الاتجاهات الجديدة في القانون الدولي للجوسسة الالكترونية(مستل)

أ.د. طلعت جياد لجي الحديدي
كلية القانون والعلوم السياسية / جامعة كركوك
سعد احمد ميدان المفرجي

Trends In The International Law Of Electronic Espionage Quoted

Prof. Dr. Talaat Jiyad Legy Al Hadidi
College of Law and Political Science/University of Kirkuk
Saad Ahmed Medan Al-Mafraji

المستخلص

الجوسسة في زمن السلم قديمة قدم البشرية, اما الجوسسة الالكترونية فإنها تماماً مثل نظيرتها التقليدية, تنطوي على عمليات اقتحام غير مصرح بها, ويتم استغلال على سبيل المثال نقاط الضعف الامنية لكي تتجاوز الخوادم المشفرة والوصول الى البيانات التابعة للدول والشركات والسفارات والوكالات الحكومية وحتى الافراد, واحد الاختلافات الرئيسية عن الجوسسة التقليدية هي الاستقلالية الجغرافية والمادية العالية التي تتمتع بها الجوسسة الالكترونية, ذلك يعني انه في حالة الجوسسة على بيانات وكالة تابعة لدولة اخرى ؛ ليس هناك حاجة الى وجود شخص مادي او جهاز في الحالة المستهدفة, ويستخدم بدلاً من ذلك الاوامر الصادرة من اي مكان وبالتالي يمكن ارتكاب اعمال الجوسسة الالكترونية بغض النظر عن حدود الدولة .

كما ان ظهور الجوسسة الالكترونية قد غيرت الصورة وتحولت الى الجوسسة بدوافع اقتصادية باعتبارها ذات صلة بالأمن القومي, واثبت الواقع الحالي الذي تعيشه الدول ان المعلومات في بعض الأوقات يكون لها قدراً من السرية المطلوبة, والذي يترتب على تداولها أو سرقتها أو العبث بها أو انتقالها وانتشارها نوع من المخاطر, وتتفاوت اهمية تلك المعلومات كونها ليست كلها على نفس الدرجة من الاهمية, لان البعض منها اذا انتقلت للغير ينتج عنها اضراراً شديدة, ولا يتصور هذا الفرض الاخير الا اذا كانت

المعلومة تشكل خطراً على الأمن القومي للدولة, وان العمليات الالكترونية التي تخترق شبكات وانظمة الحواسيب المدعومة بالبنية التحتية الالكترونية الموجودة داخل اراضي دولة اخرى تؤدي الى انتهاك قاعدة السيادة الاقليمية, كما انها تعد خرقاً لمبدأ عدم التدخل في الشؤون الداخلية للدول, بغض النظر عما اذا كانت تلك البنية التحتية الالكترونية يتم تشغيلها من قبل اجهزة الدولة او الجهات الفاعلة الخاصة, وبالتالي فإن حكم السيادة الاقليمية يوفر مصدراً مهماً وقوياً للحماية القانونية ضد الجوسسة الالكترونية .

الكلمات المفتاحية: الجوسسة, القانون الدولي, الالكترونية

Abstract

Espionage in peacetime is as old as humanity, and electronic espionage, just like its traditional counterpart, involves unauthorized intrusions, and security vulnerabilities are exploited, for example, to bypass encrypted servers and access data belonging to countries, companies, embassies, government agencies and even individuals, one The main differences from traditional espionage are the high geographical and physical independence that electronic espionage enjoys, which means that in the case of espionage on the data of an agency of another country; There is no need to have a physical person or device in the target state, and instead uses orders issued from anywhere and thus electronic espionage can be committed regardless of state borders.

The emergence of electronic espionage has changed the picture and turned to espionage with economic motives as it is related to national security, and the current reality in which countries live has proven that information at times has a degree of confidentiality required, which results in its circulation, theft, tampering, transmission and spread of a kind There are risks, and the importance of this information varies, as not all of them are of equal importance, because if some of them are transmitted to others, they will result in severe damage. Computers backed by electronic infrastructure located within the territory of another

state lead to a violation of the rule of territorial sovereignty, and it is also a violation of the principle of non-interference in the internal affairs of states, regardless of whether that electronic infrastructure is operated by state agencies or private actors, and therefore The rule of regional sovereignty provides an important and powerful source of legal protection against electronic espionage.

Keywords: Espionage, international law, electronic

المقدمـــة

الجوسسة ظاهرة قديمة قدم البشرية, وتعد ثاني اقدم مهنة في العالم, في الماضي كانت الاستخبارات البشرية الاكثر اعتماداً, وقد تطورت هذه الظاهرة شأنها شأن الكثير من الممارسات مع تطور التكنولوجيا ووسائل الاتصال, ويمكن القول ان التقدم التقني والرقمي ساعد في تطور عمليات الجوسسة والتنصت التي تمثل بدورها الوجه الاخر من الاستخدامات السيئة والضارة للتقنيات الحديثة, وان الجوسسة بين الدول ليست بالظاهرة الجديدة, لكن في العقود القليلة الماضية انتقل العالم الى عالم جديد تماماً من الجوسسة الالكترونية, وهو الشكل الجديد من الجوسسة الواقعية الذي له التأثير السلبي الواضح على العلاقات الاقتصادية والسياسية بين الدول القومية, بالإضافة الى تغيير شكل الحرب الحديثة وعلى الرغم من المزايا التي توفرها التكنولوجيا الحديثة, هناك مجموعة جديدة من المشاكل التي لها انعكاساتها على الامن القومي .

والاجراءات الالكترونية الخبيثة التي تؤثر على سبيل المثال على البنية التحتية المعلوماتية او على الامن القومي, يمكن ان تتم من خلال التدخلات الالكترونية او الاختراق الالكتروني الذي يوصف على انه اختراق للامن او التحايل عليه, ويتم ذلك على سبيل المثال من خلال اختراق جدار الحماية او القيام بذلك بالوسائل التقنية .

ولم تعد الجوسسة الالكترونية مقتصرة على النواحي العسكرية والحربية, وانما اصبحت شاملة لمختلف المجالات, ومن المعلوم ان الهدف الرئيسي من انشطة الجوسسة هو الحصول على المعلومات التي تكون سرية ومهمة في نفس الوقت, ولكن لا تمتلك الجهة المتجسسة التصريح الذي يخولها من الاطلاع او الحصول على هذه المعلومات,

والمعلومة تنقسم الى عدة انواع, يصب جمعها في نوع واحد لتعلقها بكافة مواضيعها بملفات الدولة .

من خلال ذلك لابد لنا من تسليط الضوء على اتجاهات الجوسسة الجديدة التي تبناها القانون الدولي في تعامله مع الجوسسة الالكترونية, كونها قد سايرت بموضوعات تدخل في صميم القانون الدولي, منها مبدأ حقوق الانسان ومبدأ السيادة الاقليمية ومبدأ عدم التخل ومبدأ استخدام القوة والهجوم المسلح, وغيرها من الموضوعات التي يتداخل فيها الاختصاص الداخلي مع الدولي كموضوع الامن القومي .

اولاً : اهمية الموضوع: يعد موضوع الجوسسة الالكترونية من الموضوعات المهمة, والتي تحتاج الى توضيح كونها تستلزم معالجة خاصة لمواجهة او محاولة الحد من مخاطرها وتقليل مقدار الضرر المترتب عليها, وكون الاثار والنتائج المترتبة عليها تتعدى الى الاضرار بمصالح كثيرة, إضافة انها تعد من الانشطة الخطيرة في الوقت الحاضر, وهي من الافعال العابرة للحدود والتي تهدد الدول والمنظمات والشركات وتنتهك حرمة الحياة الخاصة للافراد, فضلاً عن حجم الاثار والاضرار التي تخلفها, وانعكست بشكل واضح من خلال التطورات التكنولوجية التي طالت جميع مناحي الحياة, واثرها على مفهوم امن الدولة, حيث اصبحت مصالح الدول والشركات والمنظمات والافراد مهددة بصورة تقف معها القوانين الدولية قاصرة عن مواكبة سرعة التطور وسهولة الحصول على المعلومات منها, ذلك لسهولة الاتصالات والوسائل التكنولوجية الحديثة المتمثلة بالوسائل الالكترونية كالانترنت وتقنية المعلومات, والاقمار الصناعية

ثانياً : اشكالية الموضوع : تتلخص اشكالية الموضوع بعدم وجود تعريف جامع للجوسسة الالكترونية الدولية متفق عليه, اي انه يعتبر قصوراً على المستوى الدولي, كما تتمحور اشكالية الموضوع في مدى تأثير الجوسسة الالكترونية وخطورتها على الصعيد الداخلي والخارجي للدول, وما لها من تأثيرات وانعكاسات سلبية على الامن القومي و على حقوق الانسان الذي اقرته اغلب الدساتير العالمية والقوانين الدولية والوطنية .

ثالثاً : اسباب اختيار الموضوع :من اسباب اختيار هذا الموضوع, لحداثته والذي يستحق بذل الجهد للبحث فيه, ويعد من الظواهر المتعددة الابعاد وعميق عمق المخاطر والاضرار التي يسببها وعمق الشبكة التي يعتمد عليها, كذلك كونه من المواضيع التي شغلت اهتمام الرأي العام العالمي والاقليمي .

رابعاً : منهجية البحث: من اجل الوصول الى النتائج المتوخاة من الدراسة فاننا اتبعنا المنهج الموضوعي لبيان ماهية الجوسسة الالكترونية وصورها, كما نحاول ان نستخدم المنهج الوصفي التحليلي من خلال وصف مفهوم الجوسسة بشكل عام, والجوسسة الالكترونية بشكل خاص

خامساً : هيكلية البحث : سوف نقسم موضوع بحثنا الى ثلاثة مباحث

المبحث الاول : سنوضح فيه ماهية الجوسسة الالكترونية وصورها من خلال مطلبين, الاول لمفهوم الجوسسة الالكترونية والثاني لبيان صور الجوسسة الالكترونية .

اما المبحث الثاني سنخصصه لصلة الجوسسة الالكترونية بالأمن القومي وحقوق الانسان ومن خلال مطلبين, الاول منه لصلة الجوسسة الالكترونية بالأمن القومي, والثاني للحديث عن الجوسسة الالكترونية وحقوق الانسان .

والمبحث الثالث هو تفسيرات القانون الدولي الناشئة للجوسسة الالكترونية ويتكون من ثلاثة مطالب, الاول هو الجوسسة الالكترونية كتهديد او استخدام للقوة وهجوم مسلح, اما الثاني هو الجوسسة الالكترونية باعتبارها انتهاكاً للسيادة الاقليمية والاخير للجوسسة الالكترونية ومبدأ عدم التدخل, والخاتمة .

المبحث الاول

ماهية الجوسسة الالكترونية وصورها

يعد مصطلح الجوسسة الالكترونية احد منتجات التحول الى العصر الرقمي وعملية تحديد مدلوله لازالت في بداياتها, بحيث يتم الخلط غالباً بين الجوسسة التي تمس الدول وبين تلك التي تمس المنظمات او المؤسسات او الافراد, واصبحت الجوسسة الالكترونية الهاجس الاخطر للدولة ولا سيما بعد الانتشار السريع والواسع لوسائل تقنية الاتصالات وتكنولوجيا المعلومات التي اخذت مكانها المتقدم في استخدامات الدول

والافراد على حد سواء, وعليه فان عملية تحديد مفهوم الجوسسة الالكترونية تعد اساسية وذات اهمية بالغة, ومن اجل تناول ماهية الجوسسة الالكترونية سنتناول مفهوم الجوسسة الالكترونية في المطلب الاول, ثم نبين صورها في المطلب الثاني وكما يلي:

المطلب الاول

مفهوم الجوسسة الالكترونية

قبل الولوج الى مفهوم الجوسسة الالكترونية يقتضي بيان المفهوم العام للجوسسة ومن ثم توضيح المقصود بالجوسسة الالكترونية .

وللإحاطة بموضوع الجوسسة يتطلب التعريف بمفردات الموضوع بشكل مفصل وذلك طبقاً لما ورد في تعاريف الفقهاء والباحثين وفي امهات الكتب, اصطلاحا وقانوناً, والبحث فيها امر ضروري لكي تساعد على اكمال الصورة لدى القارئ الكريم, وسيتم التطرق لهذا المفهوم من خلال بيان المحاولات الفقهية في تعريف الجوسسة في الفرع الاول, ومن بعدها نتكلم عن الجوسسة في الاصطلاح القانوني في الفرع الثاني, وخصصنا الفرع الثالث لبيان تعريف الجوسسة الالكترونية وبالتفصيل الاتي :

الفرع الاول

المحاولات الفقهية في تعريف الجوسسة

لقد حظيت ظاهرة الجوسسة كماً هائلاً من التعريفات يمكن القول انه لم تحظ أي ظاهرة اخرى قدرها, ومع ذلك لم تفلح هذه الجهود التي بذلت في تحقيق الهدف ! الا وهو الخروج بتعريف شامل وموحد ومانع لهذه الظاهرة, لذلك يتبين انه كل من عرف الجوسسة ينظر اليها من الزاوية التي ينظر منها الى هذه الظاهرة, لذلك سوف نتناول البعض من التعريفات للتعرف على قرب مفهوم هذه الظاهرة ومعرفة جوهرها .

فمن فقهاء الغرب عرفها الاستاذ (روبير ديتوربيه) بأنها " البحث عن أي نوع من المعلومات, خفية عن دولة معينة بهدف ايصالها لدولة أجنبية وذلك بنية الاضرار

بالدولة المتجسس عليها [١], يبدو واضحا ان تعريف الاستاذ روبير يجعل الجوسسة في نطاق ضيق اي عن طريق البحث عن المعلومات, لكن المعلومات يمكن ان يتم البحث عنها وكذلك يمكن ان يتم الحصول عليها دون البحث .

اما العلامة (رينيه جارو) فان الجوسسة بالنسبة له " تتمثل في الحصول او تجميع معلومات سرية حول السياسة والمواد العسكرية والتنظيم الدفاعي او الهجومي لدولة اجنبية وتسليم هذه المعلومات الى حكومة اجنبية اخرى او لمن يعمل لحسابها بمقابل او مجانا "[٢] .

