 https://doi.org/10.12816/0054788

International Responsibility for Cyber-Attacks in Light of the Contemporary International Law

Talal Yaseen Aleisaa
Faculty of Law
Ajloun National University, Jordan
talalaleissa@yahoo.com

Odai Mohammad Innab
Faculty of Law
Ajloun National University, Jordan
odaienab55@gmail.com

Received 04/10/2018 Accepted 11/12/2018

Abstract:

The study deals with a very important subject which is the international responsibility arising from cyber-attacks, especially cybercrime which has increased in light of the great development on the Internet and Internet access in all areas of life. The study came to answer the main question: What is the international responsibility arising from cyber-attacks in Light of contemporary international law? The main objectives of the study can be summarized in the following: 1- to identify the concept of cyberspace, 2- to trace the historical stages of cyber development, 3- to clarify the legal adaptation of cyber-attacks and their effects, 4- to clarify the extent to which international responsibility arising from cyber-attacks, 5- to clarify aspects of the applicability of international responsibility for cyber-attacks, and, in the end, 6- to specify the reference to international trends in the fight against cybercrime.

The study showed a number of results, the most important of which is that most countries lack the existence of special legislation in cyberspace, and if there are laws that there are significant legal gaps in this area. In light of this, the student recommended a number of recommendations, the most important of which is the need to fill the legislative vacuum in the field of combating cybercrime, Enact legislation covering this vacuum in order to reach a secure cyber space.

Keywords: International Law, Cyber Attacks, Anarchist Network, International Responsibility.

https://doi.org/10.12816/0054788

المسؤوليّة الدّوليّة النّاشئة عن الهجمات السّيبرانيّة في ضوء القانون الدّولي المعاصر

طلال ياسين العيسى
كلية الحقوق
جامعة عجلون الوطنية – الاردن
talalaleissa@yahoo.com

عدي محمد عناب
كلية الحقوق
جامعة عجلون الوطنية – الاردن
odaienab55@gmail.com

استلام البحث 2018/10/04 قبول البحث 2018/12/11

الملخص:

تختص هذه الدراسة بالبحث في أحد أهم المواضيع الا وهو المسؤوليّة الدّوليّة النّاشئة عن الهجمات السّيبرانيّة في ضوء القانون الدّولي المعاصر وعلى وجه الخصوص الجرائم السيبرانية، والتي ازدادت مع التطور العظيم للانترنت و استخدام الانترنت في كافة مناحي الحياة. تسعى الدراسة للإجابة على السؤال الرئيسي: ما هي المسؤولية الدولية النّاشئة عن الهجمات السّيبرانيّة في ضوء القانون الدّولي المعاصر. ويمكن تلخيص الأهداف الرئيسة للدراسة في: 1. تحديد مفهوم الفضاء السايبراني. 2. تتبع التطور التاريخي لمراحل السيبرانية. 3. توضيح المواكبة القانونية للهجمات السيبرانية وتاثيراتها. 4. توضيح مدى المسؤوليّة الدّوليّة النّاشئة عن الهجمات السّيبرانيّة. 5. توضيح مدى تطبيق المسؤوليّة الدّوليّة النّاشئة عن الهجمات السّيبرانيّة. 6. تحديد المرجعية للتوجهات الدولية لمواجهة الجرائم السيبرانية.

أظهرت الدراسة العديد من النتائج وأهمها أن أغلب الدول تفتقد إلى وجود تشريعات تختص بالفضاء السيبراني وفي حال وجود قوانين فإنه يوجد ثغرات قانونية بهذا الخصوص. وبناء على على ذلك أوصى الطلاب بمجموعه من التوصيات وأهمها هو الحاجة لتعبئة الفراغ التشريعي في مجال مكافحة الجرائم السيبرانية من خلال سن التشريعات لملئ هذا الفراغ من أجل الوصول الى فضاء سيبراني آمن.

الكلمات الدالة: القانون الدولي، الهجمات السيبرانية، الشبكة العنكوتية، المسؤولية الدولية.

المقدمة :

شَهِدَ الطلب على الإنترنت سواء أكان في الإنتاج، أو التوزيع، أو الاتصال، أو التمويل، أو غيرها، تزايدًا واضحًا منذ عقد التسعينات من القرن الماضي، عندما أصبحت معظم خدمات العالم الإنتاجية، والخدميّة، والمعلوماتية، والاجتماعية، تعتمد بصورة جوهرية وأساسية على الشبكة العنكبوتية، فأدى الاعتماد الكبير على الإنترنت في زيادة المخاطر التي يتعرض لها مستخدموها من الهجمات الإلكترونية؛ لسهولة اختراق شبكة الإنترنت؛ نتيجة تطور الحواسيب والبرمجيات.

وبالتزامن مع هذا التطور الكبير في الشبكة العنكبوتية، وزيادة الاعتماد عليها، ظهر ما يسمى: قراصنة المعلومات أو الهاكرز (Hackers)، وهم أشخاص يمتلكون خبرة عميقة في ميدان تقنيات المعلومات والحواسيب، ولديهم القدرة في الدخول إلى المواقع المحظورة في نظم شبكات الحواسيب بمختلف أشكالها، ويستهدف نشاطهم المواقع الإلكترونية المهمّة، كالمواقع الإلكترونية للمؤسسات العسكرية والمالية، حيث يقومون باختراق تلك المواقع التابعة للمؤسسات؛ بقصد الحصول على أسرار، أو وثائق، أو نشر رسائل سياسية احتجاجية، أو حتى لجمع المال[37].

وأصبحت الهجمات السيبرانية من أهم التحديات التي يواجهها المختصون في القانون الدولي العام؛ وذلك لصعوبة تحديد طبيعتها وعناصرها، وما يترتب على هذه الهجمات من تبعات المسؤولية الجنائية أو المدنية الدولية، خاصة وأن تلك الهجمات قد تلجأ إليها بعض الدول لأجل تحقيق مكاسب: كالهيمنة على واقع النزاع المسلح، أو توجيه تهديدات سياسية أو عسكرية لدول أخرى، فضلًا عن النتائج السلبية من التهديدات الإجرامية والإرهابية، التي قد تنتجها تلك الهجمات في حال لجأت إلى ارتكابها مجموعات فرديّة؛ من أجل الحصول على مزايا سياسية أو اقتصادية[26].

وستتناول هذه الدراسة المسؤولية الدولية الناشئة عن الهجمات السيبرانية، في ضوء القانون الدولي المعاصر من خلال المباحث الآتية:

المبحث الأول: مفهوم الهجمات السيبرانية.

المبحث الثاني: التكييف القانوني للهجمات السيبرانية.

المبحث الثالث: المسؤولية الدولية للهجمات السيبرانية.

المبحث الأول:

مفهوم الهجمات السيبرانية:

أُطلق العديد من المصطلحات والمفاهيم على الهجمات السيبرانية، فقد أطلق مصطلح الحرب الافتراضية، أو الحرب الإلكترونية، أو الحرب السيبرانية، على الهجمات السيبرانية التي يتم من خلالها قيام القراصنة (Hackers) بمهاجمة الملفات والمواقع التي تخص الآخرين، كمهاجمة المواقع الإلكترونية للمنشآت المهمّة، أو مهاجمة الحواسيب التابعة للوحدات العسكرية أو الوحدات الاقتصادية لدول معيّنة؛ بقصد تدميرها، والسيطرة عليها، والإضرار بها[10].

ومن خلال هذا المبحث سيتم تسليط الضوء على تعريف السيبرانية، وعليه سيتم تقسيم هذا المبحث إلى المطلبين الآتيين:

المطلب الأول: تعريف السيبرانية لغة واصطلاحًا:

الهجمات السيبرانية مصطلح حديث ظهر في العقود الأخيرة؛ نتيجةً لثورة تكنولوجيا المعلومات، ولم تكن الهجمات السيبرانية معروفة إلّا في وقت قريب، ممّا يشكل أحد أهم التحديات الراهنة التي يواجهها المختصون في القانون الدولي العام، فيما يخص تحديد طبيعتها، أو تعريفها، أو الكشف عن عناصرها، خاصة أنها تستهدف جميع الحواسيب والمعلومات التي بداخلها، والأنظمة والبرامج والشبكات المفتوحة لاستعمال الجمهور العام، أو تلك الشبكات التي صممت لاستعمال فئة محددة من المستعملين، والمفصولة عن شبكة الإنترنت العامة[27].

فالهجمات السيبرانية يكتنفها غموض كبير، مما نتج عن ذلك صعوبات واجهها المختصّون في القانون الدولي العام، والإنساني على وجه الخصوص، وذلك من حيث تحديد تعريف محدّد ومتفق عليه للهجمات السيبرانية. ولغايات الوقوف على مفهوم هذا المصطلح حديثِ النشأة، سيتم التطرق إلى تعريف الهجمات السيبرانية لغويًّا في ضوء المعاجم اللغويّة، فضلًا عن التطرق لتعريف الهجمات السيبرانية اصطلاحًا في ضوء الاجتهادات الفقهية، والممارسات الدولية، ومقولات خبراء تكنولوجيا المعلومات، وذلك وَفق النحو الآتي:

الفرع الأول: تعريف السيبرانية لغةً:

لم تشر أغلب معاجم اللغة الحديثة إلى مصدر كلمة السيبرانية، ويتضح من ذلك أن السيبرانية هي مصطلح يوناني الأصل، وترجع إلى مصطلح (Kybernetes) الذي ورد في مؤلفات الخيال العلمي، ويعني القيادة والتحكم عن بُعد[47]. واستدراكًا على ذلك، فقد ورد في قاموس المورد تعريف للسيبرانية، حيث عرّفها بأنها: علم الضبط، ومصدرها (Cybernetics)، وهو مصدر يتطابق مع مفهوم الهجمات السيبرانية، أي ضبط الأشياء عن بعد، والسيطرة عليها[6]، بينما قاموس مصطلح الأمن المعلوماتي، فقد عرف السيبرانية بقوله بأنها: هجوم عبر الفضاء الإلكتروني، يهدف إلى السيطرة على المواقع الإلكترونية، أو البنى المحميّة إلكترونيًّا؛ لتعطيلها، أو تدميرها، أو الإضرار بها[46].

أما في اللغة العربية، فنجد أن مصطلح السيبرانية هو مصطلح مستخدم في اللغة الإنجليزية (Cyber)، ولا يوجد مصطلح يناظره أو يقابله في اللغة العربية، لهذا واجه المتخصصون في اللغة العربية صعوبات في اختيار مصطلح مقارب لمصطلح (Cyber) في اللغة الإنجليزية، حتى إن بعض الترجمات العربية لهذا المصطلح كانت في أغلبها غير صائبة، وهذا ما نجده في الترجمة غير الصائبة التي تناولت ترجمة عنوان: "اتفاقية أوروبا المتعلقة بالجريمة السيبرانية"، إذ تم ترجمتها إلى اللغة العربية بـ"الاتفاقية المتعلقة بالجريمة الإلكترونية"[26].

