التقرير النهائي

قطاع تنمية الاتصالات
لجنة الدراسات 2

المسألة 3/2

تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني

فترة الدراسة السادسة
2017-2014

للاتصال بنا

الموقع الإلكتروني: www.itu.int/ITU-D/study-groups

المكتبة الإلكترونية للاتحاد: www.itu.int/pub/D-STG/

البريد الإلكتروني: devsg@itu.int

الهاتف: +41 22 730 5999

المسألة 3/2: تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني

التقرير النهائي

مقدمة

توفر **لجان دراسات قطاع تنمية الاتصالات** (**ITU-D**) منصة محايدة تقوم على المساهمات المقدمة ويجتمع فيها الخبراء من الحكومات والصناعة والهيئات الأكاديمية لإنتاج أدوات عملية ومبادئ توجيهية وموارد مفيدة لمعالجة قضايا التنمية. ومن خلال أعمال لجان دراسات قطاع تنمية الاتصالات، يقوم أعضاء القطاع بدراسة وتحليل مسائل موجهة نحو مهمة محددة في مجال الاتصالات/تكنولوجيا المعلومات والاتصالات بهدف التعجيل بإحراز تقدم بشأن الأولويات الإنمائية الوطنية.

تتيح لجان دراسات قطاع تنمية الاتصالات فرصة لجميع أعضاء قطاع تنمية الاتصالات لتقاسم الخبرات وطرح الأفكار وتبادل الآراء والتوصل إلى توافق في الآراء بشأن الاستراتيجيات الملائمة لتناول أولويات الاتصالات/تكنولوجيا المعلومات والاتصالات. وتتولّى لجان دراسات قطاع تنمية الاتصالات مسؤولية إعداد التقارير والمبادئ التوجيهية والتوصيات استناداً إلى المدخلات أو المساهمات المقدمة من الأعضاء. ويتم تجميع المعلومات من خلال الاستقصاءات والمساهمات ودراسات الحالة ثم تتاح كي يحصل عليها الأعضاء بسهولة باستخدام أدوات إدارة المحتوى والنشر الشبكي. ويرتبط عمل اللجان بمختلف برامج ومبادرات قطاع تنمية الاتصالات من أجل توفير أوجه التآزر التي يستفيد منها الأعضاء من حيث الموارد والخبرات المتخصصة. ويلزم التعاون مع الأفرقة والمنظمات الأخرى التي تضطلع بأعمال تتعلق بالمواضيع ذات الصلة.

وتتحدد المواضيع التي تدرسها لجان دراسات قطاع تنمية الاتصالات كل أربع سنوات في المؤتمرات العالمية لتنمية الاتصالات (WTDC) التي تضع برامج العمل والمبادئ التوجيهية من أجل تحديد مسائل تنمية الاتصالات/تكنولوجيا المعلومات والاتصالات وأولوياتها في السنوات الأربع التالية.

ويتمثل نطاق عمل **لجنة الدراسات 1 لقطاع تنمية الاتصالات** في دراسة "**البيئة التمكينية لتنمية الاتصالات/تكنولوجيا المعلومات والاتصالات**"، أما **لجنة الدراسات 2 لقطاع تنمية الاتصالات** فيتمثل نطاق عملها في دراسة "**تطبيقات تكنولوجيا المعلومات والاتصالات والأمن السيبراني والاتصالات في حالات الطوارئ والتكيف مع تغير المناخ**".

وتولى إدارة **لجنة الدراسات 2 لقطاع تنمية الاتصالات** في فترة الدراسة 2014-2017 رئيس اللجنة السيد أحمد رضا شرفات (جمهورية إيران الإسلامية) ونوابه الذين يمثلون المناطق الست: السيدة أميناتا كابا-كامارا (جمهورية غينيا)، السيد كريستوفر كيمي (جمهورية كينيا)، والسيدة سيلينا ديلغادو (نيكاراغوا)، والسيد ناصر المرزوقي (الإمارات العربية المتحدة)، والسيد نادر أحمد جيلاني (جمهورية السودان)، والسيدة كي وانغ (جمهورية الصين الشعبية)، والسيد أناندا راج كانال (جمهورية نيبال)، والسيد يوجيني بوندارينكو (الاتحاد الروسي)، والسيد هينادز أسيبوفيتش (جمهورية بيلاروس)، والسيد بيتكو كانتشيف (جمهورية بلغاريا).

التقارير النهائية

وأُعد التقرير النهائي استجابةً **للمسألة 3/2**: **"تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني"** تحت ريادة المقرِّرَين المعنيينَ بالمسألة: السيدة روزالين بشير فقير البلوشي (هيئة تنظيم الاتصالات (TRA)، عُمان)، والسيد إليوت لير (الولايات المتحدة الأمريكية)، مع سبعة نواب معينين كنواب للمقرِّرَين: السيد دمنام كانلانفي باغوليب (توغو)، والسيد كريستوفر غانيزاني باندا (ملاوي)، والسيد ألبرت كامغا (الكاميرون)، والسيد ميهو ناغانوما (اليابان)، والسيد جان-دافيد رودني (هايتي)، والسيدة جابين س. فاهورا (الولايات المتحدة الأمريكية)، والسيد جيسوك يون (جمهورية كوريا). وقد ساعدهم أيضاً مسؤولو الاتصال لقطاع تنمية الاتصالات وأمانة لجان دراسات القطاع.

ISBN

978-92-61-22996-2 (النسخة الورقية)

978-92-61-23006-7 (النسخة الإلكترونية)

978-92-61-23016-6 (نسخة EPUB)

978-92-61-23026-5 (نسخة Mobi)

شارك في إعداد هذا التقرير العديد من الخبراء من إدارات وشركات مختلفة. ولا ينطوي ذكر شركات أو منتجات معينة على أي تأييد أو توصية من جانب الاتحاد الدولي الاتصالات.

يرجى مراعاة الجوانب البيئية قبل طباعة هذا التقرير.

جدول المحتويات

مقدمة ii

التقارير النهائية iii

ملخص تنفيذي ix
'1' ملخص تنفيذي ix
'2' مقدمة ix

1 الفصل 1 - استبيان بشأن زيادة الوعي بالأمن السيبراني 1
1.1 أساليب جمع المعلومات 1
2.1 تحليل البيانات المستمدة من حملات التوعية 2

2 الفصل 2 - وضع الرسائل الاقتحامية والبرمجيات الضارة وسبل التخفيف منها والجوانب التنظيمية 8
1.2 مصادر الرسائل الاقتحامية 10
2.2 آثار الرسائل الاقتحامية على الشبكة 10
3.2 مخاطر التصيد الاحتيالي وسبل التخفيف منه 11
4.2 أثر السياسات على الرسائل الاقتحامية 11

3 الفصل 3 - تحسين وضع الأمن السيبراني على الصعيد الوطني: تعزيز الوعي وتحسين الموارد البشرية 13
1.3 حملات التوعية 13
1.1.3 أفضل الممارسات لبرنامج خاص بالاتصالات 13
2.1.3 نموذج لخطة الاتصالات 15
3.1.3 استراتيجيات الحملات 16
4.1.3 مقياس النجاح ومعاييره 18
2.3 المقاييس الإضافية لبناء القدرات 18
1.2.3 الأنشطة المنفّذة في اليابان 18
2.2.3 الأنشطة المنفذة في جمهورية كوريا 19
3.2.3 الأنشطة المنفذة في منطقة كومنولث الدول المستقلة 20
4.2.3 الأنشطة المنفذة في النرويج 21
3.3 الشراكات بين القطاعين العام والخاص 21

4 الفصل 4 - حماية الأطفال على الخط (COP) 23
1.4 نتائج الاستقصاء المتعلق بحماية الأطفال على الخط 23
2.4 الاستراتيجيات والحلول التقنية لحماية الأطفال على الخط 28
1.2.4 التوعية بمسألة حماية الأطفال على الخط، والأنشطة المرتبطة بذلك 30
2.2.4 استراتيجيات حماية الأطفال على الخط 31

5 الفصل 5 - نتائج ورش العمل المتعلقة بالأمن السيبراني 32

1.5 ورشة العمل الأولى المتعلقة بالأمن السيبراني (8 سبتمبر 2015) 32
2.5 ورشة العمل الثانية المتعلقة بالأمن السيبراني (19-20 أبريل 2016) 33
3.5 ورشة العمل الثالثة حول الأمن السيبراني (26 يناير 2017) 36

6 الفصل 6 - الفرص والتحديات في مجال الأمن السيبراني 38
1.6 إدمان الإنترنت 38
2.6 أمن المعاملات الإلكترونية 42
3.6 الشراكات في مجال الأمن السيبراني 46

7 الفصل 7 - التجارب الوطنية استناداً إلى إطار معايير موحدة للأمن 48

8 الفصل 8 - الاستنتاجات والتوصيات لفترة الدراسة المقبلة 50

Abbreviations and acronyms 51

Annexes 54

Annex 1: The Global Cybersecurity Index 2017 54

Annex 2: Compendium on cybersecurity country case studies 66

Annex 3: Cybersecurity activities being conducted by organizations, private sector, and civil society 134

Annex 4: Contributions mapping 151

Annex 5: Survey questions 163

Annex 6: Information on ACTIVE 166

قائمة بالجداول والأشكال

الجداول

الجدول 1: عدد المشاركين في التعليم الوقائي 39
الجدول 2: عدد الخدمات الاستشارية بحسب نوعها 40
Table 1A: Most committed countries, GCI (normalized score) 55
Table 2A: Number of participants of preventive education 104
Table 3A: Number of counselling service by type 105
Table 4A: Different types of services options to be provided to Government and commercial entities 109
Table 5A: Different types of services options to be provided to individuals 109
Table 6A: Customized template for national cybersecurity measures 111

الأشكال

الشكل 1: الردود على الاستبيان الخاص بالتوعية بالأمن السيبراني بحسب كل منطقة 2
الشكل 2: أهمية إذكاء الوعي بالأمن السيبراني 2
الشكل 3: حملات لتوعية الجمهور بمسألة الأمن السيبراني 3
الشكل 4: أهمية التوعية بالأمن السيبراني في المنظمات/المجتمع المدني 3
الشكل 5: الفئات العمرية المستهدفة بحملات التوعية بالأمن السيبراني 4
الشكل 6: الفئات المستهدفة بحملات التوعية بالأمن السيبراني 4
الشكل 7: الفئات الأكثر استهدافاً بحملات التوعية بالأمن السيبراني 5
الشكل 8: قضايا الأمن السيبراني التي تعالج في حملات التوعية 6
الشكل 9: أهمية كل قضية من قضايا الأمن السيبراني التي تعالج في حملات التوعية 6
الشكل 10: إدراك الجمهور لمنافع البرمجيات/الأعتدة أو الحلول القائمة على الخدمات 7
الشكل 11: ما أتيح للجمهور من برمجيات/أعتدة أو حلول قائمة على الخدمات 7
الشكل 12: الحلقة المفرغة للرسائل الاقتحامية والأمن السيبراني 8
الشكل 13: الخروج من الحلقة المفرغة 10
الشكل 14: لمحة عن أنشطة مشروع "نشط" 19
الشكل 15: هل من وكالة/كيان لحماية الأطفال على الخط؟ 24
الشكل 16: هل من آلية عامة قائمة لغرض الإبلاغ عن القضايا المرتبطة بحماية الأطفال على الخط؟ 24
الشكل 17: هل من آليات وقدرات تقنية تم نشرها من أجل المساعدة في حماية الأطفال على الخط؟ 25
الشكل 18: هل قامت الحكومة أو منظمة غير حكومية بأي نشاط من أجل تقديم الدعم والمعرفة لأصحاب المصلحة (الأهل وقادة المجتمع والمعلمون وما إلى ذلك) بشأن كيفية حماية الأطفال على الخط؟ 25
الشكل 19: إعداد وتنفيذ حملات عامة للتوعية بالأمن السيبراني مقابل وجود وكالة/كيان لحماية الأطفال على الخط 26
الشكل 20: الحملات العامة الموجهة للأطفال للتوعية بمسألة حماية الأطفال على الخط 27
الشكل 21: الحملات العامة للتوعية بمسألة حماية الأطفال على الخط 27
الشكل 22: الحملات العامة الموجهة للأطفال والكبار من أجل التوعية بمسألة حماية الأطفال على الخط 30

Figure 1A: GCI heat map 54
Figure 2A: GCA 56
Figure 3A: GCA linkages 57
Figure 4A: Global cybersecurity agenda 59
Figure 5A: GCI approach 59
Figure 6A: Oman PKI 110
Figure 7A: General framework of NCMP major processes that collectively comprise a NCMP 115
Figure 8A: General scope for national cybersecurity measures 116
Figure 9A: Prevention of malware infection 166
Figure 10A: Damage prevention of malware infection 167
Figure 11A: Removal of malware 168

ملخص تنفيذي

'1' ملخص تنفيذي

يغطي هذا التقرير جوانب عديدة تتعلق باختصاصات المسألة 3/2 "تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني" خلال فترة دراسة تستمر لثلاث سنوات، وتنتهي في أبريل 2017. ونبدأ بتحليل لاستقصاء عن الوعي بالأمن السيبراني أجراه مكتب تنمية الاتصالات (BDT) بالاتحاد. ويُظهر الاستقصاء أنه يتعين على عدد من البلدان تحسين الوعي بالأمن السيبراني، في حين لا ينطبق الأمر على البعض الآخر. إلا أن من يتعين عليهم القيام بذلك عادةً ما لا يستهدفون فئات رئيسية في المجتمع. وغالباً ما يولى اهتمام كبير لحماية الأطفال على الخط على سبيل الأولوية. وينظر هذا التقرير في الرسائل الاقتحامية وأسبابها ووسائل التصدي لها. وعلى الرغم من أن استهلاك النطاق العريض في البريد الإلكتروني منخفض بوجه عام، فإن أثره على خفض قيمة الاتصالات لا يزال يمثل شاغلاً. وبعد ذلك، يقدّم التقرير عينة من أنشطة التوعية التي نفذتها الحكومات لتحسين موقفها المجتمعي بوجهٍ عام إزاء الأمن السيبراني.

وفي حين ركّزت فترة الدراسة السابقة (2010-2014) على إتاحة الأعمال المختلفة المتعلقة بالدورات عن طريق مكتب تنمية الاتصالات، ركزت فترة الدراسة الحالية (2014-2017) أكثر على ورش العمل التي تضم طائفة واسعة من الأطراف الفاعلة وإتاحة مضمونها للبلدان النامية. ويحتوي هذا التقرير على ملخص بورش العمل تلك، مع الإشارة إلى مضمونها.

كما يحتوي هذا التقرير، في شكل ملحق، على معلومات تتعلق بالمؤشر العالمي للأمن السيبراني (GCI) الذي طبقه مكتب تنمية الاتصالات في الاتحاد (BDT) لعدة سنوات.

ونختتم بتقديم بعض الأفكار النهائية وبعض التوصيات لإجراء مزيد من الدراسة.

'2' مقدمة

يجري في إطار المسألة 3/2 لقطاع تنمية الاتصالات إعداد تقارير عن أفضل الممارسات فيما يتعلق بمختلف جوانب الأمن السيبراني. وهذا هو التقرير النهائي للفريق المعني بالمسألة 3/2 التابع للجنة الدراسات 2 لقطاع تنمية الاتصالات بشأن أنشطته على مدى دورة الدراسات الأخيرة التي امتدت ثلاث سنوات شملت الفترة من 2014 إلى 2017. وكان المؤتمر العالمي لتنمية الاتصالات (WTDC) قد وضع في اجتماعه الذي عُقد عام 2014 في دبي بالإمارات العربية المتحدة برنامج العمل المتعلق بالمسألة 3/2. وعالج الفريق المعني بالمسألة 3/2 خلال السنوات الثلاث الأخيرة غالبية البنود التي تضمنها برنامج العمل هذا.

ويتألف التقرير النهائي هذا من عددٍ من تقارير أفضل الممارسات بشأن مختلف جوانب الأمن السيبراني.

وينظر **الفصل 1** في الاستقصاء الخاص بالتوعية بالأمن السيبراني.

ويناقش **الفصل 2** حالة البرمجيات الضارة والرسائل الاقتحامية، وسبل تخفيفها، والجوانب التنظيمية.

ويناقش **الفصل 3** الخطوات التي اتُّخذت فيما يخص التجارب القطرية على صعيد شن حملات التوعية وإعداد الاستراتيجيات وقياس الأمن السيبراني.

ويناقش **الفصل 4** الاستقصاء الذي أجري بشأن حماية الأطفال على الخط، والقضايا المطروحة في هذا المجال.

ويناقش **الفصل 5** نواتج ورش العمل المتعلقة بالأمن السيبراني والتي جرت خلال فترة دراسة لجنة الدراسات.

ويتضمن **الفصل 6** لمحة عن الأعمال التي قدمتها مختلف المنظمات إلى لجنة الدراسات.

ويناقش **الفصل 7** التجارب الوطنية بالاستناد إلى معايير موحدة.

وأخيراً، يختتم **الفصل 8** هذا التقرير بالإشارة إلى مجالات الاستكشاف المستقبلية التي ينبغي النظر فيها.

وفي بداية هذا التقرير، يجدر بالذكر أن لجنة الدراسات هذه استعرضت جميع الوثائق المنتَجة في سياق مؤشر الأمن السيبراني العالمي لعام 2017 وقامت بالتعليق عليها. وقد وُضع مؤشر عام 2017 هذا استناداً إلى تقييم لأكثر من 134 رداً وارداً من 193 دولة عضواً أجرت استقصاءً على الإنترنت عن طريق جهة الاتصال الخاصة بها المعنية بالمؤشر (التي تحددها الدولة العضو بناءً على طلب الاتحاد). وقد تم تسيير الاستقصاء المتعلق بالتوعية بالأمن السيبراني والاستقصاء المتعلق بحماية الأطفال على الخط، المرتبطين بالمسألة التي تتناولها لجنة الدراسات، من خلال إدماجهما في الاستقصاء المتعلق بمؤشر الأمن السيبراني العالمي بما مكّن من الاستفادة من ازدياد عدد الردود (من 51 رداً خلال فترة الدراسة الأخيرة إلى ما يزيد عن 129 رداً في هذه الفترة).

وقد استُعرض الاستبيان[1] الخاص بمؤشر الأمن السيبراني العالمي لعام 2017 وغيره من الوثائق المهمة (بما في ذلك النموذج المرجعي) وأُدرجت جميعها في **الملحقات**. ويمكن الاطلاع على خلاصة نتائج مؤشر عام 2017 في **الملحق 1**.

وتطرقت المسألة قيد الدراسة إلى جميع الجوانب المتعلقة باختصاصاتنا، باستثناء جانب واحد هو:

و) دراسة الاحتياجات المحددة للأشخاص ذوي الإعاقة بالتنسيق مع المسائل الأخرى ذات الصلة.

وقد تضرر هذا المجال، رغم أهميته، من آثار تقصير فترة الدراسة وقلة المساهمات مجتمعة. ويلاحظ أن 69 في المائة من الدول الأعضاء المشاركة في استبيان الوعي بالأمن السيبراني لم تدرج الأشخاص ذوي الإعاقة بين فئاتها المستهدفة. ويوضح ذلك أنه يلزم إجراء المزيد من العمل في هذا المجال (انظر **القسم 2.1** للاطلاع على مزيد من التفاصيل).

[1] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2017.aspx.

1 الفصل 1 - استبيان بشأن زيادة الوعي بالأمن السيبراني

يتعلق هذا القسم بالبند (د) من الاختصاصات المتصلة بالمسألة 3/2، الذي يدعو إلى جملة *أمور* منها:

د) مواصلة تحليل نتائج الدراسة الاستقصائية حول الوعي بشأن الأمن السيبراني التي أجريت في فترة الدراسة الماضية، وإصدار دراسة استقصائية محدثة لقياس التقدم المحرز مع مرور الوقت.

لن يُطوَّر نظام الأمن السيبراني بصورة تامة ما لم تولَ أقصى درجة من الاهتمام لزيادة وعي الجمهور والمستخدمين. فلا يمكن لأي إطار يرمي إلى تحقيق الأمن السيبراني أن يدوم إذا لم تكن التوعية أحد عناصره الأساسية. وهذا ما يؤكده إدراك المهتمين بالفضاء السيبراني أو المعنيين به أن تحقيق الأمن السيبراني يتوقف دائماً على العوامل الرئيسية التالية: '1' سن التشريعات اللازمة لحماية الأمن السيبراني؛ و'2' تحقيق التنسيق والتعاون بين الجهات المعنية (القطاع الخاص والقطاع العام)؛ و'3' توافر الأدوات التقنية اللازمة لتحقيق الأمن؛ و'4' التنسيق الدولي؛ و'5' قياس الكفاءة بصورة دورية؛ و'6' نشر الوعي وإذكاؤه.

ونظراً إلى أهمية إذكاء الوعي لتحقيق الأمن السيبراني، أعد هذا الاستبيان لقياس مدى الحماس في نشر الوعي في هذا المجال، وتحديد الفئات المستهدفة سواء الوكالات الحكومية أو الجهات المعنية مثل الشركات والمؤسسات الخاصة أو فئات أخرى مثل الأشخاص ذوي الإعاقة والأطفال، وتحديد أبرز المخاطر السيبرانية التي تواجهها البلدان.

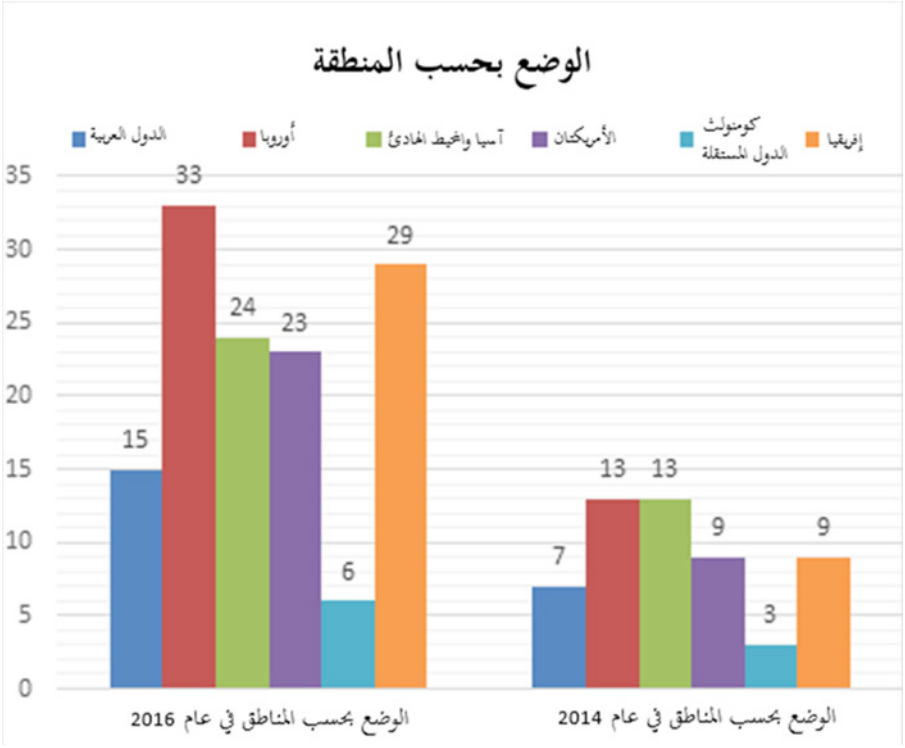
1.1 أساليب جمع المعلومات

وافقت المسألة 3/2 التابعة للجنة الدراسات 2 لقطاع تنمية الاتصالات في اجتماعها الثاني في 2015 على دمج الاستبيان الخاص بالتوعية وبحماية الأطفال على الخط (COP) مع استبيان مؤشر الأمن السيبراني العالمي[1]، بهدف تحقيق الأهداف المماثلة بكفاءة، وتفادي الازدواجية في الأعمال والجهود، وضمان مشاركة أكبر من الدول الأعضاء في الاستبيان عن طريق مساهماتها.

وفي 11 ديسمبر 2015، أُرسل الاستبيان إلى جميع الدول الأعضاء في الاتحاد البالغ عددها 193 دولة لكي تجيب عنه. فأجاب 129 بلداً من أصل 193 بلداً عن الأسئلة المتعلقة بزيادة الوعي بالأمن السيبراني (ما يعادل 63 في المائة تقريباً من الدول الأعضاء في الاتحاد)، في حين أجاب 131 بلداً عن الأسئلة المتعلقة بحماية الأطفال على الخط (ما يعادل نحو 68 في المائة من الدول الأعضاء في الاتحاد). ثم قام الفريق المكلف بتنسيق الجهود المتعلقة باستبيان مؤشر الأمن السيبراني العالمي بإحالة هذه البيانات إلى المسألة 3/2، التي قامت بعد ذلك باستعراض وتحليل هذه البيانات وبإدراج النتائج النهائية في التقرير النهائي الحالي.

[1] إن مؤشر الأمن السيبراني العالمي (GCI) هو ثمرة شراكة تعاونية بين مؤسسة خاصة ومنظمة دولية، هدفت إلى وضع مسألة الأمن السيبراني في صدارة برامج العمل الوطنية. فالمؤشر عبارة عن مشروع مشترك أجري بين مؤسسة ABI Research والاتحاد الدولي للاتصالات، وهو يوفّر معلومات عما تقوم به الدول السيادية في مجال الأمن السيبراني.

الشكل 1: الردود على الاستبيان الخاص بالتوعية بالأمن السيبراني بحسب كل منطقة

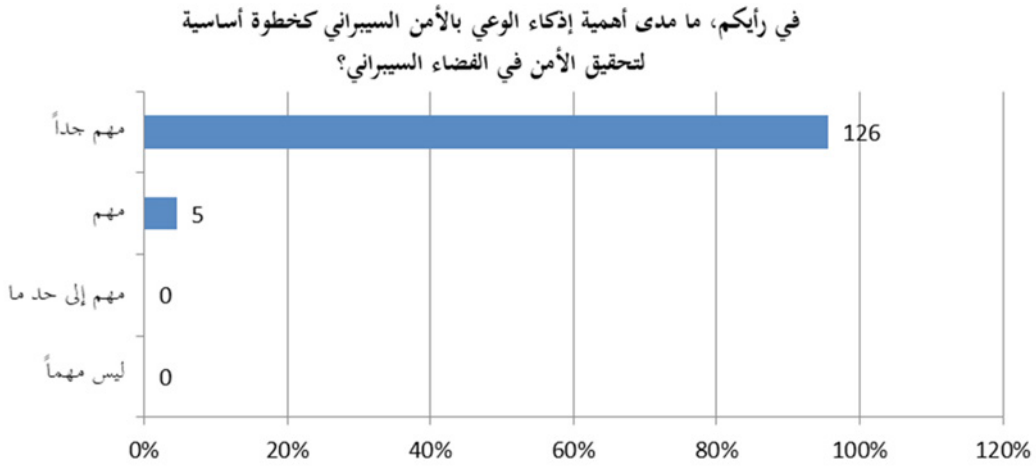


2.1 تحليل البيانات المستمدة من حملات التوعية

إن الهدف من الأسئلة المتعلقة بالمخاطر السيبرانية هو تحديد أهمية زيادة الوعي بالمخاطر السيبرانية لتحقيق الأمن في الفضاء السيبراني.

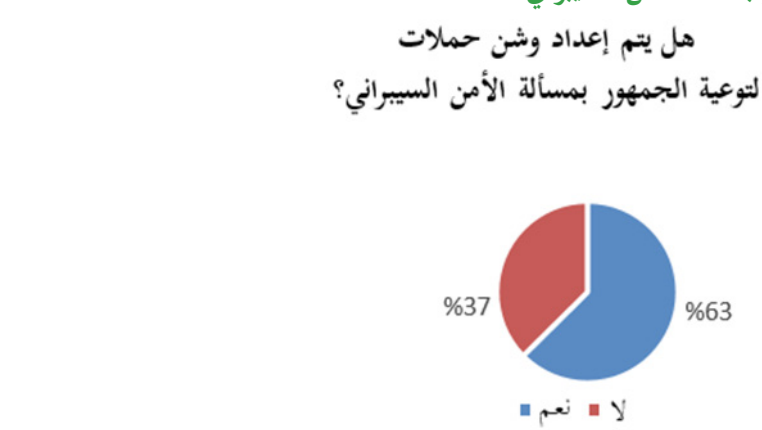
واعتبر 95,42 في المائة من المجيبين عن الاستبيان أن هذا الأمر "مهم جداً" في حين اعتبر 4,58 في المائة منهم أن الأمر "مهم". وبالمقارنة مع نتائج استبيان مماثل أجري خلال فترة الدراسة السابقة (2010-2014)، فإن نسبة المجيبين الذين أكدوا أن التوعية بالأمن السيبراني "مهم جداً" ازداد من 79 في المائة على نحو ما أشير إليه في فترة الدراسة 2010-2014.

الشكل 2: أهمية إذكاء الوعي بالأمن السيبراني



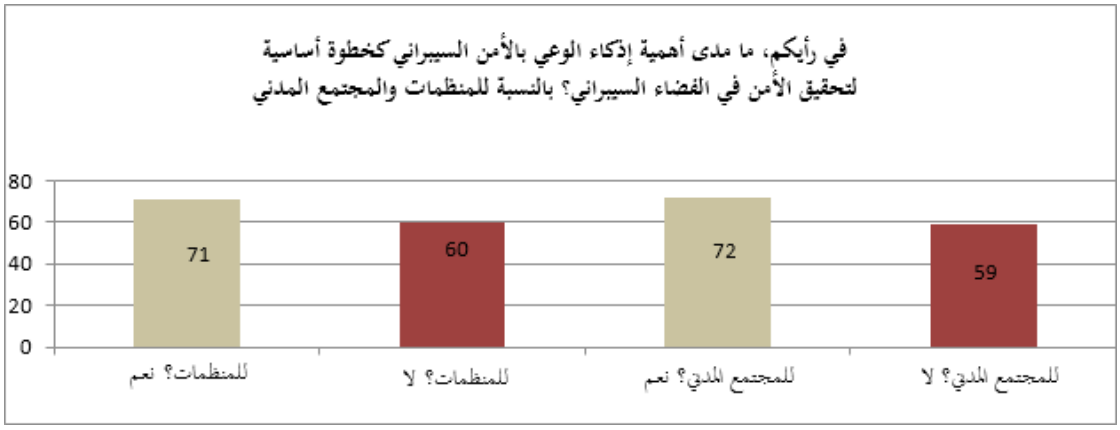
قام 82 بلداً من أصل 131 بإعداد وشن حملات للتوعية بالمخاطر السيبرانية. ويدل ذلك على إدراك الدول الأعضاء لأهمية تصميم وإعداد وشن حملات للتوعية بالمخاطر السيبرانية في بلدانها، وعلى إقرارها بهذه الأهمية.

الشكل 3: حملات لتوعية الجمهور بمسألة الأمن السيبراني



وفيما يخص القطاعات التي تستهدفها حملات التوعية، تمثلت أهداف الحملات الخاصة بالقطاع الحكومي، وفقاً لنتائج الاستبيان، 71 بلداً، والقطاع المدني 72 بلداً. ويؤكد ذلك أن الدول الأعضاء تعتبر أن أهمية إذكاء الوعي في القطاعين الحكومي والمدني متساوية نسبياً.

