|  |  |  |
| --- | --- | --- |
| itu_logo | **الجمعية العالمية لتقييس الاتصالات (WTSA-16)****الحمامات، 25 أكتوبر - 3 نوفمبر 2016** | CCITT/ITU-T 60th Anniversary logo |
|  |  |  |
|  |  |
| الجلسة العامة | المراجعة 1للوثيقة 58-A |
|  | 27 أكتوبر 2016 |
|  | الأصل: بالإنكليزية |
|  |
| مدير مكتب تقييس الاتصالات |
| استنتاجات الندوة العالمية الثالثة للمعايير |
|  |

|  |  |
| --- | --- |
| يلخص هذا التقرير استنتاجات الندوة العالمية الثالثة للمعايير (GSS). وتتضمن المراجعة 1 لهذه الوثيقة ملخصاً لجميع مناقشات الندوة العالمية للمعايير يرد في التذييل I. | **ملخص:** |

استنتاجات الندوة العالمية الثالثة للمعايير

جمعت الندوة العالمية الثالثة للمعايير، مدينة الحمامات، تونس، يوم 24 أكتوبر 2016 قادة الفكر في مجال التقييس لمناقشة أفضل الطرق التي يمكن بها لجهود التقييس أن تراعي اعتبارات الأمن والخصوصية والثقة.

# 1 مقدمة

تعد الندوات العالمية للمعايير (GSS) مناقشات رفيعة المستوى لسياسات التقييس تستكشف الديناميات المتطورة لتكنولوجيا المعلومات والاتصالات (ICT) والآثار ذات الصلة فيما يتعلق بالتقييس التقني. وتعقد الندوة في مستهل الجمعية العالمية لتقييس الاتصالات (WTSA) التي يعقدها الاتحاد كل أربع سنوات. وعقدت الندوتان السابقتان في جوهانسبرغ عام 2008 وفي دبي عام 2012.

وجاء موضوع الندوة العالمية للمعايير لعام 2012 - *التقييس عند تقاطع قطاع تكنولوجيا المعلومات والاتصالات مع قطاعات أخرى مثل الرعاية الصحية والمرافق العامة والنقل* - في وقته تماماً، ووفرت استنتاجات الندوة توجيهات قيمة لعمل التقييس المضطلع به في الاتحاد في الفترة من 2013 إلى 2016. وتطرقت ندوة عام 2012 إلى موضوع الأمن والخصوصية والثقة في البنية التحتية لتكنولوجيا المعلومات والاتصالات وخدماتها عند مناقشة موضوعات مثل الإرسال اللاسلكي للبيانات الطبية وتخزين البيانات الخاصة بتحركات المركبات الموصولة وجمع بيانات المستهلكين بواسطة شركات البيع بالتجزئة على الإنترنت. وفي بيئات كهذه، يتعين وجود إطار مقيس لتوفير الضمان لحماية أي خدمة لها نعوت أمنية موثوقة واحتياجات المستعملين المتعلقة بالأمن والخصوصية.

وناقشت الندوة العالمية الثالثة للمعايير (GSS‑16) الكيفية التي يمكن بها لأصحاب المصلحة المعنيين العمل بتعاون من أجل وضع أطر دولية للأمن والخصوصية والثقة. وجمعت الندوة خبراء بارزين في مجالات الأمن والخصوصية والثقة يمثلون حكومات وهيئات تنظيم ومنظمات معايير ودوائر الصناعة. وتبادل المشاركون الآراء بشأن العناصر الرئيسية التي يعتقدون أنها تشكل هذه الأطر، إضافة إلى، العناصر التي ينبغي منحها أولوية بين هذه العناصر فيما يتعلق بعمل التقييس الذي سيضطلع به الاتحاد في الفترة من 2017 إلى 2020.

وقدمت كلمة ترحيبية من **سعادة السيد محمد أنور معروف**، وزير تكنولوجيات الاتصال والاقتصاد الرقمي في الجمهورية التونسية. وقدمت كلمتان افتتاحيتان من كل من السيد **هولين جاو**، الأمين العام للاتحاد الدولي للاتصالات والسيد **تشيساب لي**، مدير مكتب تقييس الاتصالات بالاتحاد. وترأس الندوة السيد **منجي مرزوق**، وزير سابق لتكنولوجيا المعلومات والاتصالات في تونس.

وأعقب الجلسة الافتتاحية للندوة GSS‑16 ثلاث جلسات تناولت موضوع الندوة من منظور التنظيم والسياسات والصناعة والتقييس. ولخص القسم الثالث، الذي جاء عقب تناول لموضوع الندوة GSS‑16 في سياق منظومة الأمم المتحدة (UN) في القسم الثاني من هذا التقرير، النتائج والتوصيات الرئيسية لكل جلسة من جلسات الندوة. ويرد ملخص مفصل لجميع مناقشات الندوة GSS‑16 في التذييل I.

ويمكن الاطلاع على البرنامج النهائي والسير الذاتية للمتحدثين وكلماتهم على <http://itu.int/en/ITU-T/wtsa16/gss/>.

وطبقاً للقرار 122 (المراجَع في غوادالاخارا، 2010) والقرار 1272 (المعدل) لمجلس الاتحاد، تحال استنتاجات الندوة GSS‑16 المفصلة في هذا التقرير إلى الجمعية العالمية لتقييس الاتصالات (WTSA‑16) للنظر فيها.

# 2 الأمن والخصوصية والثقة في تكنولوجيا المعلومات والاتصالات - في سياق منظومة الأمم المتحدة

مكنت تكنولوجيا المعلومات والاتصالات مليارات من الناس من تبادل المعلومات الرقمية على صعيد عالمي. واستعمال هذه التكنولوجيات التي تعتمد بشكل كبير على المعايير التقنية أفرز مجموعة كبيرة من التحديات فيما يتعلق بخصوصية الاتصالات وأمنها وثقة المستعمل النهائي في تكنولوجيا المعلومات والاتصالات في نهاية الأمر.

ويشارك الاتحاد في مواجهة هذه التحديات من منظورين، الأول كمنظمة من منظمات وضع المعايير تهدف إلى وضع معايير دولية طوعية لتكنولوجيا المعلومات والاتصالات تراعي الخصوصية،’[[1]](#endnote-1)‘ والثاني كمنظمة حكومية دولية مكلفة ببناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات.’[[2]](#endnote-2)‘ وقد أوكلت القمة العالمية لمجتمع المعلومات للاتحاد مسؤولية العمل كمسهل لخط العمل جيم5، بالعمل مع الدول الأعضاء في الاتحاد وأصحاب المصلحة الآخرين من أجل *"زيادة تعزيز إطار الثقة والأمن باتخاذ إجراءات تعزيز متبادلة في مجالات الأمن المتعلقة باستعمال تكنولوجيا المعلومات والاتصالات، مع اتخاذ مبادرات أو وضع خطوط توجيهية فيما يتعلق بالحق في الخصوصية، وفي حماية البيانات وحماية المستهلك"*.

