التجسس السيبراني على المحفوظات الدبلوماسية

أ.م.د. بيداء علي ولي
كلية القانون جامعة القادسية
Baydaa.ali@qu.edu.iq

تاريخ الاستلام : ٥-١-٢٠٢٢
تاريخ قبول النشر: ٩-٥-٢٠٢٢

المستخلص

يوسم عصرنا لحالي، بعصر المعلومات، فالمعلومات مخزنة الكترونيا وحسابيا مما شجع على التجسس عليها، فأضحى التجسس ظاهرة، فالدول تواقة الى معرفة اسرار غيرها، سيما اذا علمنا صعوبة معرفة الفاعل، وعدم وجود نصوص قانونية تحظر هذا الفعل ، بل بالعكس ان بعض الدول ترى ان التجسس اضحى قاعدة عرفية، فقد بدء ت الدول تتجسس على (المحفوظات الدبلوماسية)الوثائق الدبلوماسية المخزنة الكترونيا، مما يعرض استقرار العلاقات والسلم الدولي للخطر، ومما لاشك ان فعل التجسس هذا وان كان لا توجد قاعدة دولية تحظره بشكل علني، الا انه غير مشروع لمخالفته العديد من القواعد القانونية سيما المتعلقة بحرمة المحفوظات والمراسلات الدبلوماسية فضلا عن انتهاك احترام السيادة الاقليمية الالكترونية (البنية التحتية الالكترونية) للدولة ضحية التجسس، وعليه فان من يقارف هذا الفعل يعد مسؤولا عنه بموجب قواعد المسؤولية الدولية، وتترتب عليه اثار المسؤولية الدولية.

الكلمات المفتاحية : التجسس – السيبراني – المحفوظات - الدبلوماسية – المسؤولية.

Abstract.

Our era is now marked by the age of information، as their formation is stored electronically and in the cloud ،which encouraged spying on it. Espionage has become a phenomenon. Countries are eager to know other secrets ،especially if we know the difficulty of knowing the perpetrator ،and the absence of legal texts prohibiting this act. On the contrary ، some countries believe that Espionage has become a customary rule ،as countries have begun to spy on (diplomatic archives) diplomatic documents stored electronically ،which endangers the stability of international relations and peace ،and there is no doubt that this act of espionage ، although there is no international rule that publicly prohibits it ،is illegal for violating many legal rules ،especially those related to the sanctity of archives and diplomatic correspondence ،as well as a violation of respect for the territorial sovereignty of electronic (infrastructure). (electronic) for the state victim of espionage ،and therefore whoever commits this act is responsible for it under the rules of international responsibility ،and it has the effects of international responsibility

Keywords: **Cyber – Espionage - Diplomatic- Archive،- Responsibility.**

المقدمة

اولا: موضوع البحث

اضحت المعلومات بعصرنا الحالي الكترونية، مما يشجع الدول على الولوج للشبكات الدولية واختراقها، و يعد التجسس السيبراني على المحفوظات الدبلوماسية، ظاهرة منتشرة بين الدول والتي تبغي من ذلك معرفة اسرار تمكنها من الضغط على الدول ضحية التجسس، الامر الذي يلحق ضررا بالدولة الضحية ويزعزع استقرار العلاقات الدولية .

ثانيا: اهمية موضوع البحث

تسليط الضوء على التجسس السيبراني على المحفوظات الدبلوماسية، لما لهذا الامر تبعات قانونية وسياسية، والسعي لا يجاد اطار قانوني لحماية المحفوظات الالكترونية على غرار المحفوظات الثابتة، من خلال الاستعانة بنصوص اتفاقية فيينا للعلاقات الدبلوماسية لعام ١٩٦١ودليل تالين المطبق على النزاعات المسلحة بعده دراسة حديثة تتناول الهجمات السيبرانية، فضلا عن التأكيد على عدم مشروعية التجسس السيبراني .

ثالثا: مشكلة البحث

لما كان التجسس السيبراني ظاهرة حديثة، ويتم في الخفاء ولا يكلف اموالا باهظة، سعت الكثير من الدول لاستعماله لمعرفة اسرار غيرها من الدول ، في ظل غياب النصوص القانونية التي تحظره ، وبالتالي انتفاء مسؤوليتها عن القيام بهذا الفعل وازاء هذه الفجوة القانونية، كان لزاما التطرق له وبيان مدى مشروعية التجسس من عدمه، وبيان الاثر القانوني المترتب عن القيام بالتجسس، لردم الفجوة القانونية لهذا الموضوع .

رابعا: منهجية البحث

من اجل سبر غور التجسس السيبراني على المحفوظات الدبلوماسية، استعنا بالمنهج التحليلي، بعده المنهج الذي يتلاءم مع موضوع بحثنا، من خلال ايراد القواعد العامة لبيان مدى انطباقها على الحالة مدار البحث، ومن ثم ايجاد اطار قانوني دولي لحظر مثل هكذا تصرف وتفعيل المسؤولية الدولية بصدده .

خامسا: هيكلية البحث

ارتأينا لبحث هذا الموضوع ان يتم تناوله على مبحثين، اذ يتناول المبحث الاول التعريف بكل من التجسس السيبراني والمحفوظات الدبلوماسية وبيان مدى شرعية التجسس من عدمه، ويتناول المبحث الثاني المسؤولية المترتبة على الدولة المتجسسة، على ان تسبق تلك المباحث مقدمة، ويختم البحث بخاتمة تتضمن الاستنتاجات والمقترحات .

المبحث الاول

مفهوم التجسس السيبراني والمحفوظات الدبلوماسية

يتيح التجسس السيبراني للفاعل، سرقة المعلومات من اي مكان في العالم ، وبصفة مجهولة وغير مكلفة، وعلى نطاق واسع، ونتيجة لتلك المزايا فقد وجدت الدول بها ضالتها، في الحصول على اسرار الدول الاخرى، سيما انه لا توجد قاعدة قانونية دولية تحظره صراحة، فقد استعملته الدول للتجسس على اسرار الدول بما فيها المحفوظات الدبلوماسية، تلك المحفوظات التي تحظى بالحرمة وفقا لاتفاقية فيينا للعلاقات الدبلوماسية لعام ١٩٦٩ لذلك سوف نقوم بتسليط الضوء على هذا الموضوع لمعرفة ما المقصود بالتجسس السيبراني وهل هو مشروع ام لا ؟. ومن جانب اخر بيان المقصود

بالمحفوظات الدبلوماسية بالمعنى المتداول والحديث وعلى النحو الاتي:

المطلب الاول : تعريف التجسس السيبراني ومدى مشروعيته .

المطلب الثاني : تعريف محفوظات البعثة الدبلوماسية .

المطلب الاول

تعريف التجسس السيبراني ومدى مشروعيته

من نافلة القول، يوسم عصرنا بعصر المعلومات، اذا ان ادارة جميع امور الحياة بات تستخدم المعلومات والتقنيات، فسارعت الدول الى استخدام مثل هذه التقنيات للحصول على المعلومات التي تمكنها من معرفة احوال واسرار الدول الاخرى لتحقيق مكاسب شتى ، فلجئت الى استخدام التجسس السيبراني، لما له من مزايا عديدة، الامر الذي يلقي على عاتقنا تسليط مزيدا من الضوء على التجسس السيبراني لبيان المقصود به ومدى مشروعيته وذلك من خلال تناوله وعلى النحو الاتي

الفرع الاول

تعريف التجسس

ان ولادة الانترنيت في التاسع والعشرين من تشرين الاول لعام ١٩٦٩، دفعت العالم الى عصر التكنولوجيا السريع والابتكار الهيكلي الذي غير بشكل جذري الطريقة التي يتعامل بها الافراد والحكومات، اذ اصبح ركيزة عالمية للتجارة والتواصل بكافة اشكاله، اذ عد الفضاء السيبراني العنصر الخامس من عناصر الدولة، و بذلك فقد اضحت المراسلات الدبلوماسية تنتقل عن طريق الشبكات[١] .

الا انه وبالرغم من هذه الاهمية فقد جلب معه الكثير من التداعيات الامنية للكيانات الخاصة والدول مما جعلها اكثر عرضة للخطر[٢].

فلقد لجئت العديد من الدول الى استغلال الفضاء السيبراني [٣].

وما يتحه من امكانيات هائلة الى التجسس على الدول الاخرى من اجل استخدام هذه المعلومات بشكل يخدم مصالحها [٤].

اوقد يساعدها هذا الولوج الى هذه الشبكات من اتلاف هذه البيانات دون ان يترك ذلك اثرا عليها .

فالتجسس السيبراني يتم بواسطة عدة طرق تتمركز على التقنية التكنولوجية والبرمجية للحصول على المعلومات غير المعلن عنها، مما تجدر الاشارة اليه ، ان التجسس بالمعنى التقليدي في اوقات النزاعات المسلحة في ادبيات القانون الدولي الانساني وهو محظور في اطار النزاعات المسلحة التقليدية ، اما التجسس السيبراني والذي نشهده اليوم بفضل التقدم التكنولوجي لا توجد قواعد قانونية دولية تتناوله باستثناء (دليل تالين)[٥].

