الهجمات السيبرانية وأثرها على تغير مفهوم السيادة لحدود الدولة من وجهة نظر جيوسياسية

م.م. عمر محمود مهدي ربيع الخزرجي
وزارة التعليم العالي والبحث العلمي / دائرة
البحث والتطوير الدراسات العليا
alkazrageomer@gmail.com
أ.م.د محمد نوح محمود عدو
جامعة كركوك كلية الاداب/ قسم الجغرافية التطبيقية
mohamedadoo@uokirkuk.edu.iq

Cyber attacks and their impact on changing the concept of sovereignty over state borders from a geopolitical point of view

Assistt Teacher. Omer Mahmood Al Khazraji
Ministry of Higher Education and Scientific Research / Department of Postgraduate Research and Development
alkazrageomer@gmail.com

Assist Prof Dr. Mohamed Nouh Adoo
Kirkuk University, College of Arts/Department of Applied Geography
mohamedadoo@uokirkuk.edu.iq

المستخلص

تتميز الجغرافية بأنها من العلوم الديناميكية بسبب التغيرات التي تحدث على الظواهر الجغرافية نتيجة الزمن متأثره بمجموعة عوامل الطبيعية وبشرية، وهذه الميزة انعكست على الجغرافيا السياسية والمفاهيم التابعة لها لاسيما السيادة والحدود فقد تأثرت بالتقدم التكنولوجي الذي يشهده العالم، وساهم هذا التطور في خرق سيادة الدول واصبحت بيانات ومعلومات الدول قابلة للاختراق، لأن قدرة كل دولة لم تعد مؤكدة في الحفاظ على اتصالاتها وقيادتها وسيطرتها وقدراتها الحاسوبية ضد التهديدات الجديدة من الانترنيت التي تواجه العالم بأكمله، كالهجمات الإرهابية وعصابات الجريمة المنظمة، فالمساحة الافتراضية التي يشغلها الانترنيت يمكن أن تهدد سيادة ومصالح الدولة بسبب نطاقها العالمي وامكانية نقل المعلومات خارج نطاق سيطرة الدول، دون اختراق حدودها البرية او البحرية او الجوية، لذلك يعد الفضاء السيبراني أحد أنواع الحدود للدولة وجزء هاما من أمنها القومي ومكانتها الدولية في ظل ما يعرف بالقوة الالكترونية وبهذا يشكل الفضاء السيبراني احد انواع الحدود الغير مرئية للدولة، وسلط البحث الضوء على ابرز هذه التحولات في اعادة تعريف مفهوم الحدود السياسية ليضم اليها الفضاء السيبراني التي يخص أمن المعلومات للدولة، وقد استعرض البحث مجموعة من الاتفاقيات التي من شأنها تنظم عمل هذه الوحدات الامنية المتخصصة في حماية دولها مع استعراض انماط الهجمات السيبرانية من حيث شدة الهجوم، ولم يغفل البحث في دراسة انموذجا من الهجمات السيبرانية متخذ من دول مجلس التعاون الخليجي مثالاً في نوع الهجمات سواء كانت اقتصادية او تخريبية او امنية وسبل مواجهتها .

مفاتيح الكلمات : الهجمات السيبرانية / الحدود السيادية / تطور الجغرافية /أمن المعلومات

Abstract

Geography is characterized as a dynamic science due to the changes that occur on geographical phenomena as a result of time affected by a group of natural and human factors, and this feature was reflected in the political geography and its concepts, especially sovereignty and borders, it was affected by the technological progress that the world is witnessing, and this development contributed to the violation of the sovereignty of countries and the data and information of countries became porous, because the ability of each country is no longer certain in maintaining its communications, leadership, control and computing capabilities against new threats from the Internet facing the world In its entirety, such as terrorist attacks and organized crime gangs, the virtual space occupied by the Internet can threaten the sovereignty and interests of the state because of its global scope and the possibility of transferring information outside the control of states, without penetrating their land, sea or air borders, so cyberspace is one of the types of borders of the state and an important part of its national security and international status in light of what is known as electronic power, and thus cyberspace is one of the types of invisible borders of the state, The research highlighted the most prominent of these transformations in redefining the concept of political borders to include the cyberspace that concerns the information security of the state, the research has reviewed a set of agreements that will regulate the work of these security units specialized in protecting their countries with a review of the patterns of cyber attacks in terms of the severity of the attack, and did not neglect the research in the study of a model of cyber attacks taken from the Gulf Cooperation Council countries as an example in the type of attacks, whether economic, sabotage or security And ways to confront them..

Keywords: Cyber attacks / Sovereign borders / Geographic evolution / Information security

المقدمة:

في العصر الرقمي سريع الخطى الذي نعيشه اليوم، أصبح الأمن السيبراني أمراً بالغ الأهمية ' وبما انه يمثل شكل من اشكال الحدود الجديدة فقد اهتمت وتأثرت الجغرافيا السياسية والمفاهيم التابعة لها لاسيما السيادة والحدود قد تأثرت بالتقدم التكنولوجي والثورة المعلوماتية والاتصالات الذي يشهده العالم، وساهم هذا التطور في خرق سيادة الدولة واصبحت بيانات ومعلومات الدول قابلة للاختراق، لأن قدرة كل دولة لم تعد مؤكدة في الحفاظ على اتصالاتها وقيادتها وسيطرتها وقدراتها الحاسوبية ضد التهديدات الجديدة من الهجمات السيبرانية التي تواجه العالم بأكمله ، فالمساحة الافتراضية التي يشغلها الانترنيت يمكن أن تهدد سيادة ومصالح الدول بسبب نطاقها العالمي وامكانية نقل المعلومات خارج نطاق سيطرة الدول، لذلك يعد الفضاء السيبراني أحد أنواع الحدود للدولة وجزء هاما من أمنها القومي ومكانتها الدولية في ظل ما يعرف بالقوة الالكترونية، من هنا جاء اهمية موضوع البحث الذي يحمل الصفة الجغرافية كونه يثبت نظرية الجغرافية المتجددة نتيجة تجدد التغيرات التي يستمر حدوثها نتيجة الزمان ،لينتقل مفهوم الحدود من الشكل المرئي (برية ، بحرية ، جوية) الى الشكل الغير مرئي الفضاء الالكتروني .

مشكلة الدراسة : ماهى السبل والاجراءات التي يجب ان تتخذ من أجل حماية سيادة الدولة من التهديدات السيبرانية المتزايدة التي تستهدف البنية التحتية الرقمية للدول والمؤسسات مثل الهجمات التجسس الالكتروني.

فرضية الدراسة :

- المساهمة في حماية الامن الالكتروني لسكان الدولة من التهديدات الالكترونية التي قد تأثر على ثقة المواطنين بقدرة الدولة على حمايتهم .

