ميثاق الأمم المتحدة.
(٤) د. إبراهيم محمد العناني، مجالات تطبيق القانون الدولي الإنساني، مجلة العلوم القانونية والاقتصادية، كلية الحقوق، جامعة عين شمس، المجلد ٤٣، العدد ١، يناير ٢٠١٠، ص: ١٩-٢٠.

المطلب الأوَّل: شمولية مبادئ وقواعد القانون الدولي الإنساني والعمليات السيبرانية.

المطلب الثاني: خصوصية المخاطر السيبرانية فى تطبيق مبادئ وقواعد القانون الدولي الإنساني.

المطلب الأوَّل

شمولية قواعد القانون الدولي الإنساني والعمليات السيبرانية

ترتَّب على الفجوة التكنولوجية والتقنية المتزايدة تحديات كبيرة بين مختلف الدول، وبخاصة على صعيد القانون الدولي الإنساني، من حيث مدى إمكانية تطبيق مبادئه وقواعده على هذا الشكل الجديد من الحروب فى ظلِّ فراغ قانوني، وعدم وجود قواعد قانونية محدَّدة تُنظِّم الهجمات السيبرانية.

ولا شكَّ أنَّ تطوُّر وسائل وأساليب الحروب الجديدة أمرٌ لم يكن بعيدًا عن التوقُّع، فالمادة (٣٦) من البروتوكول الإضافي الأوَّل الملحَق باتفاقيات جنيف الأربع لعام ١٩٤٩، حيث نصَّت على أن « يلتزم أيُّ طرف سام مُتعاقد عند دراسة أو تطوير أو اقتناء سلاح جديد أو إدارة للحرب أو اتِّباع أسلوب للحرب، بأن يتحقَّق مما إذا كان محظورًا فى جميع الأحوال أو فى بعضها بمقتضى هذا الملحَق أو أية قاعدة أخرى من قواعد القانون الدولي التي يلتزم بها الطرف السامي المتعاقد ». وبالتالي، تضع هذه المادة الإطار العام لاستخدام وسائل وأساليب قتال جديدة فى النزاعات المسلَّحة.

وتُبيِّن أحكام هذه المادة أنَّه على ضوء قانون الحرب، يتعيَّن على الدول التي تقتني أسلحة حديثة أو تُطوِّرها أن تحدِّد مشروعية استعمالها.كما يُفيد هذا النصُّ ضِمنيًا أنَّ كلَّ قواعد قانون الحرب تكون قابلة للتطبيق على وسائل القتال الحديثة وأساليبها، ففي حال غياب النصِّ الخاص يُطبَّق النصُّ العام، هذا من حيث المبدأ. وفي المقابل فإنَّ المادة (٣٦) من البروتوكول الإضافي الأوَّل لا تُحرِّم تطوير أو اقتناء أسلحة حديثة أو حتى حيازة أسلحة أو اعتماد أساليب جديدة غير منظَّمة بقواعد القانون الدولي الإنساني[1]، ومن هذا المنطلَق فإنَّ أحكام هذه المادة لا تُوقف حقَّ الدول فى ذلك، وإنما تنصُّ على ضرورة المراجعة القانونية عند اقتناء أسلحة من نوع جديد أو

(١) أ. محمد عبد الحق شربال، الأسلحة الحديثة والقانون الدولي الإنساني، رسالة ماجستير، كلية الحقوق، جامعة بن يوسف، الجزائر، ٢٠١٢، ص: ١٤.

تطويرها أو أسلوب حديث أو ما يُعرف بالمطابقة القانونية مع قواعد القانون الدولي وذلك قبل استعمالها، ومن ثَمَّ لا يُعدُّ هذا النصُّ قانونًا جديدًا، ولكنَّه يُقنِّن القاعدة القانونية العُرفية فى التزام الدول بتطبيق مُعاهدة أو قاعدة عُرفية بِنيَّة حسنة.

كما تُبيِّن أحكام هذه المادة أنَّه فى حالة اعتبار الحرب السيبرانية تُمثِّل سلاحًا للحرب أداة لها أو أسلوبًا من أساليب الحرب، وعلى الأطراف التحقُّق من مشروعيتها من عدمه وفقًا لقواعد البرتوكول الإضافي أو أيِّ قاعدة من قواعد القانون الدولي، كما أنَّ اللجنة الدولية التابعة لحلف شمال الأطلسي، قامت بنشر ما يُعرَف «بدليل تالين» الذي يرى بأنَّه يمكن تطبيق القانوني الدولي الإنساني على الحرب السيبرانية، ويستند هذا الدليل بالتقسيم التقليدي للنزاعات المسلَّحة الدولية، والنزاعات المسلَّحة غير الدولية، ويُقرِّر بأنَّ الحرب السيبرانية وحدها قد تُشكِّل نزاعًا مُسلَّحًا مُساويًا له أو قريبًا منه[١]، ويجب إخضاع الهجمات السيبرانية لقانون النزاعات المسلَّحة، وأن يخضع أطراف النزاع للاتفاقيات الدولية التي تُنظِّم هذا النزاع، حيث تركت هذه الهجمات آثارًا مدمِّرة[٢]، ويُقدِّم الدليل تعريفًا للهجوم السيبراني باعتباره عملية إلكترونية، سواء كانت هجومية أو دفاعية يتوقَّع أن تتسبَّب فى قتل أو إصابة أشخاص أو الإضرار بأعيان أو تدميرها أو تعطيلها[٣].

ويمكن الاستناد أيضًا إلى المبادئ الأساسية للقانون الدولي الإنساني لمعرفة مدى إمكانية تطبيقها بشأن ما أطلقنا عليها الحرب السيبرانية، ولعلَّ أحد أهمِّ تلك المبادئ ما يُعرَف بشرط «مارتينز»[٤]، ذلك الشرط الذي وُضِع أصلًا فى ديباجة اتِّفاقية

(١) انظر: الفصل ١٤ من دليل تالين.

(٢) انظر: المادة ٦٩ من دليل تالين.

(٣) انظر: المادة ٨٠ من دليل تالين.

(٤) شرط مارتينز، تمت تسميته بهذا الاسم نسبة إلى البروفيسور فيودور فيودوروفيتش مارتنز، المندوب الروسي في عام ١٨٩٩ لدى مؤتمر لاهاي للسلام، وقد ذكر مارتنز ذلك الشرط بعدما فشل المندوبون في مؤتمر السلام في الاتفاق على مسألة مركز المدنيين الذين يُشهرون السلاح ضد قوات الاحتلال، حيث كانت الدول العسكرية الكبرى ترى أنَّه يجب أن يُعامل هؤلاء المدنيُّون بوصفهم جنودًا غير نظاميين يخضعون لعقوبة الإعدام، في حين أنَّ الدول الصغيرة رأت أنَّه يجب معاملتهم بوصفهم محاربين نظاميين، ونتيجة لذلك الخلاف قام مارتنز بطرح رأيه الذي أصبح يُعرَف بشرط مارتنز، والذي جاء فيه: «يظلُّ المدنيون والمقاتلون تحت حماية وسُلطان مبادئ القانون الدولي كما استقرَّ بها العُرف ومبادئ الإنسانية وما يُمليه الضمير العام».

وقد ورد في ديباجة اتفاقية لاهاي لعام ١٨٩٩ وعام ١٩٠٧ بشأن قوانين وأعراف الحرب البرية، بالإضافة لذلك تَمَّ النصُّ عليه في اتفاقيات جنيف الأربع لعام ١٩٤٩ (في المادة ٦٣ من الاتفاقية الأولى، والمادة ٦٢ من الاتفاقية الثانية، والمادة ٤٢ من الاتفاقية الثالثة، والمادة ١٥٨ من الاتفاقية الرابعة)، وكذلك تَمَّ النصُّ عليه في البروتوكول الإضافي الأوَّل لعام ١٩٧٧ في المادة (م١/ف٢)، وفي ديباجة البروتوكول الثاني، وأخيرًا نصَّت عليه اتفاقية حظر أو تقييد استعمال أسلحة تقليدية معينة يمكن اعتبارها مُفرطة الضرر أو عشوائية الأثر لعام ١٩٨٠. ولا بُدَّ من الإشارة إلى أنَّ شرط مارتنز يَسري على جميع أطراف النزاع، سواء كانت طرفًا في الاتفاقيات التي تضمَّنها الشرط أم ليست كذلك، وهذا يرجع إلى طبيعته العُرفية والإنسانية. انظر: د. آيات محمد سعود، شرط مارتنز في القانون الدولي الإنساني، موقع الحوار المتمدن، متاح على الموقع الإلكتروني التالي:

https://www.ahewar.org/debat/show.art.asp?aid=591797

لاهاي الرابعة لعام ١٨٩٩ وعام ١٩٠٧، ودخل بعد ذلك فى نصّ البروتوكول الإضافي الأوَّل لعام ١٩٧٧ وفي ديباجة البروتوكول الثاني، حيث ينصُّ على ذلك الشرط على ما يلي: (فى حالة عدم وجود قاعدة معيَّنة فى القانون التعاهدي، يظلُّ المحاربون فى حمى وتحت سُلطة القانون العُرفي ومبادئ الإنسانية وما يُمليه الضمير العام[١].

وعليه يمكن الرجوع إلى شرط مارتينز كأساس لتفسير مُعاهدات القانون الدولي الإنساني كلَّما وُجدت الشكوك حول معنى بعض الأحكام الواردة فيه. واستنادًا إلى هذه القاعدة فإنَّ كلَّ ما يقع أثناء المنازعات يخضع لمبادئ القانون الدولي الإنساني، مما يعني عدم خلوّ الهجمات السيبرانية من القانون أثناء النزاع المسلَّح، وتُؤيِّد محكمة العدل الدولية عام ١٩٩٦ فى رأيها الاستشاري بشأن شرعية التهديد أو استخدم الأسلحة النووية، وذلك يُعدُّ أقرب إلى الهجمات السيبرانية بالقول: « يمنح شرط مارتينز سُلطة معالجة مبادئ القانون الدولي الإنساني وما يمليه الضمير العام بوصفها مبادئ القانون الدولي، تاركًا المحتوى الدقيق للمعيار الذي استلزم مبادئ القانون على ضوء الظروف المتغيِّرة، بما فى ذلك التغيُّرات فى وسائل الحرب ومستويات مظهر المجتمع الدولي وتسامحه [٢].

وبهذا الخصوص بيَّن المستشار القانوني للجنة الدولية للصليب الأحمر (Cordula Dorego) أنَّ الإطار القانوني الدولي الإنساني يُطبَّق على الحروب السيبرانية، ويجب احترامه، وقد تَمَّ تفنيد مزاعم مَن يُعدُّون خلوَّ الفضاء السيبراني من القوانين وعدم انطباق القانون الدولي الإنساني على الحروب السيبرانية بقولهم: أنَّ هذه ليست المرة الأولى التي يحدث فيها تطوير وتغيُّر فى التكنولوجيا المستخدَمة، وقد تعامل معها القانون الدولي الإنساني أو قانون النزاعات المسلحة، بمعنى: أنَّ القانون القائم قادر على التعامُل مع هذه التطوُّرات الجديدة دون الحاجة إلى إشعار أو وضع قواعد قانونية خاصة بالفضاء السيبراني[٣].

ويمكن الاستدلال بشأن ذلك بما ورد فى حُكم محكمة الولايات المتحدة الأمريكية العسكرية فى قضية كروب عام ١٩٤٨ والتي أشارت إلى «شرط مارتينز «

(١) د. يحيى ياسين سعود، الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني، ص: ٩٠.

(٢) انظر:

Also see : Doswald- Beck "international humanitarian law and the advisory opinion of international court of justice on the threat or use of nuclear weapons" ICRC Vol.316, 1997,pp.35-55.

(٣) د. عمر محمود أعمر، الحرب الإلكترونية في القانون الدولي الإنساني، المرجع السابق، ص: ١٣٨.

فى كونه أكثر من مجرَّد إعلان ورع، وأنَّه شرط عام يجعل العادات المستقِرَّة بين الأمم المتحضِّرة وقوانين الإنسانية وما يُمليه الضمير العام جزءًا من المقاييس القانونية التي يجب تطبيقها إذا لم وعندما لا تُغطِّي أحكام الاتفاقيات حالات مجدَّدة[١].

واتِّساقا مع ما تَمَّ الإشارة إليه، فإنَّ هناك اتفاقًا عامًّا مُنعقِدًا بين فُقهاء القانون الدولي الإنساني فى تفسير قواعد قانونية يستلزم مراعاتها بشأن النزاعات المسلَّحة مهما كانت درجتها أو أسلوب تطوُّرها، منها ما يُشير إليه البروتوكول الإضافي الأوَّل الملحَق باتفاقيات جنيف لعام ١٩٧٧، حيث نصَّ على ما يلي: «فى حالة الشكِّ بشأن شخص ما على أنَّه مدني أم غير مدني فيجب اعتبار ذلك الشخص مدنيًّا»[٢]. على أنَّ جوهر القواعد القائمة لا تستهدف حماية المدنيين فحسب، بل لا بُدَّ أن يكون فى إطار الاستهداف المشروع، وهو ما يُعبَّر عنه بمبدأ التمييز القائم بين مَن يُشارك أو يستطيع المشاركة فى العمليات العدائية، وكذلك التمييز بين الأهداف العسكرية والأعيان المدنية، حيث تجد هذه القاعدة سندها فى الفقه القانوني عندما عبَّر (بورتاليس) أنَّ الحرب هي علاقة دولة بدولة لا فرد بفرد، وأنَّها بين أمتين متحاربتين، لا يكون الأفراد الذين تتكوَّن منهم تلك الأمم أعداء إلا بصفة عرضية، ليس بوصفهم كرجال أو كمواطنين، وإنما فقط بوصفهم كجنود[٣].

ويلحق بعمومية مبادئ القانون الدولي الإنساني، مبدأ حظر الهجمات العشوائية، تلك الهجمات التي لا تُوجَّه إلى هدف عسكري محدَّد، أو الهجمات التي تستخدم طريقة أو وسيلة قتال لا يمكن تحديد آثارها على النحو الذي يقتضيه القانون الدولي الإنساني، وبالتالي من شأنها فى كلِّ حالة كهذه أن تُصيب أهدافًا عسكرية وأعيانًا مدنية ومدنيين دون تمييز[٤].

ويرتبط بما سبق الإشارة إليه، من أنَّه يُحظر الهجوم الذي قد يُتوقَّع منه أو يُسبِّب بصورة عرضية خسائر فى أرواح المدنيين أو إصابات بينهم أو الإضرار بالأعيان المدنية، أو قد يُسبِّب مجموعةً من هذه الخسائر والأضرار، ويكون مُفرِطًا فى تجاوُزه

(١) انظر:

Blimding weapons: Reports of the meetings of experts convened by the international committee of the red cross on battlefield laser weapons, 1989-1991, ICRC, 1993,P.22-23.

(٢) الفقرة ١ من المادة ٥٠ من البروتوكول الإضافي الأوَّل الملحَق باتفاقيات جنيف لسنة ١٩٧٧.

(٣) انظر:

Hall William Edward, A Treatise on international law , Fourth edition , Oxford, London, 1895,pp.68-69.

