الجرائم السيبرانية وأثرها على الامن السيبراني

م.د. نبراس ابراهيم مسلم
جامعة بغداد – كلية القانون
dr.nibras@colaw.uobaghdad.edu.iq

تاريخ الاستلام: ١٠/ ٤ / ٢٠٢١ م
تاريخ قبول النشر: ٢٧ / ٥/ ٢٠٢١ م

المستخلص

تمثل الجرائم السيبرانية أشد أنواع الجرائم التي ترتكب عبر الشبكة الدولية للمعلومات من الخطورة، حيث يتضح هذا جلياً من خلال النظر إلى فداحة الخسائر التي يمكن أنْ تُسببها عمليةٌ ناجحةٌ واحدة تندرج تحت مفهومه. إذ شهد العقد الأخير تطورات سريعة في مجال تكنولوجيا المعلومات مما أفضى الى متغيرات بعيدة المدى في جميع مجالات الحياة تقريباً. إذ استمرت الجرائم السيبرانية في النمو على مر السنين إذ تم إدخال جرائم جديدة في الشبكة الدولية للمعلومات الإنترنت العميقة. وقد أظهر الاتجاه في الهجمات الأخيرة في جميع أنحاء العالم مدى تنوع مرتكبي الجرائم وما يستطيعون فعله. إذ لا يمكن التأكيد على التأثير والأثر الواقع على المنظمات في جميع أنحاء العالم.

الكلمات المفتاحية: الجرائم الدولية، تكنولوجيا المعلومات، الأمن والسلم، الأمن القومي، السيبرانية.

Abstract

Cyber-crimes represent the most dangerous types of crimes that are committed through the international network of information, as this is evident by looking at the enormity of the losses that can be caused by a single successful operation that falls under his concept. The last decade has witnessed rapid developments in the field of information technology, which have led 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 international network of deep Internet information. The trend in recent

attacks around the world has shown just how diverse the perpetrators are and what they can do. The impact and impact on organizations around the world cannot be overemphasized.

Key words: international crimes, information technology, peace and security, national security, cyber.

.

المقدمة

الجريمة السيبرانية (cybercrime) أي الجريمة الافتراضية الواقعة في فضاء إلكتروني منبثق من (cyber space) أي الفضاء التخيلي أو الافتراضي، ويعد عالم الرياضيات نوربرت وينر (Norbert wiener)، هو أول من استخدم مصطلح السيبرانية وذلك في عام ١٩٤٨. ثم جاء المؤتمر العاشر للأمم المتحدة المنعقد في فيينا عام ٢٠٠٠م ليؤكد هذه التسمية عن الجرائم الإلكترونية (السيبرانية) التي إنتشرت في الآونة الأخيرة بسبب إنتشار شبكة الإنترنت وفتح مجالات عديدة للاستفادة منها والذي فرضته هذه التقنيات الحديثة والتدفق الغزير للمعلومات والتي يمكن استخدامها لمصلحة بشرية. إذ تعتبر مكافحة الجريمة السيبرانية كآلية لتعزيز الأمن والسلم الدوليين؛ وذلك باستخدامها مجموعة من الوسائل التقنية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به بهدف ضمان توافر إستمرارية عمل نظم المعلومات وتأمين حماية وسرية وخصوصية البيانات الشخصية ولحماية المواطنين، وذلك لتعزيز الأمن الإقليمي لمواجهة التحديات الدولية.

أهمية الموضوع

يستمد أهمية البحث من 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 الموضوع

تكمن إشكالية البحث بالجرائم السيبرانية فيما 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؟

منهجية الموضوع

لتقديم الحلول لمعالجة إشكاليات الموضوع سنقسم هذا البحث على مبحثين، وهما ما يأتي:

المبحث الأول: الإطار المفاهيمي

المبحث الثاني: دور الاتفاقيات العالمية في مكافحة الجرائم السيبرانية وآثارها الدولية

المبحث الأول
الإطار المفاهيمي

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 الجريمة 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 الجريمة 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 الجريمة السيبرانية وعدم الاتفاق على تعريف محدد، يمكن الإستدلال في ضوئه لتنظيم استخدامها بالحظر أو التقييد لمواجهة عواقبها الخطرة على الصعيد الإنسان[١].

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

المطلب الأول: تعريف الجرائم السيبرانية

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

المطلب الأول
تعريف الجرائم السيبرانية

تشير المراجع العلمية الى أن عالم الرياضيات نوربرت وينر (Norbert wiener)، هو أول من استخدم مصطلح السيبرانية وذلك في عام ١٩٤٨، في أثناء دراسته لموضوع القيادة والسيطرة والإتصال في عالم الحيوان، فضلاً عن حقل الهندسة الميكانيكية[٢]. في دراسة هذا الفرع سيتم البحث على ثلاثة نقاط: الأول يرتكز على تعريف الجريمة السيبرانية لغةً، والثاني سيرتكز على تعريف الجريمة السيبرانية إصطلاحاً، والثالث سيرتكز على تعريف الجريمة السيبرانية فقهاً وبعض التطبيقات الدولية.

أولاً: تعريف الجريمة 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[٣].

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)"[٤]، وهو مصدر يتطابق مع مفهوم الجريمة 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"[٥].

ويرى بعض الفقه العربي وبالرجوع الى المختصين للغة العربية 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 بالجريمة السيبرانية كانت ترجمة غير صائبة، إذ تُرجمَ العنوان (Convention on Cybercrime) الى اللغة العربية بأنه

(الاتفاقية المتعلقة بالجريمة الإلكترونية) ويعود السبب في ذلك الى عدم وجود مصطلح مناظر في اللغة العربية[٦].

إذ يتضح مما تقدم فإن الوثائق الصادرة عن الأمم المتحدة باللغة العربية مستخدمة لمصطلح "السيبرانية" بدل الإلكترونية، كالقرار المرقم (٢٣٩/ ٥٧) الذي صدر عن الجمعية العامة للأمم المتحدة بشأن "إنشاء ثقافة عالمية للأمن السيبراني" والقرار رقم (١٩٩/ ٥٨) الصادر عن الجمعية العامة للأمم المتحدة كذلك بشأن دعوة الدول الأعضاء الى التعاون وتعزيز ثقافة الأمن السيبراني[٧].

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[٨].

ثانياً: تعريف الجريمة السيبرانية إصطلاحاً

في هذه الدراسة إستخدمنا مصطلح الجريمة 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[٩].

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)[١٠].

أما البعض الآخر فاختار مصطلح الهجمات السيبرانية (Cyber Attacks)، كوصف واقعي يجمع بين كل ما ذكر آنفاً[١١]، 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[١٢].

ولأن مصطلح الحرب هو مصطلح غير محبذ في وقتنا الراهن على المستوى التنظيم القانوني الدولي[١٣]، 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[١٤].

