مجلة جامعة الانبار للعلوم القانونية والسياسية

اسم المقال: مفهوم الأمن السيبراني وعلاقته بالذكاء الاصطناعي (دراسة تحليلية قانونية)
اسم الكاتب: أ.م.د. حسام عبد الأمير خلف، وهج علي حمزه
رابط ثابت: https://political-encyclopedia.org/index.php/library/6302
تاريخ الاسترداد: 2026/11/03 10:41 +03

الموسوعة السياسيّة هي مبادرة أكاديمية غير هادفة للربح، تساعد الباحثين والطلاب على الوصول واستخدام وبناء مجموعات أوسع من المحتوى العلمي العربي في مجال علم السياسة واستخدامها في الأرشيف الرقمي الموثوق به لإغناء المحتوى العربي على الإنترنت.
لمزيد من المعلومات حول الموسوعة السياسيّة - Encyclopedia Political، يرجى التواصل على info@political-encyclopedia.org

استخدامكم لأرشيف مكتبة الموسوعة السياسيّة - Encyclopedia Political يعني موافقتك على شروط وأحكام الاستخدام المتاحة على الموقع https://political-encyclopedia.org/terms-of-use

تم الحصول على هذا المقال من موقع مجلة جامعة الانبار للعلوم القانونية والسياسية ورفده في مكتبة الموسوعة السياسيّة مستوفياً شروط حقوق الملكية الفكريّة ومتطلبات رخصة المشاع الإبداعي التي ينضوي المقال تحتها.

Journal of Anbar University for Law and Political Sciences
مجلة جامعة الانبار للعلوم القانونية والسياسية
P. ISSN: 2706-5804 E.ISSN: 2075-2024
Volume 13- Issue 2- December 2023 المجلد ١٣- العدد ٢ – كانون الاول ٢٠٢٣

The concept of cybersecurity and its relationship to artificial intelligence from the perspective of public international law (Legal Analytical Study)

[1] Assist. Prof. Dr.Hussam Abdul alameer Khalaf [2] Wahaj Ali Hamza
[1] college of Law /Baghdad University

1: Email: wahaj.ali1204a@colaw.uobaghdad.edu.iq
2: Email: dr.hussam@colaw.uobaghdad.edu.lg

DOI
10.37651/aujlps.2023.143654.1086

Submitted: 29/9/2023
Accepted: 10/10/2023
Published: 05/12/2023

Keywords:
cyber security
artificial intelligence
public international law
Cyber espionage
cyber threats.

Abstract:

This study deals with an important and vital topic, which is cybersecurity and its relationship to artificial intelligence from the perspective of international law. The first topic deals with the definition of cybersecurity, which refers to the protection of electronic systems, networks and data from cyber threats. A very difficult challenge in the era of technological progress.

The study then focuses on the relationship of artificial intelligence with cybersecurity, as the second topic in the branch sheds light on the integration of artificial intelligence in the field of cybersecurity, where advanced improvements in artificial intelligence can be used to improve the ability of systems to detect and address threats more effectively and quickly, and the branch deals with The second part of the second topic is the determinants of the impact of artificial intelligence on cybersecurity, as artificial intelligence provides multiple opportunities to improve cybersecurity, but it also poses new challenges and risks such as the increase in the development of advanced cyber-attacks. Countries and institutions must develop a strong international legal framework to deal with these new challenges and threats . related to cyber security and the use of artificial intelligence in a responsible and ethical manner

©Authors, 2023, College of Law University of Anbar. This is an open-access article under the CC BY 4.0 license (http://creativecommons.org/licenses/by/4.0/).

مفهوم الأمن السيبراني وعلاقته بالذكاء الاصطناعي (دراسة تحليلية قانونية)

[١] أ.م. د حسام عبد الأمير خلف [٢] وهج علي حمزه
[١] كلية القانون / جامعة بغداد

الملخص:

تتناول هذه الدراسة موضوع هام وحيوي الا وهو الأمن السيبراني وعلاقته بالذكاء الاصطناعي من منظور القانون الدولي، إذ يتناول المبحث الأول تعريف الأمن السيبراني الذي يشير إلى حماية الأنظمة الإلكترونية والشبكات والبيانات من التهديدات السيبرانية، وتُسلط الضوء على خصائص الأمن السيبراني ومنها التنوع والتعقيد والديناميكية، مما يجعله تحدياً بالغ الصعوبة في عصر التقدم التكنولوجي.

كما تركز الدراسة بعد ذلك على علاقة الذكاء الاصطناعي بالأمن السيبراني، إذ سلط المبحث الثاني الضوء على تكامل الذكاء الاصطناعي في مجال الأمن السيبراني، حيث يمكن استخدام التحسينات المتقدمة في الذكاء الاصطناعي لتحسين قدرة الأنظمة على اكتشاف ومعالجة التهديدات بشكل أكثر فعالية وسرعة ، ويتناول إضافة الى محددات تأثير الذكاء الاصطناعي على الأمن السيبراني، حيث يتيح الذكاء الاصطناعي فرصاً متعددة لتحسين الأمان السيبراني، ولكنه يشكل أيضاً تحديات ومخاطر جديدة مثل زيادة تطور الهجمات السيبرانية المتطورة ، مما يتعين على الدول والمؤسسات تطوير إطار قانوني دولي قوي للتعامل مع هذه التحديات والتهديدات الجديدة المرتبطة بالأمن السيبراني واستخدام الذكاء الاصطناعي بطريقة مسؤولة وأخلاقية .

الكلمات المفتاحية:

الأمن السيبراني، الذكاء الاصطناعي، القانون الدولي العام، التجسس السيبراني، التهديدات السيبرانية.

المقدمة

اولاً: التعريف بموضوع الدراسة

يمكن للذكاء الاصطناعي أن يكون له تأثير مزدوج في مجال الأمن السيبراني، فمن ناحية يمكن استخدام الذكاء الاصطناعي لتعزيز الأمن السيبراني وحماية البيانات، عبر تحليل البيانات والكشف عن أنماط غير طبيعية للكشف عن هجمات إلكترونية والتصدي لها قبل حدوث أي ضرر، كما يمكن أيضاً استخدامه في تعافي الأنظمة بعد الهجمات وإزالة البرامج الضارة والتهديدات.

من ناحية أخرى، يمكن أن يستخدم الذكاء الاصطناعي في أغراض خبيثة ويشكل تهديداً للأمن السيبراني، إذ يستخدم المتسللون الذكاء الاصطناعي لاختراق الأنظمة وتنفيذ هجمات متطورة، ويمكن استخدام الروبوتات والأنظمة المدعومة بالذكاء الاصطناعي للاستغلال والتجسس او إثارة البلبلة من خلال إنشاء حسابات مزيفة ونشر محتوى مضلل عبر وسائل التواصل الاجتماعي.

لذا، اصبح من الضروري أن يتعامل القانون الدولي مع هذه التحديات والتهديدات في مجال الأمن السيبراني واستخدام الذكاء الاصطناعي، إذ يجب أن يوفر القانون الدولي إطاراً قوياً للحماية السيبرانية وتنظيم الاستخدام المسؤول للذكاء الاصطناعي في هذا المجال، كما ينبغي تحديد المسؤولية والشفافية والمساءلة في استخدام التقنيات الذكاء الاصطناعي، بما يحترم حقوق البشر والخصوصية ويضمن عدم استغلاله لأغراض خبيثة.

ثانياً: هدف الدراسة

ان أهداف الدراسة تتمحور حول تحقيق رؤية متكاملة حول مفهوم الأمن السيبراني وعلاقته بالذكاء الاصطناعي وتطبيقها في إطار القانون الدولي إذ يهدف المبحث الأول إلى توضيح مفهوم الأمن السيبراني وأهميته في إطار القانون الدولي ، اما المبحث الثاني يهدف إلى فهم كيف يمكن أن يساهم الذكاء الاصطناعي في تعزيز الأمن السيبراني، إذ سيتم استعراض تكامل الذكاء الاصطناعي مع الأمن السيبراني وتحليل تأثيره على التحليل والاستجابة للتهديدات السيبرانية.

ثالثاً: إشكاليات الدراسة

ان دراسة موضوع أمن السيبراني وعلاقته بالذكاء الاصطناعي تواجه تحديات قانونية عديدة في السياق الدولي، تتضمن هذه التحديات نقص القوانين الدولية المتعلقة بأمن السيبراني، والتوازن بين التقدم التكنولوجي والتطور التشريعي وقضايا السيادة والخصوصية، كما يشكل استخدام التكنولوجيا السيبرانية والذكاء الاصطناعي تحديات قانونية فيما يتعلق

بالسيادة الوطنية وحقوق الخصوصية، لذلك يجب أن نبحث في كيفية تطبيق مبادئ القانون الدولي لحماية الدول والأفراد من التهديدات السيبرانية وضمان احترام السيادة والخصوصية.

رابعاً: تساؤلات الدراسة

تتضح مشكلة الدراسة من خلال الإجابة على التساؤلات الاتية:

١- ما هو التعريف القانوني والتقني لأمن السيبراني والذكاء الاصطناعي؟ وماهي أهمية الأمن السيبراني في إطار القانون الدولي؟

٢- كيف يمكن توضيح العلاقة بين الذكاء الاصطناعي وأمن السيبراني؟ هل يعد الذكاء الاصطناعي أداة لتعزيز أمن السيبراني، أم أن له تأثيرات محددة على تلك الأمنية؟

٣- كيف يتم تكامل الذكاء الاصطناعي في مجال أمن السيبراني؟ هل يمكن استخدام تقنيات الذكاء الاصطناعي في اكتشاف ومواجهة التهديدات السيبرانية بشكل أفضل؟

٤- ما هي المحددات التي تؤثر في تأثير الذكاء الاصطناعي على أمن السيبراني؟ هل تتعلق هذه المحددات بقدرات التعلم والتكيف الذاتي للذكاء الاصطناعي في مجال الأمن السيبراني؟

خامساً: خطة الدراسة

وفقاً لما تقدم تم تقسيم هذا الموضوع وفق خطة منهجية تتضمن مبحثين وفقاً للاتي:

- المبحث الأول: ماهية الأمن السيبراني واهميته في القانون الدولي .
- المبحث الثاني : علاقة الذكاء الاصطناعي بالأمن السيبراني.

وفي الختام سوف نستعرض اهم ما تم التوصل اليه من استنتاجات وتوصيات وفقاً لرؤيتنا المتكاملة حول الموضوع.

I. المبحث الأول

ماهية الأمن السيبراني واهميته في القانون الدولي

لقد نتج عن الحرب الباردة العديد من التهديدات الحديثة العابرة للحدود و التي لا تعترف بالسيادة الوطنية لأي دولة على اقليمها، الأمر الذي دفع الى حصول تحولات في مجال الدراسات القانونية والأمنية ، وجعل من الأمن السيبراني مطلباً ضرورياً لكافة الدول بلا استثناء، لكونه يختص بحماية امنها القومي والمعلوماتي من كافة المخاطر محتملة الوقوع عن طريق مصادر خارجية بواسطة الانترنت ، اذ يقوم الأمن السيبراني بضمان عدم السماح لأحد غير مصرح له بالدخول او الوصول الى المعلومات الخاصة بها ، فالمتسللون الذين يقومون بالجرائم السيبرانية يستخدمون الأنظمة الذكية لنشر الفيروسات ونسخ المعلومات السرية الحساسة الخاصة بالدول والمنظمات وتحريفها ، لذلك فان مهمة الأمن السيبراني تكمن في حماية امن الدول القومي والمعلوماتي من الهجمات السيبرانية الذكية ، باعتباره الركيزة الأساسية لأي مجتمع إذ من غير الممكن تصور تقدم أي دولة وازدهارها بدون تحققه ، إذ

تحول الأمن مع تزايد النشاطات في الفضاء السيبراني الى واحد من قطاع الخدمات التي تعد دعامة أساسية لأنشطة الحكومات والمنظمات على حد سواء ، ووفقاً لما تقدم نجد انه من الضروري توضيح المقصود بالأمن السيبراني وماهي أهميته في إطار القانون الدولي وفقاً لما يأتي :

المطلب الأول : تعريف الأمن السيبراني

المطلب الثاني : اهمية الأمن السيبراني في إطار القانون الدولي

I.أ. المطلب الأول

تعريف الأمن السيبراني

ان ظهور الثورة التكنلوجية الرقمية الحديثة والتي كانت نتيجتها زيادة المعلومات بصورة كبيرة، بسبب التعدد الهائل في وسائل الاتصالات ونظم الحاسوب وغيرها من نظم المعلومات، برز المفهوم الخاص بالأمن السيبراني حتى يكون محور للجانب الأمني الذي يختص بحماية قاعدة البيانات والمعلومات، ويمكن تعريف الأمن السيبراني كما يلي:

اولاً: على المستوى اللغوي والاصطلاحي

لغوياً: أن الأمن السيبراني ما هو الا مصطلح مكون من مقطعين الا وهما (الأمن) و (السيبراني).

فالأمن: يقصد به المعنى المناقض لكلمة الخوف ويرجو به السلامة، وهو مصدر الفعل امن امناً اماناً بفتحهما، وامنا وامنه محركتين وامنا بالكسر، فهو امن وامين، ويقصد بالأمن الاطمئنان الذي يصيب النفس ويسكن به القلب ويزول به الخوف واحياناً يقال أمن من الشر ويعني سَلِمَ منهُ[١]، والأمن يدل على الثقة او الطمأنينة [٢] .

اما السيبراني: فأن أصل كلمة السيبرانية تعود الى اللغة اليونانية ويراد بها السيطرة او التحكم وهي كلمة مشتقه من كلمة (Kybernetes) والتي يراد بها الشخص الذي يقوم بالتحكم بالدفة الخاصة بالسفينة [٣] ، وقد اطلقت هذه الكلمة مجازاً على الشخص المسيطر او المتحكم[٤] ، ونفهم من ذلك ان مصطلح السيبرانية يعنى به التحكم عن بعد ، فعندما تأتي هذه

---

(١) دحان حزام ناصر القريطي، *الأمن السيبراني وحماية أمن المعلومات*، (الإسكندرية: دار الفكر الجامعي، الطبعة الاولى، ٢٠٢٢)، ص١١.

