IRAQI Academic Scientific Journals
العراقية المجلات الاكاديمية العلمية
مجلة جامعة الكوت للعلوم الإنسانية
ISSN (E): 2707 – 5648 II ISSN (P): 2707 – 563x
www.kutcollegejournal1.alkutcollege.edu.iq
k.u.c.j.hum@alkutcollege.edu.iq
عدد خاص لبحوث المؤتمر العلمي الدولي السادس للإبداع والابتكار للمدة من 16 - 17 نيسان 2025

الاستراتيجيات الاستباقية للمنظمات الدولية لمواجهة تأثيرات السيبرانية على حقوق الانسان

م. م. سندس نوري حسان [1]

المستخلص

ادى التقدم المتسارع لتكنولوجيا المعلومات وعلى رأسها تقنية الانترنت وشبكات التواصل الاجتماعي العملاقة الى ظهور ما يسمى بالمجتمعات والحوكمات الالكترونية، وعلى اثر ذلك برز نوع جديد وغير مألوف من التحديات يدعى بالهجمات السيبرانية والتي تفرض مهددات لعموم الدول المتقدمة والنامية، حيث تحولت هذه الهجمات الى مصدر قلق كبير اذ ما نظرنا الى اثارها وتبعاتها على السكان المدنيين والبيئة فيما لو تم تنفيذها على منشاة نووية او مصادر الطاقة كشبكة الكهرباء والمياه فهذا يجعل المدنيين عرضة لخطر الحرمان من الاحتياجات الاساسية. ونظرا لطبيعة التهديدات السيبرانية المتجددة بصورة مستمرة ،لذا اتجهت جهود المنظمات الدولية نحو ما يعرف بالاستراتيجيات الاستباقية ،اي القدرة التوقعية على التحرك قبل الوصول الى المرحلة التي تكون فيها الظروف المهددة موجودة فعلا. بحيث توجه هذه الجهود اما نحو منع او تقليص مهددات هذه الهجمات او الحد منها ، وهذا يتطلب تبني اليات ووسائل فاعلة خاصة لمواجهتها وهذه الاليات تحتاج الى بعد النظر لتحديد التهديدات التي تؤثر على الافراد وهي بنفس الوقت تقدم تخطيط وتنفيذ الاجراءات التي من شأنها التقليل من تهديدات واضرار الهجمات على الافراد . ومن هنا انطلقنا في بحثنا هذا لبيان استراتيجيات الاستباقية التي اتخذتها المنظمات الدولية لحماية الافراد من خطر السيبرانية واثارها على حقوق الانسان.

الكلمات المفتاحية: السيبرانية، الاستراتيجيات الاستباقية، الآليات الوقائية، الآليات التشريعية

انتساب الباحث
[1] مجلس القضاء الاعلى، العراق، بغداد، 10001

[1] rihassansounds@gmail.com

المؤلف المراسل[1]

معلومات البحث
تأريخ النشر: تشرين الاول 2025

Broactive Strategies of international organization to address the impact of cyberspace on human rights

Assist. Lec. Sonos Nouri Hassan [1]

Affiliation of Author
[1] Supreme Gudicial Council, Iraq, Baghdad, 10001

[1] rihassansounds@gmail.com

[1] **Corresponding Author**

Paper Info.
Published: Oct. 2025

Abstract

The rapid progress of information technology, especially the Internet and giant social networks, has led to the emergence of what are called electronic societies and governance. As a result, a new and unfamiliar type of challenges has emerged called cyber attacks, which pose threats to both developed and developing countries. These attacks have become a major source of concern when we consider their effects and consequences on civilians and the environment if they are carried out on a nuclear facility or energy sources such as the electricity and water grid. This exposes civilians to the risk of being deprived of basic needs. Given the nature of constantly renewed cyber threats, the efforts of international organizations have turned towards what are known as proactive strategies, i.e. predictive ability, meaning the ability to act before reaching the stage where the threatening conditions actually exist, so that these proactive efforts are directed either towards preventing or reducing the threats of these attacks or limiting them. This requires the adoption of effective mechanisms and means to confront them. These mechanisms require foresight to identify the threats that affect individuals, while at the same time providing planning and implementation of procedures that would reduce the threats and damages of attacks on individuals. Hence, we set out in this research to demonstrate the proactive strategies adopted by international organizations to protect individuals from the danger of cyberspace and its effects on human rights.

Keywords: Cyber, Broactive Strategies, Breventive Mechanisms, Legislative Mechanisms

المقدمة

تشكل حماية حقوق الانسان من جميع الانتهاكات والتحديات والتهديدات هاجسا يشغل المنظمات الدولية كافة اذ يتوجب عليها ان تختار سياسة وقائية تحافظ بها على احترام مبادئ حقوق الانسان التي تقرها مواثيقها ، ومن اخطر هذه التهديدات في عصرنا الحالي

ما يعرف بمصطلح الهجمات السيبرانية اذ يعد هذا المصطلح من المفاهيم الحديثة التي لا يوجد اجماع دولي بشان تعريفه مما ادى الى صعوبة تكييف وتحديد المسؤولية الدولية عنه وعلى الرغم بما تتميز به هذه الهجمات في انخفاض التكلفة والسهولة في اللجوء اليها اذ لا تتطلب عدد كبير من المقاتلين والالاف من الاسلحة كالنزاعات التقليدية بل يكفي لتنفيذها شخص او مجموعة صغيرة ممن لديهم الخبرة والمهارة التكنلوجية السيبرانية وثغرات برامج الكومبيوترات لاستخدامها ضد دولة او دول اخرى الا ان هذه المميزات تتحول الى مصدر قلق كبير اذ ما نظرنا الى اثار هذه الهجمات وتبعاتها على السكان المدنيين والبيئة فيما لو تم تنفيذها على منشاة نووية او مصادر الطاقة كشبكة الكهرباء والمياه وهذا يجعل المدنيين عرضة لخطر الحرمان من الاحتياجات الاساسية. لذا اولت المنظمات الدولية اهتماماً غير مسبوق يتمثل بالجهد الذي تبذله من اجل حماية الافراد من مخاطر هذه الهجمات،إذ اتجهت المنظمات الدولية الى استخدام استراتيجيات استباقية مختلفة، تشمل هذه الاستراتيجيات مجموعة من الاجراءات التي تقوم بها هذه المنظمات .

اهمية البحث

تكمن اهمية البحث كونه يمثل محاولة لاعطاء رؤية حول اهم الاستراتيجيات الاستباقية التي تتخذها المنظمات الدولية في مواجهة تاثيرات السيبرانية والتحديات والمهددات التي تفرضها على حقوق الانسان ومن ثم الوقوف على نقاط القوة والضعف لها .

هدف البحث

يحاول البحث تحقيق جملة من الاهداف اهمها ، التعرف على مفهوم السيبرانية وتمييزها عن غيرها ، وبيان اثار الهجمات السيبرانية على حقوق الانسان، مع توضيح الاستراتيجيات الاستباقية التي تتخذها المنظمات الدولية لمواجهة مخاطر هذه الهجمات السيبرانية .

اشكالية البحث

بما ان الحرب السيبرانية باتت تمثل سمة مميزة للنظام الدولي لعالم ما بعد الحرب الباردة فان اشكالية البحث تتمحور حول الاسئلة الاتي :ماهي الاستراتيجيات الاستباقية المختلفة التي تتخذها المنظمات الدولية حمايتا لحقوق الانسان من اثار السيبرانية ، وما هي آليات تنفيذها وهل هي كافية وقادة على مواجهة جميع اثارها .

منهجية البحث

لتحقيق اهداف البحث فقد تم توظيف المنهج الاستقرائي وتضمين الاسلوب الوصفي التحليلي لتحليل ظاهرة السيبرانية ووصفها ومعرفة اهم اثارها وتهديداتها على حقوق الانسان والتطرق لخطة المنظمات الدولية الاستباقية في مواجهتها .

