مركز الجزيرة للدراسات
ALJAZEERA CENTER FOR STUDIES

قضايا

الأمن المعلوماتي والجرائم الإلكترونية.. أدوات جديدة للصراع

جمال محمد غيطاس*

٢٩ فبراير/شباط ٢٠١٢

Al Jazeera Centre for Studies
Tel: +974-44663454
jcforstudies@aljazeera.net
http://studies.aljazeera.net

منذ فجر التاريخ، وحتى اليوم، نشأت على الدوام علاقة وطيدة بين المعلومات والأمن كجبهتين لا غنى لإحداها عن الأخرى، ففي عصور ما قبل التاريخ كانت صرخة الإنسان البدائي في الغابة تحمل أحيانا معلومة تنذر بوقوع خطر يهدد أمن وسلامة الفرد أو الجماعة، ومع تتالي العصور تغيرت الأمور على الجبهتين، فالأمن لم يعد معادلا للحماية من الهجمات المفاجئة من قبل الأعداء أو حتى وحوش الغابة، بل أصبح نظريات وقضايا معقدة، والمعلومات لم تعد مجرد دلالة على أشياء يجري التعبير عنها بصرخة من الفم، بل انطلقت من مكامنها التقليدية داخل الأوراق والكتب والمخطوطات والأفلام والميكروفيلم، بل والنقوش على الأحجار وجدران المعابد وأذهان الناس، واتخذت لنفسها شكلا رقميا نمطيا موحدا، وراحت تجري كالأنهار الهادرة التي تتدفق بلا انقطاع عبر غابة مترامية الأطراف من الأسلاك والموجات اللاسلكية التى تلف الكرة الأرضية برمتها، وهكذا، دفعت الثورة الرقمية والتطورات الجارية في الاتصالات والمعلومات إلى الساحة بالعديد من المتغيرات الجديدة فيما يتعلق بأمن المعلومات بعد تحولها إلى الشكل الرقمي، وجعلت منها قضية ضاغطة على صناع القرار السياسي والجمهور المتخصص والعام معا.

مفهوم أمن المعلومات

تتعدد تعريفات أمن المعلومات وتتنوع حسب زاوية الرؤية، فنحن إذا نظرنا من زاوية أكاديمية سنجد أنه العلم الذي يبحث في نظريات وإستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها.

ولو نظرنا من زاوية تكنولوجية وفنية بحتة يمكننا تعريفه على أنه (الوسائل والأدوات والإجراءات المطلوب توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية)، ومن الزاوية القانونية نجد التعريف قد أخذ منحى آخر لكونه يركز على التدابير والإجراءات التى من شأنها حماية سرية وسلامة وخصوصية محتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها فى ارتكاب الجريمة المعلوماتية.

وبشكل عام يمكن القول إن أمن المعلومات هو تلك الرؤى والسياسات والإجراءات التى تصمم وتنفذ على مستويات مختلفة، فردية ومؤسسية ومجتمعية، وتستهدف تحقيق عناصر الحماية والصيانة المختلفة التي تضمن أن تتحقق للمعلومات السرية أو الموثوقية، أى التأكد من أن المعلومات لا تُكشف ولا يُطَّلع عليها من قبل أشخاص غير مخولين بذلك. والتكاملية وسلامة المحتوى أى التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو العبث به، وبشكل خاص لن يتم تدمير المحتوى أو تغييره أو العبث به فى أية مرحلة من مراحل المعالجة أو التبادل، سواء في مرحلة التعامل الداخلي مع المعلومات، أو عن طريق تدخل غير مشروع. أما الاستمرارية فتعني توفر وإتاحة المعلومات أو الخدمات المبنية عليها لمستخدميها والمستفيدين منها والتأكد من استمرار توفرها والنظم التي تخدمها واستمرار القدرة على

التفاعل معها والتأكيد كذلك على أن مستخدمها لن يتعرض إلى منع الاستخدام أو الحيلولة بينه وبين الدخول إليها، كما تعني أيضا ضمان عدم إنكار الشخص الذي قام بتصرف ما متصل بالمعلومات أو مواقعها أنه هو الذي قام بهذا التصرف.