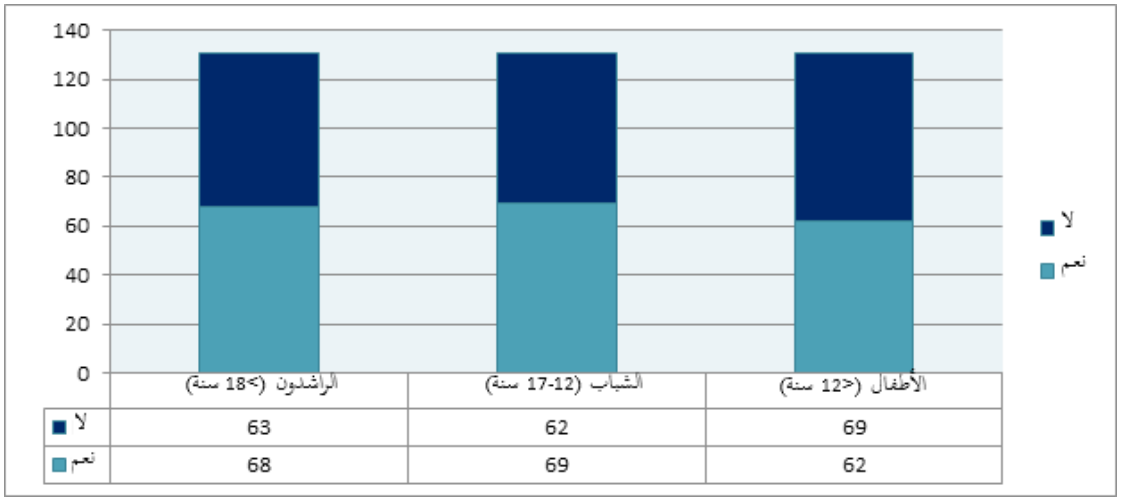
الشكل 4: أهمية التوعية بالأمن السيبراني في المنظمات/المجتمع المدني



فيما يخص الفئات العمرية التي تستهدفها حملات التوعية بالأمن السيبراني، يحدد الاستبيان ثلاث فئات: الراشدون (18 سنة وما فوق)، والشباب (12-17 سنة)، والأطفال (أقل من 12 سنة).

ويظهر **الشكل 5** أدناه أن الفئات العمرية الثلاث استُهدفت بدرجة مشابهة. واستناداً إلى النتائج، تبقى فئة الشباب هي الفئة المستهدفة الأولى في حين أن فئة الأطفال هي الفئة الأقل استهدافاً. وربما يُعزى ذلك إلى أن الدول الأعضاء تعتبر فئة الشباب الفئة الأكثر عرضة للمخاطر التي تهدد الأمن السيبراني نظراً إلى تفاعلهم مع خدمات الاتصالات ولا سيما نفاذهم إلى الإنترنت.

الشكل 5: الفئات العمرية المستهدفة بحملات التوعية بالأمن السيبراني

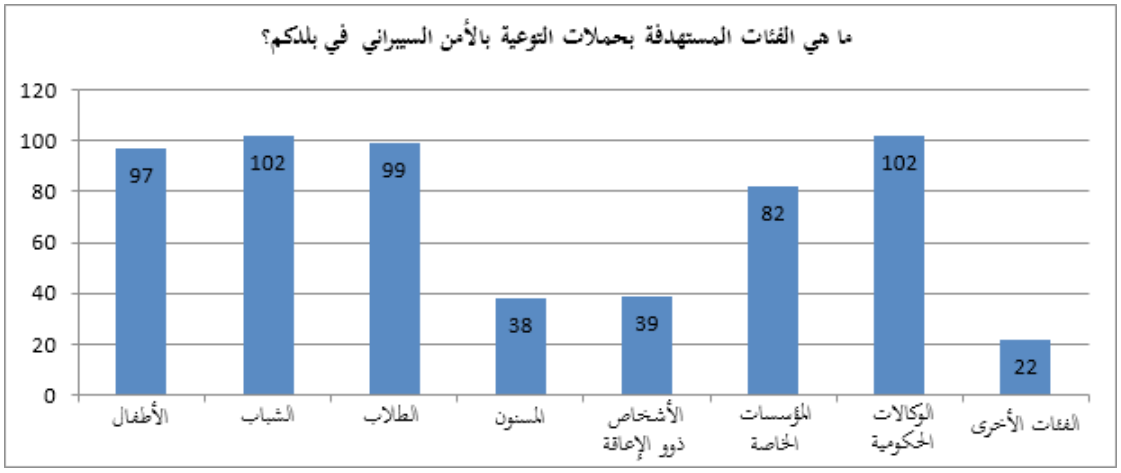


	الراشدون (<18 سنة)	الشباب (12-17 سنة)	الأطفال (<12 سنة)
لا	63	62	69
نعم	68	69	62

نشدد على أن حملات التوعية بالأمن السيبراني لا تقتصر على الفئات المذكورة أعلاه، وإنما تستهدف أيضاً فئات أخرى مثل المسنين والأشخاص ذوي الإعاقة الذين تخصَّص لهم برامج خاصة تناسب احتياجاتهم وتراعي أوضاعهم إذ إن المخاطر التي يواجهها المسنون مختلفة عن تلك التي يواجهها الأطفال.

ويُظهر الاستبيان بوضوح أن الوكالات الحكومية وفئة الشباب حظيتا بالنصيب الأكبر من تركيز الدول الأعضاء. وكذلك الأمر بالنسبة لفئة الطلاب والشباب التي حصلت على تصويت 99 بلداً و102 بلداً على التوالي. وعلى العكس من ذلك، فإن 38 بلداً فقط تستهدف فئة المسنين عند تنظيم حملات توعية متعلقة بالأمن السيبراني، أي أن نحو 70 في المائة من الدول الأعضاء التي شاركت في الاستبيان لم تستهدف هذه الفئة في حملات التوعية التي شنتها في مجال الأمن السيبراني. والجدير بالذكر أن 69 في المائة من الدول التي شاركت في الاستبيان لم تُدرج الأطفال ذوي الإعاقة في إطار الفئات التي تستهدفها. وذلك شبيه بنتائج الاستبيان الأخير الذي يُظهر أن الفئتين الأقل استهدافاً بحملات التوعية بالأمن السيبراني هما المسنون والأشخاص ذوو الإعاقة.

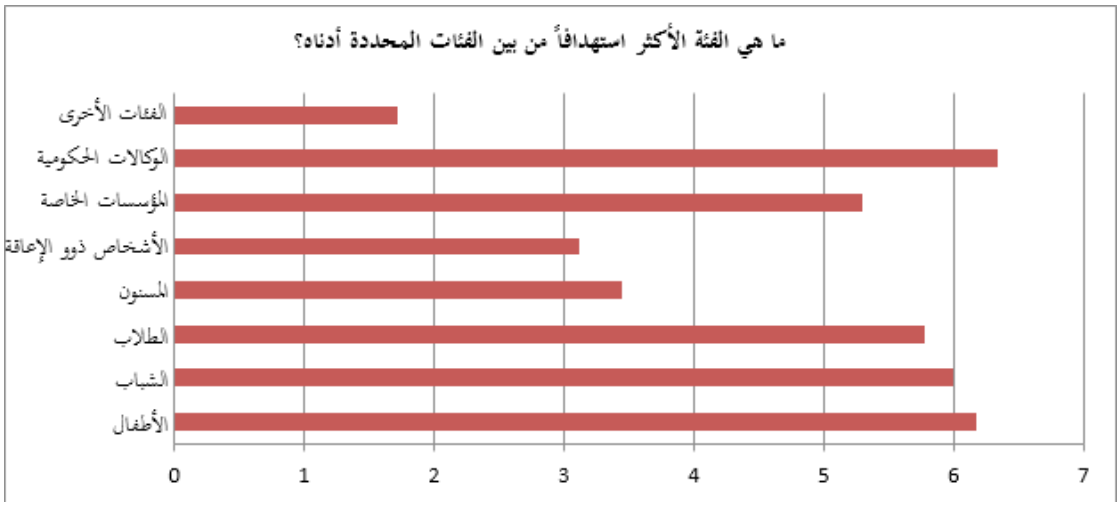
الشكل 6: الفئات المستهدفة بحملات التوعية بالأمن السيبراني



فيما يلي تحليل للمعلومات المتعلقة بالردود على السؤال: ما هي الفئات المستهدفة بحملات التوعية بالأمن السيبراني في بلدكم؟ إن النسبة الأعلى من المجيبين أجابت لصالح القطاع الحكومي يليه في المرتبة الثانية الأطفال في حين أن فئتي الشباب والطلاب تأتيان في المرتبة الثالثة والرابعة على التوالي. ومن جهة أخرى، كانت أيضاً الفئتان الأقل

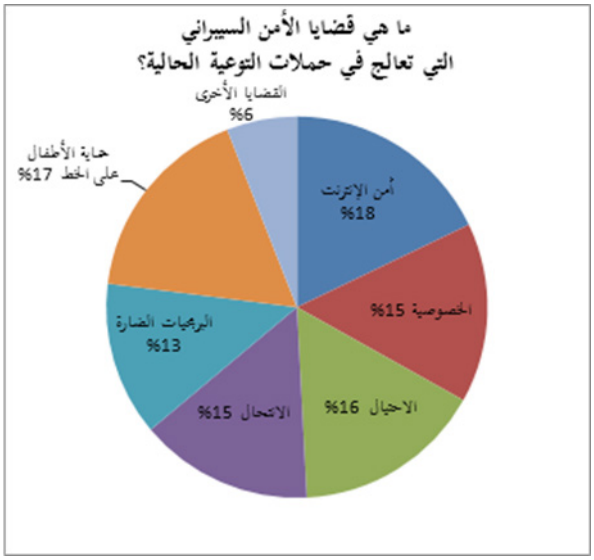
استهدافاً بحملات التوعية بالأمن السيبراني خلال فترة الدراسة السابقة 2010-2014 هما فئتي المسنين والأشخاص ذوي الإعاقة. والاختلاف الوحيد الذي كان واضحاً بين نتائج هذه الفترة ونتائج الفترة السابقة هو احتلال القطاع الحكومي المرتبة الأولى من بين الفئات الأكثر استهدافاً بعد أن كان يحتل المرتبة الثانية من ذي قبل. واحتلت فئة الأطفال المرتبة الثانية في نتائج الاستبيان بعد أن كانت تحتل المرتبة الأولى في الاستبيان الأخير، في حين احتفظت فئتا الشباب والطلاب بالمرتبة نفسها مقارنة بالاستبيان السابق.

الشكل 7: الفئات الأكثر استهدافاً بحملات التوعية بالأمن السيبراني



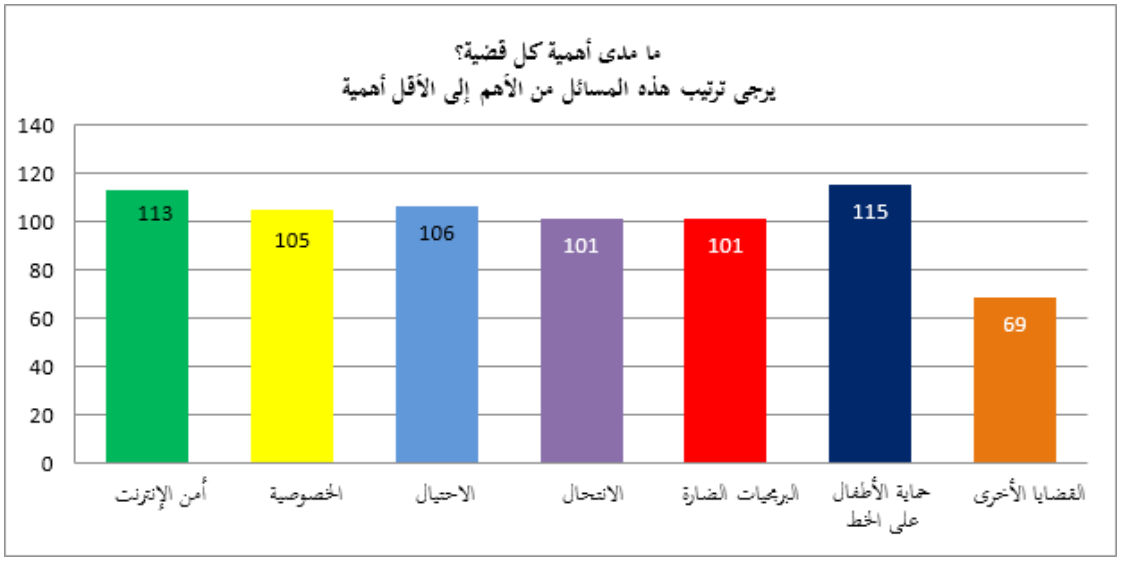
لقد كان من المهم تحديد المسائل التي تم التركيز عليها في هذه الحملات بهدف إذكاء الوعي بالمخاطر السيبرانية المتعددة. وكانت المسائل الأهم هي أمن الإنترنت، والسرية، والاحتيال، والانتحال، والبرمجيات الضارة، وحماية الأطفال على الخط. وكانت مسألة أمن الإنترنت في صدارة المسائل الأهم المتعلقة بالأمن السيبراني، تليها حماية الأطفال على الخط، والاحتيال، والانتحال على التوالي. وبشكل عام، كانت نتائج حملات التوعية بالأمن السيبراني متقاربة، وقد لوحظ نفس التقارب في استبيان فترة الدراسة السابقة، إذ احتلت مسألة أمن الإنترنت المرتبة الأولى، وتلتها حماية الأطفال على الخط، في حين احتلت السرية والاحتيال والانتحال المرتبة الثالثة بنسب متساوية. وحصلت مسألة حماية الأطفال على الخط على النسبة الأكبر في حملات التوعية بالأمن السيبراني، إذ اعتبر 43 بلداً من أصل 129 بلداً مجيباً أنها المسألة الأهم. وهذا أمر منطقي نظراً إلى أهمية مسألة حماية الأطفال على الخط التي ينبغي أن يتناولها عدد أكبر من حملات التوعية في المجتمع، ولا سيما فيما يخص الفئة المستهدفة المتمثلة في الأطفال الذين يواجهون هذه المخاطر، فضلاً عن الأهل والمعلمين. وتبرز أيضاً أهمية حماية الأطفال على الخط من خلال احتلالها المرتبة نفسها في الاستبيان الذي أجري خلال فترة الدراسة السابقة.

الشكل 8: قضايا الأمن السيبراني التي تعالج في حملات التوعية

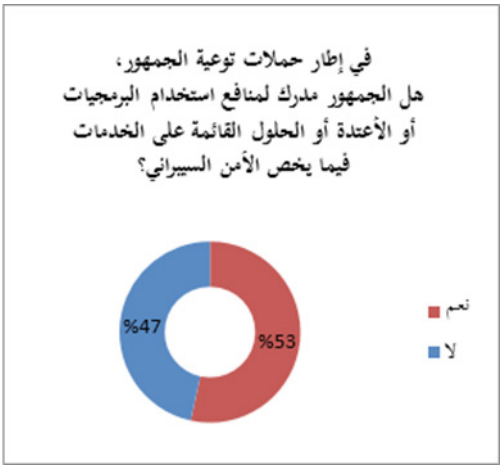


احتلت قضية أمن الإنترنت، في المتوسط، المرتبة الثانية، تلاها الاحتيال والخصوصية، في حين أن قضيتي البرمجيات الضارة والانتحال احتلتا المرتبة الأخيرة على النحو المبين في **الشكل 9**.

الشكل 9: أهمية كل قضية من قضايا الأمن السيبراني التي تعالج في حملات التوعية



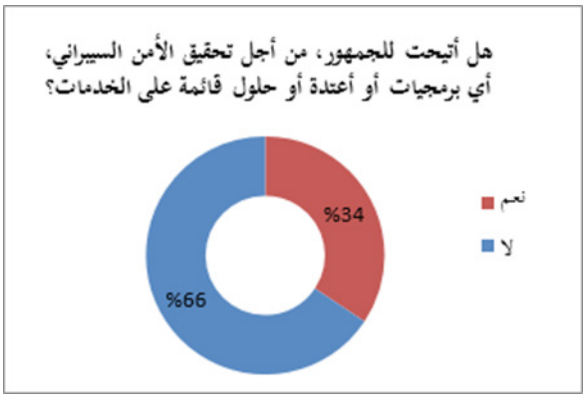
الشكل 10: إدراك الجمهور لمنافع البرمجيات/الأعتدة أو الحلول القائمة على الخدمات



عند مناقشة مسألة إذكاء الوعي، من المهم تناول مسألة الدراية بالتكنولوجيات وتوافر الأدوات التكنولوجية لضمان الحماية من شتى المخاطر السيبرانية. فتعزيز الإدراك النظري ليس كافياً إذا لم تُكتسب المعارف العملية أو التكنولوجية اللازمة. وما نعنيه بالمعارف العملية هو إعلام الجمهور بفوائد البرمجيات أو الأعتدة أو الحلول القائمة على الخدمات، المتاحة للأمن السيبراني، إذ تؤدي برامج هذه البرمجيات دوراً رئيسياً في الأمن السيبراني ومكافحة المخاطر السيبرانية. وعمد 70 بلداً من أصل 131 إلى تعزيز برامج هذه البرمجيات وبإبراز فوائدها للفئات المستهدفة. و لم يتمكن 61 بلداً حتى الآن من تحسين دراية الجمهور ببرامج البرمجيات وبالحلول التقنية الأخرى اللازمة لتناول المخاطر السيبرانية. ورغم تقارب النتيجتين، يلاحَظ أن تعميم الحلول التقنية وبرامج البرمجيات تحظى بحصّة أكبر في حملات التوعية بالأمن السيبراني.

كما يُظهر الاستبيان أن 45 بلداً أتاح بالفعل للجمهور برامجَ البرمجيات هذه أو الحلول القائمة على الخدمات، في حين أن غالبية المجيبين (86 بلداً)، أي ما يمثل 65,65 في المائة ردت بأنها لم تقم بذلك.

الشكل 11: ما أتيح للجمهور من برمجيات/أعتدة أو حلول قائمة على الخدمات



يرجى العودة إلى **الفصل 4** للاطلاع على تحليل الاستبيان المتعلق بحماية الأطفال على الخط.

2 الفصل 2 - وضع الرسائل الاقتحامية والبرمجيات الضارة وسبل التخفيف منها والجوانب التنظيمية

يتعلق هذا القسم بالبندين (أ) و(ب) من الاختصاصات المتصلة بالمسألة 3/2 اللذين يدعوان إلى جملة أمور منها:

*أ) **مناقشة النهج وأفضل الممارسات لتقييم أثر الرسائل الاقتحامية داخل الشبكات، وتوفير التدابير اللازمة، بما في ذلك تقنيات التخفيف من آثارها التي يمكن أن تستخدمها البلدان النامية، مع أخذ المعايير القائمة والأدوات المتاحة بعين الاعتبار.***

*ب) **تقديم معلومات حول تحديات الأمن السيبراني الحالية التي يواجهها مقدمو الخدمات والوكالات التنظيمية وغيرها من الأطراف ذات الصلة.***

إن الطريقة الرئيسية التي أُدخلت بها الرسائل الاقتحامية هي عبر الأنظمة المخترقة من المهاجمين (مثل المملوكة). ثم يقومون بإنتاج رسائل اقتحامية عن طريق مقدمي الخدمات. والنهج التقليدي المتبع للتصدي لهذا النوع من الهجمات هو صون وتصفح قواعد البيانات الخاصة بسمعة المرسلين. وتستند هذه السمعة إلى عنوان المقصد IP للمرسل. وتختلف الطريقة التي تتوصل بها أنظمة السمعة هذه إلى استنتاجاتها باختلاف الأنظمة. ومن النهج الشائعة استخدام عناوين بريدية تكون بمثابة "مصيدة" وترمي فقط إلى جذب المقتحمين. وعندما تصل رسالة إلى صناديق البريد هذه، تتأثر سمعة عنوان المقصد IP للمرسل سلباً.

وغالباً ما تأخذ أنظمة السمعة الحجم بعين الاعتبار. ولكن أصبح هذا الأمر صعباً في الآونة الأخيرة. وتسعى رسائل "التصيد" الاقتحامية إلى الاستفادة من عدد كبير من الشبكات الروبوتية الموزعة جغرافياً (شبكات الحواسيب المخترقة) بحيث لا يرسِل حاسوب واحد عدداً كبيراً جداً من الرسائل وإنما تتولد بفعل مجموعها حركة كبيرة الحجم.

وحتى مع وجود أشكال الرسائل الاقتحامية الجديدة هذه، تستطيع أنظمة التصدي للرسائل الاقتحامية أن تقلل عادة من حجم الرسائل الاقتحامية التي تصل إلى المستقبلات بما يزيد عن 90 في المائة وحتى بما يزيد عن 99 في المائة في أحيان كثيرة. وتُعتبر مرشحات مكافحة الرسائل الاقتحامية عنصراً مهماً للغاية للحرص على أن يبقى البريد الإلكتروني أداة تواصل فعّالة. وتُعتبر أيضاً وسيلة مهمة للغاية لتفادي اقتحام الأجهزة.

الشكل 12: الحلقة المفرغة للرسائل الاقتحامية والأمن السيبراني

إن تلقي الرسائل الاقتحامية لا يصيب بحد ذاته الجهاز أو يعطله. وفي الواقع، هناك طرائق عديدة للخروج من الحلقة المفرغة. وعلى نحو ما ذُكر سابقاً، تقضي أجهزة مكافحة الرسائل الاقتحامية على غالبية هذه الرسائل. وفي غالبية الحالات، وحتى عندما يتم تلقي الرسالة، يجب أن يقوم المستخدم بفعل ما مثل فتح وثيقة مرفقة. وعليه، فإن تثقيف المستخدمين أمر أساسي للحماية من الرسائل الاقتحامية التي لا نهاية لها. وإذا قام المستخدم بفتح الوثيقة المرفقة، فيمكن لبرامج مكافحة الفيروسات المحدثة ولبرمجيات أنظمة التشغيل أن تتيح أيضاً تجنب الإصابة. ولكل عنصر من هذه العناصر عدد من الأدوات المجانية أو ذات الكلفة المتدنية التي تكون متاحة للمستخدمين ومقدمي الخدمات في البلدان النامية.

وهناك تقنية أخرى ندرك وجودها وهي اختطاف فدرات عنوان المقصد IP في نظام التسيير. ويطرأ ذلك عندما يقيم المهاجم علاقة تناظرية مع مقدم خدمات موثوق به لتبادل معلومات التسيير. وقد وُضع مؤخراً شكل جديد من أشكال الحماية – أمن بروتوكول مسيِّر الحدود (BGPSEC)[2] مع البنية التحتية العامة الأساسية للموارد (RPKI) - لتفادي هذا النوع من الهجمات، وهو قيد الإعداد والنشر. ولكن ستحتاج هذه الحماية الجديدة لأنظمة التسيير إلى الوقت وإلى الخضوع للاختبار قبل التمكن من استخدامها على نطاق واسع. وفي الأثناء، ما زالت جميع النهوج المذكورة أعلاه فعّالة لمكافحة الرسائل الاقتحامية.

وهناك طريقة للتخفيف من هذه الرسائل وُضعت مؤخراً وتسمى "استيقان الرسالة والمطابقة على أساس الميدان" (DMARC)[3] وتعتمد هذه الطريقة على تكنولوجيتين للاستيقان: هما البريد المعرف بمفاتيح الميادين (DKIM) وإطار سياسة المرسل (SPF) للتحقق من استيقان كل رسالة. وإذا لم يتم الاستيقان من إحدى الرسائل، يمكن اتخاذ تدبير بالاستناد إلى ما يفضله مالك الميدان المرسل. وقد يشمل هذا التدبير رفض الرسالة. ولا يستخدم هذا المزيج من التكنولوجيات سوى قلة قليلة من موردي رسائل البريد الإلكتروني بأعداد كبيرة جداً، وسوى عدد من الخدمات التي تنتج أعداداً كبيرة من رسائل البريد الإلكتروني الخاصة بالمعاملات (مثل تأكيد أوامر الدفع والشراء).

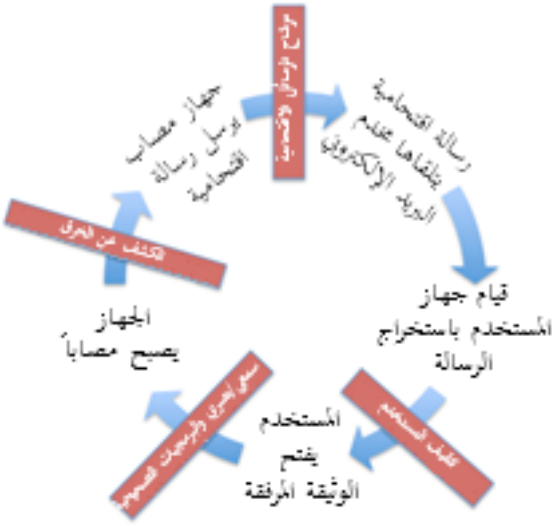
وعندما يُستخدم استيقان الرسالة والمطابقة على أساس الميدان (DMARC) مع البريد المعرف بمفاتيح الميادين (DKIM)، يحول أيضاً دون اختطاف سابقات عناوين المقصد IP. ولكن لا يتم ذلك دون ما يحمله من مشاكل. فعندما يُستخدم استيقان الرسالة والمطابقة على أساس الميدان (DMARC) بالاقتران مع رسائل لا تتعلق بمعاملات (مثل رسائل تبادل بين أفراد)، يشكو من بعض المشاكل المتعلقة بقابلية التشغيل البيني[4]. ويجري في الوقت الراهن تكثيف العمل في إطار فريق مهام هندسة الإنترنت (IETF). وإضافةً إلى ذلك، لا يستطيع استيقان الرسالة والمطابقة على أساس الميدان (DMARC) الكشف عن استخدام الأنظمة المخترقة عندما ترسل هذه الأنظمة رسالة بالبريد الإلكتروني عبر مقدمي الخدمات العاديين. فالتدبير الأساسي للحد من الرسائل الاقتحامية هو حماية الأنظمة الطرفية من الإصابة في المقام الأول.

[2] RFC 6480، https://rfc-editor.org/info/rfc6480.

[3] RFC7489، https://www.rfc-editor.org/info/rfc7489.

[4] RFC 7960، https://www.rfc-editor.org/info/rfc7060.

الشكل 13: الخروج من الحلقة المفرغة



1.2 مصادر الرسائل الاقتحامية

لقد تطورت كثيراً الحلقة المفرغة المبيّنة في **الشكلين 12 و13**، عن طريق استخدام الشبكات الروبوتية التي تتألف من مزيج من أجهزة المستهلكين، وفي بعض الحالات، من مخدمات في مراكز بيانات تم خرقها. وقد أثارت مساهمة واحدة على الأقل شواغل بشأن خطر قيام الأجهزة المتنقلة بإنتاج الرسائل الاقتحامية. وهناك شتى الأجهزة المتنقلة المعرضة للخطر بطرائق مختلفة، وفقاً لنماذجها التشغيلية. وقد أثبت مثلاً هاتف iPhone لشركة آبل مقاومته الكبيرة للهجمات، بفضل الحاجة إلى تطبيقات موقعة ومصدق عليها رقمياً، وبفضل المراقبة القوية التي تمارسه كل من المنصة والتطبيقات التي تعمل فوقه.

وهناك منصات أخرى تطرح أكثر من تحد. وإذ يستمر الاستخدام المجتمعي لتكنولوجيا المعلومات والاتصالات في التوسع، وتستمر إنترنت الأشياء (IoT) في النمو، يتم إدخال منصات جديدة في الشبكة. وإذا كانت تتضمن وحدة معالجة مركزية وإذا كانت موصولة بشبكة، فمن الممكن أن تعتريها مواطن ضعف. وقبل نشر هذا التقرير بوقت ليس بالبعيد، هاجمت الدودة الحاسوبية Mirai Worm البنية التحتية لأنظمة أسماء الميادين وعطلت موقعاً كبيراً للشبكات الاجتماعية. وفيما يتعلق بشكل مباشر بالرسائل الاقتحامية، أوضحت شركة Proofpoint موطن ضعف في عام 2013 من شأنه أن يجعل الثلاجات ومقاييس الحرارة وأجهزة الإنذار ضد السرقات ترسل رسائل اقتحامية[5]. ويؤكد هذا الاكتشاف الحاجة إلى أن يتيح مصنعو الأجهزة آليات للتحديث المؤتمت للبرمجيات تمكن من التخفيف من خطر استغلال الأجهزة.

2.2 آثار الرسائل الاقتحامية على الشبكة

هناك عدة نقاط لقياس أثر الرسائل الاقتحامية على الشبكة، وهي تتراوح من الوصلات الدولية إلى ما يدخل إلى الهاتف الخلوي عن طريق الترددات الراديوية. وخلال سنوات عديدة خلت، أثيرت مسألة معرفة حجم عرض النطاق الذي تستهلكه فعلاً الرسائل الاقتحامية على الشبكة. إن رسائل البريد الإلكتروني بذاتها تكون عادة قليلة

[5] http://www.economist.com/news/science-and-technology/21594955-when-internet-things-misbe-haves-spam-fridge.

جداً وتبلغ في المتوسط ما يناهز 000 75 بايت[6]. إلا أن العديد من الرسائل هي أصغر منها قليلاً إلى حد ما، وتتأثر القيمة المتوسطة بالوثائق المرفقة التي قد لا يتم تنزيلها في الأصل. وإذا كانت هناك أحكام مناسبة لمكافحة الرسائل الاقتحامية، فلن يصل سوى عشر في المائة تقريباً كأقصى حد. فحتى لو استخدمنا الحجم الأكبر المقدر للرسائل البالغ 259 مليار رسالة يومياً، مقترناً بأقل الحلول فعالية لمكافحة الرسائل الاقتحامية، وإذا افترضنا أن 2,5 مليار شخص يستخدمون الشبكة، فيُفترض ألا يرى الأشخاص أكثر من عشر رسائل تقريباً في اليوم للفرد. وفي غياب أي حماية من الرسائل الاقتحامية، يرتفع هذا العدد المحسوب للفرد الواحد إلى نحو 100 رسالة يومياً. وحتى عند هذا الحجم، فإن استهلاك الرسائل الاقتحامية للشبكة ضئيل جداً مقارنة بالاستخدامات الصوتية والتسجيلات الفيديوية وتصفح الشبكة. وبوجه عام، تظهر المقاييس أن جميع رسائل البريد الإلكتروني (بما فيها الرسائل الاقتحامية) تستخدم عامة حيزاً لا يذكر من عرض النطاق في الاقتصادات التي جرى قياسها.[7] ولا يتعلق التهديد الذي تطرحه الرسائل الاقتحامية بعرض النطاق المستخدم على الشبكة، بقدر ما يتعلق بخطر استخدام الأجهزة المصابة لأغراض الاحتيال أو لأغراض أخرى غير قانونية. وفي غياب مرشحات فعّالة، تقلل الرسائل الاقتحامية أيضاً من قيمة البريد الإلكتروني بالنسبة للمستخدمين.

3.2 مخاطر التصيد الاحتيالي وسبل التخفيف منه

إن التصيد الاحتيالي هو نوع من الهجمات، فترسل فيه رسالة احتيالية بالبريد الإلكتروني إلى مستخدم مستهدف وتظهر الرسالة وكأنها أرسلت من مصدر مشروع وتتضمن أيضاً ما يكفي من المعلومات الشخصية بحيث يتم الإيقاع بالمستقبل ليظن أن مصدر الرسالة أصلي. ومن الأمثلة على ذلك استخدام أرقام حسابات حقيقية، وذكر أسماء أشخاص آخرين يعرفهم المستهدَف، واستخدام صور مألوفة للمستهدَف. ويُدفع المستهدف إلى النقر على وصلة ويب أو فتح وثيقة مرفقة بما يؤدي عندئذ إلى إصابة آلة الشخص. إن التكلفة الواقعة على المهاجم الذي يلجأ إلى التصيد الاحتيالي أعلى بكثير من الهجمات غير المستهدفة لأن معرفة المستهدَفين تقتضي إجراء الأبحاث. وقد تأخذ هذه الأبحاث شكل عملية اختراق إلى متاجر التجزئة أو الإدارات الحكومية لجمع المعلومات عن المستهدفين. ويُعتبر تثقيف المستخدمين أكثر الوسائل فعالية للحماية من التصيد الاحتيالي.

