تزايد نمو الأنشطة غير القانونية عبر «الشبكة المظلمة» بسبب «كورونا»

أدى إغلاق الأسواق عقب تفشي «كوفيد 19» حول العالم إلى تزايد نمو الأنشطة غير القانونية على الشبكة المظلمة خصوصاً مع ارتفاع عمليات الرقمنة وانتشار الإنترنت بشكل كبير عقب الجائحة ، فيما تقوم قوى الأمن في جميع دول العالم بتعزيز هجومها على المجرمين الذين يرتعون في مواقع هذه الشبكة. التي تُعدّ متنفساً للأنشطة غير القانونية وللممارسات التي يمكنها إلحاق الضرر بالأفراد، والشركات والمشروعات التجارية

4 تريليونات دولار
عمليات غسيل الأموال عبر الشبكة المظلمة سنوياً تمثل 5 % من الناتج العالمي

1 مليار دولار
حجم التعاملات بعملة البيتكوين على الشبكة المظلمة نهاية 2019

400 ألف
عدد مواقع الشبكة المظلمة

900 مليار دولار
تعاملات غير شرعية سنوياً

البيان
المصدر:صندوق النقد الدولي - شركة تاليس للأمن الالكتروني

إعداد: وائل اللبابيدي - غرافيك: حسام الحوراني

«البيان» تُبحر عبر مستويات الإنترنت السطحية والعميقة والمظلمة

أدّد خبراء في الأمن السيبراني ضرورة تعاون حكومات العالم، للحّد من الأنشطة الإجرامية، التي تتم عبر الشبكة المظلمة Dark Web، التي باتت تشكّل نظاماً اقتصادياً موازياً غير شرعي، وأن استمرارها قد يؤدي إلى عواقب وخيمة على الاقتصاد العالمي في المستقبل المنظور، محذرين من تزايد حجم التعاملات المالية، التي تتم بواسطة العملات الرقمية، وعلى رأسها «بيتكوين»، والتي تقدر سنوياً بأكثر من 900 مليار دولار بعد أزمة «كوفيد 19». وتتألف شبكة الإنترنت من ثلاثة مستويات هي السطحية، وتشكل جزءاً لا يتجاوز 5%، بالإضافة إلى الشبكتين العميقة والمظلمة، التي تمثل 95% من المواقع التي تتضمنها الشبكة العنكبوتية. وتعتبر الشبكة المظلمة مرتعاً لعمليات إجرامية. تشمل الاتجار بالبشر وتجارة المخدرات والأسلحة وغيرها من الجرائم. وأضاف الخبراء: «البيان الاقتصادي» أن مستخدمي الشبكة العميقة، التي لا يمكن الوصول إليها عبر الشبكة العادية ارتفع عالمياً إلى أكثر من 10 ملايين مستخدم يومياً خصوصاً بعد إجراءات الحظر، التي تزامنت مع انتشار جائحة كورونا، محذرين من أن دخول هذه الشبكة، الذي يتم عبر شبكة TOR باستخدام الشبكات الخاصة الافتراضية VPN، بهدف الوصول إلى محتويات أو منتجات أو خدمات غير قانونية هو أمر يعاقب عليه القانون في معظم الدول، ومنها الإمارات التي تجيز الاستخدام القانوني والعادي للشبكات الخاصة الافتراضية «VPN» من قبل الشركات، ولكنها تعاقب المستخدم بالسجن والغرامة في حال القيام بأي أنشطة محظورة في الشبكة المظلمة.

أشار خبراء في الأمن السيبراني إلى أن عملية DisruptTor التي أدت إلى اعتقال 179 شخصاً في أوروبا وأمريكا مرتبطين بأنشطة غير قانونية على الشبكة المظلمة مؤخراً تشير إلى أن «الشبكة المظلمة» لم تعد ملاذاً آمناً للمجرمين، وتُظهر أن الوسائل والحيل التي يستخدمها مجرمو الإنترنت لحجب هويتهم لم يعد فعالاً، وأن تكتيكات تنفيذ القانون قد تغيرت لمواجهة التهديد بشكل أسرع وإغلاق جميع العمليات السرية، لافتين إلى أن قوانين الإمارات فعالة في مكافحة جرائم الشبكة المظلمة.وشدّد الخبراء على ضرورة تجنب الدخول لمواقع الشبكة المظلمة، والتي تعتبر مرتعاً للمجرمين الخطيرين، وذلك لتجنب التعرض للفيروسات المختلفة والاحتيال والاختراق وسرقة البيانات والهوية والمسائلة القانونية خصوصاً أن السلطات لديها فرق خاصة اليوم قادرة على تحديد هويات المتعاملين مع تلك الشبكة، التي لا يمكن الولوج إليها عبر محركات البحث الاعتيادية.


