وزارة التعليـم العالـي والبحـث العلمـي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

UNIVERSITE
Abdelhamid Ibn Badis
MOSTAGANEM

جامعة عبد الحميد بن باديس مستغانم

كلية الحقوق والعلوم السياسية

المرجع: .....

قســـم: القانون العام

مذكرة نهاية الدراسة لنيل شهادة الماستر

الإرهاب السيـبراني وإشكـــالية مكافـحته في القانون الــدولي

ميدان الحقوق والعلوم السياسية

الشعــبة: حقوق

التخصص: قانون دولي عام

من إعداد الطالب(ة):

قــدور بوخاتمي

تحت إشراف الأستاذ(ة):

جلطي أعمر

أعضاء لجنة المناقشة

الأستاذ(ة)....بن عوالي علي.....رئيسا

الأستاذ(ة).....جلطي أعمر.....مشرفا مقررا

الأستاذ(ة).....فرحات حمو.....مناقشا

السنة الجامعية: 2025/2024

نوقشت في : 17/ 06 /2025 م

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي و البحث العلمي
جامعة عبد الحميد بن باديس-مستغانم

UNIVERSITE
Abdelhamid Ibn Badis
MOSTAGANEM

كلية الحقوق و العلوم السياسية
مصلحة التربصات

SENOUSSA Khadidja

تصريح شرفي خاص بالالتزام بقواعد النزاهة العلمية في إنجاز البحث

أنا الممضي أدناه،

السيد: قدور بوخاتمي الصفة: طالب

الحامل لبطاقة التعريف الوطنية رقم: 103663349 والصادرة بتاريخ: 2017/03/02

المسجل بكلية: الحقوق والعلوم السياسية قسم: القانون العام

والمكلف بإنجاز مذكرة ماستر بعنوان:

الإرهاب السيبراني واشكالية مكافحته في القانون الدولي

أصرح بشرفي أني ألتزم بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المهنية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه.

التاريخ: 2025/06/17

إمضاء المعني

نظرا للشرعية أمام [illegible] الأمر
السيد: بوخاتمي
قدور
2025 جوان 18

* ملحق القرار الوزاري رقم 933 المؤرخ في 28 جويلية 2016 الذي يحدد القواعد المتعلقة بالوقاية من السرقة العلمية و مكافحتها

إهداء

أهدي تخرجي وثمرة جهدي الى من كانا مصدر الدعم والعطاء لي

والداي.

شكر

بسم الله الرحمن الرحيم

﴿ رَبِي أَوْزَعْنِي أَنْ أَشْكُرَ نِعْمَتَكَ الِتي أَنْعَمْتَ عَلَيَ وَعَلَى وَالِدَيْ وَ أَنْ أَعْمَلَ صَالِحًا تَرْضَاهُ وَأَدْخِلْنِي بِرَحْمَتِكَ فِي عِبَادِكَ الصَالِحِينَ.﴾ سورة النمل الآية 19 .

أتوجه بخالص الشكري وإحترامي إلى الأستاذ الدكتور جلطي أعمر الذي تكرم بإشرافه على هذا العمل وعلى نصائحه القيمة ،فجزاه الله عني كل خير.

كما لا يفوتني أن أتشكر أعضاء لجنة المناقشة على قبولهم مناقشة هذه المذكرة ، وإلى كل أساتذتي الأفاضل وزملائي الطلاب والطاقم الإداري والى كل من قدم لي يد المساعدة .

بـــوخـــاتمي قـــدور

قائمة المختصرات

باللغة العربية

ج . ر: جريدة رسمية .

ص: صفحة .

ص ص: من صفحة..... إلى صفحة.....

باللغة الأجنبية

ANSSI: Agence Nationale De La Securité Des Systèmes D'Information.

ARPANET: Advanced Research Projects Network.

BIOS: Basic Input Output System.

dDOS:Distributed Denial Of Service.

FATF:Financial Action Task Force.

FBI: Federal Bureau Of Investigation.

GIS:Geographic Information System.

GPS: Global Positoning System.

IDS: Intrusion Detection Systems.

IP: Internet Protocol.

ISOC:Internet Security Opérations Command.

ITU: International Telecommunication Union.

NSA: National Security Agency.

RGPD: Règlement Général sur la Protection des Données.

SCADA: Supervisory Control And Data Acquisition.

USB: Universal Serial Bus.

VPN: Virtuel Private Network.

WIPO: World Intellectual Property Organization

مقدمة

مقدمة

بعد نهاية الحرب العالمية الثانية وما خلفته من خسائر بشرية ومادية مهولة ، تأسست منظمة الامم المتحدة خلفا لعصبة الأمم ، وقد آلت لنفسها عبر ميثاقها مهمة الحفاظ على الأمن والسلم الدوليين.

فظهرت محاولات لمعاقبة مجرمي الحرب عن طريق انشاء قضاء دولي جنائي، بداية من محكمتي نورومبورغ و طوكيو، مرورا بمحكمتي يوغسلافيا ورواندا ، ووصولا إلى إنشاء المحكمة الدولية الجنائية الدائمة سنة 1998 م ، لمحاكمة مرتكبي الجرائم الأشد خطورة والمنصوص عليها في المادة الخامسة من قانون روما الأساسي .

جاءت هذه الجرائم على سبيل الحصر وهي: جريمة الابادة الجماعية ، جرائم الحرب ، جرائم ضد الانسانية ، وجريمة العدوان ، ولقد تم التفصيل في هذه الجرائم وطرق التمييز بينها، ولم تدرج جريمة الإرهاب في النظام الأساسي على الرغم من أنه تم تعريفها في المشروع المنشيء للمحكمة بمايلي :" **كل إستعمال للقوة، أو العنف ضد الأشخاص، أو الأموال أو الممتلكات العامة أو الخاصة، وذلك لأغراض سياسية أو إيديولوجية** "، وتم الإشارة إليه أيضا سابقا في النظام الأساسي لمحكمة رواندا الخاصة في مادته الرابعة، التي منحت الإختصاص للمحكمة في جرائم الإرهاب دون إعطاء تعريف محدد له، أما النظام الأساسي لمحكمة يوغسلافيا فجاء خاليا من تعريف الإرهاب [1].

إصطدم إذن دور الأمم المتحدة في الحفاظ على السلم والأمن الدوليين، بجريمة لا تقل خطورة عن الجرائم سالفة الذكر ألا وهي الارهاب الدولي، فهو ظاهرة قديمة، غير مرتبطة بثقافة أو ايديولوجية أو حيز جغرافي أو دين معين، رغم محاولات البعض ربطه بالدين الإسلامي ، وأصبحت هذه الظاهرة أكثر دموية مع بداية القرن التاسع عشر ولم تقتصر على إرهاب الأفراد، أو المنظمات فقط، وإنما إمتد إلى إرهاب الدول ولعل

[1] وفاء دريدي، المحكمة الجنائية الدولية ودورها في تنفيذ قواعد القانون الدولي الإنساني، مذكرة ماجستير، جامعة الحاج لخضر، كلية الحقوق، باتنة، السنة الدراسية 2008 م – 2009 م، ص . 36 .

المجازر التي إرتكبها الكيان الصهيوني في حق الفلسطينيين وجنوب لبنان خير دليل على ذلك.

فالإرهاب بشكل خاص والعنف بشكل عام ، عرفته كل الديانات والحضارات السابقة، أفرادا أو جماعات إرهابية ومتطرفة، فهو لا دين له ولا مذهب ولا لون ولا مكان ولا زمان محدد له[2] .

إن إختلاف وجهات النظر الدولية والإتجاهات السياسية حوله، وتنوع أشكاله وتعدد أساليبه وأنماطه صعَّب من توحيد المفاهيم والإتفاق على تعريف جامع مانع له، بالإضافة إلى تنوع المعتقدات و الأيديولوجيات التي تتبناها الدول تجاهه ، فما يراه البعض إرهابا ، يراه البعض الآخر عملا مشروعا[3].كما أنه أصبح ذريعة تستعمله بعض الدول لشن هجمات على دول أخرى بحجة حربها المزعومة على الإرهاب خصوصا بعد أحداث الحادي عشر من سبتمبر 2001 التي أظهرت للمجتمع الدولي بأنه ليس هناك من هو بمنأى عن هذه الظاهرة.

لكن هذا لم يمنع المجتمع الدولي من محاولة محاربة هذه الظاهرة الإجرامية سواء عن طريق المصادقة على الصكوك الدولية الصادرة عن هيئة الأمم المتحدة، أو عن طريق بعض الوكالات الدولية كالأنتربول، واليوروبول، والأفريبول، أو عن طريق عقد إتفاقيات ثنائية، أو متعددة الأطراف، دولية كانت، أو إقليمية من أجل التعاون الدولي في تسليم أو محاكمة الضالعين في جرائم الإرهاب .

لقد كان لهذه الظاهرة الحظ الوفير من الثورة الصناعية والتطور التكنولوجي، والتقني ، فظهرت صور جديدة للارهاب متمثلة في الارهاب النووي ،

---

[2] عثمان علي حسن ،الارهاب الدولي ومضاهره القانونية والسياسية في ضوء أحكام القانون الدولي العام ،مطبعة منارة –هه ولير ،ط 1،كوردستان ،2006 ،ص.20.

[3] Madaoui Nadjia, Lounici Ali, the role of artificial intelligence in combating cyber terrorisme,IUS ETSCIENTIA,Vol.9.N°2.ISSN 2444-8478,2023,P.213. https://www.researchgate.net/publication/377340615_The_role_of_artificial_intelligence_in_combating_cyber_terrorism#full-text12:30 2025/01/01

والارهـاب البيولوجي ، والإرهــاب الكيميائي والارهاب السيبراني، وهي أشد خطورة من الإرهاب التقـليدي وهذا راجع للوسائل التي يستعملها.

إن إعـتــماد الــدول عـلى إستــخدام الشـبـكة المعـلوماتـــــية وأجــهـزة الحـواســيب فـي تسـيير مخـتلف مؤسـساتها الإنــتاجية، و الخدماتية والعـسكرية، جعـلها هدفا للهجمات السيبرانية سواء من قبل دول، أو من قبل أفراد أو منظمات، فبقــدر ما تــساهم تكــنولوجيا الإعــلام والإتــصال فــي فعـالية الأداء وسرعته و تحقيق الكفـاءة التقـنية و زيـادة الإنــتاج فـي جـميع الميادين، سواء الإقتصادية أو التجارية والصناعية والخدماتية والعسكرية إلا أنها سيـف ذو حدين، بحـيث خلقـــت فضاءا جديدا متعدد الوظائف والخصائص والسمــات، وأصـبح فــضاءا موازيا، ومـؤثرا عـلى الفـضاء المـادي الواقـعي إلى جانـب تعـدد الفئات التـي تستخـدمه، فأضحى مـصدر تهديـد للأمن القـومي للـدول، بحيـث تغـير نـمط الحروب من تـقليدي مـباشر، إلــى حـديث غـير مـباشر، كـما أصبـح مـسرحا لتـخـطيـط عملـيات إرهابـية، أو تجنيد عناصر جـديدة، أو الإشـادة بالأعمال الإرهابية، أو جـمع الأمـوال لتـمويل هـذه العـمليات، أو إخـتراق مـواقع مهـمة للـدول وسـرقة الـبيانات والمعلومات، أو الجوســسة أو إنـشاء مواقـع جهادية، بحـيث يــمكن لأي كـان الدخول على هذه المواقع والتـــعلم كيفية صنع قنـبلة يـدوية ، فهـذا الفضاء خـلق صـورة جـديدة للارهاب تهــدد السلــم والأمــن الدولـيين أصـطلح علـيه بـالإرهاب الإلكــتروني أو السيبراني.

يلتـقي الإرهاب السيـبراني مـع الإرهاب التقلـيدي فـي كثير من الأسباب والدوافع والعوامل التي أدت إلى ظهوره، ويـزيد عـنه فقـط فـي الجانـب التقني ما يجعله من الجرائم المستحدثة الأكـثر تعقـيدا وتهـديدا، كـما دعا الباحـثون والدارسـون لهـذه الظاهرة إلى الإسراع في توحيد الجهود وتفعيل آليات فعالة من أجل مكافحتها.

الإشكالية:

إن الإرهاب السيبراني هو نسخة مستحدثة للإرهاب التقليدي التي ظهرت بعد التطور التكنولوجي لوسائل الاتصالات والمعلومات، وخصوصا الأنترنت التي ألغت البعد الزماني والجغرافي بحيث أصبح العالم قرية صغيرة ، وبالتالي النصوص القانونية للارهاب التقليدي أصبحت غير قادرة على مواجهة هذه الظاهرة الجديدة **فكيف يمكن للقانون الدولي تطوير آليات فعالة لمكافحة الإرهاب السيبراني في ظل التحديات التقنية والقانونية المتزايدة** ؟ وللإجابة على هذه الإشكالية، لابد من البحث في التساؤلات التي تتفرع منها، ماهية الفضاء السيبراني؟ وماهية الارهاب السيبراني ؟ماهية الأمن السيبراني ؟ ماهو الدور الذي تلعبه الدول والمنظمات لمكافحة ومجابهة هذه الظاهرة ؟

أهمية الموضوع:

لقد أثرت العولمة والثورة التكنولوجية والتقنية على العالم ايجابا و سلبا في آن واحد، بحيث أصبح هذا الأخير قرية صغيرة، وخلقت فضاءا موازيا له اصطلح عليه بالفضاء السيبراني، يعتمد عليه في قطاعات حساسة كالصحة، والقضاء والتعليم والدفاع، وأصبح كل من يمتلك تكنولوجيا المعلومات والإتصال والمعرفة التقنية يملك ماأصطلح عليه القوة السيبرانية .

إن الجرائم التي ترتكب من طرف أصحاب الياقة البيضاء كما يحلو للبعض تسميتهم في الفضاء السيبراني، قد تتطور إلى جرائم أكثر خطورة محدثة كوارث وخيمة، وهنا لا نتحدث عن القرصنة، أو الجوسسة، أوتعطيل طرق الإتصالات، أو المواصلات، أو الإختراق وتدمير البيانات والمعلومات، أو الدعاية الإعلامية وبث التهديدات، والإبتزاز الإلكتروني وغيرها من أعمال الإرهابية السيبرانية، وإنما قد تتطور إلى هجومات نووية ، أو بكتيرية ، أو كيميائية

قـد تـؤدي إلى هـلاك مئات الألاف من الضحايا والموارد الأساسية، فيجب تحديد أسبابها من أجل مكافحتها.

إن من الأهمـية بمكان دراسـة هـذا الموضـوع كذلك وتوضيح أن القـوانين الجنائية الحالية يجب أن تتكيف مع التطور التقني للجريـمة، هذا مـن جـهة ومـن جـهة أخـرى يجـب الاستفادة مـن هـذا التـطـور التكنولوجي فـي التـصدي لـهـذه الظـاهرة خـصوصا بإستعمال تقـنية الذكاء الإصطناعي مـن أجل التنبؤ والرقابة والـتتبع ، وتحصين الـدول لفضائها السيبـراني عـن طريـق تحقيق الأمـن السيبـراني، ويجب أن ننوه بأن الحـدود الزمـانية لبحثنا تبدأ مـن تسعينات القرن الماضي إلى غاية عام 2025 م ، أما الحدود المكانية ، فجميع دول العالم .

أسباب إختيار الموضوع:

يرجـع سبـب إختـيار المـوضوع لخـطـورة وحداثة هـذه الظاهرة، فهي قديمة النشأة لكن حـديثة مـقارنة بالـوسائل الـتي كانت تستخدم من قبل، كما أنها لم تستوف حـقها من الدراسة رغم وجود بعض الإجتهادات الفقهية بحقها، ولـهذا إرتأيـت محـاولة دراسـة بعض الأبـحاث السابـقة، وجمع الآراء التي صدرت بشأنها، وتكويـن نظـرة عـامة وشـاملة حـول ما أنجـز لفهم هذه الظاهرة وتشريحها بشكل أفضل، وبالتالي الـوصول إلى آلـيات قانونية و تقنية لمكافحتها.

منهج الدراسة:

إعـتمـدت عـلى المـنهج الوصـفي التحـلـيلي لوصف الظـاهرة ، لأن كـما قـلنا آنفـا الإرهـاب السيـبراني حديـث النـشأة فهـو ناتـج عـن التزاوج بين الإرهاب التقليدي والفضاء السيـبراني ، وكـذلك لتـمييزه عن الجـرائم المشـابهة لـه وتبيان خصائصه ، دوافعه وأسبابه ، أنواعه ، ووسائله .

تقسيم البحث:

تـم الإعتماد على التقسيم الثنائي لهـذه المذكرة ، بحيث سوف أتطرق في الفصل الأول إلى مفـــهـوم الإرهاب فـي البيئـة السيـبرانية وسأحاول التعرض فـي المبحث الأول إلى ماهـية الفضاء السيبـراني، أمـا المبحـث الـثاني فسأتناول ماهـية الإرهاب السيـبراني ، و سأعـرج إلى الفـصل الثـاني الموسوم بآليات مكافحة الإرهاب السيبراني الذي قسـمته بدوره إلى مبحثين، المبحث الأول : الجهود الدولية والإقليمية لمكافحة الإرهاب السيبراني والمبحث الثاني: الآليات التقنية والفنية لمكافحة الإرهاب السيبراني وختمت الدراسة بمجموعة من الاستنتاجات والتوصيات التي رأيت من المهم الإشارة إليها.

الفصل الأول

مفهوم الإرهاب في البيئة السيبرانية

مـما لا شك فـيه أدى ظـهـور الفضاء السيبـراني في ثمانـينات القـرن المـاضي إلى إحـداث تغييـرات عـلى العالم المـادي وعـلى حياة البشرية جمعاء، لأنه متاح للجميع ويمكن التجول فيه بكـل سهـولة وبأقـل تكلفة ، وسرعة الحصول على المعلومات أو نشرها ، ولعل أهم ميزة فيه هي القدرة على التخفي أو إستعمال هوية مزورة .

وإذا كانـت هيـئة الأمـم قـد حظـرت إستعـمال القـوة فـي العلاقات الدولـية وجرّمت العدوان، فإن هذا الفضاء أصبح ساحة جديدة للصراع تستعمل فيه أنواع مختلفة من الأسلحة، كالفيروسات والديدان والبرامج الضارة الـتي يمكـنها إحـداث أضرار بالـغة الخطورة تـحاكي في أثارها الهجمات بالأسلحة التقليدية دون معرفة مصدر الهجمات ، وبالتالي أصبح متغـير أساسي وعنصر مؤثر في النظام الدولي وبديلا للقـوة الصلبة .

إن تعـبـير الفـضاء السيـبراني لـه معنـيان: المعـنى الـواسـع أي الفـضـاء المتعلق بشـبكات الحاسـوب والأنتـرنت ، وهـو فـضاء عـالمي لا يرتبط بأي نطاق محدد جغرافيا ولا تـتوفر عليه أي صلاحية قانونية وطنية ، والمعنى الضيق المعّرف بشبكة حواسيب معينة أو قـاعدة معـلومات سـواء كانـت هذه الشبكة على المستوى الوطني أو مؤسسة ما داخلية أو شبكة محلية [4]. **(المبحث الأول)**

يعـيش العالـم الـيوم عـصر الأنـترنت التي أحدثت تـطورا سريعا في قطاع تكنولوجيا المعلومات والإتصال، وخلقت أنماطـا مخـتلفة ومخاطر مرتبطة بالفضاء السيبراني، كالهجمات، والحروب السيبرانية، والصراع السيبراني، والإرهاب السيبراني، فأضحت هذه الأخيرة تهدد الأمن القومي للدول، لأنها تشن حربا غير مباشرة عـن طريـق هذا الفـضاء، حيث يستطيع أحد أطراف الصراع أن يُوقـع خسائر فادحة بالطرف الأخر في جميع القطاعات التي تعتمد على هـذا الفضاء وذلك بمجرد ضغطة زر واحـدة وخـلف المكـتب دون الـحاجة إلى تـحريك الجيوش أو القيام بعمليات عسكرية ميدانية . **(المبحث الثاني)**

---

[4] أنظر نماذج تشريعات الفضاء السيبراني في الدول الأعضاء بالإسكوا ، الإسكوا الأمم المتحدة اللجنة الإقتصادية والإجتماعية لغرب أسيا على الرابط :https://archive.org/details/20201113_20201113/mode/2up?view=theater بتاريخ 2025/03/14 على الساعة: 10:17

المبحث الأول :

ماهية الفضاء السيبراني

لا يختلف إثنان على أن العولمة والأنترنت ووسائل تكنولوجيا المعلومات والاتصال أوجدوا فضاءا جديدا أصطلح عليه بالفضاء السيبراني أو الإفتراضي أو الإلكتروني، بدأ بالإعتماد عليه أكثر خصوصا بعد جائحة كورونا بحيث أصبحت مؤسسات حيوية كالصحة والتعليم والقضاء وغيرها من المجالات المهمة تعتمد عليه، والذي أثر على عدة مفاهيم ومصطلحات قديمة كالسيادة والقوة على سبيل المثال، فبرز مصطلح السيادة الرقمية، ومصطلح القوة السيبرانية (CYBER POWER)[5] أو القوة الإلكترونية، مما خلق فواعل جديدة مؤثرة إلى جانب الدول ، سواء بالإيجاب أو السلب ، فأصبحت سيادة هذه الدول مخترقة، ومعرضة لهجمات سيبرانية من طرف دول أخرى أو منظمات أو جماعات متطرفة أو حتى من طرف الأفراد.

أصبح الفضاء السيبراني يكتسي من الأهمية بمكان ماجعل البعض يصفه بالذراع الرابع للجيوش الحديثة[6]. ورغم ذلك لم يتوصل الدارسون والفقهاء إلى وضعه في إطار

---

[5] بسب الطريقة التي تأسست بها الأنترنت في سبعينات القرن الماضي (كجزء من الأبحاث العسكرية الأمريكية Arpanet) ، ظل الجزء الأعظم من المكون المادي للأجهزة التي تقوم عليها الأنترنت داخل الولايات المتحدة الأمريكية ، ويأتي في مقدمة ذلك كابلات الألياف البصرية ونقاط تبادل الأنترنت (IXPs) ومراكز البيانات الخاصة بمقدمي خدمات الأنترنت (ISPs) ، ولذا السبب يقدر الخبراء أن نحو 80% من حركة الأنترنت اليوم تمر عبر الألياف الضوئية في أراضي الولايات المتحدة الأمريكية وذلك ما أعطاها ميزة فريدة ومثلما كشفت عن ذلك تسريبات إدوارد سنودن ، إستغلت وكالة الأمن القومي (NSA) تلك الميزة للقيام بعمليات غزيرة للرقابة على أنشطة الحلفاء والخصوم على حد سواء. للإطلاع أكثر أنظر : حشاني فاطمة الزهراء، توفيق حكيمي ، الدبلوماسية السيبرانية وجيوسياسية الفضاء السيبراني : بين مساعي الحوكمة وحسابات التنافس ، مجلة الباحث للدراسات الأكاديمية ، المجلد 11 ، العدد 2 ، جوان 2024 .على الرابط : http://dspace.univ-batna.dz/xmlui/handle/123456789/8157 بتاريخ :2025/01/05 10:20

[6] عباس بدران ،الحروب الالكترونية ،الاشتباك في عالم متغير، مركز دراسات الحكومة الالكترونية ، بيروت ، 2010 ، ص.4.

مفهومي محدد وموحد ، ويرجع البعض ذلك إلى بنيته التكوينية التي تمزج بين جانب مادي HARDWARE وجانب معنوي SOFTWARE وإلى إتساع مجال إستعمالاته ومستعمليه وتأثيره على العالم الواقعي ، وللتسييس المتنامي لهذا الفضاء بسبب تضارب المصالح والقيم و الأعراف بين الدول ، ولتفاقم قضايا التجسس والهجمات السيبرانية ونشاطات القرصنة وإختراق الشبكات[7] ، من خلال ماسبق سنتطرق إلى مفهوم الفضاء السيبراني في (**المطلب الأول**) ، وإلى مكونات الفضاء السيبراني في (**المطلب الثاني**) .

المطلب الأول :

مفهوم الفضاء السيبراني

لايوجد للفضاء السيبراني تعريف دقيق أو موحد وهذا راجع كما رأينا إلى بنيته التكوينية والتطور السريع الذي يشهده ، وسنحاول التطرق إلى تعريفه اللغوي وفي القواميس وإلى مجموعة من التعاريف المختلفة التي حاولت الإحاطة به مما يسمح لنا بتقديم مفهوم اشمل له .

الفرع الأول : تعريف الفضاء السيبراني

يتكون الفضاء السيبراني من كلمتي الفضاء والسيبرانية ، وسنتطرق إلى تعريف كل كلمة على حدى.

أولا / الفضاء لغة:

جاء في لسان العرب " الفضا ": الفضاء: المكان الواسع من الأرض ، والفعل فضا يضفو فُضُوًا ، فهو فاض... وقد فضى المكان وأفضى إذا اتسع وأفضى فلان إلى فلان أي وصل إليه ، وأصله أنه صار في فرجته وفضائه وحيزه ... والفضاء : الخالي الفارغ الواسع من الأرض ... والفضاء الساحة وما اتسع من الأرض ، يقال أفضيت إذا خرجت إلى الفضاء[8]. وهناك معاني أخرى

---

[7] فاطمة الزهراء حشاني ، توفيق حكيمي ، المرجع السابق ، ص .432 .

[8] إبن منظور ، لسان العرب ،دار صادر ، بيروت ،الطبعة الثالثة ،1414 هـ ،على الرابط : https://shamela.ws/book/1687/7769#p1 بتاريخ 2025/03/14 ، 12:49.

وردت في لسان العرب لكلمة فضاء ، لكن إكتفينا بذكر المعاني التي تهم بحثنا والتي تشير إلى الحيز والمكان.

ويقابل كلمة فضاء في اللغة الفرنسية كلمة espace ويعرفه قاموس Le Robert بالفضاء الممتد الذي لا يعيق الحركة[9] ، ويقابل الفضاء في اللغة الإنجليزية لفظ space ويعني منطقة خارج المجال الجوي حيث جميع الكواكب الأخرى و النجوم موجودة[10] ، أي أنه غير محدود ولا يمكن حصره أو معرفة من أين يبدأ وأين ينتهي .

ثانيا / السيبرانية لغة:

جاءت السيبرانية من فعل (سَيبَ) أي تركه ، وأطلق سراحه أي يذهب حيث يشاء ، وجاءت من الإسم (تسيب) وجمعها (تسيوب) ، والسَيِبُ : هو كل ما سِيَبَ وخُلّيَ فساب ، ومعناه العطاء [11].

و كلمة سيبرانية أو سايبر أو سيبراني تعتبر ترجمة حرفية لكلمة (Cyber) والمشتقة من كلمة (Cybernetics) بمعنى الحاكم أو الرائد أو قائد الدفة [12] وقد أستخدم هذا المصطلح أكاديميا من قبل عالم الرياضيات الأمريكي " **نوربرت وينر** " عام 1948 في كتابه الشهير:" علم التحكم الآلي أو التحكم والإتصال في الحيوان والآلة وذلك للإشارة إلى آليات التنظيم الذاتي [13].

وهناك من يرى بأنها مصطلح مشتق من الكلمة اليونانية (kybernetes) بمعنى القيادة والتحكم عن بعد [14].

---

[9] Espace , dictionnaire le Robert :
https://dictionnaire.lerobert.com/definition/espace

[10] space , oxford dictionnaire
https://www.oxfordlearnersdictionaries.com/definition/english/space_1

[11] أبو بكر محمد الديب ، ياسمين أحمد إسماعيل صالح ، أثر الفضاء الإلكتروني على مستقبل العلاقات الدولية " دول الشرق الأوسط نموذجا " ،المجلة المصرية للقانون الدولي ،المجلد 77 ، سنة 2021 ، ص .369. على الرابط : https://ejil.journals.ekb.eg/article_295020.html بتاريخ 2025/01/05 12:20

[12] نفس المرجع ،ص.366 .

[13] محمد كمال ،الإرهاب السيبراني عندما يستخدم الإرهابي الكيبورد بدلا من القنبلة، دار الكليم للطباعة والنشر والتوزيع، ط 1، القاهرة ، مصر،2022، ص.11.

[14] يحي ياسين سعود ، الحرب السيبرانية في ضوء قواعد القانون الدولي الانساني ، المجلة القانونية ،ص.83.

في حين أشار جانب من الفقه المعاصر، أن كلمة السيبراني أشتقت من أصل كلمة (Cyber) والتي تعني شبكات الأنترنت، شبكات الإتصال والمعلوماتية، وأنظمة التحكم الرقمية، وعند إستقراء العديد من الدراسات العربية السابقة، نجد أنها بالمجمل كانت تستخدم لفظ الإلكترونية ، والتي نعتقد بأنها غير صائبة كون إلكتروني مرادف لكلمة (electronic) وليس (Cyber)، ومن ثم بات يطلق على كل ما يتعلق بالشبكات الإلكترونية عبر الحواسيب، وتطبيقات الأنترنت وكل ماله علاقة بشبكات التواصل الإجتماعي بالسيبراني[15] ونحن نؤيد هذا الرأي.