ومن الفقهاء العرب نجد ان الدكتور (مجدي محمود حافظ) عرف الجوسسة بأنها " سعي اي شخص اجنبي صوب الحصول على اسرار الدولة أو تسليمها لأي جهة خارجية متى كان ذلك يؤدي الى الاضرار بمصلحة الدولة " [٣] .

ونستنتج من التعريفات السابقة ان مصطلح الجوسسة يقصد به عملية البحث والتفتيش او جمع او محاولة الحصول وبطريقة سرية على معلومات تكون مخفية, لصالح دولة الجاسوس او تسليمها لدولة اخرى بمقابل او بدون مقابل, و تؤدي الى الاضرار بالدولة المتجسس عليها او عدم الاضرار بها, وسواء حصل الغرض من هذه العملية او لم يحصل, ومن الممكن ان تتعلق هذه المعلومات بالوضع العسكري او الامني او الوضع الاقتصادي او العلمي او التقني او السياسي او الاجتماعي او غيره .

الفرع الثاني

الجوسسة في الاصطلاح القانوني

سوف نبين في هذا الفرع تعريف الجوسسة او الجاسوس في الاصطلاح القانوني على المستوى الدولي وعلى المستوى الوطني وبالتفصيل الاتي :

---

(١) د. محمود سليمان موسى, التجسس الدولي والحماية الجنائية للدفاع الوطني وأمن الدولة, دراسة مقارنة في التشريعات العربية والقانونين الفرنسي والايطالي, الطبعة الاولى, منشأة المعارف, الاسكندرية, ٢٠٠١, ص٩٢.

(٢) د. محمود سليمان موسى, مرجع سابق, ص ٩٧ .

(٣) د. مجدي محمود محب حافظ, موسوعة جرائم الخيانة والتجسس, الطبعة الاولى, المركز القومي للاصدارات القانونية, القاهرة, ٢٠٠٨, ص ٣١٠.

اولا : على المستوى الدولي: اما بالنسبة لتعريف الجوسسة عند فقهاء القانون الدولي, فقد اختلفوا في تحديده, فجانب من الفقه اعتبروا ان القانون الدولي يبيح اعمال الجوسسة في زمن السلم والحرب, والجانب الاخر يعتبر موقف القانون الدولي لا يبيح اعمال الجوسسة في اوقات السلم, خاصةً إن كانت الوسائل المستخدمة في انشطة الجوسسة مخالفة لقواعد القانون الدولي .

واثار تعريف الجوسسة على مستوى الفقه والممارسة الدوليين خلافاً بخصوص الجوسسة وقت السلم والجوسسة وقت الحرب, بالنسبة للجوسسة وقت الحرب عرفتها المادة ٢٩ من اتفاقية لاهاي[١] لعام ١٩٠٧ بأنها "واقعة تهدف الى جمع المعلومات بطريقة سرية تتم في منطقة الاعمال الحربية المعادية "[٢].

كما عرفت المادة ٢٣ من معاهدة لاهاي لسنة ١٩٠٧ الجاسوس بأنه " الشخص الذي يعمل في خفية او تحت ستار ومظهر كاذب في جمع او في محاولة جمع معلومات في منطقة الاعمال الحربية لإحدى الدول المحاربة بقصد ايصال هذه المعلومات لدولة العدو " [٣], كذلك ورد تعريف الجاسوس في المادة ٤٦ من بروتوكول ١٩٧٧ الملحق باتفاقيات جنيف لعام ١٩٤٩ بأنه " ذلك الذي يجمع او يحاول جمع معلومات ذات قيمة عسكرية, وذلك في الخفاء او باستعمال الغش والخداع " [٤] .

ثانيا : على المستوى الوطني

١ :- الجوسسة في التشريعات العربية: تتضمن جميع قوانين الدول وتشريعاتها نصوصا تجعل من التجسس نشاطا محرما, وتصفه ضمن الجرائم الجنائية, والسبب في ذلك يعود الى مدى خطورته, ولم يتطرق المشرع العراقي بصورة مباشرة لتعريف التجسس بصورته التقليدية, شأنه شأن اغلب تشريعات الدول العربية الاخرى امثال

(١) الاتفاقية الخاصة باحترام قوانين واعراف الحرب البرية - معاهدات لاهاي, ١٨ اكتوبر / تشرين الاول ١٩٠٧.

(٢) د. مجدي محمود محب حافظ, المرجع نفسه, ص ٣٤٩-٣٥٠ .

(٣) محمد راكان الدغمي, التجسس واحكامه في الشريعة الاسلامية, الطبعة الثانية, دار السلام للطباعة والنشر والتوزيع, القاهرة, ١٩٨٥, ص ٢٩ ؛ د. مجدي محمود محب حافظ, مرجع سابق, ص ٣٤٧

(٤) عبدالرحمن لحرش, التجسس والحصانة الدبلوماسية, مجلة الحقوق, جامعة الكويت, المجلد ٢٧, العدد ٤, ٢٠٠٣, ص ١٧٩ .

القانون المصري والقانون السوري والقانون الليبي وغيرها التي لم تضع تعريفا خاصا بالتجسس, ويمكن القول انها تركت هذه المهمة اي تعريف التجسس للقضاء والفقه, او اعتمادا على ان طبيعة التجسس متغيرة ومتجددة ومتشعبة, فضلاً انها في حالة تطور مستمر, بالرغم انهم حرصوا على تسمية مختلف الجرائم المضرة بكيان الدولة, واكتفوا بتحديد الافعال والصور التي تدخل في تكوين جريمة التجسس(١).

والمشرع العراقي تناول الافعال التي تدخل في نطاق جرائم التجسس في المواد التي نص عليها قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩, ففي اطار الجوسسة التي تمس امن الدولة, نصت على تجريم السعي لدى احد الدول الاجنبية او التخابر, بأنه " يعاقب بالإعدام او السجن المؤبد كل من سعى لدى دولة اجنبية او تخابر معها او مع احد ممن يعملون لمصلحتها للقيام بأعمال عدائية ضد العراق قد تؤدي الى الحرب او الى قطع العلاقات السياسية او دبر لها الوسائل المؤدية الى ذلك " (٢) .

كذلك جرمت افعال السعي او التخابر لدى احد الدول الاجنبية المعادية, حيث نصت على انه " يعاقب بالإعدام كل من سعى لدى دولة اجنبية معادية او تخابر معها او مع احد ممن يعملون لمصلحتها لمعاونتها في عملياتها الحربية ضد العراق او الاضرار بالعمليات الحربية لجمهورية العراق وكل من دبرلها الوسائل المؤدية الى ذلك او عاونها بأي وجه على نجاح عملياتها الحربية " (٣)، يتبين ان التشريع العراقي لم يعرف جريمة التجسس في نصوص قانون العقوبات العراقي, وانما اكتفى بتحديد الافعال التي يعتبر مرتكبها جاسوساً, ولم يطلق عليها لفظ التجسس (٤) .

٢ :- **الجوسسة في التشريعات الغربية:** لقد ورد تعريف الجوسسة في بعض التشريعات الداخلية كما هو الحال في القانون السوفيتي (سابقاً), وذلك في المادة (٢) الذي اعتبر ان " الجوسسة هي فعل سرقة او جمع معلومة تمثل سر دولة او سرا عسكريا لغرض احالتها لدولة اجنبية او لأجهزة استخباراتية اجنبية او لوكلائها الذين

(١) د. محمود سليمان موسى, مرجع سابق, ص ١١٥-١١٧.
(٢) المادة (١٥٨) من قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩ المعدل .
(٣) المادة (١٥٩) من قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩ المعدل .
(٤) المواد (١٦٤, ١٧٧, ١٧٨) من قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩ المعدل .

يقدمون المعلومات الذي تمثل سرا للدولة او الجيش او المعلومات التي يتم الحصول عليها من بعثات الخدمة السرية الاجنبية من جهات اخرى تنفيذا لمهام تصب في مصالح سرية اجنبية بغية استعمالها ضد المصالح السوفياتية " [١] .

كما اورد المشرع السوفيتي تعريفاً للتجسس في قانون العقوبات, المادة (٥٨) بانه " تسليم معلومات معتبرة سرا من اسرار الدولة تقررت المحافظة عليه, او سرقتها او جمعها لتقديمها الى دولة اجنبية " [٢] .

الفرع الرابع

تعريف الجوسسة الالكترونية

ينطلق تعريف الجوسسة الالكترونية من تعريف التجسس في ضوء التعريفات السابقة, كذلك يمكن القول ان افضل التعريفات الاصطلاحية للجوسسة الالكترونية واقربها للصواب هو من ايجاز عباراته, وقصر الفاظه, وشموله كافة انواع التجسس واشكاله, لذلك يمكن القول ان الجوسسة الالكترونية التي هي صلب موضوعنا لا تختلف كثيرا عن مفهوم الجوسسة التقليدية, الا في الوسائل او الاداة المستخدمة الا وهي تقنية او تكنلوجيا المعلومات التي ساعدت كثيراً الجواسيس و وفرت لهم الحرية والسهولة في التجسس والبعد عن اعين الرقيب, لذلك تباينت تعريفات القانونين للجوسسة الالكترونية, البعض منهم يجعله عاما اي انه يشمل الدول والمنظمات والجماعات والافراد , والبعض الاخر يجعله محصورا فقط في نطاق الدول واسرارها دون البقية .

فمنهم من عرف الجوسسة الالكترونية بانها " الاطلاع على معلومات خاصة بالغير محفوظة على جهاز الكتروني وليس مسموحا لغير المخولين بالاطلاع عليها " [٣] .

---

(1) Professeur Gerard Cohnathan, Professeur Robert Kovar, L espionage en temps de paix, Annuaire francais de droit international, Paris, volume 6, 1960, p. 241-242 .

(٢) سعد ابراهيم الاعظمي, سعد ابراهيم الاعظمي, التجسس في التشريع العراقي, الطبعة الاولى, دار الكتب للطباعة والنشر, الموصل – العراق, ١٩٨١, ص ١٥-١٦ .

(٣) علي بن محمد بن سالم العدوي, مكافحة التجسس الالكتروني في القانون العماني مقارنة بالشريعة الاسلامية والقانون الجنائي الدولي, المؤتمر الدولي الاول, العلوم الشرعية تحديات الواقع وافاق المستقبل, كلية العلوم الشرعية, ديسمبر ٢٠١٨, ص ١٢٧٤ .

واخرون يرون ان الجوسسة الالكترونية هي " استخدام وسائل تقنية المعلومات الحديثة للدخول بشكل غير مسموح وغير قانوني الى انظمة المعلومات الالكترونية الخاصة بالدولة والحكومات والتنصت عليها, بقصد الاستحصال على ما لديها من معلومات مهمة تتعلق بنظامها وأسرارها, وتشمل جميع انواع المعلومات العسكرية والسياسية والامنية والعلمية والاجتماعية " [١] .

كما ورد تعريف التجسس الالكتروني في دليل تالين [٢] , في التعليق رقم (٢) على القاعدة (٦٦) من الاصدار الاول بأنه " يتم تعريف التجسس الالكتروني بشكل ضيق على انه اي فعل يتم تنفيذه بطريقة سرية او تحت ادعاءات كاذبة تستخدم القدرات السيبرانية لجمع (او محاولة جمع) المعلومات بقصد توصيلها الى الطرف المعارض, ويجب ان يحدث الفعل في الاراضي التي يسيطر عليها طرف في النزاع, وتشير كلمة بشكل سري الى الانشطة التي تتم سرا, كما هو الحال مع عملية التجسس الالكتروني المصممة لإخفاء هوية الاشخاص المتورطين أو حقيقة أنه حدث لخلق انطباع بأن الفرد المعني يحق له الوصول الى المعلومات المعنية, في المجال السيبراني غالبا ما تتكون من التنكر الفردي كمستخدم شرعي من خلال توظيف أذونات هذا المستخدم للوصول الى الانظمة والبيانات المستهدفة " [٣] .

(١) ضرغام جابر عطوش آل مواش, جريمة التجسس المعلوماتي دراسة مقارنة, الطبعة الاولى, المركز العربي للنشر والتوزيع, القاهرة, ٢٠١٧, ص ٨٩ ؛ د. علي عبود جعفر, جرائم تكنولوجيا المعلومات الحديثة الواقعة على الاشخاص والحكومة دراسة مقارنة, الطبعة الاولى, مكتبة زين الحقوقية والادبية, لبنان, ٢٠١٣, ص ٥٦٩ .

(٢) دليل تالين : هو وثيقة يتم الاستشهاد بها بشكل شائع في المناقشات (بشأن القانون الدولي المطبق على الحروب السيبرانية) اعد من قبل مجموعة من الخبراء الدوليين الذي جمعهم مركز الامتياز للدفاع السيبراني التعاوني لحلف الناتو (NATO) لوضع دليل حول القانون الذي يحكم الحرب السيبرانية واتبع الخبراء خطى الجهود السابقة مثل دليل سان ريمو و برنامج هارفارد, وذلك بدعوة من قبل(The NATO Cooperative Cyber Defence Center of Excellence) وللمزيد ينظر الى

Micheal N. Schmitt, "Tallin Manual on the International Law Applicable to Cyber Warfare ", first publishes, Cambridge University Press, 2013, p. 16 .

(3) Micheal N. Schmitt, Tallin Manual, op.cit, p. 159 .

اما مشروع قانون الجرائم المعلوماتية العراقي لعام ٢٠١١, فأنه لم يتضمن تعريفاً للجوسسة الالكترونية, بل اكتفى بتناول تجريم بعض صورها, مثال على ذلك الدخول او البقاء غير المشروع, او الاعتراض غير المشروع والافعال التي تمس او تهدد امن الدولة, او افشاء معلومات او اسرار الدولة [١] .

لكن قانون الجرائم الالكترونية في التشريع الاردني عرف الجوسسة الالكترونية بانها "دخول الجاني الى الشبكة المعلوماتية او نظام المعلومات او موقع الكتروني للحصول على محتوى الكتروني غير متاح للجمهور يمس الامن الوطني او العلاقات الخارجية للدولة او السلامة العامة او الاقتصاد الوطني "[٢].