4.2 أثر السياسات على الرسائل الاقتحامية

يمكن أن يكون للقواعد التنظيمية أثر إيجابي أو سلبي على مسألة التخفيف من الرسائل الاقتحامية. إن استخدام حاسوب لإرسال رسالة احتيالية يُعتبر فعلاً احتيالياً. وهذه ليست جريمة جديدة، وإنما مجرد شكل جديد لجريمة قديمة جداً. ويجب أن تكون التشريعات مرنة بما يكفي لمقاضاة الأشخاص الذين يرتكبون هذا الفعل الاحتيالي. وفي الولايات المتحدة، سُن قانون CAN-SPAM في عام 2003 ليشار بشكل واضح إلى عدم مشروعية هذا السلوك. إلا أن الكشف عن المهاجمين الفعليين ما زال أمراً صعباً. وقد تؤدي الشراكات بين مقدمي الخدمات من القطاعين العام والخاص والمكلفين بإنفاذ القانون إلى التقدم في تحسين القدرة على كشف المهاجمين مع الوقت. وعندما تُنفَق أموال فعلية للقيام بفعل احتيالي، يمكن تعقب المعاملات عن طريق الشبكات المالية.

ومن جهة أخرى، فإن الحؤول دون تلقي الرسائل الاقتحامية يتطلب عادة وجود وسطاء يمكنهم النفاذ إلى مضمون الرسائل لتحديد ما إذا كان هذا المضمون آمناً للأنظمة الطرفية. ويجب أن يكون هناك إطار تشريعي ملائم يتيح حماية الشبكة ومستخدميها.

[6] http://email.about.com/od/emailstatistics/f/What_is_the_Average_Size_of_an_Email_Message.htm.

[7] https://www.sandvine.com/downloads/general/global-internet-phenomena/2013/2h-2013-global-internet-phenomena-report.pdf.

ويواصل الاتحاد الدولي للاتصالات تصديه للتحديات التي تطرحها الرسائل الاقتحامية، بالشراكة مع جمعية الإنترنت. وخلال فترة الدراسة هذه، عُقدت جلسة مثمرة خلال منتدى القمة العالمية لمجتمع المعلومات لعام 2016 بشأن "الرسائل الاقتحامية: فهم التحديات التي تواجهها اقتصادات الإنترنت الناشئة، والتخفيف منها".[8] وكان من بين المتحدثين ممثلون عن مؤسسة الأمن السيبراني في ماليزيا، وهيئة تنظيم المرافق والمنافسة في البهاما، وجمعية الإنترنت (ISOC)، وأحد المقررين المعنيين بالمسألة 3 التابعة للجنة الدراسات 2 لقطاع تنمية الاتصالات، ومشروع "سبامهاوس". وحددت الجلسة المسائل التالية الواجب تناولها:

- ضرورة تعزيز التعاون فضلاً عن مواءمة خطط العمل الفعلية للدول الأعضاء، نظراً إلى أن الرسائل الاقتحامية هي مشكلة جماعية تؤثر على الجميع؛
- صحيح أن تكلفة التوصيل (للنطاق العريض) باتت ميسورة، ولكن قد لا تكون تكلفة الحماية (من الهجمات السيبرانية) ميسورة؛
- ضرورة وجود تشريع يحدد ما هو مقبول وما هو غير مقبول، وينشئ آلية تفرض عقوبات قابلة للإنفاذ على الذين يخلون بهذا التشريع، ولا تكون جامدة لدرجة معاقبة جهات فاعلة مثل الشركات المتوسطة والصغيرة (SME) التي تحاول إعداد حملات تسويقية؛
- مشاطرة أفضل الممارسات والحلول المستمدة من قوائم الثقب الأسود وخدمات السمعة مع جميع الدول الأعضاء عن طريق الاتحاد.

[8] جلسة منتدى القمة لعام 2016 بشأن *"الرسائل الاقتحامية: فهم التحديات التي تواجهها اقتصادات الإنترنت الناشئة، والتخفيف منها"*: https://www.itu.int/net4/wsis/forum/2016/Agenda/Session/152.

3 الفصل 3 - تحسين وضع الأمن السيبراني على الصعيد الوطني: تعزيز الوعي وتحسين الموارد البشرية

يتعلق هذا القسم بالبند (ج) من الاختصاصات المتصلة بالمسألة 3/2 الذي يدعو إلى جملة *أمور من بينها*:

ج) ***مواصلة جمع التجارب الوطنية المتعلقة بالأمن السيبراني من الدول الأعضاء، وتحديد المواضيع المشتركة ودراستها في إطار تلك التجارب.***

نحن نعيش في عالم يزداد توصيلاً، ومع أن هذا الواقع يولد فرصاً غير مسبوقة للابتكار وتحقيق النمو الاجتماعي والاقتصادي في جميع أنحاء العالم، يواجه الفضاء السيبراني أيضاً تحديات وتهديدات أمنية. وإضافةً إلى ذلك، وفيما تستمر هذه التحديات الأمنية في التزايد والتأثير على مختلف القطاعات، تواجه البلدان تحديات متزايدة تحثها على إيجاد الحلول للتصدي لهذه المسائل.

وللتصدي لهذه التحديات، تنظم العديد من البلدان حملات للتوعية بالأمن السيبراني تهدف إلى تثقيف الحكومات والقطاع الخاص والمربين والمواطنين الأفراد لتمكينهم من الكشف عن المشاكل المحتملة وفهم أدوارهم ومسؤولياتهم في استحداث فضاء سيبراني أكثر أماناً. وأثناء فترة دراسة لجنة الدراسات، قدّم عدد من الكيانات مساهمات بشأن هذا الموضوع. وللمزيد من المعلومات، انظر **الملحق 2** المعنون "مجموعة دراسات الحالة القُطرية بشأن الأمن السيبراني".

1.3 حملات التوعية

من الأمثلة على حملات التوعية هي حملة قف.فكر.اشتبك™ التي تهدف إلى تعزيز فهم التهديدات السيبرانية وتمكين الجمهور الأمريكي لزيادة أمنه وسلامته على الخط. وتسعى إلى نشر مفهوم الأمن السيبراني بوصفه "مسؤولية مشتركة" إذ يؤدي كل فرد، عبر اتخاذه خطوات بسيطة لتعزيز أمنه على الخط، إلى جعل استخدام الإنترنت تجربة أكثر أماناً للجميع. وتتضمن رسائلها الأساسية ما يلي:

- **قف**: قبل أن تستخدم الإنترنت، خذ الوقت اللازم لفهم المخاطر ولتعلم كيفية الكشف عن المشاكل المحتملة.
- **فكر**: فكر لحظة للتأكد من أن المسار الذي ستسلكه واضح. وانتبه لإشارات التحذير وفكر في كيفية تأثير أعمالك على الخط على أمنك أو أمن عائلتك.
- **اشتبك**: استمتع بالإنترنت بمزيد من الثقة وأنت تعلم أنك اتخذت الخطوات السليمة لحماية نفسك وحاسوبك.
- **قف.فكر.اشتبك**: احم نفسك وساهم في إبقاء الويب مكاناً أكثر أماناً للجميع.

يتضمن هذا القسم أربعة عناصر تحدد الخطوات وأفضل الممارسات الموصى باتخاذها لشن حملة توعية بالأمن السيبراني.

1.1.3 أفضل الممارسات لبرنامج خاص بالاتصالات

صحيح أن لكل بلد احتياجاته وتحدياته الفريدة المتعلقة بتهديدات الأمن السيبراني وبالحماية منها، إلا أن أفضل الممارسات التالية يمكن أن تساعد في شن حملة توعية بالأمن السيبراني.

- **وضع خطة للاتصالات تتضمن أهدافاً وغايات محددة جيداً وتحدد الجمهور (الجماهير) المستهدف (المستهدفة) بشكل رئيسي.** إن الخطوة الأولى لشن حملة توعية بالأمن السيبراني هي تحديد الأهداف والغايات المحددة للحملة فضلاً عن الجمهور المستهدف بشكل رئيسي. **وضع استراتيجيات هادفة للاتصالات وجمع موارد للوصول إلى الجماهير المحددة.** تختلف الاحتياجات المتعلقة بالأمن السيبراني باختلاف الجهات المعنية.

فعلى سبيل المثال، قد يحتاج الطلاب إلى معلومات عن المعتدين السيبرانيين في حين يحتاج الأخصائيون في مجال المعلومات والتكنولوجيا إلى معلومات عن القراصنة. وينبغي وضع مواد تختلف باختلاف احتياجات ومعارف ومستوى قدرات كل جمهور من الجماهير.

- إعداد **كتيّبات نصائح** مخصصة لكل جمهور من الجماهير المحددة لتلبية احتياجاته الفريدة ومواجهة التهديدات الفريدة التي تواجهه. وتشدد مواد التعليم الشاملة، مثل مجموعة الأدوات الخاصة بحملة قف.فكر.اشتبك، على المسؤولية المشتركة فيما يخص الأمن السيبراني، مع المساهمة في الوقت نفسه في ضمان توافر الموارد اللازمة لجميع فئات المجتمع. وتساعد رسائل التذكير البسيطة، في شكل ملصقات وسوارات وغيرهما، الأفراد في إبقاء أفضل الممارسات الخاصة بالأمن السيبراني على رأس سلم أولوياتهم.

- **استخدام وسائط التواصل الاجتماعي**. يجري قدر كبير من أعمال التوعية بالأمن السيبراني على الخط. فيساعد استخدام وسائط التواصل الاجتماعي على إيصال رسائل التوعية بالأمن السيبراني إلى الأفراد عن طريق قنوات يستخدمونها بالفعل - وهي تكون في بعض الأحيان القنوات التي يفضلون استخدامها. فنشر المعلومات على مواقع شبكات التواصل الاجتماعي، مثل فيسبوك وتويتر ويوتيوب، يُعتبر إحدى وسائل عرض وتقديم المعلومات والحصول في الوقت نفسه على مدخلات قيمة أيضاً.
استخدام وسائط الإعلام التقليدية: بث الراديو والتلفزيون، والصحف، والمجلات.

- **إقامة الشراكات مع حلفاء في الجماهير المستهدفة وصون هذه الشراكات**. لا تستطيع أي منظمة، سواء أكانت وكالة حكومية أو شركة أو منظمة غير ربحية، أن تتولى وحدها نشر الوعي بالأمن السيبراني. ولذلك، فإن الشراكات في كلا القطاعين العام والخاص ضرورية. فينبغي إقامة واستهلال شراكات مع منظمات من قبيل:

أ) *الوكالات الحكومية*. تمنح الوكالات الحكومية قيمة للرسالة الموجهة، ويمكنها الوصول إلى عدد كبير من الأفراد والأوساط.

يمكن استخدام برنامج مركزي لتدريب السلطات الحكومية المحلية والإقليمية لتتمكن بدورها من تأهيل موظفيها ومكوناتها على تحديد المخاطر الموجودة على الخط والكشف عنها. ومن بين الشركاء الحكوميين الرئيسيين، على شتى المستويات، الأفرقة المعنية بأمن الحاسوب والاستجابة للحوادث الحاسوبية (CSIRT)، ومكاتب كبار موظفي أمن المعلومات (CISO)، ومكاتب كبار موظفي المعلومات (CIO).

ب) *المنظمات غير الربحية*. *توفر المنظمات غير الربحية مجموعة متنوعة من الموارد وتتسم بالمرونة، بما يتيح لها نشر رسالة التوعية بالأمن السيبراني.*

تغطي المنظمات غير الربحية جميع مجموعات الجماهير المحددة في الخطة الاستراتيجية. وتساعد الدعوات المنتظمة، بما في ذلك جميع المنظمات الشريكة، على بناء شبكات بين كل منظمة، في القطاعين العام والخاص.

ج) *الهيئات الأكاديمية*. تساهم الهيئات الأكاديمية في البحوث الرئيسية والمحدثة التي تساعد في إبقاء الحملة مرتبطة بالواقع الراهن وعلى اطلاع بما يجري. وتتيح أيضاً النفاذ إلى القوى العاملة المستقبلية للبلد. وتُعتبر أيضاً الشراكات مع المدارس الثانوية والمدارس الابتدائية أمراً مهماً للغاية لأن التشجيع على تلقين الوعي بالأمن السيبراني منذ الصغر يساعد الطلاب على استخدام الإنترنت بطريقة آمنة طوال حياتهم. إن العمل مع الجامعات أو مراكز التميز يساهم في إرساء علاقات بين القوى العاملة قيد التدريب والمنظمات التي ستستخدمها في المستقبل.

د) *منظمات القطاع الخاص*. يمكن أن يقوم قادة الدوائر الصناعية، مثلاً في خدمات المعلومات والتجزئة والمالية والتعليم، بتثقيف الموظفين والمستهلكين والجماهير الأخرى بالتهديدات التي تؤثر عليهم، وكذلك

تلقي المعلومات بشأن تعزيز ممارسات الأمن السيبراني. ويمكن أن تؤدي الحلول الابتكارية الخاصة بالأمن السيبراني، التي وضعتها منظمات القطاع الخاص، إلى وضع أفضل الممارسات في القطاعين العام والخاص.

- **إشراك الجماهير على صعيد الفرد من خلال بذل الجهود على مستوى القاعدة الشعبية.** إن وعي الفرد أساسي لتحقيق برنامج فعّال للتوعية بالأمن السيبراني.

فتدعو مثلاً حملة قف.فكر.اشتبك الأفراد إلى أن يصبحوا "أصدقاء الحملة" من خلال القيام باشتراك شهري لتلقي رسائل إخبارية مرسلة بالبريد الإلكتروني تتضمن آخر النصائح والأخبار والمعلومات المفيدة لهم في المجال السيبراني. وتصل أيضاً الحملة إلى الأفراد من خلال إجراء أحداث للتوعية مصممة خصيصاً لكل جمهور تعرض متحدثين يمكنهم التناقش في قضايا الأمن السيبراني التي لها الأثر الأكبر على الجمهور المعني.

- **قياس مدى توصل الجهود المبذولة إلى زيادة الوعي فعلاً بين الجماهير المستهدفة.** من أجل قياس فعالية إحدى الحملات، من المهم جمع الآراء من الأفرقة المتخصصة، أو الدراسات الاستقصائية، أو الوسائل المشابهة الأخرى. وينبغي أيضاً تعقب صفحات الويب التي تستقطب أكبر عدد من المشاهدين، والمواد الأكثر تنزيلاً، والأحداث الأكثر شعبية، والممارسات التي تعتبرها الجماهير الأكثر فعالية بغية تحديد النجاحات وتعزيز التحسين. فتساعد آراء المنظمات الشريكة في جعل الخطط المستقبلية تركز على الفعالية والابتكار.

2.1.3 نموذج لخطة الاتصالات

تُعتبر خطة الاتصالات عنصراً أساسياً لنجاح الحملة إذ تتضمن خارطة طريق تبين كيف تخطط المنظمة لتحقيق أهدافها وغاياتها الرئيسية. ومع أن خطة الاتصالات يجب أن تكون مصممة خصيصاً لتلبية احتياجات منظمة معينة، فإن غالبية الخطط ستتضمن الأقسام التالية:

الهدف والخلفية

يعرض قسم الهدف والخلفية المبرر المنطقي الذي يدفع المنظمة إلى إعداد خطة اتصالات، والإنجازات التي تخطط لتحقيقها.

الأهداف الرئيسية في مجال الاتصالات

إن الأهداف الرئيسية في مجال الاتصالات هي الغايات الرفيعة المستوى لبرنامج التوعية بالأمن السيبراني. وهذه الأهداف واسعة النطاق من الناحية الاستراتيجية. ومن الأمثلة عليها:

تعزيز وعي الجمهور العام بالأمن السيبراني من خلال زيادة مستوى فهم المخاطر السيبرانية، والأعمال البسيطة الرامية إلى التخفيف منها، وتمكين الجمهور ليكون أكثر استعداداً للقيام بما يلي عندما يستخدم الإنترنت:

- إذكاء الوعي بالأمن السيبراني وبعلاقته بالأمن الوطني وبأمن حياتنا الشخصية؛
- إشراك القطاعين العام والخاص فضلاً عن السلطات الحكومية الإقليمية للسعي إلى تحسين الأمن السيبراني؛
- إعداد وتعميم النهوج والاستراتيجيات التي تتيح للمواطنين تعزيز أمنهم وأمن عوائلهم ومجتمعاتهم على الخط.

الأهداف في مجال الاتصالات

تصف أهداف الاتصالات كيفية تحقيق الحملة لأهدافها الرئيسية. وينبغي أن تكون الأهداف قابلة للقياس.

على سبيل المثال، وضعت الأهداف العامة أعلاه في أهداف محددة على النحو التالي:

- تثقيف الجمهور بالممارسات التي تحقق الأمن السيبراني كي يحموا أنفسهم، والتأكد من معرفة مجموعات أصحاب المصلحة بالموارد المتاحة؛
- زيادة عدد مجموعات أصحاب المصلحة المنخرطة في هذا المجال، وتعزيز العلاقات القائمة مع السلطات الحكومية الإقليمية، ودوائر الصناعة، والمنظمات غير الربحية، والأنظمة المدرسية، والمربين؛
- زيادة وتعزيز القوى العاملة في المجال السيبراني من خلال تعزيز تعليم العلوم والتكنولوجيا والهندسة والرياضيات (STEM).

الجماهير الرئيسية المستهدفة

إن تحديد الجماهير الرئيسية المستهدفة يساعد على ضمان تركيز الرسائل على الفئات الأكثر استجابة لهذه الرسائل أو الأشد حاجة إليها. ويقود تحديد هذه الجماهير بشكل واضح إلى إبقاء الرسالة موجهة إلى المجموعات المعينة من خلال الاحتفاظ بفهم مشترك للمعنى الذي تنطوي عليه تسمية الجمهور.

قنوات الاتصالات

إن قنوات الاتصالات هي الوسائل المتعددة المستخدمة لنقل الرسالة إلى الجمهور (الجماهير) المستهدف (المستهدفة). وينبغي النظر بعناية في جميع وسائل الاتصالات المستخدمة حالياً فضلاً عن الطرائق الإضافية التي قد تكون متاحة للاستخدام. وينبغي أن تحدد خطة الاتصالات بشكل واضح ماهية القنوات وكيفية استخدامها.

وعلى سبيل المثال:

- الأحداث: استضافة أحداث مع مجموعات جماهير مستهدفة؛
- وسائط الإعلام التقليدية: الوصول بصورة استباقية إلى وسائط الإعلام الوطنية/الإقليمية/المحلية (مثلاً البث الإذاعي، والوسائط المطبوعة، والوسائط على الويب)؛
- وسائط التواصل الاجتماعي: استخدام منصات وسائط التواصل الاجتماعي بصورة نشطة (مدونة رسمية، وفيسبوك، وتويتر)؛
- رسالة إخبارية: توزيع رسالة إخبارية شهرية فضلاً عن مجموعات أدوات إعلامية؛
- الموقع الشبكي: القيام بصورة منتظمة بتحديث المواقع الشبكية للحملات من خلال إضافة الأخبار والنصائح والمعلومات الأساسية؛
- الشركاء: تشجيع المنظمات الشريكة على التوعية.

3.1.3 استراتيجيات الحملات

تأخذ استراتيجيات الحملات بعين الاعتبار الوسائل العملية لنشر المعلومات فضلاً عن الوسائل التي تزيد من زخم الحملة وتنميها. وتتضمن كل استراتيجية شاملة العديد من الخطوات الصغيرة الواجب إنجازها، وينبغي أن تكون كلا الخطوات والاستراتيجيات مرنة بما يكفي للتكيف مع بيئة متغيرة. وعلى سبيل المثال، استُخدمت الاستراتيجيات التالية لتلبية أهداف أحد البرامج في مجال الاتصالات:

- نشر رسالة الحملة عن طريق الأحداث ووسائط الإعلام (الاجتماعية والتقليدية)؛

- تكوين مجموعة من الجهات المعنية بحمل الرسالة، من خلال إقامة شراكات مع منظمات غير ربحية والوصول إلى القواعد الشعبية؛
- العمل على نطاق الوكالات الحكومية للتعاون على تنظيم الأحداث وتوجيه الرسائل.

توجيه الرسائل

ينبغي أن تركز العملية الرئيسية لتوجيه الرسائل على الرسائل الأساسية والجوهرية التي تسعى الحملة إلى نشرها. ولكل بلد وحملة - وكل جمهور وحدث - احتياجات محددة تقتضي أن تكون عملية توجيه الرسائل معدة لها خصيصاً. وتُستخدم العملية الرئيسية كقاعدة لكل عملية من هذه العمليات المصممة خصيصاً لاستهداف مجموعات معينة.

وعلى سبيل المثال، تتضمن الرسائل الرئيسية التي تحملها حملة قف.فكر.اشتبك ما يلي:

- **قف**: قبل أن تستخدم الإنترنت، خذ الوقت اللازم لفهم المخاطر ولتعلم كيفية الكشف عن المشاكل المحتملة.
- **فكر**: فكر لحظة للتأكد من أن المسار الذي ستسلكه واضح. وانتبه لإشارات التحذير وفكر في كيفية تأثير أعمالك على الخط على أمنك أو أمن عائلتك.
- **اشتبك**: استمتع بالإنترنت بمزيد من الثقة وأنت تعلم أنك اتخذت الخطوات السليمة لحماية نفسك وحاسوبك.
- **قف.فكر.اشتبك**: احم نفسك وساهم في إبقاء الويب مكاناً أكثر أماناً للجميع.

ومن الرسائل الأخرى المعمول بها عالمياً استخدام كلمات سر قوية، وتحديث أنظمة التشغيل وبرمجيات الأمن باستمرار، والاشتباك مع الأشخاص الذين تثق بهم فقط، وتفادي مواقع الويب التي تكون رائعة لدرجة يصعب تصديقها.

الأدوار والمسؤوليات

لا شك في أن تحديد الأدوار والمسؤوليات يتيح للأفرقة العمل معاً بصورة فعّالة مع تفادي التداخل أو اللبس. ويتم هذا التمييز بين المنظمات عندما تدعم عدة مجموعات حملة ما، وكذلك بين أعضاء أحد الأفرقة التابع لمنظمة معينة.

الموارد

إن إحصاء الموارد المتاحة للحملة يعطي فكرة واضحة عن نطاق أنشطة التوعية وعن حدودها ضمن فترة زمنية معينة. وفي هذا القسم، قد يقرر المنظّم أن يفضّل عدد الموظفين والمواد المخصص للحملة والمتوافر لدى المنظمة من أجل استهداف جماهير معينة ضمن فترة زمنية محددة.

تحديات الاتصالات

قد يساعد تحديد التحديات المتوقعة للاتصالات في التغلب على الثغرات والعوائق. ومن الأمثلة على ذلك:

- يصعب على الجماهير إدراك الجوانب التقنية للتهديدات السيبرانية وفهم علاقتهم بها؛
- قد لا يرى الجمهور العام بالضرورة أن التهديدات السيبرانية حقيقية أو مهمة في حياتهم اليومية.

4.1.3 مقياس النجاح ومعاييره

تحتاج كل خطة اتصالات إلى طريقة لتلقي الآراء وقياس الفعالية. وبفعل طبيعة حملات التوعية بالأمن السيبراني، تركز عمليات القياس هذه على الأنشطة الخارجية أكثر منها على المدخلات، إلا أنه من الضروري تلقي الآراء في الوقت المناسب. ومن الأمثلة على ذلك:

- عدد المشاركين في كل حدث أو سلسلة أحداث في المنطقة؛
- عدد مواد التسويق الموزعة؛
- التغطية الإعلامية؛
- عدد أصحاب المصلحة المشاركين (مثل الأصدقاء، وأعضاء تحالف التوعية بالمسائل السيبرانية، وأعضاء الشبكة الوطنية، إلخ.)؛
- عدد الزيارات إلى صفحة الويب؛
- تعليقات وشهادات المشاركين والمنظمات الشريكة؛
- تعليقات الهيئات التشريعية والقادة/المسؤولين على المستويين الحكومي والمحلي.

المعايير

تندرج المعايير في عدة فئات عامة. وتتوقف طريقة انطباق أنواع الفئات على مختلف برامج التوعية بالأمن السيبراني على الأهداف والموارد الخاصة بالبرامج. فترتبط **مشاركة أصحاب المصلحة** بالشراكات الرسمية المعقودة مع الوكالات الحكومية والمنظمات غير الربحية. وتتعلق التوعية عبر كل من **وسائل الإعلام التقليدية والوسائل الرقمية والإنترنت** بتوزيع المواد المكتوبة والمتعددة الوسائط عن طريق قنوات الاتصال القائمة. وتغطي كل من **الأحداث والمنتديات والموارد** عمليات التفاعل مع الأفراد. ولا بد من اعتماد عدة فئات من فئات المعايير لفهم وقياس النطاق الكامل للحملة.

2.3 المقاييس الإضافية لبناء القدرات

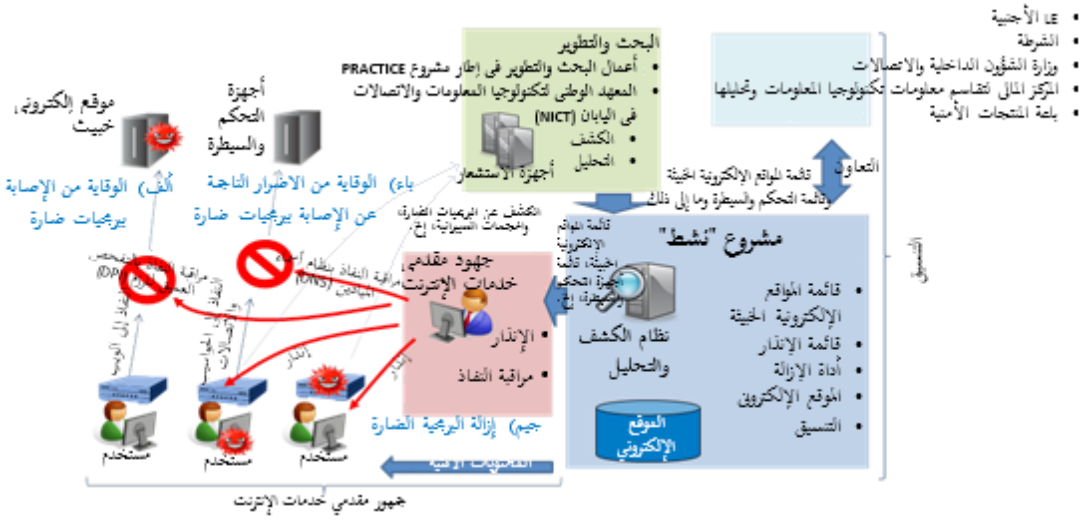
1.2.3 الأنشطة المنفّذة في اليابان

أعدت وزارة الشؤون الداخلية والاتصالات في اليابان (MIC) مشروعاً لإقامة شراكة بين القطاعين العام والخاص، بعنوان "نشط" ("ACTIVE") (ويختصر العنوان عبارة "المبادرة المتقدمة للتصدي للتهديدات السيبرانية" باللغة الإنكليزية) من أجل مساعدة مستخدمي الإنترنت على الوقاية من الإصابة ببرمجيات ضارة ومن أجل التخفيف من أثر الأضرار عند وقوعها. وتتكون هذه الشراكة من وزارة الشؤون الداخلية والاتصالات في اليابان ومقدمي خدمات الإنترنت (ISP) وباعة المنتجات الأمنية. وقد أدت هذه المبادرات إلى انخفاض عدد الإصابات ببرمجيات ضارة.

وتشمل الأنشطة الرئيسية ما يلي:

- الوقاية من الإصابة ببرمجيات ضارة؛ والتعاون مع مقدمي خدمات الإنترنت؛
- الوقاية من الأضرار الناجمة عن الإصابة ببرمجيات ضارة؛ والتعاون مع مقدمي خدمات الإنترنت؛
- إزالة البرمجيات الضارة؛ والتعاون مع مقدمي خدمات الإنترنت.

الشكل 14: لمحة عن أنشطة مشروع "نشط"



فعالية مشروع "نشط"

بناء على البيانات الساكنة الصادرة في 23 مايو 2016، أُرسل منذ بدء تشغيل مشروع "نشط" 286 إنذاراً إلى مستخدمين لتفادي الإصابة ببرمجيات ضارة، وأوقف 267 320 مخدماً من مخدمات التحكم والسيطرة لتفادي الضرر، وأُرسل 878 1 إنذاراً لمستخدمين لإزالة برمجيات ضارة.

وإضافة إلى العمليات الأساسية، يؤدي مشروع "نشط" دوراً رئيسياً في عمليات الإزالة التي تنظمها الوكالات المكلفة بإنفاذ القوانين في جميع أنحاء العالم. وقد تلقى المشروع قوائم الإصابات بالبرمجيات الضارة، مثل Game over Zeus وVAWTRAK وغيرهما، من الوكالات المكلفة بإنفاذ القوانين، وأعطى القائمة إلى المشاركين من مقدمي خدمات الإنترنت لكي ييسروا إن أمكن إزالة البرمجيات الضارة.

2.2.3 الأنشطة المنفذة في جمهورية كوريا

وضعت جمهورية كوريا خطة وطنية من أربعة أجزاء. ويتضمن الجزء الأول تحسين بنية قطاع أمن المعلومات من خلال العمل على التحول إلى سوق قائم على الأداء، وعلى استحداث نظام مناسب لدفع أسعار عادلة مقابل الحصول على الخدمات المتعلقة بأمن المعلومات. ويشمل ذلك نظاماً لتقييم السعر العادل لخدمة توفير الأمن المتواصل للمعلومات، التي تضمن الأداء الأمني المناسب للمنتجات ذات الصلة.

وإضافةً إلى ذلك، قد تلجأ الحكومات إلى تقديم الحوافز للاستثمار في مجال الأمن، مثل إعطاء الأفضلية للمشاركة في عمليات الشراء وأعمال البحث والتطوير التي تجري على الصعيدين الحكومي والعام، من أجل تحفيز المؤسسات على الاستثمار طوعاً في مجال الأمن وعلى اتخاذ تدابير فعّالة في هذا الصدد. ويتمثل نهج آخر في تحديد وتدعيم الشركات الناشئة العاملة في مجال أمن المعلومات، من خلال توفير الدعم لها مثل عرض مواطن الضعف الأمني، واستحداث منصات اختبار، ودعم الشهادات الدولية في هذا المجال، كي يتسنى للأفكار الممتازة في مجال الأمن أن تنتج شركات ناشئة ناجحة.

3.2.3 الأنشطة المنفذة في منطقة كومنولث الدول المستقلة

قدّم الاتحاد الروسي مساهمة[9] تناولت نتائج مشروع المبادرة الإقليمية لكومنولث الدول المستقلة حول بناء القدرات البشرية في مجال أمن المعلومات. وأقر المشروع بالأهمية العاجلة لبناء القدرات البشرية من أجل تعزيز الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات، وهو ما يستلزم الشراكة مع الأعمال التجارية باعتبارها عميل، ومع نظام التعليم باعتباره طرفاً تعاقدياً، ومع الدول باعتبارها الهيئة التنظيمية للعملية بأسرها.