هيكلية البحث

سوف نتناول موضوعنا هذا في مبحثين نخصص المبحث الاول لمفهوم السيبرانية وتأثيراتها على حقوق الانسان ونخصص المبحث الثاني للآليات الاستباقية للمنظمات الدولية لمواجهة مخاطر السيبرانية على حقوق الانسان وعلى النحو الاتي .

المبحث الاول / مفهوم السيبرانية وتأثيراتها على حقوق الانسان

سنقسم هذا المبحث الى مطلبين نخصص المطلب الاول لمفهوم السيبرانية ونخصص المطلب الثاني تأثيرات السيبرانية على حقوق الانسان وعلى النحو الاتي :

المطلب الاول / مفهوم السيبرانية

سنتناول في هذا المطلب تعريف السيبرانية وتمييزها عن غيرها وكلُ في فرع خاصُ به وعلى النحو الاتي :

الفرع الاول / تعريف السيبرانية

جاءت كلمة السيبرانية من الكلمة الاغريقية (Kybernetes) وتعني الطيار او قائد الدفة، ويكثر استخدام الكلمة في مجال تكنولوجيا المعلومات ، ويشير قاموس المورد الى انها (عدم السيطرة وضبط الاشياء والتحكم فيها عن بعد)، في حين ان قاموس المصطلحات الامريكي العسكري عرف السيبرانية بدلالة الهجوم عبر الفضاءات الالكترونية من اجل اختراق بنى تحتية محمية الكترونياً بقصد تعطيلها او تدميرها والحاق الاضرار بها [1]، (لبنى خمبس وتغريد صفاء ، ربيع 2020 ، ص 148) ويعد نوربرت وينر اوت من استخدم مصطلح السيبرانية في عام 1948، وتعد الحرب السيبرانية مجهولة المصدر تتحرك عبر شبكات المعلومات والاتصالات عالميا غامضة الاهداف ولا تميز لبن استهداف المنشأت المدنية او العسكرية [2] (عبد الله محمد العصيمي ، 2017 متاح على الرابط ، https:llwww.al-jazirah.com) ويرى اخرون بأن الحرب السيبرانية باتت مصطلح يشير الى ((اي نزاع يحصل في السيبراني ويأخذ طابع دولي)) الا ان هذا التعريف غير دقيق ولا يعبر عن فحوا الحروب في الفضاء بدقة . كما يرى اخرون التركيز على اشكال وانواع النزاع الذي يحدث في الفضاء السيبراني والذي يشمل المستوى الاول من النزاع في الفضاء السيبراني والمتمثل بالقرصنة الالكترونية ، والمستوى

الثاني والثالث والمتمثل بالجريمة والتجسس الالكتروني ، والارهاب الالكتروني الذي يقع في المستوى الرابع، اما الحرب السيبرانية فهي الاخطر من بين كل المستويات السابقة ومن آلياتها ووسائلها البرامج الخبيثة وتشمل الفيروسات والديدان وحيل تصيد المعلومات أو خلق فكرة تسلل على غرار فكرة (حصان طروادة) وهي عبارة عن برنامج حاسوب غير مرخصة يضاف الى البرنامج المستهدف ويسمح لرجال الفضاء السيبراني باختراق الشبكات واحيانا تسمح ثغرة التسلل بالوصول الى جذر البرنامج فتصبح لهم القدرة والصلاحية لمصمم البرنامج وبالتالي يمكنهم اضافة ما يشاؤون من برمجيات خبيثة ويمحون اي اثر على وجودهم [3] (بشلالق ليلى ،2018 ، ص41)ويرى البعض الاخر بان الحرب السيبرانية ((هي امتداد للسياسات من خلال الاجراءات المتخذة في الفضاء السيبراني من قبل جهات فاعلة تابعة للدولة او من قبل جهات فاعلة غير حكومية لديها توجيه او دعم مهم من الدولة والتي تشكل تهديدا خطير لدول اخرى))، كما عرفت ايضاً على انها ((اجراءات من قبل دولة قومية لاختراق اجهزة الكمبيوتر او الشبكات الخاصة بدولة اخرى بغرض احداث ضرر بها او تعطيلها)) [4] مهند جبار عباس وهيثم كريم صيوان ، ص 146)يشير هذا التعريف الى ان هدف ومصدر اعمال الحرب السيبرانية هما فقط بين الدول القومية [5] Humairaa Yacoob Bhaiyat and Siphesihle , p536 ومن كل ما تقدم يمكن تعريف الحرب السيبرانية على انها ((استخدام تكنلوجية المعلومات لاختراق او تعطيل اجهزة الحاسوب وشبكات المعلومات لدولة ما لغرض احداث ضرراً بها)).

الفرع الثاني / تمييز الحرب السيبرانية عن غيرها

اولاً / الحرب السيبرانية والجريمة الالكترونية

عرفت الجريمة الالكترونية بأنها ((الجريمة التي ترتكب باستخدام الجهاز الكمبيوتر وذلك من خلال الاتصال بالانترنت او يكون الغرض منها اختراق الشبكات وتخريبها والتزوير والاختلاس والتحريف وسرقة حقوق الملكية الفكرية والسرقة والقرصنة))، وعرفها اخرون بأنتها ((عبارة عن مجموعة من الافعال الغير مشروعة المرتبطة بالمعلوماتية والتي لا بد ان تكون جديرة بانزال العقاب عليها)) [6] (نايل نبيل عمر ،2013،ص 13)وعرفها اخرون بانها ((عمل اجرامي يتم بمساعد الحاسب الآلي أو هي كل جريمة ترتكب في اطار الحاسب الالي)) [7] (وليد مهند اسماعيل ، 2016،ص72) وعرفها البعض الاخر بأنها ((الجريمة التي تتطلب لارتكابها ان يكون مرتكبها لديه معرفة بتقنية الحاسوب الالي)) [8] (محمود احمد ،2005 ، ص15) وبناءً على ذلك فان الجريمة الالكترونية تختلف عن الحرب السيبرانية في الباعث على ارتكابها والهدف من ارتكابها فالجريمة الالكترونية تصدر عن جهة لا تمثل الدولة سواء كانت شخصاً طبيعيا او معنوياً سعياً وراء هدف اجرامي لأغراض شخصية ، كما ان هذه الافعال لا يصبغ عليها وصف الجريمة الا اذا كانت مجرمة وفقاً للقانون الجنائي عملاً بقاعدة ((لا جريمة ولا عقوبة الا بنص)) (9) (ذباب البدائية ،2014 ،ص 25) بينما الحرب السيبرانية تكون صادرة عن الدولة او احد مؤسساتها بهدف اضعاف الوظيفة التي تقوم بها اجهزة الحاسوب المستهدفة ، وان قواعد القانون الدولي العام هي من تطبق على هذه الهجمات .

ثانياً / الحرب السيبرانية والارهاب الالكتروني

عرف الارهاب الالكتروني بأنه ((سلوك اجرامي يتم عبر شبكة الانترنت بهدف بث الافكار المتطرفة الدينية أو السياسية أو العنصرية ، وذلك للسيطرة على وجدان الافراد من اجل افساد عقائدهم واستغلال معاناتهم من اجل تحقيق اهداف خاصة تتعارض مع مصلحة المجتمع))[10] (حسنين بوادي ،2006، ص54) فالارهاب الالكتروني اذاً هو استخدام وسائل التقنية الرقمية والالكترونية من خلال الافراد او الجماعات او الدول ضد اي شخص طبيعي او معنوي بدوافع سياسية وذلك بهدف اخافته او تهديده والتأثير عليه معنويا او ماديا وذلك بقصد التأثير بقرارات الحكومة والرأي العام [11](مايا حسن خاطر ، 2018 ، ص 58).
وبناءً على ذلك فأن الارهاب الالكتروني جريمة جنائية متساوية مع غيرها من الجرائم كالجرائم الالكترونية وجريمة قرصنة المعلومات وجرائم الإرهاب [12] (مايا حسن خاطر ، ص 61) اما الحرب السيبرانية لا تعد جريمة جنائية ، كما انها لا تقوم الا بين الدول او جماعة ودولة فضلاً عن ان دوافع الحرب السيبرانية تكون سياسية وليست دينية .