(٤) الفقرة ٤ من المادة ٥١ من البروتوكول الإضافي الأوَّل الملحق باتفاقيات جنيف لسنة ١٩٧٧.

ما ينظر إليه أو يُسفر عنه من ميزة عسكرية ملموسة ومباشرة، وهذا ما يُطلَق عليه مبدأ التناسُب، ذلك المبدأ الذي يجد أساسه أيضًا فى قواعد القانون الدولي الإنساني العُرفي والتي تُطبَّق فى النزاعات المسلَّحة الدولية وغير الدولية [١] .

ويُعدُّ مبدأ الضرورة العسكرية الذي هو هدف تحطيم الخصم والقضاء على قُدراته العسكرية، والمادية، والبشرية من شأنها أن تُعطي للمُتحاربين استخدام وسائل العنف التي لا غِنى عنها لتحقيق هذا الهدف [٢] .

فالغرض الذي يتمُّ اختياره بالهجمات السيبرانية، هو الغرَض الذي مِن المتوقَّع أن يُسبِّب خطر أقلَّ على الأعيان المدنية والمدنيين، على أنَّه فى مُراعاة لمبدأ الضرورة العسكرية يتطلَّب أن يختار الهجوم الذي يتسبَّب بأضرار وإصابات أقلَّ، وفي حالة وجود أهداف كثيرة إلا أنَّ إحداهما يتحقَّق معها ميزة عسكرية أكثر من مثيلاتها، وفي هذه الحالة من حقِّ المهاجم توجيه الهجمات السيبرانية المباشرة ضدَّ الهدف العسكري الذي يُحقِّق أكثر ميزة ممكنة فى النزاع المسلَّح. ومن هذا المنطلَق لا بُدَّ أن يُنظر إلى الهجمات السيبرانية وإلى الضرر الذي يلحق بالمنشآت والبنية التحتية المهمَّة بالنسبة للمدنيين، بالإضافة إلى ما يُصيب المدنيين من حرمان من وظائف وخدمات فى هذه المنشآت تطبيقًا لمبدأ الضرورة العسكرية [٣].

ويُكمل مبدأ الإنسانية مبدأ الضرورة العسكرية، والذي يُعدُّ الضمانة الأساسية والقانونية لاحترام حقوق الإنسانية وحمايته الأساسية أثناء سير العمليات الحربية، ويبدو أهَمِّيَّة هذا المبدأ فى إلزام الأطراف المتنازعة الأخذ به، وهو التزام قانوني دولي فى غياب الاتفاقيات الدولية التي لا يُوجَد بها حلٌّ لبعض الحالات[٤] ، حيث إنَّ هذا المبدأ يُحيط بكافة التصرُّفات بين الأطراف المشاركة فى النزاع المسلَّح.

كما يحظر بموجب هذا المبدأ، إلحاق الآلام أو الإصابة التي لا مُبرِّر لها، وبالتالي فإنَّ ذلك المبدأ يحظر اللجوء إلى وسائل أو أساليب الحرب التي لا تحظر استخدامها قاعدة أخرى من قواعد القانون الدولي الإنساني، من حيث أنَّ حقَّ أطراف

(١) الفقرة الفرعية ب من الفقرة ٥ من المادة ٥١ وكذلك المادة ٥٧ من البروتوكول الإضافي الأوَّل الملحق باتفاقيات جنيف لسنة ١٩٧٧.
(٢) د. نزار العنبكي، القانون الدولي الإنساني، الطبعة الأولى، ٢٠١٠، ص: ٦٢.
(٣) د. مايكل شميت، الحرب بواسطة شبكات الاتصال، الهجوم على شبكات الكمبيوتر والقانون في الحرب، المجلة الدولية للصليب الأحمر، ٢٠٠٢، ص: ١٣٠.
(٤) د. محمد فهاد الشلالدة، القانون الدولي الإنساني، منشأة المعارف، الإسكندرية، ٢٠٠٥، ص: ٦٣.

أيِّ نزاع مُسلَّح اختيار أساليب ووسائل القتال ليس حقًا لا تُقيِّده قيود[١]، وكذلك حظر استخدام الأسلحة والقذائف والمواد ووسائل القتال التي من شأنها إحداث إصابات أو آلام لا مُبرِّر لها[٢].

فمبدأ الإنسانية يعني الاعتراف بالحرب باعتبارها حقيقة واقعية، ويسعى فى الوقت ذاته إلى وضع حدود لاحترام الإنسان، وذلك عن طريق وضع قواعد وسلوكيات للحرب تأخذ فى حسبانها كلًا من الضرورة العسكرية، والضرورة الإنسانية التي تصون كرامة الإنسان[٣].

وبناءً على ذلك فإنَّ إمكانية تطبيق هذا المبدأ على الهجمات السيبرانية قد لا يختلف عن جميع أساليب الحرب الأخرى من حيث عدم التسبُّب فى الآلام التي لا مُبرِّر لها[٤].

(١) الفقرة ١ من المادة ٣٥ من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف لعام ١٩٧٧.
(٢) الفقرة ٢ من المادة ٣٥ من البروتوكول الإضافي الأول الملحق باتفاقيات جنيف لعام ١٩٧٧.
(٣) د. محمود حجازي محمود، العنف الجنسي ضد المرأة في أوقات النزاعات المسلَّحة، دار النهضة العربية، القاهرة، ٢٠٠٧، ص: ٦٤.
(٤) د. مايكل شميت، الحرب بواسطة شبكات الاتصال، الهجوم على شبكات الكمبيوتر والقانون في الحرب، المرجع السابق، ص: ١٣٥.

المطلب الثاني

خصوصية المخاطر السيبرانية فى القانون الدولي الإنساني

إذا كنَّا قد تطرَّقنا إلى شمولية مبادئ وقواعد القانون الدولي الإنساني، إلا أنَّ ذلك لا يعني إنكار حقيقة التغيُّرات التي شهدتها طبيعة الحروب منذ اعتماد اتفاقية جنيف الأصلية قبل ما يُقارب مائة وخمسين عامًا، حيث أصبحت وسائل وأساليب الحروب متطوِّرة إلى درجة لم يكن يتصوَّرها واضعو تلك الاتفاقية، ولعلَّ الاستخدام المتزايد للفضاء السيبراني للأغراض العسكرية أحد أهم الأسباب التي تدعو إلى إعادة النظر فى القواعد التي تُنظِّم سير النزاعات المسلَّحة وصياغتها بالشكل الذي يتلاءم مع طبيعة هذه الاستخدامات [١].

فإذا كان شرط مارتينز السابق الإشارة إليه يمكن تطبيقه على الحرب السيبرانية، فإنَّ بعض قواعد القانون الدولي الإنساني لا بُدَّ من تطوُّرها وتغيُّرها بحيث تتماشى مع الحرب السيبرانية. فنجد فى تطبيق مبدأ التميُّز، الذي يُعدُّ الأساس لأحكام البروتوكولين الإضافيين لاتفاقيات جنيف ١٩٧٧، قد نصَّت المادة ٤٨ من البروتوكول الأوَّل على: أن «تعمل أطراف النزاع على التمييز بين السكان المدنيين والمقاتلين، وبين الأعيان المدنية والأهداف العسكرية، ومن ثَمَّ تُوجِّه عملياتها ضدَّ الأهداف العسكرية دون غيرها؛ وذلك من أجل تأمين احترام وحماية السكان المدنية والأعيان المدنية» - إلا أنَّ ذلك من الصعوبة بمكان تطبيقه فى الحرب السيبرانية، فهذه الأخيرة يمكن توجيه الهجمات السيبرانية إلى الأنظمة المدنية والبنية التحتية ما لم تكن هذه الأنظمة المدنية والبنية التحتية أهدافًا عسكرية [٢].

ففي إطار تطبيق مبدأ التمييز بين المقاتلين والمدنيين على الهجمات السيبرانية أو الحروب السيبرانية، أشارت مبادئ تالين، على الرغم من عدم إلزامية قواعده، بأنَّه لا يجوز أن تكون الأعيان المدنية هدفًا للهجمات السيبرانية، فلا يجوز على سبيل المثال توجيه الهجمات السيبرانية التي من شأنها تدمير الأنظمة المدنية

(١) انظر:

Jeffrey T.G Kalsey, Hacking in to international humanitarian law: The principles of distinction and neutrality in the age of cyber warfare, Michigan law review, 2008, vol.106, issue 7 ,p.1437.

(٢) د. مايكل شميت، الحرب بواسطة شبكات الاتصال، الهجوم على شبكات الكمبيوتر والقانون في الحرب، المرجع السابق، ص: ١٠٥.

والبنية التحتية، ما لم تُعدَّ هذه الأنظمة من قبيل الأهداف العسكرية التي يجوز استهدافها وفق الظروف السائدة[١].

ولكن فى حقيقة الأمر فإنَّ تطبيق مبدأ التمييز بين المقاتلين والمدنيين على الهجمات السيبرانية هو أمرٌ فى غاية التعقيد؛ إذ إنَّ المهاجم فى الأغلب يكون بعيدًا عن مكان الهجوم ما يجعل التأكُّد من الالتزام به أمرًا غاية فى الصعوبة[٢].

ويرى خبراء الأمن أنَّه من الصعب توجيه هجوم سيبراني إلى هدف عسكري فى دولة ما دون أن يمتدَّ أثره على كافة جوانب الأمن القومي لهذه الدولة، حيث يتميَّز الفضاء السيبراني بالارتباط بين نظم الحواسيب، ويتألَّف هذا الفضاء من عدد لا يُحصى من نُظُم الحواسيب المتصلة بعضها ببعض فى أرجاء العالم. وغالبًا ما يبدو أنَّ نُظُم الحواسيب العسكرية تتصل بالنظم التجارية والمدنية، وتعتمد عليها كليًا أو جزئيًا. وبالتالي يكون من المستحيل شنُّ هجوم سيبراني على بنية تحتية عسكرية وجعل الآثار تقتصر على هدف عسكري فحسب. فإذا تَمَّ توجيه هجمات سيبرانية ضدَّ بِنية تحتية تُستخدم للاستعمال المزدوج المدني والعسكري وعن بُعد، فلا يبدو أنَّ الميزة العسكرية الملموسة والمباشرة ستكون واضحة، ما يجعل تطبيق مبدأ التناسُب فى أثناء الهجمات السيبرانية أمرًا مُعقَّدًا عمليًا(٣). ومن المسَلَّم به أنَّ أيًا من الأعيان المدنية التي تُستخدم لأغراض عسكرية تُصبح هدفًا عسكريًا، وبالتالي لا تتوافر لها الحماية بموجب القانون الدولي الإنساني.

أمَّا بالنسبة لمبدأ الضرورة العسكرية، أشار دليل تالين، إلى أنَّه فى الحالات التي يكون هناك عدَّة أهداف عسكرية لكي يكون هناك خيار، فالهدف الذي يقع عليه الخيار للهجوم السيبراني هو الذي يُتوقَّع منه أن يُلحِق خطرًا أقلَّ على المدنيين والأعيان المدنية، على أنَّ مراعاة تطبيق مبدأ الضرورة العسكرية لا بُدَّ أن يكون الذي يُسبِّب أضرارًا وإصابات أقلَّ، أمَّا فى حالة وجود أهداف عديدة وأنَّ أحدهما سوف يُحقِّق ميزة عسكرية أكثر من غيرها هنا فمن حقِّ المهاجم توجيه الهجمات السيبرانية ضدَّ الهدف العسكري الذي يُحقِّق ميزة أكثر فى النزاع المسلَّح، ومن هنا

(١) مايكل شميت، الحرب بواسطة شبكات الاتصال، الهجوم على شبكات الكمبيوتر والقانون في الحرب، المجلة الدولية للصليب الأحمر، ٢٠٠٢، ص: ١٠٥.

(٢) د. أحمد عبيس الفتلاوي، الهجمات السيبرانية: مفهومها والمسئولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، جامعة بابل- كلية القانون، العدد الرابع، السنة الثامنة، ٢٠١٦، ص: ٦٤٢.

(٣) د. أحمد الأنور، قواعد وسلوك القتال، دراسات في القانون الدولي الإنساني، دار المستقبل العربي، القاهرة، ٢٠٠٠، ص: ٣١٩.

لا بُدَّ من النظر إلى الضرر الذي يُصيب البنية التحتية والمنشآت الحيوية بالنسبة للمدنيين بالإضافة إلى حرمانهم من الوظائف وخدمات هذه المنشآت [١].

وبخصوص تطبيق مبدأ الإنسانية والذي قد يكون عدم التسبُّب بآلام لا مُبرِّر لها جزءًا منه، فإنَّه يمكن تطبيق هذا المبدأ على الهجمات السيبرانية، قد لا تختلف عن جميع أساليب وصور الحرب الأخرى من ناحية ضرورة عدم إلحاق أضرار أو الآلام التي لا مُبرِّر لها[٢].

وقد قامت جهود دولية من أجل تنظيم الحرب السيبرانية بإصدار دليل «تالين» حول القانون الدولي الذي يُطبَّق على هذه الحرب فى عام ٢٠١٢ الذي بدأ فى صياغته فى عام ٢٠٠٩، وهو من إعداد اللجنة الدولية للخبراء بدعوة من مركز التميُّز للدفاع السيبراني التعاوني التابع لحلف شمال الأطلسي، ويُطبَّق على النزاع المسلَّح الدولي أو النزاع غير المسلَّح الدولي، ويعني ذلك بأن تكون الحرب بين طرفين مُتنازعين، وتُعتبر وثيقة غير مُلزمة، ومن خصائص هذه الحرب [٣]:

١- أنَّها لا تقف عند حدود الدول، فهو نزاع مُسلَّح تتعدَّى حدود الدول.

٢- صعوبة تحديد المكان الذي ينطلق منه الهجوم وإثبات المسئولية الناشئة عنه.

٣- صعوبة معرفة القائم بالهجوم ودوافعه.

ولا تقتصر ضرورة المواءمة بين الحروب السيبرانية وأحكام القانون الدولي الإنساني على المبادئ فقط، وإنَّما هناك كثير من الإشكاليات التي تُثيرها الهجمات السيبرانية فى إطار النزاعات المسلَّحة مثل تحمُّل مسئولية الأفعال غير القانونية التي يمكن أن تتضمَّن خيارات القائد العسكري والمبرمج والمصنِّع، لا سيَّما إذا تعلَّق الأمر بالمسئولية الجنائية الفردية، وكذلك المركز القانوني لأسير الحرب الذي يصعب تطبيقه فى إطار الحروب السيبرانية.

لذلك فإنَّه من الضروري -وعلى الرغم من ضرورة التأكيد على انطباق أحكام القانون الدولي الإنساني على الحروب السيبرانية فى الوقت نفسه- صياغة

(١) د. مايكل شميت، الحرب بواسطة شبكات الاتصال، الهجوم على شبكات الكمبيوتر والقانون في الحرب، المرجع السابق، ص: ١٣٠.
(٢) د. مايكل شميت، الحرب بواسطة شبكات الاتصال، الهجوم على شبكات الكمبيوتر والقانون في الحرب، المرجع السابق، ص: ١٣٥.
(٣) د. سلافة طارق الشعلان، تكييف استخدام الحرب الإلكترونية في النزاعات المسلحة وفقًا للقانون الدولي الإنساني، مجلة كلية القانون، جامعة الكوفة، المجلد ٩، العدد ٢٦، ٢٠١٦، ص: ٥-٦.

