المجلس الأعلى للاتصالات وتكنولوجيا المعلومات
Supreme Council of Information & Communication Technology

الاتحاد الدولي للاتصالات

المنتدى الإقليمي للاتحاد بشأن الأمن السيبراني 2008
الدوحة، قطر

الوثيقة: RWD/2008/01-A
21 فبراير 2008
الأصل: بالإنكليزية

تقرير الاجتماع:

ورشة العمل الإقليمية للاتحاد بشأن أطر الأمن السيبراني وحماية البنية التحتية الحرجة للمعلومات (CIIP) وورشة العمل بشأن الأدلة القضائية في الأمن السيبراني، الدوحة، قطر، 18-21 فبراير 2008[1]

يرجى إرسال أي ملاحظات بشأن تقرير هذا الاجتماع إلى cybmail@itu.int

الغرض من هذا التقرير

1. عُقدت ورشة العمل الإقليمية بشأن أطر الأمن السيبراني وحماية البنية التحتية الحرجة للمعلومات (CIIP) وورشة العمل بشأن الأدلة القضائية في الأمن السيبراني، في الدوحة، قطر، 18-21 فبراير 2008. وترمي ورشة العمل، التي استضافها المجلس الأعلى للاتصالات وتكنولوجيا المعلومات في قطر (ictQATAR) ونُظِّمت بالتعاون مع فريق الاستجابة لطوارئ الحاسوب (Q-CERT)، إلى تحديد التحديات الرئيسية التي تواجهها البلدان في المنطقة لدى وضع أطر للأمن السيبراني ولحماية البنية التحتية الحرجة للمعلومات، وللنظر في أفضل الممارسات وتقاسم المعلومات بشأن أنشطة التنمية التي يضطلع بها الاتحاد الدولي للاتصالات وغيره من الهيئات، واستعراض دور مختلف الجهات الفاعلة في النهوض بثقافة الأمن السيبراني.

2. وقد عُقدت ورشة العمل، وهي واحدة في سلسلة لقاءات إقليمية بشأن الأمن السيبراني ينظمها قطاع تنمية الاتصالات في الاتحاد، استجابة للقرار 130 الصادر عن مؤتمر المندوبين المفوضين للاتحاد: تعزيز دور الاتحاد في بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات (أنطاليا، 2006) وخطة عمل الدوحة المنبثقة عن المؤتمر العالمي لتنمية الاتصالات لعام 2006 التي وضعت المسألة 22/1 للجنة دراسات قطاع التنمية: *تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني*. وكجزء من هذا النشاط يعكف الاتحاد على وضع *تقرير عن أفضل الممارسات من أجل نهج وطني للأمن السيبراني* تحددت فيه خمسة عناصر رئيسية للجهود الوطنية، وهي: 1) وضع استراتيجية وطنية للأمن السيبراني؛ 2) إقامة تعاون بين الحكومة الوطنية والصناعة؛ 3) استحداث مقدرة وطنية لإدارة الحوادث؛ 4) ردع الجريمة السيبرانية؛ 5) النهوض بثقافة أمن سيبراني. ونظرت ورشة العمل أيضاً في مبادرات تُتخذ على الأصعدة الإقليمية والدولية لزيادة التعاون والتنسيق بين مختلف أصحاب المصلحة.

3. وشارك في اللقاء نحو 100 شخص، من الدول العربية ومن أجزاء أخرى من العالم. ويمكن الاطلاع على كامل وثائق الورشة، بما في ذلك جدول الأعمال النهائي وجميع العروض التي قُدِّمت، في العنوان www.itu.int/itu-d/cyb/events/2008/doha/. ويلخِّص تقرير الاجتماع هذا المناقشات التي دارت طوال ثلاثة أيام لورشة

[1] موقع المنتدى الإقليمي للاتحاد بشأن الأمن السيبراني: http://www.itu.int/ITU-D/cyb/events/2008/doha/.

العمل الإقليمية بشأن أطر الأمن السيبراني وحماية البنية التحتية الحرجة للمعلومات، ويقدم صورة إجمالية للجلسات وعروض المتحدثين كما يقدم بعض المواقف ونقاط التفاهم المشتركة التي تم التوصل إليها أثناء اللقاء. ويتضمن الملحق 1 في نهاية الوثيقة نقاط التفاهم المشتركة التي اتفق عليها المشاركون في اللقاء، بما في ذلك إعلان الدوحة بشأن الأمن السيبراني.[2]

ورشة العمل الإقليمية بشأن أطر الأمن السيبراني وحماية البنية التحتية الحرجة للمعلومات (CIIP) التي عُقدت في الدوحة، قطر، 18-20 فبراير 2008

4. من قبيل المعلومات الأساسية، وبما أن المجتمعات الحديثة تزداد اعتماداً على تكنولوجيا المعلومات والاتصالات المتواصلة فيما بينها عالمياً، يتزايد إدراك البلدان بأن هذا الوضع يخلق اعتمادات متبادلة ومخاطر يتعيَّن إدارتها على الأصعدة الوطنية والإقليمية والدولية. ولذلك فإن تعزيز الأمن السيبراني وحماية البنى التحتية الحرجة للمعلومات مسألة أساسية لأمن كل بلد ورفاهه الاجتماعي والاقتصادي. وهذه مسؤولية مشتركة، على الصعيد الوطني، تتطلب إجراءات منسَّقة تتصل بجوانب الوقاية والتأهب والاستجابة وتجاوز الحوادث من جانب السلطات الحكومية والقطاع الخاص والمواطنين. ويتطلب ذلك، على الصعيدين الإقليمي والدولي، التعاون والتنسيق مع الشركاء المعنيين بالأمر. ولذلك فإن صياغة وتنفيذ إطار وطني للأمن السيبراني وحماية البنية التحتية الحرجة للمعلومات يتطلب نهجاً شاملاً متعدد التخصصات ومتعدد أصحاب المصلحة. وقد ناقش هذا المنتدى الإقليمي للأمن السيبراني بعض العناصر الرئيسية التي تدخل في وضع مثل هذه السياسة والأطر التنظيمية.

افتتاح اللقاء والترحيب بالحضور

5. افتُتحت ورشة العمل الإقليمية بشأن أطر الأمن السيبراني وحماية البنية التحتية الحرجة للمعلومات بكلمة ترحيب[3] ألقتها الدكتورة حصة الجابر، الأمين العام، المجلس الأعلى للاتصالات وتكنولوجيا المعلومات في قطر (ictQATAR). ورحَّبت الدكتورة الجابر، باسم المجلس الأعلى، بالمشاركين في ورشة العمل وسلطت الأضواء على أهمية ورشة العمل هذه بمثابة خطوة هامة نحو بناء مقدرة الأمن السيبراني في المنطقة. كما رحَّبت الدكتورة الجابر بالسيد سامي البشير المرشد، مدير مكتب تنمية الاتصالات في الاتحاد، والسيد ريتش بتيا، مؤسس ومدير فريق الاستجابة لطوارئ الحاسوب (CERT) الأول من نوعه في جامعة كارنيغي ميلون في الولايات المتحدة الأمريكية. ونوَّهت بأن الفريق CERT كان لنحو عشرين سنة يسهم في حماية المعلومات القيِّمة والحفاظ على البنى التحتية في شتى بلدان العالم، وأن قطر واحدة من هذه البلدان منذ العام الماضي. وفي عام 2007 أطلقت قطر برنامجاً وطنياً لأمن المعلومات يرمي إلى حماية كل من البالغين والأطفال على شبكة الإنترنت. وأشارت الدكتورة الجابر أيضاً إلى أن هذه المبادرة تساعد أيضاً في حماية البيانات التابعة للشركات والمنظمات.

6. ونوَّهت الدكتورة الجابر بأن المؤتمر العالمي لتنمية الاتصالات لعام 2006، الذي عُقد في الدوحة، قطر، أرسى ما يُعرف الآن باسم خطة عمل الدوحة.[4] وقالت إن قطر تمضي قُدماً في تنفيذ توصيات خطة العمل وأشارت إلى أن قطر فتحت منذ ذلك المؤتمر سوق الاتصالات أمام المنافسة ومشاركة القطاع الخاص، وصاحب ذلك بناء منصَّات بنى تحتية مشتركة وغرس البذور الطيبة لبناء مجتمع معلومات عالمي حقاً من شأنه أن يصل بالتكنولوجيا كل أولئك الذين يعيشون ويعملون في قطر. كما أطلق المؤتمر العالمي لعام 2006 رسمياً المسألة 22/1 للجنة دراسات تنمية الاتصالات، بعنوان: *تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني*. ونظراً للأهمية الملحّة التي تتسم بها مسألة الأمن السيبراني بالنسبة لكل بلد، فقد سلّطت الدكتورة الجابر الأضواء على ضرورة تحسين الأمن السيبراني والعمل في الوقت ذاته على المضي قُدماً بتكنولوجيا المعلومات والاتصالات مع كل ما تجلبه من المنافع العميمة. واختتمت الدكتورة

---

2 يمكن الاطلاع أيضاً على إعلان الدوحة بشأن الأمن السيبراني في العنوان:
http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/doha-regional-cybersecurity-forum-output-20-feb-08.pdf.

3 http://www.ict.gov.qa/files/DrHessaopeningremarks4%20ITUforum.pdf.

4 http://www.itu.int/ITU-D/conferences/wtdc/2006/index.html.

الجابر كلمتها متمنية للمشاركين كل التوفيق في أعمالهم في منتدى الأمن السيبراني الإقليمي وقالت إنها تتطلع باهتمام كبير إلى التوصيات التي ستنبثق عن اللقاء.

7. ثم أخذ الكلمة السيد سامي البشير المرشد، مدير مكتب تنمية الاتصالات في الاتحاد، مدلياً ببعض الملاحظات الافتتاحية (بالإنكليزية)[5] (بالعربية)[6] باسم الاتحاد الدولي للاتصالات. وقال السيد البشير إنه مغتبط لرؤية الكثيرين من المتحدثين المرموقين الذين جاءوا من أنحاء المنطقة وكذلك العديد من الخبراء الذين جاءوا من أقاصي البلاد للمشاركة في هذا اللقاء، وقال إن قائمة المتحدثين والمشاركين متميزة حقاً وإنه واثق من أن هذا اللقاء سيعود بالفائدة على الجميع ويسهم في تعميق الإلمام بهذا الموضوع الذي يحظى بكل الاهتمام. واسترعى السيد البشير اهتمام المشاركين إلى أن التهديدات السيبرانية ما فتئت تزداد تطوراً منذ أوائل الثمانينات عندما عُرفت أولى إصابات الحاسوب بالفيروسات. أما اليوم فقد أصبحت الجريمة السيبرانية قوة اقتصادية خفية منظمة تجني أموالاً طائلة وتسخِّر برمجيات متطورة تهدد مستعملي الحاسوب والبنى التحتية للمعلومات في كل البلدان. وقد تكون أكبر التهديدات في بعض الأحيان مجرد حوادث بسيطة. وهذا ما حدث مثلاً قبل بضعة أسابيع عندما تأثر ملايين المستعملين في هذه المنطقة جرّاء تقطُّع في كبلات الألياف في قاع البحر يقال إنه نجم عن مرساة قارب شارد. وتابع السيد البشير قوله: وقد تأثر من ذلك النفاذ إلى الإنترنت والنداءات الهاتفية وحركة البيانات والفيديو بين المؤسسات. ويقال إن التجربة من أشد المدرسين قسوة لأنها تمتحن أولاً ثم تشرح الدرس بعد ذلك. ومهما كان السبب فإن الدرس الذي نتخذه عبرة هو أن كل بلد يحتاج إلى أن يتأهب لاتخاذ إجراءات منسَّقة فيما يتعلق بمنع وقوع الأحداث السيبرانية والاستعداد لها والتصدي لها والتغلب عليها.

8. ومضى السيد البشير يقول إن الأهداف والمهام المتصلة بالأمن السيبراني والتي تواجه البلدان كبيرة من حيث الأهمية ولكن الموارد محدودة ومن ثم فإن الاتحاد الدولي للاتصالات ملتزم بالعمل مع الأعضاء للتوصل إلى تفاهم مشترك بشأن أهمية النهوض بثقافة عالمية للأمن السيبراني. ويتحقق ذلك في قطاع تنمية الاتصالات في الاتحاد من خلال البرامج والمبادرات التي وضعها المؤتمر العالمي لتنمية الاتصالات هنا في قطر والتي أقرَّها مؤتمر المندوبين المفوضين في تركيا في عام 2006. وقال إننا ندرك أن القضايا التي يثيرها الأعضاء تعبِّر عن احتياجات حقيقية تتطلب تعاوناً وثيقاً من القطاع العام ومن القطاع الخاص على السواء حرصاً على تحسين نفاذ جميع المواطنين في العالم إلى تكنولوجيا المعلومات والاتصالات، والتي من المأمول أن تسهم في تحسين ظروف معيشتهم والنهوض بأوضاعهم اقتصادياً واجتماعياً. وشكر السيد البشير حكومة قطر ممثلةً في حضرة الدكتورة حصة الجابر كما شكر كل من يعاونها في المجلس الأعلى للاتصالات وتكنولوجيا المعلومات (ictQATAR) وفي فريق الاستجابة لطوارئ الحاسوب (Q-CERT) على جهودهم وكريم ضيافتهم وتمنى للمشاركين والمنظمين لقاءً حافلاً بالنجاح.

9. وتبع هذه الملاحظات الافتتاحية عرض رئيسي لموضوع الورشة بعنوان "*البيئة المتغيرة لتهديدات الأمن السيبراني*"، تقدَّم به السيد يان كوك، فريق Cymru، المملكة المتحدة. وتناول عرض السيد كوك تطور التهديدات السيبرانية وتداعياتها في المستقبل. وبعد أن استعرض بإيجاز كيف تغيَّر كل من التكنولوجيا والتهديدات على السواء، حيث تحوَّل نطاق التهديدات ونقاط الضعف وتغيَّر على مر السنين بموازاة بيئة الأمن ذاتها التي ما فتئت تتغيَّر، وأوضح السيد كوك كيف أن البنية التحتية تتعرَّض بازدياد للهجمات الإجرامية، وتحدَّث عن الاستهتار المكشوف الذي يبديه المشترون والبائعون والمتاجرون وأمناء الصندوق، وتناول الأنشطة والتحالفات التي تسود قوى الاقتصاد الخفية والطرائق غير المشروعة للحصول على البضائع وأساليب الترويج لهذه الخدمات وكمية البيانات الشخصية التي تُحصد في كل ساعة وفي كل يوم من أيام السنة. وأشار السيد كوك إلى أن الإنترنت قد حوَّلت طوال العقدين الماضيين العديد من جوانب الحياة المعاصرة، ولا سيما أساليب التعامل التجاري. وما زالت الإنترنت تنمو بمعدل ضخم وقال إن هنالك، في ديسمبر 2007، نحو شخص واحد من كل خمسة أشخاص في العالم يستعمل شبكة الإنترنت.

---

5 http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/opening-remarks-itu-al-basheer-feb-08-english.pdf (بالإنكليزية).

6 http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/opening-remarks-itu-al-basheer-feb-08-arabic.pdf (بالعربية).

10. فقد مكّنت الإنترنت مراكز بيانات معزولة وحواسيب شخصية وأجهزة محمولة يدوياً وهواتف جوالة من الانتقال إلى بيئة لا حدود لها وقدر ضئيل جداً من الحماية الفعّالة. وقد نتج عن ذلك أن أصبح المستعملون يواجهون تهديدات أمن سيبراني مختلفة جذرياً، من حيث الطابع والنطاق والتأثير، عن تلك التي كانت قبل عشر سنوات لا غير. ولذلك ينبغي ألا نستغرب، عندما نرى تزايد استعمال المعاملات التجارية والمالية للإنترنت كآلية لتسليم الخدمات، أن تتزايد الجرائم أيضاً. وبيَّن السيد كوك أيضاً كيف أن المنظمات الإجرامية، التي هي من وراء تنفيذ هذه التهديدات الجديدة على الخط، أكثر تنظيماً من أي وقت مضى. فهذه المنظمات تستخدم مطوِّري البرمجيات وتشتري وتبيع البنى التحتية لأنشطتها الإجرامية وتستأجر الناس لعملية غسل الأموال لإخفاء هوياتها. وخلُص السيد كوك إلى القول: بينما تدعم الإنترنت اقتصاداً إجرامياً خفياً ناضجاً ومزدهراً، ما زال الجمهور يجهل الكثير عن هذا الاقتصاد الخفي وكيف يعمل فعلاً.

