جرائم الأمن السيبراني وآليات مكافحتها في إطار القانون الدولي

Doi: 10.23918/ilic2020.34

الأستاذ المساعد الدكتور
نايف أحمد ضاحي الشمري
كلية الحقوق جامعة تكريت
Nady-law2000@yahoo.com

المدرس المساعد
عمر عباس خضير العبيدي
ماجستير قانون عام/ جامعة تكريت- كلية الحقوق
omarabbas93.aa@gmail.com

المقدمة

الجرائم السيبرانية (cyber crime) أي الجرائم الإفتراضية الواقعة في فضاء إلكتروني منبثق من (cyber space) أي الفضاء التخيلي أو الإفتراضي، ويعد عالم الرياضيات نوربرت وينر (Norbert wiener)، هو أول من إستخدم مصطلح السيبرانية وذلك في عام ١٩٤٨. ثم جاء المؤتمر العاشر للأمم المتحدة المنعقد في فيينا عام ٢٠٠٠م ليؤكد هذه التسمية عن الجرائم الإلكترونية التي إنتشرت في الآونة الأخيرة بسبب إنتشار شبكة الإنترنت وفتح مجالات عديدة للإستفادة منها والذي فرضته هذه التقنيات الحديثة والتدفق الغزير للمعلومات والتي يمكن إستخدامها لمصلحة بشرية، وفي الوقت نفسه هناك أضرار حدثت خلال السنوات الأخيرة وباتت هذه الجرائم من أخطر أنواع جرائم العصر إنتقل مرتكبيها بالجرائم من صورها التقليدية الى جريمة أخرى إلكترونية. إذ تعد مكافحة الجرائم السيبرانية ضمان لتعزيز للأمن القومي وذلك بإستخدام مجموعة من الوسائل التقنية والإدارية التي يتم إستخدامها لمنع الإستخدام غير المصرح به بهدف ضمان توافر إستمرارية عمل نظم المعلومات وتأمين حماية وسرية وخصوصية البيانات الشخصية ولحماية المواطنين، وذلك لتعزيز الأمن القومي العربي لمواجهة التحديات الدولية الإقليمية.

أهمية البحث:

تستمد أهمية الموضوع في توعية الأفراد من كافة المجتمعات والدول في الوسائل والطرق التي تلجأ إليها التنظيمات الإرهابية لغايات استقطاب وتجنيد هؤلاء الأفراد، كما يستمد هذا الموضوع أهميته إدراكاً من الواقع بأنَّ ظاهرة الجرائم المستحدثة ومنها الجرائم السيبرانية قد غدتْ تشكلُ تحدياً حقيقياً للسياسات الجنائية السائدة في الدول وأجهزتها التشريعية والتنفيذية والقضائية، وكذلك الهدف من البحث هو تزايد اللجوء الى الهجمات السيبرانية وتزايد مشاركة المدنيين بصورة مباشرة وغير مباشرة في العمليات العدائية، فضلاً عن نشأة الشركات الأمنية والعسكرية والتقنية الخاصة التي تقوم بتقديم دعمها ومنتوجاتها الخاصة بالحروب، فضلاً عن مشاركتها المباشرة في قيادة العمليات العدائية.

إشكالية البحث:

تكمن إشكالية البحث بالجرائم السيبرانية في ما مدى كفاية الحماية القانونية الدولية لمكافحة الجرائم السيبرانية؟ وما هي إلتزامات الدول الأساسية بشأن مكافحة اللجوء الى الهجمات السيبرانية وكيف تقوم الدول بالحد من الآثار الضارة لهذه الهجمات؟

فرضية البحث:

تتمثلُ فرضية البحث بأنَّ الجرائم السيبرانية هي جريمة دولية إلكترونية (معلوماتية) ذات طبيعة خاصة. إذ يناقش البحث فرضيتين هما هل تستطيع التشريعات والمحاكم القضائية بوسائلها وإجراءاتها الورقية أن تواجه غموض وتحديات جرائم العصر، وماذا سيحل بمرافق العدالة إذ إنتقلت الدولة برمتها الى البيئة الإلكترونية مما يشكل عبئ جديد.

منهجية البحث:

بالنظر للخصوصية التي تتميزُ بها الجرائم السيبرانية والإهتمام الذي تحظى به من قبل المجتمع الدولي، حيث ستعتمدُ الدراسة في معالجتها لهذا الموضوع على المنهج التحليلي والمقارن بإعتبارهما الأنسب بحكمِ التطرق إلى مختلف نصوص القوانين.

خطة البحث:

على الرغم من وجود عدد من الدراسات التي قدمت في الجرائم السيبرانية من الناحية القانونية والعلوم الأخرى إلا إن دراستنا المقترحة ستناقش موضوع الجرائم السيبرانية في إطار بعض القوانين وآراء المحاكم وما تطبقه من عقوبات بحق مرتكبي هذه الجرائم لضمان تعزيز الأمن القومي العربي وتحديات الأمن الإقليمي. وتقديم الحلول لمعالجة إشكاليات البحث سنقسم دراسة هذا البحث على مبحثين، وهما ما يأتي:

المبحث الأول: التعريف بالجرائم السيبرانية

المطلب الأول: تعريف الجرائم السيبرانية وخصائصها

المطلب الثاني: التحديات التي يمثلها الأمن السيبراني وما هي العلاقة بينه وبين الأمن القومي

المبحث الثاني: آليات مكافحة الجرائم السيبرانية

المطلب الأول: جهود المنظات الدولية مكافحة الجرائم السيبرانية

المطلب الثاني: التعاون الدولي مكافحة الجرائم السيبرانية

المبحث الأول

التعريف بالجرائم السيبرانية

إستجابةً للتطور الكبير في تقنيات الاتصالات والمعلومات والزيادة الهائلة في حجم المتعاملين معها رافق ذلك من ممارسات سلبية تصل في كثير من الأحيان الى جرائم تهدد الأمن بمعناه الشامل مما أوجد بعض التحديات لمواجهة هذه الجرائم. إذ لم تكن الجرائم السيبرانية معروفة إلا في وقت قريب، ما يشكل إحدى أهم التحديات الراهنة التي يواجهها المختصون في

القانون الدولي العام، وبالخصوص في تحديد طبيعتها وعناصرها، فضلاً عن نطاق هذه الجرائم في ضوء القانون الدولي الإنساني وما يترتب عليها من تبعات المسؤولية الدولية الجنائية كانت أم مدنية. وما يزيد في إتساع التحدي الذي يواجهه المختصون في القانون الدولي العام، والإنساني على وجه الخصوص، إنما يتجسد في الغموض التي إكتنفت مفهوم الجرائم السيبرانية وعدم الاتفاق على تعريف محدد، يمكن الإستدلال في ضوئه لتنظيم إستخدامها بالحظر أو التقييد لمواجهة عواقبها الخطرة على الصعيد الإنسان[١].

ومن أجل الوقوف على تعريف الجرائم السيبرانية سنتناول دراسة هذا المبحث على مطلبين، وهما ما يأتي:

المطلب الأول: تعريف الجرائم السيبرانية وخصائصها

المطلب الثاني: التحديات التي يمثلها الأمن السيبراني وما هي العلاقة بينه وبين الأمن القومي

المطلب الأول

تعريف الجرائم السيبرانية وخصائصها

يشهد العالم في الفترة الأخيرة نوعاً جديداً من سباق التسليح لا على غرار المعروفة منها في حقل الأسلحة التقليدية وغير التقليدية، ويقوم هذا السباق على إستحداث أو تطوير برامج إلكترونية معدة لأغراض عسكرية تعرف إختصاراً بالسايبر (Cyber). لقد أعادت بعض الدول الى الأذهان نظرية توازن الرعب[٢] التي خيمت ولفترة عقود من الزمن على المجتمع الدولي وبالخصوص سباق الدول لإقتناء أسلحة الدمار الشامل، ولكن بصورة مختلفة نوعاً ما، وذلك بإستخدام تقنيات إلكترونية في نطاق أعمال عدائية[٣]. رافق ذلك من ممارسات سلبية تصل في كثير من الأحيان الى جرائم تهدد الأمن بمعناه الشامل مما أوجد بعض التحديات لمواجهة هذه الجرائم منها زيادة الحاجة الى جهات تمارس التحقيق بشكل متخصص بالإضافة الى الضغوط على الجهات القضائية والأمنية فضلاً عن الحاجة الى التكامل المعرفي بين رجال القانون والتحقيق والقضاء مع الجهات التقنية والحاسوبية[٤].

وعليه ومما تقدم سنقسم دراسة هذا المطلب على فرعين، وهما ما يأتي:

الفرع الأول: تعريف الجرائم السيبرانية

الفرع الثاني: سمات وخصائص الجرائم السيبرانية

الفرع الأول

تعريف الجرائم السيبرانية

تشير المراجع العلمية الى أن عالم الرياضيات نوربرت وينر (Norbert wiener)، هو أول من إستخدم مصطلح السيبرانية وذلك في عام ١٩٤٨، في أثناء دراسته لموضوع القيادة والسيطرة والإتصال في عالم الحيوان، فضلاً عن حقل الهندسة الميكانيكية[٥]. في دراسة هذا الفرع سيتم البحث على ثلاثة نقاط: الأول يرتكز على تعريف الجرائم السيبرانية لغةً، والثاني سيرتكز على تعريف الجرائم السيبرانية إصطلاحاً، والثالث سيرتكز على تعريف الجرائم السيبرانية فقهاً وبعض التطبيقات الدولية.

أولاً: تعريف الجرائم السيبرانية لغةً

يتضح أن مصدر كلمة سايبر (Cyber) في المعاجم اللغوية أنها يونانية الأصل وترجع الى مصطلح (kybernetes)، الذي ورد بداية في مؤلفات الخيال العلمي ويعني القيادة أو التحكم عن بُعد[٦].

وبالرجوع الى قواميس اللغة، فلم تشر في الغالب الى مصدر كلمة سايبر (Cyber)، سوى ما وجدناه في قاموس (المورد) إذ يعرفها بالقول: "السيبرانية: هي علم الضبط، ومصدرها (Cybernetics)"[٧]، وهو مصدر يتطابق مع مفهوم الجرائم السيبرانية، أي ضبط الأشياء عن بعد والسيطرة عليها.

فيما عرف قاموس مصطلحات الأمن المعلوماتي، مصطلح السيبرانية بالقول "هجوم عبر الفضاء الإلكتروني يهدف الى السيطرة على مواقع إلكترونية أو بنى تحتية محمية إلكترونياً لتعطيلها أو تدميرها أو الإضرار بها"[٨].

