



دور المنظمات الدولية في مكافحة الارهاب الرقمي.

The role of international organizations in the fight against digital terrorism.

بحث مقدم من قبل

الاستاذ الدكتور سامر مؤيد عبد اللطيف

الاستاذ المساعد الدكتور نوري رشيد نوري

الاستاذ المساعد الدكتور منى محمد عبد الرزاق

جامعة كربلاء /// كلية القانون

الخلاصة.

يهدف البحث الى تحليل طبيعة الارهاب الرقمي وتبيان خصائصه واساليبه ، وتحري دور المنظمات الدولية في مكافحته ، باستخدام منهج التحليل الوصفي والاستنباطي .وللغاية اعلاه ، تقسيم الموضوع على ثلاثة مباحث ، يتناول أولها مفهوم الإرهاب الرقمي وخصائصه بوصفه عمليات غير مشروعة تتم بواسطة الحاسوب والشبكة الدولية للمعلومات للإضرار والحاق الدمار بالبنى المعلوماتية لأغراض سياسية ، اما المبحث الثاني فيتصدى للكشف عن جهود المنظمات العالمية في مجال مكافحة الإرهاب الرقمي عبر التركيز على منظمة الأمم المتحدة والإتحاد الدولي للاتصالات اما المبحث الثالث فمجاله البحث في جهود ودور المنظمات الإقليمية (الأوربية والعربية) في المسار ذاته.وقد توصل البحث الى نتائج من اهمها ملاحظة تطور اهتمامات المنظمات الدولية تتقدمها الامم المتحدة ومن بعدها الاتحاد الاوربي بموضوعه الارهاب دون ان تميز او تخص الارهاب الرقمي بمسار مستقل عن جهودها لمكافحة هذا التهديد الدولي.

الكلمات المفتاحية: دور ، المنظمات ، مكافحة ، الارهاب ، الرقمي.

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. The research has come to the resolution that the role of international organizations led by the United Nations and later the European Union Eduard in face of the terrorism has been escalating without discriminate or belong to a separate cyber terrorism course for its efforts to combat this international threat.

Key words: Role , Organizations , Combat , Terrorism , Digital.



المقدمة.

يعد الإرهاب الدولي من أخطر الظواهر التي يواجهها المجتمع الدولي اليوم بالنظر للخسائر التي يلحقها بالأرواح وبالبنى والمؤسسات المادية الى جانب ما يلحقه من اضرار بسمعة الدولة ومعنويات مواطنيها طالما ان هدفه نشر الخوف والذعر بين هؤلاء الابرياء ، 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. ومع تنامي التطور التقني في العالم لاسيما بفضل استخدام الحاسوب وظهور الشبكة الدولية للمعلومات وتزايد اعتماد الدول عليها في ادارة 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 حتي التنسيق بين الإرهابيين أنفسهم لتنفيذ عمليات ارهابية على ارض الواقع بصورة أكثر دماراً وأكثر بعداً عن مراقبة ومتابعة الأجهزة الأمنية لينتج نمطاً جديداً من الالهاب أصطلح عليه (الإرهاب الرقمي) وشاع استخدامه بين الأوساط الرسمية والعلمية بعد هجمات 11 ايلول عام 2001 . وفي مواجهة هذا التهديد الالكتروني للأمن العالمي انبرت المنظمات الدولية العالمية والإقليمية لصياغة القرارات والاستراتيجيات وبذل الجهود لتكون على مستوى التحدي. وفي 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 . والاهم من ذلك يكمن في الحاجة لإماطة اللثام عن الدور الذي تمارسه المنظمات الدولية في مجال ملاحقة هذا النوع المستحدث من الإرهاب الرقمي وما يمكن ان تضيفه وتضفيه على قدرة الدول في مجال مكافحة هذا الخطر المتسارع الخطى. وعند هذا المقام يمكن تحري مشكلة البحث في الكشف عن كنهه وخصوصية الإرهاب الرقمي ، ومن ثم تتبع الجهود التي بذلتها المنظمات الدولية العالمية والإقليمية في مجال مكافحته وما حققت من نجاحات وما اعترها من اخفاقات وما يعوزها من ادوات لاستكمال هذا الطريق الوعر. وعبر 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 اساس تقسيمه بين ثلاثة مباحث ، يتناول أولها مفهوم الإرهاب الرقمي وخصائصه ، اما المبحث الثاني فيتصدى للكشف عن جهود المنظمات العالمية في مجال مكافحة الإرهاب الرقمي عبر التركيز على منظمة الأمم المتحدة والإتحاد الدولي للاتصالات اما المبحث الثالث فمجاله البحث في جهود ودور المنظمات الإقليمية (الأوروبية والعربية) في المسار ذاته . ثم خاتمة تضمنت اهم النتائج والتوصيات التي تم التوصل اليها في ضوء معطيات البحث.

المبحث الأول /// مفهوم الإرهاب الرقمي واساليبه.

استقطب الإرهاب الرقمي على الرغم من حداثة ظهوره اهتمام الأوساط الرسمية والاكاديمية في العالم فكان ميدانا خصبا للجدل والإختلاف ، بالنظر لهلامية أبعاده وتنوع وتطور مظاهره والياتة ، وتباين أغراض وخلفيات من تناوله بالبحث والدراسة . ولتسليط الضوء على هذا المفهوم المستحدث من الإرهاب سيتم تقسيم هذا المبحث على مطلبين ، ينصرف الأول منهما الى 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 أن كلمة إرهاب تعني (الفرع والخوف والرعب) . وكلمة إرهاب مشتقة من الفعل المزيد (أرهب)؛ ويقال أرهب فلاناً: أي خوَّفه وفرَّعه، وهو نفس المعنى الذي يدل عليه الفعل المضعف (رَهَبَ). أما الفعل المجرد من نفس المادة وهو (رَهَبَ)، يَرْهَبُ رَهْبَةً وَرَهْبًا وَرَهَبًا فيعني (خاف) مع تحرز واضطراب. فيقال رَهَبَ الشيء رهبا ورهبة أي خافه، وكذلك يستعمل الفعل ترهب بمعنى توعد إذا كان متعدياً فيقال ترهب فلاناً: أي توعد⁽¹⁾ وأرهبه وإسترهبه أي اخافه وافزعه⁽²⁾ وتتفصل الرهبة عن الخوف لدى بعض اللغويين لتعني طول الخوف واستحكامه بالنفس ومنها انطلقت تسمية الراهب الذي يديم الخوف⁽³⁾. وفي 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⁾. ويتضح مما تقدم أن معاجم اللغة وقواميسها العربية والغربية ، قد جعلت من الخوف والترويع مقصداً ومعنى لعبارة الإرهاب وهو الأساس الذي إنطلق منه وأقره من تصدى لتعريف الإرهاب إصطلاحياً على الرغم من إختلافهم في التفاصيل ، الأمر الذي أفضى الى عدم وجود مفهوم دولي مُوحَّد للإرهاب بصفة عامة، والإرهاب الرقمي بصفة خاصة. وفي هذا السياق ، كانت إتفاقية 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⁾ وعرف 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 الإمتناع عنه، وكل الأعمال الأخرى التي تشكل إساءات ضمن نطاق المعاهدات الدولية المتعلقة بالإرهاب والتي لا يمكن تبريرها بأي إعتبار سياسي أو فلسفي أو إبيدولوجي أو عرقي أو ديني"⁽⁶⁾. فكان هذا التعريف مغزقاً في التركيز على الوسائل المستخدمة في الفعل الإرهابي على سبيل الحصر والتحديد الذي لا يمكن الارتكان اليه مستقبلاً إذا ما برزت وسائل ومظاهر ارهابية مستحدثة ومن ذلك على سبيل المثل (الإرهاب الرقمي والجرثومي) الذي شهدته الساحة الدولية في الوقت الرهن لتثبت عجز هذا التعريف عن الاحاطة لكل انواع الإرهاب .