قواعد اتفاقية مُلزِمة مُكمِّلة لاتفاقيات جنيف الأربع لعام ١٩٤٩ والبروتوكولين الإضافيين الملحقَين بها لعام ١٩٧٧، تتناول بالتنظيم وبالتحديد الحروب السيبرانية؛ لضبط قواعد هذه الحرب ونتائجها دون التي تكاد لا تختلف عن النزاعات المسلَّحة التقليدية، بحيث تكون مُلزِمة للأطراف الفاعلة من جهة وغير مختلَف على مدى إلزاميتها وحالات انطباقها من جهة أخرى.

الفصل الثالث

الجهود الدولية لمواجهة المخاطر السيبرانية

أدَّى ظهور الجرائم السيبرانية -كنمط جديد من أنماط الجريمة وما تتميَّز به هذه الجرائم من خاصية عابرة للحدود الإقليمية للدول- إلى توجُّه الدول والمنظمات الدولية ببذل وتكثيف الجهود الرامية لمواجهة ومجابهة الخطورة التي يُشكِّلها هذا الإجرام المستحدَث، لا سيَّما وأنَّه من الجرائم العابرة للحدود، وفيما يلي سوف نستعرض أهمَّ الجهود الدولية، سواء تمثَّل ذلك فى جهود المنظمات الدولية أو المجهودات الفقهية أو الدول.

فقد أدركت الدول والمنظَّمات الدولية أهَمِّيَّة التعاون الدولي فى صدِّ الهجمات السيبرانية وجرائمها، فعمدت إلى عقد الكثير من الاتفاقيات؛ لتسهيل مهمَّة التحقيق فى الهجمات السيبرانية والإرهاب الإلكتروني [١].

وتعمل عددٌ من المنظَّمات الدولية باستمرار لمواكبة التطوُّرات فى شأن أمن الفضاء السيبراني، وقد أسَّست مجموعات عمل لوضع إستراتيجيات لمكافحة جرائم الإنترنت. ويُستخدَم مصطلح «الأمن السيبراني» لتلخيص أنشطة مختلفة كجمع المعلومات ووضع السياسات العامة والتدابير الأمنية، والمبادئ التوجيهية، وطُرُق إدارة المخاطر، والحماية، والتدريب، ودليل لأفضل الممارسات المهنية، ومختلف التقنيات التي يمكن استخدامها لحماية شبكة الإنترنت. وتشمل هذه السياسات: المعلومات، والخدمات، ونُظُم الاتصالات السلكية واللاسلكية، ومجمل المعلومات المنقولة أو المخزَّنة فى الأجهزة الإلكترونية؛ وذلك لضمان تحقيق سلامة المؤسَّسات والأفراد فى مواجهة المخاطر الأمنية، وكلِّ ما يتعلَّق بشبكة الإنترنت [٢].

وسوف نُوضِّح الجهود الدولية التي اتخذتها المنظمات الدولية فى هذا الشأن والمساهمات الفقهية بشأن المخاطر السيبرانية، وذلك من خلال مبحثين على النحو التالي:

المبحث الأوَّل: بعض جهود التعاون الدولي بشأن تنظيم العمليات السيبرانية.

المبحث الثاني: المجهودات الفقهية لمواجهة المخاطر السيبرانية.

---

(١) د. محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، ورقة بحثية في مؤتمر «القانون والكمبيوتر والإنترنت»، كلية الشريعة والقانون، الإمارات، خلال الفترة من ١-٣ مايو ٢٠٠٠، ص: ١٠٧٨.

(٢) انظر:

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

المبحث الأوَّل

بعض جهود التعاون الدولي بشأن تنظيم العمليات السيبرانية

حاولت الدول حماية مصالحها من التضرُّر، بسبب استهدافها بعمليات سيبرانية مختلفة، أو استهداف الشركات الخاصة بها ومواطنيها، فسعت من خلال عضويتها فى منظمات دولية، أو من خلال تشريعاتها الوطنية، إلى محاولة تنظيم هذه العمليات، كما شاركت فى بعض المؤتمرات لنفس الغرض، ونعرض لبعض هذه الممارسات من خلال المطالب التالية:

المطلب الأوَّل: جهود منظمة الأمم المتحدة.

المطلب الثاني: الاتفاقيات الدولية فى مجال مكافحة الهجوم السيبراني.

المطلب الثالث: جهود بعض المنظمات العالمية المتخصّصة والتحالُفات الدولية فى مكافحة الإرهاب السيبراني.

المطلب الأوَّل

جهود منظمة الأمم المتحدة

تلعب العديد من المنظَّمات وعلى رأسها منظمة الأمم المتحدة دورًا هامًا فى تعزيز العمل المشترك بين الدول؛ للحدِّ من انتشار الجرائم المعلوماتية، ومواجهة المخاطر السيبرانية، وعقدت فى سبيل ذلك العديد من المؤتمرات بداية من المؤتمر السابع الذي عُقِد فى ميلانو ١٩٨٥ حتى المؤتمر الثاني عشر فى ٢٠١٠ بالإضافة إلى المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات والذي عُقِد تحت إشراف الأمم المتحدة فى عام ١٩٩٤، ونتج عنه عدَّة توصيات ذات صلة بجرائم المعلومات، بعضها تناول الأفعال التي تقع تحت طائلة الإجرام المعلوماتي، والبعض الآخر يتمثَّل فى الإجراءات الواجب اتباعها لتطبيق القواعد الموضوعية.

وهكذا أصدرت منظمة الأمم المتحدة عدَّة قرارات وتوصيات بشأن العمليات السيبرانية، كما أنشأت فِرقًا من الخبراء الحكوميين المعنيين بهذه العمليات، وناقشت هيئاتها أمن الفضاء السيبراني، وفيما يلي بيان ذلك:

الفرع الأوَّل

قرارات ووثائق الجمعية العامة للأمم المتحدة بشأن الإرهاب السيبراني

أصدرت الجمعية العامة للأمم المتحدة عدَّة قرارات بشأن جرائم الإرهاب السيبراني، منها القرار رقم ٦٣/٥٥ فى ٤ ديسمبر ٢٠٠٠م، والقرار رقم ١٢١/٥٦ فى ١٩ ديسمبر ٢٠٠١، بشأن مكافحة سوء استخدام تكنولوجيا المعلومات، وقد أوصى القرار الأوَّل بأنَّ: تضمن الدول فى قوانينها وممارساتها عدم توفير ملاذات آمنة لكلِّ مَن يُسيء استخدام تكنولوجيا المعلومات، وضمان حماية سرية المعلومات وسلامة أنظمة الحاسوب، ضدَّ أيِّ اعتداء غير مشروع، مع تقرير عقوبة على ذلك الفعل. ودعا القرار ١٢١/٥٦، الدول الأعضاء عند وضع التشريعات الوطنية لمكافحة إساءة استعمال تكنولوجيا المعلومات، على أن تأخذ بالاعتبار عمل لجنة منع الجريمة والعدالة الجنائية. وفي عام ٢٠٠٢ أصدرت الأمم المتحدة القرار رقم ٢٣٩/٥٧، بشأن إرساء ثقافة عالمية للأمن السيبراني، حيث اعتمدت فيه قرارًا بشأن الأمن السيبراني والذي سلَّمَت فيه بضرورة دعم الجهود الوطنية بتبادل المعلومات والتعاون فى هذا المجال على الصُّعُد الوطنية والإقليمية والدولية؛ كي يتسنَّى التصدِّي الفعَّال لما تتَّسِم به هذه التهديدات السيبرانية بصفة متزايدة، من طابع عابر للحدود الوطنية. ويَشهد هذا القرار على التزام العالم بإنشاء ثقافة عالمية للأمن السيبراني، وأهمُّ ما فى القرار أنَّه يُؤكِّد أنَّ الأمن السيبراني للهياكل الأساسية الحيوية للمعلومات مسئولية مُلقاة على عاتق الحكومات، ومجال يجب عليها أن تحمل فيه لواء الصدارة وطنيًا، بالتنسيق مع أصحاب المصلحة ذوي الشأن.

وفي عام ٢٠٠٥ أصدرت الأمم المتحدة القرار ٦٠/١٧٧، بشأن تشجيع التعاون الدولي لمكافحة الجرائم الإلكترونية، وتقديم المساعدة للدول الأعضاء فى هذا المجال، كما أصدرت فى عام ٢٠١٠، القرار رقم ٦٤/٢١١ الذي يدعو الدول إلى تحديث قوانينها فى مجال الجرائم الإلكترونية، والخصوصية، والبيانات الشخصية، والتجارة والتوقيع الإلكترونيين، وكذلك اعتماد اتفاقيات إقليمية بهذا الشأن[1].

(١) انظر:

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

ودعا القرار رقم ٤١/٦٥ والذي صادقت الجمعية العامة للأمم المتحدة عليه فى يناير ٢٠١١ على تقرير فريق الخبراء الحكوميين فى مجال المعلومات والاتصالات السلكية واللاسلكية فى سياق الأمن الدولي. وتضمَّنت استنتاجات فريق الخبراء من بينها ما ذكرته من أنَّ هناك دول تستحدث تكنولوجيا المعلومات والاتصال كوسائل للحرب والاستخبارات، وتَلفت اللجنة الدولية فى هذا الصدد انتباه الدول إلى عواقب الحرب السيبرانية، وهي مجموعة من الهجمات على شبكة الحواسيب خلال حالات النزاع المسلَّح، وقد تشمل هذه العواقب سيناريوهات كارثية مثل: التشويش على نُظُم مُراقبة الملاحة الجوية، والتسبُّب بتصادم الطائرات أو تحطُّمها، أو قطع إمدادات الكهرباء أو الماء على السكان المدنيين، أو إلحاق أضرار بالمرافق الكيميائية أو النووية. وتُذكِّر اللجنة الدولية بضرورة التزام كلِّ الأطراف فى النزاعات المسلَّحة باحترام قواعد القانون الدولي الإنساني إذا لجأت إلى وسائل وأساليب الحرب الإلكترونية، ومن هذه القواعد مبادئ التمييز والتناسُبية والحيطة[١].

الفرع الثاني

قرارات المجلس الاقتصادي والاجتماعي

قرارات المجلس الاقتصادي والاجتماعي ٤٦/٢٠٠٦، ٨/٢٠٠٧، ٣/٢٠٠٨، ٧/٢٠٠٩، هي التي أحاطت فيها اللجنة المعنية بتسخير العلم والتكنولوجيا لأغراض التنمية علمًا بنتائج تنفيذ مؤتمر القمَّة العالمي لمجتمع المعلومات، استنادًا إلى ما ورد من مساهمات من كيانات الأمم المتحدة ذات الصلة وغيرها من الكيانات، حسب الاقتضاء. فضلًا عن ذلك افتتح المجلس الاقتصادي والاجتماعي دورته لعام ٢٠١٠ بجلسة إعلامية عن التحديات التي يطرحها الأمن السيبراني، فضلًا عن التهديدات والفُرص التي يُتيحها استخدام الإنترنت الآخذ فى الاتساع، وقد شدَّد المجلس من بين عدَّة أمور على الحاجة إلى اتخاذ مبادرات دولية تكفل تبادل المعلومات وأفضل الممارسات والتدريب والبحث، وإضافة إلى ذلك، أعلن المشاركون فى المناقشة أنَّه يتعيَّن على الأمم المتحدة أن «تُوحِّد أداءها» بشأن هذه القضية، مما سيُؤدِّي حتمًا إلى زيادة التعاون بين البلدان بل وبين الدول والقطاع الخاص أيضًا؛ لضمان الأمن السيبراني[٢] وحذروا من

(١) بيان اللجنة الدولية للصليب الأحمر للأمم المتحدة ٢٠١١ بشأن المناقشات العامة لكافة بنود جدول الأعمال في ما يتعلَّق بنزع السلاح والأمن، الجمعية العامة للأمم المتحدة، الدورة ٦٦، اللجنة الأولى، البندان ٨٧ و ١٠٦ من جدول الأعمال، بيان اللجنة الدولية للصليب الأحمر، نيويورك، ١١ أكتوبر ٢٠١١.

(٢) المجلس الاقتصادي والاجتماعي الدورة الموضوعية لعام ٢٠١٠ نيويورك ، ٢٨ يونيه -٢٣ يوليه ٢٠١٠ البند ١٣ (ب) من جدول الأعمال المؤقت، المسائل الاقتصادية والبيئية: تسخير العلم والتكنولوجيا لأغراض التنمية والتقدم المحرَز في تنفيذ ومتابعة نتائج مؤتمر القمة العالمي لمجتمع المعلومات على الصعيدين الإقليمي والدولي.

النطاق الدولي لحرب سيبرانية فعلية وعواقبها وخيمة سوف تحدث بشكل خطير إن لم يتمَّ تدارُك الأمر، ومن ثَمَّ لا بُدَّ أن تكون هناك استجابة منسَّقة بين الدول؛ ولا تكفي الآن إستراتيجيات اعتماد حلول على أساس مخصَّص وتقوية الدفاع [١].

ودعا القرار أيضًا إلى اتِّباع نهج قائم على إدراك المخاطر، بحيث يُحاط جميع أصحاب المصلحة علمًا بالمخاطر ذات الصلة والتدابير الوقائية والردود الفعَّالة على نحو مُناسب، كلٌّ فى إطار الدور المنوط به. وأشار القرار إلى أنَّ الجهود الوطنية إلزامية إلى حماية الهياكل الأساسية الحيوية للمعلومات التي تستفيد من التقييم الدوري للتقدُّم الذي تُحرزه هذه الجهود. 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 يتسنَّى إبراز «ما يتمُّ تحقيقه من الإنجازات وأفضل الممارسات والدروس المكتسَبة والإجمالات التي تتطلَّب مزيدًا من التدابير على الصعيد الوطني»، وقدَّم استقصاء طوعيًا فى شكل تقييم ذاتي للأمن الإلكتروني الوطني باعتباره أداة يمكن أن تُساعد البلدان على استعراض الجهود الوطنية المبذولة فى مجال الأمن السيبراني وحماية الهياكل الأساسية الحيوية للمعلومات [٢].

وفي سبتمبر عام ٢٠١١ عقد المجلس الاقتصادي والاجتماعي للأمم المتحدة، اجتماعًا لمناقشة أمن الفضاء الإلكتروني والتنمية، والقضايا والتحديات ذات الصلة، واشترك فى المناقشات إدارة الشئون الاقتصادية والاجتماعية، والاتحاد الدولي للاتصالات، ورئيس لجنة الأمم المتحدة المعنية بتسخير العلم والتكنولوجيا لأغراض التنمية، ومنظومة الأمم المتحدة، والقطاعين العام والخاص، بالإضافة إلى منظَّمات المجتمع المدني المهتمَّة بمجالات الفضاء السيبراني والجرائم الإلكترونية، وحُدِّدت أهداف الاجتماع بأنَّها؛ تتمثَّل فى بناء وعي على مستوى السياسات الدولية، عبر تزويد أعضاء المجلس الاقتصادي والاجتماعي، بصورة عن الوضع الحالي والتحديات المتعلِّقة بأمن الفضاء الإلكتروني، وارتباطه بالتنمية؛ وتحديد أفضل السياسات المتعلِّقة بهذا المجال، والمبادرات المطبَّقة فى مختلف أنحاء العالم؛ لبناء ثقافة أمن الفضاء السيبراني، وكذا استكشاف خيارات للاستجابة العالمية بشأن تزايد معدَّلات الجريمة السيبرانية.

