الثقل النسبي للهجمات السيبرانية واختصاص المحكمة الجنائية الدولية

https://doi.org/10.23918/ilic10.15

د. لمى فاضل نايف[1]
مسؤولة وحدة الدراسات والبحوث في المركز الوطني للتعاون القضائي الدولي - مجلس القضاء الاعلى
luma95fadel@gmail.com

The relative Gravity of cyberattacks and the jurisdiction of the International Criminal Court

Dr. Luma Fadhil Nayyef
Head of the Studies and Research Unit at the National Center for International Judicial Cooperation - Supreme Judicial Council

الملخص

نتيجة للتطور والثورة المعلوماتية التي حدثت في العقود الماضية، أنتقلت النزاعات المسلحة والانتهاكات الجسيمة الى العالم الافتراضي المعلوماتي، فأصبح الفضاء المعلوماتي او الفضاء السيبراني(Cyber Space) ، ساحة للصراعات الدولية يدخل في سياقها التجسس والاختراق، والتحكم في قواعد البيانات التي تمس الأمن القومي للدول.

قد أصبحت الهجمات السيبرانية احدى الوسائل لارتكاب الجرائم بدون خسائر سواء أكانت مادية، ام بشرية، فاذا كانت القوة العسكرية تكلف الدول الكثير من الخسائر على المستويات جميعها فأنّ الهجمات السيبرانية مكنّت الدول ان تنفذ مخططاتها، وتضرب أنظمة دولة آخرى بكبسة زر واحدة، وان آثار دمارها قد يفوق آثار الانتهاكات الجسيمة التقليدية سواء أتدمير بنى تحتية، ام خسائر بشرية، ولا سيما بعد الهجوم السيبراني الذي شنته روسيا ضد استونيا سنة ٢٠٠٧، والذي تسبب في شلل تام للدولة، ومرافقها العسكرية والحكومية الحيوية، إذ يعد أول هجوم سيبراني تشنه دولة ضد دولة اخرى.

وفي هذا المجال، ينظر الى الفضاء المعلوماتي على أنه المجال الخامس للحرب من لدن الجيش، إذ تقضي "وزارة الدفاع الأمريكية" بالقول على أنه "على الرغم من ان الفضاء المعلوماتي هو مجال من صنع الانسان، الا انه بالغ الأهمية للعمليات العسكرية مثله مثل الأرض والبحر والجو والفضاء."

لذا هل من الممكن أن تعد هذه الهجمات –السيبرانية- جرائم دولية على وفق المادة (٥) من نظام روما للمحكمة الجنائية الدولية، وتدخل ضمن اختصاصها ومن ثم مقبوليتها امامها، وما الذي يميز هذه الهجمات، عن الجرائم السيبرانية والحروب السيبرانية.

الكلمات المفتاحية: الهجمات السيبرانية، الثقل النسبي، الجرائم السيبرانية، الحروب السيبرانية، المحكمة الجنائية الدولية.

Abstract

As a result of the development and information revolution that occurred in recent decades, armed conflicts and grave violations have moved to the virtual information world. The information space or cyber space has become an arena for international conflicts, including espionage, hacking, and controlling databases that affect the national security of states.

Cyber attacks have become a means to commit crimes without losses, whether material or human. If military force costs states a lot of losses at all levels, then cyber attacks have enabled states to implement their plans and strike the systems of another state with a single click. The effects of their destruction may exceed the effects of traditional grave violations, whether it be the destruction of infrastructure or human losses, especially after the cyber attack launched by Russia against Estonia in 2007, which caused a complete paralysis of the state and its vital military and governmental facilities, as it is considered the first cyber attack launched by one state against another.

In this regard, the information space is viewed as the fifth domain of warfare by the military, as the "U.S. Department of Defense" states that "although cyberspace is a man-made domain, it is as critical to military operations as land, sea, air, and space".

Therefore, is it possible for these cyber attacks to be considered international crimes according to Article (5) of the Rome Statute of the International Criminal Court, and fall within its jurisdiction and thus its admissibility before it, and what distinguishes these attacks from cyber crimes and cyber wars, in addition to the legal classification of these cyber attacks.

Keywords: Cyber attacks, relative gravity, cyber crimes, cyber warfare, International Criminal Court.

[1] الباحثة هي محقق قضائي ومسؤولة وحدة الدراسات والبحوث في المركز الوطني للتعاون القضائي الدولي – مجلس القضاء الاعلى.

المقدمة

يعد الطابع الدولي للهجمات السيبرانية هو من الصفات التي تميزها عن غيرها، إذ يطغى عليها هذا الطابع، وتتجاوز بذلك النطاق الوطني، فهي تتميز بالخطورة؛ لأنها لا تطال الافراد فحسب، وإنما أصبحت هجمات واسعة النطاق، وضخمة منسقة تطال البنى التحتية الأساسية الحساسة للمعلومات في أكثر من دولة، او تمثل نشاطات إرهابية على الانترنيت، ومن ثم فأنّ من السمات الفريدة لها إنّها تعمل في عالم غير مادي خالٍ من الحدود الإقليمية.

وعليه يوضح الوضع الأخير في العالم من أن الهجمات السيبرانية قد تكون واحدةً من أخطر التهديدات للسلم، والأمن الدوليين، فطبيعة العمليات الهجومية في الفضاء المعلوماتي تمثل تحديات فريدة للنظام الجنائي الدولي، وعليه يدور نقاش في الأوساط الاكاديمية القانونية حول تصنيف الهجمات السيبرانية كجرائم أساسية بمقتضى القانون الدولي الجنائي، بمعنى ربط الهجمات السيبرانية بجرائم الحرب، والابادة الجماعية، والجرائم ضد الإنسانية، وجريمة العدوان. فهل يتطلب نظام روما للمحكمة الجنائية الدولية تعديلا، وزيادة الهجمات السيبرانية الى الجرائم الأساسية المنصوص عليها في المادة (٥) منه؟

اولا: اهمية البحث: تنبع أهمية هذا البحث من التطور المتسارع في مجال التكنولوجيا الرقمية وما رافقه من بروز الهجمات السيبرانية كأحد أخطر التهديدات التي تواجه الأمن والسلم الدوليين في العصر الحديث. فقد أصبحت الهجمات الإلكترونية وسيلة جديدة تُستخدم في الاعتداء على الدول والبنى التحتية الحيوية، واستهداف الأنظمة المصرفية، وشبكات الطاقة، والاتصالات، وحتى الأنظمة العسكرية، مما قد يؤدي إلى خسائر بشرية واقتصادية جسيمة دون استخدام الأسلحة التقليدية.

وتكمن الأهمية القانونية للبحث في محاولة إدراج هذه الهجمات ضمن اختصاص المحكمة الجنائية الدولية، إذ يثير ذلك تساؤلات عميقة حول مدى إمكانية اعتبار الجرائم السيبرانية جرائم حرب أو جرائم ضد الإنسانية أو جرائم عدوان بموجب نظام روما الأساس لسنة ١٩٩٨. فالبيئة الرقمية تطرح تحديات غير مسبوقة تتعلق بتحديد المسؤولية الجنائية، ونطاق الاختصاص الإقليمي للمحكمة، وإثبات الركن المادي والمعنوي للجريمة في الفضاء الإلكتروني.

