الإرهاب السيبراني.
Cyber Terrorism.

بحث مشترك مقدم من قبل
الاستاذ الدكتور نوري رشيد نوري
الباحث حيدر علي حسن
جامعة كربلاء / كلية القانون

الخلاصة.
يشير الإرهاب السيبراني إلى استخدام التقنيات الرقمية ، مثل أجهزة الكمبيوتر والشبكات والإنترنت ، لتنفيذ أعمال إرهابية، اذ إنه ينطوي على الاستغلال المتعمد للثغرات في أنظمة الكمبيوتر أو الشبكات لإحداث ضرر أو خلق الخوف أو تعطيل البنية التحتية الحيوية. يستخدم الإرهابيون السيبرانيون تكتيكات مختلفة ، بما في ذلك القرصنة ، ونشر البرامج الضارة ، وشن هجمات حجب الخدمة الموزعة (DDoS) ، والقيام بحرب المعلومات؛ وتتضمن أهدافهم عادةً التسبب في أضرار جسيمة لأنظمة الكمبيوتر ، أو تعطيل الخدمات الأساسية ، أو سرقة المعلومات الحساسة ، أو بث الخوف والذعر في نفوس السكان.
يمكن أن تختلف أهداف الإرهاب السيبراني على نطاق واسع وقد تشمل الوكالات الحكومية والمنشآت العسكرية والمؤسسات المالية وأنظمة النقل والمرافق ومؤسسات الرعاية الصحية وقطاعات البنية التحتية الحيوية الأخرى، ويمكن أن يتراوح الدافع وراء الإرهاب السيبراني من الأجندات السياسية أو الأيديولوجية إلى المكاسب المالية أو مجرد التسبب في الفوضى. ويمكن أن تكون عواقب الإرهاب السيبراني بعيدة المدى وخطيرة، كما يمكن أن تؤدي إلى خسائر اقتصادية كبيرة ، وتعريض الأمن القومي للخطر ، وتعطيل الخدمات الأساسية ، وتعريض الأرواح للخطر، تستثمر الحكومات والمنظمات والأفراد على حد سواء موارد كبيرة في تطوير تدابير الأمن السيبراني للحماية من الإرهاب السيبراني والتخفيف من تأثيره المحتمل.
الكلمات المفتاحية : الإرهاب السيبراني ، الجريمة السيبرانية ، الحرب السيبرانية ، الفضاء السيبراني.

Abstract.
Cyber terrorism refers to the use of digital technologies, such as computers, networks, and the Internet, to carry out terrorist acts. It involves the deliberate exploitation of vulnerabilities in computer systems or networks to cause harm, create fear, or disrupt critical infrastructure.
Cyber terrorists use various tactics, including hacking, spreading malware, conducting distributed denial-of-service (DDoS) attacks, and conducting information warfare; Their goals typically include causing massive damage to computer systems, disrupting essential services, stealing sensitive information, or spreading fear and panic among the population.
The targets of cyber terrorism can vary widely and may include government agencies, military installations, financial institutions, transportation systems, utilities, healthcare organizations, and other critical infrastructure sectors. The motivation behind cyber terrorism can range from political or ideological agendas to financial gain or simply causing chaos.
The consequences of cyber terrorism can be far-reaching and serious. It can lead to significant economic losses, endanger national security, disrupt essential services, and endanger lives. Governments, organizations, and individuals alike invest significant resources in developing cyber security measures to protect against cyber terrorism . and mitigate its potential impact.
Keywords: Cyber terrorisme, cyber crime, cyber war , cyberspace.

المقدمة .

اولًا / اهمية البحث .

يعيش العالم اليوم في عصر الانترنت والتكنولوجيا الرقمية، اذ أصبحت الشبكة العنكبوتية جزءًا لا يتجزأ من حياتنا اليومية، ومع هذا التطور التكنولوجي، ظهرت مخاطر جديدة تهدد استقرار المجتمعات وأمنها، واحدة منها هي الإرهاب السيبراني. يشكل الإرهاب السيبراني تهديدًا خطيرًا للأمن القومي والاستقرار العام للدول والمجتمعات، فهو يستخدم التكنولوجيا الحديثة والشبكة العنكبوتية لتنفيذ أعمال عدائية وعمليات إرهابية تستهدف الأفراد والمؤسسات والحكومات. وتتنوع أشكال هذا الإرهاب السيبراني من الاختراقات الإلكترونية والسرقة الرقمية إلى الهجمات على الأنظمة الحاسوبية الحكومية والبنية التحتية الحيوية. تتسم الجرائم السيبرانية المرتبطة بالإرهاب بالتعقيد والتنظيم، حيث يعمل المجرمون السيبرانيون ضمن مجموعات متطورة ومتخصصة، وتنطوي هذه الجرائم على استغلال الثغرات الأمنية في الأنظمة والتلاعب بالمعلومات الحساسة والترويع والتأثير على الجمهور.

ثانيًا / مشكلة البحث .

تنبع مشكلة البحث من سؤال محوري ، مفادة ما هو الإرهاب السيبراني ، وكيف نميزه عما يشتبه به ؟ وهل هو نوع من انواع الإرهاب العام ؟ وماهي مظاهره وصوره ؟ وما هي اركانه ؟ وهل هو جريمة ؟

ثالثًا / هدف البحث.

يسعى الباحث الى اثبات فرضية مفادها " ان التطور التكنلوجي والعلمي في مجال الفضاء السيبراني وبالأخص الانترنت ، مهد الارض الخصبة لاستغلال تلك التقنيات المتطورة من قبل التنظيمات والجماعات الارهابية ، لبث الرعب والخوف لدى الدول والشعوب على حد سواء " .

رابعًا / منهجية البحث.

يستعين الباحث عند معالجته لمعطيات البحث بأدوات المنهجين التحليلي والوصفي ؛ لكشف ماهية هذا النوع من الإرهاب من جهة ، وتمييزه عن الجريمة السيبرانية وكذا الحرب السيبرانية من جهة ثانية ، ومن ثم تبيان وصفه القانوني من خلال طرح اسبابه ومظاهره وأركانه .

خامسًا / خطة البحث .

تنقسم خطة البحث الى ثلاث مطالب ، اذ سنتطرق في المطلب الاول الى مفهوم الارهاب السيبراني ، اما في المطلب الثاني فسنتطرق الى التطور التاريخي للإرهاب السيبراني وأسبابه ، اما في المطلب الثالث والاخير فسنتطرق الى مظاهر الإرهاب السيبراني وأركانه ؛ وكما يلي .

المطلب الاول/ مفهوم الإرهاب السيبراني.

يعد التعريف بالإرهاب السيبراني مدخلاً لا غنى عنه للكشف عن كنه هذا الموضوع وسبر أغواره ، وهذا ادعى كون ظاهرة الارهاب السيبراني من الظواهر المستحدثة ، لذا وجب علينا في هذا المقام ان نبين المعنى اللغوي والاصطلاحي في فرعٍ اولٍ ، ومن ثم تبيان ذاتية الارهاب السيبراني متمثلًا بخصائصه وتمييزه عما يشتبه به في فرعٍ ثانٍ ، وهذا ما سيتم دراسته تباعًا .

الفرع الاول / تعريف الإرهاب السيبراني.

يتكون مصطلح الارهاب السيبراني Cyber Terrorism من مفردتي (السيبرانية) و (الإرهاب) ، ومصطلح (Cyber) تشير الى الفضاء السيبراني ، وهو مصطلح يضاف الى المصطلحات الاخرى المتعلقة بالأمن السيبراني ، كالجرائم السيبرانية ، الحرب السيبرانية ، التسلل السيبراني ، وبطبيعة الحال فان الفضاء السيبراني مصطلح متفق عليه عمومًا عكس الإرهاب.[1] لقد أصبح الإرهاب السيبراني الدولي حديثًا ، محور اهتمام المنظمات الدولية والدول والافراد ؛ بل ويمكن اعتباره من القضايا التي تؤرق المجتمع الدولي ؛ وذلك لعدة اسباب اهمها ،اتساع نطاق استخدام التكنلوجيا الحديثة وانتشار الحاسب الآلي والانترنت ، اضافة الى عدم وجود تعريف جامع مانع لمفهوم الإرهاب السيبراني ، وذلك بسبب تنوع اشكاله ومظاهره وصوره واساليبه وانماطه واختلاف اوجه نظر الفقهاء اليه ، كل ذلك بسبب حداثة المفهوم وغياب تعريف دقيق لمفهوم الارهاب التقليدي.[2] ولغرض تعريف الارهاب السيبراني سنقوم بتعريف مصطلحي (الإرهاب - السيبرانية) من ناحية لغوية وتعريف

(الارهاب السيبراني) اصطلاحًا مع ذكر بعض التعريفات في الاتفاقيات والتشريعات الدولية ان وجدت ؛ ومن ثم تعريفه من قبلنا كباحثين .

اولًا : الإرهاب السيبراني لغةً.

تُشتق كلمة الإرهاب (لُغةً) من الفعل أرهب ، حيث نقول أرهب فلانًا ، اي خوفه وفزعه ، ورهب الشيء أي أخافه ، اما الإرهابيون (Terrorists) فهو وصف يطلق على اولئك الافراد الذين يسلكون سبيل العنف والإرهاب لتحقيق اهدافهم السياسية . [3] ويقول ابن منظور في معجمه لسان العرب " رهب بالكسر يرهب رهبة ، ورهبًا بالضم ، ورهبًا بالتحريك ؛ اي خاف ". ورهب الشيء رهبًا ورهبةً اي خافه ، وورد في الدعاء " رغبةً ورهبةً اليك " ، الرهبة اي الخوف والفزع . فالإرهاب : مصدر ارهب يرهب ارهابًا ، من باب اكرم وفعله المجرد (رهب) ، قال تعالى " وإياي فإرهبون " اي خافونِ ، وقال عز وجل " ويدعوننا رغبًا ورهبًا " اي طمعًا وخوفًا . [4] اما كلمة Terror فترجع في قواميس اللغة الانكليزية الى الفعل اللاتيني Ters والذي يعني الترويع ،الهول ،الرعب ، وتدور أغلب معانيه حول نطاق ذات المعنى ، فقد ورد في قاموس المورد عن كلمة Terror انها تعني رعب او ذهل بفظاعة (كفعل) ، وكمصدر هو كل ما يوقع الرعب في النفوس لدى الافراد من مصدر قلق ، مظهر رهيب ، شيء مروع ؛ اما كلمة Terrorist فتعني إرهابي ، اما Terrorize فتعني يرهب ، يروع ، يكره . [5] اما المصدر اللغوي لمصطلح السيبرانية فتشير المراجع العلمية الى ان اول من استخدم مصطلح السيبرانية هو العالم (Norbert Wiener) وذلك عام 1948 عند بحثه لموضوع القيادة والسيطرة والاتصال في علم الحيوان ، فضلًا عن حقل الهندسة الميكانيكية.[6] اما فيما يتعلق بالبحث عن اصل كلمة (Cyber) في معاجم اللغة ، فيتبين انها ذات جذور يونانية والتي تعني (Kybernetes) والتي تدل على معنى (ربان السفينة) وقد وردت هذه الكلمة في مؤلفات الخيال العلمي لتدل على القيادة او السيطرة والتحكم عن بعد . [7]

وبالعودة الى قواميس اللغة ، فلم نرى ما يشير لكلمة (Cyber) سوى ما ورد في قاموس المورد اذ يعرفها بالقول : السيبرانية هي علم الضبط ويرجعها الى كلمة (Cybernetics) والتي تعني (علم الضبط ، علم التوجيه)[8] وهو مصدر يتوافق مع هجمات الارهاب السيبراني أي ضبط الاشياء والتحكم بها عن بعد(توجيه تلك الهجمات والتحكم بها لغرض الاضرار بالمصالح لتحقيق غايات ارهابية)

في حين اشار جانب من الفقه المعاصر ، ان كلمة السيبراني اشتقت من اصل الكلمة Cyber والتي تعني شبكات الانترنت ، شبكات الاتصال والمعلوماتية ، وانظمة التحكم الرقمية ؛ وعند استقراء العديد من الدراسات العربية السابقة ، نجد انها بالمجمل كانت تستخدم لفظة الإلكترونية متأثرة بالترجمة السابقة لمفردة Cyber ، والتي نعتقد بانها غير صائبة كون الإليكتروني مرادف لكلمة Electronic وليس Cyber ؛ ومن ثم بات يطلق على كل ما يتعلق بالشبكات الالكترونية عبر الحواسيب ، وشبكات وتطبيقات الأنترنت وكل ما له علاقة بشبكات التواصل الاجتماعي (بالسيبراني) ونحن نؤيد هذا الرأي ، فيقال على سبيل المثال الفضاء السيبراني والمقصود منه الفضاء الالكتروني ، والذي يشير الى كل ما يتعلق من قريب او بعيد بشبكات الحاسوب والانترنت وتطبيقاته المختلفة . [9] اما سبب اختيارنا لمصطلح السيبرانية في دراستنا هذه ، فيعود لعدة أسباب ؛ اهمها المصطلح الذي استخدمه (Norbert Wiener) في كتابة (Cybernetic) ولعدم وجود إتفاق في اللغة العربية للمصطلح ، كذلك إن الوثائق التي استخدمتها الامم المتحدة والصادرة باللغة العربية إستعملت مصطلح السيبرانية [10] ، بالإضافة الى استخدام الاستاذ الدكتور احمد عبيس الفتلاوي لهذا المصطلح في كتابة (الهجمات السيبرانية) ونحن نؤيد هذا الرأي ؛ ولما تقدم نلاحظ ان التسمية الاصوب هي (الإرهاب السيبراني) بدلا من المصطلحات المناظرة الاخرى مثل ، الارهاب المعلوماتي ، ارهاب الظلام ، الارهاب عبر الانترنت ، الارهاب الرقمي ، الارهاب الالكتروني ، والارهاب التكنلوجي .

ثانيًا : الإرهاب السيبراني اصطلاحًا.

سنتطرق لذكر تعريف الارهاب العام بصورة موجزة ، ومن ثم نتوسع بتعريف الارهاب السيبراني مدار البحث وكما يلي :

- **الإرهاب بمفهومه العام :** ان التعريفات التي وردت لمصطلح (إرهاب) في القواميس العربية ليس لها إمتداد تاريخي قديم وإنما تتسم بالحداثة ، فعرف صاحب المعجم الوسيط الارهابيين بانهم " وصف يطلق على من يسلكون طريق العنف لتحقيق اغراض سياسية " وعرف معجم المُنجد ، الإرهابي " هو من يلجأ للإرهاب لإقامة سلطته "[11] وقد اثار التعريف بمفهوم الارهاب جدلًا واسعًا في الفقه القانوني على المستوى الوطني والدولي ، وقد امتد ذلك الجدل الى المنظمات الدولية والاقليمية التي تصدت لتحديد هذا المفهوم ، مما حدا بالبعض بالعزوف عن تعريفه وانما الاكتفاء بتحديد صوره وانماطه ، وخصوصا انه لحد الان لا توجد معاهدة شاملة بشان الارهاب ، بالرغم من وجود 19 صكًا عالميًا متعلقًا بالإرهاب ، وهي صكوك تقضي بتجريم مظاهر السلوك الارهابي في مسعى الجهود الدولية لمنع وقمع الارهاب .[12] الامر الذي افضى الى عدم وجود مفهوم دولي موحد للإرهاب بصفة عامة ، لذا سنتناول بعض التعريفات العامة للإرهاب من وجهة نظر الفقه ، فقد عرف الفقيه الفرنسي(Gourg Levasseure) الإرهاب بانه " الاستخدام العمدي والمنظم للوسائل التي من شأنها اثارة الرعب والفزع لدى الاخرين بقصد تحقيق بعض الاهداف الخاصة والشخصية "[13] ، وعرفه الفقيه الفرنسي (Sottile) بانه " العمل الاجرامي المقترف عن طريق العنف الشديد من اجل تحديد هدف محدد "[14] كذلك عرفه (Jennings Bryan) احد المتخصصين الدوليين بالإرهاب على انه " مجموعة افعال معينة بقصد احداث رعب وخوف ، ولكن مفهوم الارهاب لا يجب ان يتوقف عند الارهاب الذي يمارسه الافراد وانما لابد من التوسع في المفهوم حتى نصل الى الارهاب التي تمارسه الدول "[15]كما عرفه الاستاذ (Alex Schmid) بانه " طريقة عنيفة او اسلوب عنف للمعارضة السياسية وهو يتكون من العنف والتهديد وقد يتضمن التهديد او العنف البدني الحقيقي وايضًا ممارسة او التهديد بممارسة العنف النفسي والذي يمارس ضد الابرياء او اهداف لها ارتباط مباشر بالقضية التي يعمل الارهابيون من اجلها "[16] في حين عرفه الاستاذ الدكتور شفيق المصري على انه " استخدام غير شرعي للقوة او العنف او التهديد باستخدامها بقصد تحقيق اهداف سياسية "[17] ونلاحظ من التعارف اعلاه ، بانها جمعت بين الاتجاهين المادي والمعنوي لتعريف الارهاب وهو ما نراه الاجدر بالاتباع ، كذلك يتبين لنا بأن مفهوم الارهاب السيبراني لا يختلف عن الارهاب التقليدي الا من حيث الطريقة التي يلجأ اليها الجاني بارتكاب فعله الارهابي ، والتي اخذت منحى مستحدث مع التطور التكنلوجي والثورة المعلوماتية.
- **الإرهاب السيبراني :** كانت البداية في استخدام مصطلح الارهاب السيبراني على يد (Barry Collin) في ثمانينات القرن العشرين حيث اقر بصعوبة وضع تعريف جامع مانع للإرهاب السيبراني ؛ وبالرغم من ذلك فانه تبنى تعريفا له وهو انه " هجمة الكترونية غرضها تهديد الحكومات او العدوان عليها ، سعيا لتحقيق اهداف سياسية او دينية او أيديولوجية ، وان الهجمة يجب ان تكون ذات اثر تدميري وتخريبي مكافئ للأفعال المادية للإرهاب "[18] وقد عرفه (James Lewis) على انه " استخدام شبكات الحاسوب في تدمير او تعطيل البنى التحتية الوطنية المهمة مثل : الطاقة والنقل ، او بهدف ترهيب الحكومة والمدنيين ،[19] اما (Dorothy Denning) فترى ان الارهاب السيبراني هو " الهجوم القائم على مهاجمة الحاسوب ، وان التهديد يهدف الى الترويع او اجبار الحكومات او المجتمعات لتحقيق اهداف سياسية او دينية او عقائدية ، وينبغي ان يكون الهجوم مدمرًا او تخريبيا لتوليد الخوف بحيث يكون مشابه للأفعال المادية للإرهاب " .[20] كذلك عرفه بعض المتخصصين والباحثين بالأمن السيبراني على انه " خرق للقانون يقدم عليه فرد من الافراد ، او تنظيم جماعي ، بهدف اثارة اضطراب خطير في النظام العام ، عن طريق شبكة المعلومات العالمية الانترنت " في حين عرفه آخرون بانه " الاستخدام العدائي والعدواني غير المشروع للإنترنت ، بهدف ترويع الحكومة والمدنيين ، او قسم منهم في اطار السعي الى تحقيق اهدف سياسية او اجتماعية ".[21] اما (Kevin Coleman) فعرف الارهاب الالكتروني بانه " الاستخدام المتعمد للأنشطة التخريبية ، او التهديد بها ، ضد اجهزة الكومبيوتر او الشبكات ، بقصد احداث ضرر ، بدوافع اجتماعية او اديولوجية او دينية او سياسية او غيرها ، او ترهيب ثمة اشخاص تحقيقًا لتلك الاهداف والدوافع "[22]