(٢) ابراهيم ابو خزام، *الحرب وتوازن القوى*، (بنغازي: دار الكتاب الجديدة المتحدة، الطبعة الاولى، ٢٠٠٩)، ص ٧٦.

(٣) جيجان أ. ش، "التأثير السيبراني في الامن القومي للدول الفاعلة (الولايات المتحدة الاميركية انموذجاً". *مجلة العلوم السياسية*، (٦٤)، (٢٠٢٢): ١–١٨. https://doi.org/10.30907/jcopolicy.vi64.628 ، ص ٤.

(٤) فارس محمد العمارات، الأمن السيبراني، *المفهوم وتحديات العصر*، (الاردن: دار الخليج للنشر والتوزيع، الطبعة الاولى ،٢٠٢٢)، ص١٤.

اللفظة مع كلمة ثانية فذلك يعني الادارة عن بعد مثل ما هو موجود حالياً في الأمن السيبراني[١].

ويرى البعض ان مصطلح السيبرانية يرجع بالأصل الى العالم "Norbert Wieners " والذي استخدمها للتعبير عن التحكم التلقائي في عام ١٩٤٨ بمؤلفه الموسوم (Cybernetics or Control and Communication in the Animal and the machine) وبعد الحرب استعاض عن مصطلح الآلة بالكمبيوتر [٢].

اما اصطلاحياً يعد مصطلح الأمن السيبراني من المصطلحات الحديثة التي تعددت التعريفات بشأنه حسب الزاوية التي ينظر اليه من خلالها:

فقد عرف ريتشارد كمرر (Richard Akemmerer) [٣] الأمن السيبراني على انه " وسائل دفاعية من شأنها كشف واحباط المحاولات التي يقوم بها القراصنة " [٤].

وعرف ادوارد امورسو الأمن السيبراني (Amorso Edward) على انه " مجموعة وسائل من شأنها الحد من خطر الهجوم الواقع على البرمجيات واجهزة الكمبيوتر او الشبكات وتشمل الوسائل والادوات المستخدمة في مواجهه القرصنة وكشف الفايروسات وايقافها " [٥].

في حين عرفه اخرون بأنه " مجموعة من الوسائل التقنية والتنظيمية والادارية المستخدمة لمنع الوصول غير المصرح به ، وسوء الاستغلال واستعادة كافة المعلومات الالكترونية ونظم الاتصالات والمعلومات التي تحتويها ، وذلك لضمان استمرارية عمل النظم الخاصة بالمعلومات والعمل على تعزيز حماية و سرية المعلومات واتخاذ كافة التدابير اللازمة لحماية المواطن والمستهلكين من المخاطر في الفضاء السيبراني"[٦].

وقد ذهب فريق من الفقهاء بتعريفه على انه " الدفاع الذي يستهدف حماية الفضاء الالكتروني من كل الهجمات الموجهة اليه سواء كانت من الداخل ام الخارج " [٧] . كما ذهب البعض الاخر في تعريفه على انه " سلاح استراتيجي موجود في يد الحكومة والافراد لاسيما

---

(١) اسراء شريف جيجان، "الأمن السيبراني الصيني: دراسة بالدوافع والاهداف"، *مجلة قضايا سياسية*، العدد ٦٥، (٢٠٢١): ص٣٦.

(٢) دحان حزام ناصر القريطي، مصدر سابق، ص ١٢.

(٣) وهو أحد المتخصصين في مجال الأمن السيبراني والذي حصل على دكتوراه من جامعة كاليفورنيا عام ١٩٧٩.

(4) Richard Kemmererm, University of California Santa Barbara, Department of Computer Science , Volume 1,2003, p.3.

(٥) فارس العمارات، مصدر سابق، ص١٥.

(٦) امنة علي البشير محمد، "الأمن السيبراني في ضوء مقاصد الشريعة"، *مجلة كلية الدراسات الاسلامية والعربية للبنات الاسكندرية*، المجلد ١، العدد ٣٧، (بلا سنة نشر): ص٤٦٠.

(٧) عبد الرحمن علي اللقاني، *دور الأمن السيبراني في تعزيز امن المعلومات المالية الالكترونية*، (دار اليازوري العلمية، الطبعة الأولى، ٢٠٢٢)، ص١٢٦.

ان الحرب السيبرانية ماهي الا جزء لا يتجزء من التكتيكات الحديثة للحرب والهجمات بين الدول" [١].

من خلال العرض السابق لأبرز التعريفات المقدمة للأمن السيبراني نجد انها قد انطوت على مجموعة من القصور، إذ ركزت بعضها على الطرق او الوسائل التي يستعان بها للدفاع او التصدي لعمليات القرصنة الواقعة على أجهزة الكمبيوتر دون الاخذ بنظر الاعتبار التهديدات التي يمكن ان تشكلها على المستوى الدولي، في حين ركز البعض على خصائص وعناصر الامن السيبراني وجعل اثارها مقتصرة على المواطنين والمستهلكين دون الاهتمام للأمن القومي ، اضافة لذلك نجد ان بعض التعريفات أعلاه قد حصر الأمن السيبراني في كونه سلاح فقط ، وكما هو معلوم لدى الجميع ان مصطلح السلاح يشتمل على مفاهيم ابعد مما هي علية في الأمن السيبراني، الذي من شأنه تحقيق الحماية من دون المخاطر التي تتسبب بها الأسلحة الذي وصف بوصفها.

ختاماً، نجد ان التعريف الأكثر ملائمة للأمن السيبراني هو النشاط الذي من شأنه تأمين الحماية لكافة الموارد سواء كانت بشرية او مالية او تلك الموارد المرتبطة ارتباطاً وثيقاً بالتقنيات الخاصة بالاتصالات والمعلومات، ويضمن ايضاً الحد من الخسائر المتحققة في حال حصول التهديدات كما يتيح إمكانية إعادة الحال الى ما كان علية بأسرع وقت ممكن .

ثانياً: على المستوى القانوني فقد كانت هناك محاولات عديدة لتعريف الأمن السيبراني إذ تم اقتراح العديد من التعريفات وهي كالاتي:

فقد عرف الاتحاد الدولي للاتصالات (ITU) الأمن السيبراني على انه "جمع من الأدوات والسياسات والمفاهيم الأمنية والمبادئ التوجيهية وأساليب إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات والضمان والتقنيات التي يمكن استعمالها لحماية البيئة السيبرانية وأصول المنظمات والمستخدمين"[٢].

في حين ان وكالة الأمن الرقمي الاوربية، التي تعد اول من أصدر قانون الاتحاد الاوربي للأمن السيبراني عام (٢٠١٨)[٣] ، قد عرفته على انه "قدرة النظام المعلوماتي على التصدي

(١) اوس مجيد غالب العوادي، *الأمن المعلوماتي السيبراني*، (بيروت: مركز البيان للدراسات والتخطيط، ٢٠١٦)، الطبعة الأولى، ص٦.

(٢) تقرير صادر عن الاتحاد الدولي للاتصالات، التابع للأمم المتحدة عام ٢٠١٠. وراجع ايضاً:
خالد ظاهر عبد الله، "دور التشريعات الجزائية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي"، *مجلة البحوث الفقهية والقانونية*، العدد ٣٨ ،(٢٠٢٢): ص٩٩٥.

(٣) عادل عبد الصادق، *الرقمنة والمرونة السيبرانية حالة المنطقة العربية مصر وتونس والمغرب*، (القاهرة: (القاهرة: المركز العربي لأبحاث الفضاء الالكتروني، الطبعة الاولى، ٢٠٢١)، ص٢٩.

لمحاولات الاختراق والحوادث غير المتوقعة التي من شأنها استهداف البيانات المتداولة او المخزونة وفق إطار توافقي"[١] .

كما عرفة الاعلان الاوربي بأنه " قدرة النظام المعلوماتي على مقاومة الاختراقات، التي من شأنها استهداف البيانات " [٢].

اما اقليمياً فقد وردت العديد من التعريفات الخاصة بالأمن السيبراني، فعلى صعيد البلدان الاجنبية نجد وزارة الدفاع الامريكية (البنتاغون) قامت بتعريفه على انه " جميع الاجراءات التنظيمية الواجبة لضمان حماية المعلومات المختلفة بكافة اشكالها سواء كانت مادية ام إلكترونية من مختلف الجرائم كالهجمات والتجسس والتخريب والحوادث وغيرها " [٣] .

اما في فرنسا فقد قامت الوكالة الوطنية الفرنسية لأمن أنظمة الاعلام (ANSS) بتعريفة على انه مجموعة كاملة من السياسات والأنشطة التي تجرى في الفضاء الالكتروني والمتعلقة بالحد من التهديدات والضعف والردع والمشاركة الدولية والاستجابة للحوادث والمرونة والتعافي، بما في ذلك تشغيل شبكات الكمبيوتر وأمن المعلومات، ومهام إنفاذ القانون والدبلوماسية والعسكرية والاستخباراتية فيما يتعلق بأمن واستقرار العالم"[٤].

في حين ان المشرع الاردني قد عرفة في قانون الامن السيبراني رقم ١٦ لسنة ٢٠١٩ على انه " الإجراءات المتخذة لحماية الأنظمة والشبكات المعلوماتية والبنى التحتية الحرجة من حوادث الأمن السيبراني والقدرة على استعادة عملها واستمراريتها سواء أكان الوصول إليها بدون تصريح أو سوء استخدام أو نتيجة الاخفاق في اتباع الإجراءات الأمنية أو التعرض للخداع الذي يؤدي لذلك " [٥].

كما عرفة المشرع المغربي في قانون رقم ٠٥.٢٠ لسنه ٢٠٢١ المتعلق بالأمن السيبراني على انه "مجموعة من التدابير والإجراءات ومفاهيم الأمن وطرق إدارة المخاطر والأعمال والتكوينات وأفضل الممارسات والتكنولوجيات التي تسمح لنظام معلومات أن يقاوم أحداثاً مرتبطة بالفضاء السيبراني ، من شأنها أن تمس بتوافر وسلامة وسرية المعطيات

---

(١) جمال بوازديه ، "الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية والافاق المستقبلية"، *مجلة العلوم القانونية والسياسية*، المجلد ١٠، العدد ١٠، (٢٠١٩): ص١٢٦٦.

(٢) تامر عيسى فائق، "اثر مقومات الأمن السيبراني في خصائص المعلومات المحاسبية: الدور المعدل CoBit 2019"، (أطروحة دكتوراة ، كلية الدراسات العليا، جامعة العلوم الإسلامية العالمية ،٢٠٢١)، ص٢١.

(٣) زمورة جمال، "اهمية حوكمة الأمن السيبراني لضمان تحول رقمي امن للخدمات العمومية في الجزائر"، *مجلة البحوث الاقتصادية المتقدمة*، المجلد ٧، العدد ٢، (٢٠٢٢): ص٤١٦.

(4) Hugo Loiseau, Daniel Ventre, Cybersecurity in Humanities and Social Sciences,WILEY, Volume 1, p.36.

(٥) المادة (١)، من قانون الأمن السيبراني رقم ١٦ لسنة ٢٠١٩.

المخزنة أو المعالجة أو المرسلة والخدمات ذات الصلة التي يقدمها هذا النظام أو تسمح بالولوج إليه"[١].

وقد اورد المشرع الاماراتي تعريفاً للأمن السيبراني في قانون رقم ٣ لسنه ٢٠١٢ حول الامن السيبراني الا وهو " تأمين وحماية الشبكة المعلوماتية وشبكة الاتصالات ونظم المعلومات وعمليات جمع المعلومات باستخدام اي من الوسائل الالكترونية " [٢].

اما بالنسبة للمشرع الوطني العراقي ، نجد انه على الرغم من استخدام مصطلح الأمن السيبراني على المستوى التنفيذي ، الا انه لم يعرف الأمن السيبراني ولم يستخدمه ، وذلك لان القاعدة التشريعية المتمثلة بقانون جرائم المعلوماتية العراقي غير كاملة الى وقتنا الحالي ومعلقة ، لذلك نرى انه من الضروري العمل على استراتيجية وطنية تخص الأمن السيبراني العراقي بصورة تتوافق مع المنهج المتبع من قبل المنظمات الدولية المختصة كالاتحاد الدولي للاتصالات والاتفاقيات الدولية التي صادق العراق عليها مثل الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الموقعة في القاهرة بتاريخ ٢٠١٣/١٢/٢١ من اجل العمل على تعزيز التعاون بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات .

من خلال التعريفات المتقدمة نتوصل الى محصلة نهائية تتمثل بأن الأمن السيبراني ما هو الا كافة الإجراءات التنظيمية والقانونية التي يجب ان تتخذ من قبل الاجهزة الأمنية او الاجهزة الاخرى التابعة للدولة ، وذلك بهدف الحفاظ على سرية المعلومات الرقمية والحد من الاختراقات الواقعة، مهما كان منشؤها سواء كانت بواسطة الفيروسات او غيرها من الوسائل، لضمان وصولها للجهات المختصة في الوقت المناسب، وعدم وقوعها في ايدي الاشخاص غير المصرح لهم بالوصول.

I.ب. المطلب الثاني

أهمية الأمن السيبراني في إطار القانون الدولي

تزداد أهمية الأمن السيبراني طردياً مع زياده التوجه لاستخدام التكنولوجيا اذا اصبحت الدول ترتكز على التكنولوجيا بصورة اكبر من اي وقت مضى، وليس هناك اي مؤشرات من شأنها ان تشير الى ان هذا الاستخدام سوف يتباطأ او يتوقف، لكونه اصبح ضرورة ملحه بعد ان ظهرت الثورة الصناعية الرابعة او ما يعرف بثوره التقنيات ، لأن الفضاء السيبراني اصبح زاخراً بالمعاملات والتعاملات الالكترونية التي تحتاج الى تشفير وتامين على الصعيد الدولي، لاسيما ان اغلب المؤسسات الحكومية والعسكرية والشركات المالية والمصرفية والتي

(١) المادة (٢)، من قانون رقم ٠٥.٢٠ المتعلق بالأمن السيبراني لسنة ٢٠٢١.
(٢) المادة (١)، من قانون الأمن السيبراني الامارات، رقم ٣ لسنة ٢٠١٢.

