# نشـــرة
# تـكـنـولـوجـيـا المـعـلـومـــات والاتـصـــالات
# للتنمية في المنطقة العربية

## ملف العدد: الجرائم الإلكترونية

١. Hacktivism: at the Crossroads of Press Freedom Human Rights and National Security
٢. سياسات تكنولوجيا المعلومات والاتصالات
٣. تطبيقات تكنولوجيا المعلومات والاتصالات
٤. استعراض تقرير
٥. أنشطة شعبة تكنولوجيا المعلومات والاتصالات

العدد
١٨


© Rolffimages - Fotolia.com

الاسكوا

الأمم المتحدة - اللجنة الاقتصادية والاجتماعية لغربي آسيا

Distr.
GENERAL

E/ESCWA/ICTD/2013/1
5 April 2013
ORIGINAL: ARABIC

**اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)**

# نشرة تكنولوجيا المعلومات والاتصالات للتنمية في المنطقة العربية

## العدد ١٨

الأمم المتحدة
نيويورك، ٢٠١٢

12-0336

# مواضيع العدد

الصفحة

# مقدمة

ظهرت الجرائم السيبرانية وتطورت لتصبح إحدى أسرع التهديدات نمواً في عالم الجريمة. فهذه الجرائم تعيق التنمية الاقتصادية والاجتماعية على الصعيد العالمي، ولها آثار خطيرة على المجتمعات وتؤدي إلى فقدان الثقة بالتكنولوجيا فتنخفض معدلات استخدام ونمو تكنولوجيا المعلومات والاتصالات. ويبقى تحديد مدى انتشار هذه الأنشطة الإجرامية بغاية الصعوبة، إلا أن تقرير "نورتن" عن الجرائم السيبرانية لعام ٢٠١٢ يقدر الخسائر الناجمة عنها بنحو ١١٠ مليارات دولار أمريكي. وتطرح هذه القضية معضلة حقيقية بالنسبة إلى البلدان ذات الاقتصاد النامي التي تكافح من أجل مواكبة التطور التكنولوجي في سوق آخذة في العولمة. ومع تخطي هذا النوع من الجرائم الحدود الجغرافية، وبسبب طبيعة شبكات المعلومات العابرة للحدود، تصبح البلدان التي لا تعتمد تشريعات سيبرانية فعالة هدفاً لمرتكبي الجرائم السيبرانية الذين يستغلون غياب الأطر التنظيمية في هذا المجال.

وقد كرّست اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا) جزءاً من أنشطتها لتطوير نهج متقدم لوضع التشريعات السيبرانية يقوم على التنسيق على الصعيد الإقليمي للتصدي لهذه الظاهرة، فأصدرت في عام ٢٠٠٧ دراسة بعنوان "نماذج تشريعات الفضاء السيبراني في البلدان الأعضاء في الإسكوا" وقامت بتحليل التشريعات المعتمدة في هذه البلدان وبمقارنتها مع التشريعات السيبرانية المطبقة في عدد من البلدان الأخرى. وفي عام ٢٠٠٩، أطلقت مشروع "تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية" الذي يهدف إلى تحسين التكامل الإقليمي وتعزيز قدرة البلدان الأعضاء على بناء قطاع قوي ومستدام لتكنولوجيا المعلومات والاتصالات، وذلك من خلال إنشاء الهياكل القانونية والتنظيمية الملائمة. وقدمت الإسكوا في هذا السياق مجموعة من الإرشادات التي ترمي إلى مساعدة البلدان العربية على تحسين البيئة المؤاتية لسن التشريعات السيبرانية فيها وتشمل المجالات الستة التالية: حماية البيانات الشخصية؛ الاتصالات الإلكترونية وحرية التعبير؛ التواقيع الإلكترونية والعمليات الإلكترونية؛ التجارة الإلكترونية وحماية المستهلك؛ الملكية الفكرية؛ والجرائم السيبرانية. ويلخص المقال الأول في هذا العدد من "نشرة تكنولوجيا المعلومات والاتصالات للتنمية في المنطقة العربية" الجهود المبذولة ولا سيما أنشطة الإسكوا في هذا المجال ويعرض تقييماً للمشروع.

والواقع أن ظهور التكنولوجيات والاتجاهات المعاصرة قد طرح تحديات جديدة وقضايا خطيرة. أولاً، ومع ارتفاع كمية المعلومات الشخصية التي يجري تحميلها، دفعت وسائل الاحتفاظ بالبيانات وتكنولوجيات تسجيل الدخول إلى الشبكات إلى إعادة تحديد توقعات المستخدمين بشأن خصوصيتهم على الإنترنت. ثانياً، ومع تزايد التداول بالعملات الافتراضية، تظهر أبعاد جديدة للقضايا المتعلقة بمنهجيات الدفع الإلكتروني. ثالثاً، ومع انتشار استخدام الخدمات المصرفية عبر الهاتف النقال لا سيما في البلدان النامية، تبرز الحاجة إلى التعامل مع بعض القضايا المطروحة كإنشاء سلطة قضائية تعمل على حل الخلافات المتعلقة بالمعاملات عبر الهاتف النقال.

وتتضمن النشرة مجموعة من المقالات التحليلية التي تتناول أثر الجرائم السيبرانية، وأداء الناشطين السياسيين والصحافيين على الفضاء السيبراني، وعمل الحكومات في هذا المجال. وفي هذا الخصوص، توصي النشرة الحكومات بتنسيق جهودها للاستفادة من النمو السريع في قطاع تكنولوجيا المعلومات والاتصالات وتدعوها إلى اتباع نهج حديث وقابل للتكيف لمكافحة هذه الجرائم لما له من دور في إيجاد بيئة مؤاتية للتقدم في تحقيق التنمية الاقتصادية والاجتماعية.

كما تتناول النشرة مجالات مواضيعية تهم المنطقة ومنها الحكومة الإلكترونية وتقدم المقالات والتحليلات الواردة فيها توصيات لمعالجة القضايا الناشئة. وتعرض النشرة أيضاً الأنشطة الرامية إلى تسخير تكنولوجيات المعلومات والاتصالات لأغراض التنمية التي اضطلعت بها الإسكوا خلال النصف الثاني من عام ٢٠١٢.

وقد عمل على إعداد هذه النشرة فريق يتألف من موظفين في شعبة تكنولوجيا المعلومات والاتصالات في الإسكوا وعدد من الخبراء في مجال مكافحة الجرائم السيبرانية وإعداد التشريعات السيبرانية. وتولى عمليات التخطيط والتنسيق والمتابعة السيد ماثيو بيركنز وذلك تحت إشراف السيدة نبال إدلبي.

# ملف العدد: الجرائم الإلكترونية

## تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية[١]

مع تطور العصر الرقمي وتنامي المساعي لبناء مجتمع مرتكز على المعلومات والمعرفة، كان لا بد من تحديث الأطر التنظيمية والقانونية لتتلاءم مع المتطلبات الحديثة الخاصة بالفضاء السيبراني وزيادة تجانسها. وتعتبر التشريعات السيبرانية عنصراً أساسياً في توفير البيئة التنظيمية والقانونية اللازمة لتطوير مجتمع المعلومات والمعرفة، ولبناء الثقة بالخدمات الإلكترونية وتأمين الحماية لمستخدمي الإنترنت. وبالرغم من الجهود الواعدة التي تقوم بها بعض الدول في المنطقة العربية، لا تزال معظمها بعيدة عما وصلت إليه الدول المتقدمة في هذا المجال. فالدول العربية تحتاج إلى المزيد من الجهود الوطنية والإقليمية لسن أو تحديث القوانين الخاصة بالفضاء السيبراني، وتوفير الهيكلية التنظيمية والإدارية لتنفيذها، كما أن هناك حاجة لتنسيق التشريعات السيبرانية بين الدول العربية.

وفي هذا الإطار، وبهدف تحفيز التكامل الإقليمي في بناء مجتمع المعرفة في المنطقة العربية، بدأ اهتمام اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا) بدعم تطوير التشريعات السيبرانية في المنطقة، بحيث أطلقت مجموعة من الدراسات وعقدت عدة اجتماعات وورش عمل متخصصة، ومن أبرز الأنشطة التي أطلقتها الإسكوا في هذا الإطار المشروع الإقليمي حول "تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية"، الذي نفذته بالتعاون مع الدول الأعضاء. والجدير بالذكر أن عدداً من المناطق في العالم قد قامت بجهود مماثلة، كجهود الاتحاد الأوروبي في إطلاق الإرشادات الأوروبية حول التشريعات السيبرانية، وجهود جماعة شرق أفريقيا في تنسيق قوانين التجارة الإلكترونية[٢].

### الحاجة إلى القوانين السيبرانية

سن القوانين السيبرانية وتنفيذها هو من القضايا التي تكتسب مزيداً من الأهمية مع انتشار استخدام تكنولوجيا المعلومات والاتصالات وتطبيقاتها في مختلف القطاعات الاقتصادية، والاجتماعية، والعلمية، والتجارية، وكذلك في الخدمات الحكومية وفي علاقات التفاعل بين الأفراد والمؤسسات. فوجود أطر وضوابط لتنظيم المعاملات الإلكترونية، ولحماية مستخدميها والمتعاملين بها، يولد شعوراً بالأمان لدى جميع المستفدين من التطبيقات والخدمات الإلكترونية عبر الإنترنت.

ومعظم التطبيقات الإلكترونية الحكومية والخدمات الإلكترونية المصرفية والصحية تتطلب تخزين بيانات هامة خاصة بالأفراد أو المؤسسات، وقد يكون البعض منها على مستوى دقيق من الحساسية أو الخصوصية. في هذا الإطار، يصبح من الضروري ضمان مسائل الخصوصية وحماية البيانات ذات الطابع الشخصي باعتماد قوانين تحظر استخدام ومعالجة هذه المعلومات دون إذن صاحبها، أو سوء استخدامها، أو وضعها في غير موضعها.

وبالرغم من التطورات الإيجابية للتكنولوجيا والفرص المتعددة لتطبيقاتها، فقد عمد البعض إلى استغلال الفضاء السيبراني واستخدامه كوسيلة للتعدي على الغير، أو إلى القيام بأفعال جرمية مؤذية كسلب الأموال، وإساءة استخدام المعلومات الخاصة، وتطوير البرمجيات الخبيثة لتخريب أنظمة الحاسوب. وقد تنامت الأفعال المسيئة مع تنامي الشبكات الاجتماعية وتزايد أعداد المستخدمين للإنترنت من كافة الفئات العمرية ومختلف الطبقات الاجتماعية. لذلك برزت الحاجة إلى تعريف هذه الأفعال وملاحقة مرتكبيها قانونياً. وقد باشرت العديد من الدول، ومنها دول الاتحاد الأوروبي وبعض الدول في المنطقة العربية، بإصدار قوانين بشأن الجرائم السيبرانية، بهدف ردع الممارسات السيئة وملاحقة مرتكبيها.

## مشروع الإسكوا حول "تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية"

أطلقت إدارة تكنولوجيا المعلومات والاتصالات في الإسكوا المشروع عام ٢٠٠٩ بهدف تعزيز وتنسيق التشريعات الخاصة بتكنولوجيا المعلومات والاتصالات في المنطقة العربية؛ أي التشريعات السيبرانية. ويهدف المشروع أيضاً إلى تعزيز استخدام تطبيقات تكنولوجيا المعلومات والاتصالات في القطاع الحكومي وفي الأنشطة الاقتصادية والثقافية والاجتماعية؛ وتقليص الفوارق القانونية بين الدول العربية، وكذلك بين الدول العربية والدول المتقدمة تكنولوجياً؛ وتسهيل المعاملات الإلكترونية والتجارة الإلكترونية بين الدول في المنطقة.

وقد شكلت الإسكوا في بداية المشروع لجنة استشارية ضمت المنظمات الدولية والإقليمية المعنية بتطوير التشريعات السيبرانية في المنطقة العربية، وهي جامعة الدول العربية ممثلة بمجلس الوزراء العرب للاتصالات والمعلومات ومجلس وزراء العدل العرب، والمنظمة العربية للتنمية الإدارية، والمكتب العربي للاتحاد الدولي للاتصالات، واللجنة الاقتصادية لأفريقيا - مكتب شمال أفريقيا، إضافة إلى خبراء في مجال التشريعات السيبرانية وفريق عمل الإسكوا. وقد قامت هذه اللجنة الاستشارية بتحديد التوجهات الأساسية للمشروع وتابعت تنفيذه من منظور إقليمي شامل.

### أنشطة مشروع تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية

**١- إعداد تقارير حول وضع التشريعات السيبرانية في المنطقة العربية واقتراح إطار عام لتطوير وتنسيق التشريعات السيبرانية في العالم العربي.**

**٢- وضع إرشادات للتشريعات السيبرانية بالاعتماد على التجارب الإقليمية والدولية، وخاصة التجربة الأوروبية، مع أخذ خصوصيات المنطقة العربية في الاعتبار.**

**٣- تنظيم اجتماع للخبراء شارك فيه الأخصائيون من المؤسسات الحكومية والمنظمات غير الحكومية والقطاع الخاص، لاستعراض ومناقشة مسودة إرشادات الإسكوا للتشريعات السيبرانية.**

**٤- تنظيم ورشتي عمل إقليميتين لتوفير التدريب العملي لصانعي القرار والسياسات حول إرشادات الإسكوا للتشريعات السيبرانية وتطبيقها على المستويين الوطني والإقليمي.**

**٥- تقديم خدمات استشارية للدول العربية من أجل تطوير تشريعاتها السيبرانية بالتوافق مع إرشادات الإسكوا.**

**٦- إنشاء شبكة افتراضية من الخبراء لإطلاق النقاش والحوار حول تطبيق إرشادات الإسكوا للتشريعات السيبرانية في المنطقة العربية، بحيث تشكل هذه الشبكة قاعدة لتبادل المعرفة وأداة لاستدامة المشروع.**

**٧- تنظيم ندوة حول المتطلبات القانونية والتنظيمية لإقامة مجتمع معرفة مستدام في المنطقة العربية، واستعراض نتائج المشروع وصياغة توصيات لضمان استدامة العمل في مجال تنسيق التشريعات السيبرانية على المستويين الوطني والإقليمي.**

المصدر: http://isper.escwa.un.org/FocusAreas/CyberLegislation/Projects/tabid/161/language/ar-LB/Default.aspx.

وقد بلورت ورش العمل والخدمات الاستشارية الجانب التطبيقي للمشروع، حيث أتاحت الفرصة للفرقاء المعنيين من وزارات تكنولوجيا المعلومات والاتصالات، ووزارات العدل، وكذلك الجهات الأكاديمية والمجتمع المدني، للاطلاع عن قرب على أنشطة المشروع وخاصة إرشادات الإسكوا للتشريعات السيبرانية. وقد تمكنت الأردن، والبحرين، والجمهورية العربية السورية، وعُمان، وفلسطين من الاستفادة من الخدمات الاستشارية التي قدمتها الإسكوا بالتعاون مع الخبراء القانونيين. وقد شملت هذه الخدمات الاستشارية مراجعة لمسودات القوانين السيبرانية التي أعدتها هذه الدول، وتقييماً لوضع التشريعات السيبرانية في الدولة، ودراسة للفوارق بينها وبين إرشادات الإسكوا في هذا المجال.

هذه الإرشادات ستة محاور أساسية لتنظيم الفضاء السيبراني، وهي التالية: الاتصالات الإلكترونية وحرية التعبير؛ المعاملات الإلكترونية والتواقيع الإلكترونية؛ التجارة الإلكترونية وحماية المستهلك؛ معالجة وحماية البيانات ذات الطابع الشخصي؛ الجرائم السيبرانية؛ والملكية الفكرية في المجال المعلوماتي والسيبراني. ويمكن الاستفادة من هذه الإرشادات إما كقوانين منفصلة بحسب المحور أو اعتبارها قانون واحد وشامل للفضاء السيبراني.

ويتضمن كل إرشاد من الإرشادات الستة ورقة مرجعية تتناول موضوع الإرشاد، يتبعها مقدمة للإرشاد ومن ثم نص الإرشاد الذي يعرض أبواب ومواد القانون المختلفة.