الجلسة 1: نحو إطار للأمن السيبراني وحماية البنية التحتية الحرجة للمعلومات

11. من الأمور المسلّم بها عموماً ضرورة بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات والنهوض بالأمن السيبراني وحماية البنى التحتية الحرجة على المستوى الوطني. وعندما تتحدث الجهات الفاعلة الوطنية العامة والخاصة عن وجهات نظرها فيما يتعلق بالأهمية النسبية للمسائل، وذلك سعياً إلى التوصل إلى منهج متسق، يتبيَّن أن بعض البلدان قد وضعت أطراً مؤسسية بينما لجأت بلدان أخرى إلى اتباع نهج مبسَّط غير مؤسسي. ولم يعمد العديد من البلدان بعد إلى وضع استراتيجية وطنية للأمن السيبراني ولحماية البنية التحتية الحرجة للمعلومات. وقد ناقشت هذه الجلسة الأولى، برئاسة ريتش بتيا، مدير مركز تنسيق فريق الاستجابة لطوارئ الحاسوب (CERT / CC)، الولايات المتحدة الأمريكية، مفهوم إطار وطني للأمن السيبراني وحماية البنية التحتية الحرجة للمعلومات والجهود القائمة لصياغة إطار لأفضل الممارسات في الاتحاد الدولي للاتصالات، وذلك لتزويد المشاركين في اللقاء بنظرة عامة واسعة تتناول المسائل والتحديات المعنية. وشدد السيد بتيا في ملاحظاته الافتتاحية للجلسة على الحاجة إلى فهم أفضل للمسائل المتصلة بالأمن السيبراني والتي برزت بسبب تزايد وتغير استعمال التكنولوجيا وتزايد وتغير الهجمات وكذلك الهجمات المتقدمة تقنياً. وأشار السيد بتيا إلى أن الغرض من ورشة العمل هذه هو مساعدة البلدان على التوصل إلى فهم أفضل لجوانب التبعية والاعتمادات المتبادلة من جرّاء التوصيل البيني ولمساعدة البلدان على وضع أطر وطنية للأمن السيبراني.

12. واستعرض السيد روبرت شو، شعبة تطبيقات تكنولوجيا المعلومات والاتصالات والأمن السيبراني، قطاع تنمية الاتصالات في الاتحاد، من منظور واسع، مختلف النُهج نحو الأمن السيبراني وأطر حماية البنية التحتية الحرجة للمعلومات ومكوناتها المتماثلة غالباً وذلك لتمكين المشاركين من التبصُّر في المسائل والتحديات الضالعة في الأمر. وقدَّم السيد شو نظرة إجمالية تناولت "أنشطة قطاع تنمية الاتصالات المتعلقة بالأمن السيبراني وحماية البنية التحتية الحرجة للمعلومات"[7] وتحدَّث عن تفاصيل برنامج عمل الأمن السيبراني في قطاع تنمية الاتصالات لمساعدة البلدان النامية (2007-2009)[8]، وتعرَّض إلى ذكر أمثلة معيَّنة لما يحاول الاتحاد أن يقوم به لمساعدة البلدان النامية في مجال الأمن السيبراني وحماية البنية التحتية الحرجة للمعلومات. ومن بين مبادرات الأمن السيبراني الجارية والمخطط لها في الاتحاد ذكر في معرض حديثه: *أنشطة تتناول تحديد أفضل الممارسات في وضع أطر وطنية للأمن السيبراني وحماية البنية التحتية الحرجة للمعلومات؛ ومجموعة أدوات للتقييم الذاتي للأمن السيبراني الوطني/وحماية البنية التحتية الحرجة للمعلومات؛ ومجموعة أدوات للحد من تأثير البرمجيات المؤذية؛ ومنشورات المبادئ التوجيهية للأمن السيبراني من أجل البلدان النامية؛ ودراسة استقصائية دولية لمقدرات الأمن السيبراني الوطنية/وفريق الاستجابة لحوادث أمن الحاسوب (CSIRT)؛ ومجموعة أدوات من أجل تشريعات نموذجية لمكافحة الجريمة السيبرانية من أجل البلدان النامية؛ ومجموعة أدوات للنهوض بثقافة أمن سيبراني إلى جانب عدد من ورش العمل الإقليمية المخطط لها لإذكاء الوعي وبناء القدرات بشأن أطر من أجل الأمن السيبراني وحماية البنية التحتية الحرجة للمعلومات.*

7 http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/shaw-itu-d-cybersecurity-overview-doha-feb-08.pdf.

8 http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf.

13. وتحدث السيد شو أيضاً عن مشروع جار لتطوير *مجموعة أدوات للتخفيف من تأثير البرمجيات المؤذية*[9] للمساعدة على التصدي للمشكلة المتعاظمة للبرمجيات المؤذية. وقال إن *مجموعة أدوات التخفيف من تأثير البرمجيات المؤذية* عبارة عن نهج متعدد أصحاب المصلحة ومتعدد الفروع لتعقُّب البرمجيات المؤذية والحد من تأثيرها، مع التركيز بصفة خاصة على المشكلات التي تنفرد بها اقتصادات الإنترنت الناشئة. وتعتمد مجموعة الأدوات على الموارد القائمة وتحدد أصحاب المصلحة المحليين والدوليين المعنيين وتأخذ في الحسبان القيود المحددة المفروضة على البلدان النامية. وترمي مجموعة الأدوات إلى إذكاء الوعي بين الدول الأعضاء بتزايد التهديدات التي تتمثل في البرمجيات المؤذية وارتباطها بالأنشطة الإجرامية كما تتضمن جوانب السياسية والجوانب التقنية والاجتماعية للحد من تأثير البرمجيات المؤذية. وقد أُتيح المشروع الأول للمواد الأساسية للمشروع في ديسمبر 2007 ومن المخطط له إجراء اختبارات رائدة في عدد من الدول الأعضاء في الاتحاد في عام 2008. وكجزء من هذا النشاط، يرجى من البلدان المهتمة في المنطقة الاتصال بمكتب تنمية الاتصالات إذا كانت ترغب في استهلال مشروع رائد لتخفيف آثار البرمجيات المؤذية لديها.

14. وأشار السيد شو كذلك إلى أن غالبية البلدان لم تعمد بعد إلى صياغة أو تنفيذ استراتيجية وطنية للأمن السيبراني ولحماية البنية التحتية الحرجة للمعلومات، وأن البلدان النامية، بحكم الموارد البشرية والمؤسسية والمالية المحدودة، تواجه تحديات خاصة في وضع وتنفيذ مثل هذه السياسات. وأشار إلى أن قطاع تنمية الاتصالات في الاتحاد استحدث المسألة رقم 22 في لجنة الدراسات 1، التي تقوم الآن بوضع وثيقة لأفضل الممارسات تشتمل على إطار مقترح لجهود الأمن السيبراني الوطنية وهي مرتبطة ارتباطاً وثيقاً *ببرنامج عمل الأمن السيبراني في قطاع تنمية الاتصالات لمساعدة البلدان النامية*. ويتناول نطاق *برنامج العمل* هذا كيف يخطط الاتحاد لمساعدة البلدان في تطوير قدرتها في مجال الأمن السيبراني/حماية البنية التحتية الحرجة للمعلومات من خلال عدة أمور منها تزويد الدول الأعضاء بالموارد المفيدة والمواد المرجعية ومجموعات الأدوات بخصوص الموضوعات ذات الصلة. وعندما تترسخ مجموعات الأدوات ذات الصلة فإن قطاع تنمية الاتصالات ينوي تعميمها على نطاق واسع من خلال قنوات متعددة إلى الدول الأعضاء في الاتحاد وعددها 191. وذكر السيد شو أن واحداً من التحديات في دفع عجلة المناقشات فيما يتعلق بالأمن السيبراني هو إيجاد الآليات الملائمة لتحسين الاتصال بين مختلف الجهات الفاعلة، نظراً إلى أن كل مجموعة من هذه الجهات لديها متطلبات مختلفة ومعيَّنة فيما يتعلق بسويات الثقة المطلوبة لتقاسم معلومات معيَّنة. وذكر السيد شو أيضاً أن الاتحاد الدولي للاتصالات يأمل في إطلاق برنامج منح الأمن السيبراني[10] في وقت لاحق من هذا العام.

15. واستأنف الحديث السيد جيمس إنيس، وزارة الخارجية، الولايات المتحدة الأمريكية، بوصفه مقرِّر لجنة الدراسات 1 في قطاع تنمية الاتصالات بالنسبة للمسألة 22 – *تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني*، لإعطاء لمحة عامة عن الأعمال الجارية بشأن *إطار لجهود الأمن السيبراني الوطنية* الذي يُطوَّر حالياً في لجنة الدراسات 1 لقطاع تنمية الاتصالات بصدد المسألة 22. وتحدث في معرض تقديمه "أفضل الممارسات لتنظيم جهود الأمن السيبراني الوطنية"[11]، عن الأعمال الأساسية في لجنة الدراسات وخصوصاً تقريرها عن *أفضل الممارسات لتنظيم جهود الأمن السيبراني الوطنية*[12] والتي بإمكان الحكومات أن تستعملها بمثابة مبادئ توجيهية عندما تقوم بوضع وتنفيذ استراتيجيات وطنية من أجل الأمن السيبراني وحماية البنية التحتية الحرجة للمعلومات. ودعا السيد إنيس المشاركين في ورشة العمل والممثلين القُطْريين إلى الانضمام إلى أنشطة المسألة 22/1، والتي استُهِّلت في المؤتمر العالمي لتنمية الاتصالات لعام 2006. وقد عُقدت ثلاثة اجتماعات للجنة الدراسات بشأن المسالة 22/1 حتى الآن ومن المقرر عقد الاجتماع التالي في 21-22 أبريل 2008.

---

9 http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html.

10 http://www.itu.int/ITU-D/cyb/cybersecurity/.

11 http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/ennis-cybersecurity-best-practices-doha-feb-08.pdf.

12 http://www.itu.int/md/D06-SG01-C-0130/en *(مطلوب التسجيل وكلمة السر في نظام TIES في الاتحاد)*. وهنالك مشروع وثيقة يقدِّم المزيد من المعلومات عن إطار الاتحاد من أجل الأمن السيبراني في العنوان: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf.

16. ويتناول التقرير الذي وضعته لجنة الدراسات المشكلات الرئيسية التي يواجهها صانعو السياسة لدى التصدي لمشكلة الأمن السيبراني. وفي مستهل مشروع التقرير تعريف عملي للأمن السيبراني ("الأمن السيبراني هو الحيلولة دون تلف المعلومات الإلكترونية وأنظمة الاتصال واستخدامها دون ترخيص واستغلالها، وإذا لزم الأمر إعادتها، وكذلك ما تحتويه من معلومات، وذلك في سبيل تعزيز سرية هذه الأنظمة وسلامتها وتيسُّرها.")، ويشير التقرير إلى ضرورة اختلاف مستويات الأمن باختلاف الأنظمة ويسلّط الأضواء على ضرورة إدارة المخاطر على النحو الوافي. ويتناول *إطار الجهود الوطنية للأمن السيبراني* في التقرير خمسة عناصر رئيسية لأفضل الممارسات في الأمن السيبراني، وهي: 1) وضع استراتيجية وطنية للأمن السيبراني؛ 2) التعاون بين الحكومة والصناعة؛ 3) ردع الجريمة السيبرانية؛ 4) المقدرات الوطنية لإدارة الحوادث؛ 5) ثقافة وطنية للأمن السيبراني، مشيراً أيضاً إلى أن الوعي بالأمن السيبراني على الصعيد الوطني له مكونة دولية.

17. ويتضمن مشروع التقرير بيان سياسة لكل مكونة من مكونات الإطار، ويحدد الأهداف والخطوات المعيَّنة لبلوغ هذه الأهداف، والمراجع والمواد المتصلة بكل خطوة معيَّنة. وأشار السيد إنيس أيضاً إلى أن تقرير *أفضل الممارسات لتنظيم جهود الأمن السيبراني الوطنية*، بما فيها الإطار، عبارة عن وثيقة حية، وبالتالي فهي تتطوَّر بتطور الزمن. ولكنه ذكر أيضاً أن جودة التقرير مرهونة بجودة المساهمات التي تقدمها البلدان إلى التقرير وأعمال لجنة الدراسات، وعليه طلب من ممثلي البلدان الحاضرين أن يتقاسموا أفضل الممارسات لديهم والتي تعود بالفائدة على البلدان الأخرى في وضع إطار لجهود الأمن السيبراني الوطنية. وختاماً نوَّه السيد إنيس بأن كل القطاعات الحرجة في المجتمع في الوقت الحاضر تعتمد على شبكات المعلومات والاتصالات لكي تعمل بشكل مستقر، وسعياً إلى تحقيق الحد الأقصى من الأمن، فإن هذه الأنظمة تحتاج إلى أن تكون آمنة وموثوقة ويعوَّل عليها. وهذا يؤثر على جميع البلدان، سواء كانت متقدمة أم نامية.

الجلسة 2: إطار الإدارة لتنظيم جهود الأمن السيبراني الوطنية/حماية البنية التحتية الحرجة للمعلومات

18. يتزايد استعمال الشبكات الإلكترونية للأغراض الإجرامية، أو لأهداف من شأنها أن تلحق الضرر بسلامة البنية التحتية الحرجة وتعرقل تعميم منافع تكنولوجيا المعلومات والاتصالات. وللتصدي لهذه التهديدات ولحماية البنى التحتية يحتاج كل بلد إلى خطة عمل شاملة تتناول المسائل التقنية والقانونية ومسائل السياسة مشفوعة بالتعاون الإقليمي والدولي. فما هي المسائل التي ينبغي النظر فيها في إطار استراتيجية وطنية للأمن السيبراني وحماية البنية التحتية الحرجة للمعلومات؟ وما هي الجهات الفاعلة التي ينبغي لها المشاركة؟ وهل هنالك من أمثلة لأطر يمكن اعتمادها؟ تسعى الجلستان 2 و3 إلى استكشاف مختلف النُهج وأفضل الممارسات بمزيد من التفصيل وإلى تحديد لبنات البناء الأساسية التي من شأنها أن تساعد البلدان في وضع استراتيجيات وطنية من أجل الأمن السيبراني وحماية البنية التحتية الحرجة للمعلومات. وعلى وجه التحديد، تقدم الجلستان بمزيد من التفصيل *إطار الاتحاد لتنظيم نهج وطني نحو الأمن السيبراني* والعناصر الأساسية الخمسة لجهود الأمن السيبراني الوطنية، وهي 1) وضع استراتيجية وطنية للأمن السيبراني، 2) إقامة تعاون وطني بين الحكومة والصناعة، 3) ردع الجريمة السيبرانية، 4) استحداث مقدرة وطنية لإدارة الحوادث، 5) النهوض بثقافة وطنية للأمن السيبراني. ورغبة في تقاسم المزيد من المعلومات بشأن هيكل الإطار ولتزويد المشاركين في الاجتماع بأفكار فيما يتعلق بكيفية عمل الإطار بالنسبة للبلدان في المنطقة، تناولت أولى الجلستين، بإدارة السيد برادفورد ويلكي، خبير تقني رفيع المستوى، إدارة المؤسسة القابلة للبقاء، فريق الاستجابة لطوارئ الحاسوب (CERT)، جامعة كارنيغي ميلون، الولايات المتحدة الأمريكية، المكونات المكرّسة لما يلي: النهوض بثقافة للأمن السيبراني، والتعاون بين الحكومة والصناعة، ومقدرات إدارة الحوادث.

19. وقدَّمت السيدة كريستين سوند، منسِّقة الأمن السيبراني، شعبة تطبيقات تكنولوجيا المعلومات والاتصالات والأمن السيبراني، قطاع تنمية الاتصالات في الاتحاد، في عرضها بعنوان "النهوض بثقافة الأمن السيبراني"[13] نظرة إجمالية لما تعنيه ثقافة الأمن السيبراني وما عساه أن يكون بعض الأدوار الممكنة لمختلف أصحاب المصلحة في مجتمع المعلومات في استحداث ثقافة عالمية للأمن السيبراني. وسلّطت الأضواء على تسعة عناصر لاستحداث ثقافة أمن سيبراني في قرار الأمم المتحدة 57/239

[13] http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/sund-promoting-a-culture-of-cybersecurity-doha-feb-08.pdf.