ويتوفر الأساس الدولي المعياري لحماية الخصوصية بشكل مبدئي من خلال معاهدات حقوق الإنسان مثل الإعلان العالمي لحقوق الإنسان الصادر عن الأمم المتحدة في 1948 ’[[3]](#endnote-3)‘ والعهد الدولي الخاص بالحقوق المدنية والسياسية الصادر عن الأمم المتحدة في 1966’‘[[4]](#endnote-4)، ويتضمن كلاهما أحكاماً بشأن الحق في الخصوصية/الحياة الخاصة (المادتان 12 و17، على التوالي). بيد أن هاتين الاتفاقيتين لا تشيران صراحة إلى المعالجة الرقمية للمعلومات الشخصية، وهو مفهوم لم يتم تناوله، في إطار منظومة الأمم المتحدة، إلا في صورة وثيقة توجيهية غير ملزمة، وهي المبادئ التوجيهية للأمم المتحدة لعام 1990 لتنظيم ملفات البيانات الشخصية المعدة بالحاسبة الإلكترونية.’[[5]](#endnote-5)‘

وعلى الرغم من وجود عدد من الاتفاقيات الدولية الملزمة قانوناً والتي تتضمن الحق في الخصوصية - اتفاقية مجلس أوروبا بشأن حماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية’[[6]](#endnote-6)‘ والاتفاقية الأوروبية لحقوق الإنسان والحريات الأساسية’[[7]](#endnote-7)‘ والاتفاقية الأمريكية لحقوق الإنسان’[[8]](#endnote-8)‘ - فقد وضعت هذه الصكوك القانونية واعتمدت على أساس إقليمي وليس على أساس عالمي. ويقوم الكثير من هذه الاتفاقيات الإقليمية على نفس المبادئ الأساسية المتعلقة بالخصوصية، مثل مفهوم موافقة الأفراد عن علم وكفاية التدابير الأمنية المتبعة قبل معالجة المعلومات الشخصية.’[[9]](#endnote-9)‘

ونادت مجموعة متنوعة من أصحاب المصلحة بإيلاء مزيد من الاهتمام إلى ضرورة وجود فهم عالمي مشترك بشأن معالجة المعلومات الشخصية. فعلى سبيل المثال، ناشد أعضاء المؤتمر الدولي لحماية البيانات والخصوصية أ) الأمم المتحدة، أن تقوم بإعداد *"اتفاقية عالمية لحماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية"* تكون ملزمة قانوناً؛ وب) المنظمات الدولية *"أن تلزم نفسها بالامتثال للمبادئ المتوافقة مع الصكوك الدولية الأساسية التي تتناول حماية البيانات والخصوصية"*؛ وج) جهات تصنيع العتاد والبرمجيات *"أن تقوم بتطوير منتجات وأنظمة تضم تكنولوجيا لتعزيز الخصوصية"*.’[[10]](#endnote-10)‘

وقد وجهت الجمعية العالمية للأمم المتحدة هذا النداء خلال دورتها الثامنة والستين (2013) باعتماد قرار بعنوان *"الحق في الخصوصية في العصر الرقمي"* تهيب فيه بجميع الدول الأعضاء في الأمم المتحدة بأن *"تحترم وتحمي الحق في الخصوصية، بما في ذلك في سياق الاتصالات الرقمية"*.’[[11]](#endnote-11)‘ وبناءً على هذا القرار، عين مجلس حقوق الإنسان التابع للأمم المتحدة مقرراً خاصاً تتمثل ولايته في عدة أمور *من بينها* رفع تقرير بشأن الانتهاكات المزعومة للحق في الخصوصية، بما في ذلك ما يتصل منها بالتحديات الناشئة من التكنولوجيات الجديدة.

# 3 الاستنتاجات الرئيسية للندوة GSS‑16

## 1.3 المبادئ التنظيمية للأمن والخصوصية والثقة

*مع التذكير بأن الخصوصية وحماية البيانات يمثلان قيماً أساسية للأفراد والمجتمعات وأن الإعلان العالمي لحقوق الإنسان تجسد الخصوصية كحق أساسي؛*

*ومع ملاحظة أن جميع مجالات الحياة تقريباً تعتمد على البنية التحتية لتكنولوجيا المعلومات والاتصالات وخدماتها ومن ثم ستتأثر إذا لم يتسن الحفاظ على الثقة فيها؛*

*ومع الاعتراف بأن للاتجاه المقلق في حالات انتهاك البيانات والحوادث الأمنية تأثيراً سلبياً على ثقة الناس،*

*أكدت الندوة العالمية للمعايير على:*

- تعزيز **الأطر الدولية** التي تتضمن مبادئ أساسية للأمن والخصوصية والثقة وإنشاء آليات لتنفيذ هذه المبادئ.

- تشجيع الالتزام **بمبادئ** **الخصوصية عند التصميم وتقييم أثر الخصوصية ووضع** **تكنولوجيات تعزز الخصوصية** (PET)، تكنولوجيات يؤدي دمجها ضمن البنية التحتية لتكنولوجيا المعلومات والاتصالات وخدماتها إلى تدنية معالجة المعلومات التي يمكن التعرف على هوية أصحابها.

- استنباط وسائل من أجل **تبادل المعلومات بين القطاعين العام والخاص** بشأن التهديدات التي تواجهها البنية التحتية لتكنولوجيا المعلومات والاتصالات وخدماتها، وأفضل الممارسات واستراتيجيات التخفيف.

- حشد المجتمع الدولي وإنشاء شراكات من أجل **تطوير القدرات الوطنية** للحماية من الهجمات السيبرانية وزيادة قدرات البلدان من أجل الكشف عن الحوادث الأمنية وإعمال الاستجابات المنسقة لهذه الحوادث.

- تحقيق توازن بين الحاجة إلى حماية خصوصية الأفراد وتشجيع **الاستعمال المبتكر للبيانات** من أجل دفع الاقتصاد الرقمي. فعندما تصمم ممارسات جيدة للخصوصية والأمن داخل التكنولوجيات والخدمات الجديدة، فإنها تصبح ميزة جذابة للمستهلكين وتسهم في تحسين الشبكة بأكملها.

- الإسهام في وضع **معايير دولية لمواجهة القضايا العالمية**، مع الاعتراف بأن الهجمات السيبرانية لا تحترم الحدود الوطنية وأن الانتهاكات المتعلقة بالخصوصية والأمن تضعف الثقة في تكنولوجيا المعلومات والاتصالات وأن الأطر الأمنية المقيسة على المستوى الدولي ضرورية من أجل توفير الضمان بأن النعوت الأمنية لخدمة ما يمكن الثقة فيها وأن احتياجات أي مستعمل فيما يتعلق بالأمن والخصوصية محمية عبر الحدود.

- التشجيع على وضع **معايير من أجل "منع تعرف" البيانات الشخصية وإمكانية تنقل البيانات**، ومعايير قادرة على الإسهام في توفير حماية أكبر للمستهلكين وخيار أكبر فيما يتعلق بقدرة المستهلكين على الاشتراك في خدمات تكنولوجيا المعلومات والاتصالات أو إلغاء اشتراكاتهم فيها.

## 2.3 كيف يمكن للصناعة تحقيق توقعات المستعملين النهائيين فيما يتعلق بالأمن والخصوصية والثقة

*مع إعادة التأكيد على الإمكانات العديدة لتكنولوجيات المعلومات والاتصالات والرقمنة في تحسين حياتنا ومجتمعاتنا؛*

*ومع الاعتراف بأن الانتهاكات المتعلقة بالأمن والخصوصية وغياب الثقة في البنية التحتية لتكنولوجيا المعلومات والاتصالات وخدماتها يمكن أن تتسبب في تهديدات خطيرة لأعمال الشركات وسمعتها؛*

*ومع الدعوة إلى وضع معايير دولية قابلة للتنفيذ،*

*أكدت الندوة العالمية للمعايير على:*

- دعم وتعزيز مبادئ **الشفافية والسلامة التكنولوجية**. ومع الإقرار بأنه لا يمكن وجود ثقة بدون شفافية، ينبغي للمستعملين أن يكونوا قادرين على معرفة أن بياناتهم جاري استعمالها وعلى تقرير ما إذا كانوا يوافقون على هذا الاستعمال أم لا. وتدعم السلامة التكنولوجية الحاجة إلى وجود أمن قوي في البنية التحتية لتكنولوجيا المعلومات والاتصالات وخدماتها وتؤيد تدابير الخصوصية وتنبذ فكرة الوظائف المخفية، لمنع التعديلات غير المرخص بها للمعلومات وترسخ الثقة في دقة المعلومات وكمالها وموثوقيتها.

- تخفيف المخاطر الناجمة عن **البرامج الروبوتية لإنترنت الأشياء** باستعمال معايير أمنية. وتتزايد الحالات المبلغة عن إساءة استعمال أجهزة إنترنت الأشياء (IoT) في هجمات رفض الخدمة الموزعة (DDoS) كبيرة الحجم. ويمكن لهذه الهجمات أن تفضي إلى انتهاكات للبيانات وأضرار كبيرة اقتصادية وخاصة بالسمعة للمنظمات المتأثرة. وتتعين دراسة الكيفية التي يمكن بها تسخير أوجه التقدم في مجالات مثل التشفير الخفيف والطرائق الأمنية المقيسة.