ثالثاً: تعريف الجريمة السيبرانية فقهاً وبعض التطبيقات الدولية

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

يتفق الأستاذ محمد أمين الشواكبة مع الأستاذ (Middet Credo) بأن الجريمة السيبرانية تسهل إستخدام الحاسوب كأداة لإرتكاب الجريمة بالإضافة الى الحالات المتعلقة بالولوج غير المصرح به للحاسوب الآلي أو البيانات الرقمية لتشمل الإعتداءات المالية المادية[١٥].

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[١٦]. 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[١٧].

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[١٨].

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[١٩]. ويرى بعض الفقه أن التعريف الذي ذهب إليه ميشيل (Michael) هو الأقرب لمفهوم الجريمة السيبرانية التي عرفها روسيني (Roscini)، إذ يعرفها بالقول: الجريمة 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[٢٠].

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[٢١]. وهذا ما يتوافق مع مفهوم إستخدام الوسائل الإلكترونية للأغراض العسكرية، ففي عام ٢٠٠٧ عرفت القيادة الإستراتيجية الأمريكية (US. Startegic Command) الجريمة السيبرانية بالقول: تطويع عمليات نظام الكمبيوتر بهدف منع الخصوم من الاستخدام الفعال لها، فضلاً عن التسلل الى أنظمة المعلومات وشبكات الإتصال بهدف جمع وحيازة وتحليل البيانات التي تحتويها[٢٢].

أن التعريف سالف الذكر، يتوافق مع ما جاءت به اتفاقية مجلس أوربا المتعلقة بالجريمة 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 "[٢٣].

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[٢٤].

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 ويخرب 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[٢٥].

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 نقطتين، وهما ما يأتي:

أولاً: 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[٢٦].

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[٢٧].

ثانياً: السياسات الأمنية للشركات ومؤسسات الدولة لحماية بياناتها 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[٢٨].

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[٢٩].

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:

١- 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).

٢- صلاحيات كل مستخدم على البيانات الموجودة على قاعدة البيانات.

٣- الدخول للشركة عن طريق البطاقة الخاصة.

٤- وضع مثلاً أجهزة التحقق من بصمة الشخص على أجهزة البيانات المهمة.

المبحث الثاني

دور الاتفاقيات العالمية في مكافحة الجرائم السيبرانية وآثارها الدولية

إن مصطلح الجرائم السيبرانية الدولية الذي شاع استخدامه عقب التقدم الكبير الذي حققته تكنولوجيا المعلومات واستخدامات الحواسيب الآلية والإنترنت تحديداً في إدارة معظم الأنشطة الحياتية، وهذا الأمر هو الذي دعا (٣٠) دولة الى توقيع الإتفاقية الدولية الأولى لمكافحة الإجرام عبر الإنترنت في العاصمة المجرية بودابست عام (٢٠٠١)، والذي يُعدُ من أشد أنواع الجرائم التي ترتكب عبر شبكة الإنترنت خطورة، وإنَّ حجم الجرائم السيبرانية على الصعيد العالمي بات أمراً ملحوظاً ومحسوساً، ويتمثل ذلك في الإحصائيات المروعة التي تُبين زيادة مخاطره والخسائر الناجمة عنه حتى باتَ يشكل تهديداً للأمن القومي وللإقتصاد الدولي، وتختلف الدول بمدى تأثرها بهذا النمط من الإجرام بحسب إعتمادها على التقنية العالمية المعلوماتية.

وعليه ومما تقدم سنتناول دراسة هذا المبحث على مطلبين وهما ما يأتي:

المطلب الأول: دور اتفاقية بودابست لعام ٢٠٠١

المطلب الثاني: آثار الجرائم السيبرانية على الأمن والسلم الدوليين والعلاقات الدولية

المطلب الأول
دور اتفاقية بودابست لعام ٢٠٠١

حرصاً على حماية مصالح المواطنين وحقوقهم، تقدمت اللجنة الأوروبية لمشكلات الجريمة ولجنة الخبراء في حقل جرائم التقنية بتاريخ (٢٠ نيسان ٢٠٠١) بمشروع اتفاقية جرائم الكمبيوتر وخضعت مواد الاتفاقية المقترحة للمناقشة وتبادل الآراء خلال الفترة من إصدار مشروعها الأوّل وحتى إعداد مسودتها

النهائية التي أُقِرت لاحقاً في العاصمة المجرية بودابست بتاريخ (٢٣/ ١١/ ٢٠٠١) وتُعرف اتفاقية بودابست (٢٠٠١) (باتفاقية الجرائم الإلكترونية سايبر كرايم)، وكان قد طرح مشروع الاتفاقية العامة ووزع على مختلفِ الجهات وأُطلق ضمن مواقع عديدة أوروبية وأمريكية على شبكة الإنترنت لجهة التباحث وإبداء الرأي، وتعكس الاتفاقية الجهد الواسع والمميز للإتحاد الأوروبي ومجلس أوروبا، وكذلك في إطار منظمات حكومية ودولية ولجان الخبراء المنصبة فيهما على مسائل جرائم الكمبيوتر وأغراضها منذ أكثر من عشرة أعوام[٣٠].

وقد وَقعتْ على هذه الاتفاقية (٢٦) دولة أوروبية بالإضافة إلى كندا وأمريكا وجنوب أفريقيا واليابان، ورغم أنَّ هذه الاتفاقية هي في الأصل اتفاقية أوروبية المنشأ، إلاَّ أنها اتفاقيةٌ ذات طابعٍ عالمي، لكونها مفتوحة للدول الأخرى لطلب الإنضمام من خارج أوروبا، مما يجعلها إطاراً دولياً مفيداً للعمل على مكافحة الجرائم السيبرانية الدولية[٣١]، وللعود إلى لجان هذه الاتفاقية وأثناء إجتماع لجنة أو فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة المعلوماتية (السيبرانية) عام (٢٠١٧) عرضَ الحاضرون تجاربهم المتعلقة بتنفيذ أنشطة المساعدة التقنية في إطار العمل العالمي لمكافحة الجريمة السيبرانية، وأشارَ بعضُ منهم إلى ضرورة وضع إطار قانون دولي لمكافحة الجرائم السيبرانية الدولية، وأعربَ بعضُ الخبراءِ عن رأيهم في اتفاقية بودابست بأنها أصبحت قديمة[٣٢].