جايمي كولير


مورغان رايت

وتحاول حكومات عدة حول العالم تحديد هوية مستخدمي هذه الشبكة من خلال تقنيات الهاكرز، في حين تصنّف وكالة الأمن القومي الأمريكية أي شخص يقول إنه قادر على الوصول إلى الشبكة المظلمة على أنه «متطرف».

مجتمع إجرامي

وقال د. جايمي كولير، محلل الاستخبارات السيبرانية لدى «مانديانت» لاستخبارات التهديدات السيبرانية: إن عملية المداهمات التي أدت إلى اعتقال 179 شخصاً مرتبطين ببيع المخدرات على الشبكة المظلمة الأسبوع الماضي كشفت كيفية قيام شبكات الويب المظلم بتسهيل بيع المخدرات والأسلحة، بالإضافة وجود مجتمع إجرامي كبير يلعب دوراً أوسع منتشراً في خفايا شبكات «تور» مكون من الهاكرز، الذين يقومون بتجارة البرامج الضارة، والبيانات المسروقة، وبيانات الوصول لشبكات الضحايا المعرضة للخطر. وأضاف: «بناء الثقة هو أولوية قصوى داخل هذه المجتمعات المجهولة الهوية، في حين أن هذه الأسواق لا تتضمن أسماء أو وجوهاً حقيقية، فلا يزال بإمكان الأفراد بناء سمعتهم من خلال أسماء مستعارة، والحصول على تقييمات مبيعات إيجابية، والمشاركة في أنظمة ضمان الدفع الموثوقة».

تعاون دوليوأشار كولير إلى أن النظام الإجرامي المظلم عابر للحدود، ومن الضرورة اتباع نهج دولي لتنفيذ القانون، فليس من المستغرب أن تأتي العديد من حملات اعتقالات، والتي تستهدف شبكات الويب المظلم على خلفية التعاون الدولي بين وكالات تنفيذ القانون في جميع أنحاء العالم. ومن المؤكد أن حجم الاعتقالات الأخيرة في العديد من البلدان سيعطل العمليات الإجرامية.وأضاف: «مع ذلك أثبتت أسواق الويب المظلمة مرونة ملحوظة، حيث كانت المكافآت المالية المرتبطة بالسلع والخدمات غير المشروعة تصل في النهاية إلى حوافز مادية، من أجل استئناف النشاط وبلوغه مراكز مرتفعة. وإحدى النتائج المحتملة هي أن المجرمين سينتقلون إلى أسواق أكثر انغلاقاً تقتصر على مجتمع أصغر موثوق به من المشترين والبائعين، وخفة الحركة في هذه الأسواق تشكل تحدياً لأولئك الذين يسعون إلى مواكبة سرعات التهديدات السيبرانية».


يوسف البحر


رشيد العمري

وقال رشيد العمري، الخبير الاستراتيجي الأول لحلول الأعمال في «في إم وير»: «تتوفر على الإنترنت العادي رقابة من الشركات المطورة لمتصفحات الإنترنت، وذلك لضمان عدم وجود محتويات غير مناسبة أو لا أخلاقية، أما الإنترنت المظلم فلا رقابة عليه من هذه الشركات، ولذلك يلجأ إليه من يقومون بعمليات لا أخلاقية على الإنترنت مثل تجارة المخدرات أو الأنشطة المرتبطة بالاغتصاب والتعذيب والدعارة». ولفت إلى أن اعتقال المجرمين على الإنترنت يتم عبر توظيف الأجهزة الأمنية مثل المخابرات الأجنبية والأجهزة الأمنية في الدول المختلفة عناصر لمراقبة الإنترنت المظلم، وملاحقة الأشخاص المتورطين بأنشطة إجرامية فيه للوصول إليهم عبر تحديد عناوينهم على الإنترنت (IP Address)، ومن ثم التعرّف على هوياتهم الحقيقية لإلقاء القبض عليهم وحماية المجتمعات من أنشطتهم الإجرامية. قال مورغان رايت، كبير مستشاري الأمن لدى شركة «سنتينل وان» إنه في عام 2011 ظهرت منصة مظلمة تسمى طريق الحرير وهي أول سوق ويب مظلم، يتم من خلاله بيع الأدوية والوثائق المزورة والأسلحة والمخدرات، موضحاً أن عمليات الدفع تتم بواسطة عملة «بيتكوين» وغيرها، حيث كان طريق الحرير غير خاضع للرقابة، وكان من المستحيل تقريباً تتبعه في ذلك الوقت، حيث نشطت لمدة عامين تقريباً قبل أن تتولى مصلحة الضرائب الأمريكية (IRS) متابعتها وحل القضية.

