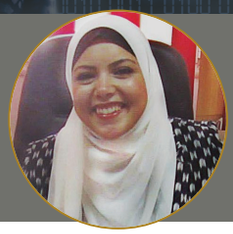
Dark Net

تهديدات "الشبكة السوداء" للأمن الافتراضي للدول



نوران شفيق

مدرس مساعد بقسم العلوم السياسية، كلية الاقتصاد والعلوم السياسية، جامعة القاهرة

أدت التحولات المتلاحقة في تكنولوجيا المعلومات والاتصالات إلى تصاعد تهديدات افتراضية غيرت من المفاهيم التقليدية للأمن بشكل يستوجب من الدول وغيرها من الفواعل وضع استراتيجيات حديثة تتلاءم معها.

أفرز انتقال العديد من التفاعلات سواء على مستوى الأفراد أو المجتمعات أو الدول إلى الفضاء الإلكتروني، وزيادة أعداد مستخدمي الإنترنت على مستوى العالم، آثاراً كبيرة على طبيعة التهديدات التي تُعنى الدول بالتصدي لها، خاصة مع صعود أنماط جديدة من الجرائم الإلكترونية، والإرهاب الافتراضي عبر استخدام أسلحة افتراضية نوعية، كالبرامج الخبيثة malwares وهجمات الحرمان من الخدمة DDOS وغيرها من الآليات.

وعلى عكس الأسلحة الإلكترونية التي تصمم خصيصاً لتنفيذ هجمات إلكترونية وحتى تكون مصدر تهديد للفاعل المستهدف، فإن تهديدات افتراضية أكثر حدة في تداعياتها على الأمن القومي للدول من دون أن يكون الهدف منه بالأساس الإضرار بأمنها، وفي هذا الصدد تعد الشبكة السوداء Dark Net- والتي تضم مجموعة من المواقع السرية على الإنترنت، من أبرز الأمثلة على ذلك. فليس كل ما هو موجود على الإنترنت يمكن رؤيته أو الوصول إليه من قبل المستخدمين، فجزء كبير من محتوياته يتسم بالسرية بحيث توفر الخصوصية لمستخدميها بعيداً عن أي نوع من الرقابة. وعلى الرغم من أن هذا النوع من الشبكات قد ظهر بالأساس لأهداف لا علاقة لها بالإضرار بأمن الدول، فإن تطور استخدامها قد حول العديد منها إلى مجتمعات افتراضية تمارس فيها العديد من الجرائم وتُستغل من قبل العديد من الجماعات الإرهابية بشكل يجعلها من أخطر التهديدات النابعة من الفضاء الإلكتروني في العالم المعاصر.

أولاً: التعريف بالشبكة السوداء

على الرغم من أن شبكة الإنترنت تقوم في الأصل على أساس الشفافية transparency، فإن ما نراه عليها لا يعبر بالضرورة عن كافة محتوياتها. فعلى سبيل المثال، عندما يقوم شخص بالبحث عن محتوى معين باستخدام محرك بحثي كجوجل Google، فهو يتمكن من الوصول إلى هذا المحتوى فقط إذا كان مدرجاً على هذا المحرك البحثي، وإذا كان مقدم خدمة الإنترنت Internet Service Provider (ISP) يسمح له بذلك. فلقد أظهرت الأبحاث أن 0.03 بالمئة فقط من محتويات الإنترنت يمكن البحث عنها والوصول إليها.

يضاف إلى ذلك أن ليس كل ما يراه المستخدم

على الإنترنت يتوافق مع إرادته الشخصية، ففي الكثير من الأوقات تتحكم في ذلك المصالح التجارية لشركات الإعلانات، إذ يتم توجيه الشخص إلى صفحات بعينها، وفي الكثير من الأحيان يتم إغلاق صفحات أخرى أمام المستخدمين تحقيقاً لهذه المصالح. ولكن لم تعد شركات الإعلانات ومقدمو خدمات الإنترنت وحدهم المتحكمون في ذلك، إذ ظهر ما يعرف بالشبكات السوداء والتي يتم فيها تقديم خدمات وتبادل معلومات بشكل سري بين أعضائها، ولا يمكن لأي مستخدم خارج الشبكة رؤية محتوياتها أو البحث عنها بالطرق التقليدية.

