AL-NAHRAIN UNIVERSITY
COLLEGE OF LAW
ISSN:3006- 0605 DOI:10.58255

تهديدات الأمن السيبراني وحق الدول في الدفاع الالكتروني عنها ـ دراسة تحليلية وصفية ـ

Cybersecurity threats and the right of states to defend themselves electronically - A - descriptive analytical study

أ.م.د. بريز فتاح يونس
جامعة كركوك / كلية القانون والعلوم السياسية
Dr.parez-fattah@uokirkuk.edu.iq
Ass.Pro. Dr. PAREZ FATTAH YOUNIS
Kirkuk University / College of Law and Political Science
Dr.parez-fattah@uokirkuk.edu.iq

المستخلص لعب الأمن السيبراني دوراً بارزاً في ميدان العلاقات الدولية وخلال العقود الاخيرة ،اذ التوجه الدولي الى الحوسبة والاعتماد على البرامج الالكترونية والانترنيت في مختلف قطاعات الدولة،ودخول القطاع الخاص وخصوصاً المالية والبنوك في هذا المجال السريع واللامحدود في تنظيم عمل الاسواق والتبادل والتحويلات المالية ،مما حذا بالغير من الدول والتنظيمات المعادية الى فكرة تحويل الهجمات العسكرية والاضرار الى جانب سريع ومن الاماكن البعيدة، والذي سوف يلحق اضراراً لاتعرف عقباه ولا الاشخاص ولا الاموال وحتى البنى التحتية ومتطلبات الحياة اليومية للافراد من الماء والكهرباء وغيرها.

حاولت الدول الى البحث عن الاليات الدولية التي تعطي لها الحق في مواجهة هذه الهجمات والانتهاكات التي تطال أمنها وسيادتها وذلك بالاستناد الى التراخيص الدولية التي منحتها لهم الجمعية العامة للامم المتحدة من الدفاع عن السيادة السيبرانية للدول باعتبارها جزءاً مهماً من جوانب السيادة والسلطة للدول، ومن جانب أخر تضع الدول في مواجهة تلك الانتهاكات مسألة الدفاع الشرعي السيبراني من خلال وضع البرامج والاشخاص المتضلعين بخبرة هذه الانظمة وادخالهم في مجالات السلك العسكري باعتبارهم جنود الميدان ومن خلف الشاشات والبرامج المعقدة في سبيل حماية أمن الدول وسلامتهم.

الكلمات المفتاحية : الأمن السيبراني– السيادة السيبرانية–الدفاع الشرعي السيبراني–أبعاد الامن السيبراني– التهديدات السيبرانية

Abstract Cyber security has played a prominent role in the field of international relations in recent decades. The global trend towards computing and reliance on electronic programs and the internet across various sectors of government, coupled with the rapid and unprecedented entry of the private sector, particularly finance and banking, into this field to regulate markets, exchanges, and financial transfers, has prompted hostile states and organizations to consider shifting military attacks and inflicting damage

from remote locations. This would cause unpredictable and potentially devastating consequences for individuals, property, infrastructure, and even essential services like water and electricity.

States have tried to find international mechanisms that give them the right to confront these attacks and violations that affect their security and sovereignty, based on the international licenses granted to them by the United Nations General Assembly to defend the cyber sovereignty of states as an important part of the aspects of sovereignty and authority of states. On the other hand, states put the issue of legitimate cyber defense in the face of these violations by putting in place programs and people who are well-versed in the expertise of these systems and bringing them into the fields of the military as soldiers in the field and behind the screens and complex programs in order to protect the security and safety of states.

Keywords (Cyber security - Cyber Sovereignty - Cyber Defense - Dimensions of Cyber security - Cyber Threats).

المقدمة

ان التطور الكبير والاكتشافات الالكترونية السريعة التي رافقت المجتمع الدولي خلال الفترة السابقة،والثورة البرمجية والمعرفية في عالم يضج بالتهديدات والتسلح العسكري والمخاوف من الاخرين ،وعدم الاستقرار التي عصفت بالمجتمع الدولي بسبب الاعمال العدائية وتوتر العلاقات القطبين المتحكمتين بالقوة، كلها كانت تدور حول حماية أمن الدول واستقرارها وتقيد سيادة الاخرين في الاعتداء أو الانتقاص من حقوق غيرهم في هذا المجال.

وبرزت خلال هذه المرحلة وخصوصاً في القرن الحادي والعشرين الاعتماد على الجانب الالكتروني وتنظيم المعلومات والامور المهمة للدول ضمن البرمجيات الالكترونية وانتشار الانترنيت وتوجه الدول الى جانب الارشفة الالكترونية وربط العديد منها بالمجالات السيبرانية كالماء والطاقة والاقتصاد والبنوك والحماية الأمنية وظهور الاسلحة الذكية كلها أصبحت تشكل تهديدات تجاه الامن القومي للدول ومصالحها بسبب اختلاف توجه الانظار من الحروب التقليدية الى الحروب السيبرانية وتعريض الامن السيبراني للدول الى الهلاك والتدمير.

ونتيجة للتقارير الدولية التي تنشرها الهيئات والمنظمات الدولية المهتمة بهذا الجانب ،من كون المخاطر الحقيقية للامن السيبراني بلغت كونها تأتي بالمرتبة الرابعة من مجموع المخاطر العالمية من حيث تأثيرها خلال مدة العامين المقبلين بعد عام ٢٠٢٤،وتصل هذه المخاطر الى المرتبة الثامنة عالمياً خلال مدة العشر أعوام القادمة،وهذا بدوره حتمت على الدول من جهة والهيئات الدولية من جهة أخرى اللى تدارك هذه المخاطر الحقيقية وايجاد الوسائل القادرة في مواجهتها ومن ثم افساح المجال للدول باستخدام الطرق الشرعية والمقبولة دولياً في الدفاع عن هذه الهجمات كونها تشكل مساساً وانتهاكاً لحقوق الدول في محيط العالم أجمع فالحماية واجبة واستخدام حق الدفاع الشرعي السيبراني أحد المجالات الحيوية لهذا الحق بالاضافة الى كونها تمثل حقاً سيادياً سيبرانيا تعمل الدول على احاطتها بالمتابعة والدفاع ،لانها من الحقوق السيادية للدول ومجالاً حيوياً تمارس الدول سلطاتها عليها وهي تمثل الجزء المتمم لأركان الدولة من بعد البر والبحر والجو.

مشكلة البحث تكمن المشكلة الرئيسية للبحث في ان الامن السيبراني للدول أصبحت متطورة بشكل ملحوظ في الاونة الاخيرة بسبب التطورات الكبيرة في الناحية العلمية والالكترونية وتحول الدول نحو تنظيم ادارة الحكومات في ظل هذه الانظمة الالكترونية والاهتمام بها ومحاولة ربط مرافق الدولة جميعها بالانظمة الحديثة تلك، مما يجعلها في خط الصد الاول من الهجمات من لدن الدول والتجمعات الاخرى التي تهدف الى النيل من هذه الحكومات وافشال انظمتها الحيوية وخصوصا المتعلقة بالمال والسلاح منها أي القوة العسكرية والمصارف والبورصات المالية وغيرها ، مما يؤثر بدورها على الامن القومي لهذه الدول، وبذلك يتطلب الامر ايجاد الحلول الدولية والتعاون في سبيل حمايتها والمحافظة على استقرار الدول وأنظمتها.

أهمية البحث تتجلى اهمية الدراسة هذه في مجال القانون الدولي العام من خلال بيان الفراغ التشريعي الدولي في مسألة الامن السيبراني وحمايته وكذلك الضعف الذي ينتاب العلاقات الدولية في مجال التعاون من أجل درء تلك المخاطر وويلاتها ،اذ أصبح الامن السيبراني مجالا للصراع والنزاع فيما بين الدول ،وهي مؤثرة بشكل واسع على مصالح الامن القومي للدول مما يستدعي البحث لايجاد فرص النجاة والحماية لهذا المجال الحيوي من حياة الدول التي لها دور بارز في المجتمع الدولي ويتطلب البحث والدراسة عنها .

منهجية البحث فقد استخدمنا طريقة المنهج التحليلي من اجل بيان معاني البحث ومفرداته الرئيسية بالاضافة الى الجانب الوصفي من أجل الاحاطة قدر الامكان لبيان الجهود الدولية الرامية لتحقيق الحماية لهذا الجانب المهم من أنظمة الدول والدفاع عنها .

خطة البحث بغية تسليط الضوء عن موضوع البحث هذا بشكل واضح ومفيد، ارتأينا تقسيم البحث الى مبحثين رئيسين، الاول يكون بخصوص بيان معنى الامن السيبراني وعلى مايشتمله هذا المفهوم في ظل الجهود الدولية في الوقت الراهن بالاضافة الى أنواع التهديدات التي تواجههاجراء تطور أنظمة ادارة الدول ومرافقها ،أما المبحث الثاني سيكون بخصوص أبرز المجالات التي تكون من حق الدول في الدفاع عنها كحماية دولية بدءاً من كونها حق سيادي بهم، مرورا بكونها من المبادئ القانونية المتعلقة بحقها في الدفاع الشرعي عنها ضمن الفضاء السيبراني الخاص بانظمتها ومجالات عملها ، واخيرا نحاول تقديم فكرة موجزة عن ابرز الاستنتاجات والتوصيات التي توصلنا اليها من خلال بحثنا هذا.