تحديات الشبكة

وتابع:"تعود تحديات وصعوبات إيقاف الشبكة المظلمة إلى أسباب مختلفة منها أن مستخدمي الشبكة لديهم برامج تُخفي هوياتهم وتُبقيهم مجهولين، كما يتطلب إيقاف تلك الشبكة أموالاً طائلة ووقتاً طويلاً، وموارد ضخمة. وينصح خبراء المعلوماتية المستخدمين بعدم دخول هذا العالم المظلم والمليء بالجرائم، لما قد يسبّب لهم مخاطر الانجرار والتورّط بقضايا، ونتائج لا تحمد عقباها، كما أن التدريب على أساليب ومبادئ الأمن السيبراني هو الوسيلة الأفضل لمساعدة الشركات والأفراد على مكافحة عالم الإنترنت المظلم، بالإضافة إلى تنزيل أحدث برامج الحماية لأجهزة الكمبيوتر، وتبليغ السلطات الأمنية الرسمية والتشاور مع إدارات مكافحة الجرائم الإلكترونية، في حالات سرقة البيانات الشخصية أو الهويات أو المعلومات".

عقوبات قانونية

قال المحامي يوسف البحر: إن الدخول إلى موقع إلكتروني دون تصريح عقوبته الحبس وغرامة لا تزيد على 300 ألف درهم أو إحداهما، مؤكداً أهمية تجنب الدخول إلى المواقع الإلكترونية مجهولة المصدر والهوية، وذلك حماية للشخص ذاته وأفراد أسرته، والحفاظ على معلوماته الشخصية كونها قد تؤدي في الوصول إلى بياناته السرية أو المالية.وأضاف: «أحياناً يتم استخدام تطبيقات VPN للتحايل على العناوين البروتوكولية المعتمدة للمواقع الإلكترونية، وهو ما ينطلي عليه مخاطرة تؤدي إلى نتيجة عكسية على المستخدم، وهنا ينبع الدور الأساسي لما يعرف بالشبكة العنكبوتية النظيفة، التي تكون واضحة المعالم ومعرفة الهوية والمصدر».

وأضاف أن المرسوم رقم 5 لسنة 2012 من قانون مكافحة جرائم تقنية المعلومات يعاقب المستخدم في حال الدخول إلى العنوان البروتوكولي للمواقع دون تصريح، سواء عبر استخدام الشبكة المظلمة أو تطبيقات VPN غير المسموحة.

100 ألف درهم

وأفاد: «ينص القانون صراحة على أنه: يعاقب بالحبس والغرامة التي لا تقل عن 100 ألف درهم ولا تزيد على 300 ألف درهم أو بإحدى هاتين العقوبتين كل من دخل موقعاً إلكترونياً أو نظام معلومات إلكترونياً أو شبكة معلوماتية، أو وسيلة تقنية معلومات، بدون تصريح أو بتجاوز حدود التصريح، أو بالبقاء فيه بصورة غير مشروعة. أما إذا استغل المستخدم الوصول إلى الموقع الإلكتروني في ارتكاب جريمة كالاحتيال أو إتلاف أو إحداث تعديلات أو التعدي على خصوصية الآخرين، فهناك عقوبات مشددة تصل إلى السجن وغرامات مالية حسب كل جرم».وبنص المرسوم أنه «يعاقب بالسجن المؤقت والغرامة التي لا تقل عن 500 ألف درهم، ولا تتجاوز مليوني درهم أو بإحدى هاتين العقوبتين كل من تحايل على العنوان البروتوكولي للشبكة المعلوماتية باستخدام عنوان وهمي أو عنوان عائد للغير أو بأي وسيلة أخرى».وقال: «هدف من يستخدم VPN للدخول إلى متصفح (تور) وغيره من متصفحات الشبكات المظلمة هو الابتعاد عن الاستخدام النظيف للشبكة العنكبوتية تجنباً للمتابعة القانونية، لذلك ظهر مؤخراً ما يعرف بالجريمة السيبرانية أو الجريمة الإلكترونية، التي تستغل الشبكات العنكبوتية. ويتم الدخول إلى الشبكة المظلمة لمحاولة تنفيذ جرائم الاحتيال والهادفة إلى الاستيلاء على أموال الناس وهذه الجريمة عقوبتها مشددة تصل للحبس مدة لا تقل عن سنة واحدة والغرامة التي لا تقل عن مائتين وخمسين ألف درهم، ولا تجاوز مليون درهم أو بإحدى هاتين العقوبتين.

