المسؤولية الجنائية الدولية الفردية عن التجسس الرقمي[١]

م. د. زينب رياض جبر
zainb.riyad@hilla-unc.edu.iq
كلية الحلة الجامعة
م. د. حيدر إبراهيم هريس
haider.ibraheam@hiuc.edu.iq
كلية الحكمة الجامعة

Individual International Criminal Responsibility for Digital Espionage

Dr. Zainab Riad Jabr
Hilla University College
Dr. Haider Ibrahim Haris
University College of Wisdom

الملخص

أن ما حدث من حروب وأرتكاب الانسان الأنتهاكات أصبح يهدد السلم والأمن الدوليين وقد صاحب هذا التطور أتجاه جديد يرى بأن الانسان هو محور التشريعات القانونية كما أن مواثيق المحاكم العسكرية ومنظمة الامم المتحدة ومشروع الجرائم ضد سلم البشرية وأمنها أكدت على المسؤولية الجنائية للأشخاص الطبيعيين ، وفيما يتعلق بالمسؤولية الدولية الجنائية الفردية عن التجسس الرقمي فانه لا توجد قواعد واضحة في هذا الشأن وعلى مستوى الجريمة المعلوماتية بصورة عامة إذ لايزال مجال المسؤولية الجنائية الدولية الفردية عن الجرائم المعلوماتية فقير جدا وما يوجد من مسؤولية عن هذه الجريمة هو فقط على مستوى القضاء الوطني ،ألا أن جانب من الفقه يرى بأنه بالإمكان التوسع في مفهوم ميثاق روما ليشمل هذه الجرائم خاصة إذ كانت ذات طابع حركي مثلًا أن ينتج عن التجسس الرقمي سرقة كلمات سرية أو رموز لأطلاق صواريخ أو تدمير محطة طاقة أو ما شابه من الاعيان المشمولة بالحماية .

فمن حيث النطاق الشخصي يمكن تكييف الجرائم التي تدخل في اختصاص المحكمة وبالذات جريمة الحرب وجريمة العدوان والتي يمكن أن تلائم مع طبيعية التجسس الرقمي ،وعليه فأن الفقرة ٤ من النقطة ٢-أ من المادة ٨ من الميثاق التي اشارت الى جريمة الحرب يمكن تكييفه على التجسس الرقمي حيث أشارت إلى "الحاق تدمير واسع النطاق بالممتلكات والاستيلاء عليها دون أن تكون هناك ضرورة عسكرية تبرر ذلك وبالمخالفة للقانون وبطريقة عابثة " أذ من الممكن أن يسبب التجسس الرقمي إلحاق ضرر كبير بالممتلكات والسيطرة عليها من خلال أختراق النظام المعلوماتي الذي يدير هذه الممتلكات والتي من الممكن أن تكون ممتلكات أعيان مدنية أما بالنسبة الى جريمة العدوان نص المادة (٨) مكرر إلى أن العدوان هو تهديد الاستقلال السياسي للدولة أو سلامتها الاقليمية ويشكل التجسس الرقمي وخاصة ما يترتب عليه من أثار وأضرار تهديدا واضحا لسلامته الدولية الاقليمية وامنها السياسي وخاصة أذا نجم عنها عمليات قتل مستهدف ـــأو أضرار بمصالح الدول أما من حيث النطاق الشخص للمسؤولية الجنائية الدوليَّة عن التجسس الرقمي ومن يتحمل المسؤولية الجنائية الدولية ضمن نطاق النظام الأساس للمحكمة الجنائية الدولية عن هذه الجريمة ،حيث حددت الميثاق عدداً من المعايير التي على أساسها يتم تحديد المسؤولية الدولية اما بالنسبة للتجسس الرقمي فان النطاق الشخصي يتحدد بالقائد العسكري الذي يأمر بالتجسس وكذلك المقاتل الذي يقوم بالمهمة فضلا عن المبرمج الذي يطلق البرنامج التجسسي .

الكلمات المفتاحية: التجسس الرقمي-المسؤولية الدولية- الفرد-المحكمة الجنائية –جريمة العدوان- جريمة الحرب.

Abstract

what happened in wars and human violations has become a threat to international peace and security. This development has been accompanied by a new trend that sees the human being at the center of legal legislation, and the charters of military courts and the United Nations and the draft crimes against human peace and security emphasized the criminal responsibility of natural persons. With regard to the individual international criminal responsibility for digital espionage, there are no clear rules in this regard and at the level of information crime in general, as the field of individual international criminal responsibility for information crimes is still very poor, and the responsibility for this crime is only at the level of the national judiciary, but that A part of the jurisprudence believes that it is possible to expand the concept of the Rome Statute to include these crimes, especially if they were of a kinetic nature, for example, that digital espionage resulted in the theft of secret passwords or codes for launching missiles or destroying a power station or the like of protected objects .In terms of the personal scope, the crimes that fall within

[١] مستل من اطروحة الدكتوراه

the jurisdiction of the Court, particularly the war crime and the crime of aggression, can be adapted to the nature of digital espionage. Therefore, paragraph 4 of point 2-a of Article 8 of the Charter, which referred to the war crime, can be adapted to digital espionage. Where she pointed out" ,the widespread destruction and seizure of property without a military necessity justifying this, and in violation of the law and in a frivolous manner ,"as digital espionage can cause great damage to property and control it by penetrating the information system that manages these properties, which could potentially Be property of civilian objects.

As for the crime of aggression, the text of Article (8) bis states that aggression is a threat to the political independence of the state or its territorial integrity, and digital espionage, especially the consequences and damages that it entails, constitutes a clear threat to its international, regional and political security, especially if it results in targeted killings - or damage to the interests of states. As for the personal scope of the international criminal responsibility for digital espionage and who bears the international criminal responsibility within the scope of the statute of the International Criminal Court for this crime, where the charter specified a number of criteria on the basis of which international responsibility is determined. As for digital espionage, the personal scope is determined by the military commander. The one who orders the spying, the fighter who performs the mission, as well as the programmer who launches the spyware.

Keywords: digital espionage - international responsibility - the individual - the criminal court - the crime of aggression - war crime.

المقدمة

يعد الفرد عضواً فعالاً في المجتمع الدولي و يحظى بالكثير من الحماية بموجب حقوق الأنسان وكذلك العديد من الأتفاقيات التي تهدف إلى حماية الفرد وفي مقابل هذه الحماية لابد من أقرار المسؤولية الجنائية عن الجرائم المرتكبة من خلاله ، وعلى الرغم من عدم وضوح المسؤولية الجنائية الفردية وتنازع الآراء بخصوصها بين عدة اتجاهات منها ما رفضت المسؤولية وعدت الدولة هي المسؤولة و قررت أن الفرد هو المسؤول ومنهم من جمع المسؤولية الجنائية في كل ،فيما يتعلق بالمسؤولية الدولية الجنائية الفردية عن التجسس الرقمي فانه لا توجد قواعد واضحة في هذا الشأن وعلى مستوى الجريمة المعلوماتية بصورة عامة إذ لايزال مجال المسؤولية الجنائية الدولية الفردية عن الجرائم المعلوماتية فقير جدا وما يوجد من مسؤولية عن هذه الجريمة هو فقط على مستوى القضاء الوطني لذا في محاولة لتكييف القواعد العامة الواردة في ميثاق روما للتوصل الى بعض الحلول فيما يتعلق بتحقيق المسؤولية الجنائية عن التجسس الرقمي ، وهذا ما سنحاول بيانه في هذا المبحث حيث سنقسم هذه البحث إلى مبحثين :

المبحث الأول عن تكييف التجسس الرقمي في ضوء الأختصاص النوعي للمحكمة الدولية الجنائي على التجسس الرقمي والمبحث الثاني سيكون على النطاق الشخص لهذه المسؤولية الدولية الجنائية والأثار المترتبة عليها مع ذكر بعض التطبيقات القضائية.

ثانيا /اهمية البحث

تبدو اهمية البحث من خلال

١- تسليط الضوء على موضوع التجسس الرقمي بسبب حداثته لكونه احدى القضايا الرئيسية التي تواجه القانون الدولي في تطبيقه قواعده عليها ، فضلا عن التعبات القانونية والسياسية والانسانية التي يشكلها اللجوء الى التجسس الرقمي سواء وقت السلم او وقت النزاع المسلح

٢- ايجاد الاطار القانوني المناسب لها سواء في القانون الدولي او القانون الدولي الانساني ،من خلال توضيح القواعد التي تنطبق عليه سواء من حيث التنظيم والمسؤولية .

ثالثا/ الدرسات السابقة : توجد بعض الدراسات السابقة حول موضوع المسؤولية الدولية ولكن لم يتم الحديث مسبقا عن المسؤولية عن التجسس الرقمي سواء كانت مسؤولية دول او افراد أذ أن ما تم تناوله في البحث هو دراسة تحليلية لنصوص النظام الاساسي للمحكمة الجنائية الدولية لتطبيقه على جريمة التجسس الرقمي، ولكن توجد دراسات تتحدث عن المسؤولية الدولية بصورة عامة والتجسس الرقمي او المعلوماتي كما يسميه البعض ومنها :

١-جريمة التجسس المعلوماتي :رسالة ماجستير مقدمة الى معهد العلمين عام ٢٠١٩ ولكن تتناول الجريمة من زاوية القانون الداخلي وليس القانون الدولي العام .