المبحث الأول

التعريف بالأمن السيبراني والتهديدات التي تواجهها

ان الامن السيبراني هو محال حديث النشأة ظهرت في الاوساط الدولية بعد التطورات التكنولوجية الرقمية التي عصفت المجتمع الدولي ،مما ادى بدورها توجه الحكومات للاستفادة منها في مجال اتمت المعلومات الحكومية وتباع الحكومة الالكترونية بغية تقليل الوقت والجهد في انجاز اعمالها ،بالاصتفة الى السرعة والدقة في اتمامها فضلا عن خزن وأرشفة المعلومات بكافة انواعها لكي تكون في متناول ايدي الحكام والمسؤولين في الدولة لسهولة الرجوع اليها ،مما عكس لنا في الجانب الاخر من هذه الميزات ظهور مطامع الدول والتنظيمات في الحاق الاضرار بالدول وشل

عمل الحكومات في توجيه ضربات قاضية الى تلك الارشفة والمعلومات وسواء كانت عسكرية وأمنية أم يخص الجانب المالي والاقتصاد للدول ،فأصبح من الضروري ايجاد طريقة لمعالجة هذه المشاكل وحصنها أمنيا من هذه الاعتداءات وحمايتها،وبغية الاطلاع عن كثب لمفوم الامن السيبراني قسمنا هذا المبحث الى مطلبين نتكلم في الاول عن التعريف بالمصطلح وفي الثاني عن أهمية وابعاد هذا المفهوم على أمن الدول وسيادتهم.

المطلب الاول

مفهوم الامن السيبراني

ان بيان مفهوم الامن السيبراني(١) قد لاقت اهتمام الشراح والفقهاء نظرا لاهميتها السياسية والقانونية ومدى تأثيرها على استقرار الوضع الدولي وحماية أمن الدول ومعلومات افرادها ومؤسساتها.

فقد اختلف اراء الفقهاء والشراح حول بيان المنطلق من هذا المفهوم فقد ذهب البعض الى اضفاء صفة مصطلح الحرب السيبرانية عليه وذلك بالاستناد الى الفكرة الامنية والعسكرية التي تضع هدفها في الوصول الى تحقيقها وفق هذا الجانبين، في حين حاول الأخرون استخدام مفردة الهجمات السيبرانية عليها بانها الهجمات الالكترونية التي يراد منها شل عمل الاجهزة الرقمية وتعطيل البيانات الاساسية للدولة ،اذ يبتغي من وراءها الوصول الى الاهداف الأمنية والعسكرية والذي تدار عمل الاجهزة الرئيسية للدولة ومصادر الطاقة وغيرها. (٢)

وقد تضافرت الجهود الدولية في مجال اعطاء الوصف التعريفي للامن السيبراني من خلال بيان المصطلح من خلال الاتحاد الدولي للاتصالات (٣) ، بانها تعني""وصف مجموعة الادوات والسياسات والمبادئ التوجيهية ونهج ادارة

---

(١) ان المعنى اللغوي لمصطلحي الامن السيبراني مكوّن من مقطعين وهما: "الأمن"، و"السيبراني"

- فالأمن: هو نقيض الخوف، أي بمعنى السلامة. والأمن مصدر الفعل أَمِنَ أَمْناً وأَمَاناً وأَمَنَةً: أي اطمئنان النفس وسكون القلب وزوال الخوف، ويقال: أَمِنَ من الشر، أي سَلِمَ منه. وقد عرّفه قاموس بنغوين للعلاقات الدولية بأنه مصطلح يشير إلى غياب ما يُهدد القيم النادرة .
- أما مصطلح السيبرانية هو واحد من أكثر المصطلحات تردداً في معجم الأمن الدولي في الوقت الراهن، وتشير المقاربة الإيتيمولوجية لكلمة "cyber" إلى أنها لفظة يونانية الأصل مشتقة من كلمة "kybernetes" بمعنى الشخص الذي يدير دفة السفينة، حيث تستخدم مجازاً للمتحكم "governor". وتجدر الإشارة إلى أن العديد من المؤرخين يرجعون أصلها إلى عالم الرياضيات الأمريكي(norbert wieners) وذلك للتعبير عن التحكم الآلي، فهوكما يقال عنه هو الأب الروحي المؤسس للسبرنيتيقية من خلال مؤلفه الشهير: Cybernetics or control and communication in" the Animal and the machine وقد أشار في كتابه إلى أن السبرنتيقية هي التحكم والتواصل عند الحيوان والآلة والإنسان والآلة ليستبدل مصطلح الآلة بعد الحرب العالمية الثانية بالحاسوب. وللمزيد حول هذا ينظر :- الموسوعة السياسية ،المتاح على الرابط :- https://political-encyclopedia.org/dictionary /

(٢)د.فارس محمد العمارات وابراهيم محمد الحماصة ،الامن السيبراني (المفهوم وتحديات العصر،ط١،دار الخليج للنشروالتوزيع ،عمان – الاردن ،٢٠٢٢،ص ١٣ ومابعدها .

(٣)الاتحاد الدولي للاتصالات هو وكالة الأمم المتحدة المتخصصة في مجال التكنولوجيات الرقمية (ICT).وتتألف المنظمة من ١٩٤ دولة عضوا وأكثر من ١٠٠٠ شركة وجامعة ومنظمة دولية وإقليمية. يقع مقر الاتحاد في جنيف، سويسرا، وله مكاتب إقليمية في كل

المخاطر والاجراءات والتدريب وأفضل الممارسات وأليات الضمان والتقنيات التي يمكن استخدامها من حماية توفر وسلامة وسرية الاصول في البنى التحتية الموصولة التابعة للحكومة والمنظمات الخاصة والمواطنين وتشمل هذه الاصول اجهزة الحوسبة الموصولة والموظفين والبنية التحتية والتطبيقات والخدمات وأنظمة الاتصالات والبيانات في البيئة السيبرانية"". (١)

نرى من خلال التعريف اعلاه بان الامن السيبراني ذو اهمية كبيرة ليس على الحكومات فقط بل وحتى المنظمات والافراد على حد سواء بسبب التحولات الرقمية واتجاه العالم اجمع نحوالحكومة الالكترونية وأرشفة البيانات والمعلومات على الحواسيب والاجهزة الالكترونية المتصلة مع بعضها البعض.

في حين بين الامن السيبراني"بانه مجموعة النشاط الذي يضمن من خلاله حماية الموارد المالية والبشرية ،الموثقة عن طريق تقنيات الاتصالات والمعلومات الحديثة،والذي يؤمن من وضع حد للخسائر والاضرار الناتجة عن تحقيق الاضرار والتهديدات ،وكما يمكن من خلاله اعادة هذه المعلومات الى سابقتها باسرع وقت في سبيل عدم توقف دفة الانتاج وعدم اكباد الخسائر الدائمة جراء تلك الاضرار المتحققة"" (٢)

وقد عرفه أخرون بانها"مجموعة الاليات والاجراءات والوسائل والاطر التي تهدف الى حماية البرمجيات وأجهزة الكومبيوتر ،الفضاء السيبراني بصيغة عامة من مختلف الهجمات والاختراقات والتهديدات السيبرانية التي قد تهدد الامن القومي للدول." (٣)

اذن يعرف الامن السيبراني من خلال النشاط الذي يهدف من خلاله توجيه المخاطر والحاق الاضرار بالمعلومات والبيانات الضرورية لدى الحكومات وافرادها بغية تحقيق المنافع المالية ،أو تحقيق الغرض الهادم باليات عمل الاجهزة وتعطيلها مما يكبد المقابل الخسائر واتلاف البيانات الهامة التي تعني بحياتهم ومجالات عملهم.

وكما حاولت الهيئات العسكرية للدول ووالمعنية بحماية أنظمة الدولة وسيادتها الى التعريف بمخاطر الامن السيبراني واضراره، حيث بين البنتاغون الاميركي هذا المفهوم من خلال ايراد مفهوم واسع له اذ اعتبرته"مجموعة الاجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والالكترونية ومن مختلف أنواع الجرائم المهددة كالهجمات –التخريب–التجسس–الحوادث"" (٤)

قارة، وهو أقدم وكالة في أسرة الأمم المتحدة – حيث يربط العالم منذ فجر التلغراف في عام ١٨٦٥ ،وللمزيد عنه ينظر الموقع الرسمي للاتحاد على الرابط :- https://www.itu.int/en/about/Pages/default.aspx#/ar

(١) دليل لوضع استراتيجية وطنية للامن السيبراني ، منشورات الاتحاد الدولي للاتصالات ،ص ١٩، والمتاح على الرابط الخاص بالاتحاد :- https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-A.pdf

(٢) سعيد عبداللطيف حسن،اثبات جرائم الكومبيوتر وجرائم المرتكبة عن طريق الانترنيت،ط٤،دارالنهضة العربية –القاهرة، ١٩٩٩م ،ص٢١٤ ومابعدها.

(٣) د.فارس محمد العمارات وابراهيم محمد الحماصة،المصدر السابق، ص ١٩.

(٤) د.حميدة علي جابر ،أليات الامم المتحدة لتحقيق الامن السيبراني وأثره على التشريعات العراقية،بحث منشور في مجلة الباحث للعلوم القانونية،الصادرعن كلية القانون–جامعة الفلوجة ،العدد(١) ،م(٦)،٢٠٢٥، ص٥٤.

وكذلك بين بانها "عنصر الحماية للشبكات وانظمة تقنية المعلومات وانظمة التقنيات التشغيلية ومكوناتها من خلال الاعتدة والبرمجيات ،ومايتم تقديمه من الخدمات وما تحتويه من المعلومات الهامة من أي محاولة للاختراق أو تعطيلها أو المساس بها أو استخدامها والتصرف بها دون وجه حق."[١] اذن الامن السيبراني مفهوم واسع ومشتمل على جميع العناصر المحققة للمخاطر وتوجيه الاضرار تجاه مصالح الدول والافراد المتعلقة بانظمة البيانات والمعلومات الاساسية التي تحكم حياتهم ومجالات عملهم بالاضافة الى الجانب الاستخباري والعسكري والمالي وكل مساس بهذه الحقوق تعتبر انتهاكا صارخا بالامن السيبراني لهم جراء تطور وتعقد الانظمة الاتصالاتية العالمية وبرامج الحواسيب المتطورة يوما بعد يوم ومن حق الجميع اضفاء طابع الحماية والدفاع تجاه اي خرق لهذه المتعلقات الحياتية . كما وقد قامت الحكومات وفق مجالها الداخلي بالاهتمام بهذا المجال والعمل على وضع الاستراتيجيات الوطنية من أجل حماية البيانات والمعلومات التابعة للحكومة واعمالها ومعلومات مواطنيها ،وقد أنشأت لهذا الغرض مديريات الامن السيبراني تابعة لوزارة الداخلية العراقي تأخذ على عاتقها هذا المهمة الوطنية لحماية الفضاء السيبراني وتقنيات الاتصالات من محاولات الخراب والدنس. [٢]

---

(١)المصدر نفسه أعلاه،ص ٥٥ومابعدها.