إذًا يستشف من التعريفات المذكورة آنفًا هو : ان الارهاب السيبراني لا يكاد يختلف في جوهره ومضمونه عن الارهاب العام ، من حيث النية والقصد الجرمي للفاعل ؛ ما خلا طريقة تنفيذ هذا الفعل الارهابي ، ففي الارهاب التقليدي يكون من خلال استخدام القوة الفعلية والعنف متمثلة بالأسلحة المتنوعة والمتفجرات وغيرها من صور الافعال الارهابية ، اما الارهاب السيبراني ، فيكون عن طريق استخدام شبكة الانترنت وتطبيقاته المتنوعة للوصول الى الاهداف التي يبغي تحقيقها الارهابي ، مثل تجنيد الاشخاص ، نشر الدعاية والاعلان للجماعات الارهابية ، التعرض للحكومات او المنظمات ، تحريض الافراد على القيام بأعمال عدائية ضد الدولة ومؤسساتها ، او ضد جماعات معينة ، اما هدفهم فهو واحد بالنسبة للإرهاب سواء كان عام أم سيبراني .

اما تعريف الإرهاب السيبراني من قبل التنظيمات الدولية والاتفاقيات ،؛ ففي اكتوبر 2012 عرفت الأمم المتحدة U.N الارهاب السيبراني انه " استخدام الانترنت لنشر اعمال ارهابية "[23] وهو تعريف مقتضب وذو صورة هلامية ومبهمة . ونتيجة لغياب التوجه الرسمي من الامم المتحدة لإيجاد تعريف محدد للإرهاب السيبراني ، ظهرت اجتهادات فقهية لمعالجة مفهوم الهجمات السيبرانية ؛ حيث عَرف دليل تالين Tallinn Manual الهجمات السيبرانية بانها " ... الهجمات الإلكترونية ، او التهديد بها ، والغرض الرئيس منها هو نشر الرعب بين السكان المدنيين ... "ومما ينبغي الاشارة اليه ان التعريف الصادر عن دليل تالين ،هو تعريف صادر عن جهة غير رسمية وانما صدر عن مجموعة من فقهاء القانون الدولي العام ويعتبر قواعد قانونية استرشادية لعمل وسلوك الدول في سياق الحرب السيبرانية ،لذلك فهو غير ملزم .

وقد عرفته الاتفاقية الدولية الاولى لمكافحة الاجرام عبر الانترنت في بودابست 2001 على انه " هجمات غير مشروعة ، او تهديدات بهجمات ضد الحاسبات او الشبكات او المعلومات المخزنة الكترونيا ، توجه من اجل الانتقام او ابتزاز او اجبار او التأثير في الحكومات او الشعوب او المجتمع الدولي باسره ، لتحقيق اهداف سياسية او دينية او اجتماعية معينة ، وبالتالي فلكي ينعت شخصا ما بانه ارهابيا على الأنترنت ، وليس فقط مخترقا ، فلابد ان تؤدي الهجمات التي يشنها الى عنف ضد الاشخاص او الممتلكات ، او على الاقل تحدث اذى كافيا من اجل نشر الخوف والرعب"[24] . ونلاحظ بانه تعريف جامع مانع للإرهاب السيبراني ، وان كان التعريف اعلاه كان تحت عنوان الجريمة السيبرانية ، الا انه لا يمنع من تكييف تلك الجريمة من ناحية تحقيق غايات ارهابية تحت عنوان الارهاب السيبراني.

اما مكتب التحقيقات الفيدرالي الامريكي FBI فقد عرف الارهاب السيبراني على انه " الاستخدام غير القانوني او غير المشروع للقوة او العنف المرتكب من قبل جماعة (جماعات) من فردين او اكثر ضد الاشخاص والممتلكات بغرض تخويف الحكومة او السكان المدنيين او قطاع منهم واجبارهم لتحقيق اهداف سياسية او اجتماعية محددة لصالح الجماعة مرتكبة العنف " [25] ، ويعوز هذا التعريف ذكر الوسيلة التي يمارس خلالها العنف ، وقد تطور مفهوم الارهاب السيبراني عبر السنين وعليه غَير مكتب التحقيقات الفيدرالي FBI صياغة التعريف عدة مرات ، واليوم يعتمد المكتب على التعاريف التي تتبنى انشطة اكبر من مجرد استهداف البنى التحتية لتكنلوجيا المعلومات ، ومنها تعريف مركز الدراسات الاستراتيجية والدولية والذي يعرف الارهاب السيبراني على انه " تخويف المؤسسات المدنية من خلال استخدام التكنلوجيا العالية لتحقيق اهداف سياسية او دينية او ايديولوجية او اعمال تؤدي الى تعطيل او حذف بيانات او معلومات البنية التحتية الحيوية " [26] ومما يمكن تأشيره على تعريفات FBI بانها تطورت بتطور الارهاب وتقنياته وهذا شيء صحي ، لكن ما يعاب على لتعريف الاخير انه لم يبين طبيعة تلك الاستخدامات ، اضافة الى عنصر الهدف اذ حدد المؤسسات المدنية فقط ، وهذا غير صائب ، اذ يمكن ان تكون المؤسسات مدنية او عسكرية وكذلك يمكن ان تكون وطنية او دولية .

وبالعودة الى التعاريف اعلاه يمكننا التوصل الى استنتاجات مهمة ، أهمها :

- لا يوجد تعريف دولي موحد للإرهاب بصفة عامة،فضلًا عن الارهاب السيبراني على وجه الخصوص وذلك بسبب تنوع اشكاله ومظاهرة وتعدد انماطه واساليبه، واختلاف وجهات النظر الدولية اليه.

- بسبب عدم توصل الفقه الى اتفاق موحد للإرهاب السيبراني ، ادى ذلك الى تباين المفاهيم لذلك المصطلح ، هذا من جانب ؛ ومن جانب آخر كان له الفضل الاكبر (اي الفقه) في تعريف الارهاب السيبراني خاصةً في ضل تأخر الاجماع الدولي على تعريفه .
- الارهاب السيبراني هو احد صور الارهاب المعاصرة ، والذي تقوم به التنظيمات الارهابية والذي يبغي تحقيق اهداف الارهاب التقليدي وذلك باستخدام تكنلوجيا المعلومات .

وعليه يمكن تعريف الإرهاب السيبراني بانه :

" هجمات غير مشروعة بدوافع سياسية او أيدولوجية او التهديد بتلك الهجمات على شبكات الحواسيب الآلية وموارد تخزينها ، توجه ضد مصالح الجماعات او الدول والمجتمع الدولي ؛ لتحقيق حالة من الاضطراب والخوف والذعر وتقويض الثقة ؛ لإكراه تلك الحكومات او المجتمع المستهدف للاستجابة لمنفذي تلك الهجمات تحقيقًا لغاياتهم " [27].

الفرع الثاني/ ذاتية الإرهاب السيبراني.

رأينا فيما سبق ان الإرهاب السيبراني هو احد مجالات وانواع الارهاب عمومًا ، لكن ما يميز الارهاب السيبراني هو استخدامه الفضاء السيبراني والتكنلوجيا كوسيلة او مقصد مباشر ، وبالمحصلة يلتقي الارهاب السيبراني مع الارهاب التقليدي في اغلب خصائصه ، ويحتفظ لذاته بخصائص مستقلة ؛ اضافة لذلك يتميز الارهاب السيبراني عن بعض المفاهيم التي قد يشتبه بها ، كالحرب السيبرانية والجريمة السيبرانية وغيرها من المصطلحات ؛ لكن يبقى الارهاب السيبراني يتميز عن غيره بالهدف والنتيجة المتحصلة من تلك الهجمات الا وهي العنف والترويع ؛ ولبيان ذلك سنقسم هذا المطلب الى خصائص الارهاب السيبراني في قسمٍ اولٍ ، اما في القسم الثاني سنتطرق الى تمييزه عما يشتبه به ، وكما موضح ادناه :

اولًا : خصائص الإرهاب السيبراني .

يتميز الارهاب السيبراني بالعديد من الخصائص والسمات التي يختلف بها عن الجرائم الاخرى وتحول دون اختلاطه بالإرهاب التقليدي ، ويمكننا ايجاز اهم تلك الخصائص والسمات فيما يأتي :

1- **المهارة التقنية :** ان الارهابي السيبراني يمارس عادةً من ذوي الاختصاص في مجال برمجة الحاسوب وتقنية المعلومات ، او على الاقل لديه قدر من الخبرة في التعامل مع التقنية المعلوماتية ؛ واستقطبته المنظمة الارهابية للقيام بأعمال ارهابية سيبرانية .

2- **سهولة التخفي :** من الصعوبة تعقب الجريمة واثباتها نتيجة اخفاء واتلاف معالمها المادية المتحصلة عن الفعل الارهابي .

3- **قوة التأثير و فداحة الخسائر :** الارهابي السيبراني لا يحتاج سوى حاسوب وبرامج وغرفة صغيرة لإكمال عمليته الارهابية ، وبذلك ينزل افدح الخسائر المادية في اماكن تبعد مسافات كبيرة.

4- **جرائم ناعمة :** ان الارهاب السيبراني لا يحتاج الى القوة والعنف ، انما يتطلب وجوده حاسوب متصل بالأنترنت.

5- **الطبيعة العابرة للحدود :** يتميز الإرهاب السيبراني كذلك بالطابع العابر للحدود ، حيث يعتبر من اهم خصائصه انها جريمة متعدية للحدود وعابرة للقارات وغير خاضعة لنطاق اقليمي محدد ، وبذلك يعتبر الارهاب السيبراني من الجرائم المنظمة عبر الوطنية .

6- **صعوبة اثباتها لسرعة غياب الدليل :** من الصعوبة اكتشاف الجريمة الارهابية السيبرانية ،بسبب ان الجاني لا يترك وراءه اي أثر مادي خارجي ملموس يمكن فحصة ، بالإضافة الى نقص الخبرة لدى الاجهزة الامنية وكذلك الجهات القضائية في مكافحة هكذا جرائم ، مما يتطلب وجود مختصين بالأمن السيبراني ، لبحث وتفحص موقع الجريمة .

7- **جرائم عمدية :** حيث تتسم جرائم الارهاب السيبراني بكونها جرائم عمدية ، حيث ترتكب بعد تدبير وتخطيط مسبق ، ولا تحدث على سبيل الخطأ او بشكل عشوائي او عفوي .

8- **تعدد الاغراض وتنوعها :** لم يعد الارهاب السيبراني مقتصرًا على تحقيق مآرب سياسية وانما امتد لتحقيق اغراض اخرى قد يكون في مقدمتها الاغراض الاقتصادية او الانتقامية او الدينية[28].

ثانيًا : تمييز الإرهاب السيبراني عما يشتبه به

بعد قيامنا بتحديد مفهوم الارهاب السيبراني وبيان خصائصه وسماته ، كان حريًا بنا ان نرفع هذا اللبس والتداخل القائم بين هذا المفهوم وبعض المفاهيم الاخرى .

1- **الجريمة السيبرانية** Cyber Crime: ان الحداثة التي تمتاز بها الجريمة السيبرانية ، واختلاف النظم القانونية والثقافية للدول ، ادت الى عدم التوصل الى اتفاق موحد لهذه الجرائم خشية حصرها في نطاق ضيق ، لذلك ظهرت عدة اتجاهات لتعريف الجريمة السيبرانية ، فبعضهم اعتمد المعيار المادي ، كما فعل مكتب تقييم التقنية في الولايات المتحدة الاميركية (OTA) عندما عرفها على انها " الجرائم التي تؤدي فيها البيانات الكمبيوترية والبرامج المعلوماتية دورًا رئيسيًا " كذلك عُرفت بانها " الجرائم التي يستخدم فيها الحاسوب وشبكاته العالمية كوسيلة مساعدة لارتكاب الجريمة كاستخدامه في النصب والاحتيال وغسل الاموال وتشويه السمعة والسب " ، ويتضح من التعاريف اعلاه بانها اعتمدت على المعيار المادي دون الاشارة الى المعيار المعنوي وهذا قصور واضح بالتعاريف اعلاه ؛ وقد اتجه رأي آخر للأخذ بمبدأ شخصية الفاعل على اساس المعرفة التقنية للمجرم ، كالتعريف الذي اعتمدته وزارة العدل الامريكية حيث عرفت الجريمة السيبرانية بكونها " اية جريمة لفاعلها معرفة فنية بتقنية الحاسب تمكنه من ارتكابها " ويتضح من التعريف اعلاه قصوره بسبب عدم توافر العناصر الاخرى للجريمة ؛ وقد اعتمد اتجاه آخر للفقه على موضوع الجريمة ، ومن اشهر فقهاء هذا الاتجاه (Rosenblatt) والذي عرفها " نشاط غير مشروع موجه لنسخ او تغيير او حذف للوصول الى المعلومات المخزنة داخل الحاسب الآلي او التي تحول عن طريقه " ويرى اصحاب هذا الرأي انهم لا يشترطون ان يكون النظام المعلوماتي اداة لارتكاب بل التي تقع عليه او في نطاقه، وهذا الاتجاه قاصر كذلك كون الجريمة السيبرانية يجب ان تحصل ضمن الشبكة المعلوماتية وموارد تخزينها. [29] وترتبط الجريمة السيبرانية والارهاب السيبراني بمصطلحات مترابطة ولكنها مختلفة تمامًا، اذ تشير الجرائم السيبرانية الى النشاط الاجرامي الذي يرتكب باستخدام الانترنت واشكال اخرى من شبكات الكومبيوتر ، ومن مظاهرها القرصنة وسرقة الهوية والاحتيال عبر الانترنت ، ومن ناحية اخرى يشير الارهاب السيبراني الى استخدام التكنلوجيا الرقمية لإحداث ضرر او تعطيل للحكومة او البنية التحتية الحيوية ، وغالبًا ما تكون الجريمة السيبرانية مدفوعة بمكاسب مالية او مكاسب شخصية ، في حين الارهاب السيبراني عادةً ما يتم تنفيذه من قبل مجموعات او افراد بدوافع سياسية او أيديولوجية .

ومن المهم ملاحظة ان بعض الاعمال التي تعتبر جرائم سيبرانية يمكن اعتبارها ايضًا ارهابًا سيبرانيًا ، اذا كان الغرض منها التسبب في الخوف والذعر او تعطيل البنية التحتية الحيوية او التأثير على التغيير السياسي او الاجتماعي [30] وبذلك يكون للجرائم السيبرانية عدة مظاهر وصور اهمها : الاعتداء على خصوصيات الحاسب الآلي ، الاعتداء السيبراني على حرمة الحياة الخاصة ، الاعتداء على حقوق الملكية الفكرية ، الاستيلاء والنصب والاحتيال السيبراني ، والكثير من النشاطات المخالفة للقوانين الوطنية.[31]

مما تقدم يتبين ان الارهاب السيبراني والجريمة السيبرانية بالرغم من اشتراكهما في البيئة التي تنفذ بها جرائمهما وهي الفضاء السيبراني ، اضافة الى الجرائم السيبرانية تستوعب الارهاب السيبراني والعكس ليس صحيح ؛ الا انهما يختلفان من حيث :

- **ارتكاب الفعل** : اذ يكون مرتكب الهجمة الارهابية حاملًا لفكر متطرف (إرهابي) وقد يكون منتمي لتنظيم او جماعة متطرفة ، اما الفعل المرتكب في الجريمة السيبرانية فيرتكب من قبل افراد (مُجرِم اعتيادي) باستخدام الحاسوب والشبكة العالمية للمعلومات (الانترنت) .
- **الأثر** : قد يشترك نوع الفعل او الأثر بينهما ، لكن الاختلاف يقع في الجهة المستهدفة ونطاق الأثر كون الارهاب يستهدف الجهات الرسمية والسيادية ويكون نطاق الدمار اكبر ، ام الجريمة السيبرانية فقد تستهدف جهات متنوعة ونطاق الأثر اقل واضيق ؛ اضافة الى ان ارتكاب الارهاب السيبراني هو ارتكاب ضد المجتمع الدولي بأكمله ، فعندما يقع الهجوم ضد دولة معينة فكإنما يقع ضد المجتمع الدولي بأجمعه .
- **الدافع** : يجب ان يكون لدى الارهابيين دافع سياسي او ايديولوجي ، كاستخدام الهجمات الارهابية في الدعاية والتجنيد او التمويل او الحصول على بيانات ؛ بينما الجريمة السيبرانية قد يكون الدافع ماليًا عن

طريق الاحتيال او مضايقة الأشخاص او الاساءة اليهم مثل التنمر والاحتقار ونشر الكراهية وازدراء الاديان .