ونظراً للتغيرات التي أحدثتها الرقمنة واستمرار التقارب بين عولمة الشبكات الحاسوبية والقلق من أن شبكات الإنترنت والمعلومات الإلكترونية قد تستخدم لإرتكاب الجرائم عن طريق الشبكات، فقد تم توقيع هذه الاتفاقية، لأنها ستوفر ما يلزم لردع أيِّ عملٍ موجه ضد السرية ونظم الحاسوب والشبكات والبيانات، هذا وتتكون الاتفاقية من مقدمةٍ وأربعةِ فصولٍ، ولأنَّ هذهِ الاتفاقية جاءت حصيلة جهود دولية فقد أكدت

المقدمة أيضاً على أهمية ما أُنجز من جهود في حقل المعلوماتية من قبل منظمة الأمم المتحدة ومنظمة التعاون الإقتصادي والتنمية والإتحاد الأوروبي ومجموعة الدول الصناعية، وبالنتيجة فإنَّ مقدمة هذه الاتفاقية إستعرضت أهدافها ومنطلقاتها ومرجعياتها السابقة وما تقوم عليه من جهودٍ إرشاديه وتوجيهية وتدابير إقليمية ودولية، وتضَّمن الفصل الثاني الذي جاء تحت عنوان: الجوانب الموضوعية والإجرائية للجرائم المعلوماتية (المواد ٢ -٢٢) معالجة النصوص الموضوعية لجرائم الكمبيوتر، والجوانب الإجرائية للجرائم المعلوماتية، وجاء الفصل الثالث: بعنوان الأحكام المتعلقة بالجرائم المعلوماتية عابرة الحدود(المواد ٢٣ -٣٥) والمتعلقة بالإختصاص و التعاون الدولي، أمّا الفصل الرابع جاء بالأحكام الختامية (المواد ٣٦- ٤٨)[٣٣].

وقد نصَّتْ هذه الاتفاقية على تسمية مجموعة من الأعمال الإرهابية عبر الوسائل الإلكترونية غير المشروعة، وحثَّ الدول الأعضاء فيها على تجريمها في تشريعات داخلية، كما تضَّمنتْ الاتفاقية عدة طوائف من الجرائم الإلكترونية[٣٤]، وهي على النحو الآتي:

الطائفة الأُولى: الجرائم التي تستهدف عناصر أمن المعلومات الإلكترونية.

الطائفة الثانية: الجرائم المرتبطة بالحاسوب الإلكتروني.

الطائفة الثالثة: الجرائم المرتبطة بالمحتوى الإلكتروني.

الطائفة الرابعة: الجرائم السيبرانية.

وبينتِ المذكرة التفسيرية لاتفاقية بودابست في (٨ شباط لسنه ٢٠٠١)، أنَّ الهدف من هذه الاتفاقية بموادها من (٢ – ١٣)، هو تحسين أو إصلاح وسائل منع وقمع الإجرام المعلوماتي، وذلك من خلال تحديد معيار بالحد الأَدنى المشترك، والذي يسمح باعتبار بعض التصرفات من قبيل الجرائم الجنائية، وهذا النوع من التجانس يسهل مكافحة هذه النوعية من الجرائم على المستويينِ الوطني والدولي[٣٥]. وسنتناول بعض من مواد هذه الاتفاقية فيما يخص الجرائم

السيبرانية، والبروتوكول الإضافي لها، ومنها ما يأتي:

أوّلاً: جريمة الولوج أو الدخول غير القانوني

حيثُ تنصُّ المادةُ (٢) من هذه الاتفاقية على أنه "يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنّها ضرورية من أجل اعتبارها جريمة جنائية وفقا لقانونه الداخلي، للولوج العمدي لكل أو جزء من جهاز الحاسوب دون حقٍّ، كما يمكن له أنْ يشترط أن ترتكبَ الجريمة من خلال إنتهاك إجراءات الأمن بنية الحصول على بيانات الحاسوب أو أي نية إجرامية أخرى، أو أنْ ترتكب جريمة في حاسوب آلي يكون متصلاً عن بعد بحاسوب آخر"[٣٦]، فيدخل بالتالي في عداد هذه الجرائم كل من الأفعال: القرصنة[٣٧] والسطو والدخول غير المشروع في النظام المعلوماتي، وتُعدُ هذه الجريمة تَعدِ على أمن الدولة ومؤسساتها بمعنى السرية والسلامة وإتاحة النظم والبيانات المعلوماتية [٣٨].

ثانياً: جريمة الاعتراض غير القانوني

حيثُ تنصُّ المادةُ (٣) من هذ الاتفاقية على أنه "يجب على كلِّ طرفٍ أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من أجل اعتبارها جريمة جنائية، كما يمكن لأي طرف أن يستوجب أن ترتكب الجريمة بنية إجرامية (بقصد الغش)، أو أن ترتكب الجريمة في حاسوب آلي يكون متصلاً عن بعد بحاسوب آخر"[٣٩]، فالهدف من هذه المادة هو حماية الحقِّ في إحترام نقل البيانات والإتصالات، والتسجيل التقليدي للمحادثات التليفونية بين الأشخاص، وهذه الحقوق كانت مكفولة سابقًا بنصِّ المادةِ (٨) من الاتفاقية الأوروبية لحقوق الإنسان[٤٠].

ونخلص مما تقدم أنّه يمكن اعتبار تعمد الإعتراض غير القانوني والدخول من دون حقٍّ بواسطة الوسائل تكنولوجية المعلومات، يمثل إنتهاكًا للحق في إحترام الإتصالات مثل التنصت على نظام سياسي لدولة معينة، وذلك للإعتداء على أمن

الدولة، وبالتالي تُعدُ من ضمن أفعال الجرائم السيبرانية.

ثالثاً: جريمة الإعتداء على سلامة البيانات

حيثُ تنصُّ المادةُ (٤) من هذه الاتفاقية على أنه "١- يجب على كلِّ طرفٍ أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنّها ضرورية للتجريم تبعاً لقانونه المحلي، إذا حدث ذلك عمداً، ودون حقٍّ، أي إضرار، أو محو، أو تعطيل، أو إتلاف، أو طمس لبيانات الحاسوب"[٤١]، وتشير المذكرة التفسيرية لاتفاقية بودابست في (٨ شباط لسنه ٢٠٠١)، الى أنَّ الهدف من تقرير هذا النص هو أن تكون بيانات وبرامج الحاسوب مكفولة بحماية مماثلة لتلك التي تتمتع بها الأشياء المادية ضد الأضرار التي تحدث عمداً، والمصالح القانونية المحمية، حيث إن التصرفات السابقة لا يتم المعاقبة عليها إلاَّ إذا إرتُكِبَت بدونِ حقٍّ، وتمثل اعتداءً على الأشخاص عن طريق الإعتداء على البيانات الشخصية ومنها البيانات الشخصية لرؤساء الدول بصفتهم المعنوية[٤٢].

رابعاً: جريمة الإعتداء على سلامة النظام

تنصُّ المادةُ (٥) على أنه "يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية للتجريم، تبعاً لقانونه المحلي، الإعاقة الخطيرة، إذا تم ذلك عمداً، ودون حقٍّ، لوظيفة نظام الحاسوب، عن طريق إدخال، أو نقل، أو إضرار، أو محو، أو تعطيل، أو إتلاف أو طمس البيانات المعلوماتية"[٤٣]، فالهدف من هذا الإعتداء هو تخريب نظام الحاسوب الذي يمسُّ بحياة الأشخاص وأمن الدولة ومؤسساتها، وتجريم الإعاقة العمدية للإستخدام الشرعي للنظم المعلوماتية، ويجب أنْ تكون الإعاقة جسيمه حتى يترتب عليها جزاءً جنائياً، وعلى سبيل المثال يشترط حدوث أذى كحد أدنى من الضرر لكي تعتبر الإعاقة جسيمة[٤٤].

