الحماية القانونية للأمن السيبراني

الدكتور/ وائل محمود فخري غريب *

الملخص:

تناول هذا البحث الحماية القانونية للأمن السيبراني، سواء كانت دولية بموجب الاتفاقيات والمعاهدات الدولية أو كانت وطنية عن طريق التشريعات الداخلية والوطنية مثل التشريع المصري والعماني، ووضع التدابير اللازمة لتقليل المخاطر ومواجهة التحديات، حيث نجد الهجمات السيبرانية ذات الجوانب السلبية، سواء في وقت السلم أو أثناء النزاعات المسلحة والتي تغير نتيجة لها تعريف أساليب ووسائل القتال المعروفة أثناء الحروب التقليدية ومدي شرعية أو عدم شرعية مثل هذه الحروب، والمسؤولية الدولية الناشئة عن تلك الهجمات في ضوء القانون الدولي المعاصر.

يوضح البحث كذلك دور المراكز الوطنية والإقليمية للأمن السيبراني، والجهود المتمثلة على سبيل المثال لا الحصر في الاستراتيجيات الوطنية (الاستراتيجيات الاستباقية في مواجهة الهجمات السيبرانية مثل الردع السيبراني) في مجال صناعة وحماية الأمن السيبراني، وكذلك تشجيع البحث والتطوير والابتكار في مجال الأمن السيبراني في ظل الثورة الرقمية الحديثة التي أفرزت وجود فضاء افتراضي يقوم على أساس بنية عالمية لتكنولوجيا المعلومات والاتصال.

هدف هذا البحث إلى تسليط الضوء على تعريف الأمن السيبراني، ودور التميز والابتكار والذكاء الاصطناعي في صناعته من خلال تطبيق أفضل الممارسات والتجارب في تطوير وصناعة الأمن السيبراني، وكذلك وسائل حمايته، حيث تم استخدام المنهج التحليلي لأحكام المعاهدات والاتفاقيات الدولية في بعض المواضع، وفي مواضع أخري المنهج المقارن بين جمهورية مصر العربية ودول مجلس التعاون الخليجي بوجه عام (وسلطنة عمان بوجه خاص).

ختم البحث بخاتمة وضحت أهم النتائج والتوصيات التي تفيد في حل مشكلة البحث، وتعزيز دور المجتمع الدولي بوجه عام والدولة داخلياً بوجه خاص في حماية وصناعة الأمن السيبراني في ظل أن أغلب الدول تفتقد وجود تشريعات تختص بالفضاء السيبراني وفي حال وجود قوانين، فإنه يوجد ثغرات قانونية في ذات الشأن، يجب العمل على ضرورة ملئ هذا الفراغ وسد الثغرات.

الكلمات المفتاحية: الهجمات السيبرانية – الفضاء الإلكتروني – المسؤولية الدولية – القانون الدولي الإنساني – الذكاء الاصطناعي.

---

* أستاذ القانون الدولي العام المساعد – كلية القانون – الجامعة العربية المفتوحة – سلطنة عمان.

Legal Protection for Cybersecurity

Dr. Wael Mahmoud Fakhry Gharib *

Abstract:

This research discusses the legal protection of cyber security, whether it is international under international conventions and treaties, or it is national through internal and national legislation such as Egyptian and Omani legislation, and puts in place the necessary measures to reduce risks and face challenges, as we find cyber-attacks with negative aspects, whether in peacetime or during armed conflicts. As a result, it changes the definition of known methods and means of fighting during conventional wars, the extent of legality or illegality of such wars, and the international responsibility arising from those attacks in the light of contemporary international law.

The research also explains the role of national and regional centers for cybersecurity, and the efforts represented, for example, but not limited to national strategies (proactive strategies in confronting cyber-attacks such as cyber deterrence) in the field of manufacturing and protecting cybersecurity, as well as encouraging research, development, and innovation in the field of cybersecurity in light of the revolution. Modern digital technology has resulted in the existence of a virtual space based on a global structure of information and communication technology. This research aims to shed light on the definition of cybersecurity, and the role of excellence, innovation, and artificial intelligence in its industry through the application of best practices and experiences in the development and industry of cybersecurity, as well as the means of protecting it, where the analytical approach was used to the provisions of international treaties and agreements in some places, and in other places the approach The comparison between the Arab Republic of Egypt and the Gulf Cooperation Council countries in general (and specially in the Sultanate of Oman).

The research concluded with a conclusion that clarified the most important results and recommendations that are useful in solving the research problem, and strengthening the role of the international community in general and the state internally in particular in protecting and creating cybersecurity in light of the fact that most countries lack the existence of legislation related to cyberspace, and if there are laws, there are legal loopholes in the same In this regard, work must be done to fill this void and fill the gaps.

Keywords: Cyber-attacks - Cyberspace - International Responsibility - International Law - Artificial Intelligence.

---

*Assistant Professor in International Public Law, Faculty of Law, AOU University, Oman.

المقدمـــة

نظراً لما يشهده العالم من ثورة هائلة في نظم المعلومات خاصة بعد جائحة كوفيد-١٩ التي اضطرت العديد من القطاعات إلى الاعتماد على تكنولوجيا المعلومات والاتصالات بشكل أكبر من ذي قبل، كان من الضروري إصدار قوانين تحمي أجهزة الكمبيوتر والهواتف من أي عملية اختراق.

زاد الاهتمام بمكافحة جرائم تقنية المعلومات[١]، أو ما يعرف بالأمن السيبراني[٢] مع زيادة الخسائر الناتجة عن الهجمات السيبرانية (والتي من أهمها: الاختراق العظيم

---

[١] الاستخدام العلمي للحوسبة والإلكترونيات والاتصالات لمعالجة وتوزيع البيانات والمعلومات بصيغها المختلفة، مرسوم سلطاني رقم ٢٠١١/١٢ بإصدار قانون مكافحة جرائم تقنية المعلومات.

[٢] السيبراني هي كلمة معربة للمصطلح الإنجليزي Cyber، ويعود في الأصل إلي الكلمة اليونانية "Kybernetes" بمعني الشخص الذي يدير دفة السفينة، وعرف الأمن السيبراني بتعريفات عديدة منها "أمن الشبكات والأنظمة المعلوماتية والبيانات والمعلومات والأجهزة المتصلة بالإنترنت، الذي يتعلق بإجراءات ومعايير الحماية المفروض اتخاذها، أو الالتزام بها، لمواجهة التهديدات، ومنع التعديات، أو للحد من أثارها " د. خالد المطيري: دور التشريعات الجزائية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي، مجلة البحوث الفقهية والقانونية، العدد ٣٨، يوليو ٢٠٢٢م، ص٩٩٤ وما بعدها، وتحدثت عنه وكالة الأمن السيبراني التابعة للاتحاد الأوربي بأنه من حيث المبدأ لا داعي للتعريفات التقليدية، فمصطلح الأمن السيبراني متجدد وفقاً للتغيرات التكنولوجية المستمرة حيث يجب دائما تغطية التعريف لكافة تلك المستحدثات، وعرفته وزارة الدفاع الأمريكية بأنه "منع الضرر والحماية والاستعادة لأجهزة الكمبيوتر وأنظمة الاتصالات الإلكترونية وخدمات الاتصالات الإلكترونية والاتصالات السلكية والإلكترونية، بما في ذلك المعلومات الواردة فيها، لضمان توفرها وسلامتها". والتعريف الأنسب من وجهة نظر الباحث هو: "جميع الأنشطة اللازمة لحماية الفضاء السيبراني ومستخدميه والأشخاص المتضررين من التهديدات السيبرانية"، راجع:

- The European Union Agency for Network and Information Security (ENISA): Definition of Cybersecurity - Gaps and overlaps in standardisation, V1.0, DECEMBER, 2015.
- Department of Defense. Instruction No.8500.01. Cybersecurity. 2014. United States of America.
- Paulo Shakarian and others, Introduction to Cyber-warfare A Multidisciplinary Approach, (USA: Syngress, Elsevier, 2013, p. 2).

The Great Hack – فضيحة تسريب بيانات ملايين من المواطنين الأمريكيين من خلال تطبيقات التواصل الاجتماعي والتأثير علي الرأي العام الأمريكي– اختراق مركز التحكم الرئيسي بكييف"أوكرانيا"– فضيحة Crypto Ag– اختراق وزارة الصحة البريطانية National Health Service[٣] –الهجوم في استونيا ٢٠٠٧– هجوم Stuxnet عام ٢٠١٠م هذا البرنامج قد صمم من بواسطة إسرائيل والولايات المتحدة خصيصا لمهاجمة البرنامج النووي الإيراني[٤]، وما يعنيه ذلك من تهديدات على الأمن القومي للدول، وبالتبعية على السلم والأمن الدوليين، وقد انتشرت القوة السيبرانية على الساحة الدولية ومنحت فاعلين أصغر قدرة ودور مهم عبر الفضاء السيبراني؛ مما يعني تغير في مقدرات القوى بالنظام الدولي، فتحتل الهجمات السيبرانية مكان الصدارة علي جداول الأعمال في جميع أنحاء العالم، حيث أنها تتحول إلى جزء من النزاعات المسلحة اليوم، ويمكنها أن تعطل عمل البنية التحتية بالغة الأهمية والخدمات الحيوية للسكان المدنيين، حيث يهدف الأمن السيبراني لتعزيز قدرة الدول على مقاومة التهديدات الكامنة

- Richard A. Clarke and Robert Knake, Cyber War: The Next Threat to National Security and What to Do About It, (New York: Harper Collins, 2010), p. 6.

- عبد الله يحي الزهراني: استراتيجيات الأمن السيبراني في ضوء التقنيات والتحديات الحديثة، دراسة مقارنة، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، كلية العلوم الإستراتيجية، السعودية، ٢٠٢٠، ص١١ وما بعدها.

[٣] من أمثلة تلك الهجمات: الدخول أو الاعتراض غير المشروع لخط سير البيانات بأي من الوسائل الفنية وقطع البث أو استقبال بيانات تقنية المعلومات، الاعتداء علي سلامة وسرية وفحوى المعلومات، تدمير أو محو أو إعاقة أو تعديل أو حجب بيانات قصداً بدون وجه حق، إساءة استخدام وسائل تقنية المعلومات، إنتاج أو بيع أو استيراد أو توزيع أو توفير أو حيازة أية أدوات أو برامج مخصصة لغاية ارتكاب جرائم تقنية أو شق كلمات سر أو شيفرة دخول، التزوير، ..إلخ، جامعة الدول العربية "المنظمة العربية لتكنولوجيا الاتصال والمعلومات"، الرؤية العربية للأمن السيبراني (الواقع– التحديات– الفرص)، تونس، ٢٠٢١م، ص ١٥ وما بعدها.

[٤] رزق سمودي: حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام، مجلة جامعة الشارقة، مجلد ١٥ العدد ٢، ديسمبر ٢٠١٨م، ص٣٣٧ وما بعدها.

في الفضاء السيبراني، ولتحقيق ذلك لابد من تشجيع البحث والتطوير والابتكار في مجال الأمن السيبراني، وفيما يلي نتناول:

هدف البحث:

تسليط الضوء على تعريف الأمن السيبراني وتعزيز التعاون وتدعيمه بين الدول في مجال مكافحة جرائم تقنية المعلومات، وإبراز دور التميز والابتكار والذكاء الاصطناعي في صناعته من خلال تطبيق أفضل الممارسات والتجارب في تطوير وصناعة الأمن السيبراني، وكذلك وسائل حمايته.

منهج البحث:

تم استخدام المنهج التحليلي لأحكام المعاهدات والاتفاقيات الدولية في بعض المواضع، وفي مواضع أخري المنهج المقارن بين جمهورية مصر العربية ودول مجلس التعاون الخليجي بوجه عام (وسلطنة عمان بوجه خاص).

مشكلة البحث:

تتمثل مشكلة البحث في حداثة موضوعه، وصعوبة تأصيل أساسه الفقهي والنظامي، في ظل محاولة الدول تحقيق هذا النوع من الأمن، عن طريق تشجيع البحث والابتكار، وكذلك محاولة الوقوف على مدى فعالية الجهات الدولية والمراكز الوطنية في مجال الأمن السيبراني ومدي كفاية آلياتها وممارساتها في الوصول للأمل المنشود المتمثل في ضمان تحقيقه.

تساؤلات البحث:

ما هي الجهات الدولية والمراكز الوطنية الفاعلة في مجال الأمن السيبراني؟

ما هي التدابير اللازمة لمواجهة الهجمات السيبرانية؟

ما هو تأثير الأمن السيبراني على هيكل النظام الدولي والداخلي؟

ما هي دور البحث والتطوير والابتكار في مجال الأمن السيبراني؟

خطة البحث:

اشتمل هذا البحث على مقدمة ومطلبين وخاتمة، أما المطلب الأول فهو الحماية القانونية للأمن السيبراني، ويتضمن الحماية الدولية والوطنية للأمن السيبراني، وكذلك

التدابير اللازمة لتقليل المخاطر ومواجهة التحديات، ويليه لمطلب الثاني عن دور المراكز الوطنية والإقليمية للأمن السيبراني، من خلال استعراض الاستراتيجيات الوطنية الاستباقية في مواجهة الهجمات السيبرانية، وتشجيع البحث والتطوير والابتكار في مجال الأمن السيبراني، وفي نهاية البحث خاتمة تشتمل على أهم النتائج والتوصيات.