- **النظام القانوني** : فالإرهاب السيبراني مُجَرمٌ بمختلف أشكاله بالنصوص التشريعية الوطنية والدولية [32] وبذلك تختلف عن النصوص التشريعية التي تجرم الجريمة السيبرانية .

ومما تقدم يتبين بان هدف الجريمة السيبرانية يختلف عن اهداف الهجمات الارهابية السيبرانية ، لان نتيجة الهجوم هي من تحدد من يقف وراءه ، بينما الجرائم السيبرانية تكون بعيدة عن سياسات الدولة ويستبعد ان تكون الدولة هي التي تقوم بالهجوم ، بل يكون اشخاص او مجاميع (Hackers) هي من يقوم بتنفيذ تلك الجرائم السيبرانية[33] ، اذ يحتمل ان يكون الهدف (مادي او اقتصادي) ؛ لذلك تكون الهجمات السيبرانية الارهابية من اختصاص القانون الدولي العام ، لأنه يمثل خرق لسيادة الدول ، بينما تكون الجريمة السيبرانية ضمن اختصاص القانون الوطني وفقًا لمبدأ اقليمية القانون.[34]؛ وفي جميع صور تلك الهجمات سواء كانت جريمة او حرب او ارهاب سيبراني ، تتحقق المسؤولية الدولية للدول عن اعمال مواطنيها ، بالإضافة الى المسؤولية الجنائية الدولية للأفراد .

2- الحرب السيبرانية Cyber Warfare

لبيان مفهوم الحرب السيبرانية [35]، لابد من التطرق للبيئة التي تحصل بها تلك الهجمات وهي الفضاء السيبراني والذي سنتناوله بإيجاز.

الفضاء السيبراني Cyber Space هو مصطلح يستخدم لوصف العالم الافتراضي الذي تم انشاؤه بواسطة شبكات الكومبيوتر والانترنت ، اذ انها المساحة الجماعية حيث يتفاعل الناس مع بعضهم البعض ، ويتشاركون المعلومات ويديرون الاعمال من خلال الوسائل الرقمية ، حيث يسمح الفضاء السيبراني للأشخاص بالتواصل ومشاركة البيانات والوصول الى المعلومات والخدمات ، ويعتبر العمود الفقري للعالم السيبراني . وبذلك يمكن اعتبار الفضاء السيبراني طريقة شائعة للعديد من اشكال الجرائم السيبرانية ، لأنها الوسيط الذي يتم من خلاله اطلاق وتنفيذ العديد من الهجمات السيبرانية ، على سبيل المثال يستخدم المتسللون الانترنت للحصول على وصول غير مصرح به الى انظمة وشبكات الكومبيوتر وسرقة المعلومات الحساسة ، وشن هجمات على البنية التحتية الحيوية وغيرها الكثير من الهجمات.[36] ظهر مصطلح الحرب السيبرانية بكثرة في بداية القرن الحادي والعشرين ، ولا يوجد مصطلح ثابت ولا تعريف واضح حول مفهوم الحرب السيبرانية حتى على مستوى منظمة الامم المتحدة ، اذ تعددت استخدامات مصطلحات وصف تلك الحالة منها ، حرب المعلومات، الحرب الالكترونية ، حرب الشبكات ، العمليات المعلوماتية ، وكذلك الحرب السيبرانية . ويقصد بالحرب السيبرانية : " اساليب الحرب ووسائلها التي تعتمد على تكنلوجيا المعلومات وتستخدم في سياق نزاع مسلح ضمن المعنى الوارد في القانون الدولي الانساني بخلاف العمليات العسكرية الحركية التقليدية " او هي " الهجمات والعمليات التي ترتكب ضد او بواسطة شبكات الحواسيب وانظمة البيانات بين دولتين او اكثر ، او بينها وبين جماعة او جماعات مسلحة منظمة ضمن سياق نزاع مسلح او سباق للتسلح او سياسات الردع المتبادل وذلك لأهداف متنوعة من بيها التسلل الى نظام الحاسوب وجمع البيانات المخزنة به او سرقتها او اتلافها او تبديلها او التلاعب بها بعد ان تصبح تحت سيطرة مدبر الهجوم " [37] نلاحظ على التعاريف السابقة بانها اعتمدت المعيار المادي والمعنوي وهذا اتجاه صائب في تعريف الحرب السيبرانية ونحن نؤيد هذا الرأي .وكذلك عرف احد الباحثين حرب المعلومات الافتراضية او الهجمات على الشبكة الحاسوبية والتي تعني " القيام بعمليات عسكرية بناءً على مبادئ مرتبطة بالمعلومات ، وهذا يعني اتلاف وتعطيل او الانتقاص من شأن المعلومات المخزنة في الحواسيب الآلية او المنقولة عبر الشبكات المعلوماتية الالكترونية في النزاعات المسلحة بوسائل الكترونية متعددة " [38] وهذا التعريف قاصر كونه يتميز بالعنصر المادي الفعلي ، اي القيام بعمل عسكري حقيقي على بنية الاتصالات الحيوية للعدو وليس هجمات سيبرانية ضد البنية التحتية الحيوية المعلوماتية للعدو .وفي احيان عدة يتم تخصيص موارد معينة للحرب السيبرانية من وجه نظر استراتيجية وتكتيكية وعملياتية ، لذا يشمل مصطلح الحرب السيبرانية ما يلي :

- القدرة الهجومية السيبرانية للبدء بالهجمات السيبرانية بالإضافة الى آليات الردع ، وكذلك السياسات والمواقف والاسلحة والقدرات والتحالفات ، واستراتيجيات وادوات لهجوم سيبراني مضاد .
- وسائل الدفاع السيبرانية والقدرات والتدابير المضادة في النظام لتكون مهيئة للحفاظ على المصالح والبنى التحتية وللتخفيف والتعافي السريع من الهجمات السيبرانية .
- استراتيجيات وعمليات الاستغلال السيبراني لتحديد الفرص السيبرانية لتكون قادرة على تحديد التهديدات الناشئة قبل ان تتطور لهجمات سيبرانية ملموسة ، كذلك التنبؤ وتحصيل معلومات لمعرفة منظمة العدو وان تكون مستعدة للرد بسرعة وكفاءة ضد اي احتمال لهجوم سيبراني .
- وحدات شبكة المعلومات (الانترنت) والمحاربون السيبرانيون ، بالإضافة الى المنظمات والكفاءات ؛ للهجوم والعمليات الاستباقية ، اذ يكون من المحتمل هدف الحرب السيبرانية هو تشويه عمليات المواقع العسكرية والاقتصادية والصناعية والادارية الهامة للعدو .[39]

ومن ابرز امثلة الحرب السيبرانية ، هي الحرب الروسية الجورجية عام 2008 ، اذ تزامنت تلك الهجمات مع غزوٍ بري وبحري وجوي من قبل روسيا الاتحادية ضد جورجيا ، ردًا على هجوم جورجيا ضد جمهورية اوسيتيا الجنوبية ، حيث استخدمت حملة سيبرانية مكثفة وشديدة التنسيق ضد جمع من الاهداف الجورجية بما فيها مواقع حكومية ذات قيمة استراتيجية ، بما فيها سفارتي الولايات المتحدة والمملكة المتحدة .[40] بالاضافة الى الهجوم على منشأة (Natanz) النووية الايرانية بواسطة فايروس (Stuxnet) عام 2010 ، حيث كان الفايروس مصمم خصيصًا لتخريب بعض الاجهزة الصناعية ، مما يؤكد الشكوك بان هدف الفاعل هو التخريب ، وجدير بالذكر ان الفايروس كان تحت رعاية الولايات المتحدة الاميركية في عملية سميت بـــ (عملية الالعاب الاولمبية).[41] وفي ذات السياق كشفت صحيفة (The New York Times) الأميركية ، ان الولايات المتحدة تعتبر المسؤول الرئيس في الهجمات السيبرانية ضد ايران ، حيث اشارت الصحيفة ان الرئيس الاميركي (باراك اوباما) مهتم شخصيًا بتسريع وتيرة استخدام الفايروسات بالهجمات ضد برنامج تخصيب اليورانيوم الايراني ، واكدت ان الولايات المتحدة الاميركية وإسرائيل هما من استخدم فايروس (Stuxnet) الذي دمر بعض انظمة تشغيل منشآت تخصيب اليورانيوم ؛ كذلك استخدمت اميركا فايروس (Flamer) ضد المنشآت النووية الايرانية ، حيث يرى مراقبون بانه تم سرقة كم هائل من معلومات المفاعل النووي الايراني.[42]

ومما تقدم يتبين بان الحرب السيبرانية والارهاب السيبراني امران يختلفان في العديد من الامور اهمها :

- **ارتكاب الفعل :** حيث يجب ان يكون الجهة المنفذة للهجمة السيبرانية تنتمي لجيش نظامي ، ويتم ذلك بإعلان الدولة مسؤوليتها عن الهجوم فضلًا عن وحدات الردع المكلفة بحماية امن الفضاء السيبراني ، بينما الارهاب السيبراني يتوقع حصوله من افراد او جماعات متطرفة ويستبعد حصوله من قبل الدول .
- **الاثر :** قد يشترك نوع الفعل او الأثر بينهما ، لكن الاختلاف يقع في النتيجة المتحصلة ونطاق الأثر كون الحرب السيبرانية اثرها المادي يحتمل ان يتجاوز الواقع العملي حيز الفضاء السيبراني مخلفًا اثرًا انسانيًا هائلًا ، ويكون نطاق الدمار اكبر اضافة لاحتمال مزامنته لنزاع عسكري ، اما الارهاب السيبراني فقد تستهدف بنية حيوية خارج النزاع المسلح او عداء سياسي ؛ اضافة الى ان ارتكاب الارهاب السيبراني هو ارتكاب ضد المجتمع الدولي بأكمله ، فعندما يقع الهجوم ضد دولة معينة فكإنما يقع ضد المجتمع الدولي بأجمعه .
- **الدافع :** يجب ان يكون الدافع للدولة المهاجمة سياسيًا او محاولة اخضاع الدولة المستهدفة ، وتتزامن تلك الهجمات مع او قبيل البدء بالعمليات العسكرية بين الطرفين او حتى في حالة عدم وجود نزاع عسكري وانما وجود عداء سياسي، بينما الارهاب السيبراني يكون دافعه تدميري لبث الذعر والخوف للجهة المستهدفة تحقيقًا لغاياته السياسية و الفكرية .
- **النظام القانوني :** تمتاز الحرب السيبرانية بخضوعها لقواعد القانون الدولي ، فضلًا عن القانون الدولي الانساني ، وبالأخص ميثاق منظمة الامم المتحدة ؛ وتحديدًا عدد من المبادئ ، منها مبدأ الحق في اللجوء للحرب (Jus in bellum) والمقررة في الفقرة الرابعة من المادة الثانية من ميثاق الامم المتحدة

والخاصة بالتهديد او استخدام القوة ، بالإضافة الى المادة الحادية والخمسون من ذات الميثاق والمتعلقة بحق الدولة باستخدام القوة في الدفاع عن نفسها ، ويضاف اليها كذلك قانون الحرب (Jus ad bello) ومبادئ الاتفاقيات الدولية المتعلقة بتنظيم الحرب. [43] بينما الارهاب السيبراني يخضع للمعاهدات والاتفاقيات الدولية المتعلقة بمنع وقمع الارهاب بكافة اشكاله وصوره ، فهو خاضع للقانون الدولي العام والتزامات المجتمع الدولي . إن الاثر المترتب بالهجوم السيبراني يختصره الخبير الروسي (Dmitry I. Grigoriev) بانه" يتجسد في التهديد على المستوى العسكري والسياسي فضلًا عن التهديدات الاجرامية والارهابية ، التي يمكن لمجموعات من غير الدول تبنيها لأجل الحصول على مزايا سياسية او اقتصادية " [44] ومما سبق نلاحظ ان الارهاب السيبراني يختلف عن الحرب السيبرانية من حيث افتقاده بصورة ضرورية الى عنصر المشروعية وارتكابه يكون من قبل افراد ، جمعات، هيئات ، دون مستوى الدول ؛ وفي ذات الوقت تكون الحرب السيبرانية التي تخوضها الدول في الفضاء السيبراني مشروعة.[45]، ان هدف الحرب السيبرانية يختلف عن اهداف الارهاب السيبراني ، لان نتيجة الهجوم هي من تحدد من يقف وراءه ، حيث ان الحرب السيبراني تقوم به دولة لتحقيق هدف (سياسي او عسكري) من اجل مقتضيات الامن القومي ، بينما الاهاب السيبراني يقوم به الافراد او الجماعات والتنظيمات الارهابية لتحقيق اهدافهم السياسية والأيديولوجية المتطرفة ، وبالمحصلة فان الهجمات السيبرانية تشمل كل من الحرب السيبرانية وكذلك الارهاب السيبراني ، الا انها تختلف فقط بالأغراض الاساسية لتلك الهجمات .

المطلب الثاني / التطور التاريخي للإرهاب السيبراني وأسبابه.

الارهاب السيبراني حديث النشأة نسبةً للإرهاب التقليدي ؛ اذ نشأ وتطور بعد ظهور الانترنت وشبكات الاتصال ، وبالخصوص بعد ثورة المعلومات التي حصلت نهاية القرن المنصرم ، ونتيجة ازدياد استخدام تقنية الاتصالات والمعلومات من قبل الدول والمؤسسات والافراد واعتمادها الكبير على تلك التقنيات مما جعل تلك المؤسسات عرضة لهجمات الارهاب السيبرانية ؛ اضافة الى ان وجود الارهاب السيبراني ليس صدفة ، وانما وجد لأسباب ودوافع متعددة ومتنوعة نتجت بسب التزاوج بين التكنلوجيا والارهاب ، لذلك سنبحث في هذا المطلب التطور التاريخي للإرهاب السيبراني في فرعٍ اول ، وفي الفرع الثاني سنتطرق الى اسباب ودوافع الارهاب السيبراني وكما يلي .

الفرع الاول/ التطور التاريخي للإرهاب السيبراني.

يقول خبير الارهاب الدولي الاميركي Gabriel Weimann " ان الارهاب الحديث اصبح أكثر ضراوة لإعتماده على التكنلوجيا المتطورة للأنترنت مما زاد من اتساع مسرح عملياتهم الارهابية ؛ وبالتالي اصبح من الصعب اصطياد هذا الوحش الالكتروني الجديد " وفي ذات السياق يكشف الخبير الاميركي عن ازدياد عدد استخدام المواقع الالكترونية والتي تستخدمها التنظيمات الارهابية ، فقد ازدادت من 12 موقع في العام 1998 الى 4800 موقع في الوقت الحالي .[46] مما لاشك فيه ان الارهاب السيبراني يزداد في الدول المتقدمة ، كونها تدير بنيتها التحتية بواسطة الحاسبة الالكترونية والاتصال بالشبكة العنكبوتية العالمية (World Wide Web) ، مما يجعلها صيدًا يسيرًا من قبل المنظمات والمجاميع الارهابية ، فبدلًا من استخدام الجماعات الارهابية للمتفجرات والاسلحة التقليدية ، صار من السهل بكبسة زر واحدة على لوحة المفاتيح بالحاسوب من تدمير وتعطيل البنية التحتية المعلوماتية للدولة ومؤسساتها بحيث يكون تأثيرها اكبر من تأثير الأسلحة التقليدية ؛ وبذلك يمكن شن هجمات ارهابية سيبرانية لتدمير واغلاق المواقع الحيوية والاضرار بأنظمة القيادة والسيطرة والاتصالات وكذلك تعطيل الاتصال بين الوحدات والقيادة المركزية ، بالإضافة الى تعطيل انظمة الدفاع الجوي والتلاعب بالصواريخ واخراجها عن مسارها المحدد او التحكم بالملاحة الجوية والبحرية والبرية وكذلك محطات المياه والطاقة واختراق الأنظمة المصرفية والحاق الضرر بالأسواق المالية والمصرفية العالمية ؛ وبذلك يعتبر الارهاب السيبراني ارهاب مستقل عن ذلك الارهاب التقليدي ، وهو الخطر العالمي الحالي والمستقبلي ، نتيجة تعدد اشكاله وتنويع اساليبه واتساع مقدرته على استهداف وسائل الاتصالات والانظمة المعلوماتية ،واستخدامها بجو هادئ ومريح وبعيد عن المخاطرة وتوفير القدر الكبير من السلامة والامان للإرهابيين المهاجمين.[47] لتأصيل ظاهرة الارهاب السيبراني والبحث عن جذوره الاولى ، يجدر بنا

العودة الى منتصف القرن العشرين وخصوصا بعد بروز فكرة حرب المعلومات Information Warfare [48] والتي ظهرت في الميدان العسكري بعد الحرب العالمية الثانية ، لتنتقل بعد ذلك الى المجال الأمني ؛ نتيجة الازدياد المضطرد لاستخدام النظم المعلوماتية المفتوحة لإنشاء البنية التحتية للدول ، اذ بانت ملامحها بإطلاق الاتحاد السوفيتي(سابقًا) اول قمر صناعي فضائي ، وهو القمر (Spotting) ذو الاغراض التكنلوجية المتعددة ، اذ ارتبط بالأذهان بتطور تكنلوجيا المراقبة والتجسس . [49]