وقريباً من التعريف أعلاه جاء الإتفاقية العربية لعام 1998 للإرهاب بأنه "كل فعل من أفعال العنف أو التهديد أيا كانت يواضعه أو أغراضه، يقع تنفيذاً لمشروع إجرامي فردي أو جماعي، ويهدف إلى إقضاء 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 اطاراً جامعاً دون تفصيلات دقيقة لاهم اليات الإرهاب دون الإشارة الواضحة الى غاياته أو دوافعه أو حتى تبيان الصور الأخرى منه. وإذا كان تعريف الإرهاب بصورته العامة مجالاً لاختلاف الراي وتباين الاجتهادات ، فان الوجه الجديد للإرهاب بصورته الرقمية ، قد إستوعب مساحة 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 الإستغراق في التفاصيل والاليات والمقاصد الإرهابية ، وذلك حين عرفت الإرهاب الرقمي على انه "إستخدام الانترنت لنشر أعمال إرهابية"⁽⁸⁾. وفي الموسوعة الالكترونية جرى تعريف الإرهاب الرقمي بأنه " إستخدام التقنيات الرقمية لإخافة وإخضاع الآخرين ؛ أو هو القيام بمهاجمة نظم المعلومات على خلفية دوافع سياسية أو عرقية أو دينية"⁽⁹⁾. وكان تعريف اللجنة الدولية للصليب الأحمر أكثر إسترسالاً في تقصي التفاصيل الفنية عند تعريفها للإرهاب الرقمي على أنه " عمليات تشن ضد أو عبر حاسوب بواسطة تيار بيانات وتهدف الى تحقيق اغراض منها اختراق النظام المعلوماتي أو جمع أو نقل أو تشفير أو تغيير البيانات أو التلاعب بها من قبل منفذ عملية الاختراق وإستخدام هذه الوسائل لتدمير أو تعطيل مجموعة متنوعة من الاهداف في العالم الحقيقي كالصناعات والبنى الاساسية"⁽¹⁰⁾ بيد أن الإرهاب الرقمي على وفق رأي آخر هو " نشاط هجومي متعمد ذو دوافع سياسية بغرض التأثير علي القرارات الحكومية أو الرأي العام بإستخدام 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 إستخدام الشبكة الدولية للمعلومات كوسيلة للاتصال والتنسيق بين الإرهابيين أو حتى منطلقاً لتنفيذ العمليات الإرهابية على ارض الواقع. على النقيض من اتجاه باحث اخر في تعريف الإرهاب الرقمي على أنه " تسخير التقنيات المتوافرة في الانترنت لأحاق إذى مادي أو معنوي أو إيجاد قلقلة كبيرة في الجهة المقصودة"⁽¹²⁾ الذي أسقط فاعلية الشبكة الدولية في الحاق الإذى 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، بإستخدام 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 والاهداف المنشودة ، إذ يشتمل على تطوير وإرسال شفرات الحاسب الالى الى الشبكة الدولية للمعلومات بغية تحقيق أغراض عدة تتمثل بالتدمير والانتقاص والتغيير والتعطيل والافساد للمعلومات أو البرامج الموجودة ، أو التهديد بإيقاع الضرر بصورة تخالف كل القوانين والمواثيق والإتفاقيات الدولية والقيم الاخلاقية وحتى الدينية.

2- جرائم تقنية ناعمة ، بعد الحاسب الالى والشبكة الدولية للمعلومات الاداة الرئيسية في ارتكابها ، مثلما يمكن إعتبار 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 الى وقت ولا الى 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 إستخدام الحاسوب واختراق انظمة الحماية المتوافرة ، إذ أن 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 متعددة الحدود، وعابرة للدول والقارات، وغير خاضعة لنطاق إقليمي محدود أو مسرح واحد إذ يمكن ان يستهدف الفاعل اماكن واهداف متفرقة في وقت واحد.⁽¹⁶⁾ إذ أن التقنيات الحديثة وما صاحبها من تقدم في مجال الاتصال الغي الحدود الجغرافية بين الدول بحيث ان الجريمة المعلوماتية تخطت حدود الدولة التي ترتكب فيها لتتعدى اثارها الى كافة البلدان على مستوى العالم، فالطبيعة العالمية للجريمة تمكن الجاني من ارتكاب جرائمه في دولة ما والتي ستؤثر على المجني عليه في دولة اخرى⁽¹⁷⁾

5- صعوبة إكتشاف 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 الإختراق للبيانات وإثبات الدليل على قيامها والقائمين عليها، والمرونة العالية لتنفيذ أنشطة الإرهاب الرقمي بإستخدام برامج وأدوات وحاسبات في اماكن وأوقات مختلفة ومتباعدة لإستهداف 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 الى الفاعل، وإنما كيانات منطقية تكون ضمن فضاء الحاسب الآلي يمكن بسهولة إخفائها والتخلص منها. وإنعدام الأثر الخارجي يعود الى 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 اساليب الإرهاب الرقمي بحسب محتواها وطريقة إستخدامها وغايات مستخدميها؛ فتتوزع بين ما يستهدف منها نظم المعلومات وبرامجياتها وما يرتبط بها من بنى بالضرر والدمار بصورة مباشرة، فتكون ساحة عملياتها وادواتها، المعلومات، وبين ما يجعل مزايا الشبكة الدولية للمعلومات وخدماتها ووسائل تنفيذ عملياته الإرهابية الدموية على ارض الواقع، فتكون المعلومات وسيلة لترجمة النوايا الاجرامية الى واقع مادي دموي دون ان تكون هذه المعلومات بحد ذاتها ساحة للفعل الإرهابي. وعلى اساس ما تقدم سيتم تقسيم هذا المطلب وفقاً لأساليب الإرهاب الرقمي على ثلاثة فروع هي الآتي:-

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

تعد الشبكة العالمية للمعلومات وسيلة إتصال 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 بإستخدام البريد الإلكتروني أو المواقع والمنديات وغرف الحوار الإلكتروني. إذ يمكن وضع رسائل مشفرة تأخذ طابعاً لا يلتفت 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⁾. والاكثر من ذلك فقد اسهمت هذه التقنية في تدفق الدعم والمساعدات اذ تتيح بواسطة الانترنت الوصول الى جمهور ضخم من المانحين المحتملين وتسمح للأعضاء بالتنسيق سريعاً مع اكبر عدد من الأتباع لضمان سريان سريع ومستمر للتعليمات يضمن اقصى درجات التنظيم لنشاطات المجموعات الإرهابية كما، وتجنيب الذين قد يتوزعون فوق رقعة جغرافية ضخمة، كما توفر منبرا للدعاية⁽²¹⁾.



وإذا كان الحصول على وسائل إعلامية كالقنوات التلفزيونية والإذاعية صعباً، فإن إنشاء مواقع على الإنترنت، وإستغلال منتديات الحوار وغيرها لخدمة أهداف الإرهابيين في الترويج لأفكارهم وكسب المؤيدين لهم أو حتى إبلاغ التعليمات والتدريبات لأنصارهم غداً سهلاً وممكناً، حتى يضمّنوا إنتشاراً أوسع، وحتى لو تم منع الدخول على بعض هذه المواقع أو تعرضت للتدمير تبقى المواقع الأخرى يمكن الوصول إليها. ومما 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 /// إختراق المواقع الإلكترونية وتدميرها.

يشمل هذا الأسلوب، اختراق المواقع والانظمة الإلكترونية عبر الشبكة والسطو على محتوياتها أو تغييرها أو إحداث الضرر أو حتى تدميرها لتحقيق أهداف غير مشروعة والمقصود بالتدمير هنا: "الدخول غير المشروع على نقطة ارتباط أساسية أو فرعية متصلة بالشبكة المعلوماتية من خلال نظام ألي (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 الإستيلاء على محتوياتها والسيطرة والتحكم فيها. ومن 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⁾ وتعد الفيروسات والديدان وسائل 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 والإنتشار، والانتقال من جهاز إلى آخر؛ إذ تحاول هذه البرامج إستغلال العيوب الموجودة في البرامج الأخرى والأخطاء التي يقع فيها مستخدمو الحاسوب قبل الدخول إلى المواقع المصابة بالعدوى الفيروسية أو فتح مرفقات الرسائل البريدية⁽²⁴⁾ ولفيروس الحاسب الآلي خصائص تتشابه إلى حد كبير مع الفيروس الطبيعي من نواح عدة، منها القدرة الفائقة على الاختفاء والاختراق والإنتشار مثل الفيروس الطبيعي، كما أن له القدرة على تغيير خصائص البرامج كما يقوم الفيروس الطبيعي بتغيير خصائص الخلايا المصابة. وتتعدد أنواع وإستخدامات 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 نظاما إلكترونيا محددًا ومنها ما يكون واسع الضرر والإنتشار. 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 إستنساخ نفسها ذاتياً بإستغلال 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 الإنتشار وصعوبة التخلص منها لقدرتها الفائقة على التناسخ والمراوغة .⁽²⁶⁾ وقد يقوم الإرهابيون بإنشاء ثغرة تسلل على غرار حصان طروادة بإستخدام برنامج غير مرخص يضاف الى برنامج ما ، ليتمكن بعد ذلك بالولوج غير المرخص فيه الى الشبكة أو البرنامج الحوسبي التي لايسمح لهم بالدخول اليها بالأحوال الاعتيادية ، تمهيداً للعبث فيه بالحذف والاضافة أو والتغيير بخصائص النظام كله فضلاً عن التجسس .⁽²⁷⁾ وقد يذهب الإرهابيون الى أبعد من ذلك بزرع القنبلة المنطقية داخل النظام الالكتروني 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 الى تدميرها⁽²⁸⁾

الفرع الثالث /// التجسس الإلكتروني.

