



دور المنظمات الدولية في مكافحة الإرهاب الرقمي.

International organizations role in combating cyber terrorism.

بحث مقدم من قبل

الاستاذ الدكتور سامر مؤيد عبد اللطيف

المدرس الدكتور نوري رشيد الشافعي

المدرس الدكتورة منى محمد عبد الرزاق

جامعة كربلاء // كلية القانون

الخلاصة.

يهدف البحث إلى تحليل طبيعة الإرهاب الرقمي وتبيان خصائصه وأساليبه ، وتحري دور المنظمات الدولية في مكافحته ، باستخدام منهج التحليل الوصفي والاستنباطي .للاغاية أعلاه ، تقسيم الموضوع على ثلاثة مباحث ، يتناول أولها مفهوم الإرهاب الرقمي وخصائصه بوصفه عمليات غير مشروعة تتم بواسطة الحاسوب والشبكة الدولية للمعلومات للإضرار وإلحاق الدمار بالبنى المعلوماتية لأغراض سياسية ، أما المبحث الثاني فيتصدى للكشف عن جهود المنظمات العالمية في مجال مكافحة الإرهاب الرقمي عبر التركيز على منظمة الأمم المتحدة والاتحاد الدولي للاتصالات أما المبحث الثالث فمجاله البحث في جهود ودور المنظمات الإقليمية (الأوروبية والعربية) في المسار ذاته.قد توصل البحث إلى نتائج من أهمها ملاحظة تطور اهتمامات المنظمات الدولية تتقدمها الأمم المتحدة ومن بعدها الاتحاد الأوروبي بموضوعة الإرهاب دون أن تميز أو تخص الإرهاب الرقمي بمسار مستقل عن جهودها لمكافحة هذا التهديد الدولي.

الكلمات المفتاحية: الدولية ، المنظمات ، الإرهاب الرقمي ، الشبكة الدولية للمعلومات ، معلومات.

Abstract.

The research aims to analyze the nature of cyber terrorism and the statement of its properties, methods, and investigate the role of international organizations in the combat it, using descriptive analysis method and deductive. The subject was split on the three sections, the first dealt with of the concept of cyber terrorism and its characteristics as illegal operations carried out by the computer and the International Network for Information of the damage and inflict mass structures of information for political purposes, while the second section studied the global organizations efforts in the fight against digital terrorism by focusing on the Nations United and the international telecommunication Union. The third section searched efforts and the role of regional organizations (European and Arabic) at the same track.

Key words: International , organizations , cyber terrorism , International network , information.



المقدمة.

يعدّ الإرهاب الدولي من أخطر الظواهر التي يواجهها المجتمع الدولي اليوم بالنظر للخسائر التي يلحقها بالأرواح وبالبنى والمؤسسات المادية إلى جانب ما يلحقه من أضرار بسمعة الدولة ومعنويات مواطنيها طالما أنّ هدفه نشر الخوف والذعر بين هؤلاء الأبرياء ، ليكون بنظر القانون الدولي من الجرائم التي يحق لكل دولة أن تمارس إزائها اختصاصاً جنائياً بغض النظر عن جنسية مرتكبيها أو ضحيتها أو مكان ارتكابها. مع تنامي التطور التقني في العالم لاسيما بفضل استخدام الحاسوب وظهور الشبكة الدولية للمعلومات وتزايد اعتماد الدول عليها في إدارة مؤسساتها وتقديم الخدمات المختلفة ، تزايد بالمقابل خطر الإرهاب الدولي الذي اساء استغلال مزايا شبكة المعلومات العالمية في تحقيق أغراضه الإجرامية في تصميم وتنفيذ عدد من العمليات الإرهابية ضد المواقع الالكترونية المرتبطة بالبنى التحتية والمؤسسات المهمة للدول ، أو حتى التنسيق بين الإرهابيين أنفسهم لتنفيذ عمليات إرهابية على أرض الواقع بصورة أكثر دماراً وأكثر بعداً عن مراقبة ومتابعة الأجهزة الأمنية لينتج نمطاً جديداً من الأهاب أصطلح عليه (الإرهاب الرقمي) وشاع استخدامه بين الأوساط الرسمية والعلمية بعد هجمات 11 ايلول عام 2001. في مواجهة هذا التهديد الالكتروني للأمن العالمي انبرت المنظمات الدولية العالمية والإقليمية لصياغة القرارات والاستراتيجيات وبذل الجهود لتكون على مستوى التحدي. في ضوء ما تقدم تبرز أهمية البحث من حادثة موضوعة الإرهاب الرقمي وندرة الكتابات عنها ، كما يستمد هذا البحث أهميته كذلك من خطورة التهديد الإرهابي على الأمن العالمي بوجه عام والتهديد الالكتروني لهذا الإرهاب على وجه الخصوص لاسيما مع صعوبة الكشف عن مرتكبيه وتنوع وسائله وصعوبة حصر وتحديد حجم الدمار الذي يخلفه في نظم المعلومات وما يرتبط فيها ويعتمد عليها من بنى تحتية ومؤسسات رسمية . والأهم من ذلك يكمن في الحاجة لإمطة اللثام عن الدور الذي تمارسه المنظمات الدولية في مجال ملاحقة هذا النوع المستحدث من الإرهاب الرقمي وما يمكن أن تضيفه وتضيفه على قدرة الدول في مجال مكافحة هذا الخطر المتسارع الخطى. عند هذا المقام يمكن تحري مشكلة البحث في الكشف عن كنه وخصوصية الإرهاب الرقمي ، ومن ثم تتبع الجهود التي بذلتها المنظمات الدولية العالمية والإقليمية في مجال مكافحته وما حققته من نجاحات وما اعترأها من اخفاقات وما يعوزها من ادوات لاستكمال هذا الطريق الوعر. عبر منهجية وصفية واستنباطية تقوم على التحليل المعمق لنصوص القرارات الدولية ومتابعة الجهود والاستراتيجيات التي وضعتها المنظمات الدولية لمكافحة الإرهاب الرقمي ، سيتم معالجة هذا الموضوع على أساس تقسيمه بين ثلاثة مباحث ، يتناول أولها مفهوم الإرهاب الرقمي وخصائصه ، أما المبحث الثاني فيتصدى للكشف عن جهود المنظمات العالمية في مجال مكافحة الإرهاب الرقمي عبر التركيز على منظمة الأمم المتحدة والاتحاد الدولي للاتصالات أما المبحث الثالث فمجاله البحث في جهود ودور المنظمات الإقليمية (الأوروبية والعربية) في المسار ذاته . ثم خاتمة تضمنت أهم النتائج والتوصيات التي تم التوصل إليها في ضوء معطيات البحث.

المبحث الأول // مفهوم الإرهاب الرقمي وأساليبه.

استقطب الإرهاب الرقمي على الرغم من حداثة ظهوره اهتمام الأوساط الرسمية والاكاديمية في العالم ، فكان ميدانا خصبا للجدل والاختلاف ، بالنظر لهلامية أبعاده وتنوع وتطور مظاهره وآلياته وتباين أغراض وخلفيات من تناوله بالبحث والدراسة . ولتسليط الضوء على هذا المفهوم



المستحدث من الإرهاب سيتم تقسيم هذا المبحث على مطلبين ، ينصرف الأول منهما إلى تبيان تعريف الإرهاب الرقمي ، ويتحرى الثاني عن أهم مظاهر هذا النوع من الإرهاب.

المطلب الأول // تعريف الإرهاب الرقمي وبيان خصائصه.

يعد التعريف بالظاهرة موضوعة البحث مدخلاً لا غنى عنه للكشف عن كنه هذه الظاهرة وسبر اغوارها ، وهذا أدعى أن يكون في ظاهرة مستحدثة مثل ظاهرة الإرهاب الرقمي ، لذا وجب علينا في المقام الأول تحديد المعنى اللغوي والاصطلاحي له ، ومن ثم تحليل أهم خصائصه المميزة . وهذا ما سيتم دراسته في هذا المطلب تباعاً.

الفرع الأول // تعريف الإرهاب الرقمي.

تجمع قواميس اللغة العربية على أنّ كلمة إرهاب تعني (الفزع والخوف والرعب) . وكلمة إرهاب مشتقة من الفعل المزيد (أرهب)؛ ويقال أرهب فلاناً: أي خوّفه وفزّعه، وهو نفس المعنى الذي يدل عليه الفعل المضعف (رهب). أما الفعل المجرد من نفس المادة وهو (رهب)، يزهب رهبته ورهباً ورهباً فيعني (خاف) مع تحرز واضطراب. فيقال رهب الشيء رهبا ورهبة أي خافه، وكذلك يستعمل الفعل ترهب بمعنى توعد إذا كان متعدياً فيقال ترهب فلاناً: أي توعد⁽¹⁾ وأرهبه واسترهبه أي أخافه وافزعه⁽²⁾ . وتتفصل الرهبة عن الخوف لدى بعض اللغويين لتعني طول الخوف واستحكامه بالنفس ومنها انطلقت تسمية الراهب الذي يديم الخوف⁽³⁾ في المعاجم المترجمة إلى اللغتين الانجليزية والفرنسية، ورد لفظ الإرهاب بدلالة المصطلحات (Terrorism) المشتقة من الفعل (Terror) بما يفيد معنى الذعر والتخويف أو إشاعة الهلع⁽⁴⁾ . يتضح مما تقدم أنّ معاجم اللغة وقواميسها العربية والغربية ، قد جعلت من الخوف والترويع مقصداً ومعنى لعبارة الإرهاب وهو الأساس الذي انطلق منه وأقره من تصدى لتعريف الإرهاب اصطلاحياً على الرغم من اختلافهم في التفاصيل ، الأمر الذي أفضى إلى عدم وجود مفهوم دولي مؤحد للإرهاب بصفة عامة، والإرهاب الرقمي بصفة خاصة. في هذا السياق ، كانت اتفاقية جنيف لقمع ومعاقبة الإرهاب لعام 1937 م، سباقة في تعريف الأعمال الإرهابية على أنها "الأعمال الإجرامية الموجهة ضد دولة ما وتستهدف ، أو يقصد بها ، خلق حالة من الرعب في إذهان أشخاص معينين، أو مجموعة من (الأشخاص، أو عامة الجمهور)"⁽⁵⁾ . عرّف مجلس الأمن الدولي الإرهاب بأنه: "كل عمل جرمي ضد المدنيين بقصد التسبب بالوفاة أو بالجروح البليغة أو أخذ الرهائن من أجل إثارة الرعب بين الناس أو إكراه حكومة أو منظمة دولية للقيام بعمل ما أو الامتناع عنه، وكل الأعمال الأخرى التي تشكل إساءات ضمن نطاق المعاهدات الدولية المتعلقة بالإرهاب والتي لا يمكن تبريرها بأي اعتبار سياسي أو فلسفي أو إيديولوجي أو عرقي أو ديني"⁽⁶⁾ . فكان هذا التعريف مغرّقاً في التركيز على الوسائل المستخدمة في الفعل الإرهابي على سبيل الحصر والتحديد الذي لا يمكن الارتكان إليه مستقبلاً إذا ما برزت وسائل ومظاهر إرهابية مستحدثة ومن ذلك على سبيل المثال (الإرهاب الرقمي والجرثومي) الذي شهدته الساحة الدولية في الوقت الرهن لتثبيت عجز هذا التعريف عن الاحاطة لكل أنواع الإرهاب قريباً من التعريف أعلاه جاء الاتفاقية العربية لعام 1998 للإرهاب بأنه "كل فعل من أفعال العنف أو التهديد أياً كانت بواعثه أو أغراضه، يقع تنفيذاً لمشروع إجرامي فردي أو جماعي، ويهدف إلى إفساء الرعب بين الناس، أو ترويعهم بإيذائهم أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر، أو إلحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة، أو احتلالها أو الاستيلاء عليها، أو تعريض أحد الموارد الوطنية (للخطر)⁽⁷⁾ . فكان إطاراً جامعاً



دون تفاصيل دقيقة لأهم آليات الإرهاب دون الإشارة الواضحة إلى غاياته أو دوافعه أو حتى تبيان الصور الأخرى منه إذا كان تعريف الإرهاب بصورته العامة مجالاً لاختلاف الرأي وتباين الاجتهادات ، فإن الوجه الجديد للإرهاب بصورته الرقمية ، قد استوعب مساحةً أكبر من الجدل والاختلاف في التوصيف والتعريف بين الباحثين والمهتمين ؛ فكان تعريف الأمم المتحدة في تشرين الأول/ أكتوبر 2012 للإرهاب الرقمي الأكثر هلامية وإجمالاً في الدلالة والنطاق دون الاستغراق في التفاصيل والآليات والمقاصد الإرهابية ، وذلك حين عرفت الإرهاب الرقمي على أنه "استخدام الإنترنت لنشر أعمال إرهابية"⁽⁸⁾ في الموسوعة الإلكترونية جرى تعريف الإرهاب الرقمي بأنه " استخدام التقنيات الرقمية لإخافة وإخضاع الآخرين ؛ أو هو القيام بمهاجمة نظم المعلومات على خلفية دوافع سياسية أو عرقية أو دينية"⁽⁹⁾ . كان تعريف اللجنة الدولية للصليب الأحمر أكثر استرسالاً في تقصي التفاصيل الفنية عند تعريفها للإرهاب الرقمي على أنه " عمليات تشن ضد أو عبر حاسوب بواسطة تيار بيانات وتهدف إلى تحقيق اغراض منها اختراق النظام المعلوماتي أو جمع أو نقل أو تشفير أو تغيير البيانات أو التلاعب بها من قبل منفذ عملية الاختراق واستخدام هذه الوسائل لتدمير أو تعطيل مجموعة متنوعة من الأهداف في العالم الحقيقي كالصناعات والبنى الأساسية"⁽¹⁰⁾ بيد أنّ الإرهاب الرقمي على وفق رأي آخر هو " نشاط هجومي متعمد ذو دوافع سياسية بغرض التأثير على القرارات الحكومية أو الرأي العام باستخدام الحاسبات ووسائل الاتصال للتأثير على إنتاج ومعالجة وتخزين المعلومات أو تعطيل خدمات لينتج عنه ترويع وتخويف وتدمير للبنية التحتية الحيوية"⁽¹¹⁾ فكان هذا التعريف دقيقاً جامعاً لأغلب وسائل الإرهاب ومقاصده ، على الرغم من اغفاله لإمكانية استخدام الشبكة الدولية للمعلومات كوسيلة للاتصال والتنسيق بين الإرهابيين أو حتى منطلقاً لتنفيذ العمليات الإرهابية على أرض الواقع على النقيض من اتجاه باحث آخر في تعريف الإرهاب الرقمي على أنه " تسخير التقنيات المتوافرة في الإنترنت لألحاق أذى مادي أو معنوي أو إيجاد قلقلة كبيرة في الجهة المقصودة"⁽¹²⁾ الذي أسقط فاعلية الشبكة الدولية في الحاق الأذى بنظم المعلومات والسيطرة على الشبكة بفعل تركيزه على الجانب المادي من الإرهاب الرقمي . وهو الاتجاه الذي سار فيه د. هشام بشير ، المستشار الإعلامي للجمعية المصرية لمكافحة جرائم الإنترنت في تعريفه للإرهاب الرقمي بأنه "العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول، أو الجماعات أو الأفراد على الإنسان، في دينه، أو نفسه، أو عرضه، أو عقله، أو ماله بغير حق، باستخدام الموارد المعلوماتية والوسائل الإلكترونية، بشتى صنوف العدوان وصور الإفساد"⁽¹³⁾ .