ولكون الارهاصات الاولى للظاهرة الارهابية تعود بنا الى اندماج مجتمع المعرفة والاتصال ، فمنذ بزوغ شمس ثورة التكنلوجيا ، وتجلي ذلك بكشف الستار عن اختراع الحاسوب الآلي(Computer) عام 1946 في جامعة بنسلفانيا في الولايات المتحدة الاميركية ، اذ كان يستخدم في الحساب والتكامل الالكتروني(ENIAC) ، وفي اواخر الستينات من القرن الماضي حيث ولادة الانترنت ، اذ من الصعوبة بمكان تحديد من له الفضل في اختراعه ، فقد اسهم فيه العديد من العلماء ، والامر المؤكد في هذا السياق بان وكالة مشاريع الابحاث المتقدمة في وزارة الدفاع الاميركية (البنتاغون) أنشأت ما يسمى (ARPANET) والذي يسمى اليوم في عالمنا بإسم الانترنت ، وفي عام 1988 بدأت المؤسسة الوطنية للعلوم بالولايات المتحدة الاميركية تزويد البلدان الاخرى بخدمة الانترنت ، وفي عام 1991 اطلقت اول صفحة على مستوى الشبكة العالمية ، وفي ابريل 1995 قامت المؤسسة الوطنية للعلوم بالولايات المتحدة بتمكين العديد من الشبكات الخاصة والاقليمية من السيطرة على الانترنت.[50]

- **ظهور التطرف على الانترنت .**

لم تكن التنظيمات الارهابية اول من استخدم التكنلوجيا الحديثة كالأنترنت والفضاء السيبراني لخدمة اغراضهم الارهابية ، بل كان للجماعات المتطرفة الريادة في استخدامها ، ففي عام 1983 استخدم المدعو George Dietz الانترنت لترويج الفكر المتطرف من خلال دعوته للنازية وذلك من خلال استخدامه انظمة Bulletin Board System كوسيلة للتواصل مع المتعاطفين معه عبر الانترنت ، وبعد تلك الفترة جاء المدعو Louis Beam ليروج لأيديولوجية " الجنس الآري " والمتأثر بحركة Ku Klux Klan المتطرفة ، اذ اسهم (لويس) بإنشاء موقع شبكة الحرية الآرية على الانترنت Aryan Liberty Network وله العديد من المقالات الداعمة لأفكاره العنصرية في مواجهة الحكومة الاميركية ، وتعد مقالته (المقاومة بغير قيادة) من اهم مقالاته ومصدر إلهام لكثير من التنظيمات الارهابية والتي تبنت فكرة الذئاب المنفردة . [51] وشهدت فترة تسعينيات القرن المنصرم تناميًا وتطورًا في عديد المواقع المتطرفة والتي تُحرض على العنف وبث الكراهية بين الناس عبر شبكة الانترنت ، اذ كان اشهرها موقع جبهة العاصفة "Stormfront" والذي انشأ من قبل شخص يدعى Black Don والمنتمي للتنظيم النازي داخل الولايات المتحدة الاميركية وظل هذا الموقع حتى عام 2017.[52] ولم يتغير المشهد مع ظهور الجماعات الارهابية التي تدعي ان لها أيديولوجية اسلامية [53] ، ففي بادئ الامر وعند ظهور تنظيم القاعدة الارهابية اعترضوا على استخدام تلك التقنيات الحديثة كونها اختراعات غربية وذلك نتيجة فكرهم الوهابي المتطرف ؛ لكن بسبب دعم المدعو عبد الله عزام [54] وامكانيته بالتأثير على الشباب ، اضافة لدور اسامة بن لادن ' اذ كان لهما دورًا بارزًا في تشجيع استغلال التكنلوجيا الحديثة في الجهاد . وفي نهايات تسعينيات القرن العشرين استخدم الارهابيون الانترنت بصورة مكثفة لنشر اعمالهم وافكارهم الارهابية .[55]

لقد اقتنعت الجماعات الارهابية التي تدعي انها ذات أيديولوجية اسلامية بأهمية الانترنت للتواصل مع الجماهير وتخلصًا من ضغوط الحكومات ، وقامت تلك التنظيمات الموجودة في افغانستان وغيرها من البلدان بتصميم شبكات الكترونية لتبادل الرسائل من خلال مواقع الويب والبريد الالكتروني . [56]

وبذلك فقد استخدمت التنظيمات الارهابية الفضاء السيبراني والانترنت بدءًا من تنظيم القاعدة الارهابي و تنظيم (داعش) الارهابي وغيرها من الجماعات بشكل متطور ، من خلال استغلاله في التواصل مع مؤيديه وانصاره والدعاية والاعلان وجمع المعلومات والتبرعات والتمويل والحرب النفسية وسرقة الافكار التجارية ، لزعزعة استقرار الدول اقتصاديًا تحقيقًا لأغراض ارهابية ، الامر الذي يعد اخلالًا جسيمًا بالسلم والامن الدوليين . [57] لكن الانعطاف الخطير والتحول الكبير كان بعد احداث 11 سبتمبر

2001 ، بعد ان اثبتت الدراسات انه بعد هذا التاريخ ، بدأت عملية الانتقال من عمليات المواجهة المباشرة الى حرب الفضاء السيبراني ، وعزم التنظيمات ذات الاصول المتشددة الى استهداف الانظمة المعلوماتية للدول لتحقيق اكبر الخسائر للدول دون الحاجة المباشرة الى المواجهة مع اجهزة الامن والاستخبارات.[58]

ونتيجة للمتغيرات الاقتصادية والسياسية التي طرأت على البيئة الدولية والتطور التكنلوجي والمعلوماتي بحيث اصبح العالم كقرية كونية صغيرة اسهمت في ان يتحول الارهاب من شكله التقليدي الى ما يسمى بالإرهاب الجديد[59] بمضمونه وتنظيمه وتسليحه ، فقد انتشر وارتبط مع حلقات الجريمة المنظمة بحيث اصبح ارهابًا عابرًا للحدود بمجموعات تربطها أيدولوجية سياسية او دينية بغض النظر عن انتمائها القومي او العرقي ، وبذلك تطور الارهاب على مستوى الوسائل المستخدمة والاسلحة المتطورة ؛ اذ ابتدع الارهابيون قنابل الوقود والتي استخدموها في هجمات 11 سبتمبر 2001 والتي تعد نقطة التحول في آليات الارهاب التسليحية والتي لم يشهدها التاريخ مسبقًا.[60]

وبسبب هذا التطور التكنلوجي ادى الى انتقال الافراد من العالم الواقعي الى العالم السيبراني ، وكذلك انتقال وتطور الجريمة من تقليدية الى سيبرانية ، فحجم التفاعلات الكبير على جميع المستويات سواء شخصية ام مؤسسية او في مجال الاعمال او الخدمات او الثقافة والاعلام تعتمد بصورة رئيسية على تكنلوجيا المعلومات ، فضلا من تزايد الهواتف الذكية وغيرها من التقنيات الحديثة والمتطورة باستمرار، ونتيجة لهذا التطور الكبير كان لابد من دخول المجال السيبراني او التكنلوجي ميادين الحروب واستخدامه من قبل المتطرفين لبث الرعب والفزع في صفوف المدنيين ؛ اذ من المتوقع ان تكون الحرب السيبرانية Cyber Warfare السمة الغالبة . اذ وصل عدد مستخدمي الانترنت والاجهزة المرتبطة به الى 4.9 مليار شخص لغاية العام (2021) اي ما يعادل ثلثي سكان العالم ، وازداد الى ثلاثة ارباع العالم في العام 2022 [61] ، ومع تزايد الاعتماد عليه في جميع مجالات الحياة سواء كانت سياسية ام اقتصادية ام عسكرية ام قانونية او غيرها من المجالات المتنوعة ، وفي ظل هذا الترابط الوثيق بين اجزاء العالم عبر التكنلوجيا والاتصالات والتطبيقات التي سمحت بتبادل التجارة والافكار والمعلومات بين جميع المستخدمين حيث بات من الضروري على كل دولة حماية مؤسساتها ورعاياها ، ومع ادراك الجميع لفوائد تقنية المعلومات الحديثة فانه لا يخفى حجم المخاطر المحدقة والكامنة في تغلغل هذه التقنيات في جميع مرافق ومؤسسات دول العالم ،والتي تتطلب من المجتمع والدولة التعاضد من اجل الحيلولة دون وقوع تلك المخاطر.[62] وفي ذات السياق قدمت Denning أستاذة الحاسب الآلي بجامعة George Town في شهادتها امام اللجنة الخاصة بمتابعة الإرهاب بالكونجرس الامريكي ، عرضًا مختصرًا لنشأة الارهاب السيبراني وكما يلي : "

- في عام 1997 استطاع الالاف من المكسيكيين تدمير احد المواقع الالكترونية المتخصص في بيع مواد فيديو على الانترنت وذلك بإغراقه بآلاف الرسائل الالكترونية .
- في عام 1998 استطاعت منظمة نمور التاميل في سيريلانكا تدمير مواقع سفارات سريلانكا بواسطة بعث ما يقارب 800 رسالة الكترونية يوميًا لكل رسالة .
- في عام 1999 فُجرت أجهزة الحاسب الآلي بالناتو(NATO) بواسطة ما يسمى بقنابل البريد الالكتروني والتي ارسلها المحتجون على حرب كوسوفو " .

وعلقت Denning على ان الامثلة السابقة قد يسميها البعض جرائم حاسب آلي ؛ وتورد امثلة لنشأة الارهاب السيبراني، وكما يلي : "

- في عام 1997 استطاع احد المحترفين من انشاء برنامج له القدرة على تحويل الفواتير الخاصة به الى اشخاص آخرين .
- في عام 1999 استطاع احد المجرمين الارهابيين من إغتيال احد خصومه السياسيين ، وذلك بالدخول على ملفه بأحد المستشفيات وتغيير مقادير العلاج الذي يصرف له واستطاع قتله .

- في عام 2001 وبعد حادثة اصطدام احدى الطائرات الجوية الامريكية بطائرة صينية واسقاطها، قام القراصنة الصينيين بتدمير آلاف المواقع الالكترونية الامريكية المهمة منها وزارة الدفاع والخارجية ، مسببة خسائر تقدر بملايين الدولارات لإعادة المواقع لوضعها قبل التدمير .
- بعد الحادي عشر من سبتمبر 2001 ظهر الارهاب السيبراني بشكل مكثف وفي كل انحاء العالم .
- في عام 2007 قامت الولايات المتحدة الامريكية بالتعاون مع الناتو ، بإرسال فريق متخصص في جرائم الارهاب السيبراني الى استونيا ، لمساعدة هذا البلد الذي تعرض لهجوم سيبراني وجه لجميع انظمة المعلومات وتمكن من ايقافها . " [63]
- اضافة الى هجمات سيبرانية ضد منظمة الصحة العالمية WHO ، ومقدمي الخدمات الطبية ومعاهد البحوث وشركات تصنيع الادوية والمستشفيات وشبكات المستشفيات اثناء انتشار وباء كورونا (Covied 19) ، اذ من الممكن اعتبار تلك الهجمات ضد المنشآت الطبية ان تصل الى جرائم دولية ، اذا ما استوفت العناصر المحددة لتلك الجرائم ومن ضمنها الجرائم ضد الانسانية وجرائم الحرب. [64]

ومما تقدم نلاحظ بان الارهاب السيبراني يتطور بتطور الاحداث ، و نتيجة تلك التطورات التقنية الكبيرة والطفرات المتسارعة في عالم الاتصالات والمعلوماتية ، والتي يطلق عليها ثورة تكنلوجيا المعلومات والاتصالات ، حيث اصبح من المستحيل على جميع الافراد والدول العيش بمعزل عن تلك التطورات التقنية ؛ وبالمقابل فان هناك مخاطر من استخدام تلك التقنيات من قبل الارهابيين لتحقيق اهدافهم الايديولوجية ، اذ بدأ يستهدف جميع القطاعات الحيوية والامنية والصحية وغيرها ، سواء من خلال جمع المعلومات وسرقة البيانات ام من خلال التدمير المباشر للبيانات المهمة المخزنة في السحابة الالكترونية لتلك المنشآت ؛ لذا يجب تعاضد جهود الافراد والدول والمنظمات المختلفة لحماية تلك المؤسسات والافراد من الهجمات السيبرانية التي ينفذها المتطرفين ، الامر الذي يستعدي التدخل الفوري دوليًا لوضع حد للإرهاب السيبراني .

الفرع الثاني/ اسباب ودوافع الارهاب السيبراني.

للإرهاب السيبراني اسباب ودوافع متعددة ومتنوعة ؛ وهي ذاتها اسباب ظاهرة الإرهاب التقليدي ، وذلك بسبب كون الارهاب السيبراني نوع من انواع الارهاب وشكلًا من اشكاله المتنوعة ، بالإضافة الى وجود عدة عوامل تجعل من ظاهرة الارهاب السيبراني موضوعًا ملائمًا وسلاحًا يسيرًا للجماعات والتنظيمات الارهابية ؛ وبنظرة عامة شمولية للظاهرة يمكننا القول : ان الاسباب متداخلة والدوافع متشابكة ، حيث تتداخل الدوافع ، الشخصية ، الفكرية ، السياسية ، الاقتصادية ، والاجتماعية ، وبذلك فان هذه الظاهرة معقدة ومركبة وشائكة ،ولكون الارهاب السيبراني يرتبط بصورة وثيقة بالتطور التكنلوجي وكذا تطور وسائل واساليب الاتصالات والتقنيات في المجتمعات والشعوب ، الامر الذي ادى الى اكساب هذا النوع من الارهاب بُعدًا جديدًا ،مما ادى الى تفاقم خطورته على المستوى الدولي ؛ ولما تقدم سنتطرق في هذا الفرع الى تبيان دوافع الإرهاب السيبراني في فقرة اولًا ، وفي فقرة ثانيًا سنتطرق الى الاسباب الخاصة للإرهاب السيبراني ، وكما يلي .

اولًا : دوافع الارهاب السيبراني.

1- **الدوافع الشخصية** : ان رغبة الظهور وحب الشهرة ترتبط بعوامل شخصية ونفسية ارتباطًا وثيقًا ، وكذلك بالعوامل السياسية والاقتصادية والأيديولوجية ، فالأفراد الذين لا يشعرون بمعنى الحياة في الدول النامية ، لعوامل تتعلق بالقهر والظلم وانعدام العدالة وعدم توفير حياة كريمة لهم ؛ تؤدي بهم للانحراف وولوجهم بعَالم الجريمة والارهاب ، بالإضافة الى عوامل تتعلق بالفرد على المستوى الشخصي ، فالفشل في الحياة العملية وكذا الاسرية يؤدي الى جنوحهم وعدم شعور الفرد بالانتماء والولاء للوطن ، اضافة الى الاخفاق في الحياة العلمية او في مختلف نواحي الحياة سواء أكانت وظيفية أم عاطفية ، مما يجعله يشعر بالفشل في حياته ورغبته في سد هذا النقص من خلال الاجرام والجريمة . [65]

2- **الدوافع الفكرية :** وذلك من خلال العقائد الوضعية المنحرفة ، كالتعصب لمبدأ فكري او ديني يؤدي بها الى استعمال العنف والارهاب من قبل فئة معينة محاولة فرض مبادئها على المجتمع ، والتشدد والغلو في

العقائد والفكر ؛ والتي ادت بالمحصلة الى ازدياد بروز ظاهرة الإرهاب وبشتى انواعه وصوره واساليبه ، كما انها أيدت وساهمت بنشوء سياسات ظالمة قاهرة ذات فكر منحرف .[66]

3- الدوافع السياسية : ويكون ذلك من خلال عدم المساواة والهيمنة على الاموال العامة ، وغياب الحكم الرشيد ، بالإضافة الى السياسات التي تنتهجها بعض الدول من الظلم والاضطهاد والكبت والتهميش وانتهاك حقوق مواطنيها .

4- الدوافع الاقتصادية : وذلك من خلال المشاكل الاقتصادية على المستوى الدولي او المحلي ، وعدم وجود تعاون دولي وانتشار البطالة والفقر ، بالإضافة الى تقدم وتطور الانظمة المصرفية تقنيًا، ادى الى سهولة انتقال الاموال وتحويلها .

5- **الدوافع الاجتماعية :** وتكون متمثلة بالتفكك الاسري وضعف التعليم والتربية ، بالإضافة الى البطالة والفراغ[67]إضافة الى غياب دور المنزل والمدرسة في رقابة الاطفال والشباب ، مما يؤدي الى استخدامهم الخاطئ لهذه التكنلوجيا ، او تمادي الطالب بالسلوك التقني السيء ، مضافًا الى ذلك الغلو والتشدد في بعض امور الدين ، حين يرى بعض الشباب بانهم اعلم من غيرهم وان بعض العلماء على ضلالة ، فيتوجب عليهم محاربة آرائهم بواسطة تلك التكنلوجيا.[68] اضافة الى دوافع دوافع تاريخية اذ قد تكون تلك الحوادث التاريخية سبب من اسباب ممارسة ارتكاب الاعمال الارهابية ، بالإضافة الى دوافع اثنية ، وذلك في حالة ممارسة النظام السياسي للتمييز العنصري ، حيث يكون دافع لممارسة الارهاب ضد الجماعات الاخرى .[69]

ثانيًا : الاسباب الخاصة للإرهاب السيبراني (اسباب تكنلوجية)

إضافة الى دوافع الارهاب السيبراني سالفة الذكر ؛ هناك العديد من الاسباب الخاصة التي تجعل من ظاهرة الارهاب السيبراني موضوعًا ملائمًا ، وبذلك يمكننا بيان ابرز دوافع تلك الظاهرة الارهابية بوجه خاص ، وكما يأتي :

1- **ضعف البنية المعلوماتية للشبكة العالمية وامكانية اختراقها :** وبذلك تتمكن المنظمات الارهابية من التسلل الى تلك الشبكات ؛ نتيجة اتسام تلك الشبكات بالانفتاح وانعدام القيود والحواجز الوقائية ، اضافة الى احتوائها على ثغرات تقنية لتسهيل الولوج والتوسع بالاستخدام .