ثالثا / تعريف القواميس للفضاء السيبراني

يعرف القاموس الإنجليزي Oxford الفضاء السيبراني بأنه " **يعتبر الأنترنت مساحة وهمية بدون موقع مادي يتم فيه الإتصال عبر شبكات الكمبيوتر** "[16]، كما يعرفه قاموس Larousse الفرنسي على أنه " **فضاء إفتراضي جمع بين ثناياه متصفحي الأنترنت وموارد المعلومات الرقمية التي يمكن الوصول إليها من خلال شبكات أجهزة الكمبيوتر**"[17]

كما تعرف موسوعة ويكيبيديا الفضاء السيبراني بالوسط الذي تتواجد فيه شبكات الحاسوب ويحصل من خلالها التواصل الإلكتروني ، وبمفهوم أشمل يعرف بأنه مجال مركب مادي وغير مادي يشمل مجموعة من العناصر هي: أجهزة الكمبيوتر، أنظمة الشبكات والبرمجيات، حوسبة المعلومات، نقل وتخزين البيانات، ومستخدمي كل هذه العناصر[18].

رابعا :التعريف الإصطلاحي للفضاء السيبراني

ظهر الفضاء السيبراني في بداياته في المجال العسكري قبل ان يتوسع ويتم إستغلاله في المجال المدني وفي نشاطات متعددة وخصوصا النشاط التجاري ، يرتكز هذا

---

[15] علي حيدر ، الإرهاب السيبراني، جامعة كربلاء، نوفمبر 2023،ص .03 .على الرابط:
https://www.researchgate.net/publication/375895130

[16] cyberspace, oxford dictionary :
https://www.oxfordlearnersdictionaries.com/definition/english/cyberspace?q=cyberspace

[17] cyber monde, dictionnaire Larousse :
https://www.larousse.fr/dictionnaires/francais/cybermonde/21258

[18] أنظر تعريف الفضاء السيبراني على الرابط:https://2u.pw/Yaa6t بتاريخ :2025/03/15 : 13:08

الفـضاء أساسا عـلى مختـلف الوسـائل التكنولوجية ، ولقد أصبح خلال وقت قصير فضاء تـبادل ومواجهات بين اشخاص متعددين[19].

أستخـدم المصـطلح لأول مـرة مـن قـبل "**ولـــيام جبـــــــسون**" فـي روايـتـــــــه الرومانسـيون الـجـدد الـتي نشـرت فـي أمريكا عام 1984 م حيث ينشئ الناس عالما، وهو ليس مكـانا واقعـيا كـما أنه ليس فضاء حقيقـيا بـل هـو مكـان خـيالي أو وهـمي، ينـشأ مـن خـلال النـقـر عـلى لـوحة مفـاتـيح الحـــاسب.

يعّـــرف " **فريديـريك مايـور**" **ذلـك الفـضاء الإلكـتروني أو المعلـوماتي بأنـه بيـئة إنـسانية وتكـنولوجية جـديدة للتعبـير و تبـادل المعلومات وهـو يتـكون أسـاسا مـن الأشخـاص الـذين يـنتـمون لكـل الأقـطار والثـقافات واللّغات والأعـمار والمهـن المرتبـطة ببعـضها البعـض عـن طريق البنية التحتـية الاتصالية الـتي تسمـح بتـبادل المعلومات ونقـلها بطريقة رقـمية**[20]. فـقد جـمع هذا التـعريف بـيـن الأشخاص الفاعلين مـن مخـتلف الأمـاكن والثـقـافات واللـغات والأعـمار والـمهـن، الـذين يستعـــــملون هـذا الفـضاء للتعـبير وتبـادل المعلومات بطريقة رقمية عن طريق أجهزة تكنولوجية متصلة ببعضها البعض.

وعرفـته الوكـالة الفـرنسية لأمن أنـظمة الإعلام **ANSSI**، وهي وكالة حكومية مكـلفة بالدفـاع السـيبراني الفـرنسي، بأنه " **فـضاء التـواصل المشكـل مـن خـلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية** "[21]. فهـو حسـب الـوكالـة مـجـموعة مـن الـمعدات الذكية سـواء كانـت أجهـزة حواسيـــب أو هواتـــف ذكـية أو لـوحات إلكترونية أو أي جهاز بـمقـدوره مـعالـجة البـيـانات بـطريقة آلـية وتـكون مـــرتبـطة

---

[19] Dr.Yasmine Abdel Moneim ,les répercussions du cybertérrorisme sur la paix et la sécurité internationales,prevue égyptienne de droit international,Vol 75,2019,P.22.

[20] وداد سميشي، الحوار الالكتروني والفضاء العام الافتراضي، منتديات النقاش الالكترونية نموذجا، **مجلة العلوم الانسانية** ، مجلد ب ،عدد 41 ، جامعة قسنطينة، الجزائر، جوان 2014 ، ص ص .570.

[21] إسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، **مجلة العلوم السياسية** ، المجلد 10 ،العدد 01 ، جامعة الشهيد حمة لخضر ، الوادي ، الجزائر ، أفريل 2019 ، ص ص.1016-1031. https://www.asjp.cerist.dz/en/article/91423 :

بـــينها عـن طـريق شـبكة أنـترنـت مـشكلـة فـضاء للـتواصل بـين مستـــــخدمين (المرسل و المتلقي). ومما يلاحظ من هـذا التعـريـف أن الوكـالة ركـــزت عـلى الجانب التقني فـقـط في حين أهـملت أهم عنـصر وهو العنصر البشري الذي يعد أحد الأسـس لتكـوين هـــذا الفـضاء. وتـم تعـريفه أيضا " على أنه بيـئة تفاعلية حديثة، تشمل عناصر مادية وغير مـادية، مـكون مـــن مجـموعـة مـن الأجهـزة الرقـمية، وأنـــظـمة الشـبكات والبـرمجيات، والمستخدمين سواء مشغلين أو مستعملين" .

عـرّفه **عـلي رحـومة** فـي كـتابه " عـلم الإجتـماع الآلي " أنه " قـــناة رقمية إلـــكترونية داخـل مســـافات متـشابكة مـن خـــطوط ، وقـــنوات إتـصال معـدنية ، وضوئية ، وهوائية ، فـي شبكة الشبكات ، أي " الأنترنت " ويشار إليه تكنولوجيا ، بأنه طريـق للمعلومات فائـق السرعـة ، متمـدد ، ومـتسع لمساحات هائـلة من الإنطـلاق الحركي المتواصل ، في آليات تفـاعلية للعـقول الإنـسانية ، والحاسوبـية بأنواعها ، ومن خلال هذا الفضاء يحدث التفاعل البـشري الآلي ، عـقليا ، ونـفسيا ، وإجـتماعيا ، بمختـلف الحواس الإنسانية ، وكذلك الآلية ، وفـي هـذا الفضاء أيضا ، يتشكل مجتمع الأنترنت ، متكونا من أعضائه الكونيين ، الأفراد ، و الـجماعات البشـريين ، في علاقتهم بعضهم ببعض ، بمختلف الخصائص التي تفرضها هذه البـيئة الإنسانية الآلية "[22] .

وعـرفه عبد القادر محمد فهمي بأنه : **يمـثل مجموع شبكات الحاسوب في العالم ، وكـل ماترتـبط بـه وتـتحكم فـيه هـذه الشبكات . و هـو لا يقتصر على شبكة الأنترنت فقط ، وإنـما يـشـمل العـديد مـن شبـكات الحـاسوب الأخرى ، فالفضاء السيبراني يشمل كـل**

[22] أنديرا عراجي ، القوة في الفضاء السيبراني : فصل عصري من التحدي والاستجابة ،رسالة لنيل دبلوم دراسات عليا في العلوم السياسية والإدارية ، كلية الحقوق و العلوم السياسية والإدارية ، الجامعة اللبنانية ، 2015-2016 ، ص .11.

شبكات الحاسوب التي تدير نشاط الدول ومؤسساتها ومرافقها وكل مايتعلق ببيئتها الحيوية ، وفي القطاعات المدنية والعسكرية[23] .

هناك محاولات عديدة أخرى لتعريف الفضاء السيبراني سواء من طرف أشخاص أو من طرف مؤسسات حكومية ، وهذا إن دّل على شيء إنما يدل على أن إعطاء تعريف دقيق لهذا الفضاء يعتبر من المسائل الصعبة حاليا ، وهذا راجع لإختلاف الرؤى والأهداف والإستراتيجيات ، خصوصا و أن هذا الفضاء هو ساحة للصراع بين الدول والفواعل الأخرى (أفراد ومنظمات وشركات متعددة الجنسيات).

وما يمكن إستخلاصه هو أن هذا الفضاء تم إنشاؤه من قبل البشر، من خلال ربط طبقات مختلفة لكل منها خصوصيتها يتطور بإستمرار مع التطور التقني والتكنولوجي ، ويرتكز على معدات إلكترونية تعمل كعقد في شبكة موسعة تتكون من هذه الأجهزة ومتصلة بتدفق من البيانات الثنائية التي يتم إرسالها من جهاز واحد إلى جهاز آخر.

الفرع الثاني: خصائص الفضاء السيبراني

يجب الإعتراف بأن الفضاء السيبراني يكتسي من الأهمية ما جعل الدول تحاول الإستثمار فيه ، فظهرت الحكومات الإلكترونية ، والدبلوماسية الإلكترونية ، الإدارة الإلكترونية والاقتصاد الرقمي وغيرها من المجالات التي تعتمد على هذا الفضاء ويرجع ذلك لمجموعة الخصائص التي يتمتع بها وأبرزها :

أولا : العالمية

الفضاء السيبراني ليست له حدود معلومة ، ويمكن لأي كان أن يبحر فيه و أن ينتقل من مكان إلى مكان فقط بضغطة زر على الحاسوب دون الحاجة إلى السفر، كما يمكنه من الحصول على المعلومات وإستنساخها وإستبدالها دون أن يتحرك من مكانه.

---

[23] صلاح حيدر عبد الواحد ، حروب الفضاء الإلكتروني ، دراسة في مفهومها وخصائصها وسبل مواجهتها ، رسالة ماجستير في العلوم السياسية ، قسم العلوم السياسية ، كلية الآداب ،جامعة الشرق الأوسط ، الأردن ، تموز ، 2021،ص.6.

ولـذلك وصـف البعـض هـذا الفـضاء بأنـه " عـالـم مـتكامل "، أو " قريـة كونـية " تقطنها مجموعات بشرية مهولة ، تعيش حياتها فيها متحدة زمانيا، – رغم إنقطاعها مكانيا – ، ويقضون أوقاتـهم فـيها بمـمارسة شـتى النشاطات ، وعددا من الفعاليات ، وصورا متعددة من التصرفات، ويعملون فـيها عـلى تـبادل مختلف الخدمات والمصالح [24]، ووصـفه البعض الآخر على أنه يمثل البعد الخامس إلى جانب البر والبحر والجو والفضاء الخارجي .

ثانيا: تعـدد مستخدمـيه

إن تعـدد المجـالات التـي يوفـرها الفـضـاء السيبـراني ، إنعـكس ذلك عـلـى الفـــئات الـتي تستخـدمه ، بحـيث يـلجأ إلـى خـدماته كـل أفراد المجتمع ، بغض النظر عن مستواهم التعـليمي أو الثقـافي أو الإجـتماعي أو جـنسهم و أياً كانـت أعمارهم ، خصوصا بعد التوجه الحديث للدول بإستعـمال الرقمـنة فـي جمـيع المـيادين والمجالات و التـوجه للإعتماد الكلي عليـها في المستقبل القريب لتـوفـير المـال والجـــهد وتحقـيقا للسـرعة والتنمية ، مما خلق نقـــاط ضعف وظهور تهديدات ومفاهيم جديدة مرتبـطة بهذا الفـضاء وبعـض المستخدمين كمصطلح الجريمة السيبرانية والإرهاب والأمن السيبراني .

ثالثا: الحـــــركية الدائمة

تبـرز هـــذه الـخاصية مـن حجـم المعـلومات والبـرامج الـتي تتدفق بإستمرار ، كإنشاء أشـخاص جـدد حسابات على مواقع التواصل الإجتماعي أو تبادل الرسائل عن طريق البريد الإلكتروني أو إنشاء تطبيقات أو التفاعل مع منشورات ، فالفضاء السيبراني وسط نشط ودائم الحـركة ولعل هـذه الخاصـية سـببت قـلقا للـدول لأنـها لا يمكـنها تحقيق الأمن أو السيطرة على هذا الفضاء .

رابعا: التفاعـــــــــــلية

ويقـصد بها حـركـة المعلومات فـــي مسلكين بـيـن المرسـل والمـتلقي بحيـث يتـبادلان الأدوار ويصبـح المتلـقي هـو المـرسل وهـذا الأخـير هـو المتـلقي ، وقوضت هذه الخاصية

[24] فايزة نجاري بن حاج علي ، مكافحة الإرهاب الإلكتروني في القانون الدولي ،رسالة لنيل شهادة دكتوراه،جامعة مولود معمري ، تيزي وزو، الجزائر، ص. 25.

من دور الدولة كفاعل وحيد في إصدار المعلومات والأخبار والأنباء، إلا أنها في المقابل قد عززت من الديمقراطية التشاركية والديمقراطية الرقمية .

خامسا: السرعة والفورية

في زمن غير بعيد كانت المراسلات والمعلومات قبل عصر المجتمع المعلوماتي تستغرق وقتا طويلا لتصل إلى وجهتها المحددة، لكن مع ظهور الإتصال الشبكي في الفضاء السيبراني أصبح لا يستغرق ذلك إلا بضع ثواني أو أجزاء من المئة ، لأنه ألغى الحاجز الزماني والمكاني فلا يشترط أن يكون المتلقي متصلا في الفضاء السيبراني في نفس اللحظة مع المرسل، كما يمكن حفظ هذه الوثائق إما على شكل نسخة ورقية ، أو رقمية على جهاز حاسوب ،كما يمكن إعادة إرسالها إلى جهات أخرى بضغطة زر واحدة .

سادسا: لا يخضع لأي سلطة وطنية

لا يمكن حاليا للفضاء السيبراني بمفهومه الموسع أن يخضع لسلطة معينة لأنه فضاء معقد، وواسع الإنتشار، وسهل الولوج إليه ، ومتغير وقابل للتوسيع آنيا ، ولا يمكن حصره في إقليم معين، كما أنه لا يمكن فرض تطبيق قوانين بعض الدول في إقليم دول أخرى فالقانون التايواني على سبيل المثال لا يعاقب من يصمم وينشر الفيروسات المعلوماتية ويسري هذا الأمر على نشاطات أخرى مثل غسيل الأموال وترويج المخدرات فهولاندا على سبيل المثال تسمح بتعاطي المخدرات في حين يعاقب عليها القانون في دول أخرى [25].

ولكن لا يفوتنا أن نشير إلى أن الدول المتقدمة في المجال التقني قادرة على بسط سلطتها على الشبكات الداخلية المحمية ولو بصفة نسبية ، سواء بتضييق مصدر الهجوم الذي يكون داخل إقليم الدولة أو بتطبيق قوانينها الجنائية على مرتكب الهجوم .

---

[25] فضيل دليو ، تكنولوجيا الإعلام والإتصال الجديدة بعض تطبيقاتها التقنية ، دار هومة للطباعة والنشر والتوزيع ، ط 1 ، الجزائر ، 2014 ، ص . 205 .

سابعا: صعوبة الكشف عن مرتكبي الهجمات السيبرانية

يمـثل الفـضاء السيبـراني أرضـا خصبة لكل أنواع الهجمات السيبرانية ، التي تعتبر فعلا غـير مشروع مـوجه ضد أنظمة الحـاسب، والشـبكات، والأنــظمة التــي تعـتمد عـلى التقنية عن طـريق إستـغلال نـقاط ضعف موجودة في هذه الشبكات، والأنظمة بهدف إحداث أضرار أو بغـرض الإبـتزاز أو التجـسس أو غيرها من الأهداف ويصعب تحديد مرتكبي هذه الأفعال وأماكنهم لصعوبة إن لـم نقـل إستحالة إيـجاد الدلـيل الرقـمي و إثباته فـقـد تـحـدث هـذه الهجـمات مـن داخـل الدولة أو مـن خارجها(جرائـم عابرة للحدود) وهذا راجع للبنية التكوينية و التوسعية لهذا الفضاء.

المطلب الثاني:

أهمية ومكونات الفضاء السيبراني

لابد مـن الإعتراف والتسليم بأن الفضاء السيبراني أصبح العصب الحيوي في حركة الأمم وتطـورها، فـبخلاف أنـه فـضاء للتـواصل والتبادل الإجتماعي ، أضحى مجالا تستغله الدول لتسيير مرافقها الحيوية وتقريب الخدمة من المواطن وللتأثير على السياسات الدولية الخارجية **(الفرع الأول)**، كـما أن بنـيته التكوينيـة تمزج بين المكونات المادية والبرامجية والسيميولوجية **(الفرع الثاني)**.

الفرع الأول: أهمية الفضاء السيبراني

بات يعتمد على الفضاء السيبراني في مجالات حيوية مهمة وحساسة أهمها:

أولا : الحكومة الإلكترونية

وتتـمثل في ربـط المـؤسسات مع بعـضها البعض عـن طريق الشبكة العنكبوتية العالمية بغرض الرفـع مـن كـفاءة الأداء الحكومي، وتحسين أسلوب أداء الخدمات للمواطنين[26] ، مع تمكينـهم من المشـاركة فـي عـملية صنع القـرار عـن طريـق الديمقـراطية التـشاركية والإدارة الإلكترونية وتقوم على أربعة ركائـز وهي:

[26] نزيهة عمران، الديمقراطية الرقمية:نحو تعزيز المشاركة من خلال تكنولوجيا المعلومات، مجلة العلوم القانونية والسياسية، المجلد 13، العدد 02، سبتمبر 2022، ص .342 . على الرابط: https://asjp.cerist.dz/en/article/203101

أ / – تجميع كافة الأنشطة والخدمات المعلوماتية و التفاعلية والتبادلية في موضع واحد هو موقع الحكومة الرسمي على شبكة الأنترنت.

ب / – تحقيق حالة إتصال دائم بالجمهور .

ج / – تحقيق سرعة وفعالية الربط والتنسيق و الأداء و الإنجاز بين دوائر الحكومة ذاتها ولكل منها على حدى .

د / – تحقيق وفرة في الإنفاق في كافة العناصر بما فيها تحقيق عائدات أفضل من الأنشطة الحكومية ذات المحتوى التجاري[27] ، وعليها أن تتنبه إلى قدرة مواطنيها على التعامل مع هذه التقنيات الحديثة وذلك من خلال قنوات كثيرة تسهم فيها جميع المؤسسات التعليمية كالجامعات و المعاهد و أن تقوم بتدريب موظفيها وإتاحة فرصة وصول شبكة الأنترنت إلى كافة مواطنيها و إقامة مراكز لتقريب خدمات الحكومة الإلكترونية[28]، وإنشاء خوادم وشبكات إكسترانات وأنترانات داخلية لتخزين البيانات والمعطيات وحمايتها لأنه كما هو معلوم للعام والخاص، أن الولايات المتحدة الأمريكية تتحكم في نسبة كبيرة من الأنترنت وخدمات التزويد بها وبالتالي قادرة على سرقة البيانات أو إنتهاك الخصوصية .

ثانيا: الدبلوماسية الرقمية

أصبح الفضاء السيبراني مجال جديدا للعمل السياسي والدبلوماسي وللوظيفة الدبلوماسية نفسها، فأضحى الدبلوماسي يتواصل مع شعوب البلد المضيف عن طريق أدوات وتطبيقات التواصل الإجتماعي كالتويتر، والفايسبوك، والأنستغرام كما برز دور المواطن فيها وأصبح يؤثر ويتأثر مما خلق جانبا مظلما لها ففي كتاب مذكرات (**هيلاري كلينتون**) المعنون بـ (**خيارات صعبة**) خصصت الفصل الرابع والعشرون للحديث عن الدبلوماسية الرقمية، روَّتْ قصة ناشطة من بيلاروسيا خضعت لدورة تدريبية في مجال

[27] حسين بركاتي، الحكومة الإلكترونية الإطار المفاهيمي ومنطلقات نظرية بالتركيز على بعض المؤشرات والتجارب الدولية، مجلة الدراسات الإقتصادية المعاصرة، المجلد 06، العدد 02، 2021 م، ص .452 . على الرابط: https://asjp.cerist.dz/en/article/174085

[28] سمية بومروان، الحكومة الإلكترونية ودورها في تحسين أداء الإدارات الحكومية (دراسة مقارنة)، الطبعة 01، مكتبة القانون والإقتصاد، الرياض، المملكة العربية السعودية، 2014، ص .10.

التكـنولوجيا فـي الولايـات المتحـدة الأمـريكية دون علم بلـدها عندما سألتـها عـن قلقها مـن مـواجهة العواقـب لـدى عودتها لبلدها ، ليكون رد الفتاة :" فلتـذهب إلى الجحيم"، هذه الدورات التـدريبـية إنتـهجتـها ولجـأت إليـها وزارة الخارجية الأمـريكـية، مـن أجـل مساعـدة المجتـمع المـدني علـى تعلم طريـقـة إستـخدام التكـنولوجيا، بـهدف تطـوير أعـمالـــــهم ومـواجهة الإضطـهاد فـي الدول صاحبة الأنظمة القمعية من وجهة نظر الأمريكان [29] .

كما أنـه علـى سبـيل المثال إستطاع " **ليفي هيرفي برنار** " تأجيج و إثارة بعض الشعوب في الـدول العـربية ومنطـقة الشرق الأوسط على زعمائهم وقلب أنظمة الحكم وهو ما أصطلح عليه بالربيع العربي.

والتاريخ مليء بالأمثلة عن دور المواطن والصحافة في مجال الدبلوماسية الرقمية كالأزمة الجزائـرية المصـرية من أجل مباراة في كرة القدم للتأهل للمونديال وتدخل بعض العقلاء لحل الأزمة عن طريق إستعمال الوسائل المتاحة في الفضاء السيبراني.

ثالثا: التقاضي الإلكتروني

توجـهت بعـض الـدول إلى التقاضـي الالكـتروني عن طريق توظيف تقنيات ونظم يوفرها الفضـاء السـيبراني، ويعـرف بأنـه : " **نـظام تقني من خلاله يمكن للمدعي أن يرفع دعواه، يسجـلها ويـقدم المـستندات، يحـضر الجلـسات، ويصدر الحكم في النزاع دون أن ينتقل إلى مبنى المحكمة، وذلك بإستخدام وسائل الإتصال الإلكتروني** "[30]، ويـــتم كـــل هـــــذا عن طريق المحكمة الالكترونية .

---

[29] نضال محسن الشرافي، الفضاء الإلكتروني والدبلوماسية ساحة الصراع الجديدة في القضية الفلسطينية، المركز الديمقراطي العربي للدراسات الاستراتيجية، الإقتصادية والسياسية، الطبعة الأولى ، برلين، ألمانيا، أبريل 2021 م، ص. 73 .

[30] ليلى عصماني، نظام التقاضي الإلكتروني آلية لإنجاح الخطط التنموية، **مجلة الفكر**، العدد 13، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر، فيفري 2016 م،ص .217 .على الرابط: https://www.asjp.cerist.dz/en/article/62437

رابعا : التجارة الإلكترونية

تـعتبر التجـارة الإلـكترونية مـن بـين المـظاهر الـتي تبرز أهمية الفضاء السيبراني وذلك مـن خـلال المزايا التي يوفرها لها كالترويج والتسويق لسلع أو خدمات معينة من أجل كسب المـزيد مـن الزبـائن و قـد عرفـتها مـنظمة التجـارة العالمـية عـلى أنـها: " **أنشـطة إنـتاج السلع والخدمـات وتـوزيعها وتسويقـها وبيـعها أو تسليمها للمشتري من خـلال الوسائط الإلكترونية** "[31].

خامسا: الإقتصاد الرقمي

يوفر الفضاء السيبراني كما هائلا من المعلومات مما يسمح من تدفق السلع والخدمات، وإنـتقال رؤوس الأمـوال متخطية الفواصل الزمانية والمكانية، ويعرف الإقتصاد الرقمي على أنه: " **التفاعل والتكامل والتنسيق بين تكنولوجيا المعلومات وتكنولوجيا الإتصال من جهة أخرى، بما يحقق الشفافية والفورية والإتاحة لجميع المؤشرات الإقتصادية المساندة لجميع القرارات الإقتصادية، والتجارية، والمالية في الدولة خلال فترة ما** "[32] .

إلى جانب ماذكرناه دأبت الدول إلى توظيف الفضاء السيبراني في قطاعات أخرى حيوية وحساسة ، كقـطاعي الصحة و التعـليم وقـطاع الثقـافة والقطاع العسكري الذي يعتبر اللبنة الأولـى في ظهور هـذا الفـضاء، وبالـتالي تـنبع أهميـته مـن خلال المجالات التي تستعمله ولهذا تحرص الدول على تحقيق الأمن السيبراني لهذه القطاعات.

الفرع الثاني :مكونات الفضاء السيبراني

يـتكون الفـضاء السيبـراني مـن الطـبقـة الماديـة (hardware) التـي تمـثل الجـزء الأساسي التي يقـوم عليها **(أولا)** ، والطبقة المنطقية أو البرامجية (software) التي تُشَغِل

---

[31] أمل تباني ، سعدة مريمد ، واقع ومستقبل التجارة الإلكترونية في الجزائر، مذكرة ماستر تخصص مالية وتجارة دولية،جامعة 08 ماي 1945 م،كلية العلوم التجارية والإقتصادية وعلوم التسيير، قسم العلوم التجارية، قالمة، 2019م/2020م، ص. 02.

[32] كنزة تنيو و محمد دهان، دور الإقتصاد الرقمي في تحقيق جودة الحياة: دراسة مقارنة بين الجزائر والإمارات، مجلة الإستراتيجية والتنمية، العدد 03 مكرر(الجزء الأول)، المجلد 09، 2019 م، ص ص .364-385.على الرابط: https://asjp.cerist.dz/en/article/98416

الطبقة المادية وتكون هدفا للهجمات السيبرانية **(ثانيا)** ، والطبقة السيميولوجية التي تتكون من كل المحتويات والمعلومات والبيانات المتنقلة عبر الربط الشبكي، والعنصر البشري الذي يعتبر جزء من الطبقة المعلوماتية سواء كمنشيء لها أو كمتلقي **(ثالثا)** .

أولا: المكونات المادية للفضاء السيبراني

لا يمكن الحديث بأي حال من الأحوال عن الفضاء السيبراني دون الحديث عن أجهزة الكمبيوتر، أو دون الأجهزة الذكية، وقنوات الوصل و الربط بينها عن طريق الكوابل أو الساتيلايت .

أ/ - الحواسيب (أجهزة الكمبيوتر)

يعرف الكمبيوتر أو الحاسوب على أنه آلة مكونة من مجموعة من الوحدات(وحدات إدخال ، وحدات تخزين ، وحدات معالجة ، وحدات إخراج) التي تقوم بمعالجة المعلومات والبيانات بطريقة أوتوماتيكية ، منطقية ، وسريعة ودقيقة، ظهر أول حاسوب سنة 1951 م كأول جهاز يدخل في الخدمة العمومية [33]وقد وصل إلى شكله الحالي وتنوعت أشكاله وخدماته فهناك أجهزة حاسوب شخصية (مكتبية أو محمولة) وحواسيب عملاقة قادرة على معالجة كم هائل من البيانات والمعطيات تعمل كخوادم .

ب/ - الأجهزة الذكية

الأجهزة الذكية هي الهواتف النقالة الحديثة والمتطوّرة التي ظهرت في الوقت الحاضر، خلفا للهاتف الكلاسيكي الثابت الغير قابل للنقل بحيث لا تحتاج إلى الربط بالأسلاك أو الكوابل لأنها تعتمد على موجات الراديو ، كما تحتوي على نظم تشغيل متطورة كنظام الأندرويد ونظام IOS وغيرها من الأنظمة ، وعلى خلاف أسلافها يمكن القيام بالعديد من الأمور من خلالها ، فهي لا تقتصر على الاستقبال والإرسال فقط ، بل تتعدى إلى القيام بعمليات التصفح المختلفة على شبكة الإنترنت، وتحميل العديد من التطبيقات الخاصّة بكل جهاز، عن طريق المتجر المتوفر فيها، وإجراء

[33] للإطلاع أكثر أنظر الحاسوب على موقع ويكيبيديا الموسوعة الحرة من خلال الرابط:https://2u.pw/Ui1HW

إتصالات مرئية ، مشاهدة القنوات وغير ذلك من الخدمات المتاحة كما أنها تعمل بخاصية اللمس .

إلى جانب الهواتف الذكية ظهرت الأجهزة اللوحية tablette التي تعرف بأنها : " **التطور الحاصل على أجهزة الكمبيوتر المحمول** "[34] .