(٢) الاستراتيجية الوطنية العراقية للأمن السيبراني هي خطة شاملة تهدف إلى توفير بيئة سيبرانية آمنة وموثوقة في العراق، وحماية البنية التحتية الحيوية للمعلومات، وتعزيز الثقة في الفضاء السيبراني. تشتمل الاستراتيجية على وضع سياسات وإجراءات فعالة، وإدارة الحوادث السيبرانية، والكشف عن الثغرات الأمنية، وتوعية المجتمع بأهمية الأمن السيبراني.للمزيد ينظر وثيقة الاستراتيجية الوطنية العراقية للامن السيبراني المتاح على الرابط :- https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/00056_06_iraqi-cybersecurity-strategy.pdf

-يعد مديرية الأمن السيبراني مديرية أمنية معلوماتية تعنى بمجالات الأمن السيبراني وترتبط بمكتب معالي السيد وزير الداخلية، وتعمل على تعزيز جهود وزارة الداخلية في بناء منظومة فعالة للأمن السيبراني ويهدف الى تطويرها وتنظيمها لحماية الوزارة من تهديدات الفضاء السيبراني ومواجهتها بكفاءة وفعالية بما يضمن استدامة العمل والحفاظ على الأمن الوطني وسلامة بيانات ومعلومات المؤسسات والأفراد، ومن مهام مديرية الامن السيبراني:-

١. وضع السياسات والاستراتيجيات الخاصة بالامن السيبراني ومتابعة تنفيذها .
٢. ادارة حوادث وتهديدات الامن السيبراني .
٣. الكشف عن الثغرات الامنية في التطبيقات والمواقع والانظمة.
٤. الكشف عن نقاط الضعف في البنى التحتية للشبكات السلكية واللاسلكية .
٥. تحليل مواقع الانترنت ومواقع التواصل الاجتماعي.
٦. تثقيف ونشر الوعي الامني بين منسوبي قوى الامن الداخلي وباقي شرائح المجتمع.
٧. مراقبة وتحليل مراكز البيانات والمحطات الطرفية الخاصة.
٨. الاستجابة والحد من عمليات اساءة استخدام تكنولوجيا المعلومات والاتصالات. للمزيد حول هذا ينظر الموقع الخاص بالمديرية على الرابط :- https://moi.gov.iq/?page=6295

المطلب الثاني

أنواع التهديدات المتعلقة بالامن السيبراني

التهديدات السيبرانية، ويقصد بها أي نوع من انواع الانشطة الضارة والتي ستهدف من خلالها الانظمة المعلوماتية والشبكات الحاسوبية ،وهي تغدو الاضرار بحقوق المستخدمين وانظمتهم والبيانات الخاصة بهم، فالتهديدات السيبرانية تشمل عادة مجاميع مختلفة من الانشطة الخبيثة في سبيل الاختراق وزرع البرامج المضرة والمتجسسة ،ومحاولة الاحتيال والبحث غير المشروع عن العملات الرقمية والاعتداء على مجمل الحقوق الخاصة بها (١) .

وهناك العديد من التهديدات السيبرانية التي تحاول النيل من انظمة وبيانات الدول والافراد جاهدة لالحاق الضرر وتعطيل الانظمة الحاسوبية لهم مما يحاول بدورها الجهات المرادة لهذه الهجمات استخدام أبشعها واكثرها خطورة للنيل من حقوق الاخرين.(٢)

ومن خلال الدراسة نحاول ان نسلط الضوء على ابرز التهديدات الذي يعاني منها المجتمعات والدول جراء انتهاكات الامن السيبراني والمتمثلة في :-

أولا- التهديدات الامنية والعسكرية...

تمثل هذا التهديد الاول والاخطر بسبب التطورات التقنية والتكنولوجيا في المجالات العسكرية والاستخبارية وانتشارها في ارجاء المعمورة ومحاولة الدول للنيل من بعضها البعض من خلالها ،بسبب انتهاء زمن الحروب التقليدية واستخدام الجيوش الالكترونية بدلا عنها.

---

(١) منال البلقاسي، تأمين التهديدات السيبرانية تحت المجهر الرقمي،ط١،مؤسسة العبيكان للنشر والتوزيع،الرياض،السعودية، ٢٠٢٤، ص٤٧.

(٢) من هذه التهديدات السيبرانية المؤثرة على انظمة المعلومات والبيانات :-

أ- الاختراقات الالكترونية

ب- البرمجيات الضارة

ت- الاحتيال الالكتروني

ث- التجسس السيبراني

ج- الهجمات الخاصة بالاسقاط الموزع للخدمة.

ح- استغلال الثغرات الامنية.

خ- الهجمات السيبرانية الدولية .مع العلم بان التهديدات السيبرانية في تطور ملحوظ ودائم ،نتيجة التطورات العلمية مما يستدعي جهودا مستمرا ومباشرا في سبيل مواجهتها وحماية الانظمة والبيانات،وكذلك نشر الوعي الثقافي حول الامن المعلوماتي وحماية البيانات بين الافراد . وللمزيد حول هذا ينظر :- منال البلقاسي،المصدر السابق، ص ٤٨ ومابعدها.

اذ تتميز هذا النوع من التهديدات الى توجيه ضربات لقواعد البيانات العسكرية في سبيل التجسس عليها أوتدميرها وحتى حالات سرقة البيانات منها (كالخرائط العسكرية واليات عمل القوات والاجهزة والرادارات وحتى الاسلحة المستخدمة وانواع القذائف وغيرها من الترتيبات العسكرية الخاصة بعمل الاجهزة العسكرية). [١]

ومن خلال الامن السيبراني فانها قادرة على التداخل والترابط بين العناصر العسكرية من خلال منظومة الشبكة العسكرية في الفضاء الالكتروني،والذي يساعد في انتقال المعلومات وتحويلها والسيطرة على سرعة اعطاء الاوامر للانظمة العسكرية في سبيل الحاق الاضرار باهداف محددة وتدميرها بالكامل ،بالاضافة الى القدرة على قطع الاتصالات بين القطعات العسكرية ومنع وصول الاوامر والمعلومات اليهم ،وشل عمل القوات الجوية والبحرية وحتى البرية من خلال هذا التداخل السيبراني . [٢]

هذا ومن جانب اخر فان من التهديدات الاخرى لهذا الجانب الخطير للدولة ،هو قيام القراصنة والجهات المتعمدة لهذه الاختراقات هو شل عمل اجهزة الدفاع الالكترونية للدولة وحتى تعطيل الطائرات بدون طيار،والاسلحة والغواصات النووية مروراُ الى الاقمار الصناعية للدول والمستحدمة في المجالات الامنية والعسكرية وتحديد المواقع وارسال البيانات ووضع التشويش واضطراب اجهزة المتابعة والرادارات ،ومنها سرقة المعلومات الخاصة بصنع الاسلحة واليات عملها مثلما حدثت وان هاجم الصينيون(شركة لوكهيد مارتن) الشركة الخاصة بصنع طائرات (أف ٣٥) الاميركية مما ادى الى سرقة البيانات والمعلومات الخفية بصنع الطائرة ومن ثم صنعت الصين على غرارها طائرة (جي ٢٠)، بالاضافة الى الاختراق الامني للحواسيب الخاصة بالجيش الامريكي في الشرق الاوسط عام ٢٠٠٨ والذي تم وضع وصلة حاسوب وتم اختراق البيانات والمعلومات السرية وغير السرية ونقلها الى حواسيب أخرى خارجية .[٣]

اذن فالخرق الامني والعسكري تشكل تهديدا كبيرا ليس على الدولة وحدها بل على الدول جميعاً،لانه من الممكن استخدام هذه البيانات وتوجيهات الاسلحة تجاه مصالح واهداف عابرة للحدود مما يشكل خرقاً امنياُ دولياً ،وخصوصاً الاسلحة النووية والطائؤات المسيرة الحديثة وحتى الصواريخ الذكية وذاتية التعامل.

ثانيا:- التهديدات المالية والاقتصادية...

وفي مجال اخر ومهم للغاية ومؤثر بشكل كبير على عمل الاسواق المالية والبورصات وحسابات البنوك والشركات المالية يلعب الامن السيبراني دورا عليها نتيجة لتحول التعاملات الدولية المالية في كثير من الجالات الى الاسلوب الالكتروني .

(١)د.سيناء علي محمود، التحديات الامنية للدول في الفضاء السيبراني ،بحث منشور في مجلة قضايا سياسية- جامعة النهرين، العدد(٨٠) ،٢٠٢٥،ص ٣٢٣،

(٢) احمد طلال احمد حسن،الامن السيبراني وتداعياته على الامن القومي المصري،بحث منشور في مجلة كلية القانون للعلوم القانونية والسياسية-جامعة كركوك ،المجلد(١٣)،العدد(٥١)،٢٠٢٤،ص٦١.

(٣)للمزيد ينظر:- د.سيناء علي محمود ،المصدر السابق ،ص ٣٢٢ومابعدها.