2- **صعوبة اكتشاف واثبات جريمة الارهاب السيبراني :** العديد من الجرائم السيبرانية لا يعلم بوقوعها اصلًا ، وبالخصوص في مجال جرائم (القرصنة) ، مما يؤدي الى سهولة الحركة للإرهابي داخل المواقع قبيل تنفيذ جريمته ، بالإضافة الى ان صعوبة الاثبات تعتبر عامل مساعد على ارتكاب جريمته لأنها تعطي الارهابي السيبراني املًا في الافلات من العقاب .

3- **القُصور التنظيمي والقانوني وضعف جهة السيطرة والرقابة على الشبكات المعلوماتية العالمية :** ان محدودية المعاهدات والاتفاقيات الدولية بالإضافة الى التشريعات الوطنية بخصوص الارهاب السيبراني ، ادى الى انتشار هذه الظاهرة وتوسعها في بلدانٍ عدة ، بالإضافة الى عدم وجود جهة مركزية للتحكم بالشبكة العالمية للمعلومات والسيطرة على مُدخلاتها ومُخرجاتها ، اذ يستطيع اي شخص الولوج بالشبكة ووضع ما يرغب بها ، وهذا الاسلوب الأنجع والخيار الامثل للمنظمات والجماعات الارهابية .

4- **يُسر الاستخدام وقِلة التكاليف :** للقيام بالأعمال الارهابية ضمن الفضاء السيبراني ، لا يتطلب سوى حاسوب الكتروني متطور متصل بالشبكة المعلوماتية ، فهو لا يكلف وقتًا ولا جهدًا، مما يعد فرصة ثمينة للإرهابيين للوصول الى غاياتهم واهدافهم غير المشروعة من دون الحاجة الى مصادر تمويل كبيرة .

5- **انعدام الحدود الجغرافية وقلة مستوى المخاطرة :** نظرًا لامتياز الشبكة العالمية للمعلومات بانعدام الحدود المكانية ، يترتب على ذلك عدم معرفة الهوية الافتراضية للمهاجم في بيئته الافتراضية ، مما يوفر للتنظيمات الارهابية بيئة ملائمة لإخفاء هوياتهم خلف هوية مستعارة مزيفة او انتحال اسم شخصية اخرى ، وبالمحصلة تمكنهم من شن هجماتهم الارهابية دون التعرض للمخاطرة.[70]

6- **زيادة الاعتماد على تكنلوجيا المعلومات في مختلف ميادين الحياة المعاصرة :** بسبب كفاءتها العالية في معالجة البيانات ، حيث اعتمدت عليها في العديد من المرافق الحيوية للدول ، مثل المستشفيات ،المطارات ،البنوك وغيرها، الامر الذي يجعلها هدفًا جذابًا وسهلًا Soft Target للإرهاب السيبراني؛

نتيجة لما يخلفه الخلل بتلك النظم المعلوماتية من فوضى عارمة ، ولهذه المخاطر وجاهتها في نظر بعض البلدان ، حتى ان المخابرات الالمانية (BND) قد ابدت تخوفها من قيام الجماعات الارهابية من شن هجمات سيبرانية ضد الحواسيب الغربية باستخدام الانترنت . [71] ومما تقدم يتبين بان الارهاب السيبراني ليس وليد الصدفة ، فالظاهرة التي نحن بصددها ظاهرة مركبة ومعقدة واسبابها كثيرة ومتداخلة ؛ و لها دوافع واسباب متنوعة ومتعددة ، منها اسباب عامة كالدوافع الفكرية والاجتماعية والسياسية وغيرها ، واخرى خاصة (اسباب تكنلوجية) ؛ تلك الاسباب ترتبط بالفاعلين سواء كانوا افراد ام جماعات ام تنظيمات ، تحقيقًا لأهدافهم السياسية او الأيدولوجية .

المطلب الثالث/ مظاهر الإرهاب السيبراني وأركانه.

اصبح الإرهاب السيبراني هاجسًا مخيفًا للعالم أجمع ، والذي اصبح عرضةً لتلك الهجمات من قبل الارهابيين الذين يمارسون نشاطهم التخريبي من اي مكان على وجه المعمورة ، وتتفاقم تلك المخاطر يومًا بعد آخر ،لان التقنيات الحديثة غير قادرة على توفير الحماية للشعوب والمجتمعات من تلك العمليات الارهابية ذات الطابع السيبراني ؛ ولكون الارهاب السيبراني متعدد بصور ومظاهر عديدة ومتنوعة وكذا وسائله[72] التي تحركه لتنفيذ تلك الهجمات تحقيقًا لنشر مبادئهم وتصوراتهم ؛ اضافةً الى ان ظاهرة الارهاب السيبراني متحققة فيها جميع اركان الجريمة ، ولبيان ذلك سنتطرق في هذا المطلب الى مظاهر الإرهاب السيبراني في فرعٍ اولٍ ، وفي فرعٍ ثانٍ سنتطرق الى اركان الارهاب السيبراني ، وعلى النحو التالي .

الفرع الاول / مظاهر الارهاب السيبراني.

تتنوع اساليب ومظاهر الارهاب السيبراني حسب محتواها وطريقة استخدامها وغايات مستخدميها ، فتتنوع بين من يستهدف انظمة التقنية المعلوماتية وما يرتبط بها من برامجها وبنيتها التحتية ، وبين ما يجعل مزايا شبكة (الانترنت) وخدماته وسيلة لتنفيذ عملياته الارهابية في الواقع المادي ، فيكون الفضاء السيبراني وسيلة لترجمة النوايا الارهابية وتطبيقها في الواقع المادي الدموي ، دون ان تكون تلك المعلومات ساحة للفعل الاجرامي.[73] ولكون اغلب تلك الهجمات تشن بواسطة الانترنت فإنها تستمد قوتها من استخدامها لتكنلوجيا المعلومات والاتصالات والتي تكون محصلتها الاضرار بالمجتمعات الانسانية دون تمييزها لمجتمع محدد [74] ؛ لذا فمن الصعب تحديد مظاهر الارهاب السيبراني بجميع انواعه ، لذا سنعرض بعض انواعه وهي :

1- **التهديد السيبراني :** كالتهديد بقتل شخصية سياسية هامة او التهديد بتفجير اماكن حيوية واستراتيجية او اتلاف البنى التحتية المعلوماتية .

2- **تعطيل شبكات وانظمة المعلومات المرتبطة بالأنترنت** بواسطة توجيه ملايين الرسائل مما يكون عرضة لتوقف هذه الانظمة .

3- **تدمير انظمة المعلومات :** من خلال اختراق شبكة المعلومات الخاصة للأفراد او الشركات العالمية بهدف تخريب نقاط الاتصال Hotspot ، كالهجوم الذي حصل في استراليا عام 2000 حيث تم تدمير شبكة صرف صحي من قبل منظمة ارهابية من خلال هجوم سيبراني مما ادى الى اضرار صحية واقتصادية .

4- **التجسس :** هو التلصص او سرقة معلومات الأفراد و المؤسسات او المنظمات او الدول لأهداف وغايات سياسية واقتصادية وعسكرية .

اضافة لذلك هناك العديد من مظاهر الارهاب السيبراني والتي استطاعت المنظمات الارهابية من خلالها نشر فكرها المتطرف المنحرف والدعوة الى مبادئها وتعريض قطاعات الخدمة العامة الى الخطر ، وأهمها :

- **انشاء مواقع الكترونية** لإبراز قوتهم وللتعبئة الأيديولوجية وتجنيد ارهابيين جدد وجمع الاموال ؛ بالإضافة الى التدريب والتعليم وتحديد المواقع المستهدفة .
- **استهداف البنى التحتية** للاقتصاد ونظم الاتصالات والمعلومات ومحطات الطاقة والمياه والمواقع الحيوية العسكرية ، مثل منظومة الاسلحة الاستراتيجية ونظام الدفاع الجوي والصواريخ النووية.

- **التهديد والترويع السيبراني** : فبالإضافة الى تهديد رجال السياسة كذلك يتم ابتزاز رجال المال والاعمال لإخضاعهم لمطالبهم الارهابية . (75)

اما ابرز واهم استخدامات الارهابيون السيبرانيون للأنترنت كما يراها Barry Wellman فهي كما يلي:

1- **التنقيب عن المعلومات** وذلك من اجل الحصول على معلومات حساسة كالمنشآت النووية والمطارات والمعلومات الخاصة بمكافحة الارهاب ، وبذلك تكون 80% من الخزين المعلوماتي للمنظمات الارهابية معتمد على المواقع الالكترونية المتاحة .

2- **الاتصال بين افراد المنظمة** الارهابية والتنسيق فيما بينهم من خلال الانترنت .

3- **التعبئة والتجنيد للإرهابيين** من اجل بقاء وديمومة التنظيم الارهابي وجذب الشباب السذج من خلال وسائل التواصل .

4- **التعليم والتلقين الالكتروني** كشرح طرق صنع القنابل والاسلحة الكيميائية الفتاكة .

5- **التخطيط والتنسيق** من خلال شبكة الانترنت لشن هجمات ارهابية محددة ، كمثل التخطيط الذي حصل ابان احداث 11 سبتمبر 2001.

6- **الحصول على التمويل** من خلال استغلالهم لذوي القلوب الرحيمة ثم استجداؤهم لدفع التبرعات بطريقة دون ان يشعر بها المتبرع بانه يساعد تنظيمات ارهابية .

7- **مهاجمة المنظمات الارهابية الاخرى** : حيث يكون الانترنت حلبة الصراع بين تلك التنظيمات او بين افراد المنظمة الارهابية ذاتها . (76)

ونتيجة لذلك تزداد صعوبة توفير الامن بصورة كبيرة في عالم بات معتمدًا وبشكل متسارع على التكنلوجيا ، وقد برهنت التنظيمات الارهابية على درايتها وسرعة تمكنها في التعامل مع ابتكارات الاتصالات والتواصل المتجددة ، بدءًا من اركان الشبكة المظلمة (77) وصولًا الى منصات التواصل الاجتماعي المتاحة للجميع ، وبذلك تسمح تقنيات هذه الوسائل بالانتشار السريع لأيديولوجياتها وتكتيكاتها الاستراتيجية بوتيرة متصاعدة لم تشهدها العقود المنصرمة ، بالإضافة الى استغلال تلك التنظيمات لنظم التشفير لتعقد الجهود الرامية لمراقبتهم وتعقبهم . (78) ومما تقدم يتبين اعتماد الجماعات الارهابية اساليب جديدة لخلق الفوضى على الساحة الدولية ، حيث استفادت تلك الجماعات من عصر التقدم التكنلوجي لشن هجمات سيبرانية مركزة ، لاختراق النظم وقواعد البيانات الآمنة وكسب مصادر تمويل جديدة ، والاستفادة من وسائل التواصل البديلة ؛ محاولة استغلال ذلك التطور التكنلوجي في تطوير استراتيجياتها وتكتيكاتها وتقنياتها وعملياتها بالتكنلوجيا المتقاربة (79) ، بالإضافة الى استغلال الارهابيين وسائل التواصل الاجتماعي لتعزيز قدراتها في مجالات متنوعة بما في ذلك التجنيد والتدريب ونشر الدعاية ،مستغلة تلك الوسائل من الاتصال بجماهير عالمية تحقيقًا لأيديولوجيتها .

الفرع الثاني / أركان الإرهاب السيبراني.

لكي نعتبر السلوك الانساني جريمة بمعناها القانوني الجزائي ، لابد من توافر شروط وعناصر معينة لتحقق تلك الجريمة وقيامها وهذا ما يسمى باركان الجريمة ، وان تلك الاركان اما ان تكون عامة تندرج تحتها جميع الجرائم وبلا استثناء ، او ان تكون خاصة بجريمة محددة بذاتها دون غيرها . (80)

وفيما يخص موضوع بحثتنا الا وهو الارهاب السيبراني ، فقد ذهبت اتفاقية جنيف الاولى والخاصة بمكافحة ومعاقبة مرتكبي فعل الارهاب ، حيث نصت في الفقرة الثانية من المادة الاولى منها على انه " الافعال الاجرامية الموجهة ضد الدولة والتي يتمثل غرضها او طبيعتها في اشاعة الرعب لدى شخصيات معينة او جماعات من الاشخاص او لعامة الشعب " ، ومن هذا التعريف اشتقت معظم ادبيات اركان جريمة الارهاب الدولي ؛ لكون التعريف اعلاه اوردته اولى الاتفاقيات التي عُنيت بالإرهاب الدولي ، فكان له البادرة الاولى في إبرازه كجريمة دولية ذات أركان متعددة . (81) وبناءً على ما تقدم ، سنقسم اركان جريمة الاهاب السيبراني الى اربعة اركان كونها من الجرائم الدولية وهي ، الركن المادي ، الركن المعنوي ، الركن الدولي ، الركن الخاص ، وكما يلي :

اولًا : الركن المادي .

يتضمن الركن المادي للجريمة ماديات تلك الجريمة ، بعبارة اخرى كل ما يندرج تحت ما يسمى كيان الجريمة وذي طابع مادي يمكن ان تلمسه الحواس ؛ وللركن المادي اهمية كبيرة لضمان قيام الجريمة ، فلا وجود لجريمة دون ركنها المادي . وبغياب العنصر المادي ينتفي الضرر الواقع على الافراد و المجتمع ، ووفقًا لذلك يعتبر الركن المادي الدليل الاول على وجود الجريمة ويسهل بذلك تتبع الجريمة والضرر الناجم عنها ، وبناءً على ذلك تتكون عناصر الركن المادي متمثلة بالفعل والنتيجة والعلاقة السببية بينهما . [82] تتوافر اشكال وصور الركن المادي لجريمة الإرهاب السيبراني ، وذلك من خلال وقع الفعل بواسطة تقنية انظمة المعلومات والاتصالات ؛ وذلك من خلال :

1- استخدام قدرٍ كافٍ من التهديد بالعنف وان كان استخدام العنف التقليدي في ظل سلوك ضمن نطاق سيبراني معنويٍ يأتيه الفاعل يبقى خارج نطاق الدراسة ؛ ولكن ان امكن تصور مفهوم مستحدث للعنف المقصود ذو بعد معنوي ،بعبارة اخرى ان ينظر الى العنف كنتيجة لسلوك معنوي سيبراني ، وبناءً على ذلك يمكننا تصور عنف معنوي ظاهر بقبال قدرة الارهابي على استخدام تقنية المعلومات بقدر معتدٍ به لإيقاع الضرر المقصود ، اما بالنسبة للتهديد بالعنف فانه ممكن في ظل بيئة سيبرانية ، وهنا يتحقق السلوك الاجرامي ويصبح موكدًا في جريمة الارهاب السيبراني .

2- ان يؤدي استخدام العنف او التهديد به الى ارهاب المجتمع والافراد او تعريض حياتهم للخطر ، وبذلك تتحقق النتيجة الضارة من خلال حدوث تغيير في نطاقه المادي والمعنوي الذي اوجده الفعل ، فالنتيجة الضارة لجريمة الارهاب السيبراني تزداد خطورتها كلما ازداد استخدام الحواسيب والشبكة المعلوماتية العالمية مما يجعلها هدفًا يسيرًا ، فبدل استخدام المواد المفرقعة والمتفجرة تستطيع التنظيمات الارهابية بالضغط على زر في لوحة المفاتيح في جهاز الحاسوب لتحقيق آثار تدميرية تفوق تلك التي يمكن تحقيقها باستخدام المتفجرات ؛ وبذلك يمكن شن هجمات سيبرانية مدمرة كإغلاق المواقع الاستراتيجية والحيوية والحاق الشلل بمنظومة القيادة والسيطرة والاتصالات ، وكذلك قطع شبكات الاتصال بين القيادة المركزية والوحدات الفرعية ، او تعطيل انظمة الدفع الجوي ، او التحكم في خطوط الملاحة الجوية والبرية والبحرية ، او شل محطات امداد الطاقة ، كذلك اختراق الانظمة البنكية والمصرفية ، وغيرها من الاعمال الارهابية المشابهة .

3- ان العلاقة السببية هي صلة الوصل التي تربط السلوك الاجرامي بالنتيجة الضارة ، وبذلك يمكن اثبات ان ارتكاب الفعل المُجَرَم هو الذي ادى الى وقوع النتيجة الضارة . اما بالنسبة للإرهاب السيبراني تكون العلاقة السببية من خلال ارتباط السلوك غير المشروع والمتمثل باستخدام الحاسوب الآلي والانترنت بالنتيجة الضارة المترتبة على ذلك الفعل ، وجدير بالذكر ان الجاني قد يقوم احيانًا بتحقيق النتيجة من خلال السلوك الاجرامي ، كاستخدام شبكة المعلومات العالمية لتجنيد الارهابيين للقيام بتشكيل تنظيم مسلح ضد جهة معينة ونتيجة لهذا الفعل او السلوك تحقق الهدف المرجو منه ، فهنا تتحقق الجريمة التامة وإن لم يترتب على الفعل اي نتيجة ، ففي جميع الاحوال يكون الجاني مسؤولًا جنائيًا في كلا الحالتين سواء عن الجريمة او الشروع فيها .

ومن خلال ما تقدم يمكننا تصور السلوك المعنوي القادر على اظهار الارهاب السيبراني الى حيز الوجود كجرائم تستحق العقاب ومنها :

أ- استخدام العنف او التهديد به بغرض تعريض امن وسلامة المجتمع للخطر او الاضرار بالنظام العام ، وهنا لا موجب لتحقيق الضرر او الاخلال به بل يكفي مجرد احتمال وقوعه ، كتلاعب الفاعل بأنظمة السيطرة والتحكم بالإشارة المرورية او اختراق انظمة ضخ الماء للمنشآت الحيوية للدولة .