واقع أمن المعلومات

إن "الفاتورة" الإجمالية لجرائم أمن المعلومات عالميا وعربيا في ٢٠١١ وحده تقدر بحوالي ٣٨٨ مليار دولار أميركي(١)، أما التكلفة النقدية المباشرة لهذه الجرائم والمتمثلة في الأموال المسروقة ونفقات إزالة آثار الهجمات فتقدر بحوالي ١١٤ مليار دولار. ومعنى ذلك أن القيمة المالية لجرائم المعلومات أكبر من السوق السوداء لمخدرات الماريجوانا والكوكايين والهيروين مجتمعين، والتى تقدر بحوالى ٢٨٨ مليار دولار، وتقترب من قيمة السوق العالمية للمخدرات عموما والتى تصل إلى ٤١١ مليار دولار، وأعلى من الإنفاق السنوي لمنظمة الأمم المتحدة للأمومة والطفولة "اليونيسيف" بحوالى ١٠٠ ضعف، حيث تصل ميزانيتها الى ٣,٦٥ مليار دولار، كما تعادل هذه الخسائر ما تم إنفاقه خلال ٩٠ عاما على مكافحة الملاريا وضعف ما تم إنفاقه على التعليم في ٣٨ عاما.

وقد بلغ المعدل الزمني لوقوع جرائم المعلومات حول العالم ٥٠ ألف جريمة واعتداء في الساعة، تأثر بها ٥٨٩ مليون شخص، وهو رقم أكبر من عدد سكان الولايات المتحدة وكندا وغرب أوروبا مجتمعين، ويعادل ٩% من إجمالى سكان العالم.

وقد توزعت هذه الجرائم ما بين جرائم الفيروسات والبريد الإلكتروني الملوث والضار، وجرائم الاحتيال والنصب والاصطياد (الحصول على معلومات بنكية سرية)، والجرائم المتعلقة باختراق الهواتف المحمولة.

ولقد شهد العام الماضي ٢٠١١ الكثير من الحوادث والمواجهات في عالم أمن المعلومات، حملت الكثير من الدلائل على أن الأمر تخطى كل الحدود المعتادة، وصار جولات صراع مكشوفة بين الدول وبعضها البعض، حتى أن جرائم المعلومات باتت أداة جديدة في الصراع السياسي والاقتصادي.

فعلى سبيل المثال إذا ما أخذنا بعين الاعتبار ما تم اكتشافه بخصوص فيروس دوكو Duqu، فسنجد أن نتائج الدراسات الخاصة بحماية البنية التحتية الحساسة مقلقة، إذ الغرض الذي صمّم من أجله فيروس دوكو هو جمع المعلومات الاستخباراتية ومعلومات عن الأصولAssets من منظمات معيّنة مثل الشركات المصنّعة للمكونات التي توجد عادة في بيئة التحكم الصناعي، كما أن من يقفون وراء هجوم دوكو كانوا يبحثون عن معلومات مثل وثائق التصميم التي يمكنها أن تساعدهم في المستقبل لشن هجوم على منشآت التحكم الصناعي. ويمثل

"دوكو" الجيل الأحدث من ستكسنت (Stuxnet) الذي ذكرت تقارير عديدة أن الأميركيين استخدموه في إحداث فوضى داخل البرنامج النووي الإيراني، وفي هذه المرحلة فإن من غير المبرّر الاعتقاد بأن من يقف وراء هجوم "دوكو" لم يتمكن من الحصول على المعلومات الاستخباراتية التي يبحث عنها، وإضافة إلى ذلك فمن المحتمل أن هجمات أخرى لجمع المعلومات قد بدأت بالفعل ولم يتم اكتشافها بعد.

وخلال عام ٢٠١١ عرف العالم جماعات متخصصة من القراصنة الإلكترونيين، مثل Anonymous و LulzSec وغيرهما، حيث استهدفت تلك الجماعات الشركات والأفراد لتحقيق مآرب سياسية مختلفة. ويرجّح خبراء شركة ترينـد مايكرو -إحدى الشركات الدولية المتخصصة في أمن المعلومات- أن تزداد أنشطة مثل هذه الجماعات خلال عام ٢٠١٢، بل وأن تزداد قدرتها على اختراق شبكات الشركات والإفلات من محاولات رصدها ومقاضاتها.

العلاقة بين الأمن المعلوماتي والأمن القومي

يمكننا القول إن اتساع قضية أمن المعلومات وتطورها على هذا النحو الخطير عالميا وعربيا يعود إلى أمرين:

- الأول: أن أغلب دول العالم -بما فيها الدول العربية- ترفع حاليا شعار التحول إلى مجتمع المعلومات والمعرفة، وتنفذ خططا واسعة النطاق لتحويل هذا الشعار إلى واقع، وفى خضم هذه الخطط يتم إنشاء سلاسل من قواعد البيانات القومية الكبرى، كما يجري تطوير شبكات الاتصالات ونشر الإنترنت عبر خطوط الاتصالات العادية والسريعة، وتتجه الأمور لتعميم خدمات نقل الصوت عبر بروتوكولات الإنترنت، وتنشط الدول في نشر مفاهيم وخدمات الحكومة الإلكترونية، وتصدر قوانين التوقيع الإلكتروني الذى يمهد الطريق صوب تفعيل أنشطة التجارة والأعمال الإلكترونية على نطاق واسع، وتتوسع فى مبادرات توفير الحاسب لفئات المجتمع المختلفة بالمنازل والمدارس وللمهنيين، كما تتبنى عشرات من برامج التنمية المعلوماتية المتكاملة فى مختلف الوزارات والهيئات والمؤسسات.