توعية الأبناء

وأضاف:«هناك جرائم عالمية تستهدف الأطفال والشباب والفتيات عبر الاعتداء على الخصوصية والتهديد والابتزاز وغيرها، وهو ما يتطلب منا ضرورة التوعية المستمرة، ويجب عدم استخدام أي موقع غير موثوق وتجنب استخدام VPN إلا في الحالات المسموحة وعدم مشاركة أي بيانات شخصية ومالية مع أي كان على مواقع الشبكة العنكبوتية والتطبيقات، إلى جانب ضرورة توعية الأبناء بعدم استخدام هذه التقنيات وعدم استخدامها».

5%
الشبكة السطحية: جوجل، ياهو، ويكيبيديا، منصات التواصل الاجتماعي المختلفة

95%
الشبكة العميقة
تشمل بيانات ضخمة وبراءات اختراع ومقالات ووثائق قانونية ومالية.

الشبكة المظلمة
تتضمن مواقع «تور» وأنشطة غير شرعية وأسواق خفية وصحافة مجهولة.

38%
ذكر تقرير حديث لشركة «أطلس في بي إن» أن واحداً من كل أربعة أو حوالي 38% من سكان الإمارات قاموا بتحميل أحد برامج الشبكات الخاصة الافتراضية VPN خلال النصف الأول من 2020، من ضمنها الشركات التي تستخدمها ذات الوجود المحلي التي تستخدم هذه الشبكات بشكل قانوني بهدف تشفير البيانات الحساسة العابرة بين الدول. ولا يعتبر استخدام شبكات VPN في الإمارات عملاً غير قانوني في حال استخدم وفقاً للضوابط الحكومية والجهات المختصة. وأفادت هيئة تنظيم الاتصالات في تصريح سابق لها لـ«البيان» أن استخدام تقنية الـVPN غير ممنوع، إنما إساءة استخدامها تستدعي المساءلة والعقوبة. ويقول متحدث رسمي باسم الهيئة إن تقنية VPN بالنسبة لعمل الشركات في الدولة تلعب دوراً مهماً في تأمين أمن شبكات الاتصال الخاصة بالشركات بشكل عام عن طريق تشفير حركة الحزم بينها، مضيفاً أنه لا توجد أي تغييرات بما يخص الوضع الحالي لتقنيات الشبكات الخاصة الافتراضية. كما لا يوجد ما يمنع الاستخدامات الشرعية للشبكات الخاصة الافتراضية VPN، وأن القوانين الحالية الخاصة بذلك تغطي إساءة استخدام شبكة الإنترنت.

وحول خطط الهيئة بخصوص منع الوصول إلى «الشبكة المظلمة» أوضح: «تعمل الهيئة بشكل دائم بالتعاون مع المرخص لهم على توفير بيئة إلكترونية آمنة لمستخدمي الإنترنت في الدولة بشكل عام وتقليل فرص تعرضهم لمخاطر الشبكة العنكبوتية. حيث يتم حجب المواقع الإلكترونية والأنظمة التي تعرض المستخدمين للخطر».

3
يتألف الإنترنت من 3 شبكات هي الشبكة العميقة من مواقع الإنترنت غير المفهرسة في محركات البحث التقليدية الشهيرة مثل «جوجل» والشبكة المظلمة، وهي تشكل جزءاً كبيراً من الشبكة العميقة، ولكنها تتميّز بأن إخفاءها عن مواقع البحث جرى بشكل مُتَعَمّد، وغالباً بهدف القيام بنشاطات إجرامية. وتشترك الشبكة العميقة والمظلمة في أن الوصول إليهما يحتاج متصفحاً خاصاً ومجهولاً، أي لا يُمكن تتبعه، يُسَمّى «تور»، وهي تسمية إنجليزية مختصرة لمصطلح يشير إلى برنامج للتخفي يستخدم الاتصال المُشَفّر بالإنترنت، من دون الكشف عن هوية الشبكة المُستَخدِمَة في الاتصال.