(2002): "استحداث ثقافة عالمية للأمن السيبراني"، وقرار الأمم المتحدة 58/199 (2004): "النهوض بثقافة عالمية للأمن السيبراني وحماية البنى التحتية الحرجة للمعلومات". وتشمل هذه العناصر التسعة: أ) الوعي، ب) المسؤولية، ج) الاستجابة، د) الأخلاق، ه) الديمقراطية، و) تقييم المخاطر، ز) تصميم الأمن وتنفيذه، ح) إدارة الأمن، ي) إعادة التقييم. وقد طُلب في هذين القرارين من الدول الأعضاء في الأمم المتحدة وجميع المنظمات الدولية المعنية أن تتناول وتأخذ هذه العناصر في الحسبان في معرض الاستعداد لمرحلتي القمة العالمية لمجتمع المعلومات[14] في عامي 2003 و2005. وقد شددت الوثائق التي تمخضت عنها مرحلتا القمة المذكورة على أهمية بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات وعلى التزام البلدان بالنهوض بثقافة الأمن.

20. وذكرت السيدة سوند في تقديمها بعض الأدوار الممكنة للحكومات في النهوض بثقافة الأمن السيبراني، ومنها: ضمان حماية مواطني البلد، والاضطلاع بدور مركزي في تنسيق وتنفيذ استراتيجية وطنية للأمن السيبراني، وضمان مرونة السياسة الوطنية وإمكانية تكيُّفها، وتنسيق المسؤوليات عبر مختلف إدارات الحكومة، واستحداث تشريعات جديدة (أو تكييف تشريعات قائمة) لتجريم إساءة استعمال تكنولوجيا المعلومات والاتصالات، والحد من التجاوزات وحماية حقوق المستهلك، والنهوض بأنشطة وطنية وإقليمية ودولية للتعاون في مجال الأمن السيبراني. وشددت السيدة سوند على أن البنى التحتية لتكنولوجيا المعلومات والاتصالات يملكها ويشغِّلها القطاع الخاص في معظم الأحيان في العديد من البلدان وأن مشاركة هذا القطاع في النهوض بثقافة وطنية وعالمية للأمن السيبراني مسألة حاسمة. فالأمن السيبراني الفعَّال يحتاج إلى فهم عميق لجميع جوانب شبكات تكنولوجيا المعلومات والاتصالات ومن ثم فإن الدراية التقنية لدى القطاع الخاص ومشاركته في هذا الصدد على درجة من الأهمية في تطوير وتنفيذ استراتيجيات الأمن السيبراني الوطنية. وعلاوة على ذلك نوَّهت السيدة سوند بأن الحكومات ودوائر الأعمال يلزم أن تساعد المواطنين في الحصول على المعلومات فيما يتعلق بكيفية حماية أنفسهم مباشرة على الخط. وعندما يكون من الميسور النفاذ إلى الأدوات الصحيحة فإن كل مشارك في مجتمع المعلومات مسؤول عن اتخاذ الحيطة وحماية نفسه علماً بأن الأمن السيبراني في نفس الوقت وفي جوهره مسؤولية مشتركة.

21. وتحدث السيد برادفورد ويلكي، موظف تقني رفيع المستوى، إدارة المؤسسة القابلة للبقاء، فريق الاستجابة لطوارئ الحاسوب، جامعة كارنيغي ميلون، الولايات المتحدة الأمريكية عن موضوع "التعاون بين الحكومة والصناعة"[15]. وبادر السيد ويلكي إلى تقديم مفهوم التعاون بين الحكومة والصناعة مشيراً إلى أن الهدف الرئيسي يتناول إقامة علاقات التعاون لإدارة المخاطر السيبرانية ولتوفير حماية أفضل للفضاء السيبراني. وتوفر هذه العلاقات آلية لتوليف كل من منظور الحكومة والصناعة والأصول والمعارف كلها معاً من أجل التوصل إلى توافق والمضي قُدماً في سبيل تعزيز الأمن على الصعيد الوطني. وأبرز السيد ويلكي أهمية العمل بنشاط لإزالة الحواجز الممكنة أمام تعاون الحكومة والصناعة بالتركيز على آليات من شأنها بناء الثقة وتعزيز التعاون من خلال أمور عدة منها إبرام اتفاق خطي يوجِّه التعاون والتبادل بين الحكومة والصناعة ويحدد معالم الرؤية المشتركة والغرض والاستفادة من القيادة القوية الفردية والتنظيمية لتمكين المشاركين من التوصل إلى نتائج ملموسة وقابلة للقياس.

22. وختاماً تناول السيد ويلكي أربع دراسات حالة للتعاون بين الحكومة والصناعة، واستخلص منها دروساً مفيدة محددة. وقد شملت هذه الدروس المبادرات التالية: 1) منتدى تقاسم المعلومات في ماليزيا، وهو عبارة عن منتدى لمقدِّمي خدمات الإنترنت والوكالات الحكومية يتناول مسائل المعلومات وأمن الشبكات في ماليزيا، 2) تحالف أمن المعلومات المالي في جمهورية كوريا، ويرمي إلى حماية أنظمة أمن المعلومات المالية من الإرهاب السيبراني والاحتيال من خلال وضع معايير لحماية المعلومات ورسم السياسات للقطاع المالي فضلاً عن عمليات التقييم والإشهاد، في جملة أمور، وتحالف ممارسة أمن المعلومات، وهو تحالف طوعي لمنظمات في القطاع الخاص والقطاع العام يرمي إلى زيادة أنشطة حماية المعلومات في القطاع الخاص بالتعاون مع مختلف شركات ورابطات الأمن بمساعدة من تحالف أمن المعلومات في كوريا، 3) برنامج نمذجة وتحليل حماية البنية التحتية الحرجة في أستراليا والذي يسعى إلى تعزيز حماية البنية التحتية الحرجة في أستراليا وتحسين طواعية الاقتصاد

14 http://www.itu.int/wsis/.

15 http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/sund-promoting-a-culture-of-cybersecurity-doha-feb-08.pdf.

والمجتمع فضلاً عن بناء تكنولوجيا من أجل نمذجة وتحليل العلاقات والروابط بين أنظمة البنى التحتية الحرجة في أستراليا. وترمي المبادرة أيضاً إلى بناء مقدرة نمذجة التأثيرات المحتملة والتقرير عنها عندما تتأثر شبكات في قطاع أو أكثر في حالات خلل (ناجمة عن الطبيعة أو عن الناس) في قطاع آخر. ومن القطاعات المشمولة حتى الآن قطاع الطاقة والاتصالات والمصارف والمالية. 4) مركز كفاءات معلومات الاتصالات الوطنية في سنغافورة وهو منظمة تدفعها الصناعة وتدعمها الحكومة أُنشئت لمساعدة الأفراد والمنظمات في سعيها إلى تحقيق مستوى عال من كفاءة تكنولوجيا المعلومات والاتصالات والحفاظ عليها. وهو يرمي، بالعمل الوثيق مع وزارة الموارد البشرية وسلطة تنمية معلومات الاتصالات، إلى النهوض بالمعارف والمهارات، وهو في الوقت ذاته هيئة التصديق الرئيسية لإصدار شهادات تكنولوجيا المعلومات والاتصالات.

23. وتحدث السيد يان دودزويل، مدير شعبة الترصد والتحذير والتحقيق والاستجابة، فريق الاستجابة لطوارئ الحاسوب (Q-CERT)، قطر، عن "مقدرات إدارة الحوادث"[16] واستعرض إجمالاً هيكل الفريق وأنشطته وارتباط هذه الأنشطة مباشرة بدعامة إطار الأمن السيبراني في الاتحاد الدولي للاتصالات "مقدرات إدارة الحوادث". ومن الأنشطة الهامة في التصدي لمشكلات الأمن السيبراني على الصعيد الوطني التأهب للحوادث السيبرانية وتقصيها وإدارتها والاستجابة إليها وذلك من خلال إقامة مقدرات الترصد والتحذير والاستجابة للحوادث. وتتطلب الإدارة الفعَّالة للحوادث اعتبارات تتناول التمويل والموارد البشرية والتدريب والمقدرة التكنولوجية وعلاقات الحكومة والقطاع الخاص والمتطلبات القانونية. ومن الضروري توفر التعاون في جميع المستويات في الحكومة وفي القطاع الخاص والدوائر الأكاديمية والمنظمات الإقليمية والدولية وذلك لإذكاء الوعي بالهجمات الممكنة والخطوات اللازمة للتغلب عليها. وأشار السيد دودزويل إلى عدة أمور منها أن البلدان مطلوب منها أن تنظر في وضع برنامج وطني لإدارة حوادث الأمن السيبراني وذلك بالتنسيق مع دوائر التحقيق وإنفاذ القوانين بالإضافة إلى المشاركة في آليات الترصد والتحذير وتقاسم معلومات الاستجابة للحوادث.

24. وقال السيد دودزويل إن الفريق Q-CERT، من خلال أنشطته المتزايدة عدداً، يرمي إلى ما يلي: توفير المعلومات الدقيقة وفي حينها عن التهديدات السيبرانية الراهنة والناشئة وعن نقاط الضعف، والاستجابة إلى التهديدات ومواطن الضعف الهامة في البنى التحتية الحرجة وذلك بإجراء الأنشطة اللازمة وتنسيقها من أجل التصدي للتهديدات، والعمل بمثابة شريك مركزي موثوق به في مجال الأمن من الحوادث، والقيام بالإبلاغ والتحليل، والنهوض باعتماد المعايير والعمليات والطرائق والأدوات الفعَّالة جداً في الحد من المخاطر المتطورة، وتقديم المعلومات وبرامج التدريب المحايدة لبناء مهارات الإدارة والمهارات التقنية اللازمة لدى المنظمات لتتمكّن بصورة فعَّالة من إدارة المخاطر السيبرانية. وأوضح السيد دودزويل أيضاً دور شبكة الأمن السيبراني في قطر، وهي مبادرة لجمع منظمات القطاع الحرجة في قطر وفي المنطقة بغية تفهم متطلبات أمن المعلومات لديها ولتمكين الفريق Q-CERT من تركيز جهوده لتلبية هذه الاحتياجات.

25. وفي مساء اليوم الأول دعا منظمو ورشة العمل المشاركين إلى حفل استقبال في مكان انعقاد الورشة، فندق ماريوت الدوحة.

الجلسة 3: إطار الإدارة لتنظيم جهود الأمن السيبراني الوطنية/حماية البنية التحتية الحرجة للمعلومات (تابع)

26. واصلت الجلسة 3 تناول المكونات المتبقية في *إطار الاتحاد لتنظيم نهج وطني للأمن السيبراني*، وعلى وجه التحديد ردع الجريمة السيبرانية ووضع استراتيجية وطنية للأمن السيبراني. وقدَّم مدير الجلسة 3، السيد شريف هاشم، وزارة الاتصالات وتكنولوجيا المعلومات في مصر، المتحدثين في الجلسة وأشار إلى المشكلات المتعاظمة فيما يتعلق بمختلف الأطر القانونية في البلدان حول العالم والحاجة الملحّة إلى زيادة التعاون بين جميع البلدان في هذا الصدد.

27. استهلّت السيدة نبال إدلبي، رئيسة فريق تكنولوجيا المعلومات والاتصالات من أجل التنمية، شعبة تكنولوجيا المعلومات والاتصالات، اللجنة الاقتصادية والاجتماعية لغرب آسيا التابعة للأمم المتحدة (UN-ESCWA)، متحدثة عن

[16] http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/dowdeswell-incident-management-qcert-doha-feb-08.pdf.

"الأساس القانوني والإنفاذ: التشريعات السيبرانية في منطقة اللجنة ESCWA – مسائل الأمن"[17]، وأشارت إلى أهمية الجهود الفعَّالة من أجل إرساء بيئة تمكينية لا غنى عنها من أجل الاستعمال الفعَّال والأخلاقي للفضاء السيبراني، وقالت إن التشريعات السيبرانية هي من المكونات التمكينية الرئيسية في سبيل النهوض بمجتمع معلومات حديث. وفيما يتعلق بالتشريعات المرتبطة بالفضاء السيبراني في منطقة ESCWA، أكدت على أهمية التكامل الإقليمي في تحسين التعامل الإلكتروني بين البلدان في المنطقة. واستعرضت بصورة مجملة دراسة استقصائية قامت بها لجنة UN-ESCWA للتشريعات الدولية والإقليمية والوطنية لحماية البيانات والخصوصية وتحدثت عن الحالة في منطقة ESCWA في هذا الصدد.

28. وأشارت السيدة إدلبي إلى أن العديد من البلدان لم تعمد بعد إلى سن قوانين لمنع جرائم الحاسوب. وتحدثت إلى المشاركين عن أمثلة لمبادرات في هذا الشأن في بلدان المنطقة ومنها القانون الفيدرالي للإمارات العربية المتحدة رقم 2 لعام 2006 بشأن مكافحة جرائم تكنولوجيا المعلومات وكذلك قانون الجريمة الإلكترونية الذي صدر في المملكة العربية السعودية في عام 2006 والأنشطة التي تجري في دول الخليج، ولا سيما في البحرين وفي قطر في مجال وضع التشريعات لمكافحة الجرائم السيبرانية والتي يؤمل أن تصدر قريباً. وقالت إن دولاً أعضاء أخرى في لجنة ESCWA تعتمد في الوقت الراهن على الأحكام الموجودة في قوانين العقوبات القائمة وقوانين حقوق التأليف بقدر ما تشمل هذه الأحكام الجرائم السيبرانية. ولكن هنالك بصفة عامة نقص حقيقي في التشريعات لتجريم إساءة استعمال تكنولوجيا المعلومات والاتصالات في المنطقة. ولذلك فإن الدراسة التي قامت بها اللجنة توصي الدول الأعضاء في المنطقة وعددها 13 بأن تتناول مسألة نقص التشريعات المتصلة بالأمن السيبراني إما بالتصديق على الاتفاقيات الدولية ذات الصلة أو بسن تشريعات وطنية تمتثل للاتفاقات الدولية و/أو القوانين الوطنية. ويمكن القيام بذلك من خلال إنشاء فريق متخصص يقوم بصياغة التشريعات السيبرانية، كما يقوم بإجراء المقابلات ويعقد ورش العمل والمناقشات بخصوص التشريعات المقترحة مع الأطراف المعنية. وختمت السيدة إدلبي كلمتها بالتطرق إلى النموذج الذي وضعته اللجنة لتطوير التشريعات السيبرانية والذي يرمي إلى مساعدة الدول الأعضاء في صياغة تشريعاتها المتعلقة بالأمن السيبراني. وقدَّمت السيدة إدلبي عرضاً حياً لموقع سوف تطلقه اللجنة قريباً على شبكة الويب وقد أنشئ لدعم هذه الأنشطة.

29. واستمراراً للعروض التي قُدِّمت آنفاً في إطار الجلستين 1 و2 من ورشة العمل والتي أبرزت مختلف دعائم إطار الأمن السيبراني وحماية البنية التحتية الحرجة للمعلومات ومختلف الاستراتيجيات والنُهج الوطنية، قام السيد جوزف ريتشاردسون، الولايات المتحدة الأمريكية، في العرض الذي تقدَّم به بعنوان "استراتيجية وطنية للأمن السيبراني"[18]، بوصف العنصر الأخير في الإطار والذي يضم المكونات الأخرى معاً، ألا وهو وضع استراتيجية وطنية للأمن السيبراني. وشدد السيد ريتشاردسون على أن حماية الأمن السيبراني مسألة أساسية بالنسبة للأمن الوطني والرفاه الاقتصادي وقدَّم بعض الأفكار الملموسة ذكر فيها كيف يمكن للبلدان المبادرة إلى وضع استراتيجية وطنية. ومن الأدوات الهامة في هذا المجهود العمل الجاري في الاتحاد لوضع مجموعة أدوات للأمن السيبراني الوطني/حماية البنية التحتية الحرجة للمعلومات[19]. وقال إن مجموعة الأدوات المذكورة، وهي تمثل واحدة من عناصر التآزر الرئيسية بين المسألة 22/1 للجنة دراسات تنمية الاتصالات بشأن "تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني"[20] وبرنامج عمل الاتحاد بشأن الأمن السيبراني لمساعدة البلدان النامية (2007-2009)[21]، تعمد إلى تطبيق الإطار قيد التطوير في لجنة الدراسات مشفوعاً بمجموعة أدوات عملية للنظر فيها على الصعيد الوطني.