- الحفاظ على مستوى العلاقات الدولية المتكافئة والتعاون الاقليمي في الجانب السيبراني من حيث امكانية تبادل المعلومات بالقدر الذي يحفظ سيادة الدولتين .
- حماية سيادة الدولة والسيطرة على الفضاء الالكتروني من خلال بناء قدرات امنية بشرية والالكترونية تمكن الدولة من منع التهديدات السيبرانية وامكانية ايقافها وتحديد مصدرها لاستجاع المعلومات بفترة زمنية محددة.
- حماية الاقتصاد الوطني من خلال التأثير على البنية التحتية الرقمية والشركات والمؤسسات الحيوية وابداء القدرة على حماية رؤوس الاموال للمستثمرين من خلال حسابات مصرفية رقمية ذات قدرة عالية من الامن والاختراق.
- الحفاظ على الاستقرار السياسي والنظام من خلال حماية المؤسسات الحكومية والانظمة السياسية .
- **هدف الدراسة** : دراسة أثر هذه التهديدات على الحدود السياسية لجغرافية الدولة ليشمل ذلك تأثيرها على السيادة الوطنية ، والعلاقات الدولية والتوترات الاقليمية .
- **منهجية البحث** : اتبع البحث المنهج الوصفي والتحليلي وذلك من خلال اعطاء شروحات وصفية عن مصطلح الموضوع واهميته وتأثيراته لينتقل الى التحليل الوصفي المستند على بيانات تخص موضوع البحث وبيان التأثيرات وطريقة التعامل مع احداث التهديدات السيبرانية التي حصلت في الاقليم والدول التي اختارها البحث .

أولا: الأمن السيبراني والمفاهيم المتعلقة بها

تطلق كلمة (سيبر Cyber) على أي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي فالسيبرانية تعني (فضاء الإنترنت) ، أما الأمن السيبراني فهو مفهوم ظهر بعد الحرب الباردة استجابة للمزيد من الابتكارات التكنولوجية والظروف الجيوسياسية المتغيرة ، وتم استخدامه لأول مرة من قبل علماء الحاسوب في أوائل

التسعينات للتأكيد على سلسلة من حالات عدم الأمان المرتبطة بأجهزة الحاسوب لكنه تجاوز مفهومه التقني لأمن الحاسوب اذ يمكن أن يكون له آثار اجتماعية سلبية. ويعرف الأمن السيبراني أيضا بأنه العملية أو قدرة الدولة التي يتم بموجبها حماية انظمة الاتصالات والمعلومات الواردة اليها والدفاع عنها ضد الضرر أو الاستخدام غير المصرح به او التعديل او الاستغلال . [1]

ثانيا: أهم المفاهيم المتعلقة بالأمن السيبراني

1. **الفضاء السيبراني:** هو مجال عالمي في بيئة المعلومات الذي يتميز من خلال استخدام الإلكترونيات والطيف الكهرومغناطيسي لإنشاء وتخزين وتعديل وتبادل واستغلال المعلومات عبر شبكات مترابطة باستخدام تقنيات الاتصالات المعلوماتية، والفضاء السيبراني كبيئة افتراضية عالمية لأنظمة المعلومات العامة والخاصة المترابطة فيما بينها الذي يتم فيه إنشاء أنواع مختلفة من المعلومات وتخزينها ونقلها داخل الفضاء السيبراني، بما في ذلك أنواع معينة من المعلومات التي تهيمن على متطلبات أمن المعلومات بشكل عام، وكذلك القوانين واللوائح الوطنية والدولية المختلفة، وهو عالم افتراضي يتشابك مع العالم المادي يتأثر به ويؤثر فيه بشكل معقد أذ تقوم العلاقة بين العالمين على نظرة تكاملية تحمل في طياتها مزايا ومخاطر لا تتوقف، بيد أن طبيعة ذلك الفضاء كساحة عالمية عابرة لحدود الدول جعل الأمن السيبراني يمتد من داخل الدولة إلى النظام الدولي ليشكل نوعا من الأمن الجماعي العالمي لاسيما مع وجود مخاطر تهدد جميع الفاعلين في مجتمع المعلومات العالمي . [2]

2. الفضاء الجيو سيبراني العلاقة بين الانترنيت والجغرافيا والديمغرافيا والاقتصاد والسياسة للدولة وسياستها الخارجية

3. **القوة السيبرانية :** امكانية استخدام الفضاء السيبراني لانشاء الايجابيات والتأثير على الأحداث وعبر أدوات القوة والمتمثلة في الوسائل، والطاقات، والإمكانيات المادية وغير المادية، المنظورة وغير المنظورة التي بحوزة الدولة وتمثل الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحاسبات والمعلومات، والشبكات الإلكترونية، والبنية التحتية المعلوماتية، والمهارات البشرية المدربة للتعامل مع هذه الوسائل، ويستخدمها صانع القرار في فعل مؤثر يحقق مصالح الدولة، وتؤثر في سلوك الوحدات السياسية الأخرى.

4. **الإرهاب السيبراني:** الهجمات ذات الطابع الامني والسياسية أو التهديد بالهجوم على اجهزة الحاسوب أو الشبكات أو أنظمة المعلومات من أجل تدمير البنية التحتية وترهيب الحكومة أو المواطنين وإجبارهم على تحقيق أهداف سياسية واجتماعية بعيدة المدى، بمعنى أوسع فإن الإرهاب السيبراني يعني استخدام الإنترنت للتواصل والدعاية والتضليل من قبل المنظمات الإرهابية.

5. **الجريمة السيبرانية:** عمل غير قانوني موجه إلى نسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو التي تنقل عن طريقه، اضافة الى انه سلوك غير مشروع فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات . [3]