وتشير الشبكة السوداء - والتي يطلق عليها أيضاً Deep net أو Underground Internet - إلى المجتمعات المغلقة على الإنترنت التي يكون الدخول إليها مسموحاً فقط لأعضائها بشكل خاص، ويتم تشفيرها وتشفير المعاملات والأنشطة كافة التي تتم عليها بحيث يستحيل ترقبها. ويتم الدخول على الشبكة السوداء من خلال تحميل برنامج معين على جهاز الحاسب الآلي يمكن المستخدم من تبادل كلمات السر مع الأجهزة الأخرى المتصلة على الشبكة نفسها، ويتم نقل المعلومات بين هذه الأجهزة بشكل مشفر تماماً كالمعاملات البنكية الإلكترونية، وهو ما يجعل الشبكات السوداء أكثر أماناً عن الشبكات الداخلية Intranet التي تستخدمها الشركات والتي لا يتم فيها تشفير الاتصالات بين الأجهزة.

وعادة ما يحتاج المستخدم إلى توصية recommendation من شخص من داخل الشبكة حتى يتمكن من الدخول إليها. ومما يسهل من استخدام هذه الشبكات هو وجود البرامج الخاصة بها بلا مقابل على الإنترنت، ومن ثم يتمكن أي شخص من تحميلها واستخدامها. ومن بين هذه البرامج Free net و Invisible NET، ولكن البرنامج الأشهر والأكثر استخداماً هو برنامج TOR، الذي تموله الحكومتان الأمريكية والسويدية، والذي تم تطويره بالأساس من قبل معمل أبحاث البحرية الأمريكية US Naval Research Laboratory لحماية الاتصالات الحكومية، ولكن انتقل استخدامه فيما بعد إلى العامة.

ثانياً: تطور استخدام الشبكة السوداء

مع ظهور الإنترنت في الثمانينيات وتنميط بروتوكولات الإنترنت، بدأت إشكالية الحفاظ على سرية المعلومات المهمة بالظهور، ومع تطور استخدام الإنترنت في التسعينيات، انتشرت عمليات تبادل الأفلام والأغاني والبرامج الإلكترونية بشكل غير قانوني يضر بحقوق الملكية الفكرية من خلال ما يطلق عليه "تبادل النظراء" Peer-to-peer والذي يتم فيه حماية عمليات التبادل بكلمات سر لتشفيرها بحيث يتمكن فقط من هم جزء من الشبكة من الدخول إليها.

وفي مارس عام 2000، طور شخص يدعى إيان كلارك Ian Clarke برنامجاً جديداً يسمى بالشبكة الحرة Free Net، والذي يمكن مستخدميه من الدخول على أي محتوى من محتويات الإنترنت بشكل سري. وفي سبتمبر 2002، ظهر لأول مرة برنامج TOR أو الذي يطلق عليه أيضاً the onion router، ومن خلاله يتم تشفير مكان وعنوان بروتكول الإنترنت للمستخدمين الذين يقومون بتحميل البرنامج، وكان الهدف الرئيسي من تطويره هو حماية هوية العاملين بمعمل أبحاث البحرية والأجهزة الحكومية في الولايات المتحدة.

ومع حلول عام 2005، أصبحت هناك خطورة كبيرة على الملكية الفكرية للأفلام والأغاني والبرامج وغيرها من المحتويات التي أصبح يتم تداولها من خلال الشبكات السوداء، وخرجت تقارير ودراسات تؤكد أن الخسائر التجارية من هذه العمليات تصل إلى 34 مليار دولار على مستوى العالم.