ثانيا: اشكالية البحث: تطرح الهجمات السيبرانية تحديات ذات صعوبة أمام المجتمع الدولي بسبب ثلاثة عوامل رئيسة، أولا، عدم وجود حدود قضائية إقليمية في الفضاء السيبراني، ثانيا، عدم وجود تشريعات موحدة بشأن هذه الهجمات في انحاء العالم بالاضافة الى عدم ادراجها ضمن احتصاص المحكمة الجنائية الدولية، ثالثا، التطور السريع والمستمر لهذه الهجمات. وسيستمر مرتكبو هذه الهجمات بالتطور، والتفوق على جهود جهات آنفاذ القانون ما لم تُعالج الدول هذه العوامل المترابطة كلها على نحو متعاون فيما بينها.

ثالثا: مناهج البحث: من اجل تحليل والوصول الى حل لاشكاليات البحث فضلا عن طبيعة البحث التي تطلبت استخدام اكثر من منهج من مناهج البحث العلمي، لذا ارتأينا الى الاعتماد على اكثر من منهج من مناهج البحث العلمي لضمان الترابط بينها، وعليه سنتبع المنهج الوصفي والمنهج التحليلي في هذا البحث.

رابعا: هيكلية البحث: سنقسم هذا البحث على مطلبين، سنتطرق في المطلب الاول الى التعريف بالهجمات السيبرانية، اما المطلب الثاني فسنتعرض فيه الى الهجمات السيبرانية وثقلها النسبي وحدود اختصاص المحكمة الجنائية الدولية.

المطلب الاول

التعريف بالهجمات السيبرانية

لم يحظ استخدام التقنيات المعلوماتية باهتمام كبير في مجال دراسة القانون الدولي الجنائي، ومع ازدياد الجرائم السيبرانية بصورة مستمرة من حيث الحجم، والتطور، والتكلفة والاضرار الواسعة النطاق، وصلنا الى نقطة التحول إذ اصبح من الضروري فحص الأنعكاسات على القانون الدولي الجنائي لهذه الظاهرة، وعلى الرغم مما تقدم لا يوجد تعريف جامع مانع لهذه الهجمات، وان عدم وجود تعريف متفق عليه من لدن المجتمع الدولي أثار صعوبات بالغة بهذا الشأن من حيث التحديات التي تواجه المختصين في القانون الدولي العام بسبب الغموض الذي يكتنف هذا المصطلح. وعليه سنقسم هذا المطلب على فرعين، في الفرع الاول سنوضح تعريف الهجمات السيبرانية، وفي الفرع الثاني سنوضح تمييز الهجمات السيبرانية عن مصطلحات مشابهة.

الفرع الاول

مفهوم الهجمات السيبرانية[١]

فضلنا استعمال هذا المصطلح بدلا من استعمال مصطلحي "الفضاء السيبراني" و "الحرب السيبرانية"، وذلك لأنّ مصطلح "الهجمات السيبرانية" أوسع نطاقا ويشتمل على بقية المصطلحات المذكورة، فضلا عن أن مصطلح "الحرب السيبرانية" غير محبذ في الوقت الحاضر على مستوى الدراسات الاكاديمية، والتنظيم القانوني الدولي.

فقد عرّفه " Fuertes " على أنه (هجوم عبر الانترنت يقوم على التسلل إلى مواقع الكترونية غير مرخص بالدخول إليها، بهدف تعطيل أو إتلاف البيانات المتوفرة فيها أو الاستحواذ عليها، وهي عبارة عن سلسلة هجمات الكترونية تقوم بها دولة ضد اخرى).

---

[١] تؤكد المراجع العلمية ان اول من استخدم مصطلح السيبرانية هو عالم الرياضيات "نوبرت وينر" "Nobert Wiener"، سنة ١٩٤٨، وذلك في كتابة الشهير "علم التحكم الالي" او "التحكم والاتصال في الحيوان والالة"، وذلك للإشارة الى اليات التنظيم الذاتي. اما فيما يتعلق بالبحث عن مصدر كلمة "سايبر" "Cyber" في المعاجم اللغوية، فيتضح انها يونانية الأصل وترجع الى مصطلح "Kybernetes"، الذي ورد بداية في مؤلفات الخيال العلمي ويعني القيادة والتحكم عن بعد. اما قاموس "مورد" يعرف "السيبرانية" هي علم الضبط، ومصدرها "Cybernetics"، وهو مصدر يتطابق مع مفهوم الهجمات السيبرانية "أي ضبط الأشياء عن بعد والسيطرة عليها". د. احمد عبيس الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، بحث منشور، مجلة المحقق الحلي للعلوم القانونية والسياسية، جامعة بابل، العدد الرابع، السنة الثأمنة، ٢٠١٦، ص٦١٤.

Cybernetics or Control and Communication in The Animal and The Machine. See: Wiener Norbert. Cybernetics or Control and Communication in The Animal and The Machine, M.I.T, Press, Second Edition, Cambridge, Massachusetts, 1948, Available At: https://cutt.ly/akhwlob. (5/12/2025).

فيما عرَفه " Schmitt "على أنه (مجموعة من الإجراءات التي تتخذها الدولة للهجوم على نظم المعلومات المعادية بهدف التأثير والإضرار بها، وفي الوقت نفسه للدفاع عن نظم المعلومات الخاصة بالدولة المهاجمة)[١].

اما بشأن الخبراء القانونيين التابعين لحلف شمال الأطلسي "الناتو" في "دليل تالين" "Manual de Tallinn"، فقد عرفوا الهجمات السيبرانية في القاعدة (٣٠) بأنّها (كل العمليات السيبرانية سواء كانت هجومية او دفاعية، يهدف من خلالها التسبب بالاصابة او الوفاة لاشخاص او الاضرار وتدمير الأهداف "الاعيان")[٢].

الفرع الثاني

تمييز الهجمات السيبرانية عن مصطلحات مشابهة

هنالك مصطلحات تتشابه مع الهجمات السيبرانية فكل منهم يرتكب في الفضاء السيبراني[٣]، لذا سنحاول توضيح وجه الشبه، والخلاف بينهم.

اولا: تمييز الهجمات السيبرانية عن الجرائم السيبرانية

عرَف مجلس الاتفاقية الأوروبية للجرائم الالكترونية (CECC) الجريمة السيبرانية بأنّها (مجموعة واسعة من الانشطة الضارة بما في ذلك الاعتراض غير القانوني للبيانات، وتدخلات النظام التي تهدد سلامة الشبكة وتوافرها وانتهاكات حقوق الطبع والنشر)[٤].

وتجدر الإشارة الى أن الجريمة السيبرانية لا يوجد تعريف معترف بها عالميا، بل هنالك جوانب لها معترف بها على نطاق واسع، إذ جاء في إرشادات "الاسكو للتشريعات السيبرانية" "ESCWA" إنّ الجريمة السيبرانية تنقسم على نوعين أساسيين، النوع الأول هو الذي يكون الحاسوب أداة تنفذ بوساطتها الجريمة (كجرائم الاختلاس والافعال الإباحية وانتحال الصفة) وهي جرائم عادية، والحاسوب مجرد "الوسيلة" التي سمحت بارتكابها.

والنوع الثاني هو الذي يكون جهاز الحاسوب وشبكات الحواسيب وبرامجها موضوعها للجريمة، أي إن الفعل الجرمي أُرتكب على هذا الجهاز (مثل اختراق نظام امان او ارسال برنامج خبيث او التعدي على اسم موقع على الانترنيت مما يشكل جريمة ضد حق من حقوق الملكية الفكرية)[٥].