٢-مشروعية التجسس عبر الاقمار الاصطناعية في القانون الدولي :بحث منشور في مجلة جامعة الانبار عام ٢٠١٩ والذي يتحدث عن التجسس الالكتروني الذي يتم عبر الاقمار الصناعية فقط .

رابعا /مشكلة البحث

يعد التجسس الرقمي من اهم المشاكل الدولية واكثرها اثارة للاهتمام ،حيث ان فهم موضوع التجسس الرقمي مهم لفهم كيف تشكل التكنلوجيا العالم اليوم ،وتؤثر عليه ولعل السبب في عدم فهم التجسس الرقمي انه يحدث في الخفاء وراء الكواليس مما يعني ان هناك نقص في المعرفة فيما يتعلق به حتى ان بعض الدول تواجه مشكلة في تحديد ما يعد تجسسا رقميا ماهي اهم الاسس القانونية التي يمكن ان تجرم فعل التجسس الرقمي وبالتالي تحقيق المسؤولية الدولية ؟في ظل عدم وجود تطبيق فعلي قضائي امام محكمة دولية بخصوص الهجمات الالكترونية عامة والتجسس الرقمي بصورة خاصة كيف يمكن ان نؤسس قواعد للمسؤولية الدولية للدول والمسؤولية الجنائية للأفراد ؟

خامسا /هيكلية البحث

ولما تقدم ارتأينا دراسة الموضوع وفقاً لخطة منهجية تقوم على تقسيم الدراسة هذه إلى مبحثين :

المبحث الأول عن تكييف التجسس الرقمي في ضوء الأختصاص النوعي للمحكمة الدولية الجنائي على التجسس الرقمي والمبحث الثاني سيكون على النطاق الشخص لهذه المسؤولية الدولية الجنائية والأثار المترتبة عليها مع ذكر بعض التطبيقات القضائية

المبحث الأول

تكييف التجسس الرقمي في ضوء الاختصاص النوعي للمحكمة الجنائية الدولية

أشار ميثاق روما إلى المسؤولية الجنائية الفردية في المادة ٢٥ حيث نص على "١- يكون للمحكمة اختصاص على الأشخاص الطبيعيين عملاً بهذا النظام الأساس ٢-الشخص الذي يرتكب جريمة تدخل في أختصاص المحكمة يكون مسؤولاً عنها بصفته الفردية وعرضة للعقاب وفقا لهذا النظام الأساس " وبناءً على هذا النص فأن المحكمة الجنائية الدولية ينعقد لها الأختصاص على الأشخاص الطبيعيين .

وفي محاولة تكييف فعل التجسس الرقمي وفق النظام الأساس للمحكمة الجنائية الدولية لأبد من إدراج التجسس الرقمي تحت طائلة الأفعال التي تدخل في أختصاص المحكمة الجنائية الدولية، فيبرز لدينا عدة تساؤلوهو وماهي الجرائم التي تدخل في اختصاص المحكمة الجنائية الدولية والتي يمكن ان يندرج التجسس الرقمي تحت نطاقها ؟ للإجابة عن هذين السؤال قسمنا هذا المبحث الى مطلبين المطلب الأول عن تكييف التجسس الرقمي في ضوء جرائم الحرب والمطلب الثاني تكييف التجسس الرقمي في ضوء جريمة العدوان.

المطلب الأول

تكييف التجسس الرقمي في ضوء أحكام جرائم الحرب

جرائم الحرب "هي الأفعال التي تشكل خروقات جسيمة لقوانين وأعراف الحرب بوجه عام سواء بحسب المفهوم التقليدي للحرب الذي يجسد قانون الحرب أم بحسب مفهومها المعاصر الذي يعبر عنه قانون النزاعات المسلحة أو التي يعبر عنها القانون الدولي الانساني [١] كما عرفت اتفاقيات جنيف الاربعة لعام ١٩٤٩[٢] جرائم الحرب بأنها "الأنتهاكات الجسيمة لقواعد القانون الدولي الأنساني التي ترتكب ضد أشخاص أو ممتلكات تحميهم الأتفاقيات الدولية " وتأسيسا على ماسبق من تعريف هل يمكن ان ينطبق مفهوم جريمة الحرب على التجسس الرقمي. للإجابة عن ذلك نوضح بان جريمة الحرب التي أشار إليها ميثاق المحكمة الجنائية الدولية في المادة ٨ وقسمها إلى قسمين فتناول في الفقرة ٢"-أ الأفعال التي تعتبر من قبيل الانتهاكات الجسمية لأتفاقيات جنيف لعام ١٩٤٩ ثم تناولت المادة ٨ في الفقرة ٢-ب الأفعال التي تعتبر من قبيل الأنتهاكات الخطيرة للقوانين والأعراف الدولية الساري " وعليه وفق هذه المادة سوف نستبعد من دراستنا المصطلحات التي تخرج من مفهوم تكيف التجسس الرقمي وبالتالي سنذكر فقط ما يتلاءم أو ما يمكن تكييفه على التجسس الرقمي ، وبالتالي فأن الفقرة ٤ من النقطة ٢-أ من الميثاق يمكن تكييفه على التجسس الرقمي حيث أشارت إلى "الحاق تدمير واسع النطاق بالممتلكات والاستيلاء عليها دون ان تكون هناك ضرورة عسكرية تبرر ذلك وبالمخالفة للقانون وبطريقة عابثة " أذ من الممكن أن يسبب التجسس الرقمي إلحاق ضرر كبير بالممتلكات والسيطرة عليها من خلال أختراق النظام المعلوماتي الذي يدير هذه الممتلكات والتي من الممكن أن تكون ممتلكات أعيان مدنية وبالتالي لا يجوز أن تكون محلا للهجوم من خلال حظر أرتكاب أي من الأعمال العدائية الموجهة ضدها أو استخدامها في دعم المجهود الحربي أو في هجمات الرد[٣].

أو قد تكون منشئات تحتوي على قوى خطرة والتي لها تأثير كبير في حال تدميرها مثل محطات الطاقة النووية أو السدود أو مرافق شرب المياه، وتلك المنشآت وإن كانت ليست ذات طبيعة مدنية ولا عسكرية على صفة الإطلاق إلا أن تدميرها أو المساس بها سيؤثر على السكان المدنيين بصورة خطيرة، وقد تؤدي لكارثة كبيرة[٤]، فجاءت المادة (٤٩) من البروتوكول الإضافي الأول لعام ١٩٧٧ لتوفير الحماية للمنشآت والأهداف التي تحتوي على قوة خطرة , من خلال حظر شن الهجمات أو تدمير السدود أو الجسور أو القناطر أو المحطات النووية المستعملة في توليد الطاقة الكهربائية , وحُرمت توجيه أعمال القمع والإنتقام ضد هذه المنشآت , ودعت الأطراف المتنازعة إلى تمييز هذه المنشآت بعلامات خاصة يسهل من خلالها التعرف عليها، كذلك جاءت أتفاقية لاهاي لحماية الممتلكات الثقافية لعام ١٩٥٤ في المواد (١و٢)ايضا للإشارة الى الحماية الممتلكات المدنية والتي تعد ممتلكات ثقافية توفر لها الحماية العامة والخاصة أثناء النزاعات المسلحة وعليه فأن الأضرار التي تصيب هذه الأعيان جراء التجسس الرقمي يمكن أن تدخل ضمن جرائم الحرب و حسب نص المادة (٨ الفقره ٤النقطة ٢أ) من نظام روما الأساسي للمحكمة الجنائية الدولية الذي ادرج ضمن مفهوم جرائم الحرب ، الانتهاكات الجسيمة لاتفاقيات جنيف الأربع لعام ١٩٤٩، بمعنى أن ارتكاب أي فعل من الأفعال ضد الأشخاص أو الممتلكات موضوع حماية بموجب اتفاقيات جنيف لعام ١٩٤٩ يشكل جريمة حرب ، ومن بين هذه الأفعال المجرمة إلحاق تدمير واسع النطاق بالممتلكات والاستيلاء عليها دون أن تكون هناك ضرورة عسكرية تبرر ذلك بالمخالفة للقانون وبطريقة عابثة.[٥]

وعليه وفقاً إلى ما سبق فأن توجيه التجسس الرقمي أثناء النزاعات المسلحة بأستهداف المنشآت المدنية أو التي تحتوي على قوى خطيرة يمكن أن يعد جريمة حرب وهذا أيضا ما يشير اليه دليل تالين في القاعدة (٣٧) من حظر الهجمات السيبرانية ضد الأعيان المدنية إلا إذا

---

[١] عبد الله سليمان سليمان ،المقدمات الاساسية في القانون الدولي الجنائي ،ديوان المطبوعات الجامعية ،الجزائر ،١٩٩٢،ص٢٦٠.