- الثاني: أن تشييد بنية معلوماتية قومية واسعة المجال وتبني التوجه نحو مجتمع المعلومات نقل المجتمع والدولة والمؤسسات إلى مرمى المخاطر، وحتم عليها مواجهة التحديات الشاملة والواسعة النطاق فى أمن المعلومات، بمعنى أن تحديات أمن المعلومات فى مجتمع يمتلك بنية معلوماتية واسعة يجعله يواجه تهديدات فى أمن المعلومات تتسم بالشمول والاتساع وعمق التأثير وتنوع الأدوات وتعدد مصادر الهجوم

وأدواته وغزارة الأهداف التى تشكل إغراء ومناطق جذب لمن يستهدفونه، فمخاطر أمن المعلومات فى عصر (مجتمع المعلومات) تضم مستويين:

- الأول: مستوى تعقب وجمع المعلومات، ويشمل الوسائل التقليدية لجمع المعلومات التى تعتمد بشكل كبير على العناصر البشرية من الجواسيس أو ما يعرف بالطابور الخامس، ووسائل الاستطلاع الحديثة وفى مقدمتها الأقمار الصناعية التي تطورت بشكل كبير، حيث بلغت الصور والمعلومات الواردة منها حدا فائقا من الجودة والدقة لم تبلغها من قبل، كما يشمل هذا المستوى العديد من أدوات تعقب وجمع من داخل البنية المعلوماتية الأساسية للجهة المستهدفة ومنها "البوابات الخلفية" ويقصد بها الثغرات أو نقاط الضعف الأمنية التى توجد بشبكات ونظم المعلومات والبرامج المختلفة، و"الرقائق الإلكترونية" التي تعتبر الجزء الحيوي بجميع أجهزة التعامل مع المعلومات من حاسبات ومعدات بناء شبكات ووسائط تخزين وغيرها والتي يمكن استخدامها في تعقب وجمع المعلومات، وأدوات التلصص على شبكات المعلومات وعمليات الاعتراض.
- الثاني: مستوى يستهدف إفساد وتعطيل المعلومات، وتستخدم فيه العديد من الأدوات كفيروسات الحاسب والاختراق المباشر لشبكات المعلومات والهجوم بفيض الرسائل والطلبات وهجمات الاختناق المروري الإلكتروني على نطاق واسع وغيرها.

وكما هو واضح فإن هذه الأخطار لا تتوقف عند كونها تهديدا لأمن المعلومات داخل شركة أو مؤسسة أو منشأة، بل تعد تهديدات جدية للأمن القومي للدول والمجتمعات ككل.

وتضعنا المعطيات السابقة أمام حقيقة واضحة وهى أن تحقيق تقدم ملموس في قضية أمن المعلومات عالميا أو عربيا لن يتم إلا بتغيير المنهج القائم حاليا والذي يتعامل مع القضية باعتبارها قضية "تقنية بحتة" تقع مسؤوليتها على الفنيين والمختصين في علوم الحاسب وتأمين الشبكات، والانتقال للأخذ بالمنهج الذي يعتبر أمن المعلومات ركيزة أساسية من ركائز الأمن القومي الشامل، ومن ثم يتعين رفعها من مستوى التعامل "الفني والتقني"، إلى مستوى التعامل السياسي والإستراتيجي، وألا تترك للتعامل العفوي غير الخاضع لإستراتيجية أو سياسة وطنية عامة ترشد مساره.

لقد اخذت الدول العربية على عاتقها -كما سبقت الإشارة - تنفيذ خطط وبرامج متنوعة تسعى لتشييد ما يمكن أن نطلق عليه (بنية معلوماتية قومية شاملة على كل المستويات) تتغلغل فى مفاصل المجتمع وشرايينه الرئيسية والفرعية وتضطلع بعبء تداول المعلومات التي

يديرها ويستخدمها، وكل هذه الأمور تقلص فارق الأهمية بين ما هو معلومات أمنية وعسكرية محضة تتجه الأنظار لحمايتها تلقائيا، وبين ما هو معلومات مدنية ارتقت أهميتها بحكم شموليتها وضرورة استمرارية إتاحتها لتصبح موردا حيويا يوميا بالغ الأهمية والتأثير فى مجموع الشعب ككل، أى تصبح المعلومات المتداولة داخل البنية المعلوماتية المدنية ركيزة من ركائز الأمن القومي التى يتعين حمايتها وتأمينها بمنظور إستراتيجي كما هو الحال مع المعلومات العسكرية والأمنية.