- تقييم أثر **الحوسبة الكمومية** على الأمن والخصوصية والثقة ودراسة **التكنولوجيات الآمنة كمومياً**. وعلى الرغم من أن الحوسبة الكمومية قد لا تزال في مراحلها المبكرة، فمن المتفق عليه على نطاق واسع أنه بمجرد أن يصبح استعمال هذه التكنولوجيا عملياً، فإن طرائق التشفير التقليدية التي تحمي عمليات الدفع التي تتم في الوقت الراهن على الإنترنت والمعاملات المصرفية والبريد الإلكتروني والمحادثات الهاتفية يمكن أن تصبح سريعاً غير كافية. لقد حان الوقت لتقييم أثر الحوسبة الكمومية والبحث والاختبار والتقييس والإعداد من أجل انتقال إلى برامج أمنية جديدة تقاوم الهجمات الكمومية، وذلك قبل أن تصبح أنظمتنا معرضة لهذه الهجمات بوقت كافٍ.

## 3.3 نهج هيئات وضع المعايير فيما يتعلق بالأمن والخصوصية والثقة

*مع الاعتراف بالدور الهام للمعايير في ضمان الأمن وحماية الخصوصية وترسيخ الثقة في البنية التحتية لتكنولوجيا المعلومات والاتصالات وخدماتها؛*

*ومع التأكيد على أن الأمن والخصوصية والثقة مجالات عمل راسخة في كثير من هيئات وضع المعايير الدولية التي تتناول تكنولوجيا المعلومات والاتصالات ومجالات التكنولوجيا الأخرى؛*

*ومع الدعوة إلى التقييس من أجل مواجهة التحديات المتعلقة بالأمن والخصوصية والثقة،*

*أكدت الندوة العالمية للمعايير على:*

- اعتماد مفهوم **الخصوصية من خلال التصميم**، مع إيلاء عناية واجبة لاعتبارات الخصوصية عبر كامل عملية وضع المعايير. ويمكن تشجيع مفهوم الخصوصية من خلال التصميم من خلال معايير تضم سمات الخصوصية وحماية البيانات ومعايير يمكن أن تكون فعالة أيضاً في ضمان التشغيل البيني بين سمات الخصوصية.

- فهم دور **البرمجيات مفتوحة المصدر** في مواجهة التحديات المتعلقة بالأمن والخصوصية والثقة. وتقدم البرمجيات والمعايير مفتوحة المصدر مساهمات تكميلية للنمو والابتكار في صناعة تكنولوجيا المعلومات والاتصالات. وقد شهدت البرمجيات زيادة في تعقيدها، وعلى الرغم من تعاون عالمي البرمجيات مفتوحة المصدر والتقييس في كثير من المجالات، فإنه ينبغي بذل مزيد من الجهود لتسهيل تبادل الأعمال فيما بينهما ومن ثم ضمان عمليات تنفيذ عالية الجودة والأمن للبرمجيات.

- **تعزيز التعاون**بين جهات وضع المعايير من أجل وضع أطر دولية للأمن والخصوصية والثقة، مع الاعتراف بالاختصاصات ومكامن القوة لدى كل منها وتعزيز العمل القائم. وينبغي لهيئات وضع المعايير الالتزام بالإجراءات الأصولية، والتوافق الواسع، والشفافية، والتوازن، والانفتاح في وضع المعايير؛ والالتزام بالجدارة التقنية، وقابلية التشغيل البيني، والمنافسة، والابتكار، وتوفير الفائدة للجميع؛ وإتاحة المعايير للجميع؛ والاعتماد الطوعي للمعايير. وينبغي لهيئات وضع المعايير أن تتعاون أيضاً في جهودها من أجل معالجة التفاوت بين البلدان النامية والمتقدمة في قدرتها على النفاذ إلى المعايير والأطر التي تتناول الأمن والخصوصية والثقة في البنية التحتية لتكنولوجيا المعلومات والاتصالات وخدماتها وتنفيذها، والمشاركة في وضعها على قدم المساواة.

التذييل I

ملخص مفصل لمناقشات الندوة GSS‑16

(لا يشكل هذا التذييل جزءاً من هذا التقرير)

الجلسة 1: ترحيب وكلمات رئيسية

رحّب **سعادة السيد محمد أنور معروف**، وزير تكنولوجيات الاتصال والاقتصاد الرقمي في الجمهورية التونسية [[سيرة ذاتية](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Maarouf)]، ترحيباً حاراً بجميع المشاركين وشكر أعضاء الاتحاد على اختيارهم الحمامات في تونس مكاناً لانعقاد الندوة العالمية للمعايير (GSS) والجمعية العالمية لتقييس الاتصالات (WTSA). وسلط الضوء على ضرورة بناء الثقة والأمل في البنية التحتية لتكنولوجيا المعلومات والاتصالات وخدماتها، اعترافاً بأهمية موضوع الندوة العالمية للمعايير لعام 2016: *الأمن والخصوصية والثقة في مجال التقييس*.

في ملاحظته الافتتاحية، رحب **السيد منجي مرزوق** (الوزير السابق لتكنولوجيا المعلومات والاتصالات في تونس) [[سيرة ذاتية](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Marzoug)]، رئيس الندوة (GSS‑16)، بجميع الحضور في تونس وتمنى لهم إقامة ممتعة في مدينة الحمامات. وسلط الضوء على دور تونس في بناء مجتمع المعلومات وشرح الدور الهام لتكنولوجيا المعلومات والاتصالات (ICT) في حياتنا اليومية في الوقت الراهن واستمرار هذا الدور في المستقبل. وأكد على أهمية خدمات لتكنولوجيا المعلومات والاتصالات مفتوحة وآمنة ومؤمنة وجديرة بالثقة من أجل التنمية في العالم عبر جميع الميادين (مثل الرعاية الصحية والشؤون المالية والمرافق العامة وإنترنت الأشياء (IoT)). وفي هذا السياق، أشار إلى أن للتقييس دوراً رئيسياً من أجل تحسين أمن تكنولوجيا المعلومات والاتصالات وحماية الخصوصية وإرساء الثقة في خدمات تكنولوجيا المعلومات والاتصالات بالنسبة للمواطنين والحكومات والشركات. وأكد على أن الهدف من هذه الندوة العالمية الثالثة للمعايير هو عرض ومناقشة المساهمات بشأن الأمن والخصوصية والثقة في البنية التحتية لتكنولوجيا المعلومات والاتصالات وخدماتها لأصحاب المصلحة الثلاثة الرئيسيين: الحكومات وهيئات التنظيم؛ والصناعة؛ وهيئات وضع المعايير؛ وتقديم استنتاجات وتوصيات بشأن هذه الموضوعات إلى الجمعية العالمية لتقييس الاتصالات لعام 2016.

وشكر **السيد هولين جاو** (أمين عام الاتحاد الدولي للاتصالات) [[سيرة ذاتية](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Zhao)] الجمهورية التونسية التي تستضيف الندوة العالمية للمعايير والجمعية العالمية لتقييس الاتصالات على ما قدمته من دعم لعمل الاتحاد. ولدى وصفة للمساهمة الإيجابية للندوات GSS السابقة، شرح كيف أن الندوة العالمية للمعايير توفر محفلاً دولياً لمناقشة سياسة التقييس، وتجمع القادة من القطاعين العام والخاص للبحث كيف ينبغي للتقييس التقني أن يستجيب لتطور الأولويات في قطاع تكنولوجيا المعلومات والاتصالات. فقد أصبحت استنتاجات وتوصيات الندوتين GSS-08 وGSS-12 جميعها أساسية لبرنامج عمل التقييس في الاتحاد. كما أشار إلى أن بيئة تكنولوجيا المعلومات والاتصالات الموثوقة من شأنها أن تمنح المستعملين وشركات الأعمال الثقة في استعمال تكنولوجيات المعلومات والاتصالات بأقصى إمكاناتها، وإلى أن عمل التقييس في الاتحاد يقوم بدور هام في تحقيق ولاية الاتحاد بشأن "بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات". وفي الختام، أعرب عن امتنانه لجميع المتحدثين والمنسقين والمشاركين على مساهمتهم في الندوة العالمية للمعايير لعام 2016.