تدخل بكافة المجالات تعمل على جمع ومعالجه وتخزين كميات ضخمه من البيانات على اجهزه الكمبيوتر(١).

و قد اشارت الجمعية العامة للأمم المتحدة لهذه الاهمية في بعض القرارات الصادرة عنها، لاسيما القرار ذو الرقم (٥٨/١٩٩) في ٣٠ كانون الثاني لسنه ٢٠٠٤ المتعلق بأنشاء ثقافة عالمية للأمن السيبراني والذي ينص على : " انشاء ثقافة عالمية للأمن السيبراني وحماية الهيكل الأساس للمعلومات والذي اعتمد من قبل الجمعية العامة للأمم المتحدة ، وأيضاً القرارين المرقمين (٥٥/٦٣) في ١ كانون الثاني لسنة ٢٠٠١ ، و(٥٦/١٢١) في ٢٣ كانون الثاني لسنة ٢٠٠٢ اللذان يرميان الى مكافحة سوء استعمال التكنلوجيا الخاصة بالمعلومات لأغراض إجرامية ، وكذلك قرارها رقم (٥٣/٧٣) في ٤ كانون الثاني لسنة ١٩٩٩ و الذي ينص على " دور العلم التكنولوجيا في سياق الامن الدولي، "الذي يبين ان للعلم والتكنولوجيا أهمية كبير في الإطار الخاص بالأمن الدولي والتسلح ، وغيرها من القرارات التي تتعلق بالتطورات الحاصلة في ميدان المعلومات والاتصالات في إطار الأمن الدولي(٢).

مع ذلك ان هذا التقدم التكنلوجي والمعرفي قد يؤدي الى اضعاف البنى التحتية للدول و يجعل منها هدفاً واضحاً للهجمات السيبرانية الإرهابية الغير مشروعة بموجب الاتفاقية الاوربية لقمع الإرهاب والبروتكول الملحق بها والتي اعتمدت في عام ١٩٧٧ (٣) ، ويعرضها لخطورة حقيقية متمثلة باستغلال نقاط الضعف التي تعتري انظمة المعلومات الخاصة بها، وتدمير هذه الانظمة من اجل تهديد امنها القومي، وهذا ما دفعها الى اللجوء للأمن السيبراني باعتباره وسيلة كفيلة بحمايه منظومه الدولة الالكترونية من اي هجوم سيبراني مهما كان منشؤه سواء كان اشخاص عاديين تم تجنيدهم من قبل التنظيمات الإرهابية (٤) او من قبل دوله أخرى من شأنه ان يؤدي الى تخريب القواعد الخاصة بالبيانات او سرقة هذه البيانات او استهداف البنى التحتية لدولة معينة(٥)، لذلك فان أهمية الأمن السيبراني على الصعيد الدولي يمكن توضيحها من خلال التطرق الى عدة جوانب أهمها ما يلي :

---

(١) منى عبد السمحان ، "متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية"، *مجلة كلية التربية، جامعة المنصورة*، العدد ١١١، (٢٠٢٠): ص١٢.

(٢) إيهاب احمد حسن، "الأمن السيبراني في اطار قواعد القانون الدولي العام"، (رسالة ماجستير، كلية القانون والعلوم السياسية، جامعة كركوك، ٢٠٢٢)، ص ٨.

(٣) خلف حسام عبد الامير، "التكامل بين القانون الدولي الجنائي والقانون الدولي الإنساني في مكافحة الإرهاب"، مجلة العلوم القانونية، ٣١ (٤)، (٢٠١٩): ١٨٧-٢٢٢. https://doi.org/10.35246/jols.v31is.106 ، ص ١٩٧.

(٤) الخاطري، راشد، وزايد علي، "تجنيد الأشخاص في التنظيمات الإرهابية تقنياته وأساليبه - القانون الإماراتي نموذجا "، *مجلة العلوم القانونية*، ٣٨ (١)، (٢٠٢٣): ٨٤-١٠٦. https://jols.uobaghdad.edu.iq/index.php/jols/article/view/638 ، ص ٩٥ .

(٥) وتشمل بالبنى التحتية: محطات الطاقة او المستشفيات او الشركات الخاصة بالخدمات المالية وغيرها.

اولاً: حماية خصوصية البيانات

تتجسد الأهمية في الحفاظ على سلامة المعلومات الخاصة بأشخاص القانون الدولي وتجانسها ، والوقاية من التهديدات التي تتعرض لها معلوماتهم الحساسة سواء كانت متعمدة ام غير متعمدة، والتخلص من الخطر والضرر الناتج عنها كالاختراق والتعطيل واتلاف قاعده البيانات(١).

مع تقدم الوقت نجد ان حكومات الدول ومؤسساتها العسكرية والمالية والصحية وغيرها ، تقوم بجمع وتخزين كميات كبيرة من المعلومات المهمة والحساسة على أجهزة الحاسوب والأجهزة الأخرى بصورة اكبر مما هي عليه في السابق ، ويشكل الوصول غير المسموح به الى هذه المعلومات اثار كبيرة ومدمرة ، لاسيما إذ كانت هذه المعلومات تنتقل بين اجهزة المؤسسات المختلفة للدولة الواحدة او الدول المتعددة عن طريق الشبكات ، وبسبب ارتفاع حدوث الهجمات السيبرانية فأن الدول والمنظمات تجد نفسها مضطرة لحماية معلومتها الخاصة من الهجمات السيبرانية والتجسس الرقمي اللذان يمثلان في الوقت الحالي اكبر تهديد للأمن القومي لأي دولة، اذ انه يفوق الخطر الناجم عن الإرهاب (٢)، ان الاستعانة بالأمن السيبراني الذي يقوم بحماية خصوصية البيانات والمعلومات خلال التصدي للفيروسات والبرامج الضارة والدفاع عنها ضد الهجمات الخاصة بخرق البيانات يؤدي الى التقليل من أنشطة الجرائم السيبرانية والتي ستزداد بصوره كبيره وسريعة مع مرور الوقت بظل التقدم التقني الهائل، ومن الجدير بالذكر ان البيانات التي يقوم الامن السيبراني بحمايتها هي بيانات حساسة يؤدي الكشف عنها الى نتائج ضاره سواء كانت على الصعيد الوطني او الدولي، سواء كانت ملكيه فرديه للأشخاص ام بيانات ماليه او خاصة بالأمن القومي للدولة .

ثانياً: مكافحة الجريمة

ان ظهور الاساليب الحديثة التي يلجأ لها مجرمي الانترنت لارتكاب جرائمهم السيبرانية ، إذ انهم قد يستهدفون بهجماتهم السيبرانية البنى التحتية الحيوية للدول ، من اجل الحصول على مكاسب سياسية او مالية من قبل جهات مختلفة غير معروفة في حال نجاح هذه الهجمات وهذا ما عزز الحاجة الى الأمن السيبراني لمواجهة الجرائم الجديدة ، ويعتمد نجاح هذه الهجمات باستغلال نقاط الضعف الموجودة في أنظمة الفضاء السيبراني في هذه البنى التحتية ، وان الامر الذي يزيد المسألة تعقيداً ويكسب الأمن السيبراني أهميته هو ان الجرائم السيبرانية تواجه دائماً مشكلة الا وهي صعوبة اسناد المسؤولية الدولية لمرتكب الجريمة، وايضاً عدم إمكانية التنبؤ بهذه الهجمات واتخاذ التدابير الاحترازية في الوقت الذي يتطلب منه اتخاذها لدرء الأخطار الناجمة عنها، وهذا كلة أدى الى تزايد الهجمات الناجحة لاسيما

(١) منى السمحان، مرجع سابق، ص ١٢.

(٢) مصطفى إبراهيم سلمان، "الأمن السيبراني واثرة في الأمن الوطني العراقي"، *مجلة العلوم القانونية والسياسية*، المجلد ١٠، العدد ١، (٢٠٢٢): ص١٥٨.

وانها تتسم بكونها غير مرئية [١] ، وفي هذا الخصوص تم ابرام الاتفاقية الاوربية لمكافحة الجريمة السيبرانية (بودابست) لعام ٢٠٠١ العديد من الاعمال غير المشروعة تحت عناوين معينة كالجرائم المرتكبة ضد سرية الانظمة والبيانات والجرائم التي تتصل بالأجهزة والجرائم الخاصة بالملكية الفكرية وغيرها .

ثالثاً: التصدي للهجمات السيبرانية

أن غالبية الدول المتطورة تجعل من الأمن السيبراني على راس أولوياتها، لاسيما بعد ظهور الحروب السيبرانية التي حصلت بين بعض الدول والتي اعتبرت حروباً عابرة للحدود الوطنية، لكونها تحدث في الفضاء الافتراضي للدول ويقصد بالفضاء الافتراضي هو الحيز المادي او غير المادي الذي يتكون من الحواسيب وأجهزة مكننة وشبكات ومعلومات محوسبة وبرامج ومضامين ومعطيات ومرور ورقابة والذين يستخدمون كل ذلك [٢] ، و تتراكم الامثلة التي من الممكن سوقها في هذا الشأن، والتي من الممكن ان توضح الخطورة الناجمة عن الهجمات السيبرانية المستقبلية وزيادة أهمية الأمن السيبراني، ومنها الهجوم السيبراني الذي وقع على دولة استونيا في عام ٢٠٠٧ ، والذي طال بنجاح البنى التحتية الخاصة بها، وذلك نتيجة حصول خلاف سياسي بين الاقلية الروسية والحكومة [٣] .

إذ حصل هجوم سيبراني أدى الى اغراق المواقع الالكترونية التابعة لها بكمية كبيرة من البيانات التي لا فائدة منها، بهدف الحاق الضرر بالعدو وتدمير بياناته الرقمية ، لاسيما تلك البيانات التي تم توظيفها لتنظيم البنى التحتية لكافة منشآت الدولة و على وجه الخصوص المنشآت العسكرية[٤] ، وقد وجهت هذه الهجمات من عدد من الحاسبات الموجودة في مختلف انحاء العالم ، إذ استهدفت العديد من مواقع الحكومة والصحف الرسمية والجامعات

---

(1) Tadas Limba and other, Cybersecurity management model for critical infrastructure, The National Journal Entrepreneurship and Sustainability, Volume 4, 2017, p. 561_563.

(٢) محمود لمى عبدالباقي و كيطان اسراء نادر، "المسؤولية الدولية عن الأضرار التي تسببها الهجمات السيبرانية"، *مجلة العلوم القانونية*، ٣٦ (ديسمبر)، (٢٠٢١): ٣٣٦_٣٦٢. https://doi.org/10.35246/jols.v36i0.435 ، ص ٣٣٩ .

(٣) وذلك بسبب قيام الاتحاد السوفيتي بوضع تمثال مصنوع من البرونز في العاصمة تالين اثناء الحرب العالمية الثانية ، و ان هذا التمثال يعد رمزاً واضحاً للاحتلال الحاصل من قبل الاتحاد السوفيتي، في حين ان روسيا عدت وضعه ما هو الا تكريماً للجنود اللذين كانوا ضحية الحرب ، ونتيجة لذلك قررت السلطات الاستوانيه ازالته لما اثارة من جدل ، الا ان هذا العمل استتبعه اعمال شغب واحتجاجات جماهيرية والتي عرفت باسم ليلة البرونزي ، انظر : حسام عبد الأمير خلف، "البعد الخامس في النزاعات المسلحة _الفضاء الالكتروني _"، *مجلة كلية الحقوق ، جامعة النهرين* ، مجلد ١٨ ، عدد ١، (٢٠١٦): ص١٢٥.

(٤) المالكي هادي نعيم وعبد مصطفى سالم، "النطاق المكاني للعمليات الحربية في النزاعات المسلحة الدولية"، *مجلة العلوم القانونية*، ٣١ (٤)، (٢٠١٧): ٢٨-٥٧. https://doi.org/10.35246/jols.v31is.100 ، ص٤٥.

والمستشفيات والمصارف وخدمات الإطفاء وذلك لغرض شل حركة الحكومة الاستوانية حتى لا تقوم بمهامها المطلوبة منها[١]، وهذه الهجمات السيبرانية قد اخذت صدى واسع وقد اطلق على هذه الهجمات الحرب السيبرانية الاولى في التاريخ، إذ اظهرت كيف يمكن استخدام انظمه الذكاء الاصطناعي وتقنياته لمهاجمة دولة حديثة والاعتداء على سيادتها الالكترونية وهذا من شأنه ان يهدد امنها القومي أيضاً، وتعريض الامن والسلم الدوليان إلى الخطر.

ويذكر في هذا المجال ايضاً الهجمات السيبرانية عام ٢٠١٠ التي استهدفت الأنظمة الخاصة بالمنشأة النووية الإيرانية وتم التلاعب بهذه الانظمة لأنهاء قدره الاسلحة النووية الإيرانية المتنامية وذلك كبديل عن عمليات التدخل العسكري [٢] ليس هذا فقط بل هناك العديد من الامثلة التي حصلت بهذا الشأن [٣] ، تعد جميعها إشارة صريحة لانتهاء حقبة الحروب التقليدية التي كان يستعمل اثنائها الأسلحة المتعارف عليها التي تتمثل بالأسلحة الثقيلة ، والاعلان عن بداية حقبة جديدة متمثلة بالحروب المعاصرة وهي الحروب السيبرانية [٤] ، وهي الحروب التي تدور الحروب في المجال الإلكتروني حيث يتم استخدام آليات وأسلحة إلكترونية في هجمات موجهة بشكل أساسي نحو أجهزة الكمبيوتر والشبكات الإلكترونية للأعداء أو الأنظمة الإلكترونية التي تديرها الدولة وتحتوي على معلومات حساسة. يهدف هذا الهجوم إلى عرقلة الخصم عن استخدام تلك الأنظمة والأجهزة أو تدميرها بالكامل [٥] ، لذلك نجد ان اغلب الدول في عامي ٢٠٠٣ و٢٠٠٥ نجد ان اغلب الدول قد قامت بالاتفاق في مؤتمر القمة العالمية الخاص بمجتمع المعلومات (WSIS) على وضع ادوات فعاله ومؤثره وتمتلك من الكفاءة ما يجعلها قادره على رفع مستوى التعاون الدولي بخصوص الأمن السيبراني ، فضلاً عن ذلك نجد ان العديد من الدول المتقدمة قد اقرت سياسيات للدفاع والوقاية من الهجمات السيبرانية وقد خصص البعض الاخر مثل الولايات المتحدة مبالغ طائله لمعالجة بعض المسائل الخاصة بحماية الامن السيبراني ، وهذا دليل على مدى اهتمام الدول في

---

(١) يحيى ياسين سعود، "الحرب السيبرانية في ضوء قواعد القانون الدولي الإنساني"، *المجلة القانونية، جامعة القاهرة، كلية الحقوق*، المجلد ٤، (٢٠١٨): ص٨٩.