وان **وجه الشبه** بينهما هو المجال الذي يرتكب به كل من الهجوم، والجريمة السيبراني، فكلاهما يقعان في الفضاء السيبراني، أما **وجه الخلاف** بينهما فيكون من ناحيتين، الناحية الأولى من حيث **الأشخاص**، فغالباً ما يكون مرتكبو الجرائم السيبرانية هم الأفراد وتوجه ضد مؤسسات مالية، أو شركات، وحتى أفراداً داخل، أو خارج إقليم الدولة، بخلاف الهجمات التي تتم من لدن دول، أو مجموعات حكومية، أو غير حكومية ضد دولة أخرى[٦].

اما الناحية الثانية فهي تختص بالأهداف، فغالباً ما يكون الهدف من الجرائم السيبرانية إثبات مهارة الفاعل تقنياً وقدرته على اختراق أجهزة الكمبيوتر، أو لأجل التسلية والترفيه أو تحقيق مكاسب شخصية كسرقة المليكة الفكرية عن طريق شبكات الحاسب الآلي، أو التسلل إلى أنظمة المصارف، والتلاعب بأرقام الحسابات وتحويل الأموال دون الحاجة إلى تدمير وتعطيل شبكة الكمبيوتر المستهدفة (على الرغم أنه قد يعطلونها في بعض الحالات وتكون هذه الأفعال مجرمة بمقتضى القانون الوطني)، بخلاف الهجمات السيبرانية التي يستهدف مرتكبوها الأمن القومي، والسياسي للدولة ويقوم هؤلاء بتخريب الشبكات التي تتحكم بالبنى التحتية الأساسية في الدولة، وتدميرها بقصد إرباكها، وزعزعة النظام فيها لتحقيق أهداف أمنية، أو عسكرية، أو سياسية[٧].

---

(1) Schmitt, M.N. Computer Network Attack and the Use of Force in International Law through on a Normative, The Colombia Journal of Transitional Law, 1999, Vol.27, No.885-937, P.7;

د. احمد عبيس الفتلاوي، الهجمات السيبرانية (دراسة قانونية تحليلية بشان تحديات تنظيمها المعاصر)، منشورات زين الحقوقية، بيروت–لبنان،ط١، ٢٠١٨،ص١٦.

(2) Kosmas Pipyros, Christos Thraska lip Mitro, Dimitris Gritzalis, Theodoros. A new strategy for improving her stacks evaluation in the context of Tallinn Manual, P. 4.

https://www.infosec.aueb.gr/Publications/COSE%20SI%20Tallinn%20Website.pdf (6/1/2026); Schmitt Michael (gen ed). Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, New York, First Published, 2013, Available At: https://cutt.ly/tkofrbK(6/1/2026) ;

محمد فخر الدين، حدود المجال الخامس – ما هي الحروب السيبرانية، مؤتمر حروب في الفضاء السيبراني، ٢٠١٥، بحث متاح على الموقع الالكتروني: https://seconf.wordpress.com/2015/05/15 (6/1/2026).

(٣) عرفت الوكالة الفرنسية لأمن أنظمة الإعلام (ANSSI) الفضاء السيبراني على أنه (فضاء التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية). كما عرفه الاتحاد الدولي للاتصالات الذي يصف الفضاء السيبراني بأنه (المجال المادي وغير المادي الذي يتكون وينتج عن عناصر هي: أجهزة الكمبيوتر الشبكات البرمجيات حوسبة المعلومات المحتوى معطيات النقل والتحكم ومستخدمو كل هذه العناصر). كما عرفه البعض بوصفه (الذراع الرابعة للجيوش الحديثة). عباس بدران، الحروب الالكترونية (الاشتباك في عالم متغير)، مركز دراسات الحكومة الالكترونية، بيروت، ٢٠١٠، ص٤.

Olivier KEMPF, Introduction à la Cyberstratégie, Paris, Economica, 2012, P. 9; The International Télécommunication Union, ITU Toolkit for Cybercrime Législation, Geneva, 2010, P. 12.

(4) Ansam Qasim Hachim. CRITICAL RESEARCH STUDY ON PREVENTING CYBER CRIMES THROUGH EFFECTIVE CYBER LAW CONCEPTS AND POLICIES FROM GLOBAL PERSPECTIVES; Research published in English, Iraqi University Journal, Issue 40/1, no publication year, p. 606.

(٥) إرشادات الاسكو للتشريعات السيبرانية، مشروع تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية، بيروت، ٢٠١٢، ص١١٧ وص١١٨، متاح على الموقع الالكتروني: https://digitallibrary.un.org/record/1292295?ln=ar .. (8/1/2026).

(٦) نور امير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الانساني، رسالة ماجستير، الجامعة الافتراضية السورية، ٢٠٢١، ص١٤؛ زهراء عماد محمد كلنتر، المسؤولية الدولية الناشئة عن الهجمات السيبرانية، رسالة ماجستير، كلية القانون، جامعة الكوفة، ٢٠١٦، ص١٧.

(7) 30. Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue & Julia Spiegel. The law of Cyber-Attack, California law review, 2012, P.835.

ثانيا: تمييز الهجمات السيبرانية عن الحرب السيبرانية

ان الحرب السيبرانية كما عرَفتها مؤسسة راند (Rand) بأنّها (حرب الدول والمنظمات الدولية ضد دول اخرى من أجل تدمير شبكات الكمبيوتر والمعلومات، وهذه الحرب تتم عن طريق الفايروسات، أحصنة طروادة والبرمجيات الخبيثة الاخرى)[١].

إنّ الحرب السيبرانية تتميز بخصائص عن النزاعات المسلحة التقليدية سواء من حيث ماهيتها، أم مضمونها، فبخلاف النزاعات المسلحة التقليدية لا يمكن تحديد وقت بدء الحرب السيبرانية، أو انتهائها، بل إن فاعلية الحرب السيبرانية تكمن في عدم إمكانية تحديد وقت بدأها[٢].

كما إنّ صعوبة التوصل، ومعرفة مصدر الحرب السيبرانية تمثل عامل اختلاف آخر، وذلك لعدة أسباب منها، كثرة الجهات الفاعلة في الفضاء السيبراني كالدول، و المنظمات والجماعات الحكومية وغير الحكومية، والإرهابيين، و القراصنة وحتى الأفراد[٣].

المطلب الثاني

الهجمات السيبرانية وثقلها النسبي وحدود اختصاص المحكمة الجنائية الدولية

لم يحظ استخدام التقنيات المعلوماتية كوسيلة لارتكاب الجرائم، او التحريض عليها او تسهيلها بمقتضى اختصاص المحكمة الجنائية الدولية حتى الآن باهتمام واسع في مجال دراسة القانون الدولي الجنائي[٤]، إذ تم تجاهل معالجة الهجمات السيبرانية في اثناء مفاوضات نظام روما الأساس للمحكمة الجنائية الدولية سنة ١٩٩٨، ومن ثم فهي غائبة في النسخة النهائية له. على الرغم من بدأ الدول بمعالجة هذه الهجمات.