فالامن السيبراني يرتبط اليوم ارتباطاً لصيقاً بالاقتصاد والمال،حيث نتيجة الترابط بين الاقتصاد المعرفي وتوسيع استخدام تقنيات المعلوماتية والاتصالات المتداخلة في مجال القيمة التي نجتويها البيانات والمعلومات المستخدمة والمخزونة والمتبادلة لاستخدامها بين المستوى الدولي والداخلي، هادفة الى تنمية وتطوير الاقتصادات للدول من خلال مجالات الاستخدام الفعلي لهذه الفرص من لدن كبريات الشركات الدولية وكما ان اليوم يمثل المال الالكتروني عنصرا مهما في التعاملات المصرفية وكذلك سهولة استخدام العملات الالكترونية ونقلها والمحفظات المالية الالكترونية كلها اصبحت أرصدة مالية افتراضية بمثل مجالاً واسعاً للتداولات الالكترونية . (١)

اذ التطور التكنولوجي قد اضحت دوراً بارزاً على القطاعات المالية والمصرفية ايضا،اذ الكثير من المعلومات والاوامر الصرفية والحسابات المالية تخزن على الحواسيب المرتبطة مع بعضها البعض عن طريق الوصلات الانترنيت لسرعة ارسال المعلومات ونقلها بين البنوك والبورصات الداخلية والخارجية مما يجعلها في مجال الانتهاك والاختراق. (٢)

ونتيجة للتطور الدولي الكبير في الاعتماد المتنامي من لدن القطاعات المالية والشركات الاقتصادية على الانظمة واتصالات الانترنيت في سبيل ترتيب العمل المالي للادارات المالية والمصرفية والذي بدورها جعلتها هدفاً للانتهاكات السيبرانية ،وتنوع الاهداف تلك سواء من ناحية السرقة للبيانات أو مهاجمتها أو انتهاك حقوق الملكية الفكرية في الابداع والتنفيذ، وسواء على الجهات المعنية أم عملائها وزبائنها،،ونتيجة للدراسات العلمية في هذا المجال من انه وفي سنة (٢٠٢٥)سوف تبلغ حجم الانتهاكات السيبرانية الى (٦)تريليون دولار ،وبموجبها تم وضع تهديدات الامن السيبراني من أكثر وابرز خمسة التهديدات العالمية التي تواجهها سوق الاقتصاد دولياً،بالاضافة الى كونها من ابرز واكثر عشر التهديدات التي تصادفها الشركات المالية والاقتصادية وهذا بدوره لن يؤثر على سمعة الشركات وثقة العملاء فحسب بل تتعدى حدود الصناعة نفسها للشركة العاملة في المجال هذا . (٣)

وبذلك نرى من ان التهديدات السيبرانية الواقعة على هذا المجال ليست باليسيرة والبسيطة بل تتمثل بكونها ذو مخاطر لاتقل جسامة عن الاتهديدات الامنية والعسكرية لانها تنصب في مجال مهم من القطاعات المالية والاقتصادية للشركات والبنوك وتنتهك حقوق تمس الجانب المتصل بالامن القومي الاقتصادي للدول والذي تعبر بحد ذاته اليوم مجالا حيوياً ومضدرا للموارد الاقتصادية ،بالاضافة الى المعلومات السرية لحاملي حسابات مالية في هذا المجال .

ثالثا:- التهديدات الثقافية والاجتماعية ...

وفي جانب اخر من التهديدات التي تواجه المجتمعات جراء الامن السيبراني هي مسألة الحقوق الاجتماعية والثقافية التي تلحقها أحكام هذا الانتهاك والذي تؤثر بدوره على الجانب النفسي والتكوين الاجتماعي للافراد داخل مجتمعات الدول .

---

(١)علي بن أحمد بن طراز,الأمن السيبراني ضرورة الوعي وحتمية التّطبيق،ط١،مركز الكتاب الأكاديمي،٢٠٢٥،عمان- الاردن،ص ٥٨.

(٢) احمد طلال احمد،المصدر السابق ،ص ٦١.

(٣)م.شهد عدنان صالح، الامن السيبراني وتأثيره على الامن القومي للدول،بحث منشور في المجلة السياسية والدولية -جامعة المستنصرية،العدد(٦٣)،٢٠٢٥ ،ص٥٢١ ومابعدها .

ونتيجة لتشابك واختلاط العوامل الفعالة في مسألة التنشئة للاجيال في المجتمعات وخصوصاً نتيجة التطور الالكتروني الواسع ،وسهولة الوصول والاطلاع على حياة وأنشطة المجتمعات والثقافات المتنوعة التي تحملها غيرهم ،عكست بشكل سلبي دور الجماعات البدائية في مجتمعاتنا بدءا من الاسر والمدارس ودور العبادة والمجاميع المكونة للاندية واصدقاء المناطق ،الذي سبق وان كان يعتمد عليهم في التنشئة الاجتماعية للافراد في المجتمعات واندماجهم فيها وجعلهم جزءاً لايتجزء منها .(١)

ومع التزايد والافراط في الاستخدام اللاعقلاني لشبكات التواصل الاجتماعي يؤثر بدوره في تجاوب الافراد مع غيرهم من الاشخاص في المجتمعات الاخرى والتي هي ذو مردود سلبي ،مما يجعلهم أخذ جانب الانعزال الاجتماعي وتدهور وحتى تفكك بالعلاقات الاسرية والاجتماعية مع بيئاتهم، فبقاء هؤلاء منعزلين ولاوقات طويلة على شيبكات الانترنيت ضمن الفضاء الافتراضي للمجتمعات سوف يجعل منهم اختيار فكرة الانعزال الاجتماعي مع الاقرباء في حياتهم ،والذي يؤدي الى مغادرة والابتعاد عن التكوين الاجتماعي القريب منهم،وهذا يؤثر سلباُ على دائرة العلاقات الاسرية والاجتماعية لهم (كالاصدقاء والجيران والاسرة وحتى زملاء الدراسة). (٢)

وكشفت الدراسات والتقارير الدولية الصادرة عن شركة (نورتون الامريكية –سمنتك) على ان الهجمات السيبرانية أسفرت عن (٢٦٣ألف) من الضحايا عام ٢٠١٦،وبلغ اجمالي (٨٥%) من السكان الى الهجمات السيبرانية عام ٢٠١٨ ،وان الاعداد تتزايد بشكل ملحوظ خلال السنوات نتيجة الاستخدام المتزايد للانظمة الالكترونية وشبكات التواصل الاجتماعي وغيرها. (٣)

ونتيجة لازدياد اعداد المستخدمين للشبكات الاتصالية والانترنيت مما بلغ حوالي خمس مليارات مستخدم ،مما جعلها من التجمعات الكبيرة الافتراضية ،وهذا يجعل هؤلاء في مكنة من تبادل للمعلومات والافكار والتوجهات المختلفة ،مما يشكل بدورها خطراً من ناحيتين الاولى من خلال قيامهم بتبادل المعلومات والتوجهات المعرفية وفي الثانية قيام الافراد من توجيه اخلاقيات مناوئة وافكار متطرفة الى غيرهم والتأثير عليهم وتكوين مجاميع افتراضية مهددة للامن والسلم المجتمعي داخل البلدان . (٤)

نرى من خلال التهديدات تلك تأثير واضح على النسيج الاجتماعي والسلم المجتمعي للمجتمعات جراء الامن السيبراني الذي يحاول من خلاله النيل من ثقة الافراد وتقليل الروابط الاجتماعية وجعلهم يكرهون أسرهم ومجتمعاتهم وافرادها بل وحتى الدول التي ينتمون اليها،ومحاولة زرع الافكار المتطرفة والمناوئة واستغلال النفسيات نحو زرع

(١) د.مريم محمد حسين وم.مصطفى صادق عواد، الامن السيبراني والتنشئة الاجتماعية،بحث منشور في المجلة العراقية للعلوم السياسية،العدد(١٣)، ٢٠٢٤،ص ١٧٨.

(٢) د.مريم محمد حسين وم.مصطفى صادق عواد،المصدر نفسه ،ص ١٧٧.

(٣)م.شهد عدنان صالح، مصدر سابق ،ص٥١٩ ومابعدها .

(٤)م.د.ياور عمر محمد،تأثير الامن السيبراني على الامن القومي العراقي(الفرص والتحديات) بحث منشور في مجلة كلية القانون للعلوم القانونية والسياسية–جامعة كركوك،المجلد(١٤)،العدد(٥٣)، ٢٠٢٥،ص ٥٢٥.

الطائفية مثلاً أو دفعهم للانخراط الى المجاميع الارهابية وخداعهم بمختلف المسميات والاهداف في سبيل النيل منهم

المبحث الثاني

حق الدول في الدفاع عن الأمن السيبراني الخاص بهم

بعد أن بينا في المبحث الأول من دراستنا هذه المقصود بالأمن السيبراني وعلى مايشتمله هذا الأمن الحيوي الحديث بنظام الدولة واستقراره بالاضافة الى الاهمية الحقيقية لوجود هذا الامن والعمل على اضفاء الحماية المستمرة والدقيقة عليها كونها تمثل جانب سيادي مهم للدول.

نحاول في هذا المبحث من القاء نظرة وبيان لحقوق الدول في مجال حماية هذا الأمن المستجد في المجتمع الدولي ،كونه يمثا جزءاً أساسياً وحيوياً من سيادتها بالاضافة الى كون أن الدفاع عنه يمثل نقطة جوهرية في مجال القانون الدولي العام ،نظراً لاتيانه ضمن المواثيق الدولية التي تعني بحفظ الامن والسلم الدوليين ،وتحديداً ضمن مواد ميثاق المنظمة الاممية التي تأسست على ضوءها ابرز وأكبر منظمة دولية بعد ويلات الحرب العالمية الثانية،اذ نص الميثاق وفي المادة(٥١) منه على ضرورة قيام الدول بالدفاع عن نفسها واتخاذ الاجراء ات المناسبة للدفاع عن نفسها حال ما كانت هناك مخاوف وتهديدات حقيقية على أمنها ويلامتها، وبغية ذلك سوف نبحث ذلك ضمن المطلبين الاتيين تباعاً.