يقوم الإرهابيون بالتجسس⁽²⁹⁾ على المواقع الالكترونية للأفراد والدول أو المنظمات والهيئات الدولية أو الوطنية بإستخدام برامج معينة ووسائل غير مشروعة مثل (الفيروسات ، أو اسلوب سلامي⁽³⁰⁾ ، أو احصنة طروادة) لكشف كلمة المرور السرية للدخول غير المصرح لهذه المواقع لتحقيق أغراض غير مشروعة مثل سرقة المعلومات أو افشاءها أو حتى استغلالها في الأنشطة الإرهابية .⁽³¹⁾ وتتم عملية التجسس الإلكتروني بعدة طرق، من أشهرها ، إختراق البريد الإلكتروني للآخرين ، وذلك حين يقوم الضحية بفتح المرفقات المرسله ضمن رسالة غير معروفة المصدر . وهناك طرق أخرى لزراع 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. ويكمن الخطر في عمليات التجسس التي تقوم بها التنظيمات الإرهابية وأجهزة الاستخبارات المختلفة من أجل الحصول غير المرخص به على أسرار ومعلومات الدولة، ومن ثم إفشائها 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 لاقترافها. وتتراوح خطورة التجسس بحسب اهمية المعلومة المنقطة ودرجة سريتها سواء اكانت سيادية أو أمنية أو اقتصادية ، أو الجهة التي قامت بمهمة التجسس منظمة ارهابية 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 ال20، فضلاً عن العديد من رؤساء دول العالم الثالث بلغ عددهم 60 زعيماً، فضلاً عن التتصت 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 أماط اللثام عن العديد من برامج المراقبة الأخرى من بينها (برنامج أوبستريم، برنامج كسكيسكور، برنامج بولرون وبرنامج تومبورا).

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

تتقدم الأمم المتحدة قائمة المنظمات الدولية المعنية بمواجهة الإرهاب على اختلاف صنوفه واهدافه ، بالنظر لقدراتها وخبراتها الواسعة في هذا المجال والتأييد الدولي ، ومن هذه المنظمة انبثقت منظمات عالمية اخرى اكثر تخصصا من امثال (الإتحاد الدولي للاتصالات ، و المنظمة العالمية للملكية الفكرية) لتكون سندا 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 الالهاب في مطالب هذا المبحث.

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

يعود إهتمام المجتمع الدولي بمشكلة الإرهاب إلى عام 1934، حين تقدمت فرنسا بطلب إلى سكرتير عصبة الأمم ، ودعت فيه إلى إتفاق دولي لمعاقبة الجرائم التي ترتكب بغرض الإرهاب السياسي أثار مقتل الملك الكسندر الأول ملك يوغسلافيا ، تم اقراره 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 الجمهور³⁴ . ومنذ ذلك الحين بدأت المنظمة الدولية رحلتها في مكافحة الإرهاب على اختلاف انواعه ومظاهره ، فكان لها دور مميز في هذا المضمار يمكن تشخيصه من خلال الرجوع الى ميثاقها في المقام الأول ، أو من خلال مراجعة ما اصدرته من قرارات وبدلته من جهود في هذا الخصوص في المقام الثاني.

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

تشكل مكافحة الإرهاب جزءًا لا يتجزأ من ولاية الأمم المتحدة التي يجعل ميثاقها من صون السلم والأمن الدوليين مقصداً رئيساً، ويوجب إتخاذ تدابير جماعية لمنع التهديدات للسلام ولقمع العدوان وتعزيز حقوق الإنسان والتنمية الاقتصادية، ليظهر الإرهاب ضمن هذا المنحى بوصفه انتهاكاً وتهديداً لشروط ومقتضيات اشاعة الأمن والسلم الدوليين ، فضلا عن انتهاكه الواضح لحقوق الإنسان، والتسوية السلمية للمنازعات، التي حرص الميثاق الأممي على تكريسها وتأمينها⁽³⁵⁾ . وعلى الرغم من كون ميثاق الأمم المتحدة لم ينص صراحة على تجريم استخدام المعلومات كأداة إرهابية ضمن اطار ما يعرف بـ (الإرهاب الإلكتروني) ؛ الا 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 الإعتبار أن الميثاق جاء لمواجهة النزاعات المسلحة، فإنه إذا ما تمّ إعتبار الإرهاب الرقمي وإستخدام حرب المعلومات يقعان ضمن العدوان والذي يُعنى بحمل وإرغام دولة على الإتيان بعمل معين.. فإنه تنطبق هنا قوة القانون ؛ لاسيما وان ميثاق الأمم المتحدة في مادته الثانية فقرة (3) قد أورد ما نصّه: "يفضُ جميع أعضاء الهيئة منازعاتهم الدولية بالوسائل السلمية على وجه لا يجعل السلم والأمن والعدل الدولي عرضة للخطر". من ثمّ فإن التجاء الدول إلى تسوية منازعاتها وصراعاتها عبر الفضاء الإلكتروني ، يعرّض الأمن والسلم الدوليين للخطر. كما ان الإرهاب الرقمي وما يتضمنه من خروقات للسيادة الوطنية لأية دولة، واساليب للتجسس على المعلومات التي تهدد الأمن الوطني للبلدان ، وتجنيد العملاء ، تناقض ما



ورد من توجه اممي ضمن مقتضيات الفقرة الرابعة من المادة نفسها لميثاق الأمم المتحدة التي تنص على أنه "يمتنع أعضاء الهيئة جميعاً في علاقاتهم الدولية عن التهديد بإستعمال القوة أو إستخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو على أي وجه آخر لا يتفق ومقاصد "الأمم المتحدة". وعلى 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 تنصُ 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 وإتفاقيات دولية يتألف من ست عشرة إتفاقية دولية لمكافحة الأنشطة الإرهابية وتجريم الدول والكيانات التي تلجأ لإستخدامها. وفي هذا السياق لم تكثف الأمم المتحدة بدعوة الدول الى الالتحاق بهذه الإتفاقيات ومتابعة مدى التزامها بتنفيذ بنودها من جانب الدول الأعضاء فحسب ، بل ذهبت الى 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 إتخذ 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 الإستشارية 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⁾ . ومن واقع قناعتها بأهمية ضمان التكامل بين البنى والادوات 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 أعمدت 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 أياً كان دوافعها أو مرتكبوها بوصفها أعمالاً إجرامية تهدد السلام والأمن الدوليين وتتنافى مع مقاصد ومبادئ ميثاق الأمم.⁽³⁸⁾ مع التأكيد بان الإرهاب لا يمكن دحره الا بإتباع نهج شامل مطرد ينطوي على مشاركة وتعاون فعليين من جانب كافة الدول والمنظمات الدولية ، ومضاعفة الجهود على الصعيدين الوطني والعالمي لنزع اسباب التطرف والإرهاب وتصفية العوامل والاجواء المساعدة عليه بالمقام الأول عبر الدعوة الى تعزيز الحوار والتفاهم بين الحضارات لمنع استهداف العشوائيين وللأديان والثقافات أو ربطها بالإرهاب ، ومعالجة الصراعات الإقليمية المتبقية دون حل والقضايا العالمية لإسهامها في تعزيز جهود مكافحة ، مع التشديد على أهمية دور وسائل الاعلام والمجتمع المدني والديني والمؤسسات التعليمية في تعزيز الحوار وتوسيع آفاق التفاهم وتشجيع التسامح وتهيئة بيئة لا تفضي الى التحريض على الإرهاب ، وبيان فاعلية تدابير إحترام حقوق الانسان والحريات



الاساسية وسيادة القانون بوصفها عناصر أساسية في الوقاية من أفة الإرهاب والتطرف. وفي ضوء ما تقدم وجه مجلس الأمن دعوة الى دول العالم لإتخاذ التدابير للتصدي للتحريض على إرتكاب اعمال الإرهاب بدافع التطرف وإستنكار المحاولات الرامية الى تبرير أو تمجيد الاعمال الإرهابية التي قد تحرض على ارتكاب المزيد من تلك الاعمال وإستعمال جميع الوسائل القانونية لهذا المسعى وحرمان من يخطون لأعمال الإرهاب أو يمولونها أو يرتكبونها مع التأكيد على اهمية التعاون الدولي في مكافحة الإرهاب عبر الدعوة الى الالتحاق وتنفيذ الإتفاقيات الدولية ذات الصلة والتنسيق فيما بين الدول لمنع وقمع اعمال الإرهاب. وفي المقام الثاني كانت الدعوة الأهمية لدول العالم الى إتخاذ الاجراءات والتدابير العملية الفاعلة لمكافحة الاعمال الإرهابية وملاحقة ومحاسبة مقترفيها عبر الزامها بالاتي:

1- الامتناع عن تقديم أي شكل من اشكال الدعم الصريح والضمني للكيانات الإرهابية ، مع وضع حد لعملية تجنيد اعضاء الجماعات الإرهابية ومنع تزويد الإرهابيين بالسلاح .
2- عدم توفير الملاذ لمن يمولون الاعمال الإرهابية أو يديرونها أو يرتكبونها ، منع إستخدام اراضي الدول لانتقال في تنفيذ تلك المارب ، فرض ضوابط مشددة على الحدود وعلى اصدار الأوراق الثبوتية ووثائق السفر.