«الشبكة المظلمة».. قاعدة انطلاق الهجمات الخبيثة

أكد خبراء في الإمارات أن «الشبكة المظلمة» تشكّل القاعدة الرئيسة لانطلاق الهجمات الخبيثة وحجب الخدمة الموزعة DDoS التي باتت تكبد الشركات عالمياً الملايين من الدولارات سنوياً، بدءاً من شراء بيانات الضحايا لاستغلالهم وحتى اقتناص الفدية، مشيرين إلى أن السلطات المختصة في الدولة تجيز الاستخدام القانوني والعادي للشبكات الخاصة الافتراضية «VPN» من قبل الشركات، ولكنها تمنع استخدام تلك الشبكات الخاصة لغرض الحد من ارتكاب الجرائم والوصول إلى المعلومات المحظورة وغيرها من الأنشطة الخبيثة.

توصيات البيان

01 توعية المستخدمين بخطورة الشبكة المظلمة
02 تعاون دولي والتدريب على أساليب الأمن السيبراني
03 استمرار الحملات الأمنية لردع المجرمين
04 رقابة مستمرة من الشركات والجهات الحكومية المعنية
05 تجنب استخدام VPN إلا في الحالات المسموحة
06 تنزيل أحدث برامج الحماية لأجهزة الكمبيوتر
07 تبليغ السلطات فوراً في حالة سرقة البيانات أو الهويات
08 تطبيق حلول أمنية مؤتمتة وموحدة برؤية واضحة
09 تغليظ العقوبات القانونية المادية والمعنوية
10 عدم استخدام أي موقع غير موثوق

بالأرقام

69
أفادت نتائج دراسة أجرتها شركة «هايبريون جراي» متعددة الجنسية والمتخصصة في خدمات الأمن الإلكتروني في عام 2018، بأن برنامج «تور» يستضيف أكثر من 65.000 مُحدد مُوَحّد للموارد «URL» - وهو ذلك الجزء من عنوان الإنترنت المُستَخدم في تحديد الموقع المطلوب دخوله - تنتهي بالجزء «onion».

10%
تضمنت دراسة شركة «هايبريون جراي» فهرساً لحوالي 10% من مُحَدِدَات «URL»، حيث تَبين أن الوظيفة أكثر شيوعاً لها هي تسهيل الاتصال عبر المنتديات، غرف الدردشة، الاحتفاظ بملفات وصور لمستضيفي الشبكة، وتيسير التجارة وتدعم هذه الوظائف استخدامات عديدة تعتبرها المجتمعات حرة قانونية ومشروعة.

400
وفقاً لبيانات دراسة أجرتها شركة «تربيوم لابز» المتخصصة في أبحاث الإنترنت على عينة عشوائية من 400 موقع تنتهي بالجزء «onion»، تبين أن أكثر من نصف نطاقات الإنترنت العميق هي في واقع الأمر قانونية.

20%
كشفت دراسة د. مايكل ماكوادر، من جامعة «سري» البريطانية في عام 2019 ارتفاع بنسبة 20% في عدد مواقع الشبكة المظلمة التي يمكنها الإضرار بالشركات والأفراد، كما رصد الباحثان دانييل مور وتوماس ريد من جامعة «كينجز كوليدج» خلال عام 2015 ، 2723 موقعاً نشطاً في غضون 5 أسابيع تعمل ضمن نطاق الإنترنت العميق، 57% منها تستضيف محتويات محظورة قانوناً.