وفي كلمته الترحيبية، أوضح **السيد تشيساب لي** (مدير مكتب تقييس الاتصالات بالاتحاد) [[سيرة ذاتية](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Zhao)] كيف سيكون على شبكات المستقبل دعم كبير من تطبيقات تكنولوجيا المعلومات والاتصالات وطيف واسع جداً من الخدمات. وستمكن مليارات الأجهزة الموصولة شبكياً والأشياء والأغراض الأنظمة من التواصل واستقاء المعلومات من بعضها، مما يكوّن أنظمة إيكولوجية ذكية تكيف سلوكياتها لتحقيق الكفاءة. وسيشهد الجيل المقبل من الاتصالات تطبيقات في مجالات تتراوح من الصوت والفيديو إلى الروبوتات الصناعية والنقل الذكي والجراحات الطبية عن بُعد والواقع الافتراضي وغيرها الكثير. وأشار السيد لي إلى أن هذه الزيادة في تعقد تكنولوجيا المعلومات والاتصالات والمستوى غير المسبوق للانتشار الشامل لتكنولوجيا المعلومات والاتصالات سيتطلب تحولات جوهرية في البنية التحتية للشبكات وخدماتها. وفي مجتمعات في طريقها إلى عالم تعتمد فيه جميع الجوانب تقريباً للنشاط الاقتصادي والاجتماعي على تكنولوجيا المعلومات والاتصالات، يصبح من الضروري أن نقِيم بنية تحتية لتكنولوجيا المعلومات والاتصالات وخدماتها تكون جديرة بثقتنا. وسلط الضوء على دور المعايير التقنية في منع نشوء "صوامع" بيانات في قطاعات مختلفة من اقتصاداتنا، وأشار إلى أن الخبراء الذين يشاركون في أعمال التقييس التي يقوم بها الاتحاد يعملون على دعم نشوء نظام إيكولوجي مشترك ومتكامل للبيانات.

الجلسة 2: المبادئ التنظيمية للأمن والخصوصية والثقة

طرحت الجلسة المبادئ التنظيمية للأمن والخصوصية والثقة وتولى إدارتها **الدكتور بلال جاموسي** (رئيس دائرة لجان الدراسات، مكتب تقييس الاتصالات بالاتحاد) [[سيرة ذاتية](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Jamoussi)].

وفي كلمته الرئيسية اعترف **السيد جون إدواردز** (مفوض الخصوصية في نيوزيلندا؛ ورئيس اللجنة التنفيذية لمؤتمر مفوضي حماية البيانات والخصوصية) [[سيرة ذاتية](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Edwards)] بوجود حركة تدريجية، ولكن متسارعة، نحو توافق في الآراء بين منظمات كانت متباينة من قبل، وتوافق في الآراء بأن الخصوصية أصبحت إحدى القضايا التي يتسم بها عصرنا. وسلط السيد إدواردز الضوء على أن الجمعية العامة للأمم المتحدة اعتمدت في دورتها الثامنة والستين (2013) قراراً بعنوان " *الحق في الخصوصية في العصر الرقمي*"، تهيب فيه بجميع الدول الأعضاء في الأمم المتحدة بأن "*تحترم وتحمي الحق في الخصوصية، بما في ذلك في سياق الاتصالات الرقمية*". وعرض العمل الذي تقوم به المنظمة التي يمثلها، المؤتمر الدولي لمفوضي حماية البيانات والخصوصية (ICDPPC)، واقترح بضعة أفكار بشأن زيادة الثقة والأمل من خلال تطبيق مبادئ الخصوصية وربما وضع معايير في قطاع الاتصالات، تشمل:

*-* تشجيع الالتزام بمبادئ الخصوصية عند التصميم وتقييم أثر الخصوصية ووضع تكنولوجيات تعزز الخصوصية.

- ضمان عدم منح الوكلاء الحكوميين النفاذ إلى الشبكات والأنظمة والمحتوى والاتصالات والبيانات الشرحية إلا وفقاً لسلطة القانونية، وفقط في الحالات التي يكون فيها النفاذ ضرورياً ومتناسباً.

- تشجيع الشفافية فيما يتعلق بالنفاذ إلى البيانات الشخصية أو استعمالها لأغراض خلاف تلك التي أبدى صاحب البيانات موافقته عليها.

- وضع معايير وضمانات مناسبة وتعزيزها "لمنع تعرف" البيانات الشخصية ومنع إعادة تعرّف الأفراد من مجموعات بيانات غير معرّفة.

- وضع معايير من أجل إمكانية تنقّل البيانات، ومعايير قادرة على الإسهام في توفير حماية أكبر للمستهلكين وخيار أكبر فيما يتعلق بقدرة المستهلكين على الاشتراك في خدمات تكنولوجيا المعلومات والاتصالات أو إلغاء اشتراكاتهم فيها.

- ضمان استمرار تمتع المواطنين والمستهلكين بالشفافية في ما يتعلق بالأساس الذي استندت إليه القرارات المؤتمتة التي تؤثر عليهم.

وفي مداخلته، تناول **السيد فيكتور مانويل مارتينيز فانيغاس** [[سيرة ذاتية](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Vanegas) | [العرض](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/GSS_IFT_Draft_Presentation.pdf)] (مدير شؤون السياسات الدولية، معهد الاتصالات الفيدرالي، المكسيك) موضوع الندوة من منظور عالمي وناقش المبادرات المتخذة على صعيد إقليمي وقدم سياقاً وطنياً للأمن والخصوصية والثقة في تكنولوجيا المعلومات والاتصالات.

وأوضح إلى أي مدى يمكن أن يكون لتنمية تكنولوجيا المعلومات والاتصالات واعتمادها أثر إيجابي على النمو الاقتصادي والاجتماعي، بيد أن هناك تهديدات وتحديات أيضاً يمكن أن تعرض هذه الفوائد للخطر. فقد أصبح الأمن والخصوصية والثقة عناصر أساسية يتعين مواجهتها بصورة ملائمة. واستشهد من المنشورات والإعلانات والاتفاقات ذات الصلة، بما في ذلك منشور الجمعية العامة للأمم المتحدة، أنشطة التقييس في قطاع تقييس الاتصالات بالاتحاد الدولي للاتصالات واللجنة الكهرتقنية الدولية وتقرير الأونكتاد بشأن اقتصاد المعلومات لعام 2015، اللذان يحددان أن *"الأمن والثقة ضروريان لتهيئة بيئة تمكينية للتجارة الإلكترونية"*. وأشار السيد مارتينيز فانيغاس إلى أن منطقته بشكل خاص، أمريكيا اللاتينية والبحر الكاريبـي، سجلت أسرع نمو في عدد السكان من مستعملي الإنترنت في العالم وأن معالجة الأمن والخصوصية والثقة في تكنولوجيا المعلومات والاتصالات أمر حتمي من أجل التنمية الاقتصادية والاجتماعية في المنطقة. وشدد أيضاً على أن التجارب في المنطقة أظهرت أنه ليس باستطاعة دولة واحدة تأمين شبكاتها بنفسها بصورة وافية وأن التعاون أمر ضروري.