المطلب الأول

الحماية القانونية للأمن السيبراني

يعتقد البعض أن الأمن لا يخرج عن نطاق مفهومه التقليدي المعروف لدي الكثيرين، إلا أن الدائرة اتسعت مؤخراً لتشمل أنواعاً كثيرة ومهمة من الأمن يأتي في مقدمتها الأمن السيبراني الذي يعني حماية المعلومات الموجودة على أجهزة وشبكات الحاسب الآلي، في مواجهة أي تدخل غير مصرح به، ومن هنا تأتي الحماية القانونية والتي تتضمن الحماية الدولية والوطنية للأمن السيبراني، بالإضافة إلى مجموعة من التدابير اللازمة لتقليل المخاطر ومواجهة التحديات، وذلك على النحو الآتي:

الفرع الأول

الحماية الدولية والوطنية للأمن السيبراني

أثر الأمن السيبراني على شكل النظام العالمي الجديد الذي أخذ في التبلور والتغير، ومن هنا جاء اهتمام دول العالم بقضايا الأمن السيبراني، وما يصاحبه من آليات وتقنيات حديثة على تغير بنية النظام الدولي، وذلك من خلال عقد بعض المعاهدات والاتفاقيات واستصدار بعض القرارات، نستعرض بعض منها على سبيل المثال لا الحصر:

أولاً– الاتفاقيات والمعاهدات:

اتفاقية المجلس الأوروبي بشأن جرائم الإنترنت (اتفاقية بودابست): اعتمد المجلس الأوروبي الطابع الدولي لجرائم الكمبيوتر منذ العام ١٩٧٦م، وفي العام ١٩٩٦م،

أنشأت اللجنة الأوروبية لمشاكل الجريمة (CDPC) لجنة خبراء للتعامل مع مشكلة الجريمة السيبرانية، عملت اللجنة بين العامين ١٩٩٧م و٢٠٠٠م على مشروع الاتفاقية التي اعتمدها البرلمان الأوروبي في الجزء الثاني من جلسته العامة في شهر أبريل ٢٠٠١م، وتم التصديق على الاتفاقية من قبل ٣٠ دولة بحلول العام ٢٠١٠م، وتعد المعاهدة الدولية الأولى الوثيقة الدولية الملزمة وتعمل كإطار عمل للتعاون الدولي بين الدول الأطراف في هذه المعاهدة لمعالجة الجرائم المتعلقة بالكمبيوتر والإنترنت عبر التنسيق بين القوانين الوطنية وقوانين الدول الأخرى، البروتوكول الإضافي بشأن تجريم الأفعال المرتبطة بالتمييز العنصري وكراهية الأجانب التي ترتكب عن طريق أنظمة الكمبيوتر ٢٠٠٣م:

- هدف إلى مواءمة القانون الجنائي الموضوعي لمكافحة العنصرية وكراهية الأجانب على شبكة الانترنت، وكذلك تحسين التعاون الدولي في هذا المجال، ويساعد هذا النوع من المواءمة في تخفيف عبئ مكافحة هذه الجرائم على الصعيدين الوطني والدولي[٥].

- اتفاقية الاتحاد الإفريقي حول الأمن السيبراني وحماية المعطيات ذات الطابع الشخصي لسنة ٢٠١٤م: تم إبرامها على عدة مراحل من إطلاق المشروع وصياغة الاتفاقية الأولية إلى اعتمادها وفتح باب التوقيع عليها، وقد بيّنت ديباجة اتفاقية مالابو أهدافها، أما عن محتواها فقد تكونت هذه الأخيرة من (٣٨) مادة موزعة على أربعة فصول. وقد تضمنت اتفاقية مالابو كأي عمل بشري إيجابيات وسلبيات عدة، إلا أنه لا يمكن تقييمها إلا بعد استقراء المناخ الذي أبرمت فيه، والذي يطرح أمامها عدة تحديات أهمها: تضاعف معدلات الجريمة الإلكترونية بأشكالها في القارة الإفريقية، وإشكالية عدم دخولها حيز النفاذ بعد سبع سنوات من اعتمادها[٦]، اتفاقية حماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية وبروتوكولها التعديلي ٢٠١٨م: وضعت

---

[٥] مجلس أوربا سلسلة المعاهدات الأوربية رقم ١٨٩.

[6] African Union Convention on Cyber Security and Personal Data Protection, Malabo, 27th June 2014.

هذه الاتفاقية القواعد المتعلقة بحماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية والقواعد المتعلقة بحرية نقل البيانات الشخصية، فهي تحمي الحقوق والحريات الأساسية للأشخاص الطبيعيين ولا سيما حقهم في حماية البيانات الشخصية، فلا يجوز تقييد أو حظر حرية نقل البيانات الشخصية داخل الاتحاد لأسباب تتعلق بحماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية[٧]، البروتوكول الإضافي الثاني لاتفاقية الجريمة الإلكترونية بشأن تعزيز التعاون والكشف عن الأدلة الإلكترونية ٢٠٢٢م: يحتوي البروتوكول الإضافي الثاني على أحكام تتعلق ببيانات تسجيل اسم النطاق، حيث هدف البروتوكول إلى تعزيز التعاون المباشر مع مقدمي الخدمات وغيرهم، وكذلك تعزيز التعاون بين السلطات للكشف عن بيانات الكمبيوتر المخزنة من خلال الكشف السريع في حالة الطوارئ والمساعدات المتبادلة[٨].

ثانياً- قرارات المحاكم الدولية:

قضت المحكمة الأوروبية لحقوق الإنسان بأن بيانات الهاتف ورسائل البريد الإلكتروني واستخدام الإنترنت[٩]، والبيانات المخزنة على خوادم الكمبيوتر[١٠]، ويمكن أن يؤدي مجرد تخزين البيانات الشخصية إلى الاعتداء علي حق المستخدم في الخصوصية، يتمثل في جمع البيانات وطريقة جمعها ومعالجتها واستخدامها ونتائج هذه المعالجة[١١]، وعلاوة على ذلك، البيانات التي تم جمعها ونقلها عبر التقنيات

---

[٧] اللائحة العامة لحماية البيانات في الاتحاد الأوروبي (GDPR) في ٢٥ مايو ٢٠١٨م.

[٨] سلسة معاهدات مجلس أوربا، ٢٠٢٢م.

[٩] حكم المحكمة الأوروبية لحقوق الإنسان بأن بيانات الهاتف ورسائل البريد الإلكتروني واستخدام الإنترنت، (كوبلاند ضد المملكة المتحدة، ٢٠٠٧، الصفحتان ٤١ و٤٢).

[١٠] حكم المحكمة الأوروبية لحقوق الإنسان" Wieser and Bicos Beteiligungen GmbH " ضد النمسا، الفقرة ٤٥.

[١١] انظر حكم المحكمة الأوروبية لحقوق الإنسان (س) و (ماربر) ضد المملكة المتحدة في القضيّة عدد ٠٤/٣٠٥٦٢ عام ٢٠٠٨، في اعتبارها أن جمع بيانات الحمض النووي في إطار النظام الوطني المُتكامل لإدارة الهويّة يُشكّل انتهاكا للحق في الخصوصية كما اعدت أن الحاجة إلى جمع بيانات

الرقمية الجديدة والإنترنت مشمولة بالمادة (١١) من الاتفاقية الأمريكية لحقوق الإنسان لعام ١٩٦٩[١٢]، وتشمل حماية البيانات إنشاء المعلومات الشخصية وجمعها وتخزينها وتحليلها واستخدامها ومشاركتها. وتغطي حماية البيانات إنشاء وجمع البيانات الشخصية لأن "الحق في الخصوصية لا يتأثر فقط بفحص أو استخدام المعلومات المتعلقة بشخص ما بواسطة إنسان أو خوارزمية مجرد توليد وجمع البيانات المتعلقة بهوية الشخص أو أسرته أو حياته[١٣].

ثالثاً- قرارات المنظمات الدولية:

تعمل الأمم المتحدة جاهدة علي تأمين سلامة استخدام التكنولوجيا وشبكات المعلوماتية (الإنترنت)، حيث تشارك أجهزة الأمم المتحدة المختلفة في مختلف المفاوضات لإيجاد توافق في الآراء بشأن عدد من القضايا، بما في ذلك وضع معايير توفير الحماية لشبكات الإنترنت[١٤]، وفي إطار جهود الأجهزة الدولية يوفّر الاتحاد

نظام تحديد المواقع العالمي ليست واضحة خاصة بالنظر إلى المخاطر التي تُهدّد الخصوصية التي يُشكّلها جمع البيانات.

[١٢] حكم محكمة البلدان الأمريكية لحقوق الإنسان في قضية تريستان دونوسو ضد بنما وإيشر وآخرون ضد البرازيل (٢٠٠٩)، أقرّت محكمة البلدان الأمريكية لحقوق الإنسان أنّ البرازيل انتهكت المادّة (١٣) من الاتفاقية الأمريكية لحقوق الإنسان (الحق في الحصول على معلومات) بفشلها الكشف عن معلومات تتعلق باختفاء اعضاء من حركة أراغويا غيريا لأقاربهم، أكدت المحكمة أن الحق في المعلومات أقوى عندما يتعلق الأمر بضحايا انتهاكات حقوق الإنسان، بما في ذلك حالات اختفاء الأفراد. وهكذا، رأت المحكمة أن على البرازيل واجب توفير المعلومات لأقارب المختفين وذلك فيما يتعلق بمواقع دفنهم. كما منحت تعويضات قدرها ٤٥٠٠٠ دولار لكل قريب مباشر و١٥٠٠٠ دولار لكل قريب غير مباشر لعضو اختفى من حركة أراغوايا غيريا.

[١٣] حكم المحكمة الأوربية لحقوق الإنسان:

CASE OF ROTARU v. ROMANIA, (Application no. 28341/95).

[١٤] قامت منظمة الأمم المتحدة بتنسيق جهودها بما في ذلك تبسيط البرامج والأنشطة المتعلقة بالأمن السيبراني لكي تكون أكثر فعالية، حيث تعمل وفقاً للمؤشرات التي توفرها عضويتها المعنية على بناء تفاهم مشترك داخل الأمم المتحدة بشأن الاحتياجات والمتطلبات اللازمة لوضع البرامج والمبادرات

الدولي للاتصالات[١٥] الذي يضم ١٩٢ دولة، و٧٠٠ شركة من القطاع الخاص والمؤسسات الأكاديمية منبرًا «استراتيجياً» للتعاون بين أعضائه باعتباره، وكالة متخصصة داخل الأمم المتحدة، حيث يعمل الاتحاد على مساعدة الحكومات في الاتفاق على مبادئ مشتركة تفيد الحكومات والصناعات التي تعتمد على تكنولوجيا المعلومات والبنية التحتية للاتصالات، وقد وضع الاتحاد الدولي للاتصالات مخططًا لتعزيز الأمن السيبراني العالمي، أما أبرز قرارات تلك الأجهزة فتتمحور حول منع الجرائم المتصلة بأجهزة الكمبيوتر ومكافحتها[١٦]، ودراسة طرق التعامل مع التطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي[١٧]، ومكافحة استخدام نظم المعلومات الإدارية الجنائية لتقنية المعلومات». يدعو هذا القرار الدول الأعضاء، عند وضع التشريعات الوطنية لمكافحة إساءة استعمال تكنولوجيا المعلومات، على أن تأخذ

التي من شأنها أن تدعم بفعالية الجهود التي تبذلها الحكومات ودوائر الصناعة وجميع أصحاب المصلحة الآخرين المعنيين، واتُخذت خطوة أولى مهمة في عام ٢٠١٠ نحو تعزيز التنسيق الداخلي بين وكالات الأمم المتحدة في مساعدتها للدول الأعضاء فيما يتعلق بالأمن السيبراني. وقاد الاتحاد ومكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC)، بالتعاون مع 33 وكالة أخرى تابعة للأمم المتحدة، جهداً لمدة سنتين لوضع إطار لمنظومة الأمم المتحدة ككل بشأن الأمن السيبراني والجريمة السيبرانية، صدق عليه مجلس الرؤساء التنفيذيين (CEB) في نوفمبر ٢٠١٣، الاتحاد الدولي للاتصالات: الوثيقة C20/65-A.

[١٥] الاتحاد الدولي للاتصالات على الرابط:

https://www.itu.int/ar/about/Pages/default.aspx (2/7/2023)

[١٦] قرار الجمعية العامة رقم ١٢١/٤٥ عام ١٩٩٠.

[١٧] قرارات الجمعية العامة للأمم المتحدة: ٧٠/٥٣ في ٤ ديسمبر ١٩٩٨، و٤٩/٥٤ في ١ ديسمبر ١٩٩٩، ٢٨/٥٥ في ٢٠ نوفمبر ٢٠٠٠، و١٩/٥٦ في ٢٩ نوفمبر ٢٠٠١ و٥٣/٥٧ في ٢٢ نوفمبر ٢٠٠٢ و٣٢/٥٨ في ١٨ديسمبر ٢٠٠٣.

بالاعتبار عمل لجنة منع الجريمة والعدالة الجنائية [١٨]، وإنشاء ثقافة عالمية للأمن السيبراني[١٩].

ومن ناحية أخرى، هناك العديد من القرارات الصادرة عن منظمة الأمم المتحدة في مجموعة من المجالات ذات الصلة بأمن الفضاء الإلكتروني مثل: المنع الفعال للجريمة والعدالة الجنائية لمكافحة الاستغلال الجنسي للأطفال[٢٠]، والتعاون الدولي من أجل منع وتحري ومقاضاة ومعاقبة جرائم الاحتيال الاقتصادي والجرائم المتصلة بالهوية[٢١]، والتعاون الدولي لمنع التحقيق والمقاضاة والمعاقبة على الاحتيال، وإساءة استعمال الهوية وتزييفها والجرائم ذات الصلة[٢٢]، وتنفيذ إعلان فيينا بشأن الجريمة والعدالة: مواجهة تحديات القرن الحادي والعشرين[٢٣]، وتعزيز أوجه التآزر والتعاون: التحالفات الاستراتيجية في مجال منع الجريمة وتحقيق العدالة الجنائية[٢٤].

تعمل الأمم المتحدة كذلك لاتخاذ التدابير كافة لمكافحة الجريمة المتصلة بأجهزة الكمبيوتر[٢٥]، وتعزيز التعاون الدولي من أجل منع استخدام شبكة الإنترنت لارتكاب

---

[١٨] قرارات الجمعية العامة للأمم المتحدة: ٦٣/٥٥ في ٤ ديسمبر ٢٠٠٠، و١٢١/٥٦ في ١٩ ديسمبر ٢٠٠١.