المطلب الثاني

صور الجوسسة الالكترونية

بالنسبة للجوسسة الالكترونية فأنها مثل نظيرتها الجوسسة الواقعية, تنطوي على عمليات اقتحام غير مصرح بها, ولكن هذا النوع من الجوسسة يعتمد على استغلال نقاط الضعف الامنية, لكي يتم تجاوز الخوادم المشفرة بهدف الوصول الى بيانات الوكالات الحكومية والسفارات لدول اخرى, وتتمتع الجوسسة الالكترونية بالاستقلالية الجغرافية والمادية العالية, والسبب في ذلك هو عند محاولة التجسس على بيانات او معلومات وكالة تابعة لدولة اخرى, لا يشترط وجود شخص مادي او جهاز يستخدم في الدولة المستهدفة, بل من الممكن الحصول عليها فقط باستخدام اوامر الكترونية صادرة من اي موقع .

وتختلف صور الجوسسة الالكترونية باختلاف طبيعة المعلومات التي تستهدفها و حاجة الدول المتجسسة, وان هذه المعلومات اكثر تطوراً من حيث الاهمية وأتساعاً من حيث الابعاد, ولم تعد المجالات العسكرية او السياسية هي موضوع الجوسسة الوحيدة,

(١) للمزيد ينظر:مشروع قانون الجرائم المعلوماتية العراقي لسنة ٢٠١١, المواد (٣, ٤, ٧, ١٦)
(٢) عبدالاله محمد النوابسة, ممدوح حسن العدوان, جرائم التجسس الالكتروني في التشريع الاردني (دراسة تحليلية), مجلة علوم الشريعة والقانون, المجلد ٤٦, العدد ١, الملحق ١, ٢٠١٩, ص ٤٦٩

بل اصبحت في الوقت الحالي المجالات الاقتصادية والصناعية والتقنية والعلمية اكثر المعلومات طلباً, والتي سوف نتناولها كما يلي :

الفرع الاول

الجوسسة الالكترونية ذات الطابع العسكري

احد اهم مؤسسات الدولة وابرزها استخداماً للمعلوماتية [١] هي المؤسسات العسكرية, فكل دولة تسعى للحصول على المعلومات العسكرية الضرورية عن الدول المعادية وغير المعادية, وبالتالي كانت مجالاً خصباً لمحاولات الجوسسة والاختراق ومازالت كذلك بالنظر لما تحتويه من معلومات ذات اهمية بالغة تهم البلد [٢] .

كذلك تعتبر الجوسسة الالكترونية العسكرية من اخطر انواع الجوسسة على الاطلاق لأنها تتعلق بمعلومات في غاية السرية لما تحتويه من معلومات حساسة وتعلقها بالأمن القومي للدول, ولعل ابرز واهم ما يتم استهدافه في هذا المجال ما يتعلق بالجيوش واسلحتها ومعداتها الحربية والخطط العسكرية الخاصة بالدول المعادية وما تمتلكه من صواريخ و ذخائر و ومواقع عسكرية, كما يتم استهداف اسرار الدفاع ومراكز اجهزة الاتصالات, و كفاءة منظومات الاسلحة و كفاءات القيادات, و كفاءات اجهزة الانذار وبرامج التصنيع العسكري و منظومات الصيانة والتصليح وعلاقة القوات المسلحة بنظام الحكم, ومدى جاهزية القوة العسكرية, ولا يقل نشاط هذا النوع من الجوسسة في وقت السلم من وقت الحرب وذلك استعداداً لأي مواجهة محتملة [٣] .

---

(١) المعلومات هي " عبارة عن بيانات تم معالجتها بحيث اصبحت ذات معنى وباتت مرتبطة بسياق معين, فهي اما ان تضيف معرفة جديدة, او تؤكد معرفة سابقة ولها انواع كثيرة منها (معلومات جنائية, امنية, سياسية, اقتصادية, بيئية, بترولية, مائية) للمزيد ينظر : الدكتور هشام المصري, الامن المعلوماتي احد الاعمدة الرئيسية للأمن القومي (اختراقه – احتوائه), مكتبة الوفاء القانونية, الاسكندرية- مصر, الطبعة الاولى, ٢٠١٩, ص٢٢ .

(٢) أ. سلامي نادية, التجسس الالكتروني كأثر للاستخدام غير المشروع للفضاء الالكتروني على امن الدولة الخارجي, بحث منشور في مجلة دراسات جامعة عمار ثليجي بالأغواط, الجزائر, العدد ٥٦, ٢٠١٧, ص٢٤٠ .

(٣) علي بن محمد بن سالم العدوى, مكافحة التجسس الالكتروني في القانون العماني مقارنة بالشريعة الاسلامية والقانون الجنائي الدولي, بحث مقدم في المؤتمر الدولي الاول, العلوم الشرعية تداعيات الواقع وافاق المستقبل, ديسمبر, ٢٠١٨, ص ١٢٨٠ .

ومن الامثلة على الجوسسة الالكترونية العسكرية عندما تعرضت احد الوكالات التابعة لوزارة الدفاع الامريكية, وهي وكالة نظم المعلومات والمعروفة اختصاراً ب (DISA) التي من مهامها هو توفير الدعم القتالي المعلوماتي للقادة والمقاتلين التابعين لوزارة الدفاع الامريكية, التي تتميز بتوفيرها منظومة دفاعية متكاملة للاتصالات بالإضافة الى بنية تحتية ضخمة في مجال المعلوماتية, وطبيعة عمل هذه المنظومة تحتاج منها الاستعانة ببعض الشركات ذات القطاع الخاص للتعامل مع هذه الوزارة لكي تساعدها في القيام بعمل برمجيات خاصة توفر الامن لشبكاتها, فقامت هذه الوزارة بتوظيف بعض الخبراء الروس من اصحاب الخبرة في مجال البرمجيات, وبذلك قاموا باختراق هذه المنظومة عن طريق زرع بعض البرامج الضارة مثل الفايروسات داخل سيرفرات الشبكة الامنة التي سهلت لديهم طريقة الوصول الى البيانات الاكثر خطورة والسرية لدى الوكالة [١] .

كما سار المشرع العراقي وقام بتحديد المعلومات العسكرية والتي اطلق عليها اسرار الدفاع, على النهج الذي سار عليه المشرع الفرنسي والمصري, بالنظر الى اهميتها وخطورتها, وللمحافظة على سريتها ومعاقبة الاشخاص الذين يحاولون إفشائها, والذي نص على انه " يعتبر سراً من اسرار الدفاع :

١- المعلومات الحربية والسياسية والاقتصادية والصناعية التي هي بحكم طبيعتها لا يعلمها الا الاشخاص الذين لهم صفة في ذلك والتي تقضي مصلحة الدفاع عن البلاد ان تبقى سراً على من هم عداهم .

٢- المكاتبات والمحررات والوثائق والرسوم والخرائط والتصميمات والصور وغيرها من الاشياء التي قد يؤدي كشفها الى افشاء معلومات مما أشير اليه في الفقرة السابقة والتي تقضي مصلحة الدفاع عن البلاد ان تبقى سراً على غير من يناط بهم حفظها او استعمالها .

(١) اياد خلف محمد المفرجي, المنازعات الدولية ذات الطابع الالكتروني, رسالة ماجستير, كلية القانون والعلوم السياسية, جامعة كركوك, جمهورية العراق, ٢٠١٩ , ص ١٣٦ .

٣- الاخبار والمعلومات المتعلقة بالقوات المسلحة وتشكيلاتها وتحركاتها وعتادها وتموينها وغير ذلك مما له مساس بالشؤون العسكرية والخطط الحربية ما لم يكن قد صدر اذن كتابي من جهة مختصة بنشره او اذاعته .

٤- الاخبار والمعلومات المتعلقة بالتدابير والاجراءات التي تتخذ لكشف وضبط الفاعلين والشركاء في الجرائم المنصوص عليها في هذا الباب وكذلك الاخبار والمعلومات الخاصة بسير التحقيق والمحاكمة اذا حظرت سلطة التحقيق او المحاكمة اذاعتها " [١] .

الفرع الثاني

الجوسسة الالكترونية ذات الطابع السياسي

غالباً ما تقوم الدول بالجوسسة بهدف الحصول على معلومات تكشف عن الاستراتيجيات السياسية والطموحات الاقتصادية والقدرات العسكرية للدول الاخرى, وتقوم بتعزيز امنها القومي من خلال الوصول الى المعلومات ذات الطابع السياسي المتعلقة بالدول الاخرى, ويشار الى هذا النوع بالجوسسة السياسية, ويستخدم هذا المصطلح لتميزه عن الجوسسة الاقتصادية والصناعية وغيرها من انواع الجوسسة .

ويقصد بالمعلومات السياسية " هي تلك المعلومات الخاصة بالسياسة الداخلية والخارجية للدولة, وكذلك المعلومات المتعلقة بالسفارات ونشاط عملها, والتي تشمل سياسة الدولة وخططها الاقتصادية والصناعية المتعلقة بمصلحة الدفاع, والتي يجب ان تبقى سرية الا للمسؤول عن حفظ هذه الاسرار " [٢].

ومن الامثلة الحية على الجوسسة الالكترونية ذات الدوافع السياسية ما تم اكتشافه مؤخراً هو وجود شبكة دولية كبيرة تعرف باسم (ECHELON) تابعة لوكالة الاستخبارات المركزية (CIA) وتعمل تحت اشرافها, وبالتعاون مع اجهزة استخبارات اخرى تابعة لكل من المملكة المتحدة (بريطانيا) و كندا و استراليا و نيوزلندا, ويعد من الانظمة التجسسية العالمية وظيفته رصد البيانات واعتراضها ونقلها ومن ثم انشاءها

(١) المادة (١٨٨) من قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩ المعدل .
(٢)ضرغام جابر عطوش آل مواش, مرجع سابق, ص ١٤٨ .

بواسطة وكالة الامن القومي الامريكية, ويتجسس هذا النظام على المكالمات الهاتفية السلكية واللاسلكية والالكترونية المدنية والعسكرية في العالم, والرسائل بكافة انواعها (الرسائل الالكترونية, البرقيات, والرسائل عبر الفاكس او التلكس), وبعد الحصول على المعلومات, تقوم بفرزها وتحليلها من اجل الحصول على المعلومات المهمة منها [١] .

الفرع الثالث

الجوسسة الالكترونية ذات الطابع الاقتصادي

تعد الجوسسة الاقتصادية مجموعة فرعية من الجوسسة, ويعد الاقتصاد من العوامل المهمة والمحرك الاساسي لنهضة الدول وحفظ سيادتها واستقرارها الامني, ويعد هذا الصنف الوجه الجديد للجوسسة, بحيث ان المتفحص للمجال الاقتصادي اليوم يتيقن ان الصراعات الاقتصادية اخذت محل المواجهة العسكرية, وكان للتطور الهائل والسريع في مجال التقنية السبب في تسريع هذه الظاهرة [٢] .

ونظراً لأهمية المعلومات الاقتصادية, فأن الدول تسعى جاهدةً لحماية هذه المعلومات وابقاءها رهين السر والكتمان, وتستخدم اهم الوسائل من اجل الحفاظ عليها وعدم تسريبها الى أيادي خصومها من الدول او المنظمات, في المقابل نجد الزيادة في نسبة الجوسسة الاقتصادية من قبل تلك المنظمات التي تستهدف موارد الدول وحجم الانتاج عندها والمرافق الاقتصادية الحيوية لديها, ومواطن الضعف, محاولة للوصول الى الثغرات الاقتصادية [٣] .

ومن الامثلة الحية على الجوسسة الالكترونية ذات الدوافع الاقتصادية, عندما تمكن احد القراصنة الروس في سنة ٢٠١٤ من اختراق (٩٠) سيرفر من مؤسسة تدعى (JP Morgan Chase) من خلال ثغرة كانت موجودة في احد هذه السيرفرات التي لم يتم حمايتها بصورة صحيحة, والتي سهلت على المهاجم التجسس على ملفات تابعة لعملاء المؤسسة البالغ عددها (٧٦) مليون من العملاء المنزليين, بالإضافة الى (٧) ملايين

(١) علي بن محمد بن سالم العدوى, مرجع سابق, ص ١٢٨١ .
(٢) أ. سلامي ناديه, مرجع سابق, ص ٢٤١ .
(٣) علي بن محمد بن سالم العدوى, مرجع سابق, ص ١٢٧٩.

من العملاء التجاريين, واستطاع المهاجم الحصول على العناوين البريدية للعملاء وارقام هواتفهم [١] .

الفرع الرابع

الجوسسة الالكترونية ذات الطابع الصناعي والعلمي

وقد ينصب هذا النوع من الجوسسة على معرفة المعلومات والاسرار التي تخص الابحاث العلمية والصناعات والاختراعات لدى الدول, بالأخص تلك التي تسهم في الانتاج الحربي وعمليات تطوير الاسلحة, ومعرفة الدراسات العلمية في المجالات الهندسية او الزراعية او الصحية او غيرها من المجالات [٢] .

ويتضح في العلم الحديث ان الدول دخلت مرحلة التزاحم والتسابق في جهودها العلمية لتزويد قواها بأحدث الوسائل العسكرية في الهجوم والدفاع, وفي اعداد برنامج الاسلحة النووية والكيمياوية والجرثومية, وقد نتج عن التقدم التقني والتكنولوجي والصناعي العالمي بين الامكانيات والقدرات العسكرية والاساليب الدفاعية والطرق الحديثة من اجل حماية المعلومات السرية الى ظهور انواع اخرى من الجوسسة, منها الجوسسة الاستراتيجية او القومية, والجوسسة التكتيكية او القتالية, بالإضافة الى الجوسسة المضادة [٣].

واحد اخطر انواع الجوسسة والاختراقات الالكترونية التي حدثت ضد الابحاث والمشاريع العلمية, تلك التي وقعت سنة ٢٠٠٩ في احد الولايات الامريكية (Maryland) وتحديدا في احد المعامل الخاصة بالعلوم الفيزيائية المتطورة والتابعة لجامعة (Johns Hopkins), والتي ترتبط بعقود مباشرة مع الحكومة الامريكية من اجل تطوير الابحاث العلمية وفي شتى المجالات, وبمبالغ كبيرة, وبالرغم من الحماية الفائقة لتلك الشبكات, تمكنت مجموعة من القراصنة المحترفين من اختراقها والجوسسة على بعض

(١) أياد خلف محمد المفرجي, مرجع سابق, ص ١٣٩ .
(٢) د. جابر المراغي, جرائم انتهاك اسرار الدفاع عن البلاد من الناحيتين الموضوعية و الاجرائية, دار النهضة العربية, القاهرة, مصر, ١٩٨٨, ص ١١٦ .
(٣) عثمان بن علي بن صالح, جريمة التجسس وعقوبتها في الشريعة الاسلامية و القانون الوضعي, رسالة ماجستير مقدمة الى قسم العدالة الجنائية " تخصص التشريع الجنائي والاسلامي ", ص ٤٧ .

