الفضاء الإلكتروني وتحديات الأمن العالمي

Cyberspace and global security challenges

الدكتورة/ حياة حسين[1,2,3]
[1]جامعة البليدة 2، (الجزائر)
[2]مخبر الرقمنة والقانون في الجزائر ، جامعة البليدة 2
[3]المؤلف المراسل: houcinehayet1@gmail.com

تاريخ الاستلام: 2020/10/26 تاريخ القبول للنشر: 2021/03/18 تاريخ النشر: 2021/04/28

❖❖❖❖❖❖❖

مراجعة المقال: اللغة العربية: د./ نور الدين لبصير (جامعة بومرداس) اللغة الإنجليزية: د./ نورة أبرسيان (جامعة بومرداس)

ملخّص:

لقد أصبح الفضاء السيبراني عنصرا مؤثرا في النظام الدولي، وكشف عن محاور جديدة للصراع الدولي يعرف بصراع الفضاء الإلكتروني، من شأنه أن يسبب خسائر عسكرية واقتصادية فادحة ، إلى جانب التهديدات الاجتماعية و الأمنية، لهذا يهدف هذا المقال إلى إبراز أهم تلك التهديدات التي يعززها الفضاء الإلكتروني بما يتيحه من سرعة وسهولة في الوصول إلى الأطراف المستهدفة، كما يقترح إطارا نموذجيا لتعزيز الأمان في الفضاء السيبراني وهو يشمل النواحي الاستراتيجية والتشريعية والتنظيمية والتنفيذية والتوعية والتدريب، بما يعزز الحفاظ على السلم و الأمن العالميين.

الكلمات المفتاحية: الفضاء السيبراني؛ الجرائم السيبرانية؛ الإرهاب الإلكتروني؛ الجريمة المنظمة؛ تحديات الأمن العالمي.

Abstract:

Cyberspace has become an influential element in today's world order and has revealed new forms of the international conflict known as the cyber conflict. The latter can cause heavy military and economic losses, along with substantial social and security threats. This article aims to highlight the most important threats that are enhanced by cyberspace which help reach the target partied quickly and easily. It also proposes a model framework for enhancing security in cyberspace which includes strategic, legislative, organizational, implementation, awareness, and training aspects, aiming at preserving the world peace and security.

***Key words**: Cyberspace; cyber crime; cyber terrorism; organized crime; global security challenges.*

مقدّمة:

أفضت الثورة المعلوماتية عن ظهور بيئة جديدة هي الفضاء الإلكتروني، وهي تختلف عن البيئات الأخرى (الإقليم البري، البحر، الجو، الفضاء الخارجي)، كونها من صنع الإنسان، ولكنها تشترك في بعض من السمات والخصائص مع البيئات الأخرى، وأضحى الفضاء الإلكتروني عنصراً مؤثراً في النظام الدولي، نظرا لما يحمله من أدوات تكنولوجية متطورة، تلعب دورا مهما في عمليات الحشد والتعبئة في العالم برمته، فضلا عن التأثير في القيم السياسية، والتأثير على أنماط "القوة – الحرب – الأمن" وتستخدم العديد من الدول القدرات التي يوفرها الفضاء الإلكتروني لاعتبارات في مقدمتها الأمن والقوة العسكرية، وهذا جعل تلك الدول تدخل الفضاء الإلكتروني ضمن حساباتها الاستراتيجية وأمنها القومي، وظهر بعد جديد في الصراعات الدولية وهو "صراع الفضاء الإلكتروني"، حيث يستطيع أحد أطراف الصراع أن يوقع خسائر فادحة بالطرف الآخر، وأن يتسبب في شل البنية المعلوماتية والاتصالية الخاصة به، وهو ما يسبب خسائر عسكرية واقتصادية فادحة، من خلال قطع أنظمة الاتصال بين الوحدات العسكرية وبعضها البعض، أو تضليل معلوماتها، أو سرقة معلومات سرية عنها، أو من خلال التلاعب بالبيانات الاقتصادية والمالية وتزيفها أو مسحها من أجهزة الحواسيب، أو من خلال استغلال التسهيلات التي يمنحها هذا الفضاء لارتكاب أو تسهيل ارتكاب الجرائم .

وبهذا أفسح الفضاء السيبراني عن محاور جديدة للصراع وأضاف مستويات كثيرة من التعقيد في العلاقات الدولية، وأصبح أكثر تأثيرا في الحسابات الاستيراتيجية، كما بات يشكل منظومة اجتماعية تقنية واقتصادية ذات تأثيرات على الأمن بأبعاده المادية والاقتصادية والاجتماعية للدول.

إن نمو قطاع تكنولوجيا الاتصالات والمعلومات جعل الصراعات أكثر سهولة و وفر إمكانيات بمتناول الدول العدائية والمنظمات الإرهابية والجريمة المنظمة، ومكّن هذه الجماعات من بلوغ المجتمعات الأخرى وتهديد المنظومات الحكومية الأساسية والتأثير على مهمات دقيقة للمؤسسات العامة والخاصة، من هنا، على الاختصاصيين في القوة العسكرية ونظرائهم المدنيين العاملين في مجال الأمن والقضاء والاقتصاد، التصدي لجهود الأعداء سواء كانوا ينتمون إلى دول أو كانوا إرهابيين منتمين إلى مجموعات أصولية متطرفة.

إن الدولة التي لا تملك التكنولوجيا السيبرانية المحصنة أمنيا سيصبح فضاؤها السيبراني المتضمن للأصول والموارد والمعلومات والخدمات والبنية التحتية التابعة لجميع القطاعات الحيوية (التجارية، الأمنية، العسكرية، المصرفية، الصحية، التعليمية، السياحية، الاقتصادية... إلخ) عرضة للهجمات والتهديدات السيبرانية (الاختراق، القرصنة، التخريب، التلاعب، التحوير، السرقة... إلخ)، وبالتالي سيؤدي ذلك إلى نتائج كارثية على أمنها القومي والاقتصادي والاجتماعي.

لهذا أصبح الفضاء الإلكتروني يدخل ضمن أولويات السياسة الخارجية للعديد من الدول وضمن استراتيجيات الأمن القومي لديها، و دفعت التهديدات المتزايدة لأمن الفضاء الإلكتروني العديد من الدول للعمل على بذل الجهود فرادى وجماعات بشأن الحفاظ على أمن الفضاء الإلكتروني.

فما هي أهم تداعيات الفضاء الإلكتروني -من الناحية الإجرامية - على السلم والأمن سواء على المستوى المحلي أو العالمي؟ وما هي أهم الاستراتيجيات الوطنية و الدولية لمواجهتها؟

سنتناول في هذه الدراسة إذن جانبا من التهديدات التي يعززها الفضاء الإلكتروني بما يتيحه من سرعة وسهولة في الوصول إلى الأطراف المستهدفة، كما نقترح إطارا نموذجيا لتعزيز الأمان في الفضاء السيبراني وهو يشمل النواحي الاستراتيجية والتشريعية والتنظيمية والتنفيذية والتوعية والتدريب، ويشكل هذا الإطار مخططا توجيهيا يبين الخطوات العملية الواجب اتباعها في كل دولة لتعزيز الأمان والأمن السيبراني ومكافحة الجرائم السيبرانية، وعليه تهدف هذه الدراسة إلى وضع الإطار التنظيمي والإجرائي للحد من الجرائم السيبرانية وضمان الأمن السيبراني.

المبحث الأول:

الفضاء الإلكتروني النمط الجديد للإجرام

فرضت الثورة التكنولوجية مجموعة من التحديات و التهديدات الأمنية الجديدة، وبرز في النظام الدولي ما يعرف بالفضاء الإلكتروني الذي أثر بدوره على التفاعلات السياسية و الدولية الحاصلة بين مختلف الفاعلين في العلاقات الدولية المعاصرة، وحتى على المستوى الوطني.

عصر المعلومات غيّر كل شيء، وبذلك تغيّر معه شكل الجرائم وأساليبها من جرائم تقليدية تعتمد على وسائل وأساليب مادية ملموسة، أصبحت في القرن الحادي والعشرين الجرائم و الحروب السيبرانية هي بديل لتلك الصورة النمطية التقليدية، وأصبحت السرعة والدقة في تنفيذ الجرائم و الهجمات من أهم ميزاتها، وهذه الجرائم بعد أن كانت تستهدف أجهزة الإنترنت والحواسيب الآن تستهدف قطاعات وصناعات محددة وحيوية واستراتيجية (الصباحي، 2017).

ساهم التطور التكنولوجي في مجال المعلوماتية بطرق مختلفة وأساليب منها المعقدة والسهلة، في تطور أشكال الاجرام على كافة المستويات الاجتماعية والاقتصادية والثقافية والسياسية ...، ومما عزّز خطورة هذه التكنولوجيا هو تجاوزها للحدود الوطنية وانتشار شبكاتها عالميا، إذ لا تقتصر تهديدات الفضاء الإلكتروني على المستوى الوطني، بل تتعداه اليوم إلى تهديد أمن وسلامة الدول.

وإن من أهم الجرائم التي شكّل الفضاء الإلكتروني إضافة ومنعرجا حاسما بالنسبة لها هي الإرهاب و الجريمة المنظمة، وهو ما سنركز عليه في هذا المبحث على اعتبار أن الجريمة المنظمة و الإرهاب هي من الجرائم التي تنعكس آثارها على المستويين الوطني و الدولي.

المطلب الأول: الفضاء الإلكتروني و الإرهاب

يجب التفرقة بين الجريمة والإرهاب في الفضاء السيبرانى، فالجريمة الإلكترونية، تتعلق بالاستيلاء على ممتلكات الغير أو تخريب الأنظمة، ولكن الإرهاب الإلكتروني هو استخدام شبكات المعلومات والانترنت والكمبيوتر من أجل التخويف والإرغام لتحقيق أهداف سياسية، ويمثل الإرهاب

الإلكتروني أحد مظاهر الانصهار بين العنف والتكنولوجيا، ويوظف التقنيات الحديثة في مجالات الاتصال والمعلوماتية التي تعد أحد تجليات العولمة الحديثة (عبد الصادق، 2013، ص 15).

وقد ثبتت جدوى الإنترنت منذ أواخر الثمانينات باعتبارها وسيلة اتصال شديدة الحيوية، لها قدرة مذهلة على الوصول إلى الجمهور في وقت قياسي وفي كل أنحاء العالم، وقد أدى استحداث تكنولوجيات تتطور باستمرار إلى خلق شبكة ذات نطاق انتشار شامل، تسهل على الفرد أن يتواصل عبر الحدود بسرعة وفعالية، ومع إمكانية عدم الكشف عن هويته إلى حد ما مع عدد يكاد يكون غير محدود من الأشخاص، ولتكنولوجيا الإنترنت فوائد عديدة، بدءا من سهولة تبادل المعلومات والأفكار التي تتيحها بشكل منقطع النظير، وهذا حق من حقوق الإنسان الأساسية المعترف بها، غير أنه لابد من الإقرار بأن نفس التكنولوجيا التي تتيح هذا النوع من التواصل يمكن أن تستغل أيضا لأغراض إرهابية، ويطرح استخدام الإنترنت في أغراض إرهابية تحديات (عبد الصادق، 2009، ص ص155-229)، كما يتيح فرصا في مجال مكافحة الإرهاب (وهو ما سنتطرق له في المبحث الثاني من هذه الدراسة).

