السيبرانية الإرهابية: المشكلة والحل؟

2019-01-13د. ميثاق بيات ألضيفي

أدى تطور الشبكة الالكترونية العالمية إلى ثورة في الاتصالات وأصبح الحوار يسيرا وممكنا مع جمهور واسع من جميع أنحاء العالم كما ويمكن استخدامها للشبكة مثل أية منصة مستقلة لمجموعة متنوعة من الأغراض بما في ذلك حتى لو كان ارتكاب أعمال غير قانونية أو هجومية أو خطيرة، وإن المنظمات الإرهابية تستخدمها لنشر أيديولوجيتها وجذب أعضاء جدد لها وللتخطيط والتجهيز وللقيام بالهجمات المتنوعة, وتستخدم الانترنيت لنشر مقاطع فيديو يظهر فيها عمليات إعدام المخطوفين والهجمات الإرهابية وكذلك تستخدمها لتجنيد أعضاء جدد ونشر وتوزيع منشورات إلكترونية عالية الجودة تحرض مؤيديها على العنف, ومع إن تلك الدعوات للعنف وللكراهية وتبرير الإرهاب هي محظورة على وسائل التواصل الاجتماعي غير انه لا يمكن كبحها لذا تبذل ادارات وسائل التواصل جهوداً كبيرة لتعقب وتعطيل الحسابات المرتبطة بالجماعات الإرهابية والمعززة للإيديولوجية الإرهابية غير إن هناك دائمًا خطر ظهور حساب مختلف على موقع الحساب المعطل.

تجدر الإشارة إلى أن إخفاء الهوية وسهولة الوصول إلى الإنترنت يسمحان للمنظمات الإرهابية باستخدام الشبكات الاجتماعية لجمع الأموال من الأشخاص الذين يتعاطفون معها وان الشبكات الاجتماعية تستخدم على نطاق واسع من قبل المنظمات الإرهابية من أجل تعزيز وإقامة اتصالات مع الأشخاص الذين يتعاطفون معهم كما ويمكن للمنظمات الإرهابية جمع كمية كبيرة من المال باستخدام الإنترنت وكما تقوم بنشاطات دعائية وإعلامية بين عدد كبير من الأشخاص عبر الوسائل الاجتماعية. وتتعد الاخطار وتتجدد كبروز خطر جديد لتمويل الإرهاب وهو طريقة "التمويل الجماعي" والتي تشمل جمع الأموال من الشركات أو المنظمات أو الأفراد الذين يستخدمون الإنترنت من خلال الاستثمارات والتبرعات لعدد كبير من الناس وهذه الطريقة لجمع الأموال بسيطة ومتاحة على نطاق واسع ويمكن للمنظمات الإرهابية أو الأفراد المتورطين في دعم الإرهاب أن يقدموا للناس معلومات لا تتوافق مع نواياهم الحقيقية حول جمع الأموال مع إنشاء منظمات غير ربحية لذا كانت هناك حالات لم يشك فيها المتبرعين حتى في أن المساهمة التي قدموها عبر الشبكات الاجتماعية يمكن لها أن تكون لصالح الإرهاب كما ويمكن تنفيذ هذه المجموعات في

شكل مساعدات إنسانية وبالتالي تغطية المنظمات الإرهابية لغرضها الحقيقي مما يجعل هذا النهج من المستحيل تحديد إعلاناتها وتحديدها عبر محركات البحث العادية. وقد أصبحت الشبكات الاجتماعية منصة لتمويل المنظمات الإرهابية وغالباً ما يحدث ذلك عن غير قصد وتجدر الإشارة إلى أن شركات المواقع الالكترونية تنشئ شبكات اجتماعية قد لا تتواطأ في تمويل الإرهاب ولكنها ربما ما تبادر بتقديم معلومات عن الحسابات المشبوهة إلى السلطات المختصة لتقوم بحجبها ومنعها.