3- تعزيز التدابير الرامية الى كشف ووقف تدفق التمويل والاموال للأغراض الإرهابية ومنع الإرهابيين من استغلال الأنشطة الاجرامية الاخرى ك(الاختطاف ، والاتجار بالبشر والمخدرات والاسلحة) لتمويل انشطتهم الإرهابية ، وتجريم ومحاسبة كل من يمول الاعمال الإرهابية أو يديرها أو يدعمها أو يرتكبها أو يورد السلاح اليهم.

4- تشجيع الدول على تبادل المعلومات على وجه السرعة مع الدول الاعضاء و تقديم تقارير الى لجنة مكافحة الإرهاب حسب جدول زمني تحدده اللجنة بعد الاجابة عن كل اسئلتها واستفساراتها ، وتزويد اللجنة بأسماء من يشاركون من أفراد تلك الكيانات الإرهابية في تمويل أو دعم اعمال أو أنشطة القاعدة والتنظيمات الإرهابية بغية المساعدة في مواجهة الأنشطة الإرهابية وانتقال الإرهابيين الزام الدول

5- دعوة المنظمات الدولية لتعزيز التعاون مع الأمم المتحدة في نطاق ولايتها بهدف تطوير قدرتها على معاونة الدول الاعضاء في جهودها على التصدي للتهديدات الإرهابية. وان تعمل مع لجنة مكافحة الإرهاب والمنظمات الدولية الاخرى من اجل تسهيل تبادل افضل الممارسات في مجال مكافحة الإرهاب ، مع عزم المجلس على عقد اجتماعات منتظمة مع رؤساء هذه المنظمات لتحقيق هذه الغايات .⁽³⁹⁾ ومع تزايد خطر الإرهاب الدولي و بروز وإنتشار نوع جديد من الجريمة المرتبطة بالحاسوب الالي بفعل تسارع وتيرة التطور التقني في انظمة المعلومات والاتصالات وما افرزه ذلك التهديد من اضرار ومخاطر على أمن البلدان والأفراد لاسيما بعد دخول الشبكة الدولية للمعلومات بوسائلها المتنوعة والمتطورة على خط الإرهاب الدولي ومواجهته ، تزايدت الحاجة إلى تظافر الجهود الدولية وتعاضدها تحت مظلة المنظمات الدولية والإقليمية لمواجهة هذا التهديد ، وكانت الأمم المتحدة المحفل العالمي الاهم لترجمة هذه الجهود واستثمارها الامثل في هذه المواجهة ، لما تتمتع به هذه الاخيرة 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 إهتمام الأمم المتحدة بهذا الخطر المتصاعد والمتجدد بوسائله وشهدت مواجهة الإرهاب نقلة نوعية الى الحاسب الالي 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 الأهمية.



وقد بدأت الأمم المتحدة رحلتها في هذا المضمار التقني في المؤتمر الدولي الأول لحقوق الانسان الخاص باثر التقدم التكنولوجي على حقوق الانسان في طهران عام 1968 إذ تبنت الجمعية العامة للأمم المتحدة توصياته وأبرزها إعتبار الحاسب الالي أكبر تهديد يواجه حق الانسان بالخصوصية والحرية الشخصية كونها تعد من ادوات المراقبة والتطفل الحديثة خاصة إذا ما تم تخزين البيانات الشخصية على الحاسب الالي 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 الالي 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 إتخاذ تدابير ملائمة ضد حالات إستعمالها ؛ مع الاشارة الى مسالة الخصوصية التي يمكن أن تخترق عن طريق الاطلاع على البيانات الشخصية المخزنة داخل نظم الحاسبات الالية والتي تشكل انتهاكا لحقوق الانسان وحرمة الحياة الخاصة ؛ مؤكداً على وجوب اعتماد ضمانات ملائمة لصون السرية وقرار نظم تكفل وصول الأفراد الى هذه البيانات لغرض تصحيح الاخطاء فيها . وشجع المؤتمر على تبني التشريعات الحديثة التي تجرم وتتناول جرائم الحاسب الالي. وفي 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 لإتخاذ الاجراءات المناسبة للحد منها . وفي المؤتمر العاشر لمنع الجريمة في بودابست ، جرى إعتبار جرائم الحاسب الالي نمطا جديداً من الجرائم المستحدثة مع وجوب العمل على إتخاذ تدابير مناسبة للحد من أعمال القرصنة⁽⁴²⁾ . وبعد أحداث الحادي عشر من سبتمبر 2001، اصبحت مكافحة الإرهاب من أولويات المجتمع الدولي ، بعد أن أمسى أكثر شمولية وتطوراً بإستخدام معطيات الثورة المعلوماتية وأشد فتكاً وتأثيراً على الأمن العالمي ، فكانت إستجابة الأمم المتحدة أكثر حزماً وشمولاً مع هذه المستجدات ، عبر قيادتها حملة دولية لمكافحة الإرهاب بطوره المعاصر ، مهدت لها بسلسلة من القرارات الدولية لتبنيه الراي العام العالمي وتنمية الوعي الأممي 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. واتخذت في هذا السبيل، الجمعية العامة للأمم المتحدة في الدورة 258/56 في 31 من يناير 2002 قراراً يدعو إلى إستخدام تكنولوجيا الاتصال والمعلومات من أجل التنمية⁽⁴³⁾ . وأصبحت قضية أمن المعلومات مرتبطة بحظر إستخدام تكنولوجيا الاتصال والمعلومات للتأثير أو الهجوم على وسائل تكنولوجيا الاتصال والمعلومات الخاصة بدولة أخرى، مواقف تشكل تهديداً للسلم والأمن الدوليين⁽⁴⁴⁾ . وهو المسعى الذي تجلت محاوره وملامحه بصورة أكثر تفصيلاً في الرسالة التي وجهها الامين العام للأمم المتحدة "كوفي عنان" في 15 من مايو 2004 وجاء فيها "في عالم يتزايد فيه الترابط وإقامة الشبكات، أضحي من المهم للغاية ضمان سلامة نظمنا وهيكلنا 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 إستعمال تكنولوجيا المعلومات والاتصالات⁽⁴⁵⁾ أدركت الأمم المتحدة أن إحكام القبضة على الفوضى الحادثة داخل الفضاء الإلكتروني يتطلب إطاراً قانونياً يحكمه وينظم إستخدامه⁽⁴⁶⁾ . وسعياً الى استكمال



هذا البناء القانوني لمكافحة الإرهاب وتوفير أدواته الفاعلة ، إتخذ 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 يتم فيها إتخاذ قرار سياسي على المستوى الدولي لترجمة الجهود الدولية إلى خطوات عملية في مجال مكافحة الإرهاب المرتبط بالانترنت (47) وفي خطوة لاحقة وتمتمة 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 إستهدف 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 نص القرار رقم (1455 في 2003) والقرار الدولي (1805 في 2008) (48) ومنذ 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). وإيماناً من الأمم المتحدة بالأمال المعلقة عليها في مجال تعضيد التعاون الدولي لنقل الخبرات في مجال الفضاء الرقمي وتقليص الهوة بين دول العالم والتنمية ، ومواجهة ما تخلفه هذه التقنيات الرقمية من تهديدات على أمن البلدان والمستخدمين. وسعيها 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 واليات إستخدامها ، فاعترفت هذه القمة بأن " الإنترنت أضحت عنصراً مركزياً 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 والافكار والمعرفة ضرورية لمجتمع المعلومات ، مع الدعوة الى مراقبة الانترنت بحجة الحفاظ على الأمن الدولي وإحترام المؤسسات الملكية الفكرية ومكافحة الاموال (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 والإستجابة لها في الوقت الحقيقي، وضع شبكة تعاونية لتبادل المعلومات (51) ولدى مراجعة حزمة القرارات التي إتخذها 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 ازاء إستعمال شتى الوسائل بما فيها الانترنت من جانب الإرهاب في الدعاية والتحريض على العنف الإرهابي". وجاءت القرارات اللاحقة لتستكمل طريق مواجهة الإرهاب بإستخدام الشبكة الدولية للمعلومات عبر متابعتها - التي لم تتعد سقف التحذير في كل الاحوال- لما يستجد من إستخدامات 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 الى " التعاون لمنع الإرهابيين من استغلال التكنولوجيا المتطورة والاتصالات والموارد التحريضية على دعم الاعمال الإرهابية ، وإبداء القلق إزاء لجوء القاعدة والتنظيمات الإرهابية الى استغلال الانترنت بشكل اجرامي لتنفيذ أعمال إرهابية" فكان مضمون المادة ينصرف الى التحذير من إمكانية الإستخدام المباشر للانترنت في الاعمال الإرهابية وليس في التحريض كما جاء في مضمون القرار السابق . وقد نبه مجلس الأمن في قرار لاحق بالعدد 1963 لعام 2010 الى " إزدياد إستخدام الإرهابيين للتكنولوجيا الجديدة للمعلومات والاتصالات وبخاصة الانترنت لأغراض التجنيد وكذا التحريض على دعم الاعمال الإرهابية" بوصفها أنماط مستحدثة لإستخدامات الإرهابيين لمعطيات الشبكة الدولية للمعلومات . وكان القرار 2255 في 2015 أكثر شمولاً لطرق إستخدام الإرهابيين للانترنت في أنشطتهم الإرهابية ، إذ تضمن " الاعراب عن قلقه من تزايد لجوء الإرهابيين الى إستعمال تكنولوجيا المعلومات ولاسيما شبكة الانترنت من اجل تيسير الاعمال الإرهابية والتحريض على الإرهاب أو تجنيد مرتكبيها أو تمويلها". وكان المحور الثالث من محاور المواجهة الأممية لمخاطر الإرهاب الرقمي ، يتمثل في وضع الاستراتيجيات العملية والشاملة لمكافحة الأنشطة الإرهابية على ارض الواقع ، وذلك حينما نجحت الجمعية العامة للأمم المتحدة في إقرار استراتيجية عالمية موحدة لمكافحة الإرهاب في 8 أيلول/سبتمبر 2006؛ إذ عدت خطة عمل إشتملت على أسس من أهمها : (التصدي للأوضاع التي تفضي إلى إنتشار الإرهاب ، وإتخاذ تدابير لبناء قدرة الدول على مكافحته والوقاية المتقدمة منه ؛ وتعزيز دور الأمم المتحدة في مكافحة الإرهاب؛ وكفالة إحترام حقوق الإنسان في سياق التصدي للإرهاب)⁽⁵²⁾ وقد كان الإرهاب بصورته الرقمية حاضراً في سياق هذه الاستراتيجية حينما أشارت الفقرة (12) من هذه الاستراتيجية الى ضرورة تنسيق الجهود المبذولة على الصعيدين الدولي والإقليمي لمكافحة الإرهاب بجميع أشكاله ومظاهره على الإنترنت؛ بل وإستخدام 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⁾ ومما تقدم يتضح الخط التصاعدي لإهتمام الامم المتحدة بموضوعة الارهاب عامة وما تمخض عنه من ارهاب رقمي بصورة خاصة من مستوى الادانة والتحذير عبر القرارات المتفرقة الصادرة لمناسبة حصول اعمال ارهابية في عدد من دول العالم ، مروراً بمستوى البناء القانوني لصيغ المواجهة وصولاً الى وضع الخطط والاستراتيجيات الشاملة والفاعلة لمواجهة الارهاب ، دون ان يعني ذلك نهاية المطاف بالنسبة لمسيرة الامم المتحدة في مجال مكافحة الارهاب بكل اشكاله او حتى نجاحها في مهمتها وانقضاء مسؤوليتها الدولية في هذا المجال ، بالنظر لتطور وسائل هذا الخطر الدولي وتباين ايقاعه وارتباطه