لذا سنبحث عن كيفية ارتكاب الجرائم الدولية، او تسهيلها، او التحريض عليها في الفضاء السيبراني، والتي تقع ضمن اختصاص المحكمة الجنائية الدولية، أي هل من الممكن ان تكوّن هذه الهجمات السيبرانية جرائم إبادة جماعية، او جرائم ضد الإنسانية، او جرائم حرب او جرائم العدوان، وإمكانية ان تختص بها المحكمة الجنائية الدولية ومن ثم قبولها اذا كانت ذات ثقل نسبي؟ فمع ازدياد هذه الهجمات السيبرانية من حيث الحجم والتطور والتكلفة اصبح من الضروري فحص الأنعكاسات على القانون الدولي الجنائي لهذه الظاهرة. فهل من الممكن تصنيفها كجرائم أساسية بمقتضى القانون الدولي الجنائي شأنها شأن الجرائم الدولية الأربع التي تختص بها المحكمة الجنائية الدولية؟ بمعنى هل من الممكن تعديل هذا النظام من اجل هذه الهجمات العابرة للحدود الوطنية، وتصنيفها كجريمة دولية؟[٥]

لذا سنقسم هذا المطلب على ثلاثة فروع، وسنوضح الثقل النسبي للهجمات السيبرانية وكيفية تحولها الى جرائم إبادة جماعية، وجرائم ضد الإنسانية، وجرائم حرب، وجريمة العدوان.

الفرع الاول

الثقل النسبي للهجمات السيبرانية بوصفها جرائم إبادة جماعية وجرائم ضد الانسانية

يمكن أن تمثل الهجمات السيبرانية وسيلة جديدة لارتكاب جريمة الإبادة الجماعية ويكون للمحكمة الجنائية الدولية اختصاص بشأنها بمقتضى نظام روما الأساس، اذا أدت هذه الهجمات عواقب مادية ضارة على الافراد، اذا تم ارتكابها كجزء من هجوم واسع النطاق او منهجي على وفق نص المادة (٦) من النظام[٦].

وعلى وفق "دليل تالين" يمكن استخدام التقنيات السيبرانية للتحريض على ارتكاب الجرائم بمقتضى اختصاص المحكمة الجنائية الدولية، او تسهيل ارتكابها، فعلى سبيل المثال، بوساطة عمل تحضيري للابادة الجماعية مثل اقتحام شبكة للحصول على أسماء الافراد المسجلين كعرق معين في تعداد الدولة من اجل ارتكاب هذه الجريمة[٧].

---

[1] Cyber Warfare, 2015, available at: http://www.rand.org/topics/cyberwarfare.htm. (10/1/2026).

[2] Martin C. Libicki. Cyber deterrence and Cyber war Project Air Force, prepared for United States Air Force, 2009, P.170-182.

[٣] زهراء عماد محمد كلنتر، المرجع السابق، ص١٩.

[٤] في سنة ٢٠٠٠، دعت الجمعية العامة للأمم المتحدة الدول أيضاً إلى "ضمان أن قوانينها وممارساتها تقضي على الملاذات الأمنة لأولئك الذين يسيئون استخدام تكنولوجيا المعلومات بشكل إجرامي (قرار الجمعية العامة للأمم المتحدة ٦٣/٥٥ في ٤ ديسمبر ٢٠٠٠، الفقرة (١/ أ)). علاوة على ذلك، تم إبرام عدد من المعاهدات للتصدي للإجرام السيبراني منها "اتفاقية بودابست" لسنة ٢٠٠١ بشأن الجرائم السيبرانية، التي تم التفاوض عليها في إطار مجلس أوروبا ودخلت حيز التنفيذ في ١ يوليو ٢٠٠٤، تتطلب من الدول الأطراف تجريم والمعاقبة عن الجرائم المعلوماتية في تشريعاتها الوطنية، وتوسيع نطاق اختصاصها ليشمل الجرائم الناشئة عن أراضيها أو من قبل رعاياها، وتقديم المساعدة المتبادلة في التحقيقات والملاحقات القضائية، إذ تعد اول صك دولي الذي اتجه الى تجريم كافة اشكال الجريمة السيبرانية. ينظر: اتفاقية بودابست: https://rm.coe.int/budapest-convention-in-arabic/1680739173. (20/1/2026).
ايمن عبد الحفيظ، حدود مشروعية دور أجهزة الشرطة في مواجهة الجرائم المعلوماتية، مجلة مركز بحوث الشرطة بأكاديمية مبارك، العدد ٢٥، يناير ٢٠٠٤، ص٣٨٩؛ خالد ظاهر عبد الله جابر السهيل المطيري، مواجهة الجرائم المعلوماتية في ضوء التشريعات الجنائية المعاصرة والاتفاقيات الدولية، بحث منشور على الأنترنيت، ٢٠٢٠، ص٤٥، https://lsej.journals.ekb.eg/article_92862_fb06c92ea27475de8608ea963e601285.pdf. (20/1/2026).

[٥] ينظر نص المادة (٣/٢٥) من النظام الأساس للمحكمة الجنائية الدولية، إذا تم اعتبار الهجمات السيبرانية جرائم جديدة وليست وسائل جديدة لارتكاب جرائم قائمة، من ناحية أخرى، فأنّ التحقيق أو المقاضاة من قبل المحكمة الجنائية الدولية سيكون مستحيلاً كما يتعارض مع مبدأ "لا جريمة ولا عقوبة الا بنص" المادة (٢٢) من النظام الأساس للمحكمة الجنائية الدولية.

[6] According to Article 6 of the ICC Statute, an act of genocide requires an ‘‘intent to destroy, in whole or in part, a national, ethnical, racial or religious group, as such’’.

[٧] دليل تالين"Tallinn Manual" ، صدرت النسخة الأولى منه في مارس ٢٠١٣، وقد تمثل هدفه الرئيسي في التحقيق في القضايا وتطبيق القانون الدولي في مجال الحرب السيبرانية، ويتكون الدليل من قسمين رئيسيين هما: قانون الأمن السيبراني الدولي، وقانون النزاعات المسلحة السيبرانية وذلك في سبعة فصول. كما تضمن (٩٥) قاعدة قانونية صاغتها لجنة الخبراء في القانون الدولي البارزين في تالين باستونيا، على نحو يحدد الخطوط الحمراء التي تستوجب التدخل العسكري، وطرق مشاركة مختلف الأطراف. وفي سنة ٢٠١٦ تم إصدار النسخة المحدثة لدليل تالين القانون الدولي المطبق على عمليات الأنترنت ليشمل القواعد التي حقق

ويمكن للافراد أيضا تحريض الآخرين على ارتكاب الإبادة الجماعية من نشر تعليقات لهذا الغرض على المدونات مثل منصة "X" او وسائل التواصل الاجتماعي الاخرى، فعلى سبيل المثال، لاحظت "اللجنة الدولية المستقلة لتقصي الحقائق بشأن ميانمار" التي انشأها مجلس حقوق الانسان التابع للأمم المتحدة[١] ما يأتي:

"دور وسائل التواصل الاجتماعي مهم، لقد كان Facebook أداة مفيدة لأولئك الذين يسعون إلى نشر الكراهية، في سياق أن يكون Facebook بالنسبة لمعظم المستخدمين هو الانترنيت على الرغم من التحسن في الأشهر الأخيرة، إلا أن استجابة Facebook كانت بطيئة وغير فعالة، ينبغي فحص المدى الذي أدت به منشورات ورسائل Facebook إلى التمييز والعنف في العالم الحقيقي بشكل مستقل ودقيق"[٢].

