

## افتتاحية العدد

إعداد

أ.د. شريف كامل شاهين  
أستاذ بكلية الآداب جامعة القاهرة  
Doi: 10.21608/jinfo.2020.166263

### افتتاحية العدد :

تتأسق المؤسسات على اختلاف أنواعها وأنشطتها في جميع أنحاء العالم نحو تطبيق تقنيات جديدة، باستخدام البيانات الدقيقة من أجل البقاء من خلال المنافسة والابتكار والنمو في عالم يتزايد ترابطه يوماً بعد يوم. وأصبحت المعلوماتية وتطبيقاتها ووسائلها التكنولوجية الناشئة المختلفة المحرك الرئيس للمنافسة والسعي نحو التميز في العالم الرقمي. وفي الجانب الآخر تواجه المؤسسات أنواعاً جديدة من المخاطر والتحديات تعرف بالمخاطر السيبرانية. ولهذه الأسباب وغيرها بادرت المؤسسة العربية للتربية والعلوم والآداب التابعة لوزارة التضامن الاجتماعي بمصر بالتجهيز والإعداد لهذه الدورية الجديدة "المعلوماتية وأمن المعلومات" لنشر الأبحاث المتميزة علمياً فقط لتكون قبلة للمتخصصين والباحثين في هذا المجال سواء على المستوى الوطني أو المؤسسي في مرافق المعلومات بأنواعها المختلفة من مكاتب وأرشيفات ومتاحف ووحدات توثيق ومراكز وشبكات معلومات وغيرها. كما تهتم ببحث قضاياها ذات الأبعاد الصحية والهندسية والزراعية والإجتماعية والاقتصادية والحكومية... وغيرها. وننتهزها فرصة لتوجيه الدعوة للباحثين الراغبين في نشر أبحاثهم الالتزام بمعايير النشر المتعارف عليها محلياً (أكاديمية البحث العلمي والمجلس الأعلى

للجامعات) وعربياً (كشاف الاستشهادات العربية ومعامل التأثير الصادر عن بنك المعرفة المصري بالتعاون مع Clarivate Analytics) وعالمياً.

يحذر منتدى أمن المعلومات Information Security Forum

(ISF)- وهو منظمة مستقلة لا تهدف إلى الربح ويوصف بأنه "السلطة الرائدة عالمياً في مجال الأمن السيبراني وأمن المعلومات وإدارة المخاطر"- في تقريره السنوي الصادر عام ١٩١٩م بعنوان: Threat Horizon من مجموعة من التهديدات الرئيسية المتوقع مواجهتها من جانب المؤسسات على مدار العامين أو الثلاثة القادمة، وقد تم تجميعها تحت ثلاثة محاور رئيسية:

الاضطراب Disruption - يخلق الاعتماد المفرط على شبكات الاتصال الإلكترونية الهشة، وارتفاع احتمالية انقطاع الإنترنت إلى فشل التجارة الإلكترونية، فضلاً عن احتمالات اختراق تطبيقات إنترنت الأشياء Internet of Things.

التشويه Distortion - يؤدي إنتشار النشر المتعمد للمعلومات الخاطئة والمضللة والمزيفة، وما يمكن أن تقدمه إبتكارات الإنسان الآلي "الروبوتات" وغيرها من المخترعات الإلكترونية إلى زعزعة الثقة في سلامة المعلومات ونزاهتها للخطر.

التدهور/ الإنحدار Deterioration - ينتج عن التطورات السريعة في التقنيات الذكية (خاصة الذكاء الاصطناعي) بالإضافة إلى الإحتياجات المتضاربة الناشئة عن تطور أنظمة الأمن القومي والخصوصية الفردية تأثيراً سلبياً على قدرة المنظمات على التحكم في معلوماتها الخاصة.

أدى الاعتماد المتزايد المستمر في مجتمعنا الرقمي على البيانات والتواصل الإلكتروني البيئي وخاصة ما يتعلق بإنترنت الأشياء إلى ظهور مخاطر جديدة لحوادث الأمن السيبراني واسعة النطاق ذات العواقب التخريبية المتتالية. وهو ما دفع

---

المؤسسات إلى مراجعة سياساتها المعلوماتية من أجل صياغة إما بنود جديدة أم سياسة مستقلة لأمن المعلومات والخصوصية وجرائم المعلومات وإدارة البيانات... وغيرها. وتعرف سياسة أمن المعلومات بأنها مجموعة من القواعد التي تسنها إحدى المؤسسات لضمان التزام جميع مستخدمي الشبكات أو البنية الأساسية لتكنولوجيا المعلومات داخل نطاق المؤسسة بالاستخدام الآمن للبيانات المخزنة رقمياً في نطاق عمل المؤسسة بما يضمن حماية المعلومات، والتي تعد واحدة من الأصول العديدة التي تحتاج المؤسسات إلى حمايتها. واختصاراً يستهدف أمن المعلومات حماية ثلاثة سمات أو أغراض رئيسية، وهي:

- السرية Confidentiality: يقتصر حق أو حقوق الوصول لأصول البيانات والمعلومات على الأشخاص المصرح لهم بذلك مع التأكيد على عدم الكشف عنها للآخرين.
  - النزاهة Integrity: الحفاظ على البيانات سليمة وكاملة ودقيقة أثناء تشغيل أنظمة تكنولوجيا المعلومات.
  - الإتاحة/ التوفر Availability: وضع المعلومات أو النظام تحت تصرف المستخدمين المصرح لهم عند الحاجة.
- والنصيحة التي خرجت بها الدول والمؤسسات من تجاربها وخبراتها العملية في مجال أمن الشبكات وتأمين المعلومات المتداولة إما على الخط المباشر من خلال أنظمة إلكترونية أو متاحة على وسائط مادية. أننا بحاجة دائمة منتظمة إلى بناء الثقافة الرقمية والمعلوماتية للأفراد من جانب وثقلها بالمعارف الحديثة ذات الصلة. فضلاً عن تقييم المخاطر الرقمية وعدم تغليب القيود والعقبات الأمنية على بناء المرونة الكافية التي تسمح بسهولة التداول والوصول والإتاحة وتحقيق الفائدة

المرجوة من منتجات وخدمات الأنظمة الإلكترونية خوفاً من الإنتهاكات والإختراقات التي لا مفر منها.