## إرشادات الإسكوا للتشريعات السيبرانية

تعد إرشادات الإسكوا للتشريعات السيبرانية[٣] أبرز مخرجات مشروع "تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية"، وهي الأولى من نوعها في المنطقة العربية. وتهدف هذه الإرشادات إلى تسهيل وضع التشريعات السيبرانية في الدول العربية أو مراجعة القائم منها لاستكمال بعض النواقص فيه وتعديلها. وتغطي

### أقسام الإرشادات وما يتضمنه كل منها من معلومات

### الأفعال المصنفة كجرائم سيبرانية

- **التعدي على البيانات المعلوماتية؛**
- **التعدي على الأنظمة المعلوماتية؛**
- **إساءة استعمال الأجهزة أو البرامج المعلوماتية؛**
- **الجرائم على الأموال؛**
- **الاستغلال الجنسي للقاصرين؛**
- **التعدي على الملكية الفكرية للأعمال الرقمية؛**
- **جرائم البطاقات المصرفية والنقود الإلكترونية؛**
- **الجرائم التي تمسّ بالمعلومات الشخصية؛**
- **جرائم العنصرية والجرائم ضد الإنسانية بوسائل معلوماتية؛**
- **جرائم المقامرة وترويج المواد المخدرة بوسائل معلوماتية؛**
- **جرائم المعلوماتية ضد الدولة والسلامة العامة؛**
- **جرائم تشفير المعلومات.**

المصدر: http://isper.escwa.un.org/Portals/0/Cyber%20Legislation/Regional%20Harmonisation%20Project/Directives/DirectivesFull.pdf.

ونورد في ما يلي مضمون الإرشاد الخامس مثالاً على إرشادات الإسكوا للتشريعات السيبرانية، وهو إرشاد الجرائم السيبرانية. يعرف هذا الإرشاد الجرائم السيبرانية بأنها الجرائم التي يكون فيها الحاسوب أداةً لتنفيذ الجريمة كالتحايل والأعمال الإباحية؛ أو بأنها الجرائم التي يكون فيها الحاسوب وشبكات الحواسيب موضعاً للجريمة، كالتعدي على أنظمة الأمان وإرسال البرمجيات الخبيثة. ويبين الإطار قائمة بما يشير إليه الإرشاد من جرائم سيبرانية.

ويختلف وضع البلدان العربية لناحية إقرار قوانين تتعلق بالجرائم السيبرانية، فقد أقرت بعض البلدان قوانين مستقلة للجرائم السيبرانية، بينما أدخلت بعض البلدان الأخرى أجزاء/أبواب خاصة بالجرائم السيبرانية ضمن قوانين العقوبات. والجدير بالذكر أن بعض البلدان العربية هي حالياً بصدد إعداد قوانين للجرائم السيبرانية، ويبين الجدول وضع التشريعات السيبرانية في المنطقة العربية.

### قوانين ومواد الجرائم السيبرانية

| البلد | القانون | سنة الإصدار |
|---|---|---|
| **القوانين الصادرة** | | |
| **الأردن** | قانون جرائم أنظمة المعلومات | ٢٠١٠ |
| **الإمارات العربية المتحدة** | القانون الاتحادي رقم ٢ بشأن مكافحة جرائم تقنية المعلومات | ٢٠٠٦ |
| **الجمهورية العربية السورية** | قانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية | ٢٠١٢ |
| **المملكة العربية السعودية** | نظام مكافحة جرائم المعلوماتية | ٢٠٠٧ |
| **السودان** | قانون رقم ١٤ | ٢٠٠٧ |
| **المواد ذات الصلة** | | |
| **البحرين** | مرسوم قانون رقم ٢٠٠٢/٢٨ بشأن المعاملات الإلكترونية<br>قانون الاتصالات رقم ٢٠٠٢/٤٨ | ٢٠٠٢ |
| **تونس** | قانون المبادلات والتجارة الإلكترونية | ٢٠٠٠ |
| **عُمان** | مرسوم سلطاني رقم ٢٠٠١/٧٢ | ٢٠٠١ |
| | مرسوم سلطاني رقم ٢٠٠٨/٦٩ بإصدار قانون المعاملات الإلكترونية | ٢٠٠٨ |
| | المادة رقم ٢٧٦ حول جرائم الحاسوب | |
| **لبنان** | تعميم رقم ٤ حول حماية برامج المعلوماتية ومكافحة القرصنة | ٢٠٠٦ |
| | قرار رقم ٧٨١٨ حول نظام مراقبة العمليات المالية والمصرفية لمكافحة تبييض الأموال | ٢٠٠١ |
| **مصر** | قرار وزاري رقم ٣٢٧ حول إنشاء إدارة مباحث مكافحة جرائم حاسبات الإنترنت | ٢٠٠٥ |
| | قانون رقم ١٥ بشأن التوقيع الإلكتروني | ٢٠٠٤ |
| **المغرب** | قانون حماية الملكية الفكرية | ٢٠٠٠ |
| **مشاريع القوانين** | | |
| **البحرين** | مشروع قانون بشأن جرائم الحاسب الآلي | |
| **الجزائر** | مشروع قانون المعاملات الإلكترونية وقانون حماية المعطيات ذات الطابع الشخصي | |
| **فلسطين** | مشروع قانون المبادلات والتجارة الإلكترونية | |
| **الكويت** | مشروع قانون لمكافحة جرائم شبكة الإنترنت<br>مشروع قانون المعاملات الإلكترونية | |
| **اليمن** | مشروع قانون لمكافحة الجرائم الإلكترونية | |

المصدر: مقتبس عن http://isper.escwa.un.org/Portals/0/Cyber%20Legislation/Regional%20Harmonisation%20Project/Directives/Directives-Full.pdf

ملاحظة: ليبيا ليس لديها حتى الآن قوانين تتعلق بمواضيع الفضاء السيبراني.

## ملاحظات ختامية

لقد تمكن مشروع "تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية" من تحقيق نتائج ملموسة خلال السنوات التي تم تنفيذه فيها، أي في الفترة ٢٠٠٩-٢٠١٢، وقد برهن التفاعل الإيجابي للبلدان العربية عن أهمية تطوير التشريعات السيبرانية وضرورة تنسيقها على المستوى الإقليمي. والجدير بالذكر أن المشروع خلص إلى مجموعة من التوصيات وضعت بشكل إطار عمل يستهدف كافة الفرقاء المعنيين ببناء مجتمع المعرفة، وتحديداً الحكومات التي تقوم بالدور الأساسي في عملية سن القوانين السيبرانية. كما أولى المشروع أهمية لاستدامة العمل ولضمان استمرار الاهتمام والاستخدام الفعلي للمخرجات، وخاصة إرشادات الإسكوا للتشريعات السيبرانية. وللوصول لهذا الهدف، عملت الإسكوا على إنشاء بوابة إلكترونية[٤] تشكل مخزناً للمعلومات والمعرفة، وتهدف إلى التوعية بأهمية التشريعات السيبرانية ودعم متخذي القرار في الدول العربية في عملية وضع الأطر القانونية الخاصة بالفضاء السيبراني. كما وضعت الإسكوا شبكة افتراضية للتشريعات السيبرانية تتضمن قاعدة بيانات للخبراء والمؤسسات الإقليمية في مجال التشريعات السيبرانية، وتتضمن كذلك منتدى للنقاش. ومن المتوقع أن يساهم المشروع في تحسين قدرات الدول في مجال سن القوانين الخاصة بالفضاء السيبراني، واعتماد أسس التنسيق الإقليمي للأطر القانونية والتنظيمية المتعلقة بمجتمع المعلومات في الدول العربية.

* * *

# بعض أنماط الجرائم المالية عبر الإنترنت[٥]

لقد أصبح العالم يتحدث عن شبكة اتصالات عالمية لا تكتفي بنقل المواد المرسلة واستقبالها، وإنما تتيح للإنسان التفاعل بكامل حواسه، ومن دون أن يبرح مكانه، مع العالم ومع مستخدمي الفضاء السيبراني في مختلف بقاع الأرض، حيث تنتفي الحدود الجغرافية وتتقلص المسافات. لقد أصبحت الاتصالات صيحة العصر ولغة العالم الجديدة، كما فرضت نفسها على كافة نواحي الحياة الاجتماعية والاقتصادية والثقافية، وأدت لبزوغ عصر جديد هو عصر مجتمع المعلومات الكوني أو عصر المعلومات.

وإزاء هذه التغيّرات الجذرية، بدت الطرق التقليدية لجمع وتنظيم المعلومات عاجزة عن تلبية الاحتياجات من المعلومات بكفاءة وفعالية، وأصبح من الضروري استخدام تقنية علمية متطورة لاستيعاب الفيض الهائل من المعلومات والتعاطي معه. وعلى مدى الأعوام الأربعين الماضية، سعى الباحثون إلى إيجاد حلول مناسبة لاستيعاب الحجم المتزايد من المعلومات عبر مسارين رئيسيين:

- تركيز العديد من دراسات المعلوماتية على تطوير عملية فهم طبيعة المعلومات، ومكوناتها، وكيفية حصرها، وتجميعها، وتبويبها، وتصنيفها، وتحليلها، بهدف الاستفادة منها بأكبر قدر ممكن من الفعالية؛
- التوصّل إلى آليات تقنية متقدمة للتحكم في المعلومات، وتجميعها، ومعالجتها، وتخزينها، واسترجاعها، وتحسين الانتفاع بها.

## الجرائم المالية عبر الإنترنت

لعل من أكثر الجرائم السيبرانية شهرة جرائم الاعتداء على سرية المعلومات وسلامتها والاعتداء على الخصوصية، إلا أن جرائم الإنترنت ليست محصورة في هذا النموذج. وقد تصنف هذه الجرائم حسب اختلاف الهدف المباشر منها، فهناك الجرائم التي تقع **على الإنترنت**، وهي الجرائم التي تكون فيها شبكة الإنترنت نفسها هدف المجرم؛ والجرائم التي تقع **بواسطة الإنترنت**، وهي تلك الأفعال التي تستخدم شبكة الإنترنت كوسيلة لارتكابها، حيث تكون مصلحة المعتدي قيمة مادية أو أدبية أو اجتماعية، تتجاوز حدود جهاز الحاسوب وشبكة الإنترنت نفسها.

والجرائم التي تقع بواسطة الإنترنت هي أيضاً متعدّدة الأوجه والأهداف، فهناك مثلاً الجرائم التي تقع على الأجهزة بهدف تعطيلها أو تخريبها؛ والجرائم التي تستهدف الأشخاص أو الجهات بشكل مباشر، كالتهديد والابتزاز؛ والجرائم المالية، وهي الجرائم التي سنستعرض بعضاً منها في ما يلي.

### جرائم السطو على أرقام بطاقات الائتمان

لقد واكب استخدام بطاقات الائتمان من خلال شبكة الإنترنت ظهور الكثير من المتسللين للسطو عليها. فبطاقات الائتمان تعد أموالاً إلكترونية والاستيلاء عليها يعد استيلاء على مال الغير. ومع انتشار التجارة الإلكترونية، عمدت العديد من شركات الأعمال إلى استخدام الإنترنت لإتاحة خدماتها على الشبكة، بهدف تسهيل العملية التجارية وتوسيع نطاقها وتطويرها. والجدير بالذكر أن الاستيلاء على بطاقات الائتمان ليس بالغ الصعوبة، فلصوص بطاقات الائتمان يستطيعون الآن سرقة مئات الآلاف من أرقام البطاقات في يوم واحد من خلال شبكة الإنترنت، ومن ثم بيع هذه المعلومات للآخرين.

وقد أثبتت شبكة "MSNBC" للتلفزة (http://tv.msnbc.com) مدى سهولة الحصول على أرقام بطاقات الائتمان من الإنترنت، إذ قامت بعرض قوائم تحتوي على أكثر من ٢ ٥٠٠ رقم بطاقة حصلت عليها من سبعة مواقع للتجارة الإلكترونية، وذلك عن طريق استخدام قواعد بيانات متوفرة تجارياً. وليس من الصعب على أي متطفل أو متسلل استخدام هذه الوسيلة للوصول إلى أرقام كهذه والاستيلاء عليها، واستخدامها في عمليات شراء يدفع الثمن فيها أصحاب البطاقات الحقيقيون.

ونحن اليوم في بداية ثورة نقدية يطلق عليها اسم "النقود الإلكترونية"، التي يُتوقع لها أن تكون مكملة للنقود الورقية أو البلاستيكية. فمن المتوقع أن يزداد الاعتماد على هذا النوع الجديد من النقود وأن تحوز في المستقبل القريب الثقة التي تتمتع بها النقود التقليدية. وفي هذا الإطار، يصبح النظر إلى الجرائم التي قد تتعرض إليها النقود الإلكترونية وجميع أنواع الأموال الإلكترونية، بما فيها بطاقات الائتمان، أمراً ضرورياً، إذ على السلطات المعنية أن تصدر التشريعات المناسبة لحماية العمليات التجارية التي تحصل عبر شبكة الإنترنت أو بواسطة أجهزة المعلوماتية المختصة.

## جرائم الاعتداء على الأموال الإلكترونية

الأموال الإلكترونية هي الأموال المتداولة إلكترونياً سواء في إطار التجارة الإلكترونية، أم في إطار عمليات السحب والإيداع في أجهزة الصرف الآلي. وعملية السداد في التجارة الإلكترونية تعتمد على التحويل الإلكتروني للأموال، أو استخدام بطاقات الائتمان الإلكترونية، أو استخدام النقود الإلكترونية. وهذه الأموال، مثلها مثل الأموال المادية، يمكن أن تكون محلاً للسرقة.

ومن صور جرائم الأموال الإلكترونية استخدام بطاقات ائتمان انتهت صلاحيتها، أو بطاقات ملغاة من الجهة التي أصدرتها، أو استخدام بطاقات مسروقة أو مزوّرة. ومن صور جرائم التعدي على الأموال الإلكترونية أيضاً التعدي على أموال الغير بالوسائل الإلكترونية، مثل الدخول إلى مواقع البنوك، والدخول إلى حسابات العملاء، وإدخال بيانات أو مسح بيانات بغرض اختلاس الأموال أو نقلها أو إتلافها.

ففي عام ٢٠٠٣، قامت الولايات المتحدة بالتحقيق في سرقة أرقام ٨ ملايين بطاقة ائتمان من شركة تجارية في حادثة تعد الأخطر من نوعها، بالرغم من تكرار مثيلاتها في فترات لاحقة. وقد اعترفت الشركة التي تجري عمليات تحويل مالية لشركات فيزا وماستر كارد وأمريكان إكسبريس وديسكفر فاينانشال سيرفيسز بتعرضها لاختراق في نظام العمل من طرف خارجي غير مصرح له بالدخول على النظام[٦].

## توصيات

في ظل هذه التغيرات المتسارعة، وأمام التطور المستمر للتجارة الإلكترونية والاعتماد المتزايد عليها في المنطقة العربية، لا بد من القيام بالخطوات التالية، بهدف حماية المستهلكين وتأكيد سيادة القانون وضبطه للمعاملات التجارية كافة:

١- دعوة المشَّرعين العرب في الدول التي لم تصدر التشريعات الخاصة بالجرائم المالية إلى الإسراع في إصدار التشريعات المنظمة للمعاملات المالية الإلكترونية، وبيان العقوبات الرادعة لارتكاب الأفعال غير المشروعة في هذه المعاملات.
٢- دعوة الدول العربية إلى إنشاء "شرطة الإنترنت"، على أن يكون من ضمن مهامها تلقي البلاغات الرقمية ذات الصلة بمنظومة المعاملات المالية الإلكترونية، وتطوير جهات التحقيق والمحاكم بما يتناسب مع التعامل مع الدعاوى القضائية الإلكترونية.
٣- حثّ متخذي القرار في المصارف المركزية العربية على إقرار لوائح وضوابط تنظم العمل في إدارات الأمن المعلوماتي، وتحديث القواعد والأعراف التي تضمن أمن نظم المعلومات في المصارف.
٤- السعي إلى تأهيل وتدريب القائمين على وضع القوانين حول كيفيّة تنظيم المعاملات المالية الإلكترونية.
٥- وضع سياسة لحماية خصوصية البيانات المتداولة في منظومة المعاملات المالية الإلكترونية، وتوعية القائمين على هذه المنظومة بأهمية حماية المحتوى المعلوماتي وخصوصيته، والتعريف ببعض الاستخدامات الخاطئة لتكنولوجيا المعلومات.
٦- تدريب الموظفين حول مفهوم الجرائم المالية التي قد ترتكب على مستوى الشبكات الداخلية أو على شبكة الإنترنت للحد منها ولمكافحتها.

٧- حث مؤسسات المجتمع الدولي المتمثلة في المؤسسات الحكومية والخاصة على رصد الاعتمادات المالية المناسبة لدعم نظم أمن المعلومات، باعتبارها استثمارات ذات دور اقتصادي.

٨- الإسراع في الانضمام إلى الاتفاقية الدولية لمكافحة الجرائم الإلكترونية (بودابست، ٢٠٠١).

٩- تأهيل العاملين في قطاع أمن المعلومات في المؤسسات المالية من أجل حماية المنظومة المعلوماتية، والتعامل باحتراف مع تكنولوجيا المعلومات والاتصالات لتعزيز الاستفادة من الخدمات المالية.

١٠- العمل على إصدار نشرات خاصة بالمعاملات المالية الإلكترونية وقواعدها وجرائمها، والقيام بدراسات مشتركة بين الهيئات الحكومية المعنيّة.

١١- تبادل الخبرات والتجارب بين المؤسسات المالية الوطنية والإقليمية حول التصدي للاستخدامات غير المشروعة في المعاملات المالية الإلكترونية.