وفي سبتمبر سنة ٢٠١٢، شجبت أذربيجان أيضاً الهجمات السيبرانية التي شنها ما يُسمّى بـ "الجيش السيبراني الأرمني" تحت توجيه وسيطرة أرمينيا، والتي كانت تسعى إلى تمجيد الإرهابيين، وإهانة ضحاياهم، وكذلك إلى الدعوة والترويج والتحريض على الكراهية والتمييز، والعنف بدوافع عرقية او دينية[٣].

وفيما يتعلق بالارتباط بين الهجمات السيبرانية، وجريمة الإبادة الجماعية، خلص خبراء من "دليل تالين" إلى أن الهجوم السيبراني سيحدث قبل شن الإبادة الجماعية إذ سيتم استخدامه لتحديد الأفراد الذين ينتمون إلى المجموعة المستهدفة من شأنه أن يتدخل في المرحلة التحضيرية للإبادة الجماعية ولكن لا يمكن وصفه بأنه إبادة جماعية. ولكن لاحظ جانب من الفقه انه يمكن أن يكون الهجوم السيبراني صورة من صور التحريض العلني والمباشر على ارتكاب الإبادة الجماعية، كما تحظر "اتفاقية منع وقمع جريمة الإبادة الجماعية"، وفي حين تم وصف التحريض على أنه عمل من أعمال الإبادة الجماعية في كُلٍ من النظام الأساس للمحكمة الجنائية الدولية ليوغوسلافيا السابقة، وفي النظام الأساس للمحكمة الجنائية الدولية لرواندا، فأنّ هذا لم يعد هذا هو الحال في نظام روما الأساس، إذ أصبح التحريض على ارتكاب الإبادة الجماعية صورة من صور المسؤولية، وعلى وفق المادة (٢٥) من نظام روما الأساس فإنّ أي شخص يسهم في ارتكاب جرائم الإبادة الجماعية يمكن أيضا تحميله المسؤولية عن الجريمة، إما بالتحريض، أو بالتواطؤ، او المساعدة[٤].

كما يمكن ان تمثل هذه الهجمات جرائم ضد الانسانية على وفق المادة (٧) من نظام روما للمحكمة الجنائية الدولية سواء أوقعت في نزاع مسلح، ام لا.

إذ خلص فريق الخبراء الحكوميين التابع للأمم المتحدة الى ان الأفعال المرتكبة بوسائل الكمبيوتر يمكن ان تمثل جرائم ضد الانسانية، وفي هذه الحالة الهجوم عن طريق الانترنت يتم ارتكابه كجزء من هجوم واسع النطاق ضد أي سكان مدنيين على وفق دولة ما، أو اتباعا لها، او سياسة تنظيمية، أو منهجية موجهة إلى ارتكاب هذا الهجوم، وفي حالات نادرة فإنّ الهجوم عن طريق الانترنت يمكن أن يكون وسيلة جديدة لارتكاب جرائم ضد الانسانية، مثل القتل، أو الإبادة[٥].

الفرع الثاني

الثقل النسبي للهجمات السيبرانية بوصفها جرائم حرب

يمكن أن تمثل الهجمات السيبرانية وسيلة جديدة لارتكاب جريمة من جرائم الحرب المنصوص عليها في نظام روما للمحكمة الجنائية الدولية، مثل الهجمات السيبرانية التي يشنها المتحاربون في سياق نزاع مسلح ومرتبط به، والتي تسعى عن قصد على سبيل المثال، الى التسبب بوقوع إصابات في صفوف المدنيين، او تدمير اعيان محمية، او إنها تؤدي الى خسائر عرضية في الأرواح، أو إصابات للمدنيين، أو إلحاق أضراراً بالأعيان المدنية، أو أضراراً جسيمة واسعة النطاق، وطويلة الأمد البيئة الطبيعية التي ستكون جسيمة على نحو واضح فيما يتعلق بالميزة العسكرية العامة الملموسة، والمباشرة، والمتوقعة إنها ترقى إلى جرائم الحرب بمقتضى المادة (٨ (٢) (ب) (١) و (٢)) و (٤) ، والمادة ٨ (٢) (هـ) (أ)) من نظام روما الأساس.

وفي الواقع، فالهجمات السيبرانية قادرة على إحداث عواقب مادية مدمرة في العالم الحقيقي المادي من إفساد أنظمة تشغيل البنى التحتية المادية مثل أنظمة التحكم الإشرافي واكتساب البيانات (SCADA)، مما قد يؤدي إلى خلل في هذه البنى

فيها الإصدار الأول، ويضم أربعة أجزاء رئيسية، وبلغت عدد القواعد التي يمكن تطبيقها على العمليات السيبرانية (١٥٤) قاعدة من قواعد القانون الدولي. للمزيد من التفاصيل ينظر:

Tallinn Manual on the International Law Applicable to Cyber Warfare, Group of Experts and the Invitation of the NATO cooperative Cyber Defense Center of Excellence, Cambridge university Press, 2013; Laszlo Kovacs. cyper security policy and strategy in the European union and NATO, Revista Academiei Fortelor Terestre, Vol. 1. No. 89, 2018.

[١] مجلس حقوق الانسان هو هيئة حكوميَّة دوليَّة تابعة لمنظومة الأمم المتحدة، ويتألف من (٤٧) دولة مسؤولة عن تعزيز جميع حقوق الانسان وحمايتها في كافة أنحاء العالم من خلال معالجة حالات انتهاكات حقوق الانسان وتقديم توصيات بشأنها، بما في ذلك الاستجابة لحالات الطوارئ في مجال حقوق الانسان. ويمتلك المجلس صلاحية مناقشة كل المواضيع لحقوق الانسان التي تتطلب اهتمامه على مدار العام. ويعقد اجتماعاته في مكتب الأمم المتحدة في جنيف. وقد حل مجلس حقوق الانسان الذي أنشأته الجمعية العامة في ١٥ آذار/مارس ٢٠٠٦ والذي يقدم التقارير مباشرة للجمعية العامة، محل لجنة الأمم المتحدة لحقوق الانسان البالغة من العمر ٦٠ سنة، بوصفها الهيئة الرئيسة للأمم المتحدة والحكومية والدولية المسؤولة عن حقوق الانسان. ينظر:

https://www.ohchr.org/ar/hrbodies/hrc/home ; https://www.un.org/ar/global-issues/human-rights . (2/2/2026).

[2] Report of the Independent International Fact-Finding Commission on Myan- mar, UN Doc. A/HRC/39/64, 24 August 2018, para. 74.

[3] Letter dated 6 September 2012 from the Charge d'affaires a.i. of the Permanent Mission of Azerbaijan to the United Nations addressed to the Secretary-General, 7 September 2012, UN Doc. A/66/897–S/2012/687, P. 1.

[٤] تنص المادة (٢٥/٣/هـ) من نظام روما للمحكمة الجنائية الدولية على انه (فيما يتعلق بجريمة الإبادة الجماعية، التحريض المباشر والعلني على ارتكاب جريمة الإبادة الجماعية).

Gianpiero Greco. CYBER-ATTACKS AS AGGRESSION CRIMES IN CYBERSPACE IN THE CONTEXT OF INTERNATIONAL CRIMINAL LAW, European Journal of Political Science Studies, Vol. 4, Issue. 1, 2020, P. 43.