[١٩] قرارات الجمعية العامة للأمم المتحدة ٢٣٩/٥٧ في ٢٠ ديسمبر ٢٠٠٢ و١٩٩/٥٨ في ٣٠ يناير ٢٠٠٤ بشأن «إنشاء ثقافة عالمية للأمن السيبراني».

[٢٠] قرار الجمعية العامة CCPCJ 16/2/2007 من أبريل ٢٠٠٧» (الفقرات ٧، ١٦).

[٢١] قرار المجلس الاقتصادي والاجتماعي E/2007/20 بتاريخ ٢٦ يوليو ٢٠٠٧ "» (E/2007/30 و E/2007/SR.45)

[٢٢] قرار المجلس الاقتصادي والاجتماعي ٢٦/٢٠٠٤ بتاريخ ٢١ يوليو ٢٠٠٤.

[٢٣] قرار الجمعية العامة ٥٩/٥٥ في ٤ ديسمبر ٢٠٠٠ والفقرة ٣٦ المرفقة بقرار الجمعية العامة ٢٦١/٥٦ المؤرخ ٣١ يناير ٢٠٠٢.

[٢٤] قرار الجمعية العامة ١٧٧/٦٠ بتاريخ ١٦ ديسمبر ٢٠٠٥.

[٢٥] قرار الجمعية العامة ١٧٧/٦٠ الفقرة ٢ التي دعت الحكومات لتنفيذ جميع التوصيات التي اعتمدها المؤتمر الحادي عشر.

الجرائم المتصلة بالمخدرات [٢٦]، ومكافحة بيع المخدرات المشروعة الخاضعة للمراقبة الدولية إلى الأفراد عن طريق الإنترنت [٢٧].

رابعاً– التشريعات الداخلية والوطنية مثل التشريع المصري والعماني:

تمتد الحماية القانونية للأمن السيبراني لتشمل بجانب الحماية المقررة على الصعيد الدولي الحماية القانونية على الصعيد الداخلي أو الوطني من خلال القوانين الداخلية، وفيما يلي نتناول كلاً من التشريع المصري وتشريع سلطنة عمان على النحو الآتي:

١– القانون المصري:

اهتمت الدولة المصرية بتعزيز الأمن السيبراني عن طريق امتلاك بنية تحتية رقمية فائقة التطور ووسائل متقدمة للتصدي للهجمات الإلكترونية الخبيثة التي تستهدفها[٢٨]، وأصبح لديها معاييرها الوطنية للأمن السيبراني تحقق من خلالها أهدافها الاستراتيجية في حماية وتأمين مكتسباتها وإنجازاتها في مختلف القطاعات والمجالات بتوفير الحماية القانونية للأمن السيبراني عن طريق قوانين وقرارات وزارية أهمها إنشاء

---

[٢٦] قرار الجمعية العامة ١٧٨/٦٠ فقرة ١٧.

[٢٧] قرار المجلس الاقتصادي والاجتماعي ٤٢/٢٠٠٤.

[٢٨] تم تشكيل المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات (EG-CERT) بالجهاز القومي لتنظيم الاتصالات في أبريل ٢٠٠٩ ويقدم المركز الدعم اللازم لحماية البنية التحتية القومية للمعلومات المهمة خاصة في قطاع تكنولوجيا المعلومات والاتصالات والقطاع المالي، ويتمثل الهدف الرئيسي للمركز في تعزيز أمن البنية التحتية المصرية للاتصالات والمعلومات من خلال اتخاذ إجراءات استباقية، وجمع وتحليل المعلومات الخاصة بالحوادث الأمنية، والتنسيق والوساطة بين الأطراف المعنية في حل تلك الحوادث الأمنية والتعاون الدولي مع غيرها من فرق الاستجابة لطوارئ الحاسبات والشبكات في الدول الأخرى، الموقع الرسمي للجهاز القومي لتنظيم الاتصالات علي الرابط:

https://www.tra.gov.eg/ar(28/6/2023).

المجلس الأعلى للأمن السيبراني[٢٩]، والذي تم تحديد اختصاصاته وتنظيم عمله[٣٠]، وضمت ممثل عن هيئة الرقابة الإدارية إلى عضوية المجلس الأعلى للأمن السيبراني[٣١]، وممثل لوزارتي المالية والتخطيط والمتابعة والإصلاح الإداري[٣٢]، وكذلك ضم ممثل لمركز المعلومات ودعم اتخاذ القرار بمجلس الوزراء[٣٣]، مع إلزام كافة الجهات الحكومية بتنفيذ توصيات المجلس الأعلى للأمن السيبراني لمواجهة أخطار الهجمات السيبرانية[٣٤].

سعت الدولة المصرية لتحقيق الحماية القانونية للأمن السيبراني عن طريق قانون مكافحة جرائم تقنية المعلومات[٣٥]، وقانون حماية البيانات الشخصية والذي موضوعه حماية البيانات الشخصية المعالجة إلكترونياً جزئياً أو كلياً لدى أي حائز أو متحكم أو معالج لها، وذلك بالنسبة إلى الأشخاص الطبيعيين[٣٦]، مما اسهم في رفع تصنيف مصر وتبؤها مكانة عالية حيث تحتل المرتبة السابعة والعشرين من بين ١٩٣ دولة وفقا لما ذُكر في تقرير أصدره الاتحاد الدولي للاتصالات (ABI)العالمي للأمن السيبراني وُنشر في ديسمبر ٢٠١٤م، وما جاء في مؤشر الأمن السيبراني (GCI) الصادر عن الاتحاد الدولي للاتصالات أعلن عن حصول مصر خلال ٢٠٢٠ على المركز ٢٣ الـ عالميا بين ١٨٢ دولة بـ ٩٥,٤٥ درجة، موضحاً عن أن مصر اتخذت خطوات مهمة لدعم الأمن السيبراني من أهمها: تأسيس مجلس أعلى

---

[٢٩] قرار رئيس مجلس الوزراء رقم ٢٢٥٩ لسنة ٢٠١٤.

[٣٠] قرار رئيس مجلس الوزراء رقم ١٦٣٠ لسنة ٢٠١٦.

[٣١] قرار رئيس مجلس الوزراء رقم ١٤٤٧ لسنة ٢٠١٥.

[٣٢] قرار رئيس مجلس الوزراء رقم ٨١ لسنة ٢٠١٥.

[٣٣] قرار رئيس مجلس الوزراء رقم ٢٣٢٨ لسنة ٢٠١٤.

[٣٤] قرار رئيس مجلس الوزراء رقم ٩٩٤ لسنة ٢٠١٧.

[٣٥] قانون رقم ١٧٥ لسنة ٢٠١٨.

[٣٦] قانون رقم ١٥١ لسنة ٢٠٢٠.

للأمن السيبرانى في عام ٢٠١٥ ووضع استراتيجية وطنية للأمن السيبراني ٢٠١٧-٢٠٢١، إلى جانب تأسيس المركز الوطني للاستعداد لطوارئ الحاسبات والشركات EG-CERT، كما جاءت مصر في المرتبة الأولى عالميًا في تنافسية قطاعي الإنترنت والهاتف خلال ٢٠٢١ وفقًا لمؤشر المعرفة العالمي[٣٧].

٢- القانون العماني:

حرصت سلطنة عمان علي مواكبة التقدم الإلكتروني في شتي مجالات الحياة من جانب ومن جانب آخر يعد الأمن السيبراني أولوية وطنية لسلطنة عمان حيث أصدرت قوانين تتعلق بالأمن السيبراني فقد نظمت العديد من المسائل القانونية ذات الصلة مثل الاتصالات[٣٨]، ومكافحة الإرهاب[٣٩] وغسل الأموال[٤٠]، وتنظيم وحماية المعاملات الإلكترونية بهدف تسهيل التعاملات الإلكترونية، وتعزيز ثقة الأوساط التجارية والمجتمع في استخدام التعاملات الإلكترونية، وحماية خصوصية الأفراد المستخدمين للتعاملات الإلكترونية[٤١]، وأيضاً قيامها بإنشاء هيئة تقنية المعلومات لضمان الحقوق القانونية للمتعاملين عند استخدام تقنية المعلومات والاتصالات لإجراء مختلف الاتصالات الرسمية والشخصية ولإنجاز المعاملات، ولتوفير مستوى عالٍ من الثقة لدى الأفراد وقطاع الأعمال والوحدات الحكومية في عملية إنجاز المعاملات إلكترونيًا[٤٢].

---

[٣٧] الاتحاد الدولي للاتصالات التابع للأمم المتحدة يصدر المؤشر العالمي للأمن السيبرانى بشكل دوري كل عامين، ويعتمد المؤشر في ترتيب الدول من ١٠٠ درجة على ٥ معايير منها السياسات التنظيمية والتشريعات والإطار المؤسسي وبناء القدرات البشرية وتوافر القدرات التقنية والفنية اللازمة. ITU: Global Cybersecurity Index 2020.

[٣٨] قانون تنظيم الاتصالات الصادر بالمرسوم السلطاني رقم ٢٠٠٢/٣٠.

[٣٩] قانون مكافحة الإرهاب الصادر بالمرسوم السلطاني رقم ٢٠٠٧/٨.

[٤٠] قانون مكافحة غسل الأموال وتمويل الإرهاب الصادر بالمرسوم السلطاني رقم ٢٠١٠/٧٩.

[٤١] قانون المعاملات الإلكترونية الصادر بالمرسوم السلطاني رقم ٢٠٠٨/٦٩.

[٤٢] المرسوم السلطاني رقم ٢٠٠٦/٥٢ بإنشاء هيئة تقنية المعلومات.

اعتمدت سلطنة عمان على الاتفاقيات الدولية والصكوك العالمية [٤٣] واستفادت من كافة التجارب والممارسات العالمية والإقليمية مثل اتفاقية مكافحة الجرائم المعلوماتية "اتفاقية بودابست"، حيث عملت على مكافحة جرائم تقنية المعلومات وتجريم التعدي علي سلامة وسرية وتوفر البيانات والمعلومات الإلكترونية والنظم المعلوماتية، ومكافحة إساءة استخدام وسائل تقنية المعلومات والتزوير والاحتيال المعلوماتي والتعدي على البطاقات المالية وتجريم مثل هذه التعديات [٤٤]، ثم جاء قانون حماية البيانات الشخصية ٢٠٢٢[٤٥].

حرصت كذلك وزارة التقنية والاتصالات على إصدار تعاميم للحفاظ على أمن قواعد البيانات لوحدات الجهاز الإداري للدولة بهدف التأكيد على التزام وحدات الجهاز الإداري في الدولة بالمعايير الأساسية لأمن قواعد البيانات وضرورة توفير الحماية اللازمة لقواعد البيانات لتفادي تعرضها إلى خطر التسريب أو التغيير الغير مصرح به أو أن يتم الاطلاع عليها من قبل الأشخاص الغير مصرح لهم [٤٦].

---

[٤٣] مرسوم سلطاني رقم ٢٠٢١/٧٦ بالموافقة على انضمام سلطنة عمان إلى معاهدة المبادئ المنظمة لأنشطة الدول في ميدان استكشاف واستخدام الفضاء الخارجي، بما في ذلك القمر والأجرام السماوية الأخرى– لمرسوم سلطاني رقم ٢٠٢١/٧٧ بالموافقة على انضمام سلطنة عمان إلى اتفاقية تسجيل الأجسام المطلقة في الفضاء الخارجي– المرسوم السلطاني رقم ٢٠٢١/٧٨ بالموافقة على انضمام سلطنة عمان إلى اتفاقية إنقاذ الملاحين الفضائيين وإعادة الملاحين الفضائيين ورد الأجسام المطلقة إلى الفضاء الخارجي– لمرسوم سلطاني رقم ٢٠٢١/٧٩ بالموافقة على انضمام سلطنة عمان إلى اتفاقية المسؤولية الدولية عن الأضرار التي تحدثها الأجسام الفضائية.

[٤٤] المرسوم السلطاني رقم ٢٠١١/١٢.

[٤٥] مرسوم سلطاني رقم ٢٠٢٢/٦ بإصدار قانون حماية البيانات الشخصية.

[٤٦] تعميم وزارة النقل والاتصالات وتقنية المعلومات رقم ٢٠٢٠/٣

الفرع الثاني

التدابير اللازمة لتقليل المخاطر ومواجهة التحديات [٤٧]

برزت الهجمات السيبرانية كبدعة جديدة قبل سنوات عديدة، إلا أنها بمرور الوقت أصبحت تشكل خطراً متصاعداً على مختلف أنواع المؤسسات، لذا أصبح من هناك ضرورة لاتخاذ خطوات أساسية نحو مكافحة تلك الهجمات أهمها:

أولاً- التعاون بين الدول والمنظمات الدولية والإقليمية:

يجب زيادة أعداد الاتفاقيات والمعاهدات الدولية التي تحمي أمن المعلومات وتجرم وتكافح أي تعدي عليها، بالإضافة للتوسع في إنشاء منظمات دولية ذات الصلة، حيث أن المنظمات الدولية في العصر الحالي هي الأهم وذلك لقدرتها علي الإنفاق حيث أننا نعيش عصر التكتلات، وتهدف لتضافر الجهود الحكومية لمواجهة الهجمات والتهديدات السيبرانية، وتتنوع دورها ما بين تبادل الخبرات والمعلومات وتوفير الكوادر المدربة، والمساعدة في وضع الخطط والاستراتيجيات لمكافحة الجريمة السيبرانية، دعم الجهود الدولية للتصدي للهجمات السيبرانية كالمنظمة الدولية للشرطة الجنائية "الإنتربول"[٤٨]، حيث تساعد تجميع وتبادل المعلومات والبيانات المتعلقة بالجريمة السيبرانية والمجرم، وبناء قدرات الأجهزة الشرطية وتبادل المعارف والمعلومات، واعتمدت كذلك منصة التعاون لمكافحة الجريمة السيبرانية "العمليات"، وإعداد فرق الانتربول العاملة لمكافحة الجريمة السيبرانية[٤٩]، وأهتمت منظمة الأمم المتحدة كذلك مثل منظمة "الشراكة التعددية ضد التهديدات السيبرانية Impact " سنة ٢٠٠٩ كأول منظمة تدعمها الأمم المتحدة للتحالف لدعم الأمن السيبراني، ومركز ابتكارات الأمن

---

[٤٧] أحمد ناصف: دمج الأمن السيبراني في منظومة الأمن القومي: الأمن السيبراني والأمن القومي، جمعية إدارة الأعمال العربية، العدد ١٧٨، ٢٠٢٢، ص٤٩ وما بعدها.