بنزعة الشر والصراع المستوطنة في النفس الانسانية ، واستمرارية الاعمال الارهابية في اغلب بقاع العالم ناهيك عن خطورة تقاعس او تواطى بعض الدول مع التنظيمات الارهابية لدواعي المصالح او الايديولوجيات 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 (الإتحاد الدولي للاتصالات ، والمنظمة العالمية للملكية الفكرية) عبر فرعين.

الفرع الأول /// الإتحاد الدولي للاتصالات.

نشأ الإتحاد الدولي للاتصالات بمقتضى إتفاقية باريس عام 1865 تحت إسم (إتحاد التلغراف الدولي) ثم عدل الاسم ليصبح (الإتحاد الدولي للاتصالات السلكية واللاسلكية) ، وفي عام 1947 إنضم الإتحاد الى 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 عضوا من الشركات العلمية والصناعية العاملة بالقطاعات العام والخاص . ومن المهام التي يضطلع هذا الإتحاد تعزيز التعاون الدولي للخدمات الهاتفية والسلكية واللاسلكية وتوسيع إستخدامها بواسطة الجمهور وتطوير امكانيات الاتصالات السلكية واللاسلكية وتوزيع الموجات اللاسلكية ، كما يقوم الإتحاد 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 البني التحتية للشبكات ضد المخاطر من خلال التوعية، والتقييم الذاتي، وبناء القدرات، وتوسيع نطاق المراقبة، والإنذار، وقدرات الاستجابة للحوادث للدول والجهات المعنية. ويعمل الإتحاد بصورة وثيقة مع المنظمات الأخرى المعنية على (وضع المعايير المتعلقة بالأمن المعلوماتي ؛ إذ يقوم الإتحاد، بالاشتراك مع الوكالة الأوروبية لأمن الشبكات والمعلومات ، بنشر خريطة الطريق المتعلقة بمعايير الأمن في مجال تكنولوجيا المعلومات والاتصالات، كما تعاون الإتحاد الدولي مع مجلس أوروبا لإنجاز الإتفاقية الأوروبية حول الجريمة الإلكترونية من أجل الاستعانة بها في عملية وضع إطار قانوني دولي. وفي مسعى اكثر شمولا ، تم في المؤتمر الإقليمي حول الأمن الإلكتروني بالتعاون مع الإتحاد الدولي للاتصال في قطر في شباط من العام 2008، دعوة جميع الدول لوضع وتنفيذ إطار وطني للأمن الإلكتروني وحماية البنية التحتية الحرجة للمعلومات، والتي تُعدُّ بمثابة خطوة أولى في سبيل التصدي للتحديات التي تواجهها جراء اتصالها بتكنولوجيا المعلومات والاتصال.⁽⁵⁵⁾ على صعيد اخر، طالبت القمة العالمية لمجتمع المعلومات في تونس في نوفمبر 2005، بأن ينسق الإتحاد الدولي للاتصالات آلية لبناء الثقة والأمن في مجال إستخدام تكنولوجيا الاتصال والمعلومات ، عبر إطلاق برنامج الأمن الإلكتروني العالمي وهو إطار أعده الإتحاد الدولي للاتصالات بهدف إقتراح إستراتيجيات للتوصل إلى حلول لتعزيز الثقة والأمن في مجتمع المعلومات. وتم لهذا الغرض تعيين فريق خبراء⁽⁵⁶⁾ لإسداء المشورة إلى الأمين العام للإتحاد ، بشأن المسائل المعقدة التي تكتنف موضوع الأمن السيبراني. وسيقوم الفريق بصياغة المقترحات التي ستقدم إلى الأمين العام للإتحاد بشأن الاستراتيجيات طويلة الأجل لتعزيز الأمن السيبراني في خمسة مجالات هي الاتي: 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 دوليا. وفي 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 "الهياكل التنظيمية" إطار العمل وإستراتيجيات الاستجابة، فيما يتعلق بمنع الهجمات السيبرانية وتتبعها والردّ عليها وإدارة



الأزمات المتعلقة بها. بما في ذلك حماية أنظمة البنية التحتية الحرجة للمعلومات. ويركز 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. ويهدف مجال "التعاون الدولي" إلى وضع إستراتيجية 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 وإستخداماتها المختلفة وتعزيز قدراتها في مجال امن المعلومات لمواجهة الاخطار التي تخلفها محاولات اساءة استغلال هذه التقنيات من قبل بعض الجهات الارهابية والدولية.

الفرع الثاني // المنظمة العالمية للملكية الفكرية.

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

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

التحقت المنظمات الاقليمية بالجهود الدولية لمكافحة الارهاب 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 الارهاب تحت مظلة الامم المتحدة مما جعلها هدفاً للتنظيمات الارهابية . وكان التحاق سائر المنظمات الاقليمية متأخراً بهذه الجهود ولم يكن الارهاب الرقمي في اجندتها لمحدودية اعتمادها على الشبكة الدولية للمعلومات وانشغال دولها بهموم وتحديات اكبر . ولتسليط الضوء على دور هذه المنظمات الاقليمية في مجال مكافحة الارهاب الرقمي مع كثرتها سيتم اختيار نموذجين منها احدهما من العالم المتقدم وهو الاتحاد الاوربي والآخر من العالم الثالث ويعيننا بصورة مباشرة هو منظمة الجامعة العربية .

المطلب الأول // دور الإتحاد الأوروبي في مكافحة الإرهاب الرقمي.

مارس الإتحاد الأوروبي دوراً مهماً في مجال التصدي لجرائم الإرهاب الرقمي عبر إقراره العديد من التوصيات الخاصة لحماية البيانات ذات الصبغة الشخصية من سوء الإستخدم وحماية تدفق المعلومات .