وفي القواميس المتخصصة في المصطلحات العسكرية، لم ترجع كلمة سايبر إلى مصدرها، بل عرفت السيبرانية في نطاق استخدامها الفعلي أيّ: العسكري، وهذا ما أشار إليه قاموس المصطلحات العسكرية الأمريكية بقوله: "السيبرانية هي أي فعل يستخدم عن طريق شبكات إلكترونية؛ بهدف السيطرة، أو تعطيل برامج إلكترونية أخرى[48]".

الفرع الثاني: تعريف الهجمات السيبرانية اصطلاحًا:

تعددت التعريفات التي تناولت مصطلح الهجمات السيبرانية على ضوء الاجتهادات الفقهية، والممارسات العملية الدولية، فالهجمات السيبرانية مصطلح يُستخدم من قبل فئات عديدة من الناس؛ للإشارة إلى أشياء مختلفة، كالإشارة إلى وسائل القتال وأساليبه، تلك التي تتألف من عمليات في الفضاء الإلكتروني، والتي يمكن أن ترتقي إلى مستوى النزاع المسلح، أو تُجرى في سياقه، ضمن المعني المقصود في القانون الدولي الإنساني.

ويمكن وصف الفضاء السيبراني الذي تجري فيه الهجمات السيبرانية، بأنه: عالم افتراضي مع عالمنا المادي، يتأثر به ويؤثر فيه بشكل معقد، وتعتمد الهجمات السيبرانية على نظم الكمبيوتر، وشبكات الإنترنت، والمخزون الهائل من المعلومات والبيانات، حيث يتم الاتصال بشبكات الإنترنت عبر الحواسيب، أو الهواتف، أو غيرها من الأجهزة دون تقيّد بالحدود الجغرافية، لذلك فإن الهجمات السيبرانية – في هذا الاتجاه– يمكن وصفها بأنها عبارة عن تصرف واقعي، يدور في عالم افتراضي قائم على استخدام بيانات رقمية، ووسائل اتصال تعمل إلكترونيًّ، ومن ثم تطور هذا المفهوم، حيث أصبح واسعًا يقوم على تحقيق أهداف عسكرية أو أمنية ملموسة ومباشرة؛ جراء اختراق

مواقع إلكترونية حساسة، عادة ما تقوم بوظائف تصنف بأنها ذات أولوية، كأنظمة حماية محطات الطاقة النووية، أو الكهربائية، أو المطارات، ووسائل النقل الأخرى[30].

وعرفت الهجمات السيبرانية بأنها وسيلة قتالية من خلال استخدامها بذاتها للتسلل إلى أنظمة إلكترونية، معدة لحماية أو لتنظيم سير عمل منشآت حيوية، كمحطات توليد الطاقة النووية، أو السدود، أو وسائل النقل كالمطارات؛ بهدف تطويعها والسيطرة عليها؛ لتدمير ذاتها بذاتها من خلال تغذيتها بمعلومات غير صحيحة لأجهزة التحكم والحماية الإلكترونية، لكن هذا الاتجاه تم توجيه النقد له، لأن هناك اتجاهًا رأى تصنيف الهجمات السيبرانية كونها وسيلة قتالية قد لا يكون صائبًا؛ لأن الهجمات السيبرانية تفتقد للطاقة الحركية التي تعد أهم صفة تُعرف بها الأسلحة التقليدية، لذلك فإنه من غير الممكن تحسس الهجوم السيبراني على نحو مادي، فضلاً عن أن وسيلة الهجمات السيبرانية، لا تحوي مواد متفجرة، ومن ثمّة لا يمكن عدّها وسيلة قتالية[23].

ومنهم من عرف الهجمات السيبرانية بأنها الذراع الرابعة للجيوش الحديثة، إلى جوار القوات الجوية والبرية والبحرية، خاصة أن عصر الإنترنت شهد بداية الحديث عن معارك حقيقية تدور في هذا العالم الافتراضي. وهناك من يرى أن الهجمات السيبرانة تمثل البعد الخامس للحرب، وفي هذا الاتجاه تم تعريف الهجمات السيبرانية بأنها: "مجموعة من الإجراءات التي تتخذها الدولة للهجوم على نظم المعلومات العادية؛ بهدف التأثير والإضرار بها، وفي الوقت نفسه الدفاع عن نظم المعلومات الخاصة بالدولة المُهاجمة[28]". بينما هناك من أشار إلى أن المقصود بها هو:" هجوم عبر الإنترنت يقوم على التسلل إلى مواقع إلكترونية غير مرخص الدخول إليها، بهدف تعطيل البيانات المتوفرة فيها، أو إتلافها، أو الاستحواذ عليها، وهي عبارة عن سلسلة هجمات إلكترونية تقوم بها دولة ضد أخرى[26]".

ويؤيد الباحث التعريف الذي أشار إلى الهجمات السيبرانية بأنها: أي تصرف، سواء أكان دفاعيًّا أم هجوميًّا، يتوقع منه، وعلى نحو معقول، في التسبب بإصابة شخص، أو قتله، أو إلحاق أضرار مادية، أو دمار بالهدف المُهاجَم[49]. إذ يعد هذا التعريف الأقرب والأشمل لمفهوم الهجمات السيبرانية.

الفرع الثالث: تعريف الهجمات السيبرانية من خلال الأمن القومي:

تُظهر المستجدات العديدة في مجال تكنولوجيا، بأنّ الحرب السيبرانية تعدّ تحديًا للمفاهيم السائدة حول الأمن القومي، وهذا يرتب إيلاء قضية الدفاع عن البنى التحتية الحيوية للدولة أهمية قصوى، لاسيما في مجالات الطاقة، والمياه، والحوسبة، والاتصالات، والمواصلات، والاقتصاد، في القطاعين المدني والأمني. وبناءً عليه، ينبغي إجراء التعديلات اللازمة في مفهوم الأمن القومي؛ بهدف الردّ على التهديدات المستجدة الناتجة عن الهجمات السيبرانية[22]. فالتصدي للتهديد المستجد الناجم عن تطور تكنولوجيا الحرب السيبرانية، يتلاءم مع عقيدة الأمن القومي لأي دولة في الوقت الحاضر؛ لأنه في الإمكان، بواسطة أدوات سيبرانية لا تتطلب قوةً مادية كبيرةً ،ولكنها تتطلب إعدادًا وتطويرًا لمهارات القوة البشرية، تنفيذ أنشطة تساهم في تعاظم قوة الردع للدولة، وترسخ مكانتها على الساحة الدولية، لذلك نجد أن الركائز الثلاث لمفهوم الأمن القومي التقليدي للدول، صالحة للتهديد السيبراني، وذلك من خلال الآتي:

أولاً: الردع:

إن القدرات السيبرانية المتطورة، تمكّن أي دولة من ردع أعدائها، فقديمًا كان من السهل تقييم قدرات الدول وإمكاناتها، وقياس قوتها، لكن عبر مضي القرون، وازدهار التكنولوجيا وتطورها، تغيرت مصادر القوة وأشكل الردع، وأصبحت القوة الإلكترونية من أهم أدوات الردع التي تستخدمها الدول في التنافس والتصارع مع بعضها بعضًا، فعلى سبيل المثال إن التغطيةَ الإعلامية الواسعة التي حظي بها فيروس "ستاكسنت"؛ الذي استُخدم لتخريب أنظمة الكمبيوتر التي تتحكم بمرافق تخصيب اليورانيوم في إيران، المنسوب إلى الولايات المتحدة وإسرائيل، والذي شكَّل قفزة نوعية في كل ما يتعلق بالقدرة الهجومية السيبرانية للدول، وقوتها، ونفوذها[10].

ثانيًا: الإنذار المبكر:

إن القدرات السيبرانية الهائلة للدولة ستمكنها من جمع معلومات كثيرة عن أعدائها، وفي الوقت ذاته ستمنع هؤلاء من الوصول إلى قاعدة بياناتها، وهذا يشكل بالنسبة للدولة إنذارًا فعّالاً بشأن نية أعدائها[10].

ثالثًا: الحسم:

فالدول الرائدة في العالم من حيث قدراتها السيبرانية، تكون متفوقة في المعركة؛ من خلال استخدام أدوات سيبرانية متقدمة بهدف حسم المعركة، فالواضح اليوم أن التفوق السيبراني المتكامل، مع قدرات حركية متقدمة، أصبح من شأنه أن يحسم المعارك[10].

المطلب الثاني: أنواع الهجمات السيبرانية:

أصبح النظام الدولي ظاهرة متعددة في أبعادها ونطاق تأثيرها وملامحها، مما فرض المزيد من التعقيد على ظاهرة الهجمات السيبرانية: (الإرهاب الإلكتروني)، التي تنطوي على كثير من الصعوبات والتحديات التي تتعلق بمدى إمكانية إدراج استخدام القوة بصورتها المرنة داخل الفضاء الإلكتروني، في الإطار القانوني الذي يتعامل مع استخدام القوة "الصلبة" في العلاقات الدولية، وما ورد في ميثاق الأمم المتحدة في المادة (2) فقرة (4)، والتي تقضي بأن "يمتنع

أعضاء الهيئة جميعًا في علاقاتهم الدولية، عن التهديد باستعمال القوة، أو استخدامها ضد سلامة الأراضي، أو الاستقلال السياسي لأية دولة، أو على أي وجه آخر لا يتفق ومقاصد الأمم المتحدة". ووضع ميثاق الأمم المتحدة شروطًا لاستخدام القوة، وردت في المادة (51) من الميثاق[8].

ويمكن القول إنّ الهجمات السيبرانية تنقسم إلى ثلاثة مستويات، هي:

أولاً: حرب المعلومات الشخصية (التجسس الإلكتروني):

التجسس الإلكتروني (Cyber espionage): هو القيام باختراق شبكة أو جهاز إلكتروني؛ بهدف سرقة المعلومات المخزّنة فيه، والتي عادة ما تكون على درجة كبيرة من الأهمية، سواء أكانت معلومات عسكرية، أم اقتصادية، أم صناعية، أم تجارية، أم غيرها، وهو ما يترتب عليه آثار إستراتيجية فادحة في الطرف المستهدف[14].

ويوصف هذا المستوى بأنه تجاوز لحدود الخصوصية الإلكترونية الفردية؛ مما يشكل اعتداء على الحقوق الشخصية للفرد، وانتهاكًا لحرمة الحياة الخاصة، ومنها سرقة البيانات المالية ونشرها عبر الشبكة الإلكترونية للمعلومات: (الإنترنت)، أو قيام أحد الأشخاص بتكوين ملف عن طريق الحاسب الآلي، يحتوي على معلومات تخص شخصًا آخر بغير علمه أو إذنه، أو العبث بالسجلات الرقمية، وتغيير مدخلاتها المخزونة في قواعد البيانات[1].