---

17 http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/idlebi-cyber-legislation-ESCWA-doha-feb-08.pdf.

18 http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/richardson-cybersecurity-framework-and-readiness-assessment-doha-feb-08.pdf.

19 http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html.

20 http://www.itu.int/ITU-D/cyb/cybersecurity/index.html.

21 http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf.

30. ومن شأن مجموعة الأدوات أن تساعد الحكومات في تناول السياسات الوطنية القائمة وكذلك الإجراءات والمعايير والمؤسسات والعناصر الأخرى اللازمة لصياغة استراتيجيات الأمن في بيئة متغيرة دائماً لتكنولوجيا المعلومات والاتصالات. ومن شأنها أيضاً أن تساعد الحكومات على فهم أفضل للأنظمة القائمة وعلى تحديد الثغرات التي تتطلب الاهتمام الخاص ولترتيب أولويات جهود الاستجابة الوطنية. وتتناول مجموعة الأدوات مستوى الإدارة ووضع السياسة لكل من العناصر الخمسة في إطار أفضل الممارسات والتي قدمها السيد إنيس في الجلسة 1. وأشار السيد ريتشاردسون إلى أن مجموعة الأدوات تحدد مسائل وتطرح عدداً من الأسئلة التي تستحق الدراسة من قبيل: ما هي الإجراءات التي اتخذت حتى الآن وما هي الإجراءات المخطط لها وما هي الإجراءات التي يتعيَّن دراستها وما هو الوضع الراهن لهذه الإجراءات؟ وأشار السيد ريتشاردسون أيضاً إلى أن ليس هنالك من بلد يعمل ابتداءً من الصفر فيما يتعلق بمبادرات الأمن السيبراني. وعلاوة على ذلك ليس هنالك من إجابة واحدة صحيحة أو منهج واحد صحيح إذ إن كل البلدان تنفرد بمتطلباتها ورغباتها الوطنية. ويحتاج الأمر إلى مواصلة الاستعراض والمراجعة مهما كان النهج المتخذ ومن الضروري أيضاً أن تشارك جميع الجهات أصحاب المصلحة، كلاً بحسب دورها الملائم، في وضع استراتيجية وطنية.

الجلسة 4: دراسات حالات قطْرية

31. للمضي في استكشاف كيف يعمد مختلف البلدان حالياً إلى تنفيذ الدعائم الخمس لإطار الإدارة لتنظيم الأمن السيبراني الوطني وجهود حماية البنية التحتية الحرجة للمعلومات، أي النهوض بثقافة الأمن السيبراني، والتعاون بين الحكومة والصناعة، ومقدرات إدارة الحوادث، والأساس القانوني والإنفاذ، ووضع استراتيجية وطنية للأمن السيبراني، تكرِّس الجلسات 4 و5 و6 لدراسات حالات قطْرية معيَّنة. وتركِّز الجلسة 4 التي تديرها السيدة مارلين كيد، المستشارة في شركة AT&T، الولايات المتحدة الأمريكية، على النظر إلى النهوض بثقافة الأمن السيبراني والتعاون بين الحكومة والصناعة.

32. وقدَّمت السيدة رجا أزرينا رجا عثمان، كبيرة خبراء التكنولوجيا، الأمن السيبراني في ماليزيا، دراسة الحالة القطْرية الأولى بشأن النهوض بثقافة الأمن السيبراني، وهي تتناول "النهوض بثقافة أمن سيبراني في إطار البنية التحتية الوطنية الحرجة للمعلومات"[22]. وقد بادرت وزارة العلوم والتكنولوجيا والابتكار في عام 2006 إلى وضع سياسة الأمن السيبراني الوطنية في ماليزيا، وذلك لتسخير الجهود الوطنية لتعزيز أمن البنية التحتية الوطنية الحرجة للمعلومات في ماليزيا. وتتمحور هذه السياسة حول ثمانية عناصر رئيسية للأمن السيبراني، على غرار الدعائم الخمس لإطار الأمن السيبراني الذي وضعه الاتحاد، ولكن جرى تفصيل بعض هذه الدعائم لكي تلبِّي متطلبات ماليزيا المحددة. وقالت السيدة رجا عثمان إن محور السياسة الرابع مكرَّس لثقافة الأمن ولبناء القدرات وهو يشمل وضع وتعزيز ثقافة أمن وطنية والحفاظ عليها إلى جانب التنسيق والتوحيد القياسي لبرامج الوعي والتثقيف في مجال الأمن السيبراني عبر كل عناصر البنية التحتية الوطنية الحرجة للمعلومات. ومن الجوانب الهامة في هذا النشاط أيضاً إقامة آلية فعَّالة لتعميم المعرفة بشأن الأمن السيبراني على الصعيد الوطني وتحديد المتطلبات والمؤهلات الدنيا للمحترفين في مجال أمن المعلومات. وعلاوة على ذلك نوَّهت السيدة رجا عثمان بمسألة الأخلاق بوصفها من المكونات الرئيسية في برنامج ماليزيا للأمن السيبراني.

33. وتقدَّمت السيدة رجا عثمان ببعض الأمثلة عن مختلف المبادرات في ماليزيا بما في ذلك منصة تقاسم المعرفة والتي أُطلقت لزيادة الوعي بالأمن السيبراني على الصعيد الوطني. وقالت إن حملات الوعي بالأمن السيبراني وسلامة الإنترنت وبرامج الإرشاد المتصلة بذلك قد بدأت بتحديد هوية الشركاء الذين يتعيَّن إشراكهم في الأمر، ويأتي بعد ذلك قدر كبير من مواد إذكاء الوعي، من قبيل المحتوى والبوابات ومواقع الويب المحددة وغير ذلك، والتي وضِعت لتلبية الاحتياجات بين سكان ماليزيا، وأهم من كل ذلك تفصيل هذه المعلومات لكي تلائم الجماعات المستهدفة المحددة.[23]

---

[22] http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/othman-promoting-a-culture-of-cybersecurity-malaysia-doha-feb-08.pdf.

[23] http://www.esecurity.org.my/.

34. وكان من التحديات المطروحة توصيل المعلومات إلى الجمهور المستهدف. وذكرت السيدة رجا عثمان أن فريق الأمن السيبراني في ماليزيا كان يعمل على نحو وثيق مع وزارة التعليم من أجل الوصول إلى الطلبة والمدرسين ومع وزارة الإعلام لتوصيل المعلومات من خلال قنوات الراديو وغير ذلك من الوسائل، وذلك لتركيز الموارد المتاحة المحدودة على تطوير المحتوى والسعي إلى عقد شراكات مع الآخرين لتوسيع رقعة النشاط وجعل المعلومات متاحة على نطاق أوسع للمواطنين. وتطرَّقت السيدة رجا عثمان أيضاً إلى وصف برامج تنمية الكفاءات والتي تشمل عمليات الإشهاد بأمن المعلومات وبوابة البنية التحتية الوطنية الحرجة للمعلومات، وهي بوابة موارد أمنية مصمَّمة خصيصاً لتلبية احتياجات ممارسي نشاط الأمن (الإدارة والمستوى التقني) ضمن منظمات البنى التحتية الوطنية الحرجة للمعلومات. وختاماً أكدت السيدة رجا عثمان من جديد، في معرض النهوض بثقافة وطنية للأمن السيبراني، على الحاجة إلى الابتكار وإلى توليد المعلومات ذات الصلة بالمجموعات المستهدفة المعيَّنة وتوسيع نطاق الشراكات مع أصحاب المصلحة بغية تحسين إمكانية الوصول إلى المستعملين النهائيين. وأكدت أيضاً على ضرورة تقييم فعالية المبادرات المتخذة، من خلال الدراسات الاستقصائية وغيرها من الآليات، كخطوة ضرورية من أجل التقدم في هذا المسعى.

35. وتحدثت السيدة ليلي دي سلفسترو، مديرة عمليات تجارة الأعمال، شركة ميكروسوفت، عن موضوع "التعاون بين الحكومة والصناعة: 7 خطوات لتحقيق الطواعية في حماية البنية التحتية الحرجة"[24]. وأكدت على ضرورة إقامة الشراكات بين الجهات الفاعلة في القطاع العام والقطاع الخاص لصالح مسألة الأمن وذلك لتحقيق الوعد الكبير الذي تعد به تكنولوجيا المعلومات. وأضافت أنه لا يمكن تعزيز الأمن السيبراني إلا من خلال التعاون بين الحكومة والصناعة. وهذه الشراكات ضرورية في كل جوانب إطار حماية البنية التحتية الحرجة، وذلك لتقييم المخاطر على نحو فعَّال وللحد من التهديدات وتقصّي حالات الاستغلال والهجمات والاستجابة بسرعة في حالة أي هجوم. والغرض من نهج خطوات الطواعية السبع هو تقديم مجموعة من عناصر أفضل الممارسات من مختلف مناطق العالم والتي اعتمدتها الحكومات. وانطلاقاً من هذه المبادئ التوجيهية بإمكان الحكومات وأصحاب البنى التحتية والمشغِّلين التعاون في مجال الأخذ بمجموعة من العناصر الرئيسية التمكينية في مجال الطواعية والبنية التحتية.

36. وتشمل الخطوات السبع: 1) *تحديد الأهداف والأدوار*. إن مسألة وضع أهداف واضحة مسألة مركزية في توليد الدعم للأمن السيبراني من جانب مختلف مجموعات أصحاب المصلحة بينما من شأن التفهم الأفضل لمختلف أدوار أصحاب المصلحة أن يعزِّز التنسيق والكفاءة والثقة. 2) *استحداث شراكات بين القطاع العام والقطاع الخاص*. أوضحت السيدة دي سلفسترو الأهمية الحاسمة لاستحداث علاقات تتسم بالصلة وذلك بالنسبة لتقاسم المعلومات وتطوير الحلول للمشاكل المستعصية. ومن الضروري استغلال المهارات الفريدة لدى الحكومات ومنظمات القطاع الخاص للتصدي لبيئة التهديدات الدينامية اليوم. 3) *تحديد الوظائف الحرجة وترتيبها بحسب الأولوية*. يحتاج الأمر إلى توثيق التعاون لفهم علاقات الترابط المتبادل الضالعة في الأمر. 4) *الاستمرار في تقييم المخاطر وإدارتها*. من الجوانب الهامة لمواصلة إدارة المخاطر تقييم المخاطر وتحديد جوانب التحكم والتخفيف من حدة المخاطر وتنفيذ عمليات التحكم وقياس فعاليتها. 5) *وضع خطط الطوارئ والتدرب عليها وتحسين التنسيق التشغيلي*. بإمكان خطط الاستجابة للطوارئ أن تخفف من الأضرار وأن تعزِّز الطواعية. 6) *تضمين الأمن والطواعية داخل العمليات نظراً إلى أن الأمن عملية مستمرة*. من شأن تسخير مبادئ الأمن أن يعزِّز أمن المنظمات وطواعيتها. 7) *تحديث التكنولوجيا والعمليات والابتكار فيها*. بما أن التهديدات السيبرانية تتطوَّر باستمرار فإن بإمكان صانعي السياسة وأصحاب المؤسسات ومشغِّلي البنى التحتية التأهب لهذه التهديدات والتخفيف من حدتها وذلك بالعمل باستمرار على استحداث التكنولوجيا المستخدمة والحفاظ عليها.

37. وختاماً تحدثت السيدة دي سلفسترو عن بعض مبادرات الأمن السيبراني التي أطلقتها شركة ميكروسوفت، بما فيها برنامج التعاون الأمني في ميكروسوفت، وهو برنامج عالمي النطاق للحكومات والمنظمات الحكومية المسؤولة عن الاستجابة

[24] http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/di-silvestro-government-industry-collaboration-casestudies-doha-feb-08.pdf.

لحوادث الحاسوب وعن حماية البنية التحتية الحرجة وأمن الحاسوب للتعاون في هذا المجال من أمن تكنولوجيا المعلومات. ونوَّهت السيدة دي سلفسترو بأن العديد من البلدان في المنطقة قد شاركت فعلاً في هذه المبادرة.

38. وناقشت السيدة مارلين كيد، المستشارة لدى شركة AT&T، الولايات المتحدة الأمريكية، في معرض حديثها عن "دراسات حالة قطْرية للتعاون بين الحكومة والصناعة"[25]، بعض المسائل التي تحتاج إلى البحث عندما يتناول الأمر التعاون بين الحكومة والصناعة من أجل الأمن السيبراني. وأشارت السيدة كيد إلى تغير المستعملين في شبكة الإنترنت ولكنها أشارت أيضاً إلى تغير الحركة في شبكة الإنترنت. وإذا كان الجميع يتذمرون من البريد الاقتحامي الذي يملأ صناديقهم الإلكترونية فإن حجم الحركة على الإنترنت مؤلف في الوقت الراهن في معظمه من التراسل بين الأقران ومن تقاسم الملفات. ومن ثم فإن مقدِّمي الخدمات بحاجة إلى مستعملي إنترنت يتسمون بالمسؤولية والأخلاق. ولكن عندما تزداد تكاليف توفير الدعم للعملاء عندئذ يتصرف القطاع الخاص ويبدأ البحث عن حلول ممكنة. وتتناول الحكومات أيضاً نفس المشكلات. واسترعت السيدة كيد انتباه المشاركين إلى أن غالبية محتوى الإنترنت ما زال باللغة الإنكليزية أساساً. بيد أن أفضل وسيلة للنهوض بثقافة عالمية للأمن السيبراني تستدعي توفر الموارد الخاصة بإذكاء الوعي بالأمن السيبراني باللغات المحلية.

39. وعرضت السيدة كيد بعض الأمثلة عن مبادرات إذكاء الوعي من شتى بقاع العالم والتي كانت نتيجة تعاون الحكومة مع الصناعة. وأشارت إلى أن الحاجة تدعو إلى كل من نهج "الجذب" ونهج "الدفع" عندما يتناول الأمر توسيع رقعة الأمن السيبراني مما يضمن توفر القدر الكبير من المعلومات على الخط مباشرة التي تشتمل على تعليمات سهلة الفهم عن كيفية تمكن المواطنين من حماية أنفسهم (نهج الجذب) وتوفير الموارد لتمكين القائمين بعملية إذكاء الوعي من الذهاب إلى المدارس وأماكن العمل وغيرها لتدريب المستعملين على كيفية التصرف بمسؤولية عندما يعملون على الخط مباشرة (نهج الدفع). وقالت السيدة كيد إن العميل المطلع، من وجهة نظر الصناعة، مستعمل أفضل بكثير من غيره وبالتالي عميل أفضل. وهنالك العديد من النماذج القائمة والأمثلة عن كيفية عمل الحكومات والصناعة (وليس في سبيل الربح) يداً بيد لتوفير المعلومات بشأن الأمن السيبراني لدوائر الأعمال من شتى الأحجام وإلى الأسر والأطفال والمدارس والمنظمات بما فيها الوكالات الحكومية. وليس هنالك من حل واحد وحيد وإنما تقدم الصناعة عادة مهارات فريدة من نوعها إلى جانب الدراية والمعلومات. وكثيراً ما تؤدي المناقشات بين وكالات الحكومة والصناعة إلى استحداث الخدمة على الخط مباشرة، وعلاوة على ذلك يضمن اهتمام الحكومة استمرار التزام الصناعة.

الجلسة 5: دراسات حالات قطْرية (تابع)

40. استمرت في الجلسة 5 المناقشات المتصلة بمختلف مكونات إطار الأمن السيبراني في الاتحاد مشفوعة بأمثلة من دراسات الحالات القطْرية. وأدارت هذه الجلسة السيدة جوليا آلن، عضو في الفريق التقني، معهد هندسة البرمجيات، جامعة كارنيغي ميلون، الولايات المتحدة الأمريكية، وتناولت عن كثب دراسات الحالات القطْرية المتصلة بمقدرات إدارة الحوادث والحاجة إلى الأساس القانوني وإلى الإنفاذ.