ففي عام 1981 وقعت إتفاقية تحت مظلة المجلس الأوروبي تتعلق بحماية الاشخاص في مواجهة المعالجة الالكترونية للبيانات ذات الصبغة الشخصية . كما صدر عن المجلس الأوروبي العديد من القواعد التوجيهية في مجال جرائم الحاسب الالي تضمنت وجوب تجريم العديد من السلوكيات التي تعد من الجرائم كالغش المعلوماتي وسرقة الاسرار المخزنة . وتضمنت هذه القواعد عددا من الاجراءات الفنية التي يتوجب إتخاذها لحماية نظم المعلومات من كل اشكال الانتهاك في عام 1980 جرى توقيع معاهدة مجلس أوربا الخاصة بحماية الاشخاص من مخاطر المعالجة الالية للبيانات ذات الطابع الشخصي والتي سرى مفعولها في اكتوبر عام 1985 وانطوت على توجيهات بصدد وجوب توفير قواعد تكفل حماية البيانات الشخصية من مخاطر المعالجة الالية⁽⁶⁰⁾ . فضلا عن ذلك فقد صدر عن مجلس أوربا العديد من التوصيات لحماية البيانات الحوسبية ولاسيما التوصية بالرقم (R81/1) بشأن تنظيم البيانات الطبية المعالجة اليا 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 و 1982 . وإذا كانت الحماية الأوروبية للبيانات الشخصية لم تتوج حتى الان ، الا انه صدر ارشاد أوروبي في 11 اذار عام 1996 يتعلق بالحماية القانونية لقواعد البيانات وإعتبار برامج الكمبيوتر ضمن مجال المؤلفات الفكرية الواجب حمايتها . وقد شملت هذه الحماية التركيب والتصميم أي حماية محتواها من الاقتطاع أو الاستعمال له أو لاي جزء منه وذلك بمجرد ان يتطلب تحضير واعداد المحتوى من واضعي القاعدة توظيفا ذا طابع اقتصادي مهم نوعا وكما يضاف الى ذلك الجهود التي قامت بها منظمة التعاون الاقتصادي والتنمية في مجال ارساء مبادئ حماية الخصوصية بشأن البيانات الشخصية والتي اهتمت بشكل عملي بحماية الخصوصية عبر الحدود والتي تبلورت على شكل قواعد ارشادية تم تبنيها رسميا من قبل مجلس المنظمة في ايلول 1980 تحت عنوان (قواعد أوسيد الارشادية بشأن حماية الخصوصية ونقل وتدقيق البيانات الشخصية) . غير أن الحدث الرئيس الذي توج جهود الإتحاد الأوروبي في هذا المضمار قد تمثل بإصدار إتفاقية شاملة تتعلق بجرائم الحاسب في إجتماع المجلس بستراسبورغ في عام 2000 تضمن الدعوة الى حماية مجتمعاتها من الجرائم الرقمية ووضع التشريعات الملائمة لمكافحتها بالنص على تجريم الافعال التي تشمل ائتلاف قواعد البيانات ووظائف الحاسب الالي وانظمتها أو التزوير فيها أو الاحتيال وعقوبة المتسبب بذلك أو حتى الشروع في مثل هذه الجرائم والمساهمة فيها وضمان التعاون الدولي في مجال التحقيق وتبادل المعلومات لتحقيق الأمن المعلوماتي⁽⁶¹⁾ . وحاليا يعتزم الإتحاد الأوروبي وضع خطة جديدة يقوم بموجبها بتفتيش اجهزة الكمبيوتر عن بعد لمكافحة الجريمة الرقمية . وستشجع هذه الخطة تبادل المعلومات بين قوات الشرطة الالكترونية لملاحقة ومقاضاة المجرمين بعد ان توجه تحذيرات حول الاخطار المحدقة تلحقها انشاء فرق تحقيق تعمل عبر الحدود وترخص استخدام دوريات افتراضية لملاحقة المجرمين وضبط بعض النواحي في الانترنت وذلك في مسعى لضمان إحترام قوانين حماية المعلومات اثناء 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 الى الارهاب وما يرتبط به من تفرعات . ومع ذلك ، فان تأويل الدلالة العامة لبعض النصوص الواردة في هذا الميثاق ، قد يخدم جهود مكافحة الارهاب ، ومن ذلك ما جاء في المادة الثانية من الميثاق والتي اوضحت مقاصد هذه المنظمة في تحقيق التعاون بين الدول الاعضاء لصيانة استقلالها وسيادتها ، والتي ستتقاطع بالضرورة مع ما تتطوي عليه وسائل الارهاب الرقمي من تجاوزات واخلال لسلطة وسيادة الدول عبر التعرض لنظم المعلومات المرتبطة بالمؤسسات السيادية او حتى امكانية التعرض ضد النظام



باستغلال وسائل التواصل الالكتروني فضلا عن امكانية استغلال المعلومات الحساسة وتوظيفها ضد مصالح الدولة العربية المستهدفة ، الامر الذي يستدعي تعاون الدول العربية طبقا لهذه المادة لمواجهة مثل هذه الانشطة الارهابية عبر الفضاء الرقمي ، وهو الاتجاه الذي اكدته المادة الثالثة من الميثاق حينما خولت مجلس الجامعة ، تقرير وسائل التعاون مع الهيئات الدولية التي قد تنشأ في المستقبل لكفالة الأمن و السلام . واذا جاز اعتبار الاعتداء على نظم المعلومات التي تعتمد عليها المؤسسات الرسمية للدول العربية ومحاولة تدميرها او الاضرار بها وسرقة المعلومات او حتى اشاعة الرعب والتخريب ضد النظام القائم التي تتم عبر اليات الارهاب الرقمي من صور العدوان وفقا لقواعد القانون الدولي وميثاق الامم المتحدة ، فان المادة السادسة من ميثاق الجامعة العربية قد اجازت للدولة او الدول التي وقع عليها أي اعتداء او 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⁾ . وبعيدا عن اجواء الميثاق ، يلاحظ تأخر اهتمام جامعة الدول العربية على صعيد العمل الميداني حتى عام 1983 ، بدأت الجهود العربية المشتركة لمكافحة الإرهاب بالتوصل الى الاستراتيجية الأمنية العربية التي اقرها مجلس وزراء الداخلية العرب والتي نصت على ضرورة الحفاظ على أمن الوطن العربي وحمايته من المحاولات العدوانية للإرهاب والتخريب الموجهة من الداخل والخارج . وفي اطار الخطة الأمنية العربية الأولى تشكلت لجنة الجرائم المنظمة التي تناولت في اجتماعها الأول موضوع جرائم الإرهاب . وبناء على توصيات اللجنة التي عرضت على مجلس وزراء الداخلية العرب في دورته السادسة بتاريخ 1987/12/12 اصدر قرارا يقضي بتكليف الامانة العامة لمجلس وزراء الداخلية العرب بإعداد مشروع استراتيجية عربية لمكافحة الإرهاب بالتنسيق مع الامانة العامة لجامعة الدول العربية. وفي مطلع 1988 اصدر مجلس وزراء الداخلية العرب قرارا ينص على تشكيل لجنة من ممثلي الدول العربية على مستوى الخبراء وبمشاركة الامانة 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 وقرارها في الدورة الرابعة عشر لمجلس وزراء الداخلية العرب في 1997/1/5 . الا أن إقرار الاتفاقية العربية لمكافحة الإرهاب لم يتم الا في اجتماعات الدورة الـ15 لمؤتمر وزراء الداخلية العرب في 5 يناير 1998 ، حيث تم وضع عدد من الآليات لتنفيذ هذه الاستراتيجية لمواجهة الإرهاب . وقد تضمن مشروع الإستراتيجية العربية لمكافحة الإرهاب عدداً من المنطلقات والاهداف والمقومات والاليات التي تحدد الاسس التي تقوم عليها سياسة مكافحة الإرهاب والسبل الكفيلة بتحقيق أقصى قدر من التعاون على الصعيد العربي والدولي لتطويق هذه الظاهرة والحد من الاخطار التي تشكلها على الدول المختلفة . فاعتبرت ان الاعمال 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 إتخاذ تدابير فعالة وحازمة لمكافحة الإرهاب بمختلف صورته واشكاله ، بعد تحديث قوانينها وتشريعاتها الجنائية لتشديد العقوبات على مرتكبي الاعمال الإرهابية ، وتجميد ومصادرة كافة الاموال الموجهة الى هذه الاعمال وتشديد اجراءات المراقبة لمنع تسلل عناصر الإرهاب والتخريب أو تهريب الذخيرة والمتفجرات والسعي الحثيث للحيلولة دون إتخاذ اراضي الدول العربية مسرحاً لتخطيط وتنظيم أو تنفيذ اعمال ارهابية . كما تطرقت الاستراتيجية الى موضوع تحديث وتطوير اجهزة الأمن من خلال دعمها بالمؤهلين وتوفير ما تحتاجه من معدات وتقنيات حديثة ، وكذلك وضع خطط وقائية لمنع أي