(١) المرجع نفسه (مناقشة «الأوراق المالية الرقمية» أو النظام النقدي الرقمي المستخدم في البلدان الإفريقية).
(٢) د. أميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسُبُل مواجهتها في القانون الدولي العام، المرجع السابق، ص: ٤٨٧.

كما ناقش الاجتماع الفوارق الاقتصادية بين الدول، وعدم قدرة الدول النامية منها على مُكافحة الجرائم السيبرانية، وكذلك افتقاد الشراكة بينها وبين الدول الصناعية، مما يُؤدِّي إلى خلق ملاذٍ آمن لمهاجمي الفضاء السيبراني لارتكاب جرائمهم.كما تَمَّ مناقشة الحاجة إلى إبرام اتفاقية دولية بشأن الفضاء الإلكتروني، بما يشمل احتمال البناء على اتفاقية «بودابست» باعتبارها تنسيقًا بين الدول بشأن بعض الجرائم السيبرانية، كالتعدِّي على حقِّ المؤلف، والغشِّ، واستغلال الأطفال فى المواد الإباحية، وجرائم الكراهية، وانتهاكات أمن الشبكات. وقرَّر «لازاروس كابامبي» رئيس المجلس الاقتصادي والاجتماعي، أنَّ أعضاء الاجتماع قد اتَّفقوا على أنَّ الأمن السيبراني قضية عالمية، لا يمكن حلُّها إلا عبر شراكة عالمية، لا سيَّما من خلال الأمم المتحدة التي يمكنها استخدام قُدراتها الإستراتيجية والتحليلية لمعالجة مثل هذه القضايا[1].

الفرع الثالث

مؤتمر الأمم المتحدة الثامن لمنع الجريمة

ومعاملة السجناء ... هافانا ١٩٩٠ بشأن الجرائم ذات الصلة بالكمبيوتر

يُعتبَر مؤتمر هافانا ١٩٩٠[2] من أبرز جهود الأمم المتحدة المتعلِّقة بالجرائم ذات الصلة بالكمبيوتر، فقد أكَّد المؤتمر على وجوب تطبيق التطوُّرات الجديدة فى مجال العلم والتكنولوجيا فى كلِّ مكان لصالح الشعوب، وبالتالي لمنع الجريمة على نحو فعَّال، كما أكَّد على أنَّ التكنولوجيا بما أنَّها قد تُولِّد أشكالًا جديدة من الجريمة فإنَّه ينبغي اتخاذ تدابير مُلائمة ضدَّ حالات إساءة الاستعمال المخلَّة لهذه التكنولوجيا، وأشاروا إلى مسألة الخصوصية التي يمكن أن تُخترَق عن طريق الاطلاع على البيانات الشخصية المخزَّنة داخل نُظُم الحسابات الآلية والتي تُشكِّل انتهاكًا لحقوق الإنسان واعتداءً على حرمة الحياة الخاصة، كما أكَّد المؤتمر على وجوب اعتماد ضمانات مُلائمة لحفظ السرية، كذلك أكَّد المؤتمر عبر قواعده التوجيهية على ضرورة تشجيع التشريعات الحديثة التي تُجرِّم وتتناول جرائم الحاسب الآلي

(١) د. محمد عادل محمد عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسُّس وقت السلم «دراسة على ضوء دليل «تالين» بشأن القانون الدولي المطبَّق على العمليات السيبرانية ٢٠١٣-٢٠١٧»، ٢٠٢٠م، ص: ٦٣.

(٢) د. محمد الأمين، د. محسن عبد الحميد أحمد، معايير الأمم المتحدة في مجال العدالة الجنائية ومنع الجريمة، أكاديمية نايف للعلوم الأمنية، الرياض، الطبعة الأولى، ١٩٩٨، ص: ١٩.

باعتبارها نمطًا من أنماط الجريمة المنظَّمة؛ كغسيل الأموال والاحتيال المنظَّم وفتح حسابات وتشغيلها بأسماء وهمية، وقد أكَّد مؤتمر هافانا ١٩٩٠ عدَّة مبادئ أهمُّها: تحديث القوانين الجنائية الوطنية بما فى ذلك التدابير المؤسَّساتية، وتحسين أمن الحاسب الآلي والتدابير الفنية، واعتماد إجراءات تدريب كافية للمُوظَّفين والوكالات المسئولة عن منع الجريمة الاقتصادية والجرائم المتعلِّقة بالحاسب الآلي والتحرِّي والادِّعاء فيها، تلقين آداب الحاسب الآلي كجزءٍ من مفردات مقرَّرات الاتصالات والمعلومات، وزيادة التعاون الدولي من أجل مكافحة هذه الجرائم.

كما حثَّ المؤتمر الدول الأعضاء على مضاعفة الأنشطة التي تبذلها على الصعيد الدولي؛ من أجل مكافحة الجرائم المتصلة بالكمبيوتر بما فى ذلك دخولها كأطراف فى المعاهدات المتعلِّقة بتسليم المجرمين وتبادل المساعدة فى المسائل الخاصة المرتبطة بهذه الجريمة، ونصح هذا القرار الدول الأعضاء بالعمل على أن تكون تشريعاتها ذات العلاقة بتسليم المجرمين وتبادل المساعدة فى المسائل الجنائية تنطبق بشكل تامٍّ على الأشكال الجديدة للإجرام مثل الجرائم السيبرانية، وأن تتخذ خطوات محدَّدة نحو تحقيق هذا الهدف، كما تُكمل الأمم المتحدة رؤيتها بشأن الجريمة السيبرانية بصفة عامة بضرورة وضع أو تطوير[1]:

١- معايير دولية لأمن المعالجة الآلية للبيانات.

٢- اتخاذ تدابير مُلائمة لحلِّ إشكاليات الاختصاص القضائي التي تُثيرها الجرائم السيبرانية العابرة للحدود أو ذات الطبيعة الدولية.

٣- إبرام اتفاقيات دولية تنطوي على نصوص تنظيم وإجراءات التفتيش والضبط المباشر الواقع عبر الحدود على الأنظمة الإلكترونية المتصلة فيما بينها والأشكال الأخرى للمساعدة المتبادلة، مع كفالة الحماية فى الوقت ذاته لحقوق أفراد وحرياتهم وسيادة الدولة.

(١) د. عبد الفتاح حجازي، الإثبات الجنائي في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص: ١٩٠.

الفرع الرابع

إنشاء فريق من الخبراء الحكوميين المعنيين بالعمليات السيبرانية

فى عام ٢٠٠٤، أنشأت الجمعية العامة للأمم المتحدة مجموعة للخبراء الحكوميين؛ لدراسة تأثير تطوُّرات تكنولوجيا المعلومات والاتصالات على الأمن القومي والشئون العسكرية للدول، وقد تابع الفريق اجتماعاته سنويًا، وخلال عام ٢٠١٠ قدَّم الفريق تقريرًا، سلَّط من خلاله الضوء على التهديدات التي تُثيرها العمليات السيبرانية للسِّلْم والاستقرار الدوليين، وأنَّ الافتقار إلى توجيه دولي بشأنها قد يتسبَّب فى أضرار جسيمة، وقد أورد التقرير التوصيات التالية:

١- مواصلة الحوار بين الدول لمناقشة المعايير المتعلِّقة باستخدام تكنولوجيا المعلومات والاتصالات للحدِّ من مخاطرها، وحماية البِنَى التحتية الإلكترونية للدول.

٢- السعي لتحقيق تدابير بناء الثقة فى مجال الحدِّ من مخاطر استخدام الدول لتكنولوجيا المعلومات والاتصالات، بما فى ذلك تبادل الآراء الوطنية بشأن استخدامها.

٣- تبادل المعلومات بشأن التشريعات الوطنية والمعلومات الوطنية، وإستراتيجيات وتقنيات وسياسات أمن الاتصال وأفضل الممارسات.

٤- تحديد تدابير لدعم بناء القدرات فى أقل البلدان نموًا.

وقدَّمت مجموعة (GGE) تقريرًا عام ٢٠١٥، تضمَّن (١١) توصية، منها: ضرورة تطبيق القانون الدولي على الفضاء السيبراني، وعدم استهداف البِنَى التحتية الإلكترونية للدول، أو دعم الأنشطة ذات الصلة، واعتبار أيِّ دولة مسئولة عن الهجمات السيبرانية التي تنطلق من أراضيها، وأشار التقرير صراحة إلى أنَّ التوصيات المقترَحة كلَّها طواعية وغير مُلزمة، ولكنَّها خطوة مهمَّة بشأن تطوير إطار معياري متفق عليه [١].

(١) د. محمد عادل محمد عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسُّس وقت السِّلْم، المرجع السابق، ص: ٦٢.

المطلب الثاني
الاتفاقيات الدولية فى مجال مكافحة الهجوم السيبراني

تُعدُّ الاتفاقيات والمعاهدات الدولية من أهمِّ 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 المتعلّقة بتكنولوجيا المعلومات، ونُبيِّنها فيم يلي:

الفرع الأوَّل
معاهدة بودابست لمكافحة جرائم الإنترنت

تُعدُّ معاهدة بودابست لمكافحة جرائم الإنترنت أُولى المعاهدات المتعلِّقة بتلك الجرائم، والتي تمت فى العاصمة المجرية بودابست فى ٢٠٠١/١١/٢٣، والتي تُبرز التعاون والتضامن الدولي فى محاربة الجرائم السيبرانية، ويُعدُّ التوقيع على تلك المعاهدة الدولية الخطوة الأولى فى مجال تكوين التضامن الدولي ضدَّ تلك الجرائم التي تتمُّ عبر شبكة الإنترنت والاستخدام السيء لها[1].

وقد وقَّعَت على تلك المعاهدة ٢٦ دولة أوروبية بالإضافة إلى كندا واليابان، وجنوب أفريقيا والولايات المتحدة الأمريكية، وتُوفِّر المعاهدة أُسُس الأمن العام، وتتضمَّن ٤٨ مادة على أربعة فصول كالآتي[2]:

الفصل الأوَّل: تعريفات خاصة ببعض التعريفات الفنية.

الفصل الثاني: يتضمَّن الإجراءات اللازم اتخاذها على المستوى المحلِّي لكلِّ دولة، وتنقسم إلى قسمين:

القسم الأوَّل: يتعلَّق بالنصوص الجنائية الموضوعية على النحو التالي:

---

(١) د. منير محمد الجهيني، د. ممدوح محمد الجهيني، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر العربي، الإسكندرية، ط ٢٠٠٤، ص: ٩٦.

(2) راد (2001 تسبادوب ةيقافتا عوض لماع) ةيتامولعملا ةمئارجلا ةيئارجلاوا ةيعوضوملا بناوجلا ىدمحأ ملالا دبع لياهلا .د
.30 :ص ،2001 ط ،ةيبرعلا ةضهنلا

١- بشأن الجرائم ضدَّ الخصوصية وسلامة وتواجد معلومات الحاسب ونُظُم الحاسب، ويشمل وصفًا لأنواع متعدِّدة من الجرائم.

٢- الجرائم المتصلة بالحاسب شاملة استخدام الكمبيوتر فى التزوير والأفعال الاحتيالية.

٣- الجرائم المتعلِّقة بالمحتوى والمضمون.

٤- الجرائم المتصلة بالتعدِّي على حقوق المؤلِّف.

القسم الثاني: القانون الإجرائي فيما يتصل بالإجراءات الجنائية شاملة الحفاظ على المعلومات المخزَّنة والأوامر الخاصة بتسليم الأدلَّة، وتتضمَّن كذلك تفتيش وضبط بيانات الحاسب المخزَّنة.

الفصل الثالث: مسائل التعاون الدولي وتسليم الجُناة والمساندة المشتركة والتعاون فى التحريات وجمع بيانات المرور والحركة الخاصة بالبيانات.

الفصل الرابع: يتعلَّق بالانضمام والانسحاب من تعديل المعاهدة وفضِّ المنازعات والتشاور بين الأعضاء.

وعلى الرغم من أنَّ هذه الاتفاقية أوروبية المنشأ، إلا أنَّها مفتوحة للدول الأخرى لطلب الانضمام إليها لتعمَّ الفائدة. وتتضمَّن الاتفاقية التعاون والعمل المشترك ما بين الدول الأعضاء وأعضاء القطاعات وأصحاب المصلحة ذوي الصلة، وهما ضروريان لبناء ثقافة للأمن السيبراني وفي الحفاظ عليها، وسُبُل مكافحة الجرائم السيبرانية، إذ تُقرِّر[1]:

١- مواصلة اعتبار الأمن السيبراني فى صدارة أنشطة الاتحاد ذات الأولوية، والاستمرار فى إطار مجالات اختصاصاته الرئيسية، بدراسة مسألة توفير الأمن

(١) وتعود أهمية توقيع هذه الاتفاقية إلى رغبة المجتمع الدولي لايجاد صيغة دولية لمكافحة ومواجهة هذا الإجرام المستحدَث، وعلى ذلك بُذلت الجهود الدولية لتحقيق هذه الرغبة، فبتاريخ ٢٠ نوفمبر تقدَّمت اللجنة الأوروبية لمشكلات الجريمة CDBC ولجنة الخبراء في حقل جرائم التقنية CYBERCRIME- PC-CU -)) بمشروع اتفاقية جرائم الكمبيوتر، وخضعت مواد الاتفاقية المقترحة للمناقشة وتبادل الآراء خلال الفترة من إصدار مشروعها الأوَّل وحتى إعداد مسودتها النهائية التي أُقرَّت لاحقًا في بودابست ٢٠٠١، وتُعرَف باتفاقية بودابست ٢٠٠١ (اتفاقية الجرائم السيبرانية - سايبر كرايم)، ولا شكَّ في أنَّ الاتفاقية قد بُذل فيها جهد واسع ومميز يُذكَر للاتحاد الأوروبي ومجلس أوروبا ولا سيَّما في المسائل المتعلِّقة بجرائم الكمبيوتر وأغراضها منذ أواخر القرن الواحد والعشرين. للمزيد انظر: د. هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية (معقبا عليها) ، دار النهضة العربية ، ط٢ ، ٢٠١١ ، ص: ١٣٠.

وبناء الثقة فى استعمال الاتصالات/ تكنولوجيا المعلومات والاتصالات؛ من خلال إذكاء الوعي، وتحديد أفضل الممارسات، وتطوير مواد التدريس المناسبة؛ لتعزيز ثقافة الأمن الإلكتروني.

٢- تعزيز العمل والتعاون وتبادل المعلومات مع جميع المنظَّمات الدولية والإقليمية ذات الصلة فيما يتعلَّق بالمبادرات المتصلة بالأمن السيبراني فى مجالات اختصاصاتها، مع مُراعاة احتياجات مساعدة البلدان النامية.

٣- تعيين نظام سريع وفعَّال للتعاون الدولي، والحفاظ بشكل سريع على البيانات المخزَّنة على أجهزة الكمبيوتر وحفظها والإفصاح الجزئي عن حركة هذه البيانات المخزَّنة على الكمبيوتر(١).