---

[1] Oona' A.Hathway, Rebecca Crootof, Philip Levtiz, aley Nix, Aileen Nowlan, William perdue and Julia Spiegel, "The Law of Cyber- Attack", California Law Review, 2012, p.7.

[٢] شاع إستعمال مصطلح "توازن الرعب" خلال فترة الحرب الباردة، ويشير ميتشل مارين (Micheal Marien)، بالقول: "إن الولايات المتحدة الأمريكية والإتحاد السوفيتي السابق تبنيا هذا المصطلح كأساس للتفاهم الثنائي بشأن سباق التسليح بإعتبارهما قوتان استأثرتا بـ ٩٦% من الأسلحة النووية الإستراتيجية، و٧٠% من مجموع الصادرات العالمية للأسلحة و٥٠% من الإنفاق العالمي على التسلح".

Micheal Marien: "Future survey annual", Transaction Publishers, 1987, p.34.

[٣] د. أحمد عبيس نعمة الفتلاوي: الهجمات السيبرانية، دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، ط١، منشورات زين الحقوقية، بيروت، ٢٠١٨، ص٥.

[٤] كوثر حازم سلطان: موقف القانون والقضاء من الجريمة الإلكترونية (السيبرانية)، دراسة مقارنة، بحث منشور في مجلة كلية التربية الأساسية، الجامعة المستنصرية، العراق، مج٢٢، ع٩٦، ٢٠١٦، ص٩٧٠.

[5] Norbert wiener: Cybernetic or control communication in the animal and the machine, M.I.T, Press, Second Edition, Cambridge, Massachusetts, 1948.

[6] Julia Cresswell, "Oxford Dictionary of word Origins: Cybernetics", Oxford Reference Online, Oxford University press, 2010.

[٧] منير البعلبكي: المورد قاموس إنكليزي- عربي، دار العلم للملايين، بيروت، ٢٠٠٤، ص٢٤٣.

[8] Richard Kissel, "Glassory of Key Information Security Terms", National Institute of Stand ards and technology, U.S Department of Commerce, Revision, 2, May 2013, p.57.

أما في اللغة العربية وبالرجوع الى المختصين فيها، فنجد أن تحدياً واجهوه في إختيار مصطلح مقارب لمصطلح (Cyber) في اللغة الإنكليزية، ولا أدل على ذلك من أن الترجمة العربية لعنوان إتفاقية مجلس أوربا المتعلقة بالجرائم السيبرانية كانت ترجمة غير صائبة، إذ تُرجمَ العنوان (Convention on Cybercrime) الى اللغة العربية بأنه (الاتفاقية المتعلقة بالجرائم الإلكترونية) ويعود السبب في ذلك الى عدم وجود مصطلح مناظر في اللغة العربية[١].

إن سبب تسليط الضوء على مصطلح السيبرانية في هذه الدراسة يعود الى المصطلح الذي إستخدمه نوربرت وينر في كتابه آنف الذكر وهو (Cybernetic)، لعدم وجود مصطلح متفق عليه في اللغة العربية من جهة، ولأن الوثائق الصادرة عن الأمم المتحدة باللغة العربية، إستخدمت مصطلح السيبرانية نفسه من جهة أخرى[٢].

ثانياً: تعريف الجرائم السيبرانية إصطلاحاً

في هذه الدراسة إستخدمنا مصطلح الجرائم السيبرانية(Cyber Crime)، على عكس ما درج عليه البعض من المختصين، فمنهم من تبنى مصطلح الفضاء السيبراني (Cyber Space)، بالإستناد الى المحيط الذي تجري فيه العمليات السيبرانية (Cyber Operations) الناشئة عن أداء أنظمة إلكترونية مهمتها متابعة وجمع المعلومات التي تعمل إلكترونياً وتحليلها ومن ثم إتخاذ إجراءات محددة لمهاجمتها عن طريق أنظمة إلكترونية أخرى مخصصة لهذا الغرض[٣].

وتبنى آخرون مصطلح الحرب السيبرانية (Cyber Warfare)، بالإستناد الى أيديولوجية أمنية أو عسكرية، تضع منهاجاً لتحقيق أهداف على الصعيد الأمني أو العسكري تجاه (العدو المفترض)[٤].

أما البعض الآخر فاختار مصطلح الهجمات السيبرانية (Cyber Attacks)، كوصف واقعي يجمع بين كل ما ذكر آنفاً[٥]، فهو تصرف يدور في عالم إفتراضي قائم على إستخدام بيانات رقمية ووسائل إتصال تعمل إلكترونياً، ومن ثم تطور ليتضمن مفهوماً أوسع يقوم على تحقيق أهداف عسكرية أو أمنية ملموسة ومباشرة، جراء إختراق مواقع إلكترونية حساسة، عادةً ما تقوم بوظائف تصنف بأنها ذات أولوية، كأنظمة حماية محطات الطاقة النووية أو الكهربائية أو المطارات ووسائل النقل الأخرى[٦].

ولأن مصطلح الحرب هو مصطلح غير محبذ في وقتنا الراهن على المستوى التنظيم القانوني الدولي[٧]، فيكون مصطلح الهجمات السيبرانية أكثر قرباً للموضوع، ولاسيما أن تصرفات دولية عدة أشارت الى مصطلح الهجمات، وعدتها بمثابة التصرف الذي يوضع في الحسبان في أثناء النزاعات المسلحة، طبقاً للقانون الدولي الإنساني[٨].

ثالثاً: تعريف الجرائم السيبرانية فقهاً وبعض التطبيقات الدولية

إنطلق فقهاء القانون من معايير لتحديد مفهوم الجرائم السيبرانية منها معيار موضوع الجرائم أو وسيلتها وآخرون ركزوا على النتيجة التي تتركها وكما يأتي:

يتفق الأستاذ محمد أمين الشواكبة مع الأستاذ (Middet Credo) بأن الجرائم السيبرانية تسهل إستخدام الحاسوب كأداة لإرتكاب الجرائم بالإضافة الى الحالات المتعلقة بالولوج غير المصرح به للحاسوب الآلي أو البيانات الرقمية لتشمل الإعتداءات المالية المادية[٩].

ويعرف بعض الفقه المختصين في القانون الدولي بأنه إستخدام الطيف الإلكتروني أو الكهرومغناطيسي لتخزين وتعديل وتبادل البيانات وجهاً لوجه مع أنظمة تحكم في بنى تحتية مرتبطة بها[١٠].

---

[١] د. أحمد عبيس نعمة الفتلاوي: مصدر سابق، ص١٢.

[٢] إنظر على سبيل المثال: مكتب الأمم المتحدة المعني بالمخدرات والجرائم: "تقرير الخبراء المعني بإجراء دراسة شاملة عن الجرائم السيبرانية، دراسة شاملة عن مشكلة الجرائم السيبرانية والتدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدي لها"، فينا، ٢٠١٣، الوثيقة: UNODC/CCPCJ/EG.4/2013/2.

[3] James A. Lewis, "Sovereignty and the role of Government in Cyberspace", Center for Strategic and International Studies Journal, spring summer, vol. XVI, Issue II, 2010, p.56.

[4] Shin, Beomchul, "The Cyber Warfare and the Right of self- Defense: Legal perspectives and the Case of the United States, IFANS, VOI.19, N1, June 2011, p.104.

[5] Scoot. J.Shckelford, "State Responsibility for Cyber Attacks: Competing Standards for a Growing problem", University of Cambridge, Dept of politicos and International STUDIES, Cambridge, UK, 2009, P194.

[6] K.saalbach, "Cyber War, Methods and practice", Version 9.0, University of Osnabruck-17 Jun 2014, p.6.

[٧] دأبت المؤسسات الدولية، فضلاً عن الاتفاقيات الدولية المعاصرة على إستخدام مصطلح "نزاع مسلح"، بدلاً من مصطلح "الحرب"، وكانت المناسبة الأولى في اتفاقيات جنيف الأربعة الموقعة في ١٢ آب/ أغسطس عام ١٩٤٨، انظر:

ICRC, "Exploring humanitarian law: IHL Guide, A legal manual for EHL teacher", ICRC, Geneva, January 2009, p.7.

[٨] الفقرة (٢) من المادة (٥٤) من البروتوكول الإضافي الأول لعام ١٩٧٧، والتي نصت بأنه: "يحظر مهاجمة أو تدمير أو نقل أو تعطيل الأعيان والمواد التي لا غنى عنها لبقاء السكان المدنيين..." كذلك المادة (٥٦) من البروتوكول نفسه والتي نصت: "لا تكون الأشغال الهندسية أو المنشآت التي تحوي قوى خطرة ألا وهي السدود والجسور والمحطات النووية لتوليد الطاقة الكهربائية محلاً للهجوم" كذلك الفقرة (٢) من المادة (١٣) من البروتوكول الإضافي الثاني، والتي نصت بأنه " لا تكون الأشغال الهندسية أو المنشآت التي تحوي قوى خطرة ألا وهي السدود والجسور والمحطات النووية لتوليد الطاقة الكهربائية محلاً للهجوم حتى لو كانت أهدافاً عسكرية، إذا كان من شأن هذا الهجوم أن يتسبب في إنطلاق قوى خطرة ترتب خسائر فادحة بين السكان المدنيين". د. أحمد عبيس نعمة الفتلاوي: مصدر سابق، ص١٤-١٥.

[٩] محمد أمين الشواكبة: جرائم الحاسوب الإنترنت، ط٤، دار الثقافة للنشر والتوزيع، الأردن، ٢٠١١، ص٨.

[10] Shin, Beomchul, op.cit.p. 105.

فيما عرفها (Fuertes) بالقول بأنه: هجوم عبر الإنترنت يقوم على التسلل الى مواقع إلكترونية غير مرخص بالدخول إليها، بهدف تعطيل أو إتلاف البيانات المتوفرة فيها أو الإستحواذ عليها، وهي عبارة عن سلسلة هجمات إلكترونية تقوم بها دولة ضد أخرى[١].

وفي ملاحظة دقيقة لإختيار مصطلح مناسب يذهب ميشيل جيرفيس (Michael Gervais) الى القول: إن مصطلح الحرب السيبرانية ليس بالمصطلح المناسب، لكونه مصطلح عام لا يميز بين آثار إستخدام السيبرانية كوسيلة أم كطريقة قتالية[٢].

وأخيراً يذهب ماركو روسيني (Marco Roscini) الى تعريفها بالقول: تطويع الإمكانيات الإلكترونية العسكرية لأجل التأثير في مواقع أخرى وتعطيلها وتدميرها سواء أكانت تقدم خدمات مدنية أو عسكرية[٣].