[5] Gianpiero Greco. Ibid, P.43.

التحتية، وإمكانية فقدان الأرواح، أو تدمير الممتلكات ومثاله، الكتاب المدرسي هو هجوم إلكتروني يقوم به أحد المحاربين، ويوقف نظام التبريد لمفاعل طاقة نووية يقع في أراضي العدو، مما يتسبب في إطلاق مواد مشعة تصل إلى المدنيين بصورة عشوائية[١].

وقد خلص فريق الخبراء الحكوميين التابع للأمم المتحدة إلى أن الأفعال المرتكبة بوسائل الكمبيوتر يمكن وصفها بأنها جرائم حرب كما هو الحال في المادة (٨) من نظام روما الأساس، إذا كانت تستوفى المتطلبات الموضوعية "الفعل الإجرامي" والمتطلبات الذاتية "القصد الجنائي"، بشرط وجود رابط قتالي أي ان مثل هذه الهجمات تكون جزءا من الصراع المستمر[٢].

الفرع الثالث

الثقل النسبي للهجمات السيبرانية بوصفها جرائم العدوان

ان وردت جريمة العدوان في المادة (٥/ف١/د) ضمن الجرائم الجسيمة التي تدخل في اختصاص المحكمة الجنائية الدولية ومع ذلك، لم يتم التوصل إلى توافق في الاراء بين المندوبين بشأن تعريفها، ولا على آلية تفعيل المحكمة، وكيفية ممارسة اختصاصها على الجريمة، وتركت هذه القضايا للمؤتمر الاستعراضي اللاحق الذي انعقد في كمبالا- أوغندا، في سنة ٢٠١٠.

وأدى المؤتمر إلى موافقة جمعية الدول الأطراف على ما يُسمّى بـ "تسوية كمبالا"، ولكن في وقت لاحق فقط فُعلت سلسلة من التعديلات على نظام روما الأساسي سنة ٢٠١٧، والتي حددت أخيرًا "جريمة العدوان" التي تعاقب عليها المادة (٨ مكررا) من نظام روما الأساس، وشروط ممارسة الولاية القضائية على هذه الجرائم، في المادة (١٥) من نظام روما الأساس.

وتنص (الفقرة ١ من المادة ٨ مكرر) من نظام روما الأساس على تعريف جريمة العدوان بأنها (التخطيط أو الإعداد أو البدء أو التنفيذ من قبل شخص قادر على ممارسة السيطرة أو توجيه العمل السياسي أو العسكري لدولة ما على نحو فعال، عمل عدواني يمثل، بحكم طابعه وخطورته ونطاقه، انتهاكا واضحا لميثاق الأمم المتحدة). وهذه الصياغة تجعل من المستحيل صراحة على المحكمة الجنائية الدولية محاكمة الأفراد الذين يتصرفون بمفردهم، أو الذين يمكن أن يقودوا مجموعة من الجهات الفاعلة غير الحكومية.

وعليه فإنّ هنالك قيدين مهمين الاول، إن تأجيل وصف الجريمة الدولية بقرار الجمعية العامة للأمم المتحدة في سنة ١٩٧٤ - عندما لم يتم التفكير في صور الحرب المعاصرة والمختلطة - يعني أن تعريفاً عفا عليه الزمن تبلور في قانون المعاهدات، ومن ثم منع المزيد من التطورات العرفية، كما يتم تعريف أعمال العدوان بالطريقة التي يتم بها تنفيذها (النهج الآلي)، وليس من عواقبها (نهج الآثار)، مما يجعل من الصعب أن تقع الهجمات السيبرانية ضمن نطاق التعريف[٣].

وهنالك قيد آخر على تصنيف الهجمات السيبرانية كجرائم عدوان مستمد من المادتين (١٥ مكرر وثالثا) من نظام روما الأساس، اللتان تنصان على أن المحكمة الجنائية الدولية لا تتمتع بالولاية القضائية؛ إلَا إذا أُرتكبت دولة عدوانا على دولة أخرى، وأن القانون لا ينطبق إلا على الدول التي قامت فعليا صدقت على تعديلات كمبالا، أي ٣٥ دولة من بين الدول الأطراف الحالية والبالغ عددها ١٢٣ دولة. وكحد إضافي من إمكانية تطبيق الجريمة الجديدة، تم توفير اخيرا إمكانية لكل دولة مصدقة أن تنأى بنفسها عن التعديلات في أي وقت ما يسمى بـ "شرط عدم الالتزام" [٤].

وان الوصول الى مستوى العدوان، ينبغي ان يفي الهجوم السيبراني بمتطلبات "الثقل النسبي"، وهو العنصر المميز لوصول السلوك المحظور[٥] الى عتبة الخطورة المطلوبة لتحريك المسؤولية الجنائية الفردية امام المحكمة الجنائية الدولية، فصلا عن تكييف العمل العدواني بكونه انتهاكا واضحا لميثاق الأمم المتحدة بحكم "طبيعته وخطورته ونطاقه"[٦].

نخلص مما تقدم، تمثل العمليات الهجومية في الفضاء المعلوماتي تحديات فريدة للنظام القانوني الدولي، وهي التحديات التي يواجهها المجتمع الدولي، إذ جُمعت معظم هذه الجهود في "دليل تالين"، وهي دراسات أكاديمية غير ملزمة على الرغم من كونها موثوقة ومع ذلك، فهي علامة على رغبة الدول في تنظيم الفضاء المعلوماتي. وان الغرض من التأكيد على شرط "الثقل النسبي"، يتجسد في حصر جريمة العدوان عند أخطر انتهاكات القانون الدولي.

وكما واضح فأنّ النقاش داخل القانون الدولي الجنائي حول تصنيف الهجمات السيبرانية كجرائم أساسية لا يزال مستمراً، ولم يسفر عن إجابات محددة حتى الآن، كما أن تصنيف الهجمات السيبرانية كجرائم عدوان أمر بالغ الأهمية على نحو خاص، واعتمادًا على النهج الذي يتبعونه لا يزال لدى الخبراء القانونيين آراء مختلفة حول هذا الموضوع. وعلى وفق

---

(1) Marco Roscini. Gravity in the statute of the international criminal court and cyber conduct that con- stitutes, instigates or facilitates international crim, Criminal Law Forum, 2019, pp 249,250.

(2) Gianpiero Greco. OP. cit, P 43.

(3) Kocibelli, A. Ibid, P 39.

(٤) تنص المادة (١٧) من اتفاقية فيينا لقانون المعاهدات لسنة ١٩٦٩ على انه (١) مع عدم الإخلال بالمواد من ١٩ إلى ٢٣، لا يكون رضا الدولة الالتزام بجزء من معاهدة نافذا إلا إذا سمحت بذلك المعاهدة أو وافقت على ذلك الدول المتعاقدة الأخرى.

٢) لا يكون رضا الدولة الالتزام بمعاهدة تسمح بالاختيار بين نصوص مختلفة ساريا إلا إذا تبين إلى أي من النصوص انصرف رضاها).

Gianpiero Greco. OP. cit, P. 45.