ج/ - الكوابـــــل

تعتبر الكوابل البحرية التي تربط القارات العمود الفقري التي تقوم عليه كل أشكال الإتصالات الأرضية بحيث تقوم بنقل البيانات والمعطيات ، و قد أنشأ أول كابل بحري عام 1858 م لربط خطوط التليغراف عبر المحيط الأطلسي ليكتمل ربط كل القارات بإستثناء القارة الجنوبية عام 1871 م [35] ، ومع التطور التكنولوجي ومن أجل تحسين سرعة وجودة نقل البيانات صوتا وصورة عن طريق الأنترنت ظهرت تقنية الألياف الضوئية أو الألياف البصرية التي تصنع من زجاج خاص نقي للغاية، تكون طويلة ورفيعة ولا يتعدى سمكها سمك الشعرة. يجمع العديد من هذه الألياف في حزم داخل الكيبلات الضوئية، وتستخدم في نقل الإشارات الضوئية لمسافات بعيدة جداً.يقوم مبدأها على ظاهرة الانعكاس الكلي [36].

د/ - الساتيلايت

توفر الأقمار الصناعية التي تدور حول الأرض الأنترنت الفضائي وهو أنترنت لاسلكي ، يضمن تغطية عالمية خصوصا المواقع التي لا يصلها الأنترنت الأرضي ، يعمل بإستخدام موجات الراديو التي تتصل مع الأقمار الصناعية ، ويجري إرسال البيانات وإستردادها من خلال شبكة إتصالات تبدأ بجهاز هوائي وتنتقل عبر المودم وطبق القمر

---

[34] حنان ولهي ، تكنولوجيا اللوحات الرقمية والادمان الإلكتروني لدى الأطفال المرافقة حل وسط بين الإتاحة والرقابة ، مجلة الدراسات ، المجلد 12 ، العدد 01 ، ماي 2023 ، ص. 341 . على الرابط :https://asjp.cerist.dz/en/article/222569 بتاريخ 2025/03/22

[35] للإطلاع أكتر أنظر كابل إتصالات بحري على موقع ويكيبيديا الموسوعة الحرة من خلال الرابط:https://2u.pw/bNaqQ

[36] ساهره مالك كاظم مغير ، الألياف الضوئية البصرية ، جزء من متطلبات نيل درجة البكالوريوس في علم الفيزياء ، جامعة بابل ، جمهورية العراق ، 2022 ، ص . 10 .

الصناعي ، إلى قمر صناعي في الفضاء ، ثم تعود إلى الأرض إلى مراكز عمليات الشبكة، بعد ذلك ، تنتقل البيانات مرة أخرى عبر هذه الشبكة ، لتخرج إلى الفضاء ثم تعود إلى طبق القمر الصناعي على الأرض ، لتوصيل البيانات إلى الجهاز[37]، ويمتاز الأنترنت الفضائي عن طريق الساتيلايت بالسرعة الفائقة كما أنه يمتاز بالجودة وعدم التأثر بكثرة المستخدمين.

ثانيا: المكونات البرامجية للفضاء السيبراني

تحتاج الطبقة المادية للفضاء السيبراني إلى الطبقة المنطقية أو البرامج لكي تشتغل ، فبدون هذه الأخيرة تبقى مجرد أجهزة إلكترونية دون فائدة، وتعرف هذه البرامج على أنها فكر الحاسب لأنها تقوم بترجمة لغة الإنسان إلى لغة الآلة في شكل خوارزميات وتنقسم إلى نظم تشغيل، وبرامج تطبيقية أو مكتبية، برامج الإتصال و تشغيل الشبكات (الداخلية والعالمية) .

ثالثا : المكونات السيميولوجية

ويقصد بها الطبقة البشرية و المعلوماتية ، فالبشر هم المنتجون للمعلومة وهنا تجدر الإشارة إلى التمييز بين الفئة المنتجة كالمبرمجون، ومقدمي الخدمات، والإعلاميون، والفئة المستهلكة، والمستفيدة من الخدمات والمزايا التي يقدمها الفضاء السيبراني كما يجب التمييز كذلك بين المعلومة المتاحة للجميع والمعلومة المحمية .

و إستخلاصا لما سلف يمكن القول أنه لا يوجد تعريف جامع موحد ودقيق للفضاء السيبراني لكن المؤكد أنه أحدث تغييرات في العلاقات الدولية وفي المفاهيم التقليدية كالسيادة والقوة والأمن وهذا راجع إلى خصائصه وبنيته التركيبية وكذا إلى إعتماد الدول على تسيير مؤسساتها عليه خصوصا بعد جائحة كورونا، كما أظهر الفضاء السيبراني الفجوة الرقمية بين الدول نظرا للتباين في القدرات التكنولوجية و اللوجيستيكية و البشرية فهناك دول تعتمد على هذا الفضاء في جميع الميادين فظهرت الحكومة الالكترونية

[37] للإطلاع أكثر أنظر الإنترنت الفضائي على موقع ويكيبيديا الموسوعة الحرة من خلال الرابط:https://2u.pw/tXcPe

و الديمقراطية التشاركية والاقتراع الرقمي والدبلوماسية الرقمية و التقاضي الرقمي إلى جانب الإقتصاد الرقمي مما خلق أنمطا جديدة للجرائم الإلكترونية أخطرها الإرهاب السيبراني .

كما تأثر علم الإجتماع كغيره من العلوم بهذا الفضاء في القرن الواحد والعشرين، وبرز فرع تخصصي جديد يدرس فئات المستخدمين للشبكة، وأنماط شخصيتهم والمواقع التي يزورونها وموضوعات إهتماماتهم، وغير ذلك من المسائل أصطلح عليه علم إجتماع الفضاء السيبراني (Cyber Sociology)[38].

المبحث الثاني :

ماهية الارهاب السيبراني

يعتبر الإرهاب من أخطر الظواهر الإجتماعية التي تهدد الأمن الدولي، وإستقرار العلاقات الدولية ، كما أنها تشيع الخوف والفزع في نفوس الأبرياء ، ولا تقتصر هذه الظاهرة على دولة دون أخرى سواء كانت ذات نظام ديكتاتوري أو نظام يدعي الديمقراطية ولعل خير دليل على ذلك ماحدث في الحادي عشر من سبتمبر 2001م في الولايات المتحدة الأمريكية .

كان الإرهاب التقليدي يستخدم التفجيرات، والاغتيالات، والتخريب، والاختطاف، وتحويل مسار الطائرات، وبعد التطور التكنولوجي والتقني لوسائل الاتصال والربط الشبكي بين الملايين من الحواسيب عن طريق الأنترنت و التوجه الجديد للدول بالإعتماد عليها في مجالات مختلفة، ظهر الفضاء السيبراني كميدان حديث للجماعات الإرهابية، بحيث وفرت شبكة الأنترنت لهذه الجماعات إمكانية الدعاية، والتحريض، والتمويل، والتدريب ، والتهديد الالكتروني وحتى تنفيذ هجومات يمتد أثرها إلى الفضاء المادي .

لقد حاول ولا يزال الفقهاء والباحثون ايجاد تعريف موحد و أسباب هذه الظاهرة من أجل القضاء عليها في المهد ، لأن الإتفاق على تعريف موحد من شأنه من أن يوحد

[38] نضال محسن الشرافي،المرجع السابق، ص.58.

الجهـود الدوليـــة للقـضاء عليـه وإستئـصاله مـن جـذوره ، لكن تغليب المصالح السياسية لبعض الدول وأخص بالـــذكر الدول العظمى حال دون ذلك.

وسنـحاول في هـذا المبحث عرض بـعـض تعريفـات للارهـاب السيـبراني وأنـواعـــــه وتمـييزه عـن الجرائم المشابهة له وأسبابه ووسائله وأهم الخصائص التي تميزه.

المطلب الأول:

مفهوم الإرهاب السيبراني

الإرهـاب السيبراني هـو جـريمة مستـحـدثة ومـستجدة للإرهـاب التقـليدي وهـي وليـدة التحولات الـتي شهـدتها الحـياة المعـاصرة ، من تقدم تكنولوجي لتكنولوجيا الإعلام والإتصال (الأنترنت) و لـظاهرة العولمة ولتـحديد مفهـومه يجـب أولا تحـديد مفـهوم الإرهاب وذلك من أجل إزالة اللبس والغموض حول هذه الظاهرة .

كما قلنا سابقا لا يوجـد تعريـف متـفق عـليه دولـيا لمفـهـوم الإرهاب ، فـهذا الأخـير يعتبر مصطلح سـياسي أقـرب إليه من مصطلح قانـوني، ولـقد تعـددت التعاريف وإختلفت فـي شـأنه الإجتهادات، و وجـهات النـظر ولـم يصل المجـتمع الـدولي حتى الآن إلى تعريف موحد، فهـو مـن بـين المفاهيم الـتي أثـارت الـجدل بـين الفـقهاء، والسياسيين، والحقـوقيين، والإجتماعيين ، ويـرجع مـرّدُ ذلك، إلـى عـدة أسباب ، أهمـها الخـلط بيـن العنـف المشروع والعنـف غيـر المـشروع ، فـما يراه البعض إرهاباً يراه البعض الآخـر عـملاً مشروعاً و كذلك إلى تغليب المصالح الدولية، ويكـفي أن نستدل فـي هـذا المقام على موقف الولايات المتحدة الأمريكـية التي تـرى عـلى أن تعـريف الإرهاب يـجب أن يتـضمـن جـميع أعـمال العـــنف الفــرديــة ، إلى جانـــب ذلك أعـمال المقاومة المسلحة مـن أجـل مقاومة الإحتلال والحصول على الإستقلال .

الفرع الأول : التعريف بالإرهاب

سنحاول تحديد تعريـف الإرهاب لغويا وفقهيا و إصطلاحا .

أولا:التعريف اللغوي للإرهاب

كلمة الإرهاب في اللغة العربية تعني الخوف والرعب ، فالإرهاب مصدر أرهب ، ومادتها رهب، ومصدره رهباً [39].

وفي القاموس الفرنسي LAROUSSE تعني كلمة " terreur " الخوف المفزع العنيف الذي يشل [40].

وفي القاموس الإنجليزي OXFORD يقصد به (إستخدام فعل العنف لتحقيق أغراض سياسية أو إجبار الحكومة على التصرف)[41].

وفي المعجم السياسي نجد كلمة أرهب تعني محاولة نشر الفزع والذعر لأغراض سياسية[42] . والإرهاب وسيلة تستخدمها دولة لإشاعة الروح الإنهزامية لدى شعب من الشعوب ويكون نشر الفزع والرعب عن طريق إستخدام العنف أو التهديد به كالإغتيالات والتخريب بغرض تحقيق هدف سياسي ككسر روح المقاومة مثلا.

فالملاحظ على التعاريف اللغوية أغلبها تربط بين الإرهاب و تحقيق أهداف سياسية وهذا راجع لإعتبارات تاريخية إرتبطت بظهور هذا المصطلح، لكن في عصرنا الحالي تعددت أسبابه وأهدافه بعدة عوامل قد تختلف حسب الجهة التي تستخدم هذا العنف إلى أهداف شخصية أو إعلامية أو إجتماعية أو دينية أو حتى إنتقامية ...إلخ.

وقد وردت كلمة الإرهاب في القرآن الكريم في أكثر من موضع كما في قوله : ﴿ **وَأَعِدُّوا لَهُمْ مَا اسْتَطَعْتُمْ مِنْ قُوَّةٍ وَمِنْ رِبَاطِ الْخَيْلِ تُرْهِبُونَ بِهِ عَدُوَ اللَّهِ وَعَدُوَكُمْ وَآخَرِينَ**

---

[39] ابن منظور ، لسان العرب ،الجزء الخامس ، الطبعة الثالثة ، دار إحياء التراث العربي ، بيروت ، 1999 ،ص .377.

[40] أنظر معنى كلمة terreur على الموقع:

https://www.larousse.fr/dictionnaires/francais/terreur/77456 بتاريخ 2025/02/21 :11:18

[41] Terrorism, oxford dictionary :
https://www.oxfordlearnersdictionaries.com/definition/english/terrorism?q=terrorism

[42] فاطمة بلحنافي ، التعاون الدولي في مكافحة الإرهاب الدولي ، مطبوعة بيداغوجية موجهة لطلبة السنة الثانية ماستر قانون دولي عام، كلية الحقوق والعلوم السياسية، الجزائر ، السنة الجامعية 2023/2022 ، ص .12 .

مِنْ دُونِهِمْ﴾ [43]. أي أعدوا ما قدرتم عليه من سلاح، وخيل تخيفون به أعداءكم و أعداء الله من مشركين وكفار.

كما ذكرت كذلك في قوله عز وجل : ﴿ **وَلَمَّا سَكَتَ عَنْ مُوسَى الْغَضَبُ أَخَذَ الْأَلْوَاحَ وَفِي نُسْخَتِهَا هُدًى وَرَحْمَةٌ لِلَّذِينَ هُمْ لِرَبِّهِمْ يَرْهَبُونَ﴾**[44]. أي لما سكن موسى وذهب عنه الغضب، أخذ الألواح التي فيها الهدى من الضلالة، ورحمة وسعادة لمن عمل بها وهم الذين يخافون الله ويخشوه .

ثانيا : التعريف الفقهي و الاصطلاحي للإرهاب

إختلف الفقهاء حول إعطاء تعريف موحد لمفهوم الإرهاب وهذا بسبب إختلاف مذاهبهم وإيديولوجياتهم ومعتقداتهم ، فأعتمدوا في تعاريفهم على إحدى المعيارين:

أ / – المعيار الموضوعي

يرى أنصار هذا المذهب أن تعريف الإرهاب يجب أن يتسم بالنظرة الموضوعية والتركيز على الغايات والأهداف التي يسعى مرتكبوا هذه الأعمال من بلوغها وتحقيقها ، ومن بين هؤلاء نذكر على سبيل المثال الفقيه الإيطالي (VIGINA) الذي يعّرف الإرهاب بأنه " **إستخدام العنف كأداة لتحقيق أهداف سياسية** "[45]، ويظهر جليا من خلال هذا التعريف أن الهدف الذي يسعى إليه الفاعل هو هدف سياسي .

كما يرى وولتر (WALTER) أن الإرهاب هو :" **عملية الرعب تتألف من ثلاثة عناصر: فعل العنف أو التهديد بإستخدامه، وردة الفعل العاطفية الناجمة عن أقصى درجات خوف الضحايا أو الضحايا المحتملة، وأخذ التأثيرات التي تصيب المجتمع بسب العنف أو التهديد بإستخدامه و الخوف الناتج عن ذلك** " [46].

---

[43] سورة الأنفال ، الآية (60).

[44] سورة الأعراف ، الآية (154).

[45] علي لونيسي ،آليات مكافحة الإرهاب الدولي بين فاعلية القانون الدولي وواقع الممارسات الدولية الإنفرادية ،رسالة لنيل شهادة الدكتوراه في القانون، جامعة مولود معمري ، تيزي وزو، الجزائر،2012،ص .23 .

[46] عثمان علي حسن ،المرجع السابق ، ص . 70 .

وعلى صعيد الفقه العربي الأستاذ " **أحمد جلال عز الدين** " يعرف الإرهاب على أنه : " **عنف منظم و متصل بقصد حالة من التهديد العام الموجه لدولة أو لجماعة سياسية، والذي ترتكبه جماعة منظمة بقصد تحقيق أهداف سياسية** "[47]. ويقصد بذلك أن الإرهاب عنف منظم ومتصل ترتكبه جماعة منظمة بغرض تحقيق أهداف سياسية يخلق حالة من التهديد العام الموجه ضد دولة أو جماعة سياسية .

ب / – المعيار المادي

يعرف أنصار هذا الإتجاه الإرهاب إستنادا إلى الوسائل المستخدمة في العملية الإرهابية و بالرعب والفزع كمحصلة له ، دون النظر الى الأهداف المرجوة منها ومن أنصار هذا الفريق الفقيه (LEMKIN) الذي يعرفه بأنه : " **تخويف الناس بممارسة أعمال العنف** "[48]، أي حسب رأيه الإرهاب يقع بمجرد إستخدام العنف دون النظر إلى الهدف و الغرض منه سواء تحقق أم لم يتحقق.

كما يرى الفقيه سالدانا (SALDANA) أن للإرهاب مفهومين أحدهما واسع وهو : " **كل جناية أو جنحة سياسية أو إجتماعية ينتج عن تنفيذها أو التعبير ما يثير الفزع العام ، لما لها من طبيعة ينشأ عنها خطر عام** " [49]، ومن خلال هذا التعريف نرى أن الفقيه قد أخلط بين الجرائم السياسية والإرهاب رغم وجود إختلافات بينهم ، وبالنسبة للمفهوم الضيق يرى بأنه:" **الأعمال الإجرامية التي يكون هدفها الأساسي نشر الخوف والرعب – كعنصر معنوي – وذلك بإستخدام وسائل من شأنها خلق حالة من الخطر العام – كعنصر مادي –** "[50].

أما على صعيد الفقه العربي نأخذ تعريف الدكتور "**عبد العزيز سرحان**" حيث يرى أنه " **كل إعتداء على الأرواح والأموال والممتلكات العامة والخاصة ، بالمخالفة لأحكام القانون**

---

[47] علي لونيسي ، المرجع السابق، ص .24 .

[48] فاطمة بلحنافي ، المرجع السابق ،ص .14 .

[49] حسام الحداد ،الارهاب المفهوم والاسباب أبرز الجهود والاسهامات لمحاربته ،كراسات تنوير 22 ، ص . 05 . على الرابط :https://2u.pw/ZsKpJ

[50] علي لونيسي ، المرجع السابق ، ص .20.

الـدولي العام بمصادره المختلفة ، بما في ذلك المبادئ العامة للقانون بالمعنى الذي تحدده المادة 38 من النظام الأساسي لمحكمة العدل الدولية "[51]، إستنادا إلى هـذا التعريف يعتبر كـل إعـتداء عـلى الأرواح والأمـوال والممتلكات العامة والخاصة إرهابا دوليا إذا خالف أحكام القانون الدولي بمختلف مصادره، وبالتالي يقع تحـت طائـلة العـقاب حسب القوانين الداخلية للدول تماشيا مع القانون الدولي.

المتـتبع لتـاريخ هــذه الظاهـرة يلاحظ أن الجهود الدولية لمحاولة تعريفها بدأت منذ عام 1919 م، عندما كلفـت لجـنة الفـقهاء المكلفة بـدراسة المشاكل المتعلقة بمـسؤولية مـجرمي الحرب بإعداد قائـمة بالجرائـم المرتكـبة، حيـث أُحصيَت 32 جريـمة، وَرَّدَ الإرهاب المـنظم في المرتبة الثانية، وتواصلت المؤتمرات والندوات منذ ذلك الحـين لـكن لـم يستـقر المجتـمع الـدولي عـلى تعريف موحـد، وفـي سـنة 1972 م دعـت منظـمة الأمـم المتحـدة إلى إنشـاء لجـنة متخصـصة مهمتها تعريـف الإرهـاب، ودراسـة الأسـباب والدوافـع وسـبل مكافحة هـذه الجريمة، وهـذا عـلى إثـر تعرض فريـق مـن الكـيان الصهيوني للإغتيال الجماعي من طرف جماعة الأسود الفلسطينية[52].وقـد فرقـت في قـرارها الصـادر عن جمعيتها العامة رقم 3034 قانونية النضال من أجل مقاومة الإحتلال والتحرر، وبين الأعمال والأفعال الإجرامية .

تعرفـه الاتفاقـية العربـية لمكافحة الإرهاب لعام 1998 م على أنه : " **كـل فعل من أفعال العنف أو التهديد به أيًّا كانـت بواعـثه، أو أغـراضه يقـع تنفيذا لمشـروع إجـرامي فـردي، أو جـماعي ويهـدف إلى إلـقاء الرعب بين الناس، أو ترويعهم بإذائهم أو تعريض حياتهم، أو حريتهم أو أمنهم للخطر أو إلحاق الضرر بالبــيئة، أو بأحد المرافق أو الأملاك العامة**

[51] فاطمة بلحنافي ، المرجع السابق ، ص .14 .

[52] رضا هداج ، المقاومة والإرهاب في القانون الدولي، مذكرة لنيل شهادة الماجيستير في القانون الدولي والعلاقات الدولية، جامعة الجزائر 1، كلية الحقوق، بن عكنون ،السنة الجامعية 2010/2009، ص . 59 .

أو الخاصة أو إحتلالها أو الإستيلاء عليها، أو تعريض الموارد الوطنية للخطر "[53].

ويـتضح من هذا التعريف أن للإرهاب ركنين:

الركن المـادي: وهو عبارة عن فعل العنف أو التهديد به أيا كانت بواعثه .

الركن المعنوي: وهـو قـيام الفـاعل بإلقـاء الرعـب والفزع بـين النـاس بـهدف ترويعهم .كما أن الإتفـاقية أكـدت على حق الشعوب في تقرير المصير بالكفاح المسلح ضد المحتل وفقا لمباديء الأمم المتحدة .

وإنـطلاقا لما سلف يـرى الباحـث أن أنسـب تعـريف هـو ماذهـبت إلـيه الأستـــاذة " **بلحنافي فاطمة** " فـي سلسـلة محاضراتـها بحيـث عرفـته عـلى أنـه :" **كــل فـعل عنيف غيـر مشروع أو التحريض عليه، يسعى دون وجه حق إلى إثارة الهلع والخوف، يستهدف مواطنا أو جماعة أو طائفة أو قومية مـن شأنها تهديد أمن الدولة أو إستقرارها، قامت به جماعة أوتبنته دولة تحقيقا لأغراض خاصـة، أو نـكاية بالغير، أو بدولة أخرى، وقع هذا الفـعل فـي أي مكـان، أو تحـت أي ظـرف، سواء تحققت النتيجة أو خاب أثرها لأسباب خارجة عن إرادة الفاعل** " . وتمـاشيا مع تم ذكـره فـي هـذا التعـريف فإنه يشترط في الفعل العنيف أن يـكون غير مشروع وبالتالي يستبعد الفـعل العنيف المشروع كالعنف الموجه ضد المحـتل أو الـذي يستهدف إسترجاع حقوق مسلوبـة، وأن يهـدد هذا الفعل دون وجه حق أمن الأفـراد أو الجـماعات أو أي طائفة أو قومية أو أمـن الـدول لأي سبـب مـن الأسـباب، وأيا كان مصدره أو المـكان الذي يستـهدفه، كـما أن التحريض على الفعل العنيف غير المشروع يعتبر من قبيل الإرهاب .

ثالثا: تعريف الإرهاب السيبراني

كانـت بـداية إسـتخدام مـصطلح الإرهـاب السيـبـرانـي (cyberterrorism) فـي فـــترة الثمانـينات عـلى يـد **(بـــاري كـولين)** والتي خلص فيها إلى صعوبة وضع تعريـف شامل له لكن تـبنى تعـريفا مقـتضاه أنـــه :" **هجمة إلكترونية غرضها تهديد الحكومات أو العـدوان**

---

[53] خالد محمد خالد خليفوه، أثر الإحتساب في مكافحة الإرهاب، دراسة تأصيلية تحليلية على دولة الكويت، مجلة الوعي الإسلامي، ط 1، الإصدار الثاني والستون، الكويت، 2013، ص .125 .

عـليها، سعـيا لتحقـيق أهـداف سيـاسية أو ديـنية أو إيـديولوجية، وأن الهـجمة يجـــب أن تكون ذات أثر مدمر وتخريبي مكافيء للأفعال للإرهاب "[54]، ويعـرفه **(جيمـــس لويس)** على أنــه : " **إستـخدام أدوات شبكات الحاسوب في تدمير أو تعطيل البنى التحتية الوطنية المهمة مثـل : الطــاقة و النقــل و العـمليات الحكومــية، أو بــهدف تــرهيب حـكومة مـا أو مدنيين "**[55] .

وعرفـــته **(دوروثي دينـينغ)** على أنه : " **الهجوم القائـم عـلى مهاجمة الحاسوب، وأن التهديد يــهدف إلى تـرويع أو إجبار الحكومات أو المجتمعات لأجل تحقيق أهداف سياسية أو دينــية أو عــقائدية، ويجب أن يكون الهجوم مدمرا وتخريبيا بالمدى الذي يسمح بتوليد الخوف بحيث يصبح مشابه للأفعال المادية الإرهابية "** [56]، وتـم تعريفه من طرف نجيب بن عمر عوينات بأنه :"**هجمات غير مشروعة أو بتهديدات بهجمات ضد الحاسب أو الشبكات أو المعلومــات المخــزنة إلـكترونيا تــوجه مــن أجـل الإنتقام أو الإبتزاز أو إجبار أو تأثير في الحكومات أو الشعوب أو المجتمع الدولــي بأسـره لتحقـيق أهداف سياسية أو دينية أو إجتماعية معينة، ولـكي يعتبر المرء إرهابيا على الأنترنت وليس مخترقا فإن الهجمات التي يشـنها يجـب أن تـؤدي إلــى عنف ضد الأشخاص أو الممتلكات أو على الأقل تحدث أذى كافيا من أجل نشر الخوف أو الرعب "**[57] .

عرفــه مكتــب التحقيـقات الفـيدرالي الأمـريكي FBI سنة 1997 بأنه" الهجوم المتعمد ذو الــدوافع الســياسية ضـد المعــلومات و أنــظمة الكومـبيوتر وبرامــج الكومـبيوتر والبـــيانات

---

[54] مصطفى خليل كامل خليل، جرائم الإرهاب الإلكتروني من منظور القانون الدولي العام، مجلة كلية الحقوق، جامعة المنيا،المجلد 05، العدد 02، ديسمبر 2022 م ، ص .15 .

[55] محمد كمال، المرجع السابق، ص . 123 .

[56] أكرم رياض، السياسات الدولية لمكافحة الإرهاب الإلكتروني السيبراني، مذكرة الماستر في العلوم السياسية ، كلية الحقوق والعلوم السياسية ، جامعة العربي بن مهيدي، أم البواقي، 2022/2021، ص . 13 .

[57] نجيب بن عمر عوينات، الإرهاب الإلكتروني : المفهوم والجهود الدولية والإقليمية لمكافحته، **مجلة الأستاذ الباحث**، المجلد 02، العدد 02، جوان 2017، ص. 13 .على الرابط:https://asjp.cerist.dz/en/article/76780

الذي ينتج عنه العنف المسلط على أهداف غير قتالية"[58]. وجاء هذا التعريف نتيجة لما قام به الرئيس الأمريكي السابق (**بيل كلينتون**) سنة 1996 م عندما شكل لجنة حماية منشآت البنية التحتية التي توصلت إلى أن هدف الهجمات الإرهابية ستكون مصادر الطاقة والإتصالات، وكذلك شبكات الكمبيوتر، حيث لم تعرفه هذه اللجنة وإنما إكتفت بدراسة هذه الظاهرة [59].

كما عرفته هيئة الأمم المتحدة في أكتوبر 2012 م بأنه : " **إستخدام الأنترنت لنشر الأعمال الإرهابية** "[60].

وعرفه **باتريك قالي (Patrick Galley)** بأنه : " **تحطيم أو إتلاف أنظمة معلوماتية، بهدف المساس أو إحداث خلل يمس بإستقرار دولة أو بهدف الضغط على حكومة ما** " وعرفه أيضا بـ : " **القيام بعملية من شأنها المساس وإحداث خلل ماس بإستقرار دولة أو بهدف الضغط على حكومة، بإستعمال طرق تدخل في صنف جرائم المعلوماتية** "[61].

من خلال التعاريف السابقة يمكن القول بأن تعريف الإرهاب السيبراني ينطلق من تعريف الإرهاب التقليدي والإختلاف الوحيد في الوسائل الحديثة المستعملة، و تعريف مجمع الفقه الإسلامي الدولي التابع لمنظمة المؤتمر الإسلامي للإرهاب التقليدي يعتبر من أفضل التعاريف وأقربها إلى الصواب وتأسيسا على ذلك يمكننا تعريف الإرهاب السيبراني بأنه : " **العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول أو الجماعات أو الأفراد على الإنسان في دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق بإستخدام**

---

[58] محمد سويلمي ،في الارهاب والارهاب الالكتروني :التباسات المفهوم وتقاطع المقاربات،مجلة قضايا التطرف والجماعات المسلحة،المركز الديمقراطي العربي،العدد 01،ماي 2019،ص-22-

[59] حسن المبروك سعد، جريمة الإرهاب الإلكتروني دراسة مقارنة، رسالة ماجستير في القانون الجنائي، الأكاديمية الليبية، فرع بنغازي، ليبيا، 2022م/2023م، ص.18.

[60] بن علية بن جدو، تحديات الأمن السيبراني لمواجهة الجريمة الإلكترونية، المجلة الجزائرية للأمن الإنساني، المجلد 07، العدد 02، جويلية 2022،ص . 303 .

[61] نسيم دردور ، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة الماجستير، جامعة منتوري، كلية الحقوق، قسنطينة، 2012 م/2013 م، ص .148.