(2) Luisa Dall'Acqua ,Transdisciplinary Perspectives on Risk Management and Cyber Intelligence , Volume1, 2020, p. 152.

(٣) وايضاً يذكر في هذا الإطار الهجوم السيبراني على شركة أرامكو السعودية في أواخر عام ٢٠١٦ والذي أدى الى مسح نظام ٣٥,٠٠٠ جهاز كمبيوتر تابع للشركة واتلافها، وايضاً تدخل روسيا سيبرانياً في الانتخابات الامريكية في عام ٢٠١٦ وتصوير الرئيس دونالد ترامب على انه عميل روسي، انظر: ايمان عصام مصطفى، *صورة أمريكا وروسيا في الخطاب الصحفي المصري*، (العربي للنشر والتوزيع: الطبعة الأولى، ٢٠٢١)، ص١١٧.

(٤) بن مرزوق عنترة، "البعد الالكتروني للسياسة الأمنية الجزائرية في مكافحة الإرهاب"، *مجلة العلوم الإنسانية والاجتماعية*، العدد ٣٨، (٢٠١٨): ص٣٦.

(٥) دهام ومحمد ومحمود خليل، "مشروعية استخدام الهجمات الإلكترونية في النزاعات الدولية والمسؤولية الدولية عنها"، *مجلة العلوم القانونية*، ٣٦ (٤)، (٢٠٢٢): ٦٧٨-٧٠٤. https://doi.org/10.35246/jols.v36i4.520 ، ص٦٩٥ .

الحفاظ على امنها السيبراني لأهميته، لاسيما أن العلاقات الدولية بين الدول مهددة بالهجمات السيبرانية [١].

نجد مما سبق ان التقدم التكنلوجي المتمثل بالأمن السيبراني له دور مهم في حياة كل من الدول والمنظمات والافراد ، لكونه يقوم بحماية معلوماتهم تجاه أي نوع من أنواع الهجمات السيبرانية، من خلال قيامه بالعمل على تأمين كافة الشبكات والأجهزة من اي اختراق محتمل الحصول والحفاظ على سرية هذه المعلومات ومنع الجهات غير المصرح لها بالوصول اليها ، ويتحقق ذلك من خلال العمل على تدريب وتزويد الافراد والأنظمة بعدة عمليات وانشطة وتوجيهها بما يناسب وينسجم مع القواعد القانونية الدولية الخاصة بحماية الأمن السيبراني والتصدي لأي اختراق او تهديد بكفاءة عالية .

II. المبحث الثاني

علاقة الذكاء الاصطناعي بالأمن السيبراني

ان البرامج التي يتم استعمالها في الوقت الحالي لحماية امن الدول والمنظمات والأشخاص من الهجمات السيبرانية ، أصبحت غير فعالة وذلك لعدم مواكبتها للأساليب التكنلوجية العصرية المستخدمة من قبل المتسللين الذين يستخدمون ابداعهم وتفكيرهم مع كل نظام جديد يتم الوصول اليه لكي يطورو هجماتهم السيبرانية بصورة مضادة له ، لذلك من الضروري اعتماد أساليب دفاعية من قبل الأمن السيبراني تقوم بالتعرف على الهجمات السيبرانية والتنبؤ بها ، وان اهم التقنيات التي من الممكن ان تؤدي هذا الدور هو الذكاء الاصطناعي الذي من شأنه العمل على كشف الهجمات السيبرانية والتنبؤ بها قبل حدوثها في إطار الأمن السيبراني ، ومن منظور اخر نجد ان استخدام الذكاء الاصطناعي في هذا المجال يؤدي الى ظهور حالة مزدوجة فهو من ناحية يعزز الأمن السيبراني وحمايته ومن ناحية أخرى يعمل على تعزيز قدرة الأسلحة السيبرانية المضادة ، لذا سوف نبحث في هذا المبحث بمدى تكامل الذكاء الاصطناعي مع الأمن السيبراني للدول والمنظمات والاشخاص في القانون الدولي وكيف يمكن للذكاء الاصطناعي ان يعزز المراقبة في الوقت الحقيقي لتهديدات الأمن السيبراني هذا من جانب ، اما من جانب اخر سوف نبحث في محددات تأثير الذكاء الاصطناعي على الأمن السيبراني وهذا من خلال تقسيم هذا المطلب الى ثلاث فروع وفق الاتي:

- **المطلب الأول : تعريف الذكاء الاصطناعي**
- **المطلب الثاني : تكامل الذكاء الاصطناعي مع الأمن السيبراني**
- **المطلب الثالث : محددات تكامل الذكاء الاصطناعي مع الأمن السيبراني**

(١) اسلام فوزي، "الابعاد الاجتماعية والقانونية: تحليل سوسيولوجي"، *المجلة الاجتماعية القومية*، المجلد ٥٦، العدد٢، (٢٠١٩): ص١١٣-١١٧.

II.أ. المطلب الأول

تعريف الذكاء الاصطناعي

قبل البدء في تعريف الذكاء الاصطناعي لابد من الاشارة الى تاريخ نشأه هذا المفهوم حتى يتسنى لنا فهمه وادراكه ، إذ يمكن إرجاع مصطلح الذكاء الاصطناعي Artificial (intelligence)[١] الى أربعينيات القرن الماضي عندما اقترح العالمان مكولوتش (McCullough) وبتس (Pitts) تطوير أول شبكة عصبية لكن لم يتم استخدامها بصوره رسمية ومباشرة [٢]، وفي عام ١٩٥٠ توصل العالم الآن تورنج (Alan Turing) الى اختبار سمي في بداية الأمر (Imitation game)[٣] وتمت تسميته بعد ذلك اختبار تورنج (Turing test)[٤]، ثم في عام ١٩٥٦ تمت صياغة مصطلح الذكاء الاصطناعي لأول مره اثناء مؤتمر دارتموث في هانوفر في الولايات المتحدة عند تأسيس احدى المدارس الصيفية في امريكا على يد اربعة باحثين الا وهم جون مكارثي (John McCarthy)، ومارفن مينيسكي (Marvin Minsky)، ناثانيل روتشستر (Nathaniel Rocheste) و كلود شانون (Claude Shannon)، على أنه قدرة النظام على التظاهر بشكل صحيح و التعلم من البيانات الخارجية و الاستفادة من التعلم لتحقيق أهداف محددة من خلال التكيف المرن [٥] ، وتعد هذه البداية الحقيقية لعصر الذكاء الاصطناعي لكونها جمعت العديد من كبار ذلك العصر، إذ نسب مصطلح الذكاء الاصطناعي الى العالم جون مكارثي (John McCarthy) لكونه اول من استعمله في ذلك الوقت.

ومع التقدم كل يوم، يتقدم الذكاء الاصطناعي بسرعة في جميع المجالات، وبما ان الذكاء الاصطناعي يمتاز بحداثة التعامل معه ضمن الاتجاهات التشريعية المختلفة فقد وردت

---

(١) يشار للذكاء الاصطناعي باختصار: (AI)

(2) Hugh McCullock and Walter Pitts, A logical calculus of ideas immanent in nervous activity. Archive copy of 27 november 2007 on wayback machine. Avtomaty Moscow, Inostr. (1956), p. 363–384.

(3) Jack Copeland, Diane Proudfoot, The Computer, Artificial Intelligence, and the Turing Test. In: Teuscher , Alan Turing: Life and Legacy of a Great Thinker, Springer, Berlin, Heidelberg, 2004، p. 135.

(٤) اختبار يقوم على تحديد امكانية الألة للقيام بسلوك ذكي يشبه الذكاء البشري وعلى اساس ذلك يتم تحديد درجة ذكائها، وتوصل العالم تورينج في ختام الامر الى نتيجة مهمه مودها ان الآلات التي تتمتع بالذكاء البشري يمكنها في الواقع ان تفكر وتتعامل مع المشكلات التي تواجهها كما يتعامل العقل البشري مع ذلك.

(5) Mohiuddin Ahmed, Explainable Artificial Intelligence for Cyber Security, Next Generation Artificial Intelligence, Springer، Volume1025، 2022, p.2.

الكثير من التعريفات بشأنه[١]، ولا يسع المجال لذكرها جميعاً وانما سوف نشير الى أبرز التعريفات التي قيلت في هذا المجال.

على المستوى العلمي، فقد عرفت عالمة الكمبيوتر الامريكية إلين ريتش Elaine (Rich) الذكاء الاصطناعي بأنه "دراسة الكيفية التي يتم بها توجيه الكمبيوتر للقيام بمهام التي يؤديها الانسان بصوره امثل وافضل"[٢]، كما عرفه الفيلسوف جون هوغلاند John (Haugeland) بأنه "عبارة عن جهد جديد مثير لجعل أجهزة الكمبيوتر تفكر"[٣]، اي انه اراد بيان ان الآلات لها عقول، بالمعنى الكامل والحرفي ، اما عالم الرياضيات الانجليزي ريتشارد إي بيلمان (Richard E. Bellman) فقد عرفه على انه "اتمته الأنشطة التي نربطها بالتفكير البشري، مثل اتخاذ القرار وحل المشكلات والتعلم"، ويعرّفه الدكتور مكديرموت (McDermott)بأنه "دراسة الكليات العقلية من خلال استخدام نموذج مفترض"[٤] ، اما عالم الحاسوب الانكليزي ريموند كرزويل (Raymond Kurzweil) فقد عرفه على انه "فكرة إنشاء آليات تؤدي وظائف تتطلب الذكاء عندما يؤديها الناس"[٥]، ويعرفه لوغر (Luger) على أنه "فرع من علوم الكمبيوتر يتعلق بأتمتة السلوك الذكي"[٦].

ونلاحظ مما تقدم ان التعاريف السابقة لمصطلح الذكاء الاصطناعي قد جاءت متنوعة ومختلفة في الاسس التي تقوم عليها إذ اشار هوغلاند وبيلمان إلى أن الذكاء الاصطناعي يهتم بعملية التفكير لاسيما التفكير المنطقي، اي انهم فسرو العقل كآلة مرتبطة تماماً بالتفكير البشري وهذا يعني أن أجهزة الكمبيوتر تفكر، لكن لوغر اهتم بالجوانب السلوكية للأنظمة، فبالنسبة له، ان اجهزة الكمبيوتر تتصرف بذكاء مثل البشر، علاوة على ذلك، يهتم ريموند كرزويل وإلين ريتش بقياس النجاح من ناحية الأداء البشري، وبالنسبة لهم، يمكن أن يُنسب

---

(١) يرجع المعنى اللغوي لمصطلح الذكاء الاصطناعي في اللغة العربية الى المصدر ذكاء: (اسم)، ذكاء: مصدر ذكي، ذكي: (فعل)، ذكي، يَذْكي، مصدر ذكاء ومنه ذكت النار اي توقد لهيبها، وذكت الشمس اي ارتفعت حرارتها، وذكت الحرب اي اشتدت، وذكت ريح المسك اي فاح عطره. ان الذكاء يعني كمال الشيء وتمامه، ويأتي منه الذكاء في الفهم اي الكمال في الفهم وسرعة القبول ومنه ايضاً الذكاء في السن والذي يعني تمام السن، ويقال ذكيت الشاه اي اتممت ذبحها. يُنظر: الخليل بن أحمد الفراهيدي: *كتاب العين مرتبا على حروف المعجم*، تحقيق، عبد الحميد هنداوي، ج٢، (بيروت: دار الكتب العلمية، ٢٠٠٢)، ص ٧٤.

(2) Rich, Elaine, Arficial Intellegeme, McGraw-Hill, Inc., Singapore, 1984, p. 1.

(3) Hangeland, Arial Intelligence TheVery Idea, MIT Press, USA, 1985, p. 4.

(4) Chamiak, Eugene & McDermott, Drew, Introduction to Artifical Intelligens, Addission Wesley Publishing Company, Canada 198, p. 6.

(5) Ray Kurzweil, The Age of Intelligent Machines, Dai Nippon, Japan, 1990, p 14. 14.

(6)Gorge Luger and Nathan Stubblefield, Arthaal Intelligence: Structures and Strategies for Complex Problem Sabang, Benjamin/Cummings, California, 1995, p. 2.

الذكاء الاصطناعي إلى الآلات، لكنه ينتمي أساساً إلى العقل البشري، اما مكديرموت فقد اهتم بالذكاء المثالي، إذ فسر الكليات العقلية من خلال استخدام النماذج الحسابية.