ولأن هذه الهجمات تستطيع إحداث خسائر كبيرة في وقت محدود، أصبحت العديد من الدول تلجأ إليه، إما في خلال أوقات النزاعات السياسية والتوتر السياسي مع دول أخرى، وإما في وقت الحروب بالتزامن مع العمليات العسكرية التقليدية، ومن أبرز أمثلة التجسس الإلكتروني الذي تقوم به دول ضد أخرى، ما ورد في تقرير لجنة التحقيقات التي شكّلها البرلمان الأوروبي في عام (2001م)، والذي اتهم الولايات المتحدة باستخدام شبكة تجسس إلكترونية تحت اسم (Echelon network)، والتي تأسست أثناء الحرب الباردة؛ للتجسس، وسرقة المعلومات الصناعية الخاصة بالصناعات الأوروبية[51].

وتجدر الإشارة إلى أن الدول ليست هي الهدف الوحيد لمثل هذه الهجمات، وإنما أيضًا الشركات سواء أكانت التجارية أم الإعلانية، والمنظمات غير الحكومية، التي أصبحت تتعرض هي الأخرى للعديد من عمليات التجسس الإلكتروني، وهذا ما سيتم شرحه لاحقًا.

ثانياً: حرب المعلومات بين الشركات والمؤسسات:

وهذا المستوى يدور ضمن إطار المنافسة بين الشركات والمؤسسات، قِوامها استباق كل شيء لتعطيل المنافس، وتهديد أسواقه، بحيث تقوم شركة معينة باختراق النظام المعلوماتي لمنافستها، وسرقة نتائج أبحاثها وتفاصيلها، وتدمير البيانات الخاصة بها، واستبدالها ببيانات أخرى غير صحيحة[1].

ثالثاً:حرب المعلومات العالمية (الحرب السيبرانية):

تشير الحرب الإلكترونية، أو الحرب السيبرانية، إلى تلك الحرب التي تتم إدارتها في مجال الفضاء الإلكتروني، والتي يتم فيها استخدام الآليات والأسلحة الإلكترونية في الهجوم، ويكون هذا الهجوم موجه بالأساس إلى أجهزة الحاسب الآلي، أو الشبكات الإلكترونية الخاصة بالعدو، أو الأنظمة الإلكترونية التي تدير الدولة، وما تحتوي عليه من معلومات؛ بهدف عرقلة الخصم عن استخدام هذه الأنظمة، والأجهزة، والشبكات، أو تدميرها بالكامل[14].

وهذا المستوى يمثل الحروب التي تحصل بين بعض الدول، أو الذي قد تشنه القوى الاقتصادية العالمية على بلدان بعينها؛ بغية سرقة أسرار الخصوم أو الأعداء، وتوجيه تلك المعلومات توجيهًا مضادًا لمصالحهم، حيث إن الدولة التي تمتلك هذه التكنولوجيا تحظى بالتفوق في ميدان المعركة؛ من خلال استخبارات نوعية وشاملة، وقدرة هجومية دقيقة وخاطفة، وقدرة على الدفاع عن بنيتها التحتية الحيوية، إلى جانب قدرات عالية على السيطرة والتحكم وما يتبع ذلك، إلا أن التطور في مجال تكنولوجيا المعلومات، وعلى وجه الخصوص الحواسيب، ووسائل الاتصال، والشبكات الإلكترونية، جعل من الممكن القيام باستهداف الخصم فردًا أو دولة أو مؤسسة، بأساليب جديدة تلائم طبيعة ذلك التطور[1].

وبنحوٍ عام يمكن تحديد ثلاثة مستويات رئيسة للحرب السيبرانية أو الهجمات السيبرانية، **المستوى الأول:** ويتمثل في تلك العمليات المصاحبة للحروب التقليدية؛ لتحقيق التفوق المعرفي، كمهاجمة نظام الدفاع الجوي، والذي يؤدي إلى خسائر إستراتيجية واسعة النطاق نتيجة لأهمية الدفاع الجوي بالنسبة للدول، **أمّا المستوى الثاني:** فيتمثل في الحرب الإلكترونية المحدودة، والتي تتعرض فيها البنية التحتية، والأهداف المدنية للهجمات السيبرانية، و**المستوى الثالث:** ويتمثل في الحرب الإلكترونية غير المحدودة، والتي يسعى من خلالها القائم بالهجوم إلى تعظيم الآثار التدميرية للبنية التحتية، حيث يؤثر سلبًا في البناء الاجتماعي للدولة، كمهاجمة أسواق رأس المال، وخدمات الطوارئ، والأنظمة الإلكترونية الخاصة بمولدات الطاقة، وغيرها من الأهداف التي يترتب عليها آثار تدميرية واسعة النطاق، ويكون الهدف من هذا النوع من الحروب، هو توسيع نطاق الخسائر المادية قدر الإمكان[50].

وعليه، فإن الهجمات السيبرانية تستهدف معلومات أو نظم معلومات محددة عند الطرف المراد مهاجمته؛ وذلك لزيادة قيمة تلك المعلومات أو نظمها بالنسبة للمهاجم، أو تقليل قيمتها بالنسبة للمدافع، أو بهما معًا، وذلك لأن قيمة المعلومات ونظمها هو المقياس لمقدار

استحواذ المهاجم أو المدافع للمعلومات ونظمها، على أن الهدف الذي يسعى المهاجم في حربه لتحقيقه قد يتشكّل ضمن أهداف مالية، كأن يقوم بسرقة وبيع سجلات لحسابات مصرفية، وقد تكون تلك الحرب لأهداف سياسية، أو عسكرية، أو حتى لمجرد الإثارة وإظهار القدرات، كما في حالة قراصنة المعلومات[7].

وسائل الهجمات السيبرانية(الأسلحة الإلكترونية):

تشير الأسلحة الإلكترونية، أو وسائل الهجمات السيبرانية، إلى تلك الأدوات التي يتم استخدامها للتهديد لإحداث الضرر المادي أو الوظيفي للأجهزة أو النظم والهياكل الإلكترونية، وتختلف هذه الأسلحة والأدوات من حيث درجة خطورتها وتعقيدها، وتتراوح ما بين أسلحة بسيطة قادرة على إحداث ضرر خارجي بالنظام الإلكتروني دون اختراقه، وأخرى معقدة يمكن من خلالها اختراق النظام، واختراق النظم، وإحداث أضرار بالغة به قد تصل إلى تدميره كليًّا، أو توقفه عن العمل كليًّا[14].

وفي النقاط الآتية، سيتم توضيح أبرز الوسائل التي تعد أسلحةً للحرب السيبرانية، والتي تُعدّ الأكثر استخدامًا على الساحة الدولية، وذلك على النحو الآتي:

1- **استخدام برامج القنابل المنطقية (Logic Bombs)**

وتعد بمثابة برنامج ينفذ في لحظة محددة، أو في فترة زمنية منتظمة، ويتم وضعه في شبكة معلوماتية بهدف تحديد ظروف أو حالة مضمون النظام؛ بغية تسهيل تنفيذ العمل غير المشروع، كإدراج تعليمات في نظام التشغيل للبحث عن عمل معين يكون محلًّا للاعتداء، كأن تسعى قنبلة منطقية إلى البحث عن حرف (A)، في أي سجل يتضمن أمرًا بالدفع، وعندما تكتشفه، تحرك متتالية منطقية تعمل على إزالة هذا الحرف من السجل[25].

2- **استخدام برامج الدودة (Worm Software)**

وهذه البرامج تعرف بأنها تستغل أيّة فجوات في نظم تشغيل الحاسب الآلي، لتنتقل من حاسب إلى آخر، مغطية شبكة بأكملها؛ لتحدث آثارًا تخريبية للملفات، والبرامج، ونظم التشغيل، وبروتوكولات الاتصال[25].

3- **استخدام فيروسات الحاسب الآلي (Programs Virus)**

وهذه تعد من أكثر الوسائل انتشارًا، وهي بمثابة مجموعة من التعليمات المرمّزة، التي تنتج لنفسها نسخًا مطابقة تلحق من تلقاء ذاتها ببرامج التطبيقات، ومكونات النظام المنفذ، لتقوم في مرحلة محمية بالتحكم في أداء النظام الذي أصابته. وقد عرّفه المركز القومي للحاسب الآلي في الولايات المتحدة الأمريكية بأنه: "برنامج مهاجم يصيب أنظمة الحاسبات، بأسلوب يماثل إلى حدٍ كبير أسلوب الفيروسات الحيوية التي تصيب الإنسان، حيث يقوم هذا البرنامج بالتجول في الحاسب الآلي باحثًا عن برنامج غير مصاب، وعندما يجد أحدها ينتج نسخة من نفسه لتدخل فيه، حيث يقوم البرنامج المصاب فيما بعد بتنفيذ أوامر الفيروس، ومن أهم خصائصه قدرته الفائقة على الاختفاء، والانتشار، والاختراق، وقدرته على تدمير نظام الحاسب الآلي بأكمله[25].

4- **هجمات إنكار الخدمة : (Denial of Service (Dos**

وهي عبارة عن هجمات إلكترونية تتم بإغراق المواقع بسيل من البيانات غير اللازمة، التي يجري إرسالها ببرامج متخصصة تعمل على نشرها، فتؤدي إلى بطءٍ في الخدمات أو ازدحامٍ في المرور على هذه المواقع؛ فيصعب بالتّالي وصول المستخدمين إليها[2].

5- **الهجوم الإلكتروني:**

كالتشويش، والخداع الإلكتروني، والصواريخ المضادة للإشعاع الكهرومغناطيسي، والقيام بالتجسس على الهدف؛ لسرقة معلومات سرية، بغض النظر عن الأهداف، والتي قد تكون اقتصاديّة كالتجارة بين الشركات، أو إستراتيجية أو عسكرية بين دولٍ معينة، ومن تلك العمليات أيضًا التعدي على الملكية الفكرية، وقرصنة المعلومات، كسرقة البرامج الحاسوبية، وتوزيع مواد مكتوبة أو مصورة بدون إذن المالك الشرعي، خاصة وأن وجود شبكة الإنترنت قد أدى إلى توسيع انتشار مثل تلك العمليات؛ لسهولة النشر والتوزيع على هذه الشبكة[1].