(٥) يعرف السلوك المحظور دوليا بانه (هو كل فعل او امتناع عن القيام بفعل مخالف لقواعد القانون الدولي يرتكب باسم دولة او منظمة او جهة غير حكومية او افراد ويترتب عليه الاعتداء على المصالح التي يحميها هذا القانون مما يسبب اخلالا بالنظام العام الدولي فيقتضي تجريمه والمعاقبة عليه). كريم طالب حمادي الشجيري، الثقل النسبي للسلوك المحظور (دراسة في تحديد الجرائم الأكثر خطورة على الصعيدين الوطني والدولي)، رسالة ماجستير، مقدمة الى معهد العلمين للدراسات العليا، قسم القانون، ٢٠٢٣، ص٤٦.

(٦) د. احمد عبيس الفتلاوي وقاسم محمد مهدي الغزي، الدليل في فهم جريمة العدوان السيبرانية (دراسة في اطار مواجهة قانونية وسياسية فاعلة)، منشورات زين الحقوقية، لبنان، ط١، ٢٠٢٤، ص٣٣٦ وص٣٣٧.

جانب من الفقه الدولي يرون بأنّ على الأقل في الوقت الحالي، من المرجح أن تمنع الحواجز العملية، والقضائية تطبيق جريمة العدوان في سياق العدوان السيبراني ومن ثم، ينبغي للمجموعات الدولية اتباع عدة أساليب أخرى في وقت واحد من أجل تعزيز الفضاء السيبراني السلمي، وان مُعالجة الآثار المترتبة على التهديدات السيبرانية العابرة للحدود الوطنية فضلا عن الأشكال الهجينة الأخرى من الحرب من منظور القانون الجنائي الدولي ربما تتطلب المزيد من التعديل لنظام روما الأساس.

الخاتمة

توصلنا في نهاية بحثنا الموسوم (الثقل النسبي للهجمات السيبرانية واختصاص المحكمة الجنائية الدولية) الى عدد من الاستنتاجات والمقترحات.

اولا: الاستنتاجات

١. ان الهجمات السيبرانية تطرح تحديات ذات صعوبة امام المجتمع الدولي بسبب ثلاثة عوامل رئيسة، أولا، عدم وجود حدود قضائية إقليمية في الفضاء السيبراني، ثانيا، عدم وجود قوانين موحدة بشأن هذه الهجمات في انحاء العالم جميعه، ثالثا، التطور السريع والمستمر لهذه الهجمات.
٢. تمثل العمليات الهجومية في الفضاء الإلكتروني تحديات فريدة للنظام القانوني الدولي، وهي التحديات التي يواجهها المجتمع الدولي، إذ تم جمع معظم هذه الجهود في دليل تالين وهي دراسات أكاديمية غير ملزمة، على الرغم من كونها موثوقة ومع ذلك، فهي علامة على رغبة الدول في تنظيم الفضاء الإلكتروني. وان الغرض من التأكيد على شرط "الثقل النسبي"، يتجسد في حصر الجرائم الدولية عند أخطر انتهاكات القانون الدولي، إذ نؤكد ان المحكمة الجنائية الدولية ليست معنية بالجرائم، الّا إذا كان لها ثقل نسبي اكبر، ويقصد بذلك تركيز المحكمة على القضايا الأكثر خطورة، ومن ذلك ان يكون الهجوم واسع النطاق، وطويل الأمد، وشديد الأثر وبخلافه تستبعد الحالات والقضايا التي لا تتمتع بهذه الصفات من قائمة التحقيق الدولي الذي تقوم به المحكمة.
٣. أن النقاش داخل القانون الدولي الجنائي حول تصنيف الهجمات السيبرانية كجرائم أساسية لا يزال مستمراً، ولم يسفر عن إجابات محددة حتى الآن، كما إن تصنيف الهجمات السيبرانية كجرائم عدوان أمر بالغ الأهمية على نحو خاص، واعتمادًا على النهج الذي يتبعونه لا يزال لدى الخبراء القانونيين آراء مختلفة حول هذا الموضوع. وعلى وفق جانب من الفقه الدولي يرون بأنّ على الأقل في الوقت الحالي، من المرجح أن تمنع الحواجز العملية، والقضائية تطبيق جريمة العدوان في سياق العدوان السيبراني ومن ثم، ينبغي للمجموعات الدولية اتباع عدة أساليب أخرى في وقت واحد من أجل تعزيز الفضاء السيبراني السلمي، وان مُعالجة الآثار المترتبة على التهديدات السيبرانية العابرة للحدود الوطنية فضلا عن الأشكال الهجينة الأخرى من الحرب من منظور القانون الجنائي الدولي ربما تتطلب المزيد من التعديل لنظام روما الأساس.

ثانيا: المقترحات

١. إنّ تطبيق القانون الدولي الجنائي على الهجمات السيبرانية، وملاحقة المتهمين قضائيا على الساحة الدولية يطرح عدة تحديات عملية، مثل قضايا السيادة الوطنية، والتعاون المتعدد الجنسيات بين الدول لمكافحة الهجمات السيبرانية، والافتقار الى آليات التشريع والتنفيذ، إذ تطرح الهجمات السيبرانية تحديات فريدة امام مسؤولي إنفاذ القانون بسبب ثلاثة عوامل رئيسة، أولا، عدم وجود حدود قضائية إقليمية في الفضاء المعلوماتي، ثانيا: عدم وجود قوانين موحدة بشأن هذه الهجمات في انحاء العالم جميعه، ثالثا، التطور السريع والمستمر لهذه الهجمات، ومن ثم سيستمر مجرمو الانترنيت في التفوق على جهود إنفاذ القانون اذا لم تعالج الدول كلها هذه العوامل المترابطة.
ومن ثم فأنّ الطريقة الواعدة لمنع الجرائم السيبرانية، ومحاكمتها تقترن باستعمال الولاية القضائية العالمية، والمعاهدات المتعددة الجنسيات، والذهاب بخطوة اخرى تتمثل في إسناد الولاية القضائية على قانون عقوبات دولي بشأن الجرائم السيبرانية إلى هيأة قضائية دولية.
٢. نقترح إسناد الولاية القضائية على الجرائم السيبرانية إلى محكمة دولية على غرار المحكمة الجنائية الدولية، إذ يستطيع المجتمع الدولي أن يضمن أن سلطة صياغة التعاريف والمعايير ستقع في يد كيان واحد يمكنه التكيف جنبا إلى جنب مع مجال الجريمة السيبرانية الدائم التطور.
٣. نقترح صياغة قانون عقوبات دولي للهجمات السيبرانية، إذ تؤدي عملية تطوير مثل هذا القانون الانموذجي إلى حلول أفضل للمشكلات القضائية في التشريعات المتعلقة بالجرائم السيبرانية، ومن شأن قانون عقوبات مفصل، ومحدد للجرائم السيبرانية أن يخفف أيضا من الكثير من التناقضات التعريفية الموجودة في الانظمة القانونية حاليا.
٤. نقترح تعديل نص المادة (١٣) من قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩ المعدل، والتي تنص على انه (في غير الاحوال المنصوص عليها في المواد ٩ و١٠ و١١ تسري احكام هذا القانون على كل من وجد في العراق بعد ان ارتكب في الخارج بوصفه فاعل او شريكا جريمة من الجرائم التالية: تخريب او تعطيل وسائل المخابرات والمواصلات الدولية والاتجار بالنساء او بالصغار او بالرقيق او بالمخدرات).

واضافة جرائم قد أُستجدت في الوقت الحالي مثل الهجمات السيبرانية، والجرائم الإرهابية، إذ تتميز هذه الجرائم بثقل نسبي عال تهدد المجتمع الوطني والدولي معا.