ونرى من جانبنا أنَّ الإعتداء على المؤسسات المالية للدولة يمثل إرهاباً وخوف وتهديد ممتلكات المواطنين يمكن أنْ يضعف ثقة المواطنين بالمؤسسات المالية.

خامساً: جريمة إساءة استخدام أجهزه الحاسوب

تضمَّنتِ المادةُ (٦) من هذه الاتفاقية على أن إقرار الإجراءات التشريعية وغيرها من الإجراءات كلما كان ضرورياً، وذلك في إطار تجريم الإنتاج أو البيع أو الحصول بغرض الاستخدام أو التوفير لجهاز يشمل برنامج كمبيوتر يتم تصميمه أو تطويقه بشكلٍ أساسي في غرض ارتكاب أية من الجرائم المنصوص عليها في إطار المواد (٢،٣،٤،٥) من هذه الاتفاقية، وكذلك كلمة السر الخاصة بالكمبيوتر أو الكود السيفري للدخول أو بيانات مماثلة تمكن الدخول لمنظومة المعلومات بأكملها أو أي جزء بقصد استعمال الجهاز لإرتكاب أي من الجرائم الواردة في المواد (٢،٣،٤،٥)، وكذلك حيازة عنصر من العناصر المشار إليها بنية استخدامها في إرتكاب الجرائم الإلكترونية[٤٥].

سادساً: الشروع والإشتراك

وتضمَّنتِ المادةُ (١١) القواعد العامة المتعلقة بالمساهمة الجنائية والشروع بشأن الجرائم المشار إليها في المواد (١٠-٢)، حيث أوجبت على الدول الأعضاء إتخاذ تدابير تشريعية للنصِّ على تجريم أفعال المساهمة الجنائية والتحريض على الجرائم التي ترتكب عمداً بقصد إرتكاب هذه الجرائم، أو ما تختاره الدولة منها، وتم تجريم الشروع عمداً في ارتكاب الجرائم المنصوص عليها في المواد (٣-٥-٧-٨-٩) من هذه الاتفاقية [٤٦].

ونرى من جانبنا أنَّ الهدف من إيراد هكذا نصوص هي للنص على الجرائم التكميلية التي ترتبط بالشروع ولم تنصْ عليها هذه الاتفاقية في موادها الأخرى.

سابعاً: مسؤوليه الأشخاص المعنوية

تضمّنت المادة (١٢) مسؤوليه الأشخاص المعنوية، وبما يتماشى مع الإتجاه القانوني الحالي القائل مسؤولية الشخص المعنوي، وذلك بهدف إقامة المسؤولية على الشركات التجارية والمؤسسات والأشخاص المعنوية المشابهة بالنسبة للأفعال الجنائية المرتكبة على حواسيبها وأجهزتها الإلكترونية الأخرى عن طريق شخصٍ يمارس سلطة القيادة

داخل الشخص المعنوي[٤٧]، حيث يتبادر في ذهن القارئ تساؤل هل هو إرهاب سيبراني، نعم عندما يتم عن طريق شخص يمارس سلطة القيادة داخل الشخص المعنوي ويعمل على إرتكاب جرائم إرهابية سيبرانية فبالتالي تكون الأشخاص المعنوية مسؤولة عن هذه الجرائم.

ثامناً: الجزاءات والإجراءات

أكدت المادة (١٣) على أن تضمن كل دوله من خلال إقرارها للإجراءات التشريعية المعاقبة على الجرائم السابقة الذكر بموجب عقوبات فعالة ومتناسبة تدعو للعدول عنها، وبالتالي قد تشمل حرمان الحرية وأي إجراء جنائي أو غير جنائي يتوافق مع متطلبات الردع في إطار السياسة الجنائية الحكيمة والراشدة المنتهجة في كل دوله لمكافحة الجرائم السيبرانية [٤٨].

هذا ولقد ألزمت هذه الاتفاقية الدول الأوروبية أو أي دولة توقع أو تنضم إليها من خارج المجموعة الأوروبية إقرار العقوبات الملائمة والتدابير الفعالة لهذه الجرائم سواءً أكانت سالبة لحرية الأشخاص الطبيعية أو حرية الأشخاص المعنوية[٤٩].

المطلب الثاني
آثار الجرائم السيبرانية على الأمن والسلم الدوليين والعلاقات الدولية

تبنتِ الجرائمُ السيبرانية عبر الوسائل الإلكترونية في الآونة الأخيرة أشكالاً ذاتَ آثارٍ ضارةٍ على العلاقات الدولية، وأصبحت تهدد الأمن والسلم الدوليين، ويتصور حدوث هذا إذا قامتْ شبهات إتجاه دولةٍ ما بأنها قامت بإيواء وتجنيد الإرهابيين عبر الوسائل الإلكترونية وتحريضهم ضد الدول عبر هذه الوسائل، فإنَّ العلاقة بينهما وبين الدولة المتضررة من الإرهاب تتأثر سلباً، وتتوقف أو ربما تمتد إلى المقاطعة[٥٠].

ومن الأمثلة التطبيقية التي قامت به داعش والقاعدة من استغلال الوسائل الإلكترونية لأعمال إرهابية أدت إلى توتر العلاقات الدولية وتهديد الأمن والسلم الدوليين، وكذلك العمل الذي قام به موقع "ويكيليكس" والذي يُعَّرف "صراع إلكتروني ذو

طبيعة ناعمة"[٥١]، وذلك أدت الى عن طريق الصراع الدولي الإلكتروني للحصول على المعلومات والتأثير في المشاعر والأفكار وشحن حرب نفسية وإعلامية من خلال تسريب المعلومات والأسرار واستخدامها عبرَ منصاتٍ إعلاميةٍ بما يؤثر على طبيعة العلاقات الدولية، فإنَّ هذا الصراع من شأنه أنْ يُهدد السلم العالمي بإعتباره حرباً إلكترونيةً بين الدول مما يحدث خلل بنظام الأمن والسلم الدوليين[٥٢].

حيث خلَّفَتِ الهجمات السيبرانية آثاراً كبيرة في بنية مجتمعات دول العالم، واستطاعت هذه العمليات بتقسيم الدول مذهبياً وطائفياً وعرقياً وإثنياً، وذلك من أجل تحقيق هدف هذه الظاهرة المتمثلة بضرب المؤسسات والأفراد للنيل من الأمن والسلم الدوليين، حيث أخذتِ الدول على عاتقها القيام بما هو ممكن من أجل تحقيق السلام والإستقرار داخل دولها من خلال الدعوة إلى ضرورة مواجهة ظاهرة الجرائم السيبرانية الدولية الذي أخذَ يضرب دولاً مختلفة مخلِّفاً آثاراً وتهديداتٍ وتداعياتٍ تمسُّ الأمن والسلم الدوليين، ومما يستدعي ضرورة العمل على تنسيق الجهود المشتركة من أجل مكافحة الجرائم السيبرانية، من خلال قاعدة معلومات وبرامج عمل مشتركة للقضاء عليه عبر محاربة الفكر المتطرف الذي أخذَ ينتشر، والعمل على تحقيق أكبر قدر ممكن من التعاون الدولي لحصر هذه الظاهرة والحد من إنتشارها، ومن ثم إعادة نشر السلام والمحافظة على الأمن والسلم الدوليين والإستقرار في المجتمع الدولي[٥٣].