وبصفة عامة يمكن تحديد مجموعة من الخصائص التي تتسم بها وسائل السيبرانية وأسلحتها، بأنواعها المختلفة، ويمكن تحديد هذه الخصائص بما هو آتٍ:

- تتسم وسائل السيبرانية وأسلحتها بخضوعها لعمليات تحديث وتطوير مستمرين؛ مما يزيد في قدرتها التدميرية، وفاعليتها في شنّ الهجمات الإلكترونية.
- سهلة الاستخدام ومتوفرة على نطاق واسع، بحيث يمكن تحميلُها من الإنترنت أو شراؤها، وتمكّن مستخدميها من القيام بهجمات معقدة تتخطى مستوى قدراتهم الحقيقية.
- تتسم بدقتها وفاعليتها وقدرتها على اختراق أكثر أنظمة الحماية تعقيدًا، كما أنها قادرة على إصابة أنواع مختلفة من الأجهزة الإلكترونية، سواء أكانت أجهزة الحاسب الآلي، أم مقدم الخدمة، أم أي جهاز متصل بشبكة إلكترونية[9].

المبحث الثاني:

التكييف القانوني للهجمات السيبرانية:

يعدّ ظهور شبكة الإنترنت وتوسّعها على الصعيد العالمي سببًا في حدوث أسرع ثورة تكنولوجية وأقواها في التاريخ البشري، إذ إنه في غضون العقدين الماضيين، ارتفع عدد الأفراد الذي يستخدمون الإنترنت من (16) مليون شخص في عام (1995م)، إلى أكثر من(1.8) بليون في أواخر عام (2016م)، وبفعل تلك الثورة أصبحت

الدول والمجتمعات غير الحكومية، والأعمال التجارية، والأوساط الأكاديمية، والأفراد، مترابطة إلى حد لا يمكن تخيله من قبل، وفي الوقت نفسه ازداد الاعتماد العسكري على أنظمة الحواسيب وشبكاتها زيادة هائلة؛ مما فتح المجال "الخامس" من القتال الحربي إلى جانب المجالات المعترف بها تقليديًّا: الأرض، والبحر، والجو، والفضاء الخارجي[32].

فأصبح العالم في الفترة الأخيرة يواجه نوعًا جديدًا من الحروب والهجمات الدولية، والتي تُعرف بالحروب والهجمات السيبرانية، والتي تتراءى مختلفة عن الحروب العسكرية، وتختلف عن الجرائم الإلكترونية التي يكون هدفها تجاريًّا، فالهجمات السيبرانية أهدافها سياسية، وخير دليل على ذلك "فيروس ستكسنت 2007" الذي غير مسار التاريخ السيبراني، حيث كان ذلك الفيروس أكبر مثال على الهجمات السيبرانية في الفترة الأخيرة، حيث ضرب المؤسسة النووية الإيرانية من قبل وكالتي الاستخبارات الأمريكية والإسرائيلية، إضافة إلى ذلك، فإن الجماعات الإرهابية لم تغفل عن الفضاء السيبراني، فقد جعلوه وسيلة سهلة للتواصل مع الأفراد والجماعات الأخرى حول العالم، ووسيلة لتنفيذ هجماتهم ومخططاتهم[36].

وهذا الاتجاه من التطورات التي أحدثها الفضاء السيبراني على الساحة الدولية، يثير التساؤل إلى أي مدى يمكن أن يكون القانون الدولي قائمًا ويمكن نقله إلى المجال السيبراني؟ وذلك من حيث المبدأ، بأن القانون الدولي القائم يحكم أنشطة الدولة أينما كانت بما في ذلك الفضاء السيبراني. ومع ذلك، فإن تطبيق القواعد القانونية الموجودة مسبقًا، والمفاهيم والمصطلحات إلى تكنولوجيا جديدة قد تنطوي على بعض الصعوبات، في ضوء الخصائص المتميزة للفضاء السيبراني، لذلك سيتم توضيح التكييف القانوني للهجمات السيبرانية، من خلال هذا مبحث، فضلًا عن كشف مدى مواءمة القانون الدولي ككل على تلك الهجمات، ثم بيان الصعوبات التي تواجه التكييف القانوني لهذه الهجمات، وذلك على النحو الآتي:

المطلب الأول: الوصف القانوني للهجمات السيبرانية:

تشكل الهجمات السيبرانية تهديدًا لأحد المبادئ الرئيسة في القانون الدولي، وهو احترام سيادة الدول، بوصفه واجبًا أساسيًّا، وهو واجب "عدم التدخل"، الذي نصت عليه الفقرة (4) من المادة الثانية من ميثاق الأمم المتحدة، لما فيها من تسريب لمعلوماتٍ أمنية وسرية عن حكومات الدول، وقد يتجاوز الأمر ذلك ويصل إلى الإضرار بالمدنيين؛ عندما تسبب مثل هذه الهجمات قطعًا للخدمات الحيوية كالماء والكهرباء، ولذلك فقد عرّف القانون الدولي الإنساني هذا الهجوم بأنه: "عملية إلكترونية سواء أكانت هجومية أم دفاعية، يتوقع أن تتسبب في إصابة أو قتل أشخاص أو الإضرار بالمنشآت أو تدميرها[36]".

لهذا فإن وضع الهجمات السيبرانية في الإطار القانوني الدولي القائم –على افتراض أنها مناسبة لهذا الغرض– أمر صعب جدًا، وذلك بسبب الطبيعة الخاصة لها، والخصائص الفريدة من نوعها التي تتميز بها الهجمات السيبرانية، إضافة إلى عدم وجود بيان قانوني رسمي ونهائي بشأن هذه المسألة، كل ذلك يجعل التساؤل قائمًا حول أي أنموذج قانوني يجب أن يضمّ إطار الهجمات السيبرانية؟ والحقّ إن هذا التّساؤل في حد ذاته مسألة نقاش كبيرة جدًا، ومحل اختلافات شائكة في مجال الحقوق القانونية والمسؤوليات التي تنتج عن تلك الهجمات[46].

كما أن تقييم مشروعية الأسلحة الجديدة يصب في مصلحة كافة الدول، حيث إنه يساعدها في ضمان توافق سلوك قواتها المسلحة مع الالتزامات الدولية، إذ تُلزم المادة (36) من البروتوكول الإضافي الأول لعام (1977م) كل دولة من الدول الأطراف التحقق من امتثال أي أسلحة جديدة تقوم بنشرها، أو تدرس مسألة نشرها لقواعد القانون الدولي الإنساني، كما طالبت الدول الأطراف في اتفاقيات جنيف أثناء المؤتمر الدولي الثامن والعشرين للصليب الأحمر والهلال الأحمر المنعقد عام (2003م)، بأن تخضع جميع الأسلحة الجديدة، ووسائل الحرب الجديدة وأساليبها "لاستعراض دقيق ومتعدد التخصصات"؛ وذلك لضمان ألّا يتخطى تطور التكنولوجيا الحماية القانونية المكفولة. ويُعَد استخدام العمليات السيبرانية أثناء النزاعات المسلحة، مثالاً جيدًا على هذا التطور التكنولوجي[38].

المطلب الثاني: التكييف القانوني للهجمات السيبرانية:

وفي مجال التكييف القانوني للهجمات السيبرانية، اختلفت الآراء بشأن ذلك، إذ يرى جانب من الفقه بأن المدة التي جرى فيها تقنين القواعد القانونية ذات الصلة باستخدام وسائل وطرائق القتال، لم يكن لاستخدام الأنظمة الإلكترونية للأغراض العسكرية أي وجود، أي أنها غير مقننة في الأصل، وأنها غير منظمة وفقًا للقواعد الدولية المتعارف عليها، كما يشير هذا الفريق إلى مدة إبرام الاتفاقيات، وذلك في منتصف القرن الثامن عشر وما بعدها، والمتمثلة باتفاقية لاهاي عام (1899–1907)، واتفاقيات جنيف الأربع لعام (1949)، والبروتوكولين الإضافيين لعام (1977)، حيث لم يكن للهجمات السيبرانية أي ذكر لذلك لا وجود لأي أساس قانوني للهجمات السيبرانية في أغلب قواعد القانون الدولي[47].

ومن الجانب الآخر، يرى[26] أن الهجمات السيبرانية لا تُكيَّف في ظلّ أحكام القانون الدولي الإنساني والجنائي فحسب، وإنما في ظلّ أحكام القانون الدولي العام ككل، على أساس أن الصورة الأولية تظهر أن تلك الهجمات يمكن أن ترتكب أثناء النزاعات المسلحة الدولية أو غير الدولية، وفي أوقات السلم أيضًا، حيث يرى هذا الجانب بأن المبادئ والقواعد التي أرساها القانون الدولي الإنساني، تنطبق على

تلك الهجمات، وأن تكييف استخدام الهجمات السيبرانية القانوني يدور في فرضيتين اثنتين:

الفرضية الأولى: عدم القدرة على إثبات الدليل المادي الناجم عن استخدام الهجمات السيبرانية، وهو العائق الأكبر الذي يواجهه المختصون، على عكس وسائل القتال الأخرى وطرقها المعروفة، والتي تترك أثرًا ماديًّا مباشرًا أو غير مباشر بعد الهجوم، كالدمار، أو التعطيل الجزئي أو الكلي الذي تتعرض له المواقع العسكرية أو المدنية، أو عمليّات القتل والإصابة التي تصيب المقاتلين أو المدنيين[26].

الفرضية الثانية: إذا ثبت أن الهجمات السيبرانية قد تؤدي إلى آثار مادية ملموسة على المستويات الاقتصادية والأمنية والعسكرية كافة، هنا يكون المعيار في تكييف الهجمات السيبرانية، فيما إذا كانت من قبيل التصرف العدائي، أو كونها تصرفًا لرد العدوان، حيث تعتمد بدرجة أساسية على القواعد القانونية ذات الصلة، وبالذات حكم الفقرة (4) من المادة(2) والمادة (51) من ميثاق الأمم المتحدة، والتي ترتب آثارًا قانونية عند اللجوء إليها[33].

كما يعد "دليل تالين" أول محاولة منهجية شاملة للبحث في التكييف القانوني للهجمات السيبرانية، إلا أنه وثيقة غير ملزمة أعدتها مجموعة من الخبراء، لكنه ساهم بشكل مفيد في النقاش بين الدول حول هذه المواضيع المثيرة للتحديات، وكيفية تفسير القانون الدولي، بما في ذلك القانون الدولي الإنساني، وكيفية تطبيقه على أنشطة الدول والأطراف من غير الدول في الفضاء الإلكتروني، إذ يقدم "دليل تالين" رؤى مثيرة للاهتمام في هذا الصدد، فهو يتمسك –على سبيل المثال– بالثنائية التقليدية للنزاعات المسلحة الدولية، والنزاعات المسلحة غير الدولية، ويقر بأن العمليات الإلكترونية وحدها قد تشكل نزاعات مسلحة تبعًا للظروف لا سيما الآثار المدمرة لتلك العمليات، كما يقدم الدليل في هذا الصدد تعريفًا "للهجوم السيبراني"، بموجب القانون الدولي الإنساني بوصفه "عملية إلكترونية سواء أكانت هجومية أم دفاعية، يتوقع أن تتسبب في إصابة أو قتل أشخاص أو الإضرار بأعيان أو تدميرها"[35].