١٢- نشر الوعي حول الاستخدام الآمن للبطاقات الائتمانية.

* * *

# دور السلطات في عمليات اختراق الشبكات الإلكترونية[٧]

يتسم عصر المعلوماتية بازدياد الاعتماد على شبكات أجهزة الحواسيب السلكية واللاسلكية وشبكة الإنترنت، مما يجعلها أكثر انفتاحاً على المجتمع، وبالتالي أكثر تعرضاً للمخاطر. وتعتبر عمليات الاختراق لنظم تكنولوجيا المعلومات والاتصالات (Hacking) من أهم الأعمال التي تستهدف هذه الشبكات، ويمكن تصنيف مخترقي الشبكات (Hackers) إما بالمخترقين الهواة الذين يرغبون بإظهار مهاراتهم التقنية العالية، أو بالناشطين المخترقين (Hacktivist) الذين يستخدمون الهجمات الحاسوبية لأغراض سياسية، أو دينية، أو اجتماعية، أو حتى اقتصادية. فهم يطبقون تقنيات الاختراق على مواقع محددة من الإنترنت للتأثير على عملها، من دون إلحاق أضرار كبيرة بها. ومن الأمثلة على هذا النوع من الاختراقات نذكر القنابل المؤتمتة عبر البريد الإلكتروني، والفيروسات، وهجمات رفض الخدمة (Denial of Service DoS)، التي تعني الهجوم المشبع على موقع معين مما يزيد الحمل على المخدِّمات بسبب الطلبات المتكررة إلى نحو يفوق قدرة هذه المخدمات على الاستجابة، مما يسبب بانهيار النظام لعدم قدرته على أداء عمله على النحو المصمم لأجله.

ومفهوم الاختراق هذا أخذ بالتطور ليشمل ما يسمى بالـ "Hacktivism"، وهو نوع من أنواع العصيان المدني الإلكتروني الذي يعمل من خلاله بعض الناشطين على اتخاذ إجراءات اختراق مباشرة لأنظمة حاسوبية خاصة بالحكومات أو الشركات، وذلك كعمل من أعمال الاحتجاج[٨]. وتجدر الإشارة بأن التداول بمفهوم الـ "Hacktivism" قد بدأ منذ عام ١٩٩٦، حيث عرف بأنه الاستخدام الشرعي و/أو غير الشرعي لبعض الأدوات الإلكترونية في سبيل السعي لتحقيق غايات سياسية. وتشمل هذه الأدوات مهاجمة مواقع الإنترنت، أو إعادة التوجيه من موقع إلى آخر، أو هجمات رفض الخدمة، أو سرقة المعلومات، أو السخرية على مواقع معينة، أو حتى الاعتصامات الافتراضية. وفي عصرنا هذا، وفي أغلب الأحيان، أصبح المقصود بمفهوم الـ "Hacktivism" كتابة وتطوير برمجيات خاصة من أجل تعزيز ودعم حرية التعبير، وحقوق الإنسان، والأخلاقيات في تداول المعلومات.

## أخلاقيّات الاختراق[٩]

استخدم مصطلح "الاختراق" لأول مرة في عام ١٩٧٠، وكان التركيز في استعماله على القدرات البرمجية الاستثنائية التي يملكها المخترق. أما اليوم، فأصبح الاختراق يعتبر عقليّة تخضع غالباً لمبادئ يشترك فيها المخترقون، وأهمها الدفاع عن حق الوصول غير المحدود إلى أجهزة الحاسوب، وعن مجانية المعلومات، وعن إمكانية التكنولوجيا في تحسين حياة الناس.

وقد استحدثت أيضاً مصطلحات للتعبير عن "أخلاقيات الشبكة" (Nethic أو Netethic)، التي يتحلّى بها من يناضل من أجل الحرية الكاملة في التعبير، وحماية خصوصية الأفراد، والاهتمام بالمصلحة العامة وخاصة بمصلحة الفئات

© oigro - Fotolia.com

المهمشة في المجتمع، واعتبار الدفاع عن حقوق هذه الفئات غاية في حد ذاتها.

ومن البديهي أن نقول أن أعمال المخترقين لا تحترم كلها مبادئ وأخلاقيات إجابية، فمن المخترقين من يرتكب جرائم ضد الأفراد والمؤسسات هدفها السرقة أو الإساءة البحتة. وبالطبع، يختلف تقييم أعمال الاختراق مع اختلاف وجهات النظر لدى المقيمين، إلا أن الأساليب المعتمدة من قبل المخترقين تضع هذه الأعمال في خانة الجرائم السيبرانية. لكن من الصعب أحياناً تحديد هوية فاعليها، ويرجح الخبراء أن السلطات نفسها التي توقف المخترقين تارة، تتحول إلى الجهة المخترقة طوراً، عندما تتمكن بذلك من تحقيق أهداف تناسب سياستها. وهذا ما يجعل من موضوع أخلاق الاختراق موضوعاً في غاية الأهمية، لن تستنفد هنا كل أوجهه.

## عينات من حملات الناشطين المخترقين

اتخذت حملات الناشطين المخترقين للشبكات العديد من الجوانب والأشكال، فمنها ما نُظم ضد حكومات، أو منظمات عالمية، أو شركات تجارية، أو مجموعات دينية، أو حتى شخصيات عامة. والدافع الرئيسي من تلك الحملات هو عدم توافق أعمال وأفكار المستهدفين مع مبادئ الناشطين. فالناشطون في الاختراق يعارضون الرقابة على الإنترنت، والحملات ضد القرصنة الرقمية، واستعمال الإنترنت لغايات غير أخلاقية كالتعدّي الجنسي على الأطفال. وفي ما يلي سرد عن بعض العمليات التي قاموا بها في هذا الإطار.

### عملية الاسترداد[١٠] (Operation Payback)

في عام ٢٠١٠، واجه موقع ويكيليكس (Wikileaks) مشاكل متعددة، ومنها إغلاق خدماته على الإنترنت وتجميد حساباته المصرفية، وذلك للتضييق عليه إجرائياً ومالياً. وقد اعتبر عدد من الناشطين المخترقين أن هذه الإجراءات ضد ويكيليكس هي اعتداء على الحرية عموماً، وعلى حرية التعبير عن الرأي بالتحديد، فقرروا الدفاع عن الموقع بإجراءات مضادة. والجدير بالذكر أن موقع ويكيليكس كان قد تعرض لهجمات من قبل ناشطين لا يروق لهم عمله، وهذا يدل على أن هناك فئات مختلفة من الناشطين لا تعمل كلها للغاية نفسها ولا تتشارك في المبادئ والأخلاقيات.

أما "عملية الاسترداد"، فاستهدفت الكيانات التي شددت الخناق على ويكيليكس، ومنها المصرف السويسري الذي جمد أصول مؤسس الموقع جوليان أسانج، وخدمة بايبال (PayPal) التي قطعت باب رزق الموقع بإغلاقها باب التبرعات. وقد استخدم الناشطون في هذه العملية حواسيبهم الخاصة، خلافاً لعمليات الاختراق الأخرى التي يجري فيها استخدام شبكات حواسيب يسيطر عليها مسبقاً وتجري عمليات الاختراق من خلالها بدون معرفة أصحابها (Botnets).

### عملية تونس (Operation Tunisia)

وفي تونس في أوائل سنة ٢٠١١، ارتأى عدد من الناشطين أن الحكومة التونسية تضيق الخناق على مستخدمي شبكة الإنترنت، وتتجسس عليهم، وتسرق أسماءهم وكلمات المرور السرية التي يستعملونها، وتمارس رقابة شديدة على نشاطاتهم على الإنترنت. وهذه الرقابة قد تصل أحياناً إلى إغلاق المواقع أو إلغاء المدونات الإلكترونية، ومنع الناشطين من الولوج إلى مواقع الحكومة التونسية. فعمد هؤلاء الناشطون إلى وضع برامج تهدف إلى التهرب من الرقابة الحكومية. وتجدر الإشارة إلى أن عدة عمليات شبيهة قد حصلت أيضاً في مصر وليبيا، وذلك للأسباب والغايات نفسها.

© mario beauregard - Fotolia.com

## تعامل السلطات مع الناشطين المخترقين

مهما كانت الأسباب المبررة لأعمال الناشطين، وإن كانت هذه الأهداف نبيلة، أو تندرج ضمن إطار الغيرة على المصلحة العامة، فإن الأساليب التي يستخدمها هؤلاء للوصول إلى غاياتهم يمكن تصنيفها بالإجرامية. ففي أغلب الحالات، ينتج عن أعمال الناشطين تعطيل للخدمات على شبكة الإنترنت، وهذا ما يحصل بعد هجمات رفض الخدمة الموزعة (Distributed Denial of Service). وإذا كان المستهدف شركة تجارية أو مصرفية، فغالباً ما تتكبّد خسارات مالية يمكن أن تكون جسيمة. أما التشويش على المواقع الإلكترونية للقطاع العام، فهو يعطل خدمات يمكن أن تكون حيوية للمواطنين.

ومن الصعب على السلطات أن تتقبل التبريرات لهذه الأعمال، حتى ولو أظهرت في بعض الأحيان تفهماً لأسبابها. فإذا تُركت الأمور بدون أي ملاحقات قانونية، تكون النتيجة الأكيدة الفوضى العارمة. وإن الوصول إلى مرحلة تتيح لكل مستخدم للإنترنت أخذ زمام الأمور بيده خطير جداً، إذ يكون هذا كناية عن سيادة شريعة الغاب وعن تغييب للسلطات الشرعية.

ولذلك، فإن ردة فعل السلطات الهولندية على عملية الاسترداد كانت توقيف شاب لا يتعدى السادسة عشرة من العمر[١١]، وذلك لمشاركته في هجمات إلكترونية على شركات بطاقات التأمين مثل فيزا وماستركارد، وشركات الدفع مثل بايبال. وأوقفت السلطات البريطانية[١٢] أيضاً خمسة رجال اشتركوا في هذه العملية. أما السلطات الأمريكية، فاكتفت بتنفيذ ٤٠ مذكرة تفتيش دون توقيف أحد، ولكنها ذكرت الجمهور بأن القيام بهذا النوع من الأعمال يعرض المسؤول للملاحقة القانونية ولعقوبات يمكن أن تصل إلى السجن لمدة عشر سنوات.

أما في ما يخص عملية تونس وعملية مصر، فقد أوقفت السلطات الإسبانية ثلاثة إسبانيين اتهمتهم بالمشاركة في عمليات التشويش التي حصلت على مواقع الحكومات التونسية والمصرية وغيرها[١٣].

## استخدام السلطات أساليب الناشطين

محاكمة السلطات للناشطين المخترقين للشبكات المعلوماتية ومعاقبتهم تدل على أنها تعتبر أعمالهم غير قانونية. وإذا سلمنا جدلاً أن السلطات تستعمل هذه العقوبات كعملية ردع لضمانة عدم تعطيل خدمات الإنترنت، فكيف يمكننا تفسير استخدام هذه السلطات نفسها أساليب الناشطين لتحقيق غايات سياسية؟

ولعل الخبر الأكثر انتشاراً في هذا الإطار يتعلق بمرافق تخصيب اليورانيوم في إيران، فقد تعرضت هذه المرافق لهجمات إلكترونية متعددة في السنوات الأخيرة. وفي مقال نشر في صحيفة نيويورك تايمز في الأول من حزيران/يونيو ٢٠١٢[١٤]، كشف الكاتب أن باراك أوباما، رئيس الولايات المتحدة الأمريكية، أمر سراً بتكثيف الهجمات الإلكترونية على أنظمة الحواسيب التي تدير مرافق تخصيب اليورانيوم الرئيسية في إيران، وأن هذه الهجمات الإلكترونية كانت قد بدأت على عهد الرئيس جورج بوش، ولقبت بـ "الألعاب الأولمبية". وسلط الضوء على أن الأمر بتكثيفها أتى بعدما كشف عنصر من عناصرها عن غير قصد، وذلك بسبب خطأ حصل في برنامجها وأدى إلى خروجها عن نطاقها، أي عن المرافق الإيرانية المذكورة آنفاً. ونقل الكاتب أيضاً آراء الخبراء الذين درسوا طبيعة هذه الهجمة وحددوا أنها كانت من نوع الدودة (worm)، وأعطوها إسم "ستاكسنت" (Stuxnet). وكشف الخبراء أن الغاية من ستاكسنت كانت اختراق شبكات المرافق النووية الإيرانية للتجسس عليها وتعطيل عملها، وقدروا دون الجزم أنها طورت من قبل الولايات المتحدة بالتعاون مع إسرائيل.

والجدير بالذكر أن تأكيد وجود ستاكسنت كحقيقة ثابتة غير ممكن، إذ إن السلطات الأمريكية تتعامل مع هذه العملية بسرية، لكن الخبراء يميلون إلى تأكيد صحة وجودها. وتختلف الآراء حول مدى فعالية هذه الهجمات الإلكترونية، إذ قد مضت إيران قدماً بتطوير تجهيزاتها النووية بعد هذه الهجمات المزعومة، لكن هذا لا ينفي حصول هذه الهجمات ولا يحدد مدى فعاليتها. ولعل الدليل غير المباشر على وجود هذه الهجمات أتى من إيران نفسها، التي نفت

وقوعها بداية لتعود وتعترف به لاحقاً. وأعلنت إيران أيضاً خلال سنة ٢٠١١ عن إنشاء وحدة خاصة لمكافحة الهجمات الإلكترونية، قد تستخدم أيضاً لشن هجمات على شبكات إلكترونية تعدها عدوة. ولكن لم يثبت وجود هذه الوحدة حتى الآن.

وفي لبنان، في شهر آب/أغسطس ٢٠١٢، كشفت شركة كاسبرسكي لاب (Kaspersky Lab) الروسية التي تعمل في مجال الأمن الإلكتروني عن فيروس إلكتروني تمكن من اختراق النظام المصرفي اللبناني ووصل إلى حسابات الآلاف من الزبائن. كما تبينت إمكانية استخدام هذا الفيروس للتجسس على البريد الإلكتروني ومواقع التواصل الاجتماعي[١٥]. وأطلقت كاسبرسكي لاب عليه اسم غاوس (Gauss)، وذلك تيمناً باسم عالم الرياضيات الألماني وإشارة لأهم مكوّن من مكونات هذا الفيروس البرمجية. وأعلنت كاسبرسكي لاب أن الفيروس يمكنه أيضاً مهاجمة البنى التحتية الإلكترونية وأشارت أنه طور من قبل الذين كانوا قد أنتجوا ستاكسنت، الدودة المذكورة أعلاه.

ويختلف هذا الفيروس عن غيره من الفيروسات المشابهة، وذات الصلة بعمليات الاحتيال المالية التي تحصل عادة على الإنترنت ويكون هدفها الكسب المالي. وهذا قد يشير إلى أن مصممي لا ينتمون إلى المنظمات الإجرامية التي تستهدف عادة أكبر عدد من الضحايا لتحقيق أكبر قدر من المكاسب المالية. ويعتقد الخبراء أن منتجي هذا الفيروس قد يكونوا هم نفسهم الذين أنتجوا ستاكسنت وأمثاله من الفيروسات والديدان[١٦].

وفي النهاية، لا يمكن تبرير القيام بالهجمات الإلكترونية حتى ولو حققت هذه الهجمات بعضاً من أهدافها، وحتى وإن كانت الوسائل الإلكترونية تتيح الوصول إلى أهداف صعبة المنال باستعمال الأساليب التقليدية. فالقيام بمثل هذه الهجمات الإلكترونية حافل بالأخطار، ويمكن أن يؤدي إلى نتائج غير متوقعة. من الممكن مثلاً أن يصمم فيروس ما للهجوم على أهداف معينة ولكن، نتيجة ضعف أو خلل في التصميم، قد ينتشر هذا الفيروس في عدد كبير من الشبكات. ويمكن تطبيق هذا المثل على فيروس غاوس الذي صمم حسب الخبراء لتكون ضحيته المصارف اللبنانية. فهذا الفيروس تم اكتشافه في عدة مئات من الحواسيب في إسرائيل، التي قد تكون أحد مواطن إنتاجه. وبالتالي يتوجب على الناشطين والسلطات المنتجة للأدوات التي تُستخدم في الهجمات الإلكترونية أخذ احتمال ارتداد هذه الوسائل عليهم بالاعتبار، فهم أكثر عرضة من غيرهم لأنهم من يستخدمون الوسائل الإلكترونية بكثرة في عملهم.