ويرى بعض الفقه أن التعريف الذي ذهب إليه ميشيل (Michael) هو الأقرب لمفهوم الجرائم السيبرانية التي عرفها روسيني (Roscini)، إذ يعرفها بالقول: الجرائم السيبرانية هو أي تصرف دفاعياً كان أم هجومياً، يتوقع منه وعلة نحو معقول في التسبب بجرح أو قتل شخص أو إلحاق أضرار مادية أو دمار بالهدف المُهاجم[٤].

أن المثال الأكثر إنسجاماً مع ما تم ذكره سابقاً، هو أن تهاجم طائرة حربية مواقع حساسة لدولة ما، كمراكز البنى التحتية المعلوماتية (Installations Information Infrastructure) تابعة لها فتطلق صواريخ موجهة تبث أطيافاً كهرومغناطيسية تتسبب في تعطيل منظومات الإتصال الإلكترونية، فضلاً عن التدمير المادي لأجهزتها[٥]. وهذا ما يتوافق مع مفهوم إستخدام الوسائل الإلكترونية للأغراض العسكرية، ففي عام ٢٠٠٧ عرفت القيادة الإستراتيجية الأمريكية (US. Startegic Command) الجرائم السيبرانية بالقول: تطويع عمليات نظام الكمبيوتر بهدف منع الخصوم من الإستخدام الفعال لها، فضلاً عن التسلل الى أنظمة المعلومات وشبكات الإتصال بهدف جمع وحيازة وتحليل البيانات التي تحتويها[٦].

أن التعريف سالف الذكر، يتوافق مع ما جاءت به اتفاقية مجلس أوربا المتعلقة بالجرائم السيبرانية في مضمون المادة (٥) والتي نصت: "تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الفعل التالي في قانونها الوطني، إذ ما إرتكب عمداً وبغير حق الإعاقة الخطيرة لعمل منظومة الكمبيوتر عن طريق إدخال أو إرسال أو إتلاف أو محو أو تغيير أو تبديل أو تدمير بيانات كمبيوتر"[٧].

إذ يتضح مما تقدم أن التركيز على نوع الآثار وجسامتها، فكلما ثبت أن المدنيين على سبيل المثال سيتأثرون جراء أي نشاط سيبراني عسكري، كإستهداف منظومة السيطرة والتحكم الإلكترونية لمفاعل نووي لتوليد الطاقة الكهربائية، وإن أجلى تطبيق على ما ذكرناه آنفاً ما تعرضت إليه (نطانز) النووية الإيرانية من هجوم سيبراني، أعلنت عنه الولايات المتحدة الأمريكية في عام ٢٠١١، إذ إستخدمت برنامجاً ويدعى (Stuxnet) عطل بعضاً من العمليات الحساسة والحق أضراراً جزئية في عمليات تخصيب اليورانيوم، وهوما يمكن معه عدَّ هذا الهجوم سابقة في حقل الجرائم السيبرانية[٨].

الفرع الثاني

سمات وخصائص الجرائم السيبرانية

مما لا شك فيه أنَّ التداول الداخلي للبيانات المبرمجة عبر الدول وتداول المعلومات البسيطة غير المبرمجة وسرعة انتشار شبكة المعلومات أدى إلى التغيير التقني المطَّرد والمتعاظم في هذا المجال، وإلى سهولة تداول المعلومات التي باتت تساعد الجرائم السيبرانية عن طريق استعمال الحاسوب الشخصي أو الحواسيب الأخرى المستخدمة في دولةٍ معينةٍ على الرغم من أنَّ النتيجة الجرمية قد تتحقق في دولةٍ أخرى، إذْ أصبحتْ الجرائم السيبرانية تمثل شكلاً جديداً من الجرائم العابرة للحدود وهذه الصور تتخذ طابعاً يميِّزها عن غيرها من الجرائم[٩].

إنَّ للجريمة السيبرانية عدد من الخصائص والسمات التي تختلف فيها عن بقية الجرائم، وتحول دون إختلاطها بالجرائم العادية، حيث يمكننا إيراد أهم هذه الخصائص وهي كما يأتي:

أولاً: جريمة عابرة للحدود: إذْ تتسم الجرائم السيبرانية بكونها جريمة إرهابية متجاوزه للحدود وعابره للدول وللقارات، إذ أنَّها غير خاضعة لنطاق إقليمي محدود، إذْ أعطى إنتشار أجهزة الحاسوب إمكانية لربط أعداد هائلة بشبكات الإنترنت والمرتبطة بالشبكة العنكبوتية من غير أنْ تخضع لحدود الزمان والمكان، وهنا تظهر الحاجة لوجود تنظيم قانوني دولي متلائم معه لمكافحة

---

(1) Micheal S.Fuertes, "Cyber warfare, Unjust Actins in a just war", Florida International University, Full 2013, p.1.

(2) Michael Gervais, "Cyber Attacks and the Laws of War", Berkeley Journal of Internatinal Law, vol. 30, Iss. 2, 2012, p.532.

(3) Marco Roscini, "World Wide Warfare- Jus ad bellum and the use of Cyber Force", Max Planck Yearbook of United Nations Law, Volume 14, 2010, p.91.

(4) Micheal N.Schmitt, "Tallinn Manual on the International Law Applicable to Cyber Warfare", Cambridge University press, first publishes, 2013, p.92.

(5) Ivan Goldberg, Institute for the Advanced Study of Information Warfare (LASIW), http/ www.psycom.net/war.1.html.

(6) K. Saalbach, "Cyber War, Methods and Practice", Version 9.0, University of Osnabruck- 17Jun 2014, p105.

(٧) المادة (٥) من اتفاقية مجلس أوربا المتعلقة بالجرائم الإلكترونية، مجموعة المعاهدات الأوربية رقم ١٨٥، بودابست عام ٢٠٠١.

(8) Michael Gervais, op. cit. p.46.

(٩) د. محمد محي الدين عوض: مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر)، ورقة عمل مقدمة الى المؤتمر السادس للجمعية للجمعية المصرية للقانون الجنائي، القاهرة، ١٩٩٣، ص٦؛ أسامة أحمد المناعسة، وآخرون: جرائم الحاسوب الآلي والإنترنت، ط١، دار وائل للنشر، الأردن، ٢٠٠١، ص١٠٥.

مثل هذا النوع من الجرائم وضبط مرتكبيها، وتظهر أيضاً مشاكل عدة منها حول الجهة صاحبة الإختصاص القضائي لهذه الجرائم وإشكالات أخرى تتعلق بإجراءات الملاحقة القضائية وتتشابه الجرائم الإلكترونية في هذه الخاصية مع بعض الجرائم مثل غسل الأموال، وجرائم المخدرات[١].

ثانياً: صعوبة الإكتشاف: تتميز صعوبة اكتشاف الجرائم السيبرانية، وذلك لنقص الخبرة لدى بعض الأجهزة الأمنية والقضائية في التعامل مع مثل هذا النوع من الجرائم، حيث أنها لا تترك في الغالب أثراً مادياً ظاهراً يمكن ضبطه، فضلاً عن التباعد الجغرافي الذي يثير الإشكال بدايةً، وتُعدُ الوسيلة المستخدمة لإرتكاب الجرائم هي نبضة إلكترونية ينتهي دورها خلال أقل من ثانية واحدة، وكأن الجاني يقوم بتدمير الدليل بمجرد استعماله ويقوم بذلك بكل هدوء ودون إحداث أية ضجة، وذلك على خلاف الكثير من الجرائم[٢].

ثالثاً: الجرائم السيبرانية جريمة مستحدثة: تعد الجرائم السيبرانية من أبرز أنواع الجرائم المستحدثة التي يمكن أنْ تشكل خطراً جسيماً في ظل العولمة، فلا تعد هذه الجرائم من الغرابة سواءً التي تتعرض لها أجهزة الكمبيوتر أو التي تسخر تلك الأجهزة في إرتكابها، إذ إن التقدم التكنولوجي الذي تحقق خلال السنوات القليلة الماضية جعل العالم بمثابة قرية صغيرة، إذْ يتجاوز هذا التقدم بقدراته وإمكاناته أجهزة الدولة الرقابية بالشكل الذي أصبح يهدد أمنها وأمن مواطنيها[٣].

رابعاً: وقوع الجرائم الإلكترونية أثناء المعالجة الآلية للبيانات: إنَّ من خصائص الجرائم الإلكترونية أنَّها تقع أثناء عملية المعالجة الآلية للبيانات والمعطيات الخاصة بالكومبيوتر، ويمثل هذا النظام الشرط الأساسي الذي يتعين توافره حتى يمكن البحث في قيام أو عدم قيام أركان الجرائم الإلكترونية الخاصة بالتعدي على نظام معالجة البيانات، وذلك لأنَّ تخلُّف الشرط يعني إنتفاء الجرائم الإلكترونية، وذلك أنَّ الجرائم الإلكترونية تقع أثناء عملية المعالجة الآلية للبيانات في أي مرحلة من المراحل الأساسية لتشغيل نظام المعالجة الآلي للبيانات سواءً عند مرحلة إدخال البيانات، أو أثناء مرحلة المعالجة، أو أثناء مرحلة إخراج المعلومات[٤].

خامساً: عولمة الجرائم السيبرانية تثير مشاكل حول القانون الواجب التطبيق.

سادساً: جاذبية الجرائم السيبرانية: نظراً لما تمثله سوق الكمبيوتر من ثروة كبيرة فقد غدت أكثر جاذبية بإستثمار الأموال وغسلها وتوظيف الكثير منها في تطوير تقنيات وأساليب تمكن الدخول الى الشبكات وسرقة المعلومات[٥].

المطلب الثاني

التحديات التي يمثلها الأمن السيبراني وما هي العلاقة بينه وبين الأمن القومي

تواجه شبكات مؤسسات الدولة والشركات الكبرى تحديات أمنية جديدة يجلب الإرتباط مع شبكة الإنترنت، إذ أنشأة هذه المؤسسات والشركات مواقع لها على الإنترنت، وزودت موظفيها بخدمات البريد الإلكتروني، ومتصفحات إنترنت، وأصبح بذلك أمام المستخدم الخارجي المسلح ببعض المعرفة وبعض الأهداف الخبيثة، طريقة جديدة للتسلل الى الأنظمة الداخلية، حالما يصبح هذا الدخيل داخل شبكة المؤسسة أو الشركة، يمكنه أن يتجول فيها

يخرب أو يغير البيانات، أو يسرقها مسبباً ضرراً من مختلف الأنواع، وحتى إذا أخذنا أكثر تطبيقات الإنترنت إستخداماً وهو البريد الإلكتروني فإنه لا يعتبر مأموناً، يمكن لمن لديه محلل بروتوكولات (protocol analyzer) وإمكانية الوصول إلى الموجهات (router) والأجهزة الشبكية الأخرى التي تعالج البريد الإلكتروني أثناء إنتقاله من شبكة الى شبكة عبر الإنترنت أن يقرأ أو يغير الرسالة المرسلة، إذا لم تتخذ خطوات معينة لضمان سلامتها، تتصرف بعض مؤسسات الدولة والشركات وكأن التحديات الأمنية لم تكن خطراً حقيقياً، حيث تتطلع الى البنية التحتية لشبكة الإنترنت، كوسيلة رخيصة نسبياً وذلك لربط شبكتين أو عدة شبكات محلية (Lan) معزولة جغرافياً مع بعضها البعض أو للربط عن بعد مع شبكة ما.