اما على المستوى الدولي ، فقد جاءت العديد من تعريفات الذكاء الاصطناعي في المواثيق الدولية كمذكرة لجنة الامم المتحدة للقانون التجاري الدولي في دورتها الحادية والخمسون لعام ٢٠١٨ ، إذ جاء تعريفه على انه "علم يستنبط انظمة تستطيع حل المشكلات، من خلال امتلاكه القدرة على دراسة هذه المشكلات ومعرفة الكيفية التي يستطيع بواسطتها حل المشكلة بمفرده بدون تدخل من الانسان"[١]، ويمكن لهذه النظم ان تصل الى مستوى مستقل ولا يمكن الاعتراض على عمل تلك النظم ولا نتائج هذا العمل لكون تصرفاتها تعد صناديق سوداء، وقد اورد التقرير الصادر عن البرلمان الاوربي في ٢٠١٧ عدة قيود من الواجب توفرها في تعريف (الذكاء الاصطناعي أو الروبوتات) في حال تم تبنيها في التشريعات الخاصة بدول الاتحاد الا وهي الاستقلال والتعلم التلقائي الذاتي من خلال التجارب والخبرات السابقة وتكيف تصرفاتها مع البيئة التي تتواجد فيها[٢]، وفي عام ٢٠٢٠ قد عرفه البرلمان الاوربي على انه" قدرة الآلة على إعادة إنتاج السلوكيات المتعلقة بالبشر، مثل التفكير والتعلم والتخطيط والإبداع" [٣] ، أيضاً تم تعريف الذكاء الاصطناعي في اعلان مونتريال للتنمية المسؤولة للذكاء الاصطناعي لعام ٢٠١٨ على انه "الأنظمة المستقلة القادرة على أداء المهام المعقدة التي كان يُعتقد أنها مخصصة للذكاء الطبيعي مثل معالجة كميات كبيرة من المعلومات، الحساب والتنبؤ، التعلم وتكييف استجاباتها مع المواقف المتغيرة و التعرف على الأشياء وتصنيفها"[٤].

كذلك قامت المجموعة الاوربية للذكاء الاصطناعي بتقديم اقتراحها لتعريف الذكاء الاصطناعي على انه "مجموعة انظمة اخترعها البشر والتي من شانها العمل ضمن الهدف المعقد في العالم المادي أو العالم الافتراضي من خلال ادراكها لبيئتها الموجودة بها، وتفسير

---

(١) الامم المتحدة الجمعية العامة ، "لجنة الامم المتحدة للقانون التجاري الدولي، الحولية القانونية للعقود الذكية والذكاء الاصطناعي"، *ورقه مقدمة من تشيك، الدورة الحادية والخمسون، نيويورك* ، (٢٠١٨): ص٢.

(2) European Parliament, Civil Law Rules on Robotics of 2017, paragraph 1. https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html
تمت الزيارة في ٢٠٢٠/١٠/١٥، الساعة ٣:٤٥ م.

(3) Parlement européen, Cadre pour les aspects éthiques de l'intelligence artificielle, de la robotique et des technologies connexes (2020) .
https://www.euro arl.europa.eu/docco/document/TA-9-2020-0275
تمت الزيارة بتاريخ ٢٠٢٠/١٠/١٥ الساعة ٩:٠٦ م.

(4) Rapport de la Déclaration de Montréal pour un développement responsable de l'intelligence artificielle, Partie 6, Les chantiers prioritaires et leurs recommandations pour le développement responsable de l'intelligence artificielle , 2018 , P١٧ .

البيانات المتوافرة في عقلها الاصطناعي، والتفكير منطقياً في المعرفة التي استمدتها من هذه البيانات وتحديد افضل الاجراءات المطلوب اتخاذها وفقاً لمعايير تم تحديدها مسبقاً وذلك لتحقيق الهدف المطلوب منها بالتحديد " [١].

ختاماً ، نجد انه على الرغم من تعدد تعريفات الذكاء الاصطناعي الا انه لم يتم الوصول الى تعريف حاسم وذلك نظراً لحداثه هذا المفهوم وتعدد مهامه وكل تعريف حاول التركيز على هدف معين من اهدافه وهذا من شأنه ان يودي الى تعدد تعريفات الذكاء الاصطناعي، وكان لابد ان يتم تقسيم المصطلح الى كلمتين الا وهما الذكاء الذي يُقصد به القوة في التفكير والثانية الاصطناعي والتي يقصد بها الشيء الذي صنعه الانسان، ولذلك يمكننا تعريف الذكاء الاصطناعي على انه العلم الذي يدرس القدرات العقلية للإنسان من خلال استخدام الرموز الحسابية لجعل الحاسوب يكتسب منها.

II.ب. المطلب الثاني

تكامل الذكاء الاصطناعي مع الأمن السيبراني

تثار العديد من التساؤلات والشكوك حول مدى تكامل أنظمة الذكاء الاصطناعي مع الأمن السيبراني للدول والمنظمات والأشخاص في القانون الدولي؟

في الواقع ، اصبح الذكاء الاصطناعي مع مرور الوقت جزء لا يتجزأ من الامن السيبراني ويصعب الفصل بينهم، وذلك بسبب قابلية أنظمة الذكاء الاصطناعي الموجودة في برامج الحاسوب[٢] على كشف التهديدات الأمنية والتصدي لها بسرعة فائقة عند توظيفها بصورة إيجابية ضمن إطار الأمن السيبراني ، لاسيما إذا علمنا ان كل من الامن السيبراني و الذكاء الاصطناعي مرتبط بشكل مباشر أو غير مباشر بالحق في الخصوصية ، وما ينطوي عليه هذا الحق من معلومات شخصية واجبة الحماية[٣]، لأن هذه المعلومات يمكن اختراقها وإساءة استخدامها من خلال العمل على اختراق الأمن السيبراني للدول والمنظمات والاشخاص وانتهاك خصوصية بياناتهم ، ومن الجدير بالذكر ان مسألة قبول الخصوصية هي مسألة متفاوتة بين الدول، ذلك لان معظم إن لم تكن جميع الدول الديمقراطية ، تبنت فكرة أن حقوق الإنسان لابد أن تشكل جزءاً اساسياً من الإطار القانوني الدولي، وهذا من شأنه ان يسمح حتماً للدول بتأكيد سيادتها وسلطتها السيادية و تطوير قوانين حماية البيانات الخاصة بها

(1)Proposal for a Regulation of The European Parliment and of the Council OF Laying Down Harmonised Rules on artifical inteIligence (artifical Intelligence act) and amending certain union , Brussel, 2021 ,p8 .

(٢) يمكن تعريف برنامج الحاسوب على انه نظام الكتروني تم تصميمة بواسطة شخص يدعى بالمبرمج ، انظر :عبد الأمير، أحمد، "الحماية القانونية لبرامج الحاسوب"، *مجلة العلوم القانونية* ، ٣٨ (١)، (٢٠٢٣): ٦٤٩-٧٣. https://doi.org/10.35246/jols.v38i1.618 ، ص٦٥٢ .

(٣) عادل عبد الصادق، *البيانات الشخصية: الصراع على نفط القرن الحادي والعشرين*، (المركز العربي لأبحاث الفضاء الالكتروني: ٢٠١٨)، ص ٥٠.

، على سبيل المثال ، نجد ان سنغافورة لا تعترف بالحق في الخصوصية ، على عكس الاتحاد الأوربي الذي كان رائداً في تطوير قوانين حماية البيانات لان الخصوصية حق أساسي بموجب الاتفاقية الأوروبية لحقوق الإنسان والحريات الأساسية لعام ١٩٥٠ والميثاق الأوروبي للحقوق الأساسية لعام ٢٠٠٠ وهذا من شأنه تعزيز الحق السيادي للجهات الفاعلة الحكومية في تطوير القواعد القانونية التي تناسب احتياجاتها[١] ، كما اكدت محكمة العدل الدولية ان هناك تكامل بين حقوق الانسان والقانون الدولي الذي هو أساس لحماية هذه الحقوق[٢].

نتيجة لما تقدم، نجد ان الحاجة قد ازدادت طردياً مع مرور الوقت الى استخدام الذكاء الاصطناعي في هذا المجال، لكون الذكاء الاصطناعي ما هو الا مجموعة أنظمة تعمل على تعزيز الأمن السيبراني للدول والمنظمات والاشخاص اذا استعملت بصورة صحيحة، وان دورها بحماية الأمن السيبراني أوسع من دور الأنظمة التي تتم برمجتها لغرض معين، إذ إن أنظمة الذكاء تقوم بالتفكير بطريقة مشابهه الى حد ما لتفكير العقل البشري في تصنيف الحالات وترتيب الأولويات[٣]. ولذلك تعد احدى أولويات الأمن السيبراني تطوير الذكاء الاصطناعي لاكتشاف نقاط ضعف البرامج وتصحيحها بشكل مستقل قبل ان يستغلها المتسللون، وذلك من خلال عدة مهام يمتاز بها الذكاء الاصطناعي بمجال الأمن السيبراني وهي كما يلي:

اولاً: القدرة على تجنب الأخطاء

تكمن قوة دور الذكاء الاصطناعي المكمل للأمن السيبراني بالدقة التي يتميز بها وتجنبه للأخطاء البشرية خاصة عند اداءه لمهام متكررة وهذا من شأنه ان يجعل من قراراته بعيدة كل البعد عن العنصرية او التحيز لجهة فاعلة ما[٤]، اذ يعد الخطأ البشري احد اهم الأسباب الرئيسية لانتهاكات البيانات ويمكن للذكاء الاصطناعي ان يتجنب ذلك الخطأ، ومن الجدير بالذكر ان الذكاء الاصطناعي ليس بديل لخبراء الأمن السيبراني، وانما يعمل على تعزيز القدرات البشرية ، لاسيما في الوقت الذي تشعر فيه فرق الأمن السيبراني بالإرهاق من

(1) Robert Walters, Marko Novak, Cyber Security, Artificial Intelligence, Data Protection & the Law, Springer, 2021, p. 73.

(٢) مسلم نبراس ابراهيم، "جرائم الحرب وجرائم العدوان في فقه محكمة العدل الدولية"، *مجلة العلوم القانونية*، ٣١ (٤)، (٢٠١٧): ٢٢٣-٤٦. https://doi.org/10.35246/jols.v31is.107 ، ص ٢٢٧.

(٣) عبد الله موسى، احمد حبيب بلال، مصدر سابق، ص٢٠.

(٤) حورية شنبي، "تنفيذ استراتيجية النقل بالسكك الحديدية بالجزائر باستخدام أنظمة النقل الذكية"، بحث *منشور في مجلة الدراسات المالية والمحاسبية، جامعة الوادي، الجزائر*، العدد ٧، (٢٠١٦): ص١٧٤.

حجم وتعقيد هذه الهجمات المتزايدة إضافة الى ان خبراء الأمن السيبراني الذين يحتاجون اليهم لإحباط هذه الهجمات بنجاح يكلفون بشكل متزايد ويصعب العثور عليهم[١].

ثانياً: القدرة التنبؤية

يكمل الذكاء الاصطناعي الأمن السيبراني ويعززه من خلال قدرة أنظمة الذكاء الاصطناعي على دراسة البيانات الموجودة ويقوم بتحليلها ومعرفة ما هو عددها وما مصدرها ويوفر الكثير من الوقت والجهد على الخبراء المختصين في هذا المجال ، إذ يقوم باكتشاف الهجمات السيبرانية بسرعة كبيرة ويعمل على تحديد حجم المخاطر الناشئة عنها من خلال التنبؤ بهذه الهجمات ، وهذا ما دفع عدد كبير من الدول والمنظمات الى تبني أنظمة الذكاء الاصطناعي لغرض قابليتها على التنبؤ باحتمال وقوع اختراق او عمل تعرضي والاستعداد لهذا الامر قبل وقوعه ، بالإضافة الى سرعة الاستجابة للتهديدات السيبرانية خلال فترة زمنية قصيرة [٢]، وذلك من خلال قيامها بمسح البيانات واجراء التنبؤ القائم على تدريب النظام، اضافةً لذلك تستطيع أنظمة الذكاء الاصطناعي ان تعين نقاط الضعف الحرجة بالشبكة تلقائياً ورفع مستوى الدفاعات الخاصة بالشبكة حتى تستطيع تحسين دفاعاتها باستمرار ضد أي هجوم سيبراني محتمل الوقوع.

ثالثاً: القدرة على الاستجابة

تمتاز تطبيقات الذكاء الاصطناعي بقابليتها على الاستجابة للتهديدات السيبرانية بصورة مستمرة، وهذا ما دفع العديد من الجهات للجوء الى الذكاء الاصطناعي لغرض تأمين امنها السيبراني من خلال قيامه باكتشاف الهجمات وايقافها في الوقت ذاته ، وان هذا من شأنه تطوير اليات حماية جديدة ، إذ يساعد الذكاء الاصطناعي الدول والمنظمات على خفض التكاليف وتحسين وقت الاستجابة للتهديدات وللانتهاكات سواء اكانت من الجهات الحكومية او الجماعات الإرهابية [٣] بغض النظر عن الأساليب او الخصائص المحددة التي تستخدم بها.

من خلال ما تقدم ، نجد ان التطور في التقنيات و التكنولوجيا المعاصرة له كالذكاء الاصطناعي له دور مهم بالنسبة للدول والمنظمات ، لكونها تضمن عدم انتهاك سيادة هذه الدول السيبرانية والاعتداء على امنها القومي ، و تحمي كافة اجهزتها بمختلف اشكالها

---

(1) Deloitte, Cybersécurité éclairée Gérer les cyberrisques grâce à la cybersécurité éclairée, 2018, p.2.
https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-fr-smart-cyber-pov-aoda.pdf . تاريخ الزيارة ٢٠٢٣/٤/٢ ، الساعة ٥:٠٠م

(٢) نبيل محمد عبد الرحمن حيدر، *التحكم في منحدرات الخطوط السريعة باستخدام الذكاء الاصطناعي مع تطبيقات على مدينة الرياض*، (الرياض :جامعة الملك سعود، ٢٠٠٠)، ص٤٧.

(٣) حميد أ. خ، "ظاهرة الارهاب وانتهاكات حقوق الانسان بعد عام ٢٠٠١"، *مجلة العلوم السياسية*، (٥٤)، (٢٠١٩): ٢١٥–٢٣٠. https://doi.org/10.30907/jj.v0i54.38 ، ص٢١٧.