ويتضح مما تقدم أنَّ على المجتمع الدولي بذل المزيد من الجهود لمكافحة الجرائم السيبرانية لما له من آثارٍ كبيرةٍ على المجتمع الدولي، وذلك من أجل تحقيق الأمن والاستقرار للمجتمع الدولي ككل، لما لهذه الجرائم من آثار وتهديدات وتداعيات تمسُّ الأمن والسلم الدوليين.

ويعد من آثار الجرائم السيبرانية التأثير على مستوى العلاقات

الدبلوماسية الدولية من خلال جمع المعلومات والتنصت والتجسس وتسهيل النشاطات السرية في العلاقات الدولية، مثل عميلة الاغتيالات، وتزايدت العلاقة بين التكنولوجيا والأمن وأصبح لا يعترف بالحدود الإقليمية أو العالمية، ولقد أدتْ ظاهرةُ الجرائم السيبرانية إلى تحُّولِ جزءً من العالم من الطابع المادي إلى عالمٍ رقمي إلكتروني، حيث أصبحَ الفضاءُ الإلكتروني مجالاً جديداً للتفاعلات الدولية سواءً أكانت تفاعلات صراعية أم تعاونية، مما أثر على تغير طبيعة القوة وبروز تهديدات الفضاء الإلكتروني، وأثر بدوره على استراتيجيات الأمن القومي للدول، والسعي إلى الإستحواذ على مصادر القوة داخل الفضاء الإلكتروني لمنع تعرض بنيتها التحتية والحيوية للخطر، ومن ثُمَّ دخول المجال الإلكتروني ضمن المحددات الجديدة للقوة وأبعادها الجديدة من حيث طبيعتها وأنماط استخدامها وطبيعة الفاعلين فيها[٥٤].

وقد أحدثَ الفضاءُ الإلكتروني آثاراً وتغيرات في طبيعة القوة وعناصرها وأنماط استخدامها، وتتميّز القوة الإلكترونية بالتحرك في مسارات متداخلة، وتعمل على نقل عملية التأثير من وإلى الفضاء الإلكتروني، إذْ يتمثلُ المسار الأول في انتقال الأحداث من أرض الواقع إلى الفضاء الإلكتروني أمّا لتصفية الصراعات وإمّا لاستخدامهِ لبث العنف والتحريض والكراهية، ويتمثل المسار الثاني في انتقال عناصر التهديد من الفضاء الإلكتروني إلى أرض الواقع عن طريق تأثير ما يتم نشره من معلومات وشائعات وغيره على المجتمع، ويتمثل المسار الثالث في استخدام الفضاء الإلكتروني كوسيلة إعلام تنقل كل ما يحدث داخلياً وعالمياً، مما يؤدي إلى ردودِ أفعالٍ عالمية مؤيدة ومعارضة[٥٥]، وكذلك التأثير على العلاقات الدولية من حيث وقوع هذه الجرائم من دولةٍ إلى دولةٍ أخرى وتعريضها للخطر نتيجة حدوث العمل الإرهابي في إقليمها، وتأثيره على مصالح دول أخرى كوقوعه على

أعضاء السلك الدبلوماسي أو على وسائل نقل أجنبية أو على رعايا عدة دول(٥٦).

ومن الأمثلةِ التطبيقية للآثار على العلاقات الدولية ومنها في يوليو عام (٢٠١٥)، أفاد مكتب الإدارة الشخصية التابع للحكومة الأمريكية أنَّ قراصنةً تمكنوا من سرقة بيانات قرابة أربعة ملايين موظف فيدرالي، إذْ إتهم مسؤولون أمريكيون حكومة الصين بالوقوف خلف هذه العملية التي تعد الفاجعة الأكبر في تاريخ البلاد، وعَدَّ الخبراء أنَّ الهدف من هذه العملية هو تحسين مستوى الصين لقدراتها على تجنيد جواسيس نظراً لأهمية المعلومات المسروقة التي تمكنهم من الوصول إلى أسرار أمن الدولة(٥٧).

ونرى من جانبنا أنّ للجرائم السيبرانية الدولية لها عدة آثار ومنها تلك التي تؤثر على مجرى العلاقات الدولية من خلال تجنيد الإرهاب عبر الشبكة الدولية للمعلومات (الإنترنت) وتحريضهم ضد الدول، حيث إنَّ كل هذه الأفعال تؤثر وتهدد أمن المجتمع الدولي ككل.

الخاتمة

أولاً: الاستنتاجات

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

٢- شهدت السنوات الأخيرة العديد من الجرائم السيبرانية التي كان من شأنها الإضرار الجسيم بالدول المختلفة أو التسبب بأضرار فادحة بأهم المنشآت الحيوية وأخطرها في الدول، وتعتبر من أهمها الهجوم على أستونيا، وهجوم (Stuxnet) ضد المنشآت النووية الإيرانية، إذ أثبت الهجوم على أستونيا قدرة الهجمات السيبرانية وسرعتها، في حين أثبت الهجوم على المنشآت النووية الإيرانية بأن الأسلحة السيبرانية تعد أدق وأذكى

من غيرها من الهجمات والأسلحة التقليدية.

٣- يوجد إغفال تشريعي فيما يتعلق بمكافحة الجرائم السيبرانية والوقاية منها على المستوى الدولي، على أنَّ هناك بعض القوانين التي صدرت حديثا والتي تعرضت لبعض أشكال الجرائم السيبرانية، إذ إن هذا الإغفال يشكل أحد أهم التحديات الرئيسية في مجال مكافحة الجرائم السيبرانية الدولية، وأخطر ما يمكن أن يترتب على ذلك إفلات مرتكبي هذا السلوك الإجرامي من العقاب على الرغم مما يتسببون فيه من أضرار وخسائر ضخمة، وهو ما يشكل حافزاً لهم على استغلال هذا الفراغ لإرتكاب المزيد من هذا السلوك الإجرامي.

٤- تعكسُ إتفاقية بودابست لعام (٢٠٠١) (اتفاقية الجرائم الإلكترونية سايبر كرايم) الجهد الواسع والمميز للإتحاد الأوروبي ومجلس أوروبا بشأن جرائم الكمبيوتر، لاسيما الجرائم الإلكترونية (السيبرانية).