هذا وقد تناولت المعاهدة الجرائم التي تُعتبَر من أكثر الجرائم شيوعًا على مستوى العالم مثل الإرهاب السيبراني وعمليات تزوير بطاقات الائتمان ودعارة الأطفال.كما حدَّدت المعاهدة الطرُق الواجب اتباعها فى التحقيق فى جرائم الإنترنت، وتعهَّدت الدول الموقِّعة بالتعاون من أجل محاربتها، كما حاولت المعاهدة إقامة التوازُن بين الاقتراحات التي تقدَّمت بها أجهزة الشرطة، وما عبَّرت عنه المنظَّمات المدافِعة عن حقوق الإنسان ومُزوِّدي خدمات الإنترنت من قلق، حيث تخشى منظَّمات حقوق الإنسان من أن تحدَّ المعاهدة من حرية الأفراد، وأن تُؤدِّي الرقابة إلى انتهاك حقوق مُستخدِمي الإنترنت (٢).

وفي عام ٢٠١٦ أصدرت لجنة اتفاقية الجرائم السيبرانية مذكرة توجيهية تتعلَّق بجوانب الإرهاب السيبراني بموجب اتفاقية بودابست، تُعلن فيها أنَّ « الجرائم الموضوعية فى الاتفاقية قد تكون أيضًا أعمالًا إرهابية على النحو المحدَّد فى القانون المعمول به « . وجاءت هذه المذكرة الإضافية بموجب الاتفاقية فى الوقت المناسب؛ لتُسلِّط المذكرة الضوء على أنَّ هذه الاتفاقية ليست معاهدة مختصَّة بالإرهاب، إلا إنَّه يمكن القول: أنَّ الجرائم الموضوعية فى الاتفاقية يمكن أن تُنفَّذ على أنَّها أعمالٌ إرهابية، لتسهيل الإرهاب ولدعم الإرهاب، ومن ذلك الجانب التمويلي، أو الأعمال التحضيرية(٣).

(١) انظر:
https://www.itu.int/ar/mediacentre/

(٢) د. هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية للجرائم المعلوماتية، المرجع السابق، ص: ٣٠ وما بعدها.

(٣) د. منير محمد الجهيني، د. ممدوح محمد الجهيني، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، المرجع السابق، ص: ٩٦.

الفرع الثاني

توصيات المجلس الأوروبي [١]

أدَّى التطوُّر السريع فى مجال تكنولوجيا الكمبيوتر والإنترنت وشعور الدول الأوروبية بأهَمِّيَّة إعادة النظر فى الإجراءات الجنائية فى هذا المجال إلى إصدار المجلس الأوروبي التوصية رقم ٩٥/١٣ فى ١٩٩٥/٩/١١ فى شأن مشاكل الإجراءات الجنائية المتعلِّقة بتكنولوجيا المعلومات، وحثِّ الدول الأعضاء بمراجعة قوانين الإجراءات الجنائية الوطنية؛ لكي تتلاءم مع التطوُّر فى هذا المجال، ومن أهمِّ ما ورد بتوصية المجلس الأوروبي ما يلي:

١- أن تُوضِّح القوانين إجراءات تفتيش أجهزة الكمبيوتر وضبط المعلومات التي تحويها ومُراقبة المعلومات أثناء انتقالها.

٢- أن تسمح الإجراءات الجنائية الوطنية لجهات التفتيش بضبط برامج الكمبيوتر والمعلومات الموجودة بالأجهزة وفقًا لذات الشروط الخاصة بإجراءات التفتيش العادية، ويتعيَّن إخطار الشخص القائم على الأجهزة بأنَّ النظام كان محلًا للتفتيش مع بيان المعلومات التي تَمَّ ضبطها، ويُسمح باتخاذ إجراءات الطعن العادية فى قرارات الضبط والتفتيش.

٣- أن يُسمح أثناء عملية التفتيش للجهات القائمة بالتنفيذ ومع احترام الضمانات المقرَّرة بمدِّ التفتيش إلى أنظمة الكمبيوتر الأخرى فى دائرة اختصاصهم، والتي تكون متصلة بالنظام محلِّ التفتيش، وضبط ما بها من معلومات، بشرط أن يكون هذا الإجراء ضروريًا.

٤- أن يُوضِّح قانون الإجراءات الجنائية أنَّ الإجراءات الخاصَّة بالوثائق التقليدية تنطبق فى شأن المعلومات الموجود بأجهزة الكمبيوتر.

٥- تُطبَّق إجراءات المراقبة والتسجيل فى مجال التحقيق الجنائي فى حالة الضرورة فى مجال تكنولوجيا المعلومات، ويتعيَّن توفير السرية والاحترام للمعلومات التي يَفرض القانون لها حماية خاصة.

(١) د. مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، ط٢٠٠٠، ص: ٨٠ وما بعدها.

٦- يجب إلزام العاملين بالمؤسَّسات الحكومية والخاصة التي تُوفِّر خدمات الاتصال بالتعاون مع سُلطة التحقيق لإجراء المراقبة والتسجيل.

٧- يتعيَّن تعديل القوانين الإجرائية بإصدار أوامر لِمَن يحوز معلومات، سواء أكانت برامج أم قواعد أم بيانات، تتعلَّق بأجهزة الكمبيوتر بتسليمها للكشف عن الحقيقة.

٨- يتعيَّن إعطاء سُلطات التحقيق سُلطة توجيه أوامر لِمَن يكون لديه معلومات خاصَّة للدخول على نظام من أنظمة المعلومات أو الدخول على ما يحويه من معلومات باتخاذ اللازم؛ للسماح لرجال التحقيق بالاطلاع عليها. وأن تُخوَّل سُلطات التحقيق بإصدار أوامر مماثلة لأيِّ شخص لديه معلومات عن طريق التشغيل والمحافظة على المعلومات.

٩- يجب تطوير وتوحيد أنظمة التعامل مع الأدلَّة الإلكترونية، وحتى يتمَّ الاعتراف بها بين الدول المختلفة، ويتعيَّن أيضًا تطبيق النصوص الإجرائية الخاصة بالأدلَّة التقليدية على الأدلَّة الإلكترونية.

١٠- يجب تشكيل وحدات خاصة لمكافحة جرائم الكمبيوتر وإعداد برامج خاصَّة لتأهيل العاملين فى مجال العدالة الجنائية لتطوير معلوماتهم فى مجال تكنولوجيا المعلومات.

١١- قد تتطلَّب إجراءات التحقيق مدَّ الإجراءات إلى أنظمة كمبيوتر أخرى قد تكون موجودة خارج الدولة، وتفترض التدخُّل السريع، وحتى لا يُمثِّل هذا الأمر اعتداءً على سيادة الدولة والقانون الدولي، يجب وضع قاعدة قانونية صريحة تسمح بمثل هذا الإجراء، ولذلك كانت الحاجة إلى عمل اتفاقيات تُنظِّم وقت وكيفية اتخاذ مثل هذه الإجراءات.

١٢- يجب أن تكون هناك إجراءات سريعة ومُتناسبة ونظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهة أجنبية لجمع أدلة مُعيَّنة، ويتعيَّن عندئذ أن تسمح السُّلطة الأخيرة بإجراءات التفتيش والضبط. ويتعيَّن كذلك السماح لهذه السُّلطة بإجراء تسجيلات للتعاملات الجارية، وتحديد مصدرها، ولذلك يتعيَّن تطوير اتفاقيات التعاون الدولي القائمة.

المطلب الثالث

جهود بعض المنظَّمات العالمية المتخصِّصة والتحالُفات الدولية فى مكافحة الإرهاب السيبراني

كان للمنظَّمات العلمية المتخصِّصة دورٌ مهمٌّ بشأن التعامُل مع العمليات السيبرانية بأنواعها المختلفة، وتحقيق قدر من الأمن فى مجال المعاملات الإلكترونية، ومن أبرز هذه المنظمات: الاتحاد الدولي للاتصالات، والمنظمة العالمية للملكية الفكرية، ومنظمة حلف شمال الأطلسي، ونتعرَّض لجهود كلٍّ مُنظَّمة منها من خلال الفروع التالية:

الفرع الأوَّل

الاتحاد الدولي للاتصالات

نشأ الاتحاد الدولي للاتصالات بمقتضى اتفاقية باريس عام ١٨٦٥ تحت اسم (اتحاد التلغراف الدولي)، ثم عُدِّل الاسم ليُصبح (الاتحاد الدولي للاتصالات السلكية واللاسلكية)، وفي عام ١٩٤٧ انضمَّ الاتحاد إلى هيئة الأمم المتحدة، وصار إحدى الوكالات المتخصِّصة فى عمل الاتصالات المنطوية تحت مظلَّة الأمم المتحدة فأصبح بمثابة مُلتقى دولي رئيسي لهذه الأنشطة. ويتكوَّن هذا الاتحاد من ١٩٢ دولة و ٧٠٠ شركة من القطاع الخاص والمؤسَّسات الأكاديمية، ويُعتبر منبرًا «إستراتيجيًا» للتعاون بين أعضائه باعتباره وكالة متخصِّصة داخل الأمم المتحدة، حيث يعمل الاتحاد على مساعدة الحكومات فى الإنفاق على مبادئ مشتركة تُفيد الحكومات أو الصناعات التي تعتمد على تكنولوجيا المعلومات والبنية التحتية للاتصالات.

ومن المهام التي يَضطلع بها هذا الاتجاه 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 المتخصِّصة فى الاتصالات اللاسلكية وجمع المعلومات ونشرها؛ من أجل بناء قدرات الدول الأعضاء -ولاسيَّما البلدان النامية- لتنسيق الإستراتيجيات الوطنية وحماية البنية التحتية للشبكات ضدَّ المخاطر من خلال التوعية، والتقييم الذاتي، وبناء القدرات، وتوسيع نطاق المراقبة، والإنذار،

وقدرات الاستجابة للحوادث للدول والجهات المعنية، ويعمل الاتحاد بصورة وثيقة مع المنظَّمات الأخرى المعنية على (وضع المعايير المتعلِّقة بالأمن المعلوماتي؛ إذ يقوم الاتحاد بالاشتراك مع الوكالة الأوروبية لأمن الشبكات والمعلومات بنشر خريطة الطريق المتعلِّقة بمعايير الأمن فى مجال تكنولوجيا المعلومات والاتصالات، كما تعاون الاتحاد الدولي مع مجلس أوروبا لإنجاز الاتفاقية الأوروبية حول الجريمة الإلكترونية؛ من أجل الاستعانة بها فى عملية وضع إطار قانوني دولي[١].

وبغية معالجة مسألة الأمن السيبراني المتنامية، قام الاتحاد الدولي للاتصالات بإنشاء فريق متخصِّص معني بالشبكات الذكية؛ من أجل جمع وتوثيق المعلومات والمفاهيم التي ستكون مُفيدة من أجل إعداد توصيات لدعم تلك الشبكات من منظور الاتصالات[٢]، وكان أحد الأدوار الأساسية التي أُنيطت بالاتحاد الدولي للاتصالات فى أعقاب القمَّة العالمية لمجتمع المعلومات ومؤتمر المندوبين المفوضين لعام ٢٠٠٦ يتمثَّل فى بناء الثقة والأمن فى استعمال تكنولوجيا المعلومات والاتصالات؛ فقد قام رؤساء الدول والحكومات وغيرهم من قادة العالم المشاركين فى القمَّة العالمية لمجتمع المعلومات، وكذلك الدول الأعضاء فى الاتحاد، بتكليف الاتحاد باتخاذ خطوات ملموسة للحدِّ من التهديدات وانعدام الأمن فيما يتَّصل بمجتمع المعلومات، ولتحقيق هذه الولاية أطلق الأمين العام للاتحاد برنامج الأمن السيبراني العالمي فى عام ٢٠٠٧؛ ليكون إطارًا للتعاون الدولي[٣].

وهكذا أعلن الأمين العام للاتحاد الدولي للاتصالات عام ٢٠٠٧ إطلاق مبادرة أجندة شاملة بشأن الأمن السيبراني، تتضمَّن التوصُّل إلى إطار أو بروتوكول لتنسيق جهود مكافحة الجرائم السيبرانية، وبما يشمل تدابير قانونية، وتقنية، وإجرائية، وتنظيمية، وتعاون دولي[٤].

---

(١) د. خالد محمد نور عبد الحميد الطباخ، المواجهة القانونية للإرهاب الإلكتروني الدولي، مجلة الدراسات القانونية والاقتصادية، جامعة مدينة السادات- كلية الحقوق، مج ٣، ع١، ٢٠١٧، ص: ٣٣.

(٢) الفرق المتخصِّصة: هي أداة من أدوات الاتحاد التي تعزِّز برنامج عمل لجان الدراسات من خلال توفير بيئة عمل بديلة لتطوير المواصفات بسرعة في مجالات عملها، مما يجعلها مثالية للتكنولوجيات المتغيِّرة والمتطوِّرة بسرعة مثل الشبكات الذكية، ويتألَّف الفريق المتخصِّص بالشبكة الذكية من ممثلين من مختلف الدول الأعضاء، وسيقوم بالتعاون مع مجتمعات الشبكة الذكية في جميع أنحاء العالم (مثل: معاهد البحوث والمنديات والأوساط الأكاديمية).

(٣) د. أميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسُبُل مواجهتها في القانون الدولي العام، المرجع السابق، ص: ٤٩٣.

(٤) د. محمد عادل محمد عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسُّس وقت السِّلم، «دراسة على ضوء دليل «تالين» بشأن القانون الدولي المطبَّق على العمليات السيبرانية ٢٠١٣-٢٠١٧»، ٢٠٢٠م، ص: ٣٠٨.

ويقترح الأمين العام للاتحاد الدولي للاتصالات خمسة مبادئ توجيهية لإحلال السلام وحفظه فى العالم السيبراني الناشئ إدراكًا منه للخطر المتنامي للهجوم السيبراني، وقد أُعِدَّت لوائح الاتصالات الدولية كإطار تنظيمي لمعالجة القضايا الناشئة والتحديات التي تُصاحب عالم الاتصالات الجديد الذي تجسَّد فى أواخر ثمانينات القرن الماضي، وقد صِيغت هذه اللوائح لتعزيز الكفاءة والتنمية الدوليين، فضلًا عن أنَّها تُبرز تركيز الاتحاد على حماية الحقِّ فى الاتصال وفي الوقت نفسه إلحاق الضرر بالمرافق(١).

وعلى غرار ذلك، تتضمَّن المبادئ الخمسة التي اقترحها الأمين العام للاتحاد الدولي للاتصالات فيما يتعلَّق بالسلام السيبراني هذه القيم الجوهرية مع تحديد إجراءات والتزامات محدَّدة من شأنها أن تضمن السلام والاستقرار فى الفضاء السيبراني، وتنصُّ هذه المبادئ على ما يلي(٢):

١- أن تلتزم كلُّ حكومة بإتاحة نفاذ شعبها على الاتصالات.

٢- أن تلتزم كلُّ حكومة بتأمين الحماية لشعبها فى الفضاء السيبراني.

٣- أن يلتزم كلُّ بلد بعدم إيواء الإرهابيين/ المجرمين فى أراضيه.