والذي اشار اليه في البند (أ) من القاعدة (٦٦) بأن "التجسس السيبراني وغيرها من صور جمع المعلومات الموجهة ضد العدو اثناء النزاع المسلح لا تنتهك قانون النزاع المسلح" [٦].

، ولما كان التجسس السيبراني في زمن السلم ظاهرة حديثة فلقد تعددت التعريفات التي تناولته ، وبدورنا سوف نورد بعض منها

عرف التجسس السيبراني على انه " الدخول غير المشروع الى الشبكة المعلوماتية او المواقع الالكترونية للحصول على المحتوى الالكتروني

غير المصرح به او غير المتاح للجمهور، يمس الامن الوطني او العلاقات الخارجية الدولية، او السلامة العامة او الاقتصاد الوطني"[٧]

ويعرف ايضا بأنه " قيام احد الاشخاص غير المصرح لهم بالدخول الى نظام تشغيل مختلف الاجهزة والبرامج كما انه، بإمكانه ان يتحكم في نظام التشغيل فيقوم بإصدار اوامر مثل اعطاء امر طباعة او التصوير او التخزين على انه يبني هذا الامر على اساس منظم او فردي بالتجسس على اشخاص او الدولة او المنظمات او الهيئات او المؤسسات الدولية والوطنية، وهذا باستخدام الموارد المعلوماتية والانظمة الالكترونية التي جلبتها حضارة التقنية في عصر المعلومات" [٨].

ويطلق البعض على هذا النوع من التجسس بالتجسس السياسي تمييزا له عن التجسس الاقتصادي، والذي يقصد به "هو الاستحواذ بدون وجه حق على اسرار التعامل التجاري والتقنية بجميع صورها "[٩].

كما يقصد بالتجسس السيبراني "قيام دولة، او جهاز تابع لها او وكيل عنها بالاطلاع على او نسخ البيانات السرية غير المتاحة للجمهور والمحفوظة على انظمة تكنولوجيا المعلومات او شبكات الكمبيوتر الموجودة في اقليم منطقة خاضعة لولاية دولة اخرى، بواسطة عمليات سرية وبذرائع مزيفيه او كاذبة، وبدون تراخيص او موافقة من مالكي او مشغلي هذه الانظمة او شبكات الحاسوب المستهدفة او الدولة الاقليمية"[١٠].

يبدو ان هذا التعريف هو الاقرب لموضوع بحثنا، والذي يمكن ان يعطينا جملة من العناصر لهذا النوع من التجسس، وهي

١. ان التجسس يمكن ان تقوم به الدولة، عن طريق مؤسساتها ، او بواسطة وكلات تقوم بتجنيدها لذلك .
٢. ان التجسس السيبراني هو الاطلاع على المحفوظات والوثائق المرسلة عن طريق البريد الالكتروني او شبكات الانترنيت او الاتصالات.
٣. ويعد تجسسا أيا كان مكان وجود هذه الوثائق سواء اكانت في الدولة المعتمدة او المعتمد اليها او دولة المرور

الفرع الثاني

مدى مشروعية التجسس السيبراني

لقد اشرنا مما سبق، ان التجسس السيبراني في زمن النزاع المسلح غير محظور استنادا الى دليل تالين الذي يعده، بانه لا ينتهك قانون النزاعات المسلحة، الا ان التجسس السيبراني الذي تقوم به الدول في زمن السلم ، قد احتدم بصدده النقاش، فمنهم من يعده مشروعا بسبب عدم وجود نص قانوني صريح على حظره كما في جرائم على الاعتداء على الحق في الخصوصية يحث توجد قرارات عدة من الجمعية العامة تؤكد الحق في الخصوصية كالقرار رقم ١٦٧/ ٦٨لعام ٢٠١٣، فضلا عن وجود اتفاقيات اقليمية التي عنيت بجرائم الانترنيت كاتفاقية (بودابست لعام ٢٠٠١) و(الاتفاقية العربية لمكافحة جرائم تقنيات المعلومات عام ٢٠١٠)، واتجاه اخر بالنقيض من ذلك ، اذ يرى ان التجسس غير مشروع، ولكل اتجاه مبرراته، وهو ما سنقوم ببيانه وعلى النحو الاتي :

اولا :الاتجاه المؤيد لمشروعية التجسس

يذهب هذا الاتجاه على ان التجسس السيبراني مشروع سواء أكان في زمن السلم ام

الحرب، ففي زمن السلم فانه يرتكز على حق الدولة في البقاء والاستمرار وتحقيق حماية الدولة ضد الاخطار الخارجية، اما في زمن الحرب(النزاعات المسلحة)فهو وسيلة من وسائل الحرب ، ومن ضمن المبررات التي يوردها هذا الاتجاه هي:

١. ان اتفاقية لاهاي لعام ١٩٠٧والتي حددت محرمات الحرب لم تذكر التجسس من ضمنها، وعليه فهو مشروع طالما لا توجد قاعدة قانونية تحظره، واستندوا في ذلك الى حكم المحكمة الدائمة للعدل الدولي في قضية اللوتس عام ١٩٢٧ والذي جاء فيه (اذ يكون على الدولة دائما ان تثبت ان تصرف الدول الاخرى المخالف للقانون هو بناء على قاعدة قانونية)وعليه فاذا غاب الحظر الصريح تبقى كل دولة حرة في ممارسة ما يحقق مصالحها [١١].

كما ويذهب الى ابعد من ذلك بتأسيس قاعدة عرفية بجواز التجسس السيبراني استنادا لعدم وجود حظر لهذا السلوك منذ نشأة القانون الدولي، مما يعني نشوء قاعدة عرفية بجوازه[١٢].

٢. ان ممارسة التجسس وسيلة ضرورية لترسيخ سيادة الدول وحماية امنها القومي من اي تدخل اجنبي او اعمال ارهاب سيما ان الدول تحتاج الى الحصول على معلومات لتعزيز استقرارها وتحقيق الكفأة السياسية من اي تهديد يكون محدقا بها، فاذا كان التجسس هو احد السبل لتحقيق ذلك، فهو مشروع [١٣].

٣. ان التجسس السيبراني يكون في الفضاء الخارجي عبر الاقمار الاصطناعية والشبكات، و ان الفضاء غير خاضع لسيادة اي دولة وان الجاسوسية في العصر الحديث كما يقول الفقيه (ستون)فهي مخصصة لمنع هجوم نووي مفاجئ سيؤدي حدوثه الى اندلاع حرب عالمية ثالثة، وعليه فهي اداة لتحقيق مصلحة جماعية [١٤].

٤. التجسس السيبراني لا يصل الى مستوى التهديد باستعمال القوة الذي يعد محظورا بموجب ف/ ٤ من م/ ٢من ميثاق الامم المتحدة، لأنه يقتصر على الحصول على المعلومات السرية، دون التسبب بأضرار مادية [١٥] .

ثانيا : الاتجاه المعارض لمشروعية التجسس

١. اما هذا الاتجاه فانه يرى بأن التجسس السيبراني غير مشروع وذلك من خلال الرد على مبررات الاتجاه المؤيد والعمل على تفنيدها

٢. بصدد ان اتفاقية لاهاي لعام ١٩٠٧ لم تذكره ضمن الوسائل المحظورة، وذلك بسبب ان ما ورد باتفاقية لاهاي قد ورد على سبيل المثال وليس الحصر، فالتجسس يعد من الامور المستهجنة وغير المشروعة استنادا الى م/ ٣٨ من النظام الاساسي لمحكمة العدل الدولية وذلك لمخالفته المبادئ العامة للقانون، فلو تم جمع القوانين التي حظرت التجسس في العالم، عد ذلك الاجماع عن حظره في تلك القوانين بمثابة العمومية، فمقارفة التجسس يعد مخالفة للمبادئ العامة التي اقرتها الامم المتمدنة .

٣. التجسس غير مشروع وفقا لاتفاقية قانون البحار لعام ١٩٨٢ والتي اشارت في ف/ ٢من م/ ١٩ (يعد مرور السفينة ضارا بسلم الدولة الساحلية او بحسن نظامها او بأمنها اذا قامت السفينة اثناء وجودها في البحر الاقليمي باي عمل يهدف الى جمع المعلومات التي تضر بدفاع الدولة الساحلية او امنها)فجمع المعلومات يعد اهم اهداف التجسس، وعليه واستنادا للنص اعلاه فان التجسس غير مشروع.

٤. اما القول بان ، الفضاء غير خاضع لسيادة دولة ما، فهذا لا يعني ان يتم استخدامه بشكل يهدد سلامة الدول، سيما ان اتفاقية الفضاء الخارجي لعام ١٩٦٧اكدت على الاستخدام السلمي للفضاء واشارت في المادة الاولى (يجب ان يكون استخدام الفضاء بما يحقق الفائدة للبشرية وشعوبها).