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- ضرورة إتخاذ التدابير الملائمة، وذلك لحل مشكلات الإختصاص القانوني والقضائي التي تثيرها الجرائم السيبرانية الدولية العابرة للحدود. ويتعين إعتبار الجرائم السيبرانية جرائم دولية، تدخل في إختصاص القضاء العالمي، وهو ما يعني إعطاء الحق للدول بملاحقة ومحاكمة مرتكبي الجرائم الدولية، دون أيَّ إعتبار لجنسية مرتكبيها، أو المكان الذي إرتكبت فيه الجريمة، بما مفاده إنعقاد الإختصاص القضاء العالمي لأي دولة ترغب في ملاحقة مرتكبي الجرائم الدولية.

٥- إنشاء وكالة دولية عالمية متخصصة بمكافحة الجرائم السيبرانية على غرار اليونيسيف واليونسكو، حيث تتولى تنسيق الجهود الدولية وتدريب الكوادر الداخلية لمواجهة الجرائم السيبرانية، وتقويض فرص إستفادة الجماعات الإرهابية من التكنولوجيا لزيادة قدراتها الإرهابية.

الهوامش:ـ

(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.

(2) Norbert wiener: Cybernetic or control communication in the animal and the machine, M.I.T, Press, Second Edition, Cambridge, Massachusetts, 1948.

(3) Julia Cresswell, "Oxford Dictionary of word Origins: Cybernetics", Oxford Reference Online, Oxford University press, 2010.

(٤) منير البعلبكي: المورد قاموس إنكليزي- عربي، دار العلم للملايين، بيروت، ٢٠٠٤، ص٢٤٣.

(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, p.57.

(٦) د. أحمد عبيس نعمة الفتلاوي: الهجمات السيبرانية، دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، ط١، منشورات زين الحقوقية، بيروت، ٢٠١٨، ص١٢.

(٧) القرار رقم ٢٣٩/ ٥٧ بتاريخ ٣١/كانون الثاني/ يناير ٢٠٠٣؛ القرار رقم ١٩٩/٥٨ بتاريخ ٣٠/كانون الثاني/ يناير ٢٠٠٤. مكتب الأمم المتحدة المعني بالمخدرات والجريمة، تقرير الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، فينان عام ٢٠١٣، الوثيقة UNODC/CCPC/EG ٤/٢/ ٢٠١٣. زهراء عماد محمد كلنتر: المسؤولية الدولية الناشئة عن الهجمات السيبرانية، رسالة ماجستير، كلية القانون، جامعة الكوفة، ٢٠١٦، ص٩.

(٨) انظر على سبيل المثال: مكتب الأمم المتحدة المعني بالمخدرات والجريمة: "تقرير الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، دراسة شاملة عن مشكلة الجريمة السيبرانية والتدابير التي تتخذها الدول الأعضاء والمجتمع الدولي والقطاع الخاص للتصدي لها"، فينا، ٢٠١٣، الوثيقة: UNODC/CCPCJ/EG.4/2013/2.

(9) 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.

(10) 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.

(11) 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.

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

(١٣) 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.

(١٤) 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.

(١٥) محمد أمين الشواكبة: جرائم الحاسوب الإنترنت، ط٤، دار الثقافة للنشر والتوزيع، الأردن، ٢٠١١، ص٨.

(16) Shin, Beomchul, op.cit.p. 105.

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

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

(19) 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.

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

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

(22) K. Saalbach op. cit, p105.

(٢٣) المادة (٥) من اتفاقية بودابست لمكافحة جرائم المعلوماتية، لسنة ٢٠٠١، صادرة عن مجلس أوربا رقم ١٨٥ في ٢٠٠١/١١/٢٣.

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

(25) S. Ghernauti-Helie: "From the Digital Divide to the lack of digital security, the challenges of development and deployment of a unified computer-security framework in a multi-dimensional" in international cooperation and the information society context, section Swiss policy manual mode, the University Institute for Development Studies publications (IUED). Geneva, November 2003. See the International Telecommunication Union, cyber security handbook for developing countries, edition 2007, ITU 2009, P.21.

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

(٢٧) 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.

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

(٢٩) 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.

(٣٠) نعيم مغبغب: حماية برنامج الكمبيوتر الأساليب والثغرات، دراسة في القانون المقارن، ط١، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٦، ص٢٢٠.

(٣١) اتفاقية بودابست لمكافحة جرائم المعلوماتية، لسنة ٢٠٠١، صادرة عن مجلس أوربا رقم ١٨٥ في ٢٠٠١/١١/٢٣.

(٣٢) تقرير عن إجتماع فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، الذي عقد في فينا في الفترة من ١٠ الى ١٣ نيسان ٢٠١٧، ص٤، منشور على شبكة الإنترنت عبر الرابط الاتي: www.unodc.org/documents/organized-crime/cybercrime/-April-2017 ، (آخر زيارة للموقع في٢٠١٨/٨/١٩، ٠٠:٥م).

(٣٣) محمد عبد الله أبو بكر سلامة: موسوعة جرائم المعلوماتية، جرائم الكمبيوتر والإنترنت، منشأة المعارف، الإسكندرية، ٢٠٠٦، ص١١٨-١٢٠؛ د. عمر أبو الفتوح عبد العظيم الحمامي: الحماية الجنائية للمعلومات المسجلة إلكترونياً، دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠١٠، ص٣٠٤-٣٠٧؛ ضياء يحى السادات: مبادئ إستخدام الحاسوب الآلي والإنترنت وجهود مكافحة الجرائم الناشئة عنهما، بلا دار نشر، ٢٠١٢، ص١٩٥-١ ٩٧؛ د. هلالي عبد اللاه أحمد: جرائم الحاسوب والإنترنت، بين التجريم الجنائي وآليات المواجهة، دار النهضة العربية، القاهرة، ٢٠١٥، ص٢٧-٢٨.

(٣٤) سمية مزغيش: جرائم المساس بالأنظمة المعلوماتية، رسالة ماجستير، كلية الحقوق والعلوم السياسية قسم القانون، جامعة محمد خيضر بسكرة، الجزائر، ٢٠١٤، ص٣٩؛ د. خالد حسن أحمد لطفي: جرائم الإنترنت بين القرصنة الإلكترونية والإبتزاز الإلكتروني، ط١، دار الفكر الجامعي، الإسكندرية، ٢٠١٨، ص٥٤.

(٣٥) د. هلالي عبد اللاه أحمد: مصدر سابق، ص٣٣-٣٤.

(٣٦) المادة (٢) من اتفاقية بودابست لمكافحة جرائم المعلوماتية، لعام ٢٠٠١.

(٣٧) يشير مفهوم القرصنة الإلكتروني: إلى ممارساتٍ غيرِ مشروعةٍ عبر شبكات الحاسوب الآلي حيث تستهدف التحايل على نظام المعالجة الآلية للبيانات بغية إتلاف مستندات المعالجة إلكترونياً، حيثُ أنَّ جريمة القرصنة تمثل إرهاباً إلكترونياً وذلك عندما يتم القرصنة على نظام سياسي لدولة معينة أو عدة دول عبر الوسائل الإلكترونية بغية حيازة مستندات أو إتلافها أو بثّها عبر الوسائل الإلكترونية تهديداً لأمن الدول.