٤- أن يلتزم كلُّ بلد بألَّا يكون الطرف الذي يبدأ شنَّ هجوم سيبراني على غيره من البلدان.

٥- أن يلتزم كلُّ بلد بالتعاون مع غيره ضمن إطار دولي للتعاون لضمان السلام فى الفضاء السيبراني.

وفي مسعى أكثر شمولًا، تَمَّ فى المؤتمر الإقليمي حول الأمن السيبراني بالتعاون مع الاتحاد الدولي للاتصالات فى قطر عام ٢٠٠٨، دعوة جميع الدول لوضع وتنفيذ إطار وطني للأمن السيبراني وحماية البنية التحتية الحرجة للمعلومات، والتي تُعدُّ بمثابة خطوة أُولى فى سبيل التصدِّي للتحديات التي تُواجهها جرَّاء اتصالها بتكنولوجيا المعلومات والاتصالات(٣)؛ وفي نفس العام وقَّع الاتحاد الدولي

(١) د. أميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسُبُل مواجهتها في القانون الدولي العام، المرجع السابق، ص: ٤٩٤.
(٢) قرارات المؤتمر العالمي لتنمية الاتصالات لعام ٢٠١٧ (٧wtdc١) المرفوعة إلى عناية مؤتمر المندوبين المفوضين، مؤتمر المندوبين المفوضين (pp- ١٨) دبي، ٢٩ أكتوبر - ١٦ نوفمبر ٢٠١٨، الاتحاد الدولي للاتصالات.
(٣) د. خالد محمد نور عبد الحميد الطباخ، المواجهة القانونية للإرهاب الإلكتروني الدولي، المرجع السابق، ص: ٣٤.

للاتصالات والشراكة الدولية المتعدِّدة الأطراف لمكافحة التهديدات السيبرانية (إمباكت) (IMPACT) مذكرة تفاهُم رسميًا، بعدها أصبح مقرُّ شراكة إمباكت فى سايبر جايا بماليزيا، الذي يضمُّ أحدث ما توصَّلت إليه التكنولوجيا، المقرَّ الفعلي للبرنامج[1].

(١) إمباكت هي مبادرة دولية مشتركة بين القطاعين العام والخاص لتعزيز قدرة المجتمع الدولية على منع الهجمات السيبرانية والدفاع ضدها والتصدي لها. ويُوفِّر هذا التعاون للدول الأعضاء في الاتحاد البالغ عددها ١٩٢ دولة وغيرها من الجهات: الخبرات الفنية والتسهيلات والموارد اللازمة؛ لتعزيز قدرات المجتمع العالمي تعزيزًا فعَّالًا، وزيادة القدرة على منع الهجمات السيبرانية، والدفاع ضدها والتصدّي 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 وسُبُل مواجهتها في القانون الدولي العام، المرجع السابق، ص: ٤٩٦.

الفرع الثاني
المنظمة العالمية للملكية الفكرية

إبَّان عام ١٩٦٧ تَمَّ التوقيع فى ستوكهولم بالسويد على اتفاقية المنظَّمة العالمية للمِلكية الفكرية، وأصبحت هذه المنظَّمة إحدى الوكالات المتخصِّصة التابعة للأمم المتحدة اعتبارًا من السابع عشر من ديسمبر عام ١٩٧٤، والتي من أهدافها حماية الملكية الفكرية فى شتَّى أنحاء العالم عن طريق التعاون بين الدول الأعضاء والمنظَّمات الدولية الأخرى، وتعمل المنظمة على مُتابعة تنفيذ الاتفاقيات المتعلِّقة بالتصميمات الصناعية وتصنيف السلع التجارية وحماية الأعمال الإدارية والفنية وحقوق الإنتاج. كما تُشجِّع 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 أوجُه القصور فى مجال التوثيق العلمي ونقل التقنية الحديثة[١].

وبالرجوع إلى اتفاقية إنشاء هذه المنظَّمة تتَّضِح غايات هذه المنظمة فى دعم الملكية الفكرية فى جميع أنحاء العالم بجميع صورها (المصنَّفات الأدبية والفنية والعلمية والاختراعات)، ومع تزايُد الحاجة العالمية لحماية البرامج شكَّلت هذه المنظمة مجموعة عمل تضمُّ 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 حقِّ المؤلف. وقد جاءت منظمة التجارة العالمية عام ١٩٩٤ لتُؤيِّد هذا التوجه، وتستكمل طريقها من خلال إبرام اتفاقية تريبس (TRIPS) المتعلِّقة بمواصفات التجارة المرتبطة بحقوق الملكية الفكرية وما تفرضه من التزامات على الدول الأعضاء لفرض إجراءات تنفيذية وعقوبات جنائية لمواجهة أيِّ اعتداء على حقِّ المؤلف، وخاصة القراصنة[٢].

(١) د. طارق عزت رخا، المنظمات الدولية المعاصرة، دار النهضة العربية، القاهرة، ٢٠٠٦، ص: ٢١٤.
(٢) د. عبد الصبور عبد القوي، الجريمة الإلكترونية، دار العلوم للنشر والتوزيع، القاهرة، ٢٠٠٨، ص: ١٥٩-١٦٣.

الفرع الثالث

منظمة حلف شمال الأطلسي

دفع عجز حلف الناتو فى مُواجهة الهجمات السيبرانية على إستونيا عام ٢٠٠٧ وجورجيا عام ٢٠٠٨ إلى تكوين وحدة للدفاع السيبراني، مقرُّها تالين عاصمة إستونيا، وعمل على تطوير المفهوم الإستراتيجي للحلف؛ بحيث أصبح الفضاء السيبراني منطقة لعمليات الحلف، وأنَّ عليه أن يُطوِّر قُدراته الدفاعية السيبرانية بما يشمل مُساندة ودعم حُلفائه الذين يتعرَّضون لهجمات سيبرانية، وأنَّه وفقًا لذلك فإنَّ أيَّ هجوم يتمُّ على أوروبا أو أمريكا الشمالية يُعتبر هجومًا ضدَّ الجميع(١).

ولذا نفَّذت الناتو السياسة الخاصة بها فى مجال الدفاع السيبراني فى ٢٠٠٨؛ من أجل حماية مواردها التكنولوجية وتلك الخاصة بالدول الأعضاء(٢)، وكجزء من هذه السياسة، أنشأ الحلف هيئة معيَّنة بإدارة الدفاع السيبراني، وفريقًا للاستجابة للحوادث الحاسوبية، يكفل إرسال فِرَق الدعم السريع إلى فُرادى البلدان الأعضاء، ومركزًا للتميُّز من أجل الدفاع السيبراني التعاوني(٣)، ويضمُّ هذا المركز الذي يُوجد مقرُّه فى إستونيا خبراء يضطلعون بالبحث والتدريب فى مجال الأمن السيبراني. وتضمُّ البلدان التي ترعى هذا المركز: إستونيا ولاتفيا وليتوانيا وألمانيا وإيطاليا والجمهورية السلوفاكية وإسبانيا(٤). ووقَّعت الناتو مذكرة تفاهُم بشأن الأمن السـيبراني مع إستونيا والولايات المتحدة الأمريكية والمملكة المتحدة وتركيا وسلوفاكيا (٥).

(١) تقرير التوازن العسكري ٢٠١١ الذي يصدر سنويًا عن المعهد الدولي للدراسات الإستراتيجية هو تقرير مستقل وشامل يعرض للقدرات العسكرية العالمية واقتصاديات الدفاع لنحو ١٧٠ دولة حول العالم. يُشير للتطور العسكري العالمي والقضايا الأمنية الراهنة.

(٢) الدفاع ضدَّ الهجمات السيبرانية « ، الناتو:

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

(٣) انظر :

https://www.nato.int/cps/en/natolive/official_texts

(٤) مركز التميُّز للدفاع السيبراني التعاوني:

WWW.ccdcoe.org

(٥) أبرمت الناتو وإستونيا اتفاقًا بشأن الدفاع السيبراني nato-news , ٢٣ أبريل ٢٠١٠:

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

المبحث الثاني

المجهودات الفقهية لمواجهة المخاطر السيبرانية

فى إطار غياب توجيه رسميٍّ من الأمم المتحدة، ظهرت اجتهادات فِقهية عديدة لمعالجة مسألة الهجمات السيبرانية، والاستجابة الدولية الأهم والأبرز لمعالجة هذه المسألة جاءت فيما يُسمَّى دليل «تالين» للقانون الدولي المنطبق على الحرب الإلكترونية، والذي قام بإعداده مجموعة من أبرز فُقهاء القانون الدولي؛ هذا بالإضافة إلى المبادئ الواردة فى إعلان ريتشي بشأن مبادئ الاستقرار السيبراني والسلام السيبراني والذي أعدَّه فريق الرصد الدائم المعني بأمن المعلومات التابع للاتحاد العالمي للعلماء (WFS)، وهو ما نتناوله من خلال مطلبين على النحو التالي:

المطلب الأوَّل: دليل تالين والهجمات السيبرانية.

المطلب الثاني: إعلان إيريتشي بشأن مبادئ الاستقرار السيبراني والسلام السيبراني (الصادر عن الاتحاد العالمي للعلماء).

المطلب الأوَّل

دليل تالين والهجمات السيبرانية

تبنَّى (NATO) إعداد دليل «تالين»، بشأن القانون الدولي المطبَّق على الحرب السيبرانية، بإصداريه لعامي ٢٠١٣، ٢٠١٧، وهو توجيه غير مُلزِم بشأن القواعد الدولية التي تحكم العمليات السيبرانية، حيث استضاف المركز التعاوني للدفاع السيبراني، التابع للحلف بمقرّه فى مدينة «تالين» عاصمة «إستونيا»، وصياغة هذا الدليل فى الفترة من عام ٢٠٠٩ وحتى ٢٠١٧، بجهود فريق خبراء قانونيين دوليين (IGE) برئاسة البروفيسور «Michael N.Schmitt»[(١)].

وقد عرَّف خُبراء تالين العمليات السيبرانية على أنَّها: «تلك التي تتضمَّن استخدام القوَّة أو التهديد بها ضدَّ سلامة الأراضي أو الاستقلال السياسي لأيِّ دولة، أو على وجه آخر لا يتفق ومقاصد الأمم المتحدة «[(٢)]؛ وذكروا أنَّ العملية السيبرانية

(١) د. محمد عادل محمد عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسُّس وقت السِّلم، المرجع السابق، ص: ٦٩.

(٢) القاعدة (١٠) من دليل تالين والمعنونة ب حظر التهديد أو استخدام القوة «.

Tallinn Mnnual on the International Law Applicable to Cyber Warfare (Michael N. Schmitt ed., 2013) , pp.106-107.

تُشكِّل استخدامًا للقوَّة عندما يكون حجمها وأثرها قابلًا للمقارنة مع العمليات غير السيبرانية التي تصل لمستوى استخدام القوَّة[١].

وقد ظهر الإصدار الأوَّل من الدليل عام ٢٠١٣، وتضمَّن (٩٥) قاعدة لسلوك الدول فى سياق الحرب السيبرانية، مع تعليقات على كلِّ قاعدة، وفي عام ٢٠١٧ ظهر الإصدار الثاني، وتضمَّن (١٥٤) قاعدة، تُشكِّل مستوى أكثر عُمقًا بشأن معالجة العمليات السيبرانية، مع تعليقات على كلِّ قاعدة، تُبيِّن النقاش الذي دار بشأنها، وأنَّ أيَّ وجهة نظر قُبلت بالأغلبية، وموقف الأقلية إن وُجد، وكذلك حالات الإجماع. وانتهى الدليل إلى أنَّ القواعد الدولية السارية فاعلة إلى حدٍّ كبير، ويمكن تطبيقها على العمليات السيبرانية، وتعرَّض الدليل لبعض الإشكاليات القانونية فى المجال السيبراني، كسيادة الدول، وقواعد ممارسة الاختصاص، وقانون مسئولية الدول، إضافة إلى قانون حقوق الإنسان، وقانون البحار، والقانون الدبلوماسي والقنصلي[٢].

ووفقًا لدليل تالين فإنَّ العمليات السيبرانية تُعتبر استخدامًا للقوَّة عندما يكون مستواها وتأثيرها متقاربين مع العمليات غير السيبرانية، وذلك اعتمادًا على معيار النطاق والأثر فى تحديد الدرجة التي يجب أن يصل إليها الهجوم السيبراني كاستخدام للقوَّة أو هجوم مسلَّح، وعليه يمكن اعتبار هجوم سيراني كهجوم مسلَّح إذا أحدث ضررًا، أو يصل إلى درجة الشدَّة، والمقصود بذلك أن يُحدث أضرارًا مادية جسيمة، واستند خبراء تالين فى اعتماد هذا الاختبار على رأي محكمة العدل الدولية فى قضية « نيكاراجوا » ، على أساس أنَّه الأنسب لتحديد الدرجة المناسبة للأعمال التي تصل إلى حدِّ استخدام القوَّة والهجمات المسلَّحة، وبالقياس على الهجمات السيبرانية، اتَّفق خبراء دليل تالين فى الإصدار الثاني، على أنَّ قيام دولة بتزويد قوَّات أو أفراد بأجهزة وتدريبهم لشنِّ هجمات سيبرانية ضدَّ دولة أخرى يُعدُّ ذلك استخدامًا غير مشروع للقوة[٣].

وطُبِّق هذا المعنى بصورة واضحة فى عملية استخدام الهجمات السيبرانية فى الحرب بين جورجيا وروسيا فى أغسطس ٢٠٠٨، وفي الهجمة السيبرانية العالمية - فيروس الفدية - التي طالت أكثر من ٦٠ دولة على مستوى العالم فى ٢٧ يونيو ٢٠١٧-

(١) القاعدة (١١) من دليل تالين والمعنونة بـ « تعريف استخدام القوة » .

(٢) د. محمد عادل محمد عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسُس وقت السلم، المرجع السابق، ص: ٧٠.

(٣) انظر:

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.