وانواعها الذكية من الاطلاع عليها ، وبالمقابل فأن الأمن السيبراني يكمل الذكاء الاصطناعي ايضاً اذ يعد البيئة الخصبة التي يمكن ان يمارس بها الذكاء الاصطناعي مهامه بكل اريحية ، لأنه من المعلوم ان الذكاء الاصطناعي ما هو الا نتاج التطور التكنلوجي الحاصل في الآونة الاخيرة ومن غير المتوقع ان يعمل في جميع البيئات التقليدية الخاصة ببيانات الدول والمنظمات او معلوماتها الحساسة ، وانما لابد ان يعمل في اطار بيئة حديثة خاصة بالمعلومات وحمايتها توفر له كافة السبل والمقومات التي تعزز اليات عمله .

II.ج. المطلب الثالث

محددات تكامل الذكاء الاصطناعي مع الأمن السيبراني

بعد ان تمت الإشارة الى ان الذكاء الاصطناعي له القدرة على تعزيز الأمن السيبراني، لاسيما بعد تزايد استخدامه في هذا المجال بشكل كبير في الآونة الأخيرة بسبب دمج الذكاء الاصطناعي في مجموعة كبيرة من التقنيات المختلفة بما في ذلك جدران الحماية وأنظمة كشف التسلل والمساعدين الشخصيين الافتراضيين وبرامج مكافحة الفيروسات، إذ تم تصميم هذه التقنيات لتحسين الأمان من خلال تحديد تهديدات الأمن السيبراني (CST)[١].

لكن في الجانب الاخر، فأن توغل تقنيات الذكاء الاصطناعي في مجالات الفضاء السيبراني، جعل مواجهه التهديدات السيبرانية امراً صعباً، وذلك لأنها تخلق عدة عوامل من شأنها التأثير سلبياً على الأمن السيبراني في نفس الوقت وكما يلي أهمها ما يلي:

أولاً: الاستعانة بقدرات الذكاء الاصطناعي لتطوير هجمات السيبرانية

سمح التقدم التكنولوجي والعلمي للمتسللين ان يستعينوا بقدرات الذكاء الاصطناعي لتطوير هجمات معقدة ومتطورة وجعلها صعبة الاكتشاف[٢]، فعلى سبيل المثال، يمكن للقراصنة التابعين لدولة معينة استخدام تطبيقات الذكاء الاصطناعي لإنشاء بيانات اعتماد وهويات مزيفة للوصول إلى الشبكات الخاصة بأمن دولة اخرى او منظمة تابعة لها واختراقها، واستخدام الأدوات الآلية لإرسال سيل كبير من البريد العشوائي إلى قوائم عناوين البريد الإلكتروني ويعد هذا جزءاً من عمليات التصيد الاحتيالي[٣].

بالإضافة إلى ذلك ، يستطيع القراصنة استخدام الذكاء الاصطناعي لشن الهجمات السيبرانية من خلال استخدام الروبوتات لتنفيذ الهجمات الموزعة على الشبكات (DDOS)[٤]، إذ يمكن برمجة هذه الأنظمة لاستهداف أنظمة اخرى خاصة بدولة معينة أو

---

(1) CST هو مختصر الاحرف الأولى من Cyber Security threat.

(2) Mohiuddin Ahmed, Op.cit., P.144 .

(٣) بيتر بي سيل، الكون الرقمي، *الثورة العالمية في الاتصالات، ترجمة ضياء وراد*، (مؤسسة هنداوي: الطبعة الأولى، ٢٠٢١)، ص٢٥٦.

(٤) DDoS : هو اختصار لهجمات حجب الخدمة الموزعة التي تعد احدى اقوى وسائل الهجوم الالكتروني التي يمكن استعمالها من قبل مجرمي الانترنت ، ولها القابلية على تعطيل اكثر الأجهزة حماية عند توجيهها اليها.

مستخدمين معينين ومحاولة للتغلب عليهم، او برمجتها لاستخدام كلمات مرور شائعة للوصول إلى حسابات متعددة في وقت واحد لزيادة فرص نجاحها، واخيراً يمكن استخدام برامج الذكاء الاصطناعي لمساعدة المتسللين على إجراء اختبارات الاختراق وأنشطة الاستطلاع الأخرى قبل اكتشافهم، وتعد تهديدات يوم الصفر[١] من اكثر الأمثلة البارزة التي توضح تأثير الذكاء السلبي على الأمن السيبراني والتي يمكن ان تفاجئ أنظمة دفاع الأمن السيبراني[٢].

قد يكون من الصعب جداً اكتشاف مثل هذه الهجمات باستخدام أساليب الكشف التقليدية، ويمكن أن يكون لها تأثير كبير على الدول إذ ينتج عنها في الكثير من الأحيان جرائم عابرة للحدود او جرائم عدوان [٣] ، لذلك من المهم أن تتخذ الدول والمنظمات مجموعة خطوات لحماية أنظمتها من مثل هذه الهجمات، وذلك من خلال تنفيذ إجراءات أمنية قوية مثل جدران الحماية وبرامج مكافحة الفيروسات لمنع حدوث الهجمات في المقام الأول اذ ان وضع جدران حماية ضعيفة من شأنه ان يسهل عملية الاستيلاء على حواسيب دولة معينه[٤].

نتيجة لذلك، فأنه من الضروري على الدول والمنظمات الاستعداد لاحتمال وقوع هجوم وتنفيذ استراتيجيات التخفيف المناسبة[٥] في حالة حدوث هجوم، لكون هذه التدابير ماهي الا جزء حيوي تعمل على التعرف على الوقت الذي تتعرض فيه للهجوم والرد بشكل مناسب، وهذا سيتطلب نظام كشف للإنذار المبكر لتحديد الهجمات المحتملة والرد عليها إذا لزم الأمر من خلال إجراء عمليات تدقيق أمنية منتظمة ومراقبة شبكتها بحثاً عن علامات النشاط المشبوه، ويمكن للدول التأكد من استعدادها للتعامل مع أي هجوم قد يحدث من شانه ان يشكل جريمة دولية.

---

(١) وهي تهديدات تستغل ثغرة عدم توافر الحصانة في امان الكمبيوتر ويسمى ايضاً بهجوم يوم الصفر او هجوم ساعة الصفر.

(2) Mohiuddin Ahmed, Op.cit., P.144 .

(٣) صلاح ومهدي وهادي المالكي، "أفضلية القواعد القطعية في القانون الدولي العام"، *مجلة العلوم القانونية*، ٣٨ (١)، (٢٠٢٣): ١٢٨-٦٦.
https://jols.uobaghdad.edu.iq/index.php/jols/article/view/641 ، ص ١٣٨.

(٤) نجلاء احمد يس، *الحوسبة السحابية للمكتبات حلول وتطبيقات*، الطبعة الأولى، (دار العربي للنشر والتوزيع: ٢٠١٤)، ص٨٨.

(٥) استراتيجيات التخفيف (Mitigation Strategies) تعني مجموعة من الإجراءات والتدابير التي يتم اتخاذها للحد من تأثير الهجمات أو الحوادث الأمنية وللتقليل من فرص وقوعها ، تهدف هذه الاستراتيجيات إلى تحسين قدرة المؤسسات والمنظمات على التعامل مع التهديدات الأمنية والتأثيرات السلبية التي يمكن أن تنشأ عنها .

ثانياً: القصور التشريعي والعملي في مواجهه الاستخدامات السلبية للذكاء الاصطناعي

في الوقت الحاضر لا يوجد أي تعاون فعلي بين صناع التشريعات والتقنين لغرض وضع قواعد قانونية دولية تشمل الاستعمالات ذات الأثر السلبي المحتملة لتقنيات الذكاء الاصطناعي بأحكامها او منعها او على الأقل العمل على التخفيف من اثارها، إذ ان الجرائم الدولية الناتجة عن استخدام تطبيقات الذكاء الاصطناعي بصورة سلبية مماثلة للجرائم الدولية التقليدية الأخرى، الا ان الاختلاف بينهم يكمن في نقطتين وهما أداة الجريمة وكيفية التجريم، فالأداة المستعملة في جرائم الذكاء الاصطناعي تمتلك تقنية عالية وفائقة الأداء، وان تجريم هذا النوع من الجرائم لا يتم بالرجوع الى النصوص القانونية التقليدية لكونها لم تكن موجودة وقت وضعها، وأيضا لا يجوز التوسع بتفسير هذه النصوص لتطبيقها على جرائم الذكاء الاصطناعي لوجود قاعدة قانونية تقضي بأن (لا جريمة ولا عقوبة الا بقانون)[١]، وقد أثيرت هذه المسألة في القضاء الفرنسي عندما طُلِب منهُ النظر في مدى إمكانية تطبيق النصوص القانونية الموجودة الخاصة بالجرائم العادية على مثيلاتها المرتكبة في الجرائم السيبرانية، فصدر حكم يقضي باعتبار قيام احد الموظفين العاملين في الشركة المختصة بتصوير التصميمات المتعلقة بألة تم تصنيعها وتسويقها لمشروع اخر بالاستعانة بالتصميمات المذكورة (جريمة سرقة) دون البحث فيما اذا كانت هذه التصميمات متعلقة بحماية براءات الاختراع ام لا[٢]، لذلك لابد من وضع قواعد قانونية دولية لمواجهة الاستخدامات السلبية للذكاء الاصطناعي، بالإضافة الى ذلك نجد ان الممارسات العملية قليلة لاسيما فيما يتعلق بمجال البحث مع سبل ومناهج أكثر نضجا لمعالجة الهجمات السيبرانية المتوقعة من التقنيات ذات الاستعمال المزدوج للذكاء الاصطناعي بمجال الامن السيبراني[٣].

ثالثاً: تسهيل الحروب والنزاعات الدولية لاسيما السيبرانية

يسهل الذكاء الاصطناعي الحروب والنزاعات الدولية وذلك نظراً للإمكانيات الكبيرة التي يتمتع بها لتحسين كفاءة العمليات العسكرية وتعزيز سلامة القوات العسكرية في ميادين القتال، إذ يمكن استخدامه لغرض تخطيط وتنفيذ المناورات التكتيكية[٤]، وأيضاً لتحديد التهديدات من خلال مراقبة ورصد تحركات قوات العدو، فضلاً عن ذلك يساعد في تنسيق

(١) مخلد إبراهيم الزغبي، "فاعلية القوانين والتشريعات العربية في مواجهه الجريمة الالكترونية"، *المجلة العربية للنشر العلمي*، العدد السابع والثلاثون، (٢٠٢١): ص٢٩٠.
(٢) مدحت رمضان، *جرائم الاعتداء على الأشخاص والانترنت*، (القاهرة، مصر: دار النهضة العربية، ٢٠٠٠)، ص١٨.
(٣) علاء عبد الرزاق السالمي، مصدر سابق، ص١٢٨.
(٤) والمقصود بالمناورة التكتيكية هو تحرك القوات العسكرية التابعة لدولة معينه لكي تحصل على موقع أفضل بالنسبة للعدو.

الأصول العسكرية وتقييم الأهداف المحتملة، مما قد يساعد في تقليل مخاطر وتكاليف العمليات العسكرية التقليدية ، إذ تستخدم الجيوش في جميع أنحاء العالم الذكاء الاصطناعي لتحسين التخطيط الاستراتيجي وقدرات صنع القرار.

فضلاً عن ذلك يؤدي الذكاء الاصطناعي الى ظهور الأسلحة المستقلة المتمثلة بالآلات التي تمتلك القابلية على العمل دون أي تدخل بشري وبصورة مستقلة دون وجود أي شكل من أشكال الرقابة البشرية أو الإشراف عند استخدامها في حالات القتال، ويمكن برمجة هذه الأسلحة لاستهداف مجموعات محددة من الافراد بناءً على معايير محدده كالعمر أو الجنس أو العرق أو الجنسية بمجرد نشرها ، وهذا من شانه ان يسهل على الدول الاستعانة بها لشن الحروب واستخدام القوة عبر الحدود الوطنية ، لأنها عندما تستخدم هذه الأسلحة لا تتكبد خسائر في أرواح المقاتلين من رعاياها وانما الخسائر والخطر تكون فقط على الدول المعادية[١] كالأسلحة الروبوتية والروبوتات القاتلة والأسلحة الفتاكة [٢] ، ايضاً يمكن لتطبيقات الذكاء الاصطناعي أن تزيد من حدوث الهجمات السيبرانية على الصعيد الدولي من خلال تزويد المتسللين بأدوات قوية لأتمتة هجماتهم وتسريعها طُرقها ، على سبيل المثال يمكن استخدامها لتطوير برامج ضارة معقدة قادرة على التعلم والتكيف مع البيئة المحيطة بها مما يزيد من صعوبة اكتشافها والتخفيف من حدتها ، علاوة على ذلك يمكن استخدام تطبيقات الذكاء الاصطناعي لفحص كميات كبيرة من البيانات وتحديد نقاط الضعف في أنظمة الكمبيوتر[٣] التابعة لدولة معينه والتي من الممكن استغلالها من قبل الدول المعادية .

رابعاً: صعوبة اسناد المسؤولية الدولية في نطاق الذكاء الاصطناعي

ان استخدام أنظمة الذكاء الاصطناعي كأسلحة ذكية مستقلة عن أي تدخل بشري ، بمعنى انها هي التي تتخذ القرارات الحاسمة للاعتداء على سيادات الدول واستقلالها وامنها السيبراني ، من شأنه ان يثير صعوبة الا وهي كيفية اسناد المسؤولية الدولية[٤] عن هذه التطبيقات بسبب التقدم التكنلوجي في مجال هذه الأسلحة الذكية التي أصبحت منتشرة وداخلة في كافة المجالات بصورة سريعة ومذهلة في مقابل التأخر الكبير في تقنين قواعد دولية خاصة بالتعامل مع هذه التقدم في نطاق الاستخدام السلبي للذكاء الاصطناعي و التي تتوغل

---

(١) عمر مكي، *القانون الدولي الإنساني في النزاعات المسلحة المعاصرة*، اللجنة الدولية للصليب الأحمر، ص١٤٢.

(٢) محمد بشير المنجد، *الالة الذكية من ديكارت وحتى دماغ غوغل*، (دار النهضة: الطبعة الأولى، ٢٠٢٠)، ص٢٥٩.

(٣) محمد إبراهيم المليجي، "الذكاء الاصطناعي وصناعة الرياضة"، *المجلة العلمية للبحوث التطبيقية في المجال الرياضي*، المجلد ٣، العدد١، (٢٠٢٣): ص٧٤.