الموارد المعلوماتية والوسائل الإلكترونية بشتى صنوف العدوان وصور الإفساد في الأرض" [62].

الفرع الثاني : أنواع الإرهاب السيبراني

يرى الدارسين لظاهرة الإرهاب السيبراني بأن هناك نوعين منه:

أولا: الإرهاب السيبراني الخالص(Pure Cyber Terrorism)

وهو ماكانت هجماته مباشرة على البنية التحتية السيبرانية للضحية ، مثل : الشبكات والحواسيب، والمعلومات المخزنة فيها وغير ذلك ، لتحقيق أهداف مختلفة، سياسية أو دينية أو أيديولوجية كإفساد وظائف أنظمة المعلومات، أو تدمير الأصول الإفتراضية و المادية، وحجب المواقع الإلكترونية، وتعطيل الحياة اليومية بإستهداف البنية التحتية التي تدار بأجهزة الكمبيوتر أو الحواسيب كشبكة إمدادات الطاقة والسكك الحديدية وإمدادات الماء وخدمات النقل والإتصالات السلكية واللاسلكية ، و الأنظمة المالية كالأسواق المالية ، البورصة والبنوك والمرافق الطبية[63].

فبالتالي الإرهاب السيبراني الخالص يستهدف إما إفساد و تدمير و إتلاف الأنظمة عن طريق إستخدام الفيروسات أو الديدان أو حصان طروادة أو القنابل المنطقية أو إلى تعطيل الحياة اليومية عن طريق مهاجمة الحواسيب التي تدار بها بحيث تأخذ هذه الهجمات أحد الشكلين ، إما مهاجمة البيانات والمعطيات أو مهاجمة أنظمة التحكم.و من أمثلة على ذلك قيام مجموعة من القراصنة التونسيين عام 2015 م التابعين لتنظيم الدولة داعش يسمون أنفسهم (Fellaga) بمهاجمة عدد من المواقع الإلكترونية التابعة لوزارة الصحة البريطانية ، حيث تم إستبدال صفحات الموقع الإلكتروني بصور عن الأزمة السورية وبعبارات " أوقفوا القتل في سوريا" .

---

[62] جاسم محمد، الإرهاب الإلكتروني، دار البداية ناشرون و موزعون، الطبعة 01، عمان، 2014 م، ص .39.

[63] مصطفى خليل كامل خليل،المرجع السابق، ص .44 .

ثانيا: الإرهاب السيبراني الهجين(Hybrid Cyber Terrorism)

ويشـير إلى إستخـدام الإرهابيـين للفـضاء السيـبراني فـي مختلف أنشطتهم مثل : الدعاية والتجـنيد، جـمع الأمـوال، جـمع البـيانات، الإتـصال الآمن، التـدريب والتخطيط للعمليات الإرهابية .

أ / – **الدعايـــة** : يسـتخدم الإنترنت لنـــشر الإيـديولوجيات الجهادية الإرهابية ومن أجل تبرير أفعـالهم، وكـذلك لبـث الذعـر و الخـوف فـي النفـوس وكـسب التعاطـف حـول قـضية ما ، ومن أمثلة على ذلك إصدار " القاعدة" مجلة Resurgence الناطقة باللغة الإنجليزية في عام 2014 م، للتواصل مع المسلمين في الغرب آنذاك.

ب / – التواصل الآمن: تسـتخدم التنـظيمات الإرهابـية الرسائـل المشفرة عـبر وسائل التواصل الإجتـماعي أو عن طريـق التطبيـقات، وغـرف دردشة الألعاب عبر الإنترنت، بهدف إرسال رسائـل أو إخـفاء المعـلومات، والتـواصل مـع الأعـضاء الآخـرين في التنظيم، والتفاعل مع المجندين والمؤيدين، وتخطيط وتنسيق الهجمات، وعمليات القرصنة [64].

ج / – تجنـيد أعضاء جدد: تقوم المنـظمات الإرهـابية بتحـديد الأهـداف المحـتملة للتجـــنيد عـبر مراقبة مواقع التواصل الإجتماعي ، وتفاعلات المستخدمين حول المنشورات ذات الفكر المتـطرف الإرهابي، ثـم يتواصلون معهم من أجل التجنيد بعد التأكد من إخلاصهم. كما يتم إغرائـهم بالـمال والنساء ويـفيد تقـرير لمجـموعة العمل المالي الدولية FATF عام 2015 م أن شبكة الأنترنت باتت الأداة الأكثر إستخداما للتجنيد ودعم التنظيمات الإرهابية[65] .

د / – التدريب: هـناك فـرق إرهابية مختصة على الإنترنت مهمتها التدريب و شرح كيفية شن الهجمات وتصنيع المتفجرات بإستـــخدام مكونات متوفرة في الأسواق اليومية بسهولة، وتوزيع الإرشادات والتعـليمات لإكساب الأعضاء الحاليين والجدد المهارات اللازمة، وتعزيز قدراتـهم الهجومية .

---

[64] محمد زهير عبد الكريم، الإرهاب السيبراني : أزمة عالمية جديدة، قضايا سياسية، كلية العلوم السياسية، جامعة الموصل، العدد 64، السنة 2021 م، ص ص . 294/277 . على الرابط:https://2u.pw/ZTtbM

[65] نفس المرجع، ص . 288 .

هـ / – جـمع التبـرعات: يتـم جـمع التـبرعات عـبر وسائل التواصل الاجتماعي، والمنصات، والمدونات، والعملات الافتراضية، والشركات و الجمعيات الوهمية .

و / – جـــمع المعـلومات: يستخـدم الإرهابيون الفضاء السيبراني لجمع معلومات عن الأهداف البشـرية المحـتملة أو الأمـاكن مـن خـلال المعـلومات الـتي شاركتها تلك الأهداف طواعية عـلى مـواقع التـواصل الإجـتماعي، كـتلك التـي تـتصل ببـياناتهم الشخـصية، والأمـــاكن التي يترددون عليها، وغير ذلك[66].

الفرع الثالث: تمييز الإرهاب السيبراني عن ما يشابهه

مـن الصعـب التميـيز بيـن الإرهـاب السيـبراني والجـرائم الأخـرى التـي تـقع فـي الفضاء السيبراني، لأنه لا يوجد تعريف قانوني موحد يحدد أركانه لإختلاف الإيديولوجيات والمصالح، ومع هذا يمكن وضع وصف له وعندئذ يتضح بأنه يتشابه مع عدة جرائم، سـواء مـن خـلال الأساليب والوسائل المستعملة أو الأهـداف المرجـو تحقـيقها، ولـكن هـذا لا يـمنع مـن وجود بعض الإختلافات وفيما يلي بعض الجرائم المشابهة له :

أولا: الإرهاب السيبراني والإرهاب التقليدي

يتـشابه الإرهـاب السيبراني مــع الإرهـاب التقليدي من حيث أن كلاهما من الأعمال غير المشروعة التي تثـير الفـزع والخـوف، والتـي جرمـتها الاتـفاقيات الـدولية، كـما أن أهـدافهما متـشابهة، بـحيث يسعى كلاهـما للمساس بالنظام العام و تعريض المجتمع للخطر، سواء أكان بـدافع سـياسي أو ديـني أو إجـتماعي أو فـردي أو غيـرها من الدوافع ويختلفان في الوسائل المستعملة، فالإرهاب السيبـراني يعـتمد على التقـنية والحاسوب وشـبكة الأنتـرنت التي تشكل الفـضاء السيبراني، ويستعمل القوة الناعمة في إثارة الرعـب، عـلى عـكـس الإرهـاب التقـليدي الذي يستعمل الوسائل التقـليدية كالسلاح والقـنابل في تنـفيذ

[66] المرجع السابق، ص . 287 .

العمليات في الفضاء المادي، أي أنه يستعمل القوة الصلبة كما أنه يصعب إكتشاف الدليل الجنائي الرقمي في الجرائم السيبرانية بصفة عامة على عكس جريمة الإرهاب التقليدية ، والإرهابي السيبراني على خلاف التقليدي يكون على درجة عالية من التعلم والذكاء و التحكم في التقنية الرقمية، كما أنه لا يحتاج للتنقل إلى موقع الهجمات وأن يعرض حياته للخطر.

ثانيا: الإرهاب السيبراني والحرب السيبرانية

تعرف الحرب السيبرانية بأنها حرب بين الدول في العالم الإفتراضي، ويمكن من خلالها تدمير البنية التحتية للمعلومات أو سرقتها عن طريق الإختراق، ويرى بعض المحللين أن حروب الأجيال القادمة ستعتمد على الحروب التكنولوجية والجيوش التكنولوجية[67]، و تعرف على أنها: " **إستخدام نظم المعلومات لإستغلال وتخريب وتدمير وتعطيل معلومات الخصم، وعملياته مبنية على المعلومات ونظم معلوماتها وشبكة الحاسب الآلي الخاصة بها، وكذلك الحماية من خطر الهجوم من قبل الخصم لإحراز السبق والتقدم على نظمه العسكرية والإقتصادية** "[68].و تنقسم إلى نمطين :

أ /- نمط هجومي: وهو إظهار الدولة لقوتها لما تملكه من إمكانيات ضخمة بحيث تقوم بتعطيل نظم المعلومات، التجسس، وسرقة البيانات والبرامج الحاسوبية .

ب /- نمط دفاعي: ويقصد به الوقاية من الأعمال التخريبية التي تتعرض لها في المجال السيبراني عن طريق عدد من الوسائل التي تختلف حسب طبيعة الهجوم .

---

[67] محمد مهني، تأثير الإرهاب الإلكتروني على تغيير مفهوم القوة في العلاقات الدولية توظيف المنظمات الإرهابية لمواقع التواصل الإجتماعي نموذجا، مذكرة ماستر في العلوم السياسية والعلاقات الدولية ، جامعة محمد بوضياف، كلية الحقوق والعلوم السياسية، المسيلة، 2017 م/2018 م،ص.24.

[68] فايزة نجاري بن حاج علي ،المرجع السابق، ص. 25.

يـرى بعـض الباحـثين أن هـناك خـيط رفـيع بـين الإرهـاب السـيبراني والحرب السيبرانية، ومعيار التمـييز بيـنهما يكمن في الهدف والغاية مـن تـلك الهجـمات، فالإرهاب السيبراني هدفه على الأغلب سياسي، أما الحرب السيبرانية فهي غالبا ناتجة عن نزاع مسلح وقـد تتـحول هذه الأخيرة إلى إرهاب ومثال ذلك ماحدث في لبنان في السابـع عـشر من سبـتمبر 2024 م مـن تفجـيرات لأجهـزة المناداة **(البيـجر)** من طرف الكيان الصهيوني، وتحدثت شركة لوبك إنـترناشـيونال الأمنية أن سـبب الإنفجار هو عـلى الأرجـح برمجيات خـبيثة رفعـت درجـة حـرارة البـطارية مـما أدى إلـى إنفـجارها[69]، مما أثـار حـالة مـن الخـوف والفـزع و اللاأمن في نفوس المواطنين، كـما يمـتلك المـحارب السيبـراني رعـاية خـاصة من قبل دولته ويخضع لرقابتـها، فـي حـين يمكـن للـدول أن تـرعى الإرهـابي السيـبراني لكن لا تستطيع إخضاعه لرقابتها .

زد على ذلك الأثر أو المحصلة الناتجة عن الحرب السيبرانية قد تفوق في قوتها التدميرية الإرهاب السيبراني، كما أن الحرب السيبرانية تمتاز بخضوعها لقواعد القانون الدولي، والقانون الدولي الإنساني، لاسيما مبادئ الأمم المتحدة كمبدأ الحق في اللجوء للحرب المقررة في الفقرة الرابعة من المادة الثانية من الميثاق، والمادة (51) من ذات الميثاق المتعلقة بحق الدولة في الدفاع عن نفسها أي بمفهوم آخر قد تكون الحرب السيبرانية مشروعة إذا توفر فيها ماقيل آنفا على عكس الإرهاب السيبراني.

ثالثا: الإرهاب السيبراني والجريمة السيبرانية

تعرف الجريمة السيبرانية على أنها: " **كـل فعـل أو إمتناع يتـم الإعـداد لـه أو التخطيط لـه ويـتم بـموجبه إسـتخدام أي نـوع مـن الحاسب الآلي، سواء حاسب شخصي أو شبكات الحاسب الآلي أو الأنـترنت أو وسائل التـواصل الإجتماعي لتسهيل إرتكاب جريمة أو عمل**

[69] للإطلاع أكثر أنظر: تفجيرات البيجر.. ما الذي جرى في لبنان؟ على موقع الجزيرة من خلال الرابط: https://2u.pw/BmIOn

مخالف للقانون أو تلك التي تقع على الشبكات نفسها عن طريق إختراقها بقصد تخزين أو تعطيل أو تحريف أو محو البيانات أو البرامج التي تحويها "[70].

تتشابه الجريمتان في الوسائل المستعملة لإرتكابهما، وهما من الجرائم المستحدثة العابراتا للحدود ، ويشتركان في طبيعة و خصوصية المجرم الذي يمتاز بالمهارة والذكاء والقدرة على التحكم في الوسائل التقنية ويختلفان في الهدف فالمجرم السيبراني يهدف إلى تحقيق مكاسب مادية على عكس الإرهابي السيبراني الذي يهدف إضافة لذلك إلى تحقيق هدف سياسي أو إقتصادي أو إعلامي ...إلخ .

رابعا: التمييز بين الإرهاب السيبراني والمقاومة السيبرانية

تعتبر المقاومة حق شرعي مكفول بموجب القوانين والأعراف الدولية وتتضمن حق الدفاع الشرعي وحق تقرير المصير ومقاومة الإحتلال، ويتسع مفهومها ليشمل أيضا الحركات الإحتجاجية داخل الوطن الواحد التي تسعى إلى تغيير واقع غير مرغوب فيه، أو تسعى في مواجهة صور الإستبداد و الظلم والإجحاف ونصرة الحق[71]، وكأي ظاهرة إجتماعية تكيفت المقاومة مع التطور التكنولوجي وظهرت المقاومة السيبرانية التي تستعمل كل الأدوات التكنولوجية ومن قبل جميع الفئات لإزاحة وطرد محتل أو تغيير سلطة مستبدة .

يكمن الإشكال في أن الدول الغربية على عكس الدول العربية ترى أن المقاومة هي شكل من أشكال الإرهاب وهذا ما يظهر جليا في مساندة هذه الدول للإحتلال.

---

[70] عبد الله دغش العجمي، المشكلات العلمية والقانونية للجرائم الإلكترونية (دراسة مقارنة)، مذكرة ماجستير في القانون العام، جامعة الشرق الأوسط، 2014 م، ص . 14.

[71] يوسف الحسن، ثقافة المقاومة، 14 فبراير 2017م، تم الإطلاع عليه بتاريخ 2025/03/27م على الساعة 15:00 على الرابط:https://2u.pw/ijv0A

الفرع الرابع: خصائص الإرهاب السيبراني

ينفـرد الإرهاب السيبراني بجـملة مـن الخصائـص والسـمات تمـيزه عـن غيره وتحول دون إختلاطه بالإرهاب التقليدي وأهمها:

أ/- لا يـحتاج الإرهـابي السيبـراني أن ينـتقل إلـى مـكان الهجوم وإستعمال القوة، بل يحتاج إلى مجرد جهاز كمبيوتر متصل بشبكة الأنترنت ومزود بالبرامج اللازمة وهـذا ما يجعله أقل تكلفة وأكثر فاعلية .

ب/- الإرهـابي السيـبراني يمـتاز بـذكاء خـارق وتعـليم عـالي، وبالمـهارة والـخبرة والتحـكم الجـيد في الوسائل التقنية.

ج/- صعوبة الإثـبات لسهولة إتـلاف الـدليل الرقـمي أو تغييره ، نظرا لنقص الكفاءة والخبرة للأجهزة المعنية بالبحث والتحري في إكتشاف الجريمة مبكرا.

د/- إستعمال أسلـحة غير تقـليدية مـن أجل بث الرعـب والفزع ، والمتمثلة في جهز حاسوب أو جهاز ذكي آخر يمكنه الإتصال بشبكة أنترنت .

هـ/- جريـمة الإرهـاب السيـبراني هـي جـريمة عابـرة للحـدود وغـير خاضعة لنـطاق إقـليمي محدد [72] ، كما تتميز بسرعة التنفيذ .

و/- إمكانـية تعـاون أكثر من شخص على إرتكاب الجريمة الإرهابية السيبرانية كإنشاء مواقع جهادية لتجنيد وتدريب المنخرطين الجدد.

[72] عبد الحكيم توات ، جريمة الإرهاب الإلكتروني، مذكرة ماستر جريمة وأمن عمومي، جامعة العربي التبسي، كلية الحقوق والعلوم السياسية، التبسة، 2021م/2022م، ص.20.

وتأسيسا عـلى ماتـقدم فـإن الـدول المتقـدمة التي تعتمد على الوسائل التقنية، وتكنولوجيا الإعـلام والإتصال في أنظمة تسييرها لمؤسساتها، و أجهزتها معرضة أكثر لمخاطر الإرهاب السيبراني، لأنه يستخدم هذه الوسائل كأدوات للهجوم .

المطلب الثاني:

دوافع و أساليب الإرهاب السيبراني

لا يـمكن معـالجة أي ظـاهرة إجتـماعية دون معرفة أسبابها ودوافعها، والمتمعن والمستقرء لجريمة الإرهـاب السيـبراني يـعي بـأنها نـوع من أنواع الإرهاب التقليدي، فدوافعها هي نفسها دوافع الإرهـاب التقـليدي مـع أسبـاب أخـرى جـديدة، حيث تتـداخل عـدة دوافع شخـصية وفـكريـة، وسياسـية، وإقـتصادية، وإجتماعية، ودينية ...الخ وتمـثل الأسـباب العـامـة والـخاصة لـــــه **(الفـــرع الأول)**، ويستعمل الإرهاب التقليدي الأسلحة التقـليـدية كالمتـفـجـرات والغـازات السـامة والإغتـيالات، عـلى خـلاف الإرهـاب السيـبـراني الـــذي يستعـمل أسـاليب متعـلـــقة بالتقـنية الـتي يستعـملها فـي الهجـمات السيبرانية **(الفـــــــرع الثاني)** .

الفرع الأول: دوافع الإرهاب السيبراني

هـناك العـديد من الأسباب والدوافع لإرتكاب الجريمة الإرهابية، مما يصعب حصرها كلها ولهذا سنتطرق إلى أهمها:

أولا: الدوافع العــامة لــلإرهاب

تخـتلف مـن مجـتمع لآخر وذلك حسب الظروف، والنـــظم السياسية والأحوال المعيشية والمعتقدات الديـنية والإيديولوجية ...إلخ، فـما يصلـح عـلى بيئة من مجتمع ما قد لا يصلح في بيئة مجتمعية أخرى وأهمها :

أ / – الأسباب الشخصية والفكرية: قد يكون الوازع والدافع هو إنتقام من الدولة أو أحد أجهزتها، أو بسبب مشاكل نفسية أو معتقدات دينية خاطئة، أو إلتماس الشهرة عبر الوسائل الإعلامية أو بهدف تحقيق مكاسب مادية أو بسبب الفشل في كل نواحي الحياة الدراسية والعملية والأسرة.

ب / – الأسباب السياسية: يلجأ بعض الأفراد أو الجماعات إلى الأعمال الإرهابية إحتجاجا على السياسات غير العادلة التي تنتهجها بعض الأنظمة الديكتاتورية المستبدة ضد مواطنيها، كتهميش دورهم في المجتمع وإنتهاك أبسط حقوقهم وحرياتهم، ونهب الأموال العامة، وعدم المساواة في توزيع الثروة، وسد قنوات الحوار، والإعتقال السياسي، وقد أشارت الجمعية العامة للأمم المتحدة في إطار جدول أعمالها الرامي إلى القضاء على الإرهاب الدولي إلى كون الإقصاء السياسي والظلم والإضطهاد من بين الأسباب الجذرية التي تقف وراء الظاهرة الإرهابية وإنتشارها [73] .

ج / – الأسباب الإجتماعية: الإنسان إجتماعي بطبعه وهو إبن بيئته يؤثر ويتأثر بالوسط الذي يعيش فيه وبالأفراد الذين يحيطون به، فالمشاكل الأسرية والحرمان الإجتماعي بسبب التميز العرقي أو الديني أو القومي يُوَّلِدْ له شعور بعدم الإنتماء لهذا الوطن، مايجعله هدفا سهلا ومرشحا من قبل الجماعات الإرهابية لتجنيده .

د / – الأسباب الإقتصادية: إن تفاقم المشكلات والأزمات الإقتصادية التي خلقت تباين في توزيع الثروة وتقسيم المجتمع إلى طبقات برجوازية وكادحة، والإستغلال غير المشروع لثروات الدول من قبل دول أخرى ونخص بالذكر نهب ثروات الدول النامية، أدى إلى تفشي

[73] أنظر البند 06 من محضر موجز للجلسة الثالثة لجنة السادسة للجمعية العامة المتضمنة التدابير الرامية إلى مكافحة الإرهاب الدولي، الدورة 69 ، المؤرخ بتاريخ 27 أكتوبر 2014: https://daccess-ods.un.org/TMP/2758755.08785248.html

الفقر وغلاء المعيشة والتضخم في أسعار المواد الأساسية وأزمة السكن و البطالة ، كـل هذه التراكمات دفعت الشباب للجوء إلى عالم الجريمة والإرهــاب إما طواعية أو بسبب الإغراءات المقدمة من طرف هذه الجماعات الإرهابية .

إلــى جانــب الأســباب السابـقة هـناك أسبــاب أخـرى عامة للإرهاب كالأسباب التاريخية والطائــفية وأسـباب إعــلامية ، فالإعـلام هـو الهدف الأسمى للجماعات الإرهابية من أجل إيـصال قضـيتهم إلـى العـالم وكـذلك مـن أجـل بـث الخـوف والـذعر في نفوس أكبر عدد من الناس .

ثانيا: الدوافع الخاصة للإرهاب السيبراني

يتميز الإرهاب السيبراني عن الإرهاب التقليدي في إستخدامه للفضاء السيبراني كـساحة يقـوم فـيها بهجـوماته، مـن خـلال إستـغلال شبكات الإتـصال وعـلى رأسـها الأنترنت، فهي مصممة فـي الأصل بشـكل مفـتوح دون قـيود أوحواجز أمـنية، لتسهـيل دخـول المستخدمـين ، كـما أنـه توجـد بـها ثغـرات يـمكن للمنظمات الإرهابـية إستغـلالها فـي التسلل للبنى التحتية والقيام بالعمليات التخريبية عليها[74]، دون أن تـظهر هـويتها الحقـيقية ، وأن تهـاجم من أي مـكان فـي العـالم وبأقـل تكـلفة دون تـرك أي دليـل رقـمي وهـذا لصعوبة إكتشاف الجريمة قبل وقوعها.

كما أن الفـراغ القـانوني والتنـظيمي لـدى بعـض المجتـمعات حـول الإرهـاب السيـبراني خاصة ، والجـرائم السيبـرانية بصفـة عامـة، وإختلافها إن وجدت من بلد إلى بلد آخر، شجع الإرهبـيين للفـرار إلـى الـدول الـتي تعتمد قوانين أقل صرامة وهنا تثار مسألة تنازع القوانين، والقـانون واجـب التطبيـق، كـذلك عـدم وجـود جـهة مركزية موحـدة تتحكم وتراقب مايعرض

[74] غادة نصار، الإرهاب والجريمة الإلكترونية ، العربي للنشر والتوزيع، الطبعة 01، القاهرة ، 2017 م، ص .81 .

على الشبكة يعد سببا مهما في تفشي هذه الظاهرة [75] ، هذا الطرح الأخير يعتبر صعبا نوعا ما لتحقيقه حتى وإن وجدت الإرادة لفعل ذلك وهـذا راجع للخصائص التي يتمتع بها الفضاء السيبراني التي ذكرناها سالفا.

الفرع الثاني: أساليب الإرهاب السيبراني

يعتمد الإرهـاب السيـبراني عـلى إستخدام الإمكانيات العلمية والتقنية، وإستغلال وسائل الإتـصال والشـبكات المعـلوماتية، مـن أجـل تخـويف وتـرويع الآخـرين، وإلحاق الضرر بهم أو تهـديدهم، مثل ماحدث في عام 2000 م، حينما أدى إنتشار فيروس "**I LOVE YOU** " إلى إتـلاف معلومات بقـيمة **10** مـليار دولار أمـريكي، وفـي عام 2003 م، أشاع فيروس "بلاستر" الدمار فـي نـصف مليون جـهاز حاسوب [76]، ومـن بـين الأسالـيب والأدوات التي يستخدمها مايلي:

أولا: البريد الإلكتروني: يعـتبر البـريد الإلـكتروني الوسـيلة الأكـثر إنـتشارا وشيـوعا مـن أجـل التواصل السريع، وهو من بين أهم الخدمات التي تقدمها الأنـترنت ، فـهو يسـمح بتـبـادل الرسائل، و الملفات مـع عــدة أشخاص مـن مستخـدمي الأنـتـرنت مـع سهـولة الإطـلاع عليها في أي مكان وفي أي وقت فهي لا ترتبط بمكان أو زمان معينين[77]، ورغـم أهميته إلا أنه يصعب تأمينه، فـقد ثـبت أن الكثير من العمليات الإرهابية التي تمت في الآونة الأخيرة كان البريد الإلكتروني السبب فيها .

ثانيا: مواقع الشبكة الإلكترونية: لقـد إستفـادت التنظيمات الإرهابية من الشبكة العالمية للأنترنت فـأتاحت لهـم إمكانية إنشاء وتصميم المواقع من أجل نشر أفكارهم، و تجنيد عناصر جديدة،

---

[75] العجلان، عبد الله بن عبد العزيز بن فهد، الإرهاب المعلوماتي، دار المنظومة،2015 م ، ص . 51 . على الرابط: https://search.mandumah.com/Record/690587

[76] وهيبة بشريف، أساليب الجريمة الإلكترونية: مسار الإنتقال من الإرهاب التقليدي إلى الإرهاب الإلكتروني في ظل المجتمع المعلوماتي، الحوار الثقافي، الطبعة 08، العدد 01، 2019م، ص.65. على الرابط: https://asjp.cerist.dz/en/article/76418

[77] خالد ممدوح إبراهيم، **حجية البريد الإلكتروني في الإثبات دراسة مقارنة**، القاهرة: دار الفكر العربي، ،2008م، ص.19.

وإقـامة معـسكرات تدريبية إفتراضية، فأصبحت ساحة لتبادل المعارف والخبرات، وآلية لتبادل المعـلومات بين عدة أفراد موزعين في أماكن مختلفة من العالم [78]، ويمكن التمييز بين ثلاث أنواع من المواقع:

أ/- مواقع الويـب على الشبكة السطحية: وهـي مـواقع عـادية يـمكن لأي شخـص الوصـول إليـها عـن طريـق محـركات البحـث العـادية أو بإستـخدام (VPN) في حالة منعها من قبل الـدول مـن حيث تمنح هذه التطبيقات لمستخدميها هوية إلكترونية مزورة عبر إستخدام (IP) مزور [79].

ب/- مواقـع الشـبكة العـميقة (Deep web): تحـتوي عـلى قـواعد البـيانات الأكـاديمية والسجـلات الحـكومية وقـواعد بـيانات الشـركات والبنـوك التـجارية ومحـتوى رسائل البريد الإلكـتروني وخـدمات البـث التلفزيوني[80]، يتـطلب الـولوج إلـيها تقـنيات عـالية يستخـدمها الإرهابيـون للـتواصل، وتبـادل المعلـومات والأموال في بيئة مشفرة يصعب فيها إكتشافهم أو تعقبهم .

ج/- مواقع الشبكة المظلمة (Dark web): تـمكن المستخدمين من إخفاء هوياتهم الحقيقية والوصول إلى الخـدمات المخفـية ،والقـيام بمخـتلف الأنشـطة غير المشروعة دون إكتشاف ذلك.

---

[78] صليحة محمدي و شفيعة حداد، الإرهاب الإلكتروني والأمن القومي للدول: (نمط جديد وتهديدات مختلفة)، **المجلة الجزائرية للأمن والتنمية**، المحلد 08، العدد 02، جامعة الحاج لخضر، باتنة، الجزائر، جوان 2019 م، ص ص.65-77.، على الرابط:https://asjp.cerist.dz/en/article/96164

[79] ربيع رافعي،الإرهاب الدولي وعلاقته بالجريمة المنظمة(الإرهاب الإلكتروني نموذجا)، **مجلة القانون والعلوم السياسية**، المجلد 07، العدد 01، المركز الجامعي صالحي أحمد، النعامة، الجزائر،2021 م، ص ص .70-78. على الرابط: https://asjp.cerist.dz/en/article/161289

[80] محمد كمال، المرجع السابق، ص .88 .