ثالثاً / الحرب السيبرانية والحرب التقليدية

عرفت الحرب التقليدية بأنها ((قتال مسلح بين الدول بهدف تغليب وجهة نظر سياسية لوسائل نظمها القانون الدولي [13] (حسنين المحمودي بوادي ، 2005 ، ص 10) وعرفها البعض بانها ((نضال مسلح بين فريقين متنازعين يستعمل كل فريق جميع ما لديه من وسائل الدمار للدفاع مصالحه وحقوقه او فرض ارادته على الغير [14] (محمد المجذوب ، 2004 ،ص 23) وفي اطار الحرب التقليدية فقد تطورت الاسلحة واستخدمت اسلحة الدمار الشامل المحظور دوليا، والتي تؤدي الى تدمير واسع النطاق لكافة الكائنات الحية ، ومنها الانسان ، وتؤدي الى تخريب البيئة ، او اتلافها

وتلويثها [15](عبد الستار حسين الجميلي ،2013 ،ص 261) وبناء على ذلك تتميز الحرب السيبرانية عن التقليدية في طبيعة السلاح المستخدم فترتب اثار تختلف عن الاثار المترتبة على الحرب التقليدية ، حيث ان الاخيرة تقوم على اساس استخدام الجيوش النظامية وقبل قيامها يكون هناك اعلان للحرب ويوجد ميدان للقتال محدد، بينما الحرب السيبرانية تكون في ميدان غير محدد حيث تدور الهجمات السيبرانية في الفضاء الالكتروني ، كما ان اسلحتها تكون الكترونية تتوافق مع طبيعتها ، كما انها تكون موجهة ضد المنشآت الحيوية او وضعها عن طريق عملاء الاجهزة الاستخباراتية [16](عمر رضا بيومي ،2002 ،ص 25) .

المطلب الثاني / اثار الحرب السيبرانية على حقوق الانسان

الفرع الاول / الاثار الايجابية للحرب السبرانية

تعتبر الاهداف غير البشرية للهجمات من ابرز ايجابيات الحرب السيبرانية ، وبالتالي تقلل من عدد الضحايا [17]،(Mohan , Computer Science ,M.S Gazula B. ,2017,p16 Cyber Warfare Conflict Analysis,)اذ يقدر عدد القتلى في الحربين العالميتين الاولى والثانية حوالي 97 مليون قتيل، اي ما يعادل 6% من سكان العالم آنذاك ، وكذلك التدمير الذي يطال البنى التحتية والاعيان المدنية وغيرها ، إضافة الى الجرحى والمرضى والمشردين واللاجئين . وفي هذا الصدد اوضحت لائحة الجمعية العامة للأمم المتحدة رقم 23/70 (2015) الصادرة في 23/ يناير /2015 المتضمنة للتطورات في ميدان المعلومات والاتصالات السلكية واللاسلكية في سياق الامن الدولي من لن التطبيقات العسكرية للتطورات العلمية والتكنولوجية يمكن ان تسهم اسهاما كبيرا في تحسين وتطوير منظومات الاسلحة المتطورة . ولا سيما اسلحة الدمار الشامل وبالتالي رفع مستوى التهديدات التي تمس الامن والسلم الدولي .لذلك استهل ميثاق الامم المتحدة في ديباجته بالاشارة الى ضرورة انقاذ البشرية من ويلات الحرب ، حيث نصت الفقرة 2 من الديباجة على ((ان ننقذ الاجيال المقبلة من ويلات الحرب التي من خلال جيل واحد جلبت على الانسانية مرتين احزاناً يعجز عنها الوصف)) . وفي سؤال للمستشار القانوني للجنة الدولية للصليب الاحمر (CICR) حول امكانية استخدام التكنولوجيا السيبرانية بشكل ايجابي اثناء النزاعات المسلحة ، اجاب بان الامر يقع على عاتق الدول اثناء سير العمليات الحربية حيث تلتزم بتجنب الاصابات في صفوف المدنيين [18](درويش سعيد ، ص 190) كما انه لا يمكن استبعاد امكانية ان يؤدي التطور التكنولوجي في المستقبل الى تطور اسلحة سيبرانية من شأنها التسبب في اصابات واضرار عرضية اقل من الاسلحة التقليدية في ظروف معينة علاوة على انه يمكن استخدام الفضاء السيبراني ورواده كشهود رقميين على الجرائم التي يمكن ارتكابها في حق المدنيين [19](هند الحناوي ، 2014، ص 10) .

الفرع الثاني / الاثار السلبية للحرب السيبرانية

ان الفضاء السيبراني اصبح يستخدم في شتى مظاهر الحياة في الدولة ، السياسية ، الامنية ، الاقتصادية ، التجارية ولهذه الاعتبارات يشبه البعض حروب الفضاء السيبراني باسلحة الدمار الشامل (20)،(BY ANDREW KREPINEVICH ,2012,p4 CYBER WARFARE;) كما ان البنى التحتية الالكترونية المدنية غالباً ما ترتبط بنظيرتها العسكرية من خلال شبكة الانترنت [21] (اللجنة الدولية للصليب الاحمر ،2015) حيث ان استهداف نظم المواصلات وشبكات الكهرباء والسدود والمستشفيات والمنشآت الكيميائية او النووية تعتبر من اهم الاثار السلبية التي تثيرها الهجمات السيبرانية وحروب الفضاء الالكتروني ، وعليه فان احتمالية اختراق المنظومة الالكترونية للمفاعلات النووية قد يسبب في كوارث مروعة بحيث يصعب التحكم في اثارها البشرية والبيئية ، كما ان اتاحة شبكات الانترنت للجميع وسهولة الولوج فيها يمكن للقراصنة والجهات الفاعلة من غير الدول كالجماعات الارهابية ان تشن هجمات على دولة معينة [22](Ryan Shandler, Michaeil L. Gross, DAPhna Canetti,2023,p41) يمكن ان تسبب في تدميرها اقتصاديا او عسكرياً لا سيما وان الفضاء الالكتروني يتميز بانه لا يعترف بتعداد الجيوش ولا بسيادة او حدود الدول فيمكن لشخص بسيط وبمفرده وفي اقصا مكان من الارض ان يشن هجوما مدمراً على دولة معينة [23](درويش سعيد ،ص189) ولهذه الاعتبارات يساور اللجنة الدولية قلق بشأن الحرب السيبرانية بسبب ضعف الشبكات الالكترونية والتكلفة الانسانية المحتملة من جراء هذه الهجمات ، فعندما تتعرض الحواسيب والشبكات التابعة لدولة ما لهجوم او اختراق او إعاقة قد يجعل هذا الامر المدنيين عرضة لخطر الحرمان من الاحتياجات الاساسية مثل مياه الشرب والرعاية الطبية والكهرباء ، كما انه اذا تعطلت انظمة تحديد الموقع GPS عن العمل يحدث اصابات في صفوف المدنيين من خلال تعطيل عمليات اقلاع مروحيات الانقاذ .