[٢] اتفاقيات جنيف الاربعة لعام ١٩٤٩ هي :المادة ٥٠ من اتفاقية جنيف الاولى لتحسين الجرحى والمرضى من القوات المسلحة بالميدان ،والمادة ٥١ من اتفاقية جنيف الثانية لتحسين الجرحى والمرضى وغرقى القوات = المسلحة في البحار ،والمادة ١٣٠ بشأن معاملة الاسرى ،والمادة ١٤٧ من اتفاقية جنيف الرابعة بشأن حماية الأشخاص المدنيين في وقت الاحتلال .

[٣] المادة (٥٣) من البروتكول الإضافي الأول لسنة ١٩٧٧- لإتفاقيات جينيف الأربعة عام ١٩٤٩

[٤] د. يوسف إبراهيم النقبي، التمييز بين الهدف العسكري والهدف المدني وحماية الأهداف المدنية والأماكن التي تحتوي على خطورة خاصة وفقاً للقانون الدولي الإنساني، القانون الدولي الإنساني، اللجنة الدولية للصليب الأحمر، القاهرة، ٢٠٠٦، ص ٤١٢ .

[٥] د. يوسف إبراهيم النقبي، التمييز بين الهدف العسكري والهدف المدني وحماية الأهداف المدنية والأماكن التي تحتوي على خطورة خاصة وفقاً للقانون الدولي الإنساني، القانون الدولي الإنساني، اللجنة الدولية للصليب الأحمر، القاهرة، ٢٠٠٦ ، ص٤١٣.

كانت الحواسيب أو شبكات الحاسوب والبنية التحتية السيبرانية أهدافاً عسكرية فيجوز أن تكون هدفا للهجمات[١]، كما أن الدليل عرف الأعيان المدنية والأعيان العسكرية ، بأن الأعيان المدنية هي كافة الأعيان التي ليست أهدافا عسكرية والأهداف العسكرية هي تلك الأعيان التي بحكم طبيعتها ..... تشكل ميزة عسكرية أكيدة.[٢]

كما يمكن بالإمكان تكييف التجسس الرقمي وفق الفقرات ١و٢و٣ من النقطة (٢-ب) من المادة ٨ وذلك وفق الانتهاكات الخطيرة الأخرى للقوانين والأعراف السارية على النزاعات الدولية حيث نصت الفقرة ١ "تعمد توجيه الهجمات ضد السكان المدنيين بصفتهم هذه أو ضد افراد مدنين لا يشاركون مباشرة في الاعمال الحربية " وبالعودة إلى أتفاقيات جنيف لعام ١٩٤٩ نجد أن البروتكول الاضافي الاول لعام ١٩٧٧ والذي نص على "١-تمتع السكان المدنيين والاشخاص المدنيين بحماية عامة ضد الأخطار الناجمة عن العمليات العسكرية ويجب أضفاء فعالية على هذه الحماية مراعاة القواعد التالية دوماً بالإضافة إلى القواعد الدولية الأخرى القابلة للتطبيق ،٢-لا يجوز أن يكون السكان المدنيين بوصفهم هذا وكذلك الاشخاص المدنيين محلا للهجوم وتحظر أعمال العنف أو التهديد الرامية أساساً إلى بث الرعب بين السكان المدنيين ...." [٣]

كذلك جاء البروتوكول الإضافي الثاني لعام ١٩٧٧ ليعزز هذه القاعدة بنصه في م(١٣) على(١-يتمتع السكان المدنيون والأشخاص المدنيون بحماية عامة من الأخطار الناجمة عن العمليات العسكرية ويجب لإضفاء فاعلية على هذه الحماية مراعاة القواعد التالية دوما.٢- لا يجوز أن يكون السكان المدنيون بوصفهم هذا ولا الأشخاص المدنيون محلا للهجوم وتحظر أعمال العنف أو التهديد به الرامية أساسا إلى بث الذعر بين السكان المدنيين.٣- يتمتع الأشخاص المدنيون بالحماية التي يوفرها هذا الباب، ما لم يقوموا بدور مباشر في الأعمال العدائية وعلى مدى الوقت الذي يقومون خلاله بهذا الدور).

وتأسيساً على ماتم أستعراضه من نصوص في أتفاقيات جنيف وميثاق روما فأن توجيه التجسس الرقمي ضد السكان المدنيين من خلال أختراق حواسيبهم أو بريدهم الالكتروني وخاصة في حالة أن يُسبب هذه الاختراق في بث الرعب أو محاولة الوصول إلى أماكن تجمهم وبالتالي توجيه العمليات العدائية ضدهم أو حرمانهم الحقوق التي اشار اليها القانون الدولي الأنساني يمكن أن تدخل في جرائم الحرب بسب إنتهاك قوانين وأعراف الحرب السارية التي تستبعد السكان المدنيين من أن يكونوا محلاً للهجوم وعليه يمكن أن يكون التجسس الرقمي جريمة حرب في هذه الحالة .

أما بالنسبة الى الفقرة ٢ من الفقرة ب من المادة ٨ والتي تشير " تعمد توجيه هجمات ضد مواقع مدنية أي مواقع لا تشكل أهداف عسكريا " أيضا بالإمكان تطبيقه على التجسس الرقمي حيث إن التجسس الرقمي حسب دليل تالين لا يوجه إلى الأعيان المدنية وانما فقط إلى الأهداف العسكرية الألكترونية وبالتالي يمكن أن يشكل التجسس الرقمي جريمة حرب في هذه الحالة كذلك ،أما الفقرة ٣ من ب من المادة ٨ فقد نصت على " تعمد شن هجوم ضد موظفين مستخدمين أو منشأت أو مواد أو وحدات او مركبات مستخدمة في مهمة من مهام المساعدة الانسانية أو حفظ السلام عملا بميثاق الامم المتحدة ما داموا يستحقون الحماية التي توفرها للمدنيين أو للمواقع المدنية بموجب قانون المنازعات المسلحة " تُشير الفقره ٣ إلى الأشخاص الذين يتمتعون بالحماية وفق أتفاقيات جنيف لعام ١٩٤٩ حيث تمت الأشارة إلى تعريف أفراد الخدمات الطبية م(٨/ج) من البروتوكول الأضافي الأول لعام ١٩٧٧ بأنهم "أفراد الخدمات الطبية" هم الأشخاص الذين يخصصهم أحد أطراف النزاع إما للأغراض الطبية دون غيرها المذكورة في الفقرة (هـ) وإما لإدارة الوحدات الطبية، وإما لتشغيل أو إدارة وسائط النقل الطبي[٤] ولكي يتمتع أفراد الخدمات الانسانية والطبية التي أشار إليهم ميثاق روما وأتفاقيات جنيف بالحماية بموجبهما يجب عدم مشاركتهم بالعمليات العدائية عند مزاولتهم هذه المهام ،وعليه فأنهم يفقدون حقهم بالحماية ولكن هذا الفقدان موقت بالمشاركة بالعمليات العدائية وتعود الحماية لهم بمجرد أنتهاء مشاركتهم في العمل العدائي [٥] ،وعليه فأن التجسس الرقمي الذي يوجه إلى هؤلاء الأشخاص أثناء النزاعات المسلحة يعد بمثابة جريمة حرب .

تأسيساً على ما سبق قوله يمكن أن ينطوي التجسس الرقمي تحت طائلة جريمة الحرب في الحالات المحددة التي يكون فيها للتجسس الرقمي تأثير على مايأتي : الممتلكات والاعيان المدنية أو المنشأت التي تنطوي على قوى خطره من خلال إخترق النظام المعلوماتي الذي يدير هذه الممتلكات ويسبب اضراراً لا حصر لها ، وكذلك في حالة توجيه التجسس الرقمي الى أفراد الخدمات الطبيبة أو السكان المدنيين .

الفرع الثاني

تكييف التجسس الرقمي وفق أحكام جريمة العدوان

جريمة العدوان دخلت إلى حيز إختصاص المحكمة في ٢٠١٠ في مؤتمر كمبالا بأوغندا حيث حظر المؤتمر نحو ٤٦٠٠ ممثل عن الدول والمنظمات لمدة أسبوعين نتج عنه قراراً عدل به نظام روما الأساس لكي يدخل تعريف العدوان ضمن ميثاق روما [٦] ، و أشارت المادة ٨ مكرر من الميثاق إلى جريمة العدوان حيث تناولت ف ١ من المادة ٨ توضيح مفهوم العدوان حيث نصت على " لأغراض هذا النظام الأساس ،تعنى جريمة العدوان قيام شخص ما له وضع يمكنه فعلاً من التحكم في العمل السياسي أو العسكري للدولة أو من توجيه هذا العمل ،بتخطيط أو أعداد أو بدء أو تنفيذ فعل عدواني يشكل بحكم طبيعته أو خطورته ونطاقه أنتهاكاً واضحاً لميثاق للأمم المتحدة " كما

---

[1] Susan W. Brenner with Leo L. Clarke, Civilians in Cyberwarfare: Conscripts , Vanderbilt Journal of Transnational Law ,Vol. 43 .2010 ,p22

[٢] القاعدة ٣٨ من دليل تالين لعام ٢٠١٢ .

[٣] المادة ٥٠ من البروتكول الاضافي الاول لعام ١٩٧٧.