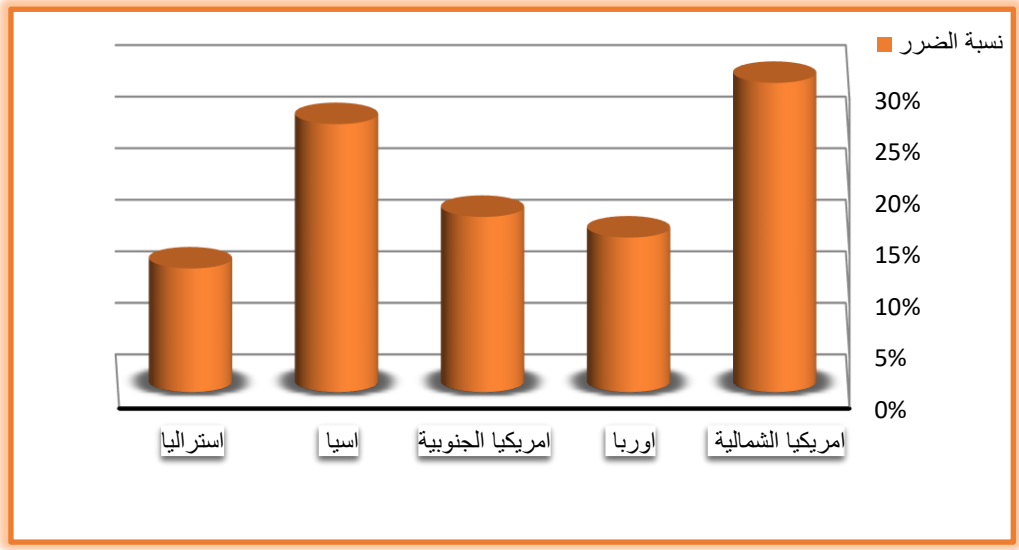
6. **الدفاع السيبراني:** مجال فرعي وظيفي للأمن السيبراني، ويتم التعامل معه على أنه جزء من عقيدة عسكرية، ينبغي أن تعتمد على الموارد والممارسات التي وضعها الأمن الإلكتروني الوطني المعني . [4]

ثالثا: واقع قارات العالم والدول الاكثر تعرضا للتجسس الالكتروني

يعد الأمن السيبراني ذات جوانب إشكالية نتيجة التطور المستمر والسريع للمخاطر الأمنية، وتتعرض جميع الدول الى عمليات تجسس الكتروني يؤثر في الاقتصاد او

الامن او يلحق الضرر في الاجهزة الخاصة والشخصية، اذ تتصدر امريكا الشمالية المرتبة الأولى بعد ان بلغت نسبة الضرر السيبراني (30%)، فيما كانت القارة الأسيوية بالمرتبة الثانية بنسبة 26%، اما القارة السمراء الأفريقية بنسبة 18%، وكانت اوربا بالمرتبة الرابعة 15%، أمريكا الجنوبية 17%، ثم استراليا بنسبة 12% والشكل (1) يوضح نسبة الضرر السيبراني لقارات العالم لعام 2020.

2نسبة الضرر السيبراني لقارات العالم لعام 2020.



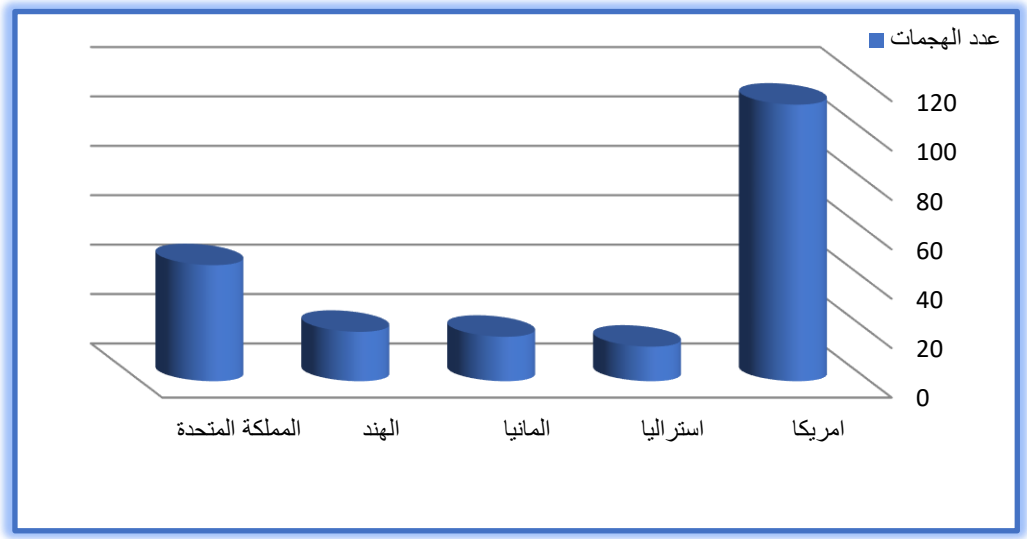
أصبحت جرائم الإنترنت الآن من الأعمال التجارية الغير مشروعة، حيث يتجاوز حجم الاحتيال عبر الإنترنت وسرقة الهوية وانتهاكات الملكية الفكرية واعمال الفنية ما يقدر بـــ تريليون دولار سنويا، مما يؤثر على ملايين الأشخاص حول العالم وعدد لا يحصى من الحكومات والشركات في مختلف البلدان. [5]

فهناك دولاً اصبحت عرضة للهجمات السيبرانية التي تأثرت بها مصالح اقتصادية وتم تعطيل بعض المصانع أو تأخير اعمال الشركات والمؤسسات المالية، وقد شهدت المملكة المتحدة وألمانيا والهند وأستراليا العديد من الهجمات الإلكترونية

المهمة التي استهدفت الخدمات الحكومية والفيدرالية في السنوات الـــ (10 الماضية)، ومع ذلك فإن وضعها كهدف يتضاءل مقارنة بالولايات المتحدة، حيث تعرضت الولايات المتحدة لـــ (112 هجوما إلكترونيا منفصلا) في الفترة ما بين سنة 2010 وسنة 2020. علما انها احتلت المرتبة الثانية في شنها الهجمات السيبرانية سنة 2017. (6)

ومن ابرز الهجمات الكبيرة (الاعتداءات على الوكالات الحكومية والإدارات الدفاعية وشركات التكنولوجيا الفائقة) في الدولة، والتي تتميز بتنسيق هجمات أدت إلى خسائر اقتصادية تجاوزت المليون دولار، وللمقارنة مع سجلات الدول الأخرى، كانت الدولة الثانية في القائمة، المملكة المتحدة، هدفا ل(47 هجوما كبيرا فترة الـــ (10 اعوام) بين عامي 2010 – 2020، فيما سجلت إحصاءات الهند وألمانيا واستراليا (20 و 18 و 14) هجوما على التوالي لم يقترب إجمالي الهجمات الإلكترونية خلال فترة العشر أعوام من إجمالي الهجمات التي تعرضت لها الولايات المتحدة، حيث سجلت في مجموعها (99)، هجوما كبيرا . [7] والشكل (2) .