عمل ارهابي.وعلى صعيد التعاون العربي فقد تضمنت الاستراتيجية عدة بنود اهمها تعزيز التعاون بين الدول الاعضاء لمنع ومكافحة الإرهاب وتقديم المساعدة المتبادلة في مجال اجراءات البحث الجنائي والتحري والقبض على الاشخاص الخارجين والمتهمين أو المحكوم عليهم في جرائم الإرهاب ، كما اكدت الاستراتيجية على اهمية تبادل الخبرات والخبراء والتقنيات الحديثة والمعلومات في مجال التعامل الأمني مع الجماعات الإرهابية ومواجهتها وتختص الامانة العامة لمجلس وزراء الداخلية العرب بمتابعة مستجدات ظاهرة الإرهاب وسبل مكافحتها والتنسيق بين الدول العربية بهذا الشأن⁽⁶⁴⁾. وفي المؤتمر العربي الثامن عشر مجلس وزراء الداخلية العرب بتونس 2015 أوصى المشاركون باتخاذ الوسائل اللازمة للحد من "إنتشار 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 ، إعتقاد مجلس وزراء العدل العرب للقانون الجزائري العربي الموحد كقانون نموذجي بموجب القرار رقم 229 لسنة 1996 الذي تضمن فصلا خاصا بالاعتداء على حقوق الاشخاص الناتج عن المعالجات المعلوماتية مع النص بموجب المواد (461-463) منه على وجوب حماية الحياة الخاصة واسرار الأفراد من خطر المعالجة الآلية وكيفية جمع المعلومات والاطلاع عليها . وعقوبة من يقوم بفعل الدخول بطريق العنق الى نظام المعالجة الآلية للمعلومات أو عرقلة وافساد نظام التشغيل أو تغيير المعلومات داخل النظام وتزوير وثائق المعالجة الآلية وسرقة المعلومات⁽⁶⁶⁾ من جانب اخر نجحت الجامعة العربية في إبرام الإتفاقية العربية لحماية حقوق المؤلف التي أوصى بها مؤتمر وزراء الثقافة المنعقد في بغداد عام 1981 التي دعت الى وضع التشريعات اللازمة لحماية الملكية الادبية والفنية والعلمية والتي قد تكون هدفاً للإرهاب الرقمي اذا ما وجدت طريقها للنشر على الشبكة الدولية للمعلومات لذا الزمت المادة الثالثة والعشرون من هذه الاتفاقية الدول الاعضاء العمل على: " إنشاء مؤسسات وطنية لحماية حقوق المؤلف ويحدد التشريع الوطني بنية هذه المؤسسات واختصاصاتها" ولضمان تحقيق بنود هذه الاتفاقية والتزام الدول الاعضاء 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 ابرمت المنظمة العربية للتربية والثقافة والفنون الإتفاقية العربية لتيسير انتقال الانتاج الثقافي العربي ، والتي ضمنت حق وسيادة الدول الاعضاء على كيانها السيادي في المجال المعلوماتي بالنص في المادة العاشرة على الاتي " 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. وتعد هاتان الإتفاقيتان مثالا واضحا على جهود الجامعة العربية والمنظمات المتخصصة التابعة لها في مجال تنظيم حقوق المؤلف وإن كان يعد هذا متواضعا بوصفها تصب في اتجاه الوقاية من جرائم الحاسوب⁽⁶⁹⁾.



الخاتمة.

أولاً /// النتائج.

- 1- يعد الحاسوب في ظل الإرهاب الرقمي الاداة والساحة الرئيسة لتحقيق النوايا الاجرامية للارهابي على ارض الواقع ، فيكون الإرهاب الالكتروني تبعاً لذلك صلة الوصل بين العالم الافتراضي والعالم المادي الذي يتحقق به التأثير المادي للمعلومات . --- الإرهاب الرقمي هو نتاج تلك الثغرات القيمة ذاتها ، مضافاً إليها الثغرات في نظم المعلومات وبرامجياتها في طور ما بعد الحداثة
- 2- إن اعتماد الدول على وسائل الاتصالات وشبكات المعلومات في ادارة 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- تنتوع وسائل الإرهاب الرقمي بدرجة كبيرة تبعاً لقدرة ومهارة الإرهابيين ، والهدف المنشود من الفعل الإرهابي ، والجهة المستهدفة . مثلما تتباين اهداف الإرهاب الرقمي بين مساحات مكانية وزمانية ونوعية مختلفة الحدود والابعاد .
- 4- مع تنامي خطر الإرهاب الرقمي وتجاوزه حدود الدول وقدرته المتنامية على تقويض سيادتها وتهديد أمنها ، تزايدت الحاجة لتظافر الجهود الدولية في اطار المنظمات الدولية لمواجهة هذا التحدي واستئصاله .
- 5- يمكن تأشير التطور التدريجي في مستوى ادراك المنظمات الدولية لخطر الإرهاب وقدرتها على مواجهته مع تطور حجم التهديد الذي يفرضه هذا الاخير على الأمن والسلم الدوليين لاسيما بعد افادته من معطيات الشبكة الدولية للمعلومات ومميزاتها لتنفيذ الاعمال 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 واطار محدد الى مرحلة التأطير القانوني ووضع الاستراتيجيات النظامية لمواجهة هذا التهديد .
- 7- مما يزيد من تعقيد مشكلة الإرهاب الرقمي ، غياب إتفاقية واضحة ومتخصصة على المستوى الدولي للتعامل مع هذا التحدي الجديد أو حتى تنظيم إستخدام 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 الى عقد إتفاقية دولية جماعية أو تبني استراتيجية واضحة المعالم تحت رعاية الأمم المتحدة لضمان الإستخدام السلمي للفضاء الرقمية والتعاون بين الدول لمكافحة مظاهر الإرهاب الرقمي .
- 2- من الضروري بمكان اعتماد معايير دولية متفق عليها لتحديد مفهوم الإرهاب الرقمي ، وتنظيم إستخدام الشبكة الدولية للمعلومات ، وتأمين الحماية الممكنة لبرامج الحاسوب .
- 3- دعوة الدول الى الانضمام الى الإتفاقات الدولية الخاصة بمكافحة جرائم الإرهاب الرقمي وبخاصة المعاهدة الدولية لمكافحة جرائم المعلوماتية والانترنت . مع الحاجة المستدامة لتطوير بنودها بما يتناغم مع التطورات المتسارعة في انظمة الحاسوب والإستخدامات الإرهابية لها .
- 4- ضرورة تعزيز اليات التعاون والتنسيق وتبادل المعلومات والخبرات بين المنظمات العالمية والإقليمية المتخصصة والشاملة وكذلك بين الدول والاجهزة المعنية بمكافحة الإرهاب عبر الانترنت ، بالاستناد الى 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 اثناء انتقالها ، والسماح للجهات القائمة على التفتيش بضبط برامج الحاسب والمعلومات الموجودة بالبرامج وفقاً للشروط الخاصة باجراءات التفتيش العادية ، والقاء القبض عليهم ، عبر تفعيل الإتفاقيات 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 الاشكال المستحدثة من الإرهاب وتجريم أي إستخدام غير أمن لتكنولوجيا المعلومات والاتصالات من جانب ، وضمان تناغم نصوصها مع الإتفاقيات والجهود الدولية في هذا المجال ، لاغلاق الثغرات القانونية التي من الممكن استغلالها من قبل التنظيمات الإرهابية للافلات من الملاحقة والعقاب .

6- تعزيز التعاون والتنسيق الدولي مع المؤسسات الدولية المعنية بمكافحة الجريمة ، وبخاصة "الانتربول" لمواجهة كل اشكال جرائم الإرهاب عبر الانترنت، 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 المُحترفة والمُنْتشرة في جميع أنحاء العالم .

7- السعي لإنشاء منظمة أو ابرام إتفاقية عربية متخصصة بإستخدامات الشبكة الدولية للمعلومات للحيلولة دون استغلالها في الاعمال الإرهابية والاجرامية . وتفعيل دور المنظمات والادارات والحكومات العربية في مواجهة هذه الجرائم عن طريق نظام الأمن الوقائي، والسعي الى انشاء الشرطة العربية اسوة بالشرطتين الافريقية والأوربية .
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 إتفاقية جنيف لقمع الإرهاب لعام 1937 م .

6 قرار مجلس الأمن الدولي بالعدد 1566 لعام 2004 .

7 المادة الأولى من الإتفاقية العربية لمكافحة الارهاب لعام 1998 م ،

8 علي مطر ، الارهاب الالكتروني في القانون الدولي ، مقال منشور على موقع السكينة الالكتروني بتاريخ 4 نوفمبر

2013 على الرابط : <http://www.assakina.com/about-php>

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

10 تقرير اللجنة الدولية للصليب الاحمر ، القانون الدولي الانساني وتحديات النزاعات المسلحة المعاصرة ، الحادي

والثلاثين ، 2011 ، ص 67 .

11 عادل عبد الصادق ، هل يمثل الارهاب 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 ،

ص100 .