٥. ان القول بانه لا يعد التجسس السيبراني تهديدا باستخدام القوة المحظور بموجب الميثاق ، قول مردود لان القيام بالتجسس السيبراني بواسطة الاقمار الاصطناعية العسكرية يعرض السلم والامن الدوليين للخطر ويتعارض مع مبدأ انماء العلاقات الودية بين الامم [١٦] .

٦. التجسس السيبراني يمثل انتهاك لمفهوم سيادة الدولة، سيما بعد تطور مفهوم السيادة ليشمل المجال الالكتروني، مما يعني بسط الدولة لسيطرتها وولايتها القضائية على الفضاء السيبراني، وهذا ما اكده دليل تالين في القاعدة الرابعة منه" ان اي تدخل في البنية التحتية السيبرانية على متن منصة تتمتع بالحصانة السيادية لدولة اخرى، اينما وجدت تشكل انتهاك لمبدأ السيادة "، اذ اكد وجوب منع الدول من استخدام البنى التحتية السيبرانية الواقعة في اقليمها والتي تخضع لسيطرتها الكاملة في نشاطات تمس الحقوق السيادية للدول الاخرى .

٧. ، فالتجسس السيبراني يتعارض مع مبدا عدم التدخل في الشؤون الداخلية والذي يعد جزء من القانون الدولي [١٧].

ويبدو ان الاتجاه المعارض لمشروعية التجسس السيبراني هو الاتجاه الصحيح، للمبررات التي اوردها ولضمان استقرار العلاقات الدولية ولصيانة سيادة الدولة من الانتهاك .

المطلب الثاني

مفهوم المحفوظات الدبلوماسية (الارشيف الدبلوماسي)

من نافلة القول ان المحفوظات الدبلوماسية لم يرد تعريفا خاصا بها سواء في اتفاقية فيينا للعلاقات الدبلوماسية لعام ١٩٦١، او في اتفاقية فيينا للعلاقات الدبلوماسية الخاصة لعام ١٩٦٩ اذ وردت نصوص تشير الى حرمتها وحصانتها، في حين ان اتفاقية فيينا للعلاقات القنصلية لعام ١٩٦٣ قد اورت تعريفا لها، وذلك بان المحفوظات القنصلية هي "جميع الاوراق والوثائق والمراسلات والكتب والافلام والاشرطة وسجلات المركز القنصلي ، وكذلك ادوات الشفرة والرموز وبطاقات الفهارس او اي جزء من الاثاث يستعمل لحمايتها او حفظها"[١٨].

ولقد استند عدد من المختصين بالقانون الدولي على هذا التفصيل الوارد بشأن المحفوظات، فقاموا بدورهم بوضع تعريفا لها بانها " كل المستندات والاوراق السرية للدولة الموفدة، والتي يحتضنها المقر التابع لها في الدولة المضيفة والتي تتمتع بحرمة مصونة وخاصية اعطاها القانون الدولي العام "[١٩].

كما عرف على انه "الاوراق والمستندات المحفوظة داخل مقر البعثة او السفارة او القنصلية الخاصة بأسرار دولة ما، مضمونها وسياستها الخارجية وعلاقتها بالدولة المستقبلة واسرار انظمتها، والتي تكون مصونة بحماية خاصة، وحماية عامة من المقر وخاصة لها، وبالتالي تكون ذات حرمة سرية برا وبحرا وجوا وفي جميع الظروف الاستثنائية " [٢٠].

وعليه فان هذه المحفوظات الدبلوماسية تتمتع بحرمة قانونية افردتها لها الاتفاقيات المعنية، فقد حظيت المحفوظات بحماية عامة بعدها جزء من مقر البعثة والذي يحظى بالحرمة[٢١].

وحماية خاصة بها بمعزل عن البعثة بالنص على ان محفوظات البعثة ووثائقها مصونة دائما أيا كان مكانها[٢٢].

واستنادا للتعاريف السالفة الذكر فان ارشيف البعثة (المحفوظات)هي جميع الاوراق والمستندات والوثائق، والتي تتضمن سياسة الدولة الخارجية للدولة الموفدة وتعاملاتها مع الدول الاخرى، وسواء اكانت هذه الوثائق موجودة في مقر البعثة، او اي مكان تابع لها، فأنها تتمتع بحصانة مزدوجة، حصانة عامة كونها جزء من مقر البعثة[٢٣].

وحصانة خاصة بإيراد نصوص قانونية تخص هذه الوثائق بالحماية أيا كان مكان وجودها، وعليه يمكن تصنيف ارشيف البعثة الى قسمين (جزئيين)وهما

١. **ارشيف البعثة الثابت** : جميع الوثائق الموجودة في وزارة الخارجية للدولة الموفدة، و ما تقوم بأرساله الى سفارتها في الخارج، وهو ما يحظى بحماية منصوص عليها في الاتفاقيات المعنية .
٢. **ارشيف البعثة المتحرك** :وهو كل ما ترسله الدولة من اسرارها او اورقها سواء أكان عن طريق الحقيبة الدبلوماسية، وهو بدوره يحظى بحماية خاصة، او ما ترسله عن طريق شبكات الانترنيت وينقل عبر الفضاء السيبراني (او ما يسمى بالمحفوظات الالكترونية وهي محركات الاقراص الثابتة والمحمولة والوسائط الاخرى التي يتم تخزين الوسائط الالكترونية عليها ورسائل البريد الالكتروني والمراسلات الرسمية والكابلات)[٢٤].

وهو ما نسعى الى حمايته من التجسس السيبراني الذي يرد عليه في وقتنا الحالي، سيما ان دليل تالين قد اشار في القاعدة (٨٤)" المحفوظات والاتصالات الدبلوماسية تعد محمية من العمليات السيبرانية في جميع الاوقات " .

ومن القضايا التي تعد سابقة خطيرة انتهكت بها حرمة الوثيقة الدبلوماسية جرت عام ٢٠١٧، عندما نشرت ويكيليكس برقية دبلوماسية من السفارة الامريكية في لندن، تلخص اجتماعا جرى بين مسؤولين أميركيين وبريطانيين حول جزيرة (Chagos) والذي عقد في ايار وعلى اثر هذا النشر رفع ممثلو جزر مستعمرة شاغوس الذين

ابعدتهم الحكومة عن الجزر بسبب تأجيرها للحكومة الامريكية كقاعدة عسكرية، وهي قضية (الشؤون الخارجية وشؤون الكومنولث ضد وزير الدولة)، صرح كولين روبرتس (وزارة الخارجية) حيث اتخذت الحكومة عدة اجراءات لمنع عودة شعب شاغوس الى الجزر ولن يكون هناك اثار اقدام بشرية، وان انشاء حديقة بحرية من شانه دفع مطالبات اعادة التوطين للمقيمين السابقين في ارخبيل شاغوس، واثناء الاستجواب (لروبرتس)في المرحلة الاولى من القضية تم ايقاف القضية، ودفعت وزارة الخارجية البريطانية بأن وثيقة ويكيليكس والتي يبدو انها نسخة من برقية دبلوماسية غير مقبولة في محكمة انكليزية، لأنها تتعارض مع اتفاقية فيينا للعلاقات الدبلوماسية لعام ١٩٦١، بالذات للمادتين (٢٤وف/ ٢من م/ ٢٧)، فجرت مناقشات حول المقصود بالحرمة، فذهب (Mann)بان المقصود بالحرمة هنا من التدخل من قبل المدعي او الدولة المستقبلة، وان الحرمة لم تكن قاعدة عامة ضد عدم المقبولية في محكمة محلية، في حين ذهب (Eileen Denza) ان الحرمة تعني عدم المقبولية في اي محكمة، لان الوثيقة تعد جزء من ارشيف البعثة ومحمية بموجب م/ ٢٤ بالشكل الذي يجعل الوثائق والنسخ غير مسموح به مالم تكن هناك ظروف استثنائية مثل مؤامرة وفي ظل غياب التنازل الصريح عن الحرمة، اما اللورد (Neuberger)يشير الى ان الحرمة الواردة على ارشيف او وثائق البعثة تؤسس على شرطين