وعمدت المبادرة الإقليمية لكومنولث الدول المستقلة إلى وضع معيار للقدرات المهنية، التي أشار الاتحاد الروسي إلى أهميتها في مساهمته، بحيث توضع في صدارة إنشاء البرامج التعليمية في مجال تدريب وإعادة تدريب أخصائي أمن المعلومات. ويشمل ذلك ما يلي:

1) القدرات المهنية العامة بما في ذلك القدرة على:
   - تشغيل نظم المعلومات والاتصالات (ICS) باستخدام طرائق ووسائل لضمان سلامتها؛
   - إدارة البرمجيات والمعدات لحماية المعلومات في نظم المعلومات والاتصالات؛
   - إجراء الأعمال المتعلقة بتقييم سلامة نظم المعلومات والاتصالات؛
   - إنشاء نظم معلومات واتصالات محمية وموزّعة.
2) القدرات في مجال تشغيل نظم المعلومات والاتصالات من أجل الحفاظ على سلامتها، بما في ذلك قدرتها على ما يلي:
   - توفير أمن المعلومات (IS) في نظم المعلومات والاتصالات عن طريق البرمجيات والمعدات؛
   - وتوفير أمن المعلومات (IS) في نظم المعلومات والاتصالات باستخدام أساليب تقنية؛
   - وتوفير أمن المعلومات (IS) في نظم المعلومات والاتصالات باستخدام تطبيقات وبرمجيات ومعدات وموارد تقنية معقدة.
3) القدرات في مجال إدارة حماية المعلومات عن طريق البرمجيات والمعدات في نظم المعلومات والاتصالات، بما في ذلك عن طريق توفير المهارات للقيام بما يلي:
   - تشكيل حماية نظم المعلومات والاتصالات في البرمجيات والمعدات؛
   - تنفيذ لوائح الصيانة وإصلاح أدوات البرمجيات والمعدات لحماية المعلومات على أساس جارٍ؛
   - إجراء تحليل للانتهاكات التي تحدث بسبب سماح المستعملين بها في مجال نظم المعلومات والاتصالات والحيلولة دون تكررها.
4) القدرات في مجال تقييم أمن نظم المعلومات والاتصالات:
   - مراقبة كفاءة وفعالية أساليب حماية المعلومات الخاصة بالبرمجيات والمعدات؛
   - تطبيق طرائق وأساليب لإجراء تقييم السلامة لنظم المعلومات والاتصالات في إطار تحليل مراقبة نظم الحماية؛

[9] **الوثيقة 2/369**، "The experience of the CIS countries in the field of experts' professional competences formation on data protection and information security in information and communication systems"، الاتحاد الروسي.

- إجراء تجارب وبحوث في حالة إصدار شهادات للأشياء مع مراعاة المتطلبات المتعلقة بضمان حماية نظم المعلومات والاتصالات؛
- إجراء المراقبة المهمة لحماية نظم المعلومات والاتصالات؛
- اكتساب الخبرات في مجال التحقيق في الحوادث الأمنية.

5) القدرات في مجال تصميم نظم المعلومات والاتصالات المحمية الموزعة:

- إعداد متطلبات نظم المعلومات والاتصالات الآمنة الموزّعة وعلاجها مع مراعاة اللوائح ووثائق التوجيهات القائمة؛
- تصميم نظم معلومات واتصالات محمية موزّعة؛
- تشغيل وصيانة نظم المعلومات والاتصالات الموزّعة مع حماية موارد المعلومات واتخاذ تدابير تنظيمية وتقنية لأمن المعلومات.

4.2.3 الأنشطة المنفذة في النرويج

قدمت النرويج تجربتها الوطنية عن طريق إعداد دراسة لتمهيد الطريق لممارسات الأمن السيبراني الفعّالة وتحسين الصمود السيبراني على المستوى الوطني.[10] وأجرى المركز النرويجي للأمن السيبراني (NorSIS) دراسة لتوفير رؤية معمقة جديدة في ثقافة الأمن السيبراني النرويجية. وتهدف الدراسة إلى تمهيد الطريق لممارسات الأمن السيبراني الفعّالة وتحسين الصمود السيبراني على المستوى الوطني. وشملت الدراسة طريقة تصميم مقياس لثقافة الأمن السيبراني، واستبيان وطني موسع كذلك. ونشر المركز مؤخراً تقريره المعنون "ثقافة الأمن السيبراني النرويجي" الذي يتضمن وصفاً كاملاً للطريقة المتّبعة، إلى جانب النتائج الرئيسية للدراسة الوطنية.

3.3 الشراكات بين القطاعين العام والخاص

خلال دورة الدراسة، تلقت المسألة عدداً من المساهمات من الدول الأعضاء بشأن أهمية التعاون المشترك بين الحكومة والدوائر الصناعية، والشراكات بين القطاعين العام والخاص. وأشارت الدول الأعضاء إلى أن إدارة المخاطر السيبرانية المهددة للبنية التحتية الحرجة تتسم بتعقيد هائل، ولكنها بالغة الأهمية، وفي كثير من الأحيان يتجاوز التصدي لتحديات الأمن السيبراني قدرة الحكومة أو القطاع الخاص على الانفراد بإدارته.

وقدمت **المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية** مساهمة[11] بشأن الأمن السيبراني في الحكومة والدوائر الصناعية، وحددت فيها نهجاً يسمى "خطة الأساسيات السيبرانية". ووُضع هذا النهج بعد تحليل عدد من الهجمات السيبرانية. وبيّن هذا التحليل أنه، في كثير من الحالات، لو اتخذ عدد ضئيل من الاحتياطات لأمكن التخفيف من حدة الهجمات أو إرغام الخصم على بذل جهود أكبر بكثير. وقد أعدت حكومة المملكة المتحدة خطة الأساسيات السيبرانية بالاشتراك مع دوائر الصناعة للوفاء بوظيفتين. فهي تعطي بياناً واضحاً للضوابط الأساسية التي ينبغي أن تنفذها جميع المنظمات للتخفيف من مخاطر التهديدات الشائعة على شبكة الإنترنت ضمن سياق خطوات الحكومة العشر في مجال الأمن السيبراني. وهي توفر، من خلال إطار الضمان، آلية للمنظمات كي تبيِّن للعملاء والمستثمرين وشركات التأمين وغيرها من الجهات أنها اتخذت هذه الاحتياطات الأساسية. ومع أن الجزء الرئيسي من إعداد

[10] الوثيقة SG2RGQ/204، "Creating a metric for cyber security culture"، النرويج.
[11] الوثيقة 2/228، "Cybersecurity in government and industry" المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية.

الخطة جرى في المملكة المتحدة، ينطبق قدر كبير من الأعمال، بصورة مماثلة، على أي بلد ويجوز للجميع الاطلاع على تفاصيل الخطة.

وإضافةً إلى ذلك، قدمت **الولايات المتحدة الأمريكية** مساهمة[12] بشأن أهمية التشارك مع القطاع الخاص لإدارة المخاطر السيبرانية. وأشارت الولايات المتحدة في هذه المساهمة إلى أن الشراكات بين القطاعين العام والخاص عنصر أساسي للحماية الفعّالة للبنية التحتية الحرجة، ولتجاوز العثرات، وللإدارة الكلية للمخاطر السيبرانية. وشددت الولايات المتحدة في مساهمتها على أهمية الشراكة مع القطاع الخاص لإدارة المخاطر السيبرانية؛ وعرضت النهج القائم على إشراك المجتمع ككل، الذي تتبعه الولايات المتحدة لإدارة المخاطر السيبرانية، وشددت على الأدوات الرئيسية التي تدعم هذا النهج؛ وقدمت أمثلة عملية لتنفيذ شراكات فعلية بين القطاعين العام والخاص.

وشددت أيضاً مساهمة **اليابان**[13] على الموضوع المشترك المتمثل في أهمية تعاون الحكومة مع شركات القطاع الخاص بما يتيح تبادل المعارف والمعلومات وأفضل الممارسات لبناء ثقافة الأمن السيبراني. وشددت اليابان في مساهمتها على الجوانب الأربعة لمجالات التركيز الخاصة بها، وهي "الشبكة" و"الأفراد" و"التكنولوجيا" و"الشراكة والتعاون على الصعيد الدولي" لضمان موثوقية شبكات المعلومات والاتصالات. ومن منظور "الشبكة"، شجعت اليابان على تبادل المعلومات بين مشغلي الاتصالات. وعلى سبيل المثال، قام 19 من أبرز مقدمي خدمات الإنترنت ومشغلي الاتصالات في اليابان، في عام 2002، بتدشين مركز Telecom-ISAC (مركز تبادل وتحليل المعلومات) طوعاً في اليابان[14]، ويقوم المركز بجمع الدراسات التحليلية ونشر معلومات الأمن بين الأعضاء، مثل مواطن الضعف والحوادث والتدابير المضادة وأفضل الممارسات. ومن منظور "الأفراد"، زادت اليابان وعي مستخدمي الإنترنت من خلال موقع إلكتروني وحلقات دراسية وغير ذلك. ومن منظور "التكنولوجيا"، شجعت اليابان البحوث المتقدمة ومشاريع التنمية مثل مشروع PRACTICE. ومن خلال إيلاء الاهتمام لهذه الجوانب، ساهمت اليابان في استحداث شبكات موثوق بها لتكنولوجيا المعلومات والاتصالات، وعززت التعاون الدولي.

[12] الوثيقة 2/198، "التشارك مع القطاع الخاص لإدارة المخاطر السيبرانية"، الولايات المتحدة الأمريكية.

[13] الوثيقة 2/90، "Sharing knowledge, information and best practice for developing a culture of cybersecurity"، اليابان.

[14] https://www.telecom-isac.jp/english/index.html.

4 الفصل 4 - حماية الأطفال على الخط (COP)

يتعلق هذا القسم بالبند (ح) من الاختصاصات المتصلة بالمسألة 3/2 الذي يدعو إلى جملة *أمور* منها ما يلي:

ح) ***مواصلة جمع التجارب والاحتياجات الوطنية في مجال حماية الأطفال على الخط، بالتنسيق مع الأنشطة الأخرى ذات الصلة.***

وتناولت في الوقت نفسه إحدى المساهمات[15] البند (ز) من الاختصاصات المتصلة بالمسألة 3/2، الذي ينص على ما يلي:

ز) ***دراسة السبل والوسائل اللازمة لمساعدة البلدان النامية، مع التركيز على أقل البلدان نمواً فيما يتعلق بالتحديات المتصلة بالأمن السيبراني.***

في عصر الإنترنت الذي نعيشه اليوم، يُعتبر الأمان على الخط مسألة من الأهمية بمكان، ويعد بوجه خاص استخدام الأطفال للإنترنت على نحو آمن ومأمون مسألة مهمة للغاية. وللأطفال احتياجات ونقاط ضعف معينة فيما يتعلق بالأمان على الخط، مقارنة بالراشدين، ويجب الإقرار بهذا الفرق.

ويقضي الأطفال، أكثر فأكثر، مزيداً من الوقت في العمل على الإنترنت واللعب على الحواسيب. ولوسائط التواصل الاجتماعي الحصة الأكبر في هذا الصدد. وفي بعض الأحيان، يجهل الأهل أن الأولاد يفصحون عن معلوماتهم الشخصية أثناء استخدامهم وسائط التواصل الاجتماعي، مما يجعلهم عرضة للمعتدين على الخط.

ومن أجل تذليل التحديات، تنظم العديد من البلدان حملات توعية ترمي إلى تثقيف الوكالات الحكومية، والقطاع الخاص، والمربين، والمواطنين الأفراد (الأهل والأطفال) لتمكينهم من الكشف عن المشاكل المحتملة وفهم أدوارهم ومسؤولياتهم في استحداث فضاء سيبراني أكثر أماناً للأطفال.

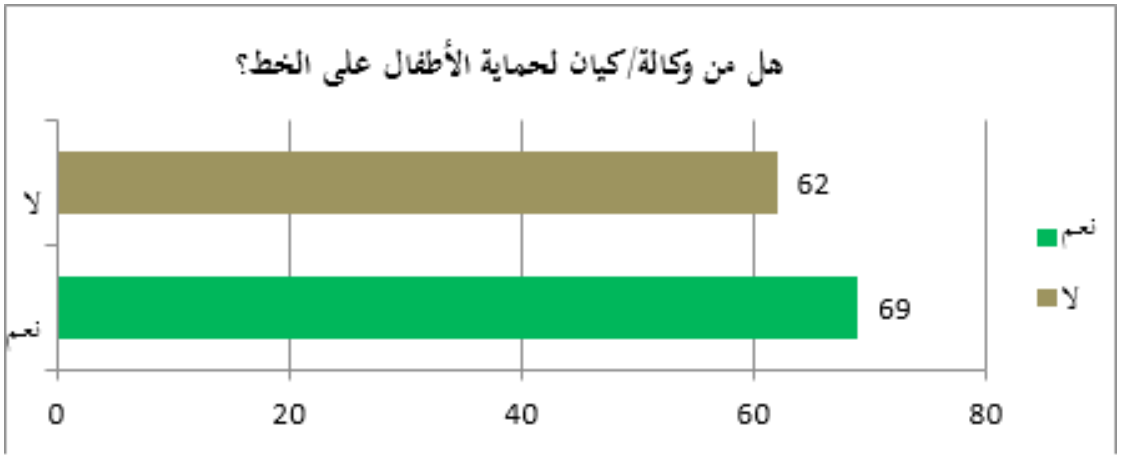
1.4 نتائج الاستقصاء المتعلق بحماية الأطفال على الخط

تناول الاستبيان المتعلق بحماية الأطفال على الخط (COP)، الذي تضمن مسائل استُمدت من مساهمات الدول الأعضاء (ولا سيما أستراليا، والمملكة المتحدة، وفانواتو) عدداً من المسائل الرئيسية المهمة بما فيها الجوانب التشريعية والاستراتيجية لحماية الأطفال على الخط، وأساليب الإبلاغ عن الحوادث، ووسائل الحماية التقنية. وردّ 131 بلداً على الاستبيان المتعلق بحماية الأطفال على الخط. وتبين نتائج الاستبيان أن 37 بلداً فقط من أصل 131 بلداً مجيباً أكد تحليه باستراتيجية وطنية لحماية الأطفال على الخط. وفي الوقت نفسه، نلاحظ أن 101 بلد تتخذ تدابير لحماية الأطفال على الخط. ومع أن نسبة عالية من البلدان المجيبة تتخذ تدابير لحماية الأطفال على الخط، لا يتحلى سوى 78 بلداً بتشريعات لحماية الأطفال على الخط، ومع أن البلدان الأخرى تفتقر إلى هذا النوع من التشريعات إلا أنها تتخذ إجراءات أخرى مثل وسائل الحماية التقنية لحماية الأطفال على الخط.

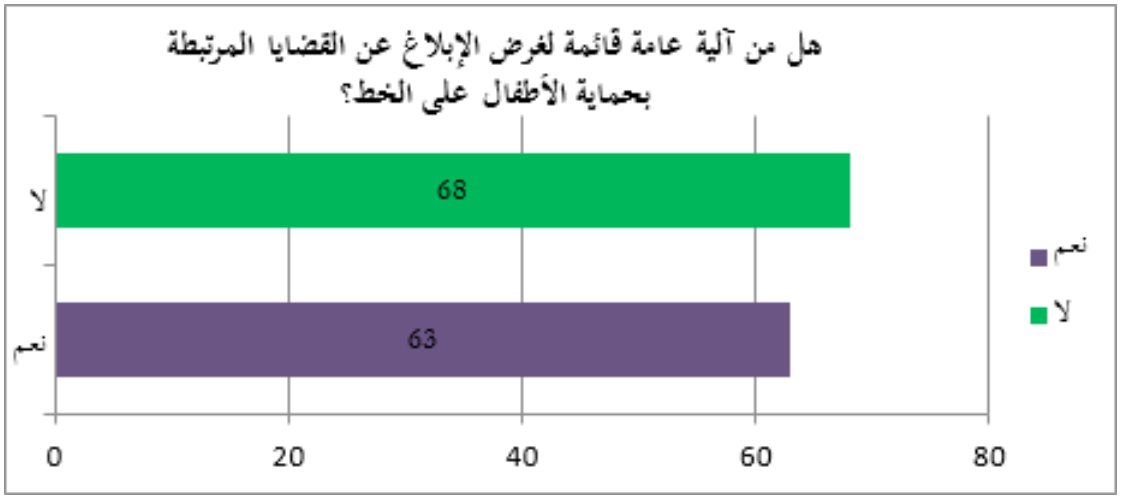
وعلاوةً على ذلك، هناك وكالات حكومية مكلفة بحماية الأطفال على الخط في 69 بلداً من أصل 131 بلداً مجيباً. إن الفرق واضح جداً بين عدد البلدان التي استحدثت كيانات أو وكالات لحماية الأطفال على الخط والبلدان التي تفتقر إلى هذا النوع من الكيانات. فمن الواضح أن هناك عدداً أكبر من البلدان التي لديها كيانات لحماية الأطفال. وصحيح أن هذه الكيانات موجودة في 69 بلداً، إلا أن 63 بلداً فقط تتحلى بنظام متين يتيح الإبلاغ عن الحالات المرتبطة بحماية الأطفال على الخط.

[15] https://www.itu.int/md/D14-SG02-C-0202/en.

الشكل 15: هل من وكالة/كيان لحماية الأطفال على الخط؟

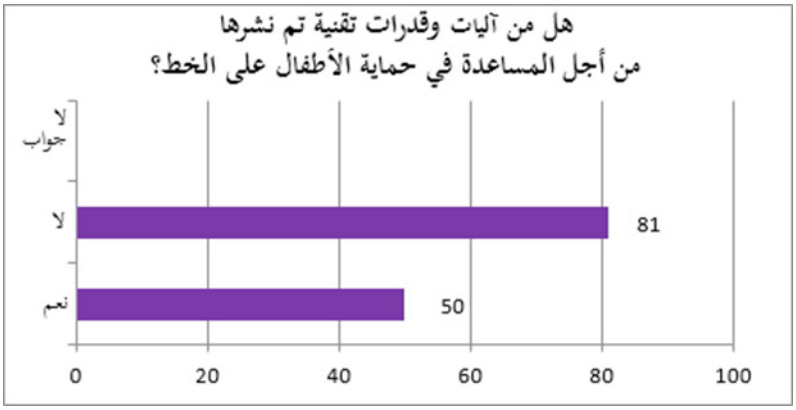


الشكل 16: هل من آلية عامة قائمة لغرض الإبلاغ عن القضايا المرتبطة بحماية الأطفال على الخط؟



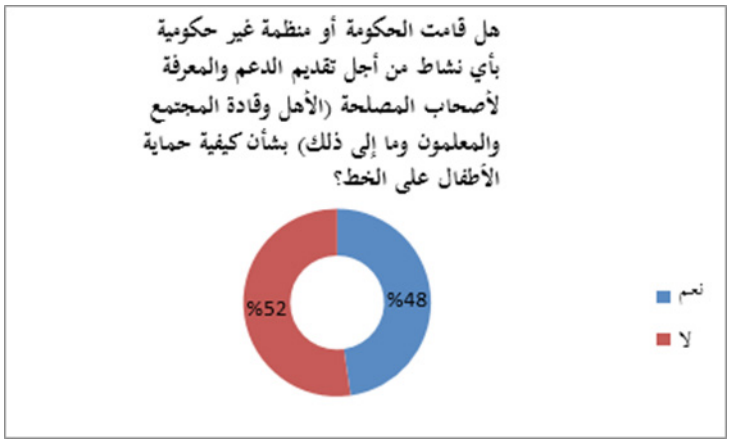
يتمتع 50 بلداً من هذه البلدان بالقدرات التقنية اللازمة للمساعدة على حماية الأطفال على الخط، مما قد يثير أسئلة بشأن الوكالات القائمة المعنية بحماية الأطفال على الخط، وبشأن طبيعة عملها والمهام المسندة إليها، أو قد يثير التساؤل عما إذا كانت حداثة هذه الوكالات هي السبب وراء قلة أنظمة الإبلاغ أو القدرات التقنية اللازمة للمساعدة على حماية الأطفال على الخط. وقد يكون السبب أن هذه الوكالات متخصصة في جميع المسائل المتعلقة بالأطفال وليس بحماية الأطفال حصراً. وهذا يقلل من التركيز على المخاطر التي يواجهها الأطفال على الخط، لأن الانتباه سيولى أيضاً للمخاطر الأخرى التي يواجهها الأطفال بوجه عام.

الشكل 17: هل من آليات وقدرات تقنية تم نشرها من أجل المساعدة في حماية الأطفال على الخط؟



فيما يخص الأنشطة التي تضطلع بها المنظمات الحكومية وغير الحكومية لتوفير المعارف ودعم أصحاب المصلحة على استخدام أساليب حماية الأطفال على الخط، تُظهر نتائج الاستبيان أن 62 بلداً شاركوا في مثل هذه الأنشطة في حين لم يشارك 68 بلداً، وهذان العددان متقاربان نسبياً.

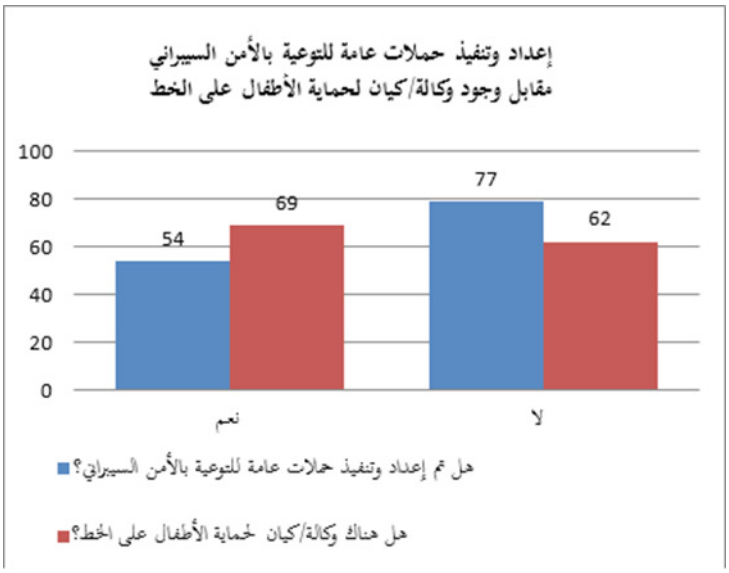
الشكل 18: هل قامت الحكومة أو منظمة غير حكومية بأي نشاط من أجل تقديم الدعم والمعرفة لأصحاب المصلحة (الأهل وقادة المجتمع والمعلمون وما إلى ذلك) بشأن كيفية حماية الأطفال على الخط؟



إذ يتعذر تناول مسألة حماية الأطفال على الخط دون التشديد على الدور التربوي المتمثل في نشر ثقافة داعمة لهذا النوع من الحماية في صفوف الجهات المعنية، وإذ تمت مناقشة مسألة حماية الأطفال على الخط في **القسم 2** الذي يتناول إذكاء الوعي بالأمن السيبراني بوصفه المسألة الرئيسية التي تُعد جزءاً لا يتجزأ من الأمن السيبراني، يناقش هنا، بمزيد من التفصيل، الدور التربوي فيما يخص حماية الأطفال على الخط وإذكاء وعي الأهل والمعلمين على حد سواء، للمساعدة على تحديد نقاط الضعف التي أوليت اهتماماً تاماً.

وكان السؤال المتعلق بالدور التربوي الخاص بحماية الأطفال على الخط سؤالاً عاماً يراد به معرفة ما إذا كانت الدول الأعضاء قد أعدت برامج تربوية لحماية الأطفال على الخط. وقد أظهرت النتائج أن 54 بلداً فقط من أصل 131 قد أعدت هذا النوع من البرامج.

الشكل 19: إعداد وتنفيذ حملات عامة للتوعية بالأمن السيبراني مقابل وجود وكالة/كيان لحماية الأطفال على الخط



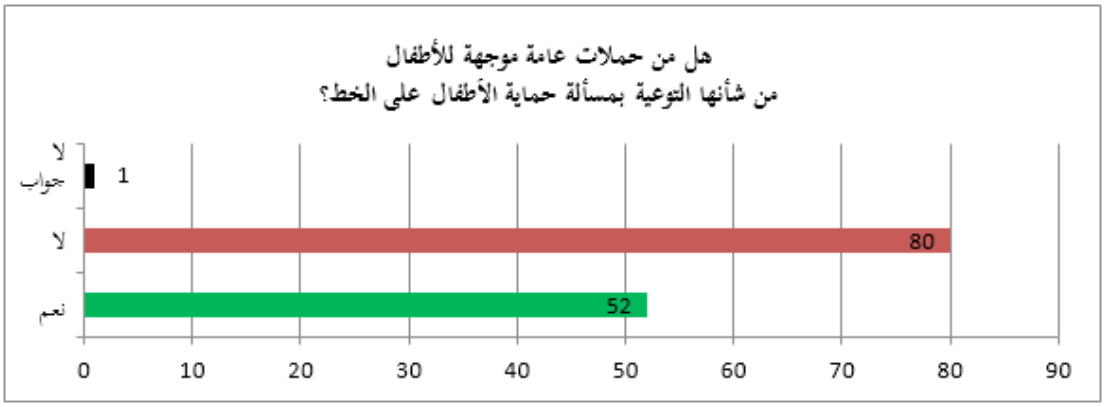
تجدر الإشارة إلى أن وجود كيانات معنية بحماية الأطفال على الخط في بلد معين لا يعني أن هذه الكيانات تؤدي الدور التربوي اللازم أيضاً. وإضافةً إلى ذلك، فإن عدم وجود كيانات متخصصة في حماية الأطفال على الخط لا يعني أن هذه البلدان مقصرة في أداء دورها التربوي في هذا المجال. والدليل على ذلك أن هذه الكيانات موجودة في 69 بلداً. إلا أن هذه البلدان لا يعتمد جميعها برامج تربوية لحماية الأطفال على الخط. ومع أن هناك 62 بلداً تفتقر إلى كيانات متخصصة في حماية الأطفال على الخط، فبعضها قد أعد ونفذ بالفعل برامج لإذكاء الوعي بمسألة الحماية.

وعند إمعان النظر في طبيعة هذه البرامج التربوية وفي المجموعات التي تستهدفها، يتبين أن المجموعة الأكثر استهدافاً هي الأطفال، إذ أكد 52 بلداً اعتماد برامج تربوية تستهدف الأطفال، في حين كان 78 بلداً يفتقر إلى برامج تستهدف الأطفال تحديداً.

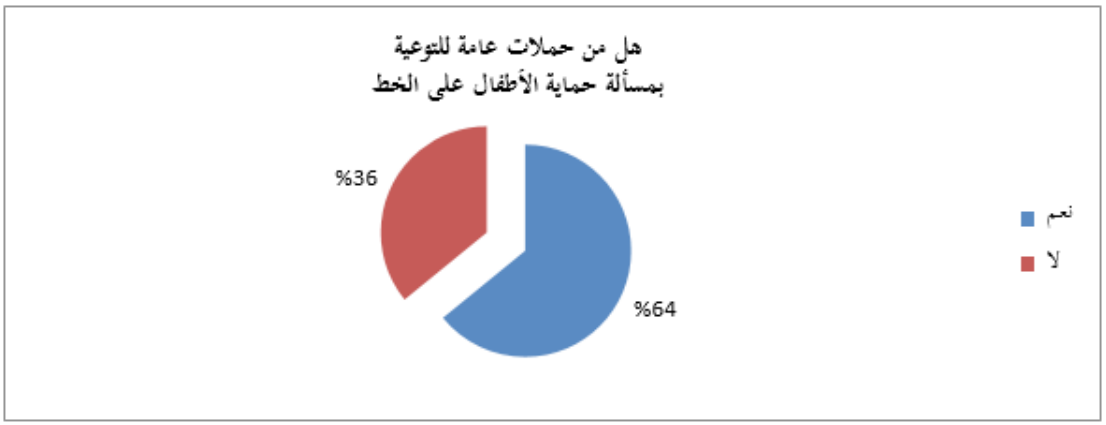
وتُظهر نتائج الاستبيان أن 50 بلداً من أصل 131 أعدّت برامج تربوية للأهل، إلا أن فئة المعلمين هي الفئة الأقل استهدافاً إذ لا يتحلى سوى 47 بلداً من أصل 131 ببرامج تربوية للمعلمين.

وفيما يخص حملات التوعية، شن 84 بلداً من أصل 131، أي ما يمثل 64,12 في المائة من البلدان، حملات توعية أُعدت خصيصاً لحماية الأطفال على الخط. وتتفق هذه النتيجة مع نتائج دعوة الدول الأعضاء إلى تحديد المسائل التي تعطيها الأولوية عندما تتناول الأمن السيبراني، إذ احتلت مسألة حماية الأطفال على الخط المرتبة الثانية بعد أمن الإنترنت واحتلت المرتبة الأولى من بين القضايا التي خُصصت لها حملات توعية في الدول الأعضاء المجيبة.

الشكل 20: الحملات العامة الموجهة للأطفال للتوعية بمسألة حماية الأطفال على الخط



الشكل 21: الحملات العامة للتوعية بمسألة حماية الأطفال على الخط



أعدّ 77 بلداً برامج توعية موجهة للأطفال حصراً، في حين لم يخصص سوى 54 بلداً هذا النوع من البرامج للأطفال فقط. ويظهر من الاستبيان أن مجموعة الراشدين حصلت على نصيب عادل من برامج التوعية أو البرامج التربوية الرامية إلى حماية الأطفال على الخط، إذ أكد 74 بلداً أن لديها هذا النوع من البرامج الموجهة للراشدين وأشار 57 بلداً إلى عدم تحليها بذلك. وبناء على ما تقدم، نشير إلى أنه من المهم استهداف كلا الراشدين والأطفال. فلا يمكن تحقيق التوعية الكاملة دون نشرها في مختلف الشرائح الاجتماعية التي ترتبط بصورة مباشرة أو غير مباشرة بمسألة حماية الأطفال على الخط. فنظراً للمخاطر التي يمكن مواجهتها على الخط، لن تكون زيادة وعي الأطفال كافية دون توعية الراشدين أيضاً بهذه المخاطر وبالتدابير التي يجب أن يتخذوها لضمان حماية الأطفال على الخط.

2.4 الاستراتيجيات والحلول التقنية لحماية الأطفال على الخط

حُدّدت بعض الاستراتيجيات والحلول التقنية الممكنة في المساهمات الواردة خلال فترة دراسة المسألة 3/2 التي تتناولها لجنة الدراسات 2. وعلى النحو المشار إليه في وثائق مختلفة، قد يساهم فعلاً التعاون بين مختلف أصحاب المصلحة، وحملات التوعية، ومشاركة دوائر الصناعة، والجهود التشريعية، في تحديد الاستراتيجيات والسياسات المتعلقة بأمن الأطفال على الخط. أولاً، تستغرق عملية تحول الاستراتيجية إلى أفعال وقتاً طويلاً وتبدأ بجمع المعلومات المهمة. وتمت الموافقة على مساهمة[16] مقدمة من المملكة المتحدة وأستراليا وفانواتو إلى اجتماع لجنة الدراسات 2 لقطاع تنمية الاتصالات المعقود في سبتمبر 2014، خلال هذا الاجتماع، وتقترح المساهمة مسار عمل لبدء تقديم المساعدة إلى الدول الأعضاء فيما يخص حماية الأطفال على الخط (COP). واستناداً إلى هذه المساهمة، تقترح هذه البلدان مجتمعة عدداً من الأسئلة الواجب طرحها على الدول الأعضاء كي يُفهَم بشكل أكثر شمولاً كيفية إقدام الدول الأعضاء على حماية الأطفال على الخط على الصعيد الوطني. ثانياً، لا تكون عملية وضع الحلول التقنية عملية جامدة أبداً؛ بل هي مسار حيوي يتطلب عملية تفكر وتكيف متواصلة. وعلى سبيل المثال، قدمت **أستراليا وبابوا غينيا الجديدة ودولة ساموا المستقلة والمملكة المتحدة وجمهورية فانواتو**[17]، إثر مناقشات اجتماع فريق المقررين المعين بالمسألة 3/2 في عام 2015، بعض المسائل المعدلة المتعلقة بحماية الأطفال على الخط. واقتُرح تقديم هذه الأسئلة إلى الجلسة العامة للجنة الدراسات لغرض تعميمها على الدول الأعضاء كي تجيب عليها بنفسها أو كجزء من استبيان أكثر تفصيلاً. وتركز هذه الأسئلة على الأنشطة المتعلقة بحماية الأطفال على الخط على المستوى الوطني، بما في ذلك التشريع وآلية الإبلاغ والقدرات وتوفير الدعم والمعارف لأصحاب المصلحة. وإضافةً إلى ذلك، وتأييداً للقرار 67 الصادر عن المؤتمر العالمي لتنمية الاتصالات (المراجَع في دبي، 2014)[18]، تقترح المملكة المتحدة وأستراليا وجمهورية فانواتو مجتمعة تقريراً تقنياً بعنوان "أفضل الممارسات لدعم الأهل في توفير حماية الأطفال على الخط"، وتقترح أخذ جميع أصحاب المصلحة بعين الاعتبار (وهم على سبيل المثال لا الحصر الحكومات، والأهل، والمدارس، ومنظمات حماية الطفل، والشرطة، وخدمات الطوارئ، والمشغلون، ومقدمو خدمات الإنترنت). ويركز هذا التقرير على تحديد الأدوار والمسؤوليات، وعلى جمع أفضل الممارسات وعلى أهمية اتباع نهج قائم على الأدلة. وأخيراً، من المهم الإشارة إلى أنه ينبغي، أثناء إعداد هذا التقرير، تقديم استبيان لجمع المعلومات عما يجري في شتى البيئات الوطنية، وينبغي تعميم المشروع الأول للاستبيان على أصحاب المصلحة ليأخذوا علماً به ويقدموا التعليقات بشأنه.