شكل (2) الهجمات السيبرانية التي تعرضت لها بعض الدول خلال (2010-2020)



وحسب مؤشر القوة الوطنية السيبرانية لعام 2020 تتصدر الولايات المتحدة الامريكية دول العالم من حيث أقوى الدول في الامن السيبراني وتاتي الصين بعدها وبرطانيا ثالثاً وبقية الدول وكما موضح في الشكل (3)

شكل (3) ترتيب اقوى عشر دول في العالم من حيث الامن السيبراني لسنة 2020

رابعاً: الاتفاقيات الدولية التي وضعت بخصوص الامن السيبراني

تعمل الاتفاقيات الدولية على الحد من الأنشطة السيبرانية كعمليات التجسس، والمراقبة وغيرها. وقد دخلت الولايات المتحدة طرفاً في هذا الاتفاقيات، إذ حدت من عملياتها السيبرانية، ويمكن ذكر أهم هذه الاتفاقيات من خلال المطالب الآتية.

1-**اتفاقية تحالف خمس عيون** : Five eyes وهو مجموعة من وكالات ا ستخباراتية لخمس من الدول تعمل وتتبادل المعلومات، وهي: (استراليا، نيوزلندا، المملكة المتحدة، كندا، الولايات المتحدة) وقد بدء هذا التحالف باتفاقية (Bursa)، إذ تم توقيعها في مارس (١٩٤٦)، وانضمت إليها كلا: (بريطانيا، وكندا، واستراليا، ونيوزلندا) في عام(1956). وتطورت الاتفاقية الأصلية إلى هذا التحالف، وتذكر مسودة (٢٠٠٥) بتوجيهات وكالة الأمن القومي (NSA) إن الشركاء يتحفظون بالحق في إجراء عمليات استخباراتية ضد مواطنين بعضهم البعض عندما يكون يصب ذلك في م صلحة الأمة، وفي يوليو عام (٢٠١٧)، رفعت الخ صو صية الدولية، إذ أقيمت دعوى قضائية ضد و كالة الأمن القومي الأمريكي (NSA)، ومكتب مدير

الاستخبارات الوطنية، ووزارة الخارجية، والإدارة الوطنية للمحفوظات، والسجلات، من قبل الدول الأعضـــاء في التحالف، وذلك بســـبب عدم الالتزام بتحالف الخمس عيون.

2- **اتفاقية مجلس أوروبا** : هى اتفاقية متعددة الاطراف، وملزمة قانونا وقعت سنة 2001م، وتم تفعليها سنة 2004م. وقد وقعت عليها (46) دولة، بما في ذلك كندا، واليابان، وجنوب إفريقيا، والولايات المتحدة الأمريكية، وصدق عليها من قبل (٢٦) دولة فقط، ولم تصدق عليها روسيا، وتقتضي اتفاقية المجلس الأوروبي أن تلتزم أطرافها بالتشريعات، لتلزم مقدمي خدمات الانترنت بحفظ بيانات معينة تخزن على خوادمها لمدة تصل إلى تسعين يوم قابلة للتجديد، إذا طلب منهم ذلك مسؤول انفاذ القانون. ويعد هذا الأمر أمراً بالغ الأهمية، نظراً للصيغة المؤقتة للبيانات الإلكترونية. كما أن الإجراءات التقليدية للمساعدة القانونية المتبادلة غالباً ما تستغرق وقتاً طويلاً في القضايا العابرة للحدود الوطنية.

اتفاقية دليل تالين : (Tallin manual) تم إبرام صك قانوني سنة 2013م، أعده مجموعة من خبراء القانون الدولي بدعوة من حلف الشمال الأطلسي (NATO)، ومدى إمكانية تطبيق قواعد القانون الدولي الإنساني على الحروب السيبرانية، وذلك إثر الهجوم السيبراني الشامل الذي شنته روسيا على استونيا سنة 2007م ويحتوي الدليل على (95) قاعدة، إذ تتمثل تحدياته الرئيسة في ضمان توجيه الهجمات ضد الأهداف العسكرية فقط، وتوخي الحذر لحقن دماء المدنيين والبنية التحتية الضرورية. وكل ذلك جاء نتيجة لوجود فضاء سيبراني واحد، تتقاسمه القوات المسلحة والجيوش السيبرانية مع باقي المستخدمين المدنيين. [8]

خامساً: مخاطر الاختراق السيبراني على أمن الدولة

تتمثل المخاطر والهجمات السيبرانية وخروق خصوصية المعلومات من أكبر التحديات التي تواجه امن الدول وخاصة القطاع المالي ، فمع زيادة الخدمات المالية الالكترونية والاستعانة بمصادر خارجية في تقديمها تزداد مخاطر حماية المستهلك وتنظيم القطاع المالي غير المصرفي، وتمثل الهجمات السيبرانية أعظم المخاطر التي تواجه هذا القطاع وذلك بسبب ازدياد تواترها وعدم إمكانية التنبؤ بها وتأثيرها القطاعي المحتمل ووجود الثغرات في إدارة مخاطرها. وأهم أشكال الهجمات على القطاع المالي هي الآتي:

أ. القرصنة عبر طرف ثالث

تمكن مجرمو الانترنت من اختراق مركزين العاجلة البطاقات الالكترونية في الهند والتي تتولى مهمة عمليات الدفع البطاقات الدفع المسبق لمصرفين أحدهما في عمان والآخر بالإمارات العربية المتحدة، وقد قام المجرمون بزيادة الأرصدة المتاحة وسقوف السحب على البطاقات الائتمانية مسبقة الدفع بالإضافة إلى إدخال بطاقات مزوراه زائفة والتي مكنتهم من سحب 45 مليون دولار من أجهزة الصراف الآلي في 27 دولة.

ب. تخريب البنية التحتية لأجهزة الصراف الآلي

استخدم مجرمو الانترنت في عام 2016م برمجيات خبيثة خاصة تجبر أجهزة الصراف الآلي على صرف النقود في عدد من دول الشرق الأوسط. وقد كانت الإمارات العربية هدفا لعدد من هذه الهجمات، فقد استهدفت هذه الهجمات مركز بيانات أجهزة الصرف الآلي والتي مكنت المجرمون من التقاط البيانات الخاصة بالعملاء بما في ذلك

رقم حساب العميل المصرفي والرقم السري للبطاقة اللائتمانية (PIN) المستخدم في الصرف الآلي بالإضافة إلى السرقة المباشرة للنقود.

ت. اختراق أنظمة الحاسوب بالبنوك

قام مجرمو الانترنت باختراق أنظمة الحاسوب بالبنوك الخليجية باستخدام وسائل البريد الالكتروني الخبيثة وبرامج القرصنة مما نتج عنها خسائر كبيرة في بعض الدول في سنة 2017م

ث. الحرمان من الخدمة الموزعة

اخترق مجرمو الانترنت في سنة 2012م المواقع الالكترونية في العديد من المؤسسات المالية العربية والتي شملت بورصة أبوظبي للأوراق المالية، والبورصة السعودية، ومواقع البنك المركزي في الإمارات والبنك العربي الفلسطيني.