١. يجب ان تشكل الوثيقة او تظل جزء من ارشيف المهمة
٢. الا يتم نشر محتوياتها على نطاق واسع في المجال العام بحيث تقضي على اية سرية او حرمة يمكن ان ترتبط بها بشكل معقول، وقد يتطابق هذان المؤهلان في بعض الاحيان ولكن بالتأكيد ليس دائما، ويشير الى ان الوثيقة لم تأت مباشرة من السفارة الامريكية في لندن، حيث من المحتمل جاءت من وزارة الخارجية الامريكية في العراق ، لذلك قضت المحكمة ان لم يتم اثبات حتى على سبيل الاحتمال ان الكابل ظل جزء من ارشيف البعثة في لندن، وعندما تم استخراجه من قبل ويكيليكس فقدت الوثيقة اية حرمة بسبب دخولها الى الملك العام، وعليه يعد وجودها في ويكيليكس متاحا للاستخدام ومقبولا كدليل على محتوياته في الاجراءات، وان بإمكان المحكمة التأكد من صحة الوثيقة دون موافقة الدولة المرسلة، حيث ان الوثيقة موجودة في المجال العام، واوضحت المحكمة ان مصطلح (أيا كان مكانها) لا يمكن ان يعني ببساطة في اي مكان من العالم توجد الوثائق، يمكن وضع الملفات الالكترونية بعيدا عن مقر البعثة، ومع ذلك قد تكون جزء من ارشيف البعثة، العامل الحاسم ما اذا كان الوصول اليها يخضع لسيطرة موظفي البعثة سواء بشكل مباشر او بموجب الشروط التي بموجبها نقلت البعثة الوثيقة الى كيان حكومي اخر، وان من الصعب على المحكمة تحديد مستوى السيطرة من خلال مهمة المستند، كما انه ليس من الواضح ماهي القيود التي يجب وضعها على مستند ترسله البعثة لا بقائه ضمن حرمة ارشيف البعثة، حيث ان وضع علامة سرية غير كاف، وعليه فقد اقرت المحكمة بعبثية محاولة الحفاظ على سرية الوثيقة في المجال العام حتى عندما

تكون الوثيقة دبلوماسية تم الحصول عليها بشكل غير قانوني وعليه فان الوثيقة تكون مقبولة امام المحكمة، ويمكن احالتها الى المحاكم لتقييمها[٢٥].

٣. يبدو ان ما سارت عليه المحكمة الانكليزية غير صحيح للأسباب التالية :

١. ان تفسير نصوص الخاصة بحرمة الوثائق وارشيف البعثة يجب ان يتم وفق القواعد المتعلقة بتفسير المعاهدات، وليس كما قامت به المحكمة الانكليزية

٢. ان وثائق البعثة ومحفوظاتها تتمتع بالحرمة أيا كان مكانها، كذلك الاتصالات والمراسلات الدبلوماسية، وعلى الدولة المضيفة تقديم جميع التسهيلات بهذا الخصوص، والحفاظ على سريتها، سيما ان الدولة المضيفة ملزمة بمنع الضرر العابر عن العمليات السيبرانية استنادا الى القاعدة (٥) من دليل تالين "لا يجوز للدولة ان تسمح بمعرفتها باستخدام البنية التحتية السيبرانية الواقعة في اقليمها او تحت سيطرتها الحكومية الحصرية ان تستخدم في الاعمال التي تؤثر سلبا وبشكل غير شرعي على الدول الاخرى "مع الاشارة ان الالتزام بالحرمة وتمتع الوثائق والمراسلات الحصانة يمتد الى الدولة التي تمر بها هذه الاتصالات والمراسلات.

٣. ان الحصانة التي تتمتع بها المحفوظات او الوثائق الدبلوماسية مقيد بقيد عدم تهديدها لأمن وسلامة الدولة المستقبلة، ففي حالة وجود ادلة تؤيد مساسها بأمن وسلامة الدولة المستقبلة كوجود حالة تامر، فلا تتمتع الوثائق بالحرمة [٢٦].

اما في القضية محل البحث فلا يوجد ما يشير الى اي تأمر او انتهاك لسيادة الدولة المستقبلة

المبحث الثاني

المسؤولية الدولية المترتبة عن التجسس السيبراني

تعد المسؤولية الدولية ضمانة لتطبيق القانون الدولي، وان اجماع شروطها اساسا لحصول الدولة الضحية على جبرا للضرر الواقع عليها جراء التجسس السيبراني، واستنادا لذلك سوف نقوم بتناول شروط قيام المسؤولية الدولية ومدى انطباقها على التجسس السيبراني في ظل الصعوبات التي تكتنف الموضوع وبيان الاثار المترتبة عليه في حالة اثبات وجود التجسس السيبراني وعلى النحو الاتي :

المطلب الاول : شروط المسؤولية الدولية

المطلب الثاني : الاثار المترتبة عن المسؤولية الدولية

المطلب الاول

شروط المسؤولية الدولية

لكي تتحقق المسؤولية الدولية المترتبة عن التجسس السيبراني على المحفوظات الدبلوماسية لابد من اجتماع الشروط اللازمة لأثارة مسؤولية الدولية للدولة ، وتتجسد هذه الشروط في

الفرع الاول

صدور فعل غير مشروع دوليا من الدولة

تشير المادة الاولى من مشروع مسؤولية الدول عن الافعال غير المشروعة دوليا "ان كل فعل غير مشروع دوليا تقوم به الدولة يستتبع مسؤوليتها الدولية "[٢٧].

وان تقدير مشروعية الفعل من عدمه يكون استنادا للقانون الدولي وليس القانون الداخلي[٢٨].

ولكي يكون الفعل غير مشروع دوليا يجب ان يكون خرقا للالتزام الدولي، وفي معرض حديثنا عن التجسس السيبراني على المحفوظات الدبلوماسية ، فلقد اتضح كما بينا انفا، بان التجسس السيبراني بحد ذاته كفعل هو غير مشروع دوليا استنادا الى عدد من المبررات المنطقية و على الرغم من عدم وجود نصوص قانونية صريحة بخصوص عدم مشروعيته باستثناء القاعدة (٦) من دليل تالين والتي نصت على " تتحمل الدولة المسؤولية القانونية الدولية للعمليات السيبرانية التي تنسب اليها والتي تشكل خرقا لالتزام دولي "، الا ان هناك ردود فعل دولية تؤكد عدم مشروعية التجسس ففي اعقاب تصريحات (سنودن)عام ٢٠١٣ التي سربها من وكالة الامن القومي عن عمليات تجسس بواسطة الانترنيت قامت بها وكالة الامن القومي الامريكي على الصين وروسيا والاتحاد الاوربي والبرازيل وعدد من الدول والافراد والموظفين، فقد وصفت رئيسة البرازيل (ديلما روسيف) برنامج مراقبة وكالة الامن القومي انه حالة من عدم احترام للسيادة الوطنية وانه حالة من الانتهاكات الجسيمة لحقوق الانسان والحريات المدنية، كما اصدرت الخارجية المكسيكية بيان صحفي يدين المراقبة الامريكية ويعدها غير مقبولة ومخالفة للقانون المكسيكي والقانون الدولي، وادعت اندونيسيا ان هذه الممارسات تنتهك القانون الدولي وميثاق الامم المتحدة، واكدت الحكومة الصينية ما ذهبت اليه اندونيسيا واضافت انه يجب رفض هذه الممارسة وادانتها من العالم باسره[٢٩].

فضلا عن هذا، فان التجسس الذي يقع على المحفوظات الدبلوماسية يعد غير مشروع لانتهاكه الالتزامات الخاصة بحرمة المحفوظات الدبلوماسية (الثابتة او المتحركة)، فأي تجسس يرد على المحفوظات والمراسلات والوثائق الدبلوماسية سواء اكانت في مقر البعثة اوفي اي مكان اخر ملحق بالبعثة ووجودها في اجهزة الكمبيوتر الخاصة بالبعثة سيما نحن في عصر اضحت تخزن جميع الوثائق في اجهزة الحاسوب ، او اثناء التراسل بها عبر البريد الالكتروني او اي من الوسائل الالكترونية، فعلى الدولة المستقبلة اتخاذ جميع الخطوات المناسبة لحماية البنية التحتية الالكترونية في مباني البعثة الدبلوماسية او القنصلية للدولة المرسلة من التطفل والضرر، كما طالب الاتحاد الاوروبي من الحكومة التركية على اثر نشر الصحف التركية لرسالة بريد الكترونية تم اعتراضها ارسلها الاتحاد الاوروبي، في(تركيا) بان تتخذ (تركيا) تدابير لتعزيز امن تمثيلها الدبلوماسي في انقرة مشيرة ان المراسلات محمية بموجب اتفاقية فيينا ، استنادا الى مبدأ العناية الواجبة، مع الاشارة الى ان كل ذلك يعتمد على حجم التهديد للمباني ومدى ادراك الدولة المستقبلة لخطر معين وقدرتها على اتخاذ اجراء[٣٠]، وبالتالي فانه يعد انتهاك لالتزاما دوليا واردا وبشكل صريح في اتفاقية دولية ، اذ تنص اتفاقية فيينا للعلاقات الدبلوماسية الدائمة لعام١٩٦١ في المادة ٢٤منها " تكون حرمة محفوظات البعثة ووثائقها مصونة دائما أيا كان مكانها "، وكذلك ف/ ٢من م/ ٢٧"تكون حرمة المراسلات الرسمية للبعثة مصونة، ويقصد بالمراسلات الرسمية جميع المراسلات المتعلقة

بالبعثة ووظائفها " ومن الجدير بالذكر ان هذه الحرمة قد وردت ايضا في اتفاقية هافانا للعلاقات الدبلوماسية لعام ١٩٢٨ واتفاقية فيينا للعلاقات القنصلية لعام ١٩٦٣، مع الاشارة ان هذه الحرمة تظل سارية حتى في حالة النزاع المسلح، اذ على الدولة المعتمد لديها احترام وحماية دار البعثة وكذلك اموالها ووثائقها [٣١].