ب- استخدام العنف او التهديد به من اجل الاضرار بالبيئة او المرافق العامة للدولة ، كالتلاعب بأنظمة ضخ الماء والكهرباء .

ت- بالإضافة الى استخدام العنف او التهديد به من اجل تعطيل الدستور والقوانين النافذة ، وكذلك الاضرار بالموارد الوطنية ، او اختراق شبكات تقنية انظمة المعلومات او التشويش عليها . [83]

وكذلك تشمل الجرائم التي يتم ارتكابها بواسطة الالكترونيات ، جرائم تشمل استخدام الفايروسات لاختراق الاجهزة والمواقع المختلفة بغية الحصول على ربح ، وتعرف تلك الاعمال بالأعمال التحضيرية

وليس بالضرورة ان يكون لكل جريمة اعمال تحضيرية ، بينما من الصعوبة التمييز بين الاعمال التحضيرية والجريمة ذاتها ، فقد يكون العمل التحضيري هو ذات الجريمة خاصة بأعمال الحاسوب والانترنت . [84]

وبالمجمل يمكننا القول ، ان اي فعل سيبراني او التهديد به يؤدي الى تعريض امن وسلامة المجتمعات والشعوب للخطر او الاخلال بالنظام العام ، يمكن ان يكون ضمن نطاق جرائم الارهاب السيبراني.[85]

ثانيًا : الركن المعنوي.

يشمل الركن المعنوي العناصر النفسية للجريمة ، حيث ان الجريمة لا تعتبر كيان مادي مستقل بما يتكون منه القوام والأثر ؛ لذلك يعتبر الركن المعنوي ركنًا نفسيًا للجريمة ويشمل الاصول النفسية لماديات الجريمة والظروف النفسية المتعلقة بها . لذلك لم يهتم المشرع بالماديات الا في حالة صدورها عن شخص مسؤول جنائيًا عن افعاله ويمكن معاقبته ، لذلك اشترط المشرع ان يصدر فعل الجريمة عن انسان تنتمي له اجزاء من الجريمة ويحتويها في اصول نفسية متعلقة به ، وبذلك تمتد سيطرة فعل الجريمة الى كل اجزائها . واستنادًا لذلك فان الكن المعنوي للجريمة يشكل مبناه القوة النفسية الكامنة للجريمة التي تسيطر على الفاعل وتدفعه لارتكاب فعله غير المشروع ، وتشمل صورة الارادة بشكل عام مؤكدًا على ان تكون تلك الارادة ارادة جرمية لتنفيذ الفعل المخالف للقانون . وتعتبر جريمة الارهاب من الجرائم المقصودة ، حيث يتوجب وجود القصد الجرمي لتحقيق ركنها المادي من خلال عنصري العلم والارادة ، فيمكن تحقيق العلم من خلال ان يكون الجاني عالمًا بعناصر جريمته ، اما الارادة فتتحقق من خلال وجود ارادة الجاني لارتكاب الفعل وتنفيذ الجريمة حيث يكون الجاني متمتعًا بالحرية في القيام بالفعل الاجرامي او الامتناع عنه قبل تنفيذ الجريمة وبذلك يحدد ارتكاب الجريمة الركن المادي لها . [86] واذا كانت الجريمة بشكل عام تقوم على وجود الركن المعنوي المتمثل بعنصري العلم والارادة ، فان الارهاب السيبراني لا يكتفي فقط بالقصد العام ، انما يتوجب ثبوت القصد الخاص وهو علم ونية الفاعل وهو يستخدم تقنية نظم المعلومات والاتصالات وان يهدد بإيقاع احد الاغراض المستمدة من الجريمة ، فضلًا عن ذلك يتوجب ان يكون التكييف القانوني لجريمة الارهاب السيبراني ان يكون قائمًا على مبدأ شرعية الجرائم والعقوبات مع التأكيد على الالتزام بمبدأي الضرورة والتناسب عند التجريم والعقاب . [87]

ثالثًا : الركن الدولي .

لاستكمال جريمة الارهاب الدولي يشترط ان تكون افعال العنف المستخدمة بالعمليات الارهابية ، قد تمت بناءً على خطة ممنهجة من قبل دولة ضد دولة اخرى ، او على اقل تقدير بتشجيع ومباركة تلك الدولة او بناء على رضاها او دعمها او موافقتها ، فالجاني في هذه الجريمة يعمل باسم الدولة ولحسابها وليس بالضرورة ان يكون حاملًا لجنسيتها.[88] حيث ان وجود هذا الركن يثير المسؤولية الجنائية الدولية للأفراد في نطاق القانون الدولي الجنائي ، بالإضافة الى ان هذا الركن هو معيار التمييز بين الجريمة الدولية والجريمة الوطنية ؛ اذ بتوفر عنصري الركن الدولي ، وهما الاعتداء على مصلحة يحميها القانون الدولي ، وكون الفعل مرتكب من قبل دولة او تنظيم مسلح او من قبل افراد يعملون باسمها او لحسابها ، هو امر هام يساعد في كشف تلك الجرائم الدولية.[89]

رابعًا : الركن الخاص .

ان ابرز سمة من سمات الارهاب السيبراني الدولي المميز لها عن غيرها من الجرائم هو الركن الخاص ، حيث بمقتضاه يمكننا اعتبار ان الجريمة لا يمكن اكتمال وصفها دون ان تتميز بوسيلتها ، وهذه الوسيلة هي ارتكاب الجريمة بإحدى وسائل نظم المعلومات والاتصالات التكنلوجية الحديثة ، وبذلك يعتبر الحاسوب [90] وهو الوسيلة الاكثر ارتكابًا للجرائم من خلالها ، الا انها ليس الوسيلة الوحيدة ، اذ قد يرتكب بوسائل اخرى ، فالعبرة في الوسيلة هو كونها من وسائل التقنيات الحديثة حيث يتصور ارتكاب تلك الجرائم بواسطة الهواتف المحمولة الذكية ، خصوصًا ان تلك الهواتف تحمل نفس صفات الحواسيب الالكترونية من خلال تعاملها مع البرامج ، اضافة الى ان هناك اجهزة لديها شبكات توصيل خاصة بها مثل هواتف (BlackBerry) [91] وبذلك فان وسيلة هذه الجريمة لا تعدو كونها التقنية التكنلوجية الحديثة التي لجأ اليها الفاعل لارتكاب فعله الارهابي.[92] ونخلص الى ان جريمة الارهاب السيبراني الدولي هو

جريمة متحققة بتحقق أركانها السالف ذكرها ، وهي من الجرائم الدولية ، وبما ان جرائم الارهاب الدولي تمثل خرقًا للأمن والسلم الدوليين ؛ فكذا ان الارهاب السيبراني – بالتبعية – بجميع صوره يعد ماسًا بالأمن والسلم الدوليين . اما بالنسبة للعراق وبالنظر لكونه من اكثر الدول التي عانت من ويلات الارهاب وما خلفه من عنف وترويع بين اوساط المواطنين الابرياء مما حدا بالمشرع العراقي الى تشريع قانون مكافحة الارهاب رقم (13) لسنة 2005 [93] حيث نصت المادة (1/3) منه على اعتبار " كل فعل ذو دوافع ارهابية من شأنه تهديد الوحدة الوطنية ويمس امن الدولة واستقرارها او يضعف من قدرة الاجهزة الامنية في الدفاع والحفاظ على امن المواطنين وممتلكاتهم وحدود الدولة ومؤسساتها سواء بالاصطدام المسلح مع قوات الدولة او اي شكل من الاشكال التي تخرج عن حرية التعبير التي يكفلها القانون " وكما اشارت المادة (2/3) من قانون جهاز مكافحة الارهاب رقم (31) لسنة 2016 [94] على ان " تنفيذ العمليات الامنية والخطط الاستراتيجية فيما يتعلق بفعاليات مكافحة الارهاب وله في سبيل ذلك وفق القانون : .... ب – مراقبة الاتصالات ومواقع التواصل الاجتماعي والمواقع الالكترونية بناء على امر قضائي " ويتضح من ذلك ان المشرع العراقي منح الاجهزة الامنية سلطات واسعة تساعدهم في مواجهة جرائم الارهاب بصورة عامة ، والارهاب السيبراني بصورة خاصة ، واشترط صدور اذن بإجراء عمليات مراقبة شبكات الاتصالات والانترنت من السلطة القضائية مع توافر التدابير الاجرائية المصرح بها كضمانات اجرائية مناسبة في تلك العمليات . الا ان التساؤل الذي يثور هنا هو كيفية مواجهة البرامج الالكترونية التي تقوم بهجمات ارهابية ، وهي غالبًا ما تدار من خارج العراق ، خصوصً وان قانون مكافحة الارهاب رقم 13 لسنة 2005 وقانون جهاز مكافحة الارهاب رقم 31 لسنة 2016 لم ينصا صراحة او يتطرقا الى تلك الحالات وهذا دليل على وجود قصور تشريعي يجب معالجته ؛ كذلك في حالة القاء القبض على شخص يدير صفحة تابعة لتنظيم او جماعة ارهابية كيف يمكن اثبات تلك الجريمة ؟ حتى لو تم اثبات آثار الجريمة فان قانون اصول المحاكمات الجزائية رقم 23 لسنة 1971 المعدل[95] ، سيقف عائقًا امام اثبات الجريمة السيبرانية ، لان القضاء العراقي لا يأخذ بالأدلة الالكترونية وهذا ما اكدته المادة 213 من ذات القانون ، وهذا يدل ايضًا على وجود قصور ينبغي معالجته .

اما بخصوص عدم تشريع قانون الجرائم المعلوماتية والمقترح من فترة ليست بالقليلة ، نلاحظ ان سبب التأخير بتشريع القانون ، هو ان فقرات القانون المقترح وحسب ما نعتقد بانه تم صياغتها من خبراء القانون فقط دون الاستعانة بخبراء الامن المعلوماتي او الامن السيبراني ، وبالتالي نلاحظ ان روح الفقرات فيه هي قانونية عقابية اكثر مما هي تركز على التقنية وامكانياتها وتأثيراتها وصورها ؛ اما اهم المعالجات المقترحة لمواجهة الجريمة السيبرانية وبالأخص الارهاب السيبراني من وجهة نظرنا ، فهي تشريع القانون بصورة عاجلة والتركيز على الثقافة الالكترونية ، وبناء بوابات نفاذ وطنية آمنة ، اضافة الى الاستعانة بتجارب الدول في هذا المجال .

الخـــاتـــمة .

اولًا / النتائج .

1. لا يوجد تعريف دولي موحد للإرهاب بصفة عامة ، فضلًا عن الارهاب السيبراني على وجه الخصوص ، وذلك بسبب تنوع اشكاله ومظاهرة وتعدد انماطه واساليبه ، واختلاف وجهات النظر الدولية اليه .
2. بسبب عدم توصل الفقه الى اتفاق موحد للإرهاب السيبراني ، ادى ذلك الى تباين المفاهيم لذلك المصطلح ، هذا من جانب ؛ ومن جانب آخر كان له الفضل الاكبر (اي الفقه) في تعريف الارهاب السيبراني خاصةً في ضل تأخر الاجماع الدولي على تعريفه .
3. الارهاب السيبراني هو احد صور الارهاب المعاصرة ، والذي تقوم به التنظيمات الارهابية والذي يبغي تحقيق اهداف الارهاب التقليدي وذلك باستخدام تكنلوجيا المعلومات .
4. ان الارهاب السيبراني يختلف عن الحرب السيبرانية من حيث افتقاده بصورة ضرورية الى عنصر المشروعية وارتكابه يكون من قبل افراد ، جمعات، هيئات ، دون مستوى الدول ؛ وفي ذات الوقت تكون الحرب السيبرانية التي تخوضها الدول في الفضاء السيبراني مشروعة، ان هدف الحرب السيبرانية

يختلف عن اهداف الارهاب السيبراني ، لان نتيجة الهجوم هي من تحدد من يقف وراءه ، حيث ان الحرب السيبراني تقوم به دولة لتحقيق هدف (سياسي او عسكري) من اجل مقتضيات الامن القومي ، بينما الاهاب السيبراني يقوم به الافراد او الجماعات والتنظيمات الارهابية لتحقيق اهدافهم السياسية والأيديولوجية المتطرفة ، وبالمحصلة فان الهجمات السيبرانية تشمل كل من الحرب السيبرانية وكذلك الارهاب السيبراني ، الا انها تختلف فقط بالأغراض الاساسية لتلك الهجمات.

5. ان هدف الجريمة السيبرانية يختلف عن اهداف الهجمات الارهابية السيبرانية ، لان نتيجة الهجوم هي من تحدد من يقف وراءه ، بينما الجرائم السيبرانية تكون بعيدة عن سياسات الدولة ويستبعد ان تكون الدولة هي التي تقوم بالهجوم ، بل يكون اشخاص او مجاميع (Hackers) هي من يقوم بتنفيذ تلك الجرائم السيبرانية ، اذ يحتمل ان يكون الهدف (مادي او اقتصادي) ؛ لذلك تكون الهجمات السيبرانية الارهابية من اختصاص القانون الدولي العام ، لأنه يمثل خرق لسيادة الدول ، بينما تكون الجريمة السيبرانية ضمن اختصاص القانون الوطني وفقًا لمبدأ اقليمية القانون؛ وفي جميع صور تلك الهجمات سواء كانت جريمة او حرب او ارهاب سيبراني ، تتحقق المسؤولية الدولية للدول عن اعمال مواطنيها ، بالإضافة الى المسؤولية الجنائية الدولية للأفراد .

6. ان الارهاب السيبراني يتطور بتطور الاحداث ، و نتيجة تلك التطورات التقنية الكبيرة والطفرات المتسارعة في عالم الاتصالات والمعلوماتية ، والتي يطلق عليها ثورة تكنلوجيا المعلومات والاتصالات ، حيث اصبح من المستحيل على جميع الافراد والدول العيش بمعزل عن تلك التطورات التقنية ؛ وبالمقابل فان هناك مخاطر من استخدام تلك التقنيات من قبل الارهابيين لتحقيق اهدافهم الايديولوجية ، اذ بدأ يستهدف جميع القطاعات الحيوية والامنية والصحية وغيرها ، سواء من خلال جمع المعلومات وسرقة البيانات ام من خلال التدمير المباشر للبيانات المهمة المخزنة في السحابة الالكترونية لتلك المنشآت ؛ لذا يجب تعاضد جهود الافراد والدول والمنظمات المختلفة لحماية تلك المؤسسات والافراد من الهجمات السيبرانية التي ينفذها المتطرفين ، الامر الذي يستعدي التدخل الفوري دوليًا لوضع حد للإرهاب السيبراني .

7. ان الارهاب السيبراني ليس وليد الصدفة ، فالظاهرة التي نحن بصددها ظاهرة مركبة ومعقدة واسبابها كثيرة ومتداخلة ؛ و لها دوافع واسباب متنوعة ومتعددة ، منها اسباب عامة كالدوافع الفكرية والاجتماعية والسياسية وغيرها ، واخرى خاصة (اسباب تكنلوجية) ؛ تلك الاسباب ترتبط بالفاعلين سواء كانوا افراد ام جماعات ام تنظيمات ، تحقيقًا لأهدافهم السياسية او الأيدولوجية .

8. اعتماد الجماعات الارهابية اساليب جديدة لخلق الفوضى على الساحة الدولية ، حيث استفادت تلك الجماعات من عصر التقدم التكنلوجي لشن هجمات سيبرانية مركزة ، لاختراق النظم وقواعد البيانات الآمنة وكسب مصادر تمويل جديدة ، والاستفادة من وسائل التواصل البديلة ؛ محاولة استغلال ذلك التطور التكنلوجي في تطوير استراتيجياتها وتكتيكاتها وتقنياتها وعملياتها بالتكنلوجيا المتقاربة ، بالإضافة الى استغلال الارهابيين وسائل التواصل الاجتماعي لتعزيز قدراتها في مجالات متنوعة بما في ذلك التجنيد والتدريب ونشر الدعاية ،مستغلة تلك الوسائل من الاتصال بجماهير عالمية تحقيقًا لأيديولوجيتها .

9. ان جريمة الارهاب السيبراني الدولي هو جريمة متحققة بتحقق أركانها السالف ذكرها ، وهي من الجرائم الدولية ، وبما ان جرائم الارهاب الدولي تمثل خرقًا للأمن والسلم الدوليين ؛ فكذا ان الارهاب السيبراني – بالتبعية – بجميع صوره يعد ماسًا بالأمن والسلم الدوليين.

10. يتميز الارهاب السيبراني بالعديد من الخصائص والسمات التي يختلف بها عن الجرائم الاخرى وتحول دون اختلاطه بالإرهاب التقليدي.

ثانيًا / التوصيات.

1- التوصية للمجتمع الدولي باعتماد تعريف محدد للإرهاب السيبراني ؛ ونقترح التعريف التالي : الإرهاب السيبراني " هجمات غير مشروعة بدوافع سياسية او أيدولوجية او التهديد بتلك الهجمات على شبكات الحواسيب الآلية وموارد تخزينها ، توجه ضد مصالح الجماعات او الدول والمجتمع الدولي ؛

لتحقيق حالة من الاضطراب والخوف والذعر وتقويض الثقة ؛ لإكراه تلك الحكومات او المجتمع المستهدف للاستجابة لمنفذي تلك الهجمات تحقيقًا لغاياتهم ".

2- نقترح انشاء اتفاقية دولية تتعلق بالجرائم ضمن الفضاء السيبراني او اعتماد اتفاقية اوربا المتعلقة بالجرائم ضمن الفضاء السيبراني (اتفاقية بودابست لعام 2001) من قبل منظمة الامم المتحدة ، كاتفاقية دولية شارعة ودعوة الدول للانضمام اليها ومنها العراق .