وينبغي إكمال الاستراتيجيات الوطنية بحلول تقنية: فعلى النحو المشار إليه من أكاديمية A.S. Popov الوطنية للاتصالات في أوديسا (أوكرانيا)[19]، من أجل تنفيذ أحد بنود المبادرة الإقليمية بشأن حماية الأطفال على الخط بخصوص منطقة كومنولث الدول المستقلة، بذلت الأكاديمية الجهود لجمع البيانات المتعلقة بالحلول التقنية المتبعة حالياً لحماية الأطفال على الخط (www.contentfiltering.info). وفي هذا الصدد، وضع فريق الخبراء قائمة بالحلول التقنية المتاحة بالاستناد إلى شتى الخصائص مثل نوع التنفيذ (برمجية أو عتاد أو سحابة)؛ ومدى التوافق مع أنظمة التشغيل (منصة واحدة، أو شامل للمنصات، أو مستقل عن المنصات)؛ ونوع نظام التشغيل (Windows أو Unix أو Marcos أو Android أو IoS)؛ ونوع الدعم (نظام مدعوم بالكامل، أو نظام مدعوم جزئياً، أو نظام غير مدعوم)؛ وكيفية التحكم (عن بُعد، أو محلي، أو غير موجود)؛ ونوع الأمن الداخلي (نظام محمي أو غير محمي).

---

16 الوثيقة 2/78، "Support of the Resolution on child online protection" ، المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية وأستراليا وفانواتو.

17 الوثيقة SG2RGQ/56، "Proposed questions on child online protection"، أستراليا وبابوا غينيا الجديدة ودولة ساموا المستقلة والمملكة المتحدة وجمهورية فانواتو.

18 القرار 67 للمؤتمر العالمي لتنمية الاتصالات بشأن "دور قطاع تنمية الاتصالات للاتحاد الدولي للاتصالات في حماية الأطفال على الخط"، متاح في العنوان التالي: https://www.itu.int/pub/D-TDC-WTDC-2014.

19 الوثيقة 2/322، "A database with data on existing technical solutions for child online protection (Contentfiltering.info)" أكاديمية A. S. Popov Odessa الوطنية للاتصالات (أوكرانيا).

وتم إدخال كل حل من الحلول التقنية الواردة في القائمة في حاسوب أو جهاز متنقل (وفي حالة المنتجات المدفوعة، تم الحصول على إذن من المطور بإجراء اختبارات)، بهدف اختبار كل وظيفة بصورة دقيقة. وأُعد تقرير عن اختبار كل حل من الحلول وأُدرج في قاعدة بيانات الخدمة contentfiltering.info. وحالما تُدرج البيانات الخاصة بكل منتج في قاعدة البيانات، يتحقق منها مطورو النظام بانتظام، ويقومون عند الاقتضاء بتحديثها وإكمالها. وإضافةً إلى ذلك، اختيرت برمجية Contentfiltering.info على أساس توصيات بشأن اختيار أفضل نظام لغربلة المحتوى فيما يخص مستخدم معين/منظمة معينة. وتتضمن وحدتين:

أ) وحدة للمستخدمين (يمكن النفاذ إليها بحرية) لأغراض تحديد مستوى مهارات المستخدم وتحديد الاحتياجات واختيار نظام لغربلة المحتوى؛

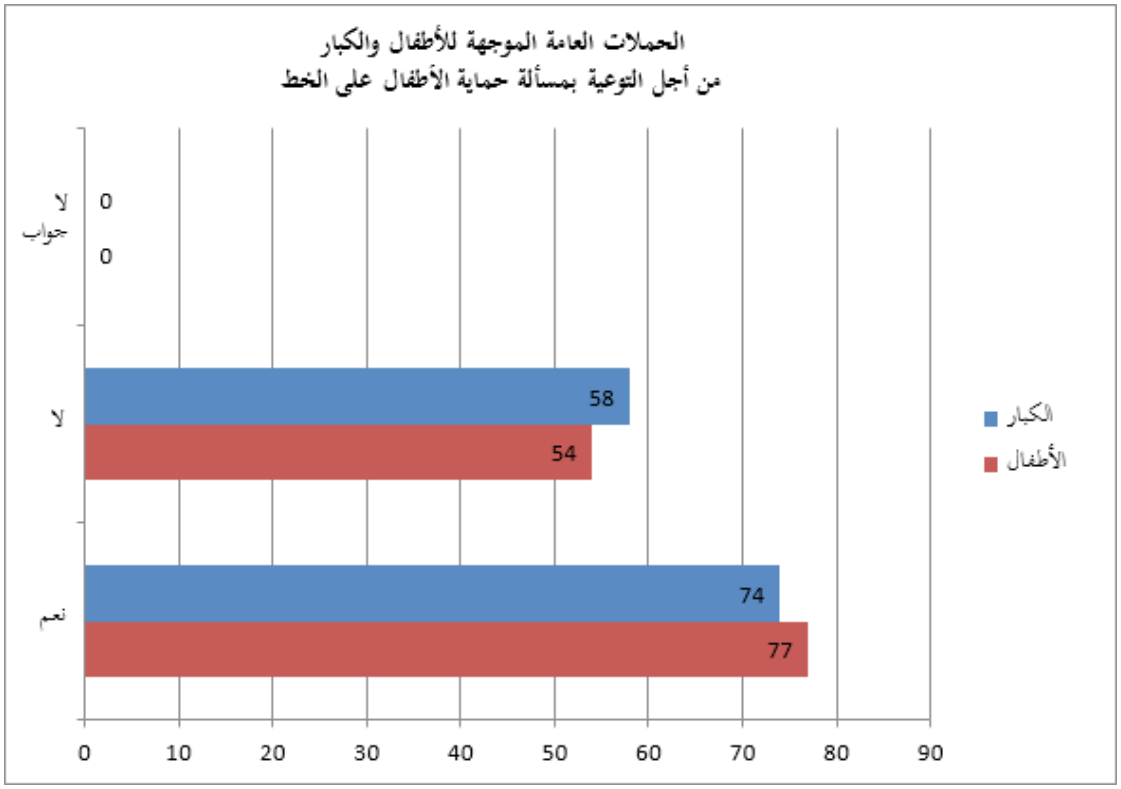
ب) وحدة للخبراء (للخبراء المرخص لهم فقط) لأغراض إدراج البيانات المتعلقة بالحلول التقنية المتبعة لحماية الأطفال على الخط.

وقدمت أكاديمية A.S. Popov الوطنية للاتصالات في أوديسا (أوكرانيا)[20] معلومات إضافية عن دورة تعليمية عن بُعد متعددة الوسائط عن الاستخدام الآمن لموارد الإنترنت (https://onlinesafety.info) نُظمت كجزء من المبادرة الإقليمية للاتحاد بشأن "إنشاء مركز لحماية الأطفال على الخط من أجل منطقة كومنولث الدول المستقلة".

ويوضح **الشكل 22** أنه في حين أطلقت بعض البلدان حملات للتوعية العامة لحماية الأطفال على الخط، ثمة عدد ليس بالقليل من البلدان لم يُجر مثل هذه الحملات.

[20] الوثيقة 2/156، "دورة تعليمية عن بُعد متعددة الوسائط عن الاستخدام الآمن لموارد الإنترنت"، أكاديمية A. S. Popov Odessa الوطنية للاتصالات (أوكرانيا).

الشكل 22: الحملات العامة الموجهة للأطفال والكبار من أجل التوعية بمسألة حماية الأطفال على الخط



1.2.4 التوعية بمسألة حماية الأطفال على الخط، والأنشطة المرتبطة بذلك

تشدد المساهمة[21] المقدمة من **جمهورية كوريا** على الجهود المختلفة المبذولة على الصعيد الوطني في شتى البلدان، فيما يخص الأطر القانونية، والحملات الاجتماعية، والتعليم على الخط، من أجل حماية الأطفال على الخط. وعلى النحو المشار إليه في المساهمة، باتت مسألة الاستخدام الآمن للإنترنت في صفوف الأطفال مسألة مهمة في العديد من البلدان نظراً إلى انخفاض متوسط عمر الأطفال الذين يمكنهم النفاذ إلى الإنترنت. وقد شددت مساهمة كوريا، بوجه خاص، على ضرورة اتخاذ تدابير طوعية للتنظيم الذاتي من أجل إكمال التدابير القانونية والإلزامية. وصحيح أن هذه التدابير قد تؤدي إلى نتائج ظاهرة بسرعة، إلا أنه يحتمل أن تكون أيضاً تقييدية بصورة مفرطة، مؤدية بذلك إلى انتهاك حرية الأفراد أو استقلالية مستخدمي الخدمات. وعلى سبيل المثال، فقد أثار التدبير القانوني الذي اتخذته كوريا لمنع القاصرين من النفاذ إلى الألعاب على الخط بعد منتصف الليل جدلاً حاداً فيما يخص صحة هذا التدبير وفعاليته. وبالتالي، يجب أن تكمل التدابير القانونية والإلزامية المتخذة في هذا الشأن ببرامج للتعليم والتوعية بالتعاون مع مختلف أصحاب المصلحة.

وترتبط إحدى المسائل الأخرى التي أثارتها جمهورية كوريا بصعوبة الفصل بين مقدمي الخدمات ومستخدميها. فقد يؤكد الأهل أنه يجب على مقدمي الخدمات بذل مزيد من الجهود لضمان أمن الأطفال على الخط أثناء توفير خدماتهم. ولكن قد يدفع بعض مقدمي الخدمات بالقول إن التوجيه والتوعية هما من مسؤولية الأهل والمربين والأوصياء. ويمكن أن تساعد الحملات والبرامج الاجتماعية على تحديد التدابير التي ستتيح تعزيز التعاون بين جميع أصحاب المصلحة المعنيين وتشجعهم على المشاركة بصورة نشطة في المساعي المبذولة بترويج من الحكومة لضمان الأمن على الخط.

[21] الوثيقة 2/362، "Proposed text for inclusion in Chapter 6 (Child Online Protection) of the Final Report"، جمهورية كوريا.

وفي سياق أقل البلدان نمواً، تشدد مساهمة[22] **جمهورية غامبيا** على الحاجة الملحة إلى الشروع في حماية الأطفال على الخط حماية شاملة، كجزء من الأطر الوطنية للأمن السيبراني. وقد بدأت أقل البلدان نمواً تستفيد للتو من وجود شبكة إنترنت سريعة على منصات مختلفة أرخص من حاسوب سطح المكتب أو الحاسوب المحمول التقليديين. ولا تبرز أهمية التعاون الدولي على صعيد تعميم التوعية بالمسائل المذكورة فحسب، وإنما تبرز أيضاً فيما يخص اتساق السياسات الدولية وتعزيز الأنشطة بغية الاستمرار في توطيد التعاون الدولي. وتدعو هذه المساهمة إلى إدماج حماية الأطفال على الخط في الإطار الوطني للأمن السيبراني وإلى التركيز على المسائل القانونية والتقنية والتنظيمية والإجرائية فضلاً عن بناء القدرات والتعاون الدولي.

وفي الختام، يشدد بيان الاتصال الموجه من نشاط التنسيق المشترك بشأن حماية الأطفال على الخط لقطاع تقييس الاتصالات،[23] على أهمية تبادل المعلومات بين الأعضاء للفت الانتباه إليها في إطار المسألة 3/2 لقطاع تنمية الاتصالات. ويورد أيضاً إقراره بالجهود الوطنية التي تبذلها جمهورية كوريا وغامبيا فضلاً عن المنظمات غير الحكومية من قبيل Defz Kidz.

2.2.4 استراتيجيات حماية الأطفال على الخط

يمكن للدول الأعضاء اعتماد الاستراتيجيات التالية المستمدة من المساهمات المقدّمة.

- التعاون بين أصحاب المصلحة المعنيين المختلفة؛
- إطلاق حملات التوعية؛
- إشراك أهل الصناعة؛
- تعزيز الجهود التشريعية؛
- وضع آلية إبلاغ مناسبة؛
- تنمية قدرات أصحاب المصلحة المعنيين ذات الصلة؛
- توفير الدعم والمعارف لجميع أصحاب المصلحة المعنيين؛
- تصميم آليات لإشراك جميع أصحاب المصلحة المعنيين (بما في ذلك على سبيل المثال لا الحصر الحكومات والآباء والمدارس ومنظمات حماية الأطفال والشرطة وخدمات الطوارئ وشركات تشغيل الاتصالات ومقدمو خدمات الإنترنت)؛
- تحديد أدوار ومسؤوليات واضحة لأصحاب المصلحة المعنيين — من يفعل ماذا ومتى وكيف؛
- جمع بيانات عن أفضل الممارسات بشأن الحلول التقنية القائمة لحماية الأطفال على الخط؛
- نشر المعلومات ذات الصلة بين أصحاب المصلحة المعنيين؛
- تنفيذ نهج مستند إلى الأدلة.

[22] الوثيقة SG2RGQ/104، "A case to adopt child online protection initiatives across LDCs" جمهورية غامبيا.

[23] الوثيقة 2/289، "Liaison statement from ITU-T JCA-COP to ITU-D SG2 Question 3/2 on Child Online Protection Ini-tiatives" نشاط التنسيق المشترك بشأن حماية الأطفال على الخط لقطاع تقييس الاتصالات.

5 الفصل 5 - نتائج ورش العمل المتعلقة بالأمن السيبراني

يتعلق هذا القسم بالبند (ط) من الاختصاصات المتصلة بالمسألة3/2 ، الذي يدعو إلى جملة أمور منها:

ط) عقد جلسات مخصصة وحلقات دراسية وورش عمل لتبادل المعارف والمعلومات وأفضل الممارسات بشأن التدابير والأنشطة الفعّالة والناجعة والمفيدة لتعزيز الأمن السيبراني باستعمال نتائج الدراسة، على أن تُعقد هذه الاجتماعات، قدر الإمكان، في نفس الوقت والمكان الذي تعقد فيه اجتماعات لجنة الدراسات 1 أو اجتماعات فريق المقرر المعني بالمسألة.

من مظاهر التعاون بين لجنة الدراسات 2 لقطاع تنمية الاتصالات ومكتب تنمية الاتصالات والقطاعات الأخرى ودوائر الصناعة والهيئات الأكاديمية مجموعة من ورش العمل التي عُقدت خلال فترة الدراسة. ويرد عدد من المساهمات في **الملحق 2**. وفيما يلي ملخص لمظاهر التعاون هذه.

1.5 ورشة العمل الأولى المتعلقة بالأمن السيبراني (8 سبتمبر 2015)

عُقدت ورشة العمل المتعلقة بالأمن السيبراني بعنوان "تحديات الأمن السيبراني العالمي – التعاون من أجل التعزيز الفعّال للأمن السيبراني في البلدان النامية"[24]، بعد ظهر يوم 8 سبتمبر 2015، بالاقتران مع اجتماعات لجنة الدراسات 2 لقطاع تنمية الاتصالات ولجنة الدراسات 17 (الأمن) لقطاع تقييس الاتصالات، وقبل اجتماع لجنة الدراسات 2 لقطاع تنمية الاتصالات بشأن المسألة 3/2.

الغرض من ورشة العمل

تمثل الغرض من ورشة عمل الأمن السيبراني في تبادل أفضل الممارسات بشأن النُهج المتخذة على المستويات الدولية والإقليمية والوطنية لتعزيز بناء قدرات الأمن السيبراني. وهدف الورشة هو تناول شواغل البلدان النامية ذات الصلة ببناء قدرات الأمن السيبراني، وتحديد طرائق ابتكارية وعملية يمكن للمنظمات الدولية والإدارات المعنية والقطاع الخاص التعاون بها من أجل تبديد تلك الشواغل.

جدول الأعمال

ألقى السيد يوشي توريغو (نائب مدير مكتب تنمية الاتصالات) والسيد رينارد شول (نائب مدير مكتب تقييس الاتصالات) ملاحظات افتتاحية. تضمّن البرنامج جلستين شملتا عروضاً وحلقات نقاش:

- الجلسة 1: أفضل الممارسات لاتباع نهج استراتيجي متعدد الطبقات لتعزيز الأمن السيبراني بصورة ناجعة في البلدان النامية (3 عروض وحلقة نقاش).
- الجلسة 2: التحديات التي تواجهها البلدان النامية؛ والتعاون الدولي من أجل تعزيز المبادرات المتعلقة بالأمن السيبراني (3 عروض وحلقة نقاش).

المناقشات واستنتاج ورشة العمل

قُدمت في ورشة العمل عروض مفيدة وحافلة بالمعلومات، وحلقات نقاش ضمت أسئلة وأجوبة عن أفضل الممارسات لاتباع نهج استراتيجي متعدد الطبقات بغية تعزيز الأمن السيبراني بصورة فعلية في البلدان النامية، والتعاون الدولي من أجل تعزيز المبادرات المتعلقة بالأمن السيبراني.

[24] http://www.itu.int/en/ITU-D/Study-Groups/2014-2018/Pages/side-events/2015/cybersecurity-workshop.aspx.

ومن خلال الجلستين، تم التركيز على أهمية الجوانب التالية للأمن السيبراني التي عُممت على المشاركين في ورشة العمل:

- إذكاء وعي جميع أصحاب المصلحة بشأن الأمن السيبراني؛
- إشراك جميع الجهات في تنفيذ الاستراتيجية الوطنية للأمن السيبراني؛
- مبادئ واضحة متعلقة بالأمن السيبراني في استراتيجية الأمن السيبراني، مثل التدفق الحر للمعلومات، وسيادة القانون، والحكم الذاتي، والانفتاح، وتعدد أصحاب المصلحة؛
- تحديد الأدوار والمسؤوليات بشكل واضح في الاستراتيجيات الوطنية؛
- مجموعة واضحة من الأهداف في الاستراتيجية الوطنية؛
- نهج إدارة المخاطر؛
- قوانين/تشريعات وطنية للأمن السيبراني؛
- قواعد تقنية بما فيها المعايير والإجراءات؛
- التعاون مع مبادرات دولية وإقليمية.

وأشير أيضاً إلى أنه من المتوقع أن تستمر إتاحة الفرص مثل ورشة العمل هذه وأنه ينبغي تحديث المناقشات. وأكد مجدداً السيد أحمد شرفات (رئيس لجنة الدراسات 2 لقطاع تنمية الاتصالات) والسيد آركادي كريمر (رئيس لجنة الدراسات 17 لقطاع تقييس الاتصالات) على أهمية الفرص السانحة لتبادل المعلومات والآراء بين المشاركين وإرساء تعاون أقوى بين لجنة الدراسات 17 لقطاع تقييس الاتصالات (الأمن) ولجنة الدراسات 2 لقطاع تنمية الاتصالات، ولا سيما فيما يخص المسألة 3/2. وأحيلت نتيجة ورشة العمل لاحقاً إلى الفريق المعني بالمسألة 3 التابع للجنة الدراسات 2 لقطاع تنمية الاتصالات وإلى لجنة الدراسات 17 لقطاع تقييس الاتصالات.

2.5 ورشة العمل الثانية المتعلقة بالأمن السيبراني (19-20 أبريل 2016)

عُقدت ورشة امل الاتحاد المتعلقة بالأمن السيبراني والمعنونة "التدريبات السيبرانية الوطنية واستراتيجية الأمن السيبراني الوطنية المصمّمة على أساس أفضل الممارسات"[25] بعد ظهر يوم 18 أبريل 2016 وصباح يوم 19 أبريل 2016، بالاقتران مع اجتماع فريق المقرر للمسألة 3/2 التابع للجنة الدراسات 2 لقطاع تنمية الاتصالات "ضمان أمن شبكات المعلومات والاتصالات: أفضل الممارسات لتطوير ثقافة الأمن السيبراني". ونظم الفريق المعني بالأمن السيبراني والتابع لمكتب تنمية الاتصالات هذه الورشة بدعم من فريق لجنة الدراسات التابعة لقطاع تنمية الاتصالات. وقد دعيت مجموعة كبيرة من المتحدثين.

[25] http://www.itu.int/en/ITU-D/Study-Groups/2014-2018/Pages/side-events/2016/cybersecurity-workshop.aspx.

الغرض من ورشة العمل

كان الغرض من ورشة العمل المتعلقة بالأمن السيبراني مشاطرة أفضل الممارسات فيما يخص النهوج الدولية والإقليمية والوطنية لتعزيز بناء القدرات في مجال الأمن السيبراني. وبهذا الصدد، كان الهدف من ورشة العمل ما يلي:

- مشاطرة تجارب التدريبات السيبرانية الوطنية مع البلدان النامية لتعزيز فهم احتياجات هذه البلدان، لا سيما وأن الاتحاد يقوم حالياً بوضع خدمة تدريبات سيبرانية وطنية جديدة لتقديمها إلى الدول الأعضاء؛
- مشاطرة الدروس المستخلصة ومشورة الخبراء لإعداد وتنفيذ الاستراتيجيات الوطنية المتعلقة بالأمن السيبراني (NCS) ومشاطرة الاتحاد مع الدول الأعضاء الأعمال الجارية بشأن النهج الجامع لعدة أصحاب مصلحة الذي اتبع مجموعة الأدوات المرتبطة بالاستراتيجيات الوطنية المتعلقة بالأمن السيبراني (NCS).

جدول الأعمال

ألقى السيد يوشي توريغو (نائب مدير مكتب تنمية الاتصالات) ملاحظات استهلالية. وشملت ورشة العمل ثلاث جلسات تخللتها عروض وحلقات نقاش:

- جلسة 18 أبريل: تعزيز التدريبات السيبرانية الوطنية من خلال تبادل التجارب.
- الجلسة 1 في 19 أبريل: المكونات الأساسية لإعداد استراتيجية وطنية شاملة متعلقة بالأمن السيبراني.
- الجلسة 2 في 19 أبريل: التنفيذ الفعلي للاستراتيجية الوطنية المتعلقة بالأمن السيبراني.

المناقشات واستنتاج ورشة العمل

قدمت في ورشة العمل عروض مفيدة وحافلة بالمعلومات، وحلقات نقاش ضمت أسئلة وأجوبة. وطوال الجلسات، تم التركيز على أهمية الجوانب التالية للأمن السيبراني التي عُممت على المشاركين في ورشة العمل:

- يجب أن تكون سيناريوهات التدريبات السيبرانية الوطنية واقعية ولا حاجة إلى الكثير من الأفلام كتلك التي يتطلبها إقناع المسؤولين الإداريين الرفيعي المستوى والحصول على التمويل اللازم؛
- يجب أن تضمّ التدريبات السيبرانية الوطنية جميع الجهات المعنية ومن بينها الحكومة والقطاع الخاص، وذلك منذ مرحلة التخطيط وما تتضمنه من تبادل استباقي للمعلومات؛
- يجب أن تحدد أهداف التدريبات السيبرانية الوطنية بشكل واضح وأن تكون لها قيمة مضافة؛
- يتم اختيار سيناريوهات التدريبات السيبرانية الوطنية على أساس نهج إدارة المخاطر: فيجب الرد على السؤال "ما هو التهديد الأكبر أو الوضع المؤثر جداً؟" ثم الاستناد إلى الرد؛
- تجرى بعض التدريبات السيبرانية الوطنية لاختبار خطط الطوارئ الوطنية؛
- هل ينبغي أن تكون الاستراتيجيات الوطنية للأمن السيبراني علنية أم لا؟ لا يوجد حتى الآن جواب واضح على هذا السؤال في هذه المرحلة، ولكن يجب أن يكون على الأقل جزء من الاستراتيجية علنياً لأغراض توعية المواطنين؛
- يُعتبر نهج إدارة المخاطر لوضع استراتيجيات وطنية متعلقة بالأمن السيبراني عنصراً أساسياً لتحديد وتحقيق الأهداف المناسبة؛
- تُعتبر البنية التحتية الحرجة (CIP) أمراً أساسياً للأمن السيبراني وهي عادة مسألة شراكة بين القطاعين العام والخاص، ولذلك تتطلب الاستراتيجية الوطنية المتعلقة بالأمن السيبراني مشاركة القطاع الخاص؛

- يجب تكوين فريق وتعيين مسؤول، ومراقبة ما يفعله الباقون، والعمل على نقل ما يفعلونه بالاستعانة بفريق متفان. وستشكل مجموعة الأدوات المرتبطة بالاستراتيجية الوطنية المتعلقة بالأمن السيبراني عنصراً إضافياً؛
- تُعتبر الاستراتيجية الوطنية المتعلقة بالأمن السيبراني الكتاب المقدس في مجال الأمن السيبراني. ويجب تحديد أهداف وتدابير مناسبة، وربطها بحماية البنية التحتية الحرجة (CIP) ووضعكم الاجتماعي الاقتصادي. ثم يجب تنفيذها مع الحرص على رصدها بصورة مناسبة؛
- يجب إضفاء طابع مؤسسي على الشراكات بين القطاعين العام والخاص من أجل الاستراتيجية الوطنية المتعلقة بالأمن السيبراني وحماية البنية التحتية الحرجة، من خلال وضع القواعد والتشريعات، إذ إن أهداف كيانات القطاع الخاص والحكومات ليست متطابقة ويجب أن يتم تنسيقها؛
- يحتاج تنفيذ الاستراتيجية المتعلقة بالأمن السيبراني إلى الوقت فيما يخص البلدان التي لم تقدم على ذلك من قبل، من أجل إقناع المعنيين بالمشاركة والحصول على إذن ببدء نشرها. ويكون الحصول على التمويل والإذن اللازمين أسهل عند ربط هذه الاستراتيجية باستراتيجية البلد الرامية إلى تنمية مجتمع المعلومات؛
- يقتضي تنفيذ الاستراتيجية الوطنية المتعلقة بالأمن السيبراني وضع خطة عمل مفصلة تعرض المبالغ المالية اللازمة؛
- تم التشديد على أهمية تحليل الأثر كجزء من دورة وضع/تنفيذ الاستراتيجية الوطنية المتعلقة بالأمن السيبراني؛
- يجب أن تشتمل خطة التنفيذ على النقل الآمن للبيانات في إطار الحكومة الإلكترونية؛
- ثمة مؤشرات (مؤشر الأمن السيبراني العالمي، وغيره) تزداد أهمية لقياس التنفيذ وباعتبارها قائمة مرجعية للاستراتيجيات الوطنية المتعلقة بالأمن السيبراني؛
- وضعت إستونيا المؤشر الوطني للأمن السيبراني (صدرت المنهجية ذات الصلة في نهاية شهر مايو 2016). وأشير إلى مؤشر الأمن السيبراني العالمي للاتحاد باعتباره مكملاً للمؤشر الوطني المذكور؛
- نُشرت الاستراتيجية الوطنية للأمن السيبراني للمملكة المتحدة في وقت لاحق من عام 2016؛
- يستغرق تقييم الاستراتيجية الوطنية للأمن السيبراني وقتاً طويلاً، ويمكن أن يسبب الإحراج، ولكنه يساعد على حشد التمويل؛
- تُعتبر التعاريف الشائعة للاستراتيجيات المتعلقة بالأمن السيبراني مهمة عند الشروع في إعداد الاستراتيجية الوطنية للأمن السيبراني، كي يتوصل جميع أصحاب المصلحة إلى فهم مشترك ورؤية موحدة. والفهم المشترك أهم من التعريف الموحد.

وشدد السيد لوك داندوراند (مكتب تنمية الاتصالات)، في ختام ورشة العمل التي نظمها، على أهمية الفرص المتاحة لتبادل المعلومات/الآراء بين المشاركين والخبراء وعلى ضرورة مواصلة التعاون مع فريق المسألة 3 التابع للجنة الدراسات 2 لقطاع تنمية الاتصالات. وفي الملاحظات الختامية، أشار السيد أحمد شرفات (رئيس لجنة الدراسات 2 لقطاع تنمية الاتصالات) إلى أن تنظيم ورشة عمل بشأن الأمن السيبراني أصبح أحد تقاليد فريق المسألة 3/2 التابع للجنة الدراسات 2 لقطاع تنمية الاتصالات، وأعرب عن أمله في استمرار هذا الأمر. وقال إنه يجني، بفعل انتمائه إلى الوسط الأكاديمي، الفوائد من هذا التبادل المثمر بصورة استثنائية. وأحيلت نتائج ورشة العمل إلى فريق المسألة 3 التابع للجنة الدراسات 2 لقطاع تنمية الاتصالات.

3.5 ورشة العمل الثالثة حول الأمن السيبراني (26 يناير 2017)

عُقدت ورشة عمل الأمن السيبراني بعنوان "الأمن السيبراني والمخاطر السيبرانية في الممارسة العملية"[26] بعد ظهر يوم 26 يناير 2017 بالاقتران مع اجتماعات مقرري لجنة الدراسات 2 لقطاع تنمية الاتصالات، وقبل اجتماع المسألة 3/2 التابعة للجنة الدراسات 2 لقطاع تنمية الاتصالات.

الغرض من ورشة العمل

كان الغرض من هذه الورشة الجمع بين خبراء عالميين لتبادل الآراء والخبرات بشأن التقييم العملي للمخاطر السيبرانية على المستوى الوطني، في المنظمات الكبرى، وفي قطاعات البنية التحتية الحرجة. وستناقش ورشة العمل مخاطر سلسلة التوريد ودور المعايير في إدارة المخاطر السيبرانية في المنظمات.

جدول الأعمال

بعد إدلاء مسؤول مكتب تنمية الاتصالات بملاحظاته الافتتاحية، استُهلت ورشة العمل بجدول أعمال يتضمن خمسة عروض إيضاحية ومناقشات للخبراء على النحو التالي:

- تهديدات الأمن السيبراني الكبرى في عام 2017 وما بعده؛
- المنهجيات والأدوات المستخدمة في القطاع الخاص لتقييم المخاطر في المنظمات الكبرى؛
- عمليات تقييم المخاطر السيبرانية في قطاعات البنية التحتية الحرجة؛
- مخاطر سلاسل التوريد؛
- دور المعايير وتحديث السلسلة ISO/IEC 27000.