المشاريع والابحاث العلمية التي يتم اجرائها داخل المعمل, ولم يتمكنوا من السيطرة على الاختراق الا بعد فصل اتصال الشبكة الخاصة بالمعمل من الشبكة العالمية (الانترنت) وقاموا بفحص الاجهزة كلاً على انفراد بغية ايجاد الثغرة التي تم الاختراق من خلالها وتوفير الحماية اللازمة لجعلها اكثر امناً [١] .

الفرع الخامس

الجوسسة الالكترونية ذات الطابع الاجتماعي

يقصد بالمعلومات الاجتماعية او السكانية, هي تلك المعلومات التي تتعلق بالوضع الاجتماعي والإحصاءات السكانية, والتي تعكس الوضع الاجتماعي والمعيشي لكل مجتمع من المجتمعات, ولأهمية هذه المعلومات بالنسبة للدول, فقد حظيت باهتمام الكثير من اجهزة المخابرات العالمية والمنظمات التي باتت تبحث عن بعض الثغرات المجتمعية الموجودة في الدول لتتمكن من الحصول على المعلومات المتعلقة بعدد السكان الاصليين وكيفية توزيعهم جغرافياً, ومدى رضا المجتمع من الحكومة, والمعلومات التي تتعلق بالطوائف والقبائل, وكل هذه المعلومات يتم تخزينها بواسطة كوادر مؤسساتها الاحصائية في حواسيب وانظمة معلومات الكترونية تابعة للدولة, ومن ثم يتم معالجة هذه المعلومات وتحليلها بغية الاستفادة منها على شكل برامج خاصة تساعد في تطوير المجتمع في المستقبل, الا انها تكون عرضة للجوسسة من بعض الجهات الخارجية او الداخلية لأغراض خاصة ومن قبل الدول المعادية والصديقة [٢].

يتضح لنا ان المعلومات السرية المتعلقة بجميع المجالات التي ذكرناها من الممكن ان تحفظ على شكل محتوى الكتروني, ومن المؤكد ان هذا المحتوى محاط بوسائل الامن المعلوماتي, ولا يخفى على الجميع ان هذا المحتوى معرض للاختراق والجوسسة, لذلك

(١) ريتشارد إيه كلارك, روبرت كيه كنيك, حرب الفضاء الالكتروني التهديد التالي للأمن القومي وكيفية التعامل معه, الطبعة الاولى, مركز الامارات للدراسات والبحوث الاستراتيجية, ابو ظبي, الامارات, ٢٠١٢, ص ١٥٦-١٥٧ .

(٢) عبد الاله النوايسة, جرائم تكنلوجيا المعلومات – شرح الاحكام الموضوعية في قانون الجرائم الالكترونية, الطبعة الاولى, دار وائل للنشر والتوزيع, عمان, ٢٠١٧, ص ٣٦١ ؛ علي عبود جعفر, مرجع سابق, ص ٥٧١ .

نرى ان على الجهات المسؤولة عن حماية هذه المعلومات وضع كافة السبل لحمايتها من الجوسسة والاختراق, لان وقوع هذه المعلومات في ايدي دول معادية او منظمات ارهابية من المحتمل ان تستغلها في زعزعة استقرار الدولة وابتزاز حكومتها وخاصة المعلومات العسكرية والامنية والسياسية, لان اغلب المنظمات الارهابية تسعى جاهدة لتفرض سيطرتها ووجودها على ارض الواقع, مع وضع نظام حماية صارم للمخولين بالاطلاع عليها, لمنعهم من تسريبها, وعمل تحديثات مستمرة لبرامج الحماية وعدم الوثوق بالشركات الاجنبية المختصة بنظام البرمجيات وجعلها ضامنة لأي تسريب اذا تعاقدت معهم, اما بالنسبة للمعلومات الاقتصادية فأنها اصبحت من العوامل الرئيسية والمهمة لحفظ سيادة الدول واستقرارها الامني, وبدأ العالم بالتسابق حول الحرب المعلوماتية الاقتصادية, واصبح الاقتصاد يشكل عصبة الامم ونهضتها وقوتها, لذلك ينبغي حمايتها بصورة صحيحة ووضعها بالحسبان ان اي اختراق لهذه المعلومات من قبل القراصنة و الجواسيس, لاسيما المنظمات المعادية والارهابية سوف يعرض كيان الدولة للانهيار ويشلها رويداً رويداً .

المبحث الثاني

صلة الجوسسة الالكترونية بالامن القومي وحقوق الانسان

وتتنوع المفاهيم والمصطلحات للامن القومي, فكل باحث ينظر اليه من وجهة نظره ومن الجانب الذي يهم دراسته, فقد تطور مفهوم الامن القومي في العقدين الاخيرين كثيراً خاصة مع تطور تكنولوجيا المعلومات والاتصالات وظهور التهديدات السيبرانية الحديثة, ولا يخفى على الجميع ان سياسة الامن القومي تهدف الى تحقيق وحماية المصالح السياسية والاقتصادية والاجتماعية الداخلية والخارجية للدولة بالاضافة الى الامن المعلوماتي الذي اصبح يشكل احد اهم الاهداف التي يجب حمايتها [1] , لذلك خصصنا المطلب الاول منه للحديث عن صلة الجوسسة الالكترونية بالامن القومي,

(١) د. هشام المصري, مرجع سابق, ص ٥٧ .

اما في الثاني سوف نتكلم عن الجوسسة الالكترونية وحقوق الانسان, وعلى النحو الاتي :

المطلب الاول

صلة الجوسسة الالكترونية بالامن القومي

يواجه الامن القومي اليوم تحديات عديدة تتمثل بزي التهديدات الاجرامية المرتبطة بتكنولوجيا الاتصالات ونظم المعلومات, وتقع هذه التكنولوجيا الحديثة في الصميم من فكرة الحرب المعلوماتية, التي يتضح ان اهدافها اقتصادية بالدرجة الاولى بعدما كانت عسكرية وسياسية في السابق, ومن الممكن ان تترتب عليها تأثيرات ضخمة عى سلوك العمليات والمعاملات التجارية والصناعية, من خلال الانترنت يمكن التلاعب بالمعلومات وتيسر عمليات الجوسسة وانشطة جمع المعلومات نظراً للسهولة التي يمكن بها اعتراض واقتحام سبيل المعلومات المسافرة عبر شبكة الانترنت, من اجل ذلك سنوضح تعريف الامن القومي في الفرع الاول, وانعكاسات الجوسسة الالكترونية على الامن القومي في الثاني, وكما يلي :

الفرع الاول

تعريف الامن القومي

الامن القومي هو" تأمين كيان الدولة والمجتمع ضد الاخطار التي تتهددها داخلياً وخارجياً وتأمين مصالحها وتهيئة الظروف المناسبة اقتصادياً واجتماعياً لتحقيق التنمية الشاملة لكل فئات المجتمع " [١], والبعض يرى انه يعني الحماية من الهجوم الخارجي, اي ينظر اليه انه يعني الدفاعات العسكرية, ولكن هذا التعريف ضيقَ من مفهوم الامن القومي على الجانب العسكري, لكن مفهوم الامن القومي يشمل جوانب عديدة اضافة الى الجانب العسكري منها الجانب الاقتصادي والسياسي والاجتماعي والتعليمي والمعلوماتي وغيرها من جوانب الحياة, كما ان جوهر الامن القومي في الماضي كان ينصب فقط على الوجود المادي للدولة وسيادتها الكاملة على اراضيها والاعتماد على

(١) معجم المعاني الجامع, معجم عربي-عربي, تعريف ومعنى الامن القومي, متاح على الموقع الالكتروني, https://www.almaany.com/ar/dict/ar-ar/ , تاريخ الزيارة ٢٠٢١/١/٢٢ .

قدرتها العسكرية والدفاعية, ولكن مع التطور التكنولوجي والتقني الذي اصاب المجتمع الدولي, والذي اصبح مصطلح الامن القومي يشمل معاني اخرى مثل الامن الاقتصادي والتجاري وامن المعلومات الى جانب امن الدفاعي [١], اما عن مستويات الامن القومي فانها تتكون من اربعة مستويات

١ – امن الفرد والمتمثلة بحمايته من الاخطار التي تهدد حياته واسرته وممتلكاته خصوصياته.

٢– امن الوطن المتمثل بحمايته من الاخطار الخارجية او الداخلية التي يعبر عنها بالامن الوطني.

٣– الامن القطري او الجماعي الذي يتم التعبير عنه باتفاق عدة دول ينتمون الى اقليم واحد لكيفية مواجهة التهديدات الداخلية او الخارجية والذي يعبر عنه بالامن القومي .

٤– الامن الدولي الذي تتولاه المنظمات الدولية سواء بواسطة الجمعية العامة للامم المتحدة او من خلال مجلس الامن الدولي, والدور الذي يلعبونه في حفظ السلم والامن الدوليين [٢].

الفرع الثاني

انعكاسات الجوسسة الالكترونية على الامن القومي

لطالما كان ردع محاولات الجوسسة من قبل الدول الاجنبية تصب دائماً في المصلحة الوطنية للدول, ونظراً لوجود موجهات الدخول الجديدة والسهلة نسبياً من قبل القراصنة عبر الانترنت تبدو ان الجوسسة الالكترونية قد ادت الى تصعيد صور التهديدات ذات الصلة بالجوسسة, اي انه يتم تضخيم فعالية الجوسسة باستخدام الوسائل الالكترونية الى اقصى الحدود, والرادع التقليدي المتاح للدول المستهدفة المتمثلة بامكانية مقاضاة وسجن الجواسيس الذين يتم القبض عليهم, يتبين انه غير مجدي, لعدم الوجود المادي

(١) د. هشام المصري, مرجع سابق, ص ٥٨ .

(٢) شيرين الضاني, الامن القومي ومشروعيته في الاسلام, مقال منشور على موقع الحوار المتمدن, العدد ٣١٦٠ – ٢٠١٠, والمتاح على الموقع الالكتروني : https://www.ahewar.org/debat/show.art.asp?aid=232581 , تاريخ الزيارة ٢٠٢١/١/٢٤ .

لعملاء المخابرات على اراضي الدولة المستهدفة, وبالتالي فمنذ نهاية الحرب الباردة وظهور الجوسسة الالكترونية, تغيرت انشطة الجوسسة في الدول الاقل تقدماً من بؤر سياسية عسكرية الى اقتصادية, كونها توفر المعرفة التكنولوجية والاجهزة الحديثة التي لايمكنهم تحقيقها دون هذه الطرق[١].

والبعض من الباحثين يقارنون الجوسسة الالكترونية في وقت السلم (بالحرب او الاحتلال), كونها تمثل محاولة لتقويض امن واستقرار الدول ذات السيادة, والمثال على ذلك الجوسسة الالكترونية من قبل الصين ضد الولايات المتحدة الامريكية التي وصلت الى هذا الحد على نطاق واسع يشبه الى حد بعيد عملاً من اعمال النهب, والذي كانت من الممكن ان تحدث قبل ظهور الانترنت فقط من خلال الاحتلال العسكري بدلاً من سلسلة الاعمال الاجرامية , وبالتالي فانها لاتفرق بين مجموعتي القانون الدولي الرئيسيتين (قانون النزاع المسلح او القانون الدولي الانساني) من جهة و قانون السلم من جهة اخرى [٢] .

كما ان بعض المحاميين الدوليين يؤكدون ان الجوسسة بدوافع اقتصادية ستكون الخط الامامي لحرب اقتصادية عالمية جديدة, او عمل من اعمال الحرب الاقتصادية, او الشكل الحديث من اشكال الحرب التي استخدمتهاالحكومة الصينية ضد الولايات المتحدة [٣] .

مما تقدم ومن مناقشة الجوسسة الالكترونية بدوافع اقتصادية التي تمارسها الحكومة الصينية ضد الولايات المتحدة, يتبين ان الامن القومي مرتبط ارتباطاً وثيقاً بحماية

(1) Karen Sepura, Economic Espionage : The Front Line of a New World Economic War, 26 Syracuse Journal of International Law and Commerce, 1998-1999, p. 129-134 .

(2) David P. Fidler, Economic Cyber Espionage and International Law : Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies, Volume 17, Issue 10, 20/march/ 2013, on site American Society of International Law, available on website : https://asil.org/insights/Volume/17/Issue/10.

(3) Jonathan Eric Lewis, THE ECONOMIC ESPIONAGE ACT AND THE THREAT OF CHINESE ESPIONAGE IN THE UNITED STATES, University of Connecticut School of Law, 2010, p. 226 .

الاسرار التجارية والصناعية للدولة, ويفهم ان الامن القومي يعادل المصالح الوطنية الاقتصادية او على نطاق اوسع بضمنها المصالح الوطنية الاقتصادية, ونتيجة ذلك ان اي نشاط يؤثر على المصالح الوطنية الاقتصادية للدولة ستصبح تلقائياً مسالة تتعلق بالامن القومي .

ورأينا في ذلك انه, عندما تكافح الشركات مالياً فان الاقتصاد الوطني للدولة المضيفة سوف يتأثر بشكل سلبي, اما الامن القومي في الوقت الحاضر فانه مرهون بالأمن الاقتصادي, ويمكن القول ان الجوسسة الاقتصادية تهدد الامن القومي وتعرض الامن والسلم الدوليين للخطر, ولخطورة هذا التهديد, الافضل ان يمتلك المجتمع الدولي قواعد قانونية دولية تحظر بشكل واضح, الجوسسة الالكترونية.

المطلب الثاني

الجوسسة الالكترونية وحقوق الانسان

ينص عدد من الاطر القانونية على المستوى الدولي ان لجميع الافراد الحق في احترام حياتهم الخاصة ومنزلهم ومراسلاتهم, كما ويشير الاعلان العالمي لحقوق الانسان لعام ١٩٤٨ صراحةً الى هذا الحق في المادة (١٢) [(١)], لذلك فهو صك غير ملزم قانوناً ومع ذلك يوجد التزام صريح وملزم بحماية

الحق في الخصوصية لجميع الدول الاعضاء في العهد الدولي الخاص بالحقوق المدنية والسياسية لعام ١٩٩٦ (ICCPR) المادة (١٧)[(٢)].