41. واستهل العرض الأول في هذه الجلسة السيد بلحسن زواري، المدير العام التنفيذي، الهيئة الوطنية لأمن الحاسوب وفريق الاستجابة لطوارئ الحاسوب – مركز التنسيق التونسي (Cert-Tcc)، تونس، دراسة حالة قطْرية – مقدرات إدارة الحوادث، موضوع "مقدرات الترصد والتحذير والاستجابة للحوادث: تنفيذ استراتيجية وطنية"[26]. وقدم السيد زواري، من مركز التنسيق التونسي وهو فريق الاستجابة لطوارئ الحاسوب الوحيد المعترف به من قِبل جمعية السعي إلى الاستلهام والاعتراف بالعلوم والتكنولوجيا (FIRST)[27] في القارة الإفريقية وثالث فريق استجابة CERT في البلدان الناطقة باللغة

---

[25] http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/cade-government-industry-collaboration-casestudy-doha-feb-08.pdf.

[26] http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/zouari-incident-response-tunisia-doha-feb-07.pdf.

[27] http://www.first.org/.

العربية، قدم للمشاركين لمحة إجمالية عن كيفية نشوء مركز التنسيق. ففي نهاية عام 1999، أنشئت وحدة (عبارة عن فريق CERT مصغر) متخصصة في أمن تكنولوجيا المعلومات. وكان الهدف الأول المرسوم لهذه الوحدة هو إذكاء الوعي بين صانعي القرارات والعاملين التقنيين بشأن مسائل الأمن واستحداث أول فريق مهام من الخبراء التونسيين في مجال أمن تكنولوجيا المعلومات بهدف مراقبة الأمن في البنى التحتية والتطبيقات الوطنية الحرجة جداً. وفي عام 2002، بادرت الوحدة إلى وضع استراتيجية وخطة وطنية في مجال أمن تكنولوجيا المعلومات.

42. وفي يناير 2003، صدر قرار عن مجلس الوزراء، برئاسة رئيس الجمهورية، باستحداث وكالة وطنية متخصصة في أمن تكنولوجيا المعلومات بغية تيسير تنفيذ الاستراتيجية الوطنية. ونتيجة لذلك أُطلق في سبتمبر 2005 فريق الاستجابة لطوارئ الحاسوب – مركز التنسيق التونسي (Cert-Tcc). ومن بعض الأنشطة التي يضطلع بها مركز التنسيق هذا: الترصد والتحذير ونشر المعلومات والتوعية (وتشتمل على أشكال مختلفة من حملات إذكاء الوعي وتطوير ثقافة أمن سيبراني وتزويد المعلومات إلى القضاة وغير ذلك)، وتقاسم المعلومات وتحليلها وجمعها والتعامل مع الحوادث والتنسيق وغير ذلك. كما يقدم مركز التنسيق الدراية التقنية المحددة بشأن أمن تكنولوجيا المعلومات. ويختلف الشركاء الذين يتعامل معهم المركز باختلاف النشاط المعني بالأمر. وأشار السيد زواري إلى أن مقدِّمي خدمات الإنترنت يمثلون شريكاً هاماً في هذا النشاط إذ إنهم يقومون بإدارة بوابات دخولاً إلى البلد وخروجاً منه. وأكد السيد زواري أيضاً على ما جاء على لسان المتحدثين قبله – أي بينما تسعى جميع مبادرات إذكاء الوعي بالأمن السيبراني إلى هدف إجمالي وهو النهوض بثقافة أمن سيبراني هنالك حاجة واضحة إلى مواد محددة بشأن إذكاء الوعي وإلى برامج تبعاً للمجتمعات المستهدفة.

43. وقدم المتحدث التالي، السيد مارك كروتوسكي، المنسِّق الوطني، برنامج الاحتيال في الحاسوب والملكية الفكرية، قسم الجريمة الحاسوبية والملكية الفكرية، وزارة العدل، الولايات المتحدة الأمريكية، دراسات حالات تتناول الأساس القانوني وجانب الإنفاذ في إطار الأمن السيبراني في الاتحاد الدولي للاتصالات. وتحدث السيد كروتوسكي عن موضوع "الأساس القانوني والإنفاذ: النهوض بالأمن السيبراني"، وناقش الدور الرئيسي الذي يؤديه الأساس القانوني والإنفاذ من أجل الأمن السيبراني. وطرح عدداً من الأسئلة لينظر فيها كل بلد: ما هي قدرات القانون في معالجة جرائم الحاسوب؟ وما هو المدى الذي يمكن أن تبلغه الإجراءات القانونية في هذا الصدد، وخاصة بوجود إثباتات دامغة في الخارج؟ وما هي فعالية نظام العدالة الجنائي في ردع الجريمة؟ ثم انتقل السيد كروتوسكي بالمشاركين عبر مختلف أمثلة الحالات مبيّناً أن عدداً متزايداً من الحالات التي تتناولها النيابة العامة في هذه الأيام، سواء كانت جريمة منظمة أم جرائم مالية أم جرائم عنف، يشتمل على بعض من مكونات متصلة بالحاسوب أو أدلة إلكترونية. وذكر الحاجة إلى النظر في الإمكانات الهائلة بالنسبة للنمو الاقتصادي التي تجلبها الإنترنت ولكن لا بد في الوقت ذاته من ملاحظة أن كل هذه المنافع تتوقف على شبكات معلومات موثوقة وآمنة وعلى نظام عدالة جنائي فعال.

44. ومن شأن الأساس القانوني أن يوفر إطاراً للتحقيق في الجريمة السيبرانية واتخاذ الإجراءات القانونية بشأنها والعمل على ردعها والنهوض بالأمن السيبراني إلى جانب زيادة الثقة بالأنظمة القانونية وتشجيع التجارة. وأشارت إلى المكونات الأساسية في اتفاقية الجريمة السيبرانية والتي توفر إطاراً مفيداً. وأضاف أن الإطار يركز على الجرائم من حيث الموضوع وعلى القواعد الإجرائية وأدوات التحقيق وإنفاذ القوانين والتعاون الدولي إلى أقصى حد ممكن. ولذلك فإن من الأهمية المتزايدة بالنسبة لكل بلد أن يعمد إلى تطوير المقدرات والكفاءات المطلوبة للتحقيق في إساءة استعمال أو سوء استعمال الشبكات والحرص على عدم إفلات المجرمين الذين يهاجمون أو يستغلون الشبكات من العقاب. وهنالك العديد من التحديات التي تواجه الأساس القانوني، ومن هذه التحديات تزايد تطور الجرائم المرتكبة على الخط والطابع المتزايد تنظيماً لهذه الجرائم. وقال غالباً ما يكون الإثبات لحل جريمة في بلد ما متوفراً في بلد آخر مما يؤكد أهمية الشراكات الدولية. وتطرق إلى حالات تهديد حديثة تناولت استعمال البريد الإلكتروني. وبينما كان التهديد في أحد البلدان كانت أدلة إلكترونية هامة لكشف الجريمة موجودة في مخدمات في بلد آخر. وبفضل تعاون دوائر إنفاذ القوانين، أمكن العثور على الجناة و لم يصب أحد بأذى. ولذلك لا بد، على الصعيد الدولي، من أن تؤخذ في الحسبان قدرة المحققين على التحقيق في الجرائم المرتبطة بالحاسوب وجمع الإثباتات والحفاظ عليها (وحساسية عنصر الزمن في كل ذلك). ولذلك نوَّه السيد كروتوسكي بأن التدريب المتخصص جزء

هام جداً في أي برنامج وطني يرمي إلى ردع الجريمة السيبرانية وإلى بناء قدرة الإنفاذ. وختم حديثه قائلاً إن وزارة العدل الأمريكية، قسم الجريمة الحاسوبية والملكية الفكرية (CCIPS)، على استعداد لمساعدة البلدان في استعراض مشاريع قوانين الأمن السيبراني.

الجلسة 6: دراسات حالات قطْرية (تابع)

45. نظرت الجلسة 6 في مختلف لبنات البناء اللازمة لوضع استراتيجية ناجحة للأمن السيبراني الوطني إلى جانب بعض الأمثلة من البلدان في المنطقة. وترأس الجلسة السيد شمس الجفني شافعي، مدير إدارة الأمن والثقة والتحكم، الهيئة الماليزية للاتصالات وتعدد الوسائط، ماليزيا.

46. وتحدث السيد ستيف هوث، مدير فريق الاستجابة لطوارئ الحاسوب (Q-CERT) في قطر، عن موضوع "دراسة حالة بشأن الاستراتيجية الوطنية للأمن السيبراني – قطر"[28]، وتناول المبادرات الجارية والمبادرات المخطط لها في قطر، من خلال أنشطة ictQATAR وQ-CERT، فيما يتعلق بوضع استراتيجية وطنية للأمن السيبراني. ولدى التماس الاتفاق بشأن وضع استراتيجية وطنية للأمن السيبراني، ذكر السيد هوث أن من الضروري إيجاد الوعي في مستوى رسم السياسة الوطنية بشأن مسائل الأمن السيبراني وضرورة تركيز الإجراءات الوطنية وزيادة التعاون الدولي في هذا الشأن. وتطرَّق إلى الحاجة إلى ضمان أن يكون جميع أصحاب المصلحة، بمن فيهم صانعو القرارات، يتفهَّمون ضرورة وضع استراتيجية وطنية لتعزيز الأمن السيبراني وذلك لتخفيض المخاطر والآثار فيما يتعلق بالأعطال السيبرانية والمادية على السواء. وعلاوة على ذلك، فإن أي استراتيجية وطنية تحتاج إلى أن تُستكمَل بالمشاركة في الجهود الدولية للعمل على منع وقوع الحوادث الوطنية والتأهب لها والاستجابة إليها والتغلب عليها. ولتحقيق الرؤية الوطنية (رؤية ictQATAR) وهي "توصيل الناس بالتكنولوجيا التي تغني حياتهم وتدفع عجلة التنمية الاقتصادية وتبعث الثقة في مستقبل أمتنا"، أُنشئ الفريق Q-CERT في عام 2006 لكي يضمن من بين عدة أمور أن تكنولوجيا المعلومات والاتصالات المنشورة في البلد تتسم بالأمن والطواعية. والآن وقد بلغت أنشطة Q-CERT حالة النضوج، قال السيد هوث إن الحاجة تدعو الآن إلى مجموعة من الشركاء، بمثابة فريق CERT لبلدان مجلس التعاون لدول الخليج، لكي تتمكّن من التعاون على نحو أفضل ومن تقاسم المعلومات والتجارب الوطنية. وأشار إلى الفرص الممتازة السانحة للتعاون مع شركاء في تطوير ثقافة للأمن السيبراني.

47. وتناول السيد هوث مثالاً عملياً عن كيفية استعمال البلدان لإطار الأمن السيبراني لدى الاتحاد ومجموعة أدوات الأمن السيبراني الوطني/التقييم الذاتي لحماية البنية التحتية الحرجة للمعلومات لكي تتمكّن من تقييم المكانة التي بلغتها في تطوير جهود الأمن السيبراني الوطنية لديها ولمعرفة ما هي الجوانب التي تتطلب المزيد من العمل. وذكر السيد هوث أن الفريق Q-CERT وجد من المفيد مقارنة المقدرات بالإطار الذي وضعه الاتحاد، وكذلك في هذا الصدد وضع المعالم لقياس التقدم المحرز. وقال إن مسألة المرونة تتسم بأهمية حاسمة عند مناقشة الاستراتيجية وخصوصاً الاستراتيجية الوطنية للأمن السيبراني. وقال إن البلد يحتاج إلى خطة واضحة ولكن كثيراً ما يأتي الواقع بخلاف ذلك وما حدث أثناء التنفيذ الفعلي للاستراتيجية يحتاج إلى المزيد من الاهتمام. ولهذا فإن النتائج التي ترونها، في تنفيذ استراتيجية الأمن السيبراني، قد تختلف في نهاية الأمر عما كان في الأذهان في بادئ الأمر. وقد يتبيَّن أننا في حال أفضل مما خططنا له ولكننا قد نلاحظ أيضاً أننا نحتاج إلى الرجوع خطوة إلى الوراء والعمل على تكييف الأنشطة التي نقوم بها. واقترح السيد هوث أن تعمد كل منظمة إلى رسم العالم كما تراه من منظور تلك المنظمة ومن ثم مقارنة الاستراتيجية المخطط لها بالاستراتيجية المرسومة. وعند وضع وتنفيذ استراتيجية وطنية تبدو الدروس العديدة المستخلصة بديهية بعد التفكير. ولذلك من الأهم أن نتعلم من أفضل الممارسات ومن تجارب الآخرين. وقال السيد هوث إن إطار الأمن السيبراني للاتحاد والأدوات المتصلة به توفر هيكلاً يمكن فيه استعراض المسائل المتصلة بوضع استراتيجية وطنية. وختاماً قال السيد هوث إن أفضل الاستراتيجيات قد تكون عديمة الفائدة ما لم يتوفر لدى

[28] http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/huth-incident-management-qcert-doha-feb-08.pdf.

المنظمة الأفراد المناسبون لتنفيذها. ولذلك فإن توظيف الأفراد المناسبين وتدريبهم والاحتفاظ بهم من المكونات الحرجة في تنفيذ أي استراتيجية وطنية للأمن السيبراني.

48. وتحدثت السيدة فاطمة بازرجان، فريق الاستجابة لطوارئ الحاسوب (aeCERT)، هيئة تنظيم الاتصالات، الإمارات العربية المتحدة، عن موضوع "استراتيجية وطنية للأمن السيبراني – خارطة الطريق لفريق الاستجابة لطوارئ الحاسوب"[29]، ووصفت رؤية ودور فريق الاستجابة في الإمارات في تنفيذ الخطة الإجمالية للإمارات بشأن الأمن السيبراني. وقالت إن فريق الاستجابة لطوارئ الحاسوب (aeCERT) قد أُنشئ بناءً على مبادرة من هيئة تنظيم الاتصالات في الإمارات العربية المتحدة كهيئة استشارية يمكنها أن توصي باعتماد سياسات ممارسات جيدة وإجراءات وتكنولوجيات للكشف عن حوادث الأمن السيبراني الجارية والمقبلة في الإمارات والحيلولة دون وقوعها والاستجابة إليها. وذكرت السيدة بازرجان أيضاً أن فريق الاستجابة يعمل بنشاط للنهوض ببناء بيئة سيبرانية آمنة وثقافة سيبرانية في الإمارات. وقد أُطلق فريق الاستجابة في عام 2007 ولسوف يكون عندما يكتمل تشغيله في خدمة الحكومة وقطاعات إنفاذ القوانين ودوائر الأعمال في الإمارات. وأبرزت السيدة بازرجان أهمية وضع صورة وخطة إجماليتين قبل إنشاء وإطلاق فريق للاستجابة، على غرار الفريق في الإمارات، وشددت على القرار الواعي المتخذ بأن يبدأ فريق الاستجابة صغيراً ثم ينمو مع الزمن.

49. وتحدثت السيدة بازرجان عن حملة وطنية جارية بشأن الوعي بالأمن وهي الأولى من نوعها في الإمارات العربية المتحدة. وقد أُطلقت الحملة في نوفمبر 2007 تحت شعار "حماية هويتك على الخط" وهي تركّز على إذكاء الوعي بشأن موضوعات من مثل أمن كلمة السر و"الهندسة الاجتماعية" وبصفة عامة أساسيات أمن المعلومات. وقد أُعدّت مواد الحملة باللغتين العربية والإنكليزية وهي تستهدف أصحاب الأعمال والمستعملين في المنـــزل وطلبة المدارس.

50. وتناول السيد سليمان السمحان، متخصص في أمن المعلومات، فريق الاستجابة لطوارئ الحاسوب (SA-CERT)، هيئة تكنولوجيا الاتصالات والمعلومات، المملكة العربية السعودية، الأنشطة في مجال "فريق الاستجابة لطوارئ الحاسوب في المملكة العربية السعودية"[30]، (SA-CERT). وتتمثل رؤية فريق الاستجابة في أن يكون مرجعاً موثوقاً ذا حجية بالنسبة لأمن المعلومات في المملكة العربية السعودية، وهو يرمي من خلال أنشطته ومبادراته إلى تحسين سوية الوعي بأمن المعلومات في المملكة. وقال السيد السمحان إن فريق الاستجابة يعمل نحو بلوغ هذا الهدف من خلال تنسيق الجهود الوطنية والدولية وبالنهوض بأفضل الممارسات في مجال أمن تكنولوجيا المعلومات وبناء الثقة في أوساط المجتمع السيبراني من خلال بناء القدرات بشأن أمن المعلومات والنهوض ببيئة موثوقة للتعاملات الإلكترونية وتدعيم هذه البيئة، من بين أمور أخرى.