(٤) محمد، وسن، وبيضاء والي، "المسؤولية الدولية عن صد لاجئي القوارب"، *مجلة العلوم القانونية*، ٣٨ (١)، (٢٠٢٣): ٧٣١-٤٧. https://jols.uobaghdad.edu.iq/index.php/jols/article/view/663 ، ص ٧٣٤.

في الكثير من الاستراتيجيات الخاصة بالتسليح والقتال لدى عدة دول وعلى رأسهم الدول الكبرى [١] ، الامر الذي من شأنه ان يزيد استخدام هذه الوسائل للتهرب من المسؤولية الدولية لاسيما في مجال الامن السيبراني وهذا من شأنه ان يؤدي الى انتهاك قواعد القانون الدولي والدولي الإنساني ، اذ انه من مخاطر انتشار الانظمة الذكية كسلاح لاختراق الأمن السيبراني لدولة ما هي انتهاكها لقواعد القانون الدولي الإنساني ، لاسيما اذ كانت في يد قائد لا يعرف معنى الرأفة وله القدرة على برمجتها فأنه لن يترك هدفه الذي يروم اليه ابداً ، لكون الروبوتات الذكية لن تعلم بأن العمل الذي تقوم به غير جائز حتى لو كان ينتهك القانون الدولي الإنساني انتهاكات واسعة ومتكررة ، وبالتالي فأن انتشارها من شأنه ان ينتهك قواعد القانون الدولي الإنساني ، لذلك لابد من وجود قواعد قانونية تحكم كيفية تصميم وانتاج وبرمجة الأسلحة الذكية ونقلها ، والعمل على انتاج الروبوتات الذكية تتوقف عن عملها اوتوماتيكياً في حالة وقوعها في يد يسئ استخدامها[٢].

الخاتمة

في ختام هذا الموضوع ، توصلنا الى مجموعة من الاستنتاجات والتوصيات والتي سوف نعمل على توضيحها كما يلي :

أولاً : الاستنتاجات

١- هو مجموعة من الإجراءات والتدابير التي تهدف إلى حماية الأنظمة الإلكترونية والمعلومات الرقمية من التهديدات والاختراقات السيبرانية، و يتعامل مجال الأمن السيبراني مع مجموعة متنوعة من التهديدات، مثل الهجمات الإلكترونية، والبرامج الضارة، والاختراقات الهاكرز، وسرقة البيانات، والاختراقات السيبرانية الحكومية والصناعية ، كما ان الهدف الرئيسي للأمن السيبراني هو الحفاظ على سرية المعلومات، وسلامة البيانات، وتوفير الخدمات المستدامة عبر الشبكات والأنظمة الرقمية .

٢- يشير مفهوم الذكاء الاصطناعي إلى قدرة الأنظمة الكمبيوترية على تنفيذ مهام تشابه الذكاء البشري و يمكن استخدام الذكاء الاصطناعي في مجال الأمن السيبراني لتحليل البيانات الكبيرة وكشف التهديدات والتصدي لها بشكل أكثر فعالية.

٣- تكامل الذكاء الاصطناعي مع الأمن السيبراني إذ يمكن استخدام الذكاء الاصطناعي لتعزيز جوانب الأمان والحماية السيبرانية ، كما يمكن استخدام تقنيات الذكاء الاصطناعي مثل تعلم الآلة والتحليل الضخم لتحديد الأنماط الاعتيادية والتهديدات المحتملة والاستجابة السريعة لها.

---

(١) احمد محمد براك، *نحو تنظيم قواعد المسؤولية عن تقنيات الذكاء الاصطناعي*، (دار وائل للنشر: الطبعة الأولى، ٢٠٢٢)، ص٨٠.

(٢) عمر مكي، مصدر سابق، ص١٤٣.

ثانياً : التوصيات

١- نقترح تعزيز التعاون الدولي في مجال الأمن السيبراني من خلال تبادل المعلومات والخبرات والممارسات الجيدة.

٢- نأمل الاستثمار في البحث والتطوير لتطوير تقنيات الذكاء الاصطناعي المتقدمة لمكافحة التهديدات السيبرانية.

٣- ضرورة وضع سياسات وقوانين فعالة تحكم استخدام الذكاء الاصطناعي في مجال الأمن السيبراني وتحمي حقوق المستخدمين والخصوصية .

٤- وجوب انشاء هيكليات مؤسسية معنية بالأمن السيبراني سواء اكانت على المستوى الدولي او الوطني .

٥- ضرورة الاستثمار في تطوير تقنيات تحليل البيانات والذكاء الاصطناعي لتحليل سريع للهجمات السيبرانية والكشف عنها ، و هذا يمكن أن يساعد في التعرف على الأنماط والتهديدات الجديدة بشكل أفضل.

المصادر والمراجع

أولاً: الكتب القانونية

١. ابراهيم ابو خزام، *الحرب وتوازن القوى*، بنغازي: دار الكتاب الجديدة المتحدة، الطبعة الاولى، ٢٠٠٩.

٢. احمد محمد براك، *نحو تنظيم قواعد المسؤولية عن تقنيات الذكاء الاصطناعي*، دار وائل للنشر: الطبعة الأولى، ٢٠٢٢.

٣. الامم المتحدة الجمعية العامة، *لجنة الامم المتحدة للقانون التجاري الدولي، الحولية القانونية للعقود الذكية والذكاء الاصطناعي*، ورقه مقدمة من تشيك، الدورة الحادية والخمسون، نيويورك: ٢٠١٨ .

٤. اوس مجيد غالب العوادي، *الأمن المعلوماتي السيبراني*، بيروت: مركز البيان للدراسات والتخطيط، الطبعة الأولى ، ٢٠١٦ .

٥. ايمان عصام مصطفى، *صورة أمريكا وروسيا في الخطاب الصحفي المصري*، العربي للنشر والتوزيع: الطبعة الأولى، ٢٠٢١.

٦. بيتر بي سيل، *الكون الرقمي، الثورة العالمية في الاتصالات*، ترجمة ضياء وراد، مؤسسة هنداوي: الطبعة الأولى، ٢٠٢١ .

٧. الخليل بن أحمد الفراهيدي: *كتاب العين مرتبا على حروف المعجم*، تحقيق، عبد الحميد هنداوي، ج٢، بيروت: دار الكتب العلمية، ٢٠٠٢.

٨. دحان حزام ناصر القريطي، *الأمن السيبراني وحماية أمن المعلومات*، الاسكندرية: دار الفكر الجامعي، الطبعة الاولى، ٢٠٢٢ .

٩. عادل عبد الصادق، *الرقمنة والمرونة السيبرانية حالة المنطقة العربية مصر وتونس والمغرب*، القاهرة: المركز العربي لأبحاث الفضاء الالكتروني ، الطبعة الاولى، ٢٠٢١.
١٠. عبد الرحمن علي اللقاني، *دور الأمن السيبراني في تعزيز امن المعلومات المالية الالكترونية*، دار اليازوري العلمية: الطبعة الأولى، ٢٠٢٢ .
١١. فارس محمد العمارات، *الأمن السيبراني، المفهوم وتحديات العصر*، الاردن: دار الخليج للنشر والتوزيع، الطبعة الاولى ،٢٠٢٢.
١٢. محمد بشير المنجد، *الالة الذكية من ديكارت وحتى دماغ غوغل*، دار النهضة: الطبعة الأولى، ٢٠٢٠ .
١٣. مدحت رمضان، *جرائم الاعتداء على الأشخاص والانترنت*، القاهرة، مصر: دار النهضة العربية، ٢٠٠٠.
١٤. نجلاء احمد يس، *الحوسبة السحابية للمكتبات حلول وتطبيقات*، الطبعة الأولى، دار العربي للنشر والتوزيع: ٢٠١٤.

ثانيا: الرسائل و الاطاريح

١. إيهاب احمد حسن، "الأمن السيبراني في اطار قواعد القانون الدولي العام"، رسالة ماجستير، كلية القانون والعلوم السياسية، جامعة كركوك، ٢٠٢٢ .

ثالثاً: المجلات العلمية

١. اسراء شريف جيجان، "الأمن السيبراني الصيني: دراسة بالدوافع والاهداف"، *مجلة قضايا سياسية*، العدد ٦٥، (٢٠٢١).
٢. اسلام فوزي، "الابعاد الاجتماعية والقانونية: تحليل سوسيولوجي"، *المجلة الاجتماعية القومية*، المجلد ٥٦، العدد٢، (٢٠١٩).
٣. امنة علي البشير محمد، "الأمن السيبراني في ضوء مقاصد الشريعة"، *مجلة كلية الدراسات الاسلامية والعربية للبنات الاسكندرية*، المجلد ١، العدد ٣٧، بلا سنة نشر.
٤. بن مرزوق عنترة، "البعد الالكتروني للسياسة الأمنية الجزائرية في مكافحة الإرهاب"، *مجلة العلوم الإنسانية والاجتماعية*، العدد ٣٨، (٢٠١٨).
٥. جمال بوازديه، "الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية والافاق المستقبلية"، *مجلة العلوم القانونية والسياسية*، المجلد ١٠، العدد ١٠، (٢٠١٩).
٦. جيجان أ. ش، التأثير السيبراني في الامن القومي للدول الفاعلة (الولايات المتحدة الاميركية) انموذجاً، *مجلة العلوم السياسية*، (٦٤)، (٢٠٢٢): ١–١٨. https://doi.org/10.30907/jcopolicy.vi64.628 .

٧. حسام عبد الأمير خلف، "البعد الخامس في النزاعات المسلحة _الفضاء الالكتروني_ ، *مجلة كلية الحقوق* ، *جامعة النهرين* ، مجلد ١٨ ، عدد ١، (٢٠١٦).

٨. حميد أ. خ، "ظاهرة الارهاب وانتهاكات حقوق الانسان بعد عام ٢٠٠١"، *مجلة العلوم السياسية*، (٥٤)، (٢٠١٩): ٢١٥_٢٣٠. https://doi.org/10.30907/jj.v0i54.38 .

٩. حورية شنبي، "تنفيذ استراتيجية النقل بالسكك الحديدية بالجزائر باستخدام أنظمة النقل الذكية"، *بحث منشور في مجلة الدراسات المالية والمحاسبية، جامعة الوادي، الجزائر*، العدد ٧، (٢٠١٦).

١٠. الخاطري ، راشد، وزايد علي، "تجنيد الأشخاص في التنظيمات الإرهابية تقنياته وأساليبه - القانون الإماراتي نموذجا"، *مجلة العلوم القانونية*، ٣٨ (١)، (٢٠٢٣): ٨٤-١٠٦. https://jols.uobaghdad.edu.iq/index.php/jols/article/view/638 .

١١. خالد ظاهر عبد الله، "دور التشريعات الجزائية في حماية الأمن السيبراني بدول مجلس التعاون الخليجي"، *مجلة البحوث الفقهية والقانونية*، العدد ٣٨ ، (٢٠٢٢) .

١٢. خديجة خير الله عبد الرحمن العظامات، "تأثير تطبيق التيك توك على القيم الاجتماعية في المجتمع الأردني من وجهة نظر طلبة الجامعة"، *مجلة كلية التربية - جامعة عين شمس* ، العدد ٤٦ ، الجزء ٤، (٢٠٢٢).

١٣. خلف حسام عبد الامير، "التكامل بين القانون الدولي الجنائي والقانون الدولي الإنساني في مكافحة الإرهاب"، *مجلة العلوم القانونية*، ٣١ (٤)، (٢٠١٩): ١٨٧-٢٢٢. https://doi.org/10.35246/jols.v31is.106.

١٤. دهام ومحمد ومحمود خليل، "مشروعية استخدام الهجمات الإلكترونية في النزاعات الدولية والمسؤولية الدولية عنها"، *مجلة العلوم القانونية*، ٣٦ (٤)، (٢٠٢٢): ٦٧٨-٧٠٤. https://doi.org/10.35246/jols.v36i4.520 .

١٥. زمورة جمال، "اهمية حوكمة الأمن السيبراني لضمان تحول رقمي امن للخدمات العمومية في الجزائر"، *مجلة البحوث الاقتصادية المتقدمة*، المجلد ٧، العدد ٢، (٢٠٢٢).

١٦. صلاح ومهدي وهادي المالكي، "أفضلية القواعد القطعية في القانون الدولي العام"، *مجلة العلوم القانونية*، ٣٨ (١)، (٢٠٢٣): ١٢٨-٦٦. https://jols.uobaghdad.edu.iq/index.php/jols/article/view/641 .

١٧. عادل عبد الصادق، "البيانات الشخصية: الصراع على نفط القرن الحادي والعشرين"، *المركز العربي لأبحاث الفضاء الالكتروني*، (٢٠١٨).

١٨. عبد الأمير، أحمد، "الحماية القانونية لبرامج الحاسوب"، *مجلة العلوم القانونية*، ٣٨ (١)، (٢٠٢٣): ٦٤٩-٧٣. https://doi.org/10.35246/jols.v38i1.618 .
١٩. المالكي هادي نعيم وعبد مصطفى سالم، "النطاق المكاني للعمليات الحربية في النزاعات المسلحة الدولية"، *مجلة العلوم القانونية*، ٣١ (٤)، (٢٠١٧): ٢٨-٥٧. https://doi.org/10.35246/jols.v31is.100 .
٢٠. محمود لمى عبدالباقي و كيطان اسراء نادر، "المسؤولية الدولية عن الأضرار التي تسببها الهجمات السيبرانية"، *مجلة العلوم القانونية*، ٣٦ (ديسمبر)، (٢٠٢١): ٣٣٦_٣٦٢. https://doi.org/10.35246/jols.v36i0.435 .
٢١. مخلد إبراهيم الزغبي، "فاعلية القوانين والتشريعات العربية في مواجهه الجريمة الالكترونية"، *المجلة العربية للنشر العلمي*، العدد السابع والثلاثون، (٢٠٢١).
٢٢. مسلم نبراس ابراهيم، "جرائم الحرب وجرائم العدوان في فقه محكمة العدل الدولية"، *مجلة العلوم القانونية*، ٣١ (٤)، (٢٠١٧): ٢٢٣-٤٦. https://doi.org/10.35246/jols.v31is.107 .
٢٣. مصطفى إبراهيم سلمان، "الأمن السيبراني واثرة في الأمن الوطني العراقي"، *مجلة العلوم القانونية والسياسية*، المجلد ١٠، العدد ١، (٢٠٢٢).
٢٤. منى عبد السمحان، "متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية"، *مجلة كلية التربية، جامعة المنصورة*، العدد ١١١، (٢٠٢٠).
٢٥. نبيل محمد عبد الرحمن حيدر، "التحكم في منحدرات الخطوط السريعة باستخدام الذكاء الاصطناعي مع تطبيقات على مدينة الرياض"، جامعة الملك سعود، الرياض، (٢٠٠٧).