3- دعوة المشرع العراقي الى تحديث التشريعات وبما يتلاءم مع التطور التكنلوجي والتقني المتسارع ، وكذلك حثه على الاسراع بتشريع قانون جرائم المعلوماتية العراقي ، وتنظيم استخدام وسائل التواصل الاجتماعي .

4- انشاء هيئة عليا مختصة بالأمن السيبراني ، وتهيئة البنى التحتية واعداد الكوادر الفنية للمباشرة بالتحول الرقمي والاتمتة الالكترونية ، وتأمينها من الاختراقات السيبرانية ، وموائمتها مع التشريعات النافذة .

5- انشاء اكاديمية للأمن السيبراني ، ترتبط بوزارة الداخلية ، تعنى بالأمن والاستخبارات والامن السيبراني ، وتشجع البحث العلمي في مجال تكنلوجيا المعلومات .

الهوامش .

(2)Chuipka,A. (2016),The Strategies of Cyber terrorism –is Cyber terrorism an Affective means to Achieving the Goals if Terrorists? Affaires publiques at internationals- memories / Public and International Affairs- Research papers. P5-6.Retrieved from https://ruor.uottawa.ca/handle/10393/35695,Last visite4/12/2022.

(2) عمر عباس خضير العبيدي ، الارهاب الالكتروني في نطاق القانون الدولي ، ط1 ، المركز العربي للنشر والتوزيع ، القاهرة ، 2021، ص22 .

(3) د. هالة احمد الرشيدي ، الارهاب السيبراني ماهيته وجهود مكافحته في ضوء التشريعات والقوانين الوطنية والدولية، ط1، دار النهضة العربية ، 2021 ، ص 20.

(4) ابن منظور ، معجم لسان العرب ، دار المعارف ، القاهرة ، بلا سنة طبع ، باب الراء ، مادة رهب ، ص 1748.

(5) د. روحي البعلبكي ، قاموس المورد، ط7، دار العلم للملايين ، بيروت ، ، 1995 ، ص77.

(7)Norbert Wiener,Cybernetic or control communication in the animal and the machine,M.I.T,Press,Second Edition,Cambridge,Massachusetts.1948.

(4)Julia Cresswell, “Oxford Dictionary of word Orgins :Cybernetics” ,Oxford Reference Online, Oxford University Press,2010.

(8) د. روحي البعلبكي ، قاموس المورد ، مصدر سابق ، ص777.

(9) محمد دهام مسعف ، حق الدفاع الشرعي ضد الهجمات السيبرانية ، رسالة ماجستير ، كلية القانون ، جامعة بغداد ، 2022، ص 9_10.

(10) د.احمد عبيس نعمة الفتلاوي ، الهجمات السيبرانية ، دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر ، منشورات زين الحقوقية ، 2018 ، ص 11_12.

(11) د. منتصر سعيد حمودة ، الارهاب الدولي - جوانبه القانونية - وسائل مكافحته في القانون الدولي العام والفقه الاسلامي ، ط1 ،الاسكندرية ، 2008 ، ص 12.

(12) د. هالة احمد الرشيدي ، ، مصدر سابق ، ص 20-21.

(13) د. إمام حسنين عطا ، الارهاب والبنيان القانوني للجريمة ، دار المطبوعات الجامعية ، بيروت ، 2004، ص 95.

(14) د. امل يازجي و د. محمد عزيز شكري ، الارهاب الدوي والنظام الدولي ، دار الفكر المعاصر ، بيروت ، 2002، ص 93.

(15)د. خالد حسن احمد لطفي ،الارهاب الالكتروني افة العصر الحديث والآليات القانونية لمعالجته، ط1 ، دار الفكر الجامعي ، الاسكندرية ، 2019 ، ص 31.

(16) د. ثامر ابراهيم ، مفهوم الارهاب في القانون الدولي ، دار حوران للطباعة ، دمشق ، 1998 ، ص 55.

(17) د. علي حسين الخلف و د. سلطان الشاوي ، المبادئ العامة في قانون العقوبات المكتبة القانونية ، بغداد، 1982 ، ص 298.

([18]) د. خالد حسن احمد لطفي ، مصدر سابق ، ص 48-49.
([19]) د. صلاح مهدي هادي الشمري و د. زيد محمد علي اسماعيل ، الامن السيبراني كمرتكز جديد في الساحة العراقية ، مجلة قضايا سياسية ، كلية العلوم السياسية ، جامعة النهرين ، العدد62، السنة الثانية عشر ، 2020 ، ص 281.
([20]) احمد ناصر ابو سعود ، الارهاب الالكتروني ، بحث منشور على موقع الموسوعة السياسية ، والمتاح على الرابط التالي : https://political-encyclopedia.org/dictionary/%D8%A7%D9%84%D8%A5%D8%B1%D9%87%D8%A7%D8%A8%20%D8%A7%D9%84%D8%A7%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A تاريخ الزيارة 2100 في 2022/12/4.
([21]) اسراء طارق جواد كاظم الجابري ، جريمة الارهاب الالكتروني ، دراسة مقارنة ، رسالة ماجستير ، كلية الحقوق ، جامعة النهرين ، 2012، ص 23.
([22]) مقالة منشورة في مجلة الاتجاهات الاميركية بتاريخ 2003/10/11 للكاتب كيفين كولمان .
([23]) علي مطر ، الارهاب الالكتروني – نوع جديد لم يتم التعامل معه بعد – مقال منشور في موقع انباء الاخبارية ، متاح على الرابط التالي : https://www.inbaa.com/ ، تاريخ الزيارة – ساعة 2100 ، 2022/12/3.
([24])ينظر اتفاقية مجلس اوربا المتعلقة بالجريمة الإلكترونية ، مجموعة المعاهدات الاوربية ، رقم 185 ، بودابست عام 2001.
([26])FBI,2002.code of Federal.Regulations.28 CFR. Section 0.85 on Judicial Administration. July 2001.

([26]) هه لاله محمد تقي محمد ، التعاون الدولي في مواجهة جريمة الارهاب الإلكتروني ، بحث منشور في مجلة مركز الدراسات القانونية والسياسية ، كلية القانون ، جامعة السليمانية ، السنة السادسة ، العدد (11) ، 2018،ص 14.
([27]) اعتمد الباحث بتعريف الارهاب السيبراني على عدة منظورات اهمها : الهدف ، الدافع ، طريقة الهجوم ، المجال ، فعل الجاني ، والاثر .
([28]) د. حسن بن احمد الشهري ، الارهاب الالكتروني – حرب الشبكات - ، بحث منشور في المجلة العربية الدولية للمعلوماتية ، المجلد الرابع ، العدد الثامن ، 2015 ،ص 13-14 ؛ كذلك ينظر ،عبد الله عبد العزيز فهد العجلان ، الارهاب الالكتروني في عصر المعلومات ، بحث مقدم الى المؤتمر الدولي الاول حول " حماية امن المعلومات والخصوصية في قانون الانترنت" والمنعقد بالقاهرة في المدة من 2 - 4 يونيو ، 2008، ص 13، متاح على الرابط التالي : http://www.shaimaaatalla.com/vb/showthread.php?t=3937 ، كذلك ينظر ، د. هالة احمد الرشيدي ، الارهاب السيبراني ، مصدر سابق ، ص 28-30.
([29]) زهراء عماد محمد كلنتر ، المسؤولية الدولية الناشئة عن الهجمات السيبرانية ، رسالة ماجستير ، كلية القانون ، جامعة الكوفة ، 2016 ، ص 14-15.
([30]) د. بشار مكي العيساوي ، استاذ امن المعلومات والامن السيبراني ، الجامعة المستنصرية ، مقابلة ميدانية تمت مع الدكتور المذكور اعلاه ، بتاريخ 2023/1/12.
([31]) روان بنت عطية الله الصحفي ، الجرائم السيبرانية ، بحث منشور في المجلة الالكترونية الشاملة متعددة التخصصات ، العدد الرابع والعشرون ، شهر5 ، 2020 ، ص 17-21.
([32]) اسراء طارق جواد كاظم الجابري ، جريمة الارهاب الالكتروني ، مصدر سابق ، ص 12-16.
([33]) د. كامل سعيد ، جرائم الكومبيوتر والجرائم الاخرى في مجال تكنلوجيا المعلومات ، بحث مقدم الى المؤتمر السادس للجمعية المصرية للقانون الجنائي ،دار النهضة العربية ، القاهرة ، 1993 ، ص 516.
([34]) د. عمر محمد ابو بكر يونس ، الجرائم الناشئة عن الانترنت ، دار النهضة العربية ، القاهرة ، 2004، ص 158.
([35]) يرى الاستاذ الدكتور احمد عبيس الفتلاوي ، ان مصطلح الهجمات السيبرانية هو الاصوب من اصطلاح الحرب السيبرانية ؛ كونه غير محبذ في العصر الحالي على مستوى التنظيم الدولي ، لاسيما ان عدة تصرفات دولية اشارت الى اصطلاح الهجمات واعتبرته بمثابة التصرف ، الذي يرتكز في الذهن اثناء النزاعات المسلحة طبقًا للقانون الدولي الانساني ؛ المصدر ، د.احمد عبيس نعمة الفتلاوي ، الهجمات السيبرانية : مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر ، مجلة المحقق الحلي للعلوم القانونية والسياسية ، كلية القانون ، جامعة بابل ، العدد الرابع ، السنة الثامنة، 2016 ، ص 615.
([36]) د. بشار مكي العيساوي ، استاذ امن المعلومات والامن السيبراني ، الجامعة المستنصرية ،مقابلة ميدانية ، مصدر سابق .
([37]) د. هالة احمد الرشيدي ، الارهاب السيبراني ماهيته وجهود مكافحته في ضوء التشريعات والقوانين الوطنية والدولية ، مصدر سابق ، ص 40.

([38]) سراب ثامر احمد ، الهجمات على شبكات الحاسوب في القانون الدولي الانساني ، اطروحة دكتوراه ، كلية الحقوق ، جامعة النهرين ، 2015 ، ص55 و ص 63 .
([39]) كاميران عزيز حسن ، الجهود الدولية في مواجهة الجرائم السيبرانية ، رسالة ماجستير ، كلية القانون والعلوم السياسية ، الجامعة العراقية ، 2019، ، ص 64.
(41) Paulo shakarian and others, introduction to cyber-Warfare, A Multidisciplinary Approach, , published by Elsevier, Waltham , USA, 2013,P24.
(42) Solange Ghernaouti, Cyber power Crime, Conflict and security in Cyberspace published by Epft Press, Switzerland, 2013,p40.
([42]) د. سامر مؤيد عبد اللطيف ، الحرب في الفضاء الرقمي ، رؤية مستقبلية ، بحث منشور في مجلة رسالة الحقوق ، كلية القانون ، جامعة كربلاء ، السنة السابعة ، العدد الثاني ، 2015 ، ص 101.
([43]) د.احمد عبيس نعمة الفتلاوي ، الهجمات السيبرانية : مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر ، مصدر سابق ، ص 629-640.

(45) Tang Lan, Zhang Xin, Harry D. Raduege, Jr., Dmitry I. Grigoriev, Pavan Duggal, and ،Stein Schjølberg,"Global Cyber Deterrence Views from China, the U.S., Russia, India ،and Norway", The EastWest Institute, Printed in the United States, 2010,p5.
([45]) د. سامر مؤيد عبد اللطيف ، الحرب في الفضاء الرقمي ،مصدر سابق ، ص 80.
([46]) علي عدنان الفيل ، الاجرام الالكتروني ، كلية الحقوق ، جامعة الموصل ، منشورات زين الحقوقية ، 2011، ص 49-50 .
([47]) عمر عباس خضير العبيدي، مصدر سابق ، ص 32.
([48]) حرب المعلومات: هي الاعمال التي تتخذ لإحراز التفوق المعلوماتي عن طريق التأثير على معلومات الخصم والعمليات المبينة على هذه المعلومات ونظم المعلومات وفي نفس الوقت حماية ورفع فعالية المعلومات والعمليات المبينة عليها ونظم المعلومات الخاصة بالمهاجم ؛ وهذا ما ذهبت اليه الاستراتيجية القومية العسكرية الامريكية ، وتنقسم حرب المعلومات إلى سبعة أقسام: حرب القيادة والسيطرة، الحرب الاستخبارية، الحرب الإلكترونية، حرب العمليات النفسية، حرب قراصنة المعلومات، حرب المعلومات الاقتصادية، حرب المعلومات الافتراضية. للاستزادة ، ينظر ، سراب ثامر احمد ، الهجمات على شبكات الحاسوب في القانون الدولي الانساني ، مصدر سابق ، ص55 .
([49]) عمر عباس خضير العبيدي ، مصدر سابق ، ص 29.
([50])القاضي الدكتور احمد يوسف جمعة ، الارهاب السيبراني والعملات الافتراضية والتجسس الالكتروني ، دراسة تحليلية تتناول استخدامات الارهاب للفضاء السيبراني ، ط1 ، دار الاهرام للنشر والتوزيع والاصدارات القانونية ، المنصورة ، 2022 ، ص 20.
([51]) يشير مفهوم الذئاب المنفردة الى المجرم الغير مرتبط بعصابة والذي يحمل افكارًا متطرفة تقوده للقيام بعمليات ارهابية منفردة ، ينظر ، د. رمزي عودة ، التعاون الدولي في مكافحة تجنيد "الذئاب المنفردة" في مواقع التواصل الاجتماعي ، بحث منشور في مجلة جامعة الانبار للعلوم الانسانية ، العدد2 ، المجلد2 ، حزيران 2020، ص 6.
([52]) د. محمد الجندي ، متاهة الارهاب – الشرق الاوسط من الخلافة الى الارهاب في الفضاء الالكتروني ، ط1 ، مجموعة النيل العربية ، 2020، ص74.
([53]) بالطبع الباحث لا يقصد بكلمة " اسلامية " ان تلك الكيانات والجماعات الارهابية تنفذ الفكر الاسلامي القويم والنهج المحمدي الاصيل الرافض للعنف بشتى صوره واشكاله ، ولكن جاءت الكلمة لتمييزها عن غيرها من الجماعات ، ولأن ذلك الوصف هو ما تشتهر به اعلاميًا وبين العوام .
([54]) عبد الله عزام ، هو احد قادة الجهاد الافغاني ضد الاتحاد السوفيتي واحد استاذة اسامة بن لادن ، كانت له جولات في مساجد اوربا والولايات المتحدة الاميركية ، لكسب التأييد والمعونة لتنظيمهم .
([55]) يقول الصحفي الباكستاني " حامد مير " : انه عندما غزت الولايات المتحدة الاميركية افغانستان عام 2001 وضربت معاقل القاعدة رأيت كل قيادي من اعضاء التنظيم يهرب ومعه جهاز كومبيوتر محمول وكلاشنكوف ، وهذا ما يؤكد استخدام تنظيم القاعدة للإنترنت قبل هجمات سبتمبر 2001 .
([56]) من الذين اسهموا في تصميم تلك الشبكات ، المدعو ابو انس الليبي و نزيه عبد الحميد الرقيعي ، ينظر د. محمد الجندي ، متاهة الارهاب ، مصدر سابق ، ص 77.
([57]) القاضي الدكتور .احمد يوسف جمعة ، مصدر سابق ، ص 23-25.
([58]) د. سليماني مباركة ، الارهاب الالكتروني وطرق مكافحته ، بحث منشور في مجلة القانون والعلوم السياسية ، جامعة عباس لغرور خنشلة ،الجزائر، العدد 8، ج1 ، 2017 ، ص 343.