[٤] ١- أفراد الخدمات الطبية، عسكريين كانوا أو مدنيين، التابعين لأحد أطراف النزاع بمن فيهم من الأفراد المذكورين في الاتفاقيتين الأولى والثانية لعام ١٩٤٩، وأولئك المخصصين لأجهزة الدفاع المدني. ٢- أفراد الخدمات الطبية التابعين لجمعيات الصليب الأحمر الوطنية (الهلال الأحمر والأسد والشمس الأحمرين) وغيرها من جمعيات الإسعاف الوطنية الطوعية التي يعترف بها ويرخص لها أحد أطراف النزاع وفقا للأصول المرعية, ٣- أفراد الخدمات الطبية التابعين للوحدات الطبية أو وسائط النقل الطبي المشار إليها في الفقرة الثانية من المادة التاسعة من البروتكول الأضافي الأول لعام ١٩٧٧).

[٥] د.طيبة احمد ،الحماية الخاصة لموظفي الخدمات الطبية اثناء النزاعات المسلحة ،مجلة المحقق الحلي للعلوم القانونية والسياسية ، العدد الثاني ,السنة الثامنة ,٢٠١٦ ، ص٢٨٠

[6] David Scheffer, The Missing Pieces in Article 8 bis(Aggression) of the Rome Statute, Harvard International Law Journal / Vol. 58 Online Journal, S PRING 2017,P84

أوضحت الفقرة ٢ العمل العدواني حيث نصت" لأغراض الفقرة ١ يعني العمل العدواني أستعمال القوة المسلحة من قبل دولة ما ضد سيادة دولة اخرى أو سلامتها الأقليمية أو استقلالها السياسي أو بأي صورة اخرى تتنافى مع ميثاق منظمة الأمم المتحدة وتنطبق صفة العمل العدواني على أي عمل عدواني من الأعمال التالية سواء بإعلان الحرب أو بدونه وذلك طبقا لقرار الجمعية العامة للأمم المتحدة رقم ٣٣١٤ (د-٢٩)لعام ١٩٧٤".

من خلال تعريف جريمة العدوان في ميثاق روما نلاحظ أن التعريف في الفقرة ٢ كان أستناداً إلى قرار الجمعية العامة لعام ١٩٧٤ ألا أن الفرق بينهما أن قرار الجمعية العامة كان لإقرار المسؤولية الدولية للدولة في حين أشار ميثاق روما إلى تعريف الفعل العدواني لسلوك الدول وتعريف السلوك العدواني للأفراد .

فيما يتعلق بالتجسس الرقمي أو العدوان الرقمي بصورة عامة وما مدى امكانية تطبيق جريمة العدوان عليه ؟نجيب عن هذه التساؤل بعدد من الآراء التي طرحت في مؤتمر كمبالا ، إذ هناك أراء مختلفة للباحثين فيما يتعلق بتطبيق جريمة العدوان على الهجمات الالكترونية ألا أنها بصورة عامة تنقسم إلى أتجاهين أتجاه ينكر أمكانية تطبيق جريمة العدوان على الهجمات الألكترونية وبالتالي التجسس الرقمي بسبب عدة أعتبارات منها مشكلة الأسناد في الجرائم الألكترونية حيث يشير البعض أن الجرائم الألكترونية غالبا ما يتم أرتكابها من قبل هواة غرضها هو المكسب المالي وتحقيق الربح وكذلك قيام بعض التنظيمات بارتكاب هذه الهجمات بدون أمكانية نسبتها الى دولة معينة[١]

ومن الأسباب الأخرى كذلك وهو متعلق أيضا بالإسناد بالدرجة الأساس هو مشكلة القيادة التي أشار إليها النص من خلال عبارات" التحكم في العمل السياسي أو العسكري للدولة أو من توجيه هذا العمل" والتي أتفق على أنها تعني القيادة المسؤولة أو التنظيم والتخطيط لهذه الأعمال الألكترونية[٢] ومن الأعتبارات الأخرى التي نفت أمكانية تطبيق جريمة العدوان على الهجمات الألكترونية هو المادة ٢٢ والتي تعد الأساس للشرعية في المحكمة الجنائية الدولية والتي تعني التقيد بأختصاص المحكمة و التقيد بالجرائم الأربع دون غيرها.

أما الأتجاه الأخر فأنه يرى بضرورة تطبيق جريمة العدوان على الهجمات الالكترونية لعدة أسباب :

أولا :أنه كان يجب أن يتضمن تعريف العدوان الهجمات الالكترونية على أعتبار أنه حدث قريب وبالتالي كان يجب الأشارة إلى الهجمات الألكترونية دون تركها من غير تنظيم

ثانيا : أن جريمة العدوان كما تم تقنينها في المادة ٨ مكرر تضع ثلاثة متطلبات متميزة للمسؤولية وهي عمل عدواني ، يشكل بحكم طبيعته وخطورته وحجمه ، انتهاكًا واضحاً لميثاق الأمم المتحدة ، فضلاً عن ذلك ولدى صياغة وتفعيل جريمة العدوان لوحظ ما يلي: أن العدوان هو أخطر أشكال الاستخدام غير المشروع للقوة[٣] ، لذلك عند تعريف جريمة العدوان في نظام روما الأساس ، يجب أن ننظر أولاً إلى المعايير الدولية السائدة حول الحرب الإلكترونية ، وخاصة تلك التي أصدرتها الأمم المتحدة والأجهزة ذات الصلة وهذه المعايير القانونية نفسها متناثرة إلى حد ما ومستوردة إلى حد كبير عن طريق القياس من قانون الحرب التي تلزم الدول بعدم استخدام القوة ضد الدول الأخرى بموجب ميثاق الأمم المتحدة.[٤]

وبناء على ما سبق قدم القرار الذي يعرف العدوان عدة أمثلة على إستخدامات القوة ، منها : غزو أو هجوم من قبل القوات المسلحة لدولة ما على أراضي دولة أخرى ، أو أي احتلال عسكري ، مهما كان مؤقتًا ، ناتج عن هذا الغزو أو الهجوم ، أو أي ضم باستخدام القوة لإقليم دولة أخرى أو لجزء منه ؛ قصف القوات المسلحة لدولة ما أراضي دولة أخرى أو استخدام أي أسلحة من قبل دولة ضد أراضي دولة أخرى و إرسال مجموعات مسلحة أو جماعات أو أفراد غير نظاميين أو مرتزقة ، من قبل دولة أو بالنيابة عنها ، ممن يقومون بأعمال القوة المسلحة ضد دولة أخرى من الخطورة بحيث ترتقى إلى مستوى الأعمال المذكورة أعلاه ، أو المشاركة الجوهرية فيها الى الكثير من الامثلة التي أوضحها قرار الجمعية العامة عند تعريف العدوان. [٥]

لذلك يمكن أن نفترض بأن الهجوم الكترونيً الذي له النطاق نفسهُ والتأثيرات على الدولة مثل الأعمال المذكورة أعلاه ، سيشكل استخداماً للقوة وبالتالي جريمة عدوان في القانون الدولي مثل غزو أو هجوم مسلح على أراضي دولة ما يمكن أن يكون مماثل من الناحية الألكترونية حيث يمكن عن طريق البرامج غزو الفضاء الرقمي للدولة بالكامل وشلها عن الحركة وتوقف كل أجراءاتها الداخلية أو أرسال مجموعة من المرتزقة أو الافراد غير نظامين وحاليا لدينا الكثير من المتسللين والمخترقين الذي يمتهنون الهجمات الألكترونية وخاصة التجسس الرقمي ،وعلى هذا الأفتراض يمكن أن يشمل المصطلحات في جريمة عدوان فعل التجسس الرقمي

علاوة على ذلك أن نص المادة(٨) مكرر أشارت إلى أن العدوان هو تهديد الاستقلال السياسي للدولة أو سلامتها الاقليمية ويشكل التجسس الرقمي وخاصة ما يترتب عليه من أثار وأضرار ذكرناها مسبقا تهديدا واضحا لسلامته الدولية الاقليمية وامنها السياسي وخاصة أذا نجم عنها عمليات قتل مستهدف ـأو أضرار بمصالح الدول .

وفي سبب اخر لتمكن من تطبيق العدوان على الهجمات الالكترونية ومن ضمنها التجسس الرقمي، تنص تعديلات (كمبالا) في المادة ٨ مكرر على نطاق محدود من الأشخاص ليتم تحميلهم المسؤولية في حالة وقوع هجوم على النحو التالي :"شخص في وضع يسمح له فعليا بممارسة السيطرة على العمل السياسي أو العسكري لدولة ما أو لتوجيهه " على الرغم من أن هذا النطاق محدود للغاية في النص ، فإن إمكانية التنفيذ في السياق الإلكتروني تتجاوز بكثير الحرب التقليدية إذ عادة ما تحد الدول من قدرة المواطنين على الوصول إلى وسائل

---

(1) K EVIN L. M ILLER, THE KAMPALA COMPROMISE ANDCYBERATTACKS:CAN THERE BE AN INTERNATIONAL C RIME OF CYBER-AGGRESSION? , Southern California Interdisciplinary Law Journal ARTICLES 2014 , Vol. 23:217,P225 .