المناقشات واستنتاجات ورشة العمل

قدمت في ورشة العمل الثالثة عروض مليئة بالمعلومات ومفيدة، وحلقات نقاش ضمت أسئلة وأجوبة. وطوال الجلسات، تم التركيز على أهمية الجوانب التالية للأمن السيبراني التي عُممت على المشاركين في ورشة العمل:

- تم تقديم التهديدات السيبرانية، والتقارب المادي السيبراني، والتقارب بين مقتضيات العمل والحياة، والتهديدات الداخلية، وتصاعد الهجمات بدافع مالي، والهجمات الموزعة للحرمان من النفاذ (DDo) القائمة على إنترنت الأشياء، ولزيادة الانتهاكات "البسيطة" باعتبارها تهديدات كبرى للأمن السيبراني، وتناول توصيات للمنظمات.
- أثيرت التحديات المتعلقة بتقييم المخاطر القائمة في القطاع الخاص، مثل المعايير المتعددة التي يتعين اتباعها، وعمليات المراجعة الخارجية، والمتطلبات التنظيمية للإدارات، وعمليات الاندماج والشراء/التنويع/والأثر على المستوى الدولي، وتم تقديم أمثلة على منهجيات على تلك التحديات بما في ذلك برمجيات الحوكمة والمخاطر، ونهج العمليات الأمنية، والأداة التكتيكية للكشف عن المخاطر، وإدارة مواطن الضعف.
- كما تم تقديم الاستراتيجية الوطنية لحماية البنية التحتية الحرجة من المخاطر السيبرانية، مع إيلاء تركيز خاص لتقييم المخاطر السيبرانية لنماذج السياق والمدخلات والعملية والمنتج (CIPP) (المنهجية ونقطة الانطلاق ومواطن الضعف في العمليات القائمة في حالة الطيران).

[26] https://www.itu.int/en/ITU-D/Study-Groups/2014-2018/Pages/side-events/2017/cybersecurity-workshop.aspx.

- تمت مناقشة أمن سلاسل توريد تكنولوجيا المعلومات والاتصالات وتحدياتها ومتطلباتها، وتم تناول النقاط الرئيسية التالية: (1) مواجهة المخاطر في إطار برنامج شامل لإدارة المخاطر؛ (2) وفهم المتطلبات المشتركة؛ (3) واستعمال المعايير الدولية؛ (4) وتعزيز القدرة الشرائية؛ (5) والعمل مع الشركاء.
- دور المعايير الدولية في إدارة المخاطر وآخر تحديثات وثائق السلسلة ISO/IEC 27000 في المعيار ISO/IEC JTC1 SC27.

وأثناء ورشة العمل وفي الملاحظات الختامية، تم التشديد على أهمية الفرص المتاحة لتبادل الآراء بين المشاركين والخبراء وعلى الحاجة إلى مواصلة التعاون مع فريق المسألة 3/2 التابع للجنة الدراسات 2 لقطاع تنمية الاتصالات.

6 الفصل 6 - الفرص والتحديات في مجال الأمن السيبراني

أمضى فريق المسألة 3/2 لقطاع تنمية الاتصالات بعض الوقت في البحث في مجالات أخرى، وكان العديد من هذه المجالات متعلقاً بالأعمال التي تجرى عادة في مواضع أخرى والتي لا تندرج في الاختصاصات الحالية المتصلة بالمسألة 3/2. وفي هذا الصدد، أجري عدد من الحوارات مع منظمات، بصورة رسمية وغير رسمية. ويتم التعمق هنا في تحليل المساهمات المتعلقة بالبند ب) من الاختصاصات.

ب) تقديم معلومات حول تحديات الأمن السيبراني الحالية التي يواجهها مقدمو الخدمات والوكالات التنظيمية وغيرها من الأطراف ذات الصلة.

1.6 إدمان الإنترنت

ظهر "إدمان الإنترنت" كأحد الآثار السلبية الناجمة عن تطور المعلومات في البلدان وعن الانتشار الواسع لاستخدام الإنترنت. ومع أنه يجب تحديد مفهوم "إدمان الإنترنت" بشكل واضح من الناحية النفسية والطبية، فهو يشير عادة إلى إلحاق أضرار بالوظائف الجسدية والذهنية والاجتماعية للفرد يصعب الشفاء منها وتنتج عن الاستخدام المفرط لخدمة شبكة تكنولوجيا المعلومات. وتظهر عادة على غالبية المدمنين على الإنترنت عوارض الانطواء وسهولة التأثر من قبيل القلق الحاد أو الانهيار العصبي، مما يعيقهم إعاقة شديدة في حياتهم اليومية. والأشخاص الذين يفرطون في استخدام الإنترنت منجذبون بعمق إلى العالم السيبراني، وتظهر عليهم عوارض تتخذ شتى أشكال الإدمان على الألعاب، وعلى الدردشة، وعلى المواد الإباحية وغيرها.

وقد ظهر الإدمان على الوسائط الذكية، خلال السنوات الأخيرة، في أنماط الحياة وأساليب التواصل السريعة التغير بما أدى إلى ازدياد اعتماد الوسائط الذكية بسرعة وتطور تكنولوجيا المعلومات والاتصالات على صعيدي الإدماج والتقارب.

جهود جمهورية كوريا للوقاية من إدمان الإنترنت والهواتف الذكية والحد منه

يمكن أن تُنسب نسبة 7 في المائة تقريباً من مستخدمي الإنترنت الذين تتراوح أعمارهم بين 5 و54 سنة، في جمهورية كوريا، إلى الفئة المعرضة للإدمان على الإنترنت، وفقاً للاستقصاء المتعلق بوضع إدماج الإنترنت لعام 2013. وقد انخفضت نسبة مجموعة مستخدمي الإنترنت المعرضة للخطر إلى مجموع مستخدمي الإنترنت من 7,7 في المائة في عام 2011 إلى 7,2 في المائة في عام 2012 و7 في المائة في عام 2013. إلا أن نسبة المستخدمين المراهقين إلى المجموعة المعرضة للخطر ارتفعت من 10,4 في المائة في عام 2011 إلى 10,7 في المائة في عام 2012 و11,7 في المائة في عام 2013.[27]

وفي الأثناء، تبين أن ازدياد إدمان الهواتف الذكية أقوى من ازدياد إدمان الإنترنت. فيُعتبر 11,8 في المائة من مستخدمي الهواتف الذكية في كوريا الذين تتراوح أعمارهم بين 10 و54 سنة مجموعة معرضة لخطر الإفراط في استخدام الهواتف الذكية، وهذا يمثل زيادة بمقدار 3,4 نقطة مئوية مقارنة بنسبة 8,4 في المائة التي سُجلت في عام 2011 عندما استُهلت الدراسة الاستقصائية المتعلقة بإدمان الهواتف الذكية. ويشكل المستخدمون المراهقون المجموعة الأكثر عرضة للخطر: فنحو 25,5 في المائة من المراهقين الكوريين (الذين تتراوح أعمارهم بين 10 و19 سنة) كانوا ضمن مجموعة المستخدمين المعرضين لخطر الإفراط في استخدام الهواتف الذكية، مقارنة بنسبة 8,9 في المائة من الكوريين الراشدين. اضطلع مركز إدمان الإنترنت في كوريا، الذي أنشأته الحكومة الكورية في عام 2002، ببرامج شاملة لإسداء المشورة وإعداد المحتوى وتوزيعه وتدريب المستشارين الأخصائيين وتوفير التعليم الوقائي في البلد بكامله،

[27] الوثيقة SG2RGQ/64، "Korea's Internet of things security roadmap"، جمهورية كوريا.

من أجل التصدي بصورة منهجية للاستخدام المفرط للإنترنت والأجهزة الذكية. وقد أجرى المركز منذ عام 2004 دراسات استقصائية سنوية عن وضع إدمان الناس عموماً على الإنترنت (والإدمان على الهواتف الذكية منذ عام 2011)، منتجاً إحصاءات وطنية تُستخدم كمؤشرات معيارية لصياغة السياسات الحكومية.

وفي يونيو 2013، أعدت الوزارات الثماني مجتمعة "خطة شاملة ثانية للوقاية من إدمان الإنترنت والتخفيف منه". ويحدد البرنامج مجموعة كاملة من المساعدات المتاحة على صعيد الوقاية والمشورة والخدمة النفسية والرعاية اللاحقة من أجل جميع الفئات العمرية للأطفال والطلاب والكبار.

وعمدت الحكومة إلى إنشاء لجنة السياسات المشتركة بين الوزارات للتصدي بصورة منهجية لإدمان الإنترنت. وفي مارس 2014، أعدت اللجنة "برنامج التنفيذ لعام 2014 من أجل الوقاية من إدمان الإنترنت والتخفيف منه". وقد نُفذ هذا البرنامج بصورة مشتركة، بإدارة لجنة السياسات المشتركة بين ثماني وزارات، بصورة فعلية ومنهجية.

التعليم الوقائي

إن النفاذ إلى الإنترنت والوسائط الذكية بات سهلاً للغاية في حياتنا اليومية ولذلك يجب أن يتركز التعليم على الوقاية قبل ظهور عوارض الإدمان مثل الانطواء أو سهولة التأثر. والبرنامج التعليمي في كوريا معدّ لتوفير الوقاية الفعّالة وهو يرمي إلى إذكاء وعي الجمهور بالمخاطر المحتملة أو الفعلية للإدمان ومساعدته على تحسين قدرته على الوقاية منه. وعلى سبيل المثال، فإنه يوفر تعليماً وقائياً يتكيف منهاجه مع احتياجات كل فئة من الفئات العمرية المختلفة للأطفال والمراهقين والراشدين. ويرسَل المستشارون المتخصصون إلى المدارس كمحاضرين لتوفير صف خاص (مدته ساعة).

وتجري كوريا برنامجاً تعليمياً مكثفاً (مدته ساعتان) لتلاميذ المدارس الابتدائية والإعدادية والثانوية منذ عام 2013؛ ويختلف الدرس باختلاف العمر المدرسي، ويركز على مشاركة التلاميذ في أنشطة الصف وعلى المناقشة. وخلال الدرس، يستخدم كل تلميذ "دفتر العمل" الخاص به كأداة للتقييم الذاتي، فيحتفظ بسجل للمراقبة الذاتية لاستخدامه الإنترنت والوسائط الذكية ويتخذ في بعض الأحيان قراراً بالحد من استخدامه الإنترنت إذا تبين أنه يستخدمها بصورة مفرطة.

الجدول 1: عدد المشاركين في التعليم الوقائي

الفئة	2010	2011	2012	2013	يونيو 2014	المجموع
مرحلة ما قبل المدرسة	-	31 279	18 200	47 890	26 050	**123 419**
المراهقون	645 981	954 425	621 621	970 696	407 512	**3 600 235**
الراشدون	33 753	90 363	93 001	105 363	25 803	**348 283**
المجموع	**679 734**	**1 076 067**	**732 822**	**1 123 949**	**459 365**	**4 071 937**

(الوحدة: شخص)

ومنذ عام 2014، استُهل برنامج "لعبة الوقاية من الإدمان" للأطفال في مرحلة ما قبل المدرسة ولتلاميذ المرحلة الأدنى من التعليم الابتدائي، من أجل اعتماد وسيلة سهلة وفعّالة لإيصال الرسالة بطريقة مسلية لهؤلاء الأطفال. وفي البرنامج، يقوم الأطفال والتلاميذ بمشاهدة مسرحية أو عرض للدمى المتحركة يحكي قصصاً عن جهود حيوانهم المفضل في مجال إدمان الإنترنت أو إدمان الإنترنت في الحياة اليومية المألوفة، وبعد مشاهدة المسرحية، يتحدث المعلم عن مخاطر إدمان الإنترنت وكيفية الوقاية منه. وهذا البرنامج فعّال لإفهام الأطفال بسهولة مفهوم الإدمان دون الشعور بالإقصاء. وقدّمت المساعدة إلى 23 مدرسة اعتُبرت "مدارس نظيفة من الوسائط الذكية". ويرمي البرنامج

إلى دعم الأنشطة/الحملات المدرسية للترويج لثقافة استخدام الوسائط الذكية بطريقة سليمة وللوقاية من إدمان الإنترنت من خلال التعاون مع الأهل والمعلمين والخبراء.

الخدمات الاستشارية وإنشاء البنى التحتية

تقوم وزارة العلوم وتكنولوجيا المعلومات والاتصالات والتخطيط المستقبلي (MSIP) في جمهورية كوريا بتوفير التعليم الوقائي والخدمات الاستشارية المتخصصة من أجل التصدي بفعالية لحالات إدمان الإنترنت والهواتف الذكية. ومن أجل توفير خدمة مخصصة لكل منطقة، تدير الوزارة 14 مركزاً للوقاية من إدمان الإنترنت (IAPC) واقعاً في 13 مدينة وإقليم في جميع أنحاء البلد منذ يونيو 2014.

وتوفر الخدمات الاستشارية المتخصصة المقدمة بواسطة مجموعة متعددة من القنوات على غرار الزيارات المنزلية أو الخدمات على الخط. وهذه الخدمات الاستشارية المتخصصة معدة لتكون استجابة فعّالة للطلب المتزايد بسرعة على الخدمات الاستشارية وليسهل الحصول عليها. وتوفرّ أيضاً خدمة استشارية على الخط[28]، فضلاً عن خدمة مركز نداء على نطاق البلد بكامله. ومن أجل توفير الخدمات المخصصة لكل منطقة في مجال إدمان الإنترنت الذي يشهده البلد برمته، يقدم المركز خدمات استشارية بالتعاون مع 48 مركزاً ذات صلة مثل مركز دعم الأسرة السليمة، ومراكز دعم الشباب، وغير ذلك.

ويجدر إيلاء عناية خاصة للخدمات الاستشارية المتمثلة في الزيارات المنزلية، التي توفر الخدمات الاستشارية المجانية إلى الأسر من خلال زيارتها في منزلها. ويحق لأي أسرة تعاني من إدمان الإنترنت أن تطلب الحصول على هذه الخدمة. وأثبت البرنامج فعاليته بوجه خاص فيما يتعلق بمدمني الإنترنت المحتاجين إلى المساعدة، الذين يعيشون في أسرة وحيدة العائل أو منخفضة الدخل أو متعددة الأعراق أو الذين يعيشون مع أجدادهم. وباب التقدم بطلب للاستفادة من هذا البرنامج مفتوح أيضاً لكل الأشخاص الآخرين الذين يحتاجون إلى المساعدة في مسألة إدمان الإنترنت: أي الأطفال أو المراهقين أو العاطلين عن العمل أو الأسر ذات المدخول المزدوج. وتدير أيضاً برنامجاً تدريبياً لتأهيل المستشارين المتخصصين في مجال إدمان الإنترنت. والبرنامج التدريبي متاح للمستشارين الحاليين والمعلمين الحاليين لكي يتمكنوا من العمل أيضاً كمستشارين متخصصين في مجال إدمان الإنترنت. وقد قام بتأهيل ما يزيد عن 13 000 مستشار متخصص منذ يونيو 2014.

الجدول 2: عدد الخدمات الاستشارية بحسب نوعها

الفئة	2010	2011	2012	2013	يونيو 2014
وجهاً لوجه (زيارة منزلية)	15 037	10 522 (6 089)	20 701 (10 595)	24 623 (19 519)	7 484 (4 919)
عبر الإنترنت	1 916	569	866	489	148
عبر الهاتف	9 569	7 915	16 138	11 512	4 779
المجموع الفرعي	**26 522**	**19 006**	**37 705**	**36 624**	**12 411**

(الوحدة: خدمة)

[28] http://www.iapc.or.kr.

إجراء البحوث الاستقصائية وإعداد/توزيع المحتوى

تجرى بصورة منتظمة بحوث متعلقة بالسياسات من أجل تعزيز الكفاءة العملية والدقة العلمية عند تنفيذ شتى البرامج المتعلقة بإدمان الإنترنت ووسائط الإعلام الذكية. وقد نُشرت مجموعة منوعة من المواد التربوية مثل الكتب الإرشادية الوقائية، أو الرسوم المتحركة التي تستخدم برمجية Flash، أو التسجيلات الفيديوية، أو كتب التعليم العادية، أو البرامج الاستشارية، وهي متاحة على الخط. وقد أُعدت هذه المواد لتنفيذ البرامج التعليمية الوقائية تنفيذاً فعّالاً وللمساعدة على تحسين إدراك الأشخاص للمخاطر المحتملة لاستخدام الإنترنت والوسائط الذكية.

وفي عام 2013، أعدت ووزعت كتب تعليم عادية للوقاية المكثفة من الإدمان. والدروس متاحة في أربع طبعات تختلف باختلاف دورة الحياة (مثلاً تلاميذ المدرسة الابتدائية، وتلاميذ المدرسة الإعدادية، وتلاميذ المدرسة الثانوية، والراشدون). وأعدت أيضاً مبادئ توجيهية للاستخدام الملائم للوسائط الذكية، ونشرتها في أربع طبعات موجهة إلى أربع فئات من القراء (أهل الأطفال في مرحلة ما قبل المدرسة، وتلاميذ المدرسة الابتدائية، وتلاميذ المدرسة الإعدادية والثانوية). ووُزعت المبادئ التوجيهية على أكثر من 000 20 مدرسة في جميع أنحاء البلد. وفي عام 2014، أعدت نوعاً من المحتوى التعليمي للتعلم الذاتي متاحاً في خمس فئات للوقاية من الإدمان (للأطفال في مرحلة ما قبل المدرسة، والمدارس الابتدائية، والمدارس الإعدادية والثانوية، والجامعات، والراشدين) كي تتمكن من مساعدة المدارس والمؤسسات العامة على أن تكون مستعدة بشكل أفضل لتوفير التعليم اللازم للوقاية من إدمان الإنترنت والذي أصبح إلزامياً بموجب القانون الوطني الأساسي للمعلومات في كوريا (مايو، 2013)، المادة 30، البند 8 (فيما يخص التعليم المتعلق بإدمان الإنترنت).

وتستخدم الإعلانات للوقاية من إدمان الوسائط الذكية بالتعاون مع قطاع الأعمال الخاص، كي تتمكن من مساعدة المراهقين والأهل على الإحجام عن الاستخدام المفرط للوسائط الذكية، وعلى الاعتياد على استخدام الوسائط الذكية استخداماً ملائماً في المنزل والمدرسة.

السمات الخاصة للسياسة الكورية

في كوريا، تُستهل غالبية الأنشطة بمبادرة من الحكومة، وبالتالي، فإن الحكومة الكورية تقدم الدعم المالي والتقني إلى المنظمات المدنية ليتسنى لها الاضطلاع بالأنشطة اللازمة للوقاية من إدمان الإنترنت. والالتزام الحكومي القوي معروف أيضاً في هذا الصدد بحيث يحظر على القاصرين الذين تقل أعمارهم عن 16 عاماً النفاذ إلى الألعاب المتاحة على الخط، من منتصف الليل حتى السادسة صباحاً، ويجوز للأهل أن يتحكموا بنفاذ أولادهم (لمن هم دون الثامنة عشرة من العمر) إلى الألعاب المتاحة على الخط وبمنع هذا النفاذ من خلال تقديم طلب إلى مقدمي الخدمات، ويتعين بحكم القانون تدريب جميع الطلاب من روضة الأطفال حتى الجامعة، وجميع الموظفين في القطاع العام، على الوقاية من إدمان الإنترنت. وعلاوةً على ذلك، تتولى الحكومة إدارة 14 مركزاً للوقاية من إدمان الإنترنت في جميع أنحاء البلد. والتحدي الذي تواجهه الحكومة الكورية في مجال الوقاية من إدمان الإنترنت هو كيفية تحفيز مشاركة جميع أصحاب المصلحة ولا سيما الأهل والمجتمع والقطاع الخاص.

خلاصة

الإدمان قضية صحية أساسية. وعليه، بدأت المسألة 3/2 لقطاع تنمية الاتصالات مناقشات مع منظمة الصحة العالمية (WHO) لاسترعاء انتباهها لهذه المسألة. وبهذا الصدد، أُرسل بيان اتصال بشأن إدمان الإنترنت إلى منظمة الصحة العالمية (WHO) واليونيسيف (UNICEF) واليونيسكو (UNESCO) وفريق العمل التابع لمجلس الاتحاد والمعني بحماية الأطفال على الخط (ITU CWG-COP) خلال فترة الدراسة 2014-2017، لفهم الأنشطة التي أجريت حتى الآن بشأن هذا الموضوع بصورة أفضل. وكانت هذه المناقشات غير حاسمة ويمكن مواصلتها.

2.6 أمن المعاملات الإلكترونية

إن تطور التجارة والمعاملات الإلكترونية، بما فيها المشتريات والمدفوعات عبر شبكة الإنترنت، وتنفيذ أوامر سوق الأوراق المالية، والإقرارات الضريبية الإدارية (ضريبة القيمة المضافة، ضريبة الدخل، صحيفة الرعاية الطبية الإلكترونية) عبر شبكة الإنترنت، وتبادل رسائل البريد الإلكتروني والوثائق الإلكترونية؛ وتنفيذ بروتوكولات أمن الشبكات الجديدة القائمة على البنى التحتية العامة الأساسية ونشرها التدريجي على نطاق واسع، وعلى وجه الخصوص منها، DNSSEC، RPKI (البنية التحتية العامة الأساسية للموارد)؛ وأمن إنترنت الأشياء؛ هي عناصر حاسمة ينبغي أن تحض البلدان النامية على أن تعمل من أجل إنشاء مؤسسات على المستوى الوطني أو الإقليمي تتولى مسؤولية إدارة البنى التحتية العامة الأساسية لديها. ويمكن لإنشاء هذه المؤسسات، إذا حظيت بالإشراف المناسب، أن يسهم في تعزيز أمن الاتصالات الإلكترونية بوجه عام، وأمن المعاملات الإلكترونية على وجه الخصوص. ويمكنها أيضاً أن تسمح بظهور الاقتصادات الرقمية وتطورها في البلدان النامية[29].

وتتطور التجارة والمعاملات الإلكترونية بسرعة في البلدان النامية. وعادة ما تستخدم هذه المعاملات قنوات غير آمنة. ولكن عندما تؤمَّن، فهي تستند إلى شهادات موقعة ذاتياً أو إلى شهادات تشترى باستخدام سلطات إصدار شهادات تتخذ عموماً من البلدان المتقدمة مقراً لها. بيد أن هذه الشهادات لا تتوافق بالضرورة مع تشريعات البلدان النامية في بعض الحالات.

ويعود نقص الحماس والتأخر الملحوظ في نشر البروتوكولات المأمونة، مثل DNSSEC وRPKI، في البلدان النامية إلى سوء فهم هذه البروتوكولات أو المعايير التي تسمح بتنفيذها؛ أو يعود إلى عدم كفاية الموارد البشرية المدربة المعنية بنشرها، أو عدم سبر أغوار سلاسل القيمة المتعلقة بها.

وطلب الفريق المعني بالمسألة 3/2 لقطاع تنمية الاتصالات من عدة منظمات التعليق على هذه الشواغل. وتلقى الفريق نظرة عامة ممتازة على هذه القضايا قدمته جمعية الإنترنت (ISOC) يرد بيانه في هذا الوثيقة.

وتؤدي أنظمة البنى التحتية العامة الأساسية (PKI) دوراً مهماً في تعزيز الثقة في الإنترنت بوصفها منصة آمنة للتنمية الاقتصادية والاجتماعية. وعلى مر الزمن، تطورت هذه الأنظمة، التي تدعم التكنولوجيات وممارسات التنفيذ، من أجل جعلها أكثر متانة وأماناً. ومن المهم أن تستند البلدان الساعية إلى تحسين بنيتها التحتية الخاصة بالإنترنت إلى هذه التجربة لنشر أحدث التكنولوجيات واللجوء إلى أفضل الممارسات الراهنة.

ويتمتع موظفو جمعية الإنترنت بخبرة كبيرة في مجال إنشاء البنى التحتية العامة الأساسية ونشرها. ولدينا مبادرة للثقة والهوية من شأنها دعم استخدام اتصالات آمنة ومستقان منها على شبكة الإنترنت. وتقوم جمعية الإنترنت أيضاً بإدارة برنامج Deploy360 الذي يروج للانتشار الواسع النطاق للتكنولوجيات المتعلقة بأمن البنى التحتية بما فيها

[29] الوثيقة SG2RGQ/153، "أمن المعاملات الإلكترونية" جمهورية توغو.

أمن طبقة النقل (TLS)، وتمديدات أمن نظام أسماء الميادين (DNSSEC)، والبنية التحتية العامة الأساسية للموارد (RPKI).

وتحتفظ جمعية الإنترنت بموارد معلومات متعلقة بهذه المواضيع ومراجع ومواد إضافية توضح كيفية إنشاء هيئات تصديق جذرية، وهو الحال لاستخدام أمن طبقة النقل (TLS)، وتمديدات أمن نظام أسماء الميادين (DNSSEC)، والبنية التحتية العامة الأساسية للموارد (RPKI)، وكيفية نشر هذه التكنولوجيات، فضلاً عن توفير المساعدة لتعزيز بناء القدرات. وإحدى نقاط الانطلاق هو موقعنا الإلكتروني بشأن مسائل تكنولوجيا الإنترنت الخاص بنا وموقعنا بشأن Deploy360.

وتبحث هذه الوثيقة في ثلاثة أنظمة مختلفة للبنى التحتية العامة الأساسية (WebPKI وRPKI وDNSSEC) تؤثر على الثقة والأمن بشكل عام فيما يخص الإنترنت. وتُبرز نقطة مهمة وهي أن هذه الأنظمة مختلفة وتتوخى أهدافاً متباينة. وتتمتع بتسلسل إداري منفصل وتعمل في إطار مجالات إدارية مستقلة. وتحدد هذه الوثيقة أيضاً إحدى التكنولوجيات الناشئة هي الاستيقان من الكيانات المسماة بالاستناد إلى نظام أسماء الميادين (DANE)، التي تعد بتعزيز الثقة في الإنترنت.

ومن غير المرجح أن تُعتبر هيئة تصديق وطنية حلاً للمشاكل الأمنية التي قد يواجهها بلد ما. فينبغي للبلدان التي تجاهد للتصدي للشواغل الأمنية أن تنظر في التكنولوجيات الجديدة الناشئة وأفضل الممارسات الراهنة التي يمكن اعتمادها بنهج تعاوني شامل.

البنى التحتية العامة الأساسية لشبكة الويب (WebPKI)

إن أول نظام للبنى التحتية العامة الأساسية يتم بحثه في هذه الوثيقة هو البنى التحتية العامة الأساسية لشبكة الويب. إن الشهادات القائمة على التوصية X.509، التي يثق بها الجمهور، تصدر عن هيئات التصديق (CA) المعتمدة لدى موردي التكنولوجيات مثل Apple وMicrosoft وMozilla، الذين يوزعون الشهادات الجذرية في أنظمة التشغيل وبرمجيات التصفح الخاصة بهم. وتَستخدم عادة البنى التحتية العامة الأساسية لشبكة الويب هذه الشهادات لتوفير دورات التصفح على الويب، ونقل البريد الإلكتروني، والمراسلة الفورية. وقد تُستخدم هذه الشهادات أيضاً للاستيقان من المستخدمين الذين ينفذون إلى الأنظمة وكذلك إلى الوثائق الإلكترونية الموقعة رقمياً وإلى البرمجيات. وتقبل التشريعات الوطنية أكثر فأكثر التواقيع الرقمية بدل وسائل الاستيقان التقليدية.

إن إضافة شهادة جذرية إلى التوزيع العام للشهادات الجذرية من أجل البنى التحتية العامة الأساسية لشبكة الويب هو عملية معقدة ومكلفة وتستغرق وقتاً طويلاً. وتتضمن هذه العملية ثلاثة عناصر أساسية هي:

1) تحديد المتطلبات التي يجب أن تفي بها هيئة التصديق لتتمكن من إصدار الشهادات وإدارتها؛

2) مراجعة أعمال هيئة التصديق للتأكد من أنها اتبعت الإجراءات والمتطلبات اللازمة بالشكل الملائم؛

3) إضافة هيئة التصديق إلى مجموعة هيئات التصديق الموثوق بها في منتوج. وقد استحدث منتدى التصفح التابع لمنظمة هيئات التصديق (CA) (انظر "المتطلبات الأساسية") المبادئ التوجيهية لإصدار الشهادات وإدارتها.

ثم يتم اختبار هذه المتطلبات بإخضاعها لمجموعة من إجراءات المراجعة التي يديرها برنامج الثقة الشبكية (WebTrust) لهيئات التصديق، الخاص بالمعهد الأمريكي للمحاسبين القانونيين (AICPA)/المحاسبين المعتمدين في كندا (CICA). ويستخدم موردو التكنولوجيات نتائج عمليات المراجعة هذه لتقرير أي هيئة يمكن إضافتها من حيث المبدأ إلى المنتوج. ويمكن للمستخدمين والشركات في بعض الأحيان إضافة هيئات أخرى إلى أجهزتها، ولكن هناك اعتبارات عملية كبيرة عند اللجوء إلى هذه العملية.

ولكن الجدير بالذكر أن إضافة شهادة جذرية جديدة إلى التوزيع العام للشهادات لا يجعل البنى التحتية العامة الأساسية لشبكة الويب بشكل عام أكثر أماناً. وعلى العكس، فإن هذا الأمر يزيد من المخاطر لأن أي موطن ضعف يعتري أي هيئة من هيئات التصديق هو موطن ضعف يشوب النظام بكامله. ولهذه الأسباب، يُستحسن إبقاء عدد الشهادات الجذرية عند أدنى حد ممكن عملياً. وإذا احتاجت الحكومات إلى وضع هيئات تصديق خاصة بها، فأحد النهوج الشائعة هو استحداث هيئات تصديق فرعية تكون تابعة لهيئة تصديق جذرية قائمة.

وهناك عدد من الشواغل بشأن هشاشة نظام البنى التحتية العامة الأساسية لشبكة الويب. ويعمل مجلس تصميم الإنترنت (IAB) حالياً بجهد https://datatracker.ietf.org/doc/draft-iab-web-pki-problems/ في إطار برنامج السرية والأمن الخاص به من أجل بلورة بعض هذه المشاكل وإصدار التوصيات بشأن الأنشطة التي يمكن أن تساعد في تحسين البنى التحتية. أما الجهات التي تسعى إلى تحديد الطرق التي يمكن أن تساعد بها أنظمة البنى التحتية العامة الأساسية على تحسين البنية التحتية، فستستفيد خير استفادة من متابعة هذه الجهود. في إطار برنامج السرية والأمن الخاص به من أجل بلورة بعض هذه المشاكل وإصدار التوصيات بشأن الأنشطة التي يمكن أن تساعد في تحسين البنى التحتية. أما الجهات التي تسعى إلى تحديد الطرق التي يمكن أن تساعد بها أنظمة البنى التحتية العامة الأساسية على تحسين البنية التحتية، فستستفيد خير استفادة من متابعة هذه الجهود.

نظام البنى التحتية العامة الأساسية للموارد (RPKI)

إن النظام الثاني المحدد للبنى التحتية العامة الأساسية هو نظام البنى التحتية العامة الأساسية للموارد. وهو نظام متخصص يرمي إلى تحسين أمن نظام تسيير الإنترنت، ولا سيما بروتوكول مسيِّر الحدود (BGP). ويقوم بذلك من خلال إصدار شهادات موارد قائمة على التوصية X.509 لأصحاب عناوين بروتوكول الإنترنت وأرقام النظام المستقل (AS) من أجل إثبات الغرض المرخص به الذي خصصت له هذه الموارد. وتصدر هذه الشهادات لسجلات الإنترنت المحلية (LIR) وعن أحد سجلات الإنترنت الإقليمية الخمسة (RIR): وهي AfriNIC وAPNIC وARIN وLACNIC وRIPE NCC - المسؤولة عن توزيع وتخصيص هذه الموارد لمناطق الخدمة الخاصة بها.

ويكون كل سجل من سجلات الإنترنت الإقليمية بمثابة هيئة تصديق جذرية ومصدر ثقة للموارد المخصصة لمناطق الخدمة الخاصة بها، مع أن شهاداتها الجذرية غير مدرجة في أي توزيع عام للشهادات الجذرية. ولذلك، لا بد من تحميلها من المواقع الإلكترونية لسجلات الإنترنت الإقليمية وتثبيتها.