المبحث الثاني: الآليات الاستباقية للمنظمات الدولية لمواجهة مخاطر السيبرانية على حقوق الانسان

تعتمد المنظمات الدولية في استراتيجتها الاستباقية لضمان حماية حقوق الانسان من اثار السيبرانية على ما يعرف بالآليات الوقائية

التي تهدف الى الحيلولة دون حدوث التهديدات ، والآليات التشريعية والتي تهدف الى وضع الاطار التشريعي الملائم لأمن الفضاء السيبراني ومكافحة التهديدات السيبرانية حمايتاً لحقوق الافراد من الانتهاكات والحد من وقوعها، وسوف نتناول هذه الآليات كلاً في مطلب خاص بها وعلى النحو الاتي:

المطلب الأول: الآليات الوقائية للمنظمات الدولية لمواجهة اثار السيبرانية على حقوق الانسان

تهدف الاليات الوقائية الى الحيلولة دون حدوث انتهاكات وشيكة بحيث تعمل على معرفة الوقت الذي يكون فيه الناس أو الافراد عرضة لخطر انتهاك حقوقها ، فاعتماد اليات وقائية يجعل من المنظمات الدولية لا تتعامل فقط مع النتائج أو تعديات أو تهديدات انما منعها أو الحد منها ، وقد ركزت المنظمات الدولية في آلياتها الوقائية على عنصرين اساسيين، الاول هو التهديد والهشاشة أو القابلية للتضرر الناتجة عن التهديدات ، اما العنصر الثاني فهو الانكشاف والذي يكون موجودا عندما يتعرض الافراد لتطورات يمكن ان تكون ضارة الى جانب نقص الوسائل لمنعها او الحد منها ، وتكمن اهمية ثنائية التهديد والانكشاف من خلال انها تسمح للمنظمات الدولية باختيار الادراكات والتصورات للخطر، بدلا من الحل التكنوقراطية التي تعزز استمرارية الوضع الراهن وتعمق الانكشاف الانساني ، وبناءً على ذلك فقد اتخذت المنظمات الدولية مبادرات عدة في مجال الوقاية من الجريمة السيبرانية حمايتاً لحقوق الانسان من قبل ذلك على سبيل المجال الجهود التي بذلتها الاتحاد الدولي للاتصالات ، منظمة الشرطة الجنائية الدولية (الانتربول) ، مؤسسة الانترنت للأسماء والارقام المخصصة ، المنظمات الدولية للمعايير ، اللجان الكهروتقنية الدولية ، وغيرها من المنظمات التي عنيت بالجرائم السيبرانية . وللوقوف اكثر على الاليات الوقائية للمنظمات الدولية سوف نتناول في هذا المطلب اهم الجهود التي تقوم عليها بعض اهم المنظمات الدولية ، نتناول اولاً جهود الاتحاد الدولي للاتصالات ، ثم جهود وكالة الاتحاد الاوربي للأمن السيبراني .

الفرع الاول / دور الاتحاد الدولي للاتصالات (ITU) في المجال الامن السيبراني

الاتحاد الدولي للاتصالات هو وكالة تابعة للأمم المتحدة المتخصصة في مجال تكنولوجيا المعلومات ، يعد هذا الاتحاد المنظمة الرئيسية المسئولة عن تطوير المعايير الدولية لتكنولوجيا المعلومات والاتصالات ، وتعزيز التوصيلية العالمية ، وتحسين الوصول الى تكنولوجيا المعلومات والاتصالات في جميع انحاء العالم [24](محمد احمد لبيب ، هيثم محمد بهاء ،مصطفى احمد كمال ، 2024،ص 134)، اطلق الاتحاد دليلاً لوضع الاستراتيجيات الوطنية للأمن السيبراني ، وقد تم تعديلها اكثر من مرة وشاركة في وضع هذا الدليل اثنا عشر شريكاً دولياً كان من ابرزهم وكالة الاتحاد الاوربي للأمن السيبراني ، اضافة لعدد من المنظمات الدولية والقطاع الخاص والمجتمع المدني ، وتحدد نطاق الدليل ليشمل مختلف جوانب التهديدات السيبرانية حيث يتم صياغة الاستراتيجية مع الاخذ في الاعتبار الواقع ، وهو الاجراءات العملية التي تتخذها الدول في مختلف مراحل الاستراتيجية وبين محتوى النص الفعلي للاستراتيجية [25](جعفر حاتم القاضي ،لبيب محمد ،2023،ص92،93)، وقد ركز هذا الدليل على مفاهيم محدد اطلق عليها مجالات التركيز وهي :

1- الحوكمة : ضرورة وضع بنية منضبطة فعالة للأمن السيبراني وذلك من خلال تحديد الاهداف المرجوة في مجال الامن السيبراني وحماية حقوق الافراد من الانتهاكات ، وضمان اعلى مستوى من الدعم لتحقيق هذه الاهداف ، وتحديد السلطة المختصة لتنفيذ هذه الاستراتيجية وتحملها المسؤولية [26](محمد احمد لبيب، هيثم محمد بهاء ، مصطفى احمد كمال، ص 135)

2- ادارة المخاطر : يتعلق مجال التركيز الثاني بضرورة اعتماد نهج ادارة المخاطر في مجال الامن السيبراني اذ يتم تحديد وتقييم المخاطر التي يمكن يتعرض لها الافراد من خلال الهجمات السيبرانية ، وذلك من خلال تحديد المخاطر الناشئة عن التبعات عبر الحدود الوطنية ، ومن خلال ادارة هذه المخاطر على نحو فعال ، كما يجب ان يشمل نهج ادارة المخاطر في مجال الامن السيبراني كامل دورة الحياة .

3- التأهب والصمود : يرتكز هذا المجال على تعزيز قدرة الدولة على التعامل مع الهجمات السيبرانية وتحمل اثارها ، وذلك من خلال تطوير قدرات الاستعداد للتعامل مع هذه الهجمات والتصدي لها ، كما يشمل هذا المجال تحديد المخاطر وتقييمها ، وتطوير خطط الطوارئ وانشاء انظمة لادارة الازمات ، وتحسين قدرات التحقق من الاصول والخدمات المهمة لضمان استمرارية عمليات البنية التحتية المختلفة، وتوفير التدريب والتوعية للفرق المختصة في مختلف المؤسسات واجراء تمارين الأمن السيبراني ، بغية رفع مستوى التأهب والصمود في حال حدوث اي هجوم سيبراني .

4- خدمات البنية التحتية الحرجة والخدمات الاساسية : يرتكز هذا المجال على تعزيز امن البنية التحتية المهمة والحرجة في

البلدان ، وذلك من خلال تطوير استراتيجيات لحماية هذه الخدمات وتقليل المخاطر المتعلقة بها ، ويشمل هذا المجال ، تحديد الخدمات الحرجة ، وتطوير خطط لادارة هذه المخاطر وتوفير التدابير الامنية لحمايتها ، بما في ذلك استخدام التقنيات الامنية المتقدمة وانشاء نظام مراقبة مستمر وتوفير التوعية لفريق الامن في مؤسسات البنية التحتية لغرض حماية هذه المؤسسات من اي تهديد سيبراني يمكن ان يحرم الافراد من خدماتها .

5- التوعية وبناء القدرات : يرتكز هذا المجال على تعزيز قدرات الافراد والمؤسسات في مجال الامن السيبراني ، من خلال تطوير برنامج تدريبية وتعليمية لتحسين الخبرات في هذا المجال ، كما يشمل هذا المجال تطوير استراتيجيات لتحفيز الابتكار في مجال الامن السيبراني ، كما يشمل هذا المجال اذكاء الوعي باهمية الامن السيبراني وتحقيق الحماية من الهجمات السيبرانية من خلال حملات توعوية واعلامية .

6- التشريع : يهدف هذا المجال الى وضع اطار قانوني وتنظيمي لحماية المجتمعات من الهجمات السيبرانية وتاثيراتها على الافراد ، ويشمل هذا المجال تحديد ما يشكل نشاطا سيبرانياً غير قانونياً ، والاعتراف القانوني بالحقوق الفردية والحريات المدنية في البيئة السيبرانية ، ويشمل هذا المجال كذلك انشاء اليات للامتثال والتحقق من تطبيق التشريعات وتطوير الاجراءات القانونية لمكافحة الهجمات السيبرانية .