[٤٨] القانون الأساسي للمنظمة الدولية للشرطة الجنائية (الانتربول)، المعتمد اثناء الدورة ٢٥ للجمعية العامة، فينا، عام١٩٥٦، رقم الوثيقة I/CONS/GA/1956(2008).

[٤٩] تقوى الرشدان: اجراءات التحقيق الابتدائي في جرائم الأمن السيبراني في القانون الأردني والاتفاقيات الدولية، كلية القانون جامعة اليرموك، ٢٠٢١، ص٣ وما بعدها.

السيبراني في عمان عام ٢٠١٢، وإقليمياً تم انشاء الاتحاد الأوروبي المجلس الأوروبي ضد الجرائم السيبرانية، وكان من أهم انجازاته اتفاقية بودابست للجريمة السيبرانية حيث تم إنشاء مكتب برنامج الجريمة السيبرانية، كما تلعب المنظمات الحكومية غير الحكومية دورا بارزا في مجال مكافحة الجريمة السيبرانية ففي مجال مكافحة الاعتداء على الطفولة، تم تأسيس "المنظمة الأوروبية غير الحكومية للتحالف من أجل أمان الطفل أونلاين Enacso" فتوفر المساعدة لجمعيات حماية الطفل في أوروبا من توفير أفضل الممارسات وتبادل الخبرات في مجال حماية الطفل أونلاين، وكذلك مرصد مراقبة الأنترنت IWF في بريطانيا حيث يقوم بحذف أية مشاهد جنسية للاعتداء على الأطفال، لذلك نجد أن الدول قد اتجهت إلى تبني العديد من المبادرات علي المستوي الإقليمي والدولي من أجل العمل علي حماية البنية التحتية الكونية للمعلومات من خطر التعرض للتهديدات السيبرانية، وعملت علي إيجاد أطر تشريعية جديدة تتعامل مع تلك الظاهرة المستحدثة في أطار صياغة مفهوم جديد للأمن الوطني ثم الاتجاه للتعاون الدولي[٥٠].

ثانياً- التوعية المجتمعية:

تثقيف الجمهور حول هذه الهجمات من خلال التعريف بأنواعها وتشجيع الإبلاغ عنها، وزيادة نمو الوعي الكوني للجمهور عبر نشر المعلومات عن العالم، ودعم الضحايا لتقليل احتمال وجود هجمات إضافية[٥١].

ثالثاً- الاطار التشريعي:

التطور السريع للهجمات السيبراني يجب أن يقابله سن قوانين حديثة من ناحية ومن ناحية أخري إجراء تعديلات علي القوانين القديمة لإصلاح أي عيوب مكتشفة، وتوسيع دوائر نطاقها، يأتي في هذا الإطار، تقاعس الإدارات أو عجزها، حتى عن

---

[٥٠] د. فارس العمارات: الأمن السيبراني "المفهوم وتحديات العصر"، دار الخليج للنشر والتوزيع، الطبعة الأولي، ٢٠٢٢، ص١٤٧.

[٥١] والت، ستيفن: العلاقات الدولية "عالم واحد ونظريات عدة"، ترجمة: منير كمال، مجلة الثقافة العالمية، عدد٨٩، أغسطس ١٩٩٨، ص ٧ وما بعدها.

تنفيذ القوانين التي وضعت آليات تنفيذها، كما هو الحال مثلا، مع قوانين حماية الملكية الفكرية والأدبية؛ حيث تنتشر ظاهرة قرصنة البرامج، بشكل كثيف، في مختلف الدول العربية ويعود ذلك إما لغياب إدارة متخصصة بالملاحقة واما لعدم إمكانية الإدارة المعنية، متابعة الوضع بشكل فاعل، نتيجة عدم توافر الإمكانات التقنية، والمادية والبشرية، وغياب القدرة على الضبط والتحقيق، ورغم إنشاء عدد من مراكز الاستجابة لطوارئ الإنترنت، في البلدان العربية، فإن بعضها ما زال غير فاعل بشكل كاف ، كما أن القوانين المنسقة بشأن الجريمة السيبرانية تنهض بالتحقيقات وتقديم المجرمين السيبرانيين إلى القضاء[٥٢].

رابعاً– الدعم السياسي والمؤسسي الاستراتيجي والتنفيذي:

شهدت العلاقات الدولية تغيراً ملموساً في طبيعتها السياسية الخارجية بعد تأثير الفضاء الإلكتروني في انتشار الفواعل من غير الدول وزيادة نشاطها وعددها وتطورها ودورها ووظيفتها عبر الفضاء الإلكتروني نتيجة للثورة المعلوماتية، وكذلك ظهور ما يسمي بالدبلوماسية الإلكترونية[٥٣] وأدوات جديدة في العلاقات الدولية وظهور تحالفات والجهود الدولية في تأمين الفضاء الإلكتروني وذلك من خلال ظهور الموجه الثالثة من الشركات في العلاقات الدولية، فإدراكاً لأهمية الأمن السيبراني، يجب على المنظمات والجمعيات والجهات الحكومية تشجيع تلك الشركات الخاصة التي تعمل على تحسين ممارساتها السيبرانية وتبادل المعلومات ووضع سياسات عالمية لموارد الانترنت والتي أصبحت تلعب دوراً في تطوير التقنيات والتحكم بها عالمياً، والذي يحقق ميزة استباقية

---

[٥٢] د. عادل عبد الصادق: الإرهاب الإليكتروني" القوة في العلاقات الدولية: نمط جديد وتحديات مختلفة": مركز الدراسات السياسية والاستراتيجية، القاهرة، ٢٠٠٩ ص١٥١ ما بعدها.

[٥٣] يمكن تعريف الدبلوماسية الإلكترونية بأنها استخدام الشبكات الإلكترونية من قبل الدول لتحديد ووضع الأهداف الدبلوماسية والقيام بوظائف الدبلوماسيين بكفاءة، متضمناً في ذلك بشكل أساسي تمثيل الدولة وتعزيز مكانتها، وترسيخ العلاقات دبلوماسية، ثنائية ومتعددة الأطراف، والخدمات القنصلية، فضلاً عن تعميق المشاركة الاجتماعية والثقافية، عائشة غنيمي: الدبلوماسية الإلكترونية وضرورة التوعية العامة، مجلة السياسة الدولية، ١٦-٢-٢٠٢١،ص١.

من خلال الاستطلاع المبكر للهجوم السيبراني لمنع الانتشار، وذلك من خلال منحهم بعض الاعفاءات الضريبية، ما قد يكون له دور في تسريع التحول الثقافي نحو الدفاع الجماعي(القطاع الحكومي والقطاع الخاص)[٥٤].

خامساً- البحث العلمي والتطوير وتنمية صناعة الأمن السيبراني:

من خلال العمل على تعزيز دور مراكز تبادل المعلومات وتحليلها، فهي منظمات مهمة لتبادل المعلومات بشكلٍ آمن تعمل من خلال المشاركة الفعَّالة للمعلومات بل تقوم كذلك بتوصيات تنفيذ أفضل الممارسات، مع وضع آلية لإدارة التوقعات وعلاج الضحايا [٥٥].

سادساً- الإعلان عن معايير الأمن:

تتطلع المؤسسات إلى هيئات مستقلة ذات مصداقية للحصول على التوجيه بشأن الشكل الجيد للأمن السيبراني، وقد أنشأ المعهد القومي للمعايير والتكنولوجيا (NIST) إطار عمل للأمن السيبراني في عام ٢٠١٤ للعمل على تنظيم وتحديد الدفاعات اللازمة لحماية الأجزاء المهمة المحددة في برنامج الأمان، وقد حدد معهد الأمن والتكنولوجيا (IST) أعلى عناصر التحكم التي تحمي من الهجمات الإلكترونية[٥٦].

سابعاً- إقرار سياسات وقائية ودفاعية:

للعمل علي بناء الثقة والاطمئنان والأمن في استعمال الاتصالات وتكنولوجيا حماية البيانات الشخصية يجب إعداد أدلة تشغيل أثناء الأزمة حيث يجب أن يكون لدى جميع المؤسسات أدلة مثل أدلة الأمن البيئي وأمن الطاقة، والأمن التكنولوجي، والأمن الغذائي، الأمن الإنساني والتي يجب أن تتضمن إلية التشغيل للاستجابة في الساعات

---

[٥٤] د. عادل عبد الصادق: العلاقات الدولية والفضاء الإلكتروني "دراسة في النظرية والتطبيق"، المركز العربي لأبحاث الفضاء الإلكتروني، القاهرة، الطبعة الثالثة، ٢٠١٦م، ص ١٦٦ وما بعدها.

[٥٥] ماجد عزيز إسكندر: التوظيف السياسي للهجمات السيبرانية ومخاطرها على الأمن القومي، مركز الإمارات للدراسات والبحوث الاستراتيجية، ٢٠٢٣م، ص١٣٠ وما بعدها.

[٥٦] الموقع الرسمي على الرباط التالي:
https://aws.amazon.com/ar/compliance/nist/(29/6/2023).

والأيام والأسابيع الأولى من الهجمات السيبرانية أيا كان القطاع الذي يتم مهاجمته، وجهات الاتصال الحكومية، وتفاصيل حول كيفية الوصول إلى تلك الجهات الاتصال الحكومية، وأي هيئات تنظيمية أو غيرها من الهيئات الرقابية وهى من الأولويات التي تستدعى تعاونًا وتنسيقًا دوليين بين الحكومات والمنظمات ذوات الصلة وشركات القطاع الخاص والكيانات المعنية في مجال بناء القدرات وتبادل أفضل الممارسات من أجل وضع السياسات العامة والتدابير القانونية والتنظيمية والتقنية التي تتناول حماية البيانات الشخصية، لضمان موثوقية وأمن شبكات وخدمات تكنولوجيا المعلومات والاتصالات ولذلك اتجهت معظم الدول المتقدمة إلى إقرار سياسات وقائية ودفاعية، ضد الهجمات السيبرانية وخصصت بعض الدول مثل الولايات المتحدة الأمريكية وأستراليا وانجلترا مبالغ طائلة، لمعالجة مسائل الأمن السيبرانى[٥٧].

ثامناً- تأمين البنى التحتية للاتصالات والمعلومات من خلال:

١- **تشكيل جهات حكومية للأمن السيبرانى:** بهدف حماية المعلومات والبيانات لدى الجهات مع الاهتمام بإدارات المعلومات والاتصالات في الوزارات والجهات المختلفة، والتأكد من توفر التمويل اللازم لضمان تنفيذ منظومة الأمن السيبرانى، مع ضرورة وضوح الإطار التشريعي الخاص بها[٥٨].

٢- **إطلاق استراتيجيات وطنية للأمن السيبراني:** وهي تهدف إلى تأمين البني التحتية للاتصالات والمعلومات بشكل متكامل لتوفير البيئة الآمنة لمختلف القطاعات لتقديم الخدمات الإلكترونية المتكاملة، وذلك في إطار جهود الدول لدعم الأمن القومي وتنمية المجتمعات[٥٩].

---

[٥٧] د. علي العلي، د. علي حميد: تكتيكات الحروب الحديثة" الأمن السيبراني والحروب المعززة والهجينة"، الطبعة الأولي، العربي للنشر والتوزيع، القاهرة، ٢٠٢٣م، ص٢٠٨ وما بعدها.

[٥٨] المجلس الأعلى للأمن السيبرانى في مصر ٢٠١٤م.

[٥٩] الاستراتيجية الوطنية المصرية للأمن السيبراني (٢٠١٧- ٢٠٢١).

٣ – **مراكز الاستجابة لطوارئ الحاسب الآلى:** تقوم تلك المراكز بتقديم الدعم الفني على مدار ٢٤ ساعة لحماية البنية التحتية الحيوية للمعلومات [٦٠].

تاسعاً– استحداث الجرائم السيبرانية:

لا يكفي تأمين المعلومات بل يجب تجريم كل اعتداء عليها، حيث اتجهت بعض الدول إلى اصدار قوانين تضمنت النص صراحة علي أن الاعتداء علي الأمن السيبراني للدولة يمثل اعتداء علي الأمن القومي [٦١]، حيث أن بناء مجتمع معرفي مستدام يحتاج بالضرورة إلى بيئة قانونية وتنظيمية ملائمة تحمي فضائها السيبراني، لكون الفضاء السيبراني أصبح ضرورة وركيزة أساسية لازمة ولا غني عنها لأي دولة في الوقت الراهن، كم انه أصبح مظهراً من مظاهر سيادة الدولة علي فضائها لسيبراني[٦٢].