الفرع الثاني//خصائص الإرهاب الإلكتروني.

يتميز الإرهاب الإلكتروني بعددٍ من الخصائص والسمات التي يختلف فيها عن سائر صور الإرهاب والجريمة ، ومن الممكن إيجاز أهم تلك الخصائص والسمات فيما يأتي:

1- عمل عدائي غير مشروع من حيث الوسائل المستخدمة والأهداف المنشودة ، إذ يشتمل على تطوير وإرسال شفرات الحاسب الآلي إلى الشبكة الدولية للمعلومات بغية تحقيق أغراض عدة تتمثل بالتدمير والانتقاص والتغيير والتعطيل والإفساد للمعلومات أو البرامج الموجودة ، أو التهديد بإيقاع الضرر بصورة تخالف كل القوانين والمواثيق والاتفاقيات الدولية والقيم الأخلاقية وحتى الدينية.

2- جرائم تقنية ناعمة ، يعد الحاسب الآلي والشبكة الدولية للمعلومات الأداة الرئيسة في ارتكابها ، مثلما يمكن اعتبار البرامجيات ونظم المعلومات الركن المعنوي لمثل هذا النوع من الجرائم ، وهي



بكل الاحوال لا تحتاج في ارتكابها إلى العنف والقوة ولا أثر فيها لأيّ دماء، وإنما مجرد أرقام وبيانات يتم تغييرها أو محوها من دليل السجلات المخزونة في ذاكرة الحاسبات الآلية؛ كما أنها سهلة التنفيذ، لا تحتاج إلى وقت ولا إلى جهد، بل تتطلب وجود حاسب آلي متصل بالشبكة المعلوماتية ومزود ببعض البرامج اللازمة لاختراق وتدمير نظم المعلومات (14).

3- يعتمد الإرهاب الرقمي على خبرات وقدرات ذهنية ومهارات عالية في استخدام الحاسوب واختراق أنظمة الحماية المتوفرة، إذ إنّ مرتكب الإرهاب الإلكتروني يكون في العادة من ذوي الاختصاص في مجال تقنية المعلومات، أو على الأقل شخص لديه قدر من المعرفة والخبرة في التعامل مع الحاسب الآلي والشبكة المعلوماتية (15).

4- جرائم عابرة للدول، يتسم الإرهاب الإلكتروني بكونه جريمة إرهابية متعدية الحدود، وعابرة للدول والقارات، وغير خاضعة لنطاق إقليمي محدود أو مسرح واحد إذ يمكن أن يستهدف الفاعل أماكن وأهداف متفرقة في وقت واحد (16).

إذ إنّ التقنيات الحديثة وما صاحبها من تقدم في مجال الاتصال ألغى الحدود الجغرافية بين الدول بحيث أنّ الجريمة المعلوماتية تخطت حدود الدولة التي ترتكب فيها لتتعدى آثارها إلى كافة البلدان على مستوى العالم، فالطبيعة العالمية للجريمة تمكن الجاني من ارتكاب جرائمه في دولة ما والتي ستؤثر على المجني عليه في دولة أخرى (17).

5- صعوبة اكتشاف جرائم الإرهاب الإلكتروني أو مصدرها والقائم بها أو إثبات الدليل على حصولها أو حتى حصر وتحديد حجم الضرر الناجم عنها (18) نظراً لصعوبة كشف عملية الاختراق للبيانات وإثبات الدليل على قيامها والقائمين عليها، والمرونة العالية لتنفيذ أنشطة الإرهاب الرقمي باستخدام برامج وأدوات وحاسبات في أماكن وأوقات مختلفة ومتباعدة لاستهداف عدد غير محدد من الضحايا والأهداف الحساسة؛ لتصعب بالنتيجة إمكانية جمع الأدلة المادية أو حتى الرقمية لإدانة القائمين بالعمل الإرهابي، كون هذه الأدلة لا تكون في الغالب مادية تشير إلى الفاعل، وإنما كيانات منطقية تكون ضمن فضاء الحاسب الآلي يمكن بسهولة إخفائها والتخلص منها. وانعدام الأثر الخارجي يعود إلى أن تنفيذ الجريمة يتم أصلاً بالنبضات الكهربائية حيث تتغير وتمحى الأرقام والدلالات والمعلومات من ذاكرة الحاسوب (19). وهكذا جاز وصف جرائم الإرهاب الرقمي من نمط الجرائم النظيفة.

المطلب الثاني // أساليب الإرهاب الرقمي وصوره.

تتنوع أساليب الإرهاب الرقمي بحسب محتواها وطريقة استخدامها وغايات مستخدميه؛ فتنوع بين ما يستهدف منها نظم المعلومات وبرامجياتها وما يرتبط بها من بنى بالضرر والدمار بصورة مباشرة، فتكون ساحة عملياتها وأدواتها، المعلومات، وبين ما يجعل مزايا الشبكة الدولية للمعلومات وخدماتها وسائط لتنفيذ عملياته الإرهابية الدموية على أرض الواقع، فتكون المعلومات وسيلة لترجمة النوايا الاجرامية إلى واقع مادي دموي دون أن تكون هذه المعلومات بحد ذاتها ساحة للفعل الإرهابي. وعلى أساس ما تقدم سيتم تقسيم هذا المطلب وفقاً لأساليب الإرهاب الرقمي على ثلاثة فروع هي الآتي:

الفرع الأول//الاتصال والتنسيق بين الإرهابيين باستخدام الشبكة الدولية للمعلومات.

تعدّ الشبكة العالمية للمعلومات وسيلة اتصال بالغة الأهمية للجماعات الإرهابية؛ إذ تتيح لهم حرية التواصل وتبادل المعلومات فيما بينها والتنسيق الشامل لشن هجمات إرهابية محددة، في جو مريح، وبعيد عن رقابة ومتابعة الأجهزة الأمنية وذلك باستخدام البريد الإلكتروني أو المواقع والمنديات



وغرف الحوار الإلكتروني، إذ يمكن وضع رسائل مشفرة تأخذ طابعاً لا يلفت الانتباه، ومن دون أن يضطر الإرهابي إلى الإفصاح عن هويته، كما أنها لا تترك أثراً واضحاً يمكن أن يدل عليه. فضلاً عن المزايا الأخرى التي توفرها هذه الوسائل الرقمية للتواصل من سرعة الاتصال وقلة تكلفته وإمكانية المناورة والتخفي عن ملاحقة الأجهزة الأمنية مقارنة بالوسائل الأخرى⁽²⁰⁾. والأكثر من ذلك فقد أسهمت هذه التقنية في تدفق الدعم والمساعدات إذ تتيح بواسطة الإنترنت الوصول إلى جمهور ضخم من المانحين المحتملين وتسمح للأعضاء بالتنسيق سريعاً مع أكبر عدد من الأتباع لضمان سريان سريع ومستمر للتعليمات يضمن أقصى درجات التنظيم لنشاطات المجموعات الإرهابية كما، وتجنيب الذين قد يتوزعون فوق رقعة جغرافية ضخمة، كما توفر منبراً للدعاية⁽²¹⁾ إذا كان الحصول على وسائل إعلامية كالقنوات التلفزيونية والإذاعية صعباً، فإن إنشاء مواقع على الإنترنت، واستغلال منتديات الحوار وغيرها لخدمة أهداف الإرهابيين في الترويج لأفكارهم وكسب المؤيدين لهم أو حتى إبلاغ التعليمات والتدريبات لأنصارهم غداً سهلاً وممكناً، حتى يضمنوا انتشاراً أوسع، وحتى لو تم منع الدخول على بعض هذه المواقع أو تعرضت للتدمير تبقى المواقع الأخرى يمكن الوصول إليها. مما يزيد من خطورة هذه المواقع، أن الجماعات الإرهابية أو المتطرفة تعتمد في خططها وأساليبها الإرهابية على طرق بسيطة تتيح للجميع الدخول المباشر إلى مواقع محجوبة عبر التصفح العادي أو عبر البرامج التبادلية، وهناك مواقع تنشر معلومات حساسة حول كيفية إعداد المتفجرات والمواد السامة وصناعة الصواعق بتفاصيل دقيقة ومكونات يمكن الحصول على الكثير منها من أي مكان دون إثارة الريبة، ولا تقتصر خطورة توفر هذه المعلومات على الفئات الضالة، بل يمكن أن تمهد الطريق لارتكاب الجرائم الفردية⁽²²⁾.

الفرع الثاني // اختراق المواقع الإلكترونية وتدميرها.

يشمل هذا الأسلوب، اختراق المواقع والأنظمة الإلكترونية عبر الشبكة والسطو على محتوياتها أو تغييرها أو إحداث الضرر أو حتى تدميرها لتحقيق أهداف غير مشروعة المقصود بالتدمير هنا: "الدخول غير المشروع على نقطة ارتباط أساسية أو فرعية متصلة بالشبكة المعلوماتية من خلال نظام آلي (Server-PC)، أو مجموعة نظم مترابطة شبكياً (Intranet)، بهدف تخريب نقطة الاتصال أو النظام"؛ إذ يمكن أن يقوم الإرهابيون بشن هجوم مدمر لإغلاق المواقع الحيوية على الشبكات المعلوماتية، وإلحاق الشلل بأنظمة القيادة والسيطرة والاتصالات، ومحطات توليد الطاقة والماء، ومواقع الأسواق المالية، بحيث يؤدي توقفها عن العمل إلى تحقيق آثار تدميرية تفوق ما تحدثه القنابل المتفجرات من آثار. كما يمكن تصور هجوم إلكتروني على أحد المواقع الإلكترونية بقصد الاستيلاء على محتوياتها والسيطرة والتحكم فيها من الوسائل المستخدمة حالياً لتدمير المواقع ضخ مئات الآلاف من الرسائل الإلكترونية (E-mails) من جهاز الحاسوب الخاص بالمدمر إلى الموقع المستهدف للتأثير على السعة التخزينية للموقع، فتشكل هذه الكمية الهائلة من الرسائل الإلكترونية ضغطاً يؤدي في النهاية إلى تفجير الموقع العامل على الشبكة وتشتيت البيانات والمعلومات المخزنة في الموقع فتنتقل إلى جهاز المعتدي، أو تمكنه من حرية التجول في الموقع المستهدف بسهولة ويسر، والحصول على كل ما يحتاجه من أرقام ومعلومات وبيانات خاصة بالموقع المعتدى عليه⁽²³⁾. تعدّ الفيروسات والديدان ووسائل أخرى من أهم وأخطر الوسائل المستخدمة في عملية الاختراق والتدمير الإرهابي للمواقع ونظم المعلومات. والفيروس عبارة عن برنامج حاسوبي خارجي صنع خصيصاً للإضرار بنظام المعلومات والبيانات، ويقدر على التضاعف والانتشار، والانتقال من جهاز إلى آخر؛ إذ تحاول هذه البرامج استغلال العيوب



الموجودة في البرامج الأخرى والأخطاء التي يقع فيها مستخدمو الحاسوب قبل الدخول إلى المواقع المصابة بالعدوى الفيروسية أو فتح مرفقات الرسائل البريدية⁽²⁴⁾ لفيروس الحاسب الآلي خصائص تتشابه إلى حد كبير مع الفيروس الطبيعي من نواح عدة، منها القدرة الفائقة على الاختفاء والاختراق والانتشار مثل الفيروس الطبيعي، كما أن له القدرة على تغيير خصائص البرامج كما يقوم الفيروس الطبيعي بتغيير خصائص الخلايا المصابة. وتتعدد أنواع واستخدامات الفيروسات سواء على مستوى الأهداف التي تنجزها ومنها على سبيل المثال (الاختراق، التدمير، الاحتيال، السرقة، التجسس) أو على مستوى الأضرار التي تلحقها بالنظام، بدءاً من الأضرار اليسيرة إلى تدمير النظام بأكمله، ومنها ما يصيب نظاماً إلكترونياً محدداً ومنها ما يكون واسع الضرر والانتشار. وقدّر المجلس الأوروبي تكلفة إصلاح الأضرار التي تسببها فيروسات المعلومات بنحو (12) مليار دولار أمريكي سنوياً⁽²⁵⁾. أما الديدان فهي برامج صغيرة مستقلة قادرة على استنساخ نفسها ذاتياً باستغلال عيوب معروفة ثم تنتشر في النظام تمهيداً لتحقيق الأغراض التي صممت لها مثل تعطيل النظام أو قطع الاتصال بالشبكة أو سرقة بعض البيانات الخاصة. وتمتاز بسرعة الانتشار وصعوبة التخلص منها لقدرتها الفائقة على التناسخ والمراوغة⁽²⁶⁾ قد يقوم الإرهابيون بإنشاء ثغرة تسلل على غرار حصان طروادة باستخدام برنامج غير مرخص يضاف إلى برنامج ما، ليتمكن بعد ذلك بالولوج غير المرخص فيه إلى الشبكة أو البرنامج الحاسوبي التي لا يسمح لهم بالدخول إليها بالأحوال الاعتيادية، تمهيداً للعبث فيه بالحذف والإضافة أو والتغيير بخصائص النظام كله فضلاً عن التجسس⁽²⁷⁾. قد يذهب الإرهابيون إلى أبعد من ذلك بزرع القنبلة المنطقية داخل النظام الإلكتروني التي تكون عبارة عن برنامج حوسبي خبيث وخفي مصمم للعمل في وقت لاحق عند وقوع حدث معين أو تحت ظروف معينة، بصورة تلحق الضرر أو حتى التوقف للنظام أو الشبكة عن العمل أو حذف كل البيانات الموجودة فيها أو توجيه أو امر لمعدات الحاسوب لتقوم بشيء معين يؤدي إلى تدميرها⁽²⁸⁾.

الفرع الثالث // التجسس الإلكتروني.