(2) K EVIN L. M ILLER,OP.CIT ,P 225.

(3) JONATHAN A. O PHARDT, CYBER WARFARE AND THE CRIME OFAGGRESSION: THE NEED FOR INDIVIDUALACCOUNTABILITY ON TOMORROW'SBATTLEFIELD, DUKE LAW & TECHNOLOGY REVIEW,2010,NO,3, P13.

(4) J ONATHAN A. O PHARDT, OP CIT ,P 14.

(5) David Scheffer,op.cit ,P84.

استخدام القوة على سبيل المثال تفرض العديد من الدول قيودًا على مراقبة الأسلحة و يتم تطبيق هذه القيود بشكل فعال على مستوى الدولة[١].

كما تشمل الهجمات العسكرية التقليدية عمومًا العديد من الأشخاص بمن فيهم المهاجمون أنفسهم وتدريبهم أو مدربيهم وموظفي الدعم والدعم اللوجستي لذلك من الصعب تخيل هجوم تقليدي يرتفع إلى المستوى الذي تضعه تعديلات (كمبالا) دون تدخل أو دعم من الدولة و على النقيض من ذلك يمكن أن يقوم شخص واحد فقط بتنفيذ الهجمات الإلكترونية بسهولة بإستخدام الأجهزة الالكترونية أو حتى الفايروسات لذلك فإن نطاق الأشخاص الذين يحتمل أن يكونوا مسؤولين عن أرتكاب هجمات إلكترونية أكبر بكثير من الحروب التقليدية[٢] لذا يمكن إستخدام جريمة العدوان في السياق السيبراني على قدم المساواة مع أي جريمة أخرى يمكن استخدامها فيها على الرغم من بعض الاختلافات المهمة في متطلبات التطبيق ، لذا قد ينطبق القانون الدولي عمومًا عن طريق القياس على مجال الإنترنت في الواقع ، أذ يقدم السياق السيبراني فرصة فريدة للمحكمة للتأثير على إجراءات العديد من الدول وتوسيع مجالها من المجال التقليدي وادخال الهجمات الالكترونية وبالتالي التجسس الرقمي ضمن اختصاصها.

المطلب الثاني

النطاق الشخصي للمسؤولية الجنائية الدوليَّة عن التجسس الرقمي

يتحدد النطاق الشخصي للمسؤولية الدولية عن التجسس الرقمي من حيث الأشخاص الذين يخضعون بموجبها لاختصاص المحكمة حيث حددت المحكمة معاييراً تطبق على المسؤولية الفردية الجنائية وكذلك تحديد الأثار التي تترتب على تطبيق المسؤولية الشخصية والتي سنوضحها في فروعين.

الفرع الاول

النطاق الشخص للمسؤولية الجنائية الدوليَّة عن التجسس الرقمي

المقصود بالنطاق الشخصي للمسؤولية من يتحمل المسؤولية الجنائية الدولية ضمن نطاق النظام الأساس للمحكمة الجنائية الدولية[٣] ،حيث حددت اللجنة عدداً من المعايير التي على أساسها يتم تحديد المسؤولية ومنها :

١-ان يكون شخصا حقيقيا غير إعتباري.[٤]

٢-ان يتجاوز سن مرتكب الجريمة الثامنة عشر.[٥]

٣-لا يستثنى شخص من المسؤولية بسبب صفته الرسمية.[٦]

يستنتج من المعايير التي وضعها نظام روما أن الشخص الطبيعي يكون محل للمسائلة سواء كان رئيساً أم مرؤوساً وأن الصفة التي يتمتع بها الشخص لا تغنيه من المسؤولية عن الجرائم التي يرتكبها وقد أكدت ذلك المادة الرابعة من مبادئ نورمبرغ "حقيقة أن يكون مرتكب الجريمة الدولية هو رئيس الدولة أو مسؤول الحكومة لا تعفيه من المسئولية بحكم القانون"[٧].

وكذلك أكد ذات المبدأ البروتوكول الاضافي الاول لعام ١٩٧٧ في المادة ٨٦ /٢ بالنص "لا يعفي قيام أي مرؤوس بانتهاك الإتفاقيات أو هذا الملحق رؤساءه من المسؤولية الجنائية أو التأديبية ....." .

وفي سياق ما تقدم ولتحديد المسؤولية الشخصية عن التجسس الرقمي لأبد من تحديد الأشخاص الذين يديرون هجمات التجسس الرقمي وتحديد مسؤولية كلا منهم ونقسمها إلى :-

١-مسؤولية مشغل برنامج التجسس الرقمي.

مشغل برنامج التجسس الرقمي هو الشخص الذي يقوم بأطلاق برنامج التجسس الرقمي أي هو من يقوم بعملية أختراق أمن الحواسيب و جمع البيانات سواء كانت بطريقة مباشرة عن طريق التغلغل المباشر في حواسيب أو شبكات الغير من خلال أختراقها بالبرامج أو بطريقة غير مباشرة من خلال شخص يقوم بتنصيب برامج التجسس بحواسيب الغير لتمكن من أختراق شبكاتهم .

وبناء على ماتقدم لابد من طرح التساؤل الأتي : هل يسأل الشخص الجالس خلف شاشة الحاسوب وقام بأطلاق برنامج التجسس الرقمي ؟ وهل يؤثر في إيقاع المسؤولية كون المشغل مدني وليس عسكري؟

للإجابة عن ذلك لابد من الأشارة إلى المادة ٢/٢٥ إذ نصت " الشخص الذي يرتكب جريمة تدخل في أختصاص المحكمة يكون مسؤول عنها بصفته الفردية وعرضة للعقاب وفقاً لهذا النظام الأساس" لذا أن النص هنا لم يحدد أذا كان الشخص مدنياً أو عسكرياً عند ارتكابه الجريمة الدولية ،وعليه فأن مسؤولية الفرد الجنائية تقوم سواء تصرف بصفته الشخصية أم لحساب شخص آخر من أشخاص القانون الدولي ،وفي ضوء التطورات التي حدثت في المجتمع الدولي فيما يتعلق بإستخدام التكنلوجيا لأغراض جرمية والتي أثارت الكثير من الأشكاليات بسبب أن أستخدام هذه التكنلوجيا وخاصة مثل التجسس الرقمي تؤدي إلى حدوث أثار وأضرار غير محدودة وخاصة بأن مجرد أطلاق البرنامج التجسسي يمكن أن يؤدي إلى سرقة المعلومات الألكترونية وأستخدامها لأغراض اخرى ،ولما كانت هذه البرامج خارج عن سيطرة الشخص بمجرد أطلاقها فبالتالي المسؤولية تكون مرتكزة تماما على البشر بصفة مبرمج أو مشغل لهذه البرامج ،أما لكون الشخص المشغل مدنياً أو عسكرياً فأنه لا يؤثر على نطاق المسؤولية وتحققها.

٢-مسؤولية القادة عن التجسس الرقمي.

---

(1) J ONATHAN A. O PHARDT, OP CIT ,P 15.

(2) K EVIN L. M ILLER,op .cit .p 225.

(٣) ماجد عمر عبادي ،جريمة العدوان قراءة تحليلية تعتمد النص والمفاوضات الدبلوماسية لمؤتمر كمبالا٢٠١٠،اطروحة دكتوراه،جامعة النجاح الوطنية ،٢٠١٨،ص١٤.

(٤) المادة ٢٥ ف ١ من النظام الاساسي لعام ٢٠٠٢.

(٥) المادة ٢٦ من النظام الاساسي لعام ٢٠٠٢.

(٦) المادة ٢٨ من النظام الاساسي لعام ٢٠٠٢.

(٧) محمد يوسف الصافي ،الاطار العام للقانون الدولي الجنائي في ضوء احكام النظام الاساسي للمحكمة الجنائية الدولية ،دار النهضة العربية ،القاهرة ،٢٠٠٢،ص٦٦.

المقصود بالقادة هنا مسؤولية القادة العسكرين والقادة الاداريين حيث أدرج هذا النص بتأثير من الوفود المشاركة في المؤتمر التحضيري لأنشاء المحكمة الجنائية الدولية وكذلك تماشيا مع أجتهادات المحكمة الدولية ليوغسلافيا وكل ذلك انعكس في المادة ٢٨ التي نصت في الفقرة الاولى منها على مسالة القادة العسكرين وفي الفقرة الثانية منها على مسألة القادة المدنيين أو الاداريين[١].