الفرع الثاني/ دور الوكالات الاوربية للأمن السيبراني (ENISA)

تعمل وكالة الاتحاد الاوربي للأمن السيبراني [27] (متاح على الموقع الالكتروني https;//ar.wikipedia.org)على تعزيز قدرة دول الاتحاد ومنظمات القطاع الخاص بدول الاتحاد على منع وكشف والاستجابة للتهديدات السيبرانية ، كما انها تقوم بتطوير خطط استراتيجية و خطط عمل تنفيذية للوقاية من الهجمات السيبرانية وتأثيراتها على الافراد ، تهدف هذه الخطة الى تحسين قدرة الاتحاد الاوربي على التصدي للتهديدات السيبرانية وحماية الشبكات والمعلومات الحيوية ، وتتضمن الخطة العديد من المبادرات والانشطة التي تشمل تحسين التعاون بين دول الاعضاء وتعزيز الوعي والتدريب في مجال الامن السيبراني وتطوير المعايير الاوربية للأمن السيبراني وتوفير المشورة الفنية في هذا المجال . وتعمل الوكالة الاوربية للأمن السيبراني على تحقيق الاهداف الاستراتيجية في مجال الامن السيبراني من خلال مجموعة من الاجراءات التي يمكن ايجازها بما يأتي :

1- توفير الدعم والمساعدة للمؤسسات والمنظمات لتصدي لتهديدات الهجمات السيبرانية ومنعها والتصدي للحوادث الامنية التي يمكن ان تخلفها هذه الهجمات .

2- تعزيز الوعي الامني وتعزيز الثقافة الامنية في مجال الامن السيبراني في كافة المؤسسات

3- تعزيز التعاون والتنسيق بين الدول الاوربية والمؤسسات والمنظمات المختلفة في كافة مجال الامن السيبراني للوقاية من الهجمات التي يمكن ان تتعرض لها الدول

4- تقييم وتحسين الامن السيبراني في كافة القطاعات الحيوية والحكومية والخدمات الرقمية والاسواق الرقمية ، والذي يؤدي بدوره الى كشف نقاط القوة والضعف في هذه القطاعات والخدمات

5- العمل على تعزيز الشفافية في مجال الامن السيبراني في كافة المؤسسات ، من خلال توفير المعلومات والتوجيهات والنصائح والتحليلات الامنية الشاملة للمؤسسات كافة وخاص منها الخدمية لتلافي تعرضها الى الهجمات السيبرانية

6- توفير الدعم والمساعدة في مجال الامن السيبراني لكافة المواطنين

7- تعزيز القدرة على التعامل مع التهديدات السيبرانية وتهيئة كافة الوسائل لمنع وقوع هذه التهديدات

المطلب الثاني: الاليات التشريعية للمنظمات الدولية لمواجهة اثار السيبرانية على حقوق الانسان

بالإضافة الى الاليات الوقائية الاجرائية التي تقوم بها المنظمات الدولية ، فأن هناك جهودا دورية اخرى تقوم بها منظمات دولية ذات طابع إقليمي[28] (بشير سبهان احمد ، 2023،ص 29)وقد ظهر دور المنظمات الاقليمية في مجال التصدي للتهديدات السيبرانية جلياً من خلال ما قدمته تلك المنظمات من اتفاقيات في هذا المجال ، اذ اجتمع المجلس الاوربي [29] (متاح على الموقع https;//www.eionet.europa.eu)، في العاصمة المجرية بودابست في نوفمبر لعام 2001 للتشاور حول الظواهر الاجرامية المستحدثة وجرائم تقنية المعلومات والاتفاق على بنود لمكافحتها والتصدي للتهديداتها ، وكان ثمرة ذلك ابرام الاتفاقية الاوربية الدولية لمكافحة الاجرام السيبراني ، والتي اصبحت هذه الاتفاقية الاساس القانوني لتصدي للتهديدات السيبرانية ، كما كان لمنظمة جامعة الدول العربية [30] (عماد عمر محمد عبد الكريم ،2018،ص 29) جهودا في هذا المجال وكان ثمرة هذه الجهود اصدار الجامعة للاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010 وبناءً

على ذلك سوف نتناول في هذا المطلب اتفاقية بودابست في فرع خاص بها والاتفاقية العربية في فرع اخر وعلى النحو الاتي :

الفرع الاول / اتفاقية بودبست لمكافحة الجرائم السيبرانية

جاءت هذه الاتفاقية نتيجة محاولات عديدة منذ ثمانينات القرن العشرين حتى ظهرت بشكلها النهائي عام 2001 في بودابست ، وقد جاءت هذه الاتفاقية نتيجة مشاورات طويلة بين الحكومات واجهزة الشرطة وقطاع الكمبيوتر ، تمثل الاتفاقية ركيزة اساسية منذ دخولها حيز النفاذ في الاول من يوليو لعام 2004 على مستوى دول اعضاء مجلس الاتحاد الاوربي [31] (سليمان قطاف ، ببورقين عبد الحليم ،2022،ص 34)،وقد وضعت هذه الاتفاقية قائمة للجرائم التي يجب على الدول المصادقة عليها تجريمها في قوانينها الداخلية ،ولأهمية هذه الاتفاقية فقد وقع عليها ثلاثون دولة بما في ذلك اربعة دول من غير الاعضاء في مجلس اوربا ، وهي كندا واليابان وجنوب افريقيا والولايات المتحدة الامريكية ، حيث ان هذه الاتفاقية مفتوحة للدول الاعضاء في مجلس اوربا وكذلك للدول من خارج المجلس ، وقد انضمت لها العديد من الدول غير اعضاء مجلس أوربا حتى بلغ عدد الدول المنضمة لها في يونيو 2023، تسعة وثمانون دولة . تضمنت الاتفاقية اربعة ابواب ، الباب الاول استخدام المصطلحات ، اذ اوردت المادة الاولى من الاتفاقية التعريفات الاساسية لكل من النظام المعلوماتي ومقدم الخدمات والبيانات والمعلومات والبيانات المتعلقة بالمرور [32] (احمد هلال،2011،ص12)، وتناول الباب الثاني التدابير الواجب اتخاذها على الصعيد الوطني ، وقد انقسمت تلك التدابير الى قسمين تناول القسم الاول القانون الجنائي الموضوعي ، بينما تناول القسم الثاني القانون الاجرائي [33] (المواد 2-13 من اتفاقية الجرائم المعلوماتية) ، وتناول الباب الثالث الولاية القضائية والتعاون الدولي [34] (المواد 23 و 25 و26 من الاتفاقية)، وتناول الباب الرابع الاحكام الختامية .

الفرع الثاني / الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

صدرت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات والموقعة في القاهرة بتاريخ 21 ديسمبر 2010 ، وتعد هذه الاتفاقية من اهم الاتفاقيات العربية في مجال التصدي لتهديدات السيبرانية بهدف منعها وملاحقة مرتكبيها [35] (حاتم بطيخ ،2021،ص 22)، تهدف هذه الاتفاقية الى تعزيز التعاون بين الدول في مجال مكافحة الهجمات السيبرانية لدرء اخطارها حفاظاً على امن الدول العربية ومصالحها وسلامة مجتمعها وافرادها ، كما اقرت الاتفاقية بالتزام كل دولة طرف بتجريم الافعال الواردة في هذه الاتفاقية والتي تضمنها الفصل الثاني والمسمى بالتجريم [36] (عبد العظيم وزير 2009،ص 166).

تتكون هذه الاتفاقية من ثلاثة واربعين مادة الزمت الدول الاطراف بإدخال التعديلات لتجريم جرائم تقنية المعلومات ، ومنها افعال الاختراق ، والاعتراض غير المشروع والاعتداء على سلامة البيانات والاعتداء على حرمة الحياة الخاصة والاعتداء على الملكية الفكرية ، والتزوير والاحتيال واساءة استخدام وسائل تقنية المعلومات والجرائم المتعلقة بالإرهاب وغسيل الاموال والابتزاز والاستخدام غير المشروع لأدوات الائتمان والوثائق الالكترونية [37] (جعفر حاتم القاضي ،لبيب محمد ،2023،ص 50،70)، وشهدت هذه الاتفاقية انعكاساً كبيرا على الجانب التشريعي العربي ، حيث هناك العديد من دول العربية عملت على محاولة التصدي للتهديدات السيبرانية وذلك بأصدار عدد من التشريعات الخاص والتي قامت بالاستناد والبناء على ما ورد بالاتفاقية المذكورة .