وأوضح **السيد إلياس شانتزوس** (المدير الأول المعني بالشؤون الحكومية، منطقة أوروبا والشرق الأوسط وإفريقيا ومنطقة آسيا والمحيط الهادئ واليابان والمستشار االمعني بحماية البنية التحتية الأساسية والخصوصية، شركة Symantec، الولايات المتحدة) [[سيرة ذاتية](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Chantzos) | [الوثيقة الأساسية](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/InternationalCyberNorms_Ch10%20-%20Symantec.pdf)] كيف تؤثر المحركات السياساتية والتنظيمية وتتأثر بدورها من أوجه التقدم التكنولوجي. واستشهد بلائحة الاتحاد الأوروبي لحماية البيانات العامة كأكثر الأمثلة وضوحاً لهذه الديناميات. ويبلغ عمر التوجيه الحالي بشأن الخصوصية أكثر من 20 سنة، وتتعين مواءمته بشكل كبير لكي يعكس التطور أو الثورة والتكنولوجيا وغيرها من العوامل التي طرأت مثل وسائل التواصل الاجتماعي. وبدوره، أصبح على استعمال التكنولوجيا ووسائل التواصل الاجتماعي الامتثال حالياً للتنظيم الجديد مع التغيرات الأساسية في الطريقة التي ستقود بها منظمات القطاعين العام والخاص إدارة بياناتها، بما في ذلك حماية البيانات الشخصية من الهجمات السيبرانية. كما عرض السيد شانتزوس مفهوم السلامة التكنولوجية الذي يدعم الحاجة إلى وجود أمن قوي في البنية التحتية لتكنولوجيا المعلومات والاتصالات وخدماتها ويؤيد تدابير الخصوصية وينبذ فكرة الوظائف المخفية، لمنع التعديلات غير المرخص بها للمعلومات ويرسخ الثقة في دقة المعلومات وكمالها وموثوقيتها.

وسلط **السيد جيمس م. كيلابا** (القائم بأعمال مدير عام هيئة تنظيم الاتصالات في تنزانيا (TCRA)) [[سيرة ذاتية](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Kilaba) | [العرض](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/GSSWTSA2016-Kilaba.pdf)] الضوء على التحديات المتعلقة بالأمن والخصوصية التي تنشأ من التحول التكنولوجي من زمن كانت فيه بضعة حواسيب شخصية موصولة بالإنترنت إلى الاتصالات في الوقت الراهن من أي شخص ولأي سبب وفي أي مكان وأي زمان. وشرح المبادرات التي اتخذت على الصعيدين الوطني والإقليمي لحماية الخصوصية وتأمين البيانات والبنى التحتية لتكنولوجيا المعلومات والاتصالات. وهي تشمل: إنشاء فريق وطني للاستجابة لحالات الطوارئ الحاسوبية (TZ-CERT) مهمته نشر المعرفة والمعلومات والمهارات المتعلقة بالأمن السيبراني عل مختلف أصحاب المصلحة، وتنفيذ تمديدات أمن نظام أسماء الميادين (DNSSEC) في نظام تسجيل أسماء الميادين، ومناقشة بشأن الأمن السيبراني في منظمة اتصالات شرق إفريقيا (EACO). ودعا السيد كيلابا إلى نهج شامل للتصدي لهذه التحديات وأبرز الحاجة إلى مواءمة المعايير الدولية لدعم البلدان النامية.

وشرح **السيد شوقي قدّاس** (رئيس الهيئة الوطنية لحماية المعطيات الشخصية، تونس) [[سيرة ذاتية](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Gaddes) | [العرض](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/GSS-Gaddes.pdf)]، دور تونس الريادي، من خلال دستورها، في ضمان حماية الخصوصية والبيانات الشخصية (المادة 24، 2014) والنفاذ إلى شبكات المعلومات والاتصالات (المادة 32، 2004) والنفاذ إلى الوثائق الحكومية (يدخل حيّز النفاذ في عام 2017). وأبرز كيف أن تونس تعلق أهمية كبيرة لخلق جوّ من الثقة بين المواطنين والقطاع الخاص والحكومة.

الجلسة 3: كيف تلبي الصناعة توقعات المستعملين النهائيين فيما يتعلق بالأمن والخصوصية والثقة

تولى **السيد إلياس شانتزوس** (المدير الأول المعني بالشؤون الحكومية، منطقة أوروبا والشرق الأوسط وإفريقيا ومنطقة آسيا والمحيط الهادئ واليابان والمستشار االمعني بحماية البنية التحتية الأساسية والخصوصية، شركة Symantec، الولايات المتحدة) إدارة جلسة من جزئين بشأن كيف تلبي الصناعة المبادئ التنظيمية وتوقعات المستعملين النهائيين فيما يتعلق بالأمن والخصوصية والثقة.

وعرض **السيد عمار الكسّار** (المدير التنفيذي لشركة Rohde & Schwarz Cybersecurity، ألمانيا) [[سيرة ذاتية](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Alkassar) | [العرض](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/3-1201601024_ITU%20GSS16_ALKASSAR_2.pptx)] الاتجاهات في تكنولوجيا المعلومات والاتصالات التي ستغير عالمنا بطريقة مستدامة. وشرح كيف أن الأمن السيبراني سيشكل عاملاً أساسياً لهذا التغيير، وكيف أنه سيصبح أكثر أهمية في المستقبل. وشدد السيد الكسّار على أن الأدوات الأمنية المنتشرة اليوم هي أبعد من أن تكون كافية مقارنة بالقيم الاقتصادية الواجب حمايتها. وشرح الحاجة إلى تحديد مجموعات جديدة من المعايير بعد التحول عن النموذج في أمن تكنولوجيا المعلومات لمواكبة بيئة التهديدات التي يتزايد ذكاؤها. وبحسب Rohde & Schwarz، فإن هذا التحول عن النموذج سيتألف من العناصر التالية: تنفيذ الأمن عند التصميم، واستخدام تدابير استباقية بدلاً من تدابير الاستجابة، والبناء على التحكم في تدفق المعلومات بدلاً من التحكم في النفاذ، والحيلولة دون تحميل المستعملين مسؤوليات غير قابلة للأداء فيما يتعلق بالأمن السيبراني. وأشار إلى أن بوسع مجتمع الاتحاد أن يقدم مساهمات كبيرة في هذا المجال، ولا سيما من خلال أنشطته المتعلقة بالتقييس ووصل مجتمع الاتصالات التقليدي بالجهات الفاعلة في تكنولوجيا المعلومات والاتصالات.

وأكد **الدكتور توماس كريمر** (عضو مجلس الإدارة لشؤون خصوصية البيانات والشؤون القانونية والامتثال، شركة Deutsche Telekom، ألمانيا) [[سيرة ذاتية](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Kremer) | [العرض](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Deutsche%20Telekom%20-%20final.pptx) | [الوثيقة الأساسية](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Getting%20out%20of%20the%20digital%20trust%20trap%20-%20deutsche%20telekom.pdf)] على أن الشفافية شرط أساسي للثقة. ويجب أن يتسنى للناس معرفة كيف تُستعمل بياناتهم ويجب أن يكونوا قادرين على أن يقرروا عن وعي ما إذا كانوا يوافقون على هذا الاستعمال أم لا. ومع ذلك، لا تكون الشفافية كافية بمفردها إذا أرادت الشركات الارتقاء إلى مسؤولياتها الرقمية. وطالب الدكتور كريمر بأنظمة يمكنها أن تغفل البيانات بموثوقية في جميع حالات الاستعمال دون الحاجة إلى إحالة شخصية مباشرة. وقد حدد التجفير كوسيلة أخرى لبناء ثقة العميل، خاصة في سياق البيانات الحساسة مثل البيانات الصحية. وطبقاً لشركة Deutsche Telekom، فإن أي مقترح بتزويد السلطات "بمفاتيح احتياطية" أو "سبل نفاذ سرية" لتأمين الأنظمة سيثبت أنه معوق للإنتاجية ويحبط جهود تعزيز الأمن، حيث ستُستغل هذه الأدوات سريعاً من جانب الخصوم. وطالب الدكتور كريمر بحلول ذكية قابلة للاستعمال وملائمة من حيث التوقيت في مجال الأمن السيبراني. ومع ظهور تكنولوجيات جديدة (إنترنت الأشياء، والتعلم الآلي والحوسبة الكمومية، وغيرها)، ستصبح الهجمات أكثر تعقيداً. ويتعين وجود نُهج مقيسة لكشف المخاطر والهجمات وتخفيف حدتها.