اضافة الى عدم مشروعية الفعل الدولي، ان يكون منسوبا الى دولة، ويكون الفعل كذلك اذا صدر من هيئات الدولة الثلاثة (التشريعية والتنفيذية والقضائية)او من رعاياها، او الاشخاص الذين يتصرفون بموجب تعليمات من اجهزتها او بإيعاز منها او تحت رقابتها[٣٢].

هذا بشكل عام، اما في التجسس السيبراني فأن اسناد التجسس على الدولة يكتفه الصعوبة من الناحية الفنية والقانونية والسياسية، فمن الناحية القانونية فان مشروع مسؤولية الدول عن الاعمال غير المشروعة دوليا لعام ٢٠٠١ لم يعنى بقضية الاثبات بالتالي لا يمكن معرفة ماهي التدابير المعتمدة لأثبات التجسس[٣٣].

اما من الناحية الفنية اذ ان الاسناد يتطلب تحديد موقع وهوية البنية التحتية التي تنشأ منها الهجمة او التجسس ويتطلب جمع المشتغلين التقنيين المبتدئين والمحترفين مع حدس وحكم المختصين في الاستخبارات لمعرفة القائمين به، وذكاء الاشارات وتاريخ العلاقات الدبلوماسية، وعلى سبيل الذكر ان هجمات(Solar Winds Microsoft Exchange)لم يتم اكتشاف القائمين بها من قبل وكالات الاستخبارات الامريكية لمدة تسعة اشهر حتى تم الاعلان عن الاسناد الرسمي عن (Solar Winds) في نيسان ٢٠٢١ [٣٤]. فاذا كان الهجوم الالكتروني والذي يترك اثرا يستغرق مثل هذه الفترة للكشف عنه، فما الحال بالتجسس الالكتروني وما يكتنفه من صعوبة بالغة بالكشف عنه لإسناد الفعل الى القائمين به سيما ان دليل تالين يشير في القاعدة (٨)" حقيقة ان العملية السيبرانية وجهت من خلال البنية التحتية السيبرانية الواقعة في دولة ما، لا يعد دليلا كافيا لإسناد العملية لتلك الدولة "، اما الصعوبة السياسية تتمثل بالحسابات الجيوسياسية والحد من مخاطر التصعيد، وضمان عدم تأثر الجهود الدبلوماسية الجارية مع دول معينة (كقضية جوناثان بولارد) فان استجابة الولايات المتحدة الامريكية لإسرائيل كانت اقل صرامة نظرا للعلاقات الثنائية ومكانتها في السياسة الامريكية المحلية[٣٥].

ليس هذا فحسب بل يحكمه ميزان القوى ايضا فالدولة قد لا تفصح عن التجسس بسبب خشيتها من معرفة الغير بذلك مما يعني الاخلال بسمعتها، او انها ترمي الى استغلال هذه الحادثة للقيام بذات الفعل على الدولة القائمة بالتجسس، او ان الدولة ضحية التجسس تكون اقل قوة من الدولة القائمة بالتجسس فمن مصلحتها عدم الافصاح[٣٦].

مع الاشارة الى ان الدولة لا تسأل عن قيامها بنشاط ايجابي بالتجسس فحسب ، بل تكون مسؤولة ايضا عن عدم منع التصرف الضار بالدول الاخرى لعدم قيامها بالإجراءات الواجب اتخاذها، فكل دولة ملزمة باتخاذ الاجراءات التشريعية والادارية في مواجهة القائمين بالتجسس ومعاقبتهم، ففشلها في القيام بذلك يعد انتهاك لالتزامها في منع التصرف، واستنادا للقاعدة

الخامسة من دليل تالين "لا يجوز للدولة ان تسمح بمعرفتها باستخدام البنية التحتية السيبرانية الواقعة في اقليمها او تحت سيطرتها الحكومية ان تستخدم في الاعمال التي تؤثر سلبا وبشكل غير شرعي على الدول الأخرى"

الفرع الثاني

الضرر

الضرر ومفرده الضر، وهو في اللغة ضد النفع، والمضرة خلاف المنفعة [٣٧].

اما في اصطلاح الفقهاء "هو" انتهاك لحق قانوني معين، او مساس بحق او مصلحة مشروعة لاحد اشخاص القانون الدولي "[٣٨].

ويعد الضرر الركن الثاني من اركان المسؤولية، فلكي تتحقق المسؤولية يلزم ان يلحق اتيان الفعل غير المشروع ضررا يلحق بالغير، ويلزم فاعله ان يقوم بإصلاح الضرر، مما يجدر ذكره في هذا الصدد، ان هناك اتجاهين فقهيين بصدد تحقق الضرر كركن في المسؤولية، فيزعم الاتجاه الاول : لأثارة مسؤولية الدولة لا يكفي فقط اتيان فعل غير مشروع، بل لابد ان يتحقق عن هذا الفعل ضرر[٣٩].

اما الاتجاه الاخر فيرى :ان المسؤولية تتحقق بإتيان شخص القانون الدولي السلوك المخالف للالتزام الدولي واثبات نسبته اليه من غير اشتراط تحقق الضرر [٤٠].

ويبدو ان هذا الاتجاه يتوافق مع المشروع النهائي لمسؤولية الدول عن الافعال غير المشروعة دوليا لعام ٢٠٠١، اذ تذهب المادة الاولى منه الى ان " كل فعل غير مشروع دوليا تقوم به الدولة يستتبع مسؤوليتها الدولية"، ففي نطاق التجسس السيبراني على المحفوظات الدبلوماسية فان الضرر المتحقق من التجسس يكون ماديا ومعنويا، فيكون الضرر ماديا عندما يؤدي الولوج الى اجهزة وانظمة الدولة صاحبة الوثائق الى حرق انظمة الامان فيها، وقد يكون الضرر المتحقق معنويا وذلك من خلال اختراق البنية التحتية السيبرانية والاطلاع على اسرار الدولة ومعلوماتها السرية غير المتاحة للجمهور.

المطلب الثاني

اثار المسؤولية الدولية

اذا ما ثبتت المسؤولية الدولية، بأسناد فعل التجسس السيبراني الى الدولة القائمة به، فانه سوف يترتب بذمتها التزاما بجبر الضرر الواقع على الدولة ضحية التجسس، وتتجلى هذه الاثار على النحو الاتي :

الفرع الاول

الكف وعدم التكرار

تناول الفقرة (أ)من المادة ٣٠ من مشروع المسؤولية الدولية الكف وعدم التكرار، ويعد الكف عن التصرف الذي يشكل خرق للالتزام دولي، الشرط الاول لإزالة عواقب التصرف غير المشروع، مع تقديم الضمانات اللازمة بعدم تكراره ، بمقتضى ذلك يتعين على الدولة القائمة بالتجسس ان تكف عن القيام بفعل التجسس هذا وان تقدم الضمانات الكافية بعدم القيام به، وخير دليل على ذلك وكأثر عن المسؤولية عن التجسس السيبراني وان لم يكن على محفوظات الدبلوماسية هي، قضية التجسس الاقتصادي الصيني الامريكي، والتي توصل الطرفان الى عقد اتفاقية ثنائية عام ٢٠١٥(اوباما- شي) بينهما وقد تعهدا بأن لا يقوما باي سلوك او دعم او سرقة الكترونية للممتلكات الفكرية بما في ذلك الاسرار

التجارية وغيرها من المعلومات التجارية السرية من اجل ميزة تجارية [٤١].

الفرع الثاني

الجبر (التعويض)

تشير المادة (٣١) من مشروع مسؤولية الدول، عن التزام الدولة المسؤولة بجبر كامل الخسارة الناجمة عن الفعل غير المشروع دوليا، (والجبر قد يكون عينيا وذلك بأعاده الحال الى ما كان عليه قبل وقوع الفعل، اذا كان ذلك غير مستحيل ماديا، او غير مستتبع لعبء لا يتناسب اطلاقا مع المنفعة المتأتية من الرد بدلا من التعويض)[٤٢].

وبصدد التجسس السيبراني على المحفوظات الدبلوماسية فان الجبر العيني يكون مستحيلا ، وذلك لان الحرمة قد انتهكت وما كان سرا قد اصبح معلوما، الا انه بالإمكان ان يصار الى التعويض النقدي اذا التعويض العيني مستحيلا، ويكون ذلك بمبلغ من المال لتعويض عن الضرر الناتج عن العمل غير المشروع، ويعد هذا السبيل هو الاكثر انتشارا، فعلى خلفية اعلان سلطنة عمان اكتشافها شبكة تجسس اماراتية تابعة لجهاز امن دولة الامارات العربية المتحدة مستهدفة نظام الحكم في عمان والية العمل الحكومي والعسكري [٤٣].