الفرع الأول: أساليب استخدام الإنترنيت في الدعاية لأغراض إرهابية

تستخدم الإنترنت لأغراض إرهابية وذلك بعدة طرق أولها الدعاية، حيث يستخدم الإرهابيون الإنترنت أكثر ما يستخدمونه لبث دعايتهم، وعادة ما تتخذ الدعاية شكل اتصالات عبر وسائط متعددة تحمل تعاليم إيديولوجية أو إرشادات عملية، أو تقدم شروحا للأنشطة الإرهابية أو تسوق المبررات لها أو تشجع على القيام بها، وإن كان بث الدعاية ليس – على وجه العموم – نشاطا محظورا باعتبار أن أحد المبادئ الأساسية للقانون الدولي هو حماية حقوق الإنسان الأساسية التي تشمل الحق في التعبير ماعدا بعض الاستثناءات التي قد تشمل الاتصالات التي تضر ضررا واضحا بالأمن القومي، والاتصالات التي يجتمع فيها عنصرا التحريض عن قصد على ارتكاب أعمال عنف ضد أفراد بعينهم أو مجموعات معينة من الأفراد، واحتمال نجاح هذا التحريض.

كما أن الترويج للخطاب المتطرف الذي يشجع على أعمال العنف توجّه شائع لدى مجموعة متزايدة من منصات الإنترنت التي تنشر محتويات يعدها المستخدمون أنفسهم، وقد أصبحت الإنترنت وسيلة لعرض الكثير من المحتويات باستخدام مجموعة كبيرة ومتنوعة من الأدوات، كالمواقع المخصصة لمواضيع معينة، أو بعض غرف الدردشة والمنتديات المحددة الأهداف، والمجلات الإلكترونية، ومنصات التواصل الاجتماعي مثل تويتر وفيسبوك، والمواقع ذات الشعبية لعرض صور الفيديو وتبادل الملفات، مثل يوتيوب.

إن أكبر خطر تشكّله الدعاية الإرهابية يتعلق بالطريقة التي تستخدم بها والقصد الذي تبث من أجله الذي قد يكون إما بهدف التجنيد أو التحريض أو الدفع باتجاه التطرف-(Weimann, 2006,pp38.39)

أولا-التجنيد

يمكن استخدام شبكة الإنترنت باعتبارها وسيلة لنشر الخطاب المتطرف ومقاطع الفيديو التي تندرج ضمنه فحسب، بل أيضا لإقامة علاقات بمن يتجاوبون مع الدعاية والتماس الدعم منهم، وتقبل

التنظيمات الإرهابية إقبالا متزايدا على استخدام مواد الدعاية التي توزع عبر منصات مثل المواقع المحمية بكلمات سر، وروابط مجموعات الدردشة التي يخضع الدخول إليها لقيود باعتبارها وسيلة للتجنيد السري، ويتيح انتشار شبكة الإنترنت الواسع للتنظيمات الإرهابية والمتعاطفين معها إمكانية التجنيد على نطاق عالمي، وتفسح منتديات الإنترنت التي يخضع الدخول إليها لقيود المجال أمام المجندين ليتعرفوا على التنظيمات الإرهابية ويقدموا دعمهم لهم وينخرطوا مباشرة في أعمال تهدف إلى تحقيق أهداف إرهابية، كما أن استخدام حواجز تكنولوجية مام دخول منصات التجنيد يزيد من تعقيد عملية تعقب الأنشطة المتصلة بالإرهاب من قبل العاملين بأجهزة الاستخبارات وإنفاذ القانون (مكتب الأمم المتحدة المعني بالمخدرات والجريمة، 2013).

وكثيرا ما تعد مواد الدعاية الإرهابية خصيصا لتلقى قبولا لدى الفئات الضعيفة والمهمشة في المجتمع، ومن الشائع استغلال إحساس الفرد بالإقصاء والمهانة لتجنيده والدفع به باتجاه التطرف، كما قد تكون شبكة الإنترنت وسيلة فعالة للغاية لتجنيد القصر الذين يمثلون نسبة كبيرة من مستخدميها، وقد تتخذ الدعاية المنشورة عبر الإنترنت بغرض تجنيد القصر شكل رسوم متحركة، أو مقاطع فيديو لموسيقى ذات شعبية، أو ألعاب الكمبيوتر، ومن الأساليب المتبعة في استهداف القصر من قبل المواقع الشبكية التي تديرها تنظيمات إرهابية أو أتباعها إقحام رسائل تشجع على الأعمال الإرهابية كالهجمات الانتحارية، وتشيد بها في رسوم متحركة وقصص للأطفال، وبالمثل، صممت بعض التنظيمات الإرهابية ألعاب فيديو على الإنرتنت بغرض استخدامها أدوات للتجنيد والتدريب، وقد تروج هذه الألعاب لاستخدام العنف ضد دولة أو شخصية سياسية بارزة، مع مكافأة اللاعب على نجاحه في تنفيذ هذه الأعمال الافتراضية، وقد تتاح هذه الألعاب بلغات متعددة،حتى تلقى قبولا لدى جمهور واسع (مكتب الأمم المتحدة المعني بالمخدرات و الجريمة، 2013).

ثانيا-التحريض و الدفع باتجاه التطرف

إذا كانت الدعاية في حد ذاتها غير محظورة على وجه العموم، فإن العديد من الدول تعتبر استخدام الإرهابيين للدعاية من أجل التحريض على أعمال إرهابية أمرا مخالفا للقانون، فشبكة الإنترنت تتيح عددا وفيرا من المواد والفرص لتحميل وتحرير وتوزيع محتويات يمكن اعتبارها تمجيدا لأعمال إرهابية أو تحريضا على ارتكاب هذه الأعمال بما يخالف القانون .

يمكن النظر إلى التجنيد والدفع باتجاه التطرف والتحريض على الإرهاب باعتبارها حلقات في سلسلة متصلة، ويشير تعبير "الدفع باتجاه التطرف" في المقام الأول إلى عملية التلقين التي غالبا ما تستخدم الدعاية إلى أفكار متطرفة، وكثيرا ما تصاحب تحول المجندين إلى أفراد عازمين على انتهاج مسلك عنيف استنادا إلى أفكار متطرفة، وكثيرا ما تستخدم الدعاية في عملية الدفع باتجاه التطرف سواء الدعاية المنقولة من شخص إلى شخص أو عبر الإنترنت على مدار فترة زمنية، ويتفاوت طول الفترة الزمنية المطلوبة ومدى فعالية الدعاية وغيرها من وسائل الإقناع المستخدمة وفقا لظروف الأفراد والعلاقات فيما بينهم (عبد الحليم، 2018).

منذ عام 2014، كشف تنظيم «داعش» للعالم عن القوة والتأثير اللذين تتمتع بهما الأنشطة التي تُمارَس عبر الإنترنت، ووسائل التواصل الاجتماعي التي يبسط من خلالها المتطرفون والجماعات الإرهابية نفوذهم، حيث يستخدمون مواقع شهيرة مثل (تويتر، وفيسبوك، ويوتيوب)، لنشر دعايتهم وفظائعهم، فمن خلال إنتاج مواد لتنظيمي القاعدة و داعش بلغات متعددة، مثل الألمانية، والروسية، والفرنسية، والإنجليزية، يمكن لهذه الجماعات توجيه الدعاية لجمهور أكبر، وتوسيع نطاق الحملات الدعائية وتوصيلها لجمهور جديد على الإنترنت، وعن طريقة تعامل منصات التواصل الاجتماعي، مثل «تويتر، وفيسبوك»، مع المحتوى المتطرف على منصاتها وإجراءات التعطيل اللاحقة التي يتم اتخاذها لمواجهة ذلك، فإن طريقا طويلا يجب قطعه لتحقيق تعاون حقيقي بين منصات وسائل التواصل الاجتماعي، وخاصة أن هذه المنصات لديها أنظمة تشغيل وإجراءات منفصلة خاصة بها للتصدي للتطرف، ومن ثمّ فإن هذه «العملية البيروقراطية» تعمل على إبطاء الإجراءات المنسقة لمكافحة التطرف، و من الناحية العملية فإن الكمية الكبيرة من المواد الإرهابية التي تتم مشاركتها على هذه المواقع يصعب تعقبها وإزالتها على الرغم من أن مواقع مثل «تويتر» توظف مئات المراجعين للمحتوى عبر الإنترنت، ولهذا السبب تظل معتمدة على وصول المستخدمين إلى هذا المحتوى والإبلاغ عنه حتى تتم إزالته، وكانت إحدى القضايا البارزة الأخيرة هي الكشف عن مقطع فيديو تعليمي عن صناعة القنابل التي استخدمها مرتكبو تفجير «مانشستر أرينا» عام 2017 ظل على الإنترنت في عام 2020، وشوهد أكثر من 17 ألف مرة، بما في ذلك على «تليغرام» وعلى موقع المكتبة الرقمية المجاني (أرشيف الإنترنت) (مركز الخليج للدراسات الإستراتيجية، 2021).

إنّ الإرهاب الإلكتروني عبارة عن عملية تتمثل في توظيف شبكة الإنترنت بوسائلها المختلفة والخدمات الإلكترونية المرتبطة من خلالها في نشر وبث واستقبال وإنشاء المواقع والخدمات التي تسهل انتقال وترويج المواد الفكرية المغذية للتطرف الفكري وخاصة المحرضة على العنف أيا كان الشخص أو الجماعة التي تتبنى وتشجع كل ما من شأنه توسيع دائرة ترويج مثل هذه الأفكار المتطرفة، لذا أصبحت مواقع التواصل الاجتماعي تؤثر تأثيراً مباشراً في الأمن القومي للمجتمعات واستقرارها، ويظهر جليا ذلك من خلال نموذج أحداث مجزرة نيوزيلندا أو كما عرف بهجوما كرايستشيرش بتاريخ 2019/3/15 حيث أشفر التحريض والعنف وبث الأفكار والاعتقادات المتطرفة عن هجومان إرهابيان، دافعهما سيادة البيض وكراهية الإسلام، وتلخصت الحادثتين في إطلاق النيران داخل مسجدي النور ومركز لينود الإسلامي في مدينة كرايستشرش في نيوزلندا ونتج عنهما 51 قتيلا، وأصيب 50 آخرون، وعثرت الشرطة على سيارتين ملغومتين وأبطَلت فيهما مفعول المتفجرات، ويعد هذا أول حادث هجوم بإطلاق نار ضد مجموعات في نيوزيلندا منذ مجزرة راوريمو عام 1997، ويعد حادث إطلاق النار الأكثر دموية في تاريخ نيوزيلندا الحديث.