رابعاً : المصادر الأجنبية

1. Chamiak, Eugene & McDermott, Drew, Introduction to Artifical Intelligens, Addission Wesley Publishing Company, Canada 198.
2. Deloitte, Cybersécurité éclairée Gérer les cyberrisques grâce à la cybersécurité éclairée, 2018.
3. European Parliament, Civil Law Rules on Robotics of 2017, paragraph 1.
4. European Parliament, Civil Law Rules on Robotics of 2017, paragraph 1. .
5. Gorge Luger and Nathan Stubblefield, Arthaal Intelligence: Structures and Strategies for Complex Problem Sabang, Benjamin/Cummings, California, 1995.
6. Hangeland, Arial Intelligence TheVery Idea, MIT Press, USA, 1985.

7. Hugo Loiseau, Daniel Ventre, Cybersecurity in Humanities and Social Sciences,WILEY, Volume 1.
8. Jack Copeland, Diane Proudfoot, The Computer, Artificial Intelligence, and the Turing Test. In: Teuscher , Alan Turing: Life and Legacy of a Great Thinker, Springer, Berlin, Heidelberg, 2004.
9. Luisa Dall'Acqua ,Transdisciplinary Perspectives on Risk Management and Cyber Intelligence , Volume1, 2020.
10. Mohiuddin Ahmed, Explainable Artificial Intelligence for Cyber Security, Next Generation Artificial Intelligence, Springer ، Volume1025 ،2022.
11. Parlement européen, Cadre pour les aspects éthiques de l'intelligence artificielle, de la robotique et des technologies connexes ,2020.
12. Proposal for a Regulation of The European Parliment and of the Council OF Laying Down Harmonised Rules on artifical inteIligence (artifical Intelligence act) and amending certain union , Brussel, 2021.
13. Proposal for a Regulation of The European Parliment and of the Council OF Laying Down Harmonised Rules on artifical inteIligence (artifical Intelligence act) and amending certain union , Brussel, 2021.
14. Ray Kurzweil, The Age of Intelligent Machines, Dai Nippon, Japan, 1990.
15. Rich , Elaine, Arficial Intellegeme, McGraw-Hill, Inc., Singapore, 1984
16. Richard Kemmererm, University of California Santa Barbara, Department of Computer Science , Volume 1,2003.
17. Robert Walters, Marko Novak , Cyber Security, Artificial Intelligence, Data Protection & the Law, Springer , 2021
18. Tadas Limba and other, Cybersecurity management model for critical infrastructure, The National Journal Entrepreneurship and Sustainability, Volume 4, 2017 .

References

First: legal books

1. Ibrahim Abu Khuzam, War and Balance of Power, New United Books, Benghazi, First Edition, 2009.
2. Ahmed Mohamed Barak, Towards Regulating Liability Rules for Artificial Intelligence Technologies, Wael Publishing House, First Edition, 2022.
3. United Nations General Assembly, United Nations Commission on International Trade Law, Legal Aspects of Smart Contracts and Artificial Intelligence, Paper Presented by the Czech Republic, Fifty-Second Session, New York, 2018.
4. Aws Majid Ghaleb Al-Awadi, Cyber Information Security, Bayan Center for Studies and Planning, Beirut, First Edition, 2016.
5. Iman Essam Mustafa, Images of America and Russia in the Egyptian Press Discourse, Arabi Publishing and Distribution, First Edition, 2021.
6. Peter B. Seel, The Digital Universe: The Global Revolution in Communications, Translated by Diaa Ward, Hindawi Foundation, First Edition, 2021.
7. Khalil ibn Ahmad Al-Farahidi, Book of Al-Ain Arranged Alphabetically, Edited by Abdulhamid Hindawi, Volume 2, Dar Al-Kutub Al-Ilmiyya, Beirut, 2002.
8. Khalil ibn Ahmad Al-Farahidi, Book of Al-Ain Arranged Alphabetically, Edited by Abdulhamid Hindawi, Volume 2, Dar Al-Kutub Al-Ilmiyya, Beirut, 2002.
9. Dahhan Hazam Nasser Al-Qurayti, Cybersecurity and Information Security Protection, Dar Al-Fikr Al-Jamei, Alexandria, First Edition, 2022.
10. Adel Abdel-Sadeq, Digitization and Cyber Resilience: The Case of the Arab Region - Egypt, Tunisia, and Morocco, Arab Center for Space Research, Cairo, First Edition, 2021.

11. Abdelrahman Ali Al-Laqani, The Role of Cybersecurity in Enhancing Electronic Financial Information Security, Dar Al-Yazouri Scientific, First Edition, 2022.
12. Fares Mohammed Al-Amrati, Cybersecurity: Concept and Challenges of the Era, Gulf Publishing and Distribution, Jordan, First Edition, 2022.
13. Mohammed Ibrahim Al-Mulji, Artificial Intelligence and the Sports Industry, Scientific Journal of Applied Research in the Sports Field, Volume 3, Number 1, 2023.
14. Mohammed Bashir Al-Munajjid, The Smart Machine from Descartes to Google's Brain, Dar Al-Nahda, First Edition, 2020, p. 259.
15. Medhat Ramadan, Crimes of Assault on Individuals and the Internet, Arab Renaissance House, Cairo, Egypt, 2000.
16. Najla Ahmed Yass, Cloud Computing for Libraries: Solutions and Applications, First Edition, Dar Al-Arabi for Publishing and Distribution, 2014.

Second : Letters and theses

1. Ihab Ahmed Hassan, Cybersecurity within the Framework of Public International Law Rules, Master's Thesis, College of Law and Political Science, University of Kirkuk, 2022.

Third :Scientific Journals

1. Israa Shareef Jijan, Chinese Cybersecurity: A Study of Motives and Objectives, Political Issues Journal, Issue 65, 2021.
2. Islam Fawzi, Sociological and Legal Dimensions: A Sociological Analysis, National Social Journal, Volume 56, Issue 2, 2019.
3. Amna Ali Al-Bashir Mohammed, Cybersecurity in Light of the Objectives of Islamic Law, Journal of the College of Islamic and Arabic Studies for Girls, Volume 1, Issue 37, No Year Mentioned.

4. Ben Merzouk Antar, The Electronic Dimension of Algerian Security Policy in Counterterrorism, Journal of Humanities and Social Sciences, Issue 38, 2018.
5. Jamal Bouazdia, Algerian Strategy in Combating Cybercrimes and Future Prospects, Legal and Political Sciences Journal, Volume 10, Issue 10, 2019.
6. Jijan, A. S. (2022). The Cyber Influence on National Security of Active States (The United States) as a Model. Political Sciences Journal, (64), 1–18. https://doi.org/10.30907/jcopolicy.vi64.628 .
7. Hussam Abdul Amir Khalf, The Fifth Dimension in Armed Conflicts: The Cyber Space, Journal of Law, University of Nahrain, Volume 18, Issue 1, 2016.
8. Hameed, A. K. (2019). The Phenomenon of Terrorism and Violations of Human Rights after 2001. Political Sciences Journal, (54), 215–230. https://doi.org/10.30907/jj.v0i54.38.
9. Horia Shanbi, Implementing the Smart Transportation Strategy in Algeria Using Intelligent Transport Systems, Published Research in the Journal of Financial and Accounting Studies, University of El Oued, Algeria, Issue 7, 2016.
10. Khattari, R., Rashed, Z., & Zayed, A. (2023). Recruiting Individuals in Terrorist Organizations: Techniques and Methods - The UAE Law as a Model. Legal Sciences Journal, 38(1), 84-106. https://jols.uobaghdad.edu.iq/index.php/jols/article/view/638.
11. Khalid Zaher Abdullah, The Role of Criminal Legislation in Protecting Cybersecurity in the Gulf Cooperation Council Countries, Journal of Jurisprudential and Legal Research, Issue 38, 2022.
12. Khadija Khair Allah Abdul Rahman Al-Azamat, The Impact of TikTok Application on Social Values in Jordanian Society from the Perspective of University Students, Journal of Education, Ain Shams University, Issue 46, Part 4, 2022.

13. Khalaf Hussam Abdul Amir. (2019). The Integration between International Criminal Law and International Humanitarian Law in Combating Terrorism. Legal Sciences Journal, 31(4), 187-222. https://doi.org/10.35246/jols.v31is.106 .
14. Daham, M., & Muhammad, M. (2022). Legitimacy of Using Cyber Attacks in International Conflicts and International Responsibility for Them. Legal Sciences Journal, 36(4), 678-704. https://doi.org/10.35246/jols.v36i4.520.
15. Jamal Zamoura, The Importance of Cybersecurity Governance to Ensure Digital Transformation of Public Services in Algeria, Advanced Economic Research Journal, Volume 7, Issue 2, 2022.
16. Salah, M., Mahdi, M., & Hadi, A. (2023). The Priority of Jus Cogens Norms in Public International Law. Legal Sciences Journal, 38(1), 128-166. https://jols.uobaghdad.edu.iq/index.php/jols/article/view/641 .
17. Adel Abdul Sadeq, Personal Data: The Struggle for the 21st Century Oil, Arab Center for Space Research, 2018.
18. Ahmed Abdul Amir. (2023). Legal Protection of Computer Programs. Legal Sciences Journal, 38(1), 649-673. https://doi.org/10.35246/jols.v38i1.618.
19. Hadi Naeem Mahmood Al-Maliki and Abd Mustafa Salim. (2017). The Territorial Scope of International Military Operations in International Armed Conflicts. Legal Sciences Journal, 31(4), 28-57. https://doi.org/10.35246/jols.v31is.100.
20. Mustafa Ibrahim Salman, Cybersecurity and Its Impact on Iraqi National Security, Journal of Legal and Political Sciences, Volume 10, Issue 1, 2022.
21. Mona Abdel Samhan, Requirements for Achieving Information Security for Administrative Information Systems, Journal of Education, Mansoura University, Issue 111, 2020.

22. Nabil Mohammed Abdul Rahman Hayder, The Effectiveness of Arab Laws and Regulations in Combating Cybercrime, Arab Journal of Scientific Publishing, Issue 37, 2021.
23. Muslim Nibras Ibrahim. (2017). War Crimes and Crimes of Aggression in the Jurisprudence of the International Court of Justice. Legal Sciences Journal, 31(4), 223-246. https://doi.org/10.35246/jols.v31is.107.
24. Mustafa Ibrahim Salman, Cybersecurity and Its Impact on Iraqi National Security, Journal of Legal and Political Sciences, Volume 10, Issue 1, 2022.
25. Mahmoud Luma Abdel Baqi and Keitan Israa Nader. (2021). International Responsibility for Damages Caused by Cyber Attacks. Legal Sciences Journal, 36(December), 336-362. https://doi.org/10.35246/jols.v36i0.435.

Fourth: Foreign sources

1. Chamiak, Eugene & McDermott, Drew, Introduction to Artifical Intelligens, Addission Wesley Publishing Company, Canada 198.
2. Deloitte, Cybersécurité éclairée Gérer les cyberrisques grâce à la cybersécurité éclairée, 2018.
3. European Parliament, Civil Law Rules on Robotics of 2017, paragraph 1.
4. European Parliament, Civil Law Rules on Robotics of 2017, paragraph 1. .
5. Gorge Luger and Nathan Stubblefield, Arthaal Intelligence: Structures and Strategies for Complex Problem Sabang, Benjamin/Cummings, California, 1995.
6. Hangeland, Arial Intelligence TheVery Idea, MIT Press, USA, 1985.
7. Hugo Loiseau, Daniel Ventre, Cybersecurity in Humanities and Social Sciences,WILEY, Volume 1.
8. Jack Copeland, Diane Proudfoot, The Computer, Artificial Intelligence, and the Turing Test. In: Teuscher , Alan Turing: Life

and Legacy of a Great Thinker, Springer, Berlin, Heidelberg, 2004.

9. Luisa Dall'Acqua ,Transdisciplinary Perspectives on Risk Management and Cyber Intelligence , Volume1, 2020.
10. Mohiuddin Ahmed, Explainable Artificial Intelligence for Cyber Security, Next Generation Artificial Intelligence, Springer ، Volume1025 ،2022.
11. Parlement européen, Cadre pour les aspects éthiques de l'intelligence artificielle, de la robotique et des technologies connexes ,2020.
12. Proposal for a Regulation of The European Parliment and of the Council OF Laying Down Harmonised Rules on artifical inteIligence (artifical Intelligence act) and amending certain union , Brussel, 2021.
13. Proposal for a Regulation of The European Parliment and of the Council OF Laying Down Harmonised Rules on artifical inteIligence (artifical Intelligence act) and amending certain union , Brussel, 2021.
14. Ray Kurzweil, The Age of Intelligent Machines, Dai Nippon, Japan, 1990.
15. Rich , Elaine, Arficial Intellegeme, McGraw-Hill, Inc., Singapore, 1984
16. Richard Kemmererm, University of California Santa Barbara, Department of Computer Science , Volume 1,2003.
17. Robert Walters, Marko Novak , Cyber Security, Artificial Intelligence, Data Protection & the Law, Springer , 2021
18. Tadas Limba and other, Cybersecurity management model for critical infrastructure, The National Journal Entrepreneurship and Sustainability ،Volume 4, 2017.