لذا نقترح ان تكون المادة على النحو الآتي: (في غير الاحوال المنصوص عليها في المواد ٩ و١٠ و١١ تسري احكام هذا القانون على كل من وجد في العراق بعد ان ارتكب في الخارج بوصفه فاعلا او شريكا جريمة من الجرائم التالية: تخريب او تعطيل وسائل المخابرات والمواصلات الدولية والاتجار بالنساء او بالصغار او بالرقيق او بالمخدرات، او الهجمات السيبرانية او الجرائم الإرهابية).

المراجع والمصادر

المراجع العربية

١. إرشادات الاسكو للتشريعات السيبرانية، مشروع تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية، بيروت، ٢٠١٢، ص١١٧ وص١١٨، متاح على الموقع الالكتروني، https://digitallibrary.un.org/record/1292295?ln=ar .

٢. ايمن عبد الحفيظ، حدود مشروعية دور أجهزة الشرطة في مواجهة الجرائم المعلوماتية، مجلة مركز بحوث الشرطة بأكاديمية مبارك، العدد ٢٥، يناير ٢٠٠٤.

٣. خالد ظاهر عبد الله جابر السهيل المطيري، مواجهة الجرائم المعلوماتية في ضوء التشريعات الجنائية المعاصرة والاتفاقيات الدولية، بحث منشور على الأنترنيت، ٢٠٢٠.

٤. د. احمد عبيس الفتلاوي وقاسم محمد مهدي الغزي، الدليل في فهم جريمة العدوان السيبرانية (دراسة في اطار مواجهة قانونية وسياسية فاعلة)، منشورات زين الحقوقية، لبنان، ط١، ٢٠٢٤.

٥. د. احمد عبيس الفتلاوي، الهجمات السيبرانية (دراسة قانونية تحليلية بشان تحديات تنظيمها المعاصر)، منشورات زين الحقوقية، بيروت – لبنان، ط١، ٢٠١٨.

٦. د. احمد عبيس الفتلاوي، الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر، بحث منشور، مجلة المحقق الحلي للعلوم القانونية والسياسية، جامعة بابل، العدد الرابع، السنة الثأمنة، ٢٠١٦.

٧. د. احمد عبيس نعمة الفتلاوي وثائر ناظم عبد الطرفي، وسائل الاثبات في اطار التحقيق الجنائي الدولي (دراسة قانونية معززة باجتهادات للمحاكم الجنائية الدولية) مكتبة زين الحقوقية والأدبية، بيروت، لبنان، ٢٠٢٢.

٨. زهراء عماد محمد كلنتر، المسؤولية الدولية الناشئة عن الهجمات السيبرانية، رسالة ماجستير، كلية القانون، جامعة الكوفة، ٢٠١٦.

٩. عباس بدران، الحروب الالكترونية (الاشتباك في عالم متغير)، مركز دراسات الحكومة الالكترونية، بيروت، ٢٠١٠.

١٠. كريم طالب حمادي الشجيري، الثقل النسبي للسلوك المحظور (دراسة في تحديد الجرائم الأكثر خطورة على الصعيدين الوطني والدولي)، رسالة ماجستير، مقدمة الى معهد العلمين للدراسات العليا، قسم القانون، ٢٠٢٣.

١١. محمد فخر الدين، حدود المجال الخامس – ما هي الحروب السيبرانية، مؤتمر حروب في الفضاء السيبراني، ٢٠١٥، بحث متاح على الموقع الالكتروني، https://seconf.wordpress.com/2015/05/15.

١٢. نور امير الموصلي، الهجمات السيبرانية في ضوء القانون الدولي الانساني، رسالة ماجستير، الجامعة الافتراضية السورية، ٢٠٢١.

Bibliography

1. Abhimanyu George Jain. Rationalising International Law Rules on Self-Defence: The Pin-Prick Doctrine, Chicago-Kent Journal of International and Comparative Law, Vol. XII, 2014.
2. Ansam Qasim Hachim. CRITICAL RESEARCH STUDY ON PREVENTING CYBER CRIMES THROUGH EFFECTIVE CYBER LAW CONCEPTS AND POLICIES FROM GLOBAL PERSPECTIVES; Research published in English, Iraqi University Journal, Issue 40/1, no publication year.
3. Cyber Warfare, 2015, available at: http://www.rand.org/topics/cyberwarfare.htm.
4. Wiener Norbert. Cybernetics or Control and Communication in The Animal and The Machine, M.I.T, Press, Second Edition, Cambridge, Massachusetts, 1948, Available At: https://cutt.ly/akhwlob.
5. Gianpiero Greco. CYBER-ATTACKS AS AGGRESSION CRIMES IN CYBERSPACE IN THE CONTEXT OF INTERNATIONAL CRIMINAL LAW, European Journal of Political Science Studies, Vol. 4, Issue. 1, 2020.
6. Janne Valo. Cyber Attacks and the Use of Force in International Law, Master's Thesis University of Helsinki, Faculty of Law, 2014.
7. Kocibelli, A, Aggression From Cyber-Attacks to ISIS: Why International Law Struggles to Adapt, Michigan Journal of InternationalLaw,2017.
8. Report of the Independent International Fact-Finding Commission on Myan-mar, UN Doc. A/HRC/39/64, 24 August 2018.
9. Kosmas Pipyros, Christos Thraska lip Mitro, Dimitris Gritzalis, Theodoros. A new strategy for improving her stacks evaluation in the context of Tallinn Manual, https://www.infosec.aueb.gr/Publications/COSE%20SI%20Tallinn%20Website.pdf
10. Laszlo Kovacs. cyper security policy and strategy in the European union and NATO, Revista Academiei Fortelor Terestre, Vol. 1. No. 89, 2018.

11. Letter dated 6 September 2012 from the Charge d'affaires a.i. of the Permanent Mission of Azerbaijan to the United Nations addressed to the Secretary-General, 7 September 2012, UN Doc. A/66/897–S/2012/687.
12. MARCO ROSCINI. GRAVITY IN THE STATUTE OF THE INTERNATIONAL CRIMINAL COURT AND CYBER CONDUCT THAT CON- STITUTES, INSTIGATES OR FACILITATES INTERNA- TIONAL CRIM, Criminal Law Forum, 2019.
13. Martin C. Libicki. Cyber deterrence and Cyber war Project Air Force, prepared for United States Air Force, 2009.
14. Miller, K. L. The Kampala Compromise and Cyberattacks: Can There Be an International Crime of Cyber-Aggression?, Southern California Interdisciplinary Law Journal, 23,2014.
15. Olivier KEMPF, Introduction à la Cyberstratégie, Paris, Economica, 2012.
16. The International Télécommunication Union, ITU Toolkit for Cybercrime Législation, Geneva, 2010.
17. Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue & Julia Spiegel. The law of Cyber-Attack, California law review, 2012.
18. Schmitt Michael (gen ed). Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, New York, First Published, 2013, Available At: https://cutt.ly/tkofrbK
19. Schmitt, M.N. Computer Network Attack and the Use of Force in International Law through on a Normative, The Colombia Journal of Transitional Law, 1999, Vol.27, No.885-937.
20. Tallinn Manual on the International Law Applicable to Cyber Warfare, Group of Experts and the Invitation of the NATO cooperative Cyber Defense Center of Excellence, Cambridge university Press, 2013.