المطلب الأول

حق الدول في الدفاع عن السيادة السيبرانية

تعتبر سيادة الدول من الامور الاساسية التي رافقت التطورات الذي لحق بالمجتمع الدولي طيلة القرون الماضية، ونظرا لعدم التنازل عنها وعدم قبول الدول في تعريض أمنها الداخلي والخارجي لاي أخطار دولية ،ظلت هي محافظة على كيانها ووجودها الى يومنا هذا ،فبدون احترام لهذه السيادة لامجال لأي شخصية دولية مستقلة للكيان الدولي وخصوصاً الدول.

ومنذ نشأة منظمة الامم المتحدة كانت فكرة السيادة مدار النقاش والبحث ،والذي بدورها لم تغفل ميثاق المنظمة عنها الى أن تم النص عليها في صلب الميثاق الأممي وذلك لأهميته ومكانته العالمية ،اذ جاءت في المادة الثانية مؤكدة على أن المنظمة تقوم على الاحترام الكامل والمساواة بين جميع الدول الاعضاء في احترام السيادة لكل منها، بالاضافة الى تعهد المنظمة من عدم القيام بالتدخلات وبانواعها السياسية والقانونية في الامور المتعلقة بالقضايا الداخلية للدول الاعضاء في المنظمة. [١]

---

(١) نص المادة (٢) من ميثاق منظمة الامم المتحدة:-

١- تقوم الهيئة على مبدأ المساواة في السيادة بين جميع أعضائها.

٧- ليس في هذا الميثاق ما يسوغ "للأمم المتحدة" أن تتدخل في الشؤون التي تكون من صميم السلطان الداخلي لدولة ما، وليس فيه ما يقتضي الأعضاء أن يعرضوا مثل هذه المسائل لأن تحل بحكم هذا الميثاق، على أن هذا المبدأ لا يخلّ بتطبيق تدابير القمع الواردة في الفصل السابع.

ونتيجة للتطورات والاكتشافات الحديثة وظهور المجالات السيبرانية لأعمال الدول وفي شتى المجالات الاقتصادية والمالية والطاقة والماء والحماية العسكرية والاسلحة وغيرها،بدأت المخاوف والهجمات من لدن أعداء الدولة تطال هذه المجالات بغية تعريض أمن وسلامة الدول للخطر أو الحاق تالاضرار الكبيرة بهم بسبب تراجع الأفكار التقليدية للحروب الدولية ومصاريفها وتبعاتها.

اذ السيادة احد أهم الامور الاساسية للدول، فهي من خلالها تمتلك القدرة الكاملة في سبيل تحقيق السيطرة والحكم الشخصي على أقليمها وأفرادها،فحق الدفاع عن هذه السيادة هي تأكيد على ديمومة الاستمرارية لهذه السيادة والقيام بمنع الاعتداءات التي تهدد كيان واستقرارية وحريات تقرير مصيرها وحياتها.

فللدول كامل الحق في اتخاذ مختلف التدابير الضرورية للحفاظ على هذه السيادة ،فأستخدامها للقوة متى ماكانت ضرورية وخصوصا في المجالات العسكرية وصد الهجمات والتهديدات الخارجية والعدوانية التي تحاول من المساس بالسيادة الوطنية للدولة. (١)

ونتيجة لظهور فكرة السيادة السيبرانية نتيجة للتطورات الدولية في أنظمة الفضاء السيبراني ،اذ أصبحت البيانات الرقمية والمعلومات ساحة للحروب في العلاقات نتيجة للمنافسة العالمية والسباق نحو التملك والسيطرة،والتي خلفت على ضوءها توترات نطلق عليها بالجيوسياسية (٢) ومن خلالها يكون للدول القدرة بالتحكم على الفضاء السيبراني الخاص بأنظمة الدولة وبياناتها جميعاً من مخاطر الشركات العالمية والمعتدية.(٣)

ونتيجة لاستخدام مفهوم السيادة السيبرانية وقبوله في الاوساط الدولية ماهو الا دليل على حاجة الدول الى ضرورة حماية المعلومات الامنية والحساسة والتي تمس مصلحة الدولة وكيانها في هذا المجال الواسع من الانترنيت ،من أجل

---

(١) د.عدنان بوزان، مبادئ القانون الدولي العام،ط١، منشورات أزادي بوست المتاح على الرابط https://azadiposts.com/attachments/article/95 ، ٢٠٢٣،ص٥٤١.

(٢) الجيوسياسية :- تعني علم دراسة تأثير الأرض (برها وبحرها ومرتفعاتها وجوفها وثرواتها وموقعها) على السياسة في مقابل مسعى السياسة للاستفادة من هذه المميزات وفق منظور مستقبلي اضاف الى الجيوبوليتيك فرع الجيو استراتيجيا.

وكان أول من استخدمه في الماضي المفكر السويدي رودولف كجلين مطلع القرن الميلادي الماضي وعرّفه بأنّه ((البيئة الطبيعية للدولة والسلوك السياسي)). بينما عرّفه المفكر كارل هوسهوفر بأنّه ((دراسة علاقات الأرض ذات المغزى السياسي، بحيث ترسم المظاهر الطبيعية لسطح الأرض الإطار للجيوبوليتيكا الذي تتحرك فيه الأحداث السياسية)).

ومن التعريفات المهمة لمصطلح الجيوسياسية عند الغربيين أنها عبارة عن ((الاحتياجات السياسية التي تتطلبها الدولة لتنمو حتى ولو كان نموها يمتد إلى ما وراء حدودها)). ومنها أيضا ً ((دراسة تأثير السلوك السياسي في تغيير الأبعاد الجغرافية للدولة)).

هذا ويمكن تبسيط مفهوم الجيوسياسية بلغة مبسطة بأنها تعني السياسة المتعلقة بالسيطرة على الأرض وبسط نفوذ الدولة في أي مكان تستطيع الدولة الوصول إليه. إذ أن النظرة الجيوسياسية لدى دولة ما تتعلق بقدرتها على أن تكون لاعبا فعّالا في أوسع مساحة ممكنة من الكرة الأرضية. للمزيد حول هذا ينظر معجم المعاني ،المتاح على الرابط الالكتروني:- https://www.almaany.com/ar/A/

(٣) خالد وليد محمود،الفضاء السيبراني وتحولات القوة في العلاقات الدولية،ط١، المركز العربي للأبحاث ودراسة السياسات،قطر،٢٠٢٥،ص٩٦.

اضفاء السرية حولها ووصول المعلومات الى المستخدمين بسلاسة وديمومة ،وان الوجهات الاساسية لظهور هذا المفهوم وتداوله بهذه الصورة المركزية بين الدول ترجع الى التخطيطات الدولية لعام ٢٠١٠،بعد كشفت المواقع الامريكية والمسمى"" ويكليكس"" عن ابرز وأهم الاوراق والخطابات والبرقيات الحكومية والمتعلقة بالحرب وخططها والخاصة بوزارتي الدفاع والخارجية الامركيتين ،وهذا كشف حجم الدور والاهمية القصوى للسيادة في مجال الامن السيبراني وحالات ترسيخه لدى الاوساط الدولية وخصوصاً ذوي الفاعلية والقوة في المحيط الدولي.(١)

فالسيادة السيبرانية هي فكرة حديثة في الاوساط الدولية ،وهي جزء من المفهوم الخاص بالأمن السيبراني الذي تختص بحماية البنى التحتية للمعلومات والبيانات المرتبطة بالعمليات العنكبوتية للانترنيت وربط الشبكات الحاسوب داخل الدول ،وتتمثل الفكرة حول كيفية الدولة في السيطرة على المجال الامني السيبراني ومحاولة تطويرها في سبيل مقدرتها الفنية في الاعتماد على خبراتها الداخلية دون الاعتماد على الجانب الاجنبي وما يلحقه بمخاوف وتهديدات حولها.(٢)

اذن السيادة السيبرانية هي مجال حديث ومهم في ميدان الواقع الدولي وضرورة العمل على ترتيب الدول لاولوياتهم الامنية السيبرانية تلعب دوراً أساسياً فيه،اذ ان الكثير من مجالات الحكومات في الوقت الحاضر أصبحت الكترونية بالاضافة الى متابعة هذه الاوامر والخطوط والشبكات تحتاج ديمومة ومراقبة ،وبالتالي حتم ضرورة على الدول في سبيل دعم المجالات والدراسات لافرادها للتعلم في هذا المجال في سبيل الاعتماد على الطاقات الوطنية والداخلية دون الاعتماد على الخارج والشركات الاجنبية التي من الممكن أن تكون عامل تهديد على الامن السيبراني للدول وبياناته الحيوية.

اذ تعاني الدول من الكثير من التحديات الدولية في مجال حماية سيادتها السيبرانية وتتلخص أهمها في(٣) :-

١- اعتبار الفضاء السيبراني للدول مجالاً حيوياً سيادياً نتيجة للممارسات الفعلية والسيادية التي تعمل في مضامينها الدول ،وبالتالي يحتاج الى الهندسة المحمية والى التشريعات الخاصة من أجل حمايته.

٢- قيام الدول بأنشاء نظام سيبراني أمن محدد فيه الافراد الذي يعملون فيه ضمن المجال السيبراني بروية ودقة، لأن الدول ليس بمقدورها أن تلقي بالمسؤولية عن هذا الفضاء الالكتروني الى جهة واحدة.

٣- محاولة الدول في تحديد الحدود الخاصة بالفضاء السيبراني ورسمها من أجل المتابعة والمراقبة والتحكم فيه بصورة فعلية، وبدون ذلك سوف يفقد الدول السيطرة على هذا المجال وحمايته.