وتجدر الإشارة الى أن الأعمال التجارية على شبكة الإنترنت والتي تتطلب الملايين من التبادلات المصرفية السرية، أصبحت قريبة من متناول الكثيرين، وتستجيب أسواق أمن الشبكات (Network SEcurity) بسرعة لتحديات أمن شبكة الإنترنت عن طريق تبني تقنيات التحقق (Authentication) والتشفير (Encryption) المتوفرة في هذا المجال لتطبيقها على روابط شبكة الإنترنت، وعن طريق تطوير منتجات جديدة في مجال أمن المعلومات.

وعليه ومما تقدم سنقسم دراسة هذا المطلب على فرعين، وهما ما يأتي:

الفرع الأول: التحديات التي يمثلها الأمن السيبراني

الفرع الثاني: السياسات الأمنية للشركات ومؤسسات الدولة لحماية بياناتها الرقمية

---

[١] د. نبيل العبيدي، عواد العبيدي: مدى ملائمة التشريعات الوطنية والدولية لمكافحة الإرهاب الدولي مع السياسة الجنائية، ط١، المركز القومي للإصدارات القانونية، مصر، ٢٠١٩، ص٥٤؛ مصطفى سعد حمد مخلف: جريمة الإرهاب عبر الوسائل الإلكترونية، دراسة مقارنة بين التشريعين الأردني والعراقي، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، الأردن، ٢٠١٧، ص٣٧؛ أمير فرج يوسف: الجرائم الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكومبيوتر والإنترنت، ط١، مكتبة الوفاء القانونية، مصر، ٢٠١١، ص٢٢٩-٢٣٠.

[٢] د. أيسر محمد عطية: دور الآليات الحديثة للحد من الجرائم المستحدثة الإرهاب الإلكتروني وطرق مواجهته، ورقة عمل مقدمة في الملتقى العلمي للجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية خلال الفترة من ٢-٢٠١٤/٩/٤م، الأردن، ٢٠١٤، ص١١-١٢؛ محمد علي محمد: كوارث الإرهاب الإلكتروني بين الفلسفة القانونية وتطور الأمن التقني، ط١، دار النهضة العربية، القاهرة، ٢٠١٨، ص٢٢.

[٣] د. مصطفى يوسف كافي: جرائم (الفساد، غسل الأموال، السياحة، الإرهاب الإلكتروني، المعلوماتية)، ط١، مكتبة المجتمع العربي للنشر والتوزيع، الأردن، ٢٠١٤، ص١٤٧؛ مصعب القطاونة: الإجراءات الجنائية الخاصة في الجرائم المعلوماتية، بحث مقدم لشبكة قانوني الأردن الإلكتروني، ٢٠١٠، ص٥؛ د. عبد القادر الشيخلي: طبيعة الإرهاب الإلكتروني، بحث مقدم الى المؤتمر العالمي (مكافحة الإرهاب) المملكة العربية السعودية، بتاريخ ٢٢-٢٥/شباط/٢٠١٥، ص٧-٨.

[٤] مشتاق طالب وهيب: مفهوم الجرائم المعلوماتية ودور الحاسوب بإرتكابها، بحث منشور في مجلة العلوم القانونية والسياسية، جامعة ديالى، مج٣، ع١، ٢٠١٤، ص٣٤٣؛ محمد علي سالم، حسون عبيد هجيج: الجرائم المعلوماتية، بحث منشور في مجلة جامعة بابل للعلوم الإنسانية، مج١٤، ع٢، العراق، ٢٠٠٧، ص٩٢.

[٥] كوثر حازم سلطان: مصدر سابق، ص٩٧٣.

الفرع الأول
التحديات التي يمثلها الأمن السيبراني

إن القضايا الإجتماعية والإقتصادية والسياسات العامة الجماهيرية والقضايا الإنسانية مهما تكن الجهة التي يتمم الإنسان نضره شَطرها، ومهما تتغير مسمياتها (أمن تكنولوجيا المعلومات وأمن الإتصالات)، فإن الأمن السيبراني يمس أمن الثروة الرقمية والثقافية للناس والمنظمات وللدول. بل إن التحديات التي ينطوي عليها ذلك معقدة، ويحتاج التصدي لها الى ضرورة توافر الإرادة السياسية اللازمة لتصميم وتنفيذ إستراتيجية لتطوير بنى تحتية وخدمات رقمية تشمل إستراتيجية للأمن السيبراني تكون متماسكة وفعالة وقابلة للتحقيق منها ومن إدارتها. ويجب أن تكون إستراتيجية الأمن السيبراني جزءاً من منهج متعدد التخصصات، مع وجود حلول جاهزة على المستويات التثقيفي، والقانوني، والتقني، والإداري. ويمكن للاستجابة القوية للأبعاد البشرية والقانونية والإقتصادية لاحتياجات أمن البنية الأساسية الرقمية لبناء الثقة، وأن تولد النمو الإقتصادي الرغوب فيه، والذي يفيد المجتمع كافة إن تملك زمام رصيد المعلومات، وتوزيع السلع غير الملموسة، وإضافة القيمة الى المحتوى، وسد الثغرة الرقمية كلها مشاكل ذات طبيعة إقتصادية وإجتماعية، تستلزم شيئاً أكثر من مجرد إتباع نهج وحيد البُعد وتكنولوجي بحت تجاه الأمن السيبراني[١].

إن غرض الأمن السيبراني هو المساعدة على حماية أصول وموارد منظمة من جميع النواحي التنظيمية والبشرية والمالية والتقنية والمعلوماتية بحيث تتمكن من أداء المهمة الموكلة إليها. إذ إن الهدف الأسمى لها هو ضمان عدم حدوث ضرر دائم للمنظمة، ويتألف ذلك من تقليل إحتمالات تجسد خطرٍ ما، والحد من الضرر أو سوء الأداء الناجمين، وتأمين عودة العمليات العادية الى مسيرتها الأولى بعد وقوع حادث أمني، وخلاة فترة زمنية مقبولة وبتكلفة معقولة. وتشمل عملية الأمن السيبراني المجتمع بأسره، بحيث يكون كل فرد مهتم بتنفيذه، ويمكن جعل هذه العملية أكثر أهمية عن طريق بلورة مدونة سلوك سيبراني، والإعلان عن سياسات أمن حقيقية تنص على المعايير التي يكون من المتوقع وفاء المستعملين، والكيانات والشركاء والموردين بها[٢].

إن تملك زمام رصيد المعلومات، وتوزيع السلع غير الملموسة، وإضافة القيمة الى المحتوى، وسد الثغرة الرقمية كلها مشاكل ذات طبيعة إقتصادية وإجتماعية، تستلزم شيئاً أكثر من مجرد إتباع نهج وحيد البُعد وتكنولوجي بحت تجاه الأمن السيبراني.

الفرع الثاني
السياسات الأمنية للشركات ومؤسسات الدولة لحماية بيناتها الرقمية

إن ربط شبكة الإنترنت مع أي نوع آخر من الشبكات لن يكون آمناً تماماً، وبدلاً من أن تلجأ الشركات الى تحقيق الأمن المطلق، عليها أن تعرف خطر تسرب المعلومات، وتحقق نوعاً من التوازن بين إحتمالات خرق الترتيبات الأمنية وبين كلفة تحقيق مختلف هذه الترتيبات[٣].

ترتكز الخطوة الأولى على إستنباط سياسة أمنية شاملة للشركة، أو على تطوير السياسة الأمنية المتبعة بحيث تأخذ في الاعتبار الربط مع الإنترنت ويجب أن تحدد هذه السياسة بالتفصيل، الموظفين الذين يحق لهم الوصول الى كل نوع من أنواع الخدمة التي يقدمها الإنترنت، كما يجب تثقيف الموظفين في مجال مسؤولياتهم تجاه حماية معلومات الشركة، مثل مسؤولياتهم تجاه حماية كلمات المرور التي يستخدموها. بالإضافة الى تحديد الإجراءات التي ستقوم الشركة بها في حال حدوث خرق لمثل هذه الخطة الأمنية، وتعتبر هذه السياسة أداة هامة جداً في تحديد المجالات التي ستنفق فيها أموال الشركة للحفاظ على أمن معلوماتها، ويقدم كتاب (site Security handbook) دليل أمن المواقع الذي أصدره مجموعة (Network Working Group) التابعة لهيئة (Internet Engineering task force) أو (IETF) فكرة جديدة عن الموضوعات التي يجب أخذها بعين الإعتبار عند وضع سياسات أمنية[٤].

تتطلب السياسة الأمنية كجزء من ترتيبها تقدير الكلفة التي ستتحملها الشركة في حال خرق الترتيبات الأمنية، ويجب أن ينخرط الموظفون على أعلى المستويات في هذه العملية، وقد يكون من المفيد أن تقوم الشركة بتوظيف مستشار لأمن الإنترنت، الإستشارة والنصح في هذا المجال وتبدأ بعد تحديد السياسة المتبعة، عملية تقويم إستخدام برامج الجدران النارية (encryption) والتشفير، (Firewall) والتثبت من المستخدم (Authentication).

وهناك بعض الأمثلة التطبيقية على السياسات الأمنية:

أولاً: مسح كلمة السر الخاصة بالموظف المنتهية عقدة فورا مثلاً كإجراء خلال سحب أوراقه من الشركة. استخدام الجهاز الخاص بالشركة الإنترنت، ويمنع إستخدام جهاز غيره مثلاً كأن يحضر (Laptop). لا يسمح بتبادل الرسائل داخل الشركة التي تحتوي على رسائل خاصة أو (Malicious gossip).

ثانياً: صلاحيات كل مستخدم على البيانات الموجودة على قاعدة البيانات.

ثالثاً: الدخول للشركة عن طريق البطاقة الخاصة.

---

(1) H Allen, Julia, The CERT Guide to System and Network Security practices, Boston. MA, Addison, Wesley. 2001.