يقوم الإرهابيون بالتجسس⁽²⁹⁾ على المواقع الإلكترونية للأفراد والدول أو المنظمات والهيئات الدولية أو الوطنية باستخدام برامج معينة ووسائل غير مشروعة مثل (الفيروسات، أو أسلوب سلامي⁽³⁰⁾، أو أحصنة طروادة) لكشف كلمة المرور السرية للدخول غير المصرح لهذه المواقع لتحقيق أغراض غير مشروعة مثل سرقة المعلومات أو إفشاءها أو حتى استغلالها في الأنشطة الإرهابية⁽³¹⁾. تتم عملية التجسس الإلكتروني بعدة طرق، من أشهرها، اختراق البريد الإلكتروني للآخرين، وذلك حين يقوم الضحية بفتح المرفقات المرسلة ضمن رسالة غير معروفة المصدر. وهناك طرق أخرى لزراعة أحصنة طروادة عن طريق إنزال بعض البرامج من أحد المواقع غير الموثوق بها، وكذلك يمكن إعادة تكوين حصان طروادة من خلال الماكرو الموجودة ببرامج معالجات النصوص. يكمن الخطر في عمليات التجسس التي تقوم بها التنظيمات الإرهابية وأجهزة الاستخبارات المختلفة من أجل الحصول غير المرخص به على أسرار ومعلومات الدولة، ومن ثم إفشاءها لدول أخرى معادية، أو استغلالها بما يضر المصلحة العامة والوحدة الوطنية للدولة، أو الاستفادة من المعلومات في العمليات الإرهابية، أو حتى تهديد تلك الجهات والأفراد وابتزازهم بها لحملهم على إتيان أفعال معينة يخططون لاقتوافها بتراوح خطورة التجسس بحسب أهمية المعلومة الملتقطة ودرجة سربيتها سواء اكانت سيادية أو أمنية أو اقتصادية، أو الجهة التي قامت بمهمة التجسس منظمة إرهابية أو فرد أو حتى دولة، فضلاً عن الغرض التي تستغل فيه هذه



المعلومات المسروقة⁽³²⁾ من أمثلة عمليات التجسس الالكتروني التي مارستها بعض الجهات الإرهابية للحصول على المعلومات العسكرية المخزنة في ذاكرة الحاسبات الآلية التابعة لوزارات الدفاع بالدول المستهدفة ما حدث في صيف 1994 عندما تمكنت إحدى هذه الجهات الإرهابية من سرقة معلومات عسكرية تتعلق بالسفن التي تستعملها الجيوش التابعة لدول أعضاء حلف شمال الأطلسي من أنظمة الحاسبات الآلية الخاصة بسلاح البحرية الفرنسية. مما أثار حفيظة قيادة أركان الحلف وحمل السلطات العسكرية الفرنسية على تصميم برامج جديدة لحماية حاسباتها الآلية⁽³³⁾ كما كشفت صحيفة واشنطن بوست (12 يونيو 2013)، ودير شبيغل الألمانية والغارديان البريطانية- على إثر تسريبات إدوارد سنودن- عن برنامج "بريزيم" الذي يعد من أضخم البرامج التي استعملتها وكالة الأمن القومي الأميركية منذ 2007 في تجسسها على العديد من الدول وشملت مواطنين وشخصيات سياسية كبيرة، ومقرات البنك الدولي والأمم المتحدة واجتماعات الثمانية ومجموعة ال-20، فضلاً عن العديد من رؤساء دول العالم الثالث بلغ عددهم 60 زعيماً، فضلاً عن التنصت على الاجتماعات في أروقة العديد من المنظمات الدولية؛ مما سبب ضجة كبيرة للحكومة الأميركية على إثر التسريبات التي اكتسبتها قضية التجسس على مواطنين أميركيين في اختراق سافر للحريات العامة. ودفعت الرئيس أوباما إلى الاعتراف بأن هذا البرنامج موجه لجمع أرقام هواتف ولا يحمل أسماء ولا مضمون مكالمات، وهو موجه للحماية الاستباقية من الإرهاب فحسب، لكن انكشاف فحوى برنامج بريزم أطمأنت اللثام عن العديد من برامج المراقبة الأخرى من بينها (برنامج أوبستريم، برنامج كسكيسكور، برنامج بولرون وبرنامج تومبور).)

المبحث الثاني // دور المنظمات العالمية في مكافحة الإرهاب الرقمي.

تتقدم الأمم المتحدة قائمة المنظمات الدولية المعنية بمواجهة الإرهاب على اختلاف صنفه واهدافه ، بالنظر لقدراتها وخبراتها الواسعة في هذا المجال والتأييد الدولي ، ومن هذه المنظمة انبثقت منظمات عالمية أخرى أكثر تخصصاً من أمثال (الاتحاد الدولي للاتصالات ، و المنظمة العالمية للملكية الفكرية) لتكون سنداً للأمم المتحدة في مجال تخصصها الذي اتسع ليواجه المظاهر المستحدثة من الإرهاب الرقمي عبر الشبكة الدولية للمعلومات . وهذا ما يستدعي تسليط الضوء على دور كل منها في مجال مكافحة الإرهاب في مطالب هذا المبحث.

المطلب الأول // دور الأمم المتحدة في مكافحة الإرهاب الرقم.

يعود اهتمام المجتمع الدولي بمشكلة الإرهاب إلى عام 1934، حين تقدمت فرنسا بطلب إلى سكرتير عصبة الأمم ، ودعت فيه إلى اتفاق دولي لمعاقبة الجرائم التي ترتكب بغرض الإرهاب السياسي أثر مقتل الملك الكسندر الأول ملك يوغسلافيا ، تم إقراره في عام 1937تضمن تحريم الإرهاب الذي يتخذ صيغة الأفعال الإجرامية الموجهة ضد دولة عندما تكون هدفها أحداث رعب لدى أشخاص أو جماعات معينة أو لدى الجمهور⁽³⁴⁾ . ومنذ ذلك الحين بدأت المنظمة الدولية رحلتها في مكافحة الإرهاب على اختلاف أنواعه ومظاهره ، فكان لها دور مميز في هذا المضمار يمكن تشخيصه من خلال الرجوع إلى ميثاقها في المقام الأول ، أو من خلال مراجعة ما أصدرته من قرارات وبذلته من جهود في هذا الخصوص في المقام الثاني.

الفرع الأول // الإرهاب الرقمي في ضوء ميثاق الأمم المتحدة.

تشكل مكافحة الإرهاب جزءاً لا يتجزأ من ولاية الأمم المتحدة التي يجعل ميثاقها من صون السلم والأمن الدوليين مقصداً رئيساً، ويوجب اتخاذ تدابير جماعية لمنع التهديدات للسلام ولقمع العدوان



وتعزيز حقوق الإنسان والتنمية الاقتصادية، ليظهر الإرهاب ضمن هذا المنحى بوصفه انتهاكاً وتهديداً لشروط ومقتضيات إشاعة الأمن والسلم الدوليين ، فضلاً عن انتهاكه الواضح لحقوق الإنسان، والتسوية السلمية للمنازعات، التي حرص الميثاق الأممي على تكريسها وتأمينها⁽³⁵⁾. على الرغم من كون ميثاق الأمم المتحدة لم ينص صراحة على تجريم استخدام المعلومات كأداة إرهابية ضمن إطار ما يعرف بـ (الإرهاب الإلكتروني) ؛ إلا أن روح الميثاق تتفق مع تجريم استخدامه بوصفه انتهاكاً لما ورد في الميثاق بخصوص "التهديد أو استخدام القوة ضد السلامة الإقليمية أو الاستقلال السياسي لأي دولة". ومع الأخذ في الاعتبار أن الميثاق جاء لمواجهة النزاعات المسلحة، فإنه إذا ما تمّ اعتبار الإرهاب الرقمي واستخدام حرب المعلومات يقعان ضمن العدوان والذي يُعنى بحمل وإرغام دولة على الإتيان بعمل معين.. فإنه تنطبق هنا قوة القانون ؛ لاسيما وأنّ ميثاق الأمم المتحدة في مادته الثانية فقرة (3) قد أورد ما نصّه: "يفضُّ جميع أعضاء الهيئة منازعاتهم الدولية بالوسائل السلمية على وجه لا يجعل السلم والأمن والعدل الدولي عرضة للخطر". من ثمّ فإنّ التجاء الدول إلى تسوية منازعاتها وصراعاتها عبر الفضاء الإلكتروني ، يعرّض الأمن والسلم الدوليين للخطر. كما أن الإرهاب الرقمي وما يتضمنه من خروقات للسيادة الوطنية لأية دولة، وأساليب للتجسس على المعلومات التي تهدد الأمن الوطني للبلدان ، وتجنيد العملاء ، تناقض ما ورد من توجه أممي ضمن مقتضيات الفقرة الرابعة من المادة نفسها لميثاق الأمم المتحدة التي تنص على أنه "يمنتع أعضاء الهيئة جميعاً في علاقاتهم الدولية عن التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو على أي وجه آخر لا يتفق ومقاصد الأمم المتحدة". على الرغم من كون الفقرة (7) من المادة الثانية نفسها تقول "ليس في هذا الميثاق ما يسوغ "للأمم المتحدة" أن تتدخل في الشؤون التي تكون من صميم السلطان الداخلي لدولة ما، وليس فيه ما يقتضي الأعضاء أن يعرضوا مثل هذه المسائل لأن تحلّ بحكم هذا الميثاق، فإن هذا المبدأ لا يخلّ بتطبيق تدابير القمع الواردة في الفصل السابع" الذي يقع ضمن طائفة المادة 39 في الفصل السابع من ميثاق الأمم المتحدة التي تنصّ على: "يقرر مجلس الأمن ما إذا كان قد وقع تهديد للسلم أو إخلال به أو كان ما وقع عملاً من أعمال العدوان".

الفرع الثاني // جهود الأمم المتحدة في مجال مكافحة الإرهاب الرقمي.

تحركت الأمم المتحدة لمقارعة خطر الإرهاب الدولي بخط تصاعدي يؤشر بوضوح تطور الوعي الدولي بمخاطر الإرهاب وتداعياته على الأمن والسلم العالمي . ويمكن التمييز في هذا التحرك الأممي بين مرحلتين رئيسيتين ، تمثلت المرحلة الأولى في مواجهة الإرهاب التقليدي بصورته المادية والدموية على أرض الواقع ؛ وكان أكبر رصيد من الانجازات حققته منظومة الأمم المتحدة في هذا المضمار يتمثل بوضع نظام معاهدات واتفاقيات دولية يتألف من ست عشرة اتفاقية دولية لمكافحة الأنشطة الإرهابية وتجريم الدول والكيانات التي تلجأ لاستخدامها . وفي هذا السياق لم تكنف الأمم المتحدة بدعوة الدول إلى الالتحاق بهذه الاتفاقيات ومتابعة مدى التزامها بتنفيذ بنودها من جانب الدول الأعضاء فحسب ، بل ذهبت إلى أبعد من ذلك على طريق ترصين البناء القانوني لمكافحة الإرهاب ، عبر تقديم المساعدة القانونية للبلدان بشأن تحري أفضل سبل تنفيذ أحكام المعاهدات في إطار تشريعاتها الوطنية؛ لاسيما بعد أن اتخذ المجلس الاقتصادي والاجتماعي التابع للأمم المتحدة توصية بأن تأخذ المنظمة على عاتقها دوراً رئيساً في رسم سياسة منع الجريمة وتحقيق العدالة الجنائية دولياً ، وقد تحقق ذلك بموافقة الجمعية العامة للأمم المتحدة في العام 1950 ، وتم إنشاء (اللجنة الاستشارية لخبراء منع الجريمة) التي يقع على عاتقها مهمة مكافحة الجريمة



وتقديم المشورة للأمين العام وإيجاد البرامج ووضع الخطط ورسم سياسات لتدابير دولية في مجال منع الجريمة ومعاملة المجرمين⁽³⁶⁾ من واقع قناعتها بأهمية ضمان التكامل بين البنى والأدوات القانونية من جهة والاستراتيجيات المطبقة على أرض الواقع لمواجهة خطر الإرهاب الدولي من جهة أخرى ، أصدرت الأمم المتحدة عبر جمعيتها العامة ومجلس الأمن فيها مجموعة من القرارات الدولية التي اعتمدت بموجب الصلاحيات الواردة في الفصل السابع من ميثاق الأمم المتحدة،⁽³⁷⁾ والتي تضمنت التحذير من تزايد الأنشطة الإرهابية وتنوع صورها وفداحة نتائجها على الأمن والسلم الدوليين، وإدانة الأعمال الإرهابية بأقوى العبارات أيًا كان دوافعها أو مرتكبوها بوصفها أعمالاً إجرامية تهدد السلام والأمن الدوليين وتتنافى مع مقاصد ومبادئ ميثاق الأمم.⁽³⁸⁾ مع التأكيد بأن الإرهاب لا يمكن دحره إلا باتباع نهج شامل مطرد ينطوي على مشاركة وتعاون فعليين من جانب كافة الدول والمنظمات الدولية ، ومضاعفة الجهود على الصعيدين الوطني والعالمي لنزع أسباب التطرف والإرهاب وتصفية العوامل والأجواء المساعدة عليه بالمقام الأول عبر الدعوة إلى تعزيز الحوار والتفاهم بين الحضارات لمنع استهداف العشوائيين للأديان والثقافات أو ربطها بالإرهاب ، ومعالجة الصراعات الإقليمية المتبقية دون حل والقضايا العالمية لإسهامها في تعزيز جهود مكافحة، مع التشديد على أهمية دور وسائل الإعلام والمجتمع المدني والديني والمؤسسات التعليمية في تعزيز الحوار وتوسيع آفاق التفاهم وتشجيع التسامح وتهيئة بيئة لا تفضي إلى التحريض على الإرهاب ، وبيان فاعلية تدابير احترام حقوق الإنسان والحريات الأساسية وسيادة القانون بوصفها عناصر أساسية في الوقاية من أفة الإرهاب والتطرف. في ضوء ما تقدم وجه مجلس الأمن دعوة إلى دول العالم لاتخاذ التدابير للتصدي للتحريض على ارتكاب أعمال الإرهاب بدافع التطرف واستنكار المحاولات الرامية إلى تبرير أو تمجيد الأعمال الإرهابية التي قد تحرض على ارتكاب المزيد من تلك الأعمال واستعمال جميع الوسائل القانونية لهذا المسعى وحرمان من يخططون لأعمال الإرهاب أو يمولونها أو يرتكبونها مع التأكيد على أهمية التعاون الدولي في مكافحة الإرهاب عبر الدعوة إلى الالتحاق وتنفيذ الاتفاقيات الدولية ذات الصلة والتنسيق فيما بين الدول لمنع وقوع أعمال الإرهاب في المقام الثاني كانت الدعوة الأممية لدول العالم إلى اتخاذ الاجراءات والتدابير العملية الفاعلة لمكافحة الأعمال الإرهابية وملاحقة ومحاسبة مقترفيها عبر الزامها بالآتي:

- 1- الامتناع عن تقديم أي شكل من اشكال الدعم الصريح والضمني للكيانات الإرهابية ، مع وضع حد لعملية تجنيد أعضاء الجماعات الإرهابية ومنع تزويد الإرهابيين بالسلاح .
- 2- عدم توفير الملاذ لمن يمولون الأعمال الإرهابية أو يديرونها أو يرتكبونها ، منع استخدام أراضي الدول لانتقال في تنفيذ تلك المارب ، فرض ضوابط مشددة على الحدود وعلى إصدار الأوراق الثبوتية ووثائق السفر .
- 3- تعزيز التدابير الرامية إلى كشف ووقف تدفق التمويل والأموال للأغراض الإرهابية ومنع الإرهابيين من استغلال الأنشطة الاجرامية الأخرى ك(الاختطاف ، والاتجار بالبشر والمخدرات والأسلحة) لتمويل أنشطتهم الإرهابية ، وتجريم ومحاسبة كل من يمول الأعمال الإرهابية أو يديرها أو يدعمها أو يرتكبها أو يورد السلاح إليهم.
- 4- تشجيع الدول على تبادل المعلومات على وجه السرعة مع الدول الأعضاء و تقديم تقارير إلى لجنة مكافحة الإرهاب حسب جدول زمني تحدده اللجنة بعد الإجابة عن كل أسئلتها واستفساراتها ، وتزويد اللجنة بأسماء من يشاركوا من أفراد تلك الكيانات الإرهابية في تمويل أو دعم أعمال أو



أنشطة القاعدة والتنظيمات الإرهابية. بغية المساعدة في مواجهة الأنشطة الإرهابية وانتقال الإرهابيين إلزام الدول.