الخاتمة

بعد ان انتهينا من دراستنا بات لزاماً علينا ايضاح اهم النتائج التي خلصت اليها الدراسة، وبيان ما يمكن اقتراحه من معالجات لأوجه الخلل والتي يمكن ايجازها بالآتي:

اولاً/ الاستنتاجات

1- تعد السيبرانية اهم متغير معاصر في العلاقات الدولية ، وذلك بفضل التقدم والتطور التكنولوجي والتي احدثت ثورة في كافة مجالات الحياة بما في ذلك الحروب وادواتها والتي اخذت تدار عبر فضاءات افتراضية وشاشات الكترونية .

2- تبين لنا من خلال دراستنا ان هناك اختلاف بين الحرب السيبرانية والارهاب الالكتروني ، فالاخير جريمة جنائية متساوية مع غيرها من الجرائم كالجرائم الالكترونية وجريمة قرصنة المعلومات وجرائم الارهاب ، اما الحرب السيبرانية لا تعد جريمة جنائية ، كما انها لا تقوم الا بين الدول او جماعة ودولة ، وان هناك اختلاف بين الحرب السيبرانية والحرب التقليدية ، اذ تتميز الحرب السيبرانية عن التقليدية في طبيعة السلاح المستخدم فترتب اثار تختلف عن الاثار المترتبة على الحرب التقليدية ، حيث ان الاخيرة تقوم على اساس استخدام الجيوش النظامية وقبل قيامها يكون هناك اعلان للحرب ويوجد ميدان للقتال محدد ، كما تختلف مع الجريمة الالكترونية ، فالجريمة الالكترونية تختلف عن الحرب السيبرانية في الباعث على ارتكابها والهدف من ارتكابها فهي تصدر عن جهة لا تمثل الدولة سواء كانت

شخصاً طبيعيا او معنوياً سعياً وراء هدف اجرامي لأغراض شخصية.

3- للسيبرانية اثار سلبية وايجابية ،اذ تعتبر الاهداف غير البشرية للهجمات من ابرز ايجابيات الحرب السيبرانية ، وبالتالي تقلل من عدد الضحايا ، بينما تعتبر استهداف نظم المواصلات وشبكات الكهرباء والسدود والمستشفيات والمنشآت الكيميائية او النووية من اهم الاثار السلبية التي تثيرها الهجمات السيبرانية وحروب الفضاء الالكتروني، اذ ان البنى التحتية الالكترونية المدنية غالباً ما ترتبط بنظيرتها العسكرية من خلال شبكة الانترنت.

4- تعتمد المنظمات الدولية في استراتيجتها الاستباقية لضمان حماية حقوق الانسان من اثار السيبرانية على ما يعرف بالآليات الوقائية التي تهدف الى الحيلولة دون حدوث التهديدات ، والآليات التشريعية والتي تهدف الى وضع الاطار التشريعي الملائم لأمن الفضاء السيبراني ومكافحة التهديدات السيبرانية حمايتاً لحقوق الافراد من الانتهاكات والحد من وقوعها.

5- ركزت المنظمات الدولية في آلياتها الوقائية على عنصرين
ة أو القابلية للتضرر
الناتجة عن التهديدات ، اما العنصر الثاني فهو الانكشاف والذي يكون موجودا عندما يتعرض الافراد لتطورات يمكن ان تكون ضارة الى جانب نقص الوسائل لمنعها او الحد منها ، وتكمن اهمية ثنائية التهديد والانكشاف من خلال انها تسمح للمنظمات الدولية باختيار الادراكات والتصورات للخطر، بدلا من الحل التكنوقراطية التي تعزز استمرارية الوضع الراهن وتعمق الانكشاف الانساني.

6- تبين لنا انه بالإضافة الى الاليات الوقائية الاجرائية التي تقوم بها المنظمات الدولية ، فأن هناك جهودا دولية اخرى تقوم بها منظمات دولية ، متمثلة بالآليات التشريعية فقد ظهر دور المنظمات الدولية في مجال التصدي للتهديدات السيبرانية جلياً من خلال ما قدمته تلك المنظمات من اتفاقيات في هذا المجال، اذ ان اي اتفاق في المجتمع الدولي يقابله التزام دولي.

التوصيات

1- يجب ان يكون هناك تعاون فعال بين الدول في مجال الوقاية من الهجمات السيبرانية ، وبناءً عليه يجب ان يمون هناك تبادل المعلومات والخبرات والتعاون في مجال التحقيقات الجنائية السيبرانية لمواجهة تهديداتها المشتركة .

2- يجب ان يكون هناك سعي دولي للعمل على اكتمال النموذج الامثل للاطار التشريعي في كافة الدول في ضوء ما تنص عليه الاستراتيجيات الدولية ، وبناء اطار تشريعي ومؤسسي وتنظيمي قادر على حماية الافراد من الهجمات السيبرانية وتحقيق الامن السيبراني ، وذلك من خلال تعزيز التشريعات القائمة بصياغة قوانين وتشريعات فعالة وشاملة تعالج جرائم الامن السيبراني وتحمي الافراد والمؤسسات .

3- حث الاعلام بمختلف اشكاله ، المرئية، والمقروءة والمسموعة والحديثة منها على الانترنت ومواقع التواصل الاجتماعي على تبني حملات توعوية عن الامن السيبراني الوعي بخطورة التهديدات السيبرانية وضرورة التعامل معها كأولوية وبأعلى قدر من الجدية تتناسب مع مختلف الثقافات والتخصصات ومستوى التعليم والمعرفة .

4- دعم الابتكارات والتطوير في مجال الامن السيبراني ، لمواجهة التهديدات المستقبلية مع تطوير تقنيات وادوات جديدة للكشف والوقاية من الجرائم السيبرانية .

الهوامش

(1) لبنى خمبس وتغريد صفاء ، اثر السيبرانية في تطور القوة ، مجلة حمورابي ، مركز حمورابي للدراسات الاستراتيجية ، العدد 33و34 ، ربيع 2020 ، ص 148

(2) عبد الله محمد العصيمي ، السيبرانية واشكال الحروب في المستقبل ، مقال ، صحيفة الجزيرة ، السعودية 2017 ، متاح على الرابط https:llwww.al-jazirah.com

(3) بشلالق ليلى ، تأثيرات الحروب الالكترونية على العلاقات الامريكية الروسية ، رسالة ماجستير ، جامعة محمد بوضياف المسيلة ، الجزائر ، 2018 ، ص 41 .

(4) مهند جبار عباس ، هيثم كريم صيوان ، الحرب السيبرانية بين التحديات واستراتيجيات المواجهة : العراق انموذجاً ، مجلة قضايا سياسية ، العدد 70 ، ص 146

(5) Humairaa Yacoob Bhaiyat and Siphesihle philezwini Sithungu , Academy of Computer Science and Software Engineering , Faculty of Science University of Johannesburg , South Africa , p 536

(6) نايل نبيل عمر ، الحماية الجنائية للمحل الالكتروني في الجرائم المعلوماتية ، مكتب الجامعي الجديد ، 2013 ، ص 13

(7) وليد مهند اسماعيل ، التنظيم القانوني للجريمة الالكترونية ، مجلة العلوم القانونية والسياسية ، المجلد الحادي عشر ، العدد الاول ، السنة السادسة ، 2016، ص172

(8) محمود احمد ، جرائم الحاسوب وابعادها الدولية ، دار الثقافة ، عمان الاردن ، 2005، ص 15 .