---

(١) الاعلان العالمي لحقوق الانسان المعتمد في ١٠ ديسمبر ١٩٤٨, قرار الجمعية العامة للامم المتحدة رقم ٢١٧ أ – المادة ١٢ تنص على انه لا يجب ان يتعرض اي شخص لتدخل تعسفي في حياته الخاصة او اسرته او مسكنه او مراسلاته, او لحملات على شرفه وسمعته .لكل فرد الحق في حماية القانون من مثل هذه التدخلات او تلك الحملات .
متاح على الموقع الالكتروني : https://www.oic-iphrc.org/ar/data/docs/legal-instruments/ .

(٢) المادة (١٧) من العهد الدولي الخاص بالحقوق المدنية والسياسية, المعتمد بموجب قرار الجمعية العامة للامم المتحدة ٢٢٠٠ أ (د-٢١) المؤرخ في ١٦ كانون الثاني ١٩٦٦, التي تنص على :
" ١- لا يجوز تعرض اي شخص ,على نحو تعسفي او غير قانوني, لتدخل في خصوصياته او شؤون اسرته او بيته او مراسلاته, ولا لأي حملات غير قانونية تمس شرفه او سمعته .
٢- من حق كل شخص ان يحميه القانون من مثل هذا التدخل او المساس .

ان لجنة حقوق الانسان التابعة للامم المتحدة (HRC), هي هيئة تتكون من مجموعة من الخبراء المستقلين التي تراقب تنفيذ العهد الدولي الخاص بالحقوق المدنية والسياسية من قبل دول الاطراف فيها, مكلفة بتوفير دليل لتفسير العهد, وتقوم اللجنة بذلك من خلال اصدار تعليقات عامة غير ملزمة قانوناً وغير خاصة ببلد, بهدف من بين امور اخرى ال تعزيز التنفيذ الفعال للعهد وتوضيح متطلباته وتحفيز انشطة الدول الاطراف والمنظمات الدولية في تعزيز حقوق الانسان وحمايته [١] .

كما يؤكد تحليل مجلس حقوق الانسان لمحتوى الحق في الخصوصية الوارد في التعليق العام رقم ١٦ ان المادة (١٧) الفقرة (١) لا تحضر فقط الدول من غزو الخصوصية ولكنها تحدد ايضاً التزامات ايجابية لاتخاذ تدابير وطنية ايجابية لحمايتها [٢], بما في ذلك انظمة الشكاوي المناسبة فضلاً عن سبيل الانصاف من انتهاكات الخصوصية, والذي لم يتم تعريف معناها (الخصوصية) لاغراض المادة (١٧) في التعليق العام رقم (١٦) او السوابق القضائية لمجلس حقوق الانسان, ومع ذلك اعترفت اللجنة بانتهاكها في سياق سرية وسلامة المراسلات, وعلاوة على ذلك تم النص صراحة على الحماية القانونية ضد التدخل في خصوصية المراسلات في الفقرة (٨) من التعليق العام رقم (١٦) والتي ينص على انه : التقيد بالمادة (١٧) يتطلب ضمان سلامة وسرية المراسلات بحكم القانون وبحكم الواقع ويجب تسليم المراسلات الى المرسل اليه دون اعتراض ودون فتحها او قرائتها بطريقة اخرى .

كما يجب حظر المراقبة الالكترونية او غير ذلك واعتراض الاتصالات الهاتفية والبرقية وغيرها من اشكال الاتصالات والتنصت على المكالمات الهاتفية وتسجيل المحادثات

(1) Ghandi, The Human Rights Committee and the Right of Individual Communication : Law and Practice, Ashgate Publishing, 1998, p. 25 .

(٢) جامعة مينيسوتا, مكتبة حقوق الانسان, اللجنة المعنية بالحقوق المدنية والسياسية, الدورة الثانية والثلاثون (١٩٨٨) التعليق العام رقم ١٦ : المادة (١٧) الحق في حرمة الحياة الخاصة :الفقرة ١ : " تنص المادة ١٧ على حق كل شخص في عدم التعرض, على نحو تعسفي او غير مشروع لتدخل في خصوصيته او شؤون اسرته او بيته او مراسلاته وكذلك من الهجمات الغير قانونية على شرفه وسمعته . وترى اللجنة انه يلزم ضمان هذا الحق في مواجهة جميع تلك التدخلات والاعتداءات فضلاً عن حماية هذا الحق ", متاح على الموقع الالكتروني : https://www.hrlibrary.umn.edu/arabic/hrc-gc16.html .

[1] , وفسرت السوابق القضائية من قبل اللجنة مصطلح المراسلات هلى انه لا يشمل الرسائل المكتوبة فحسب, بل يشمل ايضاً اشكال الاتصال الاخرى مثل الهاتف والفاكس والبريد الالكتروني.

وبعد ذلك صرحت لجنة حقوق الانسان ان يتخذ الاطراف جميع التدابير المناسبة لضمان عدم تعرض جمع البيانات الشخصية وتخزينها واستخدامها لاية انتهاكات وعدم استخدامها لاغراض تتعارض مع العهد وان تكون متسقة مع الالتزامات المنصوص عليها في المادة (١٧) من العهد .

ولتحقيق هذا الهدف يجب ان يضمن الاطراف ان معالجة المعلومات وجمعها تخضع للمراجعة والاشراف من قبل هيئة مستقلة مع ضرورة ضمان الحياد والفعالية .

وبالتالي تندرج المراقبة الالكترونية ضمن مصطلح "مراسلات" بموجب المادة (١٧) وقد تكون متوافقة مع تلك المادة ان كانت تخضع لرقابة صارمة واشراف من قبل هيئات مستقلة, ويفضل القضائية.

يتناول التعليق رقم (١٦) ايضا جمع المعلومات الشخصية والاحتفاظ بها على اجهزة الحاسوب و بنوك البيانات والاجهزة الاخرى سواء من قبل السلطات العامة او الافراد او الهيئات الخاصة والتي يجب ان تخضع للوائح وضمانات الدولة المناسبة [2] .

---

(١) التعليق العام رقم ١٦ : المادة (١٧) الحق في حرمة الحياة الخاصة :
الفقرة ٨ : " وحتى فيما يتعلق بعمليات التدخل التي تتفق مع العهد, يجب ان يحدد [.....] . ويقتضي التقييد بالمادة ١٧ ضمان سلامة وسرية المراسلات قانوناً وفي الواقع . وينبغي ان تسلم المراسلات الى المرسل دون مصادرتها او فتحها او قراءتها, وينبغي حظر الرقابة, بالوسائل الالكترونية او بغيرها على السواء, وحظر اعتراض طريق الاتصالات الهاتفية والبرقية وغيرها من اشكال الاتصالات والتنصت على المحادثات وتسجيلها, وينبغي ..... ., جامعة مينيسوتا, مكتبة حقوق الانسان, اللجنة المعنية بالحقوق المدنية والسياسية, الدورة الثانية والثلاثون (١٩٨٨), مرجع سابق .

(٢) التعليق العام رقم ١٦ الحق في حرمة الحياة الخاصة :
الفقرة ١٠ : " ويجب ان ينظم القانون عمليات جمع وحفظ المعلومات الشخصية باستخدام الحاسوب ومصارف البيانات وغيرها من الوسائل, سواء كانت تجريها السلطات العامة ام الافراد العاديون او الهيئات الخاصة, ويعين ان تتخذ الدول تدابير فعالة لكفالة عدم وقوع الملومات المتعلقة بالحياة الخاصة للشخص في ايدي الاشخاص الذين لا يجيز لهم القانون الحصول عليها او تجهيزها او استخدامها, وعدم استخدامها على الاطلاق في اغراض تتنافى مع العهد, ولكي يتسنى حماية الحياة الخاصة للفرد على اكفأ وجه ينبغي ان يكون من حق كل فرد ان يتحقق بسهولة مما اذا كانت هناك بيانات شخصية مخزونة في اضابير البيانات الاوتوماتيكية, واذا كان الوضع كذلك من ماهية هذه البيانات والغرض من الاحتفاظ بها, كما ينبغي ان يكون بمقدور كل فرد ان يتحقق من هوية

بالرغم انه يوجد انفصال قانوني فيما يتعلق بالجوسسة في وقت السلم بموجب القانون الدولي, مع ذلك فيما يتعلق بالقانون الدولي لحقوق الانسان الى الحد الذي تعتبر فيه المراقبة الالكترونية من قبل الدول الاخرى تدخلاً غير قانونياً او يمكن القول انه تعسفياً على الخصوصية وتقييداً لحرية التعبير والمعلومات, لذلك فمن مسؤولية الدولة ان تحافظ على من هم على اقليمها وتحت سيطرتها .

يتضح مما سبق ان الحاجة الى قيام لجنة حقوق الانسان التابعة للامم المتحدة بتحديث تعليقها العام بشأن الحق في الخصوصية, كما تمت الدعوى في احد المؤتمرات الحديثة لمفوضي حماية البيانات والخصوصية العالمية الى بروتوكول اضافي للمادة (١٧) من العهد الدولي الخاص بالحقوق المدنية والسياسية (ICCPR) لاصدار المعايير المعمول بها عالمياً لحماية البيانات وحماية الخصوصية [١] .

وقد صدر بهذا الصدد مجموعة من المبادئ عن مجموعة خبراء المجتمع المدني اساساً لزيادة التوافق حول المعايير, منها المبادئ العالمية للامن القومي والحق في المعلومات, مبادئ تشواني (TheTshwane Principles) التي اقرتها الجمعية البرلمانية لمجلس اوروبا[٢], والتي تركز على الشفافية واحترام الحقوق والمساءلة الديمقراطية كأساس انشطة جمع المعلومات الحكومية.

وان حق خصوصية الاتصالات مكفول في عدد من المعاهدات الدولية والاقليمية منها:

السلطات العامة او الافراد العاديين او الهيئات الخاصة التي تتحكم او قد تتحكم في هذه الاضابير, واذا كانت الاضابير تتضمن بيانات شخصية غي صحيحة او جمعت او جهزت بطريقة تتعارض مع احكام القانون, ينبغي ان يكون من حق كل فرد ان يطلب تصحيحها او حذفها . ", جامعة مينيسوتا, مكتبة حقوق الانسان, اللجنة المعنية بالحقوق المدنية والسياسية, الدورة الثانية والثلاثون (١٩٨٨), مرجع سابق .

(١) المؤتمر الدولي الخامس والثلاثون لمفوضي حماية البيانات والخصوصية, قرار بشأن ترسيخ حماية البيانات وحماية الخصوصية في القانون الدولي, وارسو, تشرين الاول ٢٠١٣, متاح على الموقع الالكتروني : https://Privacyconfenence2013.org/web/pagefiles/kefinder/files/5 .

(2) Global Principle on National Security and the Right to Information, 12 June 2013, available on website : https://www.opensocietyfoundations.org/sites/default/files/ .

- العهد الدولي الخاص بالحقوق المدنية والسياسية ١٩٦٦ (ICCPR)[١] .
- الاتفاقية الاوروبية لحقوق الانسان ١٩٥٠ (ECHR) [٢] .
- الاتفاقية الامريكية لحقوق الانسان ١٩٦٩ (ACHR) [٣] .

يتضح ان الجوسسة الاقتصادية لم تكن سائدة داخل النظام العالمي مثل الجوسسة العسكرية والسياسية التي كانت توفر المزايا للامن القومي, بل اصبحت الجوسسة الالكترونية منذ فجر الفضاء الالكتروني تمس سيادة الدولة التي تستضيف الشركة التي يتم الاستيلاء على اسرارها التجارية وتكون لها تأثيرات ضارة على اقتصادها الوطني, والجوسسة الاقتصادية اصبحت تهدد الامن القومي وتعرض الامن والسلم الدوليين للخطر, كون الامن القومي اصبح مرهوناً بالامن الاقتصادي في وقتنا الحاضر .

اما من ناحية الجوسسة الالكترونية وحقوق الانسان يتضح ان الجوسسة الالكترونية تتعارض مع الحق في الخصوصية على النحو الوارد في المادة (١٧) من العهد الدولي الخاص بالحقوق المدنية والسياسية, والمادة (٨) من الاتفاقية الاوروبية لحقوق الانسان, والتي تحمي معلومات الشخص واتصالاته من التدخل, ولكن الخصوصية ليست حقاً مطلقاً, بل هناك بعض الحالات التي حددها الدستور واكد عليها القانون الوطني التي يمكن فيها من تقييد هذا الحق في سياق المراقبة الالكترونية .

المبحث الثالث

(١) في المادة (١٧) من العهد الدولي الخاص بالحقوق المدنية والسياسية الذي اعتمد وعرض للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة ٢٢٠٠ الف (د-٢١) المؤرخ في ١٦ كانون/ديسمبر ١٩٦٦ تاريخ بدء النفاذ : ٢٣ اذار / مارس ١٩٧٦, وفقاً لأحكام المادة ٤٩ .

(٢) وهي معاهدة دولية هدفها حماية حقوق الانسان والحريات الاساسية في القارة الاوروبية, والتي تم وضع مسودتها من قبل مجلس اوروبا الذي كان حديث التكوين آنذاك سنة ١٩٥٠, وبدا تطبيقها في ٣ ايلول ١٩٥٣, وقد دعت المادة (٨) الى احترام الخصوصية, متاح على ويكيبيديا الموسوعة الحرة, الاتفاقية الاوروبية لحقوق الانسان, مرجع سابق.

(٣) الحق في الخصوصية وارد في المادة (١١) من الاتفاقية الامريكية لحقوق الانسان ١٩٦٩, للمزيد ينظر الى :

. Mrs. Eliza Watt, op.cit, p.p. 213-215

تفسيرات القانون الدولي الناشئة للجوسسة الالكترونية

تكمن صعوبة تحديد موقع وطبيعة ومضمون الفضاء الالكتروني في سبب رئيسي للخلافات حول ما اذا كان الفضاء الالكتروني يخضع لسيادة الدولة ام لا, ويجادل ممثلوا الدول بأغلبية ساحقة بان دولتهم لها السيادة على المجالات الالكترونية التي ينسبونها الى دولتهم, كما يتميز القانون الدولي بتجريده ومرونته, مما يسمح للنظام بالتكيف مع الاحتياجات الجديدة للمجتمع الدولي, مع الاخذ بالاعتبار الترابط المتبادل بين القانون الدولي والسياسة الدولية, فأن المصطلحين (استخدام القوة) و (الهجوم المسلح) يظهران مجالاً للتفسير, والتي تم استكشاف حدودها في الماضي من قبل عدة دول بهدف استيعابها السياسي او الاقتصادي او احتياجات ايديولوجية .