تُعرف الشبكة السوداء على أنها المجتمعات المغلقة على الإنترنت التي يكون الدخول إليها مسموحاً فقط لأعضائها بشكل خاص، ويتم تشفيرها وتشفير كافة المعاملات والأنشطة التي تتم عليها، بحيث يستحيل ترقبها على غرار المعاملات البنكية الإلكترونية، ويتم الدخول إليها من خلال تحميل برنامج معين على جهاز الحاسب الآلي لتبادل كلمات السر مع الأجهزة الأخرى المتصلة على الشبكة نفسها، وعادة ما يحتاج المشتركون الجدد لتوصية من أعضاء الشبكة لاستخدمها.

تصاعدت حدة تهديدات الشبكات السوداء في يناير 2009، حينما طور ساتوشي ناكاموتو Satoshi Nakamoto عملة إلكترونية أطلق عليها Bitcoin والتي كانت بمنزلة ثورة في عالم الشبكات السرية، إذ يتم استخدامها في عمليات الشراء والبيع على الشبكة السوداء حتى يتحقق قدر أكبر من السرية للمستخدمين، مما أوجد منفذاً خلفياً في النظام المالي العالمي لعمليات غسيل الأموال والأنشطة الإجرامية عبر المجال الافتراضي.

وفي عام 2010، أعلنت شركة الأمن الإلكتروني والمخابرات بروسايزف Procysive أن الشبكة السوداء أضحت تضم أكثر من 50 ألف موقع إلكتروني للفكر المتطرف، وأكثر من 300 منتدى افتراضي للجماعات الإرهابية، وأصبح البيع غير المشروع للبرامج المسروقة هو السبيل لتمويل هذه الأنشطة الإرهابية، ففي 2011 ظهر موقع جديد على الشبكة السوداء يعرف بطريق الحرير Silk Road، والذي سهل من عمليات بيع وشراء المخدرات بدرجة تُماثل عمليات التجارة الإلكترونية على مواقع كأمازون دوت كوم. وفي أغسطس 2013، بدأت السلطات الأمريكية تدرك خطورة الشبكة السوداء بعد أن تم الكشف عن محادثة سرية بين أيمن الظواهري زعيم تنظيم القاعدة وناصر الوحيشي زعيم القاعدة في جزيرة العرب، والتي تم فيها الاتفاق على مهاجمة السفارات الأمريكية في أكثر من 21 دولة، إذ تمت هذه المحادثة باستخدام الشبكة السوداء.

وبعد أن كان موقع Silk road يحقق حوالي 1.2 مليار دولار في الفترة ما بين 2011 و2013، قام مكتب التحقيقات

الفيدرالي FBI بإغلاقه والقبض على مؤسسه، وبدأت بعدها "وكالة الأمن القومي الأمريكية" NSA محاولة استغلال نقاط الضعف في بعض أجهزة مستخدمي TOR للكشف عن هويتهم الحقيقية. ثم ظهرت مواقع أخرى بعدها يطلق عليها Black Market Reloaded وDeep bay والتي تتضمن أنشطة مماثلة لموقع Silk road إلى أن ظهر موقع Silk Road 2.0 من جديد في نوفمبر 2013 بعد إغلاق الموقع الأصلي بحوالي شهر.

ويتضح مما سبق كيف أن الشبكة السوداء والبرامج الخاصة بها لم تكن تهدف في الأساس إلى تسهيل العمليات الإجرامية، ولكن يتطور استخدامها من مجرد أداة تتم من خلالها مشاركة البيانات ما بين الأفراد بشكل مشروع إلى مساحة تمارس فيها أنشطة إجرامية تضر بأمن المجتمعات.