(٢) د. عبد العزيز لطفي جاد الله: أمن المجتمع الإلكتروني، بين سياسة السوق الإلكترونية والتعاون الدولي في إطار مواجهة الجرائم الإلكترونية، ط١، مكتبة الوفاء القانونية، مصر، ٢٠١٧، ص٢١٧.

(٣) وليد أبو سعد: أمن المعلومات، الموسوعة العربية للكمبيوتر، قسم الدورات التعليمية الإلكترونية، ٢٠٠٥، ص٥-٦.

(٤) درّار نسيمة: الأمن المعلوماتي وسبل مواجهة مخاطره في التعامل الإلكتروني، دراسة مقارنة، إطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد- تلمسان، ٢٠١٧، ص٦٢.

رابعاً: وضع مثلاً أجهزة التحقق من بصمة الشخص على أجهزة البيانات المهمة.

المبحث الثاني

آليات مكافحة الجرائم السيبرانية

إن إزدياد الجرائم السيبرانية مرتبط مع التطور التكنولوجي الذي يعيشهُ العالم اليوم، إذ أنه مرتبط إرتباطاً وثيق بالأمن والسلم الدوليين، إذْ إن مكافحه الجرائم السيبرانية لا يعد على الجانب الوطني فقط، بل تمتد إلى بُعد دولي عالمي أيضاً، فالجرائم السيبرانية ترتكب في أغلب الأحيان من قبل أشخاص من خارج حدود الدولة، إذ تمر عبر شبكات إتصال دولية حتى تصل إلى النتيجة المبتغاة منه، كما إن إجراءات التفتيش والضبط تمتد إلى خارج نطاق إقليم الدولة من خلال تعاون ومجهود دولي منسق بين الدول والمنظمات التي تضررت من جراء هذه الجرائم، حتى يتم القضاء عليها، وهذا بدوره يحتاج إلى إنشاء أجهزه أمن دولية مشتركة وعقد إتفاقيات مشتركة للقضاء على هذه الجرائم والحد منها.

وعليه ومما تقدم سنتناول دراسة هذا المبحث على مطلبين، وهما مايأتي:

المطلب الأول: جهود المنظمات الدولية في مكافحة الجرائم السيبرانية

المطلب الثاني: التعاون الدولي في مكافحة الجرائم السيبرانية

المطلب الأول

جهود المنظمات الدولية في مكافحة الجرائم السيبرانية

من المعلوم أن أحد الأهداف الرئيسية لمنظمة الأمم المتحدة هو حفظ السلم والأمن الدوليين، حيث تغيرت الطرق التي تجري فيها النزاعات المسلحة في السنوات الأخيرة، إذ إنتقلت المعارك من المجال المادي الى مجال إفتراضي يسمى بالفضاء السيابر والحروب السيبرانية، ولهذا السبب قد تمكن العديد من الأشخاص من المشاركة في العمليات العدائية والنزاعات المسلحة الحديثة، ومن أجل الوصول الى تلك الغاية، فإن هذه المنظمة وبعض المنظمات الأخرى تميل الى إتخاذ إجراءات دولية لسحق العدوان ورد المتعدي. وعليه سنتناول دراسة هذا المطلب على نقطتين.

أولاً: دور منظمة الأمم المتحدة:

بالرغم من كون ميثاق منظمة الأمم المتحدة لم ينصْ صراحةً على تجريم استخدام المعلومات كأداة إرهابية ضمن إطار ما يعرف بـــ الإرهاب السيبراني، إلّا أنَّ روح الميثاق يتفق مع تجريم استخدامه بوصفه إنتهاك لما ورد في الميثاق بخصوص "التهديد أو استخدام القوة ضد السلامة الإقليمية أو الإستقلال السياسي لأي دولة"، ومع الأخذ في الإعتبار أنَّ الميثاق جاء لمكافحة النزاعات المسلحة، على اعتبار إن الجرائم السيبرانية واستخدام حرب المعلومات يقعان ضمن العدوان، حيث إن هذا النوع من الإرهاب لا يتفق مع السيادة الدولية، لأنه يهدد العلاقات الدولية باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الإستقلال السياسي لأية دولة أو على أي وجه آخر لا يتفق ومقاصد منظمة الأمم المتحدة[١].

وتبذل منظمة الأمم المتحدة جهوداً فاعلة لا يستهان بها في مجال مكافحة الجرائم السيبرانية الدولية، وذلك لمنع محاولات الإعتداء من قبل إرهابي الإرهاب السيبراني على أمن الدولة وأفرادها، ويتمثل هذا الجهد في المؤتمرات التي تعقد برعايتها والخاصة بمنع الجريمة ومعاملة السجناء[٢]، وكذلك مؤتمرات الجمعية الدولية لقانون العقوبات[٣] التي تعقد كل خمس سنوات، إذ تسعى منظمة الأمم المتحدة من خلال هيئاتها والوكالات التابعة لها لوضع الإطار التشريعي لهذه الظاهرة الإجرامية المستحدثة، وكانت الإنطلاقة بهذا الشأن في المؤتمر السابع المنعقد بميلانو(عام ١٩٨٠)، والذي أكد على الإستفادة من التطورات العلمية والتكنولوجية في مواجهة هذه الظاهرة الإجرامية المتعلقة بالحاسوب الآلي[٤]، وفي المؤتمر التاسع برعاية منظمة الأمم المتحدة في القاهرة (عام ١٩٩٥) تم التأكيد على وجوب حماية مخاطر التكنولوجيا، ووجوب التنسيق والتعاون بين الدول، وفي المؤتمر العاشر لمنع الجريمة في بودابست جرى اعتبار جرائم الحاسوب الآلي نمطاً جديداً من الجرائم المستحدثة مع وجوب العمل للحد من أعمال القرصنة الإلكترونية[٥]، وأقرتْ الجمعية العامة للأمم المتحدة في الدورة (٥٦/ ٢٥٨) في (٣١ كانون الثاني عام ٢٠٠٢) قراراً يدعو إلى استخدام تكنولوجيا الإتصال والمعلومات من أجل التنمية، وجاء هذا بعد سلسلة من القرارات الدولية لتنبيه الرأي العام العالمي وتنمية الوعي بحجم المخاطر بسبب هذه الجرائم، هذا وأصبحتْ قضية أمن المعلومات مرتبطة بحظر استخدام تكنولوجيا الإتصال والمعلومات للتأثير أو الهجوم على وسائل تكنولوجيا الإتصال والمعلومات الخاصة بدولةٍ أخرى، إذْ أنَّ هذه المواقف تشكل تهديداً للأمن والسلم الدوليين[٦].

وإنَّ تزايد الجرائم المرتكبة عبر الإنترنت تثير مشاكل، وهذا ما أدى بمنظمة الأمم المتحدة الى عقدِ اتفاقيةٍ خاصةٍ لمكافحة إساءة استعمال التكنولوجيا الإجرامية لسنة (٢٠٠٠)، والذي أكد على الحاجة الى التعزيز والتنسيق والتعاون بين الدول في مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية[٧].

---

[١] د. سامر مؤيد عبد اللطيف، د. نوري رشيد الشافعي: دور المنظمات الدولية في مكافحة الإرهاب الرقمي، جامعة كربلاء، ٢٠١٦، ص١٥، بحث منشور عبر الرابط الآتي:
http://elearning.uokerbala.edu.iq/mod/resource/view.php?id=12861، (آخر زيارة للموقع في ٢٠١٨/٧/٢، ٢:٠٥م).

[٢] د. علي يوسف الشكري: المنظمات الدولية، ط١، دار صفاء للنشر والتوزيع، عمان، ٢٠١٢، ص٩٧-٩٨.

[٣] الجمعية الدولية لقانون العقوبات، هي جمعية أُنشئت في عام ١٩٨٩ ومقرها في باريس فرنسا، ولها الصفة الإستشارية لدى هيئة الأمم المتحدة.

[٤] مريم محمد حسن: التنظيم القانوني لجريمة التجسس المعلوماتي، رسالة ماجستير، كلية القانون، جامعة الكوفة، العراق، ٢٠١٦، ص١٦٢.

[٥] محمود أحمد عبابنة: جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، الأردن، ٢٠٠٥، ص١٥٦-١٥٧.

[٦] د. سامر مؤيد عبد اللطيف، د. نوري رشيد الشافعي: دور المنظمات الدولية في مكافحة الإرهاب الرقمي، مصدر سابق، ص٢٠، (آخر زيارة للموقع في ٢٠١٨/٧/٢، ٢:٠٥م).

[٧] اتفاقية مكافحة إستعمال تكنولوجيا المعلومات لأغراض إجرامية رقم (٦٣/٥٥) الصادرة عن هيئة منظمة الأمم المتحدة، لسنة ٢٠٠٠.

وقد صدر أيضا عن الجمعية العامة للأمم المتحدة القرار رقم (٤٥/ ٩٥) الصادر في (١٤/ ١٢ /١٩٩٠)، والذي يتعلق بشكل دقيق بالمعطيات الحساسة والتي تعني بموجب هذا القرار كل معلومة تؤدي إلى التفرقة العنصرية أو التميز بشكل عام بين البشر مثل معلومات عن العرق، اللون، الآراء السياسية، الآراء الفلسفية.... الخ[١].

هذا وقد نبَّه مجلس الأمن في القرار ذي العدد (١٩٦٣) لعام ٢٠١٠) إلى "ازدياد استخدام الإرهابيين التكنولوجيا الجديدة للمعلومات والإتصالات وخاصه الإنترنت لأغراض التجنيد عبر الإنترنت وكذلك التحريض على دعم الأعمال الإرهابية" بوصفها أنماط مستحدثة لإستخدامات الإرهابيين لمعطيات الشبكة الدولية للمعلومات، وكان القرار ذي العدد (٢٢٥٥ في شباط عام ٢٠١٥) أكثر شمولاً لطرق استخدام الإرهابيين للإنترنت في أنشطتهم الإرهابية، إذْ تضمن "الإعراب عن قلقه من تزايد لجوء الإرهابيين إلى استعمال تكنولوجيا المعلومات ولا سيما شبكة الإنترنت من أجل تسيير الأعمال الإرهابية والتحريض على الإرهاب أو تجنيد مرتكبيها أو تمويلها"[٢].

وفي مؤتمر منظمة الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية عام (٢٠١٠)، عُقد هذا المؤتمر في سلفادور- البرازيل من (١٢-١٩ نسيان عام ٢٠١٠) تحت عنوان إستراتيجيات شاملة في تحديات عالمية والذي نظم منع الجريمة والعدالة الجنائية وتطورها في عالمٍ متغيّر، وتضمن جدول الأعمال ثمانية بنود وكان من ضمنها جرائم الإنترنت، والتعاون الدولي في مكافحة هذه الجريمة[٣].