لذلك يتم طرح مجموعة من الاسئلة المهمة حول ما اذا كانت الجوسسة الالكترونية مسموحاً بها, ام انها ممارسة ضارة تقوض التعاون الدولي ويحظرها القانون الدولي, لذلك قمنا بتقسيم هذا المبحث الى ثلاث مطالب, خصصنا الاول منه لبيان مدى اعتبار الجوسسة الالكترونية كتهديد او استخدام للقوة وهجوم مسلح, اما في المطلب الثاني فقد تناولنا الجوسسة الالكترونية باعتبارها انتهاكاً للسيادة الاقليمية, وفي المطلب الثالث سوف نتحدث عن الجوسسة الالكترونية ومبدأ عدم التدخل, وفقاً للتفصيل الاتي :

المطلب الاول

الجوسسة الالكترونية كتهديد او استخدام للقوة وهجوم مسلح

يناقش في هذا الفرع تفسيرات الهجوم المسلح (المادة ٥١ من ميثاق الامم المتحدة) [١] التي تتم عن طريق الانترنت او انظمة تكنولوجيا المعلومات الاخرى, بالإضافة

(١) المادة (٥١) من ميثاق الامم المتحدة والتي تنص على " ليس في احكام هذا الميثاق ما يضعف او ينقص الحق الطبيعي للدول, فرادى او جماعات, في الدفاع عن انفسهم اذا اعتدت قوة مسلحة على احد اعضاء الامم المتحدة, وذلك الى ان يتخذ مجلس الامن التدابير اللازمة لحفظ السلم والامن الدوليين, والتدابير التي اتخذتها الاعضاء استعمالاً لحق الدفاع عن النفس تبلغ الى المجلس فوراً, ولا تؤثر تلك التدابير باي حال فيما للمجلس – بمقتضى سلطته ومسؤولياته المستمدة من احكام هذا الميثاق – من الحق في ان يتخذ في اي وقت ما يرى ضرورة لاتخاذه من الاعمال لحفظ السلم والامن الدولي او اعادته الى نصابه ", للمزيد ينظر : لحرش فضيل شريف, استثناءات حظر استخدام القوة في ميثاق الامم المتحدة, مقال منشور على موقع اضواء للبحوث والدراسات, متاح على الموقع الالكتروني : https://www.adhwaa.net .

الى استخدام القوة المسلحة (المادة ٢ (٤) من ميثاق الامم المتحدة)[١], ويمكن التأكيد في هذه المرحلة على مايلي :

١. يوجد هجوم مسلح في حالات استخدام القوة المسلحة الشديدة في العلاقات الدولية ذات النطاق والاثار الكبيرة .
٢. يمكن افتراض استخدام القوة المسلحة اذا ادت الانشطة الالكترونية المعنية بشكل غير مباشر الى:
   - الموت او الاصابة الجسدية للكائنات الحية او تدمير الممتلكات .
   - تعطيل هائل ومتوسط وطويل الامد لأنظمة البنية التحتية الحيوية لدولة ما اذا كان تأثيره مساوياً للتدمير المادي للأنظمة المعنية .

والاهم من ذلك ان تقييم الانشطة الالكترونية على انها تمثل استخدام القوة المسلحة يجب ان يستند الى تفسير قائم على التاثيرات للمصطلح, والذي يتوافق تماماً مع النهج القائم على الاثار المتأصلة في القانون الدولي العام, ولا يمكن اعتبار الانشطة الالكترونية بانها تنتهك المادة ٢ (٤) و المادة (٥١) من ميثاق الامم المتحدة الا اذا كانت ولو بشكل غير مباشر تؤدي الى تأثيرات مماثلة للأثار التي عادة ماتسببها او تقصدها استخدام الاسلحة التقليدية او البايولوجية او الكيميائية [٢] .

يشير احد فقهاء القانون في تعليق له ان الجوسسة الالكترونية قد تسبب للامن القومي لدولة ما اضراراً اكبر بكثير من التدمير المادي التي تسببه نظام اسلحة المنشأت العسكرية [٣].

(١) المادة (٢) : ٤ – " يمتنع اعضاء الهيئة جميعاً في علاقاتهم الدولية عن التهديد باستعمال القوة او استخدامها ضد سلامة الاراضي او الاستقلال السياسي لأية دولة او على اي وجه اخر لا يتفق ومقاصد الامم المتحدة ", للمزيد ينظر موقع الامم المتحدة, الفصل الاول : في مقاصد الهيئة ومبادئها, والمتاح على الموقع الالكتروني : https://www.un.org/ar/sections/un-charter/chapter-i/index.html .

(2) Scott J. Shackelford and Richard B. Andres, State Responsibility for Cyber Attacks : Competing Standards for a Growing Problem , Georgetown Journal of International Law 971, 2010, p. 980 .

(3) Russell Buchan, op.cit, p. 79 .

وبشكل عام فان اثار الجوسسة الالكترونية التي هي في الاساس ليست سوى نسخ غير مصرح به للبيانات, لا يمكن مقارنتها بالاثار التي تسببها الاسلحة التقليدية, وبالتالي لا يمكن اعتبارها استخداماً للقوة المسلحة او هجوماً مسلحاً [١] .

لكنه من غير المرجح ان تنتهك الجوسسة الالكترونية قاعدة عدم التدخل نظراً لان مثل هذا السلوك يفتقر الى عنصر الاكراه المطلوب, وبالمثل فأن حظر استخدام القوة لا ينطبق على الجوسسة الالكترونية على اساس ان هذا النشاط لا ينتج عنه ضرر مادي داخل اراضي الدولة الضحية .

المطلب الثاني

الجوسسة الالكترونية باعتبارها انتهاكاً للسيادة الاقليمية

تشير السيادة الى القدرة على ممارسة السلطة الكاملة والحصرية في القانون الدولي, وتزامن ظهور مفهوم السيادة مع ظهور الدولة كوحدة سياسية بعد تقسيم الاراضي والاعتراف السياسي والقانوني بهذا التقسيم الاقليمي بموجب معاهدة وستفاليا [٢] .

بالنتيجة تفهم السيادة على انها حق الدول في ممارسة سلطتها الحصرية على اراضيها, وكذلك يستخدم مبدأ السيادة في القانون الدولي للتعبير عن العلاقة بين الدولة واراضيها, وبناءً على هذا المبدأ يمكن لكل دولة ان تدعي من جميع الدول الاخرى الاحترام الكامل لسلامة اراضيها واستقلالها السياسي[٣].

والاهم من ذلك ان مفهوم السيادة في القانون الدولي هو بنية قانونية على عكس مايسمى بالسيادة السياسية التي تعكس امتلاك السلطة و القوة في الممارسة, وهناك العديد من العناصر لمبدا السيادة وتوفير كل شيء خارج نطاق هذا البحث, باختصار يميلون الى الدوران حول الفعالية الاقليمية, ومن ثم هناك صلة وثيقة بالمبدأ الاقليمي الذي يعد نتيجة طبيعية لدولة لها السيادة على اراضيها .

---

(1) Katharina Ziolkowski (ed.), op.cit, p. 452 .

(2) Nicholas Tsagourias, The Legal State of Cyberspace : in Research Handbook on International Law and Cyberspace, ed. Nicholas Tsagourias and Russell Buchan, Edward Elgar, 2015, P. 15 .

(٣) ويكيبيديا الموسوعة الحرة, سيادة, مرجع سابق .

تسلتزم سيادة الدولة ان يكون لها الحق في وضع القوانين التي تحدد حدود النظام العام للدولة, ويمتد هذا الحق الى الاعمال داخل اراضيها التي لها اثارها في الخارج, والى الاجراءات في الخارج التي لها اثار داخل المنطقة, وان مبدأ السيادة الاقليمية ينص على ان الدول تمارس سلطة كاملة وحصرية على اراضيها ذات السيادة, وتشمل هذه الاراضي, اليابسة والمياه الداخلية والبحر الاقليمي والمياه الارخبيلية والمجال الجوي الوطني (على سبيل المثال السفن والطائرات والاقمار الصناعية) والبنية التحتية المعلوماتية, وبالتالي ليس هناك شك في ان مبدأ السيادة الاقليمية راسخ بقوة في القانون الدولي [١] .

من اجل ان يشكل انتهاكاً لمبدأ السيادة الاقليمية, هل مجرد التدخل في اراضي الدولة امر غير قانوني او هل يجب ان يؤدي التدخل الى ضرر مادي ؟

هذا سؤال مهم في سياق الجوسسة الالكترونية كونها ممارسة تصف الوصول الى المعلومات السرية ونسخها ويتم الالتزام بها بغض النظر عما اذا كانت المعلومات مفقودة او تالفة (بمعنى انها تم

تعديلها او حذفها), باختصار لا يمكن القول بان الجوسسة الالكترونية تتسبب في اضرار مادية.

يجادل (Quincy Wright) من اجل تعريف واسع لمبدأ السيادة الاقليمية, لا يتطلب الحاق ضرر مادي, ويوضح ذلك في سياق الجوسسة التقليدية انه " في اوقات السلم ... التجسس, وفي الواقع, اي اختراق لاقليم دولة من قبل عملاء دولة اخرى هو انتهاك للقانون المحلي, ويعد انتهاكاً لحكم القانون الدولي الذي يفرض على الدول واجب احترام السلامة الاقليمية والاستقلال السياسي للدول الاخرى "[٢].

(1) Ella Shoshan, Applicability of International Law on Cyber Espionage Intrusions, Faculty of Law –Stockholm University, 2014, P. 33 .

(2) Quincy Wright, Espionage and the Doctrine of Non-Intervention in International Affairs, Essays on Espionage and International Law, ed. Richard Falk, Ohio State University Press, 2013, p. 12 .

وعلى نفس الاساس يتم قبول استخدام طائرات الاستطلاع في المجال الجوي الاقليمي لدولة اخرى على انه انتهاك غير مشروع للسيادة الاقليمية لتلك الدولة, وهناك مايؤكد هذا التفسير الواسع لمبدأ السيادة الاقليمية في فقه القانون الدولي, في قضية لوتس اوضحت محكمة العدل الدولية الدائمة ان " القيد الاول والاهم الذي يفرضه القانون الدولي على دولة ما هو انه في حالة عدم وجود قاعدة تسمح بعكس ذلك – لا يجوز لها ممارسة سلطتها بأي شكل من الاشكال في اراضي دولة اخرى " [١], ذلك يعني ان انتهاك السيادة الاقليمية تحدث عندما تقوم دولة بالتدخل غير المصرح به الى اراضي دولة اخرى .

بالانتقال الى الشرعية الدولية للسلوك الالكتروني العابر للحدود, فان السؤال الاول هو ما اذا كانت الدول تمتلك السيادة الاقليمية في الفضاء الالكتروني, كونه سوف يعطي للدولة الحق في ممارسة وظائفها داخل الفضاء الالكتروني .

البعض يؤكدون ان الفضاء الالكتروني عبارة عن بيئة اقليمية, وبسبب العلاقة المترابطة بين الاقليم والسيادة تحتوي الارض على سلطة سيادية ضمن معايير مادية محددة بدقة, فأن المفاهيم القانونية الدولية مثل السيادة الاقليمية لا تنطبق على الفضاء الالكتروني [٢] .

ولكن على وجه الخصوص تكشف ممارسات الدول بوضوح ان الدول تعتبر نفسها تمارس السيادة في الفضاء الالكتروني, وتؤكد انها تمارس السيادة الاقليمية في الفضاء الالكتروني على الرغم ان الفضاء الالكتروني يبدو ظاهرياً محصناً من السيادة الاقليمية كونه مجال افتراضي بلا حدود, الا انه يجب تقدير ان الفضاء الالكتروني هو بيئة من صنع الانسان ويتطلب منه وجود بيئة مادية, ككابلات الالياف الضوئية والاسلاك النحاسية واجهزة الارسال والاستقبال عبر الاقمار الصناعية واجهزة توجيه الانترنت وغيرها, لذلك عندما يتم التداخل مع شبكات الحواسيب, او التدخل في

(1) The Case of the S.S. Lotus, (Merits), 1927, PCIJ Rep Sir A, No 7, P. 18.
(2) David Johnson and David Post, Law and Borders : The Rise of Law in Cyberspace, Stanford Law Review 48, 1996, p. 1367 .

المعلومات الموجودة على تلك الشبكات, تكون اراضي الشبكات مدعومة من خلال البنية التحتية الالكترونية الموجودة فعلياً في اراضي الدولة, ويمكن اعتبار تلك الدولة منتهكة وبالتالي يحدث انتهاك لمبدأ السيادة الاقليمية [١] .

يلاحظ ان القضية الرئيسية ليست لمن تنتمي البنية التحتية الالكترونية, بل اذا كانت تقع على اراضي الدولة, اي ليس من المهم ما اذا كانت البنية التحتية الالكترونية المحمية بموجب مبدأ السيادة الاقليمية تنتمي الى المؤسسات الحكومية او تديرها كيانات خاصة او بواسطة الافرا د, بل تعتبر ممارسات الدول في هذا المجال مفيدة وتشير الى انه عند الوصول الى انظمة الحواسيب والحصول على المعلومات الموجودة على شبكات الحواسيب هذه او التي يتم نقلها من خلالها, تعتبر الدول ان سيادتها الاقليمية منتهكة عندما تكون هذه الشبكات مدعومة بالبنية التحتية الالكترونية الموجودة داخل اراضيها, وان ممارسات الدول تشير الى انه عندما تعتبر الدولة نفسها ضحية للجوسسة الالكترونية, فانها تعتبر مثل هذا السلوك انتهاكاً لمبدأ السيادة الاقليمية, بل قد ينظر اليها على انها تعادل التعدي المادي على اراضي الدولة, ولكن هذه القضايا لم يتم معالجتها بعد في المجتمع الدولي, ومع مرور اكثر من عقد من الزمان لايزال السؤال مفتوحاً بما يتفق مع سياسة الصمت داخل المجتمع الدولي فيما يتعلق بمسائل الجوسسة[٢] .