المبحث الثالث:

المسؤولية الدولية للهجمات السيبرانية:

تعد المسؤولية الدولية من أهم موضوعات القانون الدولي في الوقت الحاضر، فعند النظر إلى التطورات العلمية الحديثة التي أثرت تأثيرًا بالغًا على العلاقات الدولية، نجد أنه ظهرت مشكلات جديدة لم تتناولها قواعد القانون الدولي بالتنظيم؛ مما أدى إلى ضرورة معالجة هذه المشكلات بطريقة جديدة تتلاءم مع طبيعتها، إضافة إلى ذلك فإن قواعد المسؤولية الدولية يكتنفها الغموض وعدم الوضوح بشكل عام[29]، وبشكل خاص فيما يتعلق بالهجمات السيبرانية، وما ينتج عنها من أضرار، ومدى خضوعها لقواعد القانون الدولي، وعليه سيتم التطرق إلى المسؤولية الدولية للهجمات السيبرانية من خلال المطلبين الآتيين:

المطلب الأول: أركان المسؤولية للهجمات السيبرانية:

هنالك تشابه بين النظام القانوني الداخلي والنظام القانوني الدولي، فإذا كان شخص النظام القانوني الداخلي الفرد، فإن النظام القانوني الدولي له أشخاصه الخاصون ومنهم الدول، فيفرض النظام القانوني الدولي التزامات على أشخاصه، كما يرتب لهم حقوقًا، فالدولة التي تقوم بأي فعل من شأنه إحداث ضرر يصيب دولة أخرى أو عدة دول، فتتحمل الدولة التي أحدثت ذلك الضرر، أو تسببت في إحداثه، تبعات المسؤولية الدولية عن ذلك الفعل، فالهجمات السيبرانية يقوم بها أشخاص يخضعون للقانون الدولي، وتؤدي إلى أضرار، وبذلك تكون الهجمات السيبرانية مستوفية شروطَ قيام المسؤولية الدولية، لكن لنقص القواعد القانونية، وصعوبة إثبات مصدر تلك الجهات؛ فإنه يتعذر ذلك[2].

أركان المسؤولية الدولية للهجمات السيبرانية، والتي تتمثل هي على النحو الآتي:

1- **نسبة الفعل إلى الدولة:** فلا يكفي القول بوجود المسؤولية أن يكون الفعل ضارًا، أي أنه فعل غير مشروع، بل يجب أن يستند الفعل إلى دولة، ففي التشريعات الداخلية يشترط القانون إسناد الفعل إلى شخص ما لإمكان قيام المسؤولية في مواجهته، أي أنه لا يكفي أن يكون العمل منسوبًا إلى دولة ما، بل يجب أن تكون هذه الدولة تامة السيادة، بمعنى أن تكون الدولة دولة مستقلة تامة الأهلية أو السيادة، لكي تُسأل عن أعمال سلطاتها الثلاث: (التشريعية والتنفيذية والقضائية)، وتسأل في بعض الأحيان عن أعمال الأفراد العاديين، أو الموظفين الرسميين، وبهذا فإن الدولة المنضمّة إلى دولة اتحادية لا تسأل عن أعمالها؛ لأنه لم تعد من أشخاص القانون الدولي العام، كما أن الدولة المنقوصة لا تسأل عن أعمالها، لأنها لا تمارس حقوق الدولة التامة الأهلية[5].

وفي حالة الهجمات السيبرانية، نجد أن الضرر يتحقق بمجرد إطلاق تلك الهجمات، خاصة وأن تلك الهجمات تستهدف البنى التحتية للدولة مما قد يخلف أضرارًا كبيرة، وأن من يقوم بهذه الهجمات هي الدول المتقدمة التي تمتلك قوة إلكترونية كبيرة، وقد تقوم بهذه الهجمات أطراف عديدة خاصة في ظل الانتشار الإلكتروني وسهولة الوصول إليه، وزيادة الاعتماد الدولي على الفضاء السيبراني، فقد تقوم بهذا الهجمات الدول القومية، أو المنظمات الحكومية سواء أكانت عالمية أم إقليمية، أو بعض الأفراد ممن تهيأت لهم دون غيرهم

إمكانية التحرك على قاعدة واسعة نسبيًّا من الاتصالات الدولية، أو الجماعات الإرهابية والمتمرّدون، وحركات التحرر الوطني، وفي المجمل نجد أن هؤلاء الفاعلين ينطبق عليهم الركن الأول، وهو نسبة الفعل إلى الدولة، وذلك لأن الدول تسأل عن أفعال رعاياها في حالة التقصير[2].

2- **أن يكون الفعل غير مشروع دوليًّا:** فالفقه الدولي أجمع بأن الفعل غير المشروع، هو ذلك الفعل الذي يعد انتهاكًا لأحكام القانون الدولي، إذ هو الفعل الذي يتضمّن مخالفة لقواعد القانون الدولي، أو مخالفة مبادئ القانون العامة، فالفعل غير المشروع دوليًّا هو السلوك المنسوب إلى الدولة وفقًا للقانون، والذي يتمثل في القيام بفعل، أو امتناع عن القيام بفعل، يشكّل مخالفة لأحد التزاماتها الدولية، فمعيار عدم المشروعية هو معيار دولي موضوعي، لا عبرة فيه لمنشأ الالتزام، لأن مخالفة أي التزام دولي أيًّا كان مصدره، تولد المسؤولية الدولية دون النظر لوصف الفعل في القانون الداخلي، كما لا يعتد بالوسيلة التي يتحقق بها انتهاك القانون الدولي، سواء أكان ذلك بفعل أم امتناع عن فعل، أم إهمال[16].

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

3- **الضرر:** يعد عنصر الضرر أهم عنصر من عناصر المسؤولية؛ لأنه إذا انعدم الضرر انعدمت المسؤولية، وللضرر أنواع، تقسّم تبعًا لمصلحة المعتدى عليه، أو للجهة التي لحقها الضرر:(ضرر مباشر، وضرر غير مباشر)، فمن حيث مصلحة المعتدي عليه ينقسم الضرر نوعين، أولهما: الضرر المادي، وهو كل مساس بحق من حقوق الشخص القانوني الدولي المادية، أو بحقوق رعاياه؛ مما يترتب عليه أثر ملموس ظاهر للعيان، ويكون مباشرًا. والثّاني الضرر المعنوي: وهو كل مساس بشرف أو اعتبار الشخص الدولي، أو بأحد رعاياه، أي أن الضرر المعنوي هو كل اعتداء على حق من حقوق الأشخاص الدوليين أو رعاياهم، وتترتب عيه آثارٌ غير ملموسة[16].

وعند التطبيق على الهجمات السيبرانية، نجد أن الضرر بكافة أشكاله يتحقق من تلك الهجمات، سواء أكان الفاعل دولاً قومية، كما حصل في الهجوم الفيروسي على البرنامج النووي الإيراني، أو ما تقوم به منظمات إجرامية تلحق أضرارًا فادحة بالآخرين، خاصة في الهجمات التي تهدف لسرقة المعلومات، أو اختراق حسابات بنكية، وسرقة أرقام بطاقات الائتمان، حيث تكلّف تلك الهجمات أكثر من تريليون دولار سنويًّا، لكن على الرغم من توافر أركان المسؤولية الدولية في الهجمات السيبرانية، إلا أن الكشف عن هوية الفاعلين ومراقبتهم وتتبعهم؛ من أجل تقديمهم للمحاكمة، تكون مصحوبة بالصعوبة البالغة؛ لما يتمتع به الفضاء السيبراني من قابلية التخفي[31].

المطلب الثاني: الاتجاهات الدولية في مكافحة الجريمة السيبرانية:

تعتمد الجرائم السيبرانية على تقنيات عالية التقدم، وكلما زاد التطور التكنولوجي، زادت نسبة هذا النوع من الجرائم، ففي ظل هذه الثورة المعلوماتية، لم يعد يقتصر ارتكاب الجرائم السيبرانية على المجالين العسكري أو السياسي، بل تعداه إلى المجالات الاقتصاديّة والتجاريّة والثقافيّة، وقد تزايدت هذه الجرائم في العقود الأخيرة، وبالأخص بعد أحداث الحادي عشر من سبتمبر التي شهدتها الولايات المتحدة الأمريكية، مما تطلب ذلك الوضع جهودًا دولية، ووضع سياسة دولية لمكافحة مثل هذه الجرائم[8].

أولاً: أوجه التعاون الدولي في مكافحة الجريمة السيبرانية:

يعد ظهور الحاسب الآلي والإنترنت من أهم إنجازات العلم الحديث في هذا العصر، وأعظمها جدوى للإنسان، حيث قدمت هذه الإنجازات: (الحاسب الآلي والإنترنت)، خدمات للإنسانية في أغلب مناحي الحياة الاقتصادية، والتعليمية، والطبية، والعديد من المجالات الأخرى.

ولكن رافق هذه الإنجازات بروز خبراء جدد يتمتعون بالخبرة والحرفية في تطويع هذه التقنية؛ للقيام بأعمال إجرامية، مما أدى ذلك إلى ظهور جرائم عصرية تقنية إلى جانب الجريمة التقليدية، بل إنها حولت الجريمة من صفتها العادية، وأبعادها المحدودة، إلى أبعاد جديدة تعتمد التقنية في تنفيذ الفعل الإجراميّ، وبأساليب مبتكرة وطرق جديدة لم تكن معروفة من قبل، وقد استفاد هؤلاء المجرمون من تطور الوسائل المعلوماتية الحديثة، في زيادة سرعة نشر جرائمهم، حتى- أصبحت تهدد النظام المعلوماتي، بل أصبح في إمكانهم التسبب في خلق شلل كامل للأنظمة المدنية والعسكرية، الأرضية والفضائية، - وتعطيل المعدات الإلكترونية، واختراق النظم المصرفية، وإرباك حركة الطيران، وشلّ محطات الطاقة وغيرها؛ بواسطة قنابل معلوماتية ترسلها لوحة مفاتيح الكمبيوتر من على مسافات تتعدى عشرات الآلاف من الأميال، مما جعل الجريمة السيبرانية جريمة دولية عابرة للحدود[17].

فأدت هذه الجرائم إلى ظهور تحديات جديدة للمنظومة القانونية على المستوى الدولي، خاصة بعدما ألقت الجريمة السيبرانية بظلالها على العالم بأسره، لذا تضافرت الجهود الدولية من أجل مكافحة هذه الظاهرة بنجاعة وفاعلية، كان أولها الجهود المبذولة على صعيد الهيئات الدولية التي أدّت دورًا ملحوظًا في هذا المجال، وعلى رأسها

منظمة الأمم المتحدة التي بذلت جهودًا كبيرة في مجال مكافحة الجرائم السيبرانية، والحث على التعاون الدولي؛ من أجل الحد من انتشار هذا النوع من الجرائم[19].