ثالثاً: دوافع وتهديدات استخدام الشبكة السوداء

ليست كل استخدامات الشبكة السوداء استخدامات إجرامية بالضرورة، إذ ترتب على السرية التي تحققها الشبكة السوداء تعدد استخداماتها بحيث باتت تشمل ما يلي:

1- ممارسة النشاط السياسي political activism بعيداً عن رقابة الحكومات في الدول ذات الأنظمة السلطوية أو تلك التي تفرض قيوداً على حرية الرأي أو تحظر دخول المواطنين على مواقع معينة. ولذا، يكثر اللجوء إلى الشبكة السوداء في إيران، وروسيا، والصين، حيث تفرض الحكومات رقابة صارمة على الإنترنت تحول دون قدرة المواطنين الدخول إلى العديد من المواقع، أو التعبير عن الآراء السياسية بحرية كاملة. ففي دولة كالصين، على سبيل المثال، هناك ما يعرف ب"الجدار الناري العظيم" Great Firewall وهو مشروع طورته أجهزة الأمن الصينية، وتقوم من خلاله بالرقابة على أنشطة المواطنين كافة على الإنترنت، والحيلولة دون وصولهم إلى مواقع أو معلومات معينة.

2- توفر الشبكات السوداء أيضاً الخصوصية للمستخدمين ممن لا يريدون أن يتم تعقبهم من قبل الشركات المقدمة لخدمة الإنترنت ISP أو حتى لا يتم تخزين بياناتهم من قبل شركات الإعلانات. فلكل جهاز حاسب آلي على الإنترنت رقم خاص به يسمى عنوان بروتكول الإنترنت IP address يمكن من خلاله تحديد مكان الجهاز، ورصد أنشطته. ولذا، لتحقيق الخصوصية، تقوم برامج الشبكة السوداء بإخفاء رقم بروتكول الإنترنت بحيث يستحيل تعقب أنشطة المستخدم.

3- قد تلجأ أيضاً الشركات الكبرى إلى هذا النوع من الشبكات عند تبادل المعلومات المهمة مع شركائها في الخارج. وتلجأ إليها أيضاً بعض المؤسسات الحكومية، خاصة العسكرية والأمنية، حتى تجري اتصالاتها بشكل سري، وحتى تتمكن من الدخول إلى أي موقع من دون أن تترك أثراً لعنوان بروتكول إنترنت تابع لجهاز حاسب آلي حكومي.

ولكن إلى جانب هذه الاستخدامات الإيجابية، تظهر أنماط أخرى لاستخدام الشبكة السوداء تهدد أمن الدول وتفرض نفسها كأحد أبرز التحديات الأمنية التي تواجهها الحكومات في العالم المعاصر. إذ تُستغل السرية التي تمنحها تلك الشبكات لمستخدميها من قبل المجموعات الإجرامية والإرهابية على مستوى العالم لممارسة أنشطتها بشكل سري بعيداً عن الملاحقة الحكومية. فمن خلال الشبكة السوداء، تتمكن هذه الجماعات من العمل في تجارة السلاح، والمخدرات، واستقطاب عناصر للعمل في الجماعات الإرهابية، وتدريبهم، ونشر الدعاية التي تخدم مصالحهم، وتبادل المعلومات والاتصالات بين أعضاء الجماعة، مستغلة في ذلك سرية هذه الشبكات وعالمية استخدامها.

تُستغل السرية التي تمنحها الشبكة السوداء من قبل المجموعات الإجرامية والإرهابية على مستوى العالم لممارسة أنشطتها بشكل سري بعيداً عن الملاحقة الحكومية. وتتزايد معدلات تجارة السلاح، والمخدرات، واستقطاب وتدريب كوادر للجماعات الإرهابية، وتدريبهم، ونشر الدعاية، وتبادل المعلومات والاتصالات ما بين خلايا تلك التنظيمات على مستوى العالم، كما يتم استغلال تلك الشبكات في عمليات تزوير المستندات الحكومية، وبطاقات ائتمان، إلى جانب الترويج لخدمات القتلة المحترفين، وقراصنة الإنترنت.

ليس ذلك فحسب، بل هناك مواقع على هذه الشبكات تعرض تزوير مستندات من بطاقات هوية، وجوازات سفر، وبطاقات ائتمان، ومستندات حكومية وغيرها، إلى جانب عرض خدمات القتلة المحترفين، وقراصنة الإنترنت، بحيث يقوم أي مستخدم على الشبكة بالتواصل معهم للحصول على هذه الخدمات في سرية تامة من دون أن يتعرض أي من الطرفين لأي نوع من الرقابة الحكومية.