وقد وصفت رئيسة وزراء نيوزيلندا جاسيندا آردرن وعدد من الحكومات في العالم الحادث بأنهُ هجوم إرهابي. وقد اشتُبه بضلوع أربعة مجرمين في الهجوم أحدهم أسترالي الجنسية وصفه الإعلام بأنه من اليمين البديل ومؤمن بسيادة البيض، ويبلغ من العمر 28 عاماً، وكان يستخدم رموزًا وشعارات تعود

للنازين الجدد، وقد ربط بين الهجومين وبين الزيادة العالمية في نشاط متطرفي سيادة البيض واليمين البديل، والذي لوحظ منذ منتصف عقد 2010، وفي 27 أوت 2020، صدر الحكم على مُنفذ الهجومين برينتون تارانت بالسجن المؤبد مدى الحياة دون إمكانية الإفراج عنه.

إن الإرهاب الإلكتروني في سياق مجزرة نيوزيلندا أثبت بالدليل القاطع أن لهذه المنابر الإرهابية الافتراضية، نتائج عكسية كشفت عن الوجه القبيح للإرهاب الأسود، بقدرتها على تهديد الأمن والاستقرار الاجتماعيين، والتأثير في الأوضاع السياسية والاقتصادية، وخلق حالة من الذعر والفوضى في المجتمعات المستهدفة (الدحدوح، 2019).

الفرع الثاني: استخدام الإنترنت في الأعمال الإرهابية

هناك مجالات أخرى تستخدم فيها الجماعات الإرهابية الإنترنت ، سواء لتمويل الأعمال الإرهابية إما عن طريق الطلب المباشر، أو التجارة الإلكترونية، أو استغلال أدوات الدفع عبر الإنترنت، أو من خلال استغلال المنظمات الخيرية، كما تعتبر المنصات الإلكترونية بالنسبة لهذه الجماعات بمثابة معسكر تدريبي افتراضي، أو وسيلة للتخطيط لعمل إرهابي وتنفيذه، وبالتالي أصبحت الإنترنت عاملا مساعدا للعمل الإرهابي التقليدي المادي، وذلك بتوفير المعلومات الضرورية عن الأماكن المستهدفة، أو استخدامه كوسيط في عملية التنفيذ، إذ يعد الإنترنت إحدى أدوات تحقيق الترابط التنظيمي بين الجماعات و الخلايا التي تمكنهم من تبادل المقترحات و الأفكار والمعلومات الميدانية حول كيفية إصابة الهدف واختراقه و التخطيط و التنسيق و للعمل الإرهابي، وقد استغلت "القاعدة" الإنترنت لتحقيق أهدافها سواء العسكرية أو الدعائية، فكثير من العمليات الإرهابية التي قامت بها لعب فيها "جوجل إيرث" الدور الأكبر، هذا بالرغم من السيطرة المحكمة على الشبكة الدولية ، غير أن ذلك لم يمنع من ظهور برامج تشفير تساعد الإرهابيين على التواصل، وسنلخص أهم استخدامات الجماعات الإرهابية للإنترنت في أعمالها كما يلي :

أولا -التمويل

يمكن للتنظيمات الإرهابية وأنصارها أن يستخدموا الإنترنت أيضا لتمويل الأعمال الإرهابية، ويمكن أن تصنف الطرق التي يستخدمها الإرهابيون لطلب الأموال والموارد وجمعها عبر الإنترنت إلى أربع فئات عامة هي : الطلب المباشر، والتجارة الإلكترونية، واستغلال أدوات الدفع عبر الإنترنت، واستغلال المنظمات الخيرية.

ويكون الطلب المباشر عن طريق استخدام المواقع الشبكية، ومجموعات الدردشة، ورسائل البريد الإلكتروني الجماعية،والاتصالات الموجهة للأنصار لطلب تبرعات منهم، كما يمكن أن تستخدم المواقع الشبكية باعتبارها متاجر إلكترونية تبيع الكتب وتسجيلات صوتية ومرئية وغيرها من المواد للأنصار، وتسهيل خدمات الدفع عبر الإنترنت المتاحة عبر المواقع الشبكية المخصصة أو عبر منصات الاتصالات، تحويل الأموال إلكترونيا بين الأطراف المعنية، وكثيرا ما تحول الأموال عن طريق التحويلات البرقية الإلكترونية، أو بطاقات الائتمان، أو خدمات الدفع البديلة مثل السكايب (بن طالب، 2011، ص 11).

كما يمكن استغلال خدمات الدفع عبر الإنترنت بأساليب احتيالية مثل انتحال الشخصية، وسرقة بطاقات الائتمان، والاحتيال في التحويلات البرقية الإلكترونية، والاحتيال في معاملات الأوراق المالية، وجرائم الملكية الفكرية و الاحتيال في المزادات.

كما يمكن تحويل وجهة الدعم المالي الموجه إلى منظمات مشروعة ظاهريا مثل المؤسسات الخيرية، إلى أغراض غير مشروعة، ومن المعروف أن بعض التنظيمات الإرهابية تنشئ شركات صورية، تحت غطاء مشاريع خيرية، لطلب التبرعات عبر الإنترنت، وقد تدعي هذه المنظمات أنها تقوم بدعم أهداف إنسانية في حين تستخدم التبرعات في الواقع لتمويل أعمال إرهابية، وتشمل الأمثلة على المنظمات التي تدعي في العلن أنها منظمات خيرية لكنها في الأصل تستخدم لأغراض إرهابية عددا من المؤسسات التي تحمل أسماء لا توحي بأغراضها الحقيقية، كما أن الإرهابيين قد يخترقون فروعا لمنظمات خيرية، فيستخدمونها غطاء للترويج لأفكار التنظيمات الإرهابية، أو تقديم دعم مادي لجماعات المقاتلين(Maura, , 2006, pp12-13) .

ثانيا: التدريب

أصبحت التنظيمات الإرهابية - في السنوات الأخيرة- تستخدم الإنترنت استخداما متزايدا بوصفه ساحة تدريب بديلة للإرهابيين، وهناك مجموعة متزايدة من الوسائط التي توفر منصات لنشر أدلة عملية في صورة كتيبات إلكترونية، ومقاطع صوت وفيديو، ومعلومات، ونصائح، وتتيح هذه المنصات أيضا تعليمات مفصلة، غالبا ما تتخذ شكل وسائط متعددة بلغات متعددة يسهل الإطلاع عليها، حول موضوعات مثل كيفية الانضمام إلى تنظيمات إرهابية، وكيفية صنع المتفجرات، أو الأسلحة النارية، أو غيرها من الأسلحة أو المواد الخطرة، وكيفية التخطيط للهجمات الإرهابية وتنفيذها، وهكذا تكون هذه المنصات بمثابة معسكر تدريبي افتراضي، كذلك فإن هذه المنصات تستخدم لأمور في جملتها تبادل أساليب أو تقنيات أو معلومات عملية محددة بغرض ارتكاب عمل إرهابي (Bozabar, 2002, p24).

ثالثا: التخطيط

إن التخطيط لعمل إرهابي عادة ما ينطوي على اتصال عن بعد ما بين عدة أطراف،كذلك من الممكن اتخاذ خطوات عبر شبكة الإنترنت لتحديد هدف محتمل لهجوم إرهابي، وللوقوف على أكثر الوسائل فعالية لتحقيق غرض إرهابي، وقد تتراوح هذه الخطوات التحضيرية بين الحصول على تعليمات حول الأساليب الموصى بها لتنفيذ الهجوم وجمع المعلومات حول هدف مقترح من مصادر علنية ومن غيرها من المصادر، فالإمكانية التي تتيحها شبكة الإنترنت لتقريب المسافات وتجاوز الحدود، والكم الهائل من المعلومات.

كذلك من الممكن اتخاذ خطوات عبر شبكة الإنترنت لتحديد هدف محتمل لهجوم إرهابي وللوقوف على أكثر الوسائل فعالية لتحقيق غرض إرهابي، وقد تتراوح هذه الخطوات التحضيرية بين الحصول على تعليمات حول الأساليب الموصى بها لتنفيذ الهجوم وجمع المعلومات حول هدف مقترح من مصادر علنية ومن غيرها من المصادر، فالإمكانية التي تتيحها شبكة الإنترنت لتقريب المسافات وتجاوز الحدود، والكم الهائل من المعلومات المتاحة للجمهور في الفضاء السيبراني، تجعل من هذه الشبكة أداة رئيسية في التخطيط للأعمال الإرهابية (تلة، 2016، ص 20).

رابعا: التنفيذ

يتم تنفيذ أعمال إرهابية باستخدام الإنترنت عن طريق بث تهديدات صريحة باستخدام العنف، بما في ذلك التهديد باستخدام السلاح لإشاعة القلق أو الخوف أو الذعر بين أفراد مجتمع من المجتمعات أو فئة منه، وتوجيه تهديدات من هذا القبيل قد يعتبر في العديد من الدول ولو لم تنفذ، بمثابة جريمة، ويمكن أيضا أن يتم التواصل عبر الإنترنت مع الضحايا المحتملين، أو لتنسيق تنفيذ أعمال إرهابية مادية، فعلى سبيل المثال، استخدمت شبكة الإنترنت على نطاق واسع في التنسيق ما بين المشاركين في هجمات 11 سبتمبر 2001 على الولايات المتحدة.

وقد يكون استخدام شبكة الإنترنت في تنفيذ الأعمال الإرهابية في أغراض من بينها الحصول على مزايا لوجستية، أو الحد من احتمالات الكشف عن هذه الأعمال، أو إخفاء هوية الأطراف المسؤولة، كما يمكن أن تستخدم الإنترنت لتسهيل الحصول على المواد الضرورية لتنفيذ الهجوم، فقد يعمد الإرهابيون إلى شراء كل مكون وخدمة من المكونات أو الخدمات اللازمة لارتكاب أعمال إرهابية عنيفة عن طريق التجارة الإلكتروني، وقد تستخدم بطاقات الائتمان المختلسة أو غيرها من أشكال الدفع الإلكترونية الاحتيالية لتمويل هذه المشتريات (تلة، 2016، ص 26).

خامسا: الهجمات السيبرانية

يقصد بالهجمات السيبرانية، على العموم، استغلال الشبكات الحاسوبية عن عمد باعتبارها وسيلة لشن هجوم، وتهدف هذه الهجمات عادة إلى تعطيل النظم التي تستهدفها، وتتضمن تلك الأهداف نظم الحاسوب والخواديم وبنيتها التحتية الأساسية، وذلك عبر استخدام الاختراق الحاسوبي، أو التقنيات المتقدمة للتهديد المستمر، أو فيروسات الحاسوب، أو البرمجيات الضارة،أو غيرها من وسائل الدخول غير المصرح به أو ذي الأهداف الضارة، وقد تحمل الهجمات السيبرانية سمات عمل إرهابي، بما في ذلك الرغبة في زرع الخوف دعما لأهداف سياسية أو اجتماعية (مكتب الأمم المتحدة المعني بالمخدرات والجريمة، 2013، ص ص 11- 12).