وعليه تقرر مسؤولية القادة العسكرين أو الذي يقوم محلهم بموجب الفقرة الاولى من المادة (٢٨) حيث نصت "١-يكون القائد العسكري أو الشخص القائم فعلاً بأعمال القائد العسكري مسؤولاً مسؤولية جنائية عن الجرائم التي تدخل في اختصاص المحكمة والمرتكبة من جانب قوات تخضع لأمرته وسيطرته الفعليتين أو تخضع لسلطته وسيطرته الفعليتين حسب الحالة نتيجة لعدم ممارسة القائد العسكري أو الشخص سيطرته على هذه القوات ممارسة سليمه أ- أذا كان القائد العسكري أو الشخص قد علم ويفترض أن يكون قد علم بسبب الظروف السائدة في ذلك الحين ،بأن القوات ترتكب أو تكون على وشك أرتكاب هذه الجرائم

ب- اذا لم يتخذ القائد العسكري او الشخص جميع التدابير اللازمة والمعقولة في حدود سلطته لمنع او قمع ارتكاب هذه الجرائم او لعرض المسالة على السلطات المختصة للتحقيق والمقاضاة"

وبذلك يكون القائد العسكري مسؤول مسؤولية مفترضة عما يرتكبه الاشخاص التابعين له والذين يعملون تحت امرته حتى وأن لم يُخطط أو يأمر بأرتكاب الجريمة التي تدخل في أختصاص المحكمة تأسيساً على مبدأ العلم المفترض بوقوع افعال جريمة ولم يتأخذ كذلك الاجراء لمنع وقوعها[٢] وعليه فان القائد العسكري يسأل عن التجسس الرقمي الذي من الممكن أن يرتكبهُ الأشخاص تحت امرته وسيطرته دون إمكانية الإحتجاج بعدم العلم , وذلك بسبب عدم اتخاذ الاجراءات اللازمة لمنع القيام بالتجسس الرقمي .

وبالمقابل فأن الفقرة الثانية من المادة (٢٨) قررت مسؤولية الرئيس الاداري الأعلى حيث نصت "٢- فيما يتعلق بعلاقة الرئيس والمرؤوس غير الوارد وصفها في الفقرة (١)- يسأل الرئيس جنائيا عن الجرائم التي تدخل في أختصاص المحكمة والمرتكبة من جانب مرؤوسين يخضعون لسلطته وسيطرته الفعليتين نتيجة لعدم ممارسة سيطرته على هؤلاء المرؤوسين ممارسة سليمة أ- اذا كان الرئيس قد علم أو تجاهل عن وعي اية معلومات تبين بوضوح ان مرؤوسيه يرتكبون أو على وشك أن يرتكبوا هذه الجرائم ب- اذا تعلقت الجرائم بأنشطة تندرج في أطار المسؤولية والسيطرة الفعلية للرئيس ج- أذا لم يتخذ الرئيس جميع التدابير الازمة والمعقولة في حدود سلطته لمنع او قمع أرتكاب هذه الجرائم أو لعرض المسألة على السلطات المختصة للتحقيق و المقاضاة "

نص الفقرة الثانية من المادة ٢٨ توضح مسؤولية القائد الاداري إذ كما تشير المادة إلى أن يسأل الرئيس عن جرائم الاشخاص الذين يعملون تحت أمرته سواء أصدر الأمر بارتكاب الجريمة أم لا على أنه في حالة تقديم ما يفيد بانه أتخذ الأجراءات اللازمة لمنع الجريمة أضافة إلى عدم العلم بوقوعها يعفيه من العقاب، إلا أن ما يؤخذ على نص المادة ٢٨ بأنها لم تبين بصورة صريحة ماهي الاجراءات التي تعد كافية لإعفاء الرئيس من المسؤولية حيث جاء نص المادة عامة مما يجعل أمكانية الافلات من العقاب ممكنة كما لم تحدد المعايير لاعتبار هذه الإجراءات المتخذة كافية لمنع وقوع الفعل ألا أنه من الناحية الواقعية المحكمة هي من تفصل في كفاية ومعقولية الإجراءات من عدمها وبالتالي تحديد مسؤولة القائد سواء كان مدنياً أم عسكرياً[٣].

ومن خلال النصوص السابقة فأن مسؤولية القائد أو الرئيس تتضمن مفهومين للمسؤولية الجنائية أولهما المسؤولية المباشرة حيث يعد القائد مسؤولاً بإصدار الأوامر بارتكاب أفعال غير قانونية وهذا على أساس المادة ٢٥ من النظام الأساس للمحكمة الجنائية ويستند البعض في ذلك على قضية (تاديش) حيث أن المحكمة الجنائية ليوغسلافيا السابقة أشارت الى انه " بالرغم من أن المتهم لم يضطلع بطريق مباشر في الافعال المدعي بها ،الا انه يظل مسؤولا إذا أستطاع ممثل الادعاء أن يثبت انه شارك عن وعي في التخطيط أو الاوامر أو ارتكاب أو بشكل آخر في مساعدة أو مساندة في أرتكاب الجريمة "[٤].

أما المفهوم الآخر هو المسؤولية المفترضة حيث يعتبر القائد أو الرئيس عن أفعال الأشخاص تحت ولايته غير القانونية برغم أنه لم يأمر بأرتكابها وهذا يرجع الى نص المادة (٢٨) وعليه فأن مبدأ مسؤولية الرؤساء لا يشمل فقط القادة العسكريين بل حتى المدنيين الذين يشغلون مناصب رئاسية ذات طبيعية واقعية أو ذات طبيعة قانونية .

وبالنسبة إلى أوامر الرؤساء والقادة فقد أشرت المادة ٣٣ " في حالة ارتكاب أي شخص لجريمة من الجرائم التي تدخل في اختصاص المحكمة لا يعفى الشخص من المسؤولية الجنائية أذا كان أرتكابه لتلك الجرائم قد تم امتثالا لأمر حكومة أو رئيس عسكري أو مدني "

كما أشار النص أعلاه إلى عدم الاعتداد باتباع أوامر الرؤساء والقادة للإفلات من العقاب في أطار المسؤولية الجنائية الدولية حيث لم يتفق الفقه على أعتبار أن تنفيذ أوامر الرؤساء والقادة سبب من أسباب الاباحة حيث أشار الاتجاه الأول من الفقه أن العسكري عليه دائما أطاعة رؤسائه ولا يجب أن يسأل عن نتائج هذا الامر[٥] أما الاتجاه الثاني يذهب خلاف الاول ويشير إلى ضرورة التأكد من مشروعية الأمر قبل الاقبال عليه ويجب عدم الأطاعة في هذه الحالة إلاَّ أن الفقه الدولي حسم الأمر بأن لا يجوز الطاعة في حال كانت ظاهرةً وواضحة عدم المشروعية الفعل[٦] وقد اشارت المحاكم السابقة مثل محكمة نورمبرغ في المادة ٨ من نظامها الاساس إلى عدم الإعتراف باتباع اوامر القادة للإفلات من العقاب ولكن يمكن استخدامه الامر كأساس لتخفيف العقوبة وكذلك أستبعدتها محكمة يوغسلافيا في المادة ٧ ورواندا في

---

[١] داودي منصور ،المسؤولية الجنائية للفرد على ضوء النظام الاساسي للمحكمة الجنائية الدولية ، رسالة ماجستير مقدمة الى جامعة الجزائر يوسف بن خدة كلية الحقوق ،٢٠٠٧،ص٨٥.

[٢] محمد صافي يوسف ،مصدر سابق ،ص١٣٢.

[٣] د.ايهاب الروسان، المسؤولية الجنائية الدولية للرؤساء والقادة ،بحث منشور في مجلة دفاتر السياسة والقانون ،العدد١٦ ، ٢٠١٧ ،ص١١٥.

[٤] د.هلالي عبد اللاه احمد ،المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء اتفاقية بودابست ،المجلد السادس ،العدد الثالث عشر ،مجلة الحقوق ،جامعة البحرين ،٢٠٠٩، ص٨ .

[٥] حسين عيسى مال الله ،مسؤولية القادة والرؤساء والدفع بإطاعة الاوامر العليا ،كتاب القانون الدولي الانساني من منشورات اللجنة الدولية للصليب الاحمر ، ٢٠٠٦ ،ص ٣٩٠.

[٦] د. يوسف حسن يوسف ،الجرائم الدولية للأنترنيت ،مصر المركز القومي للإصدارات القانونية ،ط١ ،٢٠١١ ،ص ١٣٥.

المادة ٦ إلا أن محكمة روما جاءت ببعض الحالات الاستثنائية التي يمكن الاعفاء به من العقاب "لا يعفي الشخص من المسؤولية الجنائية اذا كان ارتكابه لتلك الجريمة قد تم امتثالا لأمر حكومة او رئيس عسكريا كان او مدنيا عدا في الحالات التالية أ- اذا كان على الشخص التزام قانوني بإطاعة اوامر الحكومة او الرئيس المعني ب – إذا لم يكن الشخص على علم بأن الأمر غير مشروع ج- إذا لم تكن عدم مشروعية الأمر ظاهرية ".

يتضح مما تقدم أن بالإمكان مسائلة كل المساهمين عن شن هجمات التجسس الرقمي على شبكات الحواسيب ، وعلى الرغم من أن القائمين بالتجسس الرقمي غير موجودين في ساحة القتال حيث يجري تشغيلها عن بعد مع ذلك فأن القائمين بالهجمات يتولون تحديد الأهداف وجمع البيانات من هذه الأهداف وفضلاً عن ذلك إلى ذلك يعمل هؤلاء تحت قيادة مسؤولية ومن ثم فأنهم وقياداتهم لا يعفون من المسؤولية عن التجسس الرقمي وخاصة أن هذا النوع من الهجمات غالبا مايتم إرتكابها بناء على توجيه اوامر من قيادة عسكرية أذا كل دولة لها وحده خاصة تتولى عمليات التجسس الرقمي[١].