ج. خروقات البيانات

تمكن مجرمـــو الأنترنت من القرصنة على أحد البنوك الإماراتية وطالبوا بدفع الفديـــة بالعملة الرقمية (Bit Coin) في مقابل عدم تسريب المعاملات المالية السرية وتفاصيل العميل على الشبكات الاجتماعية في سنة 2015م. كما عاني أحد أكبر بنوك قطر من اختراق للبيانات الخاصة والذي تضمن بيانات العملاء الخاصة في سنة 2016م. [9]

سادساً: القدرات السيبراني وأثاره على طبيعة الصراعات والتهديدات الأمنية

إختصر الفضاء السيبراني حاجز الزمان والمكان وخلق مساحات للتفاعلات الداخلية والدولية في الواقع الإفتراضي، ومن ثم برزت فضاءات جديد للصراعات بادوات مختلفة وأنماط جديد تختلف عن الصراعات التقليدية، وتعود أسباب إهتمام الفاعلين من الدول أو غير الدول لتحقيق الهيمنة من خلال إمتلاكها لعدة سمات منها:

1-**ساحة صراع افتراضية:** يتخطى الفضاء السيبراني عدد من الثنائيات الموجودة في الصراعات التقليدية وهو أقل تكلفة من حيث الخسائر المادية وأكثر تحديدا للهدف.

1-**زيادة الإعتماد الإلكتروني:** حيث باتت الدول تربط ببنيتها التحتية بالفضاء السيبراني خاصة شبكات الكهرباء والمياه والبنوك والإتصالات وجمع المعلومات.

2- **صعوبة وضع الحدود:** زادت حالة التأثير الشبكي داخل الدول وخارجها وإتسع إستخدام الأفراد والجماعات والدول للتكنولوجيا الحديثة المرتبطة بالفضاء السيبراني من مواقع التواصل الإجتماعي، هواتف ذكية ومواقع للتعاملات المالية والتجارية. اذ أصبح للفضاء الإلكتروني دور في حركة التفاعلات والتحولات البنيوية في العلاقات الدولية وبدأ ينتقل تأثيره من تغييرات هيكلية وتحتية إلى إحداث تغييرات كيفية على النظام الدولي، وأصبح يشهد العالم تطور المخاطر الأمنية مع التطور التكنولوجي وأصبحت مسألة أمن الفضاء الإلكتروني مصدر إهتمام على أجندة القضايا الأمنية الدولية، خاصة بعد أحداث 11 سبتمبر بدأ التركيز على الفضاء الإلكتروني كتهديد أمني جديد وفي سنة 2007م برز بوضوح دور الفضاء الإلكتروني كمجال جديد في العمليات العدائية في الصراع بين إستونيا وروسيا وفي سنة 2008 خلال الحرب بين روسيا وجورجيا، وفي عام 2010 أكتشف فيروس الكتروني مدمر باسم ستكسنيت Stuxnet تمكن من إختراق أكثر من عشرة مواقع صناعية إيرانية فائقة الحساسية منها حواسيب آلية في معامل تخصيب اليورانيوم، كما هو الحال لباقي العمليات السيبرانية خلال سنة2012 حيث تعرضت مؤسسات مالية أمريكية ضخمة لهجوم سيبراني أسفر عن محاولة تعطيل المواقع الإلكترونية لبنك أمريكا وكذلك موقع بنك سيتي جروب Citi Group كما تعرضت في نفس السنة شركة أرامكو السعودية التي تعد أكبر شركة نفط في العالم ، طالت هذه الهجمات أيضا قيادة النقل الأمريكية سنة

2012 ، وبهذا دخل الفضاء السيبراني ضمن المحددات الجديدة للقوة من حيث طبيعتها وأنماط إستخدامها، لتحديد الهدف الإستراتيجي للقوة السيبرانية لانشاء ميزة لصناع القرار، وفهم البيئة الإستراتيجية للسلام والحرب مع افتقار العدو لهذه الميزة في الوقت نفسه من خلال فهم التحديات والفرص في الفضاء السيبراني، وقد أدى تزايد عدد الهجمات السيبرانية التي شنتها الدول وبعض الفاعلين من غير الدول إلى الإعلان عن شكل جديد من الحروب في العصر الرقمي الذي يهدد القوى العسكرية، وأدت الصراعات السيبرانية إلى دخول الدول في عمليات هجومية ضد دول أخرى دون اشتباك وهذا ما يميز الصراعات السيبرانية في مقابل الاستراتيجية العسكرية الكلاسيكية، وتعد روسيا والصين والولايات المتحدة من أكبر القوى في مجال الإستحواذ على القوة الإلكترونية القادرة على توفير أقصى درجات الأمن الإلكتروني Cyber Secuity وهو ما فرض على الدول إتخاذ إجراءات حماية عبر تبني سياسات دفاعية من أجل الدفاع ضد الأخطار المحتملة وحماية نظام المعلومات ومنع تعرضها لعمليات هجومية وتعزيز الأمن الإلكتروني بأبعاده المتعلقة بالبرمجيات والبنية التحية، بالإضافة لتبني سياسات هجومية عبر اتخاذ إجراءات لمهاجمة مصادر التهديد. وقد ظهرت قوى إقليمية سيبرانية جديدة كايران وتركيا وفاعلون من غير الدول يحاولون توظيف القدرات الإلكترونية لتحقيق مارب إستراتيجية وإقتناص مزايا سياسية وإقتصادية، إذ برزت إيران كواحدة من أهم الأطراف الإقليمية في تطوير القدرات السيبرانية لها مهام وأنشطة دفاعية وهجومية، وبات يدخل ضمن نطاق إستراتيجية الأمن القومي الإيراني والتي بنيت على ركزتين أولها تتمثل بحماية الأمن الوطني الإيراني عن طريق بناء بنية تحية علمية تكنولوجية وإستخبارية تعتمد على إستراتيجية وقائية في أثناء الدفاع وإستراتيجية استباقية في أثناء الهجوم، أما الركيزة الثانية بتطوير العديد من المفاهيم والتقاليد القتالية

الخاصة بها، وذلك عن طريق تشكيل شبكة معقدة من الجيوش الإلكترونية القادرة على شن هجمات سيبرانية، إلى جانب تفعيل قدراتها الإستخبارية في نشر المعلومات المضللة [10].