المطلب الثاني: الفضاء الإلكتروني والجريمة المنظمة

إن التطور التكنولوجي في وسائل المواصلات والاتصالات والتقنيات الحديثة أدى إلى التقارب الشديد بين الدول، وجعل الجريمة لا تعرف الحدود الطبيعية أو الصناعية التي تفصل بين الدول، وأصبح الإجرام ينتقل في لحظات من دولة إلى أخرى لدرجة أن الجريمة قد يتم الإعداد لها في دولة ثم يشرع في ارتكابها في دولة ثانية، وربما تُنفَّذ في دولة ثالثة، وقد تظهر آثارها في دولة رابعة، فالعصابات الإجرامية تستخدم الوسائل التكنولوجية الحديثة لتوسيع نشاطها الإجرامي في مجالات الاتجار في المخدرات وغسيل الأموال والفساد والإرهاب وتجارة الرقيق.

الفرع الأول: أوجه الترابط بين الفضاء الإلكتروني والجريمة المنظمة

تستغل مجموعات الجريمة المنظمة الدول الضعيفة كقاعدة عمل تؤمّن من خلالها ملاذا آمنا تستطيع من خلاله ممارسة عملياتها العابرة للأوطان، مما يوفر لها في الواقع قدرا إضافيا من الحماية من تطبيق القانون، ويمكّن تلك المجموعات من ممارسة نشاطاتها بأقل قدر من المخاطر، وتتلاءم الصفات

المتأصِّلة للإنترنت كشبكة تتخطى حدود البلدان، مع هذا النمط من النشاط الإجرامي ومع الجهد الساعي إلى تحقيق أقصى الأرباح ضمن درجة مقبولة من المخاطر، ففي العالم الافتراضي، أي في عالم الشبكات الإلكترونية، لا توجد أي حدود، ويشكّل ذلك مزية تجعل النشاط الإجرامي عملاً جذاباً للغاية، عندما تحاول السلطات المختصة مراقبة هذا العالم الافتراضي تبدو أمامها حدود البلدان ومناطق الصلاحيات واسعة جداً، ممّا يجعل التحقيق في الجرم بطيئاً جداً في أحسن الأحوال، أو مستحيلاً في أسوأ الأحوال.

توفّر الإنترنت فرصاً للقيام بمختلف أشكال السرقات، سواء كانت من المصارف الموصولة بالشبكة أو من الممتلكات الفكرية، كما تؤمّن أيضاً وسائل جديدة لارتكاب جرائم قديمة كالاحتيال، وتوفر مكامن ضعف جديدة تتعلق بالاتصالات والمعلومات ما يتيح أهدافاً جذابة لجريمة الابتزاز، وهي الجريمة التي كانت دائماً السلعة الرئيسية لمنظمات المافيا.

ونظرا لإمكانية استخدام شبكة الانترنت من دون معرفة المستخدم ما يجعل منها وسيلة مثالية وجهازاً مثالياً لتنفيذ العديد من نشاطات الجريمة المنظمة، فالسرية تشكّل عادة جزءاً رئيسيا من إستراتيجية الجريمة المنظمة، وشبكة الانترنت توفّر فرصاً ممتازة للمحافظة على هذه السرية، فبالإمكان إخفاء المسار الذي تتبعه المعاملات عبر الانترنت لتصل إلى مقصدها (الفتلاوي، 2012، ص 612).

إنّ الترابط بين الجريمة المنظمة وشبكة الإنترنت ليس ترابطا منطقيا و طبيعياً فقط، ولكنه ترابط من المرجح له أن يزدهر وأن يتطور إلى حد أبعد و أخطر في المستقبل، فشبكة الإنترنت تؤمّن الأقنية والأهداف في نفس الوقت للجريمة، وتُمكِّن من استغلال هذه الأقنية والأهداف لتحقيق أرباح كبيرة بأقل قدر ممكن من المخاطر، وجماعات الجريمة المنظمة لا تريد أكثر من ذلك (عبد المنعم، 2010، ص 26).

الفرع الثاني: بعض الصور عن تأثير الفضاء الإلكتروني على الجريمة المنظمة

يتبادر إلى الذهن فور التحدث عن الجريمة المنظمة عصابات المافيا كون تلك العصابات من أشهر المؤسسات الإجرامية المنظمة، وقد سارعت عصابات المافيا بالأخذ بوسائل التقنية الحديثة سواء في تنظيم أو تنفيذ أعمالها، ومن ذلك إنشاء مواقع خاصة بها على شبكة الإنترنت لمساعدتها في إدارة العمليات وتلقي المراسلات واصطياد الضحايا وتوسيع أعمال وغسيل الأموال، كما تستخدم تلك المواقع في إنشاء مواقع افتراضية تساعد المنظمة في تجاوز قوانين بلد محدد بحيث تعمل في بلد آخر يسمح بتلك الأنشطة (العريان، 2006، ص 34)، كما يرتبط نشاط الجريمة المنظمة بالحرب الإلكترونية من خلال التمويه و التجسس.

والجريمة المنظمة ليست وليدة التقدم التقني وإن كانت استفادت كثيرا منه، فالجريمة المنظمة وبسبب تقدم وسائل الاتصال والتكنولوجيا والعولمة أصبحت غير محددة لا بقيود الزمان ولا بقيود المكان، وإنما أصبح انتشارها على نطاق واسع وكبير وأصبحت لا تحدها الحدود الجغرافية، كما استغلت عصابات الجريمة المنظمة الإمكانيات المتاحة في وسائل الإنترنت في تخطيط وتمرير وتوجيه المخططات الإجرامية وتنفيذ وتوجيه العمليات الإجرامية بيسر وسهولة.

فمن البديهي مثلا أن يأخذ المجرمون بأحدث ما توصلت إليه التقنية لخدمة أنشطتهم الإجرامية ويشمل ذلك بالطبع طرق غسيل الأموال التي استفادت من عصر التقنية فلجأت إلى الإنترنت لتوسعة وتسريع أعمالها في غسيل أموالها غير المشروعة، ويجد المتصفح للانترنت مواقع متعددة تتحدث عن غسيل الأموال، كما يجد ولا شك أيضا المواقع التي تستخدم كساتر لعمليات غسيل الأموال ومنها المواقع الافتراضية لنوادي القمار، ومن المميزات التي تعطيها الإنترنت لعملية غسيل الأموال السرعة، إغفال التوقيع وانعدام الحواجز الحدودية بين الدول، كما تساهم البطاقات الذكية، والتي تشبه في عملها بطاقات البنوك المستخدمة في أجهزة الصرف الآلية، في تحويل الأموال بواسطة الإنترنت مع ضمان تشفير وتأمين العملية، كل هذا جعل عمليات غسيل الأموال عبر الإنترنت تتم بسرعة أكبر وبدون ترك أي آثار في الغالب (العريان، 2006، ص ص 39- 40).

أما في ما يتعلق بالمخدرات فهناك مواقع على شبكة الإنترنت لا تتعلق بالترويج للمخدرات وتشويق النشىء لاستخدامها، بل تتعداه إلى تعليم كيفية زراعة وصناعة المخدرات بكافة أصنافها وأنواعها وبأبسط الوسائل المتاحة، يمكن للمراهق الانزواء في غرفته والدخول إلى أي من هذه المواقع ومن ثم تطبيق ما يقرأه وقد أكد العديد من الخبراء التربويين أن ثمة علاقة يمكن ملاحظتها بين ثالوث المراهقة والمخدرات والإنترنت، ولا تقتصر ثقافة المخدرات على تلك المواقع فقط بل تساهم المنتديات وغرف الدردشة في ذلك أيضا (عبد الرحمان، 2010).

كما لم يعد استهلاك المخدرات يقتصر على الطرق التقليدية بالحقن في الوريد أو المضغ أو الشّم أو التدخين، بل تطور الأمر ليصبح التعاطي إلكترونيا أو رقميا يُحدِث ذات التأثير الذي يحدثه المخدر الطبيعي، ويتم استخدام الإنترنت في تعاطي المخدرات من خلال جلوس تاجر المواد المخدرة أمام الحاسوب ليتلقى طلبات الشراء للمواد المخدرة عبر موقعه الالكتروني، وهنا لا يقوم بإرسال أحد تابعيه ليسلم المادة المخدرة المشتراة، وإنما يقوم المشتري بإجراء عملية تحميل المخدر الذي يرغبه في شكل ملفات وهو ما يعرف بالمخدرات الرقمية وتحتوي هذه الملفات الصوتية على نغمات أحادية أو ثنائية يستمع إليها المستخدم تجعل الدماغ يصل إلى حالة من الخدر تشابه تأثير المخدرات التقليدية.

وتتم تجارة هذا النوع من المخدرات عبر الانترنت، وتأخذ منتجاته شكل ملفات صوتية تحمّل أولا بشكل مجاني كعينة تجريبية غالباً ما تحقق غرضها وتوقع المستمع إليها ضحية الإدمان، كما يوجد للمخدرات الرقمية قواعدها الخاصة، حيث يقوم المستخدم الراغب في شراء المادة المخدرة باختيار الجرعة الموسيقية ونوعها من بين عدة جرعات متاحة على الموقع يمثل كل منها نوعاً من أنواع المخدرات التي يرغب فيها هذا المستخدم (United nation office on drugs and crime, 2013,p9)، ثم يقوم بتحميل ما تم اختياره وشراؤه من ملفات على مشغّل أغاني وسماعات ستيريو للأذنين والاستلقاء في غرفة بها ضوء خافت وتغطية العينين والتركيز على المقطوعة الموسيقية التي يتراوح مدتها بين 15 إلى 30 دقيقة للمخدرات المعتدلة أو 45 دقيقة للمخدرات شديدة التأثير (عبد الرحمان، 2010).

المبحث الثاني:
آليات مواجهة مخاطر الفضاء الإلكتروني

إنّ التهديدات التي أصبح يمثلها الفضاء الإلكتروني اليوم لم ولن تستثني أية دولة في العالم، لهذا بات من الضروري لجميع الدول من خلال الاتفاقيات الدولية وإصدار القوانين التشريعية تجريم أي استخدام غير آمن لتكنولوجيا المعلومات والاتصالات، بالإضافة إلى التعاون والتنسيق الدائم مع الأجهزة الدولية كالإنتربول الدولي في مجال تبادل المعلومات والاتصالات والخبرات الأمنية والفنية، حيث بات من الصعب اليوم تخيل أي صراع دون أن يكون لهذا الصراع أبعاداً إلكترونية، وأصبحت في صلب اهتمامات الأنظمة الدفاعية لأي صراع يمكن أن يحدث في المستقبل.