تؤدي الطبيعة المتعددة الوظائف للتكنولوجيات المعلوماتية إلى مجموعة واسعة من تعريفات الإرهاب السيبراني وإن مفهوم تقنيات الإنترنت بمعناه الواسع يجعل المرء ينتبه للسياسة الوطنية لتنظيم الشبكة وإن انتشار دعاية العنف والتطرف عبر الشبكات الاجتماعية يُعترف به على أنه إرهاب سيبراني يهدف إلى تعطيل المناطق الحيوية وتنفيذ الأهداف الإرهابية وفقدان الحياة أو الهلع أو الانهيار الاقتصادي أو الترهيب من أجل التأثير في السياسات الحكومية. وفي عصر تكنولوجيا المعلومات هناك قلق متزايد بشأن إمكانية قيام الجماعات الإرهابية بارتكاب هجمات على الإنترنت وملاحظة مدى تعرض الدول لهذه الهجمات لدرجة انه من الممكن أن يصبح الإرهاب السيبراني تكتيكًا مرغوبًا فيه على نحو متزايد للجماعات الإرهابية ونظرًا لأنه يمكن أن تشن تلك الهجمات الإرهابية من على بعد آلاف الكيلومترات من الهدف فلذا سيكون من الصعب تتبعها, وإن الأهداف المحتملة للإرهاب الإلكتروني هي الصناعة المصرفية والمنشآت العسكرية ومحطات الطاقة ومراكز مراقبة الحركة الجوية وأنظمة المياه ومع ذلك لكنه والى ألان لا يوجد توافق في الآراء بين مختلف الحكومات ومجتمع أمن المعلومات بشأن ما يمكن اعتباره فعلاً من أفعال الإرهاب السيبراني. وهناك نوعان من الإرهاب السيبراني وهما النقي و الهجين, فالنقي هو الذي ينطوي على هجوم مباشر على البنية التحتية الإلكترونية والشبكات الاجتماعية والمعلومات المخزنة فيها لأغراض سياسية واجتماعية, اما الهجين فهو عندما يتم استخدام الإنترنت لتجنيد ونشر وإشراك الآخرين في الأعمال الإرهابية, وكلا النوعين يشكلان تهديدًا خطيرًا ومصدر قلق كبير.

إن استخدام الإنترنت لتجنيد وتخطيط هجمات إرهابية حقيقية افرز عن كوارث ارهابية ادت الى أكبر عدد من الوفيات, وان أعظم نقاط القوة الإرهابية السيبرانية هي قدرتها على استخدام الإنترنت لترويج إيديولوجيتها ومتطلباتها التنظيمية, فخطر التهديد الإلكتروني خطير وتتغير طبيعته مع تقدم التكنولوجيا فلذا ارى انه لابد أن تواكب الهياكل البحثية والتدريبية والقانونية والجنائية وتيرة العالم

المتغير, ولانه وطالما ما بقيت الأسباب الجذرية للمشكلة ستتضاعف الفرص لتلك المنظمات فلابد من اتخاذ التدابير التي من شأنها تأمين الفضاء الرقمي تجاه الاخطار الإرهابية والعمل على ان تكون مخططاتها السيبرانية غير فعالة. وان الدول التي ليس لديها قوانين تجرم الهجمات السيبرانية ستستخدم كملاذ لمجرمي الإنترنت والإرهابيين عبره لذا لابد ان تلتزم جميع الدول بمنع وقمع وبكافة الوسائل القانونية أنشطة إعداد وتمويل أية أعمال إرهابية وتوفير التدابير القانونية لتطوير ومواءمة الآليات القانونية للحد من ذلك النوع الإرهابي السيبراني وكذلك زيادة فعالية التعاون عبر الحدود لمنع مثل ذلك السلوك أو التحقيق فيه.

وهنا نبادر ونقترح بوجوب إنشاء آلية تنظيمية وقانونية دولية وتعميمها لتحرم الإرهابيين السيبرانيين وتحافظ على أقصى قدر من السيطرة على الإنترنت من قبل الوكالات المتخصصة وهذه إن تمت فستكون خطوة هامة نحو تحقيق مفهوم المسؤولية الجماعية للدول لردع الإرهاب السيبراني وأنشطة المنظمات الإرهابية على الإنترنت كما وينبغي وضع واقرار وتوقيع قانون دولي ومعاهدة دولية لمكافحة الأنشطة الإرهابية على الإنترنت والمجال السيبراني وبالنظر إلى الطبيعة العالمية للإنترنت والطبيعة الفوضوية والخطيرة للإرهاب السيبراني فلا يمكن لنا وقف أنشطة المنظمات الإرهابية إلا إذا التزمت جميع الدول بالوفاء بذلك القانون والمعاهدة المقترحتين.