ثانياً: مجموعة الدول الثماني: G-8):

في واشنطن عام (١٩٩٧) أنشأتْ مجموعة الدول الثماني (G-8) الفريق الفرعي للجرائم الإرهابية الإلكترونية التقنية في قمة مجموعة (G-8) في (١١/١٠/ ٢٠٠٤)، حيث تمّ اعتماد وزراء العدل والداخلية التابعين لبلدان مجموعة (G-8) في إجتماعاتهم المختلفة آلية لمكافحة العديد من جرائم الإنترنت والتي تستند الى المبادئ التالية:

١- التنسيق بين جميع الدول المعنية في ملاحقة مرتكبي جرائم الإنترنت ومحاكمتهم بصرف النظر عن مكان حدوث الضرر.

٢- عدم إتاحة ملاذات آمنة للمعتدين على تكنولوجيا المعلومات، تدريب الموظفين المكلفين بتنفيذ القوانين.

٣- تجهيزهم بالمعدات الضرورية للتعامل مع الجرائم ذات التقنية العالمية[٤].

وفي بيان صادر عن إجتماع مجموعة الدول الثماني (G-8) عام ٢٠٠٥ تم التأكيد على أنَّ وكالات إنفاذ القانون تستجيب بسرعة لتهديدات الجرائم السيبرانية والحوادث الخطيرة، وفي إجتماع مجموعة الدول الثماني (G8) في (موسكو- روسيا) عام (٢٠٠٦) تمتْ مناقشة الجرائم السيبرانية وقضايا الفضاء الإلكتروني (Cyberspace)، وصدر بيان موسكو الذي تم التأكيد فيه على منع الأعمال الإجرامية المحتملة وإتخاذ التدابير الضرورية، وكذلك إجتماع وزراء العدل والداخلية لدول مجموعة الثماني (G-8) في (٢٣-٢٥ آيار عام ٢٠٠٧) في (ميونخ المانيا): واتفق الأعضاء على العمل من خلال الأُطر القانونية لتجريم أشكال معينة بشأن استخدام الإنترنت لأغراض إرهابية وكذلك إجتماع الدول الثماني (G8) في (إيطاليا) عام (٢٠٠٩)، إذْ إلتقى وزراء العدل والداخلية في روما (٢٨ -٣٠ آيار ٢٠٠٩)، وأصدرتْ القمة بياناً تضمَّن جرائم الإنترنت والأمن السيبراني، وأشار البيان الذي قُدِّم لمفوضية منظمة الأمم المتحدة لمنع الجريمة والعدالة الجنائية إلى أنَّ التقدم التكنولوجي أسفر عن إساءة استعمال الشبكات الإجتماعية، وخدمات التشفير، وأنَّ الهجمات الإجرامية الجديدة المتطورة الأخرى على أنظمة المعلومات تشكل تحديات إضافية تواجه إنفاذ القانون، وكذلك في قمة الدول ثماني (G-8) في (دوفيل فرنسا ٢٦ آيار ٢٠١١) ، والتي صدر فيها الجزء الثاني من الإعلان في قضايا الإنترنت في البنود (٤ الى ٢٢)، وأكد الإعلان على أنَّ شبكة الإنترنت أصبحتْ ضرورية في كافة أنحاء دول العالم لمجتمعاتنا وإقتصادياتها ونموها، وهي مصدر للتعليم ولتعزيز الحرية والديمقراطية وحقوق الإنسان، ودعى الإعلان الى تعزيز التعاون داخل جميع المحافل الدولية التي تتناول حركة الإنترنت[٥].

ويتضح مما تقدم أنَّ منظمة الأمم المتحدة بذلتْ جهوداً كبيرةً لمكافحةِ الجرائم السيبرانية من خلال إصدار قرارات عن طريق مجلس الأمن والجمعية العامة للأمم المتحدة، ولكنْ مثل هذه الجرائم تتطلب المزيد من الجهود بسبب الحداثة والتطور الهائل، وكذلك عمِلتْ مجموعة الدول (G-8) على مكافحة الجرائم السيبرانية من خلال الإعلانات والمؤتمرات والملتقيات والإجتماعات، وذلك لمكافحة الجرائم السيبرانية وتعزيز الحرية والديمقراطية وحقوق الإنسان وتعزيز التعاون الدولي في جميع المحافل الدولية التي تتناول قضايا الإنترنت.

المطلب الثاني
التعاون الدولي مكافحة الجرائم السيبرانية

تكمن أهمية التعاون الأمني الدولي بضرورة شعور المجتمع الدولي بمخاطر الجرائم السيبرانية وما يمكن أن تحدثهُ من آثار سلبية على مصالح المجتمع الدولي المشتركة، وإدراكه للنمو السريع والمتزايد لهذا النمط المستجد والخطر من الجرائم الإرهابية الإلكترونية[٦]، حيث تمثل هذه الجرائم نقطه مشتركة تتلاقى فيها جهود المجتمع الدولي في بذل الإهتمام لأجل إتخاذ

---

[١] محروس نصار غايب: الجريمة المعلوماتية، بحث منشور في مجلة التقني، مج٢٤، الإصدار٩، العراق، ٢٠١١، ص١١٨.

[٢] د. سامر مؤيد عبد اللطيف، د. نوري رشيد الشافعي: دور المنظمات الدولية في مكافحة الإرهاب الرقمي، مصدر سابق، ص٢٣، (آخر زيارة للموقع في ٢٠١٨/٧/٢، ٢:٠٥م).

[٣] د. ليلى الجنابي: فعالية القوانين الوطنية والدولية لمكافحة جرائم السيبرانية، ٢٠١٧، بحث منشور عبر شبكة الإنترنت متاح على الرابط الاتي: www.m.ahewar.org/s.asp/aid=5714238r=0 ، (آخر زيارة للموقع في٢٠١٨/٧/٢٠، ٣:٠٠م).

[٤] د. خالد حسن أحمد لطفي: الإرهاب الإلكتروني آفة العصر الحديث والآليات القانونية للمواجهة، ط١، دار الفكر الجامعي، الإسكندرية، ٢٠١٨، ص١٥٩.

[٥] د. خالد حسن أحمد لطفي: المصدر نفسه، ص١٦٠.

[٦] د. هناء إسماعيل إبراهيم الأسدي: الإرهاب وغسيل الأموال كأحد مصادر تمويلة، دراسة مقارنة، ط١، منشورات زين الحقوقية، بيروت، ٢٠١٥، ص٦٩٨.

تدابير وآليات وتدعيم سبل التعاون الدولي في مكافحة تلك جرائم، وهذا التعاون يكون بين أجهزة الشرطة الدولية المتخصصة لمكافحه الجرائم السيبرانية عن طريق إنشاء مكاتب متخصصه لجمع المعلومات عن مرتكبي هذه الجرائم وتعميمها، فينبغي أن يكون هناك تعاون بين أجهزة الشرطة المختلفة في الدول، والتنسيق فيما بينهم لضبط المجرمين ومكافحه هذه الجرائم التي تتجاوز حدود الدولة[١].

وفي ضوء ما تقدم سنتناول دراسة هذا المطلب على ثلاثة نقاط، هي ما يأتي:

أولاً: صور التعاون الأمني الدولي لمكافحة الإرهاب الإلكتروني: ومن أهم هذه الصور هي ما يأتي:

١- ربط شبكات الإتصال والمعلومات: تحتاج الأجهزة الشرطية إلى وسائل للإتصال تحقق السرعة الممكنة في أجهزة العدالة الجزائية من خلال التواصل بين سلطات التحقيق والملاحقة المختلفة، وهذا ما عمدت له الدول والمنظمات الدولية بتطوير الإتصال وتبادل المعلومات فيما بينها[٢].

٢- القيام ببعض العمليات الشرطية والأمنية المشتركة: تشترك الدول فيما بينها للقيام بعمليات شرطية وأمنية بما يؤدي إلى صقل مهارات وخبرات القائمين على مكافحة تلك الجرائم ووضع حدٍ لها، وذلك من خلال تعقب المجرم وتعقب الأدلة الرقمية وضبطها، والقيام بعمليه التفتيش العابرة للحدود لمكونات الحاسوب الآلي والأنظمة المعلوماتية وشبكات الإتصال بحثاً عما قد تحويه من أدلة وبراهين على إرتكاب الجرائم الإرهابية الإلكترونية، فالقيام بهذه الأمور يستدعي هكذا عمليات[٣].

ثانياً: التعاون الأمني وجهود المنظمة الدولية للشرطة الجنائية (الإنتربول) في مكافحة الجرائم السيبرانية الدولية: أُنشأت منظمة الإنتربول عام (١٩٢٣)، وهي أكبر منظمة دولية مقرها الرئيسي في مدينة ليون بفرنسا، وقد أنشأت هذه المنظمة وحدة تحليل المعلومات الجنائية والتي تقضي بإستخلاص المعلومات الهامة عن المنظمات الإجرامية وتبويبها، وذلك بهدف وضع تلك المعلومات في متناول هيئة الشرطة، أو الدول الأعضاء في الإنتربول، حيث تعمل هذه المنظمة على تأكيد وتشجيع التعاون بين سلطات البوليس[٤].

كذلك قد أنشأت هذه المنظمة خلال عام (٢٠٠٤) وحدات خاصه لمكافحة جرائم التكنولوجيا، كما قامت المنظمة بالتعاون مع مجموعة الدول الثمانية الكبرى (G-8)[٥] بوضع إستراتيجيات لمواجهة هذا النوع من الجرائم، وأبرزها إنشاء مركز إتصالات أمني عبر الشبكة المعلوماتية يعمل على مدار (٢٤ ساعة) على مستوى الشرطة في الدول الأطراف، وإستخدام وسائل حديثه في تلك العملية، وتزويد شرطة الدول الأطراف بكتيبات إرشادية حول الجرائم الإرهابية الإلكترونية وكيفية التدريب على مكافحتها والتحقيق فيها، وبالتالي فإن هذه الجرائم تعد عالميه وآثارها تمتد لأكثر من دولة[٦].

ويحصل تدعيم التعاون بين سلطات البوليس في الدول المختلفة من خلال إبرام إتفاقيات دولية، بحيث إذا اكتشفت الشرطة الوطنية لدولة ما جريمة تم بثها على الإنترنت من خلال موقع موجود بالخارج، فإنها تقوم بإبلاغ البوليس بالدولة التي تم فيها البث، لذلك يجب على كل دولة تعيين إدارة لتلقي هذه البلاغات، وإتخاذ الإجراءات القانونية طبقا لقوانين كل دولة، هذا ونجد إن بعض الدول تلزم مستخدم شبكة الإنترنت بتسجيل نفسهُ لدى مكاتب الشرطة، فبوليس الإنترنت هو نوع من الإجراءات والضمانات للمحافظة على أموال الغير وأسرارهم[٧]، وبهذا فإن دور الإنتربول لا يقتصر على مجرد إرسال النشرات الدولية ومتابعتها، بل يمتد إلى إجراءات الملاحقة، وتتبع الشخص المطلوب والتحفظ عليه[٨].