عاشراً– إقرار المسؤولية الدولية[٦٣] الناشئة عن الهجمات السيبرانية:

تقتضي مكافحة الهجمات والجرائم السيبرانية إقرار مسؤولية أي دولة لها علاقة من قريب أو من بعيد عن تلك الأفعال لما لقواعد المسؤولية الدولية من إلزام علي الدول، فالدولة التي تقوم بأي فعل من شأنه إحداث ضرر يصيب دولة أخرى أو عدة دول، فتتحمل الدولة التي أحدثت ذلك الضرر، أو تسببت في إحداثه، تبعات المسؤولية الدولية عن ذلك الفعل، فالهجمات السيبرانية يقوم بها أشخاص يخضعون للقانون الدولي، وتؤدي إلى أضرار، وبذلك تكون الهجمات السيبرانية مستوفية شروط قيام المسؤولية الدولية (الحدة – الضرر "الحال أو اللاحق" – أن يكون أثر الهجوم مباشراً – العدائية – نسبة الفعل إلى دولة – أن يكون الفعل غير مشروع دولياً)[٦٤] مما يجعلها مضطرة

---

[٦٠] المركز المصري للاستجابة لطوارئ الحاسب الآلي "سيرت ".

[٦١] المادة (٥/١) من قانون حماية الأمن السيبراني في أوكرانيا رقم (٤٥) لسنة ٢٠١٧.

[٦٢] د. حازم الجمل: الحماية الجنائية للأمن السيبراني في ضوء رؤية المملكة ٢٠٣٠م، مجلة البحوث الأمنية، مجلد٣٠، عدد٧٧، ٢٠٢٠م، ص٢٤٣ وما بعدها

[63] See, CH.Ronsseau :La responsabilité international 1959-1960, P.24.

[٦٤] رزق سمودي: حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام، مرجع سابق، ص٣٥١ وما بعدها.

لدفع تعويضات للدول المتضررة، لذلك نجد أنه من الضروري إقرار المسؤولية الدولية عن تلك الهجمات السيبرانية لما لها أثر رادع لكل دولة تسول لها نفسها القيام بهجمات سيبرانية علي دولة أخري أو تشارك فيها حيث أن الواقع العملي يؤكد أنه علي الرغم من توفر أركان المسؤولية الدولية في الهجمات السيبرانية، إلا أن الكشف عن هوية الفاعلين ومراقبتهم وتتبعهم، من أجل تقديمهم للمحاكمة، تكون صعبة لما يتمتع به الفضاء السيبراني من قابلية التخفي[٦٥].

إحدى عشر- تطبيق القانون الدولي الإنساني[٦٦] علي الهجمات السيبرانية[٦٧]:

إن أبرز مواطن قوة القانون الدولي الإنساني أنه قد وُضع بطرق تجعله ينطبق على كافة أشكال الحرب وكافة أنواع الأسلحة، بما فيها "الأشكال والأنواع المستقبلية، وتتسم القواعد الأساسية بالوضوح، وهي أنه: يُحظر استهداف المدنيين والأعيان المدنية، ويجب ألّا تُستخدم الأسلحة والهجمات العشوائية، وتُحظر الهجمات غير المتناسبة[٦٨]، ويجب احترام الخدمات الطبية وحمايتها.، وتنطبق القواعد والمبادئ نفسها – بما فيها

---

[٦٥] طلال العيسى، عدي عناب: المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مجلة الزرقاء للبحوث والدراسات الإنسانية – المجلد التاسع عشر، العدد الأول، ٢٠١٩، ص٨٨ وما بعدها.

[٦٦] د. جان بكتيه، القانون الدولي الإنسان: تطوره ومبادئه، دار المستقبل العربي، القاهرة، ١٩٨٤م، ص٣٣، د. أحمد فتحي سرور، القانون الدولي الإنساني، ط ٣، عمان: منشورات اللجنة الدولية للصليب الأحمر، ٢٠٠٦م ص ٢٥ وما بعدها.

[٦٧] لم تنظم الهجمات السيبرانية فظهورها لاحق لها. خاصة في ظل عدم القدرة على إثبات الدليل المادي للهجمات السيبرانية، وكذا الإقرار المادي الملموس المباشر أو الغير مباشر عقب الهجمات السيبرانية كالدمار أو التعطيل الجزئي أو الكلي للأهداف المدنية أو العسكرية، كذلك الحال بشأن القتل أو الجرح الذي يصيب العسكريين أو المدنيين مما يصب في عدم قدرة تصدي القانون الدولي للهجمات السيبرانية، اتفاقيات لاهاي لعام ١٨٩٩ و١٩٠٧ واتفاقيات جينيف الأربعة لعام ١٩٤٩ والبروتوكولان الإضافيان لعام ١٩٧٧.

[٦٨] أنس جميل اللوزي: مفهوم الضرورة العسكرية في القانون الدولي الإنساني، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، ٢٠١٤، ص٨٥.

مبادئ الإنسانية والضرورة العسكرية والتمييز والتناسب[٦٩] واتخاذ الاحتياطات – على جميع العمليات العسكرية، سواء كانت ذات طابع حركي أو سيبراني، ويجب احترامها، وتتمثل خطورة الهجمات السيبرانية في أنها لا تطول الدول المتقدمة تكنولوجياً فقط، فالفضاء الإلكتروني بطبيعته مترابط ترابطاً وثيقاً، ومن هنا فقد تؤثر الهجمات التي تُشن في الفضاء السيبراني ضد دولة واحدة على العديد من الدول الأخرى، سواء عمداً أو عرضاً، أينما كان موقعها، وبالتإلى فإن التنظيم الفعال للعمليات السيبرانية أثناء النزاع المسلح هو مسألة تهمّ جميع الدول، بغض النظر عن مستوى تطورها التكنولوجي، أو قدراتها العسكرية السيبرانية، أو مشاركتها في النزاعات المسلحة، حيث يجب ان ينطبق القانون الدولي الإنساني علي العمليات السيبرانية التي تنفذ في سياق نزاع مسلح، لكي نحد من العمليات السيبرانية أثناء النزاعات المسلحة تماماً مثل الحد من استخدام أي أسلحة ووسائل وأسإلبب حرب أخرى أثناء نزاع مسلح، جديدة كانت أم قديمة، ولقد اعتمدت محكمة العدل الدولية هذا الرأي[٧٠].

المطلب الثاني

دور المراكز الوطنية والإقليمية للأمن السيبراني والابتكار في حماية الأمن السيبراني

في إطار جهود الدول لدعم الأمن القومي وتنمية المجتمعات، ومع تزايد التهديدات والتحديات المستقبلية في المجال السيبراني والمجتمع الرقمي ولرصد ومجابهة المخاطر والتهديدات المتزايدة، أصبحت تقنية المعلومات والاتصالات هي المحرك الأساسي لعجلة التنمية لذلك تبنت العديد من الدول انشاء مراكز وطنية وإقليمية للأمن السيبراني وابتكار طرق لمكافحة الهجمات السيبرانية ومنها:

---

(69) See, Micheal Newton & Larry May, Proportionality in International Law, Oxford University Press, 2014; Arbitral Award in the Naulilaa Case 1928, 2 Reports of the International Arbitral Awards 1011-1028.

(70) اللجنة الدولية للصليب الأحمر: الحرب السيبرانية والقانون الدولي الإنساني، منشور على الرابط:

https://www.icrc.org/ar/document/ (1/7/2023).

الفرع الأول

المراكز الوطنية والإقليمية للأمن السيبراني

تطلع الدول لحماية أمنها السيبراني من خلال: مسح ومراقبة المجموعات المحلية من خلال قيام الدولة بالمراقبة الإلكترونية لرصد واكتشاف التهديدات المحلية والجهات الفاعلة داخل حدودها لحماية أمنها القومي ، وكذلك تقوية وتعزيز الدفاعات السيبرانية الوطنية، من خلال التحكم في بيئة المعلومات ومعالجتها، وتحقيق مكاسب تجارية و تعزيز نمو الصناعة المحلية، وتحديد القواعد والمعايير التقنية الإلكترونية الدولية عن طريق مشاركة الدولة بنشاط في المناقشات القانونية والسياسية والفنية الدولية حول المعايير الإلكترونية[٧١]، كل ذلك يتحقق من خلال المراكز الوطنية والإقليمية والتي من أهمها:

أولاً- المركز العربي الإقليمي للأمن السيبراني (ITU-ARCC) في دول الخليج:

توجد صور للتعاون الإقليمي في مجال الأمن السيبراني بين دول مجلس التعاون الخليجي، ويتمثل ذلك في ممارسات عدة أهمها المركز العربي الإقليمي للأمن السيبراني في دول الخليج، والذي يعمل علي التعاون من أجل تأسيس برامج دفاعية عسكرية أمنية وبحثية مشتركة ومتطورة في مجال الأمن السيبراني في ظل تطور الحكومات الرقمية الذكية في دول مجلس التعاون الخليجي[٧٢]، وتم تأسيس المركز من قبل الاتحاد الدولي للاتصالات (ITU) وسلطنة عمان في ديسمبر ٢٠١٢ ممثلة في وزارة النقل والاتصالات وتقنية المعلومات (هيئة تقنية المعلومات سابقا) بهدف الاشراف على تنفيذ البرنامج العام للأمن السيبراني للاتحاد الدولي للاتصالات في جميع أنحاء المنطقة

---

(71) See: JuliaVoo (& others), National Cyber Power Index 2020 Methodology and Analytical Considerations, China Cyber Policy Initiative, Belfer Center for science and International Affairs, Harvard Kennedy School, https://www.belfercenter.org/sites/default/files/2020-09/NCPI.pdf, accessed on 02/07/2023.

[٧٢] أمل المشايخي: مستقبل الأمن السيبراني في سلطنة عمان: وجهات النظر والرؤى الوطنية والإقليمية، رسالة ماجستير، جامعة السلطان قابوس، ٢٠١٧م، ص١٠٠ وما بعدها.

العربية، والاستجابة لمتطلبات الأمن السيبراني لأحدث التطورات، وأن يكون مركزا للإدارة ومنصة لتنفيذ أهداف الأمن السيبراني، وتوفير مركز موحد للدول الأعضاء لإدارة برامج مبادرات الأمن السيبراني للدول الأعضاء، مع العمل على وضع الأطر والخطط في مجال الامن السيبراني من خلال إجراء الدراسات الإقليمية وعقد ورش العمل، رفع مستوى الوعي والخبرات في الأمن السيبراني في قطاع البنى التحتية للمعلومات، ويعمل الخبراء في المركز العربي الإقليمي للأمن السيبراني جنباً إلى جنب مع القطاعين العام والخاص من أجل تطوير استراتيجيات الأمن السيبراني الوطني مع وجود مسؤوليات واضحة، ويستخدم الخبراء في المركز العربي الإقليمي للأمن السيبراني أفضل المعايير التقنية العالمية مثل الآيزو ٢٧٠٠١ التي تمكن الدول الأعضاء من تحديد المواضع الواجب تحسينها أمنياً، ويساعد في بناء قدرات مؤسسية للأمن السيبراني وتطوير حلول وبرامجية فاعلة، ويعمل فريق المركز العربي الإقليمي للأمن السيبراني مع الشركاء على مساعدة وتشجيع الدول الأعضاء في الاتحاد الدولي للاتصالات في إنشاء فرق وطنية للاستجابة للطوارئ للحوادث الأمنية، حيث تأخذ هذه الفرق مسؤولية وطنية لتكون مركزا موثوقاً لتنسيق جهود الأمن السيبراني، كما تساعد هذه الخدمة في تقييم مقدرات فرق الاستجابة للحوادث الأمنية في الحكومات والقطاع العام، وتحديد الثغرات وتقديم خارطة الطريق لتحسين هذه الفرق[٧٣].

ثانياً –المجلس الأعلى للأمن السيبراني بجمهورية مصر العربية:

يختص باعتماد تحديد البنى التحتية للاتصالات و المعلومات الحرجة في كافه قطاعات الدولة و وضع أطر تقييم و متابعه تامين لها في القطاعات المختلفة، واعتماد أطر واستراتيجيات وسياسات تامين البنى التحتية للاتصالات والمعلومات الحرجة لكافه قطاعات الدولة، ووضع خطط وبرامج تنميه صناعه الامن السيبراني واعداد الكوادر اللازمة لمواجهه التحديات والمخاطر السيبرانيه ووضع إطار للبحث العلمي والتطوير في مجال الامن السيبراني، والتعاون و التنسيق اقليميا ودوليا مع الجهات ذات صله

---

[٧٣] الموقع الرسمي للمركز العربي الإقليمي للأمن السيبراني في دول الخليج، على الرابط: https://arcc.om/(30/6/2023).

في مجال الامن السيبرانى وتأمين البني التحتية الحرجة للاتصالات والمعلومات وإعداد توصيات بأية تدخلات تشريعيه لازمه للتأمين، ووضع المعاير الملزمة لكافه الجهات كحد أدنى لتأمين البني التحتية الحرجة للاتصالات والمعلومات والزامها بإعداد خطط الطوارئ، ووضع آليات رصد المخاطر والمتابعة الدورية للهجمات السيبرانيه وتوزيع الادوار علي المستوى الوطني، ووضع و تفعيل معايير وآليات لتحديد الاعتماديات البنيه الموجودة بين عناصر البنيه الأساسية الحرجة والقائمين عليها وما يقع خارجها بحيث يتم تجنب التأثيرات المتتالية، واقرار مواصفات الأمن السيبراني القياسية للأنظمة في مختلف القطاعات وإضافه معايير الجودة السيبرانيه، واعتماد توصيف التقويم الامني للقائمين علي تشغيل البني التحتية الحرجة للاتصالات والمعلومات، ووضع آلية لمتابعه تأمين وحمايه المواقع الحكومية الرسمية علي الإنترنت[٧٤].

ثالثاً- المركز الوطني المصري للاستعداد لطوارئ الحاسبات والشبكات(EG-CERT) :

تم تشكيله بالجهاز القومي لتنظيم الاتصالات في أبريل ٢٠٠٩م حيث يقدم المركز الدعم اللازم لحماية البنية التحتية القومية للمعلومات الهامة خاصة في قطاع تكنولوجيا المعلومات والاتصالات والقطاع المالي، وبمراقبة الأمن السيبراني والاستجابة للحوادث وتحليل معامل الطب الشرعي الرقمي وتحليل البرمجيات الخبيثة والهندسة العكسية ويتمثل الهدف الرئيسي للمركز في تعزيز أمن البنية التحتية المصرية للاتصالات والمعلومات من خلال اتخاذ إجراءات استباقية، وجمع وتحليل المعلومات الخاصة بالحوادث الأمنية، والتنسيق والوساطة بين الأطراف المعنية في حل تلك الحوادث الأمنية والتعاون الدولي مع غيرها من فرق الاستجابة لطوارئ الحاسبات والشبكات في الدول الأخرى[٧٥].