سابعاً: اثر الحروب السيبرانية في طبيعة وخصائص الصراع الدولي

1. **ساحة جديدة للصراع الدولي**

برزت العلاقة بين الفضاء الإلكتروني والسيطرة على الحدود الفضائية باعتبارها بعداً جديداً يتضمن كل شبكات الاتصالات ومصادر المعلومات التي يتم تبادلها إلكترونياً والصراع الإلكتروني "هو حالة من التعارض في المصالح والقيم يتم تسويته عبر الفضاء الإلكتروني، واتجه الصراع الدولي حول الموارد والمصالح والقيم نحو الاعتماد على تكنولوجيا الاتصال والمعلومات فيما يعرف بصراع "عصر المعلومات"

2. **اتساع دائرة الصراع والفاعلين فيه:** مع انتشار الفضاء الإلكتروني وسهولة الدخول إليه يمكن أن يوسع دائرة الاستهداف بالإضافة إلى زيادة عدد المهاجمين، ولتدور تلك الهجمات المتبادلة على نحو من الكر والفر ليعبر عن حالة صراع ممتد يرتبط بطبيعة الفضاء الإلكتروني المختلفة. ودفعت الأهمية المتصاعدة للفضاء الإلكتروني في الاستحواذ على القوة إلى الصراع حول امتلاك مقدراتها وأدواتها من أجل العمل على الحماية والدفاع وتطوير القدرات الهجومية في سبيل تعظيم القوة والتفوق والهيمنة بين الدول والفاعلين من غير الدول وتعزيز التنافس حول السيطرة والابتكار والتحكم في المعلومات، وتعظيم القدرات القادرة على زيادة النفوذ والتأثير، ليس على نطاق محلي فقط، بل على نطاق دولي أيضاً.

3. **تعدد ادوات الصراع وطرق الحروب :**ولأن المتصارعين "الفعليين" يستخدموا شتى أنواع أسلحة التدمير الممكنة فانهم نقلوا كذلك جبهات القتال التقليدية بشكل موازٍ لها إلى ساحة الفضاء الإلكتروني. وكان لتلك التغييرات دور في إعادة التفكير في حركية وديناميكية الصراع وظهور ما يعرف بـــ"عصر القوة النسبية" الذي يعني بعجز" القوة

العسكرية" عن تأمين الأهداف السياسية المترتبة عليها، مما يخلف آثاراً استراتيجية هائلة على مستوى تركيبة وتوازنات النظام الدولي. وتتأثر حالة الصراع وانعدام الأمن الحدود في الفضاء الإلكتروني بكل أنواع البيئات الأخرى غير المتصلة بالفضاء الإلكتروني كالنزاعات بين الأفراد والصراع بين الجماعات والصراع بين الدول أو صراع بين الشركات الدولية.

4-الصراع الالكتروني وتغير براديم الحرب : تغير"براديم" الحرب جذرياً بانتقاله من نسق "الحروب الصناعية بين الدول" إلى نسق "الحرب في وسط الشعوب". ففي الحروب القديمة كان الغرض هو تدمير الخصم، إما باحتلال أرضه أو الاستيلاء على موارده، بينما أصبح في الحرب الجديدة هو التحكم في إرادته وخياراته، ومن ثم كان الدور المحوري للشعوب في هذا الصنف الجديد من الحروب، سواء تعلق الأمر بالسكان المستهدفين في أرضية المواجهة، أو بالرأي العام في الدولة التي تشن الحرب، أو بالرأي العام الإقليمي والدولي. وأصبحت أهداف الحرب أقل مادية، يؤدي فيها العامل النفسي والدعائي دوراً محورياً، وسببه تنامي التغطية الإخبارية السمعية البصرية المباشرة للأحداث لحظة وقوعها عبر مواقع الإنترنت والفضائيات إلى جانب ضعف سيطرة أنظمة الحكم على توجهات مواطنيها.

4. بروز صراعات محلية –دولية ذات طبيعة عالمية: ساعدت البيئة المحلية والسياق الدولي للفضاء الإلكتروني على بروز الصراعات ذات البعد المحلي– الدولي من خلال توفير بيئة مناسبة لدمج الفئات والقوى المهمشة في السياسة الدولية وخلق شبكة تحالفات مؤيدة أو معارضة ذات نطاق دولي عريض إما على أساس قيم حقوقية أو انتماءات عرقية أو دينية. وساهم الفضاء الإلكتروني في دعم الهيكل التنظيمي والاتصالي للحركات والجماعات والمنظمات المدنية إلى جانب بروز ظاهرة الفاعلين من غير الدول في عمليات التجنيد والحشد والتعبئة والتمويل. (11)

ثامناً: تطبيقات وأنماط الحروب السيبرانية في الشأن العالمي [12]

1- نمط "الحرب "الباردة الالكترونية والصراع "منخفض الشدة":

يعبر هذا النمط عن صراع ذو طبيعة ممتدة ومستمرة ودائمة النشاط العدائي أو غير السلمي، وقد تكون اهدافه ذات نواحي ثقافية أو اقتصادية أو اجتماعية. ويتميز هذا النمط بدرجة كبيرة من التعقيد والتداخل في معركة لا نهاية لها، ما بقيت الأبعاد الأخرى للصراع، ولا يتطور هذا النوع من الصراعات بالضرورة إلى حالة استخدام القوة المسلحة بشكلها التقليدي أو من خلال شن حرب إلكترونية واسعة النطاق. ويمكن ان تسمى "الحرب الباردة الإلكترونية" من خلال شن الحرب النفسية والاختراقات المتعددة والتجسس وسرقة المعلومات وشن حرب الأفكار، ولا ترقى لعمل عسكري عنيف، ويتمثل في حالات الصراع السياسي ذو البعد الاجتماعي- الديني الممتد، مثل: حالة الصراع العربي الإسرائيلي أو الصراع ما بين الهند وباكستان أو ما بين كوريا الجنوبية والشمالية. [13]

2: نمط "الحرب" الالكترونية متوسطة الشدة

يتمثل هذا الصراع من خلال الفضاء الإلكتروني إلى ساحة موازية لحرب تقليدية دائرة، ويكون تعبيراً عن حدَّة الصراع القائم بين الأطراف، وقد يكون مقدمة لعمل عسكري. وتدور حرب عبر الفضاء الإلكتروني عن طريق اختراق المواقع وقصفها وشنِّ حرب نفسية وغيرها. ويستمد ذلك الصراع سخونته من قوة أطرافه وارتباطه بعمل عسكري تقليدي، وبخاصة مع تكلف فقط 4% من تكلفة الآلة العسكرية، بما يمكِّن من تمويل حملة حربية كاملة عبر الإنترنت بتكلفة دبابة. كما أنَّها لا تستغرق إلا وقتًا بسيطًا. ويتم استخدام الفضاء الإلكتروني في الصراع بطريقة موازية للحرب التقليدية. وتاريخيًّا تم استخدامه في هجمات حلف الناتو سنة 1999م على يوغسلافيا، وتستهدف الهجمات شبكات الاتصالات ويعطلها، ما يؤدي تلقائيًّا لتوقف شبكات الجيش، وتم استخدام هذا النمط من الهجمات في الحرب بين حزب الله وإسرائيل في سنة 2006م ، وتم استخدام الهجمات الإلكترونية في حالة الحرب الجورجية-الروسية

سنة 2008م. وتم ذلك في المواجهات بين حماس وإسرائيل في سنة 2009 و2012م .