منهم بريطانيا ومصر وروسيا وأوكرانيا وألمانيا والمكسيك وإسبانيا، إلى ظهور الفضاء السيبراني على الساحة الدولية على نحو مباشر وعلني فى الصراع الدولي، وكأداة ووسيلة فى الصراع المسلَّح، لذلك ثار الجدل حول مدى اعتبار تلك الهجمات عملاً من أعمال الحرب، وتُقارب الهجمات السيبرانية الهجمات التقليدية فى النتائج مع اختلاف الوسائل وإستراتيجيات التنفيذ، مما أدَّى إلى خلق حرب مفتوحة يمكن أن تكون هناك صعوبة فى تحديد أطرافها، لذا تسعى الدول إلى تطوير أساليب جديدة فى الحروب المستقبلية. وقد وضعت اللجنة مجموعة من الصفات التي يجب أن تتَّسِم بها الهجمات السيبرانية؛ حتى ترقى إلى درجة الهجوم المسلَّح، وبالتالي تُعطي الدولة المعتدَى عليها حقَّ الدفاع الشرعي وتفعيل المادة ٥١ من الميثاق:

حيث اعتبرت اللجنة أنَّ أهمَّ المعايير التي يجب الاستناد إليها فى تحديد المستوى المطلوب لوصول العمليات السيبرانية إلى درجة الهجوم المسلَّح يتمثَّل فى جسامة هذا التصرُّف أو حدَّته، ومدى تأثيره على الدولة المعتدَى عليها، وأن يكون هناك ضررٌ ماديٌّ حالٌّ على الأفراد والممتلكات فى الدولة المعتدَى عليها بهجوم سيبراني، وفي سبيل ذلك قامت اللجنة بالمقارنة بين أثر الهجمات العسكرية التقليدية والهجمات السيبرانية استنادًا إلى قياس نتائج الأخيرة، وفيما إذا كانت مُنتجة لأضرار مماثلة للهجمات العسكرية التقليدية أم لا؛ فالهجمات السيبرانية يمكن لها أن تُنتج مثل هذا الضرر المماثِل للهجمات العسكرية التقليدية أو يفوقه كما لو حدث اعتداء سيبرانيٌّ على شبكات الكمبيوتر الخاصة بمطار إحدى الدول؛ مما أدَّى إلى مقتل الآلاف بسبب الخلل الذي أحدثته الهجمة، وأدَّى إلى تصادم الطائرات هبوطًا وصعودًا، ففي مثل هذه الحالة تُعتبر العملية السيبرانية هجومًا عسكريًا، أمَّا تلك التصرُّفات التي لا تُلحق مثل هذا النوع من الضرر فتَخرج حسب اللجنة من دائرة الهجوم العسكري، إلا فى الحالة التي تضرُّ فيها هذه العمليات السيبرانية بمصلحة وطنية حسَّاسة للدولة المعتدَى عليها دون أن تتَّصِل بضرر مادي محسوس[١].

وتجدر الإشارة إلى أنَّ هذا الدليل ليس صكًّا دوليًا رسميًا أو مُلزِمًا، أو يُمثِّل وجهة نظر (NATO)، أو الدول التي شارك خبراء من جنسيتها فى وضع الدليل، وإنَّما هو رؤية الخبراء المستقلِّين الذين صاغوه بصفاتهم الشخصية، ومع ذلك، فإنَّ أهَمِّيَّته كبيرة، كوثيقة رائدة فى مجال العمليات السيبرانية، وخطوة مهمَّة لتنظيم الفضاء السيبراني، وإن كانت غير كافية، ويلزم أن تتبعها خطوات أخرى[٢].

(١) د. أميرة عبد العظيم محمد عبد الجواد، المخاطر السيبرانية وسُبُل مواجهتها في القانون الدولي العام، المرجع السابق، ص: ٥٠٦.
(٢) د. محمد عادل محمد عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسُّس وقت السِّلْم، المرجع السابق، ص: ٧٠.

المطلب الثاني

إعلان ايريتشي بشأن مبادئ الاستقرار السيبراني والسلام السيبراني (الصادر عن الاتحاد العالمي للعلماء)

أُعِدَّ إعلان إيريتشي بشأن مبادئ الاستقرار السيبراني والسلام السيبراني بواسطة فريق الرصد الدائم المعني بأمن المعلومات التابع للاتحاد العالمي للعلماء (WFS)[1]، حيث اعتمدته الجلسة العامة للاتحاد العالمي للعلماء فى الدورة الثانية والأربعين للحلقات الدراسية الدولية بشأن الطوارئ العالمية وفي إيريتشي (صقلية) فى ٢٠ أغسطس ٢٠٠٩؛ وقد نشر فريق الرصد ورقات عديدة بشأن الأمن السيبراني والحرب السيبرانية، ويتناول بانتظام قضايا أمن المعلومات باعتبارها موضوعًا من موضوعات الطوارئ الحرجة أثناء الدورات العامة للاتحاد العالمي للعلماء التي تنعقد فى شهر أغسطس من كلِّ عام فى إيريتشي. ويُبيِّن هذا الإعلان أنَّ تحقيق الاستقرار السيبراني وتحقيق السلام السيبراني أمران مُتداخلان تداخُلًا وثيقًا، ويتَّسِم الإعلان بالإيجاز ويُركِّز على العناصر التشغيلية الأساسية للسلام السيبراني، وهي كالتالي:

١- ينبغي لجميع الحكومات الاعتراف بأنَّ القانون الدولي يضمن للأفراد التدفُّق الحرُّ للمعلومات والأفكار؛ وتنطبق هذه الضمانات أيضًا على الفضاء السيبراني، وينبغي عدم فرض القيود إلا عند الاقتضاء، على أن تخضع لعملية مراجعة قانونية.

٢- ينبغي لجميع البلدان العمل معًا لوضع مدوَّنة مشتركة للسلوك السيبراني وإطار قانوني عالمي مُنسَّق، بما فى ذلك أحكام إجرائية تتعلَّق بالمساعدة فى التحقيق والتعاون بما يكفل احترام الخصوصية وحقوق الإنسان، وينبغي لجميع الحكومات ومُزوِّدي الخدمات والمستعمِلين دعم الجهود المبذولة فى سبيل إنفاذ القانون الدولي ضدَّ مُرتكِبي الجرائم السيبرانية.

---

(١) في عام ١٩٧٣ قامت مجموعة من العلماء البارزين بإنشاء الاتحاد العالمي للعلماء في إيرتشه بجزيرة صقلية، ومنذ ذلك الحين انضمَّ كثير من العلماء الآخرين إلى الاتحاد، والاتحاد تجمُع حرَّ أخذ ينمو حتى أصبح يضمُّ أكثر من ١٠٠٠ عالم من ١١٠ دولة. ويتقاسم جميع الأعضاء نفس الأهداف والمثل العُليا، ويُساهمون طواعية في الدفاع عن مبادئ الاتحاد، ويُشجع الاتحاد على التعاون الدولي في العلم والتكنولوجيا بين العلماء والباحثين من كل أنحاء العالم، ويسعى الاتحاد وأعضاؤه إلى تحقيق حرية تبادل المعلومات كهدف مثالي، بحيث لا تكون الاكتشافات والتقدمات العلمية قاصرة على قلة مختارة. والهدف هو تقاسُم هذه المعارف بين شعوب كل الدول؛ ليتمتَّع كل شخص بفوائد تقدم العلم.

وكان إنشاء الاتحاد العالمي للعلماء ممكنًا بفضل وجود مركز للثقافة العلمية أُقيم في إيرتشه؛ لتخليد ذكرى عالم الفيزياء إيتوري مايورانا باسم «مؤسسة إيتوري مايورانا ومركز الثقافة العلمية (المركز). وأصبح هذا المركز الذي أُطلق عليه تسمية «جامعة الألفية الثالثة» قوَّة تعليمية عالمية، وقام هذا المركز منذ إنشائه في عام ١٩٦٣ بتنظيم ١٢٣ مدرسة و١٤٩٧ دورة دراسية حضرها أكثر من ٤٨٤ ألف مشاركًا (منهم ١٢٥ من الحاصلين على جائزة نوبل) من ٩٢٣ جامعة ومختبرا في ١٤٠ دولة.

٣- ينبغي لجميع المستعمِلين ومُزوِّدي الخدمة والحكومات العمل معًا لضمان ألا يُستخدَم الفضاء السيبراني بأيِّ شكل من شأنه أن يُفضي إلى استغلال المستعمِلين، لا سيَّما الشباب والمستضعفين منهم، من خلال العنف أو الإذلال.

٤- ينبغي للحكومات والمنظَّمات والقطاع الخاص بما فى ذلك الأفراد، تنفيذ برامج شاملة للأمن وتحديثها بناءً على أفضل الممارسات والمعايير المقبولة دوليًا، واستعمال تكنولوجيات حماية الخصوصية والأمن.

٥- ينبغي لمطوِّري البرمجيات والمعدَّات السعي إلى تطوير تكنولوجيات آمنة تُعزِّز القُدرة على التصدِّي وتُقاوم نقاط الضعف.

٦- ينبغي للحكومات أن تُشارك بفعالية فى جهود الأمم المتحدة الرامية إلى النهوض بالأمن السيبراني والسلام السيبراني فى العالم، وأن تتفادى استعمال الفضاء السيبراني من أجل النزاعات.

وقد دعا الاتحاد العالمي للعلماء منذ سنة ٢٠٠٢ إلى العمل على وضع قانون عالمي للفضاء السيبراني - وأنَّه من الأفضل أن يكون تحت رعاية الأمم المتحدة [١] - خاصَّة فى مجال الاستخدامات العدوانية والعسكرية للفضاء السيبراني.

(١) 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 ٢٠٠٣، تقرير مقدَّم إلى القمَّة العالمية لمجتمع المعلومات: http://www.itu.int/dms_pub/itu-s/md./pdf

الخاتمة

وبعد... ينتهي بنا المطاف فى شأن دراستنا للنظام القانوني الدولي للمَخاطر السيبرانية ذلك الموضوع الذي شغل بال المهتمّين بالجرائم السيبرانية، بعد أن باتت المخاطر السيبرانية تُمثّل الخطر الجديد الذي يُهدِّد العالم بأسره فى عصر المعلوماتية، وقد أبرزت الدراسة مفهوم المخاطر السيبرانية وطبيعته وصوره، ومدى تأثيرها على تهديد السِّلْم والأمن الدوليين، بالإضافة لبيان الجهود الدولية لمواجهة المخاطر السيبرانية.

وقد خلصنا فى نهاية دراستنا لموضوع النظام القانوني الدولي لمواجهة المخاطر السيبرانية إلى جُملة من النتائج والتوصيات، نتناولها على التفصيل التالي:

أوَّلًا: النتائج:

١- الفضاء السيبراني لم يعد خيالًا علميًا، بل أصبح واقعًا علميًا، ذا تأثيرات اجتماعية وسياسية واقتصادية، وتبدو الحاجة واضحة إلى آليات شاملة للأمن السيبراني، عن ضمان أمن شبكات اتصالاتها وبنيتها التحتية، واعتماد المعايير والمقاييس الدولية الخاصة بالحماية والأمن المعلوماتي، وأصبح ساحة جديدة للصراع بشكله التقليدي، ولكنَّه ذو طابع إلكتروني يعكس النزاعات التي تخوضها الدول أو الفاعلون من غير الدول على خلفيات دينية أو عِرقية أو أيدلوجية أو اقتصادية أو سياسية، ويتمدَّد الصراع الإلكتروني بداخل شبكات الاتصالات والمعلومات متجاوزًا الحدود التقليدية وسيادة الدول.

٢- إنَّ الهجوم السيبراني وقت السِّلْم من الأمور التي يُوجد اختلاف حولها، من خلال تحليل المبادئ العامة للقانون الدولي العام نجد أنَّ للدولة التي تعرَّضت للهجوم السيبراني إذا كانت آثاره تُشبه آثار الهجوم المسلَّح يكون لها حقُّ الدفاع عن النفس، سواء أكان بهجمة سيبرانية أم بهجوم مسلَّح.

٣- لا بُدَّ من مُراعاة التناسُب عند استخدام حقِّ الدفاع الشرعي.

٤- إنَّ القانون الدولي الإنساني يُطبَّق على الهجمات السيبرانية التي تُشنُّ وقت الحرب أو أثناء النزاع المسلَّح، وإنَّ دليل تالين هو المنظم لتلك الهجمات بشكل خاص

على الرغم من أنَّه وثيقة غير مُلزِمة لكنَّها الوحيدة التي نظَّمت موضوع الحرب والهجمات السيبرانية فى هذا الإطار، ومن ثَمَّ فإنَّ مبادئ القانون الدولي الإنساني تُطبَّق على تلك الهجمات استنادًا لدليل تالين على الرغم من الصعوبات الواقعية لتطبيقها فى ذلك الفضاء.

٥- إنَّ هناك جهودًا دولية وإقليمية لمكافحة هذه الظاهرة، وذلك من خلال المؤتمرات والاتفاقيات الدولية لمنع الجريمة السيبرانية، ومعاملة المجرِمين السيبرانيين.

٦- انتقلت جهود المنظمات الدولية التي تُقدِّمها منظمة الأمم المتحدة فى مجال مجابهة المخاطر السيبرانية من مرحلة الشجب والتحذير غير المنتظم بنسق وإطار محدَّد إلى مرحلة التأطير القانوني ووضع الإستراتيجيات النظامية لمواجهة هذا التهديد.

ثانيًا: التوصيات:

١- تتمثَّل الخطوة الأولى المقترَحة بشأن التعامُل مع العمليات السيبرانية فى التعجيل بالتفاوُض على صكٍّ دولي بشأنها فى إطار الأمم المتحدة، يستند إلى القواعد الدولية السارية لا سيَّما القانون الدولي الإنساني، وقواعد دليل تالين بإصداريه ٢٠١٣، ٢٠١٧، والتي تُعتبر أكثر ملاءمة لهذا المجال.

٢- لا بُدَّ من تكاتف الجهود الداخلية والدولية لإنشاء منظمات دولية وإقليمية وإبرام اتفاقات ثنائية وجماعية، وتكون متخصِّصة، مهمَّتها الأساسية التنسيق بشأن مواجهة الجرائم الإلكترونية واحتوائها، ومحاولة التخفيف منها.

٣- العمل على تزويد الجيوش بتقنيات ومهارات التعامل مع التهديدات السيبرانية، ويتمُّ ذلك من خلال تعليم وتدريب المهندسين المعلوماتيين العاملين فى القوَّات المسلَّحة، على اكتساب مهارات الأمن السيبراني؛ من أجل أن يكونوا قادرين على تولِّي مسئوليات حماية البنى التحتية الوطنية من تهديدات الهجمات السيبرانية القائمة حاليًا، وكذلك تلك المستقبلية.

٤- مساعدة البلدان بعضها البعض فى هذا الشأن لمواجهة تلك المخاطر والتي يتمُّ من خلالها أبشع ما يمكن تصوُّره وهو «الإرهاب» الذي لا يعرف دِينًا ولا وطنًا، والذي من الممكن أن يذهب ضحيَّته الملايين من البشر الأبرياء، والذي لا يعرف حينها الدول النامية من الدول المتقدِّمة، ومن هذا المنطلَق جاءت «دعوة للتعاون الدولي من أجل حماية البشرية».

٥- التواصل مع خبراء معلوماتيين وذلك لإيجاد برمجة معيَّنة تقوم بفصل البنية التحتية والشبكات السيبرانية العسكرية عن المدنية؛ وذلك لحماية السكان المدنيين من مخاطر الحروب السيبرانية.

٦- على الدول -خاصة العظمى والكبرى- أن تستغلَّ التطوُّر التكنولوجي فى مجال الثورة المعلوماتية بما يخدم رفاهية الدول بصورة عامة، والإنسان بصورة خاصة، بدل من تسخيرها فى الصراعات والحروب.

المراجع

أوَّلًا: المراجع العربية:

أ- الكتُب:

- د. أحمد الأنور، قواعد وسلوك القتال، دراسات فى القانون الدولي الإنساني، دارالمستقبل العربي، القاهرة، ٢٠٠٠.

- د. إسماعيل صبري مقلد، أصول العلاقات الدولية فى إطار عام، دار النهضة العربية، الطبعة الأولى، ٢٠٠٧.

- تيري ديبيل، إستراتيجية الشئون الخارجية منطق الحكم الأمريكي، ترجمة: وليد شحادة، دار الكتب العربية، مؤسسة محمد بن راشد آل مكتوم، بيروت، ٢٠٠٩م.

- د. جمال محمد غيطاس، الحرب وتكنولوجيا المعلومات، الطبعة الأولى، دار النهضة العربية، ٢٠٠٦.