5- دعوة المنظمات الدولية لتعزيز التعاون مع الأمم المتحدة في نطاق ولايتها بهدف تطوير قدرتها على معاونة الدول الأعضاء في جهودها على التصدي للتهديدات الإرهابية. وأن تعمل مع لجنة مكافحة الإرهاب والمنظمات الدولية الأخرى من أجل تسهيل تبادل أفضل الممارسات في مجال مكافحة الإرهاب ، مع عزم المجلس على عقد اجتماعات منتظمة مع رؤساء هذه المنظمات لتحقيق هذه الغايات⁽³⁹⁾. مع تزايد خطر الإرهاب الدولي وبروز وانتشار نوع جديد من الجريمة المرتبطة بالحاسوب الآلي بفعل تسارع وتيرة التطور التقني في أنظمة المعلومات والاتصالات وما أفرزه ذلك التهديد من أضرار ومخاطر على أمن البلدان والأفراد لاسيما بعد دخول الشبكة الدولية للمعلومات بوسائلها المتنوعة والمتطورة على خط الإرهاب الدولي ومواجهته ، تزايدت الحاجة إلى تضافر الجهود الدولية وتعاضدها تحت مظلة المنظمات الدولية والإقليمية لمواجهة هذا التهديد ، وكانت الأمم المتحدة المحفل العالمي الأهم لترجمة هذه الجهود واستثمارها الأمثل في هذه المواجهة ، لما تتمتع به هذه الأخيرة من مصداقية في مجال تعزيز التعاون الدولي لتحقيق مقاصدها في ضمان الأمن والسلم الدوليين في مواجهة مختلف التهديدات العالمية بضمنها خطر الإرهاب الدولي،⁽⁴⁰⁾ . فتزايد تبعاً لذلك اهتمام الأمم المتحدة بهذا الخطر المتصاعد والمتجدد بوسائله وشهدت مواجهة الإرهاب نقلة نوعية إلى الحاسب الآلي والفضاء الرقمي. وتحركت المنظمة الدولية المتحدة في طريق هذه المواجهة المستجدة عبر ثلاثة محاور؛ تمثل المحور الأول في الادانة والتحذير من مخاطر الإرهاب بطوره الجديد وتطوير الوعي الدولي بتداعياته على أمنها والسلام الدولي عبر سلسلة من القرارات والجهود الأممية. قد بدأت الأمم المتحدة رحلتها في هذا المضمار التقني في المؤتمر الدولي الأول لحقوق الإنسان الخاص باثر التقدم التكنولوجي على حقوق الإنسان في طهران عام 1968 إذ تبنت الجمعية العامة للأمم المتحدة توصياته وأبرزها اعتبار الحاسب الآلي أكبر تهديد يواجه حق الإنسان بالخصوصية والحرية الشخصية كونها تعد من أدوات المراقبة والتطفل الحديثة خاصة إذا ما تم تخزين البيانات الشخصية على الحاسب الآلي وتحليلها⁽⁴¹⁾. فتم في مؤتمر الأمم المتحدة السابع لمنع الجريمة في ميلانو عام 1985 تكليف لجنة من عشرين خبيراً لدراسة موضوع حماية نظم المعلومات والاعتداء على الحاسب الآلي وإعداد تقرير يتضمن أهم المقترحات والتوصيات لمكافحة الظواهر الاجرامية المتعلقة بالحاسبة الالكترونية لعرضه على المؤتمر الثامن للوقاية من الجريمة الذي تبناه مؤتمر هافانا والذي تم فيه أيضاً التأكيد على أن التكنولوجيا قد تولد أشكالاً جديدة من الجريمة ، ينبغي اتخاذ تدابير ملائمة ضد حالات استعمالها ؛ مع الإشارة إلى مسألة الخصوصية التي يمكن أن تخرق عن طريق الاطلاع على البيانات الشخصية المخزنة داخل نظم الحاسبات الآلية والتي تشكل انتهاكاً لحقوق الإنسان وحرمة الحياة الخاصة ؛ مؤكداً على وجوب اعتماد ضمانات ملائمة لصون السرية وإقرار نظم تكفل وصول الأفراد إلى هذه البيانات لغرض تصحيح الأخطاء فيها . وشجع المؤتمر على تبني التشريعات الحديثة التي تجرم وتتناول جرائم الحاسب الآلي. في المؤتمر التاسع لمنع الجريمة برعاية الأمم المتحدة في القاهرة عام 1995 تم التأكيد على وجوب حماية الحياة الخاصة للإنسان في ملكيته الفكرية من تزايد مخاطر التكنولوجيا ووجوب التنسيق والتعاون بين أفراد المجتمع الدولي لاتخاذ الاجراءات المناسبة للحد منها . وفي المؤتمر العاشر لمنع الجريمة في بودابست ، جرى اعتبار جرائم الحاسب الآلي نمطاً جديد من الجرائم المستحدثة مع وجوب العمل على اتخاذ تدابير مناسبة للحد من أعمال القرصنة



(42) بعد أحداث الحادي عشر من سبتمبر 2001، أصبحت مكافحة الإرهاب من أولويات المجتمع الدولي، بعد أن أمسى أكثر شمولية وتطوراً باستخدام معطيات الثورة المعلوماتية وأشد فتكاً وتأثيراً على الأمن العالمي، فكانت استجابة الأمم المتحدة أكثر حزمًا وشمولاً مع هذه المستجدات، عبر قيادتها حملة دولية لمكافحة الإرهاب بطوره المعاصر، مهدت لها بسلسلة من القرارات الدولية لتنبية الرأي العام العالمي وتنمية الوعي الأمني بمخاطر هذه الموجة الجديدة من الإرهاب تبعتها حملة عالمية نفذتها ووكالات الأمم المتحدة مثل: (منظمة التربية والعلوم والثقافة التابعة للأمم المتحدة "اليونسكو"). في المؤسسات التربوية والثقافية ووسائل الاعلام، للتوعية في أنحاء العالم ضد التشدد، الذي يلقي مساعدة من الإنترنت. اتخذت في هذا السبيل، الجمعية العامة للأمم المتحدة في الدورة 258/56 في 31 من يناير 2002 قراراً يدعو إلى استخدام تكنولوجيا الاتصال والمعلومات من أجل التنمية (43). وأصبحت قضية أمن المعلومات مرتبطة بحظر استخدام تكنولوجيا الاتصال والمعلومات للتأثير أو الهجوم على وسائل تكنولوجيا الاتصال والمعلومات الخاصة بدولة أخرى، مواقف تشكل تهديداً للسلم والأمن الدوليين (44). هو المسعى الذي تجلت محاوره وملامحه بصورة أكثر تفصيلاً في الرسالة التي وجهها الأمين العام للأمم المتحدة "كوفي عنان" في 15 من مايو 2004 وجاء فيها "في عالم يتزايد فيه الترابط وإقامة الشبكات، أضى من المهم للغاية ضمان سلامة نظمنا وهياكلنا التحتية الحيوية من هجمات مجرمي الفضاء الإلكتروني، والعمل في الوقت نفسه على بث الثقة في التعاملات الإلكترونية وغيرها من الخدمات والتطبيقات الإلكترونية الأخرى". وطالب أمين عام الأمم المتحدة الدول الأعضاء وأصحاب المصلحة بالمساعدة في: زيادة الوعي العالمي بأمن الفضاء الإلكتروني، إنشاء شبكة دولية للمبادرات والتدابير المضادة القائمة على تكنولوجيا المعلومات والاتصالات لتعزيز الأمن وبناء الثقة في استعمال تكنولوجيا المعلومات والاتصالات. (45) أدركت الأمم المتحدة أن إحكام القبضة على الفوضى الحادثة داخل الفضاء الإلكتروني يتطلب إطاراً قانونياً يحكمه وينظم استخدامه (46). وسعيًا إلى استكمال هذا البناء القانوني لمكافحة الإرهاب وتوفير أدواته الفاعلة، اتخذ مجلس الأمن، في 28 سبتمبر عام 2001 قراراً بالعدد (1373) أجاز تأسيس لجنة خاصة لمكافحة الإرهاب تتألف من 15 خبيراً دولياً في مجال مكافحة الإرهاب، هدفها، مناقشة الأخطار القائمة والمحتملة في مجال أمن المعلومات الدولي، والإجراءات الممكنة لوضع الأسس الدولية التي تهدف إلى تقوية أمن نظم الاتصالات والمعلومات العالمية. وكانت تلك هي المرة الأولى التي ينتم فيها اتخاذ قرار سياسي على المستوى الدولي لترجمة الجهود الدولية إلى خطوات عملية في مجال مكافحة الإرهاب المرتبط بالإنترنت (47) في خطوة لاحقة و متممة صدر قرار من مجلس الأمن في عام 2004، بالعدد 1535، بإنشاء المديرية التنفيذية للجنة مكافحة الإرهاب بهدف توفير مشورة الخبراء إلى اللجنة في كافة المجالات التي يتناولها القرار 1373. كما استهدف إنشاء المديرية التنفيذية تيسير تقديم المساعدة التقنية للبلدان، فضلاً عن زيادة توثيق التعاون والتنسيق داخل منظومة مؤسسات الأمم المتحدة وفيما بين الهيئات الإقليمية وحكومات الدول لتعزيز التعاون وتبادل الخبرات وتطوير قدرتها على مواجهة الإرهاب كما جاء في نصّ القرار رقم (1455 في 2003) والقرار الدولي (1805 في 2008) (48) منذ حزيران 2008 قامت لجنة مكافحة الإرهاب ومديريتها التنفيذية بإحالة 213 طلباً للمساعدة التقنية؛ وافق المانحون على متابعة 92 منها؛ وأنجز بنجاح 42 منها. كما قامت فرقة العمل المعنية بالتنفيذ في مجال مكافحة الإرهاب والمديرية التنفيذية للجنة مكافحة الإرهاب وفرع منع الإرهاب التابع لمكتب الأمم المتحدة المعني بالمخدرات والجريمة أيضاً بتشكيل شراكات مع ثلاث دول



أعضاء في سياق مبادرة المساعدة المتكاملة لمكافحة الإرهاب، بغية تيسير توفير المساعدة التقنية للدول الأعضاء بطريقة متكاملة. وتساعد هيئات مكافحة الإرهاب التابعة لمجلس الأمن، إلى جانب فرع منع الإرهاب بمكتب الأمم المتحدة المعني بالمخدرات والجريمة، البلدان في صياغة تشريعات وطنية ملائمة للتصدي للإرهاب⁽⁴⁹⁾. إيماناً من الأمم المتحدة بالأمال المعلقة عليها في مجال تعزيز التعاون الدولي لنقل الخبرات في مجال الفضاء الرقمي وتقليص الهوة بين دول العالم واستثمار ما تتيحه تكنولوجيا الاتصال والمعلومات من فرص لدفع جهود التنمية والاستثمار في الدول النامية، ومواجهة ما تخلفه هذه التقنيات الرقمية من تهديدات على أمن البلدان والمستخدمين. وسعيًا منها لتهيئة المسار الدولي لاعتماد خطوات أكثر فاعلية في تطوير القدرة على مواجهة الإرهاب الرقمي، تبنت هذه المنظمة العالمية مسألة عقد قمة عالمية في تونس في تشرين الثاني عام 2005 حول مجتمع المعلومات وآليات استخدامها، فاعترفت هذه القمة بأن "الإنترنت أضحت عنصرًا مركزيًا في البنى التحتية لمجتمع المعلومات ووسيلة عالمية مهمة للاتصالات والتجارة، اكتسبت أهمية فائقة لدى الشعوب والحكومات في البلدان كافة، كما يتزايد دورها الحيوي في مجال الأمن القومي". كما أكدت هذه أن حرية التعبير والتنقل الحر للمعلومات والأفكار والمعرفة ضرورية لمجتمع المعلومات، مع الدعوة إلى مراقبة الإنترنت بحجة الحفاظ على الأمن الدولي واحترام المؤسسات الملكية الفكرية ومكافحة الأموال⁽⁵⁰⁾. بيد أن أهم ما يمكن تسجيله بخصوص موضوعه الإرهاب الرقمي، من نتائج لهذه القمة العالمية توصيتها بضرورة العمل على تبني إجراءات وقائية للأمن الحاسوبي بالتركيز على المصارف لإجراء معاملات موثوق بها مباشرة على الإنترنت، وتشجيع البلدان على صياغة تشريعات أمنية تتعلق بتكنولوجيا المعلومات، إقامة جهاز اتصال لمعالجة الحوادث والاستجابة لها في الوقت الحقيقي، وضع شبكة تعاونية لتبادل المعلومات⁽⁵¹⁾ لدى مراجعة حزمة القرارات التي اتخذها مجلس الأمن الدولي في مواجهة الموجة الجديدة من إرهاب القاعدة بعد عام 2001، يلاحظ غياب الإشارة الصريحة لمفهوم الإرهاب الرقمي، وتأخر الإشارة الضمنية والعبارة بصيغة التحذير للإرهاب المرتبط بصورة أو أخرى بالشبكة الدولية للمعلومات في هذه القرارات، حتى عام 2005، حينما صدر قرار مجلس الأمن الدولي بالعدد (1617) الذي أعرب عن "قلقه إزاء استعمال شتى الوسائل بما فيها الإنترنت من جانب الإرهاب في الدعاية والتحريض على العنف الإرهابي". وجاءت القرارات اللاحقة لتستكمل طريق مواجهة الإرهاب باستخدام الشبكة الدولية للمعلومات عبر متابعتها - التي لم تتعد سقف التحذير في كل الأحوال - لما يستجد من استخدامات لهذه الشبكة في العمليات الإرهابية، وهو التطور الذي يمكن تأشيرته بوضوح في القرارات اللاحقة التي صدرت عن مجلس الأمن ولاسيما القرارين (1624 لعام 2005)، (1822 لعام 2008) الذي دعى الدول إلى "التعاون لمنع الإرهابيين من استغلال التكنولوجيا المتطورة والاتصالات والموارد التحريضية على دعم الأعمال الإرهابية، وإبداء القلق إزاء لجوء القاعدة والتنظيمات الإرهابية إلى استغلال الإنترنت بشكل إجرامي لتنفيذ أعمال إرهابية" فكان مضمون المادة ينصرف إلى التحذير من إمكانية الاستخدام المباشر للإنترنت في الأعمال الإرهابية وليس في التحريض كما جاء في مضمون القرار السابق. وقد نبه مجلس الأمن في قرار لاحق بالعدد 1963 لعام 2010 إلى "ازدياد استخدام الإرهابيين للتكنولوجيا الجديدة للمعلومات والاتصالات وبخاصة الإنترنت لأغراض التجنيد وكذا التحريض على دعم الأعمال الإرهابية" بوصفها أنماط مستحدثة لاستخدامات الإرهابيين لمعطيات الشبكة الدولية للمعلومات. وكان القرار 2255 في 2015 أكثر شمولاً لطرق استخدام الإرهابيين للإنترنت في أنشطتهم