3:نمط الحرب الالكترونية "الساخنة "والصراع مرتفع الشدة.

لم يشهد العالم حربا الكترونيا منفردة ودون العمل العسكري التقليدي الا ان هناك ارهاصات لتحول ذلك في المستقبل. ويتميز هذا النمط من الصراع على سيطرة البعد التكنولوجي على إدارة العمليات الحربية حيث يتم استخدام الأسلحة الإلكترونية فقط ضد منشآت العدو، ويتم استخدام الروبوتات الآلية في الحروب والتي يتم إدارتها عن بعد فضلاً عن الطائرات بدون طيار، ويتم تطوير القدرات في مجال الدفاع والهجوم الإلكتروني والاستحواذ على القوة الإلكترونية، ويتم استخدام الفضاء الإلكتروني في الاستعداد لحرب المستقبل والقيام بتدريبات على توجيه ضربة أولى لحواسب العدو، واختراق العمليات العسكرية عالية التقنية، أو حتى باستهداف الحياة المدنية والبنية التحتية المعلوماتية. ولعل الهدف من وراء ذلك؛ تحقيق "الهيمنة الإلكترونية الواسعة" بشكل أسرع في حالة نشوب صراع.

ويتم التقدم في مجال استخدام كافة أنواع الأسلحة الإلكترونية مثل أسلحة الميكروويف عالية القدرة، وتم توجيه هجمات إلكترونية باستخدام عدد من الفيروسات مثل قيام اسرائيل بشن هجمات فيروس ستاكس نت في سنة 2010م ضد المنشآت النووية الإيرانية بالتعاون مع الولايات المتحدة .

تاسعاً: الهجمات السيبرانية واستراتيجيات الردع المعتمدة لدول الخليج العربية انموذجا

الردع السيبراني هو منع الأعمال الضارة ضد الأحوال الوطنية في الفضاء. ويرتكز على ثلاث ركائز هي : مصداقية الدفاع، والقدرة على الانتقام والرغبة في الانتقام . وفي ظل تعدد التهديدات التي تشمل الحرب الرقمية والإرهاب الرقمي والتجسس الرقمي، بجانب التزايد المفرط في أعدادها في السنوات القليلة الماضية،

تتزايد أهمية الردع لتأمين أجهزة الحاسب الآلي، وأنظمة المعلومات والبنى التحتية من ناحية والحيلولة دون تكرار تلك الهجمات من خلال تحديد الخصم على نحو دقيق وتوعده بالانتقام ردا على هجومه من ناحية ثانية وحماية الأمن القومي للدول الذي بات رهناً بالفضاء السيبراني من ناحية الثالثة. ويتم تحقيق الردع السيبراني من خلال رفع تكلفة الهجوم الإلكتروني للدولة المعتدية، عبر إنشاء نظم دفاعية الكترونية صعبة الاختراق تحتاج إلى وقت وجهد كبيرين لاختراقها مع تطوير قدرات تتبع الهجمات السيبرانية واكتشاف مصدرها بما يؤدي إلى التأثير على قرارات الخصم وردعه عن شن هجمات سيبرانية على الدولة في النهاية. وقد شهدت دول الخليج العربي في السنوات الأخيرة تزايد الهجمات السيبرانية بشكل حاد نظرا لتعددها لتشمل الحروب والإرهاب والتجسس الرقمي وغيرها، وبالرغم من اختلاف غرض وأهداف كل منها إلا أن القاسم المشترك بينها هو استغلال ثغرات ونقاط الضعف في المجال السيبراني بهدف اختراق الكومبيوتر وشبكات الحاسوب ، وقد أدت الهجمات التي وقعت خلال السنوات القليلة الماضية في الفضاء السيبراني لدول الخليج العربي إلى قيام نشاط ملحوظ بين دول مجلس التعاون الخليجي لبناء قدرات الأمن السيبراني وإنشاء المؤسسات المتخصصة بهذا الشأن ووضع الاستراتيجيات اللازمة للحد من هذه الهجمات كما تم سن قوانين خاصة بمكافحة الجرائم السيبرانية. ولردع الهجمات السيبرانية في فضاء دول مجلس التعاون تم تأسيس مراكز وطنية لحماية الأمن السيبراني وفرق الاستجابة لطوارئ الحاسب الآلي والمركز الإقليمي للأمن الإلكتروني للمنطقة العربية .[14]

الاستنتاجات:

1- السيبرانية هو كل شئ متعلق بالحاسوب المرتبط بالشبكة العالمية الانترنيت .

2- الهجمات السيبرانية هو اختراق الحدود الغير مرئية للدولة (الفضائية) من قبل طرف اجنبي اومحلي لوثائق رسمية او سرية بغض النظر عن نوعها سواء كانت امنية او مالية او مصرفية او وسائل سمعية وبصرية .

3- تم تنظيم عدد من الاتفاقيات الدولية للحد من الهجمات السيبرانية التي من شأنها ان تخترق سيادة الدول او التي تؤدي الى الحاق ضرر في البنى التحتية المدنية .

4- رغم تعرض عدد من الدول الى عدد من الهجمات السيبرانية الى انها لم تعلن بشكل رسمي وذلك لاسباب تتعلق بسيادة الدولة وعدم ضهورها كدولة ضعيفة .

5- تصنف الهجمات السيبرانية من حيث الغرض منها الى ثلاث اصناف

الاولى : تسعى الى سرقة الاموال سواء من الاشخاص او المصارف والتحويلات المالية وعادة ما تكون بين اشخاص محترفين ضد اشخاص او مؤسسات غير حكومية وهى ترتقي الى مستوى الجريمة الالكترونية دون هدف سياسي .

الثانية : تسعى الى كشف معلومات سرية تخص امن الدولة وامكانياتها الحالية والمستقبلية وعادة ما تكون بين اجهزة استخبارتية بين دولتين لايشترط ان يكون هناك عداء بينهم وهى ترتقي الى التجسس الالكتروني .

الثالثة : الهجمات السيبرانية المعلنة وهدفها تخريب وتدمير البنى التحتية العسكرية او الامنية للدولة وعادة ماتكون مقدمة للصراح عسكري كلاسيكي تكون عادة بين دول متصارعة .