وفي هذا الإطار، أظهرت إحدى الدراسات أن تكلفة التزوير الإلكتروني الذي يعتمد على الشبكات السوداء يكلف الاقتصاد البريطاني عشرات المليارات سنوياً، كما أعلنت الشركة الروسية للأمن الإلكتروني Kaspersky أن الشبكات السوداء قد أفرزت نوعاً جديداً من البرامج الخبيثة يطلق عليه Ransom Ware، أصبح يعتمد على برنامج TOR حتى يتمكن المهاجمون من إخفاء هويتهم. هذا النوع من البرامج الخبيثة يتم من خلاله السيطرة على الحاسب الآلي وإغلاق نظام التشغيل الخاص به، وإجبار المستخدم على دفع فدية حتى يعود جهازه للعمل من جديد. ولقد زادت خطورة هذه البرامج إلى الحد الذي باتت فيه تهدد الأجهزة الحكومية ذاتها. إذ أصيب جهاز الشرطة في ولاية ماساتشوستس الأمريكية العام الماضي بأحد هذه البرامج والذي أطلق عليه Cryptolocker واضطروا إلى دفع 1338 دولاراً كفدية حتى يتخلصوا من هذا البرنامج.

وكما ذكرنا من قبل، كان موقعSilk Road هو أكبر موقع لتجارة المخدرات على الشبكة السوداء. بالإضافة لتقديم خدمات قتلة ومزورين وقراصنة إنترنت، ويعتبر هذا الموقع هو الأكثر تعقيداً والأكثر استخداماً من بين كافة الأسواق الإجرامية الموجودة على الشبكة السوداء. ولقد أعلن مكتب التحقيقات الفيدرالي في الولايات المتحدة أن الموقع قد حقق منذ إنشائه عمولات تقدر بحوالي 80 مليار دولار. وبعد إغلاقه، تمكنت الأجهزة الأمريكية من التوصل إلى تجار مخدرات من مستخدمي الموقع من الولايات المتحدة، وبريطانيا، وأستراليا، والسويد. ولكن لم تعلن الولايات المتحدة عن كيفية قيامها باختراق الموقع والقبض على مؤسسه ومديره روس وليام أولبريشت Ross William Ulbricht.

وبعد أن تخيل البعض أن هذه بداية النهاية لمثل هذه المواقع، وأن تمكن الأجهزة الأمنية الأمريكية من اختراقها، هو دليل على استحالة ضمان استمرار سريتها، عاد موقع Silk Road 2.0 بعد شهر من إغلاق الموقع السابق ليثبت أن هذه المواقع ستظل تهدد أمن المجتمعات، وأن محاربتها صارت من الصعوبة بمكان بحيث يستحيل القضاء عليها نهائياً.

وعلى الرغم من التشابه بين موقع Silk Road 2.0 والموقع القديم، فإنه يستخدم كلمات سر إضافية في كل الأنشطة التي تتم عليه بحيث يحقق قدراً أكبر من السرية لمستخدميه. وبعد أسبوع واحد من إطلاقه، تضمن الموقع أكثر من 500 قائمة من المخدرات، وأصبح يتولى إدارتها شخص جديد بعد القبض على روس أولبريشت.

والأكثر من ذلك، أن إغلاق موقع Silk Road، أدى لظهور مواقع متعددة تحاول أن تحل محله والقيام بالعمليات نفسها التي كانت تتم عليه. ومن ثم، أصبحت المواقع الإجرامية على الشبكة السوداء تتسم باللامركزية مما يصعب من مواجهتها في اجتذابها لقطاعات واسعة من مستخدمي الإنترنت.