* * *

# HACKTIVISM: AT THE CROSSROADS OF PRESS FREEDOM, HUMAN RIGHTS AND NATIONAL SECURITY[1]

## Hacktivists: Public vigilantes or public nuisance?

Hacktivism is a controversial subject: for some, it represents a vehicle for progress and positive change; for others, it represents an obstacle and a threat. It is associated with criminality and anarchy on the one hand, and with freedom and human rights on the other hand. Hacktivism has existed in one form or another since the late 1980's, although the term 'hacktivism' is itself relatively new. In 1989, an Australian group was identified as responsible for the computer virus Worms Against Nuclear Killers, which attacked the computer systems of the National Aeronautics and Space Administration and the United States Department of Energy.[2] The attack coincided with anti-nuclear protests over the launch of Galileo, a plutonium-powered spacecraft, and the message which appeared on the screens of infected computers read, "You talk of times of peace for all, and then prepare for war".[3] This attack is regarded as the first clear act of hacktivism, defined as an amalgamation of computer hacking and political activism.

While the term 'hacktivism' describes a set of activities rather than an ideology, hacktivists claim to operate in the public interest, using technology to defend human rights, freedom of information and the freedom of the Internet. But their lack of a transparent structure can make them seem just as intransigent as the corporations and state institutions they target. In the 2012 Data Breach Investigations Report published by Verizon, hacktivism accounted for 58 per cent of all data stolen in 2011. The Report goes on to say that in the same year, hacktivists were responsible for a larger percentage of data breaches (35 per cent) than traditional organized crime groups.[4]

### WikiLeaks

In November 2010, WikiLeaks collaborated with major global news organizations to release redacted cables from the United States Department of State. WikiLeaks, alongside the whistle-blowers and media outlets involved, claimed to be acting in the public interest. But the reactions of the United States and foreign Governments were hostile, and public responses were at best mixed. Many objected to the release of sensitive documents, highlighting the potential threat to national security and the exposure of innocent people that were identified in them.

The WikiLeaks example illustrates the fine line that is emerging between the freedom of the press and national security, with advocates on either side using the grey areas to their advantage. The stated objectives of WikiLeaks are similar to those of many other hacktivist groups, but WikiLeaks has sought to operate largely within the accepted bounds of bureaucracy and institutions. It does so by citing the public's right to information under the legislation related to the freedom of information, and through its partnerships with respected mainstream news organizations.

### Anonymous

Of the many different groups and individuals that fall under the hacktivist banner, the initiative known as Anonymous is by far the most prolific and popular. In its 2012 'Time 100' poll, Time magazine readers voted Anonymous the most influential entity in the world.[5]

Anonymous has a very particular membership and affiliation structure, which makes it exceedingly easy for an individual or group to aid or participate in its activities, while making it almost as difficult for those people to be identified in isolation. In essence, Anonymous is composed of many different online communities which act collectively to target specific organizations. It is a type of decentralized network with no clear leadership, united by a shared goal or outcome. In the McAfee white paper "Hacktivism: Cyberspace has become the new medium for political voices", Anonymous is described as a 'meme' which can be adopted by its members and affiliates in order to act incognito.[6] The paper noted that the online chat rooms frequented by Anonymous members reached a peak of 3,000 simultaneous connections during the Arab uprisings and 'Operation Payback'.[7] Its members include computer programmers who actively hack sites and inject malicious code, as well as others who contribute to conversations on the morals and ethics of selecting a target, or who simply download software that enables their machines to be used by other members when launching attacks. One example of an attack that relies on this kind of passive participation is a Distributed Denial of Service (DDoS) attack, which involves saturating a target website with traffic until the server falls offline. This helps to illustrate the loose structure, lack of accountability and lack of hierarchy that characterize Anonymous.

On 19 June 2011, operation AntiSec was jointly launched by Anonymous and LulzSec, another hacktivist cell. The targets were Governments, law enforcement agencies and organizations perceived by hacktivists as limiting individual freedoms. Such initiatives were a cause for concern for both hacktivists and non-hacktivists, particularly given the fact that hacktivist ideals were at times contested and challenged by the same individuals who approved of them in the context of other initiatives.

One of the dangers of the hacktivist label is that it provides an ideal cover for illicit cyberattacks that do not mean to defend any human right. Remaining anonymous works both for and against the hacktivist culture, given that those other hackers may operate outside the generally accepted ethical framework of hacktivists, while claiming to represent the community. Meanwhile, activists who do stand for legitimite rights are often ignored or even arrested once they are perceived as having taken 'extreme' actions such as hacking. Authorities sometimes take advantage of this situation to push their own political agenda through fear-mongering, especially fear of the unknown. Indeed, fear of hackers can multiply exponentially, given the scale and potential reach of groups like Anonymous.

## State-sponsored hacktivism?

The umbrella of national security has always provided a convenient cover for the state, allowing it to operate in secret with the justification of acting in the interests of public safety and security. Recently, States have also begun to enter the hacktivist fray. New computer worms like Stuxnet, Duqu, Flame and Gauss have caused alarm, prompting many countries and corporations to rethink their strategies to cyberwarfare. Some of these worms were designed to attack state targets, such as Iranian nuclear facilities, Saudi Arabian oil refineries and Lebanese banks accused of laundering money for Iran. Many of these worms have in fact been linked to the same group of developers through similarities in their coding. While these attacks could be attributed to hacktivists at first glance, upon closer inspection researchers determined that they were most likely

state-sponsored, given the sophistication and scale of the coding involved.[8]

## Rights, freedoms and national security in the digital age: The Arab region in focus

The link between cyberactivity and public security has been clearly demonstrated by the events of the Arab uprisings. During these events, some Governments accused online communities of disrupting national stability through their facilitation of public protests, while many of these forums claimed that they were making legitimate demands for improvements to government transparency, employment opportunities and the promulgation of civil rights and freedoms. As will be illustrated below, however, the online struggle for rights and freedoms in the Arab region is not easily separated from the imperatives of national security and stability. Ultimately, an integrated approach to addressing these issues must be developed by the Governments of the region.



The 2011-2012 Press Freedom Index (PFI), compiled annually by Reporters Without Borders, shows a significant decline in press freedom in the Arab region relative to global rankings. The official Press Release that accompanied the 2011 PFI described the results of the Arab uprisings as "mixed": increasing crackdown in some countries alongside great leaps for press freedom in others. Compared to the 2010 PFI, six countries rose in the ranks (Kuwait, Libya, Oman, Qatar, the Sudan and Tunisia), four dropped significantly (Bahrain, Egypt, Lebanon and the United Arab Emirates), and the remaining seven saw their ranking drop moderately. Many of these changes can be directly attributed to the popular uprisings that broke out across the region in 2011. Reported crackdowns on popular movements, trials of human rights activists, state violence, censorship, surveillance and, in some cases, government manipulation of journalists were all taken into account when PFI was compiled.

Countries in the Arab region should be aware that they may be viewed by hacktivists as potential targets. Their perceived lack of support for press freedom and human rights, alongside the increasing sophistication and popularity of hacktivism, create a serious risk of attracting hacktivist attention. In some cases, political activism or cybercrime could be perpetrated under the guise of upholding the freedom of expression or the right to information, as the WikiLeaks example illustrates. These activities will continue to expand and gain sophistication, given the ever-evolving technological arsenal and increasing human resources available to hacktivist cells.

ESCWA member countries should take stock of the lessons learned since the establishment of WikiLeaks and its public exposure of sensitive and confidential documents. Many hacktivists thrive on the culture of confidentiality that surrounds

government administrations, because it enables a straightforward use of their talents as divulgers of sensitive information. Governments may consider providing public access to more information and documentation as a form of counter-exposure. They may even wish to reconsider the classification of some confidential documents as a way of pre-empting hacktivists and undermining their value in the public eye. Any act seeking to disrupt the stability of a Government that is acknowledged as open and transparent would be understood by the public as a legitimate cause for concern. It will better serve both public interest and national security if space is made for civil dialogue and interaction with the government, and for civil participation. Here technology can play a key role in providing an open and accessible environment, while maintaining some form of peer moderation.

## Conclusion

Given the evolution of journalistic practices; the perception of poor human rights records in some ESCWA member countries; the significance of hacktivism and the trend towards its alignment with traditional media frameworks; and the ever-increasing sophistication of hacker technology, there is a growing possibility that those countries may face a threat to their national security posed by hacktivists. This is particularly true in cases where conventional media outlets are perceived by the general population to be biased or inaccessible; where hacktivism is viewed in a positive light and where its technologies are accessible; where individual freedoms and human rights laws are not enforced; and where a belief already exists that collective action could achieve the desired changes to the political structure.

Taking pre-emptive measures against the exposure and threats caused by hacktivism, government institutions may be well-advised to consider making their administrations more transparent and open in general. Such reforms would certainly be in keeping with current information transparency trends, and would render the work of many hacktivists largely obsolete.

❋ ❋ ❋

# سياسات تكنولوجيا المعلومات والاتصالات

## إطلاق أول مؤشر عالمي لقياس الوب[١]

يصعب قياس مجتمع المعلومات وتقييمه بدقة، حيث طبيعة الأنشطة والمنتجات غير ملموسة، وذلك على عكس قياس الأنشطة الاقتصادية. فالعلاقة بين السبب والنتيجة هي علاقة غير واضحة في مجتمع المعلومات، إذ لا يؤدي ارتفاع نسبة انتشار تكنولوجيا المعلومات والاتصالات بالضرورة إلى فوائد اقتصادية مباشرة يمكن قياسها بطريقة واضحة ومحددة.

ومن أجل قياس مجتمع المعلومات، قد يبدو كافياً قياس وضع تكنولوجيا المعلومات والاتصالات الدائمة التطوّر. غير أن بعض الدراسات أظهرت أن رصد عدد الحواسيب الموصولة بالإنترنت لا يعكس بالضرورة حقيقة الوضع بالنسبة لاستخدام الإنترنت أو المحتوى الذي يتم النفاذ إليه. والواقع أن تقييم مجتمع المعلومات ينبغي أن يتخطى قياس انتشار الأدوات التكنولوجية ليتناول السياق الاقتصادي والاجتماعي لمستخدمي التكنولوجيا[٢].

والجدير بالذكر أن العقد المنصرم قد شهد تطوير نماذج عديدة هدفت جميعها إلى قياس مجتمع المعلومات، لكنها لم تتمكن فعلاً إلا من قياس بعض من أوجهه، نظراً لصعوبة تحديد جميع عناصره. وفي هذا السياق وفي عام ٢٠١٢، أطلقت مؤسسة شبكة الوب العالمية[٣]، التي أنشئت من قبل تيم بيرنرز لي مخترع الوب عام ٢٠٠٩، أول مؤشر عالمي متعدد الأبعاد يعنى بقياس الوب من حيث نموه، ومنفعته لمستخدميه، وتأثيره على عامة الناس وبلدان العالم[٤].

### قياس الوب

تنحصر غالبية الجهود العالمية لقياس الوب اليوم بعملية القياس الكمي، مثل إحصاء عدد مستخدمي الإنترنت، وسرعة النفاذ إلى الوب، وعدد مشتركي الإنترنت بالحزمة العريضة. وتغطي بعض هذه الجهود الأثر الاقتصادي للوب. وقد اعترف مخترع الوب نفسه أنه من أجل تحسين قياس التقدم في تطوير شبكة إنترنت أكثر انفتاحاً وذات مغزى، ومن أجل تحقيق الوب لكامل إمكاناته كأداة يمكنها المساهمة في رفع مستويات المعيشة، والحد من الصراعات وتحسين الحكم والرفاه، ينبغي فهم كيفية تأثير الوب على الصعيد الاجتماعي والتنموي والاقتصادي والسياسي في كافة بلدان العالم.

ويسعى مؤشر الوب إلى تعميق الفهم لكيفية تسخير البلدان لأثر هذه الأداة القوية، من خلال دراسة إحصائية تجمع البيانات حول أبعاد الوب المختلفة وتتيحها مجاناً للجميع. ويمكن لنتائج هذه الدراسة أن تستخدم من قبل صانعي القرار في القطاع العام، والأوساط الأكاديمية، والمنظمات غير الحكومية، وحتى قطاع تكنولوجيا المعلومات والاتصالات نفسه. ويغطي الإصدار الأول من مؤشر الوب هذا، والذي من المزمع نشره سنوياً، ٦١ بلداً من البلدان النامية والمتقدمة، من بينها ستة بلدان عربية أعضاء في الإسكوا؛ وتتضمن مؤشراته تقييماً لأثر الوب السياسي والاقتصادي والاجتماعي، بالإضافة إلى مؤشرات حول علاقة الترابط بين شبكة الإنترنت والبنية الأساسية للاتصالات. ويتيح مؤشر الوب إجراء مقارنات بين الاتجاهات على مر الزمن (comparison of trends) وقياس الأداء بين البلدان، وتسهيل الفهم للقيمة المضافة التي يقدمها الوب للعالم.

### تركيبة مؤشر الوب

يُقيّم المؤشر جاهزية الوب واستخدامه وأثره، وذلك من خلال مقاييس ومؤشرات مختلفة في كل من هذه المحاور

الثلاثة. ويُخصص مؤشر فرعي لقياس كل محور، يتألف بدوره من عناصر عدة، تتشكل هي أيضاً من مجموعة من المؤشرات قوامها ٨٥ مؤشراً. ويتم تخصيص وزن لكل من المؤشرات الفرعية والعناصر المرتبطة بها لتحديد قيمتها واحتسابها. ويبين الشكل التالي تركيبة مؤشر الوب، وعناصره، وأوزان مؤشراته الفرعية.

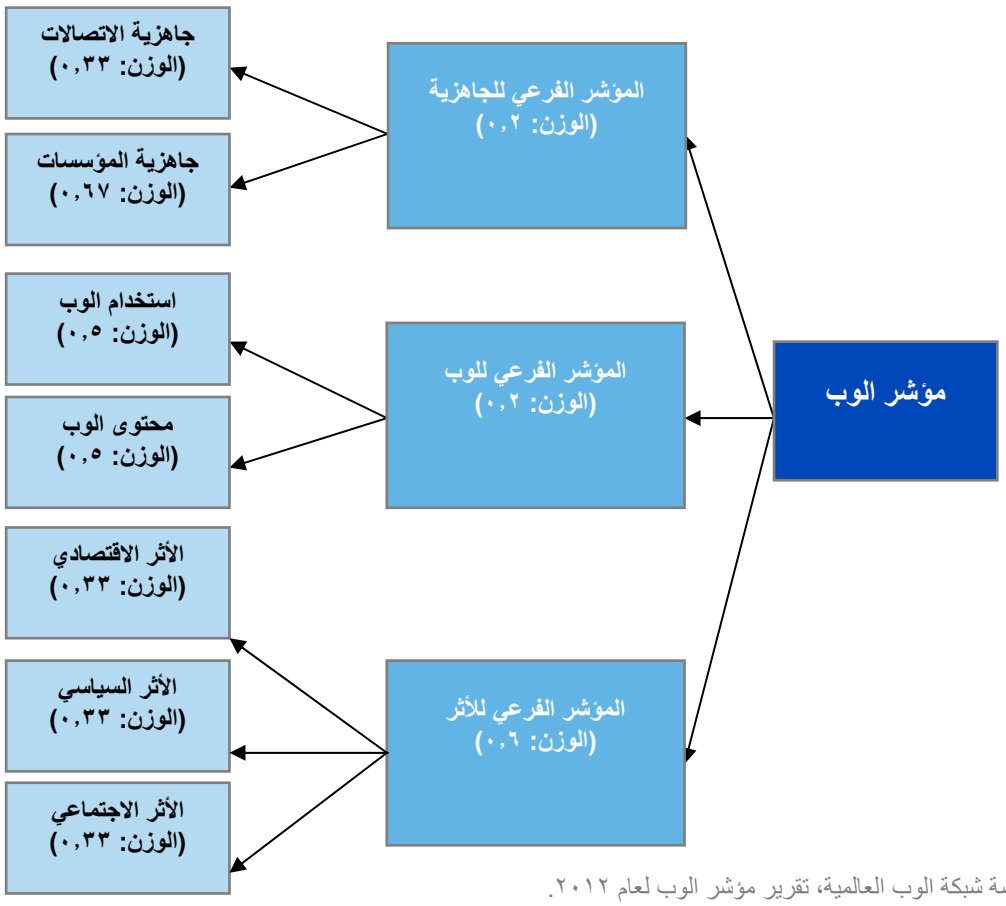
**جاهزية الوب:** هو مؤشر فرعي لقياس نوعية البنية الأساسية للاتصالات ومدى تطورها، إذ هي التي تمكّن من النفاذ إلى الإنترنت. ويتناول المؤشر أيضاً الآليات المؤسسية التي تشمل سياسات النفاذ إلى الإنترنت، وبناء المهارات، ومستويات التعليم التي تُمكن من الاستفادة الكاملة من الوب. ويتألف هذا المؤشر الفرعي من عنصرين:

١- البنية الأساسية للاتصالات: يقيس هذا العنصر عدة عوامل مرتبطة بتكنولوجيا الاتصالات كنصيب الفرد من عرض الحزمة الدولية للإنترنت، وعدد المشتركين في خدمة الإنترنت بالحزمة العريضة، واشتراكات الهاتف النقال، وكلفة النفاذ إلى شبكة الإنترنت.