الفرع الثاني

أثار المسؤولية الجنائية الدوليَّة الفردية عن التجسس الرقمي

وبعد أن تناولنا الأشخاص الذين يخضعون للمسؤولية عن التجسس الرقمي وأن بالإمكان تكييف التجسس الرقمي ضمن جرائم الحرب أو جريمة العدوان فلابد من الإشارة إلى الأثار التي تترتب على هذه المسؤولية الجنائية الفردية والتي أشارت أليها المادة ٨٥ من مشروع مسؤولية الدول التي نصت "لا تخل هذه المواد بأية مسألة تتصل بالمسؤولية الفردية بموجب القانون الدولي لأي شخص يعمل نيابة عن الدولة " وبالتالي فأن الفقه يشير إلى أن العلاقة بين مسؤولية الدولة ومسؤولية الأفراد يمكن وصفها بالتبعية فمسؤولية الأفراد هي مسؤولية تبعية بالنسبة للدولة ،أي هي مسؤولية مرافقة لمسؤولية الدولة لا يمكن فصلها وأن المسؤولية مترتبة على الاثنان معا[٢].

وليس هذا فقط بل أن انعقاد الاختصاص للمحكمة سواء كان اختصاص موضوعياً أو شخصياً : وذلك عبر تطبيق أحكام جريمة العدوان او جرائم الحرب على التجسس الرقمي أو ان يكون الشخص الماثل أمامها يتمتع بالأهلية ويبلغ من العمر ١٨ فيتحقق أختصاص المحكمة على التجسس الرقمي وبالتالي بالإمكان فرض العقوبات الواردة في الميثاق في حالة اثبات التجسس الرقمي

حيث أشار نظام روما إلى العقوبات السالبة للحرية التي ممكن أن تُفرض على مرتكبي التجسس الرقمي سواءً كانوا مدنيين أم عسكرين وهي تتمثل بالسجن لمدة اقصاها ٣٠ عاماً وفي حالة رأت المحكمة خطورة الفعل وظروف الشخص المدان ممكن أن تشدد العقوبة إلى السجن المؤبد[٣] ،أما بالنسبة إلى العقوبات المالية أذ تناولها نظام روما أذ أجاز للمحكمة أن تأمر بفرض أية عقوبة اخرى تراها فضلاً عن لها أن تأمر بمصادرة الغرامة او الممتلكات والاصول الناتجة بصورة مباشر او غير مباشرة عن الجريمة.[٤]

أما بالنسبة إلى التعويض فقد أشارت المادة ٧٥ من نظام روما إلى جبر أضرار المجني عليهم حيث نصت "١- تضع المحكمة مبادئ فيما يتعلق بجبر الاضرار التي تلحق بالمجني عليهم أو فيما يخصهم بما في ذلك رد الحقوق والتعويض ورد الأعتبار وعلى هذا الاساس يجوز للمحكمة ان تحدد في حكمها عند الطلب أو بمبادرة منها في الظروف الاستثنائية نطاق ومدى أي ضرر أو خسارة أو أذى يلحق بالمجني عليهم أو فيما يخصهم وأن تبين المبادئ التي تصرفت على أساسها "

كما بينت المادة ٧٩ أن جبر الضرر يكون في ثلاثة أشكال : رد الحقوق والتعويض ورد الاعتبار وللمحكمة أن تامر بتنفيذ التعويض أو أي شكل من أشكال جبر الضرر عن طريق صندوق الاستئماني وهو صندوق تنشأه المحكمة بقرار من جمعية الدول الأطراف .

مع ذلك فأن إختصاص المحكمة اختصاصاً تكميلياً بموجب ميثاقها إذ تشير في المادة الخامسة بأن إختصاصها هو إختصاص تكميلي ، أي أنه مكمل لاختصاص المحاكم الوطنية وذلك بإعطاء القضاء الوطني للدول الولاية المبدئية فيما يتعلق بإقامة الدعوى على الجرائم الداخلة في اختصاصها ،وفي حالة تبين للمحكمة بأن هذه السلطات غير قادرة للتصدي لهذه الجرائم لسبب او لأخر فأن المحكمة تباشر إختصاصها بذلك.[٥]

لذا تباشر الدول اختصاصها الجنائي بموجب ما تملك من سيادة على أقليمها وبما تُصدر من قوانين وأنظمة أذا من خلالها تضع المسؤولية على مرتكب الجريمة ،كما أن القانون الدولي يعترف للدولة بممارسة إختصاصها القضائي على بعض المجرمين في خمس الحالات ومنها اولاً :حالة الأختصاص الأقليمي[٦] وثانياً : مبدأ جنسية الفاعل أذ أن الدولة تملك إختصاصاً قضائياً على مواطنيه ممن يحملون جنسيتها أين ما كانوا والمبدأ الثالث: هو المبدأ الوقائي وهو الأختصاص الذي تتمتع به الدول في حالة الجرائم التي تضر بأمنها الداخلي والمبدأ الرابع : هو مبدأ الجنسية السلبية وهي الحالة التي تقع الجريمة على مواطن يحمل جنسية الدولة أما الأخير هو مبدأ العالمية والذي يمنح للدولة أفضلية أيقاع العقاب على من تضع يدها عليه من المجرمين في حالة أرتكاب جرائم معينة مثل تجارة المخدرات أو الاتجار بالأطفال.

أما بالنسبة إلى التجسس الرقمي فنجد إن القضاء الجنائي الوطني نشط في إيقاع العقاب على مرتكب جريمة التجسس إذا تعد الدول جريمة التجسس من جرائم الخيانة العظمى أو انتهاك لسيادته وبالتالي تفرض لها أشد انواع العقوبات تصل الى الاعدام احيانا خاصة اذا تعلق الامر بالأسرار السياسية للدولة أو العسكرية التي تضر بالمصلحة العامة وخاصة مع عدم وجود أليات دولية مناسبة للمسؤولية على الجرائم المعلوماتية بصورة عامة والتجسس الرقمي خاصة.

الخاتمة

في نهاية كل بحث لابد ان يختم الباحث عمله بجملة من الاستنتاجات والتوصيات وهي كالأتي:

---

[١] من الامثلة على ذلك تملك اسرائيل العديد من الاجهزة التي تتولى فقط القيام بالتجسس مثل الموساد وكالة الامن القومية في الولايات الامم المتحدة :ينظر في ذلك د.عبد الهادي محمود الزيدي التجسس الإسرائيليّ على الدول العربية، مجلة العلوم الإسلاميَّة، ٢٠١٨م ،ص١٥٤.

[٢] محمد محمود امين ، نظرية الفعل غير المشروع دراسة في المسؤولية الدولية ،اطروحة دكتوراه ،جامعة بغداد ،كلية القانون ،٢٠٠٧ ،ص ١٣٨.

[٣] المادة ١/٧٧ من نظام روما الاساسي للمحكمة الجنائية الدولية .

[٤] المادة ٢/٧٧ من نظام روما الاساسي للمحكمة الجنائية الدولية .

[٥] د.عمر محمود المخزومي ،القانون الدولي الانساني في ضوء المحكمة الجنائية الدولية ،دار الثقافة للنشر ،الاردن ،٢٠٠٩ ،ص ٣١٧.

[٦] د.رشيد حمد العنزي ,محاكمة مجرمي الحرب في ظل قواعد القانون الدولي، مجلة الحقوق ،الكويت ،العدد ١، ١٩٩١ ، ،ص ٣٤٦.

اولا :-استنتاجات

١-التجسس الرقمي يمكن أن يكون تحت طائلة جريمة الحرب في الحالات المحددة التي يكون فيها للتجسس الرقمي تأثير على مايأتي : الممتلكات والاعيان المدنية أو المنشآت التي تنطوي على قوى خطره من خلال إختراق النظام المعلوماتي الذي يدير هذه الممتلكات ويسبب اضراراً لا حصر لها ، وكذلك في حالة توجيه التجسس الرقمي الى أفراد الخدمات الطبية أو السكان المدنيين.

٢- يمكن أن ينطوي التجسس الرقمي تحت جريمة العداون في حالة أن نفترض بأن هجوماً الكترونياً الذي له النطاق نفسهُ والتأثيرات على الدولة مثل الأعمال العسكرية كالاحتلال أو الهجوم المسلح ، سيشكل استخداماً للقوة وبالتالي جريمة عدوان في القانون الدولي حيث يمكن عن طريق البرامج غزو الفضاء الرقمي للدولة بالكامل و شلها عن الحركة وتوقف كل أجراءاتها الداخلية أو أرسال مجموعة من المرتزقة أو الافراد غير النظامين ،وعلى هذا الأفتراض يمكن أن يشمل المصطلحات في جريمة عدوان فعل التجسس الرقمي.