ثالثاً: تبادل التعاون لمواجهة الكوارث والأزمات والمواقف الحرجة: يمثل عنصر الوقت دوراً أساسياً في المواقف الحرجة، ومن الأمور الحاسمة في مواجهة الأمر الذي يحتاج إلى تكثيف الجهود الخاصة والخبرات والإمكانيات بشكل يصعب تحقيقه إلا بتظافر الجهود الدولية، وهذا التعاون الأمني يمثل أهم الصور لمكافحة الجرائم السيبرانية الدولية، سيما وأن أجهزة العدالة الجزائية ليست بنفس المستوى والجاهزية في جميع الدول، وإنما هناك تفاوت فيما بينها، فبعض الدول المتقدمة تقنياً وتكنولوجياً لها دور كبير في مواجهة مثل هذه الجرائم تشريعياً وفنياً، والبعض الأخر تفتقد لذلك، ومن هنا كان لابد من التعاون بين الدول[٩].

إذ يتضح مما تقدم ضرورة التعاون الدولي للحد من مخاطر الجرائم السيبرانية بإعتباره أحد الأخطار الحالية والمستقبلية، إذ أن التعاون بين جميع الدول في جميع المجالات يقلل من نسبة خطورة هذه الجرائم، وكذلك زيادة التعاون في مجال التدريب لزيادة الثقة والوعي لرجال الشرطة والعدالة الجزائية.

---

[١] أحمد سعد محمد الحسيني: الجوانب الإجرائية للجرائم الناشئة عن إستخدام الشبكات الإلكترونية، إطروحة دكتوراه، كلية الحقوق، جامعة عين شمس، مصر، ٢٠١٢، ص٤٢٧٨؛ د. جميل عبد الباقي الصغير: الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٢، ص٧٥.

[٢] د. عادل عبد العال إبراهيم خراشي: إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة، الإسكندرية، ٢٠١٥، ص٢٤-٢٥.

[٣] د. سليمان أحمد محمد فضل: المواجهة التشريعية والأمنية للجرائم الناشئة عن إستخدام شبكة المعلومات الدولية (الإنترنت)، دار النهضة العربية، القاهرة، ٢٠١٣، ص٤١٥-٤١٦.

[٤] نسرين عبد الحميد نبيه: الجرائم الدولية والإنتربول، المكتب الجامعي الحديث، مصر، ٢٠١١، ص٢٥٤.

[٥] مجموعة الثمانية أو مجموعة الدول الصناعية الثمانية تضم الدول الصناعية الكبرى في العالم أعضائها هم: الولايات المتحدة الأمريكية، اليابان، ألمانيا، روسيا الاتحادية، إيطاليا، المملكة المتحدة، فرنسا، وكندا، ويمثل مجموع اقتصاد هذه الدول الثمانية ٦٥% منإقتصاد العالم وأغلبية) القوة العسكرية تحتل ٧ من ٨ مراكز الأكثر أنفاقاً على التسلح وتقريباً كل الأسلحة النووية عالمياً)، وأنشطة المجموعة تتضمن مؤتمرات على مدار السنة ومراكز بحث سياسية مخرجاتها تتجمع في القمة السنوية التي يحضرها زعماء الدول الأعضاء.

[٦] نبيلة هبة هروال: الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الإستدلالات، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، ٢٠٠٧، ص١٥٣؛ محمد أمين الرومي: جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية، ٢٠٠٣، ص١٣٦.

[٧] د. علاء الدين شحاته: التعاون في مجال مكافحة الجريمة، إتراك للنشر والتوزيع، القاهرة،٢٠٠٠، ص١١٠.

[٨] د. محمد نيازي حتاتة: حماية الأمن العام مكافحة الجريمة على المستوى الوطني والإقليمي والدولي، الضوابط الإجرائية الوطنية والعالمية وصكوك المبادئ الإرشادية العالمية والإتفاقيات الدولية، ج١، مطبعة كلية الشرطة، القاهرة، ١٩٩٥، ص٢٩٩.

[٩] أحمد سعد محمد الحسيني: مصدر سابق، ص٢٧٩؛ د. عادل عبد العال إبراهيم خراشي: مصدر سابق، ص٢٨-٢٩.

الخاتمة

من مجمل بحثنا في موضوع (جرائم الأمن السيبراني وآليات ومكافحتها في إطار القانون الدولي) توصلنا الى جملة من الإستنتاجات والتوصيات بهذا الشأن، وعلى النحو الآتي:

أولاً: الإستنتاجات:

١- عدم وجود إجماع فقهي على تعريف معين للجرائم السيبرانية، وذلك يرجع الى الإختلاف حول تحديد نطاق الجرائم السيبرانية خصوصاً أنَّ بعض الفقه وسع كثيراً من هذا النطاق فَعَدَ الجرائم السيبرانية كل أشكال السلوك غير المشروع الذي يرتكب بإستخدام الحاسوب الآلي.

٢- إنَّ للجرائم السيبرانية الدولية خصائص وأهداف وأشكال تميزها عن بقية الجرائم الإعتيادية والسياسية، فالجرائم السيبرانية تختلف عن الجرائم العادية في إسلوب إرتكابها وشخص مرتكبها والوسيلة المستعملة في إرتكابها، وهي من الجرائم صعبة الإكتشاف كما أنَّها تحتاجُ إلى خبراءَ مختصين في التحقيق فيها.

٣- إنَّ منظمة الأمم المتحدة بذلتْ جهوداً كبيرةً لمكافحةِ الجرائم السيبرانية من خلال إصدار قرارات عن طريق مجلس الأمن والجمعية العامة للأمم المتحدة، ولكن مثل هذه الجرائم تتطلب المزيد من الجهود بسبب الحداثة والتطور الهائل، وكذلك عملت مجموعة الدول (G-8) على مكافحة الجرائم السيبرانية من خلال الإعلانات والمؤتمرات والملتقيات والإجتماعات وذلك لمكافحة الجرائم السيبرانية وتعزيز الحرية والديمقراطية وحقوق الإنسان وتعزيز التعاون الدولي في جميع المحافل الدولية التي تتناول قضايا الإنترنت.

ثانياً: التوصيات:

١- العمل على اعتماد تعريف جامع مانع للجرائم السيبرانية الدولية، من خلالِ عقد مؤتمر دولي بإشراف الأمم المتحدة، ويتم من خلاله تحديد تعريف للجرائم السيبرانية، وتحديد خطة عملية دولية لمكافحته بجميع صورها وأشكالها، مع إحترام سيادة الدول الأعضاء.

٢- إصدار اتفاقية مستقلة لمكافحة الجرائم السيبرانية الدولية وصورها المختلفة، تحت عنوان "الاتفاقية الدولية لمكافحة الجرائم السيبرانية" والتي تسد الثغرات التي تكتنف الجرائم السيبرانية الدولية، وأنْ تتضمَّنَ هذه الاتفاقية بالإضافةِ إلى النصوصِ الموضوعية، نصوصاً إجرائية مناسبة للتحقيق في الجرائم السيبرانية وأساليب إرتكابها.

٣- ضرورة التعاون الدولي للحد من مخاطر الجرائم السيبرانية بإعتباره أحد الأخطار الحالية والمستقبلية، إذ أن التعاون بين جميع الدول في جميع المجالات يقلل من نسبة خطورة هذه الجرائم، وكذلك زيادة التعاون في مجال التدريب لزيادة الثقة والوعي لرجال الشرطة والعدالة الجزائية.

٤- إيجاد منظومة قانونية دولية تحت مظلة الأمم المتحدة يعهد إليها توحيد جهود الدول في مكافحة الجرائم السيبرانية، ويتفرع منها جهة أو هيئة محايدة، تتولى التحقيق في الجرائم السيبرانية، ويكون لها سلطة الأمر بضبط وإحضار المجرم للتحقيق معه أياً كان مكان وجوده وجنسية بلده.

المصادر

القران الكريم

أولاً: الكتب:

١. د. أحمد عبيس نعمة الفتلاوي: الهجمات السيبرانية، دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، ط١، منشورات زين الحقوقية، بيروت، ٢٠١٨.
٢. أسامة أحمد المناعسة، وآخرون: جرائم الحاسوب الآلي والإنترنت، ط١، دار وائل للنشر، الأردن، ٢٠٠١.
٣. أمير فرج يوسف: الجرائم الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكومبيوتر والإنترنت، ط١، مكتبة الوفاء القانونية، مصر، ٢٠١١.
٤. د. جميل عبد الباقي الصغير: الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، ٢٠٠٢.
٥. د. خالد حسن أحمد لطفي: الإرهاب الإلكتروني آفة العصر الحديث والآليات القانونية للمواجهة، ط١، دار الفكر الجامعي، الإسكندرية، ٢٠١٨.
٦. د. سليمان أحمد محمد فضل: المواجهة التشريعية والأمنية للجرائم الناشئة عن إستخدام شبكة المعلومات الدولية (الإنترنت)، دار النهضة العربية، القاهرة، ٢٠١٣.
٧. د. عبد العزيز لطفي جاد الله: أمن المجتمع الإلكتروني، بين سياسة السوق الإلكترونية والتعاون الدولي في إطار مواجهة الجرائم الإلكترونية، ط١، مكتبة الوفاء القانونية، مصر، ٢٠١٧.
٨. د. عادل عبد العال إبراهيم خراشي: إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة، الإسكندرية، ٢٠١٥.
٩. د. علاء الدين شحاته: التعاون في مجال مكافحة الجريمة، إتراك للنشر والتوزيع، القاهرة،٢٠٠٠.
١٠. د. علي يوسف الشكري: المنظمات الدولية، ط١، دار صفاء للنشر والتوزيع، عمان، ٢٠١٢.
١١. محمد أمين الرومي: جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية، ٢٠٠٣.
١٢. محمد أمين الشواكبة: جرائم الحاسوب الإنترنت، ط٤، دار الثقافة للنشر والتوزيع، الأردن، ٢٠١١.
١٣. محمد علي محمد: كوارث الإرهاب الإلكتروني بين الفلسفة القانونية وتطور الأمن التقني، ط١، دار النهضة العربية، القاهرة، ٢٠١٨.