ثالثا: البرامجيات الخبـيثة (Malware): هـي بـرامج حاسوب خبيـثة تجعـل أجهزة الحاسوب أو الشبكات تفعل أشياء لا يريد أصحابها أو مستخدموها أن تفعلها [81] ومن أمثلتها:

أ/- حصان طـروادة (Cheval de Troy): هـو نوع مـن البـرامج الضـارة يتخـفى غـالبا فـي صـورة برنامـج شـرعي، يمـكنه الـوصول إلـى أنـظمة المستخـدمين عـن طريـق البريد الإلكتـروني أو عـن طـريق تحمـيل برامـج وملـفات مـن المواقـع وتسمـح فيروسات حصان طـروادة بمـجرد تنشيطها لمـجرمي الإنترنت بالتجسس عليك وسرقة بياناتك الحساسة والتسلل إلى نظامك [82].

ب/- الديدان الحاسوب (Computer Worms): هـي بـرامج صغـيرة قائـمة بذاتها غير معتـمدة على غـيرها صنعـت للقيام بأعمال تدميرية أو لغرض سرقة بعض البيانات الخاصة ببعـض المستخدميـن أثـناء تصفـحهم للإنـترنت أو إلحاق الضرر بهم تمتاز بسرعة الانتشار ويصعب التخلص منها نظرا لقدرتها الفائقة على التلون والتناسخ والمراوغة [83].ولعل أشهرها (دودة ستاكسنت) التي تم اكتشافها عام 2009 م عندما أصابت أجهزة الطرد المركزي الإيراني في منشأة ناتانز لتخصيب اليورانيوم، وتسببت في تعطيل وخروج عدد كبير منها عن العمل، حيث استهدفت نظم تشغيل أجهزة الطرد المركزي التي تعمل عبر برنامج التحكم الصناعي SCADA من صنع شركة سيمنز الألمانية، وقامت بتسجيل مؤشرات تتعلق بعملية تخصيب اليورانيوم، ثم قامت بالتلاعب بآلية عمل أجهزة الطرد وتخريبها، حيث لدى ستاكسنت القدرة على إعادة برمجة وحدات التحكم المنطقي القابلة للبرمجة، وإخفاء التغييرات التي تم تنفيذها، وفي الوقت نفسه عرض المعلومات القديمة التي قامت بتسجيلها على

---

[81] ريتشارد كلارك و روبرت نيك، حرب الفضاء الإلكتروني التهديد التالي للأمن القومي وكيفية التعامل معه، مركز الإمارات للدراسات والبحوث الإستراتيجية، الطبعة 01، أبو ظبي، الإمارات العربية المتحدة، 2012 م، ص .331.

[82] أنظر: فيروس حصان طروادة على الرابط:https://me.kaspersky.com/resource-center/threats/trojans

[83] أنظر: ماهي الديدان Worms وكيف تعمل وسبل الوقاية منها؟ على الرابط:
https://www.momar.tech/2021/10/What-are-worms-how-do-they-work-and-how-to-prevent-them.html

الشاشات لكي يظهر الأمر للمراقبين والفنيين بأن كل شيء يسير بصورة طبيعية، حتى نجحت في إنهاء مهمتها. وبصورة عامة، تقوم ستاكسنت بمهاجمه أنظمة التحكم الصناعية المستخدمة على نطاق واسع في المنشآت الهامة، مثل: خطوط نقل النفط، ومحطات توليد الكهرباء، والمفاعلات النووية، وغيرها من المنشآت الاستراتيجية الحسّاسة، وتقوم بالانتقال بين الأجهزة عبر أجهزة USB مستغلة أحد نقاط الضعف في برنامج التشغيل ويندوز.

ج/- الفيروسات (Virus): وهي عبارة عن برامج تستنسخ نفسها في الجهاز وعندما تنشط تحدث تغييرات في البرامج، أو في البيئة التي تعمل فيها، ولها أضرار مختلفة تتمثل في فقد الملفات المخزنة، وقد تصل ثلك الأضرار إلى تحطم نظام التشغيل في الجهاز وأهمها:

1- فيروس الفدية (Ransomware): يقوم بتشفير البيانات ويعتبر من أخطر الوسائل لأنه يحول بين المستخدم والبيانات فلا يتمكن من الوصول إليها إلا بمقابل فدية يقدمها للجاني [84].

2- فيروس تشيرنوبيل: يقوم بالهجوم على أنظمة تشغيل الويندوز، فيخرب النظام، كما يحاول القيام بمسح (Bios)، وهو نظام معقد ضروري لإقلاع الجهاز، فإن حدث وأستطاع مسحه يصبح مستعصيا إعادة تنصيبه ويلجأ الكثير لتغيير اللوحة الأم لأجهزتهم[85].

3-فيروس فلام (Flame): أكتشف في 28 ماي 2012 م ويفوق ستاكسنت في تعقيده بأكثر من 20 ضعف، وهو عبارة عن منصة لها القدرة على إستقبال وتثبيت وحدات برمجية مختلفة ذو أهداف مختلفة، يبلغ حجمه حوالي 20 ميغابايت يستعمل للإختراق، التجسس، والتدمير [86].

---

[84] إيهاب خليفة، الهجمات الصفرية(كيف يمكن الإستعداد لليوم الأسود في الأنترنت؟)، 17 مايو 2017 م، تم الإطلاع عليه بتاريخ 2025/03/29 م، على الساعة 14:40 على الرابط:https://2u.pw/ezMKW

[85] أنظر: فيروس تشيرنوبيل على موقع ويكيبيديا الموسوعة الحرة على الرابط: https://2u.pw/eHBiy

[86] أنظر: فيروس flame على موقع ويكيبيديا الموسوعة الحرة على الرابط:https://2u.pw/vNqBX

د/- القنابل المنطقية (Logic Bombs) والقنابل الموقوتة (Time Bombs): هي نوع من أنواع حصان طروادة، مقيدة بشرط منطقي محدد لكي تعمل، كبلوغ الموظفين عددا معينا، أو كتابة كلمة معينة، أو عند تشغيل برنامج معين لعدد محدد من المرات، أما القنابل الموقوتة فتعمل وفقا لتوقيت معين [87].

رابعا:شرائح الأردوينو(Arduino): وهي نوع من الهجمات السيبرانية التي تعرف بالإختراق المادي، تتمثل في شريحة قابلة للبرمجة للقيام بأوامر معينة ومن ثم دمجها مع ملحق مادي كلوحة المفاتيح أو هاتف نقال... إلخ [88].

خامسا:خدمات حجب الخدمة (dDOS): أو قطع خدمة الأنترنت عن طريق الإغراق الموزع للموقع، أو السيرفر باللآلاف من الرسائل والزيارات الوهمية في آن واحد، مما يؤدي إلى تعطل الخدمة لمحدودية السيرفرات في تحمل عدد الطلبات على الموقع[89].

سادسا: القنابل الكهرومغناطيسية: القنبلة الكهرومغناطيسية هي سلاح دمار شامل يستهدف تعطيل الأجهزة الإلكترونية من خلال النبضة المغناطيسية الكهربائية الكبرى "النبضة الكهرومغناطيسية"، التي يمكنها التداخل مع الأجهزة الكهربائية والإلكترونية ونظم تشغيلهم لإلحاق أضرار فيهم وإصابتهم بالتلف[90]. ومن أهمها:

---

[87] فاتن سعيد بامفلح، حماية أمن المعلومات في شبكة المكتبات بجامعة أم القرى :(دراسة حالة)، **الإتجاهات الحديثة في المكتبات والمعلومات**،العدد 18، المكتبة الأكاديمية، القاهرة، مصر، 2002، ص ص .249-282. على الرابط: https://www.kau.edu.sa/Show_Res.aspx?Site_ID=0012433&Lng=AR&RN=56927

[88] ربيع رافعي، المرجع السابق، ص.75.

[89] نفس المرجع، ص. 75 .

[90] منال وراقي، ماذا نعرف عن القنبلة الكهرومغناطيسية التي هددت إسرائيل أنها قد تعيد إيران إلى العصر الحجري؟،14 أفريل 2024 م، تم الإطلاع عليه بتاريخ 2025/03/29 م، على الساعة 16:10 على الرابط: https://www.shorouknews.com/news/view.aspx?cdate=14042024&id=ee610ec3-932e-43ff-90ef-4bdebfa2b038

أ/- الحقيبة كهروستاتيكية (Electrostatic Bag): هي أحد أنواع التكنولوجيا العسكرية وأحدثها، تأتي على شكل حقائب محمولة صغيرة، تقوم بتوليد نبضات كهرومغناطيسية (Electromagnetic Pulses) فائقة القدرة، يمكن من خلالها تدمير الوحدات الإلكترونية في أية دارة، أو محطات الإرسال فتفقد قدرتها التشغيلية أو الإنتاجية[91] .

ب/- قنابل التعتيم الميكروويفية: هي قنابل صغيرة تعمل على قطع جميع مصادر الطاقة والمعلومات في المكان المستهدف عن طريق النبض الكهرومغناطيسي[92].

ج/- قنبلة الغرافيت: وهي قنبلة غير قاتلة تستعمل لتعطيل أنظمة الطاقة الكهربائية، تعمل عن طريق نشر سحابة دقيقة جدا من أليياف الكربون المعالج كيميائيا على المكونات الكهربائية فتسبب ماسا وإنقطاعا في الكهرباء[93].

سابعا:الطائرات دون طيار(Aircraft Drone): تمتلك هذه الطائرات قدرات عالية على التصوير والرصد والمراقبة، وقصف الأهداف بدقة وقد ظهرت هذه التكنولوجيا لدى العديد من التنظيمات الإرهابية المسلحة كداعش والجماعات في أمريكا اللاتينية .

وفي الختام هناك أسباب متعددة مشتركة بين الإرهاب التقليدي والإرهاب السيبراني ، أسباب شخصية وفكرية وسياسية وإجتماعية وإقتصادية...إلخ، بالإضافة إلى أسباب خاصة المتعلقة بالتقنية المستخدمة في الهجمات، ومدى توفرها وسهولة إستعمالها، وقلة تكاليفها وصعوبة إكتشافها أو إثباتها، بالإضافة إلى الفراغ القانوني وإختلاف القوانين بين الدول للأفعال المجرَّمة، كما أنه تستعمل عدة أدوات من طرف الإرهابي السيبراني من أجل التجسس أو التزوير أو إتلاف البيانات أو المعلومات أو إعتراض الخدمة أو الإغراق والقصف المعلوماتي مما يسبب ضرر مادي ومعنوي للمستهدف .

---

[91] وليد غسان سعيد جلعود، دور الحرب الإلكترونية في الصراع العربي الإسرائيلي، أطروحة ماجستير في التخطيط والتنمية السياسية، كلية الدراسات العليا، جامعة النجاح ، نابلس، 2013 م، ص .103.

[92] نفس المرجع، ص.105.

[93] أنظر: قنبلة غرافيت على موقع ويكيبيديا الموسوعة الحرة على الرابط:https://2u.pw/nlyCK

الفصل الثانـي
آليات مكافحة الإرهاب السيبرانـي

إن الإعـتماد المتـزايد للفضاء السيـبراني مـن قـــبل الـدول فـي جـميع المــجالات دون إستثـناء، وخصـوصا في المجالات المدنية الحيوية والعسكرية، أصبح يشكل هدفا للمجموعات الإجـرامية المنظمة والإرهابية و تهديدا للسلم والأمن الدوليين، بحيث تكيفت هذه المجموعات مـع هـذا التـطور، وأضحـت تسـتعمل هـي الأخـرى الوســائل التكـنولوجية والتقـنية الحديثة فـي هجـماتها ضـد الـدول، التـي إتخـذت عدة أشكال كالهجوم بإستعمال الفيروسات والبرامج الضارة، أو التجسـس والتخـريب، وهجـمات حجـب الخـدمة، وغـيرها من الوسائل التكنولوجية المستحدثة.

ولقـد شهـد العـالم العـديـد مـن الهجمات بإستعمال الفضاء السيبراني، التي خلفت خسائر وأضـرار ماديــة فـي البـنى التحتـية، وفـي البيانات والمعلومات، ولعل أشهرها كما رأينا سابقا دودة **(ستاكسـنات)** التي إستهدفت أجهزة الطرد المركزي النووية الإيرانية، وفي سنة 2014 م قامـت مجمـوعة من المتسللين التابعين لدولة كوريا الشمالية بتسريب وثائق سرية تابعة لشركة (Sony Pictures Entertainment)، إحتـجاجا عـلى فـيلم **(المقـابلة)** الذي صور كوريا الشمـالية فـي وضـع غير موات، وفي 2017 م تم الهجوم من قبل كوريا الشمالية على مئات الآلاف مـن أجهـزة الكمـبيوتر الشـخصية فـي أكـثر من 150 دولة، بواسطة فيروس الفدية (WannaCry) الذي إستغل ثغرة أمنية في نظام الويندوز لإلغاء الوصول إلى البيانات[94].

كما أصبح الفضاء السيبراني وسيلة للتواصل الآمن بين مختلف التنظيمات الإرهابية حول العالـم، ومجال جديد من أجل التجنيد وإستقطاب فئات جديدة عن طريق إنشاء مواقع جهادية عـلى مختـلف مـواقع الـتواصل الإجـتماعي والمـنصات وللإعلام، فعلى سبيل المثال يعتبر تنـظيم **(داعــش)** الإعـلام أداة قـتال رئيسية ومن أبرز المنصات الإلكترونية التي تبث أخبار التـنظيم بإنتـظام : مؤسـسة آفـاق، الأشهاد، الفرقان، الفرات للاعلام النصرة الشامية، الوعد،

[94] سكينة قيش، سلوى السماتي، الآليات الوطنية والدولية لمكافحة الحروب السيبرانية، مجلة قراءات علمية في الأبحاث والدراسات العلمية، العدد 41، مارس 2025 م، ص.77.

البتار، الثبات...وغيرها[95]، وكذلك بحثت هذه التنظيمات عن طرق جديدة لتمويل عملياتها عن طريق إستخدام العملات المشفرة .

في ظل إزدياد مخاطر الجرائم السيبرانية وعلى رأسها الإرهاب السيبراني، بات من الضروري تظافر الجهود الدولية والإقليمية من أجل تحقيق التعاون الدولي ووضع إستراتيجية قانونية وأمنية لمواجهته والوقوف على أهم المعوقات (**المبحث الأول)** وكذلك إستخدام آليات تقنية وفنية تبدأ بالرصد والمتابعة والمراقبة وتنتهي بإتخاذ إجراءات عملية وقائية وحصر العراقيل من أجل معالجتها (**المبحث الثاني).**

المبحث الأول:

الجهود الدولية والإقليمية لمكافحة الإرهاب السيبراني

ظهرت الصلة واضحة بين الإرهاب والفضاء السيبراني خصوصا بعد أحداث الحادي عشر من سبتمبر، عندها أدركت الدول والمنظمات أهمية التعاون الدولي في مواجهة الهجمات السيبرانية، فعمدت إلى عقد الكثير من الإتفاقيات وحثت الدول للمصادقة عليها من أجل ضمان الحد من الهجمات السيبرانية ومعاقبة منفذيها عملا بمبدأ الشرعية الجنائية " **لا جريمة ولا عقوبة إلا بنص** ". كما أصدرت المنظمات قرارات، وإعلانات، وتوجيهات، وحثت على التعاون بين القطاع العام والخاص من أجل مواجهة الجرائم السيبرانية عن طريق حوكمة الأمن السيبراني، وتكييف قوانينها الداخلية وتطويرها مع تطور الأنشطة الإرهابية.

المطلب الأول:

جهود المنظمات الدولية في مكافحة الإرهاب السيبراني

وسنتناول في هذا المطلب جهود منظمة الأمم المتحدة (**الفرع الأول**)، وجهود المنظمة العالمية للملكية الفكرية **(الفرع الثاني)**، وجهود الإتحاد الدولي للإتصالات **(الفرع الثالث)**، وجهود المنظمة الشرطة الجنائية الدولية **(الفرع الرابع)** .

---

[95] إنجي محمد مهدي، الجهاد الإلكتروني: دراسة لتنظيم داعش، وإستراتيجية الولايات المتحدة لمواجهته، مجلة دراسات، المجلد 22، العدد 02، أفريل 2021 م، ص.153.

الفرع الأول: جهود منظمة الأمم المتحدة:

تظهـــر جليا جهـــود منظمة الأمـــم المتحدة في مكافحة الإرهاب بكل أنواعه وأشكاله من خلال القرارات الصادرة عن أجهزته، وخصوصا قرارات مجلس الأمن وجمعيته العامة، والتي في المجمل تدعو إلى مكافحة الإرهاب بكافة أنواعه عن طريق التعاون الدولي والأمن السيبراني، كما أن لجنة مكافحة الإرهاب المنشئة من طرف مجلس الأمن إعتمدت إعلان (**دلهي**) بشأن (**مكافحة إستخدام التكنولوجيات الجديدة والناشئة لأغراض إرهابية**).

صدر هذا الإعلان عن الإجتماع الخاص الذي عقد بالهند بتاريخ: 29/28 أكتوبر 2022 م، ويحتوي على (35) مادة، بدأ بالتذكير أن الإرهاب بأشكاله ومظاهره يمثل أحد أشد الأخطار التي تهدد السلام والأمن الدوليين، كما أنه لم يعط تعريفا له، وأشار إلى إزدياد الأعمال الإرهابية بإستخدام التكنولوجيات الجديدة والناشئة، ولاسيما لأغراض التجنيد و التحريض وكذلك لتمويل الأنشطة الإرهابية، والتخطيط والتحضير لها، وإستخدامه للمنظومات الجوية غير المأهولة على الصعيد العالمي، والإتجار بالمخدرات والأسلحة[96].

دعا الإعلان دول الأعضاء إلى تنفيذ القرارات الصادرة عن مجلس الأمن لاسيما: القرار 1373 (2001)، القرار 1624 (2005)، القرار 2178 (2014)، القرار 2396 (2017) و القرار 2617 (2021)، وأن تعمل بشكل تعاوني من أجل منع ومكافحة إستخدام تكنولوجيات المعلومات والإتصالات الجديدة والناشئة لأغراض إرهابية والعمل على القضاء على المحتوى الإرهابي على الأنترنت .

كما شدد الإعلان على ضرورة التعاون الطوعي بين القطاع العام والخاص والمجتمع المدني من أجل تطوير وتنفيذ وسائل أكثر فعالية للتصدي لإستخدام التكنولوجيات الجديدة والناشئة لأغراض إرهابية ومكافحة الخطاب الإرهابي مع إحترام القانون الدولي.

---

[96] أنظر إعلان دلهي بشأن مكافحة إستخدام التكنولوجيات الجديدة الجديدة والناشئة لأغراض إرهابية الصادر عن لجنة مكافحة الإرهاب التابعة لمجلس الأمن بالهند بتاريخ 28-29 أكتوبر 2022 م.

دعا إلى إحترام حقوق الإنسان والحريات الأساسية ومراقبة الأصول الإفتراضية والصكوك المالية الجديدة كمنصات التمويل الجماعي من أجل مكافحة غسيل الأموال ومكافحة تمويل الإرهاب وتعزيز إمكانية تعقب المعاملات المالية وشفافيتها.

كما دعا كذلك إلى تعزيز الخبرة المتخصصة وقدرات السلطات العاملة من أجل مواكبة التطور السريع في الأدوات المالية وأساليب تمويل الإرهاب[97] .

ومن أجل تعزيز قدرات الدول والمنظمات الخاصة منع إساءة إستعمال الإرهابيين لتكنولوجيا الإتصال الحديثة، أو التخفيف من حدة أثر إساءة إستعمالها، إتخذ مكتب الأمم المتحدة لمكافحة الإرهاب عدة مبادرات أهمها: "**برنامج أمن الفضاء الإلكتروني والتكنولوجيات الجديدة**"، الذي يهدف إلى تطوير إستخدام وسائط التواصل الإجتماعي لجمع المعلومات من مصادر مفتوحة و الأدلة الرقمية لمكافحة الإرهاب على الأنترنت، وذلك في ظل إحترام حقوق الإنسان، ويتيح البرنامج الخبرة في المحافل الدولية بشأن الإستخدامات الإرهابـية للمنظـومات الجوية غـير المأهولة، كما يسعى إلى تخفيف أثار هذه الهجمات في حالة وقوعها وإصلاح وإستعادة النظم المستهدفة [98] .

ونظرا لوجود معوقات والكثير من العقبات التي تعترض التعاون الدولي لمكافحة هذه الظاهرة والمتمثلة في :

أ/- عدم وجود نموذج موحد للفعل المجرم، فما يعتبر إساءة إستخدام نظم المعلومات والأنترنت في بلد ما، يعتبر مباحا في بلد آخر وهذا ما يعيق تسليم المجرمين لعدم توفر التجريم المزدوج .

ب/- تنوع وإختلاف الإجراءات المتبعة في التحري والتحقيق والمحاكمة .

ج/- مشكلة الإختصاص في الجرائم المتعلقة بالأنترنت وإثارة مسألة السيادة .

إعتمدت الجمعية العامة للأمم المتحدة في أواخر سنة 2024 م إتفاقية **منع ومكافحة الجرائم الإلكترونية** التي تهدف إلى منع ومكافحة الجرائم الإلكترونية بكفاءة وفعالية أكبر،

---

[97] أنظر المادة (27) من إعلان دلهي بشأن مكافحة إستخدام التكنولوجيات الجديدة الجديدة والناشئة لأغراض إرهابية .

[98] مصطفى خليل كامل خليل، المرجع السابق، ص.60.

من خلال تعزيز التعاون الدولي، وتقديم المساعدة الفنية ودعم بناء القدرات، وخاصة للدول النامية، وإعتمدت الجمعية العامة القرار دون تصويت وإستغرق التفاوض على النص بين الدول الأعضاء، والمؤسسات الأكاديمية والقطاع الخاص والمجتمع المدني أكثر من خمس سنوات، وسيتم فتح الاتفاقية للتوقيع في حفل رسمي تستضيفه فييتنام في عام 2025 . وستدخل الاتفاقية حيز التنفيذ بعد 90 يوما من التصديق عليها من قبل الدولة الموقعة الأربعين[99] .

الفرع الثاني: جهود المنظمة العالمية للملكية الفكرية (Wipo):

كانت للثورة الصناعية وتـزايد التـبادل التجـاري بيـن الـدول الفضل في ظهور العديد من الإختراعات والإبتكارات، مما أعطى دفعة قوية لدعم الإعتراف الدولي بحماية الملكية الفكرية وضرورة تنسيق هذه الحماية على المستوى الدولي لكل من الملكية الصناعية في صورة براءات إختراع، العلامات التجارية في التصميمات الصناعية، فأبرمت إتفاقية سنة 1883 م بباريس لحماية الملكية الصناعية، ثم أدخلت عليها تعديلات وتنقيحات سنة 1967 م ثم تلتها إتفاقية " **برن** " لحماية الملكية الأدبية والفنية، وللعلم تشرف المنظمة العالمية للملكية الفكرية على تطبيق عدة إتفاقيات وهي:

أ/- إتفاقية باريس لسنة 1883 م وتعديلاتها المختلفة .

ب/- إتفاقية برن لسنة 1886 م وتعديلاتها المختلفة .

ج/- إتفاقية مدريد لسنة 1896 م وتعديلاتها المختلفة (إتفاق مدريد بشأن التسجيل الدولي للعلامات)

د/- إتفاقية روما لسنة 1961 م لحماية المؤدين ومنتجي التسجيلات الصوتية وهيئات الإذاعة و إتفاقية جنيف لسنة 1970 م لحماية منتجي التسجيلات ضد النسخ غير المشروع لتسجيلاتهم.

[99] أنظر الجمعية العامة تعتمد إتفاقية تاريخية بشأن الجرائم الإلكترونية على الرابط:
https://news.un.org/ar/story/2024/12/1137776

هـ/- إتفاقية بروكسل لسنة 1974 م بشأن توزيع إشارات البث عبر الأقمار الصناعية، وإتفاقية واشنطن لسنة 1989 م لحماية الدوائر المتكاملة.

و/- الإتفاقية العالمية لحقوق المؤلف الموقعة في جنيف لسنة 1952 م و صيغة باريس لسنة 1971 م .

ز/- إتفاقية التسجيل الدولي للمصنفات السمعية والبصرية الموقعة في سنة 1989 م[100] .

شكلت المنظمة تحت لواء الأمم المتحدة مجموعة عمل، تضم عددا كبيرا من الخبراء بهدف دراسة الأساليب المناسبة لحماية برامج الكمبيوتر من خلال إخضاعها لقوانين حماية المؤلف، وهذا من خلال المواد (04) و (05) من إتفاقية التريبس.

الفرع الثالث: جهود الإتحاد الدولي للإتصالات(ITU):

تأسس الإتحاد الدولي للإتصالات (ITU) سنة 1865 م وهو متخصص في مجال تقنية المعلومات والإتصالات، يهدف إلى تسهيل الإتصال الدولي عبر تخصيص مدارات الأقمار الصناعية، وتطوير المعايير التقنية، وتحسين الوصول لتقنية المعلومات والإتصالات في جميع أنحاء العالم، وهو وكالة متخصصة تابعة للأمم المتحدة، وقد وضع عدة التشريع في مجال الجرائم السيبرانية سنة 2010 م، من خلال الجمع بين تشريعات الدول المتقدمة في مجال مكافحة الجرائم السيبرانية، وتحليل شامل لإتفاقية مجلس أروبا المتعلقة بجرائم الفضاء السيبراني، ووضع خارطة طريق لتعزيز الأمن السيبراني العالمي، ويعتمد على أربع ركائز إستراتيجية لمساعدة الدول على التحول الرقمي: تهيئة البنى التحتية، تأمين الإستثمار، تعزيز الإبتكار، وضمان الشمولية وذلك من أجل تحقيق مايلي:

أ /- وضع إستراتيجيات لتطوير نماذج التشريعات السيبرانية ، يكون قابلا للتطبيق محليا وعالميًا موازيا للتدابير القانونية الوطنية و الدولية النافذة.

ب/- وضع إستراتيجيات لتهيئة الأسس الوطنية والإقليمية الملائمة ، لوضع الهيكليات

---

[100] أحمد عبد الخالق، حماية حقوق الملكية الفكرية في ظل إتفاقية التربس والتشريعات الإقتصادية، دار الفكر و القانون، الطبعة 01، مصر، سنة 2011 م، ص . 09 .

التنظيمية والسياسية المتعلقة بجرائم الانترنت.

ج/- وضـع إسـتراتيجية لتحـديد الحـدود الدنـيا المقبولة عالميًا، في موضوع معايير الأمن ونظم تطبيقات البرامج والانظمة.

د/- تحـديد إسـتراتيجيات لوضـع آلية عالمية للمراقبة والانذار والرد المبكر ، مع ضمان قيام التنسيق عبر الحدود.

هـ/- وضـع إسـتراتيجيات لإنشـاء نـظام هـوية رقـمية عالـمية وتطبيـقه، وتحديد الهيكليات التنظيمية اللازمة للإعتراف بالوثائق الرقمية للأفراد عبر الحدود الجغرافية.

و/- تطـوير إسـتراتيجية عالـمية لتسـهيل بـناء القدرات البشرية ، والمؤسسية لتعزيز المعرفة والدراية لضمان الإعتراف بالوثائق الرقمية ، وفي جميع مجالات المعلوماتية.

ز/- تقـديم الإستـشارة بـشأن إمـكانية إعـتماد إطـار إستراتيجي عالمي لأصحاب المصلحة ، من أجل التعاون الدولي، والحوار والتعاون والتنسيق في المجالات السالفة الذكر[101].

وقـد تـم عـقد إتفاق تعاون بـين الأنتربول والإتـحاد الدولي للإتصالات سنة 2018 م لأن هذا الأخير هو الوكالة المتخصصة لتكنولوجا المعلومات والإتصالات التابعة لمنظمة الأمم المتحدة من أجل مكافحة الإرهاب السيبراني عن طريق موائمة التشريعات الوطنية والإتفاقيات الدولية، إضافة إلى تبادل المعلومات مع مراعاة السرية في ذلك[102].كما تم قبل ذلك في ديسمبر 2012 م مع سلطنة عمان تأسيس المركز العربي الإقليمي للأمن السيبراني حيث يسعى المركز لإنشاء بيئة أكثر أمنا وتعاونا في مجال الأمن السيبراني في المنطقة العربية [103] .

---

[101] علي حيدر، المنظمة الدولية للشرطة الجنائية ودورها في مكافحة الإرهاب السيبراني، رسالة ماجستير في القانون العام، كلية القانون، جامعة كربلاء، 2023 م، ص .169.

[102] نفس المرجع، ص.170.

[103] محمد كمال، المرجع السابق، ص .132.

الفرع الرابع: جهود منظمة الشرطة الجنائية الدولية (أنتربول)

أنشئت منظمة الشرطة الجنائية الدولية (الأنتربول) من أجل مكافحة الجريمة المنظمة، حيث يعتبر الإرهاب الدولي بكل أشكاله أحد أخطر هذه الجرائم المنظمة، فإن كانت هذه الأخيرة تهدف إلى الربح المادي فإن الإرهاب يهدف لتحقيق مطالب سياسية عن طريق إثارة الرعب والخوف وسنتطرق في هذا الفرع إلى نشأة المنظمة**(أولا)** و مبادئها ومهامها **(ثانيا)** وأهدافها **(ثالثا)** وجهودها في مكافحة الإرهاب والإرهاب السيبراني **(رابعا)**.