ونتيجة لقيام امير الكويت بالوساطة ما بين الدولتين والتي اسفرت عن قيام الامارات بتحويل مبلغ ٢٠ مليار درهم لحساب السلطان قابوس مباشرة والاستثمار في السلطنة بمبلغ ٢٠ مليار درهم في خمس سنوات [٤٤].

اذ يعد هذا نوع من التعويض النقدي عن الضر عن التجسس

الفرع الثالث

الترضية

تعد الترضية طريق لإصلاح الاضرار غير المادية، وهي من صور التعويض التي يصعب معالجتها بالتعويض بالصور السالفة الذكر، وتكون الترضية في الاضرار المعنوية التي تصيب الدولة بسمعتها وكرامتها او الاعتداء على دبلوماسيتها والترضية تتناسب مع طبيعة العلاقات الدولية بين الدولة المعتمدة والمعتمد لديها، كتقديم الاعتذارات الشفوية والتحريرية ومعاقبة الجناة وطردهم من الوظيفة [٤٥].

وعلى سبيل المثال، ففي حادثة التجسس الاماراتية على سلطنة عمان، وعلى اثر قيام امير الكويت بالمساعي لاحتواء الازمة، فقد اصطحب امير الكويت بن زايد الى السلطنة وتقديمه اعتذار مباشر لسلطان قابوس[٤٦].

وللدولة المتضررة ان تتخذ تدابير مضادة (وهي ردود افعال استخدمت في العلاقات الدبلوماسية كأحد الاجراءات التي تقوم بها الدولة المعتمدة (المضرورة) من خلال تعليق التزاماتها وعلاقتها مع الدولة المسؤولة لغرض اجبارها على الالتزام والامتثال بتعهداتها، وتتخذ الافعال صور مختلفة كقرارات انفرادية او سحب بعثاتها وقطع العلاقات الدبلوماسية، ففي اطار الرد على الهجوم التجسس الالكتروني الروسي على الولايات المتحدة الامريكية عملية Solar Winds)، فرضت الولايات المتحدة عقوبات اقتصادية على روسيا ردا على ما تصفه بهجمات الكترونية، كما طردت البعثة الدبلوماسية الروسية من واشنطن في اجراءات تهدف الى ردع انشطة روسيا الخارجية الضارة [٤٧].

الخاتمة

في نهاية رحلة البحث في (التجسس السيبراني على المحفوظات الدبلوماسية)، تمخضت جملة من الاستنتاجات والمقترحات، والتي هي:

اولا: الاستنتاجات

١. نتيجة لثورة المعلومات التقنية، باتت المعلومات محفوظة الكترونيا، ولما كان الولوج الى تلك الشبكات غير مكلف ويجعل هوية القائم به غير معروفة، سهل الامر للقيام بالتجسس السيبراني على معلومات الدول الاخرى سيما المحفوظات الدبلوماسية.

٢. ولما فقد كان التجسس السيبراني ظاهرة حديثة اختلفت الآراء بصدد مشروعيته من عدمها، وكان لكل اتجاه مبرراته واسانيده، مع الاشارة الى ان الاتجاه الراجح هو عدم المشروعية .

٣. ان المحفوظات الدبلوماسية(ارشيف البعثة) قد تكون ثابتة او متحركة، فالأرشيف الثابت والحقيبة الدبلوماسية يحظى بحماية واردة في اتفاقية فيينا للعلاقات الدبلوماسية لعام ١٩٦١، اما المتحرك (الالكتروني) الذي ترسله الدول عبر شبكات الانترنيت والفضاء وهو محفوظ على محركات الاقراص الثابتة والمحمولة والوسائط الاخرى، والذي يعد جزء من البتية التحتية الالكترونية فهو يحظى بذات الحماية الواردة اعلاه، وان الدولة المستقبلة او دولة المرور، تكون ملزمة بحفظ تلك المحفوظات استنادا الى مبدا العناية الواجبة .

٤. تقوم مسؤولية الدولة المتجسسة نتيجة لقيامها بفعل التجسس الذي يعد فعلا غير مشروع كما تم بيانه في متن البحث، وانها خرقت التزاما دوليا بالحفاظ على حرمة المحفوظات سواء أكان من الدولة المستقبلة ام دولة المرور، وتم اسناد التجسس للدولة، ولا يخفى ان مسألة الاسناد تكتنفه صعوبات فنية وسياسية وقانونية .

ثانيا : المقترحات

١. على كل دولة ان تسعى لتامين البنية التحتية الالكترونية الخاصة بها للحد من التهديد السيبراني، وان تعمل على التعريف الرقمي للأرشيفات والوثائق الدبلوماسية، مثل التسجيل الخاص او استخدام خوادم دبلوماسية مخصصة .

٢. العمل على بناء وتطوير وتعزيز ثقافة الامن السيبراني الوطني، وانشاء وتنسيق برامج التوعية والتثقيف في مجالات الامن السيبراني

٣. تعزيز التعاون بين الدول اذ يعد وسيلة اساسية للتشجيع على اتباع نهج تعاوني شامل يعود بالفائدة على الجميع والحث على المشاركة في المنتديات الدولية والاقليمية للتعاون في مجال الامن السيبراني .

٤. السعي لأبرام اتفاقية دولية تحظر التجسس السيبراني بشكل عام، لما لذلك اثر في حفظ السلم واستقرار العلاقات الدولية، او على الاقل اعتماد بروتوكول انترنيت ملحق لاتفاقية فيينا لعام ١٩٦١، ويوفر توضيحا للمشكلات الحالية مثل حصانة المحفوظات الدبلوماسية المخزونة في سحابة رقمية .

٥. على الدولة المستقبلة اتخاذ خطوات تقنية لتحديد الاصول الرقمية الدبلوماسية من اجل مساعدة شركات الانترنيت على توفير الحماية المحددة للوثائق الدبلوماسية للدول المعتمدة لديها

الهوامش

(١) من المفيد الإشارة اليه ان الشبكات التي يتم من خلالها التجسس السيبراني تنقسم بدورها الى شبكات الانترنيت وشبكات الاتصالات، فشبكة الانترنيت يكون التجسس بها اما عن طريق البريد الالكتروني، اذ يتم مراقبة الرسائل في طريقها عبر الانترنيت او ارسال ملفات على البريد الشخصي للشخص المراد التجسس عليه، فتفتح هذه الملفات ضمن رسالة عادية وغالبا ما تكون مجهولة المصدر، اذ تسمح للمرسل الدخول الى جميع الملفات الموجودة على جهاز الحاسوب او الهاتف المحمول وتتيح امكانية تتبع الشخص وبياناته ، وبذلك يمكن المرسل ان يطلع على جميع اسرار المرسل اليه لمزيد من التفاصيل ينظر علي عدنان الفيل، الاجرام الالكتروني (دراسة مقارنة)، منشورات زين الحقوقية، ٢٠١١ ، ص ٩٧ او البرامج التقنية وهي برامج التي بمجرد اختراقها الكمبيوتر او الشبكة المعلوماتية، بإمكانها ان تسجل كل ما يتم كتابته وكذلك الصوت والتقاط الصور والوصول الى الكثير من البيانات على الشبكة المعلوماتية

Sullivan ،D. ،Phishing Attacks Using Public Data ،2019 Https://resourse.infosecinstitute.com

اما شبكات الاتصال كالكابلات البحرية او ترددات او موجات ارادیو Cyber Espionage and International Law Hart publishing PLC ،2019 ، P.2. Russell Buchan ،

(2)Jose de Armateia da Cruz Stephanie Pedron ، Cyber Mercenaries :Anew Threat to National Security ، International Social Science Review ، Volume 96 ،Issue 2 ،Article 3 .https://digital commons .north Gorgia .ed// issr/vol96/issu2/3

(٣) يقصد بالفضاء السيبراني كما عرفه الاتحاد الدولي للاتصالات ووكالة الامم المتحدة في مجال تكنولوجيا المعلومات والاتصالات بأنه "الحيز المادي وغير المادي، الذي ينشأ او يتكون من جزء او من كل العناصر التالية : حواسيب، اجهزة ممكنة وشبكات ومعلومات محوسبة وبرامج ومضامين ومعطيات مرور ورقابة والذين يستخدمون كل ذلك . نقلا عن خالد وليد محمود، ساحة الصراع الالكتروني الجديدة، سلسلة دراسات ودراسة السياسات، المركز العربي للأبحاث، قطر، ٢٠١٣، ص٤ .