١٤. د. محمد نيازي حتاتة: حماية الأمن العام مكافحة الجريمة على المستوى الوطني والإقليمي والدولي، الضوابط الإجرائية الوطنية والعالمية وصكوك المبادئ الإرشادية العالمية والإتفاقيات الدولية، ج١، مطبعة كلية الشرطة، القاهرة، ١٩٩٥.
١٥. محمود أحمد عبابنة: جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، الأردن، ٢٠٠٥.
١٦. د. مصطفى يوسف كافي: جرائم (الفساد، غسل الأموال، السياحة، الإرهاب الإلكتروني، المعلوماتية)، ط١، مكتبة المجتمع العربي للنشر والتوزيع، الأردن، ٢٠١٤.
١٧. منير البعلبكي: المورد قاموس إنكليزي- عربي، دار العلم للملايين، بيروت، ٢٠٠٤.
١٨. د. نبيل العبيدي، عواد العبيدي: مدى ملائمة التشريعات الوطنية والدولية لمكافحة الإرهاب الدولي مع السياسة الجنائية، ط١، المركز القومي للإصدارات القانونية، مصر، ٢٠١٩.
١٩. نبيلة هبة هروال: الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الإستدلالات، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، ٢٠٠٧.
٢٠. نسرين عبد الحميد نبيه: الجرائم الدولية والإنتربول، المكتب الجامعي الحديث، مصر، ٢٠١١.
٢١. د. هناء إسماعيل إبراهيم الأسدي: الإرهاب وغسيل الأموال كأحد مصادر تمويلة، دراسة مقارنة، ط١، منشورات زين الحقوقية، بيروت، ٢٠١٥.
٢٢. وليد أبو سعد: أمن المعلومات، الموسوعة العربية للكمبيوتر، قسم الدورات التعليمية الإلكترونية، ٢٠٠٥.

ثانياً: الرسائل والأطاريح الجامعية:

١. أحمد سعد محمد الحسيني: الجوانب الإجرائية للجرائم الناشئة عن إستخدام الشبكات الإلكترونية، إطروحة دكتوراه، كلية الحقوق، جامعة عين شمس، مصر، ٢٠١٢.
٢. درّار نسيمة: الأمن المعلوماتي وسبل مواجهة مخاطره في التعامل الإلكتروني، دراسة مقارنة، إطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد- تلمسان، ٢٠١٧.
٣. مريم محمد حسن: التنظيم القانوني لجريمة التجسس المعلوماتي، رسالة ماجستير، كلية القانون، جامعة الكوفة، العراق، ٢٠١٦.
٤. مصطفى سعد حمد مخلف: جريمة الإرهاب عبر الوسائل الإلكترونية، دراسة مقارنة بين التشريعين الأردني والعراقي، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، الأردن، ٢٠١٧.

ثالثاً: البحوث والمؤتمرات:

١. د. أيسر محمد عطية: دور الآليات الحديثة للحد من الجرائم المستحدثة الإرهاب الإلكتروني وطرق مواجهته، ورقة عمل مقدمة في الملتقى العلمي للجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية خلال الفترة من ٢-٢٠١٤/٩/٤م، الأردن، ٢٠١٤.
٢. د. عبد القادر الشيخلي: طبيعة الإرهاب الإلكتروني، بحث مقدم الى المؤتمر العالمي (مكافحة الإرهاب) المملكة العربية السعودية، بتاريخ ٢٢-٢٥/شباط/٢٠١٥.
٣. كوثر حازم سلطان: موقف القانون والقضاء من الجريمة الإلكترونية (السيبرانية)، دراسة مقارنة، بحث منشور في مجلة كلية التربية الأساسية، الجامعة المستنصرية، العراق، مج٢٢، ع٩٦، ٢٠١٦.
٤. محروس نصار غايب: الجريمة المعلوماتية، بحث منشور في مجلة التقني، مج٢٤، الإصدار ٩، العراق، ٢٠١١.
٥. محمد علي سالم، حسون عبيد هجيج: الجرائم المعلوماتية، بحث منشور في مجلة جامعة بابل للعلوم الإنسانية، مج١٤، ع٢، العراق، ٢٠٠٧.
٦. د. محمد محي الدين عوض: مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر)، ورقة عمل مقدمة الى المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، ١٩٩٣.
٧. مشتاق طالب وهيب: مفهوم الجرائم المعلوماتية ودور الحاسوب بإرتكابها، بحث منشور في مجلة العلوم القانونية والسياسية، جامعة ديالى، مج٣، ع١، ٢٠١٤.
٨. مصعب القطاونة: الإجراءات الجنائية الخاصة في الجرائم المعلوماتية، بحث مقدم لشبكة قانوني الأردن الإلكتروني، ٢٠١٠.

رابعاً: الوثائق والاتفاقيات الدولية:

١. الوثيقة: UNODC/CCPCJ/EG.4/2013/2.
٢. اتفاقية مجلس أوربا المتعلقة بالجرائم الإلكترونية، مجموعة المعاهدات الأوربية رقم ١٨٥، بودابست عام ٢٠٠١.
٣. اتفاقية مكافحة إستعمال تكنولوجيا المعلومات لأغراض إجرامية رقم (٦٣/٥٥) الصادرة عن هيئة منظمة الأمم المتحدة، لسنة ٢٠٠٠.

خامساً: المصادر المتاحة عبر الشبكة الدولية للمعلومات

١. د. سامر مؤيد عبد اللطيف، د. نوري رشيد الشافعي: دور المنظمات الدولية في مكافحة الإرهاب الرقمي، جامعة كربلاء، ٢٠١٦، ص١٥، بحث منشور عبر الرابط الآتي: http://elearning.uokerbala.edu.iq ، (آخر زيارة للموقع في ٢٠١٨/٧/٢، ٠٥:٢م).
٢. د. ليلى الجنابي: فعالية القوانين الوطنية والدولية لمكافحة جرائم السيبرانية، ٢٠١٧، بحث منشور عبر شبكة الإنترنت متاح على الرابط الاتي: www.m.ahewar.org/s.asp/aid=5714238r=0 ، (آخر زيارة للموقع في٢٠١٨/٧/٢٠، ٠٠:٣م).

سادساً: المصادر الأجنبية:

1. Oona' A.Hathway, Rebecca Crootof, Philip Levtiz, aley Nix, Aileen Nowlan, William perdue and Julia Spiegel, "The Law of Cyber- Attack", California Law Review, 2012.
2. Micheal Marien: "Future survey annual", Transaction Publishers, 1987.
3. Norbert wiener: Cybernetic or control communication in the animal and the machine, M.I.T, Press, Second Edition, Cambridge, Massachusetts, 1948.
4. Julia Cresswell, "Oxford Dictionary of word Origins: Cybernetics", Oxford Reference Online, Oxford University press, 2010.
5. Richard Kissel, "Glassory of Key Information Security Terms", National Institute of Stand ards and technology, U.S Department of Commerce, Revision, 2, May 2013.
6. James A. Lewis, "Sovereignty and the role of Government in Cyberspace", Center for Strategic and International Studies Journal, spring summer, vol. XVI, Issue II, 2010.
7. Shin, Beomchul, "The Cyber Warfare and the Right of self- Defense: Legal perspectives and the Case of the United States, IFANS, VOI.19, N1, June 2011.
8. Scoot. J.Shckelford, "State Responsibility for Cyber Attacks: Competing Standards for a Growing problem", University of Cambridge, Dept of politicos and International STUDIES, Cambridge, UK, 2009.
9. K.saalbach, "Cyber War, Methods and practice", Version 9.0, University of Osnabruck- 17 Jun 2014.
10. ICRC, "Exploring humanitarian law: IHL Guide, A legal manual for EHL teacher", ICRC, Geneva, January 2009.
11. Micheal S.Fuertes, "Cyber warfare, Unjust Actins in a just war", Florida International University, Full 2013.
12. Micheal N.Schmitt, "Tallinn Manual on the International Law Applicable to Cyber Warfare", Cambridge University press, first publishes, 2013.
13. Michael Gervais, "Cyber Attacks and the Laws of War", Berkeley Journal of Internatinal Law, vol. 30, Iss. 2, 2012.
14. Marco Roscini, "World Wide Warfare- Jus ad bellum and the use of Cyber Force", Max Planck Yearbook of United Nations Law, Volume 14, 2010.
15. Ivan Goldberg, Institute for the Advanced Study of Information Warfare (LASIW), http/ www.psycom.net/war.1.html.
16. H Allen, Julia, The CERT Guide to System and Network Security practices, Boston. MA, Addison, Wesley. 2001.

المستخلص

شهد العقد الأخير تطورات سريعة في مجال تكنولوجيا المعلومات مما أفضى الى متغيرات بعيدة المدى في جميع مجالات الحياة تقريباً. إذ إستمرت الجرائم السيبرانية في النمو على مر السنين حيث تم إدخال جرائم جديدة في الشبكة الدولية للمعلومات الإنترنت العميقة. وقد أظهر الإتجاه في الهجمات الأخيرة في جميع أنحاء العالم مدى تنوع مرتكبي الجرائم وما يستطيعون فعله. لا يمكن التأكيد على التأثير والأثر الواقع على المنظمات في جميع أنحاء العالم. كما تم دمج القوانين السيبرانية على مر السنين ليتم تنفيذها على مختلف المستويات والإختصاص القضائي. وقد دعا الاتجاه الهجمات والحاجة المتزايدة بين الجناة الى مخاوف بشأن ما قامت به القوانين السيبرانية المدمجة للحد من الجرائم المتنامية. سنتطرق في دراسة هذا البحث في جرائم الإنترنت والقوانين الإلكترونية من أجل أن تكون قادرة على جعل القوانين أكثر فاعلية وتطبيقها في منع المزيد من الجرائم السيبرانية.

الكلمات المفتاحية: الفضاء السيبراني، الهجمات السيبرانية، جرائم الإنترنت، الأمن السيبراني، الحرب السيبرانية، نظم المعلومات، الوسائل الإلكترونية.

Abstract

The last decade has witnessed rapid developments in the field of information technology, leading to far-reaching changes in almost all areas of life. Cybercrime has continued to grow over the years as new crimes have been introduced into the deep Internet. The trend in recent attacks around the world has shown how diverse the perpetrators are and what they can do. The impact on organizations around the world cannot be emphasized. Cyber laws have also been incorporated over the years to be implemented at various levels and jurisdiction. The trend has called for attacks and the growing need among culprits for concerns about what cybercrime laws have done to curb growing crime. In this research, we will look at cybercrime and cyber laws in order to be able to make laws more effective and apply them in preventing more cybercrime.

Keywords: cyberspace, cyber-attacks, cybercrime, cybersecurity, cyberwar, information systems, electronic means.