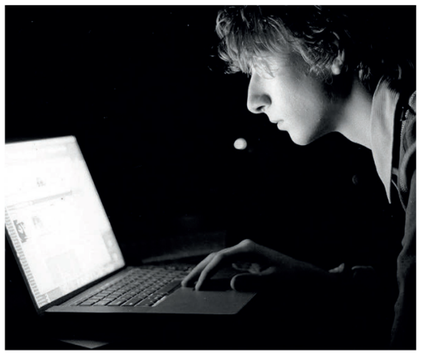
«البصل».. حماية من التتبع

يعتبر متصفح «تور»، بوابة الدخول الرئيسية للشبكة العميقة والمظلمة، وهو برنامج يحوي العديد من طبقات التشفير لحماية البيانات المتدفقة عبر الشبكات التي تستخدمه من التتبع. وتتداخل هذه الطبقات مع بعضها البعض في تصميم يشبه التشريح الداخلي لثمرة «البصل»، وذلك بحسب التصور الذي وضعه مطورو هذا البرنامج، وهم عالم الرياضيات بول سيفرسون وعالما الحاسوب مايكل جي. ريد وديفيد جولدشلاغ، وجميعهم يعملون لدى «مختبر الأبحاث البحرية الأمريكية». وبدأ الثلاثي تطوير فكرة برنامج «تور» في أواخر التسعينيات أيضاً، وذلك بالتزامن مع فكرة الشبكة المخفية لحماية بيانات الجواسيس. ومن الواضح أن الغرض من تطوير الفكرة الثانية هو بساطة التخديم على الفكرة الأولى. و«تور» يعيش على أطراف شبكة الإنترنت، ويُعَد بمثابة التقنية الكامنة التي يعتمد عليها الإنترنت المظلم والإنترنت الخفي.

الحكومة الأمريكية أول من بدأ عمليات الإنترنت العميق

رصد صندوق النقد الدولي في بحث نشره على موقعه العام الماضي، جذور وبدايات مفهوم الإنترنت العميق، موضحاً أنها تعود إلى أواخر حقبة التسعينيات من القرن الماضي، وكانت البداية أمريكية ولغرض استخباراتي بحت، وذلك حينما كلّفت منظمتان بحثيتان تابعتان لوزارة الدفاع الأمريكية جهودهما بُغيَة تطوير شبكة بيانات مُشَفّرَة ومخفية الهوية قادرة على حماية بيانات الاتصال السرية الحساسة، التي تخص الجواسيس الأمريكيين المنتشرين في كل أنحاء العالم. وتعتمد فكرة عمل هذه الشبكة السرية بالأساس على منع محركات البحث التقليدية من الوصول إليها أو حتى معرفة شفراتها. وأفاد البحث بأنه على الرغم من إخفاق وزارة الدفاع في بلوغ الهدف الأصلي، إلا أن الفكرة في حد ذاتها باتت ملهمة لأفكار ومساعي أخرى، ومن أهمها على سبيل المثال، إطلاق شبكات غير هادفة للربح تركز بالأساس على إخفاء هويتها، وذلك لغرض ضمان الخصوصية والحماية من تعقب السلطات الأمنية، حيث غالباً ما تخص هذه الشبكات نشطاء، معارضين للأنظمة السياسية القمعية ومدافعين عن القضايا المتعلقة بحقوق الإنسان.

هجمات طلب الفدية مستمرة مع استكشاف طرق جديدة



توقع طارق عباس، مدير هندسة النظم لدى بالو ألتو نتوركس في الشرق الأوسط وأفريقيا، أن تستمر هجمات طلب الفدية خلال 2020 نظراً لقيام العديد من الجماعات المعادية ببيع برمجيات طلب الفدية وتقديمها كونها خدمة إضافة إلى التدريب على استخدامها. وستواصل هذه الجماعات محاولة استكشاف طرق جديدة للتربح من أجهزة إنترنت الأشياء، التي تم اختراقها لا سيما أن فيها إمكانات غير محدودة لتوليد الأرباح. وتبقى أجهزة إنترنت الأشياء أحد أهم الأهداف لدى المهاجمين، ويرجع ذلك غالباً لأن الوعي والثقافة الأمنية المتعلقة بإنترنت الأشياء غير منتشرة كما ينبغي، وسيستمر عدد أجهزة إنترنت الأشياء في النمو بشكل متسارع مع تطور تقنيات الاتصالات من الجيل الخامس وانتشارها.


طارق عباس

وأضاف: «واحدة من أبرز التحديات الأمنية التي تواجه العصر الرقمي اليوم حقيقة وجود عدد كبير جدًا من الأجهزة والسياسات الأمنية الموضوعة، الأمر الذي يجعل مراقبتها وصيانتها أمراً صعباً جداً. وإيلاء الأولوية لنشر وتطبيق حلول أمنية مؤتمتة بشكل كبير وقادرة على تغطية بيئات عدة، سيؤدي إلى زيادة وضوح الرؤية وتبسيط إجراءات الإدارة وخفض التكاليف، ووتوفير الوقت لأجل التركيز على تحديد جوانب الضعف القائمة».