51. وتحدث السيد السمحان عن المراحل الثلاث لإقامة فريق الاستجابة (SA-CERT) وما يقوم به من أنشطة. وتشمل المرحلة 1 التخطيط وبداية التنفيذ لعمليات خط الأساس من خلال بناء الوعي والثقة ومقدرات الاستجابة الضرورية. وتتطلب المرحلة 2 خطوات زيادة تدريجية للنهوض بالقدرة التشغيلية وما يتصل بها من بناء القدرات وذلك من خلال أنشطة الرصد والاستجابة والتنسيق وما يتصل بها من مبادرات. وأخيراً، فإن المرحلة 3 هي التشغيل الكامل لجميع الأنشطة المتصلة بالموضوع. وفي الوقت الراهن، يركّز فريق الاستجابة السعودي بالدرجة الرئيسية على إذكاء الوعي بالأمن السيبراني من خلال برامج توعية معدّة باللغة العربية وزيادة وتعزيز الخدمات المقدمة. وعلى غرار من سبقه في الحديث، أكد السيد السمحان أيضاً على الحاجة إلى توفر عاملين محليين مدربين ومكرّسين للعمل وأفراد قادرين على دعم أنشطة فريق الاستجابة. وذكر السيد السمحان أن هنالك حاجة ماسة إلى مركز وطني مرجعي ونظام لتوفير المعلومات بشأن الأمن السيبراني. وتلبية لهذه الحاجة تم إعداد "كتيِّب أمن المعلومات". وسوف يُنشر هذا الكتيِّب باللغتين العربية والإنكليزية قريباً في موقع فريق الاستجابة على شبكة الويب. وقال إن الفريق يعكف على تطوير قدر وافر من مختلف مواد إذكاء الوعي بشأن الأمن السيبراني، ما يشار إليه باسم "منشورات الأمن"، باللغة العربية، بشأن مواضيع تتناول مثلاً الأمن اللاسلكي وأمن البريد

[29] http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/bazargan-national-strategy-aeCERT-doha-feb-08.pdf.

[30] http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/alsamhan-national-strategy-CERT-SA-doha-feb-08.pdf.

الإلكتروني وحماية الحواسيب الشخصية في المنـــزل من تهديدات الإنترنت وحماية الخصوصية ومكافحة الاقتحام والاحتيال فضلاً عن دليل لأولياء الأمر لتعزيز أمن الأطفال على شبكة الإنترنت.

الجلسة 7: مراجعة ومناقشة: إطار إدارة لتنظيم الأمن السيبراني الوطني/جهود حماية البنية التحتية الحرجة للمعلومات

52. تناولت الجلسة 7، الجلسة الأخيرة في اليوم، استعراض ومناقشة *إطار إدارة لتنظيم الأمن السيبراني الوطني/جهود حماية البنية التحتية الحرجة للمعلومات*، وحددت بعض المقتبسات الرئيسية من العروض المقدمة بشأن الإطار ودراسات الحالات القطْرية المتصلة به تمهيداً لمناقشات ختام ورشة العمل. وتيسيراً لتنظيم الجلسة، طلب مدير الجلسة السيد روبرت شو، رئيس شعبة تطبيقات تكنولوجيا المعلومات والاتصالات والأمن السيبراني، قطاع تنمية الاتصالات في الاتحاد، من ستة خبراء أن يقدموا المقتبسات الرئيسية من الجلسات الست الأولى، وإذا أمكن تقديم بعض المقترحات والتوصيات من أجل الخطوات العملية التالية في المنطقة.

53. قالت السيدة مارلين كيد، المستشارة لدى شركة AT&T، الولايات المتحدة الأمريكية، إننا ما زلنا في الأيام الأولى من بناء ثقافة الأمن السيبراني وفي المراحل الأولى من بناء إطار في كل بلد. ولذلك يمكننا أن نبدأ في التفكير في المسائل المشتركة عبر مختلف ورش العمل التي تُعقد وأن نستخلص المعلومات من هذه الورش ونقارنها مع احتياجاتنا لمواصلة تقاسم المعلومات وجمع المعلومات التي يمكن تقاسمها مع البلدان الأخرى (مثال ذلك النُهج المجدية وتلك غير المجدية وما إلى ذلك). وأشارت إلى أننا عندما نتحدث عن التعاون بين الحكومة والصناعة علينا أن نتأكد من استمرار مشاركة الصناعة وأن نتساءل ما هي الجهات الأخرى في دوائر الصناعة التي ينبغي إشراكها في المستويات الوطنية والإقليمية والدولية. وفي النظام الإيكولوجي الإجمالي للأمن السيبراني، هنالك العديد جداً من الأطراف التي يتعيَّن أن تشارك في المسألة، ولهذا السبب ذكرت السيدة كيد ضرورة بلوغ أفرقة مشغِّلي الشبكات الإقليمية ومكاتب تسجيل الإنترنت الإقليمية ومشغِّلي أسماء الميادين القطْرية ذات المستوى الأعلى (ccTLD) وغيرها، للحرص على دعوتها لحضور ورش العمل المقبلة حول هذا الموضوع وذلك للتمكُّن حقاً من بناء ثقافة للأمن السيبراني.

54. وقال السيد سليمان السمحان، المتخصص في أمن المعلومات، فريق الاستجابة لطوارئ الحاسوب (SA-CERT)، هيئة تكنولوجيا الاتصالات والمعلومات، المملكة العربية السعودية، إن أهم ما حدث في مجال الأمن السيبراني في المملكة العربية السعودية وفي بلدان مجلس التعاون لدول الخليج هو إصدار القوانين الضرورية بحيث بدأ الناس التفكير في عواقب ما يقومون به من أعمال. وفي غالبية الحالات سوف تبدأ هذه القوانين في فرض الشروط على مقدِّمي خدمات الإنترنت للاحتفاظ بالمعلومات وتخزينها للاحتياجات الممكنة في المستقبل. وعلاوة على ذلك، فإن بناء القدرات في مجال الأمن السيبراني مسألة حاسمة. ولدى المصارف وشركات الاتصالات الآن عاملون أكفاء في مجال الأمن ولكن الحاجة ماسة إلى مزيد من بناء القدرات. وقال إن بناء القدرات وإذكاء الوعي، من خلال مختلف البرامج والمبادرات، يتطلب بل ويستحق المزيد من الاهتمام في المنطقة.

55. وقال السيد شمس الجفني شافعي، مدير إدارة الأمن والثقة والتحكم، اللجنة الماليزية للاتصالات وتعدد الوسائط، ماليزيا، بعد أن استمع إلى العروض المقدمة من مختلف أفرقة الاستجابة للطوارئ في المنطقة، من الممتع الاستماع إلى الحديث عن الاستراتيجيات والأهداف من هذه الأفرقة المنشأة حديثاً. ومن الواضح أن النُهج المقدمة تعتمد على التجارب التي مرت بها أفرقة أخرى للاستجابة لطوارئ الحاسوب. وتابع السيد شافعي القول، من الضروري جداً، من منظور السياسة والإنفاذ، أن تتوفر السياسات الصحيحة والإنفاذ الصحيح عندما نتصدى إلى الأمن السيبراني. إذ من الميسور نسبياً الحصول على المعلومات والمساعدة في صياغة التشريعات ولكن المشكلة تكمن حقاً في جانب الإنفاذ من هذه المسألة. إذ تتطلب زيادة الفهم في دوائر القضاء، وجميع مستويات الإنفاذ على اختلافها، قدراً مكثفاً من التدريب. فالجهات المعنية بتنظيم المصارف وتلك المعنية بتنظيم الاتصالات وكذلك أفراد الشرطة بحاجة إلى معارف فيما يتعلق بالجريمة السيبرانية. وفيما عدا القوانين

المناسبة والإنفاذ المناسب فإن الأمر يحتاج إلى معالجة جوانب بناء القدرات على وجه السرعة. ولا بد في هذا الصدد من توفر الأفراد المناسبين في الأماكن المناسبة للقيام بما ينبغي القيام به. ونوَّه السيد شافعي بعمل قطاع تنمية الاتصالات في البلدان وفي المناطق في إيجاد ثقافة لتقاسم المعلومات وأعرب عن أمله في أن يستمر ذلك في المستقبل. وعلاوة على ذلك، فإننا نحتاج، عندما نضطلع بهذه الجهود، إلى أن نتذكر بأننا لسنا وحدنا، فهنالك بلدان أخرى تحاول أن تتصدى لنفس المسائل.

56. وأشار السيد برادفورد ويلكي، الموظف التقني رفيع المستوى، إدارة المؤسسة القابلة للبقاء، CERT، جامعة كارنيغي ميلون، الولايات المتحدة الأمريكية، إلى أننا عندما ننظر في التصميم الفعلي وفي مضمون الأنشطة الضالعة في الأمر ينبغي لنا أيضاً أن ننظر إلى معايير قدرة المخاطر. وقال السيد ويلكي إن إدارة الحوادث أكثر من مجرد مسألة التكنولوجيا. وينبغي في معرض الحديث عن ذلك تركيز الاهتمام على هدف واحد وهو المقدار القابل للقياس لما لا نريد أن يحدث وكذلك مقياس لما نريد أن يكون لدى الاقتصاد. ومن الممكن أن يكون بين هذه المعلومات أيضاً دواعي الثقة في الحكومة. فالبريد الاقتحامي مثلاً عبارة عن مقدار قابل للقياس ثقافياً حيث تكون بعض الأشياء مقبولة أو غير مقبولة إلى حد ما. فعدم القيام بأي شيء إزاء البريد الاقتحامي يبيِّن أهمية ذلك بالنسبة لبلد ما. ومن الموصى به اعتماد نموذج مفتوح وكذلك الحاجة إلى التفكير محلياً والتخطيط عالمياً. فالبنى التحتية للاتصالات في قَطَر مثلاً مسألة حاسمة ولذلك فإننا نحتاج في السعي إلى تحقيق أهدافنا إلى العمل على إقامة تعاون عملي بين الحكومة والصناعة في هذا المجال. وهنالك قدر لا بأس به من التعاون مع الصناعة ويتعيَّن على الحكومات أن تستغل ذلك وأن تتجنب اضطراب هذا التعاون من جرّاء انتهاج سياسات جديدة.

57. واسترعى السيد شريف هاشم، نائب الرئيس التنفيذي، وكالة تنمية صناعة تكنولوجيا المعلومات، وزارة تكنولوجيا الاتصالات والمعلومات، جمهورية مصر العربية، اهتمام المشاركين إلى الأدوار والمسؤوليات المتصلة بإطار الأمن السيبراني للاتحاد. ونظراً لتعدد واختلاف الوكالات الحكومية وأصحاب المصلحة في القطاع الخاص (من شركات ومؤسسات متعددة الجنسيات والمشاريع المتوسطة والصغيرة، وغير ذلك) فلا بد لنا من توضيح الجهة المقصودة التي نتحدث عنها. وقال إن أثر الأمن السيبراني يهم كل الناس ولذلك يتعيَّن مشاركة جميع الأطراف في عملية تحديد وتنفيذ استراتيجية وطنية من أجل الأمن السيبراني. وعندما ننظر في مسألة وضع استراتيجية وطنية للأمن السيبراني، ينبغي أن يشارك في هذه الجهود جميع أصحاب المصلحة سواء بصورة مباشرة أو غير مباشرة. ومن الشروط الأساسية المسبقة أيضاً التوجيه والامتلاك على مستوى رفيع. وعندما ننظر إلى أدوار ومسؤوليات مختلف الجهات أصحاب المصلحة والتعاون بين هذه الجهات، لا بد لنا من أن ننظر في تعريف ما هو المقصود بالتعاون. ومن الجهود الهامة جداً دور الاتحاد الدولي للاتصالات وغيره من المنظمات الدولية في تقاسم المعلومات وتعميم أفضل الممارسات. ونوَّه السيد هاشم أيضاً بأهمية اعتماد نهج محايد تكنولوجياً في مكافحة الجرائم السيبرانية.

58. وقال السيد جوزف ريتشاردسون، الولايات المتحدة الأمريكية، وهو المتحدث الأخير بين الخبراء، إنه استمع إلى بعض الأسباب الوجيهة لكي تعمل الحكومات مع دوائر الصناعة من أجل الأمن السيبراني وأن هنالك العديد من مختلف الأساليب للتعاون مع الصناعة. ونحن نواجه في جميع البلدان مسألة عدم التمكُّن من إشراك كل الأطراف في الصناعة، جميع القطاعات والمؤسسات على اختلافها. ولحل هذه المسألة، تحتاج البلدان بدلاً من ذلك إلى إيجاد نهج يضم هؤلاء الممثلين في رابطات صناعية يمكنها بدورها أن تشارك في المناقشات باسم تلك الأطراف. ويحتاج الأمر إلى مزيد من العمل لتحديد الأطر المطلوبة لهذا التعاون. كما يتعيَّن النظر إلى التعاون مع الصناعة بأساليب مختلفة. ومن المجالات التي تحتاج إلى أن تتطوَّر بصفة خاصة هو دور العلاقات، لا العلاقات مع الصناعة فحسب وإنما مع العناصر الأخرى في الحكومة أيضاً. ونحن بحاجة في المستقبل إلى ضمان مشاركة وزارات أخرى، بالإضافة إلى وزارات الاتصالات، في ورش العمل هذه التي تتناول الأمن السيبراني وما يتصل بها من أنشطة. وختم السيد ريتشاردسون قوله مشيراً إلى أنه لم يسمع أي شيء يوحي بأن إطار الأمن السيبراني لدى الاتحاد لا يمثل أداة مفيدة لبناء قدرات الأمن السيبراني.

الجلستان 8 و9: مجموعة أدوات الاتحاد الدولي للاتصالات للتقييم الذاتي للأمن السيبراني الوطني/ حماية البنية التحتية الحرجة للمعلومات: تمرين

59. تعتمد مجموعة أدوات الاتحاد للتقييم الذاتي للأمن السيبراني الوطني/حماية البنية التحتية الحرجة للمعلومات[31] على دراسات جارية في إطار المسألة 22 في لجنة الدراسات 1 لدى قطاع تنمية الاتصالات: *تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني*. وتطبِّق مجموعة الأدوات هذه، والتي تمثل واحداً من جوانب التآزر الرئيسية بين عمل المسألة 22/1 وأنشطة برنامج عمل الأمن السيبراني لدى الاتحاد لمساعدة البلدان النامية (2007-2009)[32]، الإطار الجاري تطويره في لجنة الدراسات مشفوعاً بمجموعة أدوات عملية للنظر فيها على المستوى الوطني. وترمي مجموعة الأدوات إلى مساعدة الحكومات الوطنية على النظر فيما لديها من سياسات وإجراءات ومعايير ومؤسسات وطنية وعلاقاتها في ضوء الاحتياجات الوطنية لتعزيز الأمن السيبراني وتتناول مسألة حماية البنية التحتية الحرجة للمعلومات. ومجموعة الأدوات موجهة للقائمين على مستوى وضع السياسة والإدارة في الحكومات وتتناول السياسات والإطار المؤسسي والعلاقات من أجل الأمن السيبراني. وهي تسعى إلى تصوير الوضع الراهن فيما يتعلق بالسياسة والمقدرة الوطنية والمؤسسات والعلاقات المؤسسية والموظفين والدراية التقنية والعلاقات القائمة بين الهيئات الحكومية والعلاقات فيما بين الحكومات ودوائر الصناعة والهيئات الأخرى في القطاع الخاص.