رابعاً: إشكاليات مواجهة الشبكة السوداء على الانترنت

تتجه الآن العديد من دول العالم للتصدي إلى المواقع الموجودة على الشبكة السوداء ومحاولة الكشف عن مستخدميها، حيث قامت بعض الدول بتطوير برامج خبيثة تتم من خلالها مهاجمة أجهزة الحاسب الآلي لعدد كبير من الأفراد للتوصل إلى مستخدمي برنامج TOR والكشف عن هويتهم، وهو الأسلوب نفسه الذي اتبعته أيرلندا في 2013 للقبض على إريك أوين ماركيز Eric Eoin Marques الذي كان يدير شبكة سوداء كبيرة تدعى Freedom hosting. كما أعلنت روسيا أيضاً عن جائزة 4 ملايين روبل لمن يستطيع اختراق مواقع الشبكة السوداء.

ولكن كما أوضحنا من قبل، وكما أظهرت حالة Silk Road، ليس من السهل محاربة هذا النوع من الشبكات، والتصدي لانتشار استخدامها، والحد من الأنشطة الإجرامية التي تمارس من خلالها. كما أن هناك العديد من الأصوات التي تقف أمام محاربة برنامج TOR والبرامج المثيلة له، نظراً لاستخدامهم كآليات للتعبير عن الرأي في الأنظمة القمعية وحماية خصوصية المواطنين في مواجهة الرقابة الحكومية.

يضاف إلى ذلك، أن التطور في استخدام الشبكات السوداء والمواقع والتطبيقات المنبثقة عنها من الممكن أن يحدث تغييرات جذرية في النظام العالمي وفواعله. فمع التقليل من أهمية العملات الرسمية المتداولة وتصاعد استخدام العملات الرقمية Bitcoin في هذه المجتمعات الافتراضية، سوف يواجه النظام الاقتصادي العالمي إشكالية تآكل الثقة في التعاملات المالية، مما قد يتسبب في أزمات اقتصادية على المستوى العالمي، في مقابل تزايد نفوذ أصحاب ومديري هذه الشبكات الافتراضية وتراكم ثرواتهم بطريقة غير مشروعة. كما أن هذه الشبكات من الممكن أن تحتكر مستقبلاً خدمات الاتصالات في الفضاء الإلكتروني بشكل يؤثر على سيادة الدول ويفقدها السيطرة على التفاعلات عبر المجال الافتراضي.

1- Hal Hasdon, “Web of Darkness”, **New Scientist**, Vol. 221, Issue 2961(March 2014).

2- Terry Allen, “The Underground Internet”, **Business Week**, (September 15, 2003). pp80-82

3- Scaachi Koul, “The dark side of the Internet”, **Maclean's**, Vol. 125, Issue 41.

4- Ty McCormick, “The Darknet: A short History”, **Foreign Policy** (December 9, 2013) URL: http://goo.gl/oNmY0k. Accessed on October 10, 2014.

5- Kim-Kwang Raymond Choo, “Organized Crime Groups in Cyberspace: a Typology”, **Trends in Organized Crime**, Volume 11, Issue 3 (September, 2008), pp 270-295. p282

6- Donna Leinwand Leger, “How The FBI Brought Down Silk Road”, **USA Today**, (May 15, 2014). URL: http://goo.gl/F15nV1/. Accessed on October 9, 2014.

7- Terry Allen, **Op.cit.**

8- Donna Leinwand Leger, **Op.cit.**

9- Kim-Kwang Raymond Choo, **Op.cit.**

10- Jake Wallis Simons. Guns, “Drugs and Freedom: the Great Dark Net Debate”, **Telegraph**, (September 17, 2014). URL: http://goo.gl/Y8XQpq. Accessed on: October 11, 2014.

11- Donna Leinwand Leger, **Op.cit.**

12- Andy Greenberg, “Silk Road 2.0' Launches, Promising A Resurrected Black Market For The Dark Web”, (June 11, 2013). URL: http://goo.gl/HCmoH6/. Accessed on October 13, 2014.

13- Jake Wallis Simons, **Op.cit**.

14- Geoffrey L. Herrera, “**Dreams of Anarchy: Darknets**, Digital Money, and the Quest for a Post Hierarchical World Order”, (Paper prepared for the **Millennium Annual Conference**, London, UK, October 20, 2012). URL: http://goo.gl/MEURcS, p4. Accessed on October 13,2014.