(9) ذباب البدائية ، الجرائم الالكترونية المفهوم والاسباب ، ورقة عمل ضمن الملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الدولية ، كلية العلوم الاستراتيجية عمان ، الاردن ، 2014، ص25 .

(10) حسنين بوادي ، الارهاب ، الطبعة الاولى ، مكتبة العبيكان ، الرياض ، المملكة العربية السعودية ، 2006،ص54 .

(11) مايا حسن خاطر ، الاطار القانوني لجرائم الارهاب الالكتروني ، مجلة العلوم الاقتصادية والادارية والقانونية ، المجلد الثاني ، العدد السابع ، المركز القومي للبحوث ، غزة ، 2018، ص58

(12) مايا حسن خاطر ، المرجع نفسه ، ص61 .

(13) حسنين المحمدي بوادي ، غزو العراق بين القانون الدولي والسياسة الدولية ، منشاة المعارف ، الاسكندرية ، 2005، ص10

(14) محمد المجذوب ، القانون الدولي العام ، الطبعة الخامسة ، منشورات الحلبي الحقوقية ، بيروت ، 2004، ص723

(15) عبد الستار حسين الجميلي ، النظام القانوني لنزع اسلحة الدمار الشامل في ضوء القانون الدولي العام ، مجلة كلية القانون للعلوم القانونية والسياسية ، جامعة كركوك ، المجلد الثاني ، العدد الرابع ، العراق ، 2013، ص261

(16) عمر رضا بيومي ، مخاطر اسلحة الدمار الشامل الاسرائيلية على الامن القومي العربي، الطبعة الاولى ، دار النهضة ، 2002، ص25

(17) Mohan B. Gazula M.S ,Computer Science ,Cyber Warfare Conflict Analysis and Case S tudies , Submitted to the Systems Design and Management Program in Partial Fulfillment of the Requirements for the Degree of Master of Science in Engineering and Management ,june 2017, p16.

(18) درويش سعيد ، الحروب السيبرانية واثرها على حقوق الانسان دراسة على ضوء احكام دليل (تالين) ، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية ، العدد الخادي عشر ، ص 190

(19) هند الحناوي ، مبرمجون للحرب : تخيل مستقبل الصراع المسلح ، مجلة حركة الصليب الاحمر والهلال الاحمر الدولي ، العدد 1،2014 ص 10

(20) BY ANDREW KREPINEVICH , CYBER WARFARE;A NUCLEAR OPTION, CENTER FOR STRATEGIC AND BUDGETARY ASSESSMENTS, 2012, P 4

(21) حول هذه المسالة راجع تقرير اللجنة الدولية للصليب الاحمر عن القانون الدولي الانساني وتحديات النزاعات المسلحة المعاصرة ، ورقة مقدمة اثناء المؤتمر الدولي الثاني والثلاثون للصليب الاحمر والهلال الاحمر بعنوان ، قوة الانسانية ، جنيف ، سويسرا ،8-10 ديسمبر 2015 ، وثيقة رقم IC/15XXX/32

(22) Ryan Shandler, Michaeil L. Gross ,and DAPhna Canetti , Cyberattaks, psychological Distress ,and Military Escalation ; An lnternal Meta-Analysis ,University of Oxford ,UKand University of Haifa , jounal of global Studies ,8 (1) 2023,p4l.

(23) درويش سعيد ، الحروب السيبرانية واثرها على حقوق الانسان دراسة على ضوء احكام دليل (تالين) ، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية ، العدد الخادي عشر ، ص 189

(24) محمد احمد لبيب ، هيثم محمد بهاء ، مصطفى احمد كمال، دور الاتفاقيات الدولية والاقليمية في مجال الامن السيبراني وموقف الدولة المصرية منها، مجلة الحوكمة والوقاية من الفساد ومكافحتها، العدد الاول، السنة الاولى ، سبتمبر 2024 ، ص 134

(25) جعفر حاتم القاضي ولبيب محمد ، الاطر الاستراتيجية والقانونية للأمن السيبراني ، الاكاديمية الوطنية لمكافحة الفساد ، 2023 ، ص 93و92

(26) محمد احمد لبيب ، هيثم محمد بهاء ، مصطفى احمد كمال، دور الاتفاقيات الدولية والاقليمية في مجال الامن السيبراني وموقف الدولة المصرية منها، مصدر سابق ، ص 135

(27) هي وكالة تابعة للاتحاد الاوربي يقع مقرها في مدينة اثينا تم انشاءها 2004 ، بموجب لائحة الاتحاد الاوربي رقم 460/2004 تحت اسم الوكالة الاوربية لامن الشبكة والمعلومات ، تعمل بشكل وثيق مع الدول الاعضاء في الاتحاد الاوربي واصحاب المصلحة الاخرين لتقديم المشورة والحلول بالاضافة الى تحسين قدرات الامن السيبراني ، كما انها تدعم وتطوير استجابة تعاونية لحوادث وازمات وتهديدات الامن السيبراني ، منشور على الموقع الالكتروني https://ar.wikipedia.org

(28) تقسم المنظمات الدولية من حيث الرقعة الجغرافية التي تقوم عليها الى منظمات عالمية واقليمية ، فالمنظمات تتصف بالعالمية اذا كانت تشمل جميع دول العالم وتعتبر المنظمة اقليمية اذا كانت تتكون من دول تقوم فوق اقليم معين ، ويقتضي تحقيق الهدف من انشائها اقتصار عضويتها على فئة معينة من الدول ترتبط فيما بينها برابطة خاصة يبرر تعاونها لتحقيق مصالح مشتركة ، بشير سبهان احمد ، الوجيزة لدراسة المنظمات الدولية ، مكتبة القانون المقارن ، الطبعة الاولى ، 2023 ، ص 29.

(29) مجلس الاتحاد الاوربي مؤسسة لها صلاحيات التشريع واتخاذ القرار ، وفي الوقت نفسه يمثل المنتدى الذي يمكن من خلاله لممثلي حكومات الدول الاعضاء التأكد على مصالح دولهم ومحاولة الوصول الى حلول وسط ، مجلس الاتحاد الاوربي ، مقال منشور على الموقع الالكتروني https://www.eionet.europa.eu

(30) منظمة اقليمية تجمع الدول الناطقة باللغة العربية ، وتسعى لتنسيق سياسات الدول العربية ، وتتكون من اثنان وعشرون دولة تتوزع على قارتي اسيا وافريقية ، وينص ميثاقها على التنسيق بين الدول الاعضاء للشؤون الاقتصادية والعلاقات الثقافية والتجارية ، تأسست في 1945 وقد شاركت في تأسيسها ستة دول وهي ، العراق،السعودية، سوريا، مصر، لبنان ، شرق الاردن ، واكب تأسيس الجامعة العديد من الاحداث التي اثرت بشكل في بلورة ملامحها ، واهدافها، وذلك من خلال العديد من المتغيرات العربية والدولية ، عماد عمر محمد عبد الكريم ، دور جامعة الدول العربية في حل القضايا العربية (2011- 2017) ، رسالة ماجستير ، كلية الاداب والعلوم ، قسم العلوم السياسية ، جامعة الشرق الاوسط ، الاردن ، 2018، ص 29

(31) سليمان قطاف وبوبورقين عبد الحليم ، مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية ن كلية الحقوق والعلوم السياسية ، جامعة عمار ثليجى الأغواط ، الجزائر، 2022 ، ص34

(32) احمد هلال ، اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقاً عليها ، دار النهضة العربية ، 2011 ، ص12

(33) تناولت المواد(2-13) من الاتفاقية الجرائم المعلوماتية وتشمل ، جرائم ضد سرية وسلامة واتاحة البيانات والنظم المعلوماتية وهي خمس جرائم ، جريمة النفاذ (الولوج) غير المشروع ن وجريمة الاعتراض غير المشروع وجريمة الاعتداء على سلامة البيانات وجريمة الاعتداء على سلامة النظام واساءة استخدام اجهزة الحاسوب ، والجرائم المتصلة بالحاسوب الالي وهي التزوير المعلوماتي وجريمة الاحتيال المعلوماتي ، والجرائم المتصلة بالمحتوى والجرائم الاعتداء على الملكية الفكرية والحقوق .