(٤) ففي حادثة حديثة وفي خضم جائحة كورونا اتهمت كل من الولايات المتحدة الامريكية والمملكة المتحدة والحكومة الكندية، دولة روسيا لمحاولتها استخدام الوسائل الالكترونية لسرقة المعلومات الاستخباراتية عن اللقاحات من الجامعات والمؤسسات الصحية الاخرى

William Banks ،Cyber Attribution and State Responsibility ، International Law Studies ،Vol97 ، 2021 ،p.1064

(٥) (دليل تالين) هو دراسة اكاديمية غير ملزمة، اعد من قبل مجموعة دولية من الباحثين، حوالي عشرون خبيرا بدعوة من مركز التميز للدفاع الالكتروني التعاوني التابع لحلف الشمال الاطلسي يطبق على المنازعات الالكترونية والحرب الالكترونية بين عامي ٢٠٠٩-٢٠١٢ ، وتم نشره في نيسان ٢٠١٣ من مطبعة كامبريدج .

Stringfixer .com /ar/t

(٦) من الجدير بالذكر ان هذه النصوص تم نقلها عن ترجمة، علي محمد كاظم، دليل تالين بشأن القانون الدولي المطبق على الحروب السيبرانية، ٢٠١٩، متاح على الانترنيت، تاريخ الزيارة ٢٠ أذار ٢٠٢٢ .

(٧) عبد الاله محمد النوايسة و ممدوح حسن العدوان، جرائم التجسس الالكتروني في التشريع الاردني، مجلة علوم الشريعة والقانون المجلد ٤٦، عدد ١، ٢٠١٩، ص ٤٦٩

C.F.The Mi5،Cyber Threat .available at :https://www.Mi5.gov.U.K/home/theThreat /Cyber.htm.

(٨) محمد سلمان خوالدة، جريمة الدخول غير المشروع الى الموقع الالكتروني او نظام معلوماتي وفق التشريع الاردني، دراسة مقارنة، ط١، دار الثقافة، عمان، ، ٢٠١٢، ص١٣٩.

(٩) محمد الشوابكة، جرائم الحاسوب والانترنيت، الجريمة المعلوماتية، دار الثقافة، عمان، ٢٠٠٩، ص٢٩

(10) Katharina Ziol kwski،Peacetime Regim for Activities In CyberSpeace، international Law، International Relations And Diplomacy،CCDCOE،2013،p.429.

(١١) مريم احمد لوكال، التجسس في ضوء أحكام القانون الدولي العام، المجلة العربية للدراسات الامنية، جامعة نايف للعلوم الامنية، المجلد ٣٥، العدد٢، ٢٠١٩، ص٢٦٦.

(١٢) د. محمد عادل محمد عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسس وقت السلم "دراسة على ضوء دليل تالين بشأن القانون الدولي المطبق على العمليات السيبرانية ٢٠١٣-٢٠١٧"بدون طبعة، ٢٠٠٩، ص٤٠٧.

(13)Inaki Navarrete &Russell Buchant،Out of The Legal Wilderness:Peacetime Espionage، International Law and The Existence of Customary Exceptions،Cornell International Law Journal .Vol 51،2019،p. 923

(١٤) د. جمال محمد الحبيشي، الاضرار الناجمة عن بعض الاجسام الفضائية (دراسة قانونية)، مجلة جامعة الجزيرة، المجلد الاول، العدد الاول، ٢٠١٨، ص ٢٥٦.و ينظر د. محمد سعادي، اثر التكنولوجيا المستحدثة على القانون الدولي العام، دار الجامعة الجديد، ٢٠١٤، ص ١٢٧.

(١٥) د. محمد عادل محمد عسكر، مصدر السابق، ص ٣٨٨.

(١٦) عبير علي عبد العزيز شري، مشروعية التجسس عبر الاقمار الصناعية في القانون الدولي، مجلة جامعة الانبار للعلوم القانونية والسياسية، المجلد التاسع، العدد الثاني، ٢٠١٩، ص٨٠٤

(١٧) محمد عادل محمد عسكر، مصدر سابق، ص٣٧٤

(١٨) البند (ك)من الفقرة الاولى من المادة الاولى من اتفاقية فيينا للعلاقات القنصلية لعام ١٩٦٣.

(١٩) د. محمد المجذوب، القانون الدولي العام، ط٧، منشورات الحلبي الحقوقية، بيروت، لبنان، ٢٠٠٧، ص ٧٤١-٧٤٢.

(٢٠) د. غازي حسن صباريني، الدبلوماسية المعاصرة، ط١، دار الثقافة للنشر والتوزيع، عمان، الاردن، ٢٠٠٩، ص١٤٢

(٢١) ينظر في ذلك م/ ٢٢من اتفاقية فيينا للعلاقات الدبلوماسية لعام ١٩٦١وكذلك م/ ٣١من اتفاقية فيينا للعلاقات القنصلية لعام ١٩٦٣

(٢٢) ينظر م/ ٢٤و ف/ ٢من م/ ٢٧ و ف٣من م/ ٤٠من اتفاقية فيينا للعلاقات الدبلوماسية ١٩٦١، وكذلك م/ ٣٣، و ف/ ٢من م/ ٣٥و ف/ ٣من م/ ٥٤من اتفاقية فيينا للعلاقات القنصلية لعام ١٩٦٣.

(24) Inaki Navarrete &Russell Buchant، OP.CIT. ،P 910

(25)Robert Mc Corquodale، Wikileaks Documents are Admissible in A Domestic Court، Blog of European Journal of International Law ، 2018 ،ejiltalk.org/wikileaks .

(٢٦) د. فاوي الملاح، سلطات الامن والحصانات والامتيازات في الواقع النظري والعملي مقارنا بالشريعة الاسلامية، دار المطبوعات الجامعية، الاسكندرية، ١٩٩٣، ص٤٥

(٢٧) الامم المتحدة، الجمعية العامة، حولية لجنة القانون الدولي، المجلد الثاني، الجزء الثاني، الدورة ٥٣، لعام ٢٠٠١، A/CN.4/SER.A/2001/Add.1(part2)

(٢٨) ينظر م/ ٣ من مشروع مسؤولية الدول عن الافعال غير المشروعة دوليا .

(29) Barrie Sander،The Sound of Silence :International Law and the Governance of Peacetime Cyber Operations ، 2019 11th International Conference on Cyber Conflict pp.371-373،Electronic copy available at :https://ssrn.com/abstract=3411907.

(30) Eric Talbot Jenesen،Tallinn Manual 2.0 High Lights in Sights،Georgetown Journal of Internsational Law ،2017 ،p 762 ،Katharina Ziolkowski ، Op.cit.p ،416.

(٣١) ينظر ف/ أ من م/ ٤٥ من اتفاقية فيينا للعلاقات الدبلوماسية لعام ١٩٦١ وكذلك ف/ ١ من م/ ٢٧ من اتفاقية فيينا للعلاقات القنصلية لعام ١٩٦٣ .

(٣٢) من المفيد ذكره ان توماس بوسرت مستشار الامن الداخلي بالبيت الابيض صرح ان وزارة الخارجية الامريكية لاتقدم الادعاء بدون تقديم ادلة على ضلوع (بارك جين هيوك) بالتجسس لذا فأن الخزانة الامريكية في الولايات المتحدة قد عاقبت (بارك جين هيوك)المواطن الكوري الشمالي الذي كان يعمل في فريق اختراق ترعاه الحكومة لدعم الاجراءات السيبرانية الخبيثة . الاخرى

William Banks OP.CITE. ،p.1064

(33) Ibide. ،p.1065.

(٣٤) William Banks، OP.CIT. ، p.1052. ، ان نتائج الاسناد غير الفني هي ذات جودة مشكوك بها، اذ يمكن ان تكون نتاج تقييم شخصي وبالتالي فهي غير متناسبة في تحديد المسؤولية القانونية وبالتالي فان التدابير المستندة الى تلك التقييمات تكون غير قانونية، وعليه فان من الضرورة بمكان ان تظل الدولة المضرورة في حدود القانون وان اي اسناد يجب تقييمه مقابل الاطار القانوني

Andraz Kastelic ،Including Compliance with International Law in Cyberspace –State Responsibility ، Counter measures and The Obligations of Due diligence ، Thesis ،University Of Sheffield School Of Law ،2019 ،p.128.

(35) Joe Devanny ، Ciaran Martin &Tim Stevens ، On The Strategic Consequences Of Digital Espionag e ، Journal Of Cyber Policy ، Routledge Taylor&Francis Group ،2021 ، p.6

(36) Barrie Sender ،OP.CIT. ،368

(٣٧) الرافعي احمد بن علي المقري القيومي، المصباح المنير في غريب الشرح الكبير، المكتبة العلمية، بيروت .

(٣٨) د. جعفر عبد السلام، مبادى القانون الدولي العام، ط٢، دار النهضة العربية، ١٩٨٦، ص٢٤٥ .