أولا: نشأة المنظمة

تأسست المنظمة عام 1923 م وجعلت من باريس مقرا لها، تجمع بين أجهزة الشرطة للدول الأعضاء والبالغ عددهم 196 دولة، من أجل تحقيق التعاون المتبادل و تسهيله في سبيل مكافحة الجريمة المنظمة، عن طريق تبادل المعلومات، و تطوير المعارف والمهارات اللازمة بين الدول الأعضاء، ملاحقة وتسليم المجرمين الفارين من دولهم إلى دول أخرى شريطة أن تكون الدولة عضو في المنظمة [104] .

ثانيا:مبادئ ومهام المنظمة

تستند المنظمة على مجموعة من المبادئ، التي تساهم وتكفل تحقيق أهدافها خصوصا في تشجيع التعاون الدولي بين الدول في مكافحة الجرائم العابرة للحدود [105] وهي:

أ/- إحترام السيادة الوطنية للدول الأعضاء، وإلتزام الحياد حسب المادة (03) من نظامها الأساسي.

ب/- تساوي المراكز القانونية للدول الأعضاء، بحيث تستفيد من جميع الخدمات التي تقدمها المنظمة على قدم المساواة، وتتساوى في تحمل الإلتزامات الناشئة عن إكتساب العضوية فيها حسب المادة (04) المتعلقة بالعضوية والمادة (13) المتعلقة بالتصويت.

ج/- إحترام حقوق الإنسان والتعاون المستمر والنشط .

---

[104] عبد الرحمن علي إبراهيم غنيم، مدى فاعلية أنتربول في مكافحة الإرهاب، مجلة الباحث في العلوم القانونية والسياسية، العدد 02، ديسمبر 2019 م، ص . 126 .

[105] أنظر النظام الأساسي للمنظمة الدولية للشرطة الجنائية على الرابط:-https://www.legal /tools.org/doc/5b26fd/pdf

د/- إلزامية القرارات الصادرة عن الجمعية العامة للمنظمة وهذا مانصت عليه المادة (09) من نظامها الأساسي .

هـ/- الطابع الشمولي لعمل المنظمة من أجل المساهمة في الوقاية من جرائم القانون العام و مكافحتها[106] .

ويمكن تلخيص مهام المنظمة في : تفعيل التعاون بين أجهزة الشرطة للدول الأعضاء والتنسيق بينها، تبادل المعلومات، ملاحقة المجرمين الفارين والقبض عليهم عن طريق تعميم نشرات دولية والتعاون مع المنظمات والوكالات الدولية الأخرى، تقديم دورات تدريبية وورش عمل حول التحقيقات في الجرائم السيبرانية والأدلة الجنائية الرقمية للدول الأعضاء .

ثالثا:أهداف المنظمة

الهدف من إنشاء الأنتربول حسب المادة (02) من نظامها الأساسي [107]هو:

أ/- تـأمين وتنــمية التعـاون المتبادل على أوسع نطاق بين كافة سلطات الشرطة الجنائية في إطار القوانين القائمة في مختلف البلدان، وبروح الإعلان العالمي لحقوق الإنسان.

ب/- إنشاء وتنمية كافة المؤسسات القادرة على المساهمة الفعالة في الوقاية من الجرائم العابرة للحدود وفي مكافحتها.

رابعا:جهودها في مكافحة الإرهاب السيبراني :

شكلت المنظمة وحدة دولية متخصصة في مكافحة الإرهاب سنة 2001 م، حيث إهتمت هذه الوحدة بتنسيق الجهود لمكافحة الإرهاب، عن طريق الرصد والتحري وتوفير المعلومات عن الأشخاص المتهمين في التورط في الأعمال الإرهابية على المستوى الدولي، بالإضافة إلى تبادل المعلومات بين المراكز الرئيسية للإنتربول[108].

---

[106] لمياء محمد عبد السلام جودة، دور المنظمة الدولية للشرطة الجنائية في مكافحة الإرهاب الدولي، مجلة البحوث الفقهية والقانونية، العدد 42، يوليو 2023 م، ص . 207 .

[107] أنظر الموقع الإلكتروني الرسمي للمنظمة الدولية للشرطة الجنائية على الرابط:

https://www.interpol.int/ar/3/4/1 بتاريخ 2025/04/25 م على الساعة: 14:00

[108] عبد الرحمان علي إبراهيم غنيم، المرجع السابق، ص.128.

وتعد (اللجنة الدائمة لتكنولوجيا المعلومات) من أهم لجان المنظمة التي تعنى بمراقبة المواقع الإلكترونية التي تساعد على إرتكاب الجرائم السيبرانية أو التي تحرض على إرتكابها، وفي نفس الوقت تتأكد من الجاهزية التقنية والفنية للمنظمة في مكافحة هذه الجرائم .

المطلب الثاني:

الجهود الإقليمية في مكافحة الإرهاب السيبراني

سنتطرق في هذا المطلب إلى جهود الإتحاد الأروبي (**الفرع الأول**) وإلى الجهود العربية (**الفرع الثاني**) وإلى جهود الإتحاد الإفريقي (**الفرع الثالث**).

الفرع الأول: جهود الإتحاد الأوروبي

سعى الإتحاد الأوروبي للوصول إلى إطار قانوني لمواجهة الجرائم السيبرانية العابرة للحدود الدولية، وبالتعاون بين مجلسه وبين دول خارج الإتحاد وهي الولايات المتحدة الأمريكية، و جنوب إفريقيا، وكندا واليابان توج هذا التعاون بإتفاقية بودابست لمواجهة جرائم المعلوماتية والإتصالات وتعتبر الإتفاقية الصك الدولي الأول الذي إتجه إلى تجريم كافة أشكال الجريمة الإلكترونية .

تمت المصادقة على الإتفاقية في 23 نوفمبر 2001 م، في العاصمة المجرية بودابست ووقع عليها من قبل 30 دولة ودخلت حيز التنفيذ في 01 يوليو 2004 م، وبالرغم أن هذه الإتفاقية أوروبية المنشأ، إلا أن عضويتها مفتوحة لجميع الدول، وقد راعت وأهتمت الدول أثناء صياغة الإتفاقية بالتوصيات الصادرة عن لجنة الوزراء بالإتحاد الأوروبي، وهي [109]:

أ/- التوصية رقم10/85 المتعلِّقة بتنفيذ الإتفاقية الأوروبية للمساعدة المتبادلة في المسائل الجنائية فيما يتعلق بالإنابة القضائية بشأن اعتراض الاتصالات السلكية واللاسلكية.

ب/- التوصية رقم 2/88 المتعلقة بالقرصنة في مجال حقوق التأليف والنشر والحقوق المجاورة .

ج/- التوصية رقم 15/87 المتعلِّقة بتنظيم إستخدام البيانات الشخصية في قطاع الشرطة .

[109] انظر إتفاقية بودابست المتعلقة بالجريمة الإلكترونية الصادرة عن مجلس أوروبا بتاريخ 2001/11/23 م.

د/-التوصـية رقـم 4/95 المتعلقة بحماية البيانات الشخصية في مجال خدمات الإتـصالات لاسيما الخدمات الهاتفية.

هـ/- التوصـية رقـم 9/89 المتعـلـقة بالجـرائم المـتصلة بالكمـبيوتر الـتي توفـــر مـبادئ توجيهية للجهات التشريعية الوطنية بشأن تعريف بعض جرائم الكمبيوتر.

و/- التوصية رقـم 13/95 المتعلـقة بالمـشاكل التـي يطـرحها قـانون الإجراءات ذات صلة بقانون تكنولوجيا المعلومات[110].

تضمنت الإتفاقية ديباجة و ثماني وأربعين مادة، مقسمة إلى أربعة أبواب:

1/- الباب الأول: إستخدام المصطلحات .

2/- الباب الثاني: التدابير الواجب إتخاذها على الصعيد الوطني .

3/- الباب الثالث: التعاون الدولي .

4/- الباب الرابع: أحكام ختامية حول الإنضمام للإتفاقية.

وأهم ماجاء في الباب الثالث للتعاون الدولي ، إلزام دول المجلس بإتخاذ الإجراءات و التشريعات الكفيلة بتحقيق التعاون الكامل وتطبيق التشريعات الدولية فيما يتعلق بمجالات التحقيق في الجرائم الإلكترونية، كسرقة البيانات و إعتراضها وإتلافها وتعطيل أنظمة الحاسب وتدمير المواقع ومهاجمتها على الأنترنت، وكافة جرائم الحاسب المعروفة والمصنفة قانونا لدى كل دولة، كما ألزم دول المجلس بجمع وتبادل الأدلة الإلكترونية وكذلك الإلتزام بمعاهدات تسليم المجرمين .

الفرع الثاني : الجهود العربية

فتحت إتفاقية بودابست لمكافحة جرائم المعلوماتية الصادرة عن مجلس أروبا المجال لمبادرات إقليمية أخرى من أجل تجريم كل أشكال الجرائم السيبرانية ولم تحد الجامعة العربية عن هذا المسار فصدر عنها:

[110] انظر المرجع السابق.

أولا: القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها سنة 2004 م

تمخضت عن الجهود العربية لمواجهة الإرهاب السيبراني، القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها سنة 2004 م ، ويعتبر قانونا نموذجيا عربيا موحدا أصدر من قبل الأمانة الفنية لمجلس وزراء العدل العرب، وأعتمد في الدورة التاسعة عشر للمجلس بالقرار 495 – د 19 – 2003/10/08 م، كما أعتمد من قبل وزراء الداخلية للعرب بالقرار 417 – د 21 – 2004 م [111].

يتكون هذا القانون على 27 مادة جاءت مادته الأولى لتوضيح الكلمات والعبارات الموظفة فيه وقد جرم الأفعال الآتية:

أ/- كل من دخل عمداً وبغير وجه حق موقعاً أو نظاماً معلوماتيا يعاقب بالحبس والغرامة أو بإحدى هاتين العقوبتين فإذا كان الدخول بقصد إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات شخصية يكون الحد الأدنى لعقوبة الحبس ولعقوبة الغرامة [112].

ب/- كل من أدخل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها، ما من شأنه إيقافها عن العمل أو تعطيلها أو تدمير أو مسح أو حذف أو إتلاف أو تعديل البرامج أو البيانات أو المعلومات بغرض ذلك ولم يتحقق غرضه يعاقب بالحبس والغرامة أو بإحدى هاتين العقوبتين فإذا تحقق الغرض كان الحد الأدنى لعقوبة الحبس ولعقوبة الغرامة [113] .

ج/- كل من أعاق أو شوش أو عطل عمداً وبأية وسيلة عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها الوصول إلى الخدمة أو الدخول إلى الأجهزة أو

---

[111] خالد جمعة سبيت أحمد المخمري، المواجهة الأمنية للإرهاب الإلكتروني، مجلة البحوث القانونية والإقتصادية، المجلد 58، العدد 02، أكتوبر 2023 م، ص ص .379-413.

[112] أنظر المادة (3) من القانون العربي الإسترشادي لمكافحة جرائم الإرهاب الإلكتروني وما في حكمها.

[113] أنظر المادة (6) و المادة (22) من نفس القانون.

البرامج أو مصادر البيانات أو المعلومات يعاقب بالحبس والغرامة أو بإحدى هاتين العقوبتين[114].

د/- كل من استعمل الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها في تهديد أو ابتزاز شخص آخر لحمله على القيام بفعل أو الامتناع عنه، ولو كان هذا الفعل أو الامتناع مشروعاً ، يعاقب بالحبس والغرامة أو بإحدى هاتين العقوبتين[115].

هـ/- كل من أنتج أو أعد أو هيأ أو أرسل أو خزن عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها ما من شأنه المساس بالنظام العام أو الآداب العامة يعاقب بالحبس والغرامة فإذا كان الفعل موجهاً إلى حدث يكون الحد الأدنى لعقوبة الحبس ولعقوبة الغرامة[116] .

هـ/- كل من أنشأ أو نشر موقعاً على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها لأي مجموعة تدعو لتسهيل وترويج برامج وأفكار مخالفة للنظام العام يعاقب الحبس والغرامة [117].

و/- كل من أنشأ أو نشر موقعاً على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها لجماعة إرهابية تحت مسميات تمويهية لتسهيل الاتصالات بقياداتها أو أعضائها أو ترويج أفكارها أو تمويلها أو نشر كيفية تصنيع الأجهزة الحارقة أو المتفجرة أو أية أدوات تستخدم في الأعمال الإرهابية يعاقب بالسجن[118].

كما عاقب القانون على التحريض وتقديم المساعدة والشروع وعاقب عليها بنصف العقوبة للجرائم المذكورة من المواد (3 – 15) وبالعقوبة الكاملة للجرائم المذكورة في المواد (16 – 22) .

---

[114] أنظر المادة (7) من نفس القانون

[115] أنظر المادة (9) من نفس القانون.

[116] أنظر المادة (13) من نفس القانون.

[117] أنظر المادة (20) من نفس القانون.

[118] أنظر المادة (21) من نفس القانون.

ثانيا: الإتفاقية العربية لمكافحة جرائم تكنولوجيا المعلومات لسنة 2010 م :

في إطار الجهود الحثيثة لجامعة الدول العربية لتدعيم التدابير الأمنية لمكافحة الجرائم المتعلقة بتقنية المعلومات، إجتمع وزراء الداخلية والعدل الممثلين لواحد وعشرين دولة عربية في القاهرة بتاريخ 21 ديسمبر 2010 م للتوقيع على الإتفاقية العربية لمكافحة جرائم تقنية المعلومات تتكون الإتفاقية من ديباجة و43 مادة موزعة على خمسة فصول.

يتضمن الفصل الأول أحكاما عامة، الهدف من الإتفاقية، والمصطلحات، ومجالات تطبيق الإتفاقية .

أما الفصل الثاني يتضمن الأفعال المجرمة بموجب هذه الإتفاقية وهي: الدخول والإعتراض غير المشروع في المادتين (06) و (07)، الإعتداء على سلامة البيانات في المادة (08)، إساءة إستخدام وسائل تقنية المعلومات في المادة (09)، جرائم التزوير والإحتيال في المادتين (10) و (11)، جرائم الإباحية والجرائم المتعلقة بها في المادتين (12) و (13)، والإعتداء على الحرمة الخاصة في المادة (14)، والجرائم المتعلقة بالإرهاب في المادة (15) وغسيل الأموال والمخدرات والإتجار في الجنس البشري والأعضاء البشرية والأسلحة في المادة (16)، والمساس بالقيم الدينية أوالنظام العام، والتهديد، والإبتزاز، و الإتجار في الأثار والتحف الفنية، والإستخدام غير المشروع لأدوات الإئتمان والوثائق الإلكترونية، والإعتداء على الملكية الفكرية.

وقد جاء الفصلان الثالث والرابع بتوضيح نطاق تطبيق الأحكام الإجرائية، والتعاون القانوني والقضائي، المتعلق بتسليم المجرمين، والمساعدة المتبادلة بين الدول والمساعدة ذات الصلة أيضا بسلطات التحقيق، كما ألزمت الدول الأطراف أن تتبنى تعديلات في قوانينها الداخلية وتشريعاتها لتجريم الأفعال المشار إليها في الإتفاقية، وجاء الفصل الخامس بأحكام ختامية[119] .

حددت الإتفاقية مجال تطبيقها في أربع نقاط وردت على النحو التالي:

[119] للإطلاع أكثر أنظر الإتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010 م

أ/- إذا أرتكبت في أكثر من دولة .

ب/- إذا كانت الجريمة المرتكبة في الدولة العضو قد تم التخطيط والإعداد لها أو الإشراف والتوجيه بشأنها، في دولة أو دول أخرى.

ج/- إذا كانت الجهة الضالعة في إرتكاب الجريمة، جماعة إجرامية منظمة، لها أنشطة في أكثر من دولة.

د/- إذا كان للجريمة المرتكبة في إحدى الدول آثار بالغة الخطورة والضرر على دولة أو دول أخرى[120].

نصت الإتفاقية على آليات إجرائية لمكافحة جرائم تقنية المعلومات تتمثل في الحفظ العاجل للبيانات المعلوماتية المخزنة والأمر بتسليمها في المادة (23) وأمر تسليم المعلومات في المادة (25) و تفتيش المعلومة المخزنة في المادة (26) وتأمين وضبط المعلومات في المادة (27) والجمع الفوري لمعلومات تتبع المستخدمين في المادة (28) وإعتراض معلومات المحتوى في المادة (29) واستخلاصا مما سبق يمكن القول بأن القانون العربي الإسترشادي هو إطار توجيهي للدول العربية، يهدف إلى تقديم نموذج يمكن للدول تبنيه أو تعديله، وفقا لإحتياجاتها الوطنية أما الإتفاقية العربية فهي ملزمة للدول الموقعة عليها وخلافا للقانون الإسترشادي الذي يركز على التعريفات، فالإتفاقية تتناول تفاصيل أكثر دقة حول التعاون الدولي، تبادل المعلومات، وتسليم المجرمين بين الدول العربية .

ثالثا: الجهود على الصعيد الوطني

صادقت الجزائر على الإتفاقية العربية لمكافحة جرائم تقنية المعلومات بموجب المرسوم الرئاسي رقم: 14 – 252 المؤرخ في 08 سبتمبر 2014 م (ج . ر 57 لسنة 2014)[121]، ولكنها قبل ذلك بذلت جهود لمكافحة الإرهاب والإرهاب السيبراني عن طريق ترسانة من القوانين والآليات نذكر منها:

---

[120] أنظر المادة (03) من نفس الإتفاقية.

[121] أنظر قائمة الإتفاقيات المتعددة الأطراف المصادق عليها من طرف الجزائر على موقع وزارة العدل على الرابط: https://2u.pw/X2qLV بتاريخ : 2025/05/30 م على الساعة 09:25 .

أ/- القانون رقم 04 - 15 المعدل لقانون العقوبات والمؤرخ بتاريخ 10 نوفـــمبر 2004 م (ج . ر العدد 17)، الذي يجرم كل دخول غير مصرح به عن طريق الغش على المنظومة المعلوماتية، إتلاف وتدمير المعطيات، الإستيلاء على المعطيات، الجوسسة والتحريض على الفسق، وقد حددت العقوبة بالحبس والغرامة، أو بالعقوبات التكميلية كغلق المواقع، ومصادرة الأجهزة والبرامج والوسائل المستخدمة[122] .

ب/- القانون رقم 09 - 04 للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها المؤرخ في 05 أوت 2009 م حددت المادة (02) منه في الفقرة (أ) بأن " الجرائم المتصلة بتكنولوجيات الإعلام والإتصال هي: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل إرتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية " [123] .

ج/- إنشاء هيئة بموجب المادة (13) من القانون 09 - 04 سميت الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها بتاريخ 08 أكتوبر 2015 م عن طريق مرسوم رئاسي رقم: 15-261 وهيئات أخرى تضطلع بأدوار هامة في مكافحة الجرائم الإلكترونية وهي:

- مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني .
- المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني .
- المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني[124].

حاولت الجزائر تكييف تشريعاتها وقوانينها الداخلية مع الجرائم السيبرانية، فنظمت القواعد الإجرائية وطرق الإثبات، كما حددت الأفعال المجرمة والعقوبات المترتبة عليها، لكن في نفس الوقت تعد متأخرة كثيرا في جانب الأمن السيبراني، وهذا راجع لضعف البنى التحتية التقنية وبروز فجوة رقمية بينها وبين الدول الأخرى، ولهذا عليها بتحصين فضائها السيبراني

---

[122] أكرم رياض، المرجع السابق، ص . 81 .

[123] عبد الحكيم توات، المرجع السابق، ص . 83 .

[124] عنترة بن مرزوق، محمد الكر، البعد الإلكتروني للسياسة الأمنية الجزائرية في مكافحة الإرهاب، مجلة العلوم الإنسانية والإجتماعية، المجلد 19، العدد 38، جامعة الحاج لخضر، باتنة، الجزائر، جوان 2018 م، ص ص . 29 - 50 . على الرابط: https://2u.pw/P3zgL

عن طريق القيام بالتعاون والشراكة مع الدول الحليفة والقوية في هذا المجال كالصين وروسيا.

الفرع الثالث: جهود الإتحاد الإفريقي

إعتمد الإتحاد الإفريقي إتفاقية مالابو لسنة 2014 م لتحقيق الأمن في الفضاء السيبراني وحماية البيانات ذات الطابع الشخصي، تتكون هذه الإتفاقية من ديباجة و 38 مادة موزعة على أربعة فصول:

أولا: الفصل الأول من المادة (02) إلى المادة (07) يعالج المعاملات الإلكترونية.

ثانيا: الفصل الثاني من المادة (08) إلى المادة (23) عالجت حماية البيانات الشخصية.

ثالثا: الفصل الثالث من المادة (24) إلى المادة (31) عالجت موضوع تعزيز الأمن السيبراني ومكافحة الجريمة السيبرانية .

رابعا: الفصل الرابع من المادة (32) إلى المادة (38) جاءت بأحكام ختامية.

مايميز هذه الإتفاقية عن غيرها، هو إنشاء لـ " آلية مراقبة " للإتفاقية تهدف لمتابعة تحقيق الإتفاقية للإلتزامات الواردة بها، ومن مهامها:

أ/- جمع الوثائق والمعلومات عن إحتياجات الأمن السيبراني وطبيعة الجرائم السيبرانية.

ب/- تقديم المشورة للحكومات الإفريقية حول كيفية الترويج للأمن السيبراني، ومحاربة الجريمة السيبرانية وإنتهاكات حقوق الإنسان.

ج/- جمع المعلومات وإجراء التحليلات على السلوك الإجرامي لمستخدمي الشبكات والأنظمة المعلوماتية[125].

دعت إتفاقية مالابو إلى تعزيز الجهود الدولية لمحاربة الإجرام الإلكتروني دون الإخلال بحقوق الإنسان، كما أن آلية المراقبة تسهر على التأكد من وفاء الدول بإلتزماتها، وما يعاب

[125] مريم لوكال، قراءة في إتفاقية الإتحاد الإفريقي حول الأمن السيبراني وحماية المعطيات ذات الطابع الشخصي لسنة 2014، مجلة الدراسات القانونية والإقتصادية، المجلد 04، العدد 03، السنة 2021 م، ص ص .657 – 673 .على الرابط: https://asjp.cerist.dz/en/article/175553

على الإتفاقية أنها مفتوحة لإنضمام الدول الإفريقية فقط، كما أنها لم تتطرق لآليات التعاون لمجابهة الجرائم السيبرانية.

المبحث الثاني:

الآليات التقنية والفنية لمكافحة الإرهاب السيبراني

تسعى الدول إلى حماية فضاءها السيبراني بالإعتماد على عدة أساليب منها ماهو تشريعي قانوني ومنها ماهو تقني فني، ولهذا تتجه أغلبية الدول للمصادقة على الإتفاقيات الدولية المعنية بهذا الشأن، وتكييف قوانينها الداخلية وفقها، كما أن مفهوم الأمن لم يصبح يقتصر على المجالات الأربع المعروفة، فالسلاح المستخدم في الهجمات السيبرانية، يختلف عن السلاح التقليدي، لهذا إهتمت الدول بالأمن السيبراني **(المطلب الأول)**.

هناك سباق محموم وتنافس بين كل من الصين والولايات المتحدة الأمريكية وروسيا لإمتلاك آخر تكنولوجيا للسيطرة على الفضاء السيبراني، فظهرت تطبيقات الذكاء الاصطناعي التي ساعدت كثيرا في التنبؤ والرصد وإكتشاف الجرائم السيبرانية وتتبعها وملاحقة مرتكبيها (**المطلب الثاني**) .

المطلب الأول:

الأمن السيبراني كآلية لمكافحة الإرهاب السيبراني

يحظى الأمن السيبراني اليوم بإهتمام عالمي بحيث أصبح يشكل جزءا أساسيا من أي سياسة أمنية وطنية، وهو مفهوم ظهر حديثا ويعني مجمل القوانين السياسية، الأدوات، النصوص، المفاهيم وميكانيزمات الأمن وطرق تسيير الأخطار والممارسات التكنولوجية المتعلقة بتكنولوجيا المعلومات والإتصالات المستخدمة لحماية الدول و المنظمات والأشخاص، كما يعرف أنه الحالة المرغوب فيها لعمل أنظمة المعلومات والإتصالات والتي

تمنحها القدرة على المقاومة والتصدي لكل ما ينجم عن الفضاء السيبراني، والذي من شأنه أن يعرض المعلومات المخزنة أو المعالجة أو المنقولة للتلف أو التغيير أو التجسس [126].

ويعد الأمن السيبراني مهما لأن المنظمات الحكومية والعسكرية والشركات والمؤسسات المالية والطبية تعالج وتخزن كميات هائلة من البيانات على أجهزة الكمبيوتر والخوادم، يمكن أن يكـون جزء منها حساس للغاية، والتي يمكن أن يؤدي الوصول غير المصرح به إليها إلى نتائج سلبية، كذلك يمكن أن تنقل هذه البيانات عبر الشبكات وإلى أجهزة أخرى، لهذا تحتاج إلى الحماية [127]. فالهدف الأسمى للأمن السيبراني هو القدرة على مواجهة التهديدات السيبرانية ومقاومتها سواء كانت متعمدة أو غير متعمدة، وإزالة خطرها قبل إحداثها أضرار بالبنى التحتية التي تعتمد على تكنولوجيا المعلومات والإتصالات أو التعافي منها.

الفرع الأول: مباديء الأمن السيبراني

حددت جمعية الأنترنت (ISOC) إستنادا إلى توجيهات الخبراء الإقليميين بشأن الأمن السيبراني المباديء الأساسية لتأمين الأنترنت وهي:

أولا: الوعي: يتعين على جميع الجهات المعنية في كل من القطاعين العام والخاص فهم المخاطر التي تهدد أمنها .

ثانيا: المسؤولية: يجب على جميع الجهات المعنية تحمل مسؤولياتها في مواجهة المخاطر الأمنية، مع تحديد المسؤوليات وإتخاذ الإجراءات في حالة التقاعس.

ثالثا: التعاون: يجب إشراك الجميع في حوار مستمر حول الأمن السيبراني من أكاديميين ومجتمع مدني، وإعلاميين لمواجهة التهديدات السيبرانية وسبل مواجهتها[128].

يبدأ أمن هذه المعلومات والبيانات أولا بحماية الأصول المادية من مباني والأشخاص العاملين فيها بتوفير الأمن التقليدي عن طريق رفع الأسوار، ووضع كاميرات مراقبة

---

[126] محمد مسيكة، الفضاء السيبراني وتحديات الأمن القومي للدول، مجلة العلوم القانونية والإجتماعية، المجلد 07، العدد 04، ديسمبر 2022 م، ص ص.447 – 462 .

[127] ماجد محمد الحنيطي، تكنولوجيا الصراعات الدولية المعاصرة، الآن ناشرون وموزعون، الطبعة 01، عمان، 2021 م، ص.125.

[128] بن علية بن جدو، المرجع السابق، ص ص . 299 – 319 .

وإستحداث نظام البصمة أو تقنية التعرف على الوجوه لمراقبة دخول وخروج الأشخاص ثم حماية البيانات.

الفرع الثاني :الردع السيبراني

ويعرف بأنه :" **منع الأعمال الضارة ضد الأصول الوطنية في الفضاء والأصول التي تدعم العمليات الفضائية** " ويرتكز الردع السيبراني على ثلاثة ركائز هي عماد إستراتيجية الدفاع السيبراني، تتمثل في :مصداقية الدفاع ، والقدرة على الانتقام، والرغبة في الانتقام[129].

أولا: مصداقية الدفاع: يتطلب الدفاع عن أنظمة المعلومات، توافر أنظمة نسخ احتياطية Backup Systems، مما يعني أن أي هجوم ناجح عليها، لن يسفر عن التدمير التام لها أو الفقدان الكلي لما تحويه من معلومات؛ ورغم تزايد تكلفة هذا الحل إلا إنه الحل العملي الأكثر فعالية.

ثانيا: القدرة على الانتقام: وإلحاق ضرر على المهاجم يفوق ما وقع على المدافع من أضرار، ولكن هذا يتطلب القدرة على الانتقام وتنفيذ هجمة سيبرانية أو أكثر ضد المهاجم الأصلي، بعد التعرف عليه وهو صعب التحقق نظرا لصعوبة إكتشاف مرتكبي الجرائم السيبرانية .

ثالثا: الرغبة في الانتقام: فعلى المدافع أو من تعرض للهجوم أن يعلن عن رغبته في الانتقام من المهاجم، ذلك أن امتلاك القدرة على الانتقام لا تكفي بمفردها لردعه [130].