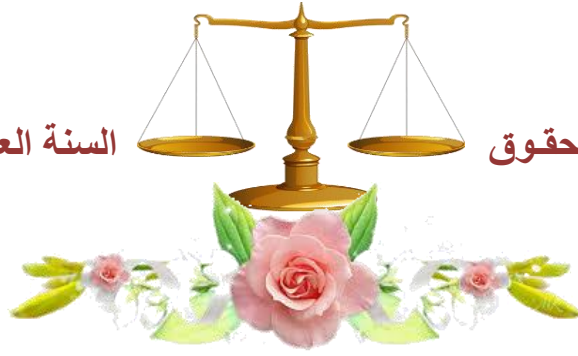
13 د. هشام بشير ، "مستقبل الإرهاب الإلكتروني.. تحديات وأساليب المُواجهة"، ندوة المركز الدولي للدراسات المُستقبلية

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 الزغبى 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 الرشيدى ، 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. معتر محي الدين ، الارهاب 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 الانساني ، اطروحة دكتوراه ، جامعة النهريين ، 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 الرشيدى ، 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 الى : 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 النهريين ، 2015 ، ص 171 .
- ²⁹ التجسس هو التلصص وسرقة المعلومات من الأفراد أو المؤسسات أو الدول أو المنظمات ، ينظر : مهرا ن زهير المصري ، الارهاب 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 اذار 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 الارهاب ، 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 : ادانة هجمات القنابل الإرهابية في نيروبي ودار السلام ،



- القرار 1438 في 2002 : ادانة هجمات بالي في اندنوسيا 12 تشرين 2002
- القرار 1516 في 2003 : ادانة الاعتداءات بالقنابل في اسطنبول 15 تشرين 2003
- القرار 1465 في 2003 : ادانة الهجوم بالقنابل في بوغوتا كولومبيا في 7 شباط 2003 .
- القرار 1530 في 2004 : ادانة هجمات مدريد الإرهابية في 11 آذار 2004 .
- القرار 1611 في 2005 : ادانة الاعمال الإرهابية في لندن
- القرار 1618 في 2005 : دعم الشعب العراقي واستقلال سيادته ، ادانة الاعمال الإرهابية في العراق .
- القرار 2170 في 2014 : ادانة الاعمال الإرهابية لداعش في العراق وسوريا .
- القرار 2178 في 2014 : ادانة التطرف العنيف المفضي الى الإرهاب والعنف الطائفي .
- القرار 2249 في 2015 : ادانة 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 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 الإستخدام السلمي للفضاء الإلكتروني ، دوريات - قضايا استراتيجية

الخميس، 6 اغسطس 2015 - 12:14 م ، على الرابط : www.accronline.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 الارهاب 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 الى 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 الى 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 الإلكتروني 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 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 الإتحاد الدولي للاتصالات - التقرير السنوي للإتحاد، 2007، ص38.
- 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 ص 75-76
- 62 عبد الصبور ، مصدر سابق ، ص 168 .
- 63 ميثاق جامعة الدول العربية ، المواد (2،3،6)
- 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 الإتفاقية العربية لحماية حقوق المؤلف لعام 1981
- 68 المادة العاشرة من الإتفاقية العربية لتيسير انتقال الانتاج الثقافي العربي لعام 1987
- 69 عبد الصبور ، مصدر سابق ، ص ص 170-172.
- المصادر.**
- اولا /// 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 والكرارز ، درا البراء ، الاسكندرية ، 2007.
- المكتب العلمي لهيئة الشام الاسلامية ، القانون العربي الموحد: دراسة وتقييم ، سلسلة مطبوعات هيئة الشام الاسلامية بالعدد 24 ، 2014
- جلال محمد الزغبي واسامة احمد المناعسة ، جرائم تقنية نظم المعلومات الالكترونية : دراسة مقارنة ، دار الثقافة للنشر والتوزيع ، عمان ، 2010.
- حارث سليمان الفاروقي، المعجم القانوني ، مكتبة لبنان ، بيروت ، ط5 ، 2003.
- د. خليل حسين ، التنظيم الدولي : النظرية العامة والمنظمات العالمية ، دار المنهل اللبناني ، بيروت ، 2010.
- ريتشارد كلارك وروبرت نيك ، حرب الفضاء الالكتروني : التهديد الالي للأمن القومي وكيفية التعامل معه ، مركز الامارات للدراسات الاستراتيجية ، الامارات العربية المتحدة ، 2012.
- 69 سايمون كولن ، التجارة عبر الإنترنت ، ترجمة يحيى مصلح ، بيت الأفكار الدولية ، نيويورك ، 1999 .
- د. طارق عزت رخا ، المنظمات الدولية المعاصرة ، دار النهضة العربية ، القاهرة ، 2006 .
- عبد الصبور عبد القوي ، الجريمة الالكترونية ، دار العلوم للنشر والتوزيع ، القاهرة ، 2008.
- د. عفيفي كامل عفيفي ، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون : دراسة مقارنة ، منشأة المعارف ، الاسكندرية ، بلا سنة طبع
- د. محسن الحيدري ، الإرهاب والعنف في ضوء القران والسنة والتاريخ والفقہ المقارن ، ج1، دار الولاة ، بيروت ، 2010.
- محمد امين الشوابكة ، جرائم الحاسوب والانترنت (الجريمة المعلوماتية) ، دار الثقافة للنشر والتوزيع ، عمان ، 2009.



- محمد بن يعقوب الفيروزبادي ، القاموس المحيط ، ط2، مؤسسة الرسالة ، بيروت ، 1987.
- محمود احمد عبابنة ، جرائم الحاسوب وابعادها الدولية ، دار الثقافة للنشر والتوزيع ، 2005.
- محمود الرشدي ، العنف في جرائم الانترنت ، الدار المصرية اللبنانية ، القاهرة ، 2011.
- ثانياً /// الأطاريح 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 الانساني ، اطروحة دكتوراه ، جامعة النهريين ، 2014.
- ثالثاً /// البحوث والدوريات.**
- الإتحاد 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 الارهاب ، إعداد مكتب الأمم المتحدة المعني بالمخدرات والجريمة (فيينا)، 2008.
- اللجنة الدولية للصليب الاحمر ، القانون الدولي الانساني وتحديات النزاعات المسلحة المعاصرة ، الحادي والثلاثين ، 2011 .
- عادل عبد الصادق ، هل يمثل الارهاب شكلاً جديداً من اشكال الصراع الدولي ، ملف الاهرام الاستراتيجي ، مركز الاهرام 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
- إتفاقية جنيف لقمع الإرهاب لعام 1937 م.
- الإتفاقية العربية لمكافحة الارهاب لعام 1998 م
- الإتفاقية العربية لحماية حقوق المؤلف لعام 1981
- الإتفاقية 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 الامن الدولي بالعدد 1189 لسنة 1998
- قرار مجلس الامن الدولي بالعدد 1267 لسنة 1999
- قرار مجلس الامن الدولي بالعدد 1333 لسنة 2000
- قرار مجلس الامن الدولي بالعدد 1363 لسنة 2001
- قرار مجلس الامن الدولي بالعدد 1373 لسنة 2001
- قرار مجلس الامن الدولي بالعدد 1377 لسنة 2001
- قرار مجلس الامن الدولي بالعدد 1390 لسنة 2002
- قرار مجلس الامن الدولي بالعدد 1438 لسنة 2002
- قرار مجلس الامن الدولي بالعدد 1452 لسنة 2002
- قرار مجلس الامن الدولي بالعدد 1455 لسنة 2003



- قرار مجلس الامن الدولي بالعدد 1465 لسنة 2003
 - قرار مجلس الامن الدولي بالعدد 1516 لسنة 2003
 - قرار مجلس الامن الدولي بالعدد 1526 لسنة 2004
 - قرار مجلس الامن الدولي بالعدد 1530 لسنة 2004
 - قرار مجلس الامن الدولي بالعدد 1566 لسنة 2004
 - قرار مجلس الامن الدولي بالعدد 1611 لسنة 2005
 - قرار مجلس الامن بالعدد 1618 لسنة 2005
 - قرارا مجلس الامن الدولي بالعدد 1617، و 1624 لسنة 2005
 - قرارات مجلس الامن الدولي بالعدد 1699 ، 1730 و 1735 لسنة 2006
 - قرار مجلس الامن الدولي بالعدد 1822 لسنة 2008
 - قرار مجلس الامن الدولي بالعدد 1904 لسنة 2009
 - قرارات مجلس الامن الدولي بالعدد 1988، و 1989 لسنة 2011
 - قرار مجلس الامن الدولي بالعدد 2170 في 2014
 - قرار مجلس الامن الدولي بالعدد 2178 في 2014
 - قرار مجلس الامن الدولي بالعدد 2249 في 2015
 - مجلس الامن الدولي بالعدد 2082 لسنة 2012
 - خامساً // 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 ، الارهاب الالكتروني في القانون الدولي ، مقال منشور على موقع السكينة الالكتروني بتاريخ 4 نوفمبر 2013
 على الرابط : <http://www.assakina.com/about-php>
 - د.معتز محي الدين ، الارهاب وتكنولوجيا المعلومات ، مقال منشور على موقع مدارك الالكتروني ، على الرابط :
www.madarik.net/News_Details.php?ID=21
 - مهران زهير المصري ، الارهاب الالكتروني ، مجلة باحثون العلمية ، بتاريخ 10/4 /2011 على الرابط :
www.albahethon.com/?page=show_det&id=1320
www.un.org/arabic/conferences/ws15
 - 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/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
 - 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