الإرهابية ، إذ تضمن " الإعراب عن قلقه من تزايد لجوء الإرهابيين إلى استعمال تكنولوجيا المعلومات ولاسيما شبكة الإنترنت من أجل تيسير الأعمال الإرهابية والتحريض على الإرهاب أو تجنيد مرتكبيها أو تمويلها " . كان المحور الثالث من محاور المواجهة الأممية لمخاطر الإرهاب الرقمي ، يتمثل في وضع الاستراتيجيات العملية والشاملة لمكافحة الأنشطة الإرهابية على أرض الواقع ، وذلك حينما نجحت الجمعية العامة للأمم المتحدة في إقرار استراتيجية عالمية موحدة لمكافحة الإرهاب في 8 أيلول/سبتمبر 2006؛ إذ عدت خطة عمل اشتملت على أسس من أهمها : (التصدي للأوضاع التي تقضي إلى انتشار الإرهاب ، واتخاذ تدابير لبناء قدرة الدول على مكافحته والوقاية المتقدمة منه ؛ وتعزيز دور الأمم المتحدة في مكافحة الإرهاب؛ وكفالة احترام حقوق الإنسان في سياق التصدي للإرهاب).⁽⁵²⁾ وقد كان الإرهاب بصورته الرقمية حاضراً في سياق هذه الاستراتيجية حينما أشارت الفقرة (12) من هذه الاستراتيجية إلى ضرورة تنسيق الجهود المبذولة على الصعيدين الدولي والإقليمي لمكافحة الإرهاب بجميع أشكاله ومظاهره على الإنترنت؛ بل واستخدام الأخير بالمقابل كأداة لمكافحة نقشي الإرهاب، مع التسليم في الوقت نفسه بأن الدول قد تحتاج إلى المساعدة في هذا الصدد؛ وهو الأمر الذي شجعتة الأمم المتحدة في الفقرة (13) من الاستراتيجية عبر العمل مع الدول الأعضاء والمنظمات الدولية والإقليمية ودون الإقليمية المعنية لتحديد وتبادل أفضل الممارسات في مجال منع الهجمات الإرهابية ضد الأهداف المعرضة للخطر بشكل خاص. تشجيع لجنة مكافحة الإرهاب ومديريتها التنفيذية على مواصلة تحسين اتساق وفعالية عملية تقديم المساعدة التقنية في مجال مكافحة الإرهاب، بتعزيز حوارها مع الدول والمنظمات الدولية والإقليمية ودون الإقليمية المعنية والعمل معها عن كثب، بعدة طرق من بينها: (تبادل المعلومات مع جميع الجهات المقدمة للمساعدة التقنية الثنائية والمتعددة الأطراف) .⁽⁵³⁾

مما تقدم يتضح الخط التصاعدي لاهتمام الأمم المتحدة بموضوعة الإرهاب عامة وما تمخض عنه من إرهاب رقمي بصورة خاصة من مستوى الإدانة والتحذير عبر القرارات المتفرقة الصادرة لمناسبة حصول أعمال إرهابية في عدد من دول العالم ، مروراً بمستوى البناء القانوني لصيغ المواجهة وصولاً إلى وضع الخطط والاستراتيجيات الشاملة والفاعلة لمواجهة الإرهاب ، دون أن يعني ذلك نهاية المطاف بالنسبة لمسيرة الأمم المتحدة في مجال مكافحة الإرهاب بكل أشكاله أو حتى نجاحها في مهمتها وانقضاء مسؤوليتها الدولية في هذا المجال ، بالنظر لتطور وسائل هذا الخطر الدولي وتباين أيقاعه وارتباطه بنزعة الشر والصراع المستوطنة في النفس الإنسانية ، واستمرارية الأعمال الإرهابية في أغلب بقاع العالم ناهيك عن خطورة تقاعس أو تواطئ بعض الدول مع التنظيمات الإرهابية لدواعي المصالح أو الأيديولوجيات المتقاربة.

المطلب الثاني // دور المنظمات العالمية المتخصصة في مكافحة الإرهاب الرقمي.

سيتم في هذا المطلب معالجة دور منطمتين عالميتين متخصصتين في مجال مكافحة الإرهاب الرقمي هما كل من (الاتحاد الدولي للاتصالات ، والمنظمة العالمية للملكية الفكرية) عبر فرعين. الفرع الأول // الاتحاد الدولي للاتصالات.

نشأ الاتحاد الدولي للاتصالات بمقتضى اتفاقية باريس عام 1865 تحت اسم (اتحاد التلغراف الدولي) ثم عدل الاسم ليصبح (الاتحاد الدولي للاتصالات السلكية واللاسلكية) ، وفي عام 1947 انضم الاتحاد إلى هيئة الأمم المتحدة وصار إحدى الوكالات المتخصصة في عمل الاتصالات المنضوية تحت مظلة الأمم المتحدة فأصبح بمثابة ملتقى دولي رئيس لهذه الأنشطة يضم في عضويته 482 عضواً من الشركات العلمية والصناعية العاملة بالقطاعين العام والخاص.ومن



المهام التي يضطلع هذا الاتحاد تعزيز التعاون الدولي للخدمات الهاتفية والسلكية واللاسلكية وتوسيع استخدامها بواسطة الجمهور وتطوير امكانيات الاتصالات السلكية واللاسلكية وتوزيع الموجات اللاسلكية ، كما يقوم الاتحاد بتقديم التوصيات الخاصة والدراسات الفنية المتخصصة في الاتصالات اللاسلكية وجمع المعلومات ونشرها .⁽⁵⁴⁾ من أجل بناء قدرات الدول الأعضاء - ولاسيما البلدان النامية- لتنسيق الاستراتيجيات الوطنية وحماية البنية التحتية للشبكات ضد المخاطر من خلال التوعية، والتقييم الذاتي، وبناء القدرات، وتوسيع نطاق المراقبة، والإنذار، وقدرات الاستجابة للحوادث للدول والجهات المعنية يعمل الاتحاد بصورة وثيقة مع المنظمات الأخرى المعنية على (وضع المعايير المتعلقة بالأمن المعلوماتي ؛ إذ يقوم الاتحاد، بالاشتراك مع الوكالة الأوروبية لأمن الشبكات والمعلومات ، بنشر خريطة الطريق المتعلقة بمعايير الأمن في مجال تكنولوجيا المعلومات والاتصالات، كما تعاون الاتحاد الدولي مع مجلس أوروبا لإنجاز الاتفاقية الأوروبية حول الجريمة الإلكترونية من أجل الاستعانة بها في عملية وضع إطار قانوني دولي. في مسعى أكثر شمولاً ، تم في المؤتمر الإقليمي حول الأمن الإلكتروني بالتعاون مع الاتحاد الدولي للاتصال في قطر في شباط من العام 2008، دعوة جميع الدول لوضع وتنفيذ إطار وطني للأمن الإلكتروني وحماية البنية التحتية الحرجة للمعلومات، والتي تُعدّ بمثابة خطوة أولى في سبيل التصدي للتحديات التي تواجهها جراء اتصالها بتكنولوجيا المعلومات والاتصال.⁽⁵⁵⁾ على صعيد آخر، طالبت القمة العالمية لمجتمع المعلومات في تونس في نوفمبر 2005، بأن ينسق الاتحاد الدولي للاتصالات آلية لبناء الثقة والأمن في مجال استخدام تكنولوجيا الاتصال والمعلومات ، عبر إطلاق برنامج الأمن الإلكتروني العالمي وهو إطار أعدّه الاتحاد الدولي للاتصالات بهدف اقتراح استراتيجيات للتوصل إلى حلول لتعزيز الثقة والأمن في مجتمع المعلومات. وتم لهذا الغرض تعيين فريق خبراء⁽⁵⁶⁾ لإسداء المشورة إلى الأمين العام للاتحاد ، بشأن المسائل المعقدة التي تكتنف موضوع الأمن السيبراني . وسيقوم الفريق بصياغة المقترحات التي ستُقدّم إلى الأمين العام للاتحاد بشأن الاستراتيجيات طويلة الأجل لتعزيز الأمن السيبراني في خمسة مجالات هي الآتي: في المجال القانوني ، يتم إسداء المشورة بشأن كيفية التعامل مع الأنشطة الإجرامية التي تُرتكب عبر شبكات تكنولوجيا المعلومات والاتصالات من خلال وضع تشريعات بطريقة متوافقة دولياً في مجال "التدابير التقنية والإجرائية" فيتم التركيز على التدابير الرئيسية الرامية إلى معالجة مواطن الضعف في منتجات البرمجيات، بما في ذلك خطط الاعتماد والبروتوكولات والمعايير. وتضع "الهيكل التنظيمية" إطار العمل واستراتيجيات الاستجابة، فيما يتعلق بمنع الهجمات السيبرانية وتتبعها والردّ عليها وإدارة الأزمات المتعلقة بها. بما في ذلك حماية أنظمة البنية التحتية الحرجة للمعلومات يركز مجال "بناء القدرات" على وضع استراتيجيات لآليات بناء القدرات من أجل: زيادة الوعي، نقل الخبرة المتخصصة، تعزيز الأمن السيبراني في إطار برنامج السياسات العامة الوطنية يهدف مجال "التعاون الدولي" إلى وضع استراتيجية للتعاون والحوار والتنسيق على الصعيد الدولي في مجال التصدي للأخطار الإلكترونية⁽⁵⁷⁾. الملاحظ مما تقدم انخراط الاتحاد الدولي للاتصالات في التفاصيل التقنية غير السياسية لمساعدة الدول والمنظمات والجهات المرتبطة بهذا الاتحاد في تهيئة وتطوير بيئة المعلومات واستخداماتها المختلفة وتعزيز قدراتها في مجال أمن المعلومات لمواجهة الأخطار التي تخلفها محاولات إساءة استغلال هذه التقنيات من قبل بعض الجهات الإرهابية والدولية.



الفرع الثاني // المنظمة العالمية للملكية الفكرية.

في عام 1967 تم التوقيع في ستوكهولم في السويد على اتفاقية المنظمة العالمية للملكية الفكرية وأصبحت هذه المنظمة إحدى الوكالات المتخصصة التابعة للأمم المتحدة اعتباراً من السابع عشر من ديسمبر عام 1974 . ومن أهدافها حماية الملكية الفكرية في شتى أنحاء العالم عن طريق التعاون بين الدول الأعضاء والمنظمات الدولية الأخرى كما تعمل المنظمة على متابعة تنفيذ الاتفاقيات المتعلقة بالتصميمات الصناعية وتصنيف السلع التجارية وحماية الأعمال الإدارية والفنية وحقوق الإنتاج . وتشجع المنظمة كذلك على توقيع معاهدات دولية جديدة والتنسيق بين التشريعات القومية وتقديم المساعدات القانونية والفنية للدول النامية بهدف حماية الملكية الفكرية وتنميتها وتغطية بعض أوجه القصور في مجال التوثيق العلمي ونقل التقنية الحديثة⁽⁵⁸⁾ بالرجوع إلى اتفاقية انشاء هذه المنظمة تتضح غايات هذه المنظمة في دعم الملكية الفكرية في جميع أنحاء العالم بجميع صورها (المصنفات الأدبية والفنية والعلمية والاختراعات) ومع تزايد الحاجة العالمية لحماية البرامج شكلت هذه المنظمة مجموعة عمل تضم عدداً من الخبراء بهدف حماية برامج الحاسب الآلي وبعد سلسلة من الاجتماعات والدراسات حول الأساليب المثلى لحماية برامج الحاسوب ، ساد الاتجاه لدى اغلب الدول إلى الميل إلى خضوع برامج الحاسوب لقوانين حماية حق المؤلف . وقد جاءت منظمة التجارة العالمية عام 1994 لتؤيد هذا التوجه وتستكمل طريقه من خلال ابرام اتفاقية التريبس المتعلقة بمواصفات التجارة المرتبطة بحقوق الملكية الفكرية وما تفرضه من التزامات على الدول الأعضاء لفرض اجراءات تنفيذية وعقوبات جنائية لمواجهة أيّ اعتداء على حق المؤلف وخاصة القرصنة .⁽⁵⁹⁾

المبحث الثالث // دور المنظمات الإقليمية في مجال مكافحة الإرهاب الرقمي.

التحقت المنظمات الإقليمية بالجهود الدولية لمكافحة الإرهاب بعد الامم المتحدة ، وكان الاتحاد الاوربي متصدراً في هذا الجانب بالنظر لتقدم دوله في مجال تقنية المعلومات من جانب ، ومشاركة هذه الدول في الجهود الدولية لمكافحة الإرهاب تحت مظلة الأمم المتحدة مما جعلها هدفاً للتنظيمات الإرهابية . وكان التحاق سائر المنظمات الإقليمية متأخراً بهذه الجهود ولم يكن الإرهاب الرقمي في اجندتها لمحدودية اعتمادها على الشبكة الدولية للمعلومات وانشغال دولها بهوموم وتحديات أكبر . ولتسليط الضوء على دور هذه المنظمات الإقليمية في مجال مكافحة الإرهاب الرقمي مع كثرتها سيتم اختيار نموذجين منها أحدهما من العالم المتقدم وهو الاتحاد الاوربي والآخر من العالم الثالث ويعيننا بصورة مباشرة هو منظمة الجامعة العربية.

المطلب الأول // دور الاتحاد الأوربي في مكافحة الإرهاب الرقمي.