---

[129] إيناس ممدوح محمد محمد سليمان، دور الأمن السيبراني في مواجهة الإرهاب الإلكتروني، المجلد 64، العدد 01، السنة 2022 م، ص ص . 175-227 .على الرابط:https://jelc.journals.ekb.eg/article_232151.html

[130] رغدة البهي، الردع السيبراني: المفهوم والإستراتيجيات، الدوريات:مفاهيم إستراتيجية، المركز العربي لأبحاث الفضاء الإلكتروني، 2017 م. على الرابط:https://accronline.com/article_detail.aspx?id=28706

الفرع الثالث : الوسائل الفنية للحماية

أولا: الأنظمة البديلة: يجب على الدول أن تقوم بإنشاء أنظمة بديلة ونسخ إحتياطية وأن لا تعتمد على نظام واحد، خاصة إذا تعلق هذا النظام بالبنى التحتية الرئيسية للدولة، يمكن الاستعانة بتلك الأنظمة البديلة أو الاحتياطية في حالة حدوث هجوم سيبراني.

ثانيا: إعادة التأسيس: فإذا أمكن للدولة التغلب على الهجوم الذي تعرضت له بسرعة، وإعادة تشغيل النظام، ستكون الآثار هامشية. ولكن الطريقة الوحيدة لتجنب الهجوم هي الاحتجاب عن الجميع، ورغم كونه السبيل الأفضل للردع، إلا أنه يكتنفه مسائل قانونية عدة[131].

ثالثا: التشفير: يمثل التشفير الوسيلة الأكثر أهمية لتحقيق وظائف الأمن الثلاثة:السرية، التكاملية وتوفير المعلومات، ويعرّف بـ :" **عملية دمج المعلومات في شيفرة سرية غير مفهومة ثم فك هذه الشيفرة بعد وصولها إلى وحدة الويب الآمنة، أي أن الشيفرة هو إستبدال مستند أو رسالة بإستخدام برنامج معين، ولهذا تنطوي عملية التشفير على تحويل النصوص البسيطة إلى رموز(حروف، أرقام، إشارات) قبل إرسالها إلى مستقبلها شريطة أن يكون لهذا الأخير القدرة على حل الشيفرة وتحويل الرسالة إلى صيغتها الأصلية بإستخدام مفتاح التشفير** " [132].

رابعا: الجدران النارية

تعرف جدران الحماية على أنها:" **عبارة عن برمجيات هدفها الأساسي تأمين الحماية الكافية لمعلومات الشركة والقضاء على عمليات الإختراق والتدمير التي تتعرض لها ملفات خوادم الويب، من خلال إقامة حاجز بين شبكة الأنترنت والشبكة الداخلية للمؤسسة ليقوم**

---

[131] رغدة البهي، نفس المرجع.

[132] مصطفى بوعقل، آليات وقاية المعاملات الإلكترونية في ظل حوكمة تكنولوجيا المعلومات، مجلة دفاتر MECAS ، المجلد 12، العدد 01، جامعة أبو بكر بلقايد، تلمسان، جوان 2016 م، ص ص .380-396. على الرابط: https://asjp.cerist.dz/en/article/8799

هذا الحاجز بتصفية وفحص كل عمليات الدخول والخروج إلى الشبكة لمنع دخول المستخدمين غير المصرح لهم وغير المسجلين ولتجنب خطر الفيروسات والبرامج الدخيلة[133]**.**

خامسا: برامج مكافحة الفيروسات

تقوم هذه البرامج المثبتة على أجهزة الحاسوب بإزالة الفيروسات من النظام أول بأول، عن طريق إكتشافها والقضاء عليها قبل حدوث الضرر، كما تقوم بعمل تحديثات لنفسها بصفة آلية وبشكل تلقائي عن طريق الأنترنت، لزيادة قدرتها و كفاءتها على مكافحة الفيروسات الجديدة، وتقوم برامج مكافحة الفيروسات بإستخدام تقنية البحث عن الفيروسات، من خلال تفحص السلوك، و مراقبة جميع الملفات الموجودة على الجهاز، برصد أي تغيير يحدث من خلال تقنية إختيار لتكامل ببناء سجل يتضمن أسماء جميع الملفات الموجودة على الحاسب، وحجمها، وتاريخها، ومتابعة أي تغيير أو نشاط غريب عليها[134]. ويمكن وصف عمل برامج مكافحة الفيروسات حسب النمط التالي:

أ/- إجراء مسح كلي لجهاز الحاسب عن طريق فحص الأقراص وإكتشاف البرامج الغريبة عن الجهاز.

ب/- إزالة الفيروسات التي تم العثور عليها عن طريق حذفها أو إبطال مفعولها، أو تقوم بحجبها في حالة عدم قدرتها على إزالتها أو إبطال مفعولها.

---

[133] سيمة دميش، التجارة الإلكترونية: حتميتها وواقعها في الجزائر، مذكرة ماجستير في العلوم الإقتصادية، كلية العلوم الإقتصادية وعلوم التسيير، جامعة منتوري، قسنطينة، السنة الجامعية 2010 م – 2011 م، ص ص .94.

[134] أشرف عبد المحسن الشريف، أمن وحماية المستندات الإلكترونية على بوابة الحكومات العربية، مجلة اعلم، الاتحاد العربي للمكتبات والمعلومات، العدد 16، يناير 2016 م، ص ص .87-114. على الرابط: http://www.arab-afli.org/media-library/Journal%20Issues/l3lem-16-2016_Achref_Abdel.pdf

ج/- تحليل البريد الإلكتروني عن طريق تحليل الرسائل الواردة، فمن الضروري ربط برنامج مكافحة الفيروسات مع البريد .

د/- مراقبة صفحات الويب عن طريق إرسال رسائل للمستخدم في حالة وجود فيروسات على الصفحة .

سادسا: أنظمة كشف التسلل(IDS)

وهي برامج مصصمة للكشف عن محاولات الوصول إلى نظام الحاسب الآلي غير مرغوب بها، أو محاولة تعطيل هذا النظام بشكل عام والتلاعب به، وتتألف من عدة مكونات، هي: جهاز إستشعار، ولوحة تحكم لمراقبة الأحداث والتنبيهات ومحرك يقوم بإدخال الأحداث إلى قاعدة البيانات، إلى جانب ذلك يمكن اللجوء إلى عمل فصل جزء إحتياطي بين الشبكات فلا تكون كلها كتلة واحدة، بحيث يتم تقسيم الشبكات إلى شبكات فرعية فلا تمتد أثر الهجمة على الشبكة الأخرى إذا حدث الهجوم على إحدى الشبكات [135] .

سابعا: حجب المواقع المشبوهة

تلجأ كثير من الدول إلى حجب المواقع، فالصين على سبيل المثال تنفق كل عام موارد ضخمة في بناء وصيانة أحد أكبر أنظمة الترشيح وأكثرها تطورا في العام، وتوظف المملكة العربية السعودية أيضا نظام بروكسي الويب لحجب الوصول للمواقع المحظورة[136]، ويعرف نظام حجب المواقع بـ :" **أسلوب لحجب صفحات معينة يمكن أن تكون مؤذية أو عدوانية**

[135] صلاح حيدر عبد الواحد، المرجع السابق، ص .61 .

[136] Nikolaos KOUMARTZIS, Andreas VEGLIS, Internet regulation: (The need for more transparent Internet filtering systems and improved measurement of public opinion on Internet filtering), First Monday (peer-reviewed journal on the internet), Volume 16, Number 10 - 3 October 2011: https://firstmonday.org/ojs/index.php/fm/article/view/3266

أو إباحية بالنسبة لمستخدم الأنترنت فإذا حاول المستخدم الوصول إلى صفحة محجوبة ظهرت له رسالة تبلغه أن الوصول إلى هذه الصفحة غير مسموح به " [137].

أثبتت الدراسات فشل هذا الأسلوب أمام فئة من المستخدمين الذين يملكون البراعة الفنية والتقنية، بحيث يستطعون الوصول إلى المعلومات المحجوبة عن طريق إستخدام برنامج VPN، أو الإستفادة من الأدوات والتطبيقات التي توفرها بعض المواقع الإلكترونية لتجاوز الحظر والحجب.

إن تحقيق الأمن السيبراني يستدعي التعاون بين جميع الفئات والأطراف، سواء دول أو منظمات أو أفراد، وكذلك التعاون بين القطاع العام والخاص وعلى الدول المتحكمة في تدفق الأنترنت، وعلى تجهيزاته تحمل مسؤولياتها كاملة في مواجهة الهجمات السيبرانية، وأن تلتزم بالشفافية في التعامل مع الجميع فهي بإستطاعتها القضاء على هذه الهجمات في المهد، كما أنها يمكنها حجب المواقع الجهادية أو الإباحية التي تستغل الأطفال أو التي تروج للمخذرات أو التي تدعوا إلى مختلف الجرائم المجرمة دوليا.

المطلب الثاني:

الذكاء الإصطناعي كآلية لمكافحة الإرهاب السيبراني

إنتقل العالم من عصر الثورة الصناعية إلى عصر المعلومات، فظهر الذكاء الإصطناعي وبرز في العديد من المجالات، وبات يشكل أداة فاعلة ووسيلة قوية تعتمد عليها الدول والمنظمات ومختلف الأفراد والتنظيمات، وتتمثل تكنولوجيا الذكاء الإصطناعي في محاكاة الذكاء الإنساني من خلال برمجة الحاسوب والآلة بحيث تصبح مشابهة ومقاربة لبعض خصائص وجوانب الذكاء الإنساني، فتتم برمجة الحاسوب من خلال تزويده بالمدخلات ليقوم

[137] فايزة نجاري بن حاج علي، المرجع السابق، ص .277.

بمعالجتها على نحو معين وفق ماتمت برمجته عليه ويخرج حلولا للمشكلات على نمط معين معروف لدى المبرمج غالبا[138].

الفرع الأول: تعريف الذكاء الإصطناعي

لا يوجد تعريف محدد للذكاء الإصطناعي وهذا راجع لحداثته وقد عرفه " **مارفن مينسكي** " في كتابه خطوات نحو الذكاء الإصطناعي بأنه:" **فرع من العلوم يهتم بالآلات التي تستطيع حل نوع من المشاكل التي يعجز الإنسان عن حلها بذكائه** "[139]، وعرفه البعض الآخر على أنه:" **فرع من فروع علوم الحاسوب وهو علم هندسة صناعة الآلات الذكية** "، وفي تعريف آخر كذلك :" **بناء آلات قادرة على القيام بالمهام التي تحتاج إلى الذكاء البشري عند أدائها مثل الإستنتاج المنطقي والقدرة على التعديل** " [140]، وتم تعريفه أيضا على أنه:" **وسيلة للتحكم في الحاسوب أو الروبوت بواسطة برنامج يفكر بنفس الطريقة التي يفكر بها البشر الأذكياء** " وتأسيسا على ما سبق يمكن تعريف الذكاء الإصطناعي على أنه: " **أحد علوم الحاسب الآلي الحديثة التي تبحث عن أساليب متطورة لبرمجته للقيام بأعمال و إستنتاجات تشابه الأساليب التي تنسب الذكاء للإنسان، من خلال فهم العمليات الذهنية الشائكة التي يقوم بها العقل البشري أثناء التفكير ثم ترجمتها إلى ما يوازيها من عمليات حسابية تزيد من قدرة الحاسب على حل العمليات الشائكة** " [141].

يعمل الذكاء الإصطناعي وفق خوارزميات أو مجموعة من الأوامر التي تمكن الآلات من تحليل البيانات، وأداء المهام، وإتخاذ القرارات بشكل مستقل، فالخوارزميات تمكن أجهزة

---

[138] محمد علي أبو علي، المسؤولية الجنائية عن أضرار الذكاء الإصطناعي، دار النهضة العربية للنشر والتوزيع، الطبعة 01، القاهرة، 2024 م، ص.13.

[139] Madaoui Nadjia, Lounici Ali,op.cit

[140] منال لقرع، إستخدامات الذكاء الإصطناعي للكشف عن الجرائم والبحث عن مرتكبيها، مجلة قراءات علمية في الأبحاث والدراسات العلمية، العدد 41، مارس 2025 م، ص.203.

[141] جمال بدري، الذكاء الإصطناعي : بحث عن مقاربة قانونية، المجلة الجزائرية للعلوم القانونية والسياسية، المجلد 59، العدد 04، السنة 2022 م، ص . 175 .

الكمبيوتر من التنبؤ بالأنماط، وتقييم الإتجاهات وحساب الدقة وتحسين العمليات[142]، فعلى سبيل المثال: قامت إمرأة تبلغ من العمر 27 عاما تدعى " **ماري غارنريتير**" من باريس بإدخال أعراضها في **ChatGPT**، والتي تضمنت التعرق ليلا، وحكة في الجلد، وإرهاق، فإقترح الذكاء الإصطناعي أنها قد تكون مصابة بمرض " هودجكين " وهو نوع من سرطان الدم، فلم تأخذ الأمر على محمل الجد، لكن بعد مرور عام تقريبا تفاقمت الأعراض، فكشفت الفحوصات بأنها بالفعل تعاني من المرض الذي توقعه الذكاء الإصطناعي.

الفرع الثاني: خصائص الذكاء الإصطناعي

يتمتع الذكاء الإصطناعي بالعديد من الخصائص والسمات وسنذكر فقط منها مايخدم موضوع بحثنا وهي:

أولا: الذكاء الإصطناعي له القدرة على حل المسائل وإن كانت لا تتوفر على جميع بياناتها اللازمة وقت الحاجة .

ثانيا: يستطيع الذكاء الإصطناعي التعامل مع البيانات المتضاربة والتي يشوبها الخطأ، والتوصل الى تصحيحها أو تجميعها أو حلها .

ثالثا: قابلية الذكاء الإصطناعي للتعلم والإستفادة من الخبرات السابقة، وتحسين الأداء، القدرة على الإستنتاج والإستدلال، التعلم والمعرفة الخارجية، القدرة على التعلم والمعرفة الداخلية (الذكاء الإصطناعي التوليدي)

رابعا: الإستدلال وذلك بإستغلال معطيات و بيانات سابقة والإسترشاد بها .

خامسا: الذكاء الإصطناعي أصبح ينوب عن الإنسان في القيام ببعض المهام، والعالم متجه في السنوات القادمة إلى الإعتماد عليه في جميع المجالات لتميزه بالسرعة والدقة وقلة التكلفة[143].

---

[142] طاهر أبو العيد، الذكاء الإصطناعي ومستقبل العدالة التحديات وآفاق المستقبل، إصدارات مبادرة تطوير تعليم القانون، 2024 م، ص.09.

[143] محمد علي أبو علي، المرجع السابق، ص.28.

سادسا: التنبؤ بالجرائم وذلك عن طريق تحليل البيانات الضخمة للأفراد والمواطنين بحيث تقوم برامج الذكاء الإصطناعي بتحليل الرسائل الصوتية والمرئية والتحويلات و المعاملات المالية المشبوهة .

سابعا: التتبع والرقابة عن طريق إستخدام شبكات كاميرات المراقبة المختلفة لرصد مئات الآلاف من الوجوه، وإستعمال برنامج الذكاء الإصطناعي للتعرف على تلك الوجوه، والكشف التلقائي عن الأشخاص الذين يظهرون سلوكات غير عادية مثل تكرار زيارة موقع معين أو البقاء في مكان واحد[144] .

ثامنا: إستخدام الذكاء الإصطناعي في إعادة بناء مسرح الجريمة وتسهيل القبض على المجرمين وتصنيفهم [145].

تاسعا: تحديد مواقع المجرمين بدقة وتتبع أثارهم وحتى إختراق أجهزتهم الإلكترونية والتنصت عليهم صوتا وصورة بإستعمال نظام تحديد الأماكن (GPS)، ونظام المعلومات الجغرافية (GIS).

الفرع الثالث:دور الذكاء الإصطناعي في منع الهجمات الإرهابية

يُمَكِنُ التنبؤ من معرفة موقع الهجمات وزمانها وبالتالي منعها قبل وقوعها، ويتم التنبؤ بإستخدام خوارزميات الذكاء الإصطناعي عن طريق تحليل البيانات الضخمة الناتجة عن مراقبة مواقع التواصل الإجتماعي، أو شبكات الإتصال الخلوية أو الفضائية، أو عن طريق تحليل الفيديوهات، التتبع والمراقبة بواسطة الكاميرات المزروعة في الطرق العامة أو على المؤسسات الحساسة عن طريق تقنية التعرف على الوجوه[146].

---

[144] Madaoui Nadjia, Lounici Ali,op.cit

[145] يوسف هنيدة، السياسة الجنائية في مواجهة الذكاء الإصطناعي، مذكرة ماستر، جامعة سيدي محمد بن علي، فاس، المغرب، السنة الجامعية 2022 م- 2023 م، ص. 113.

[146] تبنت الشرطة التنبؤية فكرة التطبيقات الذكية التنبؤية، ومن أهم تلك التطبيقات تطبيق (PredPol) الذي يستشعر أماكن الخطر ويتنبأ بمرتكبيها عن طريق تحليل البيانات التي يحوزها والتي يجمعها بإستمرار، ويقوم بإرسال تنبؤاته إلى دوريات الشرطة مع خرائط توقعات حدوثها، زد على ذلك هناك أجهزة إستشعار تعمل بالذكاء الإصطناعي تقوم بتجميع البيانات

كما يمكن تحديد ومعرفة هوية الإرهابيين ومراقبتهم من أجل كشف كل التنظيم والخلايا النائمة، أو مصادر التمويل خصوصا عن طريق العملات المشفرة بإستخدام تقنية **(بلوك تشين)** التي تعتبر ثورة جديدة في عملية توثيق المعاملات المالية .

الفرع الرابع: الآثار القانونية للذكاء الإصطناعي على حقوق الإنسان

إن الإعتماد على الذكاء الإصطناعي في مواجهة مختلف الجرائم بدءًا من التنبؤ بوقوعها وردعها قبل حدوثها أو تتبعها للكشف عن التنظيمات من وراءها، قد أثار جدلا بخصوص إستغلال تطبيقات الذكاء الإصطناعي للمحادثات والرسائل المتبادلة والمراقبة من خلال الكاميرات المنتشرة في كل مكان، بحيث أعتبرت هذه الأفعال إنتهاكا للحياة الخاصة ولأهم عصب فيها وهو حق الخصوصية.

تعتبر الخصوصية ركيزة أساسية لحقوق الإنسان والحريات العامة، وقد نصت عليها مختلف الإعلانات والإتفاقيات الدولية والوطنية، لاسيما الماد (12) من الإعلان العالمي لحقوق الإنسان لسنة 1948 م والمادة (17) من العهد الدولي للحقوق المدنية والسياسية لسنة 1966 م، ومع التقدم التكنولوجي أصبح من اليسير تداول المعلومات الخاصة بين الأفراد والجماعات .

أصبحت هذه الحقوق منتهكة خصوصا من طرف تطبيقات الذكاء الإصطناعي التي تحارب الجرائم، لهذا من الواجب تحقيق توازن بين القانون والتطور التكنولوجي لهذه التطبيقات مع مراعاة المصلحة العامة، وفي هذا الصدد حاولت الشركات العالمية العاملة في مجالات الذكاء الاصطناعي أخذ المبادرة بإقرار ميثاق شرف أخلاقي في تطويرها لمجالات الذكاء الاصطناعي، خاصة في أوربا من خلال ملحق la RGPD لخلق مجالات الثقة في مسارات الذكاء الاصطناعي وجعلها أداة لتعزيز الحريات الأساسية وليس المس بمضامينها من خلال إعداد معايير دولية متفق بشأنها أخلاقيا وتحيين القوانين ذات الصلة بالسياسات

وتحليل السلوك في وقت واحد، ومن أمثلتها جهاز (BrickStream 3D) .... وللإطلاع أكثر أنظر يوسف هنيدة، المرجع السابق.

العمومية والممارسات الفضلى في مجالات الذكاء الاصطناعي والمعرفة به بما يعود على الإنسانية بالخير، تقودها الأمم المتحدة في شخص مقرر خاص لحرية التعبير[147].

إعتمد المشرع الأوروبي بروتوكول تعديلي للوائح الأوروبية لحماية المعطيات الشخصية تحت رقم 2016/679 الصادر بتاريخ 2016/04/27 م، الذي يضمن للأشخاص مجموعة من الحقوق ويفرض غرامات ضخمة على الشركات المخلة بتطبيق هذا القانون، وأن تقوم هذه الشركات بالحماية الفنية والتقنية وضمان السرية عند معالجتها لهذه المعطيات ومحاولة التقليل من المخاطر عن طريق معالجة المعطيات المستهدفة دون سواها، كما أقر النظام الأوروبي إلزامية تعيين مندوب مكلف بحماية الحياة الخاصة وتقديم النصائح القانونية[148].

أصدرت اليونيسكو توصية خاصة بأخلاقيات الذكاء الإصطناعي سنة 2021 م إبان المؤتمر المنعقد بباريس مابين 09 و 24 نوفمبر، وأشارت إلى تعزيز التعاون والتضامن على الصعيد العالمي والإنتفاع العادل بوسائل تكنولوجيا الذكاء الإصطناعي مع إحترام القانون الدولي لحقوق الإنسان والحريات الأساسية[149].

يظهر كذلك أن الإعتماد على الذكاء الإصطناعي في مختلف المجالات قد يؤدي إلى إختفاء مئات الآلاف من الوظائف (الحق في العمل)، خصوصا أنه يتميز بالسرعة في الإنتاج مع قلة التكاليف والجهد. ولهذا يجب على الدول التفكير في إيجاد حل قانوني كأن تلزم الشركات بالإعتماد على نسبة معينة من الذكاء الإصطناعي في الشغل.

---

[147] عبد المجيد كوزي، حماية الحياة الخاصة في زمن المعلوماتي وتحديات الذكاء الإصطناعي، مجلة عدالة للدراسات القانونية والقضائية، العدد 24، السنة الخامسة 2022 م، ص.23.

[148] عبد المجيد كوزي، نفس المرجع، ص ص.25-26.

[149] عصام الدين محمد إبراهيم، الأثار القانونية للذكاء الإصطناعي على حقوق الإنسان في إطار القانون الدولي العام، المجلة المصرية للقانون الدولي، المجلد 80، العدد 02، ديسمبر 2024 م، ص ص .216-274.

خاتمة

خاتمة

أصبح الفضاء الإلكتروني مجالا لا يمكن الإستغناء عنه في المجتمع المعاصر، لأنه أمسى يوظف كثيرا وفي مختلف المجالات، سواء في التعليم أو الصحة أو التجارة و الإقتصاد الرقمي، أو في المجالات العسكرية، وهذا راجع للفعالية والكفاءة في التسير، كما أنه متاح لعدة فواعل سواء دول أو أفراد أو منظمات مما جعله ساحة جديدة للنزاعات والصراعات الخطيرة، فظهرت الحروب السيبرانية والإرهاب السيبراني الذي يعتبر نسخة محدثة عن الإرهاب الدولي التقليدي، فالتراكمات السياسية والإجتماعية والدينية والإعلامية والمعرفة التقنية، والذكاء الذي يمتاز به الإرهابي السيبراني، وصعوبة إكتشاف منفذ الهجمات السيبرانية ساعدت في تفشي وتفاقم هذه الظاهرة.

يعـرف الإرهـاب السيبـراني عـلى أنــه تـزاوج بين الإرهاب التقليدي و التكنولوجيا الحديثة للإتصالات والمعلومات وخـلافا لـهذا الأخير يستعمل الإرهاب السيبراني أساليب وأدوات تقنية وفنـية فـي شـن هجـماته عـلى الأهـداف، فهو يستهدف إما سرقة البيانات أو إتلافها وإتلاف الأجهـزة أو التجسـس وإعـتراض أو حجـب الخدمة، أو يستهدف نظم التحكم في الإتصالات ووسائل النقل أو تعطيل الخدمات ونشر الفزع والرعب.

تعددت الأساليب التي يستعملها في تنفيذ هجماته، إما بإستعمال برمجيات ضارة وخبيثة كالفيروسات والديدان وحصان طروادة، مموهة في رسائل أو روابط تبعث عن طريق البريد الإلكتروني للجهة المستهدفة، أو من خلال مواقع على شبكة الأنترنت، أو بإستعمال وسائل مادية كشرائح الأردوينو، أو القنابل الكهرومغناطيسية، أو إستغلال منظومة الطائرات دون طيار.

كثفت المنظمات و الوكالات الدولية و الحكومية جهودها للحد من هذه الظاهرة، و سعت الدول وفي إطارها إلى تبني سياسات واستراتيجيات لمكافحة الجرائم الإلكترونية، فتبنت سياسات تشريعية عن طريق عقد إتفاقيات دولية وإقليمية، وحث الدول على تبنيها في تشريعاتها الداخلية، ودعت إلى التعاون الدولي من أجل التحقيق، أو تسليم، أو محاكمة المجرمين، وأبرز هذه الإتفاقيات إتفاقية بودابست المتعلقة بالجريمة الإلكترونية لسنة 2001

م التي كانت الأولى من نوعها التي تطرقت إلى مختلف هذه الجرائم، وبالرغم من أنها أوروبية المنشأ إلا أنها مفتوحة للتوقيع لجميع الدول، فكانت مرجعا للجامعة العربية التي صدر عنها القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها لسنة 2004 م، والإتفاقية العربية لمكافحة جرائم تكنولوجيا المعلومات لسنة 2010 م، وإعتمد الإتحاد الإفريقي إتفاقية مالابو لسنة 2014 م لتحقيق الأمن في الفضاء السيبراني وحماية البيانات ذات الطابع الشخصي.

تبنت هذه الإتفاقيات سياسات تقنية وفنية وأمنية ودعت للتعاون في مجال الأمن السيبراني، لكن هذه السياسات و الإستراتيجيات تعد غير كافية وهذا راجع لعدم وجود تعريف موحد للإرهاب، وكذلك إزدواجية المعايير في التعامل مع هذه الظاهرة من طرف بعض الدول، وتأثير الوسائل التقنية المستعملة في مواجهة هذه الآفة كالذكاء الإصطناعي على بعض حقوق الإنسان (كإنتهاك حق الخصوصية المحمي بموجب الإتفاقيات والإعلانات الدولية)، وبما أن منظمة الأمم المتحدة هي التي تجمع في عضويتها أغلب الدول إعتمدت جمعيتها العامة في أواخر سنة 2024 م إتفاقية **منع ومكافحة الجرائم الإلكترونية**، وسيتم فتح الاتفاقية للتوقيع في حفل رسمي تستضيفه فييتنام في عام 2025 م .

توصيات

ومن خلال ماتقدم ذكره و لمواجهة الإرهاب السيبراني ومكافحته نرى أنه يجب:

- البحث عن معالجة أسباب الهجمات السيبرانية الداخلية، سواء كانت إرهابا أو مجموعة من المتسللين، ومحاولة إدماجهم في المجتمع والإستفادة من خبراتهم .
- تجفيف منابع التمويل بالعملات المشفرة للجماعات الإرهابية، وذلك بالتعاون الدولي بين مختلف الأجهزة الشرطية الدولية، والمؤسسات المالية لأن التمويل هو أساس الجريمة الإرهابية.
- ضرورة إهتمام الدول وخصوص النامية بالأمن السيبراني عن طريق الإهتمام بالعنصر البشري، و إدراجه ضمن المناهج التعليمية، و إقامة دورات تكوينية،

وتوعوية للعاملين بالمؤسسات الحساسة للدولة و الإهتمام بالتقنيات الجديدة، خصوصا الذكاء الإصطناعي التوليدي.

- مواكبة تطور وسائل تكنولوجيا الإعلام والإتصال تشريعيا عن طريق إصدار مراسيم أو أوامر أو قوانين لتنظيمها، لأن القانون أبطأ مقارنة بالتطور السريع لهذه الوسائل.
- إنشاء فرق مختصة مهمتها مراقبة وسائل التواصل الإجتماعي من أجل الكشف عن أفكار التطرف والمحرضين عليها، لأن الإرهاب يبدأ بالبحث عن تجنيد عناصر جديدة مستغلا الظروف المعيشية للفئات الهشة و نقص وعيهم الفكري .
- حجب المواقع غير المرغوب فيها عن طريق إنشاء مراكز مهمتها محاربة الفكر المتطرف على مواقع التواصل الإجتماعي وصد هجمات الإرهابيين والمتسللين.
- ضرورة التعاون الدولي في مجال ملاحقة المجرمين أوتسليمهم أو محاكمتهم، وذلك عن طريق إبرام إتفاقيات ثنائية أو متعددة الأطراف لكي يكون هناك تجريم مزدوج وإمكانية المتابعة.
- إنشاء أنظمة بديلة أو النسخ الإحتياطية بالبنى التحتية الرئيسية للدولة، يمكن الإستعانة بها في حالة حدوث هجوم سيبراني أوتم إختراق هذا النظام، وتكون هذه الأنظمة البديلة غير متصلة بالشبكة العالمية .
- إعادة التأسيس عن طريق إعادة تشغيل النظام، مع أخذ إحتياطات أمنية وحمائية جديدة لتجنب الهجوم من جديد .
- إنشاء بيانات مزيفة تكون هدفا للهجمات السيبرانية مع وضع فيها ديدان، وفيروسات تكشف مركز الهجمة لملاحقته أو لتخريب معداته .
- مراجعة الإتفاقيات الدولية المعنية بالجرائم المعلوماتية، وإعطاء تعريف موحد متفق عليه لها، خصوصا الإرهاب السيبراني، وبالتالي توحيد العقوبة .
- إنشاء لجنة دولية تحت لواء الأمم المتحدة مهمتها تسيير الأنترنت، تظم ممثلين عن كل الدول الأعضاء في الأمم المتحدة .
- إحترام حقوق الإنسان بما في ذلك حقوق المتهمين، لأن لمكافحة الإجرام ليس بالضرورة الدعس على هذه الحقوق وإنتهاكها، وإنما بإحترام هذه الحقوق تسود العدالة وتزول الأسباب التي أدت إلى الإجرام، كما يجب الأخذ بعين الإعتبار حق

الخصوصية والمعطيات الشخصية عند تصميم تطبيقات الذكاء الإصطناعي وتكييف الخوارزميات مع ذلك .