مثال على ذلك عندما تم الكشف عن قيام الولايات المتحدة بالجوسسة الالكترونية ضد البرازيل, وقيام السيدة ديلما روسيف (Dilma Rousseff) رئيسة البرازيل بالغاء زيارتها الى ولاية واشنطن للقاء ممثلين عن ادارة الرئيس اوباما (Obama) لمناقشة القضايا الهامة ذات الاهتمام الدولي, وانتقلت بدلاً من ذلك الى ولاية نيويورك للتنديد رسمياً بانشطة وكالة الامن القومي امام الجمعية العامة للامم المتحدة, واوضحت ان الجوسسة الالكترونية تنتهك سيادة الدولة, وتم ابلاغ الولايات المتحدة بهذه الاعتراضات التي تعد

(1) Micheal N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare, op.cit, p. 25 .
(2) Katharina Ziolkowski (ed.), op.cit, p. 457-458 .

من الاعمال الغير القانونية, وبدورها طلبت رئيسة البرازيل بالتوضيحات والاعتذارات والضماناتلعدم تكرار مثل هذه الاعمال, وكذلك قامت المانيا بالتصريح ايضاً وادعت ان هذا السلوك غير مقبول تماماً, وقيام فرنسا بالادعاء بانها لا تستطيع قبول هذا النوع من السلوك من الشركاء والحلفاء [١] .

يتبين من ذلك ان الدول تتمتع بالسيادة على اية بنية تحتية الكترونية تقع على اراضيها والانشطة المرتبطة بهذه البنية التحتية الالكترونية, وينطبق مبدأ السيادة على الطبقات الثلاث للفضاء الالكتروني وهي الطبقة المادية والمنطقية والمحتوى, وبغض النظر لمن تنتمي البنية التحتية سواء للمؤسسات الحكومية او الشركات الخاصة ام للافراد, ويجب ان تتم حمايتها بموجب مبدأ السيادة الاقليمية, طالما انها تقع على اراضي تلك الدولة, وان العمليات الالكترونية التي تخترق شبكات وانظمة الحواسيب المدعومة بالبنية التحتية الالكترونية الموجودة داخل اراضي دولة اخرى تؤدي الى انتهاك قاعدة السيادة الاقليمية, بغض النظر عما اذا كانت تلك البنية التحتية الالكترونية يتم تشغيلها من قبل اجهزة الدولة او الجهات الفاعلة الخاصة, وبالتالي فأن حكم السيادة الاقليمية يوفر مصدراً مهماً وقوياً للحماية القانونية ضد الجوسسة الالكترونية .

المطلب الثالث

الجوسسة الالكترونية ومبدأ عدم التدخل

يستخدم الفضاء الالكتروني في المقام الاول كمجال لاتصالات المعلومات, وعلى هذا النحو يمكن ان يتم اعتراض المعلومات السرية للدولة اثناء نقلها عبر البنية التحتية الالكترونية الموجودة في اراضي دولة اخرى, ولايمكن ان يحدث التدخل الا في المجال المحفوظ للدولة, والذي يتم تعريفه بأنه " الاختصاص الداخلي للدولة الذي يصبح بذلك مجموعة من الامور التي تستطيع الدول التصرف بصددها بحرية كاملة دون ان يحدد من قدرتها على تصرف التزام دولي او اتفاقي " [٢] .

(1) Russell Buchan ,The International Legal Regulation of State –Sponsored Cyber Espionage, op.cit, p. 71,72 .

(٢) د. سعد حقي توفيق, مبادئ العلاقات الدولية, دار وائل للطباعة والنشر, عمان – الاردن, ٢٠٠٠, ص ٣٨٨.

وبالتالي فان مبدأ عدم التدخل يمثل محاولة القانون الدولي لحماية الحق السيادي للدولة في تحديد شؤونها الداخلية والخارجية دون تدخل خارجي, ويتضح من ذلك ان مبدأ عدم التدخل مكرس بقوة في القانون الدولي ومدرجة في العديد من المعاهدات الدولية[١] .

وكذلك اظهرت الدول من خلال ممارساتها وجهة نظر واضحة مفادها ان التدخل الخارجي في شؤونهم الداخلية والخارجية محظور بموجب القانون الدولي العرفي, فعلى سبيل المثال, اعلان العلاقات الودية الصادر عن الجمعية العامة للامم المتحدة لعام ١٩٧٠, حيث تصرفت الدول المشاركة بغرض التعبير عن المبادئ ذات الطابع القانوني واعلنت على وجه التحديد ان الدولة ملزمة بعدم التدخل في الامور الواقعة ضمن الولاية القضائية المحلية لأية دولة [٢] .

وفي توضيح نطاق مبدأ عدم التدخل اوضحت محكمة العدل الدولية انه يجب ان يكون التدخل المحظور ذا علاقة بالمسائل التي يسمح فيها لكل دولة, بموجب مبدأ سيادة الدولة ان تقرر بحرية, في اختيار النظام السياسي والاقتصادي والاجتماعي والثقافي, وصياغة السياسة الخارجية, ويعتبر التدخل غير مشروع عندما يستخدم اساليب الاكراه فيما يتعلق بمثل هذه الخيارات التي يجب ان تبقى حرة.

وعلى اساس هذه الفقرة يتكون مبدأ عدم التدخل غالباً من عنصرين اساسين, ذلك يعني انه من اجل حدوث تدخل غير قانوني يجب اثبات ان :

١. الفعل المرتكب يتدخل في الشؤون السيادية للدولة .
٢. ان يكون الفعل قسري بطبيعته [٣].

لذلك سوف يتم النظر من خلال تطبيق هذين العنصرين على اعمال الجوسسة الالكترونية على المعلومات التي يتم خزنها او نقلها عبر البنية التحتية الالكترونية

(1) Maziar Jamnejad and Michael Wood ,The Principle of Non-Intervention, Leiden Journal of International Law 22, 2009, p. 362 .

(٢) القرارات التي اعتمدتها الجمعية العامة خلال دورتها الخامسة والعشرون, رقم القرار A/RES/2625, ٢٤ تشرين الاول ١٩٧٠, المتاح على الموقع : https://www.reseach.un.org/en/docs/ga/quick/regular/25 .

(3) Maziar Jamnejad and Michael Wood, op.cit, p. 347 ; Ella Shoshana, op.cit, p. 44 .

الموجودة داخل اراضي دولة اخرى, اي عندما تقوم الدولة بتخزين المعلومات السرية في خوادم موجودة في دولة اخرى او تنقل هذه المعلومات من خلال البيئة التحتية الالكترونية الموجودة في دولة اخرى, فأن تلك المعلومات تمثل بعداً حاسماً للسيادة الوطنية التي تفترض مسبقاً الدولة القومية, والحق ان حماية هذه المعلومات من الاختراق ينبع من الحق العام للدول في احترام سلامتها السياسية وهذا هو سيادتها, وان الحجة القائلة بأن المعلومات جزء لايتجزأ من سيادة الدولة مقنعة بشكل خاص عندما تتعلق المعلومات التي تم اعتراضها بممارسة الوظائف العامة للدولة, ودعماً لهذا النهج, تنص المادة (٥) من اتفاقية الامم المتحدة بشأن حصانات الدول وممتلكاتها من الولاية القضائية على ان " الدولة تتمتع بالحصانة, فيما يتعلق بنفسها وممتلكاتها, من الولاية القضائية لمحاكم دولة اخرى [١] .

والنتيجة هي ان البيانات التي تنتمي الى دولة ولكن يتم تخزينها او نقلها عبر البنية التحتية الالكترونية الموجودة على اراضي دولة اخرى تمتلك سيادة البيانات الوطنية والتدخل في تلك البيانات (على سبيل المثال لغرض الجوسسة) يعتبر تدخلاً في سيادة الدولة [٢] .

اما عند فحص مبدأ عدم التدخل بخصوص المادة ٢ (٤) من ميثاق الامم المتحدة[٣], يتم وصف كلمة تدخل لحظر الاكراه او التدخل الديكتاتوري في الشؤون الداخلية للدولة من قبل دولة اجنبية, و وفقاً لهذا التفسير الصارم فان العنصر التدخلي للجوسسة الالكترونية ليس تدخلاً بمعنى المبدأ كونه يفتقر الى العنصر القسري او الديكتاتوري, ومع ذلك وجد انه من خلال تطبيق منظور اوسع حيث يتم الجمع بين مبدأ عدم التدخل

(١) المادة (٥) من اتفاقية الامم المتحدة لحصانات الدول وممتلكاتها من الولاية القضائية, اعتمدت بموجب قرار الجمعية العامة للأمم المتحدة رقم ٥٩/٣٨ المؤرخ في ٢ كانون الاول لعام ٢٠٠٤, مكتبة حقوق الانسان, جامعة مينيسوتا .

(٢) Russell Buchan, op.cit, p. 76 .

(٣) المادة (٢) : ٤ – " يمتنع اعضاء الهيئة جميعاً في علاقاتهم الدولية عن التهديد باستعمال القوة او استخدامها ضد سلامة الاراضي او الاستقلال السياسي لأية دولة او على اي وجه اخر لا يتفق ومقاصد الامم المتحدة ", للمزيد ينظر موقع الامم المتحدة, الفصل الاول : في مقاصد الهيئة ومبادئها, والمتاح على الموقع الالكتروني : https://www.un.org/ar/sections/un-charter/chapter-i/index.html .

ومبادئ السيادة والولاية القضائية الاقليمية, يمكن بالفعل اعتبار الجوسسة الالكترونية بمثابة تدخل غير قانوني [١] .

ويمكن القول ان الجوسسة الالكترونية تمثل على اقل تقدير وبشكل صريح خرقاً لمبدأ عدم التدخل في الشؤون الداخلية للدول, وخرقاً لمبدا سيادة الدول واستقلالها والذي اقرته المادة (٢) من ميثاق الامم المتحدة في فقرتيها (٤) و (٧) واكدت عليه الامم المتحدة في العديد من قراراتها واعلاناتها, كما تبنتها العديد من المنظمات الاقليمية في مواثيقها واعتمدها القضاء الدولي في العديد من قراراته .

الخاتـــمـــة

بعد هذا التقديم الذي تناولنا فيه موضوع الاتجاهات الجديدة للجوسسة الالكترونية في القانون الدولي, لابد وان نضع له خاتمة تلخص اهم الاستنتاجات والمقترحات التي تضمنها البحث وكما يلي :

اولاً : الاستنتاجات

١- بالرغم من الكم الهائل من التعاريف التي حظيت بها ظاهرة الجوسسة, وبذل الكثير من الجهود من قبل الجميع لتحقيق هدف ؛ الا وهو تعريف عام وشامل للجوسسة, ومع ذلك لم تفلح هذه الجهود بالخروج بتعريف موحد وشامل لهذه الظاهرة, اي عدم وجود اجماع فقهي جامع ومانع للجوسسة الالكترونية على الصعيد الدولي او القانوني او الفقهي, ويرجع ذلك الى عدة امور منها الاختلاف حول تحديد نطاق الجوسسة الالكترونية, كون البعض من الفقه وسع من هذا نطاق, والبعض الاخر يراه من منظور ضيق .

٢- بالإضافة الى عدم وجود اتفاق شامل حول مفهوم الجوسسة الواقعية, جاء التحول الى العصر المعلوماتي والرقمي وبروز الفضاء الالكتروني ليضع نقاط غموض اخرى امام محاولات التصدي لإعطاء مفهوم للجوسسة الالكترونية .

(1) Ella Shoshana, op.cit, p. 44-45 .

٣- عكست الجوسسة الالكترونية الصورة , حيث ان الدول المتقدمة ما بعد الصناعية معرضة بشكل خاص للجوسسة الالكترونية, بسبب مستوى وتعقيد تكنولوجيا المعلومات المستخدمة, وكونها تخسر الكثير من حيث التقدم التكنولوجي والريادة التنافسية في السوق العالمية .

٤- من ناحية الجوسسة الالكترونية وحقوق الانسان يتضح ان الجوسسة الالكترونية تتعارض مع الحق في الخصوصية على النحو الوارد في المادة (١٧) من العهد الدولي الخاص بالحقوق المدنية والسياسية, والمادة (٨) من الاتفاقية الاوروبية لحقوق الانسان, والتي تحمي معلومات الشخص واتصالاته من التدخل, ولكن الخصوصية ليست حقاً مطلقاً, بل هناك بعض الحالات التي حددها الدستور واكد عليها القانون الوطني التي يمكن فيها من تقييد هذا الحق في سياق المراقبة الالكترونية .

٥- الجوسسة الالكترونية لا تقع ضمن نطاق المادة ٢ (٤) من ميثاق الامم المتحدة وحظر استخدام القوة, كون الجوسسة الالكترونية لا تشمل بحد ذاتها استخدام القوة ولا تتضمن في جوهرها استخدام القوة .

٦- العمليات الالكترونية التي تخترق شبكات وانظمة الحواسيب المدعومة بالبنية التحتية الالكترونية الموجودة داخل اراضي دولة اخرى تؤدي الى انتهاك قاعدة السيادة الاقليمية, بغض النظر عما اذا كانت تلك البنية التحتية الالكترونية يتم ادارتها من قبل اجهزة الدولة او الجهات الفاعلة الخاصة, وبالتالي فان حكم السيادة الاقليمية يوفر مصدراً مهماً وقوياً للحماية القانونية ضد الجوسسة الالكترونية .

٧- الجوسسة الالكترونية تمثل على اقل تقدير وبشكل صريح خرقاً لمبدأ عدم التدخل في الشؤون الداخلية للدول, وكذلك مبدا سيادة الدول واستقلالها والذي اقرته المادة (٢) من ميثاق الامم المتحدة في فقرتيها (٤) و (٧) واكدت عليه الامم المتحدة في العديد من قراراتها واعلاناتها, كما تبنتها العديد من المنظمات الاقليمية في مواثيقها واعتمدها القضاء الدولي في العديد من قراراته

ثانيا : المقترحات

١- نقترح ان يسعى المجتمع الدولي الى ايجاد مفهوم جامع ومتفق عليه حول مفهوم الجوسسة الالكترونية وتحديد خطة عملية دولية للإسهام في وضع حد لهذه الظاهرة الخطيرة ومكافحتها والحد منها, مع احترام سيادة الدول الاعضاء .