إنّ تهديدات الفضاء الإلكتروني كما رأينا لا تقتصر على الأمن الداخلي للدول بسبب ما يعرف بالجرائم السيبرانية، بل تتعداه إلى تهديد السلم و الأمن العالميين، فالتطورات الهائلة في وسائل التكنولوجيا والاتصالات قد وضعت أيضا في يد كل من الدول والفاعلون من غير الدول بما في ذلك الجماعات الإرهابية كما رأينا مجموعة جديدة من الأسلحة الهجومية، تمكنهم من تنفيذ هجمات إلكترونية أو سيبرانية، لتحقيق أهدافهم، والتي تتنوع ما بين تدمير أنظمة إلكترونية لمنشآت حيوية عسكرية أو مدنية، فقد أصبح من الممكن تعطيل أو إتلاف شبكات الدفاع العسكرية من عن بعد، واختراق أو تعطيل أو تدمير شبكات القطاع الخاص، وتعطيل البنية التحتية للبلد، والتدخل في سلامة البيانات العسكرية الداخلية لبلد آخر، ومحاولة إرباك أو التشويش على معاملاتها المالية أو تحقيق أي عدد من الأهداف الأخرى، ورغم ذلك فلم تصدر حتى الآن أية استجابة قانونية من قبل الأمم المتحدة وجهازها الرئيسى مجلس الأمن، أو محكمة العدل الدولية بشأن خطورة الهجمات الإلكترونية التي أصبحت واقعا يوميا يهدد السلم والأمن الدوليين، فلا توجد دولة مهما عظمت قدراتها العسكرية، ولا مؤسسة مهما عظمت قوتها الاقتصادية في مأمن من خطر الهجمات الإلكترونية(Waxman, 2011,p423) .

المطلب الأول: الإستراتيجية الدولية للحد من تهديدات الفضاء الإلكتروني

تتطلب مواجهة مخاطر الفضاء الإلكتروني العمل على عدة جبهات في آن واحد، حيث أنّ جهود دولة لوحدها لا يمكن أن يحد أو يمنع تلك المخاطر، لهذا فإن تحقيق الأمان السيبراني يتطلب تعاونا دوليا بين الدول، وبينها وبين الأجهزة الدولية وفي مقدمتها منظمة الأمم المتحدة، بالإضافة إلى التعاون الإقليمي، وكذلك ما يتطلبه الأمر من جهود فردية على كل دولة أن تتخذها داخل إقليمها من حيث التشريع و التوعية والتدريب، سنحاول من خلال هذا المطلب تبيان مختلف الآليات الدولية لمكافحة تهديدات الفضاء الإلكتروني.

الفرع الأول: التوجهات العامة العالمية لتحقيق الأمان السيبراني

ونخص بالذكر هنا أهم الجهود الدولية التي تقوم بها الهيئات الدولية في سبيل مكافحة الجرائم الإلكترونية وفي مقدمتها منظمة الأمم المتحدة والإتحاد الدولي للاتصالات، بالإضافة إلى آليات التعاون الدولي خاصة من خلال الاتفاقيات الإقليمية المبرمة في هذا المجال.

أولا: أبرز جهود المؤسسات الدولية لمواجهة مخاطر الفضاء السيبراني

1-قرارات ووثائق الأمم المتحدة: في نطاق العمل الأمني، أصدرت الأمم المتحدة عدة قرارات بخصوص الجرائم السيبرانية أو المعلوماتية، أهمها القرار رقم 55-63 بتاريخ 4 ديسمبر 2000 والقرار رقم 56-121بتاريخ 19 ديسمبر 2001 حول محاربة سوء استخدام تكنولوجيا المعلومات، وقد أوصى القرار 55-63 بأن تضمن الدول في قوانينها وممارساتها إلغاء أية ملاذات آمنة لكل من يسيء استخدام تكنولوجيا المعلومات،كما أقر بأن الأنظمة القانونية يجب أن تحمي سرية المعلومات وأنظمة الحاسوب وسلامتها من أي اعتداء غير مشروع، وأن تضمن معاقبة التصرف الجرمي، ويدعو القرار 56-121الدول عند صياغة قوانين وطنية أو سياسات أو ممارسات لمحاربة سوء الاستخدام الجزائي لتكنولوجيا المعلومات، أن تأخذ في الحسبان أعمال وإنجازات لجنة الوقاية من الجرائم والوقاية الجزائية (Schjolberg, 2008, p9) .

وقد أصدرت الجمعية العامة للأمم المتحدة في عام 2005 القرار رقم 60-177 الذي يشجع التعاون لمكافحة الجرائم السيبرانية وتقديم المساعدة للدول الأعضاء في هذا المجال، كما أصدرت الأمم المتحدة عام 2010 القرار 64-211 الذي يدعو الدول إلى تحديث قوانينها في مجال الجرائم السيبرانية والخصوصية والبيانات الشخصية والتجارة والتواقيع الإلكترونية، وإلى اعتماد الاتفاقيات والتجارب الإقليمية في هذه المراجعة.

كما بينت وثائق القمة العالمية لمجتمع المعلومات في جنيف عام 2003 ثم في تونس عام 2005 أهمية تطوير مجتمع المعلومات في مختلف الدول، وضرورة بناء الثقة والأمن في مجتمع المعلومات، وحددت الأطر التي يجب العمل بها من أجل تأمين ذلك.

2-جهود الإتحاد الدولي للاتصالات: أعلن الأمين العام للإتحاد الدولي للاتصالات عام 2007 إطلاق مبادرة أجندة الاتحاد الشاملة حول الأمن السيبراني، ويعمل الإتحاد الدولي منذ ذلك العام على هذه الأجندة التي تهدف إلى إنشاء إطار أو بروتوكول للتنسيق بين جهود مكافحة الجرائم السيبرانية، وهو يشمل تدابير قانونية وتقنية وتدابير إجرائية وتنظيمية وتدابير تخص بناء القدرات والتعاون الدولي، وقد جرى في عام 2008 نشر التقرير النهائي الذي تم إعداده من قبل أكثر من 100خبير، ويعمل الاتحاد الدولي للاتصالات على تنفيذ آلية لوضع إطار مشترك للأمن السيبراني للأمم المتحدة يعالج الأمن السيبراني على المستوى الوطني والإقليمي والدولي.

ثانيا-اليات التعاون بين الدول من خلال الاتفاقيات والمبادرات الإقليمية: توصي الأمم المتحدة بضرورة إيجاد آليات رسمية وغير رسمية للتعاون القضائي بين الدول بكل صوره، إما بموجب اتفاقيات دولية أو ثنائية، أو بموجب القانون الوطني، أو وفق مبدأ المعاملة بالمثل، وذلك تفاديا للتعرض لسيادة الدول، إذ قد يكون من الضروري تمكين الدول من القيام بأعمال تحقيق في أراضي دول أخرى، باعتبار أن أغلب الجرائم السيبرانية تتضمن عنصرا دوليا، أو تبادل المعلومات والمستندات، أو تحديد وجود المتهمين أو الشهود، ومن تبادل للمعلومات ونقل للإجراءات، والإنابة القضائية الدولية (الزهراني، 2020، ص 750).

وإضافة إلى التعاون الدولي في مجال التحقيقات القضائية، أو تبادل المعلومات والمستندات، أو تحديد وجود المتهمين أو الشهود، وتسليم المجرمين ، يتطلب التعاون الدولي كذلك تبادل المعلومات والدروس المستفادة من التجارب والممارسات الفضلى في دول أخرى لرفع مستوى الأمن السيبراني في الدولة، وتجدر الإشارة هنا إلى اتفاقية الأمم المتحدة حول الجريمة المنظمة العابرة للدول وبروتوكولاتها الثلاثة التي تتضمن آليات التعاون وهي غير مخصصة للجرائم السيبرانية لكنها قابلة للتطبيق في هذا السياق على الجرائم التي ترتكبها مجموعات منظمة وتكون داخلة ضمن نطاق الاتفاقية (اللجنة الإقتصادية و الإجتماعية لغربي آسيا، 2017، ص 22).

وتعتبر اتفاقية مجلس أوروبا حول الجرائم السيبرانية (اتفاقية بودابست)التي دخلت حيز التنفيذ في 1 جويلية 2004 من أهم الاتفاقيات الإقليمية، وتهدف هذه الاتفاقية إلى تنسيق التشريعات الوطنية حول الجرائم السيبرانية وتحسين القدرات الوطنية للتحقيق في هذه الجرائم والتعاون في هذا المجال، وهي تعنى بجمع الأدلة المعلوماتية في مختلف أنواع الجرائم، وليس في الجرائم السيبرانية فقط، وتتضمن الاتفاقية ثلاثة أجزاء: الجزء الأول حول القواعد الموضوعية للجرائم، والجزء الثاني حول إجراءات التحقيق، والجزء الثالث حول آليات التعاون الدولي.

وفي المنطقة العربية تم وضع الاتفاقية العربية في 21 ديسمبر 2010 لمكافحة جرائم تقنية المعلومات، والتي تضمنت خمسة فصول أساسية منها فصل خاص بالتجريم ويحدد أنواع الجرائم السيبرانية، وفصل يتعلق بالأحكام الإجرائية، وفصل خاص بالتعاون القانوني والقضائي في ما بين الدول العربية.

ولتنسيق التشريعات حول جرائم الحاسوب في دول الكومنولث، أعدت مجموعة من الخبراء قانونا نموذجيا في عام 2002 مستوحى من اتفاقية بودابست سمي "قانون الجرائم المتعلقة بالحاسوب"، كما أقر الاتحاد الأوروبي في عام 2003 إطارا قانونيا حول الاعتداءات على الأنظمة المعلوماتية ودخل حيز التنفيذ عام 2005، وقد كانت منظمة التعاون والتنمية في الميدان الاقتصادي أول منظمة دولية أصدرت توجيهات حول جرائم الحاسوب وحول أمن أنظمة المعلومات والشبكات وكذلك اعتمدت عام 2014 اتفاقية الاتحاد الإفريقي الخاصة بمجال الأمن السيبراني، وحماية البيانات الشخصية .

وقد عمدت بعض المناطق إلى إنشاء مؤسسات متخصصة لتعزيز التعاون فيما بينها في مجال الأمن السيبراني، وذلك بهدف تبادل المعلومات والخبرات والممارسات الفضلى، ومن أهمها وكالة الإتحاد الأوروبي لأمن الشبكات والمعلومات التي تؤدي دور مركز الخبرة للاتحاد الأوروبي ولدوله وللقطاع الخاص فيه وللمواطنين الأوروبيين، وهي تقدم نصائح حول الممارسات الفضلى في السلامة المعلوماتية، وتساعد دول الاتحاد الأوروبي على تطبيق إرشاداته وتحصين البنية الأساسية الحساسة للمعلومات والشبكات، وتعزيز قدرات الدول على تفادي المخاطر السيبرانية ومعالجتها.

الفرع الثاني: دور الإنتربول في مكافحة الهجمات السيبرانية

يعد الإنتربول أهم آليات التعاون الشرطي الدولي لمكافحة الجرائم العالمية العابرة للحدود الوطنية بصفة عامة والجريمة المعلوماتية بصفة خاصة، فمهمة الإنتربول الأساسية تفعيل التعاون بين أجهزة

الشرطة التابعة للدول الأعضاء في المنظمة بتوحيد إجراءات التسليم، ومن خلال تنسيق العمل الشرطي وتجميع البيانات وتبادل المعلومات لتيسير خدمات التحقيق لضبط وملاحقة المجرمين الهاربين وتسليمهم إلى الدولة التي تطلب تسلمهم، وإنشاء و تطوير كل النظم القادرة على المساهمة بفاعلية في الوقاية والعقاب على جرائم القانون العام (شحاته، 2000، ص 110).