60. وترمي الجلستان 8 و9 في ورشة العمل إلى الأخذ بيد البلدان خلال عملية التقييم الذاتي لمساعدة الحكومات على ما تبذله من جهود في الوقت الراهن وتحديد الثغرات التي تتطلب الاهتمام وترتيب أولويات الجهود الوطنية والآثار العملية المترتبة على الإطار. ولاحظ السيد جوزف ريتشاردسون، الذي قام بعملية تيسير التمرين في توجيه البلدان من خلال عملية التقييم الذاتي، إلى أن ليس هنالك من جانب واحد أو نهج واحد صحيح وأن جميع البلدان تنفرد بمتطلبات ورغبات على الصعيد الوطني. ويحتاج الأمر إلى استمرار الاستعراض والمراجعة لأي نهج يُتبع ومن الضروري أيضاً ضمان مشاركة جميع أصحاب المصلحة، بما يناسب دور كل منها، في وضع استراتيجية وطنية للأمن السيبراني ولحماية البنية التحتية الحرجة للمعلومات.

61. وذكر السيد ريتشاردسون أن مجموعة الأدوات والموارد المتصلة بها تُستحدث باستمرار في موقع الأمن السيبراني لقطاع تنمية الاتصالات (www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html)، كما يضطلع بمشروعات قطْرية رائدة لاختبار وتقييم مجموعة الأدوات وذلك بالاقتران مع عدد من ورش العمل القطْرية لبناء القدرات التي ينظمها الاتحاد في عامي 2008 و2009. وشجَّع السيد ريتشاردسون المشاركين في الاجتماع على تقاسم تجاربهم القطْرية المعيَّنة وطرح الأسئلة على الخبراء الذين تحدثوا عن كل من الدعائم الخمس في إطار الأمن السيبراني للاتحاد.

الجلسة 10: التعاون الإقليمي والدولي

62. يتسم التعاون الإقليمي والدولي بأهمية كبرى في تعزيز ثقافة الأمن، إلى جانب دور المنتديات الإقليمية في تيسير التفاعلات والتبادلات. وقد استعرضت هذه الجلسة بعض مبادرات التعاون الإقليمي والدولي الجارية لإحاطة المشاركين علماً بها ولتشجيعهم على الدعم والمشاركة في المزيد من الإجراءات الملموسة التي يمكن تنفيذها في الدول العربية وكذلك على الصعيد الدولي. وافتتح الجلسة مديرها السيد مايكل لويس، نائب المدير، فريق الاستجابة لطوارئ الحاسوب (Q-CERT)، قطر، وقدم المتحدثين الأربعة في الاجتماع.

63. وتحدث السيد مارك كروتوسكي، المنسِّق الوطني، برنامج الاحتيال الحاسوبي والملكية الفكرية، قسم الجريمة الحاسوبية والملكية الفكرية، وزارة العدل، الولايات المتحدة الأمريكية، وممثل مجموعة 24/7 لشبكة جريمة التكنولوجيا الرفيعة،

---

31 http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html.

32 http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf.

في عرضه بعنوان "تعزيز التعاون الإقليمي والدولي بشأن مسائل الأمن السيبراني"[33]، عن أنشطة شبكة جريمة التكنولوجيا الرفيعة 24/7. وقال إن الغرض من شبكة جريمة التكنولوجيا الرفيعة 24/7، وهي في الأصل مبادرة انطلقت من مجموعة الدول الصناعية الثماني (G8)، توفير شبكة اتصال في حالة الطوارئ على الخط مباشرة بشأن مسائل الجريمة. وتتألف الشبكة من عاملين في مجال إنفاذ القوانين يتقاسمون المعلومات والمشورة بشأن صيانة البيانات وجهاز الاتصال لدى مقدِّمي خدمات الإنترنت، وكيفية الشروع في عمليات المساعدة القضائية المتبادلة. ولدى شبكة جريمة التكنولوجيا الرفيعة 24/7 جهات اتصال في نحو 50 بلداً، بالإضافة إلى مشاركة العديد من البلدان الآسيوية والأوروبية وبلدان أمريكا الجنوبية، بالإضافة إلى الدول الأعضاء في مجموعة G8. والشبكة مفتوحة أمام جميع البلدان، والانضمام إلى شبكة 24/7 مسألة في منتهى السهولة. والاشتراط الوحيد هو الإتاحة ولكن هذا لا يعني بالضرورة الالتزام بالمساعدة. ويتعيَّن على البلدان المهتمة بالانضمام إلى الشبكة تحديد جهة اتصال أولية لديها القدر الكافي من المعارف التقنية عندما يتناول الأمر الجرائم السيبرانية – وخصوصاً أن واحداً من المسائل الرئيسية في مجال الجريمة السيبرانية هو التعامل بالأدلة القضائية الرقمية. ويتعيَّن أيضاً على جهة الاتصال في شبكة جريمة التكنولوجيا الرفيعة 24/7 الإلمام بالقوانين والإجراءات المحلية في هذا المجال على وجه التحديد. وذكر السيد كروتوسكي أن بإمكان البلدان المهتمة بمعرفة المزيد عن هذه الشبكة الاتصال بقسم الجريمة الحاسوبية والملكية الفكرية في وزارة العدل الأمريكية (CCIPS).

64. وتحدث السيد إبراهيم الحداد، رئيس المكتب الإقليمي للدول العربية في الاتحاد الدولي للاتصالات، عن بعض الأنشطة الجارية والمخطط لها التي يضطلع بها الاتحاد والمكتب الإقليمي للاتحاد في الدول العربية بغية النهوض بثقافة أمن في المنطقة. وذكر السيد الحداد أن الاتحاد الدولي للاتصالات قد طُلب منه، من خلال عملية القمة العالمية لمجتمع المعلومات، أن يكون بمثابة منسِّق للأنشطة التي ترد في إطار خط العمل جيم5 في القمة المذكورة المكرّس لبناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات. ولكن الاتحاد ليس بوسعه الاضطلاع بالمهام المنوطة به إلا بالعمل مع الدول الأعضاء لديه، مما يعني أيضاً بلدان المنطقة الممثلة في ورشة العمل هذه بشأن الأمن السيبراني. وبناء الثقة بين أصحاب المصلحة مسألة عسيرة وتحتاج إلى الوقت، وعلى عاتق المكتب الإقليمي للاتحاد تقع مسؤولية أن تؤخذ في الحسبان احتياجات 22 بلداً عربياً أعضاء في جامعة الدول العربية. وورشة العمل هذه المعقودة في الدوحة واحدة من سلسلة لقاءات يعقدها الاتحاد بشأن الأمن السيبراني في جميع أرجاء العالم في الفترة 2009/2008 كما يعمل الاتحاد على نحو وثيق مع عدد من المنظمات الدولية والإقليمية المعنية في محاولة لضمان أن تعمل هذه البلدان معاً في المسائل المتصلة بالأمن السيبراني. ونظراً لتزايد عدد أحداث الأمن السيبراني الإقليمية والدولية، من الواضح أن فرداً واحداً لا يستطيع المشاركة فيها جميعاً، لذلك يتعيَّن على كل بلد أن يختار تلك اللقاءات وورش العمل ومجالات الاهتمام ذات الصلة بذلك البلد. ولكن من الواضح أن ليس بوسعنا العمل في معزل من أجل الأمن السيبراني، وإنما نعتمد على غيرنا ونحتاج إلى مساعدة الآخرين، ولذلك فإن الدعم والتعاون الإقليميين لهما أهمية متزايدة في هذا المجهود.

65. ونوَّه السيد مجيد الشرهان من المملكة العربية السعودية، ممثلاً مجلس التعاون لدول الخليج، بالعروض القيِّمة التي تقدم بها الخبراء وممثلو البلدان في الاجتماع. وتحدث السيد الشرهان عما يقوم به مجلس التعاون لدول الخليج في مجال الأمن السيبراني والأنشطة المحددة التي يخطط للاضطلاع بها في المستقبل. وأشار إلى أن مجلس الاتحاد كان منذ عام 2004 يشجِّع بنشاط البلدان في المنطقة على إنشاء أفرقة للاستجابة لطوارئ الحاسوب كما عُقد اجتماع لبلدان مجلس التعاون في قطر لمناقشة مسألة الأمن السيبراني في المنطقة. ونتيجة لذلك، وُقِّعت مذكرة تفاهم نوقش فيها مسودة مشروع لمركز أمن سيبراني إقليمي/فريق للاستجابة لطوارئ الحاسوب. ولكن الاجتماع لم يعتمد المقترح الرامي إلى إقامة فريق للاستجابة لطوارئ الحاسوب على مستوى بلدان مجلس التعاون.

66. وذُكر في الاجتماع آنف الذكر إذا كان المقصود من فريق الاستجابة لطوارئ الحاسوب أن يكون مركزاً مشتركاً لجميع بلدان مجلس التعاون لدول الخليج فإن الأمر يحتاج إلى عملية أخرى لتمويل المركز إذ إن ميزانية المركز لا يمكن أن

[33] http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/krotoski-regional-international-cooperation-doha-feb-08.pdf.

تدعمها حكومة واحدة فقط. ولذلك، وكحل مؤقت، اقتُرح أن يخوَّل فريق الاستجابة لطوارئ الحاسوب في قطر (Q-CERT) بإقامة اتفاقات ثنائية بين قطر والبلدان الأخرى في مجلس التعاون للمساعدة على بناء مقدرات هذا الفريق. وللأسف لم يوفَّق هذا الاقتراح أيضاً وإنما اتُفق في اجتماع وزاري على إنشاء لجنة لوضع مبادئ توجيهية من أجل هذا التعاون وأُسندت إلى قطر مسؤولية القيام بذلك. وذكر السيد الشرهان أن بلدان مجلس التعاون متحمسة جداً لمشروع إقامة فريق للاستجابة لطوارئ الحاسوب من أجل بلدان مجلس التعاون وأن تنفيذه في المستقبل سيكون حقاً واحداً من منجزات مجلس التعاون. وختاماً قال السيد الشرهان إن مجلس التعاون لدول الخليج ما زال ينتظر ردود الدول الأعضاء فيه بشأن النهج الواجب اتباعه من أجل فريق الاستجابة لطوارئ الحاسوب في بلدان مجلس التعاون لدول الخليج.

67. وتحدث السيد خالد فوده، رئيس قسم تكنولوجيا المعلومات، إدارة الاتصالات وتكنولوجيا المعلومات، جامعة الدول العربية، عن كيفية تناول الدول الأعضاء في جامعة الدول العربية المسائل المتصلة بالأمن السيبراني. وذكّر السيد فوده بأن البلدان العربية كانت من بين أولى المجموعات الإقليمية التي أدركت أهمية اعتماد وتنفيذ استراتيجية على المستوى الإقليمي لبناء مجتمع المعلومات. وقد أدى ذلك إلى اعتماد وثيقة استراتيجية للمجموعة العربية بشأن تكنولوجيا الاتصالات والمعلومات في عام 2001 في قمة عمّان. كما ساهمت البلدان العربية مساهمة فعَّالة في مرحلتي القمة العالمية لمجتمع المعلومات. ونظراً لسرعة تطور وتغير التكنولوجيات أدركت البلدان العربية الحاجة إلى صياغة وثيقة جديدة والموافقة عليها لتمكين البلدان من العمل بصورة أكثر فعالية على الصعيدين الوطني والإقليمي. ونظراً للحاجة إلى تعزيز التفاعل بين مختلف الأطراف المعنية، وأخذاً في الحسبان للتطورات الإقليمية والدولية ذات الصلة أثناء العام الماضي في المنطقة، عمدت البلدان إلى صياغة "الاستراتيجية العربية لتكنولوجيا الاتصالات والمعلومات – بناء مجتمع المعلومات 2007-2012"، والتي ستُقدَّم أثناء القمة المقبلة في دمشق، الجمهورية العربية السورية، في مارس 2008.

68. وتسعى الاستراتيجية إلى تحقيق ثلاثة أهداف استراتيجية رئيسية، وهي: 1) إيجاد سوق تنافسية لمجتمع المعلومات العربي كجزء من مجتمع المعلومات العالمي، 2) تحقيق النفاذ الشامل وتحسين نوعية الخدمات للمواطن العربي الذي يستعمل تكنولوجيا المعلومات والاتصالات، 3) المضي في تطوير تكنولوجيا المعلومات وصناعة الاتصالات من أجل إيجاد فرص عمل جديدة وخدمات وفرص خبرة جديدة. وبناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات جزء لا يتجزأ من هذه الأنشطة. فمجتمع المعلومات وأمن الشبكات وحماية البيانات والخصوصية من الشروط المسبقة التي لا غنى عنها من أجل تطوير مجتمع المعلومات وبناء الثقة بين المستعملين. وذكر السيد فوده أيضاً أن جامعة الدول العربية سوف تسعى إلى تنفيذ هذه الأهداف: أ) بالمساهمة في تأمين وإدارة حقوق التأليف الرقمية على الإنترنت وصياغة السياسات الملزمة لمكافحة تجاوز حقوق الملكية الفكرية؛ ب) من خلال التعاون على الصعيد الدولي لمكافحة الجرائم في الفضاء السيبراني وإساءة استعمال تكنولوجيا المعلومات والاتصالات؛ ج) من خلال وضع التشريعات لحماية البيانات وضمان حماية الخصوصية للمواطن العربي؛ د) من خلال توفير أمن المعلومات والشبكات لضمان خصوصية المستعمل؛ ه) من خلال سن قوانين وتشريعات لتجريم عملية اقتحام الشبكات. ويجري الآن انتقاء المشاريع التي تسعى إلى تحقيق هذه الأهداف الاستراتيجية. وقد بدأت البلدان العربية تدرس مختلف النُهج والاختيارات وهنالك مقترحات من المغرب ومن الكويت ومقترح ثالث من قطر لإنشاء مركز عربي للاستجابة للحوادث.

الجلسة 11: الخلاصة والتوصيات وآفاق المستقبل

69. تناولت الجلسة الختامية للاجتماع، ومديرها السيد روبرت شو، رئيس شعبة تطبيقات تكنولوجيا المعلومات والاتصالات والأمن السيبراني، قطاع تنمية الاتصالات في الاتحاد، الإبلاغ عن بعض الاستنتاجات الرئيسية التي انبثقت عن اللقاء، كما تناولت بالتفصيل مجموعة من التوصيات من أجل الأنشطة المقبلة بغية تعزيز الأمن السيبراني وتعزيز حماية البنى التحتية الحرجة للمعلومات في المنطقة. واتفق المشاركون على النتائج التالية المنبثقة عن اللقاءات (انظر كامل إعلان الدوحة بشأن الأمن السيبراني في الملحق 1 أدناه):

- الاعتراف بأن تحسين الأمن السيبراني مشكلة عالمية وأن كل بلد يجب عليه أن يتخذ الإجراءات اللازمة لكي ينضم إلى الجهود الدولية لتحسين الأمن السيبراني وأن يدعم هذه الجهود.
- الاعتراف بالمبادرات والإجراءات والنُهج التي أثبتت جدواها في عدد من البلدان وفي مناطق أخرى وبالجهود التي يبذلها الاتحاد الدولي للاتصالات وغيره من المنظمات من أجل إعداد مجموعة من "أفضل الممارسات" ووضع أدوات من شأنها تدعيم الجهود الوطنية داخل المنطقة العربية.
- الاعتراف بأن إطار الاتحاد للأمن السيبراني/حماية البنية التحتية الحرجة للمعلومات يوفر دليلاً مفيداً لإذكاء الوعي وللمبادرة باتخاذ الإجراءات الوطنية و/أو مراجعتها من حيث إنها تساعد في ضمان الاتساق والمواءمة في الإجراءات بين الدول.
- التوصية باستكمال إطار الاتحاد للأمن السيبراني/حماية البنية التحتية الحرجة للمعلومات والموارد المتصلة به ومجموعات الأدوات وذلك في أقرب وقت ممكن وتوفيرها بجميع لغات العمل في الاتحاد، والاهتمام بصفة خاصة باللغة العربية لدعم الجهود في المنطقة.
- تشجيع كل بلد في المنطقة على استخدام الإطار ومجموعة أدوات الاتحاد للتقييم الذاتي للأمن السيبراني الوطني/ حماية البنى التحتية الحرجة للمعلومات المتصلة به كوسيلة لتطوير مؤسساتها وسياساتها وعلاقاتها من أجل الأمن السيبراني وحماية البنى التحتية الحرجة للمعلومات.
- الاعتراف بأن بعض البلدان في المنطقة قد تحتاج إلى الدعم والمساعدة في تنفيذ الإطار وفي استعمال مجموعة أدوات التقييم الذاتي للأمن السيبراني الوطني/حماية البنية التحتية الحرجة للمعلومات ومطالبة قطاع تنمية الاتصالات بأن ينظر في أساليب توفير هذا الدعم.
- الاتفاق على أن يقوم كل بلد في المنطقة، إن لم يكن قد فعل ذلك، بتطوير مقدرة على إدارة الحوادث (فريق للاستجابة لحوادث أمن الحاسوب (CSIRT)/فريق الاستجابة لطوارئ الحاسوب (CERT)) مشفوعة بالمسؤولية الوطنية واستعمال الأمثلة الراهنة وأفضل الممارسات للأفرقة CSIRT/CERT في المنطقة لدى تطوير المقدرات الوطنية.
- الاتفاق على أن واحداً من المكونات الهامة لتطوير إطار وطني هو الانضمام إلى الجهود الإقليمية والدولية للنهوض بثقافة الأمن السيبراني.
- التأكيد على أهمية تطوير مبادرات وموارد تعاون إقليمية تكون بمثابة أمثلة لأفضل الممارسات وفرص التدريب والتعليم ووضع النماذج لبناء القدرات التي يمكن تكييفها تبعاً لاحتياجات كل بلد في الإقليم.
- مطالبة قطاع تنمية الاتصالات بالشراكة مع المنظمات الإقليمية والإدارات الوطنية باتخاذ المبادرات الضرورية لمتابعة نتائج الاجتماع ولتوفير تحديثات بشأن التقدم والتعاون الإقليمي. وينبغي، في مبادرات المتابعة هذه، تشجيع المشاركة من جانب الأطراف الإضافية المحددة في الإطار (مثال ذلك جميع الوزارات المعنية ودوائر الأعمال والمنظمات الأخرى).
- التعبير عن التقدير للمجلس الأعلى للاتصالات وتكنولوجيا المعلومات في قطر (ictQATAR) وفريق الاستجابة لطوارئ الحاسوب في قطر (Q-CERT) والاتحاد الدولي للاتصالات، على ما قدَّمته من دعم وتسهيل للاجتماع.