مارس الاتحاد الأوربي دوراً مهماً في مجال التصدي لجرائم الإرهاب الرقمي عبر إقراره العديد من التوصيات الخاصة لحماية البيانات ذات الصبغة الشخصية من سوء الاستخدام وحماية تدفق المعلومات . ففي عام 1981 وقعت اتفاقية تحت مظلة المجلس الأوربي تتعلق بحماية الأشخاص في مواجهة المعالجة الالكترونية للبيانات ذات الصبغة الشخصية . كما صدر عن المجلس الأوربي العديد من القواعد التوجيهية في مجال جرائم الحاسب الآلي تضمنت وجوب تجريم العديد من السلوكيات التي تعد من الجرائم كالغش المعلوماتي وسرقة الأسرار المخزنة وتضمنت هذه القواعد عدداً من الاجراءات الفنية التي يتوجب اتخاذها لحماية نظم المعلومات من كل أشكال الانتهاك في عام 1980 جرى توقيع معاهدة مجلس أوربا الخاصة بحماية الاشخاص من مخاطر المعالجة الآلية



للبيانات ذات الطابع الشخصي والتي سرى مفعولها في أكتوبر عام 1985 وانطوت على توجيهات بصدد وجوب توفير قواعد تكفل حماية البيانات الشخصية من مخاطر المعالجة الآلية⁽⁶⁰⁾. فضلاً عن ذلك فقد صدر عن مجلس أوروبا العديد من التوصيات لحماية البيانات الحوسبية ولاسيما التوصية بالرقم (R81/1) بشأن تنظيم البيانات الطبية المعالجة آلياً في بنوك المعلومات وكذا البيانات الخاصة بحماية البحوث العلمية . ولا يمكن التغاضي كذلك عن جهود السوق الأوروبية المشتركة في مجال اصدار القرارات المعنية بحماية الفرد في مواجهة التطور التقني للمعلوماتية كما حصل في الاعوام 1979 و1982. وإذا كانت الحماية الأوروبية للبيانات الشخصية لم تتوج حتى الآن ، إلا أنه صدر إرشاد أوروبي في 11 آذار عام 1996 يتعلق بالحماية القانونية لقواعد البيانات واعتبار برامج الكمبيوتر ضمن مجال المؤلفات الفكرية الواجب حمايتها . وقد شملت هذه الحماية التركيب والتصميم أي حماية محتواها من الاقتطاع أو الاستعمال له أو لأي جزء منه وذلك بمجرد أن يتطلب تحضير وإعداد المحتوى من واضعي القاعدة توظيفاً ذا طابع اقتصادي مهم نوعاً وكما يضاف إلى ذلك الجهود التي قامت بها منظمة التعاون الاقتصادي والتنمية في مجال إرساء مبادئ حماية الخصوصية بشأن البيانات الشخصية والتي اهتمت بشكل عملي بحماية الخصوصية عبر الحدود والتي تبلورت على شكل قواعد إرشادية تم تبنيها رسمياً من قبل مجلس المنظمة في أيلول 1980 تحت عنوان (قواعد أوسيد الإرشادية بشأن حماية الخصوصية ونقل وتدقيق البيانات الشخصية). غير أن الحدث الرئيس الذي توج جهود الاتحاد الأوروبي في هذا المضمار قد تمثل بإصدار اتفاقية شاملة تتعلق بجرائم الحاسب في اجتماع المجلس بستراسبورغ في عام 2000 تضمن الدعوة إلى حماية مجتمعاتها من الجرائم الرقمية ووضع التشريعات الملائمة لمكافحتها بالنص على تجريم الأفعال التي تشمل اتلاف قواعد البيانات ووظائف الحاسب الآلي وانظمتها أو التزوير فيها أو الاحتيال وعقوبة المتسبب بذلك أو حتى الشروع في مثل هذه الجرائم والمساهمة فيها وضمن التعاون الدولي في مجال التحقيق وتبادل المعلومات لتحقيق الأمن المعلوماتي⁽⁶¹⁾ حالياً يعترزم الاتحاد الأوروبي وضع خطة جديدة يقوم بموجبها بتفتيش أجهزة الكمبيوتر عن بعد لمكافحة الجريمة الرقمية . وستشجع هذه الخطة تبادل المعلومات بين قوات الشرطة الالكترونية لملاحقة ومقاضاة المجرمين بعد أن توجه تحذيرات حول الأخطار المحدقة تلحقها انشاء فرق تحقيق تعمل عبر الحدود وترخص استخدام دوريات افتراضية لملاحقة المجرمين وضبط بعض النواحي في الإنترنت وذلك في مسعى لضمان احترام قوانين حماية المعلومات أثناء جمعها وتبادلها⁽⁶²⁾.

المطلب الثاني // جهود الجامعة العربية.

عند مراجعة ميثاق جامعة الدول العربية بوصفه دستور هذه المنظمة ، لا يمكن العثور فيه على ما يشير إلى الإرهاب وما يرتبط به من تفرعات. ومع ذلك ، فان تأويل الدلالة العامة لبعض النصوص الواردة في هذا الميثاق ، قد يخدم جهود مكافحة الإرهاب ، ومن ذلك ما جاء في المادة الثانية من الميثاق والتي اوضحت مقاصد هذه المنظمة في تحقيق التعاون بين الدول الأعضاء لصيانة استقلالها وسيادتها ، والتي ستتقاطع بالضرورة مع ما تنطوي عليه وسائل الإرهاب الرقمي من تجاوزات وإخلال لسلطة وسيادة الدول عبر التعرض لنظم المعلومات المرتبطة بالمؤسسات السيادية أو حتى امكانية التحريض ضد النظام باستغلال وسائل التواصل الالكتروني فضلاً عن امكانية استغلال المعلومات الحساسة وتوظيفها ضد مصالح الدولة العربية المستهدفة ، الأمر الذي يستدعي تعاون الدول العربية طبقاً لهذه المادة لمواجهة مثل هذه الأنشطة الإرهابية عبر الفضاء



الرقمي ، وهو الاتجاه الذي أكدته المادة الثالثة من الميثاق حينما خولت مجلس الجامعة ، تقرير وسائل التعاون مع الهيئات الدولية التي قد تنشأ في المستقبل لكفالة الأمن و السلام . وإذا جاز اعتبار الاعتداء على نظم المعلومات التي تعتمدها المؤسسات الرسمية للدول العربية ومحاولة تدميرها أو الإضرار بها وسرقة المعلومات أو حتى إشاعة الرعب والتحريض ضد النظام القائم التي تتم عبر آليات الإرهاب الرقمي من صور العدوان وفقاً لقواعد القانون الدولي وميثاق الأمم المتحدة ، فإن المادة السادسة من ميثاق الجامعة العربية قد أجازت للدولة أو الدول التي وقع عليها أيّ اعتداء أو حتى خشي وقوعه ، أن تطلب دعوة المجلس للانعقاد فوراً. ليقدر المجلس التدابير اللازمة لدفع هذا الاعتداء ، ويصدر القرار بالإجماع، فإذا كان الاعتداء من إحدى دول الجامعة، لا يدخل في حساب الإجماع رأى الدولة المعتدية⁽⁶³⁾ بعيداً عن اجواء الميثاق ، يلاحظ تأخر اهتمام جامعة الدول العربية على صعيد العمل الميداني حتى عام 1983 ، بدأت الجهود العربية المشتركة لمكافحة الإرهاب بالتوصل إلى الاستراتيجية الأمنية العربية التي أقرها مجلس وزراء الداخلية العرب والتي نصّت على ضرورة الحفاظ على أمن الوطن العربي و حمايته من المحاولات العدوانية للإرهاب والتخريب الموجهة من الداخل والخارج. وفي إطار الخطة الأمنية العربية الأولى تشكلت لجنة الجرائم المنظمة التي تناولت في اجتماعها الأول موضوع جرائم الإرهاب . وبناءً على توصيات اللجنة التي عرضت على مجلس وزراء الداخلية العرب في دورته السادسة بتاريخ 1987/12/12 أصدر قراراً يقضي بتكليف الأمانة العامة لمجلس وزراء الداخلية العرب بإعداد مشروع استراتيجية عربية لمكافحة الإرهاب بالتنسيق مع الأمانة العامة لجامعة الدول العربية. في مطلع 1988 أصدر مجلس وزراء الداخلية العرب قراراً ينصّ على تشكيل لجنة من ممثلي الدول العربية على مستوى الخبراء وبمشاركة الأمانة العامة لجامعة الدول العربية ، وأمانة مجلس وزراء الداخلية العرب لوضع تصور عربي لكيفية مواجهة ظاهرة الإرهاب . وبعد سلسلة من الاجتماعات التي عقدتها هذه اللجنة تم الانتهاء من الصياغة النهائية لمشروع الاستراتيجية العربية لمكافحة الإرهاب وإقرارها في الدورة الرابعة عشر لمجلس وزراء الداخلية العرب في 1997/1/5 . إلا أن إقرار الاتفاقية العربية لمكافحة الإرهاب لم يتم إلا في اجتماعات الدورة الـ15 لمؤتمر وزراء الداخلية العرب في 5 يناير 1998 ، حيث تم وضع عدد من الآليات لتنفيذ هذه الاستراتيجية لمواجهة الإرهاب. قد تضمن مشروع الاستراتيجية العربية لمكافحة الإرهاب عدداً من المنطلقات والأهداف والمقومات والآليات التي تحدد الأسس التي تقوم عليها سياسة مكافحة الإرهاب والسبل الكفيلة بتحقيق أقصى قدر من التعاون على الصعيد العربي والدولي لتطويق هذه الظاهرة والحد من الأخطار التي تشكلها على الدول المختلفة. فاعتبرت أن الأعمال الإرهابية هي أعمال عنف منظم يسبب رعباً وفزعاً ، كما حددت هذه الاستراتيجية لكل دولة عدة إجراءات وتدابير للوقاية من الإرهاب يبرز في مقدمتها زيادة دعم الدولة للأسرة بما يكفل التربية السليمة للنشء والشباب ، وتكثيف استخدام وسائل الاعلام المختلفة لتنمية الوعي الوطني والقومي ، مع حث الدول على اتخاذ تدابير فعالة وحازمة لمكافحة الإرهاب بمختلف صورته وأشكاله ، بعد تحديث قوانينها وتشريعاتها الجنائية لتشديد العقوبات على مرتكبي الأعمال الإرهابية ، وتجميد ومصادرة كافة الأموال الموجهة إلى هذه الأعمال وتشديد إجراءات المراقبة لمنع تسلل عناصر الإرهاب والتخريب أو تهريب الذخيرة والمتفجرات والسعي الحثيث للحيلولة دون اتخاذ أراضي الدول العربية مسرحاً لتخطيط وتنظيم أو تنفيذ أعمال إرهابية . كما تطرقت الاستراتيجية إلى موضوع تحديث وتطوير أجهزة الأمن من خلال دعمها بالمؤهلين وتوفير ما تحتاجه من معدات وتقنيات حديثة ، وكذلك وضع



خطط وقائية لمنع أي عمل إرهابي. على صعيد التعاون العربي فقد تضمنت الاستراتيجية عدة بنود أهمها تعزيز التعاون بين الدول الأعضاء لمنع ومكافحة الإرهاب وتقديم المساعدة المتبادلة في مجال إجراءات البحث الجنائي والتحري والقبض على الأشخاص الخارجين والمتهمين أو المحكوم عليهم في جرائم الإرهاب ، كما أكدت الاستراتيجية على أهمية تبادل الخبرات والخبراء والتقنيات الحديثة والمعلومات في مجال التعامل الأمني مع الجماعات الإرهابية ومواجهتها وتخص الأمانة العامة لمجلس وزراء الداخلية العرب بمتابعة مستجدات ظاهرة الإرهاب وسبل مكافحتها والتنسيق بين الدول العربية بهذا الشأن⁽⁶⁴⁾. في المؤتمر العربي الثامن عشر مجلس وزراء الداخلية العرب بتونس 2015 أوصى المشاركون باتخاذ الوسائل اللازمة للحد من "انتشار خطاب التطرف والطائفية". ودعا المؤتمر الدول الأعضاء إلى تبادل المعلومات بشأن المقاتلين الأجانب في بؤر التوتر في المنطقة العربية، وتقاسم التجارب بشأن التعامل مع المقاتلين العائدين. ووافق المؤتمر على الخطة النموذجية لتعزيز الدور الاستخباري في "الكشف عن المخططات الإرهابية"⁽⁶⁵⁾. إن أبرز ما يمكن رصده من جهود على صعيد منظمة جامعة الدول العربية في مضمار التصدي لجرائم الإرهاب الرقمي وجرائم الحاسوب ، اعتماد مجلس وزراء العدل العرب للقانون الجزائري العربي الموحد كقانون نموذجي بموجب القرار رقم 229 لسنة 1996 الذي تضمن فصلاً خاصاً بالاعتداء على حقوق الأشخاص الناتج عن المعالجات المعلوماتية مع النص بموجب المواد (463-461) منه على وجوب حماية الحياة الخاصة وأسرار الأفراد من خطر المعالجة الآلية وكيفية جمع المعلومات والاطلاع عليها . وعقوبة من يقوم بفعل الدخول بطريق الغش إلى نظام المعالجة الآلية للمعلومات أو عرقلة وإفساد نظام التشغيل أو تغيير المعلومات داخل النظام وتزوير وثائق المعالجة الآلية وسرقة المعلومات⁽⁶⁶⁾. من جانب آخر نجحت الجامعة العربية في إبرام الاتفاقية العربية لحماية حقوق المؤلف التي أوصى بها مؤتمر وزراء الثقافة المنعقد في بغداد عام 1981 التي دعت إلى وضع التشريعات اللازمة لحماية الملكية الأدبية والفنية والعلمية والتي قد تكون هدفاً للإرهاب الرقمي إذا ما وجدت طريقها للنشر على الشبكة الدولية للمعلومات لذا ألزمت المادة الثالثة والعشرون من هذه الاتفاقية الدول الأعضاء العمل على: "إنشاء مؤسسات وطنية لحماية حقوق المؤلف ويحدد التشريع الوطني بنية هذه المؤسسات واختصاصاتها" ولضمان تحقيق بنود هذه الاتفاقية والتزام الدول الأعضاء بها ، فقد انشئت المادة الرابعة والعشرون منها " لجنة دائمة لحماية حقوق المؤلف من ممثلي الدول الأعضاء لمتابعة تنفيذ هذه الاتفاقية وتبادل المعلومات بما يكفل حماية المصالح المعنوية والمادية للمؤلفين"⁽⁶⁷⁾. كما أبرمت المنظمة العربية للتربية والثقافة والعلوم الاتفاقية العربية لتيسير انتقال الإنتاج الثقافي العربي ، والتي ضمنت حق وسيادة الدول الأعضاء على كيانها السيادي في المجال المعلوماتي بالنص في المادة العاشرة على الآتي " مع عدم الإخلال بالاتفاقيات المبرمة فيما بين الدول عربياً ودولياً لا تمس أحكام هذه الاتفاقية حق كل دولة من الدول الأعضاء في أن تسمح أو تراقب أو تمنع وفقاً لتشريعها الوطني تداول أي مصنف في إطار سيادتها"⁶⁸. تعدّ هاتان الاتفاقيتان مثلاً واضحاً على جهود الجامعة العربية والمنظمات المتخصصة التابعة لها في مجال تنظيم حقوق المؤلف وإن كان يعد هذا جهداً متواضعاً بوصفها تصب في اتجاه الوقاية من جرائم الحاسوب⁽⁶⁹⁾.



الخاتمة.

أولاً // النتائج.