من هنا يصبح من الخطأ تخطيطيا وإداريا أن تنشط أى دولة فى تشييد بنية معلوماتية قومية متعددة الأوجه والمستويات على هذا النحو ثم لا تطور سياسة أو إستراتيجية قومية لحماية هذه البنية وصيانة أمنها وأمن ما يتداول داخلها من بيانات ومعلومات، وتترك ذلك للتصرفات العفوية والمبادرات الفردية والمشروعات والخطط الجزئية المنفرطة التى تجري هنا أو هناك دون سياسة أو إستراتيجية واضحة، فالبنية المعلوماتية الأساسية الشاملة تتطلب بالتبعية سياسة أمن معلوماتية شاملة، وليس هناك أدنى مبالغة في القول بأن المضي قدما في تشييد بنية معلوماتية قومية ضخمة بلا إستراتيجية أمنية شاملة وكافية يشكل خللا جسيما في مسيرة التنمية المعلوماتية، ويؤثر سلبيا على الأمن القومى، لأنه يجعل البنية المعلوماتية القومية -وهى تتحول مع الزمن إلى مورد إستراتيجي للدولة- كيانا هشا يمكن أن يتعرض لانكشاف أمني في كل أو بعض جوانبه.

وبما أن مخاطر أمن المعلومات باتت ترقى إلى مستوى تهديد الأمن القومي ككل، فإن وسائل المواجهة والحماية لابد وأن تظللها منظومة أمن قومي، لأنه من الخطأ أن تكون الأخطار والتهديدات شاملة وربما منسقة ومخططة أحيانا ثم تأتي سبل ووسائل مواجهتها جزئية وعفوية وخالية من التخطيط وتفتقر للتنسيق والرشد، وقد قدمت اليابان نموذجا لهذا المستوى من التعامل مع أمن المعلومات حينما أعلنت منذ أوائل أكتوبر/تشرين ٢٠٠٥ البدء في تنفيذ برنامج شامل على مستوي مؤسسات وهيئات الدولة والشركات الخاصة يستهدف التدريب علي صد الهجمات الإلكترونية الشاملة بتنويعاتها المختلفة، سواء بالفيروسات أو عمليات القرصنة والتلصص والتجسس الاقتصادي أو التخريب الإلكتروني أو هجمات تعطيل شبكات الاتصالات والمعلومات، وجاء هذا البرنامج التدريبي المستمر حتى في إطار إستراتيجية متكاملة لأمن المعلومات باليابان تنفذها الدولة حماية لاقتصادها، وقد تزامنت مع المخطط الياباني مخططات مماثلة في عشرات الدول حول العالم.

وأخيرا لابد من الإشارة إلى أن إدارة المعلومات المتداولة داخل البنية المعلوماتية القومية بما يدعم الأمن القومي أمر يتطلب فهما ورؤية جديدة لأساليب ومناهج وأدوات تداول المعلومات بين أطراف المجتمع وبعضها البعض داخليا، وكذلك مناهج وأدوات وأساليب إدارة وتداول المعلومات بينها وبين الجهات الخارجية، كشركاء السياسة والتجارة والأعمال والتعليم والبحث العلمي والتصنيع...، وهذه قضية مهمة ومعقدة في آنٍ معا، ولا يصح تركها لاجتهادات أفراد

ومؤسسات وخبراء من هنا وهناك مهما علا شأنهم وتجاربهم وقدراتهم، بل تحتاج جهدا مؤسسيا لن يتحقق على النحو المطلوب إلا عندما تتبوأ قضية أمن المعلومات مكانها الصحيح كركيزة أساسية للأمن القومي.

** جمال محمد غيطاس، باحث ورئيس تحرير مجلة لغة العصر الصادرة عن مؤسسة الأهرام، محرر تكنولوجيا المعلومات بصحيفة الأهرام.*

هامش

١- اعتمد الباحث في المعلومات الواردة بتقدير حجم جرائم المعلومات عالميا وعربيا على تقرير 2011 The Norton Cybercrime Report الصادر عن شركة سيمانتك العالمية المتخصصة في أمن المعلومات حول أوضاع جرائم المعلومات في عام ٢٠١١، والذي حمل عنوان "صورة إجمالية لأوضاع أمن المعلومات حول العالم".

انتهى