اختتام الاجتماع

70. أعرب السيد مايكل لويس، نائب المدير، فريق الاستجابة لطوارئ الحاسوب، بالنيابة عن المجلس الأعلى للاتصالات وتكنولوجيا المعلومات (ictQATAR) وفريق الاستجابة لطوارئ الحاسوب (Q-CERT)، عن أمله في أن تكون ورشة العمل

قد أثبتت جدواها بالنسبة للمشاركين فيها، وما تضمنته من مناقشات مثمرة ومثيرة. وأشار السيد لويس إلى أن ورشة العمل الإقليمية بشأن أطر الأمن السيبراني وحماية البنية التحتية الحرجة للمعلومات، والتي دامت ثلاثة أيام، تعقبها مباشرة ورشة العمل بشأن الأدلة القضائية في الأمن السيبراني يوم الخميس 21 فبراير 2008. وللاطلاع على المزيد من المعلومات عن ورشة العمل بشأن الأدلة القضائية في الأمن السيبراني، بما في ذلك وصلات النفاذ إلى العروض التي قُدِّمت أثناء الورشة، يرجى زيارة الموقع التالي:
www.itu.int/ITU-D/cyb/events/2008/doha/presentations.html#forensics[34].

71. وشكر السيد إبراهيم الحداد، رئيس المكتب الإقليمي للدول العربية في الاتحاد، كل من ساهم بصورة مباشرة أو غير مباشرة في نجاح المنتدى الإقليمي بشأن الأمن السيبراني. وتوجَّه بالشكر الخاص إلى مضيفي الورشة على الجهود الفائقة المبذولة في جعل ورشة العمل الإقليمية هذه بشأن الأمن السيبراني حدثاً على درجة عالية من النجاح. كما توجَّه السيد الحداد بالشكر إلى المتحدثين في ورشة العمل لأنهم اقتطعوا جزءاً من برنامج أعمالهم الحافل لتقاسم تجاربهم ودرايتهم التقنية مع المشاركين في الورشة. وأخيراً، شكر السيد الحداد المترجمين الفوريين على خدماتهم الممتازة في توفير الترجمة الشفوية بين اللغتين والإنكليزية والعربية طوال أيام الورشة الثلاثة كما شكر المندوبين على اهتمامهم ومشاركتهم الفعَّالة ومساهماتهم. وقال إن الاتحاد الدولي للاتصالات، من منطلق خبرته الطويلة في أنشطة تقييس الاتصالات وتنميتها، يأمل في أن يستمر في توفير منتدى يمكن فيه مناقشة مختلف وجهات النظر من الحكومات ومن القطاع الخاص وغيرهما من أصحاب المصلحة فيما يتعلق بالأمن السيبراني وحماية البنية التحتية الحرجة للمعلومات وذلك من خلال مختلف الأنشطة والمبادرات لدى الاتحاد.

تقرير الاجتماع هذا[35] مفتوح حالياً للتعليق عليه لفترة 30 يوماً من استلامه ونشره على موقع ورشة العمل على شبكة الويب. وعنوان البريد الإلكتروني لإرسال التعليقات على مشروع التقرير هذا، ومن أجل التعليقات على برنامج عمل الاتحاد في الأمن السيبراني لمساعدة البلدان النامية (2007-2009)[36]، هو كما يلي **cybmail(at)itu.int**[37].

لأغراض تقاسم المعلومات، تضاف أسماء جميع المشاركين في الاجتماع إلى الموقع **cybersecurity-arab-states(at)itu.int**[38] بالنسبة للمسائل المتعلقة بأنشطة قطاع تنمية الاتصالات في مجال الأمن السيبراني. ويرجى ممن لم يشارك مباشرة في ورشة العمل، أو ممن لا يكون اسمه مدرجاً في قائمة البريد ولكنه مهتم بالمشاركة في هذه المناقشات من خلال قوائم البريد والمنتديات ذات الصلة، إرسال بريد إلكتروني إلى العنوان **cybmail(at)itu.int**.

34 http://www.itu.int/ITU-D/cyb/events/2008/doha/presentations.html#forensics.

35 http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/doha-cybersecurity-forum-report-feb-08.pdf.

36 http://www.itu.int/ITU-D/cyb/cybersecurity/index.html#workprogramme.

37 يرجى إرسال أي تعليقات على تقرير ورشة العمل إلى العنوان: cybmail@itu.int.

38 قائمة بريد الأمن السيبراني الإقليمي للاتحاد: cybersecurity-arab-states@itu.int. لإدراج الاسم في قائمة البريد الإلكتروني يرجى إرسال بريد إلكتروني إلى العنوان: cybmail@itu.int.

الملحـــق 1

حصيلة ما اتفق عليه المنتدى الإقليمي للاتحاد الدولي للاتصالات بشأن الأمن السيبراني

18-20 فبراير 2008

الدوحة، قطر

عُقد المنتدى الإقليمي للاتحاد الدولي للاتصالات بشأن الأمن السيبراني[39] في الفترة 18-20 فبراير 2008 في الدوحة في قطر بالتعاون مع المجلس الأعلى للاتصالات وتكنولوجيا المعلومات في قطر (ictQATAR) وفريق الاستجابة لطوارئ الحاسوب في قطر (Q-CERT). وشارك في المنتدى أكثر من 80 ممثلاً من 18 بلداً في المنطقة العربية وخبراء من خارج المنطقة (مثال ذلك من ماليزيا والولايات المتحدة الأمريكية) وممثلون من منظمات إقليمية رئيسية منها جامعة الدول العربية ومجلس التعاون لدول الخليج واللجنة الاقتصادية والاجتماعية لغرب آسيا التابعة للأمم المتحدة.

وأثناء اللقاء الذي دام ثلاثة أيام، بُحث الأمن السيبراني وحماية البنية التحتية الحرجة للمعلومات في سياق مشروع "إطار الأمن السيبراني للاتحاد الدولي للاتصالات"[40] الذي يجري تطويره في إطار المسألة 22/1 لدى لجنة الدراسات 1 في قطاع تنمية الاتصالات في الاتحاد الدولي للاتصالات. ونوقش عدد من العروض المثيرة للاهتمام بشأن التجارب الوطنية والمبادرات الإقليمية (منها مثلاً جامعة الدول العربية ومجلس التعاون لدول الخليج واللجنة الاقتصادية والاجتماعية لغرب آسيا) تتناول كل عنصر من عناصر الإطار المذكور، ومنها:

- وضع استراتيجية وطنية للأمن السيبراني؛
- إقامة تعاون وطني بين الحكومة ودوائر الصناعة؛
- ردع الجريمة السيبرانية؛
- استحداث مقدرة للتحكم في الحوادث وطنياً؛
- النهوض بثقافة وطنية للأمن السيبراني.

ومن المسلّم به أن كل عنصر من هذه العناصر يشكّل جزءاً من نهج وطني شامل لتحقيق الأمن السيبراني.

وقد نظر المنتدى أيضاً في مصدر آخر متصل بالموضوع، وهو مشروع "مجموعة أدوات الاتحاد الدولي للاتصالات للتقييم الذاتي للأمن السيبراني الوطني/حماية البنية التحتية الحرجة للمعلومات"[41] ومجموعة الأدوات التي وضعها الاتحاد مصمَّمة لمساعدة الحكومات الوطنية على استعراض وفهم النهج الوطني القائم لديها ووضع خط أساس من حيث "أفضل الممارسات" الراهنة وتحديد المواطن التي تستحق الاهتمام وترتيب أولويات الجهود الوطنية لتناول مسألة الأمن السيبراني.

ونوقش دور الحكومة في قيادة الجهود الوطنية لتحقيق الأمن السيبراني وكذلك التحديات التي تواجهها جميع الحكومات من أجل اتخاذ الإجراءات الضرورية. ودارت مناقشات بشأن الحاجة إلى إذكاء الوعي بين جميع المشاركين والحاجة إلى تفصيل

---

39 كان عنوان اللقاء "ورشة عمل بشأن أطر الأمن السيبراني وحماية البنية التحتية الحرجة للمعلومات (CIIP)" الموصوف في العنوان http://www.itu.int/ITU-D/cyb/events/2008/doha/.

40 http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-draft-cybersecurity-framework.pdf.

41 http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html.

المناقشات والحجج لتلائم مختلف الجماهير المستهدفة سواء كانت مناقشات سياسية موجهة لكبار القادة أو مناقشات اقتصادية لدوائر الأعمال أو مناقشات أمن شخصي موجهة للأفراد من المستعملين.

ودارت مناقشات حول أهمية إشراك القطاع الخاص وغيره من المجموعات في وضع السياسات والقوانين في هذا المجال وفي تنفيذ وتشغيل استراتيجية وطنية للأمن السيبراني.

ودارت مناقشات حول أهمية استعراض التشريعات الوطنية للجريمة السيبرانية للتأكد من أنها تتناول المخاطر في الفضاء السيبراني. وأحيط المشاركون علماً بالاتفاقية الخاصة بالجريمة السيبرانية (بودابست، 2001) والتي توفر أساساً تطوراً دولياً لفحص قوانين الجريمة السيبرانية الوطنية القائمة ولتحديد ما هي الأحكام الجديدة الجوهرية والإجرائية وأحكام المساعدة المتبادلة اللازمة في القوانين الوطنية لمكافحة الجريمة السيبرانية.

ودارت مناقشات حول أهمية تحديد جهة تنسيق وطنية لإدارة الحوادث السيبرانية مهمتها الترصد والتحذير والتحقيق والاستجابة والتغلب. ومن شأن جهة اتصال وطنية من هذا القبيل أن تعمل على الحفاظ على التعاون داخل الحكومة وبين الحكومة والقطاع الخاص ومع الشركاء الدوليين.

ودارت مناقشات حول ضرورة النهوض بثقافة وطنية للأمن السيبراني للتأكد من أن جميع المستعملين والمالكين والمشغِّلين لأنظمة المعلومات والشبكات على علم بمسؤولياتهم فيما يتعلق بالأمن ولديهم الأدوات اللازمة لاتخاذ الإجراءات الملائمة لدورهم.

إعلان الدوحة بشأن الأمن السيبراني – المنتدى الإقليمي للاتحاد الدولي للاتصالات بشأن الأمن السيبراني[42]

في ختام هذا اللقاء، اتفق المشاركون على ما يلي:

- الاعتراف بأن تحسين الأمن السيبراني مشكلة عالمية وأن كل بلد يجب عليه أن يتخذ الإجراءات اللازمة لكي ينضم إلى الجهود الدولية لتحسين الأمن السيبراني وأن يدعم هذه الجهود.
- الاعتراف بالمبادرات والإجراءات والنُهج التي أثبتت جدواها في عدد من البلدان وفي مناطق أخرى وبالجهود التي يبذلها الاتحاد الدولي للاتصالات وغيره من المنظمات من أجل إعداد مجموعة من "أفضل الممارسات" ووضع أدوات من شأنها تدعيم الجهود الوطنية داخل المنطقة العربية.
- الاعتراف بأن إطار الاتحاد للأمن السيبراني/حماية البنية التحتية الحرجة للمعلومات يوفر دليلاً مفيداً لإذكاء الوعي وللمبادرة باتخاذ الإجراءات الوطنية و/أو مراجعتها من حيث إنها تساعد في ضمان الاتساق والمواءمة في الإجراءات بين الدول.
- التوصية باستكمال إطار الاتحاد للأمن السيبراني/حماية البنية التحتية الحرجة للمعلومات والموارد المتصلة به ومجموعات الأدوات وذلك في أقرب وقت ممكن وتوفيرها بجميع لغات العمل في الاتحاد، والاهتمام بصفة خاصة باللغة العربية لدعم الجهود في المنطقة.
- تشجيع كل بلد في المنطقة على استخدام الإطار ومجموعة أدوات الاتحاد للتقييم الذاتي للأمن السيبراني الوطني/ حماية البنى التحتية الحرجة للمعلومات المتصلة به كوسيلة لتطوير مؤسساتها وسياساتها وعلاقاتها من أجل الأمن السيبراني وحماية البنى التحتية الحرجة للمعلومات.

42 إعلان الدوحة بشأن الأمن السيبراني متاح أيضاً على الخط في العنوان: http://www.itu.int/ITU-D/cyb/events/2008/doha/docs/doha-regional-cybersecurity-forum-output-20-feb-08.pdf.

- الاعتراف بأن بعض البلدان في المنطقة قد تحتاج إلى الدعم والمساعدة في تنفيذ الإطار وفي استعمال مجموعة أدوات التقييم الذاتي للأمن السيبراني الوطني/حماية البنية التحتية الحرجة للمعلومات ومطالبة قطاع تنمية الاتصالات بأن ينظر في أساليب توفير هذا الدعم.
- الاتفاق على أن يقوم كل بلد في المنطقة، إن لم يكن قد فعل ذلك، بتطوير مقدرة على إدارة الحوادث (فريق للاستجابة لحوادث أمن الحاسوب (CSIRT)/فريق الاستجابة لطوارئ الحاسوب (CERT)) مشفوعة بالمسؤولية الوطنية واستعمال الأمثلة الراهنة وأفضل الممارسات للأفرقة CSIRT/CERT في المنطقة لدى تطوير المقدرات الوطنية.
- الاتفاق على أن واحداً من المكونات الهامة لتطوير إطار وطني هو الانضمام إلى الجهود الإقليمية والدولية للنهوض بثقافة الأمن السيبراني.
- التأكيد على أهمية تطوير مبادرات وموارد تعاون إقليمية تكون بمثابة أمثلة لأفضل الممارسات وفرص التدريب والتعليم ووضع النماذج لبناء القدرات التي يمكن تكييفها تبعاً لاحتياجات كل بلد في الإقليم.
- مطالبة قطاع تنمية الاتصالات بالشراكة مع المنظمات الإقليمية والإدارات الوطنية باتخاذ المبادرات الضرورية لمتابعة نتائج الاجتماع ولتوفير تحديثات بشأن التقدم والتعاون الإقليمي. وينبغي، في مبادرات المتابعة هذه، تشجيع المشاركة من جانب الأطراف الإضافية المحددة في الإطار (مثال ذلك جميع الوزارات المعنية ودوائر الأعمال والمنظمات الأخرى).
- التعبير عن التقدير للمجلس الأعلى للاتصالات وتكنولوجيا المعلومات في قطر (ictQATAR) وفريق الاستجابة لطوارئ الحاسوب في قطر (Q-CERT) والاتحاد الدولي للاتصالات، على ما قدَّمته من دعم وتسهيل للاجتماع.