وقد تُرجمت هذه الجهود من خلال المؤتمرات الدولية لمنع الجريمة ومعاملة المجرمين، بدءًا من المؤتمر السابع عام (1985م)، حتّى المؤتمر الثاني عشر عام (2012 م)، إضافة إلى المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات، تحت إشراف الأمم المتحدة عام (1994م)، والذي نتج عنه عدة توصيات وقرارات ذات صلة بالجرائم السيبرانية والجرائم المعلوماتية، إذ تضمنت تلك التوصيات والقرارات جانبين، الأول جانب موضوعي: يتناول الأفعال التي تقع تحت طائلة الإجرام المعلوماتي، وجانب ثانٍ إجرائي: يتضمن الإجراءات الواجب اتباعها لتطبيق القواعد الموضوعية على الجرائم المعلوماتية[17].

كما يعد القرار الصادر عن مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء (هافانا_1990م)، بشأن الجرائم ذات الصلة بالكمبيوتر، من الجهود التي بذلتها الأمم المتحدة في هذا الميدان؛ حيث حثّ في قراره المتعلق بالجرائم ذات الصلة بالكمبيوتر الدول الأعضاء، أن تكثف جهودها لمكافحة إساءة استعمال هذا الجهاز، وتجريم تلك الأفعال جنائيًّا، كما حث الدول الأعضاء على مضاعفة الأنشطة التي تبذلها على الصعيد الدولي؛ من أجل مكافحة الجرائم المتصلة بالكمبيوتر، بما في ذلك دخولها كأطراف في المعاهدات المتعلقة بتسليم المجرمين، وتبادل المساعدة في المسائل الخاصة المرتبطة بهذه الجريمة، وحث هذا القرار الدول الأعضاء بالعمل على أن تكون تشريعاتها ذات العلاقة بتسليم المجرمين، وتبادل المساعدة في المسائل الجنائية، تنطبق بشكل تام على الأشكال الجديدة للإجرام، مثل الجرائم الإلكترونية، وأن تتخذ الدول الأعضاء خطوات محددة نحو تحقيق هذا الهدف[11].

كما تم الاتفاق بين الدول على إصدار قانون (الأونستيرال النموذجي)، وذلك اقتناعًا من الدول بضرورة منع هذه الجرائم ومكافحتها، خاصة وأن ذلك يتطلب استجابة ديناميكية في ضوء الطابع الدولي لإساءة استخدام الكمبيوتر والجرائم المتعلقة به، إذ تم صياغة قانون الأونيسترال النموذجي بشأن التجارة الإلكترونية، وقانون آخر بشأن التوقيعات الإلكترونية (2001م)[18].

إضافة إلى الجهد الكبير المبذول من قبل الاتحاد الدولي للاتصالات، في إطار برنامج الأمن المعلوماتي العالمي المعلن عنه من قبل الأمين العام للاتحاد عام (2007م)، والذي يرمي إلى تحقيق عدة أهداف أبرزها استحداث تشريع أنموذجي لمكافحة الجريمة المعلوماتية، يمكن تطبيقه عالميًّا، ويكون قابلًا للاستخدام، مع التدابير التشريعية القائمة على الصعيدين الوطني والإقليمي[13].

وعلى الصعيد الإقليمي، فهناك جهود كبيرة من قبل المنظمات الإقليمية، فقد كان للاتحاد الأوروبي دور فاعل في هذا المجال، حيث أثمرت جهوده عن أولى المعاهدات الدولية الخاصة بمكافحة الجرائم السيبرانية والجرائم المعلوماتية، فقد تم عقد اتفاقية في الاتحاد الأوروبي عام (2001م)، في العاصمة المجرية بودابست، وقد سعت هذه الاتفاقية إلى بناء سياسة جنائية مشتركة؛ من أجل مكافحة الجرائم المعلوماتية والسيبرانية في جميع أنحاء العالم، من خلال تنسيق وانسجام التشريعات الوطنية مع بعضها بعضًا، وتعزيز قدرات القضاء، وكذلك تحسين التعاون الدولي في هذا الإطار، إضافة إلى تحديد عقوبات الجرائم السيبرانية في إطار القوانين المحلية، كما أنشأ الاتحاد الأوروبي أجهزة تساعد على مكافحة هذا النوع من الجرائم، من بينها جهاز اليوروبول، والمركز الأوروبي لمكافحة الجريمة المعلوماتية[12].

وعلى الصعيد العربي، فقد بذلت جهود كبيرة في مكافحة الجرائم السيبرانية والإلكترونية، أسفرت عن وضع اتفاقية عربية لمكافحة جرائم تقنية المعلومات، والتي انبثقت عن الاجتماع المشترك لمجلس وزراء الداخلية والعدل العرب، الذي عُقد بمقر الأمانة العامة لجامعة الدول العربية في عام (2010م)؛ بهدف تعزيز التعاون بين الدول العربية في مكافحة جرائم تقنية المعلومات، والجرائم السيبرانية التي تهدد أمنها ومصالحها وسلامة مجتمعاتها، وتلبية الحاجة إلى تبنّي سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد جرائم تقنية المعلومات، وقد جاءت هذه الاتفاقية من منطلق الالتزام بالمعاهدات والمواثيق العربية والدولية المتعلقة بهذا الشأن[20].

ثانيًا: التعاون القضائي الدولي في مجال مكافحة الجرائم السيبرانية:

أولى الفقهُ الجنائي الدولي، التعاونَ القضائي اهتمامًا بالغًا لتحقيق القدرة على التصدي للإجرام، وسد أوجه القصور القانوني التي ساعدت المنظمات الإجرامية على اختراق النظم القانونية، وتعد المساعدة القضائية المتبادلة في المسائل الجنائية، من الآليات الفاعلة لمواجهة الجريمة الدولية[3].

وتقتضي فاعلية التحقيق والملاحقة القضائية في الجرائم السيبرانية–في الغالب– إلى تتبع أثر النشاط الإجرامي من خلال مجموعة متنوعة من مقدمي خدمات الإنترنت، أو الشركات المقدمة لتلك الخدمات مع توصيل أجهزة الحاسب الآلي بالإنترنت، وحتى ينجح المحققون في ذلك فعليهم أن يتتبعوا أثر قناة الاتصالات بأجهزة الحاسب الآلي المصدر والجهاز الخاص بالضحية، أو بأجهزة أخرى تعمل مع مقدّمي خدمات وسطاء في بلدان مختلفة. ولتحديد مصدر الجريمة غالبًا ما يتعين على أجهزة إنفاذ القانون الاعتماد على

السجلات التاريخية، التي تبين متى أجريت تلك التوصيلات؟ ومن أين؟ ومن الذي أجراها؟[42].

وفي أحيان أخرى قد يتطلب إنفاذ القانون تتبع أثر التوصيل ووقت إجرائه، وعندما يكون مقدمو الخدمات خارج نطاق الولاية القضائية للمحقق –وهو ما يحدث غالبًا– فإن أجهزة إنفاذ القانون تكون بحاجة إلى مساعدة من نظرائها في ولايات قضائية أخرى. وبمعنى آخر تحتاج مكافحة الجرائم السيبرانية إلى إيجاد بيئة قانونية قادرة على مواجهة تلك الجرائم، وإنفاذ رجال قانون متخصصين ذوي قدرات، وتدريب، وكفاءة عالية من النيابة العامة والقضاة.

التعاون الأمني في الجرائم السيبرانية على المستوى الدولي:

أثبت الواقع العملي أن أي دولة لا تستطيع بجهودها المنفردة القضاء على الجريمة مع هذا التطور الملموس والمذهل في كافة ميادين الحياة، فنتيجة للتطور الملموس والمذهل في الاتصالات وتكنولوجيا المعلومات، وظهور الإنترنت، والانتشار الواسع والسريع لها، أدى إلى ظهور أشكال وأنماط جديدة من الجرائم، ومنها الجرائم المتعلقة بشبكة الإنترنت أو ما تسمى الجرائم السيبرانية، التي باتت تشكل خطرًا لا على سرية النظم الحاسوبية أو سلامتها أو توافرها فحسب، بل تعدت إلى أمن البنى الأساسية الحرجة، والمنشآت العسكرية والاقتصادية[39].

ومع تميز الجرائم السيبرانية بالعالمية، ولأنها عابرة للحدود، فإن مكافحتها لا تتحقق إلا بوجود تعاون دولي على المستوى الإجرائي الجنائي، بحيث يسمح بالاتصال المباشر بين أجهزة الشرطة في الدول المختلفة، وذلك بإنشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي الجرائم المتعلقة بالإنترنت وتعميمها، خاصة وأن عمليات البحث والتحريات تجاه جمع الأدلة والمعاينة والتفتيش، حتى الوصول إلى مرتكبي الجريمة والبدء في استجوابهم، عمليات معقدة وصعبة لا يقوم بها إلا رجال إنفاذ القانون المؤهلون والمدربون تدريبًا كافياً على الجرائم السيبرانية التي ليس لها وجود في الواقع الملموس، بل لها وجود في الواقع الافتراضي (التخيلي)، وهذا يتطلب معرفة علمية وفنية واسعتين، كمعرفة أسبابها وطبيعتها، فضلًا عن معرفة الأدلّة وكشفها، وتحديد أنواعها، ومعرفة طريقة الوصول إليها، بالإضافة إلى معرفة أسلوب كل فعل من الأفعال غير المشروعة في هذا المجال[15].

وترتكب الجرائم السيبرانية بواسطة استخدام الحاسوب والإنترنت، لذا يتمتع المجرمون السيبرانيون بصفات وخصائص تميزهم عن غيرهم من المجرمين العاديين، وذلك كانعكاس حتمي لما تتطلبه عمليات استخدام هذه الشبكة من قدرات تقنية وفنية هائلة، بيد أن ذلك لا يعني حصر مرتكبي الجرائم السيبرانية في طبقة، أو فئة معينة، أو جنس معين، فمرتكبو الجريمة السيبرانية قد يكونون من البالغين أو الأحداث، سواء أكانوا من المتعلمين أم المثقفين، أو من الفقراء أو الأغنياء[3].