٢- الآليات المؤسسية: في حين يقيس عنصر البنية الأساسية للاتصالات تقنيات النفاذ إلى شبكة الإنترنت، يقيم عنصر الآليات المؤسسية مدى الدعم الذي تقدمه المؤسسات الخاصة والمنظمات الحكومية لتعزيز النفاذ إلى شبكة الإنترنت، بما في ذلك المحتوى الذي تتيحه هذه المؤسسات والمنظمات على الشبكة. ولحساب هذا العنصر، تُجمع البيانات المتعلقة بحرية الصحافة والرقابة العامة، والتعليم، وانفتاح الحكومة على مشاركة المعلومات.

**الوب:** يقيم هذا المؤشر الفرعي نوعية المحتوى على شبكة الإنترنت، فضلاً عن أعداد مستخدمي الإنترنت في بلد معيّن. ويتألف هذا المؤشر الفرعي من عنصرين: استخدام الوب ومحتوى الوب.

**تركيبة مؤشر الوب وأوزان مؤشراته الفرعية**




المصدر: مؤسسة شبكة الوب العالمية، تقرير مؤشر الوب لعام ٢٠١٢.

١- استخدام الوب: يشتمل هذا العنصر على مؤشرات وبيانات حول نسبة الأشخاص الذين يستخدمون الإنترنت، فضلاً عن مؤشرات النفاذ إلى الوب لذوي الاحتياجات الخاصة، ومنهم كبار السن، وذوي التحصيل العلمي المتواضع.

٢- محتوى الوب: يستند حساب هذا العنصر إلى بيانات حول عدد المقالات المنشورة على ويكيبيديا (Wikipedia) لكل لغة، بسبب صعوبة الحصول على بيانات موثوقة ومتسقة من قبل البلدان حول عدد الصفحات على شبكة الإنترنت باللغات المختلفة.

**أثر الوب**: هذا المؤشر الفرعي أُعطي الوزن الأكبر، وهو ما يمثل نسبة ٦٠ في المائة من مجموع نقاط مؤشر الوب (مقارنة بـ ٢٠ في المائة لكل من المؤشرين الفرعيين "جاهزية الوب" و"استخدام الوب"). وإلى حد ما، يعكس هذا المؤشر الفرعي فائدة الوب وقيمته، فضلاً عن أثره على الناس والبلدان. ويتألف هذا المؤشر الفرعي من ثلاثة عناصر تعنى بقياس آثار الوب على الصعيد الاجتماعي، والاقتصادي، والسياسي.

١- الأثر الاجتماعي: لتحديد الأثر الاجتماعي للوب، تم اعتماد عدد من المؤشرات بما في ذلك استخدام الشبكات الاجتماعية، واستخدام شبكة الإنترنت لنشر معلومات هامة حول الصحة العامة، وتوفر خدمات التعلم الإلكتروني، وأثر تكنولوجيا المعلومات والاتصالات على النفاذ إلى الخدمات الاجتماعية الأساسية.

٢- الأثر الاقتصادي: يقيم هذا العنصر مدى تأثير الوب على قطاعي الاقتصاد والأعمال في بلد ما. وتشمل المؤشرات المستخدمة لحسابه مدى نشر المعلومات الخاصة بالمزارعين من قبل الحكومات والمنظمات، ومدى استخدام الإنترنت في الأعمال التجارية، ومدى ثقة الناس في استخدام الوب كوسيلة لإجراء عمليات بيع وشراء السلع والخدمات. ويشمل هذا العنصر أيضاً مؤشرات حول الجرائم السيبرانية في البلدان، وفق معلومات تم استقاؤها من المسوح الوطنية التي أجراها خبراء مؤسسة شبكة الوب العالمية. وقد لحظ التقرير صعوبة الحصول على بيانات موثوقة حول الجرائم السيبرانية من قبل البلدان، فقد تم جمعها من مصادر ثانوية، وأمل التقرير بإتاحة المزيد من هذه البيانات في المستقبل.

٣- الأثر السياسي: يقيم هذا العنصر مدى استخدام الأحزاب السياسية للإنترنت من أجل التعبئة العامة وإجراء الحملات الانتخابية، فضلاً عن استخدام تكنولوجيا المعلومات والاتصالات لتعزيز الكفاءة الحكومية والمشاركة عبر الوسائل الإلكترونية.

## منهجيّة العمل

مؤشر الوب هو مؤشر مركب يختصر في رقم واحد أثر الوب والقيمة المستمدة منه في مختلف بلدان العالم. وقد واجهت عملية تطويره تحديات كبيرة، وخاصة بشأن محاولة تحديد وقياس بعض الأبعاد الاجتماعية والسياسية التي يغطيها المؤشر.

وقد استُخدم نوعان من البيانات: البيانات المتوفرة والمتاحة من قبل مزودي البيانات (أو البيانات الثانوية)، وبيانات جديدة أخرى قد تمّ جمعها بواسطة استبيانات تم تصميمها خصيصاً من أجل حساب مؤشر الوب في عدد من البلدان (أو البيانات الأولية). وقد عمد الأخصائيون إلى استخدام بيانات غير مباشرة (aproxy dat) عند الضرورة. ومن المتوقع أن تملأ البيانات الأولية بعض الثغرات الموجودة في قياس منفعة وأثر الإنترنت في مختلف البلدان. ويعتبر استخدام البيانات الأولية إحدى الجوانب المبتكرة في الإصدار الأول من مؤشر الوب، إذ تلعب هذه البيانات دوراً ملحوظاً في بناء المؤشر لأنها تمثل نحو ٦٠ في المائة من مكوناته.

وبما أن مؤشر الوب يغطي ٦١ بلداً من البلدان المتقدمة والنامية، فقد عانت مؤسسة شبكة الوب العالمية في بعض الحالات من عدم توفر البيانات المتاحة من قبل مزودي البيانات الرئيسيين، مثل الاتحاد الدولي للاتصالات والبنك الدولي والمنتدى الاقتصادي العالمي. ولذلك، عملت المؤسسة مع خبراء في الإحصاء بهدف

التغلب على هذه التحديات وإنتاج مؤشر صلب، وقد أجرت عمليات تقدير للبيانات (data imputation) المفقودة عند الضرورة.

## ترتيب البلدان العربية وفق مؤشر الوب

شمل تقرير مؤسسة شبكة الوب العالمية لعام ٢٠١٢ ستة بلدان عربية، ويبين الجدول ترتيب هذه البلدان وفق مؤشر الوب، ويسلط أيضاً الضوء على قيمة كل من مؤشراته الفرعية لهذه البلدان. وقد حلت قطر في المرتبة الأولى بين البلدان العربية وفي المرتبة الحادية والعشرين بين بلدان العالم بعد اليابان في الترتيب العام لمؤشر الوب. وهي نتيجة جيدة جداً لدأب قطر المستمر في بناء اقتصاد قائم على المعرفة، وارتفاع استثماراتها في قطاع تكنولوجيا المعلومات والاتصالات. وتسعى قطر لتوفير الإنترنت بالحزمة العريضة لنسبة ٩٥ في المائة من السكان بحلول عام ٢٠١٥. ونتيجة لذلك، تشهد الدولة تطوراً كبيراً في استخدامها لشبكة الإنترنت. وبالتزامن مع هذا الاستثمار في البنية الأساسية، يشهد قطاع التربية والتعليم تطوراً مماثلاً، يهدف إلى بناء قدرات المواطنين والتزوّد بالمهارات اللازمة لبناء اقتصاد المعلومات.

أما تونس، فاحتلت المرتبة الثانية بين البلدان العربية، والأولى في أفريقيا، والحادية والثلاثين بين بلدان العالم بعد الصين. وقد سجلت تونس لمؤشر الأثر أعلى نتيجة بين البلدان الأفريقية. وحل الأردن في المرتبة الثالثة بين البلدان العربية، ولكنه سجل نقصاً من حيث المحتوى المتاح على الإنترنت، وانخفاضاً في مؤشر الأثر وخاصة الأثر السياسي، على الرغم من التطوّر النسبي في البنية الأساسية للاتصالات. وسجلت مصر ارتفاعاً في مؤشر الأثر، وخاصة الأثر السياسي، حيث استُخدمت شبكة الإنترنت كأداة للتواصل قبل الحراك الشعبي وأثناءه، ولكنها سجلت انخفاضاً في مؤشري الجاهزية والوب، في ظل تدني نسبة انتشار الإنترنت في هذا البلد، إذ تقدر بحوالي ٣٦ في المائة في عام ٢٠١١، وفق بيانات الاتحاد الدولي للاتصالات.

واحتل اليمن أدنى مرتبة عربية وعالمية وفق مؤشر الوب، وهو الذي عرف انتفاضة سياسية في عام ٢٠١١ كجزء مما يسمى "الربيع العربي". ومن المتوقع صياغة دستور جديد للبلاد يدعم تعزيز المحتوى على شبكة الإنترنت. وكغيره من أقل البلدان نمواً، يعاني اليمن من ضعف في البنية الأساسية للاتصالات وارتفاع كلفة النفاذ إلى الإنترنت بالحزمة العريضة كنسبة مئوية من الناتج المحلي الإجمالي للفرد الواحد.

### ترتيب البلدان العربية وفق مؤشر الوب لعام ٢٠١٢

| البلد | مؤشر الوب | المؤشر الفرعي للجاهزية | المؤشر الفرعي للوب | المؤشر الفرعي للأثر | الترتيب العام (٦١ بلداً) |
|---|---|---|---|---|---|
| **قطر** | ٦٠,٧٥ | ٦٤,١٦ | ٤٦,٠٦ | ٦٢,٤٣ | ٢٠ |
| **تونس** | ٥٠,٦٨ | ٤٥,٥٠ | ٤١,٦١ | ٥٤,٠٦ | ٣١ |
| **الأردن** | ٤٤,٥٢ | ٥٠,٩ | ٣١,٧٥ | ٤٦,٦٥ | ٣٥ |
| **مصر** | ٤١,٠٥ | ٢٢,٢٩ | ٣٠,١٦ | ٤٩,٦٧ | ٣٩ |
| **المملكة المغربية** | ١٩,٣٩ | ٢٣,٢٥ | ١٩,٧٥ | ٢١,٠٥ | ٥٠ |
| **اليمن** | ٠ | ٤,١ | ١٢,٧٧ | ٠ | ٦١ |

## الخاتمة

تعتمد معظم نماذج القياس الحالية على مؤشرات مركبة تستخدم للدلالة باختصار على أوجه مجتمع المعلومات المعقدة والمتعددة الأبعاد. وفي هذا السياق، يُجمع عدد من المؤشرات، وتستحدث مؤشرات فرعية منها، وتحدد أوزان لها، بحيث تسمح هذه المؤشرات المركبة باختصار صورة متشعبة ومتداخلة الملامح، وتسهّل مهمة وصفها وتحليلها. إلا أنه في حال لم يتم وضع هذه المؤشرات المركبة بالشكل الملائم، قد تمد صانعي القرار وواضعي السياسات بمعلومات خاطئة وغير واقعية، مما قد يؤدي إلى استنتاجات مبسطة وغير صحيحة. لهذا السبب، تم وضع هذا المؤشر الجديد لقياس الوب بأبعاده المتعددة بعناية، وبناءً على مشورة من المجلس الدولي للعلوم والفريق التوجيهي لمؤسسة شبكة الوب العالمية، وهما يضمان كبار الخبراء والأكاديميين من مختلف المجالات والمؤسسات في جميع أنحاء العالم.

وأخيراً، في حين أن تركيبة مؤشر الوب على مستوى مؤشراته الفرعية الثلاثة ينبغي أن تبقى ثابتة من سنة إلى أخرى، وذلك من أجل إجراء مقارنات صحيحة، فإنه لا يزال قابلاً للتحسين، لا سيما على مستوى المؤشرات الأساسية الخمسة والثمانين. فمؤشر الوب هو مؤشر ناشىء وفي تطور مستمر، ويمكن أن يستوعب في تركيبته مؤشرات أساسية جديدة؛ وهذا أمر هام جداً نظراً لطبيعة بيئة الوب التكنولوجية السريعة التغيّر.

❋ ❋ ❋

# INFORMATION AND COMMUNICATIONS TECHNOLOGY APPLICATIONS

## Smart E-Governance: ICT for Economic Development in the Arab Region[1]

E-government has enjoyed substantial investment and attention over the last ten years in most parts of the world, including in member countries of the Gulf Cooperation Council. It has focused strongly, first, on the efficiency of performance in the back office through automating previously paper-based processes, and second on providing a large number of public services to citizens and businesses online, in order to enhance their efficiency. Implementing both of these approaches to e-government is currently on the high priority list of many countries seeking 'more for less', within the context of international economic downturn and increasingly restricted national finances.

Today, a third approach to e-government is becoming of critical importance. Even though it is more difficult to implement and requires some initial investment, it is likely to deliver exponential benefits in the medium to long term. This approach focuses on 'smart e-governance' and can be characterized as accomplishing more by doing things differently. It applies ICT to the public sector as a whole, rather than separately to individual government ministries and agencies, with the goal of rationalizing and sharing processes, data and resources across the system. This approach has the benefits of cutting out duplication, improving decision-making processes and enhancing the impact of governmental action.

This article seeks to demonstrate how Governments in the Arab region could use ICT and data to adopt a 'smart e-governance' approach, with the specific aims of boosting economic growth and supporting job creation. Four areas will be considered: open data, e-business support, e-procurement and using ICT to connect with the diasporas. Examples will also be drawn from the experience of global leaders in e-governance. Some of the suggested strategies are focused on the long term and are relatively challenging to implement, while others are more straightforward and offer the possibility of positive results in the short term.

### Integrated e-governance: A quantum leap in efficiency

E-government traditionally involves a ministry or governmental agency making its existing services available online. Joined-up or whole-of-government approaches,[2] in contrast, use ICT to establish links both within government offices and between them, in order to increase efficiency. Indeed, linking the back offices of agencies and ministries together by re-engineering their work processes can help cut out waste and support the sharing of data and resources. Data about a business can be shared so that the business is not obliged to re-enter it each time it applies for a service; or, for example, so that a ministry of trade and customs, which has information in its database about a company supplying overseas hospitals, may link this information to the procurement plans of the ministry of health. The same data could also be shared with the ministry of employment, which

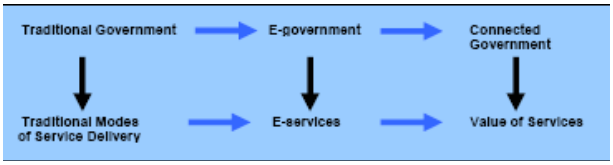
can then source appropriate manpower or ensure that training programmes are geared toward available opportunities. These approaches are in use in many European countries such as Denmark, Germany and the United Kingdom of Great Britain and Northern Ireland, where surveys consistently show that they help both Governments and businesses save time and money. In the United Kingdom, for example, sharing data across new internal cloud computing systems is part of a radical plan that is expected to save up to 3.2 billion pounds (£) a year from a total annual bill of at least £16 billion. Key to the new strategy is the concentration of the Government's computing power into about a dozen highly secure data centres. The construction cost could reach £250 million for each centre. These facilities would replace the more than 500 smaller data centers currently in use, each handling one department of the central Government, police forces and local authorities.

Some Governments have cited legal and ethical reasons for not sharing data between ministries, such as privacy and data protection rights. Joining up back offices could, however, dramatically increase the overall efficiency of public sector operations. That objective has been pursued in the Arab region, for example in Dubai through its E-Business Strategy; in Egypt though the Administrative Reform Program; and in Lebanon through the Office of the Minister of State for Administrative Reform – but with mixed results. Problems or failures tend to be associated with three factors: first, the lack of technical, semantic and organizational interoperability between ministries appears to be preventing the exchange of data. Second, management tends to be reluctant to share data and other resources, perceiving it as a threat to their authority. Third, the necessary organizational skills, awareness and attitudes are not in place.

One insight of the smart e-governance approach is that citizens and businesses do not normally care which department or agency provides a service, as long as the service is efficient and of good quality. Therefore, it isn't necessary for users to understand the structure of government or to deduce which ministry or agency they should apply to. Instead, different agencies and ministries can cooperate and link together when useful, to provide, for example, 'life event' or 'business event' services that draw on data from different places. By way of illustration, registering a company normally requires dealing with the business register, the tax authorities, the employment ministry, trade and customs agencies, and perhaps securing building permits. These services could all be provided in one package as a 'business event', with the cooperation of all agencies and ministries concerned. Joining up front and back offices in this way could dramatically improve the efficiency of government services and the experience of end users, benefits which could be enhanced through mobile and social media applications, services providing location-based and real-time support, and feedback and participatory facilities. Together, these developments would improve user satisfaction and the impact of government services.

The United Nations (2008) illustrated such developments in a figure which underlines how the value of services increases when they are delivered in a joined-up and integrated way, as compared to when services are simply made available online as in traditional e-government.