٤- العمل على تأسيس بيئة توافق فيه أراء الجهات الوطنية في سبيل ايضاح ما يكون اعتداء وخرقاً لتهيئة الدفاعات اللازمة عن الامن والسيادة الوطنية،فالتلكئ والضعف في هذا الجانب سوف يضعف الرؤية الصحيحة في توجيه الرد الحاسم أو غير الملائم بها.

---

(١) المصدر نفسه أعلاه ،ص ٩٧.

(٢)د. فراس جمال شاكر محمود، الحروب المعلوماتية في المجال الأمني والعسكري أمريكا والصين،ط١،العربي للنشر والتوزيع، ٢٠٢٢،ص ٢٣٢.

(٣) المصدر نفسه أعلاه ، ٢٣٣ ومابعدها.

وقد قامت الدول الكبرى بتخصيص مبالغ كبيرة في سبيل حماية الانظمة الدفاعية السيبرانية، ومنها الولايات المتحدة الامريكية والصين باعتبارهما أكبرمستخدمي للفضاء السيبراني الدولي ومحاولة منهما في سبيل حماية سيادتهما السيبراني،اذ اعتمدت الدول في رصد التكاليف من أجل انشاء وحدات خاصة بالانترنيت وشبكات الحاسوب المعدة في سبيل تنمية وتطوير التكنولوجيات الخاصة بالهجمات الالكترونية ،اذ وضع هذه التكاليف للاسلحة الالكترونية على عوامل كثيرة منها ذو ابعاد اقتصادية تختص بمجال الحماية ومنع الاعتداءات كالتجسس أو تسريب المعلومات السرية والاساسية الى خارج البلد والذي بدورها تكلف ملايين الدولارات ،وهذا تعتبر خطوة سباقة من أجل العمل على تبني خطط استراتيجية الكترونية جيدة وموثوقة من أجل العمل على التطوير والتعبئة للترسانة الالكترونية للدول والذي بدورها تكون سرية ومخفية اذ لايصرح الدول بها على العكس من الاسلحة العادية والتقليدية التي تكون معلنة في أغلبها . (١)

ونتيجة لكثرة الازمات الدولية والمشاكل التي خلفتها مسألة الامن السيبراني واجراءات حماية صون سيادة الدول وبياناتها الدقيقة التي من الممكن أن تؤدي الى الاضرار وتعريض أنظمتها لمخاطر الانتهاك والهكرات،بادرت منظمة الامم المتحدة الى اتخاذ الاجراءات الكفيلة التي تقع على عاتقها في مجال حفظ السلم والامن الدوليين الى عقد الاتفاقية الدولية المعنية بحماية الامن السيبراني. (٢)

ومن نصوص موادها المادة (٥) الملفت للنظر في صوب بحثنا هذا والمتعلقة بحماية سيادة الدول من الناحية السيبرانية،اذ تؤكد على الدول جميعاً تنفيذ التزاماتهم الاساسية والخاصة بحماية سيادة الدول الاخرى وعدم التدخل في شؤونهم وعدم تعريض مبادئ المساواة الدولية للخطر،بالاضافة الى منع الدول في التدخل بحجة الولاية القضائية والملاحقة على مرتكبي تلك الجرائم وانما ذلك تعتبر من صميم الاختصاص الداخلي للدولة نفسها. (٣)

وقد شهد العالم خلال العقدين الاخيرين الكثير من الحالات التي دخلت في مجال الانتهاك السيبراني وتعريض السيادة السيبرانية للدول الى مخاطر جمة مما كانت أن تؤدي الى حروب دولية.

---

(١) د.عادل عبد الصادق ،الاقتصاد الرقمي وتحديات السيادة السيبرانية،ط١،المركز العربي لابحاث الفضاء الالكتروني ،القاهرة ، ٢٠٢٠،ص ٢١.

(٢)أعتُمدت الاتفاقية في ٢٤ ديسمبر/كانون الأول ٢٠٢٤ بموجب القرار ٢٤٣/٧٩ في الجلسة العامة الخامسة والخمسين للجمعية العامة للأمم المتحدة. ووفقًا للمادة ٦٤ منها، يُفتح باب التوقيع على الاتفاقية لجميع الدول ومنظمات التكامل الاقتصادي الإقليمي في هانوي، يومي ٢٥ و٢٦ أكتوبر/تشرين الأول ٢٠٢٥، ثم في مقر الأمم المتحدة بنيويورك حتى ٣١ ديسمبر/كانون الأول ٢٠٢٦.

(٣) نصت المادة من الاتفاقية أعلاه ٥: وتحت عنوان ((صون السيادة))

١ – تنفذ الدول الأطراف التزاماتها المنصوص عليها بموجب هذه الاتفاقية على نحو يتسق مع مبدأي المساواة في السيادة والسلامة الإقليمية للدول ومع مبدأ عدم التدخل في الشؤون الداخلية للدول الأخرى.

٢ – ليس في هذه الاتفاقية ما يبيح لدولة طرف أن تقوم في إقليم دولة أخرى بممارسة الولاية القضائية وأداء المهام التي يناط أداؤها حصرا بسلطات تلك الدولة الأخرى بموجب قانونها الداخلي.

ومن هذه الانتهاكات السيبرانية ،ما حدثت بين روسيا واستونيا خلال عام ٢٠٠٧،وكذلك بين روسيا وجورجيا خلال عام ٢٠٠٨،ومن أهمها ما دارت بين الولايات المتحدة الامريكية وايران بدءاً من عام ٢٠٠٩لغاية ٢٠١٣،وكوريا الشمالية والجنوبية خلال الفترة من ٢٠١١-٢٠١٣، وغيرها في الشرق الاوسط بين ايران والسعودية خلال فترة ٢٠١٦ و٢٠١٧، وأمريكا وروسيا خلال الانتخابات الرئاسية عام ٢٠١٦ ،وغيرها التي اجتاحت دول العام خلال الفترة تلك [١] وبذلك تعتبر حماية السيادة السيبرانية ووضع البرامج الدفاعية عنها من الاولويات الحديثة للدول في الوقت الراهن ، والذي تكمن فيه القدرات الحقيقية للدول في سبيل الحماية والدفاع عن مختلف أنظمتها السيبرانية،وسواء تعلق الامر بالبيانات الالكترونية والمعلومات الاساسية والسرية لقطاع الدولة والحكومة وأجهزتها الامنية أم في مجال القطاع الخاص بالدولة ومجال استثمارات الافراد من نواحي المعلومات البنكية والحسابات المصرفية وغيرها ودورها في سوق الدول والاوراق النقدية،لانه وعن طريق هذه الحماية سوف يؤدي بالدولة للكشف المبكر عن الخروقات والانتهاكات ووضع السبل الكفيلة بالحماية لتقليل حجم الاضرار ومنعها ،وهذا يتطلب التعاون الدولي المشترك واشراك المنظمات العالمية في هذا المجال بغية توحيد الصف الدولي وتوجيه الالتزامات الدولية صوبها وعدم تعريض سيادات الدول وأمنها الى هذه المخاطر الحقيقية التي تمس كيان الدول وأفرادها.

المطلب الثاني

حق الدول في الدفاع الشرعي السيبراني

بعد أن بينا في المطلب الاول اهمية حماية الدول لسيادتها السيبرانية وسبل حمايتها،نتطرق في هذا المطلب عن الحق الاساسي للدول والذي سبق وان عرفته المجتمع الدولي في فترة العرف الدولي وقبل ظهور المنظمات الدولية واعطاء هذا الحق للدول،لأن الدفاع الشرعي للدول تعتبر من الحقوق الاساسية والاصيلة لكل دولة ومن حقها استخدامها في حال تعرضها لأي شكل من أشكال التهديد والخروقات تجاه أمنها وسيادته.

فحق الدفاع الشرعي أقره القانون الدولي العام الحديث وفي الكثير من المعاهدات والاتفاقيات الدولية ،وهو الذي يمكن للدولة التي يقع عليها أي اعتداء أو عدوان مسلح ان تجاوب على هذا الرد وتتخذ الخطوات اللازمة للدفاع عن نفسها ووجودها وخصوصاً المادة (٥١) من ميثاق منظمة الامم المتحدة [٢] الذي أعطى هذا الحق والذي أسماه بالحق الطبيعي أي هو شيئ ثابت ومقرر لمصلحة الدول وتعتبر من ضمن قواعد القانون الطبيعي ، ويأتي هذا المبدأ

(١) د.ايهاب خليفة ،الحرب السيبرانية الاستعداد لقيادة المعارك العسكرية في الميدان الخامس، ط١،العربي للنشر والتوزيع، القاهرة ،٢٠٢١،ص٧٤ ومابعدها .

(٢) نصت المادة (٥١) ميثاق منظمة الامم المتحدة على انه:- ليس في هذا الميثاق ما يضعف أو ينتقص الحق الطبيعي للدول، فرادى أو جماعات، في الدفاع عن أنفسهم إذا اعتدت قوة مسلحة على أحد أعضاء "الأمم المتحدة" وذلك إلى أن يتخذ مجلس الأمن التدابير اللازمة لحفظ السلم والأمن الدولي، والتدابير التي اتخذها الأعضاء استعمالاً لحق الدفاع عن النفس تبلغ إلى المجلس فورا، ولا تؤثر تلك التدابير بأي حال فيما للمجلس – بمقتضى سلطته ومسؤولياته المستمرة من أحكام هذا الميثاق – من الحق في أن يتخذ في أي وقت ما يرى ضرورة لاتخاذه من الأعمال لحفظ السلم والأمن الدولي أو إعادته إلى نصابه.