([59]) يمكن رصد اشكال الارهاب الجديد على النحو التالي : الارهاب الكيمياوي ، الارهاب البيولوجي ، الارهاب النووي ، الارهاب السيبراني .
([60]) د. خالد محمد طاهر شبر ، الارهاب والنظام السياسي الدولي ، بعد احداث 11 ايلول / سبتمبر 2001(رؤية مستقبلية) ط1 ، مركز الرافدين للحوار ، ، بيروت/النجف الاشرف ، 2022، ص 34.
([61]) الاتحاد الدولي للاتصالات ، اخبار الامم المتحدة ، اهداف التنمية المستدامة ، 30 نوفمبر 2021، متاح على الرابط : https://news.un.org تاريخ الزيارة 2022/12/5.
([62]) عمر عباس خضير العبيدي ، مصدر سابق ، ص 30-31.
([63]) د. حسن بن احمد الشهري ، مصدر سابق ، ص 10-11.
([64]) القاضي الدكتور احمد يوسف جمعة ، مصدر سابق، ص 65.
([65]) زين العابدين عواد كاظم الكردي ، جرائم الارهاب المعلوماتي وبعض تطبيقاته في القانون العراقي ، دراسة مقارنة ، رسالة ماجستير ، كلية القانون ، جامعة بابل ، 2008 ، ص 72-77.
([66])عمر عباس خضير العبيدي ، مصدر سابق، ص39.
([67]) د. حسن بن احمد الشهري ، مصدر سابق، ص 14.
([68]) د. خالد حسن احمد لطفي ، مصدر سابق ، ص 59 .
([69]) د. خالد حسن احمد لطفي ، المصدر السابق ، ص 41.
([70]) د. عبير احمد محمد الحميري واحمد شكران بن بحر الدين و نور زاهدي عثمان ، التنظيم القانوني لجرائم الارهاب الالكتروني ، بحث منشور في مجلة الشريعة والقانون ، كلية الشريعة والقانون ، جامعة العلوم الاسلامية في ماليزيا ،2020، ص 758-760 ؛ كذلك ينظر عمر عباس خضير العبيدي ، الارهاب الالكتروني في نطاق القانون الدولي ، مصدر سابق ، ص 40-41.
([71]) د. هالة احمد الرشيدي ، مصدر سابق ، ص 34.
([72]) وسائل الارهاب السيبراني ، تتعدد الى 1- البريد الالكتروني 2- انشاء موقع الكترونية 3- اختراق وتدمير المواقع الاخرى ، وتقسم وسائل الاختراق الى أ- فيروسات الكومبيوتر ب- الديدان جـ- احصنة طروادة د- الابواب الخلفية هـ- الاختناق المروري الالكتروني و-القصف الالكتروني ي- الهاكرز ، 4- دور مواقع التواصل الاجتماعي في دعم الارهاب الالكتروني ، وتشمل مواقع مغلقة واخرى مفتوحة ، وتقسم المواقع المفتوحة الى وسائل التواصل الاجتماعي وتشمل ، أ- الفيس بوك ب- تويتر جـ- اليوتيوب ؛ ينظر د. خالد حسن احمد لطفي ، الارهاب الالكتروني ، مصدر سابق ، ص 60-73.
([73]) د. سامر مؤيد عبد اللطيف وآخرون ، دور المنظمات الدولية في مكافحة الارهاب الرقمي ، مصدر سابق ،ص50.
([74]) د. حسن بن احمد الشهري ، مصدر سابق ، ص 15.
([75]) د. حسن بن احمد الشهري ، المصدر السابق ، ص 15-16.
([76]) د. حسن بن احمد الشهري -، المصدر السابق ، ص 16.
([77]) وتسمى ايضا باسم شبكة الويب المظلمة Dark Net او الويب المظلم او الانترنت المظلم وهو مصطلح يشير الى محتوى مشفر عبر الانترنت غير مفهرس في محركات البحث التقليدية ، تعد شبكة الويب المظلمة جزءً من شبكة الويب العميقة Deep Web وهي عبارة عن مجموعة اكبر من المحتوى الذي لا يظهر من خلال تصفح الانترنت العادي فيجب وجود متصفح معين مثل Tor للوصول الى مواقع الويب المظلمة ، اصبحت شبكة الويب المظلمة سوقا عبر الانترنت للسلع غير القانونية وتم تطبيق العديد من الابتكارات من البائعين الشرعيين على الانترنت مثل Amazon وE Bay مثل آراء العملاء وتصنيفات البائعين لتسهي عملية بيع المخدرات والاسلحة والمعلومات المسروقة واكثر من ذلك عامل الجذب الرئيس لشبكة الويب المظلمة هو القدرة على الحفاظ على اخفاء الهوية اثناء اجراء الاعمال التجارية ، يمكن ان تكون النوايا نبيلة كما هو الحال مع الصحفيين الذين يجرون مقابلات مع اشخاص يعيشون في بلدان قمعية حيث تكون الاتصالات مراقبة ، الجانب الاخر الاقل شيوعا للشبكة المجهولة الهوية هو تجارة المخدرات والاسلحة وحتى المجالات الاكثر ازعاجا مثل ادوات القرصنة القوية وتجارة المواد الاباحية للأطفال ، وتحتوي الشبكة على منصات رسائل مجهولة الهوية واسواق الكترونية وتبادلات للبيانات المالية والخاصة المسروقة واكثر من ذلك ، وتجرى المعاملات في هذا الاقتصاد الخفي عادة بعملة Bitcoins وتشحن السلع المادية بطريقة تحمي كلا من المشتري والبائع من التعقب من قبل المكلفين بتطبيق القانون ، المصدر : https://www.meemapps.com/term/dark-web
([78]) المنهج المرجعي لمكافحة الارهاب ، حلف الناتو ، مايو/ايار 2020 ، ص 5 .
([79])التكنولوجيات المتقاربة تعكس مزيجًا من اثنين أو أكثر من التقنيات المتقدمة لإنشاء تكنولوجيا أكثر تقدمًا ذات أهمية استراتيجية أكبر. مثال على ذلك قد يكون المزج الصريح لعلم أمن المعلومات مع الروبوتات والذكاء الاصطناعي لإنتاج نوع جديد من الروبوت المحاربة. وتشمل التكنولوجيات ذات الاستخدام المزدوج المتقدمة الأخرى علم الروبوتات وعلم

الجينوم، وتكنولوجيا النانو والتقنيات العصبية والضوئيات واستخدام أشعة الليزر. فهذه التكنولوجيات لم تعد مقتصرة على عالم الخيال العلمي، المصدر : https://www.sasapost.com/convergent-technologies/
([80]) د. علي حسين الخلف و د. سلطان عبد القادر الشاوي ، مصدر سابق ، ص 137.
([81]) د. خالد حسن احمد لطفي ، مصدر سابق ، ص 35.
([82]) د. عبير احمد محمد الحميري واحمد شكران بن بحر الدين و نور زاهدي عثمان ، مصدر سابق ، ص 764.
([83]) د. هادي طلال هادي ، المواجهة القانونية والامنية لجرائم الارهاب الالكتروني ، بحث منشور في مجلة الجامعة العراقية ، العدد 45 ،ج2، 2019 ، ص278-288.
([84]) د. عبير احمد محمد الحميري واحمد شكران بن بحر الدين و نور زاهدي عثمان ، ، مصدر سابق ، ص 765.
([85]) د. هادي طلال هادي ، المواجهة القانونية والامنية لجرائم الارهاب الالكتروني ، مصدر سابق ، ص278-288.
([86])د. عبير احمد محمد الحميري واحمد شكران بن بحر الدين و نور زاهدي عثمان ، التنظيم القانوني لجرائم الارهاب الالكتروني ، مصدر سابق ، ص 767.
([87]) د. هادي طلال هادي ، مصدر سابق ، ص288.
([88]) د. خالد حسن احمد لطفي ، مصدر سابق ، ص 36.
([89])عمر عباس خضير العبيدي ، الارهاب الالكتروني في نطاق القانون الدولي ، مصدر سابق ، ص 56-57.
([90]) الحاسوب : جهاز متعدد الاغراض يمكن استغلاله لتنفيذ عمل معين ، من خلال امداده بالبرامج الذي يقوم بتنفيذ هذا العمل .
([91]) بلاك بيري (بالإنجليزية: BlackBerry) ويعني (التوت الأسود)، هو نوع من الهواتف الذكية التي تدعم خدمة البريد الإلكتروني، تم تطويره من قبل شركة ريسرش إن موشن الكندية. يتميز البلاكبيري بشكل رئيسي بقدرته على استقبال وإرسال البريد الإلكتروني حيثما توفرت شبكة اتصالات خلوية لعدد كبير من شركات الاتصالات حول العالم.
([92]) د. صلاح هادي الفتلاوي ، جريمة الارهاب الالكتروني ، بحث منشور في مجلة القانون للدراسات والبحوث القانونية ، كلية القانون ، جامعة ذي قار ، العدد 13 ، 2016، ص 608.
([93]) ينظر قانون مكافحة الارهاب رقم 13 لسنة 2005 ، المصدر الوقائع العراقية ، العدد 4009 ،لسنة 2005.
([94]) ينظر قانون جهاز مكافحة الارهاب رقم 31 لسنة 2016 ، المصدر الوقائع العراقية ، العدد 4420 ،لسنة 2016.
([95]) ينظر قانون اصول المحاكمات الجزائية رقم 23 لسنة 1971 المعدل ، المصدر الوقائع العراقية ، العدد 204 ، لسنة 1971.

المصادر والمراجع .

اولًا / المعاجم والقواميس اللغوية.

1. ابن منظور ، معجم لسان العرب ، دار المعارف ، القاهرة ، بلا سنة طبع .
2. روحي البعلبكي ، قاموس المورد، ط7، دار العلم للملايين ، بيروت ، 1995 .

ثانيًا / الكتب.

1. احمد عبيس نعمة الفتلاوي ، الهجمات السيبرانية ، دراسة قانونية تحليلية بشأن تحديات تنظيمها المعاصر ، منشورات زين الحقوقية ، 2018 .
2. احمد يوسف جمعة ، الارهاب السيبراني والعملات الافتراضية والتجسس الالكتروني ، دراسة تحليلية تتناول استخدامات الارهاب للفضاء السيبراني ، ط1 ، دار الاهرام للنشر والتوزيع والاصدارات القانونية ، المنصورة ، 2022 .
3. إمام حسنين عطا ، الارهاب والبنيان القانوني للجريمة ، دار المطبوعات الجامعية ، بيروت ، 2004.
4. امل يازجي و د. محمد عزيز شكري ، الارهاب الدوي والنظام الدولي ، دار الفكر المعاصر ، بيروت ، 2002.
5. ثامر ابراهيم ، مفهوم الارهاب في القانون الدولي ، دار حوران للطباعة ، دمشق ، 1998 .
6. خالد حسن احمد لطفي ،الارهاب الالكتروني افة العصر الحديث والآليات القانونية لمعالجته، ط1 ، دار الفكر الجامعي ، الاسكندرية ، 2019 .
7. خالد محمد طاهر شبر ، الارهاب والنظام السياسي الدولي ، بعد احداث 11 ايلول / سبتمبر 2001(رؤية مستقبلية) ، ط1 ، مركز الرافدين للحوار ، ، بيروت/النجف الاشرف ، 2022.
8. علي عدنان الفيل ، الاجرام الالكتروني ، كلية الحقوق ، جامعة الموصل ، منشورات زين الحقوقية ، 2011.
9. علي حسين الخلف و د. سلطان الشاوي ، المبادئ العامة في قانون العقوبات المكتبة القانونية ، بغداد، 1982 .
10. عمر محمد ابو بكر يونس ، الجرائم الناشئة عن الانترنت ، دار النهضة العربية ، القاهرة ، 2004.
11. عمر عباس خضير العبيدي ، الارهاب الالكتروني في نطاق القانون الدولي ، ط1 ، المركز العربي للنشر والتوزيع ، القاهرة ، 2021.
12. كامل سعيد ، جرائم الكومبيوتر والجرائم الاخرى في مجال تكنلوجيا المعلومات ، بحث مقدم الى المؤتمر السادس للجمعية المصرية للقانون الجنائي ،دار النهضة العربية ، القاهرة ، 1993 .

13. منتصر سعيد حمودة ، الارهاب الدولي - جوانبه القانونية - وسائل مكافحته في القانون الدولي العام والفقه الاسلامي ، ط1 ،الاسكندرية ، 2008 .
14. هالة احمد الرشيدي ، الارهاب السيبراني ماهيته وجهود مكافحته في ضوء التشريعات والقوانين الوطنية والدولية، ط1، دار النهضة العربية ، 2021 .

ثالثًا / البحوث والدراسات.

1. سامر مؤيد عبد اللطيف وآخرون ، دور المنظمات الدولية في مكافحة الارهاب الرقمي ، بحث منشور في مجلة رسالة الحقوق ، جامعة كربلاء ، السنة العاشرة ، العدد الثاني ، 2018 .
2. محمد دهام مسعف ، حق الدفاع الشرعي ضد الهجمات السيبرانية ، رسالة ماجستير ، كلية القانون ، جامعة بغداد ، 2022.
3. صلاح مهدي هادي الشمري و د. زيد محمد علي اسماعيل ، الامن السيبراني كمرتكز جديد في الساحة العراقية ، مجلة قضايا سياسية ، كلية العلوم السياسية ، جامعة النهرين ، العدد62، السنة الثانية عشر ، 2020 .
4. اسراء طارق جواد كاظم الجابري ، جريمة الارهاب الالكتروني ، دراسة مقارنة ، رسالة ماجستير ، كلية الحقوق ، جامعة النهرين ، 2012.
5. هه لاله محمد تقي محمد ، التعاون الدولي في مواجهة جريمة الارهاب الإلكتروني ، بحث منشور في مجلة مركز الدراسات القانونية والسياسية ، كلية القانون ، جامعة السليمانية ، السنة السادسة ، العدد (11) ، 2018.
6. حسن بن احمد الشهري ، الارهاب الالكتروني – حرب الشبكات - ، بحث منشور في المجلة العربية الدولية للمعلوماتية ، المجلد الرابع ، العدد الثامن ، 2015 .
7. زهراء عماد محمد كلنتر ، المسؤولية الدولية الناشئة عن الهجمات السيبرانية ، رسالة ماجستير ، كلية القانون ، جامعة الكوفة ، 2016 .
8. روان بنت عطية الله الصحفي ، الجرائم السيبرانية ، بحث منشور في المجلة الالكترونية الشاملة متعددة التخصصات ، العدد الرابع والعشرون ، شهر5 ، 2020 .
9. سراب ثامر احمد ، الهجمات على شبكات الحاسوب في القانون الدولي الانساني ، اطروحة دكتوراه ، كلية الحقوق ، جامعة النهرين ، 2015 .
10. كاميران عزيز حسن ، الجهود الدولية في مواجهة الجرائم السيبرانية ، رسالة ماجستير ، كلية القانون والعلوم السياسية ، الجامعة العراقية ، 2019.
11. سامر مؤيد عبد اللطيف ، الحرب في الفضاء الرقمي ، رؤية مستقبلية ، بحث منشور في مجلة رسالة الحقوق ، كلية القانون ، جامعة كربلاء ، السنة السابعة ، العدد الثاني ، 2015 .
12. سليماني مباركة ، الارهاب الالكتروني وطرق مكافحته ، بحث منشور في مجلة القانون والعلوم السياسية ، جامعة عباس لغرور خنشلة ،الجزائر، العدد 8، ج1 ، 2017 .
13. زين العابدين عواد كاظم الكردي ، جرائم الارهاب المعلوماتي وبعض تطبيقاته في القانون العراقي ، دراسة مقارنة ، رسالة ماجستير ، كلية القانون ، جامعة بابل ، 2008 .
14. عبير احمد محمد الحميري واحمد شكران بن بحر الدين و نور زاهدي عثمان ، التنظيم القانوني لجرائم الارهاب الالكتروني ، بحث منشور في مجلة الشريعة والقانون ، كلية الشريعة والقانون ، جامعة العلوم الاسلامية في ماليزيا ،2020.
15. المنهج المرجعي لمكافحة الارهاب ، حلف الناتو ، مايو/ايار 2020 .
16. هادي طلال هادي ، المواجهة القانونية والامنية لجرائم الارهاب الالكتروني ، بحث منشور في مجلة الجامعة العراقية ، العدد 45 ،ج2، 2019 .
17. صلاح هادي الفتلاوي ، جريمة الارهاب الالكتروني ، بحث منشور في مجلة القانون للدراسات والبحوث القانونية ، كلية القانون ، جامعة ذي قار ، العدد 13 ، 2016.

رابعًا / المقابلات .

1. مقابلة مع الدكتور بشار مكي العيساوي ، استاذ امن المعلومات والامن السيبراني ، الجامعة المستنصرية ، بتاريخ 2023/1/12.

خامسًا / المقالات .

1. مقالة منشورة في مجلة الاتجاهات الاميركية بتاريخ 2003/10/11 للكاتب كيفين كولمان .

سادسًا / مصادر الشبكة الدولية للمعلومات.

1. احمد ناصر ابو سعود ، الارهاب الالكتروني ، بحث منشور على موقع الموسوعة السياسية ، والمتاح على الرابط التالي : https://political-encyclopedia.org/dictionary/%D8%A7%D9%84%D8%A5%D8%B1%D9%87%D8%A7%D8

%A8%20%D8%A7%D9%84%D8%A7%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A
2. علي مطر ، الارهاب الالكتروني – نوع جديد لم يتم التعامل معه بعد – مقال منشور في موقع انباء الاخبارية ، متاح على الرابط التالي : https://www.inbaa.com
3. عبد الله عبد العزيز فهد العجلان ، الارهاب الالكتروني في عصر المعلومات ، بحث مقدم الى المؤتمر الدولي الاول حول " حماية امن المعلومات والخصوصية في قانون الانترنت" والمنعقد بالقاهرة في المدة من 2 - 4 يونيو ، 2008، ص 13، متاح على الرابط التالي : http://www.shaimaaatalla.com/vb/showthread.php?t=3937
4. الاتحاد الدولي للاتصالات ، اخبار الامم المتحدة ، اهداف التنمية المستدامة ، 30 نوفمبر 2021، متاح على الرابط : https://news.un.org
5. https://www.meemapps.com/term/dark-web
6. /https://www.sasapost.com/convergent-technologies

سابعًا / التشريعات الوطنية .

1. قانون مكافحة الارهاب رقم 13 لسنة 2005.
2. قانون جهاز مكافحة الارهاب رقم 31 لسنة 2016.
3. قانون اصول المحاكمات الجزائية رقم 23 لسنة 1971 المعدل.

ثامنًا / الصكوك والاتفاقيات الدولية .

1. اتفاقية مجلس اوربا المتعلقة بالجريمة الإلكترونية ، مجموعة المعاهدات الاوربية ، رقم 185 ، بودابست عام 2001.

تاسعًا / المصادر الاجنبية .

First : Research and studies

1. Norbert Wiener,Cybernetic or control communication in the animal and the machine,M.I.T,Press,Second Edition,Cambridge,Massachusetts.1948.
2. Chuipka,A. (2016),The Strategies of Cyber terrorism –is Cyber terrorism an Affective means to Achieving the Goals if Terrorists? Affaires publiques at internationals- memories / Public and International Affairs- Research papers.
3. Julia Cresswell, "Oxford Dictionary of word Orgins :Cybernetics" ,Oxford Reference Online, Oxford University Press,2010.
4. FBI,2002.code of Federal.Regulations.28 CFR. Section 0.85 on Judicial Administration. July 2001.
5. Paulo shakarian and others, introduction to cyber-Warfare, A Multidisciplinary Approach, , published by Elsevier, Waltham , USA, 2013.
6. Solange Ghernaouti, Cyber power Crime, Conflict and security in Cyberspace published by Epft Press, Switzerland, 2013.
7. Tang Lan, Zhang Xin, Harry D. Raduege, Jr., Dmitry I. Grigoriev, Pavan Duggal, and Stein Schjølberg,"Global Cyber Deterrence Views from China, the U.S., Russia, India, and Norway", The EastWest Institute, Printed in the United States, 2010.