٣-فيما يتعلق بالمسؤولية الدولية الجنائية عن التجسس الرقمي نفترض بأن بالإمكان مسائلة كل المساهمين عن شن هجمات التجسس الرقمي على شبكات الحواسيب سواء كان مشغل البرنامج أم القائد العسكري أم الاداري ، على الرغم من أن القائمين بالتجسس الرقمي غير موجودين في ساحة القتال حيث يجري تشغيلها عن بعد مع ذلك فأن القائمين بالهجمات يتولون تحديد الأهداف وجمع البيانات من هذه الأهداف وفضلاً عن ذلك إلى ذلك يعمل هؤلاء تحت قيادة مسؤولية ومن ثم فأنهم وقياداتهم لا يعفون من المسؤولية عن التجسس الرقمي.

ثانيا-التوصيات

١-ندعو المحكمة الجنائية الدولية أن يكون لها سابقة خاصة بها فيما يتعلق بتحديد أختصاصها بالجرائم الالكترونية وأدخالها تحت مسمى العدوان أو جرائم الحرب متى ما توفر شروط أي من الجرميين ، فمن المهم للمحكمة أن تحدد سابقة خاصة بها تعتقد أنها تجسد أفضل نوايا الدول الأطراف في نظام روما الأساسي إذ تمتلك المحكمة الجنائية الدولية قدرة على تحديد سابقة خاصة بها وهذه القدرة إلى جانب العصر الحديث للقانون السيبراني ، قد تسمح للمحكمة بوضع بصماتها على القانون الدولي.

٢- يجب على المحكمة الدولية الجنائية أن تتعامل مع القضايا السيبراينة ، فلا ينبغي لها أن تنتظر تصرف الآخرون أولاً ،إذ نجد أن المحكمة لازالت تتخذ الصمت في هذا الجانب وهذا لايتلائم مع كونها محكمة دولية دائمة هدفها الاساسي تحقيق الانصاف ، إذ إن قدرة المحكمة على فرض تأثير رادع على هذه الجرائم ستحد بشدة من قدرة الدول على تنفيذ الهجمات الإلكترونية وستكون بمثابة ضغط في التأكد من الطرف المسؤول النهائي عن أي هجوم الكتروني معين.

٣-بما أن من صلاحية المدعي العام في المحكمة الجنائية الدولية توجيه التهم فلا ينبغي للمدعي العام أن يلاحق فقط الجهات الحكومية المسؤولة عن الأعمال العسكرية في الفضاء السيبراني ، بل يجب أن يكون منفتحًا أيضًا على ملاحقة الأفراد الذين ينفذون هذه الهجمات نيابة عن الدولة أو مع بعض من خلال دعم الدولة هذا من شأنه أن يعمل على زيادة نطاق فعالية المحكمة وأهدافها الرادعة.

٤-اصبحت الهجمات السيبرانية ومن ضمنها التجسس الرقمي عنصرًا أساسيًا مشتركًا في الشؤون الدولية ومع ذلك فإن المفهوم بأكمله غائب من تعريف المادة ٨ مكرر . هذا ليس مفاجئًا نظرًا لحقيقة أن الحرب الإلكترونية لم تكن موجودة في عام ١٩٧٤ عندما حددت الجمعية العامة أعمال العدوان بين الدول لكن غيابها عن المادة ٨ مكرر هو إغفال صارخ في العصر الحديث وسوف يشل المحكمة الجنائية الدولية في كيفية التحقيق في العدوان الذي قد يتكون فقط أو إلى حد كبير من تكتيكات الحرب الإلكترونية لذا ندعو الى الإنفاذ السليم لجريمة العدوان في السياق السيبراني من شأنه أن يقلل العواقب الوخيمة للأنخراط في نزاع سيبراني ، حيث يجب أن يخشى المعتدي ليس فقط رد الدولة التي تم غزوها سيبرانيا ورد الفعل الدولي كذلك ، و أيضًا من التهديد بالمقاضاة الفردية.

المصادر

اولا :الكتب

(١) .ايهاب الروسان ،المسؤولية الجنائية الدولية للرؤساء والقادة ،بحث منشور في مجلة دفاتر السياسة والقانون ،العدد١٦ ، ٢٠١٧

(٢)حسين عيسى مال الله ،مسؤولية القادة والرؤساء والدفع بإطاعة الاوامر العليا ،كتاب القانون الدولي الانساني من منشورات اللجنة الدولية للصليب الاحمر ، ٢٠٠٦

(٣)جاسم يونس الحريري ،مستقبل الحريات السياسية في دولة الامارات المتحدة ، دار الجنان للنشر والتوزيع ،عمان ،٢٠٢٠

(٤) .خالد ممدوح ابراهيم ،فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي,الاسكندرية,٢٠١٠،ص٦٧-٦٨.

(٥)عبد الله سليمان سليمان ،المقدمات الاساسية في القانون الدولي الجنائي ،ديوان المطبوعات الجامعية ،الجزائر ،١٩٩٢،ص٢٦٠.

(٦) .عمر محمود المخزومي ،القانون الدولي الانساني في ضوء المحكمة الجنائية الدولية ،دار الثقافة للنشر ،الاردن ،٢٠٠٩

(٧)محمد يوسف الصافي ،الاطار العام للقانون الدولي الجنائي في ضوء احكام النظام الاساسي للمحكمة الجنائية الدولية ،دار النهضة العربية ،القاهرة ،٢٠٠٢

(٨) . يوسف إبراهيم النقبي، التمييز بين الهدف العسكري والهدف المدني وحماية الأهداف المدنية والأماكن التي تحتوي على خطورة خاصة وفقاً للقانون الدولي الإنساني، القانون الدولي الإنساني، اللجنة الدولية للصليب الأحمر، القاهرة، ٢٠٠٦

(٩) يوسف حسن يوسف ،الجرائم الدولية للأنترنيت ،مصر المركز القومي للإصدارات القانونية ،ط١ ،٢٠١١

ثانيا: الرسائل والاطاريح

١-داودي منصور ،المسؤولية الجنائية للفرد على ضوء النظام الاساسي للمحكمة الجنائية الدولية ، رسالة ماجستير مقدمة الى جامعة الجزائر يوسف بن خدة كلية الحقوق ،٢٠٠٧،

٢-ماجد عمر عبادي ،جريمة العدوان قراءة تحليلية تعتمد النص والمفاوضات الدبلوماسية لمؤتمر كمبالا٢٠١٠،اطروحة دكتوراه ،جامعة النجاح الوطنية ،٢٠١٨

٣-محمد محمود امين نظرية الفعل غير المشروع دراسة في المسؤولية الدولية ،اطروحة دكتوراه ،جامعة بغداد ،كلية القانون ،٢٠٠٧

ثالثا /البحوث

١- د .أحمد عبيس الفتلاويّ، الهجمات السـيبرانيَّة مفهومها والمسـؤولية الدوليَّة الناتجة في ضـوء التنظيم الدوليّ المعاصـر عنها، بحث منشور في مجلَّة المحقِّق الحِلِّيّ، جامعة بابل،العدد ٤، ٢٠١٦م .

٢-د.رشيد حمد العنزي ,محاكمة مجرمي الحرب في ظل قواعد القانون الدولي، مجلة الحقوق ،الكويت ،العدد ١، ١٩٩١.

٣-عبد الهادي محمود الزيديّ، التجسس الإسرائيليّ على الدول العربية، مجلة العلوم الإسلاميَّة، ٢٠١٨م

٤-د.طيبة احمد ،الحماية الخاصة لموظفي الخدمات الطبية اثناء النزاعات المسلحة ،مجلة المحقق الحلي للعلوم القانونية والسياسية ، العدد الثاني ,السنة الثامنة ,٢٠١٦.

٤-د.هلالي عبد اللاه احمد ،المواجهة التشـريعية لجرائم المعلوماتية في النظام البحريني على ضـوء اتفاقية بودابسـت ،المجلد السـادس ،العدد الثالث عشر ،مجلة الحقوق ،جامعة البحرين ،٢٠٠٩.

رابعا :المصادر الاجنبية

1- Susan W. Brenner with Leo L. Clarke, Civilians in Cyberwarfare: Conscripts , Vanderbilt Journal of Transnational Law ,Vol. 43 .2010

2- David Scheffer, The Missing Pieces in Article 8 bis(Aggression) of the Rome Statute, Harvard International Law Journal / Vol. 58 Online Journal, S PRING 2017,P84 1/3/6 . https://blogs.icrc.org/alinsani/2019/02/03/2593

3-K EVIN L. M ILLER, THE KAMPALA COMPROMISE ANDCYBERATTACKS:CAN THERE BE AN INTERNATIONAL C RIME OF CYBER-AGGRESSION? , Southern California Interdisciplinary Law Journal ARTICLES 2014 , Vol. 23:217,P225 .

4-JONATHAN A. O PHARDT, CYBER WARFARE AND THE CRIME OFAGGRESSION: THE NEED FOR INDIVIDUALACCOUNTABILITY ON TOMORROW'SBATTLEFIELD, DUKE LAW & TECHNOLOGY REVIEW,2010,NO,3, P13.

خامسا: الاتفاقيات الدولية

١. اتفاقيات جنيف الاربعة لعام ١٩٤٩
٢. البروتكول الاضافي الاول لعام ١٩٧٧.
٣. اتفاقية بودابست لعام ٢٠٠١
٤. النظام الاساسي لمحكمة روما لعام ٢٠٠٢
٥. دليل تالين لعام ٢٠١٢