وقد وضعت منظمة الإنتربول 12 نظاما خاصا للتعاون، وهو النظام الوطني الخاص بالنقطة المرجعية المركزية NCRP ويوجد في كل دولة من الدول الأعضاء في الإنتربول مكتب مركزي وطني يُعد نقطة الاتصال مع الإدارات الأجنبية التي تجري تحقيقات خارج حدودها و تضم شبكة من المحققين العاملين في الوحدات الوطنية المعنية بالجرائم السيبرانية لتيسير الاتصالات الميدانية بين البلدان الأعضاء وتسريعها قدر الإمكان، ومن مهامها إنماء الاستراتيجيات والتقنيات والمعلومات بشأن أحدث الأساليب الجرمية في مجال جرائم تكنولوجيا المعلومات، وهناك فرق عاملة إقليمية لإفريقيا والأمريكيتين وآسيا وجنوب المحيط الهادئ و أوروبا والشرق الأوسط وشمال إفريقي، كما قامت منظمة الإنتربول بوضع برنامجً خاص لمكافحة الإجرام المعلوماتي يرتكز على التدريب والعمليات ويعمل على مواكبة التهديدات الناشئة (الأنتربول، 2014).

ولمكافحة ظاهرة استخدام الإنترنت من طرف الجماعات الإرهابية، أصدر الإنتربول ومركز الأمم المتحدة لمكافحة الإرهاب بشكل مشترك دليلا لمساعدة المحققين على جمع وتحليل وتبادل المعلومات التي يتم العثور عليها عبر الإنترنت ولا سيما على وسائل التواصل الاجتماعي، ويعرض الدليل المعنون ب "استخدام الإنترنت ووسائل التواصل الاجتماعي للتحقيقات المتعلقة بمكافحة الإرهاب" عددا من الممارسات الجيدة في المجالات التالية ويحصر بصورة شاملة أدوات شبكية عملية:

- فهم الطريقة التي يكيّف بها الإرهابيون استخدام الإنترنت ووسائل التواصل الاجتماعي لمواصلة الأنشطة على الشبكة.
- الممارسات الجيدة المعتمَدة في إجراء التحقيقات عبر الإنترنت لمكافحة الإرهاب.
- الخطوات المتبعة لطلب حفظ الأدلة الإلكترونية وجمعها، بما في ذلك من المزودين بخدمات الإنترنت (الإنتربول، 2019).

ويقدّم الإنتربول المساعدة للبلدان الأعضاء في كشف التهديدات السيبرية وتصنيفها حسب الأولوية وتنسيق إجراءات التصدي لها المركز المتعدد الاختصاصات لمكافحة الجريمة السيبرية، حيث يضم المركز المتعدد الاختصاصات لمكافحة الجريمة السيبرية خبراء في شؤون الإنترنت من أجهزة إنفاذ القانون والقطاع الخاص لجمع وتحليل جميع المعلومات المتاحة عن الأنشطة الإجرامية المرتكبة في الفضاء السيبري بهدف تزويد البلدان بمعلومات استخباراتية متسقة يمكن ترجمتها إلى تحرك عملي، وينشر المركز تقارير لتنبيه البلدان إلى تهديدات سيبرية جديدة وشيكة أو متطورة، وشملت التقارير السابقة التي قدمها المركز تهديدات محددة، ولا سيما برمجيات خبيثة، ورسائل تصيّد احتيالي، ومواقع إلكترونية حكومية مخترقة، واحتيال باستخدام أساليب الهندسة الاجتماعية وغير ذلك، ومنذ عام 2017أصدر المركز ما يزيد على 800 تقرير موجه للشرطة في أكثر من 150 بلدا (الإنتربول، 2019).

وعلى صعيد آخر رصد الإنتربول من جانفي إلى أفريل2020، وفقاً لـ "يورونيوز" 4 أوت2020 نحو (907) آلاف رسالة إلكترونية غير مرغوب فيها و (737) حادثة ناجمة عن برامج خبيثة و (48) ألف رابط لعناوين مواقع إلكترونية ضارة، كلها تتعلق بفيروس كورونا، وجمع الإنتربول هذه البيانات بفضل مسح أجري بين أفريل وماي في (194) دولة عضوا، واستجابت (48) دولة، بينها (42%) في أوروبا و(19%) في آسيا و(17%) في إفريقيا و(12%) في أمريكا و(10%) في الشرق الأوسط، وفق ما أفادت به الشركات المتخصصة بالأمن المعلوماتي.

المطلب الثاني: دور الفضاء الإلكتروني في دعم السلم والأمن الدوليين

لا يخفى على أحد الجوانب السلبية للفضاء الإلكتروني، سيما في تهديده للسلم والأمن الدوليين من خلال مختلف صور الاستخدامات التي أوردنا الأهم منها في المبحث الأول من هذه الدراسة، لكن وكما يقال فإن التكنولوجيا سلاح ذو حدين، فكما يمكن استغلالها في تحقيق أهداف إجرامية، يمكن كذلك أن تستغل التكنولوجيا نفسها في الكشف عن الجرائم ومكافحتها.

الفرع الأول: استخدام الإنترنت في مكافحة بعض الجرائم

إذا كان الإرهابيون قد استحدثوا العديد من الطرق لاستخدام الإنترنت في أغرا ض غير مشروعة، فإن استخدامهم لشبكة الإنترنت يتيح كذلك فرصا لجمع المعلومات الاستخبارية وغير ذلك من الأنشطة الهادفة لمنع الأعمال الإرهابية ومكافحتها، فضلا عن جمع الأدلة من أجل الملاحقة القضائية عن هذه الأعمال، فقدر كبير مما نعرف عن طريقة عمل التنظيمات الإرهابية وأنشطتها وأحيانا أهدافها يستمد من اتصالات المواقع الشبكية ومنتديات الدردشة وغيرها من الاتصالات عبر الإنترنت، وعلاوة على ذلك، فإن زيادة استخدام الإنترنت في أغرا ض إرهابية يتيح زيادة مقابلة في توافر البيانات الإلكترونية التي يمكن جمعها وتحليلها لأغراض مكافحة الإرهاب، وتقوم جهات إنفاذ القانون والمخابرات وغيرها من السلطات باستحداث أدوات تتطور باستمرار للمبادرة إلى منع الأنشطة الإرهابية التي تستخدم فيها شبكة الإنترنت وكشف هذه الأنشطة وردعها، كما أن استخدام أساليب التحري التقليدية، مثل الموارد المخصصة للترجمة بغرض كشف التهديدات الإرهابية المحتملة في وقت مناسب، آخذ في الازدياد بدوره.

وتتيح المناقشات التي تجرى على الإنترنت فرصة لطرح وجهات النظر المعارضة أو الدخول في نقاش بناء، وهو ما قد يؤدي إلى ثني أنصار محتملين للتنظيمات الإرهابية عن الانخراط في أعمالها، ومن الممكن طرح أفكار مضادة تقوم على أساس راسخ من الحقائق عبر منتديات النقاش والصور وشرائط الفيديو على الإنترنت، كذلك فمن الممكن ضمانا لفعالية الأفكار المطروحة، إظهار التعاطف إزاء القضايا الدفينة التي تساهم في الدفع باتجاه التطرف، مثل الظروف السياسية والاجتماعية، وتسليط الضوء على بدائل لتحقيق النتائج المرجوة دون اللجوء للوسائل العنيفة ، كما يمكن بث رسائل استراتيجية تحتوي على أفكار مضادة للدعاية الإرهابية عبر الإنترنت بلغات متعددة للوصول إلى جمهور عريض ومتنوع جغرافيا (مكتب الأمم المتحدة المعني بالمخدرات والجريمة، 2013، ص 12).

ويقّدم مركز الاتصالات الاستراتيجية لمكافحة الإرهاب، التابع لوزارة الخارجية في الولايات المتحدة الأمريكية، مثالا على مبادرة مشتركة بين الوكالات، بهدف الحد من التحول إلى التطرف والعنف، بدافع

من التطرف عبر الكشف في الوقت المناسب عن أمور في جملتها الدعاية المتطرفة على شبكة الإنترنت والرد السريع عليها بخطاب مضاد محدد الهدف عبر مجموعة واسعة من تكنولوجيات الاتصالات، بما في ذلك الأدوات الرقمية، فعلى سبيل المثال، ذكر في ماي 2012أن المركز قد رد في غضون 48 ساعة، على لافتات إعلانية تروج للعنف بدافع التطرف، نشرها تنظيم القاعدة في شبه الجزيرة العربية على مختلف المواقع الشبكية، بإعلانات مضادة على المواقع نفسها، تتضمن نسخة معدلة من الرسالة نفسها، فحواها أن ضحايا أنشطة هذا التنظيم الإرهابي كانوا من المواطنين اليمنيين، وقد نفذت هذه الحملة بالتعاون بين وزارة خارجية الولايات المتحدة ودوائر المخابرات والجيش، كما أن المركز يستخدم منصات إعلامية مثل فيسبوك ويوتيوب لبث رسائله المحتوية على خطابات مضادة (مكتب الأمم المتحدة المعني بالمخدرات والجريمة، 2013، ص 13).

الفرع الثاني: تجارب بعض الدول في مجال مكافحة مخاطر الفضاء السيبراني

اعتمدت بعض الدول ومنها اليابان وكوريا الجنوبية وماليزيا على بعض الإجراءات القانونية منها والتعاونية والداخلية لمواجهة تهديدات ومخاطر الفضاء الإلكتروني، فمن حيث الإجراءات القانونية، وللحفاظ على البيانات والمعلومات الحساسة ومختلف المؤسسات من الهجمات، أقر البرلمان الياباني قانونًا في عام 2014 يهدف لتعزيز الأمن السيبراني، حيث منح صلاحية واسعة للمركز الوطني لمجلس الوزراء من حيث الجاهزية و استراتيجية الأمن السيبراني، أما بالنسبة للجهود الماليزية في هذا الصدد فنجد أن الهيئة القومية للأمان الإلكتروني قد قامت بإصدار عدد من البيانات والتحذيرات للمستخدمين حول نقاط الضعف المختلفة في أنظمتهم والتي تجعلهم عرضة لمثل هذه التهديدات، كما أنها قامت بعدد من التدريبات وألقت عددًا من المحاضرات حول الموضوع في مناسبات مختلفة للتوعية من تلك المخاطر.

أما من حيث الإجراءات التعاونية وفي إطار سعي اليابان لحماية مؤسساتها الحيوية من الهجمات الإلكترونية، قامت بالاتفاق مع الولايات المتحدة الأمريكية على مد ما بات يعرف بـ (مظلة الدفاع الإلكتروني)، حيث تعهدت واشنطن أن تمد مظلتها للدفاع الإلكتروني لحماية اليابان، ومساعدتها في التصدي للتهديدات المتزايدة من الهجمات الإلكترونية على القواعد العسكرية، والبنية التحتية، مثل محطات الكهرباء، كما تعهدت وزارة الدفاع اليابانية بالإسهام في الجهود المبذولة من أجل التصدي لمختلف التهديدات الإلكترونية، بما في ذلك التهديدات ضد البنية الأساسية اليابانية والخدمات التي تستخدمها قوات الدفاع الذاتي اليابانية والقوات الأميركية (صحيفة العرب القطرية، 2015).