كما أنه لا يمكننا أيضًا أن نحصر جرائم الإنترنت في نوع معين من الجرائم، فقد تكون من الجرائم الماسة بأمن الدولة من الداخل أو من الخارج، وقد تكون من جرائم الاعتداء على الأشخاص، أو جرائم الاعتداء على الأموال، وقد يترتب على نشاط الجاني خسائر مادية غير محدودة، تتجاوز الضرر المترتب على ارتكاب جريمة من الجرائم التقليدية، لذلك فهي تتطلب إجراءات خاصة من قبل الشرطة، ورجال إنفاذ القانون، الذين يباشرون التحقيق في الجرائم السيبرانية، وتتطلب تعاونًا دوليًّا في هذا المجال؛ لأن أغلب الإجراءات تكون مشتركة بين الدول، وحتى لا يعد التحقيق في تلك الجرائم تعديًا على سيادة الدولة[8].

لذلك نجد أن القواعد العامة لاستجواب المتهم في أي جريمة تقليدية، تنطبق على استجواب المتهم من قبل الشرطة في جرائم الحاسب الآلي، لكن الفارق بين الجريمتين يكمن في ضرورة تأهيل السلطة المختصة التي تتولى إجراء الاستجواب، ذلك أن المحقق الجنائي لا بد أن يكون مؤهلًا للتحقيق في الجرائم السيبرانية، حتى يمكن له استيعاب واقعة التحقيق، والتعامل مع مفردات الجريمة ومصطلحاتها، لاسيما وأن المجرم الذي يتولى التحقيق معه ليس مجرمًا نمطيًّا، فالمجرم في الجريمة المعلوماتية له طبيعة خاصة في استخدام تقنيات الحاسب الآلي، وعلى ذلك فالقواعد العامة واحدة في استجواب الجريمة السيبرانية والجريمة التقليدية، ولكن يتعين لنجاح إجراء الاستجواب في الجريمة السيبرانية، ضرورة تأهيل المحقق الجنائي بمفردات الحاسب الآلي وتطبيقاته[41].

وبما أن هناك خصوصية لهذه الجرائم، فإنه يتحتم أن يكون هناك تعاون أمني وشُرطي على المستوى الدولي لمكافحة هذه الجرائم على المستوى الدولي، لأن أي دولة بمفردها لا تستطيع القضاء على الجريمة السيبرانية؛ نظرًا للتطور المذهل والكبير في قطاع الاتصالات وتكنولوجيا المعلومات، وظهور الإنترنت وانتشاره في جميع أنحاء العالم؛ مما أدى ذلك إلى حدوث زيادة كبيرة في الجرائم السيبرانية، وزيادة خطورتها على جميع القطاعات الاقتصادية والاجتماعية والعسكرية، مما يفرض ذلك الواقع حتمية التعاون الأمني لمكافحة الجريمة السيبرانية على المستوى الدولي[15].

لذلك أصبحت الحاجة ماسة إلى وجود كيان دولي يأخذ على عاتقه القيام بهذه المهمة، وتتعاون من خلاله أجهزة الشرطة في الدول المختلفة، خاصة فيما يتعلق بتبادل المعلومات المتعلقة بالجريمة والمجرمين بأقصى سرعة ممكنة، بالإضافة إلى تعقب المجرمين الفارين من وجه العادلة، وتعود البدايات الأولى للتعاون الدولي الشُرَطي إلى عام(1904م)، عندما تم إبرام الاتفاقية الدولية الخاصة بمكافحة الرقيق الأبيض بتاريخ (1904/5/18م)، والتي أكدت على تعهد كل الحكومات المتعاقدة بإنشاء أو تعيين سلطة لجمع المعلومات الخاصة باستخدام النساء والفتيات لغرض الدعارة في الخارج، ولهذه

السلطة الحق في أن تخاطب مباشرة الإدارة المماثلة لها في كل الدول الأطراف المتعاقدة[21].

واستمرت الجهود الدولية والمحاولات الكثيرة لتعزيز التعاون الدولي في المجال الأمني والشُّرَطي لمكافحة الجريمة السيبرانية، حيث عقد في عام(1923م)، مؤتمر دولي يعد الثاني على المستوى الدولي للشرطة الجنائية، ضمّ مندوبي تسع عشرة دولة، ولعلّ أبرز ما نتج عن هذا المؤتمر ولادة اللجنة الدولية للشرطة الجنائية، والتي يتلخص عملها في إدامة التنسيق بين أجهزة الشرطة؛ من أجل التعاون في مكافحة الجريمة على المستوى الدولي[44].

بعد ذلك استمرت الجهود الدولية لإحياء اللجنة الدولية للشرطة الجنائية، بعد توقفها بسبب الحرب العالمية الثانية، وتم تغيير اسمها ليصبح: (المنظمة الدولية للشرطة الجنائية)، حيث ضمت في عضويتها أكثر (190) عضوًا، وتهدف هذه المنظمة إلى تأكيد التعاون بين أجهزة الشرطة في الدول الأطراف، وتشجيعه على نحو فاعل في مكافحة الجريمة، من تجميع البيانات والمعلومات المتعلقة بالمجرم والجريمة؛ وذلك عن طريق المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أقاليم الدول المنضمّة إليها، وتبادلها فيما بينها، بالإضافة إلى التعاون في ضبط المجرمين بمساعدة أجهزة الشرطة في الدول الأطراف، وإمدادها بالمعلومات المتوفرة لديها على إقليمها، خاصة بالنسبة للجرائم المتشعبة في عدة دول، ومنها جرائم الإنترنت[41].

بعد ذلك مرت جهود المنظمة في هذا المجال بمراحل عديدة، إلى أن تم إنشاء عدة مراكز اتصالات إقليمية، وعلى غرار هذه المنظمة أنشأ المجلس الأوروبي في لكسمبورج عام (1991م) شرطة أوروبية؛ لتكون همزة وصل بين أجهزة الشرطة الوطنية في الدول المنضمّة، ولملاحقة الجناة في الجرائم العابرة للحدود، ومنها بطبيعة الحال الجرائم المتعلقة بالإنترنت[15].

أما على المستوى العربي، فنجد أن مجلس وزراء الداخلية العرب، أنشأ المكتب العربي للشرطة الجنائية؛ بهدف تأمين التعاون وتنميته بين أجهزة الشرطة في الدول الأعضاء في مجال مكافحة الجريمة، وملاحقة المجرمين في حدود القوانين والأنظمة المعمول بها في كل دولة، بالإضافة إلى تقديم المعونة في مجال دعم أجهزة الشرطة في الدول الأعضاء وتطويرها [43].

فهذا التعاون الأمني يعد من أهم الصور في مجال مكافحة الجرائم السيبرانية، لا سيما وأن أجهزة العدالة الجزائية ليست بالمستوى والجاهزية نفسها في جميع الدول، وإنما هناك تفاوت فيما بينها، فبعض الدول متقدمة تقنيًّا وتكنولوجيًّا ولها سمعتها الكبيرة في مواجهة الجرائم المعلوماتية، ومنها الجرائم المتعلقة بالإنترنت تشريعيًّا وفنيًّا، وبعضها الآخر تفتقد ذلك؛ من هنا كان لا بد من التعاون الأمني بين الدول[45].

ويقتضي هذا التعاون تعقب مجرمي المعلوماتية عامة، وشبكة الإنترنت خاصة، وتعقب الأدلة الرقمية وضبطها، والقيام بعملية التفتيش العابر لحدود الحاسب الآلي ومكوناته المنطقية، والأنظمة المعلوماتية، وشبكات الاتصال، بحثًا عما قد تحويه من أدلة وبراهين على ارتكاب الجريمة السيبرانية، فكل ذلك ممّا يستدعي القيام ببعض العمليات الشرطية والفنية والأمنية المشتركة على المستوى الدولي؛ لأن ذلك من شأنه صقل مهارات القائمين على مكافحة تلك الجرائم وتعزيز خبراتهم؛ لغايات وضع حد لها[40].

ومن الأمثلة على دور الانتربول، وهو أحد المنظمات الدولية الشرطية في ما يتعلق بالجرائم المتعلقة بالإنترنت: ما حصل في الجمهورية اللبنانية، عندما تم توقيف أحد الطلبة الجامعيين من قبل القضاء اللبناني، بتهمة إرسال صور إباحية لقاصرة دون العشرة أعوام، من موقعه على شبكة الإنترنت؛ وذلك أثر تلقي النيابة العامة اللبنانية برقية من الانتربول في ألمانيا بهذا الخصوص.

الخاتمة:

تعد الجرائم السيبرانية وجرائم الإنترنت من الجرائم المعلوماتية العابرة للحدود، والتي ظهرت مؤخرًا مع الانتشار التكنولوجي لارتباطها بجهاز الحاسب الآلي (الكمبيوتر)، وتتمثل أداة الجريمة السيبرانية في شبكة الإنترنت، إذ تثير هذه الجريمة في مجملها الكثير من الإشكالات من مختلف الجوانب؛ كصعوبة اكتشافها وإثباتها، واتسامها بطابع الحيلة والدهاء من طرف مرتكبيها؛ من خلال استعمال تقنيات معلوماتية عالية الكفاءة، مما يؤدي إلى اختراق الشبكات، وأجهزة الحاسب الآلي المرتبطة بالإنترنت، حيث يتم اختراق نظام الأمن بالشبكة والدخول إلى الجهاز للكشف عن محتوياته، أو إتلافها، والتلاعب بالمعلومات المخزنة فيها، ومن خلال ما سبق عرضه، فقد توصّلتِ الدّراسة إلى النتائج الآتية:

1- إن وضع الهجمات السيبرانية في الإطار القانوني الدولي القائم، أمر صعب جدًا؛ وذلك بسبب الطبيعة الخاصة لها، إضافة إلى عدم وجود بيان قانوني رسمي ونهائي متفق عليه بشأن هذه الظاهرة.
2- إن هناك سباقًا للتسلح السيبراني والإلكتروني بين الدول، وذلك لرغبة الدول المتزايدة في تعزيز دفاعاتها ضد خطر التعرض للهجمات السيبرانية.
3- إن هناك جهودًا دولية وإقليمية لمكافحة هذه الظاهرة، وذلك من خلال المؤتمرات والاتفاقيات الدولية لمنع الجريمة السيبرانية، ومعاملة المجرمين السيبرانيين.

4- إن هناك صعوبات ومعيقات وقفت عائقًا في وجه المساعي والجهود الحثيثة في إيجاد آليات فاعلة بين الدول لمكافحة الجرائم السيبرانية.
5- إن الجرائم السيبرانية –بوصفها جرائم عالمية عابرة للحدود– لا تتحقق مكافحتها إلا من خلال التعاون الدولي على المستوى الإجرائي الجنائي.