استثناء على القاعدة الاساسية التي أقرتها الامم المتحدة بعد ويلات الحرب العالمية الثانية أثناء تنظيم الميثاق الاممي لها،والذي منع بموجبه من أستخدام القوة أو التهديد بها في المجتمع الدولي وخصوصاً بين الدول الاعضاء في التنظيم الدولي الحديث (١).

فالدفاع الشرعي هو حق مقرر في كافة الانظمة القانونية العالمية،فهو حق طبيعي وليس حق قانوني،فمعيار التمييز بينهما،هو ان الحق الطبيعي ليس بمقدورالقانون الغاءه أو منعه غير تنظيم الحصول عليه وترتيبه،أما الحق القانوني هو الحق الذي بمقدور القانون منعه أو منحه ،وبالتالي فان القانون الدولي العام أو القانون الداخلي للدول المرعية حالياً لايستطيعون منع حق الدفاع الشرعي للافراد والدول لانه مستقر وفق توجهات الحقوق الطبيعية. (٢)

وقد سار الفقه الدولي على أن حق الدول في الدفاع الشرعي يحكمها شرطين أساسيين:-

١- من ناحية قوة الرد ،يجب ان يكون قوة الرد هذه مخصصة باتجاه فعل الدفاع والدولة التي أتت منها هذا الانتهاك ،اذ لايجوز توجيهها الى دولة أو مصدر أخر غير المسبب للضرر.

٢- من ناحية حجم الرد، اذ يجب أن يكون الرد تلك متناسباً مع حجم الانتهاك والعدوان الذي أصاب الدولة،ويكون من الضروري الرد بهذا النمط اللازم لرد العدوان تلك وايقاف تأثيره بعلى مواقع الدولة ومؤسساته،في حين أعطى القانون الدولي الحديث المجال للغير توجيه الرد الشرعي ضرورة مراعاة موافقة مجلس الامن الدولي عنها وبصورة حصرية لاختصاصه دون غيره. (٣)

ونتيجة للتطورات الكبيرة التي حلت بميدان العلاقات والمصالح الدولية ،نرى بأنه قد يبادر رد الدفاع الشرعي من خلال مجموعة الخطوات الحماية أو من باب التعاون الدولي للقضايا الامنية المشتركة،حيث يكون هذا النمط الدفاعي في جانب الدعم والاسناد للبنى التحتية لقواعد وأنظمة البيانات وحماية الفضاء الالكتروني لها، او من خلال الرد الوقائي للعدوان أو في حالة العدوان نفسه أو بعد صدور فعل الانتهاك والتعرض . (٤)

ونتيجة لتلك الهجمات السيبرانية وازدياد مخاطرها على الأمن القومي للدول والمجتمع ،بادرت التوجهات الدولية الى ضرورة انشاء جيوش سيبرانية دفاعية جاهزة لمجابهة هذه الحالات الاستثنائية واعتبارها حقاً مشروعاً من حقوقها الدولية في الدفاع والامن عن نفسها. من حيث الدول ،فقد بادرت الولايات المتحدة الامريكية الى أنشاء جيش واسع وضخم من القوات السيبرانية من خلال جمع اعداد ضخمة من المخترفين والخبراء في تقنيات القرصنة ومهكري أنظمة المعلومات والبرامج الاساسية ضمن أفراد قواتها المسلحة وجعلهم ضمن الاهداف الحيوية لحماية وتقوية النظام

---

(١) نصت المادة(٢/ ٤) من ميثاق منظمة الامم المتحدة :- تعمل الهيئة وأعضاؤها في سعيها وراء المقاصد المذكورة في المادة الأولى وفقاً للمبادئ الآتية:- يمتنع أعضاء الهيئة جميعاً في علاقاتهم الدولية عن التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو على أي وجه آخر لا يتفق ومقاصد الأمم المتحدة.....

(٢)د. مصطفى ابو الخير، القانون الدولي المعاصر،ط١،دار الجنان للنشر والتوزيع، عمان ،٢٠١٧،ص٣٧٦.

(٣)د.عادل عبد الصادق ،الاقتصاد الرقمي وتحديات السيادة السيبرانية،مصدر سابق ، ص٢٧٢.

(٤) المصدر نفسه أعلاه،ص ٢٧٩.

الحاسوب والالكتروني للولايات المتحدة ،وكما يقال عنهم بأنهم رجال الظل ، وتكمن مهمتهم خلف شاشات الكومبيوتر وعن البعد، اذ بمقدور هؤلاء تغير الخطط والاهداف الحربية اثناء النزاع والخلافات الدولية من خلال التحكم بمصدر القوة وتغيرها واستخدام نقاط تمثل نقاط الضعف للاخرين. (١)

وكما بادرت الحكومة الفرنسية الى اصدار الكتاب الابيض للدفاع والأمن الوطني عام ٢٠١٣،أصبح الفضاء السيبراني ساحة للمواجهة الدولية واعطيت لها أهمية استراتيجية ،اذ وضع تعريف عسكري للجيش لهذا المصطلح"" وعرفت بانها مجموعة من الانشطة التي يتم القيام بها بهدف التدخل العسكري أو بطريقة مغايرة في الفضاء السيبراني لضمان فعالية عمل القوات المسلحة وحسن سير أعمال الوزارة في هذا المجال""،وقد ترأس مهمة هذا المجال الحيوي السيبراني الى نائب الأميرال(أرنو كوستيير) خلال الاعوام (٢٠١١-٢٠١٧) وبأشراف قائد أركان الجيش الوطني الفرنسي ورئيس جهاز المكتب العسكري لوزير الدفاع الفرنسي. (٢) وبحلوم عام ٢٠١٧ قامت الحكومة الفرنسية بتأسيس (comycyber) أي مايسمى بقيادة الدفاع السيبراني،وباشراف قائد أركان الجيش الوطني الفرنسي،ولعد من تأسيسه وصل عدد المقاتلين في هذا المجال بحوالي(٣٢٠٠) مقاتل سيبراني ،كما وتم الاعتماد على أجهزة فنية دقيقة وخاصة مروراً بالمركز العسكري للتنسيق بين الانشطة الخاصة والمؤثرة بالبيئة المحيطة بالحماية،وفي سبيل الاهتمام بهذا الجانب الحيوي الحديث تم تأسيس الوكالة الوطنية الفرنسية لأمن أنظمة المعلوماتبالاضافة الى العديد من الاجهزة الرئيسية الاخرى المختصة بهذا المجال. (٣)

وليست الدول فقط بل حاولت التحالفات الدولية والمنظمات الدولية السير نحو طريق وضع الاليات الخاصة بالتعاون في مسألة الدفاع الشرعي السيبراني في سبيل الحماية الجماعية فيما بينهم ضد المخاطر والهجمات السيبرانية.

اذ بادرت الاحلاف العسكرية الى تضافر الجهود في هذا المجال ،منها مبادرة حلف شمال الاطلسي وما يسمى بالناتو،وبزعامة الولايات المتحدة الامريكية الى دعوة الدول الاعضاء في الحلف الى العمل على تحسين قدراتهم العسكرية الدفاعية ضد المخاطر والهجمات السيبرانية المستجدة في الساحة الدولية،من خلال تغير التفكير الاستراتيجي العسكري للدخول في الفضاء السيبراني ،اذ كانت الخطوة الاولى لهم من خلال اضفاء التدابير اللازمة للحكاية السلمية من هكذا هجمات بالاضافة الى مسألة الدفاع السيبراني، بعد ما تم توجيه الهجمات لهم بحلول عام ٢٠٠٧ الذي وقعت في أستونيا ،حيث تم تغير التوجه الى الاعتماد على الدفاع ضد الهجمات والمخاطر ورفعه الى المستويات الحديثة ،والذي تمخض عنه التحالف الدولي الاول للدفاع السيبراني (٤) في كانون الاول ٢٠٠٨.(١)

---

(١)د. إيهاب خليفة، الحرب السيبرانية الاستعداد لقيادة المعارك العسكرية في الميدان الخامس، ط١،العربي للنشر والتوزيع،القاهرة ٢٠٢١،ص٩٩

(٢)دافيد كولون ،حرب المعلومات: كيف تسيطر الدول على عقولنا،دون طبعة،٢٠٢٥ نوفل دمغة –هاشيت أنطوان، ص١٨٨٩ومابعدها.

(٣)المصدر نفسه أعلاه ،ص١٨٩٠ومابعدها.

(٤) يشكل الدفاع السيبراني جزءًا من المهمة الأساسية لحلف شمال الأطلسي في الردع والدفاع وتركز منظمة حلف شمال الأطلسي في مجال الدفاع السيبراني على حماية شبكاتها الخاصة، والعمل في الفضاء الإلكتروني (بما في ذلك من خلال عمليات ومهام التحالف)،

وبهذا نرى أن الاحداث الدولية والتطورات السريعة في مجال الامن السيبراني قد دفعت بالدول المتقدمة أولاً بالسير نحو اتخاذ الاجراءات الكفيلة بواجب الدفاع الشرعي السيبراني ومحاولة حماية أنظمتها ومعلوماتها و أمنها القومي المتعلق بتلك الانظمة ومتعلقاتها،لأن العالم اليوم يعيش في جو حروب معلوماتية وسيبرانية وان البنى التحتية للدول ومجالاتها العسكرية كلها منظمة وفق مجال البيانات والايعازات الحاسوبية مما يجعلها في مواجهة مخاطر الهجمات الحقيقية والارهابية ومحاولات زعزعة أمن الدول وسلامتها مما دفع بهؤلاء الى تدارك المواقف والوصوصل الى بر الامان والحماية لانظمتها وسيادتها الالكترونية على عكس الدول النامية أو المتأخرة بهذا المجال الحيوي والمهم من مجال الطفرة الدولية للانظمة والبرامج الوقائية.