**Evolving approach to public service delivery**




*Source*: United Nations, 2008, p. 4.

## Sharing resources and 'big data' for better decisions and better policies

Another important benefit of smart e-governance is that linking back and front offices can improve policymaking for overall socioeconomic development. Ministries or agencies for trade, business development, health, education or transport all have good data on their own areas, but linking them together provides a more powerful overall picture. Policymakers can use this integrated or 'big data' to take better-informed decisions and advance policy development. The 'big data' resources now available in some countries are being used for policy modelling, visualisation and simulation, as well as data mining and pattern recognition using ICT and semantic web applications. The combination of these tools with analytical methods (statistical, contextual, quantitative, predictive, cognitive, etc.) has given rise to the new discipline of 'analytics', which some countries are now using to dramatically increase government efficiency and effectiveness.

One example comes from the Government of Singapore, which employs 'smart e-government' to support broader policy goals, such as economic vitality and foreign investment. Its Land Transport Authority (LTA) launched the world's first congestion charging system and has since continued to introduce innovation into its business model. LTA has seen an 80 per cent reduction in revenue leakage from "lost transactions", while tripling its performance capacity to 20 million fare transactions per day. At the same time, its ability to look holistically across the network to help manage current demand allows it to predict future needs and sustainable solutions to accommodate a growing population.

## Open data for economic growth and job creation

Making public data open and accessible to everyone, and not just other government agencies, can do more than encourage a better-informed, more transparent society. It can also lead to economic gains from the reuse or recombination of data in creative ways. Government, with minimal cost to itself, can make large amounts of data available so that others build innovative apps and e-services. This makes sense, given that Governments are often not in the best position to extract commercial value from their own data. According to the European Commission (2011), open government data policies would increase direct business activity in Europe by up to 40 billion euros (€) per year, or 0.3 per cent of GDP. The same study showed that overall benefit, including direct and indirect effects, could be worth up to €200 billion per year, or 1.7 per cent of GDP. In September 2011, an Australian study found that open data unlocked value equal to five times the cost associated with making it available to the public. Specifically, the estimated value of new economic activity plus cost savings was 25 million Australian dollars (A$) per year, compared to a cost of A$4.6 million per year.

Coupled with appropriate macrochanges to regulation and internal changes to the public sector, a strategy to free up and open public data could start to realize some of these benefits. One concrete step in this direction would be the establishment of a virtual platform for collaboration between the public sector, companies, social entrepreneurs and the youth. This platform could have the immediate objective of providing resources and support for the development and implementation of applications and e-services for public, commercial and community users, aimed at both the domestic

market and the foreign one. The platform should also become a tool for boosting local and national economies through developing skills, and helping to establish companies and creating jobs. Such a platform could tap into the talent and enthusiasm of students and the youth, and enhance the international profile of the country's ICT sector.

The collaborative platform here described could be a hub for:

- Sharing resources such as standard tools and applications for developing services, content and applications;
- Sharing data from the public sector, as well as data from other public domain sources, which are structured, linked and machine readable;
- Sharing knowledge through consultancy, communities of practice and working groups; exchanging skills;
- Making apps available for copying and adapting;
- Creating discussion forums, blogs, idea banks, etc.

It is important that such a platform focuses not just on existing companies but also on social entrepreneurs, the hacker community, university students and young people more generally. One purpose of this kind of initiative is to include hackers and young people within a collaborative framework, rather than treating them as a threat. The role of government, in addition to serving as the initiator, active collaborator and partial funder, is to ensure minimum standards, including maintaining basic e-accessibility and e-inclusion, as well as taking responsibility for the overall legal and regulatory framework to ensure fairness and fight corruption. Thus the government maintains its unique responsibility, while also learning to draw on other actors who have relevant interests, expertise and resources to improve the overall quality of services.

## Streamlining regulation to support thriving e-business

According to the World Bank Report Doing Business (2011a), a fundamental prerequisite of healthy economic activity is the existence and application of good rules. The goal is to set regulations that are efficient, accessible to all and simple in their implementation. Rules must strike a balance between safeguarding some important aspects of the business environment and avoiding distortions that impose unreasonable costs on businesses. Where business regulation is burdensome and competition limited, success depends more on whom you know than on what you can do. But where regulation is relatively easy to comply with, transparent, accessible, and includes a clear and open complaints procedure, anyone with talent and a good idea should be able to start and grow a business in the formal sector. The level of corruption is also lower in such environments.

The World Bank indicators focus on a number of 'business events', including starting a business, dealing with construction permits, securing electricity, registering property, paying taxes and trading across borders. Much depends on access to basic information, such as the documentation needed for complying with regulations and formalities. Although the Middle East and North African region has improved its business regulatory procedures over the last six years, obtaining and using such information typically still requires meetings with officials, involving inconvenience, excessive wait times and possibly corruption. By way of contrast, documentation requirements for all high-income member countries of the Organization of Economic

Co-Operation and Development are accessible online, at an agency or through public notices.

In order to thrive, businesses need efficient and transparent government institutions in the economic development field. ICT is a powerful tool for achieving this goal, saving time and money for businesses and government alike. ICT also facilitates access to information and compliance with regulations.

## Impressive savings through e-procurement and e-invoicing

E-procurement both within and between European countries is now a key policy priority. It involves digitizing as much as possible of the value chain, from the initial expression of interest to finalizing the contract. Although progress is piecemeal, there is convincing evidence that e-procurement can become a major source of savings and economic development. European government revenues are among the highest in the world, at 45 per cent of total GDP. Public authorities purchase 15 to 20 per cent of GDP (more than €1,500 billion) per year, and it is estimated that widespread e-procurement and e-invoicing could save at least 5 per cent of GDP, while reducing transaction costs by at least a further 10 per cent.

However, currently less than 5 per cent of public procurement is processed electronically, meaning that potential annual savings of tens of billions of euros have yet to materialize. Furthermore, the European economy is composed largely of Small and Medium Enterprises (SMEs) which could benefit from easier access to public procurement markets, increasing their ICT capability and thus their level of competitiveness. E-procurement is also very much about making things transparent, and this is an important issue for SMEs, which often suffer from a knowledge disadvantage compared to larger firms (European Commission 2006 and 2010).

For example, the Danish e-procurement system, which was launched in January 2002, is not compulsory but still leads to annual savings of €95 million for the Government. E-invoicing was launched in January 2005 and was made compulsory in 2006, resulting in annual savings of €120 million. For both e-procurement and e-invoicing, SMEs and micro companies are a special focus of Government assistance. The policy in Denmark, as in other Scandinavian countries, is that if small businesses start to interface with the Government electronically, for example through e-invoicing, then they will be more likely to use other parts of the e-procurement value chain, as well as to better develop the electronic presence of their business more broadly (Hein 2011and Skulason 2010).

Dubai has had its "Tejari" e-procurement system in place since 2000, supplemented by a 2002 Electronic Transactions and Commerce Law. The system enables all purchase processes to be undertaken electronically (Lootah 2006), allowing for:

- e-tendering (submit – collect – evaluate tenders);
- e-cataloguing (upload – search);
- e-ordering (orders – invoices);
- e-auctioning (e-marketplace–negotiations).

Since its launch in 2000, over 2 billion of United States dollars (US$) worth of business has been conducted using Tejari. The use of e-procurement by the Emirati Armed Forces has resulted in 40 per cent savings on equipment purchases, and 14 per cent savings for IT hardware through structured online comparisons and negotiations. In the Department of Health and

Medical Services, efficiency has increased by 40 per cent, and 70 per cent of pharmaceuticals, medical equipment and consumables have been procured online, with more than 6,000 auctions having taken place since the Ministry joined Tejari.

The Tejari system offers numerous benefits, including simplified, transparent procedures, the reduced duplication of procurement functions and offices, more transparent and accountable decisionmaking, benefits of scale due to consolidated purchasing, and significant time and cost savings. The obstacles to Tejari's success include a lack of awareness within the business community, low numbers of participating suppliers and buyers, and resistance to change from traditional purchasing methods.

## Connecting with the diasporas

According to the World Bank (2011b), Jordan is number 11 in the global list of remittance-receiving countries measured as a percentage of GDP, while it is number 20 in the list of remittance-sending countries in absolute terms, with US$3.8 billion received and just over US$0.5 billion sent in 2010. These transfers are largely in the form of workers' remittances and employee compensation. In 2008, remittances sent home by migrants accounted for 2 per cent of GDP for all developing countries; but they accounted for 16 per cent of GDP in Jordan and 22 per cent in Lebanon in 2009.

Remittances sent home to developing countries by migrants are three times the size of official development assistance and represent a lifeline for the poor. Flows are expected to continue to rise in the future, having recovered in 2010 to pre-crisis levels. The World Bank's view is that remittances generally reduce the level and severity of poverty. They frequently lead to higher human capital accumulation; higher health and education expenditures; access to information and communication technologies; greater involvement in private enterprises; reductions in child labor; and improvements to household preparedness for natural disasters. This means that Governments should treat remittances as private transactions, and not as a substitute for debt or aid flows. They should also attempt to tap into and channel diaspora remittances much more systematically and efficiently.

As technologies have improved and the financial sector and telecommunications industry have intermeshed, money transfers have become simpler, cheaper and more widely available. Many migrants have now switched from sending goods and money by way of traders, and instead execute money transfers through a variety of channels. The composition of diasporas is highly diverse: it typically includes professionals who contribute strongly to remittances alongside unskilled and semi-skilled workers. Although most remittances are still very directly sent to family and friends, the more professional members of diasporas are likely to be open to opportunities to invest their resources in banks, funds and bonds to support their home country and perhaps make a small return. This could be worth millions if not billions of dollars, yet most countries lack a suitable channel for such investments. Governments should seek to develop alliances with their countries' diaspora to facilitate investment and ensure sustainable financing to further the development objectives of their countries. Using the Internet for information and outreach, as well as to support a diaspora community, can dramatically reduce barriers and create incentives. Such a community could link not only individual members of the diaspora together, but also create a link between them and the private sector, banks, non-banking institutions,

non-profit and civil society organizations of their country of origin. This opportunity has been seized upon and developed over many years by India and Latin America, and is now gaining ground in Kenya and Nigeria.

Social media is another area of great potential, especially social and professional networks like Facebook and LinkedIn. Although there are some Arab diaspora networks that use these tools, most seem to be region-specific, for example covering the Lebanese diaspora in North America, and are typically developed bottom-up by the diaspora community itself, rather than being linked to a government initiative. Efforts could be made to link these groups with an umbrella initiative for the specific purpose of increasing economic channels between the diaspora and structured investment opportunities in the country of origin. Both online and offline infrastructures can also target the skilled diaspora in particular, to serve as technical advisers, knowledge brokers and catalysts for projects in the home country. Such initiatives could also provide investment channels for returning expatriates to establish their own businesses. This could help reverse the brain-drain into a brain-gain for ESCWA member countries.

## Conclusion

Simply put, smart e-governance is a tool and a means to the end of improved social, economic, cultural and democratic development. If it cannot be proven to serve these goals, then it is meaningless, at least in the long term. The purpose of this article has been to focus specifically on the economic aspects of smart e-governance, suggesting a variety of strategies and illustrating them with numerous examples. Some of these strategies and examples are taken from countries on the cutting edge of e-government technology, and are probably beyond the short-term objectives of many member countries of ESCWA. Nevertheless, they have been included in order to raise awareness and spark a dialogue on e-government in the Arab region. However, many of the strategies here outlined – especially support for e-business, e-procurement, e-invoicing and connecting with the diasporas – could be adopted by ESCWA member countries relatively quickly and easily, as they carry the prospect of significant benefits for the economy and society more broadly.

# References

European Commission (2006). *I2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All.* Brussels, 25 April. Available from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0173:FIN:EN:PDF.

European Commission (2010). Green Paper on Expanding the Use of E-Procurement in the European Union. Brussels, 18 October. Available from http://ec.europa.eu/internal_market/consultations/docs/2010/e-procurement/green-paper_en.pdf.

European Commission (2011). Proposal for Amending Directive 2003/98/EC on Re-use of Public Sector Information. Brussels, 12 December. Available from http://ec.europa.eu/information_society/policy/psi/docs/pdfs/directive_proposal/2012/en.pdf.

Hein, J.M. (2011). *Denmark: Public Administration – The State as a Practical Example.* Available from http://e-businessguide.eu/2011/01/denmark-public-administration-the-state-as-a-practical-example/.

Lootah, R. (2006). *E-Procurement in the United Arab Emirates.* Available from http://www.oecd.org/dataoecd/57/51/36238605.pdf.

Skulason, B. (2010). *NemHandel: e-Invoicing in Denmark*. European e-Business Lab, 16 November 2010. Available from http://www.slideshare.net/EuropeanBusinessLab/nemhandel-einvoicing-in-denma.

United Nations (2008). E-Government Survey 2008: From e-Government to Connected Governance. New York. Available from http://www2.unpan.org/egovkb/global_reports/08report.htm.

United Nations (2012). E-Government Survey 2012: E-Government for the People. New York. Available from http://www2.unpan.org/egovkb/global_reports/12report.htm.

World Bank (2011a). Doing Business 2012: Doing Business in a More Transparent World. 21 October. Available from: http://www.doingbusiness.org/.

World Bank (2011b). Migration and Remittances Factbook 2011. Available from http://econ.worldbank.org/WBSITE/EXTERNAL/EXTDEC/EXTDECPROSPECTS/0,,contentMDK:21352016~pagePK:64165401~piPK:64165026~theSitePK:476883,00.html.

❋ ❋ ❋

# UNDERSTANDING CYBERCRIME: PHENOMENA, CHALLENGES AND LEGAL RESPONSE

Cybercrime has become a concern for developed and developing countries. The subject matter is complex and includes technical, ethical and legal issues. As for other aspects of crime, a solid understanding of cybercrime is crucial for developing strategies, policies and legislation, and prevention; as well as for establishing the processes of investigation and prosecution.

The third edition of the International Telecommunication Union publication, "Understanding Cybercrime: Phenomena, Challenges and Legal Response",[1] written by Marco Gercke, aims to provide a comprehensive overview of the main topics linked to the legal aspects of cybercrime. The report targets judges, prosecutors, lawyers, law drafters, policy experts and investigators. In order to ensure a broad outreach, the publication will be translated to all official languages used at the United Nations. The first edition (2009) is already available in Arabic, Chinese, English, French, Spanish and Russian from http://www.itu.int/ITU-D/cyb/cybersecurity/projects/crimeguide.html. The translations of the third edition are expected in 2013.

The publication contains six main chapters:

The first chapter provides an introduction to the topic. It addresses the relevance of fighting cybercrime for developing and developed countries, and explains the relation between cybercrime and cybersecurity.

The second chapter provides an account of the different approaches that could be used to define cybercrime and presents a typology. The chapter also reviews the development of computer crime and cybercrime over the last 50 years. It provides detailed information about the phenomena, about the main types of offences which are hacking, identity theft and denial-of-service attacks, and how they are usually committed. The chapter also provides various references to scientific and technical publications for further studies.

The third chapter is dedicated to the challenges of fighting cybercrime. They include the transnational dimension of crime, the speed of data exchange and the ability of offenders to hide their identity by using means of anonymous communication.

The fourth chapter highlights the importance of strategy and legislation to address those problems. It introduces possible components of the needed strategy and legislation, underlining the role of regulators in the fight against cybercrime.

Over the last few years, international organizations participated intensely to the fight against cybercrime. Chapter five provides a summary of some of the activities undertaken by international and regional organizations, including the United Nations, the United Nations Office on Drugs and Crimes, the International Telecommunication Union, the European Union, the Council of Europe, the African Union.

The main chapter of the publication is chapter six, which provides an overview of the legal response to cybercrime. It examines the issues of definitions, substantive criminal law, procedural law, electronic evidence, jurisdiction, procedural law, international cooperation and the liability of Internet service providers. It compares, discusses and analyses the different texts of legal frameworks established by regional organizations and individual countries.

* * *

# أنشطة شعبة تكنولوجيا المعلومات والاتصالات

## الأنشطة الرئيسية المنفذة خلال النصف الثاني من عام ٢٠١٢

فيما يلي الأنشطة الرئيسية التي تولت إدارة تكنولوجيا المعلومات والاتصالات في الإسكوا تنفيذها خلال النصف الثاني من عام ٢٠١٢.

### عقد ورشات عمل تدريبية حول إرشادات الإسكوا للتشريعات السيبرانية

بناء على طلب من البلدان الأعضاء، نظمت الإسكوا سلسلة ورشات عمل لبناء القدرات في مجال تطوير التشريعات السيبرانية، وذلك بالاعتماد على مطبوعة "إرشادات الإسكوا للتشريعات السيبرانية"[١]. وقد تم إعدادها وتنظيمها في إطار المشروع الإقليمي حول "تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية"[٢].