٢- عقد اتفاقيات دولية فعالة لمكافحة انشطة الجوسسة الالكترونية وتنظيم الاجراءات المتعلقة بالحماية والوقاية من هذه الانشطة, وتفعيل اتفاقيات تسليم الجناة في نطاق الجوسسة الالكترونية, بالإضافة الى استيعاب هذه الاتفاقيات لجميع المستجدات والمغيرات التي تطرأ على هذه الانشطة .

٣- السعي الى تخصيص قانون مستقل موحد ومنظم وشامل لجميع اشكال وصور الجوسسة الالكترونية, يتم تقنينه من خلال لجنة قانونية وفنية متخصصة في هذا المجال, ويتم فيها معالجة جميع اساليب الجوسسة الالكترونية وخاصةً الاساليب الحديثة منها, وكذلك يعالج أوجه الاشكالات والاختلافات القائمة بين قوانين الدول بما يتوافق والقانون الدولي, والعمل على توقيع اشد انواع العقوبات على الدول التي تتبنى الجوسسة بصورة عامة والجوسسة الالكترونية بصورة خاصة, والتي تعد اخطر انواع الجوسسة كونها تقع في بيئة هادئة وصعوبة اكتشافها وملاحقة الجناة فيها .

٤- يقترح حماية الاسرار الامنية والعسكرية والسياسية بكافة السبل مخافة وقوعها بيد دول معادية او منظمات ارهابية تستعملها في زعزعة استقرار الدول وابتزاز الحكومات, ويقترح عزل المعلومات العسكرية والامنية عن الشبكة العالمية (الانترنت) قدر المستطاع, مع وضع انظمة حماية جيدة وصارمة للمخولين بالاطلاع عليها, وبالنسبة للمعلومات الاقتصادية فأنها اصبحت من العوامل الرئيسية والمهمة لحفظ سيادة الدول واستقرارها الامني, وبدأ العالم بالتسابق حول الحرب المعلوماتية الاقتصادية, واصبح الاقتصاد يشكل عصبة الامم ونهضتها وقوتها, لذلك ينبغي حماية هذه المعلومات بصورة صحيحة و وضعها بالحسبان ان اي اختراق لهذه المعلومات من قبل القراصنة و الجواسيس, لاسيما

المنظمات المعادية والارهابية سوف يعرض كيان الدولة للانهيار ويشلها رويداً رويداً .

٥- نقترح قيام الدولة على تدريب الكوادر على استخدامات تقنيات الحواسيب الالية والانترنت, والعمل على تكثيف الدورات التدريبية للكوادر والقيادات والموظفين المختصين في مجال المعلومات, وإعداد المؤتمرات والندوات والحوارات واللقاءات و ورش العمل اللازمة لتزويد الكوادر بالخبرات والثقافة الالكترونية المطلوبة في هذا المجال, من اجل الحصول واكتساب مهارات عالية في مجال حماية المعلومات الالكترونية وتأمينها, كي تؤهلهم لإجراء تقنيات الحماية والسرية .

المصادر

أولاً : الكتب

١- د. جابر المراغي, جرائم انتهاك اسرار الدفاع عن البلاد من الناحيتين الموضوعية و الاجرائية, دار النهضة العربية, القاهرة, مصر, ١٩٨٨ .

٢- حسنين المحمدي البوادي, ارهاب الانترنت الخطر القادم, الطبعة الاولى, دار الفكر الجامعي, الاسكندرية, ٢٠٠٦ .

٣- ريتشارد إيه كلارك, روبرت كيه كنيك, حرب الفضاء الالكتروني التهديد التالي للأمن القومي وكيفية التعامل معه, ط ١, الامارات للدراسات والبحوث الاستراتيجية, ابوظبي, ٢٠١٢.

٤- سعد ابراهيم الاعظمي, التجسس في التشريع العراقي, الطبعة الاولى, دار الكتب للطباعة والنشر, الموصل – العراق, ١٩٨١ .

٥- د. سعد حقي توفيق, مبادئ العلاقات الدولية, دار وائل للطباعة والنشر, عمان, ٢٠٠٠ .

٦- ضرغام جابر عطوش آل مواش, جريمة التجسس المعلوماتي دراسة مقارنة, الطبعة الاولى, المركز العربي للنشر والتوزيع, جمهورية مصر العربية – القاهرة, ٢٠١٧ .

٧- عبد الاله النوايسة, جرائم تكنلوجيا المعلومات – شرح الاحكام الموضوعية في قانون الجرائم الالكترونية, الطبعة الاولى, دار وائل للنشر والتوزيع, عمان, الاردن, ٢٠١٧.

٨- د. علي عبود جعفر, جرائم تكنولوجيا المعلومات الحديثة الواقعة على الاشخاص والحكومة دراسة مقارنة, الطبعة الاولى, مكتبة زين الحقوقية والادبية, لبنان, ٢٠١٣ .

٩- د. مجدي محمود محب حافظ, موسوعة جرائم الخيانة والتجسس, الطبعة الاولى, المركز القومي للاصدارات القانونية, القاهرة, ٢٠٠٨ .

١٠- محمد راكان الدغمي, التجسس واحكامه في الشريعة الاسلامية, الطبعة الثانية, دار السلام للطباعة والنشر والتوزيع, القاهرة, ١٩٨٥ .

١١- د. محمود سليمان موسى, التجسس الدولي والحماية الجنائية للدفاع الوطني وأمن الدولة, دراسة مقارنة في التشريعات العربية والقانونين الفرنسي والايطالي, الطبعة الاولى منشأة المعارف, الاسكندرية, ٢٠٠١ .

١٢- د. هشام المصري, الامن المعلوماتي احد الاعمدة الرئيسية للأمن القومي (اختراقه – احتوائه), الطبعة الاولى, مكتبة الوفاء القانونية, الاسكندرية ' مصر, , ٢٠١٩ .
١٣- وولفغانغ كريغر, تاريخ المخابرات من الفراعنة حتى وكالة الامن القومي الامريكية (NSA), ترجمة عدنان عباس علي, عالم المعرفة للنشر, الكويت, ٢٠١٨ .

ثالثاً : الاطاريح والرسائل الجامعية

١- أياد خلف محمد المفرجي, المنازعات الدولية ذات الطابع الالكتروني, رسالة ماجستير, كلية القانون والعلوم السياسية, جامعة كركوك, جمهورية العراق, ٢٠١٩ .
٢- عثمان بن علي بن صالح, جريمة التجسس وعقوبتها في الشريعة الاسلامية و القانون الوضعي, رسالة ماجستير مقدمة الى قسم العدالة الجناية " تخصص التشريع الجنائي والاسلامي " .
٣- محمد عدنان عثمان, دور القانون الدولي في مواجهة التجسس الدبلوماسي, رسالة ماجستير في القانون العام, كلية الحقوق, جامعة الشرق الاوسط, عمان, ٢٠١٥ .

رابعاً : البحوث والدوريات

١- أ. سلامي نادية, التجسس الالكتروني كأثر للأستخدام غير المشروع للفضاء الالكتروني على امن الدولة الخارجي, بحث منشور في مجلة دراسات جامعة عمار ثليجي بالاغواط, الجزائر, العدد ٥٦, ٢٠١٧ .
٢- عبدالاله محمد النوابسة, ممدوح حسن العدوان, جرائم التجسس الالكتروني في التشريع الاردني (دراسة تحليلية), مجلة علوم الشريعة والقانون, المجلد ٤٦, العدد ١, الملحق ١, ٢٠١٩ .
٣- عبد الرحمن لحرش, التجسس والحصانة الدبلوماسية, مجلة الحقوق, جامعة الكويت , المجلد ٢٧, العدد ٤, ٢٠٠٣ .

خامساً : المواثيق والاتفاقيات الدولية

المواثيق الدولية

١. ميثاق الامم المتحدة لعام ١٩٤٥ .
٢. الاعلان العالمي لحقوق الانسان المعتمد في ١٠ ديسمبر ١٩٤٨ .

الاتفاقيات الدولية

١- الاتفاقية الخاصة باحترام قوانين واعراف الحرب البرية - معاهدات لاهاي, ١٨ اكتوبر / تشرين الاول ١٩٠٧.
٢- العهد الدولي الخاص بالحقوق المدنية والسياسية, المعتمد بموجب قرار الجمعية العامة للامم المتحدة ٢٢٠٠ أ (د-٢١) المؤرخ في ١٦ كانون الثاني ١٩٦٦ .
٣- الاتفاقية الامريكية لحقوق الانسان ١٩٦٩ .
٤- اتفاقية الامم المتحدة لحصانات الدول وممتلكاتها من الولاية القضائية, اعتمدت بموجب قرار الجمعية العامة للامم المتحدة رقم ٥٩/٣٨ المؤرخ في ٢ كانون الاول لعام ٢٠٠٤, مكتبة حقوق الانسان, جامعة منيسوتا .

سادساً : الوثايق الدولية

١- القرارات التي اعتمدتها الجمعية العامة خلال دورتها الخامسة والعشرون, رقم القرار A/RES/2625, ٢٤ تشرين الاول ١٩٧٠ .
٢- UN HRC, Report of the Special Rapporteur on the Promotion and Protection of the Right to the Freedom of Opinion and Expression, Frank La Rue, UN Doc A/HRC/23/40, 17 April 2013 .

سابعاً : القوانين الوطنية

١- قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩ المعدل .
٢- مشروع قانون الجرائم المعلوماتية العراقي لسنة ٢٠١١ .

ثامناً : المؤتمرات والندوات والتقارير

١- علي بن محمد بن سالم العدوي, مكافحة التجسس الالكتروني في القانون العماني مقارنة بالشريعة الاسلامية والقانون الجنائي الدولي, المؤتمر الدولي الاول, العلوم الشرعية تحديات الواقع وافاق المستقبل, كلية العلوم الشرعية, ديسمبر ٢٠١٨ .

تاسعاً : المواقع الالكترونية (الانترنت)

١- المادة (١٧) الحق في حرمة الحياة الخاصة : متاح على الموقع الالكتروني : https://www.hrlibrary.umn.edu/arabic/hrc-gc16.html .
٢- شيرين الضاني, الامن القومي ومشروعيته في الاسلام, مقال منشور على موقع الحوار المتمدن, العدد ٣١٦٠ – ٢٠١٠, والمتاح على الموقع الالكتروني : https://www.ahewar.org/debat/show.art.asp?aid=232581 .
٣- لحرش فضيل شريف, استثناءات حظر استخدام القوة في ميثاق الامم المتحدة, مقال منشور على موقع اضواء للبحوث والدراسات, متاح على الموقع الالكتروني : https://www.adhwaa.net .
٤- معجم المعاني الجامع, معجم عربي-عربي, تعريف ومعنى الامن القومي, متاح على الموقع الالكتروني, https://www.almaany.com/ar/dict/ar-ar/ .
٥- لمؤتمر الدولي الخامس والثلاثون لمفوضي حماية البيانات والخصوصية, قرار بشأن ترسيخ حماية البيانات وحماية الخصوصية في القانون الدولي, وارسو, تشرين الاول ٢٠١٣, متاح على الموقع الالكتروني : https://Privacyconfenence2013.org/web/pagefiles/kefinder/files/5 .
٦- موقع الامم المتحدة, الفصل الاول : في مقاصد الهيئة ومبادئها, والمتاح على الموقع الالكتروني : https://www.un.org/ar/sections/un-charter/chapter-i/index.html.
٧- ويكيبيديا الموسوعة الحرة, فضاء الكتروني, متاح على الموقع الالكتروني : http://ar.wikipedia.org/wiki/ .

❖ **المصادر والمراجع باللغات الاجنبية**

First : Books and Researches

1- Christina Skinner, An International Law Response to Economic Cyber Espionage, 46 Connecticut Law Review, 2014 .
2- David Johnson and David Post, Law and Borders : The Rise of Law in Cyberspace, Stanford Law Review 48, 1996 .
3- Ella Shoshan, Applicability of International LAW on Cyber Espionage Instrusions, Thesis combined with practical experience in International Law, Faculty of Law –Stockholm University, 2014 .
4- Ghandi, The Human Rights Committee and the Right of Individual Communication : Law and Practice, Ashgate Publishing, 1998 .
5- Jonathan Eric Lewis, THE ECONOMIC ESPIONAGE ACT AND THE THREAT OF CHINESE ESPIONAGE IN THE UNITED STATES, University of Connecticut School of Law, 2010 .

6- Karen Sepura, Economic Espionage : The Front Line of a New World Economic War, 26 Syracuse Journal of International Law and Commerce, 1998-1999 .

7- Katharina Ziolkowski (ed.) ,Peacetime Regime for State Activities in Cyberspace :(International Law, International Relations and Diplomacy), NATO CCD COE Publication, Tallinn, Estonia ,2013 .

8- Maziar Jamnejad and Michael Wood ,The Principle of Non-Intervention, Leiden Journal of International Law 22, 2009 .

9- Micheal N. Schmitt, "Tallin Manual on the International Law Applicable to Cyber Warfare", first publishes, Cambridge University Press, 2013 .

10- Nicholas Tsagourias, The Legal State of Cyberspace : in Research Handbook on International Law and Cyberspace, ed. Nicholas Tsagourias and Russell Buchan, Edward Elgar, 2015 .

11-Professeur Gerard Cohnathan, Professeur Robert Kovar, L espionage en temps de paix, Annuaire francais de droit international, Paris, volume 6, 1960 .

12- Quincy Wright, Espionage and the Doctrine of Non-Intervention in International Affairs, Essays on Espionage and International Law, ed. Richard Falk, Ohio State University Press, 2013 .

13- Russell Buchan, The International Legal Regulation of State – Sponsored Cyber Espionage, in Anna – Maria Osule and Henry Roigas (eds), International Cyber Norms : Legal, Policy and Industry Perspective (NATO CCD COE Publishations, 2016 .

14-Scott J. Shackelford and Richard B. Andres, State Responsibility for Cyber Attacks : Competing Standards for a Growing Problem , Georgetown Journal of International Law 971, 2010 .

15- The Case of the S.S. Lotus, (Merits), 1927, PCIJ Rep Ser A, No 7 .

Second : Electronic Resources

1- Global Principle on National Security and the Right to Information, 12 June 2013 ,available on website : https://www.opensocietyfoundations.org/sites/default/ .