الـخـــــــاتـمـــــة

في نهاية بحثنا المعني بمجال الامن السيبراني وحقوق الدول في الدفاع الالكتروني عن أمنها وسلامتها،والذي يعتبر بجد من المواضيع المستجدة والدقيقة والحساسة والتي تمس كيان الدول ووجودها توصلنا الى جملة من الاستنتاجات والتوصيات...

أولا:- الاستنتاجات

ومساعدة الحلفاء على تعزيز قدرتهم الوطنية على الصمود وتوفير منصة للتشاور السياسي والعمل الجماعي، في يوليو/تموز ٢٠١٦، أكد الحلفاء على التفويض الدفاعي لحلف شمال الأطلسي واعترفوا بالفضاء الإلكتروني كمجال للعمليات. يُمثّل حلف الناتو منصةً للحلفاء للتشاور سياسيًا، وتبادل المخاوف بشأن الأنشطة السيبرانية الخبيثة، وتبادل النهج والاستجابات الوطنية، ودراسة الاستجابات الجماعية المُمكنة. ويلتزم الحلفاء بتعزيز تبادل المعلومات والمساعدة المتبادلة في منع الهجمات السيبرانية، والتخفيف من آثارها، والتعافي منها، والتصدي لها.و يسعى الحلفاء إلى تعزيز فضاء إلكتروني حرّ ومفتوح وسلمي وآمن، ويبذلون جهودًا لتعزيز الاستقرار والحد من مخاطر الصراعات من خلال دعم القانون الدولي والمعايير الطوعية لسلوك الدول المسؤول في الفضاء الإلكتروني. في عام ٢٠١٦، وافق الحلفاء على تنفيذ تعهد الدفاع السيبراني. وفي عام ٢٠٢٣، عززوا هذا التعهد والتزموا بأهداف جديدة طموحة لتعزيز الدفاعات السيبرانية الوطنية كأولوية، بما في ذلك البنى التحتية الحيوية. ويعمل حلف شمال الأطلسي على تعزيز قدراته السيبرانية، بما في ذلك من خلال التعليم والتدريب والمناورات.و تدعم سياسة الدفاع السيبراني الشاملة لعام ٢٠٢١ المهام الأساسية لحلف شمال الأطلسي وموقف الردع والدفاع الشامل لتعزيز قدرة التحالف على الصمود بشكل أكبر.وفي قمة حلف شمال الأطلسي لعام ٢٠٢٣ في فيلنيوس، أقر الحلفاء مفهومًا جديدًا لتعزيز مساهمة الدفاع السيبراني في الردع الشامل وموقف الدفاع لحلف شمال الأطلسي، وأطلقوا قدرة دعم الحوادث السيبرانية الافتراضية لحلف شمال الأطلسي (VCISC) لدعم جهود التخفيف الوطنية استجابةً للأنشطة السيبرانية الخبيثة الكبيرة. وفي قمة حلف شمال الأطلسي لعام ٢٠٢٤ في واشنطن العاصمة، اتفق الحلفاء على إنشاء مركز الدفاع السيبراني المتكامل التابع لحلف شمال الأطلسي لتعزيز حماية الشبكة والوعي الظرفي وتنفيذ الفضاء الإلكتروني كمجال عملياتي. ويعمل حلف شمال الأطلسي مع جهات أخرى، بما في ذلك الاتحاد الأوروبي والأمم المتحدة ومنظمة الأمن والتعاون في أوروبا، في مجال الدفاع السيبراني. للمزيد ينظر الموقع الرسمي لحلف الناتو باللغة الانكليزية والمتاح على الرابط:-

https://www.nato.int/cps/en/natohq/topics_78170.htm

(١) المصدر السابق،ص ١٠٠ ومابعدها.

١. بروز أهمية الامن السيبراني نتيجة للتطورات التي شهدتها الدول وخصوصا في مجال المعلومات والامن الخاص ببيانات الدول وأنظمتها الحكومية والخاصة.
٢. تتنوع التهديدات السيبرانية على الدول وأمنها القومي مابين العسكرية والمالية والاقتصادية وصولاً الى الجانب الاجتماعي والثقافي لشعوب وافراد الدول كافة.
٣. تلعب سيادة الدول دوراً حيوياً في الاوساط الدولية وفي مجال الاستقلال والحماية لها،مما تدفع الدول الى حمايتها تحت جميع المسميات والمستجدات بما فيها السيبرانية وتداخلها لانتهاك والاضرار بها.
٤. تداركت الدول سريعاً مسألة الدفاع الشرعي السيبراني بعد ما بدأت الجهات والدول استخدام هذه الطريقة للحروب الحديثة دولياً ،مما أولد لديهم الفكرة في انشاء الجيوش الالكترونية وبمتابعة قادة الدفاع والعسكرين وجعلها جزء من المنظومة العسكرية لهم.

ثانيا :- التوصيات

١- العمل على انشاء معاهدة دولية شارعة ،وباشراف منظمة الامم المتحدة تجمع فيها الدول العالم ،وتجعل الدفاع الشرعي السيبراني متطلب دولي حديث ضمن أهداف الامن الجماعي الدولي..
٢- العمل على الموائمة بين التحالفات الدولية الخاصة بمجال الامن السيبراني والتشريعات الداخلية للدول في سبيل اضفاء الحماية اللازمة لحماية الأمن السيبراني للدول كافة.
٣- ضرورة التعاون الدولي بين الدول المتقدمة والمؤسسة لهكذا دفاعات مع غيرها من دوللاالعالم الثالث وذي الامكانيات المحدودة في مجال الدفاع الشرعي السيبراني.
٤- التنسيق بين دول الاعضاء في التنظيمات الاقليمية ،كجامعة الدول العربية في سبيل اتخاذ الخطوات اللازمة في مجال انشاء التحالفات الامنية والمعززة للدفاع الشرعي السيبراني،ومحاولة حماية الافراد والمؤسسات الخاصة من الاعتداءات والاضرار التي لاتعرف الحدود والاوقات.

المصادر

أولا :- الكتب والابحاث العلمية

١. د.ايهاب خليفة ،الحرب السيبرانية الاستعداد لقيادة المعارك العسكرية في الميدان الخامس، ط١،العربي للنشر والتوزيع، القاهرة ،٢٠٢١.
٢. م.م.احمد طلال احمد حسن،الامن السيبراني وتداعياته على الامن القومي المصري،بحث منشور في مجلة كلية القانون للعلوم القانونية والسياسية-جامعة كركوك ،المجلد(١٣)،العدد(٥١)،٢٠٢٤.
٣. د.خالد وليد محمود،الفضاء السيبراني وتحولات القوة في العلاقات الدولية،ط١، المركز العربي للأبحاث ودراسة السياسات،قطر،٢٠٢٥.
٤. د.سيناء علي محمود، التحديات الامنية للدول في الفضاء السيبراني ،بحث منشور في مجلة قضايا سياسية- جامعة النهرين، العدد(٨٠) ،٢٠٢٥،ص ٣٢٣،

٥. م.شهد عدنان صالح، الامن السيبراني وتأثيره على الامن القومي للدول،بحث منشور في المجلة السياسية والدولية –جامعة المستنصرية،العدد(٦٣)،٢٠٢٥ .
٦. دافيد كولون ،حرب المعلومات: كيف تسيطر الدول على عقولنا،دون طبعة،٢٠٢٥ نوفل دمغة –هاشيت أنطوان.
٧. د.مريم محمد حسين وم.مصطفى صادق عواد، الامن السيبراني والتنشئة الاجتماعية،بحث منشور في المجلة العراقية للعلوم السياسية،العدد(١٣)، ٢٠٢٤،ص ١٧٨.
٨. عادل عبد الصادق ،الاقتصاد الرقمي وتحديات السيادة السيبرانية،ط١،المركز العربي لابحاث الفضاء الالكتروني ،القاهرة ، ٢٠٢٠.
٩. عادل عبد الصادق ،الاقتصاد الرقمي وتحديات السيادة السيبرانية،مصدر سابق ، .
١٠. عدنان بوزان، مبادئ القانون الدولي العام،ط١، منشورات أزادي بوست المتاح على الرابط https://azadiposts.com/attachments/article/95، 2023،ص٥٤١.
١١. علي بن أحمد بن طراز , الأمن السيبراني ضرورة الوعي وحتمية التّطبيق،ط١،مركز الكتاب الأكاديمي،٢٠٢٥، عمان– الاردن.
١٢. فراس جمال شاكر محمود، الحروب المعلوماتية في المجال الأمني والعسكري أمريكا والصين،ط١،العربي للنشر والتوزيع، ٢٠٢٢،
١٣. د.مصطفى ابو الخير، القانون الدولي المعاصر،ط١،دار الجنان للنشر والتوزيع، عمان ،٢٠١٧.
١٤. د.منال البلقاسي، تأمين التهديدات السيبرانية تحت المجهر الرقمي،ط١،مؤسسة العبيكان للنشر والتوزيع،الرياض،السعودية، ٢٠٢٤، ص٤٧.
١٥. م.د. ياور عمر محمد،تأثير الامن السيبراني على الامن القومي العراقي(الفرص والتحديات) بحث منشور في مجلة كلية القانون للعلوم القانونية والسياسية–جامعة كركوك،المجلد(١٤) ،العدد(٥٣)، ٢٠٢٥.

ثانيا :- مواقع الانترنيت

١. الموقع الرسمي لحلف الناتو...
https://www.nato.int/cps/en/natohq/topics_78170.htm
٢. موقع معجم المعاني... https://www.almaany.com/ar/ A
٣. الموقع الرسمي لمنظمة الامم المتحدة.... www.un.org
٤. الموسوعة السياسية ....المتاح على الرابط :- https://political-encyclopedia.org/dictionary /
٥. موقع الاتحاد الدولي للاتصالات .....
https://www.itu.int/en/about/Pages/default.aspx#/ar
٦. الموقع الخاص بمديرية الأمن السيبراني، على الرابط :- https://moi.gov.iq/?page=6295