المراجع

المراجع

أولا: قائمة المصادر

01/- القرآن الكريم

- الآية 19 من سورة النمل.
- الآية 60 من سورة الأنفال.
- الآية 154 من سورة الأعراف.

ثانيا: الإتفاقيات والإعلانات الدولية والإقليمية والقوانين

1/- الإتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010 م .

2/- القانون العربي الإسترشادي لمكافحة جرائم الإرهاب الإلكتروني وما في حكمها.

3/- النظام الأساسي للمنظمة الدولية للشرطة الجنائية.

4/- إتفاقية بودابست المتعلقة بالجريمة الإلكترونية الصادرة عن مجلس أوروبا.

5/- إعلان دلهي بشأن مكافحة إستخدام التكنولوجيات الجديدة الجديدة والناشئة لأغراض إرهابية .

أولا : قائمة الكتب باللغة العربية

01/- أحمد عبد الخالق، حماية حقوق الملكية الفكرية في ظل إتفاقية التربس والتشريعات الإقتصادية، دار الفكر و القانون، الطبعة 01، مصر، سنة 2011 م .

02/- ابن منظور ، لسان العرب ،الجزء الخامس ، دار إحياء التراث العربي ،الطبعة 03 ، بيروت ، 1999 م .

03/- جاسم محمد، الإرهاب الإلكتروني، دار البداية ناشرون و موزعون، الطبعة 01، عمان، 2014 م .

04/- ماجد محمد الحنيطي، تكنولوجيا الصراعات الدولية المعاصرة، الآن ناشرون وموزعون، الطبعة 01، عمان، 2021 م .

05/- محمد كمال، الإرهاب السيبراني عندما يستخدم الإرهابي الكيبورد بدلا من القنبلة، دار الكليم للطباعة والنشر والتوزيع، ط 1، القاهرة ، مصر، 2022 م .

06/- محمد علي أبو علي، المسؤولية الجنائية عن أضرار الذكاء الإصطناعي، دار النهضة العربية للنشر والتوزيع، الطبعة 01، القاهرة، 2024 م.

07/- نضال محسن الشرافي، الفضاء الإلكتروني والدبلوماسية ساحة الصراع الجديدة في القضية الفلسطينية، المركز الديمقراطي العربي للدراسات الاستراتيجية، الإقتصادية والسياسية، الطبعة الأولى ، برلين، ألمانيا، أبريل 2021 م .

08/- سمية بومروان، الحكومة الإلكترونية ودورها في تحسين أداء الإدارات الحكومية (دراسة مقارنة)، الطبعة 01، مكتبة القانون والإقتصاد، الرياض، المملكة العربية السعودية، 2014 م .

09/- عباس بدران ،الحروب الالكترونية ،الاشتباك في عالم متغير، مركز دراسات الحكومة الالكترونية ، دون طبعة، بيروت ، 2010 م .

10/- عثمان علي حسن، الارهاب الدولي ومضاهره القانونية والسياسية في ضوء أحكام القانون الدولي العام، مطبعة منارة –هه وليز، ط 1، كوردستان، 2006 .

11/- فضيل دليو، تكنولوجيا الإعلام والإتصال الجديدة بعض تطبيقاتها التقنية، دار هومة للطباعة والنشر والتوزيع ، ط 1 ، الجزائر ، 2014 .

12/- ريتشارد كلارك و روبرت نيك، حرب الفضاء الإلكتروني التهديد التالي للأمن القومي وكيفية التعامل معه، مركز الإمارات للدراسات والبحوث الإستراتيجية، الطبعة 01، أبو ظبي، الإمارات العربية المتحدة، 2012 م .

13/- خالد محمد خالد خليفوه، أثر الإحتساب في مكافحة الإرهاب، دراسة تأصيلية تحليلية على دولة الكويت، مجلة الوعي الإسلامي، ط 1، الإصدار62، الكويت، 2013 م .

14/- خالد ممدوح إبراهيم، **حجية البريد الإلكتروني في الإثبات دراسة مقارنة**، دار الفكر العربي، دون طبعة، القاهرة ،2008م .

15/- غادة نصار، الإرهاب والجريمة الإلكترونية، العربي للنشر والتوزيع، الطبعة 01، القاهرة ، 2017 م .

ثانيا : الرسائل الجامعية

أ/- مذكرات ودبلوم الدراسات

01/- أكرم رياض، السياسات الدولية لمكافحة الإرهاب الإلكتروني السيبراني، مذكرة الماستر في العلوم السياسية ، كلية الحقوق والعلوم السياسية ، جامعة العربي بن مهيدي، أم البواقي، 2021 م/2022 م .

02/- أمل تباني ، سعدة مريمد ، واقع ومستقبل التجارة الإلكترونية في الجزائر، مذكرة ماستر تخصص مالية وتجارة دولية، جامعة 08 ماي 1945 م، كلية العلوم التجارية والإقتصادية وعلوم التسيير، قسم العلوم التجارية، قالمة، 2019 م/2020 م .

03/- أنديرا عراجي ، القوة في الفضاء السيبراني : فصل عصري من التحدي والاستجابة ،رسالة لنيل دبلوم دراسات عليا في العلوم السياسية والإدارية ، كلية الحقوق و العلوم السياسية والإدارية ، الجامعة اللبنانية ، 2015 م-2016 م.

04/- وليد غسان سعيد جلعود، دور الحرب الإلكترونية في الصراع العربي الإسرائيلي، أطروحة ماجستير في التخطيط والتنمية السياسية، كلية الدراسات العليا، جامعة النجاح ، نابلس، 2013 م .

05/- وفاء دريدي، المحكمة الجنائية الدولية ودورها في تنفيذ قواعد القانون الدولي الإنساني، مذكرة ماجستير، جامعة الحاج لخضر، كلية الحقوق، باتنة، السنة الدراسية 2008 م – 2009 م.

06/- حسن المبروك سعد، جريمة الإرهاب الإلكتروني دراسة مقارنة، رسالة ماجستير في القانون الجنائي، الأكاديمية الليبية، فرع بنغازي، ليبيا، 2022 م/2023 م .

07/- يوسف هنيدة، السياسة الجنائية في مواجهة الذكاء الإصطناعي، مذكرة ماستر، جامعة سيدي محمد بن علي، فاس، المغرب، السنة الجامعية 2022 م- 2023 م.

08/- محمد مهني، تأثير الإرهاب الإلكتروني على تغيير مفهوم القوة في العلاقات الدولية توظيف المنظمات الإرهابية لمواقع التواصل الإجتماعي نموذجا، مذكرة ماستر في العلوم

السياسية والعلاقات الدولية ، جامعة محمد بوضياف، كلية الحقوق والعلوم السياسية، المسيلة، 2017 م/2018 م .

09/- نسـيم دردور ، جـرائم المعـلوماتية عـلى ضـوء القانون الجزائري والمقارن، مذكرة الماجستير، جامعة منتوري، كلية الحقوق، قسنطينة، 2012 م/2013 م .

10/- ساهـره مالك كاظـم مغير ، الألياف الضوئية البصرية ، جزء من متطلبات نيل درجة البكالوريوس في علم الفيزياء ، جامعة بابل ، جمهورية العراق ، 2022 م .

11/- سيمة دميش، التجارة الإلكترونية: حتميتها وواقعها في الجزائر، مذكرة ماجستير في العلوم الإقتصادية، كلية العلوم الإقتصادية وعلوم التسيير، جامعة منتوري، قسنطينة، السنة الجامعية 2010 م – 2011 م.

12/- عبد الله دغش العجمي، المشكلات العلمية والقانونية للجرائم الإلكترونية (دراسة مقارنة)، مذكرة ماجستير في القانون العام، جامعة الشرق الأوسط، 2014 م .

13/- علي حيدر، المنظمة الدولية للشرطة الجنائية ودورها في مكافحة الإرهاب السيبراني، رسالة ماجستير في القانون العام، كلية القانون، جامعة كربلاء، 2023 م.

14/- صـلاح حـيدر عـبد الواحـد ، حـروب الفـضاء الإلكتـروني ، دراسـة فـي مفـهومها وخصائصها وسـبل مواجهـتها ، رسالة ماجستير في العلوم السياسية ، قسم العلوم السياسية ، كلية الآداب ،جامعة الشرق الأوسط ، الأردن ، تموز ، 2021 م .

15/- عبد الحكيم توات ، جريمة الإرهاب الإلكتروني، مذكرة ماستر جريمة وأمن عمومي، جامعة العربي التبسي، كلية الحقوق والعلوم السياسية، التبسة، 2021 م/2022 م .

16/- رضـا هـداج ، المقـاومة والإرهاب في القانون الدولي، مذكرة لنيل شهادة الماجيستير فـي القانـون الدولـي والعلاقـات الدولـية، جامعة الجزائر 1، كلية الحقوق، بن عكنون ،السنة الجامعية 2009 م/2010 م .

ب/-أطروحات

17/- علي لونيسي ،آليات مكافحة الإرهاب الدولي بين فاعلية القانون الدولي وواقع الممارسات الدولية الإنفرادية ،رسالة لنيل شهادة الدكتوراه في القانون، جامعة مولود معمري ، تيزي وزو، الجزائر،2012 م .

18/- فايزة نجاري بن حاج علي ، مكافحة الإرهاب الإلكتروني في القانون الدولي ،رسالة لنيل شهادة دكتوراه،جامعة مولود معمري ، تيزي وزو، الجزائر.

ثالثا: البحوث والمقالات و المطبوعات

01/- أبو بكر محمد الديب ، ياسمين أحمد إسماعيل صالح ، أثر الفضاء الإلكتروني على مستقبل العلاقات الدولية " دول الشرق الأوسط نموذجا " ،المجلة المصرية للقانون الدولي ،المجلد 77 ، سنة 2021 ، ص .369. على الرابط : https://ejil.journals.ekb.eg/article_295020.html بتاريخ 2025/01/05 .12:20

02/- أشرف عبد المحسن الشريف، أمن وحماية المستندات الإلكترونية على بوابة الحكومات العربية، مجلة اعلم، الاتحاد العربي للمكتبات والمعلومات، العدد 16، يناير 2016 م، ص ص .87-114. على الرابط:http://www.arab-afli.org/media-library/Journal%20Issues/I3lem-16-2016_Achref_Abdel.pdf

03/- إيهاب خليفة، الهجمات الصفرية(كيف يمكن الإستعداد لليوم الأسود في الأنترنت؟)، 17 مايو 2017 م، تم الإطلاع عليه بتاريخ 2025/03/29 م، على الساعة 14:40 على الرابط:https://2u.pw/ezMKW

04/- إيناس ممدوح محمد محمد سليمان، دور الأمن السيبراني في مواجهة الإرهاب الإلكتروني، المجلد 64، العدد 01، السنة 2022 م، ص ص . 175-227 . على الرابط: https://jelc.journals.ekb.eg/article_232151.html

05/- إنجي محمد مهدي، الجهاد الإلكتروني: دراسة لتنظيم داعش، وإستراتيجية الولايات المتحدة لمواجهته، مجلة دراسات، المجلد 22، العدد 02، أفريل 2021 م.

06/- إسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، **مجلة العلوم السياسية**، المجلد 10،العدد 01، جامعة الشهيد حمة لخضر، الوادي، الجزائر، أفريل 2019، ص ص.1016-1031. https://www.asjp.cerist.dz/en/article/91423

07/- بن علية بن جدو، تحديات الأمن السيبراني لمواجهة الجريمة الإلكترونية، المجلة الجزائرية للأمن الإنساني، المجلد 07، العدد 02، جويلية 2022 م .

08/- جمال بدري، الذكاء الإصطناعي : بحث عن مقاربة قانونية، المجلة الجزائرية للعلوم القانونية والسياسية، المجلد 59، العدد 04، السنة 2022 م، ص ص. 173- 190 .

09/- وداد سميشي ،الحوار الالكتروني والفضاء العام الافتراضي ،منتديات النقاش الالكترونية نموذجا،**مجلة العلوم الانسانية**، مجلد ب، عدد 41 ،جامعة قسنطينة، الجزائر، جوان 2014 ،ص .570.

10/- وهيبة بشريف، أساليب الجريمة الإلكترونية: مسار الإنتقال من الإرهاب التقليدي إلى الإرهاب الإلكتروني في ظل المجتمع المعلوماتي، الحوار الثقافي، الطبعة 08، العدد 01، 2019م، ص.65. على الرابط:https://asjp.cerist.dz/en/article/76418

11/- حيدر علي، الإرهاب السيبراني، جامعة كربلاء، نوفمبر 2023،ص .03 .على الرابط:https://www.researchgate.net/publication/375895130 .

12/- حنان ولهي ، تكنولوجيا اللوحات الرقمية والادمان الإلكتروني لدى الأطفال المرافقة حل وسط بين الإتاحة والرقابة ، مجلة الدراسات ، المجلد 12 ، العدد 01 ، ماي 2023 ، ص. 341 . على الرابط : https://asjp.cerist.dz/en/article/222569 بتاريخ 2025/03/22 م .

13/- حسين بركاتي، الحكومة الإلكترونية الإطار المفاهيمي ومنطلقات نظرية بالتركيز على بعض المؤشرات والتجارب الدولية، مجلة الدراسات الإقتصادية المعاصرة، المجلد 06، العدد 02، 2021 م، ص .452 . على الرابط: https://asjp.cerist.dz/en/article/174085

14/- طاهر أبو العيد، الذكاء الإصطناعي ومستقبل العدالة التحديات وآفاق المستقبل، إصدارات مبادرة تطوير تعليم القانون، 2024 م.

15/- يحي ياسين سعود ، الحرب السيبرانية في ضوء قواعد القانون الدولي الانساني ، المجلة القانونية، ص.83.

16/- كنزة تنيو و محمد دهان، دور الإقتصاد الرقمي في تحقيق جودة الحياة: دراسة مقارنة بين الجزائر والإمارات، مجلة الإستراتيجية والتنمية، العدد 03 مكرر(الجزء الأول)، المجلد 09، 2019 م، ص ص .364-385.على الرابط: https://asjp.cerist.dz/en/article/98416

17/- ليلى عصماني، نظام التقاضي الإلكتروني آلية لإنجاح الخطط التنموية، **مجلة الفكر**، العدد 13، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر، فيفري 2016م،ص .217 .على الرابط:https://www.asjp.cerist.dz/en/article/62437

18/- لمياء محمد عبد السلام جودة، دور المنظمة الدولية للشرطة الجنائية في مكافحة الإرهاب الدولي، مجلة البحوث الفقهية والقانونية، العدد 42، يوليو 2023 م.

19/- منال وراقي، ماذا نعرف عن القنبلة الكهرومغناطيسية التي هددت إسرائيل أنها قد تعيد إيران إلى العصر الحجري؟،14 أفريل 2024 م، تم الإطلاع عليه بتاريخ 2025/03/29 م، على الساعة 16:10 على الرابط: https://www.shorouknews.com/news/view.aspx?cdate=14042024&id=ee610ec3-932e-43ff-90ef-4bdebfa2b038

20/- محمد زهير عبد الكريم، الإرهاب السيبراني : أزمة عالمية جديدة، قضايا سياسية، كلية العلوم السياسية، جامعة الموصل، العدد 64، السنة 2021 م، ص ص . 277/294 . على الرابط:https://2u.pw/ZTtbM

21/- محمد مسيكة، الفضاء السيبراني وتحديات الأمن القومي للدول، مجلة العلوم القانونية والإجتماعية، المجلد 07، العدد 04، ديسمبر 2022 م، ص ص.447 – 462 .

22/- محمد سويلمي، في الارهاب والارهاب الالكتروني :التباسات المفهوم وتقاطع المقاربات،مجلة قضايا التطرف والجماعات المسلحة،المركز الديمقراطي العربي،العدد 01، ماي 2019 م .

23/- منال لقرع، إستخدامات الذكاء الإصطناعي للكشف عن الجرائم والبحث عن مرتكبيها، مجلة قراءات علمية في الأبحاث والدراسات العلمية، العدد 41، مارس 2025 م.

24/- مصطفى بوعقل، آليات وقاية المعاملات الإلكترونية في ظل حوكمة تكنولوجيا المعلومات، مجلة دفاتر MECAS ، المجلد 12، العدد 01، جامعة أبو بكر بلقايد، تلمسان، جوان 2016 م، ص ص .380-396. على الرابط: https://asjp.cerist.dz/en/article/8799

25/- مصطفى خليل كامل خليل، جرائم الإرهاب الإلكتروني من منظور القانون الدولي العام، مجلة كلية الحقوق، جامعة المنيا،المجلد 05، العدد 02، ديسمبر 2022 م .

26/- مريم لوكال، قراءة في إتفاقية الإتحاد الإفريقي حول الأمن السيبراني وحماية المعطيات ذات الطابع الشخصي لسنة 2014، مجلة الدراسات القانونية والإقتصادية، المجلد 04، العدد 03، السنة 2021 م، ص ص .657 - 673 .على الرابط: https://asjp.cerist.dz/en/article/175553

27/- نجيب بن عمر عوينات، الإرهاب الإلكتروني : المفهوم والجهود الدولية والإقليمية لمكافحته، **مجلة الأستاذ الباحث**، المجلد 02، العدد 02، جوان 2017، على الرابط: https://asjp.cerist.dz/en/article/76780

28/- نزيهة عمران، الديمقراطية الرقمية:نحو تعزيز المشاركة من خلال تكنولوجيا المعلومات، مجلة العلوم القانونية والسياسية، المجلد 13، العدد 02، سبتمبر 2022، ص 342. . على الرابط: https://asjp.cerist.dz/en/article/203101

29/- سكينة قيش، سلوى السماتي، الآليات الوطنية والدولية لمكافحة الحروب السيبرانية، مجلة قراءات علمية في الأبحاث والدراسات العلمية، العدد 41، مارس 2025 م.

30/- العجلان، عبد الله بن عبد العزيز بن فهد، الإرهاب المعلوماتي، دار المنظومة،2015 م ، ص ص .50-65 . على الرابط: https://search.mandumah.com/Record/690587

31/- عبد المجيد كوزي، حماية الحياة الخاصة في زمن المعلوماتي وتحديات الذكاء الإصطناعي، مجلة عدالة للدراسات القانونية والقضائية، العدد 24، السنة الخامسة 2022 م.

32/- عبد الرحمن علي إبراهيم غنيم، مدى فاعلية أنتربول في مكافحة الإرهاب، مجلة الباحث في العلوم القانونية والسياسية، العدد 02، ديسمبر 2019 م، على الرابط: https://asjp.cerist.dz/en/article/220173

33/- عنترة بن مرزوق، محمد الكر، البعد الإلكتروني للسياسة الأمنية الجزائرية في مكافحة الإرهاب، مجلة العلوم الإنسانية والإجتماعية، المجلد 19، العدد 38، جامعة الحاج لخضر، باتنة، الجزائر، جوان 2018 م، ص ص . 29 - 50 . على الرابط: https://2u.pw/P3zgL

34/- عصام الدين محمد إبراهيم، الأثار القانونية للذكاء الإصطناعي على حقوق الإنسان في إطار القانون الدولي العام، المجلة المصرية للقانون الدولي، المجلد 80، العدد 02، ديسمبر 2024 م، ص ص .216-274.

35/- فاطمة بلحنافي ، التعاون الدولي في مكافحة الإرهاب الدولي ، مطبوعة بيداغوجية موجهة لطلبة السنة الثانية ماستر قانون دولي عام، كلية الحقوق والعلوم السياسية، الجزائر ، السنة الجامعية 2022 م/2023 م .

36/- فاطمة الزهراء حشاني ، توفيق حكيمي ، الدبلوماسية السيبرانية وجيوسياسية الفضاء السيبراني : بين مساعي الحوكمة وحسابات التنافس ، مجلة الباحث للدراسات الأكاديمية ، المجلد 11 ، العدد 2 ، جوان 2024 .على الرابط: http://dspace.univ-batna.dz/xmlui/handle/123456789/8157 بتاريخ :2025/01/05 10:20.

37/- فاتن سعيد بامفلح، حماية أمن المعلومات في شبكة المكتبات بجامعة أم القرى :(دراسة حالة)، **الإتجاهات الحديثة في المكتبات والمعلومات**،العدد 18، المكتبة الأكاديمية، القاهرة، مصر، 2002، ص ص .249-282. على الرابط: https://www.kau.edu.sa/Show_Res.aspx?Site_ID=0012433&Lng=AR&RN=56927

38/- صليحة محمدي و شفيعة حداد، الإرهاب الإلكتروني والأمن القومي للدول: (نمط جديد وتهديدات مختلفة)، **المجلة الجزائرية للأمن والتنمية**، المحلد 08، العدد 02، جامعة الحاج لخضر، باتنة، الجزائر، جوان 2019 م، ص ص.65-77.، على الرابط: https://asjp.cerist.dz/en/article/96164

39/- ربيع رافعي،الإرهاب الدولي وعلاقته بالجريمة المنظمة(الإرهاب الإلكتروني نموذجا)، **مجلة القانون والعلوم السياسية**، المجلد 07، العدد 01، المركز الجامعي صالحي أحمد، النعامة، الجزائر،2021 م، ص ص .70-78. على الرابط: https://asjp.cerist.dz/en/article/161289

40/- رغدة البهي، الردع السيبراني: المفهوم والإستراتيجيات، الدوريات:مفاهيم إستراتيجية، المركز العربي لأبحاث الفضاء الإلكتروني، 2017 م. على الرابط: https://accronline.com/article_detail.aspx?id=28706

41/- خالد جمعة سبيت أحمد المخمري، المواجهة الأمنية للإرهاب الإلكتروني، مجلة البحوث القانونية والإقتصادية، المجلد 58، العدد 02، أكتوبر 2023 م، ص ص .379-413. على الرابط:https://jslem.journals.ekb.eg/article_302713.html

رابعا: المواقع الإلكترونية

01/- إبن منظور ، لسان العرب، دار صادر، بيروت ،الطبعة الثالثة ،1414 ه ،على الرابط :https://shamela.ws/book/1687/7769#p1 بتاريخ 2025/03/14 ، 12:49.

02/- حسام الحداد ،الارهاب المفهوم والاسباب أبرز الجهود والاسهامات لمحاربته ،كراسات تنوير 22 ، ص . 05 . على الرابط :https://2u.pw/ZsKpJ

03/- يوسف الحسن، ثقافة المقاومة، 14 فبراير 2017م، تم الإطلاع عليه بتاريخ 2025/03/27م على الساعة 15:00 على الرابط:https://2u.pw/ijv0A

04/- للإطلاع أكثر أنظر كابل إتصالات بحري على موقع ويكيبيديا الموسوعة الحرة من خلال الرابط:https://2u.pw/bNaqQ

05/- أنظر نماذج تشريعات الفضاء السيبراني في الدول الأعضاء بالإسكوا ، الإسكوا الأمم المتحدة اللجنة الإقتصادية والإجتماعية لغرب أسيا على الرابط : https://archive.org/details/20201113_20201113/mode/2up?view=theater بتاريخ 2025/03/14 10:17 .

06/- أنظر تعريف الفضاء السيبراني على الرابط:https://2u.pw/Yaa6t بتاريخ 2025/03/15: ،على الساعة: 13:08

07/- للإطلاع أكثر أنظر: تفجيرات البيجر.. ما الذي جرى في لبنان؟ على موقع الجزيرة من خلال الرابط:https://2u.pw/BmlOn

08/- أنظر البند 06 من محضر موجز للجلسة الثالثة لجنة السادسة للجمعية العامة المتضمنة التدابير الرامية إلى مكافحة الإرهاب الدولي، الدورة 69 ، المؤرخ بتاريخ 27 أكتوبر 2014: https://daccess-ods.un.org/TMP/2758755.08785248.html

09/- أنظر فيروس حصان طروادة على الرابط: https://me.kaspersky.com/resource-center/threats/trojans

10/- أنظر: ماهي الديدان Worms وكيف تعمل وسبل الوقاية منها؟ على الرابط: https://www.momar.tech/2021/10/What-are-worms-how-do-they-work-and-how-to-prevent-them.html

11/-أنظر الموقع الإلكتروني الرسمي للمنظمة الدولية للشرطة الجنائية على الرابط:
https://www.interpol.int/ar/3/4/1
12/- أنظر الجمعية العامة تعتمد إتفاقية تاريخية بشأن الجرائم الإلكترونية على الرابط:
https://news.un.org/ar/story/2024/12/1137776
13/- أنظر قائمة الإتفاقيات المتعددة الأطراف المصادق عليها من طرف الجزائر على موقع وزارة العدل على الرابط:https://2u.pw/X2qLV بتاريخ : 2025/05/30 م على الساعة 09:25 .

خامسا: مراجع أجنبية

01/- Madaoui Nadjia, Lounici Ali, the role of artificial intelligence in combating cyber terrorisme,IUS ETSCIENTIA,Vol.9.N°2.ISSN 2444-8478,2023,P.213.
https://www.researchgate.net/publication/377340615_The_role_of_artificial_intelligence_in_combating_cyber_terrorism#full-text .12:30 2025/01/01
02/-Dr.Yasmine Abdel Moneim ,les répercussions du cybertérrorisme sur la paix et la sécurité internationales,prevue égyptienne de droit international,Vol 75,2019 .
03/- Espace , dictionnaire le Robert sur :
https://dictionnaire.lerobert.com/definition/espace
04/- Nikolaos KOUMARTZIS, Andreas VEGLIS, Internet regulation: (The need for more transparent Internet filtering systems and improved measurement of public opinion on Internet filtering), First Monday (peer-reviewed journal on the internet), Volume 16, Number 10 - 3 October 2011:
https://firstmonday.org/ojs/index.php/fm/article/view/3266

05/- space , oxford dictionnaire sur:
https://www.oxfordlearnersdictionaries.com/definition/english/space_1
06/- cyber monde, dictionnaire Larousse sur :
https://www.larousse.fr/dictionnaires/francais/cybermonde/21258

فهرس

ملخص

إن إعتماد الدول على إستخدام الشبكة المعلوماتية وأجهزة الحواسيب في تسيير مختلف مؤسساتها الإنتاجية و الخدماتية والعسكرية جعلها هدفا للهجمات السيبرانية سواء من قبل دول أو من قبل أفراد أو منظمات ، فبقدر ما تساهم تكنولوجيا الإعلام والإتصال في فعالية الأداء وسرعته و تحقيق الكفاءة التقنية و زيادة الإنتاج في جميع الميادين إلا أنها سيف ذو حدين ، بحيث خلقت فضاءا جديدا أضحى مصدر تهديد للأمن القومي للدول .

تهدف هذه الدراسة إلى الإحاطة بمفهوم الإرهاب في البيئة السيبرانية و إلى تبيان الجهود الدولية و الإقليمية لمكافحته كما يجب الاستفادة من التطور التكنولوجي في التصدي لهذه الظاهرة خصوصا بإستعمال تقنية الذكاء الإصطناعي من أجل التنبؤ والرقابة والتتبع ، وتحصين الدول لفضائها السيبراني عن طريق تحقيق الأمن السيبراني وكذا تبيان المعوقات التي تحول دون ذلك .

الكلمات المفتاحية: الإرهاب السيبراني، الفضاء السيبراني، الأمن السيبراني، الذكاء الإصطناعي

Abstract

Countries' reliance on the use of the information network and computers in managing various Its production, service and military institutions have become targets for cyber attacks, whether by countries or by individuals or organizations, as much as information and communication technology contributes to the effectiveness of Performance, speed, technical efficiency and increased production in all fields, but it is a sword double-edged, so that it created a new space , and has become a source of threat to the national security of countries,

This study aims to understand the concept of terrorism in the cyber environment and to demonstrate the efforts International and regional efforts to combat it must also benefit from technological development in confronting it.

This phenomenon, in particular, is being addressed by using artificial intelligence technology for prediction and monitoring, and the follow-up, and the countries' fortification of their cyberspace by achieving cyber security and so on, Identify the obstacles that prevent this.

Keywords :Cyber terrorism, cyberspace, cybersecurity, intelligence artificial