فقد نظمت الإسكوا ورشة عمل حول "التشريعات السيبرانية في المنطقة العربية" بالتعاون مع كلية الحقوق في جامعة الإمارات العربية المتحدة، في مدينة العين في الإمارات العربية المتحدة، يوم ١٦ تشرين الأول/أكتوبر ٢٠١٢. وقد تناولت هذه الورشة الإرشادات حول التشريعات السيبرانية، ونماذج لهذه التشريعات، وأنشطة الإسكوا في هذا المجال. وشاركت الإسكوا بمحاضرة حول النماذج العالمية لحماية الأطفال في استخدامهم لشبكة الإنترنت، والتوجهات المستقبلية للمنطقة العربية في هذا الشأن. وقد تم استعراض البيئة التشريعية للفضاء السيبراني في الإمارات العربية المتحدة خلال أعمال هذه الورشة. وشارك فيها أساتذة الجامعة من كليتي الحقوق والمعلوماتية، وعدد من الخبراء في مجال التشريعات السيبرانية والمعلوماتية، وطلاب الدراسات العليا والسنوات المتقدمة في كلية الحقوق.

وشاركت الإسكوا في ورشة عمل حول "تطوير التشريعات السيبرانية في الجزائر"، تحت رعاية وزير البريد وتكنولوجيات الإعلام والاتصال، في ١٨ و١٩ تشرين الثاني/نوفمبر ٢٠١٢. وقد عرضت الإسكوا خلال هذه الورشة الأنشطة والإرشادات المتعلقة بالتشريعات السيبرانية، وتم النقاش حول أفضل السبل للاستعانة بهذه الإرشادات من أجل وضع التشريعات السيبرانية في الجزائر. كما شاركت الإسكوا بالنقاش الذي دار حول أفضل المنهجيات التي يمكن أن تتبعها الحكومة من أجل المضي قدماً بتطوير البيئة التشريعية اللازمة لمجتمع المعلومات. وقد جمعت هذه الورشة مدراء وخبراء من القطاع العام، يمثلون جميع الوزارات والهيئات المعنية بتكنولوجيا المعلومات والاتصالات وتطبيقاتها، ومنها وزارة البريد وتكنولوجيات الإعلام والاتصال، ووزارة العدل، ووزارة التجارة، ووزارة الإعلام، ووزارة التربية الوطنية، ووزارة الثقافة. كما شارك في هذه الورشة أيضاً ممثلون عن المنظمات غير الحكومية المعنية.

وضمن هذه السلسلة من ورشات العمل، نظمت الإسكوا، بالتعاون مع وزارة العدل في السودان، ورشة عمل حول "إرشادات الإسكوا للتشريعات السيبرانية في المنطقة العربية"، يومي ٢٥ و٢٦ تشرين الثاني/نوفمبر ٢٠١٢. وقد خصصت جلسات خلال ورشة العمل لتحديد مواطن النقص في التشريعات السيبرانية القائمة في السودان، كما تم الحوار حول آليات وضع القوانين القائمة موضع التنفيذ. وقد شارك في هذه الورشة المسؤولون عن وضع وتحسين التشريعات السيبرانية في السودان من وزارة العدل، ومن الهيئات الحكومية الأخرى. كما شارك في الورشة مشرعون وقضاة ومحامون في السودان.

## ندوة حول المتطلبات القانونية والتنظيمية لبناء مجتمع المعرفة المستدام في المنطقة العربية

عقدت الإسكوا ندوة حول "المتطلبات القانونية والتنظيمية لبناء مجتمع المعرفة المستدام في المنطقة العربية" في ١٩ و٢٠ كانون الأول/ديسمبر ٢٠١٢، وذلك في مقر الأمم المتحدة في بيروت. وكان هدف هذه الندوة استعراض النتائج الأساسية لمشروع الإسكوا الخاص بالتشريعات السيبرانية، ومناقشة خارطة الطريق لتنسيق التشريعات السيبرانية على المستوى العربي، وبخاصة الدور الحيوي الذي ستؤديه كل من جامعة الدول العربية والإسكوا في عملية التنسيق هذه. وناقشت الندوة أيضاً آليات ضمان استدامة عملية تنسيق التشريعات السيبرانية إقليمياً، واستمرار التفاعل بين مختلف الفرقاء المعنيين بتطوير القوانين السيبرانية. كما تضمنت الندوة جلسات حول التحديات القانونية الجديدة التي يفرضها التطور المتسارع لتكنولوجيا المعلومات والاتصالات وتطبيقاتها، وعرض لنتائج دراسات بعض المنظمات الدولية، وعروض حول بعض التجارب المتقدمة لدول الإسكوا في مجال التشريعات السيبرانية.

وقد خلصت الندوة إلى مجموعة من التوصيات من أجل تطوير التشريعات السيبرانية وتنسيقها في المنطقة العربية، وبعض هذه التوصيات خاصة بالحكومات ودورها على المستوى الوطني، وأخرى خاصة بالتعاون والتكامل الإقليميين في مجال التشريعات السيبرانية. وقد تطرقت مجموعة أخرى من التوصيات إلى أهمية بناء القدرات والتوعية والتدريب لمختلف المعنيين بصياغة القوانين وتطبيقها، إضافة إلى متطلبات وآليات تطوير العملية التشريعية في المنطقة العربية، بهدف تحسين البيئة التمكينية لبناء مجتمع المعرفة في المنطقة العربية. كما عرضت الإسكوا في نهاية هذه الندوة أنشطتها في المستقبل القريب في مجال التشريعات السيبرانية والتي ستشمل: (١) متابعة عملية التعاون مع جامعة الدول العربية من أجل اقتراح اعتماد الإرشادات على المستوى العربي الإقليمي، (٢) الاستمرار في تقديم الخدمات الاستشارية للدول العربية في مجال تطبيق الإرشادات وتحديث الأطر التشريعية الخاصة بالفضاء السيبراني، (٣) التحضير لإعداد دراسة حول السياسات الخاصة بالاستخدام الآمن للفضاء السيبراني على المستويين الوطني والإقليمي، وذلك خلال عام ٢٠١٤.

وشارك في هذه الندوة حوالي ٥٠ مشاركاً من ١٤ دولة عربية، يمثلون الحكومات وخاصة وزارات وهيئات تكنولوجيا المعلومات والاتصالات ووزارات العدل، بالإضافة إلى ممثلين عن بعض المؤسسات الأكاديمية والقطاع الخاص ومنظمات المجتمع المدني. كما ضم المشاركون ممثلين عن جامعة الدول العربية وبعض منظمات الأمم المتحدة.

## عقد اجتماعات في إطار عملية المنتدى العربي لحوكمة الإنترنت

يشكل المنتدى العربي لحوكمة الإنترنت منبراً إقليمياً للحوار حول قضايا حوكمة الإنترنت التي تهم المنطقة العربية، وقد أطلق العمل به في أوائل عام ٢٠١٢، تحت المظلة المشتركة للإسكوا وجامعة الدول العربية، وذلك إثر انعقاد "المؤتمر التشاوري لتأسيس المنتدى العربي لحوكمة الإنترنت" (بيروت، ٣١ كانون الثاني/يناير - ١ شباط/فبراير ٢٠١٢) وحصول الوثيقة الناتجة عنه على دعم الاجتماع الحادي والثلاثين للمكتب التنفيذي لمجلس الوزراء العرب للاتصالات والمعلومات (بيروت، ٢ شباط/فبراير ٢٠١٢). وتأتي عملية إنشاء هذا المنتدى، على غرار المنتدى العالمي لحوكمة الإنترنت الذي أسس عام ٢٠٠٥، تحت مظلة الأمم المتحدة وبناءً على مقررات القمة العالمية لمجتمع المعلومات. وفي السنة الأولى لتأسيس المنتدى، أكدت الإسكوا على أهمية هذه الجهود من خلال اعتمادها للقرار ٣٠٦ (د-٢٧) بتاريخ ١٠ أيار/مايو ٢٠١٢ بعنوان "تطوير عملية المنتدى العربي لحوكمة الإنترنت ومواصلة الجهود في مجال تطوير أسماء النطاقات العربية"، وتعاونت مع الشركاء في عملية المنتدى في عقد اجتماعات للجنة الاستشارية المتعددة الأطراف والاجتماع السنوي الأول للمنتدى في عام ٢٠١٢، وفيما يلي نبذة عن هذه الاجتماعات.

**الاجتماع الأول للجنة الاستشارية المتعددة الأطراف**

عقد الاجتماع الأول للجنة الاستشارية المتعددة الأطراف الخاصة بالمنتدى العربي لحوكمة الإنترنت في القاهرة، يومي ١٨ و١٩ حزيران/يونيو ٢٠١٢، وقد نظمته الأمانة العامة للمنتدى ممثلة في الجهاز القومي لتنظيم الاتصالات في مصر بالتعاون مع المنظمة العربية للتنمية الإدارية، وبتمويل من الجمعية الكويتية لتقنية المعلومات وشركة سيسكو سيستمز. وشاركت الإسكوا في الإعداد وفي أعمال الاجتماع، حيث قدمت ورقة عمل مشتركة مع جامعة الدول العربية حول الآليات الناظمة لأعمال المنتدى واللجنة الاستشارية المتعددة الأطراف.

وناقش الاجتماع الإجراءات المتعلقة بعملية المنتدى العربي لحوكمة الإنترنت، الذي يسعى إلى إيجاد التكامل المطلوب على المستوى الإقليمي في صناعة القرار في مجال حوكمة الإنترنت، ونقل الرأي العربي إلى الساحة العالمية بما يتواءم مع الفرص والحاجات والمتطلبات الإقليمية. وشكل الاجتماع نقطة الانطلاق لعمل اللجنة الاستشارية المتعددة الأطراف، التي تشمل عضويتها خبراء متميزون من الحكومات، والقطاع الخاص، والمجتمع المدني، بالإضافة إلى المجتمع التقني والأكاديمي. وتناول المجتمعون أبرز قضايا حوكمة الإنترنت، كالتمكين المؤسساتي، وموارد الإنترنت الحرجة، والنفاذ، والمحتوى الرقمي، والأمن والخصوصية، والانفتاح، ودور الشباب.

**اجتماع المشاورات المفتوحة والاجتماع الثاني للجنة الاستشارية المتعددة الأطراف**

عقد اجتماع المشاورات المفتوحة والاجتماع الثاني للجنة الاستشارية المتعددة الأطراف للمنتدى العربي لحوكمة الإنترنت في القاهرة، من ٤ إلى ٦ أيلول/سبتمبر ٢٠١٢. وعقدت هذه الاجتماعات في إطار الإعداد للاجتماع السنوي الأول للمنتدى، وقد تناولت المواضيع الرئيسية التالية: مراجعة لبرنامج الاجتماع السنوي الأول للمنتدى ولمجموعة ورش العمل التي ستقام خلاله، دراسة برنامج التمويل وتنظيم توزيع الموارد المالية المحدودة على الأنشطة التحضيرية الأساسية، وضع برنامج عمل زمني يحدد المسؤوليات بين الفرقاء ويعزز التنسيق في العمل للإعداد للاجتماع، ومراجعة أنشطة الإعلام والتوعية حول المنتدى وموقع الاجتماع على الإنترنت. وتجدر الإشارة إلى أن اجتماع يوم ٤ أيلول/سبتمبر ٢٠١٢ كان مفتوحاً لمشاركة الجميع، وذلك من خلال المشاركة الإلكترونية، حيث تناولت المشاورات المكونات الرئيسية لجلسات الاجتماع السنوي الأول للمنتدى، بما في ذلك نقاط الحوار المواضيعية وقضايا الرعاية والتنظيم.

**الاجتماع السنوي الأول للمنتدى العربي لحوكمة الإنترنت**

تحت شعار "إنترنت أفضل لعالم عربي أفضل"، عقد "الاجتماع السنوي الأول للمنتدى العربي لحوكمة الإنترنت" (الكويت، ٩-١١ تشرين الأول/أكتوبر ٢٠١٢) برعاية سمو ولي العهد الشيخ نواف الأحمد الجابر الصباح ممثلاً بوزير المواصلات المهندس سالم مثيب الأذينة، وباستضافة الجمعية الكويتية لتقنية المعلومات، وتحت المظلة المشتركة لجامعة الدول العربية والإسكوا، وبالتعاون مع أمانة المنتدى ممثلة بالجهاز القومي لتنظيم الاتصالات في مصر. وشارك في الاجتماع مجموعة من أصحاب المصلحة من الحكومات، والقطاع الخاص، ومؤسسات المجتمع المدني، والقطاع الأكاديمي، والمجتمع التقني، والمنظمات الإقليمية والدولية، وقد ضم الاجتماع ما يقارب ٣٠٠ شخص من ١٨ دولة عربية.

وتضمنت نشاطات الافتتاح حلقة حوار رئيسية حول المنظور الاستراتيجي لأهمية وأهداف المنتدى. وقد تناولت دور المنتدى في سد الفجوة على مستوى السياسات والتنمية في المنطقة والعالم، ومراحل تطور عملية منتدى حوكمة الإنترنت على مدى السنين منذ عام ٢٠٠٦، بما فيها تجربة المنتدى في المنطقة العربية في مصر عام ٢٠٠٩، وأهمية خارطة الطريق الإقليمية لحوكمة الإنترنت التي وضعتها الإسكوا بالتعاون مع جامعة الدول العربية في تأطير عملية المنتدى على المستوى الإقليمي، وكيفية متابعتها وضمان التنفيذ الفعال للمبادرات والأنشطة المتعلقة بحوكمة الإنترنت.

وتضمن الاجتماع السنوي الأول للمنتدى ست جلسات عمل رئيسية وثلاث عشرة ورشة عمل موضوعية، وقد تناولت هذه الجلسات مواضيع مختلفة: النفاذ والمحتوى،

الانفتاح وحرية التعبير والمحتوى، الموارد الحرجة للإنترنت، الأمن والخصوصية، الشباب، تقييم الاجتماع والخطوات المستقبلية. ونظمت مؤسسات مساهمة مختلفة ورش عمل موضوعية ساهمت في دعم الحوار القائم ضمن جلسات العمل الرئيسية، وتناولت ورش العمل مواضيع عدة، ومنها: نقاط تبادل الإنترنت، الوسائل الإلكترونية لذوي الاحتياجات الخاصة، نموذج أصحاب المصلحة المتعددين، حرية التعبير، تمكين المرأة، الوسائط الاجتماعية والتحول الديمقراطي، حماية الأطفال على الإنترنت وسياسات الحجب، النسخة السادسة من بروتوكول الإنترنت، صناعة أسماء النطاقات، الشباب يقودون تقنيات وشركات المستقبل.

وقد اختتم الاجتماع بالتأكيد على الأهمية التي توليها الإسكوا لعملية المنتدى، وتحديد سبل تقديم الجهات المهتمة لمقترحاتها لاستضافة المنتدى الثاني في عام ٢٠١٣، وذلك من أجل عرض هذه المقترحات على اللجنة الاستشارية المتعددة الأطراف المكلفة باختيار المؤسسة المضيفة للاجتماع الثاني للمنتدى. والمعلومات الإضافية متوفرة على المواقع التالية: موقع الاجتماع السنوي الأول للمنتدى العربي لحوكمة الإنترنت: http://arabigf.kits.org.kw، موقع أمانة المنتدى: http://igfarab.org، ومواقع المنتدى على فايسبوك وتويتر: www.facebook.com/ArabIGF، twitter.com/igfarab.

## عقد اجتماع حول مبادرة الإسكوا لتعزيز صناعة المحتوى الرقمي العربي

عقدت إدارة تكنولوجيا المعلومات والاتصالات في الإسكوا اجتماع خبراء حول "مبادرة تعزيز صناعة المحتوى الرقمي العربي من خلال الحاضنات التكنولوجية" (عمّان، ١- ٢ تشرين الأول/أكتوبر ٢٠١٢) في الجمعية العلمية الملكية الأردنية. وهدف الاجتماع إلى تحفيز الشراكات بين أصحاب المصلحة المعنيين بصناعة المحتوى الرقمي العربي، ومناقشة آليات التعاون الوطني والإقليمي من أجل تنفيذ المبادرة في أكبر عدد ممكن من الدول العربية وعلى أوسع نطاق. كما هدف الاجتماع إلى مناقشة نماذج الأعمال الجديدة لصناعة المحتوى الرقمي العربي، حيث أعدت الإسكوا دراسة خاصة بهذا المحور، وإلى تحفيز تبادل التجارب والخبرات في مجال المحتوى الرقمي العربي وصناعته. وأوضحت الإسكوا خلال الاجتماع الأسس والتوجهات التي ستعتمدها في تنفيذ هذه المبادرة، وأهمها: الاهتمام بالتطورات التكنولوجية الحديثة وخاصة تطبيقات الهواتف الذكية؛ وعقد شراكات إقليمية ووطنية بين الجهات الحكومية والحاضنات التكنولوجية والمؤسسات الداعمة للإبداع والابتكار، لتطوير صناعة المحتوى الرقمي العربي في كل دولة وعلى المستوى الإقليمي؛ وإمكانية ملاءمة المبادرة مع الأولويات الوطنية للمحتوى الرقمي العربي في كل دولة.