---

[٧٤] قرار رئيس مجلس الوزراء المصري رقم ١٦٣٠ لسنة ٢٠١٦.

[٧٥] الموقع الرسمي للمركز الوطني المصري للاستعداد لطوارئ الحاسبات والشبكات EG-CERT)، على الرابط:

https://egcert.eg/ar/(30/6/2023)

رابعاً- المركز الوطني للسلامة المعلوماتية بسلطنة عمان:

في ظل سعي سلطنة عمان لتوفير بيئة معلوماتية آمنة لأي مستخدم لمواقع جهات حكومية أو خاصة على حد سواء، والعمل علي بناء الثقة في استخدام الخدمات الحكومية، وتطوير استراتيجيات وسياسات أمن المعلومات لتستفيد منها الجهات الحكومية والخاصة وتقديم النصائح الفنية المبدئية وتقارير تقنية تساعد إداري الشبكات والأنظمة والتطبيقات في كل من القطاع العام أو الخاص على تجنب تعريض مواقعهم لأية مخاطر أمنية، والسعي نحو توفير بيئة معلوماتية آمنة عند استخدام الخدمات الالكترونية الحكومية لكل مواطن عماني ومقيم، وتشجيع الأفراد الذين يتلقون التدريب في المركز على العمل في قطاع أمن المعلومات في أي جهة أو مؤسسة في السلطنة، والاستجابة لأية حوادث أمنية ومحاولة الحد من أثارها، ونشر الوعي حول أهمية أمن المعلومات بين أفراد المجتمع العماني، و توفير العديد من الخدمات مثل: تأهيل كوادر عمانية متخصصة في هذا المجال، مراقبة مواقع حية من أجل اكتشاف أية أخطار قد تهدد هذه المواقع، وتقديم دورات وورش وحلقات تدريبية لكافة المستهدفين، والاستجابة الاستباقية والتفاعلية لأية مشكلة مباشرةً، وحماية أي نظام ومعالجته في حالة تعرضه لأية مشكلة عن طريق تقديم التوجيه، تم إنشاء المركز الوطني للسلامة المعلوماتية كأحد مبادرات عمان الرقمية والنقطة المحورية للحوادث الأمنية في سلطنة عُمان وذلك خلال شهر أبريل عام ٢٠١٠م، وقد قام المركز بالكشف عن أكثر من ٨,٧١٣ هجمة خطيرة ومرتبطة بالأمن المعلوماتي موجهة للفضاء المعلوماتي العماني ناتجة عن تحليل ملايين من محاولات الاتصال وتصنيفها، والكشف عن ٥٣٧ حالة ألحقت أضرارا وانتشاراً لبرمجياتٍ خبيثة تستهدف الفضاء المعلوماتي في الدولة، وإجراء ١٣ تقييم لنقاط الضعف الأمنية واختبارات اختراق وتحقق للمؤسسات الحكومية وللهياكل الوطنية الحساسة عام ٢٠١٤، وعلاج ١١٨ حالة للأدلة الرقمية ناتجة عن تحليل ٢٨٨ جهاز

بما فيها أجهزة الكمبيوتر والهواتف والأقراص الصلبة الخارجية ووحدات التخزين المتنقل، واكتشاف ٢٨٨ دليلَ إدانة رقمي خلال عام ٢٠١٤م[٧٦].

- **المختبر الوطني للأدلة الرقمية:**

يتعامل هذا المختبر مع الأدلة الرقمية التي يتم اكتشافها من الجرائم الإلكترونية وتقديمها للقانون من أجل تطبيق الإجراءات القانونية اللازمة وبالتالي تضمن تقديم المجرمين إلى وجه العدالة، ويهدف هذا المختبر لإيجاد اعتماد دولي يعزز مصداقية عمل المختبر والأدلة الرقمية، وتشمل خدمات المختبر العثور على الأدلة الرقمية في أجهزة الكمبيوتر والهواتف واستعادة بياناتها.

- **مركز أمن المعلومات الإقليمي:**

تم بدء العمل للمركز الإقليمي للأمن السيبراني التابع للاتحاد الدولي للاتصالات رسميا عام ٢٠١٣م ، والانتهاء من إنشاء خارطة طريق لدراسة الأمن السيبراني في المنطقة العربية، حيث يقوم هذا المركز بتلبية متطلبات الوطن العربي فيما يتعلق بأمن المعلومات، حيث يشكل عاملا أساسيا في دعم شبكات الشراكة الدولية متعددة الأطراف ضد التهديدات السيبرانية (IMPACT) على مستوى العالم في مختلف المناطق من خلال اضفاء الطابع العربي على خدمات أمن المعلومات وذلك بناء على حاجة الوطن العربي، وقد قام المركز بعقد وتنظيم المؤتمر الاقليمي الثالث للأمن السيبراني عام ٢٠١٤، وشارك المركز في اجتماع الفريق العامل التابع لمجلس الاتحاد الدولي للاتصالات حول حماية الأطفال من مخاطر الإنترنت الذي عقد في جنيف، وقد حصل المركز على جائزة القمة العالمية لمجتمع المعلومات في سويسرا في فئة بناء الثقة والحماية في استخدام تقنية المعلومات والاتصالات، وحصلت السلطنة على المركز الأول في قائمة أمن المعلومات العالمي على مستوى الوطن العربي التي نظمها الاتحاد الدولي للاتصالات.

---

[٧٦] المركز الوطني للسلامة المعلوماتية – الموقع الرسمي للمركز علي:
1/7/2023 (omanportal.gov.om)

الفرع الثاني

المراكز واللجان الوطنية والإقليمية للابتكار

تصاعد اهتمام العالم بحماية البنية التحتية الرقمية، والرقابة الإلكترونية وسبل التصدي لاختراقات الارهابيين، والحرب الإلكترونية، والإرهاب الإلكتروني[٧٧] والهجمات الإلكترونية، ومن هنا وضعت سلطنة عمان على رأس أولوياتها استقطاب الكوادر الوطنية المؤهلة والطموحة وتأهيلها، وكذلك تحفيز الابتكار والاستثمار في مجال الأمن السيبراني عن طريق:

أولاً- لجنة التقنية والابتكار بمجلس الدولة العماني:

تعمل سلطنة عمان علي تشجيع البحث والتطوير والابتكار في مجال الأمن السيبراني، وذلك عن طريق سن القوانين مثل: قانون "استثمار التقنية والابتكار" و"الأمن السيبراني" من أجل إيجاد بيئة استثمارية محفزة للابتكار في المجالات التقنية وداعمة من أجل تطوير الفرص الاستثمارية في مجالات التقنية والابتكار وتمويل البحث والتطوير، وتختص بدراسة مشروعات القوانين المحالة إلى المجلس والمتعلقة بالتقنية والابتكار، واقتراح مشروعات القوانين التي تدخل في نطاق اختصاصات اللجنة، ومراجعة القوانين النافذة التي تدخل في نطاق اختصاصات اللجنة، ومراجعة الإستراتيجيات الوطنية والدراسات التي تسهم في تطوير وتوطين توظيف نقل التقنية، ومراجعة الآليات وسياسات التقنية والاستثمار في البنية الأساسية للتقنية وتقديم المقترحات، وتحليل المستجدات المتعلقة بالتقنية والابتكار ودراسة الآثار المترتبة عليها[٧٨].

---

[٧٧] أحمد ناصف: دمج الأمن السيبراني في منظومة الأمن القومي: الأمن السيبراني والأمن القومي، مرجع سابق، ص٥٥.

[٧٨] المادة (٦٨) من النظام الأساسي للدولة الصادر بالمرسوم السلطاني رقم (٢٠٢١/٦) التي نصت على أن يتكون مجلس عمان من مجلسي الدولة والشورى.

ثانياً- مجمع الابتكار مسقط:

يتطلب تحقيق الأمن السيبراني البحث العلمي واستغلال أي منظومة إبداعية تستجيب للمتطلبات المحلية والتوجهات العالمية، وتعزز الانسجام الاجتماعي وتقود إلى الابتكار والتميز العلمي، من خلال بناء السعة البحثية، وتحقيق التميز البحثي، وتأسيس الروابط البحثية ونقل المعرفة، وتوفير البيئة البحثية المحفزة، حيث أن مواجهة الهجمات السيبرانية تحتاج قدر كبير من التكنولوجيا والحلول الابتكارية الإبداعية، ويعد أحد أبرز مبادرات مجلس البحث العلمي لتطوير البحوث العلمية والتشجيع على الابتكار انشاء مجمع الابتكار بمسقط بهدف تفعيل الربط بين القطاع الأكاديمي والخاص وبين مختلف شرائح المجتمع المحلي والعالمي، والسعي نحو توفير بيئة حاضنة ومحفزة للباحثين والمبتكرين ورواد الأعمال، ومن خلال تقديم الدعم المناسب وتوفير كافة الاحتياجات، التي ستُسهم في المقابل في تنمية القوى البشرية وتزيد دافعيتهم نحو البحث العلمي، فضلاً عن رفع مشاركتهم في استغلال المعارف وتطوير الافكار والمنتجات القائمة على البحوث العلمية، وتحويلها إلى منتج محلي قائم على البحث العلمي والابتكار، مما سيؤدي إلى تعزيز جهود الحكومة في تحقيق الأمن السيبراني، وقد تم البدء في تنفيذ المرحلة الأولى من المشروع في مارس من عام ٢٠١٣م[٧٩].

أدركت دول العالم أهمية وضرورة تبني برامج مبنية على استراتيجيات وخطط مدروسة، لذلك تعمل كافة المراكز السابقة في كافة دول العالم على تبني استراتيجيات وبرامج لتطوير الخدمات الإلكترونية وبنيتها التحتية، ومنها:

- **الاستراتيجية الوطنية المصرية للأمن السيبراني (٢٠١٧-٢٠٢١):**

نص الدستور المصري علي أن أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه، علي النحو الذي ينظمه القانون[٨٠]، حيث تم انشاء المجلس الأعلى لتأمين البني التحتية

---

[٧٩] مجمع الابتكار، على الرابط:

https://www.trc.gov.om/(1/7/2023)

[٨٠] المادة (٣١) من دستور مصر ٢٠١٤.

للاتصالات والمعلومات (المجلس الأعلى للأمن السيبراني) [٨١] لوضع استراتيجية لتأمين البني التحتية للاتصالات والمعلومات بشكل متكامل، بهدف "مواجهة المخاطر السيبرانية، وتعزيز الثقة في البني التحتية للاتصالات والمعلومات وتطبيقاتها وخدماتها في شتي القطاعات الحيوية وتأمينها من أجل تحقيق بيئة رقمية آمنة وموثوقة للمجتمع المصري بمختلف أطيافه" والتي تتضمن عددا من البرامج التي تدعم الأهداف الاستراتيجية للأمن السيبراني. كما توضح توزيع الأدوار بين الجهات الحكومية والقطاع الخاص ومؤسسات الاعمال والمجتمع المدني وما ستقوم به الدولة من إجراءات للتقدم نحو تحقيق تلك الأهداف، وتقدم الاستراتيجية ملامح خطة عمل تمتد على مدار الأعوام ٢٠١٧-٢٠٢١، بما يدعم التحول نحو اقتصاد رقمي متكامل يحقق طموحات المواطنين في تنمية اجتماعية واقتصادية شاملة ويحمي مصالحهم، ويحافظ علي مصالح الدولة العليا ويسهم في نهضتها وازدهارها ورخاءها[٨٢].

- **برنامج صناعة الأمن السيبراني العماني (حداثة):**

توجد ممارسات ممتازة لحماية الأمن السيبراني منها سياسة الوصول عن بعد لموارد وبيئة التقنية والاتصالات الصادرة عن وزارة التقنية والاتصالات ٢٠٢٠، وكذلك التقارير السنوية لهيئة تقنية المعلومات والتي من أهمها أعوام ٢٠١٧- ٢٠١٩-٢٠٢٠-٢٠٢١-٢٠٢٢، ويوجد أدلة (إرشادات) حوكمة الأمن السيرباني، وهناك إطار عمل إدارة أمن المعلومات، والضوابط الأساسية لأمن المعلومات، وسياسة إدارة أمن المعلومات، أما برنامج صناعة الأمن السيبراني (حداثة) تتمثل رؤيته في الأمن

---

[٨١] انشئ المجلس الأعلى للأمن السيبراني بقرارات (قرار رئيس مجلس الوزراء رقم ٢٢٥٩ لسنة ٢٠١٤- قرار رئيس مجلس الوزراء رقم ١٦٣٠ لسنة ٢٠١٦- قرار رئيس مجلس الوزراء رقم ٩٩٤ لسنة ٢٠١٧- قرار رئيس مجلس الوزراء رقم ٢٧٦ لسنة ٢٠٢٠) يختص المجلس بوضع استراتيجية وطنيه لمواجهه الاخطار و الهجمات السيبرانية والإشراف على تنفيذها و تحديثها وعلى أعضاء المجلس مراجعه مهامه وتشكيل أمانة فنية تنفيذية تابعة له.

[٨٢] الاستراتيجية الوطنية للأمن السيبراني (٢٠١٧-٢٠٢١).