- د. حسين المحمدي بوادي، الإرهاب الدولي بين التجريم والمكافحة، دار الفكر العربي، ٢٠٠٦.

- د. صالح بن علي بن عبد الرحمن الربيعة، الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت، هيئة الاتصالات وتقنية المعلومات، المملكة العربية السعودية، ٢٠١٨م.

- د. طارق عزت رخا، المنظمات الدولية المعاصرة، دار النهضة العربية، القاهرة، ٢٠٠٦.

- د. عادل عبد الصادق، الفضاء الإلكتروني والرأي العام، تغير المجتمع والأدوات والتأثير، المركز العربي لبحوث الفضاء الإلكتروني : قضايا إستراتيجية، ٢٠١٣م.

- د. عباس بدران، الحروب الإلكترونية، الاشتباك فى عالم متغير، مركز

دراسات الحكومة الإلكترونية، بيروت، لبنان، ٢٠١٠م.

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

- د. كلاوس شواب، الثورة الصناعية الرابعة، ملخصات لكتب عالمية، تصدر عن مؤسسة محمد بن زايد للمعرفة، دبي، الإمارات، ٢٠٢٠ م.

- د. محمد الأمين، د. محسن عبد الحميد أحمد، معايير الأمم المتحدة فى مجال العدالة الجنائية ومنع الجريمة، أكاديمية نايف للعلوم الأمنية، الرياض، الطبعة الأولى، ١٩٩٨.

- د. محمد فهاد الشلالدة، القانون الدولي الإنساني، منشأة المعارف، الإسكندرية، ٢٠٠٥.

- د. محمود حجازي محمود، العنف الجنسي ضد المرأة فى أوقات النزاعات المسلحة، دار النهضة العربية، القاهرة، ٢٠٠٧.

- د. مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، ط٢٠٠٠.

- د. مصطفى محمد موسى، الإرهاب الإلكتروني، بدون دار نشر، الطبعة الأولى، ٢٠٠٩.

- منير البعلبكي « المورد: قاموس إنكليزي - عربي » ، دار العلم للملايين، بيروت ٢٠٠٤م.

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

- د. هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية للجرائم المعلوماتية (على ضوء اتفاقية بودابست ٢٠٠١) دار النهضة العربية، ط ٢٠٠١.

- د. هلالي عبد اللاه أحمد، جرائم الحاسب والإنترنت بين التجريم الجنائي

وآليات المواجهة دار النهضة العربية، ٢٠١٥ م.

- د. هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية (معلقًا عليها)، دار النهضة العربية، ط٢، ٢٠١١.

- د. نزار العنبكي، القانون الدولي الإنساني، الطبعة الأولى، ٢٠١٠.

ب- الأبحاث والرسائل:

- د. إبراهيم محمد العناني، مجالات تطبيق القانون الدولي الإنساني، مجلة العلوم القانونية والاقتصادية، كلية الحقوق، جامعة عين شمس، المجلد ٤٣، العدد ١، يناير ٢٠١٠.

- د. أحمد عبيس الفتلاوي، الهجمات السيبرانية: مفهومها والمسئولية الدولية الناشئة عنها فى ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي للعلوم القانونية والسياسية، جامعة بابل- كلية القانون، العدد الرابع، السنة الثامنة، ٢٠١٦.

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

- د. حازم حسن أحمد الجمل، الحماية الجنائية للأمن السيبراني فى ضوء المملكة ٢٠٣٠، مجلة البحوث الأمنية، كلية الملك فهد الأمنية، مركز الدراسات والبحوث، مج ٣٠، ع٧٧، أغسطس ٢٠٢٠م.

- د. خالد محمد نور عبد الحميد الطباخ، المواجهة القانونية للإرهاب الإلكتروني الدولي، مجلة الدراسات القانونية والاقتصادية، جامعة مدينة السادات- كلية الحقوق، مج ٣، ع١، ٢٠١٧.

- د. سلافة طارق الشعلان، تكييف استخدام الحرب الإلكترونية فى النزاعات المسلحة وفقًا للقانون الدولي الإنساني، مجلة كلية القانون، جامعة الكوفة، المجلد ٩، العدد ٢٦، ٢٠١٦.

- د. عبد بن عبد العزيز بن فهد، بحث بعنوان «الإرهاب الإلكتروني فى عصر

المعلومات»، مقدَّم إلى المؤتمر الدولي الأول حول «حماية أمن المعلومات والخصوصية في قانون الإنترنت» المنعقد بالقاهرة في الفترة من ٢-٤ يونيو ٢٠٠٨م.

- د. عبد الله عبد العزيز العجلان، الإرهاب الإلكتروني في عصر المعلومات، بحث مقدَّم إلى المؤتمر الدولي الأول لحماية أمن المعلومات والخصوصية في قانون الإنترنت والمنعقد بالقاهرة في الفترة ٢-٤ يونيو ٢٠٠٨.

- د. عادل عبد الصادق، موقع ويكيليكس وتحدّي عالم الاستخبارات الأمريكي، ملف الأهرام الإستراتيجي، مركز الأهرام للدراسات السياسية والإستراتيجية، أكتوبر، ٢٠١٠.

- د. عادل عبد الصادق، القوة الإلكترونية « أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني « ، المركز العربي لأبحاث الفضاء الإلكتروني، قضايا إستراتيجية، ٢٠١٢.

- د. عادل عبد الصادق، هل يُمثِّل الإرهاب الإلكتروني شكلًا جديدًا من أشكال الصراع الدولي، ملف الأهرام الإستراتيجي، مركز الدراسات السياسية والإستراتيجية بالأهرام، العدد ١٥٦، ديسمبر ٢٠٠٧.

- د. عصام فاعور ملكاوي، الفضاء الإلكتروني ساحة حرب دولي مفترضة، إربد للبحوث والدراسات - القانون، جامعة إربد الأهلية - عمادة البحث العلمي والدراسات العليا، مج ١٨، ع ٢، تموز ٢٠١٥.

- د. لامية طالة، الإرهاب السيبراني والأمن القومي: قراءة في تحوُّلات الإستراتيجية الدفاعية، حوليات جامعة الجزائر ١، المجلد ٣٥، العدد ٤، ٢٠٢١م.

- د. مايكل شميت، الحرب بواسطة شبكات الاتصال، الهجوم على شبكات الكمبيوتر والقانون في الحرب، المجلة الدولية للصليب الأحمر، ٢٠٠٢.

- د. محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، ورقة بحثية في مؤتمر «القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، الإمارات، خلال الفترة من ١-٣ مايو ٢٠٠٠.

- د. محمد عادل محمد عسكر، وضع العمليات السيبرانية فى القانون الدولي مع التطبيق على ممارسة التجسُّس وقت السلم « دراسة على ضوء دليل « تالين « بشأن القانون الدولي المطبَّق على العمليات السيبرانية ٢٠١٣-٢٠١٧ »، ٢٠٢٠م.

- أ. محمد عبد الحق شربال، الأسلحة الحديثة والقانون الدولي الإنساني، رسالة ماجستير، كلية الحقوق، جامعة بن يوسف، الجزائر، ٢٠١٢.

- د. مصطفى جاد، مقال بعنوان « مستقبل الإرهاب السيبراني « ، فى ندوة نظمها المركز الدولي للدراسات المستقبلية والإستراتيجية فى ١١ أبريل ٢٠١٢، جريدة السياسة الدولية التابعة لمؤسَّسة الأهرام، إعداد / شريهات نشأت المنيري.

- د. ممدوح عبد الحميد عبد المطلب، جرائم استخدام شبكة المعلومات، الجريمة عبر الإنترنت، بحث مقدَّم لمؤتمر القانون والكمبيوتر، كلية الشريعة والقانون، جامعة الإمارات، ٢٠٠٠.

- د. يحيى ياسين سعود، الحرب السيبرانية فى ضوء قواعد القانون الدولي الإنساني، المجلة القانونية، جامعة القاهرة، كلية الحقوق فرع الخرطوم، نوفمبر ٢٠١٨م.

ج- الاتفاقيات والوثائق الدولية:

- ميثاق الأمم المتحدة ١٩٤٥م.

- اتفاقية جنيف ١٩٤٩ وبروتوكولاتها الإضافية.

- النظام الأساسي لمحكمة العدل الدولية.

ثانيًا: المراجع الأجنبية:

- Blimding weapons : Reports of the meetings of experts convened by the international committee of the red cross on battlefield laser weapons, 1989-1991, ICRC, 1993.

- Christian Agrum, Words for Understanding Cyber Security: Enjoying a Calm Internet, Edition, October, 1, 2010.

- Doswald- Beck "international humanitarian law and the advisory opinion of international court of justice on the threat or use of nuclear weapons" ICRC Vol.316, 1997.

- Dorothy E. Denning, Activism, Hacktivism and cyber terrorism, the internet as a tool for influencing Foreign policy in : Arquilla & D. Ronfold (eds), Networks and net wars, the future of terror crime and miletences, National Defense Research Institute, 2001.

- Ebert Hannes and Maurer Tim. "Cyber Security" oxford bibliographies, Last Modified : 11 January,2017.

- Fahad Ullah Khan, States rather than criminals pose a greater threat to global cyber security: a critical analysis, the Institute of Strategic Islamabad ISSI ..olume xxxi, no3, Autumm 2011, p.93, available at: http://issi.org.pk/wp-content/uploads/2014/06/1328592265_43276030.pdf

- Harvard, Joseph S. Nye : The future of power .press realise, Belfer center for Science and international Affairs, Kennedy Scholl, 31 january 2011.

- Hall William Edward, A Treatise on international law , Fourth edition , Oxford, London, 1895.

- in The Charter of the United Nations : Article 51, A. Randelzhofer .664 (B.Simma ed.) 1995, A Commentary 661.

- Jack L. Brock, Computer Security: Hackers Penetrate DOD Computer System (Washington DC: General Accounting Office, 1991) Full Text available online at: http://www.globalsecurity.org/security/library/report/ gao/145327.pdf

- Jeffrey T. G Kalsey, Hacking in to international humanitarian law: The principles of distinction and neutrality in the age of cyber warfare, Michigan law review, 2008, vol.106, issue 7.

- Jennie M. Williamson "Information Operations : computer U.S.Army, PA, Carlisle Barracks, Network Attack in the 21 st century" war college, 2002.

- Joseph. S. Nye, Cyberpower Haward Kennedy School, Belfer center for science and International Affairs 2010 ,Available at:

http://www.Belfercenter.Ksg. Harvard .Edufilescyber –power ,pdf

- Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004, JCJ Rep 136, para 35, Separate opinion of Judge Higgins.

- Maura Conway, Terrorism and new media : the cyber-battl espace in: Forest, James F., (eds.), Countering terrorism and insurgency in the 21st century, Greenwood Publishing Group, Inc., Westport. CT, 2007,PP.363-384. http://www.shaimaaatalla.com/vb/

- Michael N Schmitt, Computer Network Attack and The Use of Force in International Law: Thoughts on a normative framework, Co;ombia Journal of transnation law, 1998-1999.

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

- 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.

- N.TSAGOURLAS, Cyber Attacks, Self-defence and the Problem of Artibution, J.Conflict & Sec L.Vol.17, no 2, 2012,.

- Rohas Nagpal, Cyber terrorism in the context of globalization, Paper presented at II World Congress on Informatics and Law, Madrid, Spain, September 2002, p.4, available at: http://www.asianlaws.org/aboutus/ spain.pdf

- Ruseell Buchan, "Cyber espionage and international law", In: Nicholas Tsagourias and Russell Buchan (eds), Research. Handbook on International law Cyberspace, (Edward Elgar Publishing 2015).

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

- Tallinn Mnnual on the International Law Applicable to Cyber Warfare (Michael N. Schmitt ed., 2013), pp.106-107.

- Toward a Universal order of Cyberspace :managing Threats from Cybercrime of Cyberya The International Telecommunication Union, ITU Toolkit for Cybercrime Legislation, Geneva, 2010.

- United Nation, General Assembly, Development in the field of information and telecommunications in the context of international security, Report, Sixty-sixh session, 15 July 2011, (UN DOC.A/66/152).

- United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at : https://unctad.org/

المُلخَّص:

شهد المجتمع الدولي خلال العقد الأخير مَوجة انتشار واسعة لتكنولوجيا الأجهزة الحاسوبية والشبكة المعلوماتية التي أحدثت ثورة فى الطريقة التي نعيش بها فى حياتنا، كالمرونة فى الحصول على المعلومات، واعتماد العديد من الخدمات والبِنَى التحتية الأساسية عليهم.

لكن لكلِّ أمر جانبه السلبي كما له جانبه الإيجابي، فعلى الرغم من التطوُّر الهائل لثورة المعلومات، إلا أنَّها فى ذات الوقت جعلت المجتمع الدولي يُواجه مخاطر جديدة مُرتبطة بهذا التطوُّر، فقد ظهرت الهجمات السيبرانية التي لا تقتصر آثارها على البيانات فى أجهزة الكمبيوتر أو أنظمته، بل تتجاوز ذلك لتقوم بالتأثير بشكل مباشر على العالم الحقيقي؛ كاختراق أنظمة الكمبيوتر للسيطرة على الحركة الجوية، وتعطيل عمل محطَّات الطاقة النووية، والعديد من التأثيرات السلبية التي قد تُؤدِّي إلى وقوع حوادث كارثية، ويكون المدنيون هم الضحايا الرئيسيين لمثل هذه الهجمات.

لذا قامت العديد من الدول باعتماد إستراتيجيات من شأنها دعم الجانب العسكري فى الفضاء السيبراني، ليس فقط ضدَّ الهجمات التي قد يقوم بها الأفراد والقراصنة، بل أيضًا ضدَّ احتمال استخدام الدول لمثل هذا المجال الجديد فى الصراع، ولذلك بات من الضروري توحيد الجهود الدولية لوضع الأطر القانونية والتنظيمية لمُواجهة المخاطر السيبرانية، وآثارها على المستوى الدولي.

الكلمات المفتاحية:

السيبرانية، المخاطر السيبرانية، الهجمات السيبرانية، الفضاء السيبراني، حق الدفاع الشرعي، الأمن السيبراني، الحرب السيبرانية، دليل تالين.

The international legal system for combating cyber risks

Dr . Hani Muhammad Khalil Ibrahim Al-Azzazi

Abstract:

During the last decade, the international community witnessed a widespread wave of computer hardware and information network technology that revolutionized the way we live in our lives, such as flexibility in obtaining information and the adoption of many basic services and infrastructures on them.

But every matter has its negative side as well as its positive side, despite the tremendous development of the information revolution, but at the same time it made the international community face new dangers associated with this development, cyber attacks have appeared whose effects are not limited to data in computers or systems, but rather It goes beyond that to directly affect the real world, such as hacking computer systems to control air traffic, disrupting the work of nuclear power plants and many negative effects that may lead to catastrophic accidents and civilians are the main victims of such attacks.

Therefore, many countries have adopted strategies that would support the military side in cyberspace, not only against attacks that may be carried out by individuals and pirates, but also against the possibility of countries using such a new field of conflict, and therefore it has become necessary to unify international efforts to develop legal and regulatory frameworks to confront Cyber risks, and their effects at the international level.