وأوضح **السيد دافيد فرانسيس** (مسؤول الأمن السيبراني في أوروبا، شركة Huawei Technologies، الصين) [[سيرة ذاتية](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Francis) | [العرض](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Huawei%20-%20final.pptx)] ما الذي تطلبه حماية الخصوصية والأمن من منظور موردي التكنولوجيا. وناقش السياسات والعمليات القائمة في شركة مثل Huawei Technologies لضمان الأمن والصمود لمنتجاتها وهو ما يؤدي في نهاية الأمر إلى المساعدة على حماية خصوصية وبيانات المستعمل النهائي. وتشمل العناصر الأساسية التي يجب النظر فيها في نهج شامل: الأجهزة الآمنة، والمعمارية – حيث تُنشأ الشبكة من عدة منتجات معقدة؛ والأشخاص الذين يهيئون البيئة ويديرونها ويحدثونها ويقومون بصيانتها وتقييمها. وتناول السيد فرانسيس الحاجة إلى إدارة لسلسلة الإمداد العالمية يعتمد فيها قطاع تكنولوجيا المعلومات كلياً على تخفيف حدة أي مخاطر أمنية ودور الشفافية والمعايير العالمية إضافة إلى الحاجة إلى التعاون الدولي من أجل تحسين الأمن السيبراني حول العالم.

وبحثت **السيدة جايا بالو** (كبيرة مسؤولي أمن المعلومات، شركة KPN، هولندا) [[سيرة ذاتية](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Baloo) | [العرض](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/3-4ITU-GSS-Tunesia.pdf)] في السباق نحو التكنولوجيات الكمومية بدءاً بالحوسبة الكمومية وانتهاء بالتجفير الكمومي. ويشكل توافر حاسوب كمومي خطراً أمنياً على البلدان والشركات التي تعتمد على التجفير اللامتناظر RSA)، (ECC. والإجابة الضرورية المطلوبة هي الحلول ما بعد الكمومية التي قد تطرح على ثلاث مراحل. أولاً، زيادة طول المفتاح في خوارزميات التجفير الحالية. ثانياً، استعمال توزيع كمومي للمفاتيح في نقاط حرجة محددة من الشبكات. ثالثاً، استحداث ودعم خوارزميات تجفير ما بعد كمومية تصمد في المستقبل. ويحقق المجتمع العالمي لأمن المعلومات خطوات في الابتكار حول التكنولوجيات الكمومية. ومع ذلك، ثمة خطر في أن يشكل ذلك فجوة أمنية رقمية جديدة تزيد الهوة بين البلدان التي تملك الموارد المالية والأكاديمية لامتلاك حاسوب كمومي قادر على اختراق تجفير البلدان الأخرى وحماية الاتصالات الخاصة بها في الوقت نفسه، وبين البلدان التي لا تستطيع أن تهاجم أو تدافع عن أنفسها.

وأشار **السيد جيمس سنو** (خبير استراتيجي في مجال الأمن والمطابقة، شركة غوغل، الولايات المتحدة) [[سيرة ذاتية](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Snow) | [العرض](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Google-final.pptx) | [الوثيقة الأساسية](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/GoogleExecSummary_2016.pdf)] إلى أن من بين الأولويات الرئيسية لشركة غوغل لكسب ثقة عملائها والاحتفاظ بها، معالجة البيانات في بيئة مؤمنة وموثوقة ومطابقة. فالأمن والخصوصية أمران يتسمان بالأهمية البالغة لشركة غوغل، وهذا هو السبب وراء استثمار الشركة بشكل كبير من أجل حماية بيانات العملاء. ويشمل ذلك استعمال مخدمات مؤمنة وبنى تحتية شبكية محددة الأغراض وتجفير بيانات العملاء سواء كانت على الطاولة أو مخزنة في وسائط احتياطية أو تنتقل عبر الإنترنت أو تسافر بين مراكز البيانات.

وأوضح السيد سنو كيف تبدأ ثقة العميل بالفهم، وأن الفهم لا يمكن أن ينشأ إلا من خلال الشفافية، وذلك مثلاً من خلال توفير المستندات التفصيلية وتقارير المراجعة والشهادات. وتقر شركة غوغل بأهمية التعاون الدولي وتعزيز العديد من المعايير الدولية بشأن الأمن والخصوصية بما في ذلك ما يلي:

- المعيار ISO 27001:2013، تكنولوجيا المعلومات - تقنيات الأمن - أنظمة إدارة أمن المعلومات - المتطلبات؛

-المعيار ISO 27017:2015، تكنولوجيا المعلومات - تقنيات الأمن - مدونة القواعد المراعية لضوابط أمن المعلومات في خدمات الحوسبة السحابية استناداً إلى المعيار ISO/IEC 27002 بشأن الحوسبة السحابية؛

- المعيار ISO 27018:2014، تكنولوجيا المعلومات - تقنيات الأمن - مدونة القواعد لحماية المعلومات المحددة لهوية الشخص وخدمات الحوسبة السحابية العمومية التي تعمل كوسائل معالجة لهذه المعلومات؛

- المعيار SOC 2/SOC 3، إطار مراجعة بشأن المبادئ غير المتعلقة بالخصوصية والتي تضم الأمن والتيسر وسلامة المعالجة والسرية.

وتطرق **الدكتور يوجين دو** (نائب الرئيس المعني بالأمن، شركة Alibaba Group، الصين) [[سيرة ذاتية](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Du) | [العرض](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Yuejin-DU.pptx)] إلى أهمية الأمن والخصوصية في البنية التحتية التي توفرها الشركة لعملائها في مجال التجارة وتكنولوجيا البيانات. فعلى سبيل المثال، توفر الشركة منتجات لأمن المعلومات للشركاء وتعزز المعايير من خلال التحالف بشأن أمن النظام الإيكولوجي للتجارة الإلكترونية (EESA)، الذي أطلقته الشركة في يوليو 2016. في هذا التحالف يتسنى للشركة وشركاؤها تسخير نماذج اكتشاف المخاطر القائمة لفحص التهديدات وتحديدها، والعمل معاً لتعزيز الأمن وحماية الخصوصية في النظام الإيكولوجي للتجارة الإلكترونية من خلال تنفيذ معاير التحالف القائمة.

وأوضح **السيد بيرنارد بينواه** (مدير عام White Noise / Kudelski Security، سويسرا) [[سيرة ذاتية](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Benoit) | [العرض](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Kudelski%20-%20final.pdf)] التضارب المحتمل في مصالح المستعملين وموردي الخدمات والحكومات وكيف أن شبكات الاتصالات القائمة محفوفة بالثغرات الأمنية وبالتالي، غير قادرة على ضمان أمن الاتصالات وخصوصيتها. ولتقوية الأمن والخصوصية على شبكات غير موثوقة، استنبط مكون عتاد أمني قابل للتوسع يقوم على نهج وحدات فك التشفير، يتم تشغيله بشكل مستقل عن الشبكات والبروتوكولات الأساسية. وذكر السيد بينواه الحضور بالحاجة إلى حلول لا تعتمد على المنصات مع سطوح بينية مقيسة متوافقة لكي تلبي متطلبات الاعتراض القانوني السارية، دون تعريض السلامة التكنولوجية للخطر من خلال سبل النفاذ السرية والمفاتيح الاحتياطية وما إلى ذلك.

الجلسة 4: نهج هيئات وضع المعايير فيما يتعلق بالأمن والخصوصية والثقة

جرى في الجلسة 4 استعراض للنهج المتبعة في منظمات وضع المعايير (SDO) المختلفة فيما يتعلق بالأمن والخصوصية والثقة. وتولى إدارة الجلسة **السيد طوني عيد** (رئيس تحرير مجلة Telecom Review) [[سيرة ذاتية](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Eid)].