(34) تقرر المادة (23) من الاتفاقية الاحكام العامة المتعلقة بالتعاون الدولي ، والمادة (24) شملت تسليم المجرمين ، اما المادة (25) فقد تناولت الاحكام العامة التي تحكم المساعدة القضائية المتبادلة ، والمادة (26) وهي خاصة بالمعلومات التلقائية اي التي تأتي عفواً أو بطريقة عفوية

(35) حاتم بطيخ ، تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات ، دراسة تحليلية مقارنة ، مجلة الدراسات القانونية والاقتصاد ، جامعة السادات ، مجلد الخامس ، العدد (1) اغسطس ، 2021، ص22

(36) عبد العظيم وزير ، شرح قانون العقوبات القسم العام ، الجزء الاول، النظرية العامة للجريمة ، دار النهضة العربية ، 2009 ، ص 166

(37) جعفر حاتم القاضي ، ولبيب محمد ، الاطر الاستراتيجية والقانونية للأمن السيبراني ، الاكاديمية الوطنية لمكافحة الفساد ، 2023 ، ص 50 و70.

المصادر

الكتب

- احمد هلال، 2011 ، اتفاقية بودابست لمكافحة جرائم المعلوماتية معلقاً عليها ، دار النهضة العربية .
- بشير سبهان احمد، 2023، الوجيزة لدراسة المنظمات الدولية ، مكتبة القانون المقارن ، الطبعة الاولى .

- بوادي حسنين، 2006، الارهاب ، الطبعة الاولى ، مكتبة العبيكان ، الرياض ، المملكة العربية السعودية .
- بوادي حسنين المحمدي ، 2005، غزو العراق بين القانون الدولي والسياسة الدولية ، منشاة المعارف ، الاسكندرية .
- حمد المجذوب ، 2004، القانون الدولي العام ، الطبعة الخامسة ، منشورات الحلبي الحقوقية ، بيروت .
- عمر رضا بيومي ،2002، مخاطر اسلحة الدمار الشامل الاسرائيلية على الامن القومي العربي، الطبعة الاولى ، دار النهضة .
- عبد العظيم وزير، 2009 ، شرح قانون العقوبات القسم العام ، الجزء الاول، النظرية العامة للجريمة ، دار النهضة العربية .
- نايل نبيل عمر، 2013 ، الحماية الجنائية للمحل الالكتروني في الجرائم المعلوماتية ، مكتب الجامعي الجديد .
- محمود احمد ، 2005، جرائم الحاسوب وابعادها الدولية ، دار الثقافة ، عمان الاردن .

الرسائل والاطاريح

- بشلالق ليلى، 2018 ، تأثيرات الحروب الالكترونية على العلاقات الامريكية الروسية ، رسالة ماجستير ، جامعة محمد بوضياف المسيلة ، الجزائر .
- سليمان قطاف وبيورقين عبد الحليم ، 2022 ، مواجهة الجرائم السيبرانية في ضوء الاتفاقيات الدولية ، كلية الحقوق والعلوم السياسية ، جامعة عمار ثليجى الأغواط ، الجزائر.
- عماد عمر محمد عبد الكريم، 2018 ، دور جامعة الدول العربية في حل القضايا العربية (2011- 2017) ، رسالة ماجستير ، كلية الاداب والعلوم، قسم العلوم السياسية ، جامعة الشرق الاوسط ، الاردن .

البحوث

- درويش سعيد ، الحروب السيبرانية واثرها على حقوق الانسان دراسة على ضوء احكام دليل (تالين) ، المجلة الجزائرية للعلوم القانونية والاقتصادية والسياسية ، العدد الخادي عشر.
- البدائية ذباب ،2014، الجرائم الالكترونية المفهوم والاسباب ، ورقة عمل ضمن الملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الدولية ، كلية العلوم الاستراتيجية عمان ، الاردن .
- جعفر حاتم القاضي ، 2023 ، ولبيب محمد ، الاطر الاستراتيجية والقانونية للأمن السيبراني ، الاكاديمية الوطنية لمكافحة الفساد .
- جعفر حاتم القاضي ولبيب محمد ، 2023 ، الاطر الاستراتيجية والقانونية للأمن السيبراني ، الاكاديمية الوطنية لمكافحة الفساد .
- حاتم بطيخ ،2021، تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات ، دراسة تحليلية مقارنة ، مجلة الدراسات القانونية والاقتصاد ، جامعة السادات ، مجلد الخامس ، العدد (1) اغسطس .
- الجميلي عبد الستار حسين ، 2013، النظام القانوني لنزع اسلحة الدمار الشامل في ضوء القانون الدولي العام ، مجلة كلية القانون للعلوم القانونية والسياسية ، جامعة كركوك ، المجلد الثاني ، العدد الرابع ، العراق .
- لبنى خمبس وتغريد صفاء ، ربيع 2020، اثر السيبرانية في تطور القوة ، مجلة حمورابي ، مركز حمورابي للدراسات الاستراتيجية ، العدد 33و34 .
- مايا حسن خاطر ، 2018، الاطار القانوني لجرائم الارهاب الالكتروني ، مجلة العلوم الاقتصادية والادارية والقانونية ، المجلد الثاني ، العدد السابع ، المركز القومي للبحوث ، غزة .
- مهند جبار عباس ، هيثم كريم صيوان ، الحرب السيبرانية بين التحديات واستراتيجيات المواجهة : العراق انموذجاً ، مجلة قضايا سياسية ، العدد 70 .
- وليد مهند اسماعيل ، 2016، التنظيم القانوني للجريمة الالكترونية ، مجلة العلوم القانونية والسياسية ، المجلد الحادي عشر ، العدد الاول ، السنة السادسة .
- الحناوي هند ، 2014 ، مبرمجون للحرب : تخيل مستقبل الصراع المسلح ، مجلة حركة الصليب الاحمر والهلال الاحمر الدولي ، العدد .
- محمد احمد لبيب ، هيثم محمد بهاء ، مصطفى احمد كمال، سبتمبر 2024، دور الاتفاقيات الدولية والاقليمية في مجال الامن السيبراني وموقف الدولة المصرية منها، مجلة

الحوكمة والوقاية من الفساد ومكافحتها، العدد الاول، السنة الاولى .

المواقع الالكترونية

- مقال منشور على الموقع الالكتروني https://ar.wikipedia.org
- مجلس الاتحاد الاوربي ، مقال منشور على الموقع الالكتروني https://www.eionet.europa.eu
- عبد الله محمد العصيمي ، 2017 ، السيبرانية واشكال الحروب في المستقبل ، مقال ، صحيفة الجزيرة ، السعودية ، متاح على الرابط https:llwww.al-jazirah.com

المصادر الانجليزية

- Humairaa Yacoob Bhaiyat and Siphesihle philezwini Sithungu , Academy of Computer Science and Software Engineering , Faculty of Science University of Johannesburg , South Africa
- Mohan B. Gazula M.S june 2017,Computer Science ,Cyber Warfare Conflict Analysis and Case S tudies , Submitted to Systems Design and Management Program in Partial Fulfillment of the Requirements for the Degree of Master of Science in Engineering and Management ,
- BY ANDREW KREPINEVICH , 2012 CYBER WARFARE;A NUCLEAR OPTION, CENTER FOR STRATEGIC AND BUDGETARY ASSESSMENTS.
- Ryan Shandler, Michaeil L. Gross ,and DAPhna Canetti , 2023 Cyberattaks, psychological Distress ,and Military Escalation ; An lnternal Meta-Analysis ,University of Oxford ,UKand University of Haifa , jounal of global Studies ,8 t