6- مع التقدم التكنولوجي في مجال المعلوماتية والاتصالات اتخذت اغلب الدول اقسام خاصة للتصدي الى مثل هذه الهجمات وامكانية الردع المضاد وتحاشي اختراق انظمتها الحاسوبية سواء كانت اعلامية او مالية او امنية او عسكرية.

7- اعتبار الامن السيبراني احد انواع الحدود السيادية للدولة كونه يخترق خصوصيتها وامنها القومي .

الهوامش

[1] احمد السيد الشوادفي النجار، المواجهة الجنائية لجرائم تقنية المعلومات وفقاً لاحكام القانون ، مجلة دراسات القانونية والاقتصادية ،العدد 2 ، لسنة 2018 ، ص662

[2] . البشري، محمد أمين التحقيق في الجرائم المستحدثة، الرياض: جامعة نايف العربية للعلوم الأمنية، مركز الدراسات والبحوث ، 2004، ص210

[3] احمد السيد الشوادفي النجار، المواجهة الجنائية لجرائم تقنية المعلومات وفقاً لاحكام القانون، مصدر سابق ، ص 638

[4] البشري، محمد أمين التحقيق في الجرائم المستحدثة ، مصدر سابق ،ص 212

[5] العنزي، سليمان وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير ، الرياض: جامعة نايف العربية للعلوم الأمنية 2003، ص165

[6] نفس المصدر ، ص178

[7] هربرت لين ، النزاع السيبراني والقانون الدولي الانساني ، مجلة الصليب الاحمر ، مجلد 94 ، العدد 886، 2012، ص 518

[8] دليل تالين ، عن يحيى ياسين مسعود ، الحرب السيبرانية في ضوء قواعد القانون الدولي الانساني ، المجلة القانونية ، المجلد 4، 2018، ص94

[9] السحيباني، عبدالله كفاءة الإجراءات الإدارية في المحافظة على أمن المعلومات، رسالة ماجستير، الرياض: جامعة نايف العربية للعلوم الأمنية ، 1996، ص235

[10] محمد صلاح عبد اللاه ربيع ، الهجمات السيبرانية بين مشروعيتها كوسيلة للدفاع الشرعي وادانتها كاعتداء غير مشروع ، مجلة الدراسات القانونية والاقتصادية ، العدد 2 ، 2021،ص 4157–4179

[11] محمد صلاح عبد اللاه ربيع ، الهجمات السيبرانية بين مشروعيتها كوسيلة للدفاع الشرعي وادانتها كاعتداء غير مشروع ، مصدر سابق،ص 4181

[12] عادل عبد الصادق ، أنماط الحرب السيبرانية وتداعياتها على الأمن العالمي السياسية الدولية ، القاهرة ، 2011، ص17

[13] محمد صلاح عبد اللاه ربيع ، الهجمات السيبرانية بين مشروعيتها كوسيلة للدفاع الشرعي وادانتها كاعتداء غير مشروع ، مصدر سابق ، ص 4177

[14] Emarah,S. (2007) : The Control of Firewalls using Active Networks, Information Technology and national security Conference, Riyadh.

المصادر:

1. احمد السيد الشوادفي النجار، المواجهة الجنائية لجرائم تقنية المعلومات وفقاً لاحكام القانون ، مجلة دراسات القانونية والاقتصادية ،العدد 2 ، لسنة 2018 .

2. البشري، محمد أمين التحقيق في الجرائم المستحدثة، الرياض: جامعة نايف العربية للعلوم الأمنية، مركز الدراسات والبحوث ، 2004.

3. العنزي، سليمان وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير ، الرياض: جامعة نايف العربية للعلوم الأمنية 2003.

4. عادل عبد الصادق ، أنماط الحرب السيبرانية وتداعياتها على الأمن العالمي السياسية الدولية ، القاهرة ، 2011.

5. السحيباني، عبدالله كفاءة الإجراءات الإدارية في المحافظة على أمن المعلومات، رسالة ماجستير، الرياض: جامعة نايف العربية للعلوم الأمنية ، 1996.

6. دليل تالين ، عن يحيى ياسين مسعود ، الحرب السيبرانية في ضوء قواعد القانون الدولي الانساني ، المجلة القانونية ، المجلد 4، 2018.

7. محمد صلاح عبد اللاه ربيع ، الهجمات السيبرانية بين مشروعيتها كوسيلة للدفاع الشرعي وادانتها كاعتداء غير مشروع ، مجلة الدراسات القانونية والاقتصادية ، العدد 2 ، 2021.

8. محمد صلاح عبد اللاه ربيع ، الهجمات السيبرانية بين مشروعيتها كوسيلة للدفاع الشرعي وادانتها كاعتداء غير مشروع .

9. هربرت لين ، النزاع السيبراني والقانون الدولي الانساني ، مجلة الصليب الاحمر ، مجلد 94 ، العدد 886، 2012.

المصادر الاجنبية

1. Emarah,S. (2007) : The Control of Firewalls using Active Networks, Information Technology and national security Conference, Riyadh.

References

1. Ahmed Al-Sayed Al-Shawadfi Al-Najjar, Criminal Confrontation of Information Technology Crimes According to the Provisions of the Law, Journal of Legal and Economic Studies, Issue 2, 2018.

2. Al-Bishri, Muhammad Amin, Investigation into New Crimes, Riyadh: Naif Arab University for Security Sciences, Center for Studies and Research, 2004.

3. Al-Anazi, Suleiman, Methods of Investigating Information Systems Crimes, Master's Thesis, Riyadh: Naif Arab University for Security Sciences, 2003.

4. Adel Abdel Sadiq, Patterns of Cyber Warfare and its Implications for Global Security and International Political Affairs, Cairo, 2011.

5. Al-Suhaibani, Abdullah, The Efficiency of Administrative Procedures in Maintaining Information Security, Master's Thesis, Riyadh: Naif Arab University for Security Sciences, 1996.

6. Tallinn Guide, on Yahya Yassin Masoud, cyber warfare in light of the rules of international humanitarian law, Legal Journal, Volume 4, 2018.

7. Muhammad Salah Abdullah Rabie, Cyberattacks between their legitimacy as a means of legitimate defense and their condemnation as an unlawful attack, Journal of Legal and Economic Studies, Issue 2, 2021.

8. Muhammad Salah Abdullah Rabie, cyber attacks between their legitimacy as a means of legitimate defense and their condemnation as an unlawful attack.

9. Herbert Lane, Cyber Conflict and International Humanitarian Law, Red Cross Magazine, Volume 94, Issue 886,.

10. **E**m arah,S. (2007) : The Control of Firewalls using Active Networks, Information Technology and national security Conference, Riyadh**.**