التوصيات:

1- العمل على تحقيق الأمن السيبراني، وحفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية.
2- سد الفراغ التشريعي في مجال مكافحة الجريمة السيبرانية، وضرورة سن التشريعات التي تغطي هذا الفراغ من أجل الوصول إلى فضاء سيبراني آمن.
3- تطوير البنية التشريعية الجنائية الوطنية، بما يتماشى مع الجهود الدولية في مكافحة الجرائم السيبرانية.
4- تفعيل التعاون الدولي، ودور المعاهدات الدولية، ومبدأ المساعدة القانونية والقضائية والأمنية المتبادلة في مجال مكافحة الجرائم السيبرانية.
5- يوصي الباحث بإنشاء شراكات بين القطاعين العام والخاص على المستوى الوطني والإقليمي والدولي لمكافحة الجرائم السيبرانية، وتبادل الخبرات، وتحسين طرق مكافحتها؛ بوصفها جرائم عابرة للحدود الوطنية.

المراجع (References) :

الكتب:

1- الباشا، فائزة يونس، الجريمة المنظمة في ظل الاتفاقيات الدولية والقوانين الوطنية، القاهرة، دار النهضة العربية، ط1، (2001م).
2- البداينة، ذياب(2003م)، الأمن وحرب المعلومات، الأردن: دار الشروق للنشر والتوزيع.
3- بشير، نبيل(1994م)، المسؤولية الدولية في عالم متغير، القاهرة، دار المكتبة الجامعية الحديثة.
4- البعلبكي، منير(2004م)، المورد: قاموس انكليزي– عربي، دار العلم للملايين، بيروت.
5- أبو بكر، محمد عبد الله(2006م) ، جرائم الكمبيوتر والإنترنت، منشأة المعارف، الإسكندرية.
6- جانكارلو أ. باراليتا(2011م) النزاع السيبراني والاستقرار الجيوسيبراني، الاتحاد الدولي للاتصالات، القاهرة.
7- حجازي، عبد الفتاح بيومي(2007م)، الإثبات الجنائي في جرائم الكمبيوتر والإنترنت.
8- الحمداني، بشرى حسين(2013م)، القرصنة الإلكترونية: أسلحة الحرب الجديدة، عمان، نبلاء ناشرون وموزعون، (2013م).
9- الحمداني، بشرى حسين(2014م)، القرصنة الإلكترونية: أسلحة الحرب الحديثة، عمان، دار أسامة للنشر والتوزيع.
10- خليفة، إيهاب(2014م)، القوة الإلكترونية وأبعاد التحول في خصائص القوة، الإسكندرية، مكتبة الإسكندرية.
11- الردايدة، عبد الكريم(2010م)، الجرائم المستحدثة وإستراتيجية مواجهتها، عمان، دار ومكتبة الحامد للنشر والتوزيع.
12- سكر، عبد الصمد(2010م)، التعاون الدولي الأمني في مكافحة الجرائم المعاصرة، القاهرة، مطابع كلية الشرطة.
13- شرابشة، ليندة(2012م)، السياسة الدولية والإقليمية في مجال مكافحة الجريمة في مجال مكافحة الجريمة الإلكترونية، الرباط، المركز الجامعي.
14- شفيق، نوران(2016م)، أثر التهديدات الإلكترونية على العلاقات الدولية: دراسة في أبعاد الأمن الإلكتروني، القاهرة، المكتب العربي للمعارف.
15- الصغير، جميل عبد الباقي(1998م)، الجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة.
16- الطائي، صلاح(2009م)، حق الاسترداد في القانون الدولي، القاهرة، مكتبة الجامعة الحديث.
17- عبابنة، محمود، والرازقي(2005م)، محمد معمر، جرائم الحاسوب وأبعادها الدولية، عمان، دار الثقافة للتوزيع والشر.
18- غنام، شريف محمد(2007م)، حماية العلامات التجارية عبر الإنترنت في علاقتها بالعنوان الإلكتروني، القاهرة، دار الجامعة الجديدة.

الرسائل الجامعية:

19- المويشر، تركي عبد الرحمن(2009م)، بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته، أطروحة دكتوراه في العلوم الأمنية، الرياض: جامعة نايف العربية للعلوم الأمنية.

القوانين والمعاهدات والاتفاقيات الدولية:

20- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الديباجة، الأمانة العامة لجامعة الدول العربية، إدارة الشؤون القانونية، (2010م).

المجلات والصحف والأبحاث:

21- إيفين، شمويل وسيمان توف، دافيد(2011م)، "حرب الفضاء الإلكتروني... المفاهيم.. الاتجاهات.. معهد أبحاث الأمن القومي، فلسطين.

22- إيفين، شمويل وسيمان توف، دافيد (2011م)، حرب الفضاء السبراني: مفاهيم واتجاهات ودلالات لإسرائيل، معهد دراسات الأمن القومي، مذكرة رقم(109)، تل أبيب، ترجمة (محمود خليل).

23- شحاته، علا الدين محمد وآخرون(1987م) ، دور وزارة الداخلية في تدريب ضباط الشرطة غير المصريين، بحث مقدم لمعهد تدريب ضباط الشرطة، أكاديمية الشرطة، القاهرة.

24- شريف عتلم، ومحمد ماهر عبد الواحد(2007م)، موسوعة اتفاقيات القانون الدولي الإنساني، النصوص الرسمية لاتفاقيات والدول المصدقة عليها"، إصدار بعثة اللجنة الدولية للصليب الحمر بالقاهرة.

25- عبد الصادق، عادل(2015م)، القوة الإلكترونية أسلحة الانتشار الشامل في عصر الفضاء الإلكتروني، مجلة السياسة الدولية.

26- الفتلاوي، أحمد عبيس نعمه(2016م)، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، مجلة المحقق الحلي، جامعة بابل.

27- كاخيا، إبراهيم(2010م)، الحرب الإلكترونية، مجلة الدفاع العربية، بيروت.

28- محارب، محمود(2011م)، قراءة في كتاب: حرب في الفضاء الإلكتروني: اتجاهات وتأثيرات على إسرائيل، المركز العربي للأبحاث ودراسة السياسات، الدوحة.

29- المحمدي، حسنين(2006م)، إرهاب الإنترنت: الخطر القادم، الجزائر، (د.ن).

30- المركز الاستشاري للدراسات والتوثيق(2014م)، التحولات في العقيدة العسكرية الأمريكية: دعائم الضعف السبع، أوراق إستراتيجية، سلسلة غير دورية.

المواقع الإلكترونية:

1- الحمدان، منيرة فهد، موقف القانون الدولي من الحرب السيبرانية، جريدة الرياض السعودية، (2015م)، العدد 17389، (2016م)، متوفر على الرابط الإلكتروني: http://www.alriyadh.com/1124892

2- خليفة، إيهاب عبد الحميد، الفضاء الإلكتروني وتهديد الأمن القومي المصري، المركز العربي لأبحاث الفضاء الإلكتروني، (2015م)،متوفر على الرابط الإلكتروني: www.accrononline.com

3- خليفة، إيهاب عبد الحميد، القوة الإلكترونية والصراع الدولي، المركز العربي للأبحاث الفضاء الإلكتروني،(2016م)، www.accronline.com

4- الصديقي، إلياس، تحديات القوانين: الفضاء الافتراضي والقانون الدولي، أبو ظبي، مركز دلما للدراسات، (2016م)، متوفر على الرابط الإلكتروني: http://delma.io/ar/draft.

5- فؤاد، شيماء، أوراق تناقش الصراع الدولي في الفضاء الإلكتروني، منشور على موقع شبكة الإعلام العربية، (2017م)، ومتوفر على الرابط الإلكتروني: www.moheet.com

6- الموقع الرسمي شركة نورتون، التدرج المروع للجرائم الإلكترونية، (2012م)، متوفر على الرابط الإلكتروني: mwww.nowstatic.co

وقائع المؤتمرات والندوات:

7- البداينة، ذياب موسى، الجرائم الإلكترونية: المفهوم والأسباب، عمان، ورقة عمل مقدمة للملتقى العلمي "الجرائم لمستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية خلال الفترة 2-2014/9/4م"، عمان، الأردن، (2014م).

8- تدابير مكافحة الجرائم المتصلة بالحواسيب –مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية– المنعقد في بانكوك في الفترة (18-2005/4/5م)– وثيقة رقم A/CONF.203/14 .

9- رستم، هشام محمد فريد، الجرائم المعلوماتية " أصول التحقيق الجنائي الفني، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت – كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة في الفترة (1-2000/5/3م) المجلد الثاني– الطبعة الثالثة – (2004 م).

10- صالح، محمود، الجرائم المعلوماتية، مسقط: ورقة عمل قدمت إلى ورشة العمل الإقليمية حول تطوير التشريعات في مجال مكافحة الجرائم الافتراضية، سلطنة عمان 2-4 نيسان (2006م).

11- مسعود، ماهر أسامة، موقف القانون الدولي الإنساني من الهجوم عن طريق الإنترنت "CyberWar" ، ورقة عمل قدمت لمؤتمر الفضاء السيبراني، كلية الحقوق، جامعة الأزهر، القاهرة، (2015م).

12- اللوسي، محمود، جرائم الحاسب الآلي – ورقة عمل مقدمة من الأمانة العامة لمجلس التعاون الخليجي لاجتماع اللجنة الفنية المتخصصة بدراسة سبل مكافحة الجرائم الإلكترونية " الإنترنت" الأول والذي أنعقد بمقر الأمانة العامة بالرياض خلال الفترة من (2-2006/3/5م).

13- ورشة العمل الإقليمية " تطوير التشريعات في مجال مكافحة الجرائم الافتراضية والتي عقدت بمدينة مسقط بسلطنة عمان في الفترة من (2-4/ 2006/4م) بتنظيم مشترك بين هيئة تنظيم الاتصالات العمانية ومركز التميز العربي التابع للاتحاد الدولي للاتصالات.

14- وقائع المؤتمر الدولي لأمن المعلومات الإلكترونية والذي عقد بمدينة مسقط بسلطنة عمان في الفترة من (18-2005/12/20م) بتنظيم مشترك بين بلدية مسقط وبين المنظمة العربية للتنمية الإدارية.

English References :

15- Donnb . Parker, fighting computer crime ,Charles Scribner Son, New York (1983).

16- Richard Kissel (2013), Glassory of Information Security Terms, National Institute of Standers and technology, U.s Department of Commerce.

17- Julia Cresswell (2010), Oxford Dictionary of word Origins: Cybernetics, Oxford Reference Online, Oxford University Press.

18- U.S. Department of Defense(2010), Dictionary of Military and Associated Terms, Joint Publication 1-02, Nov. 8, (2010), as amended through Feb. 15,(2012).

19- MichealN.Schmitt(2013),"Tallinn Manual on the International Law Applicable to Cyber Warfare ", Cambridge University press, first publishes.

20- Kenneth Greers, Straedic Cyber Security, NATO Cooperative Cyber Defence Center of Excellence,(2011).

21- Clay Wilson, Cyber Crime. In Franklin D. Kramer et al (eds), Cyber power and National Security, Potomac Book,(2009).