السيبراني تعزز وتنوع النمو الاقتصادي، ومهمته إنشاء صناعة متخصصة في الأمن السيبراني في المنطقة، تُركز على رأس المال البشري وتستند الى الابتكار والإبداع والتميز، وذلك من خلال السعي نحو التوافق مع رؤية عُمان ٢٠٤٠ في مواجهة تحديات الأمن السيبراني، وتطوير نظام ايكولوجي وطني لصناعة الأمن السيبراني، وتطوير قدرات الأمن السيبراني المتخصصة، وإنشاء شركات ناشئة و شركات صغيرة ومتوسطة متخصصة ومتميزة في مجال الأمن السيبراني لخدمة الاحتياجات والتحديات المحلية، والترويج لشركات الأمن السيبراني المحلية المتخصصة على المستوى الدولي، وتعزيز الابتكار في مجال الأمن السيبراني، وتشجيع البحث والتطوير في مجال الأمن السيبراني، وإقامة شراكة مع القطاع الخاص والقطاعات الأكاديمية والحكومية، والتعاون مع الشركاء الدوليين في مجال الصناعة والابتكار في الأمن السيبراني، وإيجاد حوافز خاصة للأمن السيبراني، وجذب الاستثمار الأجنبي في مجال الأمن السيبراني للسلطنة، وتحققت عدة نتائج لبرنامج صناعة الأمن السيبراني منها: وصول سلطنة عُمان لمرتبة متقدمة في قائمة أفضل (١٠) دول في المؤشر العالمي للجاهزية في الامن السيبراني عن طريق استيفاء متطلبات المؤشر العالمي، ورفع مساهمة سوق الأمن السيبراني في سلطنة عُمان بنسبة ٢٠% من إجمالي مساهمة قطاع تقنية المعلومات، وتوفير ١٠٠٠ فرصة عمل او فرص مدرة للدخل في مجال الامن السيبراني، وتعمين مهن الامن السيبراني في القطاع الحكومي بنسبة ٩٠%، وزيادة نسبة العمل الحر في الامن السيبراني بنسبة ٨٠%، واستقطاب ٢ من الشركات الاجنبية العاملة في مجال الامن السيبراني ليكون لها وجود بسلطنة عُمان[٨٣].

- **الاستراتيجية الوطنية للأمن السيبراني الإماراتية:**

تسعى لتحقيق الأهداف التالية: تعزيز ثقة أفراد المجتمع للمشاركة بشكل آمن في العالم الرقمي، وبناء كادر بشري على مستوى عالمي في مجال الأمن السيبراني في دولة الإمارات العربية المتحدة، وتعزيز الابتكار في مجال الأمن السيبراني، وتمكين

---

[٨٣] المركز الوطني للسلامة المعلوماتية: برنامج صناعة الأمن السيبراني (حداثة)، على الرابط: https://cert.gov.om/sp/hadatha (1/7/2023).

الشركات الصغيرة من حماية نفسها ضد الهجمات السيبرانية، وترسيخ ثقافة الاستثمار في الأمن السيبراني، وحماية المعلومات الحساسة والبنية التحتية للدولة، وذلك من خلال إنشاء منظومة متكاملة للأمن السيبراني من خلال تنفيذ ٦٠ مبادرة ضمن ٥ محاور هي: قوانين ولوائح الأمن السيبراني، وبيئة متكاملة وحيوية للأمن السيبراني، والخطة الوطنية للاستجابة للحوادث السيبرانية، وبرنامج حماية البنية التحتية للمعلومات الحيوية، والشراكات[٨٤].

- **الاستراتيجية الوطنية للأمن السيبراني السعودية:**

تم وضعها لكي تعكس الطموح الاستراتيجي للمملكة بأسلوب متوازن بين الأمان والنمو ولتحقيق مفهوم (فضاء سيبراني سعودي آمن وموثوق يمكّن النمو والازدهار)، سعت من خلالها لتحقيق حوكمة متكاملة للأمن السيبراني على مستوى وطني، وإدارة فعالة للمخاطر السيبرانية على المستوى الوطني، وحماية الفضاء السيبراني، وتعزيز القدرات الوطنية في الدفاع ضد التهديدات السيبرانية، وتعزيز الشراكات والتعاون وبناء القدرات البشرية الوطنية وتطوير صناعة الأمن السيبراني في المملكة، من خلال:(التكامل، التنظيم، التوكيد، الدفاع، التعاون، البناء)[٨٥]، ويدعم ويعزز تلك الاستراتيجية بالمملكة بعض المؤسسات مثل الاتحاد السعودي للأمن السيبراني والبرمجة، هيئة الأمن السيبراني، كلية الأمن السيبراني والذكاء الاصطناعي والتقنيات المتقدمة، أكاديمية متخصصة بالأمن السيبراني[٨٦].

---

[٨٤] هيئة تنظيم الاتصالات والحكومة الرقمية (TDRA)، الاستراتيجية الوطنية للأمن السيبراني، على الرابط:
https://tdra.gov.ae/ar/national-cybersecurity-strategy (1/7/2023).

[٨٥] الهيئة الوطنية للأمن السيبراني: الاستراتيجية الوطنية للأمن السيبراني، على الرابط:
https://www.nca.gov.sa/strategic (1/7/2023).

[٨٦] وزارة الخارجية– معهد الأمير سعود الفيصل للدراسات الدبلوماسية: الأمن السيبراني: درع المملكة الواقي لحماية مصالحها الحيوية وبنيتها التحتية، مجلة الدبلوماسي، عدد ٩٠، ٢٠١٨، ص ٨–١١.

الخاتمـــة

في ظل الجهود السابق استعراضها للدول العربية نجد ترتيبها وفق مؤشر الامن السيبراني لعام ٢٠٢٠ كالتالي[٨٧]: المملكة العربية السعودية في المركز الأول، الامارات العربية المتحدة في المركز الثاني، سلطنة عمان في المركز الثالث، جمهورية مصر العربية في المركز الرابع[٨٨]، مما يعكس بدوره جهود واهتمام تلك الدول بحماية الأمن السيبراني، وقد توصلنا لمجموعة من النتائج والتوصيات هي:

أولاً- النتائج:

- كشف البحث عن اضطرار العديد من القطاعات في أغلب دول العالم إلى الاعتماد على تكنولوجيا المعلومات والاتصالات بشكل أكبر من ذي قبل؛ نظراً لما يشهده العالم من ثورة هائلة في نظم المعلومات خاصة بعد جائحة كوفيد-١٩.
- توصل البحث إلى زيادة الاهتمام بمكافحة جرائم تقنية المعلومات وبالأمن السيبراني نتيجة لزيادة الخسائر الناتجة عن الهجمات السيبرانية وتهديد الأمن القومي للدول والسلم والأمن الدوليين.
- وضح البحث تعاظم دور الأمم المتحدة وأجهزتها في تأمين سلامة استخدام التكنولوجيا وشبكات المعلوماتية، وتعزيز الأمن السيبراني العالمي، وأمن الفضاء الإلكتروني، واتخاذ التدابير كافة لمكافحة الجريمة السيبرانية.
- بين البحث مدي اهتمام الدول العربية بمواكبة التقدم الإلكتروني في شتي مجالات الحياة من جانب ومن جانب آخر اعتبار الأمن السيبراني أولوية وطنية، حيث تعمل الدول العربية علي تعزيز الأمن السيبراني عن طريق امتلاك بنية تحتية رقمية فائقة التطور ووسائل متقدمة للتصدي للهجمات الإلكترونية الخبيثة التي تستهدفها، وأصبح لديها معاييرها الوطنية للأمن السيبراني تحقق من خلالها أهدافها الاستراتيجية في حماية وتأمين مكتسباتها وإنجازاتها في مختلف القطاعات والمجالات بتوفير الحماية القانونية للأمن السيبراني عن طريق قوانين وقرارات وزارية، ومكافحة جرائم تقنية

---

[٨٧] ماجد سالم: الأمن السيبراني العراقي وأثره في قوة الدولة، مجلة العلوم التربوية والإنسانية، كلية الإمارات للعلوم التربوية، عدد (١٨)، ٢٠٢٢، ص٧٥ وما بعدها.

[88] See: Global Cybersecurity Index 2020. Measuring commitment to cybersecurity.ITU.UN. 2021.p29.

المعلومات، عن طريق الاعتماد علي التعاون الدولي من خلال الاتفاقيات الدولية ، والاستفادة من كافة التجارب والممارسات العالمية والإقليمية.

- **كشف البحث عن توفر بعض الآليات لمواجهة الهجمات السيبرانية أهمها:** التعاون بين الدول والمنظمات الدولية والإقليمية– التوعية المجتمعية– الاهتمام بسن قوانين حديثة مواكبة للتطور السريع في مجال تقنية المعلومات – الدعم السياسي والمؤسسي الاستراتيجي والتنفيذي–البحث العلمي والتطوير وتنمية صناعة الأمن السيبراني– الإعلان عن معايير الأمن السيبراني– إقرار سياسات وقائية ودفاعية– تأمين البنى التحتية للاتصالات والمعلومات– إقرار المسؤولية الدولية الناشئة عن الهجمات السيبرانية– تطبيق قواعد القانون الدولي الإنساني.– تبني العديد من الدول انشاء مراكز وطنية وإقليمية ، وبرامج مبنية علي استراتيجيات وخطط مدروسة للأمن السيبراني وابتكار طرق لمكافحة الهجمات السيبرانية مثل المملكة العربية السعودة ودولة الإمارات العربية المتحدة وسلطنة عمان وجمهورية مصر العربية– استقطاب الكوادر الوطنية المؤهلة والطموحة وتأهيلها، والعمل من أجل إيجاد بيئة استثمارية محفزة للابتكار في المجالات التقنية وداعمة من أجل تطوير الفرص الاستثمارية في مجالات التقنية والابتكار وتمويل البحث والتطوير، نتيجة لتصاعد اهتمام العالم بحماية البنية التحتية الرقمية، والرقابة الإلكترونية وسبل التصدي لاختراقات الإرهابيين، والحرب الإلكترونية، والإرهاب الإلكتروني، والهجمات الإلكترونية، والجريمة الإلكترونية.

ثانياً- التوصيات:

- تحديث دوري لقوانين واستراتيجيات حماية الأمن السيبراني: مثل القوانين التي تنظم عمليات مزودي خدمات الإنترنت والتي تحتاج إلى تحديث بشكل مستمر، مع إمكانية اعتماد نموذج التشريعات السيبرانية يكون قابلاً للتطبيق محليًا وعالميًا بالتوازي مع التدابير القانونية الوطنية والدولية المعتمدة، واستراتيجيات تساعد في القضاء على الخطر المحتمل من تلك الجرائم من خلال وضع آلية عالمية للمراقبة والإنذار والرد المبكر مع ضمان قيام التنسيق عبر الحدود، مع العمل علي إنشاء نظام هوية رقمي عالمي وتطبيقه، وتحديد الهيكليات التنظيمية اللازمة لضمان الاعتراف بالوثائق الرقمية للأفراد عبر الحدود الجغرافية، وبناء القدرات البشرية والمؤسسية لتعزيز

المعرفة في مختلف القطاعات وفي جميع المجالات المعلوماتية، لتتلاءم مع التكنولوجيات الجديدة، مع ضرورة قيام الدول بتشجيع قيام المزيد من الأبحاث من أجل زيادة فعالية تقنيات تطبيق القانون و اعتماد نظام عقوبات صارم.

- التطوير المستمر للتعاون بين الدول لاعتماد معايير وأدلة موحّدة لمكافحة الجرائم السيبرانية: مثل المساعدات المتبادلة في جمع حركة المعلومات واعتراضها، حيث أنه لا يوجد إجماع بين هذه الدول بشأن تعريف جرائم المعلوماتية وتحديدها بصورة دقيقة، لمنع المجرمين من استغلال البلدان التي لديها قوانين أقل صرامة؛ لأنهم يميلون إلى ارتكاب الجرائم الإلكترونية في البلدان ذات القوانين الأقل تشددًا، حيث يجد المجرم أنه من الأسهل ارتكاب الجرائم الإلكترونية في هذه البلدان.
- إنشاء مراكز وأجهزة دولية حديثة لحماية الأمن السيبراني لتوظيف خبراء من المتخصصين ذوي معرفة تقنية عالية ومواكبة أحدث التقنيات في هذا المجال، تتضمن مختبرات حديثة لجمع الأدلة الرقمية وتدريب المحققين.
- إشراك القطاع الخاص في حماية الأمن السيبراني لأنها ضرورية لمساعدة الحكومات من خلال تحسين الحماية الذاتية كخط دفاع أول لهذا القطاع، واعتماد الحلول التقنية المتقدمة والخطوات الإدارية الضرورية لحماية أمن المعلومات، خاصة لعدم قدرة حكومات البلدان النامية على امتلاك الموارد والتقنيات اللازمة لمكافحة الجرائم السيبرانية والتعامل معها.
- نشر الوعي العام بحماية الأمن السيبراني: من خلال التعريف بـ: التكنولوجيات الملائمة والتطوير المستمر للخبرات والقدرات – المخاطر الذي تخلقها التكنولوجيات المستجدة – تدابير حماية فعالة للأطفال من جميع أنواع الاستغلال على الإنترنت – المشاكل المستقبلية وكيفية معالجتها والتي قد تنتج عن التطورات في مجال تكنولوجيا المعلومات.
- تشجيع الابتكار والإبداع في مجال حماية الأمن السيبراني: حيث يجب على كافة الدول تنظيم مبادرات وطنية وسن تشريعات لرعاية وحماية المبتكرين حيث أن الواقع يرصد أن السبيل الوحيد لمكافحة الجرائم السيبرانية هو الأمن السيبراني.

المراجـــع

أولاً- المراجع العامة:

- د. أحمد فتحي سرور، القانون الدولي الإنساني، ط ٣، عمان :منشورات اللجنة الدولية للصليب الأحمر،٢٠٠٦.
- د. جان بكتيه، القانون الدولي الإنساني :تطوره ومبادئه، دار المستقبل العربي، القاهرة، ١٩٨٤.