- 1- يُعدّ الحاسوب في ظل الإرهاب الرقمي الأداة والساحة الرئيسة لتحقيق النوايا الاجرامية للإرهابي على أرض الواقع ، فيكون الإرهاب الإلكتروني تبعاً لذلك صلة الوصل بين العالم الافتراضي والعالم المادي الذي يتحقق به التأثير المادي للمعلومات . -- الإرهاب الرقمي هو نتاج تلك الثغرات القيمية ذاتها ، مضافاً إليها الثغرات في نظم المعلومات وبرامجياتها في طور ما بعد الحداثة
- 2- إنّ اعتماد الدول على وسائل الاتصالات وشبكات المعلومات في إدارة مؤسساتها وتقديم خدماتها المختلفة ، قد ضخم من خطر الإرهاب الرقمي ، وزاد على ذلك التطور المستمر والتنوع في وسائله وصعوبة تعقب القائم به ، أو حتى تحديد حجم الضرر الذي يخلفه .
- 3- تتنوع وسائل الإرهاب الرقمي بدرجة كبيرة تبعاً لقدرة ومهارة الإرهابيين ، والهدف المنشود من الفعل الإرهابي ، والجهة المستهدفة . مثلما تتباين أهداف الإرهاب الرقمي بين مساحات مكانية وزمانية ونوعية مختلفة الحدود والأبعاد .
- 4- مع تنامي خطر الإرهاب الرقمي وتجاوزه حدود الدول وقدرته المتنامية على تقويض سيادتها وتهديد أمنها ، تزايدت الحاجة لتظافر الجهود الدولية في إطار المنظمات الدولية لمواجهة هذا التحدي واستئصاله .
- 5- يمكن تأشير التطور التدريجي في مستوى إدراك المنظمات الدولية لخطر الإرهاب وقدرتها على مواجهته مع تطور حجم التهديد الذي يفرضه هذا الأخير على الأمن والسلم الدوليين لاسيما بعد إفادته من معطيات الشبكة الدولية للمعلومات ومميزاتها لتنفيذ الأعمال الإرهابية ، دون أن نرصد توجهها مستقلاً من جانب تلك المنظمات لمواجهة الإرهاب الرقمي على سبيل الحصر والتخصيص .
- 6- انتقلت جهود المنظمات الدولية التي تقدمتها منظمة الأمم المتحدة في مجال مجابهة الإرهاب بضمنه الإرهاب الرقمي من مرحلة الشجب والتحذير غير المنتظم بنسق وإطار محدد إلى مرحلة التأطير القانوني ووضع الاستراتيجيات النظامية لمواجهة هذا التهديد .
- 7- مما يزيد من تعقيد مشكلة الإرهاب الرقمي ، غياب اتفاقية واضحة ومتخصصة على المستوى الدولي للتعامل مع هذا التحدي الجديد أو حتى تنظيم استخدام الفضاء الإلكتروني عبر تبيان حقوق مستخدميه وواجباتهم وبيان المعايير الواجب اتباعها للحيلولة دون وقوعهم في كمائن الإرهاب المعتمد على الشبكة الدولية للمعلومات .

ثانياً // التوصيات.

- 1- الحاجة إلى عقد اتفاقية دولية جماعية أو تبني استراتيجية واضحة المعالم تحت رعاية الأمم المتحدة لضمان الاستخدام السلمي للفضاء الرقمية والتعاون بين الدول لمكافحة مظاهر الإرهاب الرقمي.
- 2- من الضروري بمكان اعتماد معايير دولية متفق عليها لتحديد مفهوم الإرهاب الرقمي ، وتنظيم استخدام الشبكة الدولية للمعلومات ، وتأمين الحماية الممكنة لبرامج الحاسوب .
- 3- دعوة الدول إلى الانضمام إلى الاتفاقات الدولية الخاصة بمكافحة جرائم الإرهاب الرقمي وبخاصة المعاهدة الدولية لمكافحة جرائم المعلوماتية والإنترنت. مع الحاجة المستدامة لتطوير بنودها بما يتناغم مع التطورات المتسارعة في أنظمة الحاسوب والاستخدامات الإرهابية لها .



4- ضرورة تعزيز آليات التعاون والتنسيق وتبادل المعلومات والخبرات بين المنظمات العالمية والإقليمية المتخصصة والشاملة وكذلك بين الدول والأجهزة المعنية بمكافحة الإرهاب عبر الإنترنت ، بالاستناد إلى بروتوكولات عمل مشترك بغية الوقاية الاستباقية من الهجمات الإرهابية الرقمية والدموية ، والتعاون الفاعل في مجال ملاحقة الإرهابيين عبر تطوير اجراءات تفتيش الحاسب وضبط المعلومات التي يحويها ومراقبة المعلومات أثناء انتقالها ، والسماح للجهات القائمة على التفتيش بضبط برامج الحاسب والمعلومات الموجودة بالبرامج وفقاً للشروط الخاصة بإجراءات التفتيش العادية ، وإلقاء القبض عليهم ، عبر تفعيل الاتفاقيات الدولية الخاصة بضبط وتسليم المجرمين والإرهابيين .

5- التوصية بتقديم المنظمات الدولية والإقليمية المساعدة الكافية للدول في مجال تطوير وتكييف التشريعات الوطنية بما يضمن فاعليتها في مواجهة الأشكال المستحدثة من الإرهاب وتجريم أي استخدام غير أمن لتكنولوجيا المعلومات والاتصالات من جانب ، وضمان تناغم نصوصها مع الاتفاقيات والجهود الدولية في هذا المجال ، لإغلاق الثغرات القانونية التي من الممكن استغلالها من قبل التنظيمات الإرهابية للإفلات من الملاحقة والعقاب .

6- تعزيز التعاون والتنسيق الدولي مع المؤسسات الدولية المعنية بمكافحة الجريمة ، وبخاصة "الانتربول" لمواجهة كل أشكال جرائم الإرهاب عبر الإنترنت، ولاسيما في مجال تبادل المعلومات والخبرات الأمنية والفنية في رصد ومُتابعة كافة الأنشطة الإجرامية والإرهابية، خاصة فيما يتعلق بالنشاط الإرهابي التكنولوجي لتزايد المستمر من خلال عناصره الإجرامية المحترفة والمُنشرة في جميع أنحاء العالم .

7- السعي لإنشاء منظمة أو إبرام اتفاقية عربية متخصصة باستخدامات الشبكة الدولية للمعلومات للحيلولة دون استغلالها في الأعمال الإرهابية والإجرامية . وتفعيل دور المنظمات والإدارات والحكومات العربية في مواجهة هذه الجرائم عن طريق نظام الأمن الوقائي، والسعي إلى إنشاء الشرطة العربية أسوة بالشرطتين الأفريقية والأوروبية .
الهوامش.

1- أبو الفضل جمال الدين محمد بن مكرم ابن منظور ، لسان العرب ، الجزء الثاني ، مؤسسة الاعلمي للمطبوعات ، بيروت ، 2005 ، ص 1595 . أنظر كذلك : ابراهيم مصطفى واخرون ، المعجم الوسيط ، المكتبة الاسلامية للطباعة والنشر ، القاهرة ، 1972 ، ص 376.

2 - محمد بن يعقوب الفيروزبادي ، القاموس المحيط ، ط2، مؤسسة الرسالة ، بيروت ، 1987 ، ص118.

3- د.محسن الحيدري ، الإرهاب والعنف في ضوء القرآن والسنة والتاريخ والفقہ المقارن ، ج1، دار الولاة ، بيروت ، 2010 ، ص20

4- حارث سليمان الفاروقي، المعجم القانوني ، مكتبة لبنان ، بيروت ، ط5 ، 2003، ص690

5- المادة الأولى من اتفاقية جنيف لقمع الإرهاب لعام 1937 م.

6- قرار مجلس الأمن الدولي بالعدد 1566 لعام 2004 .

7- المادة الأولى من الاتفاقية العربية لعام 1998 م،

8- علي مطر ، الإرهاب الإلكتروني في القانون الدولي ، مقال منشور على موقع السكينة الإلكتروني بتاريخ 4 نوفمبر 2013 على الرابط : <http://www.assakina.com/about-php>

9- الموسوعة الإلكترونية على الرابط : <https://ar.wikipedia.org/>

10- تقرير اللجنة الدولية للصليب الاحمر ، القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة ، الحادي والثلاثين ، 2011 ، ص 67.

11- عادل عبد الصادق ، هل يمثل الإرهاب شكلاً جديداً من اشكال الصراع الدولي ، ملف الازهرام الاستراتيجي ، مركز الازهرام للدراسات السياسية والاستراتيجية ، اكتوبر 2010 .



- 12- الإرهاب والجرائم المعلوماتية ، مجلة معلومات ، المركز العربي للمعلومات ، بيروت ، العدد 80 ، تموز 2010 ، ص 100.
- 13- د. هشام بشير ، "مستقبل الإرهاب الإلكتروني.. تحديات وأساليب المواجهة"، ندوة المركز الدولي للدراسات المستقبلية والاستراتيجية في 11 أبريل 2012 على الرابط : <http://www.siyassa.org.eg/UI/Front/InnerPrint.aspx?NewsContentID=2450>
- 14- مشتاق طالب وهيب ، مفهوم الجريمة المعلوماتية ودور الحاسوب بارتكابها ، مجلة العلوم القانونية والسياسية ، جامعة ديالى ، المجلد الثالث ، العدد الأول ، 2014 ، ص 343 .
- 15- د. عفيفي كامل عفيفي ، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون : دراسة مقارنة ، منشأة المعارف ، الاسكندرية ، بلا سنة طبع ، ص 33
- 16- جلال محمد الزغبي واسامة احمد المناعسة ، جرائم تقنية نظم المعلومات الالكترونية : دراسة مقارنة ، دار الثقافة للنشر والتوزيع ، عمان ، 2010 ، ص 91.
- 17- مشتاق طالب ، مصدر سابق ، ص 347 .
- 18- محمود الرشدي ، العنف في جرائم الانترنت ، الدار المصرية اللبنانية ، القاهرة ، 2011 ، ص ص 38-39.
- 19- مشتاق طالب وهيب ، مصدر سابق ، ص 344 .
- 20- عبدالله بن عبدالعزيز بن فهد العجلان ، الإرهاب الإلكتروني في عصر المعلومات ، بحث مقدم إلى المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الإنترنت"، المنعقد بالقاهرة في المدة من 2 - 4 يونيو 2008م.
- 21- د. معتز محي الدين ، الإرهاب وتكنولوجيا المعلومات ، مقال منشور على موقع مدارك الإلكتروني ، على الرابط : www.madarik.net/News_Details.php?ID=21
- 22 - سايمون كولن ، التجارة عبر الإنترنت ، ترجمة يحيى مصلح ، بيت الأفكار الدولية ، نيويورك ، 1999 م ، ص 26 .
- 23- سراب ثامر احمد ، الهجمات على شبكات لحاسوب في القانون الدولي الإنساني ، اطروحة دكتوراه ، جامعة النهدين ، 2014 ، ص 84
- 24- ريتشارد كلارك وروبرت نيك ، حرب الفضاء الإلكتروني : التهديد الالي للأمن القومي وكيفية التعامل معه ، مركز الامارات للدراسات الاستراتيجية ، الامارات العربية المتحدة ، 2012 ، ص 107 .
- 25- محمود الرشدي ، العنف في جرائم الانترنت : الحماية والتأمين ، الدار المصرية اللبنانية ، القاهرة ، 2011 ، ص 85-87.
- 26- سراب ثامر احمد ، مصدر سابق ، ص ص 86-87 .
- 27- للمزيد من التفاصيل حول خصائص وقدرات هذا النوع من البرامج الالكترونية يمكن الرجوع إلى : احمد حسن خميس ، الهاكرز والكرارز ، درا البراء ، الاسكندرية ، ص 36 وما بعدها .
- 28- انمار موسى جواد ، الحرب في السياسة الخارجية الأمريكية بعد الحرب الباردة ، اطروحة دكتوراه ، كلية العلوم السياسية - جامعة النهدين ، 2015 ، ص 171.
- 29- التجسس هو التلصص وسرقة المعلومات من الأفراد أو المؤسسات أو الدول أو المنظمات ، ينظر : مهرا ن زهير المصري ، الإرهاب الإلكتروني ، مجلة باحثون العلمية ، بتاريخ 10/4 /2011 على الرابط : www.albahethon.com/?page=show_det&id=1320
- 30- تقوم فكرة هذا الاسلوب على السرقة من عدد كبير من المصادر بكميات ومقادير ضئيلة بحيث لا يفتن لها المجني عليه للسرقة . انظر : د. عفيفي كامل عفيفي ، مصدر سابق ، ص 28
- 31- John Knittel and Michael Soto, The danger of computer Hacking , The Rosen publishing Group, 200, p.37
- 32- عبد الصبور عبد القوي ، الجريمة الالكترونية ، دار العلوم للنشر والتوزيع ، القاهرة ، 2008 ، ص ص 92-93.
- 33- مهرا ن زهير المصري ، مصدر سابق .



- 34- كاظم مهدي النجار ، الإتفاقيات الدولية ومكافحة الإرهاب ، صحيفة النهار ، بغداد ، العدد 854 ، التاريخ 24 آذار 2016.
- 35- مصدر رقم 33
- 36- بعد انعقاد مؤتمر الأمم المتحدة لمنع الجريمة في كيوتو باليابان عام 1970 تم استبدال اللجنة الاستشارية بلجنة منع الجريمة ومكافحتها بناء على توصية للمجلس الاقتصادي والاجتماعي عام 1971 .
- 37- الدليل التشريعي للنظام القانوني العالمي لمكافحة الإرهاب ، إعداد مكتب الأمم المتحدة المعني بالمخدرات والجريمة (فيينا)، 2008 .
- 38- لقد ادانت العديد من قرارات مجلس الأمن الدولي ، أعمال الإرهاب في مختلف دول العالم ، ومنها على سبيل المثال:

- القرار 1189 في 1998 : إدانة هجمات القنابل الإرهابية في نيروبي ودار السلام ،
- القرار 1438 في 2002 : إدانة هجمات بالي في إندونيسيا 12 تشرين 2002
- القرار 1516 في 2003 : إدانة الاعتداءات بالقنابل في اسطنبول 15 تشرين 2003
- القرار 1465 في 2003 : إدانة الهجوم بالقنابل في بوغوتا كولومبيا في 7 شباط 2003 .
- القرار 1530 في 2004 : إدانة هجمات مدريد الإرهابية في 11 آذار 2004 .
- القرار 1611 في 2005 : إدانة الأعمال الإرهابية في لندن
- القرار 1618 في 2005 : دعم الشعب العراقي واستقلال سيادته ، إدانة الأعمال الإرهابية في العراق .
- القرار 2170 في 2014 : إدانة الأعمال الإرهابية لداعش في العراق وسوريا .
- القرار 2178 في 2014 : إدانة التطرف العنيف المفضي إلى الإرهاب والعنف الطائفي .
- القرار 2249 في 2015 : إدانة الاعتداءات الإرهابية التي ارتكبتها التنظيم في سوسة وانقرة وبيروت وباريس وكل الاعتداءات الأخرى .

- 39- راجع قرارات مجلس الأمن الدولي بهذا الخصوص : (1267 لسنة 1999) و (1333 لسنة 2000) و (1363 لسنة 2001) وكذلك القرارات (1373 لسنة 2001) و (1390 لسنة 2002) و (1452 لسنة 2002) والقرار (1455 لسنة 2003) وكذلك القرارات (1526 لسنة 2004) و (1566 لسنة 2004) و (1617 ، و 1624 لسنة 2005) والقرارات (1699 ، 1730 و 1735 لسنة 2006 و (1822 لسنة 2008) و (1904 لسنة 2009) و (1988 ، و 1989 لسنة 2011) و (2082 لسنة 2012)

- 40- محمود احمد عبابنة ، جرائم الحاسوب وابعادها الدولية ، دار الثقافة للنشر والتوزيع ، 2005، ص253 .
- 41- محمد امين الشوابكة ، جرائم الحاسوب والانترنت (الجريمة المعلوماتية) ، دار الثقافة للنشر والتوزيع ، عمان ، 2009، ص 73.