ويشار إلى أنّ الأمن الإلكتروني أصبح مجالا رئيسيا تعمق فيه اليابان والولايات المتحدة شراكتهما العسكرية، في إطار مجموعة من المبادئ التوجيهية الأمنية الجديدة، ومن شأنها أيضا أن تدمج أنظمة الدفاع الصاروخية، وتعطي طوكيو دورا أمنيا أكبر في آسيا، حيث تتنامى القوة العسكرية للصين.

وتأتي المظلة الدفاعية الإلكترونية في ظل شعور كل من الولايات المتحدة واليابان بالقلق من التهديدات الإلكترونية، بما في ذلك الهجمات المحتملة من قبل الصين وكوريا الشمالية، كما تأتي هذه المظلة في ظل وجود ثاني أكبر قاعدة عسكرية أمريكية في آسيا، حيث تتواجد في اليابان، وعليه فإن الولايات المتحدة تستثمر لبناء قوة للتصدي والرد على الهجمات الإلكترونية.

أما في ماليزيا فعلى الرغم من أن معدلات التهديد التي تمثلها القرصنة والجرائم الإلكترونية بماليزيا مقارنة بغيرها من الدول ليست بالمرتفعة، إلا أن السلطات تقوم بالتعاون مع كبرى الشركات الإلكترونية لتطوير أنظمة الحماية من تلك التهديدات، وأن تزيد من حملات التوعية لمستخدمي الكمبيوتر والإنترنت وأن تعمل على توفير التحديثات المختلفة بشكل سريع وفعال لهؤلاء المستخدمين (طه، 2019، ص 139).

ومن حيث الإجراءات الداخلية وفي إطار تطوير اليابان قدراتها الدفاعية الإلكترونية، نظمت اليابان مسابقة دولية لمن يُعرفون بقراصنة القبعات البيض، وهم أشخاص ذوو مهارات عالية في برمجة الحاسوب، حيث أن هؤلاء لا يستخدمون مهاراتهم في القيام بعمليات قرصنة إلكترونية غير قانونية، بل يُسخّرونها لمساعدة السلطات في مواجهة الهجمات الإلكترونية وكشف الثغرات في البرامج والمواقع الإلكترونية، وإن الهدف من هذه المسابقة هو الاستفادة من المهارات الاستثنائية للشباب في مجال الإنترنت، وبدلاً من أن يستخدموا مهاراتهم في القرصنة الإلكترونية فإنهم يقومون بتسخيرها لخدمة المجتمع، وتأتي هذه الخطوة اليابانية لأن القراصنة ذوو القبعات البيض يساهمون من خلال هجماتهم القانونية في التعرف على نقاط الضعف في أنظمة حماية الإنترنت، والثغرات في خوادم أجهزة الحاسوب الخاصة بالمؤسسات الحكومية والخاصة، وتأمل اليابان في أن تساعدها هذه المسابقات على تنشئة جيل من محترفي الإنترنت كي يساهموا في حماية فضائها الإلكتروني، في ظل تزايد كبير في عدد الهجمات التي تتعرض لها (شكر، 2019)،كما قامت بتطوير فيروس لملاحقة وتعطيل مصادر الهجمات الإلكترونية التي تشن ضدها ، وقامت الصين التي تعد أول دولة في العالم تنشىء وحدة خاصة بالحرب الإلكترونية بتطوير أسلحة نبض كهرومغناطيسية (درويش، 2016، ص 127).

وقد قامت السلطات في كوريا الجنوبية بتقديم دورة تدريبية متقدمة لأبرز قراصنة الشبكة العنكبوتية في البلاد، بهدف تأهيل أفراد على مستوى عال من الخبرة لمواجهة الهجمات الإلكترونية على عدد من المنشآت الحساسة، وبحسب المعهد الكوري لبحوث تكنولوجيا المعلومات، فإن هذه الدورة التدريبية يطلق عليها اسم "Best Of The Best" ، حيث يقوم العاملون عليها بتدريب مجموعة مختارة من أبرز محللي أنظمة الترميز في البرامج والأنظمة الحاسوبية، وأشار المعهد إلى أن هذه الخطوة تأتي على خلفية العديد من الهجمات التي تعرضت لها البلاد خلال الأعوام الماضية، كانت أبرزها الهجوم الإلكتروني الذي وقع في العام 2011 والذي استهدف أحد أكبر البنوك وتسبب بخسائر فادحة، بالإضافة إلى الاعتداء الذي وقع بالعام 2009 على عدد من المواقع الإلكترونية التابعة للحكومة، الأمر الذي أدى إلى إلحاق خسائر وصلت قيمتها إلى 50.5 مليون دولار بحسب بعض التقديرات (شكر، 2019).

وفي نموذج آخر أنشأت بريطانيا "القوة السيبرانية الوطنية" National Cyber Force التي طال انتظارها والقادرة على تنفيذ مهمات ضد أهداف منها دول معادية وتنظيمات إرهابية وشبكات الجريمة المنظّمة ودوائر دولية تنشط في استغلال الأطفال جنسيا، وتهدف المنظمة التي ينضوي تحت سقفها عدد من أجهزة الأمن والاستخبارات، إلى توفير أكثر أنواع الدعم التكنولوجي تطوراً بهدف مؤازرة عمليات تتراوح

بين مهمات القوات الخاصة في القتال الميداني وبين التصدي لاستخدام الإنترنت من أجل استغلال الأطفال جنسياً.

حيث شهدت بريطانيا خلال عام 2020 وتيرة من الهجمات الموجّهة ضد البنية التحتية الاستراتيجية والمجالات المتعلقة بـ"كوفيد- 19"، ومن ضمنها محاولات اختراق أبحاث اللقاحات ونشر المعلومات الكاذبة بشأن الجائحة، كما تعرض الجيش البريطاني لهجمات مستمرة، إذ واجه أكثر من 180 هجوماً شهرياً أو 60 يومياً، وقد شنّت المملكة المتحدة العملية السيبرانية الهجومية الأولى بجهود مشتركة موجهة ضد تنظيم "الدولة الإسلامية (داعش)" بواسطة مهمات نهضت بها أجهزة الاستخبارات والجيش في العراق وسوريا، قبل سنتين، وسوف تعمل "القوة السيبرانية الوطنية" على مواصلة عرقلة مخططات التنظيمات الجهادية ونشاطاتها في التجنيد (عبر الإنترنت)، وفي هذ الصدد، أشار جيريمي فليمينغ، مدير "قيادة الاتصالات الحكومية" GCHQ إلى أن: "القوة السيبرانية الوطنية تُنشأ كقوة دفاعية. وتجمع القدرات الاستخباراتية والدفاعية لتحويل قدرات المملكة المتحدة للتصدي للأعداء في الفضاء السيبراني، وحماية بلدنا وشعبنا وطريقة عيشنا" (سنغوبتاِ، 2020).

كما قامت إيران بتأسيس مقر الدفاع الإلكتروني في أكتوبر عام 2011، وأصبحت من بين الدول التي تملك منظومة دفاعية كاملة في مواجهة تهديدات الفضاء الإلكتروني.

أما في ما يخص التشريع الجزائري فقد تبنى المشرع سياسة مزدوجة للتصدي لظاهرة الإجرام المعلوماتي، بحيث قام من جهة بتعديل الجوانب الموضوعية(القانون 04-15المؤرخ في 2004/11/10) والإجرائية (القانون06-22المؤرخ في 2006/12/20)للتشريعات العقابية العامة (قانون العقوبات و قانون الإجراءات الجزائية)، وجعلها تواكب التحديات الجديدة الناتجة عن التطور المتسارع للتكنولوجيات الحديثة، و قام من جهة ثانية باستحداث قوانين أخرى خاصة أكثر تجاوبا مع الطبيعة الخاصة للجرائم الإلكترونية، وهذا التنوع التشريعي من شأنه أن يساهم بشكل فعّال على الأقل في الوقت الراهن في الحدّ من تفاقم ظاهرة الإجرام الإلكتروني في الجزائر.

ومع ذلك تجدر الإشارة إلى أنه ورغم كل تلك الجهود في التصدي لظاهرة الإجرام الإلكتروني تبقى غير كافية نظرا لخصائص هذا النوع من الجرائم الذي لا يعترف بالحدود الجغرافية من جهة، والمرتبط بالتطور التكنولوجي السريع و المذهل من جهة أخرى، لهذا يتطلب الأمر جهودا أكثر وتعاونا أكبر على جميع المستويات الوطنية والإقليمية و الدولية ومن كل النواحي التشريعية و القضائية والأمنية .

الخاتمة:

من خلال الدراسة البحثية السابقة توصلنا إلى عدة **نتائج**: أهمها أن العصر الذي نعيش فيه بات عصرا رقميا بامتياز، تتحكم فيه المعرفة والمعلومات ووسائل الاتصالات، فمن يملك المعرفة يتحكم في كل شيء، وأصبح الفضاء السيبراني واقعي والجرائم السيبرانية حقيقة لا مفر منها، وأصبحت الرقمنة هي الصياغة السائدة في العصر الحالي، فكل شيء يتعامل عبر الفضاء الإلكترونى، ولذلك يتوجب على الدول

والأفراد الحذر والحيطة عند استخدام البيانات والمعلومات في المجال الافتراضي لتجنب الوقوع في مخاطر التصيد الشبكي والهاكرز والجماعات الإرهابية.

لقد غيّر الفضاء السيبراني الكثير من الجوانب الحياتية، الاقتصادية والاجتماعية، لكن كما نشأت عنه المنافع، شابته الكثير من المخاطر التي تتطلب مقاربة جديدة لحماية مستخدمي الإنترنت وبناء ثقتهم بالفضاء السيبراني، وبالتالي تعظيم الاستفادة منه، فمن أجل الاستفادة من الإمكانات التي توفّرها تكنولوجيا المعلومات والاتصالات، لابد من أن تبقى التكنولوجيا آمنة وفعّالة، دون اعتراض للمعلومات في خط سيرها، مع ضمان خصوصيتها وسلامتها من التحوير، وذلك أساسي لطمأنة الناس وبث الثقة في نفوسهم حول الإنترنت.

وعلى العكس من ذلك فإنّ للجرائم السيبرانية ولانتهاكات الأمان في الفضاء السيبراني عواقب عديدة ووخيمة على الصعيد الاقتصادي والاجتماعي والفكري وعلى الصحة العامة، وكذلك على الأمن القومي، وكما تطال الجرائم السيبرانية الأمن الاقتصادي، تطال كذلك سمعة الأفراد أو الشركات، وفي كلتا الحالتين تؤثر هذه الجرائم على ثقة المستخدم بالفضاء السيبراني.