لقد بينت المداخلات والنقاشات خلال الاجتماع الاهتمام المتزايد في الدول العربية بصناعة المحتوى الرقمي العربي، والذي يعبر عنه بإطلاق الحكومات لمبادرات وطنية للمحتوى الرقمي، وتنظيم الحاضنات التكنولوجية لمسابقات خاصة بهذا الموضوع، وقيام المنظمات الدولية بإعداد دراسات استراتيجية حول المحتوى الرقمي العربي وصناعته. ومع ذلك، فما زالت نسبة اللغة العربية على الإنترنت متدنية مقارنة مع اللغات الأخرى، وبالتالي لا بد من تعزيز الجهود وتكثيفها من أجل تقليص الفجوة اللغوية القائمة حالياً، ولا بد من التعاون بين الدول العربية من أجل تحقيق التكامل الإقليمي ووضع سياسات وخطط عمل إقليمية لتطوير صناعة المحتوى الرقمي العربي. كما أوضحت النقاشات ضرورة تحفيز الإبداع والابتكار والريادة، خاصة لدى الشباب، من أجل استثمار الفرص المتاحة إقليمياً وعالمياً في مجال صناعة المحتوى.

وشارك في الاجتماع أكثر من ثلاثين خبيراً من إثنتي عشرة دولة عربية يمثلون جهات حكومية، وحاضنات تكنولوجية، ومنظمات دولية، والقطاع الخاص، وجمعيات مهنية. وقد أشاد المشاركون في الاجتماع بدراسات الإسكوا ومبادرتها بتحفيز صناعة المحتوى الرقمي العربي في المنطقة العربية، وأبدوا استعدادهم للتعاون مع الإسكوا من أجل تنفيذ المبادرة. للمزيد من المعلومات، انظر http://www.escwa.un.org/information/meetingdetailsAR asp?referenceNUM=1901a.

## الاجتماع التحضيري الإقليمي لغربي آسيا حول "العلوم والتكنولوجيا والابتكار من أجل التنمية المستدامة"

خلال التحضير للاستعراض الوزاري السنوي للمجلس الاقتصادي والاجتماعي لعام ٢٠١٣، عُقد اجتماع إقليمي تحضيري حول موضوع "العلوم والتكنولوجيا والابتكار من أجل التنمية المستدامة" في ٢٦ تشرين الثاني/نوفمبر ٢٠١٢ في عمّان. واستضافت حكومة الأردن الاجتماع، وذلك بالتعاون مع مركز الإسكوا للتكنولوجيا، وإدارة الشؤون الاقتصادية والاجتماعية في الأمم المتحدة (DESA)، ومنظمة الأمم المتحدة للتربية والعلم والثقافة (اليونسكو). وضم الاجتماع مجموعة مختارة من أصحاب القرار الإقليميين الذين ناقشوا الوضع الراهن للبحث العلمي والابتكار في غرب آسيا وشمال أفريقيا، وتداولوا في الخيارات المتاحة لتحسين السياسات والحوافز لزيادة الاستثمار في العلوم والتكنولوجيا والابتكار. وقد تبلورت عن المناقشات الرسائل التالية:

١- بناء ورعاية المجتمعات المُبتكِرة

- إن بناء ورعاية المجتمعات المُبتكِرة يتطلب التزاماً من جميع طبقات المجتمع من أجل تعزيز المعارف والعلوم والانفتاح؛
- إن للحكومات دوراً محورياً في تشجيع الابتكار، حتى لو كان مصدره عادة من القطاعين الخاص والتطوعي؛
- ينبغي أن توضع السياسات التي تشجع على التكيف مع التحديات الجديدة، كما يجب توفير الحوافز لبناء القدرات من أجل الابتكار؛
- ينبغي أن تكون سياسات الابتكار شمولية، وتتناول التعليم الأساسي، وتطوير مهارات الشباب، وخلق البيئة اللازمة للاستثمار وفرص العمل والتسويق؛
- ينبغي اعتماد سياسة استراتيجية للابتكار وسياسات وطنية متكاملة أكثر وضوحاً، تهدف لتحسين الأنظمة التي تحفز التغيير والابداع.

٢- التأكيد على شمولية التقدم في مجال العلوم والتكنولوجيا والابتكار

- في السياق الحالي، حيث العولمة والتنمية تكافئ الابتكار التكنولوجي والأنظمة الديناميكية، قد تستثنى قطاعات كبيرة من السكان من المشاركة والمساهمة في مجتمعاتهم، مما قد يعيق التنمية في بعض البلدان ويعزز عدم الاستقرار الاجتماعي؛
- إن اكتساب المعرفة والتكنولوجيا العالمية، وتكييفها لاستيعاب السياقات المحلية، له أثر كبير، إذ يتيح بيئة تمكن الجميع من العمل وتحقيق إمكاناتهم والمساهمة في المجتمع، خاصة الشباب والنساء؛
- إن الوصول إلى الموارد مفتوحة المصدر - سواء الموارد التعليمية المفتوحة والمكتبات الافتراضية أو المعلومات المتعلقة بالبراءات المفتوحة - أمر مهم لتطوير حلول لمواجهة تحديات التنمية المستدامة. وإن ضمان استخدام هذه المواد وتعزيز إمكانية النفاذ إليها في المنطقة أمر أساسي للابتكار.

٣- تحسين الشراكات داخل المنطقة وخارجها

- إن الحاجة ماسة لمزيد من الجهود لتطوير التعاون الإقليمي والشراكات بين بلدان المنطقة. وقد ركزت العديد من الشراكات الناجحة على الروابط الدولية مع الشركاء من خارج المنطقة. وعلى الرغم من تنوع المنطقة اجتماعياً واقتصادياً وثقافياً، فإن هناك بعض الأولويات والتحديات المشتركة التي يمكن أن تجد حلولاً جماعية داخل المنطقة؛
- هناك عدد من "حالات التميز المعزولة" والمتناثرة في جميع أنحاء المنطقة، ويمكن استغلالها في شراكات مثمرة للتصدي لتحديات الاستدامة الإقليمية؛
- على مستوى الجامعات ومراكز البحوث، يجب أن تستغل الزيادة الكبيرة في التعاون الدولي للبحث المشترك، والفرص المتاحة عالمياً لتبادل المعارف والعلوم، مما يساعد على تعزيز شبكات البحوث وتشجيع الابتكار.

## عقد اجتماعات في إطار عمل مركز الإسكوا للتكنولوجيا

في السنة الأولى من عمل مركز الإسكوا للتكنولوجيا الذي تستضيفه حكومة الأردن في مدينة الحسن العلمية، نظم المركز عدة اجتماعات وتعاون في عقدها مع جهات عدة. وتشمل هذه الاجتماعات ما يلي:

- ورشة عمل حول تسويق البحوث ونقل التكنولوجيا (بيروت، ٢٩ آذار/مارس ٢٠١٢)، عقدت بالتعاون مع المجلس الوطني للبحوث العلميه في لبنان، ومكتب حماية حقوق الملكية الفكرية. وهدفت الورشة إلى وضع الأسس لتسويق البحوث في لبنان، ومراجعة وتحليل النموذج الأردني في هذا المجال، والنظر في الإمكانيات والمزايا لتكييف نموذج مماثل في لبنان، واقتراح نموذج ومسودة خارطة طريق لإنشاء وحدة عمل في المجلس الوطني للبحوث العلميه، تعنى بتسويق البحوث الوطنية وتقدم خدماتها للجامعات ومراكز البحوث في لبنان؛
- ورشة عمل حول الريادة والجودة في البرامج الهندسية (بيروت، ١٩ نيسان/أبريل ٢٠١٢)، عقدت بالتعاون مع قسم الهندسة في الجامعة اللبنانية، ومركز الملكة رانيا للريادة في الأردن. وتناول الاجتماع محاور ضمان الجودة في الجامعات والريادة في الأعمال الجامعية؛
- ورشة عمل حول الريادة والابتكار في مناطق جنوب البحر الأبيض المتوسط (بيروت، ٢٣-٢٦ نيسان/أبريل ٢٠١٢)، عقدت بالتعاون مع المصرف الأوروبي للاستثمار؛
- الاجتماع الإقليمي الأول للجنة الفنية (عمّان، ٢٦ نيسان/أبريل ٢٠١٢)، عقد بمشاركة أعضاء اللجنة الفنية لمركز الإسكوا للتكنولوجيا، المكونة من أحد عشر خبيراً من الدول الأعضاء، واستعرض الاجتماع مراحل تأسيس المركز ولجنته الفنية وعملية تنظيم العمل، ثم تمّ عرض لإنجازات المركز وتداول حول ملاحظات الخبراء ومقترحاتهم بشأن خطة العمل؛
- ورشة عمل تدريبية حول النمذجة السريعة (قطر، ٦-٧ حزيران/يونيو ٢٠١٢)، عقدت بالتعاون مع جامعه تكساس في قطر (Texas A&M University at Qatar)، وشارك فيها مديري التكنولوجيا في المؤسسات العربية المعنية بالتصميم الهندسي واستخدام النمذجة كجزء من نظم الابتكار؛
- ورشة عمل حول الابتكار والرياده لتحقيق الإنماء الاقتصادي (بيروت، ٥-٦ أيلول/سبتمبر ٢٠١٢)، عقدت بالتعاون مع المنظمة العالمية للملكية الفكرية؛
- جلسات حول المشاريع الابتكارية (عمّان، ٩ آب/أغسطس و١٣ أيلول/سبتمبر ٢٠١٢)، عقدت بهدف توليد أفكار للمشاريع الابتكارية، وشارك فيها عدد من الخبراء من أجل إيجاد حلول لمشاكل تقنية مختارة بطرق ابتكارية.

# الحواشي

## تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية

(١) أعدت هذا المقال السيدة هانيا الديماسي، من شعبة تكنولوجيا المعلومات والاتصالات في الإسكوا.

(٢) http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=251.

(٣) الإسكوا، إرشادات الإسكوا للتشريعات السيبرانية المتوفرة على الموقع http://isper.escwa.un.org/Portals/0/Cyber%20Legislation/Regional%20Harmonisation%20Project/Directives/Directives-Full.pdf.

(٤) http://cyberlegislation.escwa.org.lb.

## بعض أنماط الجرائم المالية عبر الإنترنت

(١) أعد هذا المقال القاضي محمد محمد الألفي، رئيس الجمعية المصرية لمكافحة جرائم الإنترنت، ونائب رئيس الاتحاد العربي للتحكيم الإلكتروني.

(٢) http://www.al-jazirah.com.sa/digimag/16032003/por676.htm.

## دور السلطات في عمليات اختراق الشبكات الإلكترونية

(١) أعد هذا المقال السيد جورج يونس والسيدة ميرنا بربر من شعبة تكنولوجيا المعلومات والاتصالات في الإسكوا.

(٢) http://en.wikipedia.org/wiki/Hacktivism.

(٣) الصحافي ستيفن ليفي هو أول من استعمل هذه العبارة للدلالة على المبادئ التي يشترك فيها معظم المخترقون، وهي مفصلة في دراسة أجرتها فيكتوريا مكلولين، متاحة على الموقع http://pages.shanti.virginia.edu/Victoria_McLaughlin/files/2012/04/McLaughlin_PST_Thesis_2012.pdf.

(٤) للمزيد من المعلومات عن هذه العملية، أنظر مثلاً http://www.pcworld.com/article/212701/operation_payback_wikileaks_avenged_by_hactivists.htm.

(٥) http://www.pcworld.com/article/213120/article.html.

(٦) http://www.fbi.gov/news/pressrel/press-releases/warrants_012711.

(٧) http://elpais.com/elpais/2011/06/10/actualidad/1307693819_850215.html.

(٨) http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=1&pagewanted=all.

(٩) http://almustaqbal.com/storiesv4.aspx?storyid=534189.

(١٠) http://www.guardian.co.uk/technology/2012/aug/09/cyber-espionage-state-sponsored-lebanon.

## Hacktivists: Public vigilantes or public nuisance?

1 This article was prepared by Syed Ahmad, ESCWA, Information and Communication Technology Division.

2 Dreyfus Suelete (1998). *Computer Hackers: Juvenile Delinquents or International Saboteurs?* Paper presented at the Conference on Internet Crime. Melbourne, 16-17 February. Available from http://www.aic.gov.au/media_library/conferences/internet/dreyfus.pdf.

3 Computer Emergency Response Team (CERT). Advisory Warning Against the WANK Worm Issued on 17 October 1989. Available from http://www.cert.org/advisories/CA-1989-04.html.

4 Verizon RISK Team (2012). *Data Breach Investigations Report.* Available from http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf.

5 The 2012 TIME 100 Poll, available from http://www.time.com/time/specials/packages/article/0,28804,2107952_2107959,00.html.

6 McAfee (2012). *Hacktivism: Cyberspace has become the new medium for political voices.* Available from http://www.mcafee.com/us/resources/white-papers/wp-hacktivism.pdf.

7 'Operation Payback' was launched under the Anonymous banner, in response to high-profile targets opposing internet piracy, and was later extended to also target those who opposed WikiLeaks. A timeline infographic is available from http://www.myce.com/news/anonymous-operation-payback-timeline-infographic-36481/.

8 http://www.guardian.co.uk/technology/2012/sep/21/cyberwar-iran-more-sophisticated?INTCMP=SRCH.

## إطلاق أول مؤشر عالمي لقياس الوب

(١) أعدّ هذه المقالة السيد رامي الزعتري من شعبة تكنولوجيا المعلومات والاتصالات في الإسكوا، وذلك استناداً إلى تقرير مؤسسة شبكة الوب العالمية لعام ٢٠١٢ حول مؤشر الوب، وهو أول مؤشر عالمي لقياس الوب.

(٢) Pruulmann-Vengerfeldt, P. 2006. Exploring Social Theory as a Framework for Social and Cultural Measurementsof the Information Society. The Information Society. Vol. 22, No. 5, pp. 303-310.

(٣) World Wide Web Foundation: http://www.webfoundation.org

(٤) يمكن الاطلاع على تقرير عام ٢٠١٢ على العنوان التالي: http://thewebindex.org.

## الأنشطة الرئيسية المنفذة خلال النصف الثاني من عام ٢٠١٢

(١) انظر المقال حول تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة.

(٢) http://isper.escwa.un.org/FocusAreas/CyberLegislation/Projects/tabid/161/language/en-US/Default.aspx.

باتت الجرائم السيبرانية تشكل خطراً عالمياً يهدد البلدان النامية والبلدان المتقدمة على السواء. هذا العدد من نشرة تكنولوجيا المعلومات والاتصالات للتنمية في غربي آسيا يعرض بعض جوانب الجريمة السيبرانية ويبحث في آثارها على التنمية الاقتصادية والاجتماعية في المنطقة العربية. وتشمل هذه الجوانب الأنشطة التي يقوم بها المعارضون على شبكة الإنترنت وقراصنة الشبكة وجرائم سيبرانية معينة في المنطقة. كما تعرض النشرة مشروع تنسيق التشريعات السيبرانية في المنطقة العربية الذي تضطلع بتنفيذه الإسكوا وأهميته في مكافحة الجريمة السيبرانية.

وتتناول النشرة أيضاً موضوع الحوكمة الإلكترونية ومساهمتها في تحقيق التنمية الاقتصادية في المنطقة العربية على ضوء تجارب بلدان مختلفة في هذا المجال. وتعرض المؤشر العالمي الأول لقياس الوب الذي أطلقته مؤسسة شبكة الوب العالمية ونتائج استخدامه لقياس الوب في المنطقة العربية. وتقدم النشرة أيضاً لمحة عن الأنشطة التي نفذتها الإسكوا في مجال تكنولوجيا المعلومات والاتصالات في النصف الثاني من عام ٢٠١٢.

Cybercrime is an emerging global threat which affects developed and developing countries alike. This Review examines selected aspects of cybercrime, underlining its effect on the socioeconomic development of the Arab region. Those aspects include the action of cyberdissidents and hacktivists, as well as specific cases of cybercrime in the region. The publication reviews the project on the regional harmonization of cyberlegislation undertaken by ESCWA, and stresses its importance in the fight against cybercrime.

The Review also addresses the issue of e-governance and its contribution to the economic development of the Arab region, in the light of international experiences in the field. It presents the first global web index launched by the Web Foundation and discusses its results for the Arab region. The publication finally reviews ESCWA activities in the field of ICTs for the second half of 2012.

الاسكوا

بيت الأمم المتحدة، ساحة رياض الصلح
صندوق بريد: ٨٥٧٥-١١، بيروت، لبنان
هاتف: ٩٨١٣٠١ ١ ٩٦١+، فاكس: ٩٨١٥١٠ ١ ٩٦١+
www.escwa.un.org



Printed at ESCWA, Beirut

E/ESCWA/ICTD/2013/1
United Nations Publication

12-0336 - August 2013