- 42- محمود احمد عبابنة ، مصدر سابق ، ص 156-157 .
- 43- قرار الجمعية العامة للأمم المتحدة في الدورة 258/56 ، في 4 أبريل 2002.
- 44- د. عادل عبد الصادق الأمم المتحدة ودعم الاستخدام السلمي للفضاء الإلكتروني ، دوريات - قضايا استراتيجياتية الخميس، 6 اغسطس 2015 - 12:14 م ، على الرابط :

www.acronline.com/print_article.aspx?id=22762

- 45- د. عادل عبد الصادق ، المصدر السابق
- 46- David G. Post, "Against Cyber Anarchy", Berkeley university, US, vol.7, 2002
- 47- عادل عبد الصادق ، مصدر سابق .

- 48 - في اطار ارساء الاساس القانوني لمكافحة الإرهاب في اطار الأمم المتحدة ، تبنى مجلس الامن الدولي القرار 1373 في 2001 : المتضمن انشاء لجنة تابعة لمجلس الأمن لتراقب تنفيذ هذا القرار على ان تقوم بالتشاور مع الامين العام بتحديد مهامها وتقديم برنامج عمل في غضون 30 يوم والنظر فيما تحتاجه . كما دعى القرار 1377 في تشرين الثاني 2001 ، لجنة مكافحة الإرهاب إلى استكشاف السبل التي يمكن من خلالها مساعدة الدول ، وان تستطلع بوجه خاص مع المنظمات الدولية والإقليمية تعزيز افضل الممارسات في المجالات المشمولة بالقرار 1373 في 2001 بما فيها اعداد قوانين نموذجية ، ومدى اتاحة برامج المساعدة التقنية والمالية والتنظيمية التي من



- شأنها تيسير تنفيذ القرار المذكور . وفي القرار 1455 في 2003 : دعى مجلس الامن إلى تحسين التنسيق بين لجنة القرار 1267 في 1999 واللجنة المشكلة بموجب القرار 1373 في 2001 .
- 49- الأمم المتحدة في مواجهة الإرهاب ، مقال منشور على الموقع الالكتروني للامم المتحدة على الرابط : <http://www.un.org/ar/terrorism>
- 50- د. خليل حسين ، التنظيم الدولي : النظرية العامة والمنظمات العالمية ، دار المنهل اللبناني ، بيروت ، 2010 ، ص 394-395.
- 51- للمزيد حول إعلان القمة يمكن الاطلاع على موقع القمة على الإنترنت على الرابط : www.un.org/arabic/conferences/ws15
- 52- ينظر للتفاصيل قرار الجمعية العامة للامم المتحدة الخاص بوضع استراتيجية لمكافحة الإرهاب بالعدد A/RES/60/288 الذي اتخذته في 8 أيلول/سبتمبر 2006 .
- 53- المصدر السابق .
- 54- د. خليل حسين، مصدر سابق ، ص 454-455.
- 55- للمزيد حول الإعلان الختامي للمؤتمر يمكن الاطلاع عليه على الرابط الآتي:
(http://www.ituarabic.org/2008/CIIP/Doha_Declaration.pdf)
- 56- يتألف فريق الخبراء رفيع المستوى من متخصصين مرموقين عالمياً في مجال الأمن السيبراني ومستمدين من خلفية واسعة النطاق تمثل: صانعي السياسات، الحكومات، الأوساط الأكاديمية، القطاع الخاص.
- 57- الاتحاد الدولي للاتصالات - التقرير السنوي للاتحاد، 2007، ص 38.
- 58- د. طارق عزت رخا ، المنظمات الدولية المعاصرة ، دار النهضة العربية ، القاهرة ، 2006 ، ص 214
- 59- عبد الصبور ، مصدر سابق، ص 159 - 163 .
- 60- محمد امين ، مصدر سابق ، ص 73
- 61- محمد امين، مصدر سابق ، ص 75-76
- 62- عبد الصبور ، مصدر سابق ، ص 168 .
- 63- ميثاق جامعة الدول العربية ، المواد (6، 3، 2)
- 64- عماد علو ، الجهود العربية المشتركة لمكافحة الإرهاب ، صحيفة الزمان ، لندن ، العدد 5377، السبت 26 اذار 2016 .
- 65- <http://www.alhurra.com/content/arab-interior-minister-meeting/284372.html>
- 66- ينظر للتفاصيل : المكتب العلمي لهيئة الشام الاسلامية ، القانون العربي الموحد: دراسة وتقييم ، سلسلة مطبوعات هيئة الشام الاسلامية بالعدد 24 ، 2014، ص 12 وما بعدها
- 67- المادتان (23 ، 24) من الاتفاقية العربية لحماية حقوق المؤلف لعام 1981
- 68- المادة العاشرة من الاتفاقية العربية لتيسير انتقال الانتاج الثقافي العربي لعام 1987
- 69- عبد الصبور ، مصدر سابق ، ص 170-172 .

المصادر.

أولاً // الكتب.

- ابراهيم مصطفى وآخرون ، المعجم الوسيط ، المكتبة الاسلامية للطباعة والنشر ، القاهرة ، 1972.
- أبو الفضل جمال الدين محمد بن مكرم ابن منظور ، لسان العرب ، الجزء الثاني ، مؤسسة الاعلمي للمطبوعات ، بيروت ، 2005 .
- احمد حسن خميس ، الهاكرز والكرakers ، درا البراء ، الاسكندرية ، 2007.
- المكتب العلمي لهيئة الشام الاسلامية ، القانون العربي الموحد: دراسة وتقييم ، سلسلة مطبوعات هيئة الشام الاسلامية بالعدد 24 ، 2014
- جلال محمد الزغبى واسامة احمد المناعسة ، جرائم تقنية نظم المعلومات الالكترونية : دراسة مقارنة ، دار الثقافة للنشر والتوزيع ، عمان ، 2010.
- حارث سليمان الفاروقي، المعجم القانوني ، مكتبة لبنان ، بيروت ، ط 5 ، 2003.
- خليل حسين ، التنظيم الدولي : النظرية العامة والمنظمات العالمية ، دار المنهل اللبناني ، بيروت ، 2010.



- ريتشارد كلارك وروبرت نيك ، حرب الفضاء الالكتروني : التهديد الآلي للأمن القومي وكيفية التعامل معه ، مركز الامارات للدراسات الاستراتيجية ، الامارات العربية المتحدة ، 2012.
- سايمون كولن ، التجارة عبر الإنترنت ، ترجمة يحيى مصلح ، بيت الأفكار الدولية ، نيويورك ، 1999 .
- طارق عزت رخا ، المنظمات الدولية المعاصرة ، دار النهضة العربية ، القاهرة ، 2006 .
- عبد الصبور عبد القوي ، الجريمة الالكترونية ، دار العلوم للنشر والتوزيع ، القاهرة ، 2008.
- عفيفي كامل عفيفي ، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون : دراسة مقارنة ، منشأة المعارف ، الاسكندرية ، بلا سنة طبع
- محسن الحيدري ، الإرهاب والعنف في ضوء القرآن والسنة والتاريخ والفقہ المقارن ، ج1، دار الولاة ، بيروت ، 2010.
- محمد امين الشوابكة ، جرائم الحاسوب والإنترنت (الجريمة المعلوماتية) ، دار الثقافة للنشر والتوزيع ، عمان ، 2009.
- محمد بن يعقوب الفيروزبادي ، قاموس المحيط ، ط2، مؤسسة الرسالة ، بيروت ، 1987.
- محمود احمد عباينة ، جرائم الحاسوب وابعادها الدولية ، دار الثقافة للنشر والتوزيع ، 2005.
- محمود الرشدي ، العنف في جرائم الإنترنت ، الدار المصرية اللبنانية ، القاهرة ، 2011.

ثانياً // الإطار الجامعية.

- انمار موسى جواد ، الحرب في السياسة الخارجية الأمريكية بعد الحرب الباردة ، اطروحة دكتوراه ، كلية العلوم السياسية - جامعة النهريين ، 2015.
- سراب ثامر احمد ، الهجمات على شبكات لحاسوب في القانون الدولي الإنساني ، اطروحة دكتوراه ، جامعة النهريين ، 2014.

ثالثاً // البحوث والدوريات .

- الاتحاد الدولي للاتصالات - التقرير السنوي للإتحاد ، 2007.
- الإرهاب والجرائم المعلوماتية ، مجلة معلومات ، المركز العربي للمعلومات ، بيروت ، العدد 80 ، تموز 2010.
- الدليل التشريعي للنظام القانوني العالمي لمكافحة الإرهاب ، إعداد مكتب الأمم المتحدة المعني بالمخدرات والجريمة (فيينا)، 2008.
- اللجنة الدولية للصليب الاحمر ، القانون الدولي الإنساني وتحديات النزاعات المسلحة المعاصرة ، الحادي والثلاثين ، 2011 .
- عادل عبد الصادق ، هل يمثل الإرهاب شكلاً جديداً من اشكال الصراع الدولي ، ملف الازهرام الاستراتيجي ، مركز الازهرام للدراسات السياسية والاستراتيجية ، اكتوبر 2010 .
- عبدالله بن عبدالعزيز بن فهد العجلان ، الإرهاب الإلكتروني في عصر المعلومات ، بحث مقدم إلى المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الإنترنت"، المنعقد بالقاهرة في المدة من 2 - 4 يونيو 2008م.
- عماد علو ، الجهود العربية المشتركة لمكافحة الإرهاب ، صحيفة الزمان ، لندن ، العدد 5377، السبت 26 اذار 2016
- كاظم مهدي النجار ، الإتفاقيات الدولية ومكافحة الإرهاب ، صحيفة النهار ، بغداد ، العدد 854 ، التاريخ 24 اذار 2016.
- مشتاق طالب وهيب ، مفهوم الجريمة المعلوماتية ودور الحاسوب بارتكابها ، مجلة العلوم القانونية والسياسية ، جامعة ديالى، المجلد الثالث ، العدد الأول ، 2014 .

رابعاً // المواثيق والقرارات الدولية.

- ميثاق الامم المتحدة لعام 1945
- ميثاق جامعة الدول العربية لعام 1945



- اتفاقية جنيف لقمع الإرهاب لعام 1937 م.
- الاتفاقية العربية لمكافحة الإرهاب لعام 1998 م
- الاتفاقية العربية لحماية حقوق المؤلف لعام 1981
- الاتفاقية العربية لتيسير انتقال الانتاج الثقافي العربي لعام 1987
- قرار الجمعية العامة للأمم المتحدة في الدورة 258/56 ، في 4 أبريل 2002.
- قرار الجمعية العامة للأمم في الدورة 288 /60 في 8 أيلول/سبتمبر 2006 .
- قرار مجلس الأمن الدولي بالعدد 1189 لسنة 1998
- قرار مجلس الأمن الدولي بالعدد 1267 لسنة 1999
- قرار مجلس الأمن الدولي بالعدد 1333 لسنة 2000
- قرار مجلس الأمن الدولي بالعدد 1363 لسنة 2001
- قرار مجلس الأمن الدولي بالعدد 1373 لسنة 2001
- قرار مجلس الأمن الدولي بالعدد 1377 لسنة 2001
- قرار مجلس الأمن الدولي بالعدد 1390 لسنة 2002
- قرار مجلس الأمن الدولي بالعدد 1438 لسنة 2002
- قرار مجلس الأمن الدولي بالعدد 1452 لسنة 2002
- قرار مجلس الأمن الدولي بالعدد 1455 لسنة 2003
- قرار مجلس الأمن الدولي بالعدد 1465 لسنة 2003
- قرار مجلس الأمن الدولي بالعدد 1516 لسنة 2003
- قرار مجلس الأمن الدولي بالعدد 1526 لسنة 2004
- قرار مجلس الأمن الدولي بالعدد 1530 لسنة 2004
- قرار مجلس الأمن الدولي بالعدد 1566 لسنة 2004 .
- قرار مجلس الأمن الدولي بالعدد 1611 لسنة 2005
- قرار مجلس الأمن بالعدد 1618 لسنة 2005
- قرارا مجلس الأمن الدولي بالعدد 1617، و 1624 لسنة 2005
- قرارات مجلس الأمن الدولي بالعدد 1699 ، 1730 و 1735 لسنة 2006
- قرار مجلس الأمن الدولي بالعدد 1822 لسنة 2008
- قرار مجلس الأمن الدولي بالعدد 1904 لسنة 2009
- قرارات مجلس الأمن الدولي بالعدد 1988، و 1989 لسنة 2011
- قرار مجلس الأمن الدولي بالعدد 2170 في 2014
- قرار مجلس الأمن الدولي بالعدد 2178 في 2014
- قرار مجلس الأمن الدولي بالعدد 2249 في 2015
- مجلس الأمن الدولي بالعدد 2082 لسنة 2012

خامسًا // مصادر الشبكة الدولية للمعلومات.

- الأمم المتحدة في مواجهة الإرهاب ، مقال منشور على الموقع الالكتروني للامم المتحدة على الرابط:
[/http://www.un.org/ar/terrorism](http://www.un.org/ar/terrorism)
- الموسوعة الالكترونية على الرابط : [/ https://ar.wikipedia.org](https://ar.wikipedia.org)
- علي مطر ، الإرهاب الالكتروني في القانون الدولي ، مقال منشور على موقع السكينة الالكتروني بتاريخ 4 نوفمبر 2013 على الرابط : <http://www.assakina.com/about-php>
- معتز محي الدين ، الإرهاب وتكنولوجيا المعلومات ، مقال منشور على موقع مدارك الالكتروني ، على الرابط :
www.madarik.net/News_Details.php?ID=21



-
- مهران زهير المصري ، الإرهاب الإلكتروني ، مجلة باحثون العلمية ، بتاريخ 10/4 /2011 على الرابط :
www.albahethon.com/?page=show_det&id=1320
- هشام بشير ، "مستقبل الإرهاب الإلكتروني.. تحديات وأساليب المواجهة"، ندوة المركز الدولي للدراسات المستقبلية والاستراتيجية في 11 أبريل 2012 على الرابط :
<http://www.siyassa.org/eg/UI/Front/InnerPrint.aspx?NewsContentID=2450>
(http://www.ituarabic.org/2008/CIIP/Doha_Declaration.pdf -
<http://www.alhurra.com/content/arab-interior-minister-meeting/284372.html> -
[www.accronline.com/print_article.aspx?id=22762-](http://www.accronline.com/print_article.aspx?id=22762)

المصادر الاجنبية.

- John Knittel and Michael Soto, The danger of computer Hacking , The Rosen publishing Group, 2000.
- David G. Post, "Against Cyber Anarchy", Berkeley university, US, vol.7, 2002 .