إن التدابير التقنية وحدها، بالرغم من ضرورتها وأهمّيتها غير قادرة على مكافحة هذا النوع من الأفعال، وهنا تبرز أهمية وضع إطار تشريعي وطني، في ظل تنسيق إقليمي، يستكمل بتعاون دولي، فمسألة التعاون الدولي مهمة وحتمية، حيث أن الأخطار الإلكترونية ذات طبيعة عالمية، وتحتاج بالتالي إلى حل عالمي، على اعتبار أن الفضاء الإلكتروني مرفقا دوليا تقع به مصالح جميع الدول، ويتجاوز الحدود القومية والسيادة التقليدية للدول، وعلى الرغم من عدم وجود اتفاق دولي ينظم التعامل مع الفضاء الإلكتروني، فإن هناك وعيا متزايدا داخل بلدان العالم بشأن تلك الأخطار، الأمر الذي دفع بعض تلك البلدان إلى تبني تشريعات خاصة بالجريمة الإلكترونية.

إلا أن هذه التشريعات وحدها غير كافية، والدولة بمفردها لا تستطيع السيطرة على تلك المخاطر، أو أن تتحمّل بمفردها مسئولية حل مشكلات الأمن الإلكتروني، لذلك يتعين اتخاذ عدة إجراءات على جميع المستويات الوطنية والإقليمية والدولية في آن واحد للحد من تلك المخاطر ولذلك نقترح **التوصيات** التالية:

- تطبيق التشريعات التقليدية على الجرائم السيبرانية والتي تركّز على الأشياء الملموسة ضمن حدود معينة، على أن يصاحبها صياغة نصوص قانونية جديدة لتحكم مفاهيم جديدة غير ملموسة مثل البيانات والاختصاص القضائي وإجراءات التحقيق و الأدلة المعلوماتية.

- ضرورة تحديث التشريعات الموجودة في الجانب الموضوعي وكذلك في الجانب الإجرائي، وذلك لضمان محاربة الجرائم السيبرانية، ويجب أن يتمتع التشريع بصفة الحياد التقني، بحيث يمكن تطبيقه في المستقبل على التقنيات الحديثة التي تؤدي ذات الوظائف.

- تنسيق التشريعات بين الدول، وهذا التنسيق يمكن تحقيقه بفضل الاتفاقيات الدولية والتوصيات أو الإرشادات التي تصدرها المنظمات الدولية والإقليمية المعنية.

- إنشاء المحاكم وأجهزة التحقيق المتخصصة في ما يخص تطبيق التشريعات السيبرانية، هناك حاجة إلى وجود جهاز تحقيق رسمي متخصص يضطلع بدور مهم من حيث إجراء التحقيقات في الجرائم السيبرانية، وكذلك في الجرائم العادية التي تستند إلى أدلة معلوماتية معقدة، من خلال تدعيم إجراءات التحقيق بخبرات فنية تمكّنها من جمع الأدلة الرقمية من مسرح الجريمة أو من خارجه، وحفظ هذه الأدلة مع ضمان موثوقيتها ومصداقيتها وتحليلها وتقديمها للقضاء ضمن تقرير متكامل.

- يفترض أيضا تدريب العناصر غير المتخصصة من الشرطة على المهارات الأساسية في مجال الأدلة الجنائية المعلوماتية باعتبارها قد تدخل ضمن إطار أي تحقيق جزائي متعلق حتى بجريمة تقليدية.

- كما يتعين إنشاء محاكم متخصصة في الجرائم السيبرانية، حيث يفترض بالقاضي المتخصص في هذه الحالة فهم المفاهيم التقنية والإنترنت ومعرفة قوانين المعلوماتية والأدلة المعلوماتية، وخلاصة القول يجب على كل دولة أن تملك جهاز شرطة يملك قدرات للحد من الجرائم السيبرانية وكشفها وتحليلها.

- التعاون داخل الدولة الواحدة بين جميع الهيئات المعنية والقطاعين العام والخاص والشركات العاملة في مجال تكنولوجيا الاتصال و المعلومات من أجل وضع استراتيجية موحدة للأمن الإلكتروني.

- ضرورة إيجاد طرق جديدة للتعاون الإقليمي والدولي تحت مظلة الأمم المتحدة أو المنظمات الدولية المتخصصة كالاتحاد الدولي للاتصالات.

- التنسيق بين النظم القضائية في العالم.

- العمل على مساعدة الدول النامية والتي تعرف تأخرا في مجال المعلوماتية، فهي الأكثر عرضة لمخاطر الفضاء الإلكتروني، ومن شأن ذلك أن يعمل على إحراز تقدم في مجال مكافحة مخاطر وجرائم الفضاء الإلكتروني .

- إن مكافحة مخاطر الفضاء الإلكتروني يتطلب دورًا واضحًا ومحددًا للأمم المتحدة، مع أهمية الموازنة بين حدود الحرية والأمن في استخدام الفضاء الإلكتروني، وذلك إما عن طريق إقامة منظمة دولية خاصة بالأمن الإلكتروني، أو اتفاقية دولية بشأن الفضاء الإلكتروني، أو إنشاء منظمة عالمية متخصصة في شؤون الفضاء الإلكتروني باستقلال كامل عن هيئة الأمم المتحدة تتولى وضع القوانين المنظمة لاستخدامه، لأن الواقع يتطلب الإسراع في إيجاد نظام قانوني يعمل على تقليص درجات التهديد التي يمثلها استخدام القوة غير المشروع في هذا الفضاء، والعمل على حماية الدول من خطر التعرض لهذا الاستخدام، أو العمل على تعزيز دور الأمم المتحدة من خلال منظماتها المتخصصة كاليونسكو أو الاتحاد الدولي للاتصالات وغيرها من سائر الوكالات الدولية المتخصصة التابعة للأمم المتحدة التي تهتم بشؤون الفضاء الإلكتروني كل في حدود اختصاصها.

الإحالات والمراجع:

1. أبو سريج أحمد عبد الرحمان. (2010). استخدام الإنترنت في تعاطي المخدرات-المخدرات الرقمية-http://www.child-trafficking.org/sites/default/files/14.pdf.
2. أحمد عبيس نعمة الفتلاوي. (2012). الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر: مجلة المحقق الحلي للعلوم القانونية والسياسية، جامعة بابل كلية القانون، العدد الرابع، السنة الثامنة.
3. الإنتربول . (2014). الإنتربول: الإجرام السبراني، مجالات الإجرام السيبيري http://www.interpol.int/ar.
4. الإنتربول. (2019). الإنتربول والأمم المتحدة يُصدران دليلا مشتركا عن التحقيقات عبر الإنترنت لمكافحة الإرهاب https://www.interpol.int/ar.
5. اللجنة الإقتصادية والإجتماعية لغربي آسيا. (2017). الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية. الأمم المتحدة.
6. بن طالب ليندا. (2011). غسل الأموال وعلاقته بمكافحة الإرهاب. الإسكندرية.
7. سعيد درويش. (2016). ماهية الحرب الإلكترونية في ضوء قواعد القانون الدولي، مجلة حوليات جامعة الجزائر.العدد 29 ج 2.
8. سهير عثمان عبد الحليم. (2008). الإرهاب والإنترنت:دراسة حالة فى ضوء التجربة المصرية، ورقة مقدمة للمؤتمر الدولى الأول حماية أمن المعلومات والخصوصية فى قانون الإنترنت.القاهرة: مركز الأبحاث والدراسات القانونية، (2008/12/18).
9. شيحة حسين الزهراني. (2020). التعاون الدولي في مواجهة الهجوم السيبراني. الشارقة: مجلة جامعة الشارقة للعلوم القانونية، المجلد 17 العدد 1.
10. صحيفة العرب القطرية. (2015). أمريكا تمد مظلتها للأمن الإلكتروني لحماية اليابان، 30 مايو 2015.
11. عادل عبد الصادق. (2009). الإرهاب الإلكتروني. القاهرة: مركز الدراسات السياسية والاستيراتيجية.
12. عادل عبد الصادق. (2013). الفضاء الإلكتروني والرأي العام. المركز العربي لأبحاث الفضاء الإلكتروني: قضايا استيراتيجية.
13. عبد الحميد ابراهيم محمد العريان. (2006). العلاقة بين الإرهاب المعلوماتي والجرائم المنظمة. المغرب.
14. عبد المنعم علي ابراهيم أسامة. (2010). حظر ومكافحة غسل الأموال، الطبعة الأولى. الأردن: المركز القومي للإصدارات القانونية.
15. علاء الدين شحاتة. (2000). التعاون الدولي في مجال مكافحة الجريمة،القاهرة: بدون ناشر
16. عمر حامد شكر. (28, 6، 2019). المجال الخامس الفضاء الإلكتروني. تاريخ الاطلاع 25 -6-2020، المعهد المصري للدراسات: http://eipss-eg.org
17. فادي محمد الدحدوح. (2019). الإرهاب الإلكتروني في سياق مجزرة نيوزيلندا، https://www.aljazeera.net/blogs تاريخ النشر 2019/3/22، تاريخ الإطلاع: 2021/3/9
18. كيم سنغوبتا. (2020). المملكة المتحدة تعلن عن "قوة سيبرانية وطنية" تتصدى للتهديدات على الإنترنت https://www.independentarabia.com/node/171301.

19. نسرين الصباحي. (2017). الحروب السيبرانية وتحديات الأمن العالمي. تاريخ الاطلاع 15- 7- 2020، المركز العربي للبحوث والدراسات: http://www.acrseg.org/40594.
20. نور الله تلة. (2016). الإرهاب بالوسائل الالكترونية، مذكرة ماجستير في القانون الجزائي. دمشق: كلية الحقوق.
21. مركز الخليج للدراسات الاستراتيجية.(2021). مخاطر نمو الشبكات الإرهابية عبر الإنترنت http://www.akhbar-alkhaleej.com/news/article/1233668
22. مكتب الأمم المتحدة المعني بالمخدرات و الجريمة. (2013). استخدام الإنترنيت في أغراض إرهابية. نيويورك: الأمم المتحدة.
23. يسرا محمد طه. (2019). ماليزيا والتحديات الأمنية في القرن الحادي والعشرين. دراسة تطبيقية في مفهوم أمن الإنسان، في هدي ميتكيس وخليل رسلان، (محرران)، ماليزيا وتحديات القرن الحادي والعشرين.
24. *United nation ,office on drugs and crime .(2013). comprehensive study on cybercrime. UNODC.*
25. *Matthew C. Waxman, Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), The Yale Journal of International Law, Vol.36, 2011, P423.*
26. *Mohamed Bozabar.(2002).La criminalité informatique sur l' internet, journal of law academic, n°01, voulum26 ,faculté de droit, universite kowit.*
27. *Maura, C. (2006). back fighting and internet of terrorist. securité and information.*
28. *Schjolberg, S. (2008). The history of global hormonization on cybercrime legislation. Geneva: the Road to Geneva.*
29. *Weimann, G. (2006). terror on the intern. Cambridge University Press, UK.*

الفضاء الإلكتروني وتحديات الأمن العالمي ـــــــ