والجدير بالذكر أن موارد الترقيم لا توزَّع أو تخصَّص على أساس وطني باستثناء سبعة سجلات إنترنت وطنية (NIR) موروثة في منطقة مركز معلومات شبكات آسيا والمحيط الهادئ (APNIC). ولكن يمكن للحكومات الوطنية أن تؤدي دوراً في تشجيع مقدمي خدمات الإنترنت (ISP) وسجلات الإنترنت المحلية الأخرى على استخدام مرافق البنى التحتية العامة الأساسية للموارد.

تمديدات أمن نظام أسماء الميادين (DNSSEC)

إن آخر نظام جرى بحثه للبنى التحتية العامة الأساسية هو تمديدات أمن نظام أسماء الميادين. والهدف من نظام أسماء الميادين (DNS) هو ترجمة أسماء المضيفين التي يمكن أن يقرأها الإنسان مثل http://www.isoc.org إلى عناوين لبروتوكول الإنترنت يمكن أن تقرأها الآلة مثل 212.110.167.157. وأصبح نظام أسماء الميادين الوسيلة الرئيسية لتحديد موقع خدمات الإنترنت. ولكن هناك العديد من المنظمات المختلفة التي تدير نظام أسماء الميادين، ولأن طابعها الموزَّع يعني أن التغيرات لا تنتشر من فورها، فمن الصعب ضمان أن المعلومات تعود من مصدر موثوق به. وبعبارة أخرى، لا شيء يضمن أن مخدم اسم لا يقدم معلومات خاطئة لتوجيه المستخدمين نحو المضيفين الذين يديرون معاملاتهم أو يتظاهرون بأنهم مواقع أخرى.

وكلف فريق مهام هندسة الإنترنت (IETF) تمديدات أمن نظام أسماء الميادين بالاستيقان من معلومات نظام أسماء الميادين من خلال التوقيع الرقمي لسجلات نظام أسماء الميادين. وهذا يضمن فقط إمكانية قيام مالك الميدان بتغيرات وإمكانية التصديق على السجلات من خلال سلسلة ثقة تمتد حتى منطقة الجذور. وهذا يعني أن الزبون الذي يطلب أمراً قادر على التحقق من أن الإجابة التي يحصل عليها آتية بالفعل من كيان مخول بإعطائها.

ويمكن اعتبار نظام أسماء الميادين، بدعم من تمديدات أمن نظام أسماء الميادين، نوعاً متخصصاً من البنى التحتية العامة الأساسية. ولكن مع الأسف، فإن هذه التمديدات منتشرة بصورة محدودة فقط حتى الآن على الرغم من تزايد التوقيع على اسم ميدان المستوى الأعلى (TLD). ويمكن لمديري الميادين الوطنيين أن يؤدوا دوراً هاماً في ضمان أمن هذه البنية التحتية المهمة للإنترنت من خلال التوقيع على منطقة ccTLD وتيسير نشر التمديدات في التراتب الوطني لنظام أسماء الميادين. وإضافةً إلى ذلك، سيسمح انتشار التمديدات باستخدام تكنولوجيا الاستيقان من الكيانات المسماة بالاستناد إلى نظام أسماء الميادين (DANE) الموضحة أدناه للمساعدة في تحسين البنى التحتية العامة الأساسية لشبكة الويب.

الاستيقان من الكيانات المسماة بالاستناد إلى نظام أسماء الميادين (DANE)

إن أحد مواطن الضعف الخاصة بالبنى التحتية العامة الأساسية لشبكة الويب هو قدرة الطرف الثالث المتمثل في هيئات التصديق على إصدار شهادات لأي ميدان أو منظمة، بغض النظر عما إذا كان الكيان مقدم الطلب يملك فعلاً الميدان أو يديره. ومع ازدياد عدد هيئات التصديق، يزداد احتمال إصدار إحدى هذه الهيئات شهادة غير سليمة. إن مستوى الثقة في نظام البنى التحتية العامة الأساسية يعادل القوة التي يتحلى بها أضعف رابط. وهذا هو السبب الرئيسي وراء قيام التوزيع العام للشهادات الجذرية بتشديد شروط إدراج هيئات التصديق على نحو ما نوقش في القسم أعلاه المتعلق بالبنى التحتية العامة الأساسية لشبكة الويب.

وعلى الرغم من تشديد إجراءات إصدار الشهادات بقدر كبير إثرَ عدة حوادث هامة أصدرت فيها هيئات تصديق شهادات غير سليمة، ما زال النظام يعتمد على ثقة الطرف الثالث. وقد أدى هذا الاعتماد مؤخراً إلى وضع بروتوكول الاستيقان من الكيانات المسماة بالاستناد إلى نظام أسماء الميادين (DANE). وبفضل هذا الاستيقان، يستطيع مديرو الميادين اعتماد مفاتيحهم العامة من خلال تخزينها في نظام أسماء الميادين. ويتطلب هذا النهج استخدام تمديدات أمن نظام أسماء الميادين وتحتاج الآن غالبية برمجيات التصفح إلى استحداث جهاز إضافي. وإضافةً إلى ذلك، يُرجح أن يتطلب الاستيقان من الكيانات المسماة بالاستناد إلى نظام أسماء الميادين نهجاً أكثر صرامة للتصديق على مالكي الميادين، وقد تقع هذه الجهود في نهاية الأمر على عاتق سجلات أسماء ميادين المستوى الأعلى (TLD) عوضاً عن هيئات التصديق.

هيئات التصديق الوطنية

أُعدت جميع أنظمة البنى التحتية العامة الأساسية، التي يرد وصفها أعلاه، من أجل توفير ثقة عامة من خلال الاستيقان من موارد الإنترنت، مثل العناوين والأسماء والبنى التحتية للمخدمات. ولا علاقة لهذه الأنظمة بالمحتوى الذي يتم نقله عبر الإنترنت بين الكيانات المستقان منها. فتتولّد الثقة من إجراءات التشغيل الخاضعة لتوافق عام. وهذه الإجراءات تخضع في نهاية الأمر للكيانات النهائية التي تقرر أن تثق بهيئات التصديق المشكّلة في أنظمتها. وعلى سبيل المثال، يؤدي استخدام هيئة تصديق لتنظيم المحتوى إلى انتهاك هذه الثقة ويرجح أن يفضي ذلك إلى نزع صفة الطرف الموثوق به عن هيئة التصديق. ومن غير المرجح أن تُعتبر هيئة تصديق وطنية حلاً للقضايا الأمنية التي قد يواجهها بلد ما.

وتؤكد جهات أخرى وجهة النظر هذه بقدر كبير. وأشير بوجه خاص في رد مؤسسة الإنترنت للأسماء والأرقام المخصصة (ICANN) إلى أن إضافة هيئة تصديق جذرية أخرى يزيد مساحة الهجوم على النظام على نحو يمكن قياسه. ولا يتخطى مستوى أمن النظام مستوى هيئة التصديق الأقل أماناً أو موثوقية في المجموعة بكاملها، وتشكل أي هيئة تصديق بشهادة جذرية راسخة في برمجية الطرف المعوَّل عليه مشكلة محتملة. ونتيجة لذلك، فإن فساد أي هيئة تصديق أو سوء تصرفها يقوض الأمن والثقة في النظام برمته. وأشاروا إلى أنهم يستشرفون مستقبلاً يساعد فيه استخدام الأمن القائم على الميادين (تمديدات أمن نظام أسماء الميادين (DNSSEC)) والاستيقان من الكيانات المسماة بالاستناد إلى نظام أسماء الميادين (DANE)، فضلاً عن التطورات على صعيد النهوج الخاصة بشفافية التصديق، على الحد من هذه المخاطر. ويقترحون أن يتعاون الأعضاء المعنيون مع كل من فريق مهام هندسة الإنترنت، ومنتدى التصفح التابع لمنظمة هيئات التصديق.

وقد ردّ مركز تنسيق الشبكات الأوروبية العاملة ببروتوكول الإنترنت (RIPE NCC)، وهو سجل الإنترنت الإقليمي الذي يغطي مساحة كبيرة من أوروبا ومناطق أخرى، للتناقش بشأن نظام البنى التحتية العامة الأساسية للموارد. ويوفر المركز أشكالاً متنوعة من التدريب على الخط، واقترح تمكين البلدان النامية (ولا سيما إداراتها العامة) من الاستفادة بالكامل من نظام البنى التحتية العامة الأساسية للموارد، الذي تديره سجلات الإنترنت الإقليمية، من خلال كونه مثالاً يحتذى به وعن طريق تشجيع المشغلين الخاصين في بلدانها على الحصول على شهادات موارد أرقام الإنترنت التي يملكونها. وسيسمح التوسع في اعتماد مشغلي الشبكات لها في جميع أنحاء العالم للمزيد من المشغلين باتخاذ قرارات التسيير استناداً إلى صحة شهادات البنية التحتية العامة الأساسية للموارد، بما يؤدي إلى نظام لتسيير الإنترنت أكثر أماناً للجميع.[30]

3.6 الشراكات في مجال الأمن السيبراني

على النحو المشار إليه سابقاً في **القسم 3** من التقرير، فإن الموضوع المشترك الذي تم التشديد عليه في شتى المساهمات هو أهمية الشراكات في مجال الأمن السيبراني. فلا يمكن لحكومة واحدة أو شركات خاصة أو منظمة دولية أن تتصدى لهذه التحديات وحدها. فيتطلب ذلك نهجاً تعاونياً. وقد تناولت هذه المسألة الولايات المتحدة الأمريكية وهولندا، في مساهمتهما المشتركة بشأن المنتدى العالمي للخبرات السيبرانية (GFCE)[31]. وقدمت هذه المساهمات معلومات أساسية عن المنتدى العالمي للخبرات السيبرانية ولمحة عامة عنه. ويشكل المنتدى مبادرة رئيسية طوعية جامعة لعدة أصحاب مصلحة هدفها تعزيز التضامن الدولي وتوفير الدعم السياسي والتقني والمالي للجهود الرامية إلى توطيد التعاون الدولي بين جميع أصحاب المصلحة فيما يخص القضايا السيبرانية. ويقوم المركز بتعزيز بناء القدرات السيبرانية من منظور الارتباط الوثيق بين الاهتمامات الأمنية والاقتصاد وحقوق الإنسان. وقد تبين أن تعزيز القدرات والخبرات في المجال السيبراني يعزز من فعالية الجهود التعاونية الدولية القائمة. وشددت المساهمة أيضاً على المبادرات الرئيسية للمنتدى العالمي للخبرات السيبرانية، وقدمت معلومات قيمة بشأن عضوية المنتدى وكيفية انضمام الدول الأعضاء وأعضاء القطاعات إلى هذه المبادرة العالمية.

---

30 يمكن الاطلاع على مزيد من المعلومات بشأن كل خيار من هذه الخيارات على دليل العناوين التالي:
Resource Certification (RPKI) Webinar: https://www.ripe.net/support/training/learn-online/webinars/certifica-
.tion-webinar BGP Operations and Security Training Course: https://www.ripe.net/support/training/courses/bgp

31 الوثيقة 2/332، "The Global Forum on Cyber Expertise (GFCE)"، الولايات المتحدة الأمريكية وهولندا.

مجالات أخرى

تناولت مساهمات عديدة جوانب أخرى للأمن السيبراني، بما في ذلك حسبما يتعلق بصناعة الصيرفة[32] والحاجة إلى اعتماد نُهج محايدة تكنولوجياً؛ ومخاطر انتهاك البيانات الشخصية، والحاجة إلى تمتع المدن الذكية بالقدرة على الصمود[33]. و لم تُستكشف هذه المجالات بتعمق خلال فترة الدراسة.

[32] الوثيقة SG2RGQ/141، ''Fintech and security in Korea''، جمهورية كوريا.

[33] الوثيقة 2/77، ''Cyber-security's role and best practices to ensure Smart Cities' service continuity and resilience''، مؤسسة Symantec.

7 الفصل 7 - التجارب الوطنية استناداً إلى إطار معايير موحدة للأمن

دعتنا اختصاصات المسألة 3/2 إلى استهلال بحث في التجارب الوطنية استناداً إلى إطار معايير موحدة للأمن. وفي إطار هذا البحث، تلقت المسألة 3/2 مساهمة[34] من **المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية** عرضت فيها خبراتها في تطبيق "المعايير الموحدة" باعتبارها مخططاً دولياً مرموقاً ومفتوحاً يساعد القائمين على تصميم وتنفيذ أنظمة تكنولوجيا المعلومات في اختيار منتجات تكنولوجيا المعلومات التي تتضمن مستويات مناسبة للضمانات الأمنية. وفي حين لا توجد أداة واحدة أو نهج واحد يضمن أمان الأنظمة، تعد "المعايير الموحدة" مخططاً يحظى بقبول واسع وجاهز لمساعدة المشترين في اختيار المنتجات التي ينبغي ضمانها. ويطبق "اتفاق الاعتراف بالمعايير الموحدة (CCRA)" منذ عام 2000. وتتمثل وظيفته في تحسين توفر منتجات لأمن تكنولوجيا المعلومات تكون خاضعة للتقييم، وإزالة عبء التقييم المزدوج. ويجرى اختبار الأمن في مختبرات مستقلة على أساس معايير متفق عليها. ويتعين أن تحصل هذه المختبرات على رخصة تؤكد تمتعها بالإمكانات والاستقلال اللازم. وفي وقت قريب (2014)، تم تحديث الاتفاق ليدعم نهجاً أكثر تفصيلاً قائماً على المواصفات، يشمل خبراء من دوائر الصناعة، والدوائر الأكاديمية، وما إلى ذلك، لوضع متطلبات أساسية لكل مجال من مجالات التكنولوجيا والتي يمكن للكل تقييمها بوضوح لاحقاً.

كما تلقت المسألة 3/2 مساهمتين من **جمهورية إيران الإسلامية** التي شرعت في النظر في نُهج بديلة. وتعتبر هذه النظرة أن تقييم الأمن السيبراني على الصعيد الوطني يتطلب قياس مؤشرات الأمن السيبراني بصورة متواصلة. ومن أجل تخطيط وتنفيذ نظام وطني فعّال لإدارة الأمن السيبراني (NCMS)، تمس الحاجة إلى وضع برنامج وطني مناسب لقياس الأمن السيبراني (NCMP). وييسر البرنامج اتخاذ القرارات ويحسن الأداء والمحاسبة على الصعيد الوطني.[35]

وأعربت مساهمة ثانية عن الحاجة إلى إطار لأفضل الممارسات من أجل تحديد واستخدام مجموعة تدابير ومقاييس بهدف تقييم فعالية أي نظام لإدارة أمن المعلومات على المستوى الوطني. وعلى غرار إطار الأمن السيبراني الوطني (NCSec)[36]، المستوحى بالكامل من المعيار ISO/IEC 27001[37] لأي نظام لإدارة أمن المعلومات (ISMS) على المستوى التنظيمي، اقتُرح إعداد "إطار لقياس الأمن السيبراني على المستوى الوطني"[38]. وهو مستوحى من المعيارين ISO/IEC 27004[39] و NIST-800-55-R1[40] اللذين وضعا لتقييم الأمن السيبراني على المستوى التنظيمي. وأيضاً على غرار الحالة المستوحاة من المعيار ISO/IEC 27001، ثمة حاجة إلى "تحديد كيفية قياس فعالية الضوابط أو مجموعة الضوابط المختارة، وتحديد كيفية استخدام هذه المقاييس لتقييم فعالية الضوابط في توليد النتائج القابلة للمقارنة وللنقل" على المستوى الوطني. وبما أن هذه المساهمات تتخطى على ما يبدو التجربة الوطنية، تعاونت المسألة 3/2 في العمل مع لجنة ISO/IEC JTC 1/SC 27، التي أجابت قائلة إنها تتطلع إلى المزيد من الأنشطة في هذا المجال.

---

34 الوثيقة 2/364، ''Common criteria as a tool for giving assurance about the security characteristics of IT products''، **المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية**.

35 الوثيقة SG2RGQ/46، ''National cybersecurity measures and measurements''، جمهورية إيران الإسلامية.

36 لجنة الدراسات 1 لقطاع تنمية الاتصالات، التقرير النهائي، المسألة 1/1-22، أفضل الممارسات لتأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني، 2014، متاح في https://www.itu.int/pub/D-STG-SG01.22.1-2014.

37 المعيار ISO/IEC 27001، تكنولوجيا المعلومات - تقنيات الأمن - أنظمة إدارة أمن المعلومات - المتطلبات، 2013.

38 الوثيقة SG2RGQ/47، National cybersecurity measures، جمهورية إيران الإسلامية.

39 المعيار ISO/IEC 27004، تكنولوجيا المعلومات - تقنيات الأمن - إدارة أمن المعلومات - المراقبة والقياس والتحليل والتقييم، 2016.

40 المعهد الوطني للمعايير والتكنولوجيا، النشرة الخاصة رقم 800-55 المراجعة 1، دليل قياس الأداء فيما يخص أمن المعلومات، 2008.

يوفر قطاع تقييس الاتصالات تقريراً تقنياً بشأن "الاستعمال الناجح لمعايير الأمن"[41]. والهدف من هذا التقرير مساعدة المستعملين وخصوصاً المستعملين من البلدان النامية في الحصول على فهم أفضل لقيمة استخدام توصيات قطاع تقييس الاتصالات المتصلة بالأمن في سياقات مختلفة (مثل الأعمال والتجارة والحكومة والصناعة).

ويوفر قطاع تقييس الاتصالات أيضاً إضافة للتوصية ITU-T X.1054 بشأن أفضل الممارسات لتنفيذ التوصية ITU-T X.1054 | ISO/IEC 27014 بشأن إدارة أمن المعلومات - حالة بوركينا فاصو[42].

41 https://www.itu.int/pub/T-TUT-SEC-2016.

42 https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13072.

8 الفصل 8 - الاستنتاجات والتوصيات لفترة الدراسة المقبلة

خلال فترة الدراسة المضغوطة هذه، نظر الفريق المعني بالمسألة 3/2 في الجوانب العديدة للأمن السيبراني وأجرى عدداً من دراسات الحالة القُطرية وعقدنا عدداً من ورش العمل التي وفرت توجيهات بشأن جوانب عديدة متعلقة بتصميم استراتيجيات للأمن السيبراني. ونظر الفريق في مدخلات بشأن مؤشر الأمن السيبراني العالمي وقدمها إلى مكتب تنمية الاتصالات.

ويوصي الفريق المعني بالمسألة 3/2 لقطاع تنمية الاتصالات بمواصلة جميع الأنشطة المدرجة في الاختصاصات الحالية. ويوصي بالنظر في التهديدات (التقنية) المتزايدة والناشئة بخلاف الرسائل الاقتحامية والبرمجيات الضارة. وينبغي زيادة دراسة مشكلة الاحتيال من خلال التلاعب باستخدام صندوق البطاقات SIM، إحدى المشاكل التي أثارها العديد من البلدان النامية. وينبغي التأكيد على إجراء مزيد من أنشطة بناء القدرات من قبيل ورش العمل والمواد التدريبية لاستعمالها في البيئات الإقليمية والمحلية. وينبغي كذلك التأكيد على مواصلة التعاون مع المنظمات ذات الصلة مثل FIRST وGFCE وISOC. كما ينبغي مواصلة التعاون من خلال تجميع الخبرات الوطنية. وينبغي أيضاً مواصلة إجراء استبيان الوعي بالأمن السيبراني، بافتراض أن المواد المناسبة يمكن تحديدها قبل المؤتمر العالمي لتنمية الاتصالات. وفي إطار المسألة، ينبغي استمرار التعاون الوثيق مع مكتب تنمية الاتصالات بشأن إقرار وتطوير التدابير المتعلقة بالأمن السيبراني، مثل مؤشر الأمن السيبراني العالمي. وينبغي أن يتواصل في إطار هذه المسألة على وجه الخصوص تحديد تدابير التحسين فيما يتعلق بالمؤشرات وجمع البيانات وتحليلها. وينبغي مواصلة العمل على حماية الأطفال على الخط كذلك.

واستُعملت فترات الدراسة المتعددة الأخيرة في تطوير طرائق عمل لجان دراسات قطاع تنمية الاتصالات. ويشيد الفريق المعني بالمسألة 3/2 بالمؤتمر العالمي لتنمية الاتصالات لتشجيعه استمرار التطوير. وعلى وجه التحديد، ينبغي للمؤتمر النظر في السماح بتنظيم العمل على أساس فترات سنوية، بحيث يمكن للأنشطة التركيز على قضايا محددة.

والنقطة الأخيرة هي أن مسألة الدراسة هذه (المسألة 22/1 "تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني") استهلّت أعمالها بتقديم توصيات لإعداد استراتيجيات وطنية لتحسين الأمن السيبراني في البنى التحتية الحرجة. وينبغي أن تخضع هذه الأعمال للمراجعة نظراً لمرور الوقت.

Abbreviations and acronyms

Various abbreviations and acronyms are used through the document, they are provided here.

Abbreviation/acronym	Description
ACTIVE	**A**dvanced **C**yber **T**hreats response Initiati**VE**
AICPA	American Institute of Certified Public Accountants
ANTIC	National Information and Communication Technologies Agency
APT	Advanced Persistent Threats
BDT	Telecommunication Development Bureau
BGP	Border Gateway Protocol
BGPSEC	Border Gateway Protocol Security
C&C	Command and Control
CCRA	Common Criteria Recognition Agreement
CIIs	Critical Information Infrastructures
CIOs	Chief Information Officer
CISO	Chief Information Security Officer
CISOs	Chief Information Security Officer
COP	Child Online Protection
CRR	Cyber Resilience Review
CSRIC	Communications Security, Reliability and Interoperability Council
CSRIC	Communications Security, Reliability and Interoperability Council
DANE	DNS-based Authentication of Named Entities
DHS	U.S. Department of Homeland Security
DKIM	Domain Keys Identified Mail
DMARC	Domain-based Message Authentication and Conformance
DNSSEC	DNS Security Extensions
DOE	U.S. Department of Energy
FCC	U.S. Federal Communications Commission
GCA	Global Cybersecurity Agenda
GCI	Global Cybersecurity Index
GCSCC	Global Cyber Security Capacity Centre
GFCE	Global Forum on Cyber Expertise

Abbreviation/acronym	Description
GFCE	Global Forum on Cyber Expertise
IAB	Internet Architecture Board
IAPCs	Internet Addiction Prevention Center
ICS	Incommunication systems
ICS-CERT	Industrial Control Systems Computer Emergency Response Team
ICT	Information and Communications Technology
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IMPACT	International Multilateral Partnership against Cyber Threats
IoT	Internet of Things
IoT	Internet of Things
IP	Internet Protocol
IS	Information Security
ISACA	Information Systems Audit and Control Association
ISACs	Information Sharing and Analysis Centers
ISPs	Internet service providers
ITU	International Telecommunication Union
ITU-D	ITU Telecommunication Development Sector
KISA	Korea Internet & Security Agency
LDCs	Least Developed Countries
MIC	Japan's Ministry of Internal Affairs and Communications
MSIP	Korea’s Ministry of Science, ICT and Future Planning
NCCIC	National Cybersecurity and Communications Integration Center
NCMP	National Cybersecurity Measurement Program
NCMP	National Cybersecurity Measurement Program
NCMS	National Cybersecurity Management System
NCS	National Cybersecurity Strategies
NCSA	National Cyber Security Alliance
NIRs	National Internet Registries
NIST	National Institute of Standards and Technology

Abbreviation/acronym	Description
NorSIS	Norwegian Centre for Cybersecurity
PKI	Public Key Infrastructure
PPP	Public-private partnerships
RIRs	Regional Internet Registries
RPKI	Routing Public Key Infrastructure
RRNs	Resident Registration Numbers
SMEs	Small and Medium sized Enterprises
SoC	Security System-on-Chip
TLS	Transport Layer Security
UK	United Kingdom
UNODC	United Nations Office on Drugs and Crime
US-CERT	United States Computer Emergency Readiness Team
WSIS	World Summit on the Information Society
WTDC	World Telecommunication Development Conference

Annexes

Annex 1: The Global Cybersecurity Index 2017

The Global Cybersecurity Index (GCI) is a survey that measures the commitment of Member States to cybersecurity in order to raise awareness.

The GCI revolves around the ITU Global Cybersecurity Agenda (GCA) and its five pillars (legal, technical, organizational, capacity building and cooperation). For each of these pillars, questions were developed to assess commitment. Through consultation with a group of experts, these questions were weighted in order to arrive at an overall GCI score. The survey was administered through an online platform through which supporting evidence was collected.

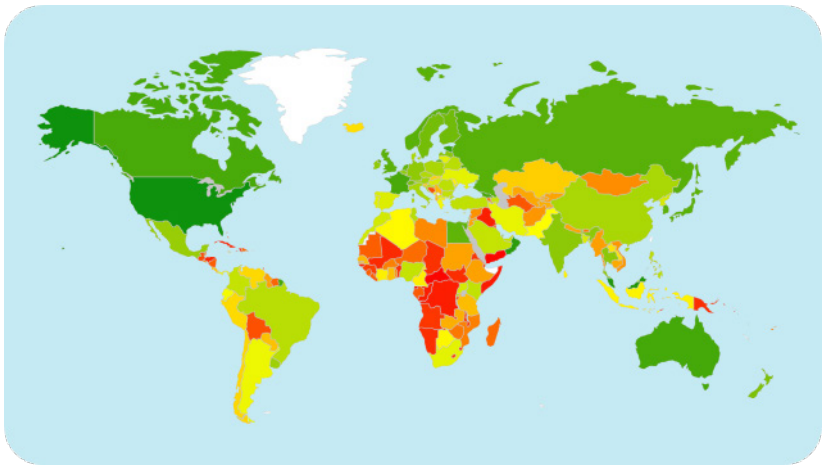
One-hundred and thirty-four Member States responded to the survey throughout 2016. Member States who did not respond were invited to validate responses determined from open-source research. As such, the GCI results cover all 193 ITU Member States.

Key findings and results

There is a huge range in cybersecurity commitments around the world as the heat map below illustrates. Out of the 193 Member States covered, scores range from less than one to over 90.

Level of commitment: from dark green (highest) to red (lowest).

Figure 1A: GCI heat map



The GCI 2017 continues to show the commitment of countries around the world to cybersecurity. The overall picture shows improvement and strengthening of all five elements of the cybersecurity agenda in various countries in all regions. The level of development of the different pillars varies from country to country in the regions. In addition to the score, this index provides a set of illustrative practices that give useful insights into the achievements of certain countries.

The six ITU regions were presented in the report (Africa, Americas, Arab States, Asia and the Pacific, Commonwealth of Independent States and Europe). For a global view, all of the six regions are represented in the top ten commitment level in the GCI. This suggests that being a leading performer is not strictly tied to geographic location.

Table 1A: Most committed countries, GCI (normalized score)

Country	GCI score	Legal	Technical	Organizational	Capacity building	Cooperation
Singapore	0.92	0.95	0.96	0.88	0.97	0.87
United States	0.91	1	0.96	0.92	1	0.73
Oman	0.87	0.98	0.82	0.85	0.95	0.75
Estonia	0.84	0.99	0.82	0.85	0.94	0.64
Mauritius	0.82	0.85	0.96	0.74	0.91	0.70
Georgia	0.81	0.91	0.77	0.82	0.90	0.70

The full GCI 2017 report with global and regional scores can be found at http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2017.aspx.

As the GCI shows, there is a wide gulf in cyber preparedness around the globe. This gap exists between and within regions. The research revealed that while increased Internet access and more mature technological development is correlated with improvement in cybersecurity at the global level, it has the opposite effect among countries with developing economies and lower levels of technological development. The data collection shows that there is need for the developed world to help and more cooperation could be initiated between developed and developing countries to assist them in cybersecurity development. For the GCI to have an impact on raising awareness on this crucial emerging concern over time, continuity of GCI efforts is essential; ITU welcomes all Member States and industry stakeholders to actively participate in the future research and development, to enhance the current reference model.

The success of the future data collection exercise largely depends on the response rate and quality to the questionnaire and ITU calls on all Member States to take part in the next GCI exercise.

GCI reference model

The Global Cybersecurity Index (GCI) is a composite index combining 24 indicators into one benchmark measure to monitor and compare the level of Member States' cybersecurity commitment with regard to the five pillars identified by the High-Level Experts Group and endorsed by the Global Cybersecurity Agenda (GCA). These pillars form the five sub-indices of GCI. First developed by ITU in partnership with ABI Research in 2013, and with results presented in November 2014, the GCI is included under Resolution 130 (Rev. Busan, 2014). It is being enhanced in response to ITU Member States' request to develop a cybersecurity index and publish updates regularly.

The main objectives of the GCI are to measure:

- The type, level and evolution over time of cybersecurity commitment in countries and relative to other countries;
- Progress in cybersecurity commitment of all countries from a global perspective;
- Progress in cybersecurity commitment from a regional perspective;
- The cybersecurity commitment divide, i.e. the difference between countries in terms of their level of engagement in cybersecurity initiatives.

The objective of the GCI as an initiative is to help countries identify areas for improvement in the field of cybersecurity, as well as to motivate them to take action to improve their ranking, thus helping raise the overall level of cybersecurity worldwide. Through the information collected, the GCI aims to illustrate the practices of other countries so that Member States can implement selected aspects

suitable to their national environment, with the added benefit of helping harmonize practices and foster a global culture of cybersecurity.

Background

The GCI is included under Resolution 130 (Rev. Busan, 2014) on strengthening the role of ITU in building confidence and security in the use of information and communication technologies. Specifically, Member States are invited "to support ITU initiatives on cybersecurity, including the Global Cybersecurity Index (GCI), in order to promote government strategies and the sharing of information on efforts across industries and sectors".

A first iteration of the GCI was conducted in 2013/2014 in partnership with ABI Research, and the final results have been published. A total of 105 countries had responded out of 193 ITU Member States. Secondary data was used to build the index for non-respondents and was sent to them for verification/endorsement.

Following feedback received from various communities, a second iteration of the GCI was undertaken and the Report[1] was presented during WSIS-17. This new version is formulated around an extended participation from Member States (134 countries responded to the online survey while 59 countries did not provide primary data), experts and industry stakeholders as contributing partners. An enhanced reference model has thereby been devised. Throughout the steps of this new version, Member States were consulted using various vehicles including ITU-D Study Group 2 Question 3/2.

Conceptual framework

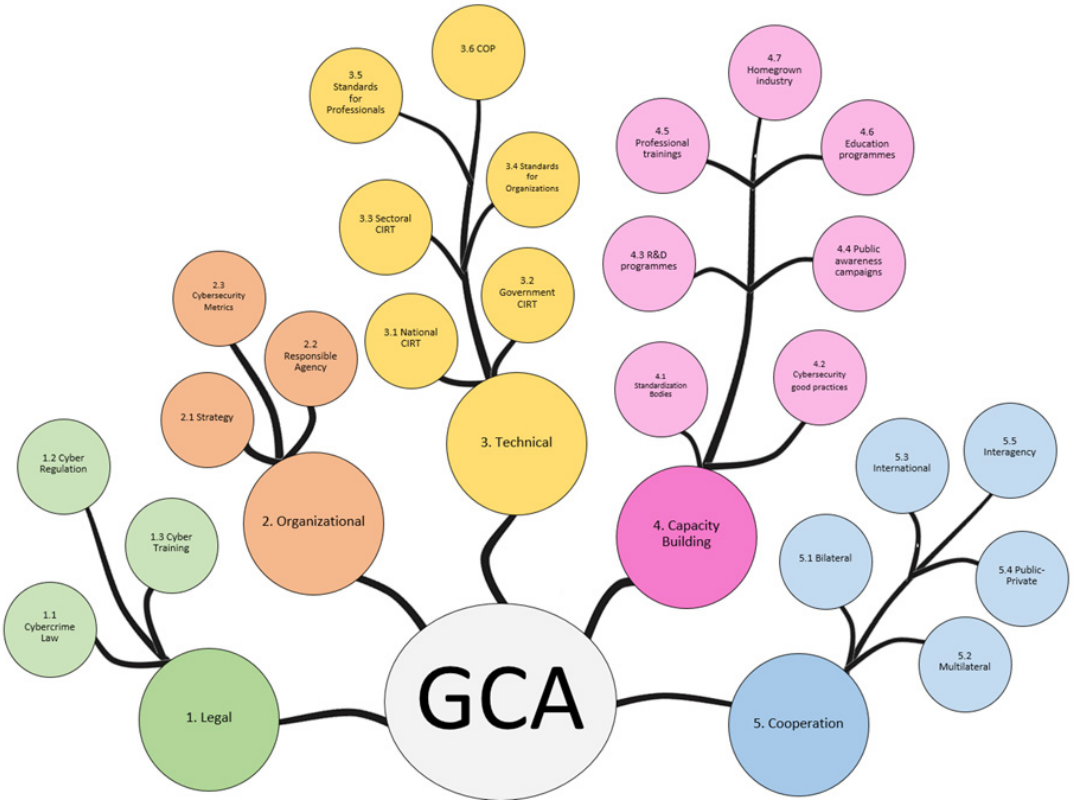
The GCA is the ITU framework for international multi-stakeholder cooperation in cybersecurity aimed at building synergies with current and future initiatives. It focuses on the following five pillars: legal, technical, organizational, capacity building and cooperation.