(٣٩) علي صادق ابو هيف، القانون الدولي العام، ط١، منشأة المعارف، الاسكندرية، مصر، بدون سنة طبع، ص٢٥٧.

(٤٠) محمد صافي يوسف، القانون الدولي، دار النهضة العربية، القاهرة، مصر، ٢٠١٩، ص٣٦٩ .

(41) Joe Devanny ، Ciaran Martin &Tim Steven .OP.CIT. p.9

(٤٢) الجمعية العامة، الدورة السادسة والخمسون، البند ١٦٢(تقرير لجنة القانون الدولي عن اعمال دورتها الثالثة والخمسين، تقرير اللجنة السادسة)في ٢٨/ ١١/ ٢٠٠١.A/56/689

(٤٣) تفكيك شبكة تجسس اماراتية تستهدف نظام الحكم، الشرق الاوسط، France 24.com /ar/20110130

(٤٤) سلطنة عمان تعلن الكشف عن خلية تجسس امارتية داخل قصر السلطان قابوس والقبض عليهم، الصدى الصحيفة الالكترونية، ٢٠١٣، ESSAD.NET

(٤٥) مسلم طاهر حسون الحسيني، حماية مقر البعثة الدبلوماسية في القانون الدولي، رسالة ماجستير، كلية القانون / جامعة كربلاء، ٢٠١٦، ص١٠٩

(٤٦) جواسيس ابو ظبي في عمان ..هل يعتذر" بن زايد" عن خيانة عهده مع السلطان قابوس، الشرق / ١٢نيسان ٢٠١٩ M.al-sharq.com/art..

(47)Joe Devanny ، Ciaran Martin &Tim Stevensm ،OP.CIT. ،P.10 .

المصادر

اولا :المراجع باللغة العربية

أ: **الكتب**

١. الرافعي احمد علي المقري القيومي، المصباح المنير في غريب الشرح الكبير، المكتبة العلمية، بيروت .

٢. د.جعفر عبد السلام، مبادئ القانون الدولي العام، ط٣، دار النهضة العربية، ١٩٨٦.

٣. خالد وليد محمود، ساحة الصراع الالكتروني الجديدة، سلسلة دراسات ودراسة السياسات، المركز العربي للأبحاث، قطر، ٢٠١٣.

٤. علي عدنان الفيل، الاجرام الالكتروني (دراسة مقارنة)، ط١، منشورات زين الحقوقية، ٢٠١١.

٥. د.علي صادق ابو وهيف، القانون الدولي، ط١منشاة المعارف الاسكندرية، مصر، بدون سنة طبع.

٦. د.غازي حسن صباريني، الدبلوماسية المعاصرة، ط١، دار الثقافة للنشر والتوزيع، عمان، الاردن، ٢٠٠٩.

٧. د.فاوي الملاح، سلطات الامن والحصانات والامتيازات في الواقع النظري والعملي مقارنا بالشريعة الاسلامية، دار المطبوعات الجامعية، الاسكندرية، ١٩٩٣ .

٨. د. محمد المجذوب، القانون الدولي العام، ط٧، منشورات الحلبي الحقوقية، بيروت، لبنان، ٢٠٠٧ .

٩. محمد الشوابكة، جرائم الحاسوب والانترنيت: (الجريمة المعلوماتية)، دار الثقافة، عمان، ٢٠٠٩.

١٠. د. محمد عادل عسكر، وضع العمليات السيبرانية في القانون الدولي مع التطبيق على ممارسة التجسس وقت السلم، دراسة على ضوء دليل تالين بشأن القانون المطبق على العمليات السيبرانية، ٢٠١٣.-٢٠١٧، بدون طبعة، ٢٠٠٩ .

١١. د. محمد سعادي، اثر التكنولوجيا المستخدمة على القانون الدولي العام، دار الجامعة الجديدة، ٢٠١٤.

١٢. محمد سلمان خوالدة، جريمة الدخول غير المشروع الى الموقع الالكتروني او نظام معلوماتي وفق التشريع الاردني، دراسة مقارنة، ط١، دار الثقافة، عمان، ٢٠١٢.

١٣. محمد صافي يوسف، القانون الدولي، دار النهضة العربية، القاهرة، مصر، ٢٠١٩.

ب: الرسائل

١. مسلم طاهر حسون الحسيني، حماية مقر البعثة الدبلوماسية في القانون الدولي، رسالة ماجستير، كلية القانون، جامعة كربلاء، ٢٠١٦

ج: المجلات والدوريات

١. د. جمال محمد الحبيشي، الاضرار الناجمة عن بعض الاجسام الفضائية (دراسة قانونية)، مجلة جامعة الجزيرة، المجلد الاول، العدد الاول، ٢٠١٨.

٢.عبد الاله محمد النوايسة ومحمد حسن العدوان، جرائم التجسس الالكتروني في التشريع الاردني، مجلة علوم الشريعة والقانون، المجلد ٤٦ عدد١، ٢٠١٩.

٣. عبير علي عبد العزيز شري، مشروعية التجسس عبر الاقمار الصناعية في القانون الدولي، مجلة جامعة الانبار للعلوم القانونية والسياسية، المجلد التاسع، العدد الثاني، ٢٠١٩ .

٤. مريم جمال لوكال، التجسس في ضوء احكام القانون الدولي العام، المجلة العربية للدراسة الامنية، جامعة نايف للعلوم الامنية، المجلد ٣٥، العدد ٢، ٢٠١٩ .

خ : الاتفاقيات والوثائق الدولية

٣. ميثاق الامم المتحدة ١٩٤٥.

٤. اتفاقية فيينا للعلاقات الدبلوماسية ١٩٦١.

٥. اتفاقية فيينا للعلاقات القنصلية ١٩٦٣.

٦. اتفاقية الفضاء الخارجي ١٩٧٦

٧. اتفاقية قانون البحار لعام ١٩٨٢

٨. الامم المتحدة، الجمعية العامة، حولية لجنة القانون الدولي، المجلد الثاني، الجزء الثاني، الدورة ٥٣، ٢٠٠١ A/CN.4/SER.A/2001/Add.1(part2)

٩. الجمعية العامة، الدورة السادسة والخمسون، البند ١٦٢ (تقرير لجنة القانون الدولي)عن اعمال دورتها الثالثة والخمسون، تقرير اللجنة السادسة، ٢٠٠١ .A/56/689

ثانيا :المراجع باللغة الانكليزية

A:.Books

1. Katharina Ziol kwski,Peacetime Regim for Activities In CyberSpeace ،international Law ،International Relations And Diplomacy ،CCDCOE,2013 .

B.::Thesis.

1. Andraz Kastelic,Including Compliance with International Law In cyber PaceTime State Responsibilty ، Counter Measures and the Obligations Of Due Diligences ،Thesis,University Of Sheffield SCHOOL of Law ،2019.

C:Reserchers

1. Eric Talbot Jensen ،Tallinn Manual2.0 Hights in Sights ،GeorgetownJournual of International Law ،2017
2. .InakiNavarrete&Russell Bacchant ،Out of The Legal Wildernese: Peacetime Espionage ،International Law and The Exceptions ،Cornell International LawJournual ، vol 51,2019.
3. JoeDevanny,Ciaran Martin &Time Stevens ،on Strategic Consequences of Digital Espionage ،Journal of Cyber Policy ،Routleduge Taylor&Francis Croup,2021.
4. Jose de Armateia da Cruz Stephanie Pedron ،Cyber Mercenaries:Anew Threat to National Security ، International Social ScienceReview,Volume96,Issue2 ،Artical3,https;digital commons ،north Gorgia.ed//ed//issr/vol96/issu2/3.
5. Robert Mc Corquodale ،Wikileaks Documents are Admissible in Adomestic Court ،Blog Of Europan Journal of I nternational Law ،201`8,Ejiltal;.org/Wikileaks.
6. William Banks ،Cyber Attribution and State Responsibility ،International LawStudies ،Vol 91,2021.

ثالثا : مواقع الانترنيت

سلطنة عمان تعلن الكشف عن خلية تجسس اماراتية داخل قصر السلطان قابوس والقبض عليهم، الصدى الصحيفة الالكترونية، ٢٠١٣ .Essad.net

جواسيس ابو ظبي في عمان، هل يعتذر بن زايد عن خيانته عهده مع السلطان قابوس، الشرق ١٢ نيسان، ٢٠١٩ .M.al-Sharq,com /art

علي محمد كاظم، دليل تالين بشان القانون الدولي المطبق على الحروب السيبرانية، ٢٠١٩، متاح على الانترنيت .

تفكيك شبكة تجسس اماراتية تستهدف نظام الحكم / الشرق الاوسط .France29.com/ar/20110130

Barrie Sander ،The Sound Of S ilence:I nternational Law and Governance of Peace time Cyber Operations,2019,11th International Conference On Cyber Conflict ، https://com/abstract=3411007

Cyber Espionage and Russell Buchan ،International Law ،Hart Publihshing.2014.