وقدمت **السيدة صوفي كليفيو** (مديرة التقييس والسياسات التقنية، المنظمة الدولية للتوحيد القياسي (ISO)) [[سيرة ذاتية](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Clivio) | [العرض](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/ISO%20-%20final.PPTX)] نهج المنظمة الواسع ومتعدد القطاعات في مجال الأمن والخصوصية والثقة. وركزت على عمل لجان المنظمة المعنية بالأمن والصمود؛ وإدارة المخاطر؛ وتكنولوجيات السجلات الإلكترونية وقواعد بيانات سلاسل المجموعات الموزعة؛ والأنشطة المشتركة للمنظمة ISO واللجنة الكهرتقنية الدولية بشأن أمن المعلومات والخصوصية في اللجنة المشتركة المعنية بتكنولوجيا المعلومات (ISO/IEC JTC 1). وتشمل المجالات الرئيسية التي تغطيها اللجنة JTC 1 إدارة أمن المعلومات، وإدارة التجفير والأمن، وتكنولوجيا إدارة الهوية والخصوصية، والقياسات البيومترية؛ وتعرف هوية البطاقات والأشخاص؛ وإدارة تكنولوجيا المعلومات؛ وآليات الأمن والخصوصية والثقة من أجل الحوسبة السحابية والبيانات الضخمة وإنترنت الأشياء. وأشارت السيدة كليفيو إلى أن للمنظمة ISO ومعاييرها حضوراً في القطاعات الاقتصادية بما في ذلك الرعاية الصحية والنقل (مثل الطيران، وأنظمة النقل الذكية والتكنولوجيا البحرية) والطاقة والتشييد والتصنيع (بما في ذلك التصنيع الجمعي) وأنه قد أبرمت اتفاقات تعاون مع منظمات تعمل على معالجة احتياجات وخصائص هذه القطاعات.

وشرح **السيد فرانس فريزويجك** (الأمين العام والمدير التنفيذي للجنة الكهرتقنية الدولية (IEC)) [[سيرة ذاتية](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Vreeswijk) | [العرض](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/IEC%20-%20final.pptx)] كيف جمعت اللجنة الكهرتقنية الدولية جميع أصحاب المصلحة في مجال التكنولوجيا الإلكترونية في مسعى لبناء الثقة في منتجات وأنظمة آمنة وكفوءة من خلال استخدام المعايير الدولية للجنة IEC وأنظمة اللجنة IEC لتقييم المطابقة. وقد نشرت اللجنة أكثر من 200 معيار في الأمن السيبراني مع تركيز خاص على حماية البنى التحتية الأساسية من قبيل توليد الكهرباء وتوزيعها، وإدارة المياه والمخلفات، والمستشفيات والرعاية الصحية، والتصنيع ومراكز البيانات، من مواطن الضعف والهجمات السيبرانية. كما ساهمت اللجنة في إيجاد طريقة هامة لسلامة وأمن جميع الأعتدة الكهربائية والإلكترونية التي تتيح جمع البيانات أو النفاذ إليها وتفعّل بروتوكولات التحكم. ويشمل ذلك، على سبيل المثال، أجهزة الاستشعار والأجهزة الطبية والأجهزة الذكية التي يمكن ارتداؤها فضلاً عن تكنولوجيات الحوسبة وتخزين البيانات. وتعد المعايير الدولية التي وضعتها اللجنة عوامل أساسية في البحث عن تحسين المرونة وإدارة المخاطر والكفاءة.

وتتعاون اللجنة بشكل وثيق مع المنظمة الدولية للتوحيد القياسي (ISO) من خلال اللجنة المشتركة المعنية بتكنولوجيا المعلومات (ISO/IEC JTC1) في مجالات من قبيل إدارة أمن المعلومات، وإدارة الهوية، والتجفير والتعرّف الآمن، والتكنولوجيات المتعلقة بالخصوصية، والقياس الحيوي، والبطاقات والتعرّف الشخصي، والحوسبة السحابية، والبيانات الضخمة، وما إلى ذلك. واللجنة على علاقة مستمرة مع الاتحاد، إلى جانب المنظمة الدولية للتوحيد القياسي من خلال التعاونية العالمية للمعايير القياسية.

ودعا السيد فريزويجك إلى تعاون واسع بين جميع منظمات وضع المعايير للتعاطي مع مواضيع الأمن والخصوصية والثقة. وفي جوهر الأمر، لا توجد منظمة واحدة قادرة على تقديم جميع المعايير المطلوبة في هذا المجال.

وأكدت **السيدة كارين مكيب** (مديرة أولى لسياسات التكنولوجيا والشؤون الدولية، رابطة المعايير التابعة لمعهد مهندسي الكهرباء والإلكترونيات (IEEE‑SA)) [[سيرة ذاتية](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#McCabe) | [العرض](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/IEEE-final.pptx)] على أن للمعايير دوراً حاسماً في المساعدة على ضمان الأمن والخصوصية والثقة في تكنولوجيا المعلومات والاتصالات. وللتمكن من أداء هذا الدور، فإن من بين أفضل الممارسات العمل في إطار مجموعة من المبادئ، يفضي إلى مجتمع عالمي للتعاون الطوعي بين الأطراف المعنية ويسمح بالتميز التقني وقابلية التشغيل البيني عالمياً والابتكار. وتشمل هذه المبادئ المشاركة المباشرة؛ والعمليات الواجبة؛ والتوافق الواسع في الآراء؛ والتوازن؛ والشفافية؛ والانفتاح الشامل؛ والتماسك؛ والبعد المتعلق بالتنمية.

وأشارت إلى أن العمليات المفتوحة تعتبر ممارسات جيدة من منظور أمني، حيث يمكن من خلال الاستعراض الذي يقوم به خبراء متعددون اكتشاف الثغرات المحتملة وتحسين المعايير عند تطويرها. وتزيد الشفافية في العملية المفتوحة لوضع المعايير من الثقة في المنصات والخدمات والمنتجات القائمة على هذه المعايير والملتزمة بها. بالإضافة إلى ذلك، فإن المعايير المفتوحة تتيح لتكنولوجيات تعزيز الخصوصية والأمن، تبنيها على نطاق واسع نظراً إلى أنها تعزز قابلية التشغيل البيني. واختتمت بالقول إن المعايير المفتوحة تغذي الابتكار الذي يمكن أن يدفع بحلول لمواجهة التحديات المتعلقة بالأمن والخصوصية والثقة.

ولمعهد مهندسي الكهرباء والإلكترونيات مجموعة كبيرة من المعايير في حافظته، تبدأ من اعتبارات الأمن والخصوصية والثقة بالنسبة للسلسلة IEEE 802 لمعايير الشبكات، وصولاً إلى التجفير في السلسلة IEEE 1363 (مع التركيز على الخوارزميات القائمة على البنية التحتية للمفاتيح العمومية (PKI)، وفي السلسلة IEEE 1619، وغيرها الكثير. وفريق أمن توصيلات الصناعة التابع للمعهد (ICSG) عبارة عن فريق من كيانات أمن الحاسوب التي توحدت لتجميع الخبرات والموارد في مجال مكافحة الزيادة المنتظمة والسريعة في التهديدات الأمنية لأجهزة الحاسوب. وفي جهد آخر في الفترة الأخيرة، أطلقت مبادرة الإنترنت للمعهد IEEE لزيادة تأثير المنظمة وحضورها في سياسات التكنولوجيا العالمية في مجالات إدارة الإنترنت والأمن السيبراني ووضع سياسات الخصوصية من خلال تحقيق توافق في الآراء حول المعارف التقنية والعلمية السليمة وتقديم التوجيهات للعملية. والمبادرة العالمية للمعهد IEEE بشأن الاعتبارات الأخلاقية في تصميم أنظمة مستقلة واللجنة المخصصة التابعة لها للأخلاقيات والمجتمع والتكنولوجيا، تقوم باستكشاف معايير جديدة وحلول، وشهادات ومدونات سلوك، وبناء توافق في الآراء بشأن التنفيذ الأخلاقي للتكنولوجيات الذكية، بما في ذلك الذكاء الاصطناعي والأنظمة المستقلة.

وواصلت السيدة مكيب بالدعوة إلى إشراك جيل جديد من مهنيي الخصوصية والأمن والأخلاقيات من شتى القطاعات في عمليات وضع المعايير وإرساء الخصوصية والأمن والأخلاقيات ضمن المعايير المفتوحة ذاتها من أجل الإسهام في بناء الثقة في تكنولوجيا المعلومات والاتصالات.