(٣٨) د. خالد ممدوح إبراهيم: الجرائم المعلوماتية، ط١، دار الفكر الجامعي، الإسكندرية، ٢٠٠٩، ص٢٧٧-٢٧٨؛ محمد كمال محمود الدسوقي: الحماية الجنائية لسرية المعلومات الإلكترونية، ط١، دار الفكر والقانون، ٢٠١٧، ص٥٥.

[٣٩] المادة (٣) من اتفاقية بودابست لمكافحة جرائم المعلوماتية، لعام ٢٠٠١.

[٤٠] سمية مزغيش: مصدر سابق، ص٤١.

[٤١] المادة (٤) من اتفاقية بودابست لمكافحة جرائم المعلوماتية، لعام ٢٠٠١.

[٤٢] عمر عباس خضير العبيدي: الإرهاب الإلكتروني في نطاق القانون الدولي، ط١، المركز العربي، القاهرة، ٢٠٢١، ص٨٧.

[٤٣] المادة (٥) من اتفاقية بودابست لمكافحة جرائم المعلوماتية، لسنة ٢٠٠١.

[٤٤] ملياني عبد الوهاب: أمن المعلومات في بيئة الأعمال الإلكترونية، إطروحة دكتوراه، كلية الحقوق والعلوم السياسية قسم الحقوق، جامعة أبي بكر بلقايد–تلمسان، الجزائر، ٢٠١٧، ص١٤٦.

[٤٥] سمية مزغيش: مصدر سابق، ص٤١–٤٢.

[٤٦] ملياني عبد الوهاب: مصدر سابق، ص١٤٧.

[٤٧] د. هلالي عبد اللاه أحمد: مصدر سابق، ص١٥٠.

[٤٨] عمر عباس خضير العبيدي: مصدر سابق، ص٩٢.

[٤٩] لينا محمد متعب الأسدي: مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، رسالة ماجستير، كلية الحقوق، جامعة النهرين، ٢٠١٢، ص٦٤.

[٥٠] عمراني كمال الدين: السياسة الجنائية المنتهجة ضد الجرائم الإلكترونية، دراسة مقارنة، إطروحة دكتوراه، كلية الحقوق والعلوم السياسية قسم الحقوق، جامعة أبو بكر بلقايد– تلمسان، الجزائر، ٢٠١٦، ص١١٠–١١١.

[٥١] هي جرائم هادئة بطبيعتها(Soft Crime) لا تحتاج إلى عنف ولا سفكاً للدماء، بل كل ما تحتاج إليه هذه الجرائم هو القدرة على التعامل مع جهاز الحاسوب وكيفية تشغيله على مستوى عالي من التقنية بالشكل الذي يوظف في إرتكاب الأفعال غير المشروعة. خليل يوسف جندي: المواجهة التشريعية للجريمة المعلوماتية على المستويين الدولي والوطني (دراسة مقارنة)، بحث منشور في مجلة كلية القانون للعلوم القانونية والسياسية، جامعة كركوك، مج٧، ع٢٦، العراق، ٢٠١٨، ص٩٣.

[٥٢] د. عادل عبد الصادق: خطر الحروب السيبرانية عبر الفضاء الإلكتروني، ٢٠١٧، بحث منشور في مجلة لغة العصر متاح على شبكة الإنترنت عبر الرابط الآتي: aitmag.ahram.org.eg/news/83562.aspx، (آخر زيارة للموقع في ٢٠١٨/٧/١٣– ص١١:٠٠)؛ د. حمدان رمضان محمد: الإرهاب الدولي وتداعياته على الأمن والسلم العالمي، دراسة تحليلية من منظور إجتماعي، بحث منشور في مجلة أبحاث التربية الأساسية، جامعة الموصل، مج١١، ع١، العراق، ٢٠١١، ص٢٨٢–٢٨٣.

[٥٣] أيمن عبد الكريم حسين: الإرهاب دوافعه وتداعياته على الأمن والسلم الدوليين، مركز البيان للدراسات والتخطيط، بغداد، ٢٠١٨، ص٥.

(٥٤) نوران شفيق: أثر التهديدات الإلكترونية على العلاقات الدولية، المكتب العربي للمعارف، القاهرة، ٢٠١٥، ص١٠٨٠.

(٥٥) عادل عبد الصادق الجحة: الإرهاب القوة في العلاقات الدولية نمط جديد وتحديات مختلفة، ط١، مركز الدراسات السياسية والإستراتيجية، القاهرة، ٢٠٠٩، ص٤٤.

(٥٦) محمد محي الدين عوض: تشريعات مكافحة الإرهاب في الوطن العربي، أكاديمية نايف العربية للعلوم الأمنية، ١٩٩٩، ص٩٢.

(٥٧) د. محمود رجب فتح الله: الوسيط في الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، ٢٠١٩، ص٥١٤.

المصادر

أولاً: المعاجم:

١- منير البعلبكي: المورد قاموس إنكليزي- عربي، دار العلم للملايين، بيروت، ٢٠٠٤.

ثانياً: الكتب

١- د. أحمد عبيس نعمة الفتلاوي: الهجمات السيبرانية، دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر، ط١، منشورات زين الحقوقية، بيروت، ٢٠١٨.

٢- أيمن عبد الكريم حسين: الإرهاب دوافعه وتداعياته على الأمن والسلم الدوليين، مركز البيان للدراسات والتخطيط، بغداد، ٢٠١٨.

٣- د. خالد حسن أحمد لطفي: جرائم الإنترنت بين القرصنة الإلكترونية والإبتزاز الإلكتروني، ط١، دار الفكر الجامعي، الإسكندرية، ٢٠١٨.

٤- د. خالد ممدوح إبراهيم: الجرائم المعلوماتية، ط١، دار الفكر الجامعي، الإسكندرية، ٢٠٠٩.

٥- ضياء يحى السادات: مبادئ إستخدام الحاسوب الآلي والإنترنت وجهود مكافحة الجرائم الناشئة عنهما، بلا دار نشر، ٢٠١٢.

٦- عادل عبد الصادق الجحة: الإرهاب القوة في العلاقات الدولية نمط جديد وتحديات مختلفة، ط١، مركز الدراسات السياسية والإستراتيجية، القاهرة، ٢٠٠٩.

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. عمر أبو الفتوح عبد العظيم الحمامي: الحماية الجنائية للمعلومات المسجلة إلكترونياً، دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠١٠.

٩- عمر عباس خضير العبيدي: الإرهاب الإلكتروني في نطاق القانون الدولي، ط١، المركز العربي، القاهرة، ٢٠٢١.

١٠- محمد أمين الشواكبة: جرائم الحاسوب الإنترنت، ط٤، دار الثقافة للنشر والتوزيع، الأردن، ٢٠١١.