ثانياً- المراجع المتخصصة:

- أحمد ناصف: دمج الأمن السيبراني في منظومة الأمن القومي: الأمن السيبراني والأمن القومي، جمعية إدارة الأعمال العربية، العدد ١٧٨، ٢٠٢٢.
- تقوى الرشدان: اجراءات التحقيق الابتدائي في جرائم الأمن السيبراني في القانون الأردني والاتفاقيات الدولية، كلية القانون جامعة اليرموك، ٢٠٢١.
- د. حازم الجمل: الحماية الجنائية للأمن السيبراني في ضوء رؤية المملكة ٢٠٣٠، مجلة البحوث الأمنية، مجلد٣٠، عدد٧٧، ٢٠٢٠.
- د.عادل عبد الصادق:
- الإرهاب الإلكتروني" القوة في العلاقات الدولية: نمط جديد وتحديات مختلفة": مركز الدراسات السياسية والاستراتيجية، القاهرة، ٢٠٠٩.
- العلاقات الدولية والفضاء الإلكتروني "دراسة في النظرية والتطبيق"، المركز العربي لأبحاث الفضاء الإلكتروني، القاهرة، الطبعة الثالثة، ٢٠١٦.
- د. علي العلي، د. علي حميد: تكتيكات الحروب الحديثة" الأمن السيبراني والحروب المعززة والهجينة"، الطبعة الأولي، العربي للنشر والتوزيع، القاهرة، ٢٠٢٣.
- د. فارس العمارات: الأمن السيبراني "المفهوم وتحديات العصر"، دار الخليج للنشر والتوزيع، الطبعة الأولي، ٢٠٢٢.
- ماجد عزيز إسكندر: التوظيف السياسي للهجمات السيبرانية ومخاطرها على الأمن القومي، مركز الإمارات للدراسات والبحوث الاستراتيجية، ٢٠٢٣.

ثالثاً- المجلات والدوريات العلمية:

- د. خالد المطيري: دور التشريعات الجزائية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي، مجلة البحوث الفقهية والقانونية، العدد ٣٨، يوليو ٢٠٢٢.
- رزق سمودي: حق الدفاع عن النفس نتيجة الهجمات الإلكترونية في ضوء قواعد القانون الدولي العام، مجلة جامعة الشارقة، مجلد ١٥ العدد ٢، ٢٠١٨.

- طلال العيسى، عدي عناب: المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مجلة الزرقاء للبحوث والدراسات الإنسانية–المجلد التاسع عشر، العدد الأول، ٢٠١٩.
- عائشة غنيمي: الدبوماسية الإلكترونية وضرورة التوعية العامة، مجلة السياسة الدولية، ١٦–٢–٢٠٢١.
- ماجد سالم: الأمن السيبراني العراقي وأثره في قوة الدولة، مجلة العلوم التربوية والإنسانية، كلية الإمارات للعلوم التربوية، عدد (١٨)، ٢٠٢٢.
- والت، ستيفن: العلاقات الدولية" عالم واحد ونظريات عدة"، ترجمة: منير كمال، مجلة الثقافة العالمية، عدد٨٩، أغسطس ١٩٩٨.
- وزارة الخارجية– معهد الأمير سعود الفيصل للدراسات الدبلوماسية: الأمن السيبراني: درع المملكة الواقي لحماية مصالحها الحيوية وبنيتها التحتية، مجلة الدبلوماسي، عدد ٩٠، ٢٠١٨.

رابعاً– الرسائل العلمية:

- أنس جميل اللوزي: مفهوم الضرورة العسكرية في القانون الدولي الإنساني، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، ٢٠١٤.
- أمل المشايخى: مستقبل الأمن السيبرانى فى سلطنة عمان: وجهات النظر والرؤى الوطنية والإقليمية، رسالة ماجستير، جامعة السلطان قابوس، ٢٠١٧.
- عبد الله يحي الزهراني: استراتيجيات الأمن السيبراني في ضوء التقنيات والتحديات الحديثة، دراسة مقارنة، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، كلية العلوم الاستراتيجية، السعودية، ٢٠٢٠.

خامساً– الوثائق:

- المادة (٣١) من دستور مصر ٢٠١٤.
- جامعة الدول العربية "المنظمة العربية لتكنولوجيا الاتصال والمعلومات"، الرؤية العربية للأمن السيبراني (الواقع– التحديات– الفرص)، تونس، ٢٠٢١.
- مجلس أوربا سلسلة المعاهدات الأوربية رقم ١٨٩.
- اللائحة العامة لحماية البيانات في الاتحاد الأوروبي (GDPR) في ٢٥ مايو ٢٠١٨.
- سلسة معاهدات مجلس أوربا،٢٠٢٢.
- الاتحاد الدولي للاتصالات: الوثيقة C20/65–A.

- قرارات الجمعية العامة للأمم المتحدة: ١٢١/٤٥ عام ١٩٩٠، ٧٠/٥٣ في ٤ ديسمبر ١٩٩٨، و٤٩/٥٤ في ١ ديسمبر ١٩٩٩، ٢٨/٥٥ في ٢٠ نوفمبر ٢٠٠٠، و١٩/٥٦ في ٢٩ نوفمبر ٢٠٠١ و٥٣/٥٧ في ٢٢ نوفمبر ٢٠٠٢ و٣٢/٥٨ في ١٨ديسمبر ٢٠٠٣، ٦٣/٥٥ في ٤ ديسمبر ٢٠٠٠، و١٢١/٥٦ في ١٩ ديسمبر ٢٠٠١، ٢٣٩/٥٧ في ٢٠ ديسمبر ٢٠٠٢و١٩٩/٥٨ في ٣٠ يناير ٢٠٠٤ بشأن «إنشاء ثقافة عالمية للأمن السيبراني، CCPCJ 16/2/2007 من أبريل ٢٠٠٧» (الفقرات ٧، ١٦)، ٥٩/٥٥ في ٤ ديسمبر ٢٠٠٠ والفقرة ٣٦ المرفقة بقرار الجمعية العامة ٢٦١/٥٦ المؤرخ ٣١ يناير ٢٠٠٢، ١٧٧/٦٠ بتاريخ ١٦ ديسمبر ٢٠٠٥، ١٧٧/٦٠ الفقرة ٢ التي دعت الحكومات لتنفيذ جميع التوصيات التي اعتمدها المؤتمر الحادي عشر، ١٧٨/٦٠، فقرة ١٧.
- قرار المجلس الاقتصادي والاجتماعي E/2007/20 بتاريخ ٢٦ يوليو ٢٠٠٧ "» (E/2007/30 وE/2007/SR.45)، ٢٦/٢٠٠٤ بتاريخ ٢١ يوليو ٢٠٠٤- ٤٢/٢٠٠٤.
- قرارات رئيس مجلس الوزراء المصري أرقام ٢٢٥٩ لسنة ٢٠١٤- ٢٣٢٨ لسنة ٢٠١٤- ١٤٤٧لسنة ٢٠١٥- ٨١ لسنة ٢٠١٥-١٦٣٠ لسنة ٢٠١٦- ٩٩٤ لسنة ٢٠١٧- ٢٧٦ لسنة ٢٠٢٠.
- قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨.
- قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠.
- قانون تنظيم الاتصالات الصادر بالمرسوم السلطاني رقم ٢٠٠٢/٣٠.
- قانون مكافحة الإرهاب الصادر بالمرسوم السلطاني رقم ٢٠٠٧/٨.
- قانون مكافحة غسل الأموال وتمويل الإرهاب الصادر بالمرسوم السلطاني رقم ٢٠١٠/٧٩.
- قانون المعاملات الإلكترونية الصادر بالمرسوم السلطاني رقم ٢٠٠٨/٦٩.
- المراسيم السلطانية العمانية أرقام: رقم ٢٠٠٦/٥٢ بإنشاء هيئة تقنية المعلومات- مرسوم سلطاني رقم ٢٠١١/١٢ بإصدار قانون مكافحة جرائم تقنية المعلومات- ٢٠٢١/٧٦ بالموافقة على انضمام سلطنة عمان إلى معاهدة المبادئ المنظمة لأنشطة الدول في ميدان استكشاف واستخدام الفضاء الخارجي، بما في ذلك القمر والأجرام السماوية الأخرى- المرسوم السلطاني رقم ٢٠٢١/٧٧ بالموافقة على انضمام سلطنة عمان إلى اتفاقية تسجيل الأجسام المطلقة في الفضاء الخارجي- المرسوم السلطاني رقم ٢٠٢١/٧٨ بالموافقة على انضمام سلطنة عمان إلى اتفاقية

إنقاذ الملاحين الفضائيين وإعادة الملاحين الفضائيين ورد الأجسام المطلقة إلى الفضاء الخارجي- المرسوم السلطاني رقم ٢٠٢١/٧٩ بالموافقة على انضمام سلطنة عمان إلى اتفاقية المسؤولية الدولية عن الأضرار التي تحدثها الأجسام الفضائية- ٢٠١١/١٢- ٢٠٢٢/٦ بإصدار قانون حماية البيانات الشخصية.

- المادة (٦٨) من النظام الأساسي للدولة الصادر بالمرسوم السلطاني رقم (٢٠٢١/٦).
- تعميم وزارة النقل والاتصالات وتقنية المعلومات رقم ٢٠٢٠/٣.
- القانون الأساسي للمنظمة الدولية للشرطة الجنائية (الانتربول)، المعتمد اثناء الدورة ٢٥ للجمعية العامة، فينا، عام ١٩٥٦، رقم الوثيقة I/CONS/GA/1956(2008).
- الاستراتيجية الوطنية المصرية للأمن السيبراني (٢٠١٧- ٢٠٢١).
- قانون حماية الأمن السيبراني في أوكرانيا رقم (٤٥) لسنة ٢٠١٧- المادة (٥/١).
- Department of Defense. Instruction No.8500.01. Cybersecurity. 2014.United States of America.
- Global Cybersecurity Index 2020. Measuring commitment to cybersecurity.ITU.UN. 2021.p29
- ITU: Global Cybersecurity Index 2020.
- The European Union Agency for Network and Information Security (ENISA): Definition of Cybersecurity - Gaps and overlaps in standardization, V1.0, DECEMBER, 2015.

سادساً- الأحكام القضائية:

- حكم المحكمة الأوروبية لحقوق الإنسان بأن بيانات الهاتف ورسائل البريد الإلكتروني واستخدام الإنترنت، (كوبلاند ضد المملكة المتحدة، ٢٠٠٧، الصفحتان ٤١ و٤٢).
- حكم المحكمة الأوروبية لحقوق الإنسان " Wieser and Bicos Beteiligungen GmbH " ضد النمسا، الفقرة ٤٥.
- حكم المحكمة الأوروبية لحقوق الإنسان (س) و (ماربر) ضد المملكة المتحدة في القضيّة عدد ٠٤/٣٠٥٦٢ عام ٢٠٠٨.

- حكم محكمة البلدان الأمريكية لحقوق الإنسان في قضية تريستان دونوسو ضد بنما وإيشر وآخرون ضد البرازيل (٢٠٠٩).
- حكم المحكمة الأوربية لحقوق الإنسان:

- CASE OF ROTARU v. ROMANIA, (Application no. 28341/95).

سابعاً– المراجع الإلكترونية:

- الموقع الرسمي للمركز العربي الإقليمي للأمن السيبراني في دول الخليج، منشور علي:

https://arcc.om/(30/6/2023).

- الاتحاد الدولي للاتصالات منشور علي:

- https://www.itu.int/ar/about/Pages/default.aspx (2/7/2023)

- الجهاز القومي لتنظيم الاتصالات منشور علي:

- https://www.tra.gov.eg/ar (28/6/2023).

- معهد الأمن والتكنولوجيا (IST) الموقع الرسمي على الرباط التالي:

- https://aws.amazon.com/ar/compliance/nist/(29/6/2023).

- اللجنة الدولية للصليب الأحمر : الحرب السيبرانية والقانون الدولي الإنساني، منشور علي:

- https://www.icrc.org/ar/document/ (1/7/2023).

- الموقع الرسمي للمركز الوطني المصري للاستعداد لطوارئ الحاسبات والشبكات EG-CERT، على الرباط التالي:

-https://egcert.eg/ar/(30/6/2023)

- JuliaVoo (& others), National Cyber Power Index 2020 Methodology and Analytical Considerations, China Cyber Policy Initiative, Belfer Center for science and International Affairs, Harvard Kennedy School, https://www.belfercenter.org/sites/default/files/2020-09/NCPI.pdf accessed on 02/07/2023.

- المركز الوطني للسلامة المعلوماتية الموقع الرسمي منشور علي:

-https://omanportal.gov.om/(1/7/2023).

- مجمع الابتكار، منشور علي:

-https://www.trc.gov.om/(1/7/2023)

- المركز الوطني للسلامة المعلوماتية: برنامج صناعة الأمن السيبراني"حداثة)، منشور علي:

https://cert.gov.om/sp/hadatha (1/7/2023).

- هيئة تنظيم الاتصالات والحكومة الرقمية (TDRA)، الاستراتيجية الوطنية للأمن السيبراني، منشور علي:

https://tdra.gov.ae/ar/national-cybersecurity-strategy (1/7/2023).

- الهيئة الوطنية للأمن السيبراني: الاستراتيجية الوطنية للأمن السيبراني، منشور علي:

- https://www.nca.gov.sa/strategic (1/7/2023).

ثامناً- المراجع الأجنبية باللغة الانجليزية:

- African Union Convention on Cyber Security and Personal Data Protection, Malabo, 27th June 2014.
- CH.Ronsseau :La responsabilité international 1959-1960.
- Micheal Newton & Larry May, Proportionality in International Law, Oxford University Press, 2014; Arbitral Award in the Naulilaa Case 1928, 2 Reports of the International Arbitral Awards 1011-1028.
- Paulo Shakarian and others, Introduction to Cyber-warfare A Multidisciplinary Approach, (USA: Syngress, Elsevier, 2013, p. 2).
- Richard A. Clarke and Robert Knake, Cyber War: The Next Threat to National Security and What to Do About It, (New York: Harper Collins, 2010), p.6.