وأكد **السيد أشوك غانيش** (المدير المسؤول عن الابتكار باللجنتين الأوروبيتين للتقييس (CEN) والتقييس الكهرتقني (CENELEC)) [[سيرة ذاتية](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Ganesh) | [العرض](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/CEN-CENELEC-final.pptx)] أن جميع قطاعات الصناعة تشهد تحولاً مع تبنيها للتكنولوجيات والنهج الرقمية (مثل إنترنت الأشياء والحوسبة السحابية والروبوتات وتكنولوجيات أجهزة الاستشعار) التي تغير عملياتها وأنظمتها، بل ونماذج الأعمال الخاصة بها بصورة جذرية. وقطاعات الصناعة الرأسية التقليدية هذه (مثل التصنيع والطاقة والنقل) التي لم تكن من المستعملين الأساسيين لتكنولوجيا المعلومات والاتصالات والتكنولوجيات الرقمية من قبل، تلتمس الدعم وحلول التقييس من أجل هذا التحول. وأشار السيد غانيش إلى أن منظمات وضع المعايير مثل ISO وIEC وCEN وCENELEC في أوروبا "بصمة" واضحة في هذه القطاعات الرأسية وترغب في تطوير نهجها من أجل تلبية هذه الاحتياجات ذات الصلة بتكنولوجيا المعلومات والاتصالات/التكنولوجيات الرقمية. وينطوي تبني هذه التكنولوجيات على إدخال أنظمة من أجل المنشآت الصناعية وعمليات التصنيع إضافة إلى توليد ومعالجة وتبادل وتخزين كميات ضخمة من البيانات. وأشار السيد غانيش إلى أن التحدي الماثل أمام منظمات وضع المعايير متعدد الجوانب: الحفاظ على إشراك أصحاب المصلحة التقليديين وجذب أصحاب المصلحة في مجال تكنولوجيا المعلومات والاتصالات/التكنولوجيات الرقمية وتعديل نهجها لكي يتسنى لها تقديم حلول التقييس بصورة مباشرة وغير مباشرة في مجال متزايد التعقيد وسريع التغير. ومن أولويات منظمات وضع المعايير التركيز على الاحتياجات والتطبيقات الرأسية، بما في ذلك معالجة الربط بين الأمن السيبراني والسلامة الوظيفية واعتمادية المنتجات وأمن البيانات والخصوصية.

وذكّر **الدكتور رينهارد شول** (نائب مدير مكتب تقييس الاتصالات بالاتحاد الدولي للاتصالات) [[سيرة ذاتية](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Scholl) | [العرض](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Reinhard-final.pptx)] جميع المشاركين بندوة الأمن السيبراني التي عُقدت على هامش الجمعية WTSA-04 في فلوريانوبوليس، البرازيل. وقد اختتم هذا الحدث بـ 11 رسالة رئيسية ما زال معظمها صالحاً إلى اليوم، مثل "الأمن عنصراً أساسياً وليس مكملاً"، أو "أصحاب المصلحة بحاجة إلى تقاسم المعلومات"، أو " التقييس هو بالضرورة جزء حيوي في النهج العالمي للأمن السيبراني".

ولتوضيح الحالة السائدة اليوم، قدم بعض الأرقام عن عدد الحوادث السيبرانية المعروفة في البنية التحتية لشبكة الاتحاد. وذكر أن الأمن والخصوصية هما برأيه أمران لا يستبعد أحدهما الآخر. كما شرح أن عمل الاتحاد من أجل بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات يتواصل بكثافة في مسعى من أجل تيسير تطوير بنى تحتية للشبكات وخدمات وتطبيقات أكثر أمناً. وعرض الأعمال الحديثة للاتحاد في مجالات الأمن والثقة، بما في ذلك تقرير يشدد على أهمية وضرورة الثقة في بيئة تكنولوجيا المعلومات والاتصالات وطرح المفاهيم ذات الصلة والسمات الرئيسية للثقة. ومن بين الأفكار التي يناقشها التقرير "دليل الثقة"، وهو رقم يجمع عدة مؤشرات متعلقة بالثقة في مؤشر قياس مرجعي واحد. ويمكن استخدام دليل الثقة لمقارنة الثقة بين أصحاب المصلحة حين ينشؤون علاقات ثقة جديدة أو سلسلة من قيم الثقة.

وأشار الدكتور شول إلى أن الأعضاء استهلوا العمل من أجل استكشاف جملة أمور من بينها المتطلبات والقدرات وسيناريوهات الخدمة من أجل توفير الثقة؛ والإطار المعماري من أجل شبكات اتصالات جديرة بالثقة؛ والحلول التقنية لتوفير الثقة؛ وتوفير الثقة في تحليلات البيانات الضخمة؛ وإدارة الثقة بين الخدمات السحابية. وتغطي جهود التقييس بقطاع تقييس الاتصالات في هذا الشأن مجالات مثل الأمن السيبراني؛ وإدارة الأمن؛ ومعماريات وأطر الأمن؛ ومكافحة الرسائل الاقتحامية؛ وإدارة الهوية؛ وحماية المعلومات التي يمكن التعرف على هوية أصحابها.

كما أوصى السيد شول بدراسة المساهمة التي يقدمها مجتمع المصادر المفتوحة إلى المعايير التي تتناول الأمن والخصوصية والثقة في البنية التحتية لتكنولوجيا المعلومات والاتصالات وخدماتها, وقال إنه ينبغي بذل المزيد من الجهود لتسهيل تبادل العمل بين مجتمع المصادر المفتوحة ومجتمع التقييس، وبالتالي ضمان تنفيذ المعايير العالية الجودة والبرمجيات.

الحواشي

1. ’‘ انظر على سبيل المثال التوصية ITU‑T X.1171 "التهديدات ومتطلبات حماية المعلومات التي يمكن تعرف هوية أصحابها شخصياً في التطبيقات التي تستعمل تعرف الهوية على أساس العلامة [↑](#endnote-ref-1)
2. ’‘ انظر على سبيل المثال القرار 130 (المراجَع في بوسان، 2014) بشأن تعزيز دور الاتحاد في مجال بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات [↑](#endnote-ref-2)
3. ’‘ <http://www.un.org/en/universal-declaration-human-rights/> [↑](#endnote-ref-3)
4. ’‘ <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx> [↑](#endnote-ref-4)
5. ’‘ [http://www.un.org/documents/ga/res/45/a45r095.htm؛](http://www.un.org/documents/ga/res/45/a45r095.htm%D8%9B) وثيقة الأمم المتحدة E/CN.4/1990/72 <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G90/107/08/PDF/G9010708.pdf?OpenElement> [↑](#endnote-ref-5)
6. ’‘ <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37> [↑](#endnote-ref-6)
7. ’‘ <http://www.echr.coe.int/Documents/Convention_ENG.pdf> [↑](#endnote-ref-7)
8. ’‘ <https://www.oas.org/dil/treaties_B-32_American_Convention_on_Human_Rights.htm> [↑](#endnote-ref-8)
9. ’‘ انظر على سبيل المثال إطار الخصوصية لمجلس التعاون الاقتصادي لآسيا والمحيط الهادئ (APEC) والإطار التنظيمي بشأن الخصوصية للاتحاد الأوروبي والمستوحيين إلى حد ما من المبادئ التوجيهية لحماية الخصوصية وتدفقات البيانات الشخصية العابرة للحدود الصادرة عن منظمة التعاون والتنمية في الميدان الاقتصادي <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf> [↑](#endnote-ref-9)
10. ’‘ إعلان مونترو للمؤتمر الدولي لمفوضي حماية البيانات والخصوصية، <https://icdppc.org/wp-content/uploads/2015/02/Montreux-Declaration.pdf> [↑](#endnote-ref-10)
11. ’‘ القرار 68/167 للجمعية العامة للأمم المتحدة،<http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167> [↑](#endnote-ref-11)