١١- محمد عبد الله أبو بكر سلامة: موسوعة جرائم المعلوماتية، جرائم الكمبيوتر والإنترنت، منشأة المعارف، الإسكندرية، ٢٠٠٦.
١٢- محمد كمال محمود الدسوقي: الحماية الجنائية لسرية المعلومات الإلكترونية، ط١، دار الفكر والقانون، ٢٠١٧.
١٣- محمد محي الدين عوض: تشريعات مكافحة الإرهاب في الوطن العربي، أكاديمية نايف العربية للعلوم الأمنية، ١٩٩٩.
١٤- د. محمود رجب فتح الله: الوسيط في الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، ٢٠١٩.
١٥- نعيم مغبغب: حماية برنامج الكمبيوتر الأساليب والثغرات، دراسة في القانون المقارن، ط١، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٦.
١٦- نوران شفيق: أثر التهديدات الإلكترونية على العلاقات الدولية، المكتب العربي للمعارف، القاهرة، ٢٠١٥.
١٧- د. هلالي عبد اللاه أحمد: جرائم الحاسوب والإنترنت، بين التجريم الجنائي وآليات المواجهة، دار النهضة العربية، القاهرة، ٢٠١٥.
١٨- وليد أبو سعد: أمن المعلومات، الموسوعة العربية للكمبيوتر، قسم الدورات التعليمية الإلكترونية، ٢٠٠٥.

ثالثاً: الرسائل والأطاريح الجامعية

١- درّار نسيمة: الأمن المعلوماتي وسبل مواجهة مخاطره في التعامل الإلكتروني، دراسة مقارنة، إطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد- تلمسان، ٢٠١٧.
٢- زهراء عماد محمد كلنتر: المسؤولية الدولية الناشئة عن الهجمات السيبرانية، رسالة ماجستير، كلية القانون، جامعة الكوفة، ٢٠١٦.
٣- سمية مزغيش: جرائم المساس بالأنظمة المعلوماتية، رسالة ماجستير، كلية الحقوق والعلوم السياسية قسم القانون، جامعة محمد خيضر بسكرة، الجزائر، ٢٠١٤.
٤- عمراني كمال الدين: السياسة الجنائية المنتهجة ضد الجرائم الإلكترونية، دراسة مقارنة، إطروحة دكتوراه، كلية الحقوق والعلوم السياسية قسم الحقوق، جامعة أبو بكر بلقايد- تلمسان، الجزائر، ٢٠١٦.
٥- لينا محمد متعب الأسدي: مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية، رسالة ماجستير، كلية الحقوق، جامعة النهرين، ٢٠١٢.
٦- ملياني عبد الوهاب: أمن المعلومات في بيئة الأعمال الإلكترونية، إطروحة دكتوراه، كلية الحقوق والعلوم السياسية قسم الحقوق، جامعة أبي بكر بلقايد-تلمسان، الجزائر، ٢٠١٧.

رابعاً: البحوث العلمية

١- د. حمدان رمضان محمد: الإرهاب الدولي وتداعياته على الأمن والسلم العالمي، دراسة تحليلية من منظور إجتماعي، بحث منشور في مجلة أبحاث التربية الأساسية، جامعة الموصل، مج١١، ع١، العراق، ٢٠١١.

٢- خليل يوسف جندي: المواجهة التشريعية للجريمة المعلوماتية على المستويين الدولي والوطني (دراسة مقارنة)، بحث منشور في مجلة كلية القانون للعلوم القانونية والسياسية، جامعة كركوك، مج٧، ع٢٦، العراق، ٢٠١٨.

خامساً: الاتفاقيات والبروتوكولات الدولية

١- اتفاقية بودابست لمكافحة جرائم المعلوماتية، لسنة ٢٠٠١، صادرة عن مجلس أوربا رقم ١٨٥ في ٢٠٠١/١١/٢٣.

٢- البروتوكول الإضافي الأول لعام ١٩٧٧.

سادساً: القرارات والوثائق الدولية

١- القرار رقم ٢٣٩/ ٥٧ بتاريخ ٣١/كانون الثاني/ يناير ٢٠٠٣.

٢- القرار رقم ٥٨/١٩٩ بتاريخ ٣٠/كانون الثاني/ يناير ٢٠٠٤.

٣- الوثيقة: UNODC/CCPCJ/EG.4/2013/2.

سابعاً: مصادر الشبكة الدولية للمعلومات

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

٢- تقرير عن إجتماع فريق الخبراء المعني بإجراء دراسة شاملة عن الجريمة السيبرانية، الذي عقد في فينا في الفترة من ١٠ الى ١٣ نيسان ٢٠١٧، ص٤، منشور على شبكة الإنترنت عبر الرابط الاتي: www.unodc.org/documents/organized-crime/cybercrime/-April-2017 ، (آخر زيارة للموقع في٢٠١٨/٨/١٩، ٠٠:٥م).

٣- د. عادل عبد الصادق: خطر الحروب السيبرانية عبر الفضاء الإلكتروني، ٢٠١٧، بحث منشور في مجلة لغة العصر متاح على شبكة الإنترنت عبر الرابط الآتي: aitmag.ahram.org.eg/news/83562.aspx، (آخر زيارة للموقع في ٢٠١٨/٧/١٣- ص١١:٠٠).

ثامناً: مصادر اللغة الأجنبية

1- Geneva, November 2003. See the International Telecommunication Union, cyber security handbook for developing countries, edition 2007.
2- H Allen, Julia, The CERT Guide to System and Network Security practices, Boston. MA, Addison, Wesley. 2001.
3- ICRC, "Exploring humanitarian law: IHL Guide, A legal manual for EHL teacher", ICRC, Geneva, January 2009.
4- 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.
5- Julia Cresswell, "Oxford Dictionary of word Origins: Cybernetics", Oxford Reference Online, Oxford University press, 2010.
6- K.saalbach, "Cyber War, Methods and practice", Version 9.0, University of Osnabruck-17 Jun 2014.

7- Norbert wiener: Cybernetic or control communication in the animal and the machine, M.I.T, Press, Second Edition, Cambridge, Massachusetts, 1948.
8- Micheal N.Schmitt, "Tallinn Manual on the International Law Applicable to Cyber Warfare", Cambridge University press, first publishes, 2013.
9- Marco Roscini, "World Wide Warfare- Jus ad bellum and the use of Cyber Force", Max Planck Yearbook of United Nations Law, Volume 14, 2010.
10- Michael Gervais, "Cyber Attacks and the Laws of War", Berkeley Journal of International Law, vol. 30, lss. 2, 2012.
11- Micheal S.Fuertes, "Cyber warfare, Unjust Actins in a just war", Florida International University, Full 2013.
12- 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.
13- Richard Kissel, "Glassory of Key Information Security Terms", National Institute of Stand ards and technology, U.S Department of Commerce, Revision, 2, May 2013.
14- 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.
15- 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.