Figure 2A: GCA

Figure 2A is an illustration of the linkages between the main index, the five sub-indices (different colours) and the GCA. This is in keeping with the cybersecurity development tree map elaborated in the methodology section and its maturity increases as indicated by the deeper tones of colour. The tree has been expanded for a sub-part of the legal pillar only for the sake of clarity and given the space constraint in presenting the complete picture.

[1] http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2017.aspx.

Figure 3A: GCA linkages



Legal sub-index: Legal measures empower a nation state to establish basic response mechanisms through investigation and prosecution of crimes and the imposition of sanctions for non-compliance or breach of law. A legislative framework sets the minimum standards of behaviour across the board on which further cybersecurity capabilities can be built. Ultimately, the goal is to enable all nation states to have adequate legislation in place in order to harmonize practices at the regional/international level, and facilitate international combat against cybercrime. ***The legal environment is evaluated based on the number of legal institutions and frameworks dealing with cybersecurity and cybercrime.***

Technical sub-index: Technology is the first line of defence against cyber threats. Without adequate technical capabilities to detect and respond to cyberattacks, nation states remain vulnerable. Effective ICT development and use can only truly prosper in a climate of trust and security. Nation states therefore need to establish accepted minimum security criteria and accreditation schemes for software applications and systems. These efforts need to be accompanied by the creation of a national entity focused on dealing with cyber incidents, a responsible government agency and a national framework for watch, warning and incident response. ***The technical component is evaluated based on the number of frameworks dealing with cybersecurity by the nation state.***

Organizational sub-index: Organizational measures are necessary for the proper implementation of any national initiative. A broad strategic objective needs to be set by the nation state, along with a comprehensive plan in implementation, delivery and measurement. National agencies need to be present to implement the strategy and evaluate the results. Without a national strategy, governance model and supervisory body, efforts in different sectors become disparate, thwarting efforts to attain national harmonization in cybersecurity capability development. ***The organizational structures are evaluated based on the existence of institutions and strategies concerning cybersecurity development at the national level.***

Capacity-building sub-index: Capacity building is intrinsic to the first three measures (legal, technical and organizational). Cybersecurity is most often tackled from a technological perspective even though there are numerous socio-economic and political implications. Human and institutional capacity

building is necessary to enhance knowledge and know-how across sectors, to formulate appropriate solutions, and promote the development of competent professionals. ***Capacity building is evaluated based on the number of research and development, education and training programmes and certified professionals and public sector agencies.***

Cooperation sub-index: Cybercrime is a global problem and is blind to national borders or sectoral distinctions. As such, tackling cybercrime requires a multi-stakeholder approach with inputs from all sectors and disciplines. Greater cooperation can enable the development of much stronger cybersecurity capabilities, helping to deter repeated and persistent online threats and enable better investigation, apprehension and prosecution of malicious agents. ***National and international cooperation is evaluated based on the number of partnerships, cooperative frameworks and information sharing networks.***

Methodology

The GCI 2017 includes 25 indicators (157 questions). The indicators used to calculate the GCI were selected on the basis of the following criteria:

- Relevance to the five GCA pillars and in contributing towards the main GCI objectives and conceptual framework;
- Data availability and quality;
- Possibility of cross verification through secondary data.

The whole concept of a new iteration of the GCI is based on a cybersecurity development tree map and binary answer possibilities. The tree map concept, which is illustrated below, is an answer to different possible paths that might be taken by countries in order to enhance their cybersecurity commitment. Each of the five pillars are associated with a specific colour (the same code as that used in the Cyberwellness country profiles). The deeper the path taken, indicating a more developed level of commitment, the deeper the colour depicting it becomes.

The various levels of cybersecurity development among countries, as well as the different cybersecurity needs reflected by a country's overall ICT development status, were taken into consideration. The concept is based on an assumption that the more developed cybersecurity is, the more complex the solutions observed will be. Therefore, the further a country goes along the tree map by confirming the presence of pre-identified cyber solutions, the more complex and sophisticated the cybersecurity development is within that country, allowing it to obtain a higher score with the GCI.

The rationale behind using binary answer possibilities is the elimination of opinion-based evaluation and of any possible bias towards certain types of answers. Moreover, the simple binary concept will allow quicker and more complex evaluation as it will not require lengthy answers from countries. This, in turn, is assumed to accelerate and streamline the process of providing answers and further evaluation. The idea is that the respondent will only confirm the presence or lack of certain pre-identified cybersecurity solutions. An online survey mechanism, which will be used for gathering answers and uploading all relevant materials, will enable the extraction of good practices, information for Cyberwellness profiles and a set of thematic qualitative evaluations by a panel of experts.

The key difference in methodology between GCI Version 1 and GCI Version 2 is the use of a binary system instead of a three-level system. The binary system evaluates the existence or absence of a specific activity, department or measure. Unlike GCI Version 1, it does not take 'partial' measures into consideration. The facility for respondents to upload supporting documents and URLs, is a way of providing more information to substantiate the binary response. Furthermore, a number of new questions have been added in each of the five pillars in order to refine the depth of research.

The detailed computation of the sub-indices and of the main index are provided in the report. Apart from building the index, open-ended questions have been included in the questionnaire to cater

for additional requirements from ITU-D Study Group 2 Question 3/2 which do not fit within the GCI computation.

Figure 4A: Global cybersecurity agenda

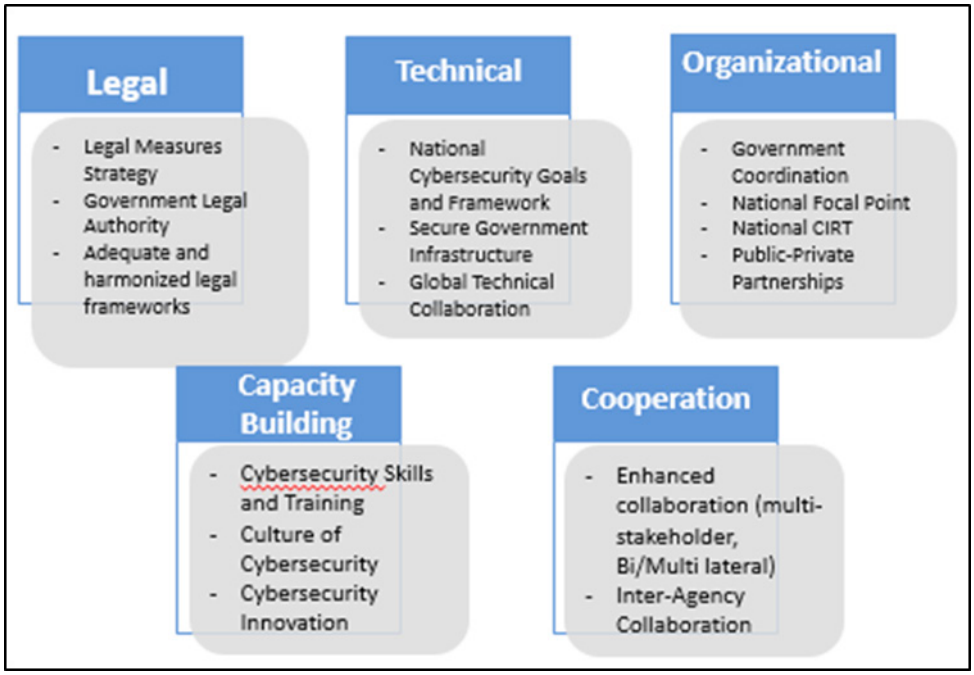
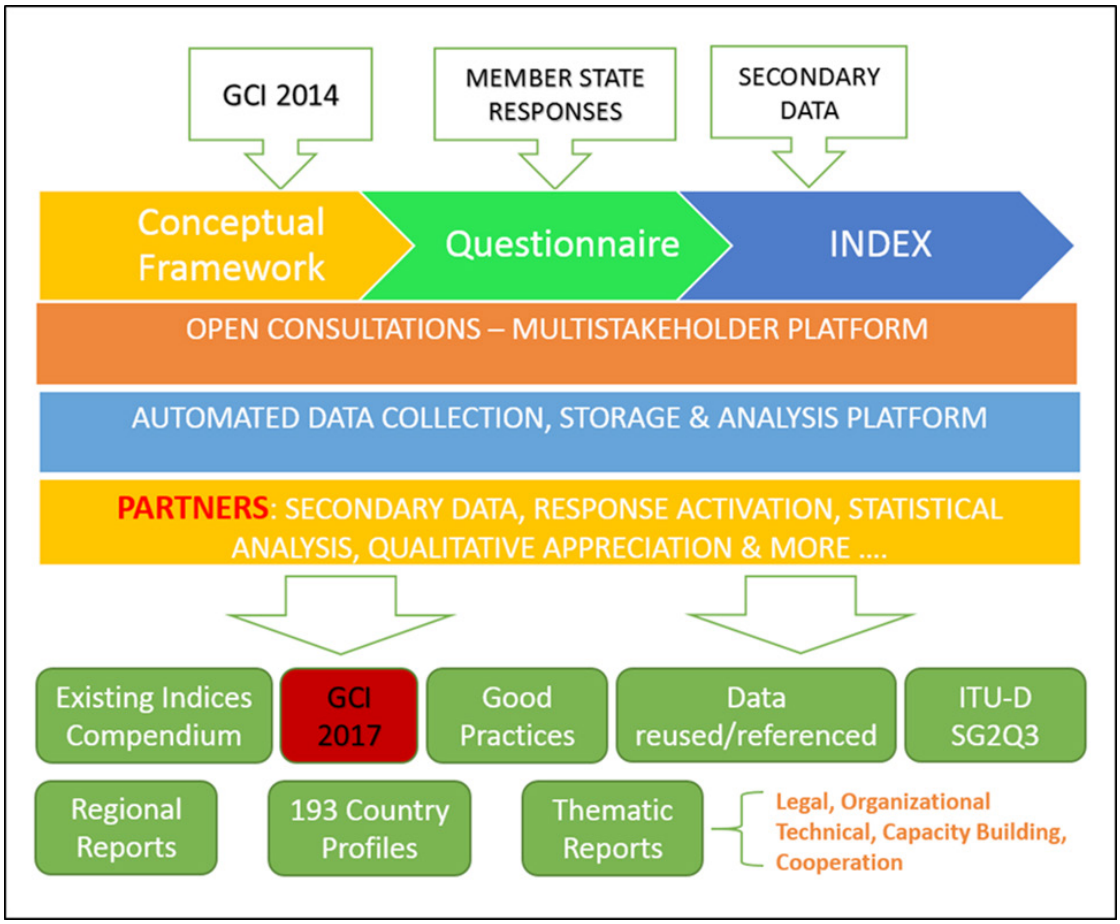


Figure 5A: GCI approach



1.1 Definition of indicators

– Legal measures

Legislation is a critical measure for providing a harmonized framework for entities to align themselves to a common regulatory basis, whether on the matter of prohibition of specified criminal conduct or on minimum regulatory requirements. Legal measures also allow a nation state to set down the basic response mechanisms to breaches: through investigation and prosecution of crimes and the imposition of sanctions for non-compliance or breach of law. A legislative framework sets the minimum standards of behaviour across the board, applicable to all, and on which further cybersecurity capabilities can be built. Ultimately, the goal is to enable all nation states to have adequate legislation in place in order to harmonize practices supranationally and offer a setting for interoperable measures, facilitating international combat against cybercrime.

The legal environment can be measured based on the existence and number of legal institutions and frameworks dealing with cybersecurity and cybercrime. The sub-group is composed of the following indicators:

– Cybercriminal legislation

Cybercrime legislation designates laws on the unauthorized (without right) access, interference, interception of computers, systems and data. This also includes procedural law, and any existing articles on the expedited preservation of stored computer data, production orders, real-time collection of computer data, extradition, mutual assistance, confidentiality and limitation on use; as well as any case law on cybercrime or computer misuse.

– Cybersecurity regulation

Cybersecurity regulation designates laws dealing with data protection, breach notification, cybersecurity certification/standardization requirements, implementation of cybersecurity measures, cybersecurity audit requirements, privacy protection, child online protection, digital signatures and e-transactions, and the liability of Internet service providers.

– Cybersecurity training

Cybersecurity training for law enforcement officers, judicial and other legal actors designates professional and technical training that can be recurring for police officers, enforcement agents, judges, solicitors, barristers, attorneys, lawyers, paralegals and other persons of the legal and law enforcement profession.

1.2 Technical measures

Technology is the first line of defence against cyber threats and malicious online agents. Without adequate technical measures and the capabilities to detect and respond to cyberattacks, nation states and their respective entities remain vulnerable to cyber threats. The emergence and success of ICTs can only truly prosper in a climate of trust and security. Nation states therefore need to be capable of developing strategies for the establishment of accepted minimum security criteria and accreditation schemes for software applications and systems. These efforts need to be accompanied by the creation of a national entity focused on dealing with cyber incidents at a national level, at the very least with a responsible government agency and with an accompanying national framework for watch, warning and incident response.

Technical measures can be measured based on the existence and number of technical institutions and frameworks dealing with cybersecurity endorsed or created by the nation state. The sub-group is composed of the following indicators:

1.2.1 National CERT/CIRT/CSIRT

The establishment of a CIRT/CERT/CSIRT[2] with national responsibility provides the capabilities to identify, defend, respond and manage cyber threats and enhance cyberspace security in the nation state. This ability needs to be coupled with the gathering of the nation's own intelligence instead of relying on secondary reporting of security incidents whether from the CIRT's constituencies or from other sources.

1.2.2 Government CERT/CIRT/CSIRT

A government CERT/CIRT/CSIRT is an entity that responds to computer security or cybersecurity incidents which affect solely governmental institutions. Apart from reactive services, it may also engage in proactive services such as vulnerability analysis and security audits. Unlike the national CERT which services both the private and public sectors, the government CERT provides its services to constituents from the public sector only.

1.2.3 Sectoral CERT/CIRT/CSRIT

A sectoral CERT/CIRT/CSIRT is an entity that responds to computer security or cybersecurity incidents which affect a specific sector. Sectoral CERTs are usually established for critical sectors such as healthcare, public utilities, emergency services and the financial sector. Unlike the government CERT, which services the public sector, the sectoral CERT provides its services to constituents from a single sector only.

1.2.4 Cybersecurity standards implementation framework for organizations

This indicator measures the existence of a government-approved (or endorsed) framework (or frameworks) for the implementation of internationally recognized cybersecurity standards within the public sector (government agencies) and within the critical infrastructure (even if operated by the private sector). These standards include, but are not limited to those developed by the following agencies: ISO, ITU, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, IEC, NERC, NIST, FIPS, PCI DSS, etc.

1.2.5 Cybersecurity standards and certification for professionals

This indicator measures the existence of a government-approved (or endorsed) framework (or frameworks) for the certification and accreditation of professionals by internationally recognized cybersecurity standards. These certifications, accreditations and standards include, but are not limited to, the following: Cloud Security knowledge (Cloud Security Alliance), CISSP, SSCP, CSSLP CBK, Cybersecurity Forensic Analyst (ISC²), GIAC, GIAC GSSP (SANS), CISM, CISA, CRISC (ISACA), CompTIA, C|CISO, CEH, ECSA, CHFI (EC Council), OSSTMM (ISECOM), PCIP/CCISP (Critical Infrastructure Institute), (No Suggestions) Certification, Q/ISP, Software Security Engineering Certification (Security University), CPP, PSP, PCI (ASIS), LPQ, LPC (Loss Prevention Institute), CFE (Association of Certified Fraud Examiners), CERT-Certified Computer Security Incident Handler (SEI), CITRMS (Institute of Consumer Financial Education), CSFA (Cybersecurity Institute), CIPP (IAPP), ABCP, CBCP, MBCP (DRI), BCCP, BCCS, BCCE, DRCS, DRCE (BCM), CIA, CCSA (Institute of Internal Auditors), (Professional Risk Managers International Association), PMP (Project Management Institute), etc.

1.2.6 Child Online Protection

This indicator measures the existence of a national agency dedicated to child online protection, the availability of a national telephone number to report issues associated with children on line, any

[2] A Computer Incident Response Team (CIRT), Computer Emergency Response Team (CERT), or Computer Security Incident Response Team (CSIRT) is a team of IT security experts whose main business is to respond to computer security incidents. It provides the necessary services to handle them and support their constituents to recover from breaches. Source: A step by step approach on how to set up a CSIRT – ENISA.

technical mechanisms and capabilities deployed to help protect children on line, and any activity by government or non-government institutions to provide knowledge and support to stakeholders on how to protect children online.

1.3 Organizational measures

Organization and procedural measures are necessary for the proper implementation of any type of national initiative. A broad strategic objective needs to be set by the nation state, with a comprehensive plan in implementation, delivery and measurement. Structures such as national agencies need to be established in order to put the strategy into effect and evaluate the success or failure of the plan. Without a national strategy, governance model and supervisory body, efforts in different sectors and industries become disparate and unconnected, thwarting efforts to reach national harmonization in terms of cybersecurity capability development.

The organizational structures can be measured based on the existence and number of institutions and strategies organizing cybersecurity development at the national level. The creation of effective organizational structures is necessary for promoting cybersecurity, combating cybercrime and promoting the role of watch, warning and incident response to ensure intra-agency, cross-sector and cross-border coordination between new and existing initiatives. The sub-group is composed of the following indicators:

1.3.1 Strategy

The development of policy to promote cybersecurity is recognized as a top priority. A national strategy for cybersecurity should maintain resilient and reliable information infrastructure and aim to ensure the safety of citizens; protect the material and intellectual assets of citizens, organizations and the State; prevent cyber-attacks against critical infrastructures; and minimize damage and recovery times from cyber-attacks. Policies on national cybersecurity strategies or national plans for the protection of information infrastructures are those officially defined and endorsed by a nation state, and can include the following commitments: establishing clear responsibility for cybersecurity at all levels of government (local, regional and federal or national), with clearly defined roles and responsibilities; making a clear commitment to cybersecurity, which is public and transparent; encouraging private sector involvement and partnership in government-led initiatives to promote cybersecurity; a roadmap for governance that identifies key stakeholders.

1.3.2 Responsible agency

A responsible agency for implementing a national cybersecurity strategy/policy can include permanent committees, official working groups, advisory councils or cross-disciplinary centres. Most national agencies will be directly responsible for watch and warning systems and incident response, and for the development of the organizational structures needed for coordinating responses to cyberattacks.

1.3.3 Cybersecurity metrics

This indicator measures the existence of any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development, risk-assessment strategies, cybersecurity audits, and other tools and activities for rating or evaluating resulting performance for future improvements. For example, based on ISO/IEC 27002-2005, a national cybersecurity standard (NCSec Referential) can help nation states respond to specify cybersecurity requirements. This referential is split into five domains: NCSec Strategy and Policies; NCSec Organizational Structures; NCSec Implementation; National Coordination; Cybersecurity Awareness Activities.

1.4 Capacity building

Capacity building is intrinsic to the first three measures (legal, technical and organizational). Understanding the technology, the risk and the implications can help to develop better legislation,

better policies and strategies, and better organization as to the various roles and responsibilities. Cybersecurity is a relatively new area, not much older than the Internet itself. This area of study is most often tackled from a technological perspective; yet there are numerous socio-economic and political implications that have applicability in this area. Human and institutional capacity building is necessary to enhance knowledge and know-how across sectors, to apply the most appropriate solutions, and promote the development of the most competent professionals.

A capacity-building framework for promoting cybersecurity should include awareness-raising and the availability of resources. Capacity building can be measured based on the existence and number of research and development, education and training programmes, and certified professionals and public sector agencies. Some data is collected through reliable secondary sources which actually provide certified training worldwide. The sub-group is composed of the following indicators:

1.4.1 Standardization bodies

Standardization is a good indicator of the level of maturity of a technology, and the emergence of new standards in key areas underlines the vital importance of standards. Although cybersecurity has always been an issue for national security and treated differently in different countries, common approaches are supported by commonly recognized standards. These standards include, but are not limited to those developed by the following agencies: ISO, ITU, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, IEC, NERC, NIST, FIPS, PCI DSS, etc. This indicator measures the existence of a national cybersecurity standardization body and activities in the development and implementation of cybersecurity standards.

1.4.2 Cybersecurity best practices

This indicator measures the research and publication of best practices and guidelines on cybersecurity technology and its use, management, and application to various scenarios. Best practices are methods or procedures which have a proven track record of success. Adopting best practices will not only reduce the probability of failure but also increase efficiency.

1.4.3 Cybersecurity research and development programmes

This indicator measures the investment into national cybersecurity research and development programmes at institutions which could be private, public, academic, non-governmental or international. It also considers the presence of a nationally recognized institutional body overseeing the programme. Cybersecurity research programmes include, but are not limited to, malware analysis, cryptography research and research into system vulnerabilities and security models and concepts. Cybersecurity development programmes refer to the development of hardware or software solutions that include but are not limited to firewalls, intrusion prevention systems, honey-pots and hardware security modules. The presence of an overarching national body will increase coordination among the various institutions and sharing of resources.

1.4.4 Public awareness campaigns

Public awareness includes efforts to promote widespread publicity campaigns to reach as many people as possible as well as making use of NGOs, institutions, organizations, ISPs, libraries, local trade organizations, community centres, computer stores, community colleges and adult education programmes, schools and parent-teacher organizations to get the message across about safe cyber-behaviour on line. This includes actions such as setting up portals and websites to promote awareness, disseminating support material and establishing cybersecurity adoption.

1.4.5 Cybersecurity professional training courses

This indicator measures the existence of national or sector-specific educational and professional training programmes for raising awareness with the general public (i.e. national cybersecurity

awareness day, week, or month), promoting cybersecurity courses in the workforce (technical, social sciences, etc.) and promoting certification of professionals in either the public or the private sector.

1.4.6 National education programmes and academic curricula

This indicator looks at the existence and the promotion of national education courses and programmes to train the younger generation in cybersecurity-related skills and professions in schools, colleges, universities and other learning institutes. Cybersecurity-related skills include, but are not limited to, setting strong passwords and not revealing personal information on line. Cybersecurity-related professions include, but are not limited to, cryptanalysts, digital forensics experts, incident responders, security architects and penetration testers.

1.4.7 Incentive mechanisms

This indicator looks at any incentive efforts by government to encourage capacity building in the field of cybersecurity, whether through tax breaks, grants, funding, loans, disposal of facilities, and other economic and financial motivators, including dedicated and nationally recognized institutional body overseeing cybersecurity capacity-building activities. Incentives increase the demand for cybersecurity-related services and products, which improves defences against cyberthreats.

1.5 Home-grown cybersecurity industry

A favourable economic, political and social environment supporting cybersecurity development will incentivize the growth of a private sector around cybersecurity. The existence of public awareness campaigns, manpower development, capacity building and government incentives will drive a market for cybersecurity products and services. The existence of a home-grown cybersecurity industry is testament to such a favourable environment and will drive the growth of cybersecurity start-ups and associated cyber-insurance markets.

1.6 Cooperation

Cybersecurity requires input from all sectors and disciplines, and for this reason needs to be tackled from a multi-stakeholder approach. Cooperation enhances dialogue and coordination, enabling the creation of a more comprehensive cybersecurity field of application. Information sharing is difficult at best between different disciplines, and within private sector operators. It becomes increasingly so at the international level. However, the cybercrime problem is one of a global nature and is blind to national borders or sectoral distinctions. Cooperation enables sharing of threat information, attack scenarios and best practices in response and defence. Greater cooperative initiatives can enable the development of much stronger cybersecurity capabilities, helping to deter repeated and persistent online threats, and enable better investigation, apprehension and prosecution of malicious agents. National and international cooperation can be measured based on the existence and number of partnerships, cooperative frameworks and information sharing networks. The sub-group is composed of the following indicators:

1.6.1 Bilateral agreements

Bilateral agreements (one-to-one agreements) refer to any officially recognized national or sector-specific partnerships for sharing cybersecurity information or assets across borders by the government with one other foreign government, regional entity or an international organization (i.e. the cooperation or exchange of information, expertise, technology and other resources). The indicator also measures whether the agreement is legally binding or pending ratification. Information-sharing refers to the sharing of threat intelligence while assets designate the sharing of professionals (secondments, placements or other temporary assignments of employees), facilities, equipment and other tools and services.

1.6.2 Multilateral agreements

Multilateral agreements (one to multiparty agreements) refers to any officially recognized national or sector-specific programmes for sharing cybersecurity information or assets across borders by the government with multiple foreign governments or international organizations (i.e. the cooperation or exchange of information, expertise, technology and other resources). The indicator also measures whether the agreement is legally binding or pending ratification. Information sharing refers to the sharing of threat intelligence while assets designate the sharing of professionals (secondments, placements or other temporary assignments of employees), facilities, equipment and other tools and services.

1.6.3 Public-private partnerships

Public-Private Partnerships (PPP) refer to ventures between the public and private sector. This performance indicator can be measured by the number of officially recognized national or sector-specific PPPs for sharing cybersecurity information (threat intelligence) and assets (people, processes, tools) between the public and private sector (i.e. official partnerships for the cooperation or exchange of information, expertise, technology and/or resources), whether nationally or internationally.

1.6.4 Interagency partnerships

This performance indicator refers to any official partnerships between the various government agencies within the nation state (does not refer to international partnerships). This can designate partnerships for information – or asset-sharing between ministries, departments, programmes and other public sector institutions.

Annex 2: Compendium on cybersecurity country case studies

This annex presents the Question 3/2 compendium of relevant cybersecurity activities being conducted by Member States, (including Member States' national experiences), organisations, the private sector and civil society at the national, regional and international levels. The compendium is based on contributions submitted during the 2014-2017 study cycle.

Member States' National Experiences Relating to Cybersecurity

Country: Korea (Republic of)

Document: 2/65

Title: Personal information breaches and countermeasures of the Government of Republic of Korea

Summary: Republic of Korea discusses their experiences with personal information breaches and countermeasures. This document discussed the loss of at least of 20 million bank and credit card users in Korea in January of 2014, as an example. The government of Korea developed four measures to respond to the breaches, which included creation of an atmosphere for activating private investment on information security, expansion of the information security budget in the public sector, government support for the information security industry as a new economic growth engine, expansion of training of information security experts, and reinforcement of response measures to cyber threats.

Background

As new information communication technologies and services such as cloud computing, SNS and big data develop, so do new threats, and at times they can outpace even the new regulatory requirements for information security. Recently, there has been increasing attention on these emerging technologies, services and the risks, challenges they present to those providing and utilizing them to assess their risks as well as the benefits.

Setting aside the benefits of these technologies and services, the cost of those challenges is enormous. According to recent study, the annual cost to the global economy from cybercrime is more than $400 billion.[3] A conservative estimate would be $375 billion in losses, while the maximum could be as much as $575 billion. Cyber threats, data breaches and high-risk vulnerabilities continued to grow, and the severity of these attacks have intensified, especially against financial and banking institutions as well as retail outlets. Nevertheless, governments and companies underestimate how much risk they face from cybercrime and how quickly this risk can grow.

Most of enterprises and public organizations have regarded the investment on information security as a mere burden so the level of investment ratio on information security remain still very low. Since the growth of electronically collected, transmitted, distributed and stored information has resulted in more and larger damages and data breaches present a costly and significant threat to companies in all lines of business, it is imperative to foster the capability of information security in both private and public sector.

The wide spectrum of cyber threats can have a disastrous impact globally, and it is desired that information on current cybersecurity challenges and national experiences from Member States in this regard are collected and shared.

Cases of personal data breach in the Republic of Korea

For the past few years, Korea has been experiencing massive data breaches in online game industry, e-commerce, financial industry, and so on. However, unprecedented credit card data breaches

[3] Net Losses: Estimating the Global Cost of Cybercrime, McAfee, June 2014.

panicked the whole nation. The personal data of at least 20 million bank and credit card users in Korea has been leaked January 2014, one of the country's biggest ever breaches.

Many major firms in Korea have seen customers' data leaked in recent years, either by hacking attacks or by their own employees. In the latest case, an employee who had been dispatched to upgrade the security systems of client card companies from personal credit ratings firm, Korea Credit Bureau(KCB), has been arrested and accused of stealing the data from customers of three credit card firms while working for them as a temporary consultant. Korean financial regulator, the Financial Supervisory Service (FSS) confirmed the total number of affected users as at least 20 million, in a country of 50 million populations.

The stolen data includes the customers' names, resident registration numbers (RRNs), phone numbers, credit card numbers and expiration dates. The employee later sold the data to phone marketing companies. And the case was much worse than initially thought. As the inspection of the authority went on, the scope of personal data leaked from the three major local credit card companies, snowballed to an unexpected scale. Many of the country's major financial institutions were affected by the leaks, too.

Personal data breach not only causes damages on brand reputation, but also make negative impact on confidence in online environment as a whole. For better and safer activities online, it is very important to make a concerted and comprehensive effort to prevent the incident beforehand and take appropriate measures for recovery.

Response and way forward

After thorough investigation and survey on current status of information security both in private and public sector, Korean government announced "Comprehensive Personal Data Protection Plan" in July and suggested investment stimulation as one of main objectives to prevent personal information breach and make safer online environment.

With the recognition that nationwide investment on information security is necessary to minimize the damages from data breaches and information spill, Korean government declared its intention to promote information security industry and train cybersecurity experts actively while fostering conditions for the voluntary investment on information security in private sector.

Among major schemes, Korean government has unveiled the plan which involves 5 main measures to expand the information security market size to double by 2017. The measures and detailed plans are as follows:

- The first measure involves the creation of atmosphere for activating private investment on information security. For this purpose, various incentives would be provided such as deduction of tax payment for SMEs that invest on information security facilities and products, advantages for enterprises which abide by government guidelines on information security when they apply for the government projects, and incentives for SMEs which hire information security experts.
- The second measure involves the expansion of information security budget in public sector. For this purpose Korean government plans to develop the information security budget appropriation guideline and raise the ratio of information security budget compared with informatization budget to 10 per cent until 2017. Also government plans to develop the guideline for calculating cost of information security services and standard form for information security service contracts in public sector.
- The third measure involves the government support for information security industry as a new economic growth engine. Korean government plans to develop the information security roadmap for Internet of Things (IoT) in 2014 and establish test bed, secure imbedded OS, and so on. In addition, government plans to develop 10 advanced information security technologies and products including cyber black box, anti-APT tools. Furthermore, government plans to develop

technologies that can guarantee the certain level of security of personal information such as light encryption technologies that can be utilized in various devices while preventing the falling off in quality of the performance of encrypting personal information and detection technology of information extraction by newly raging malwares.

- The fourth measure involves the expansion of information security experts training. Korean government plans to proceed the education and management system of core information security experts. First of all, government plan to foster approximately 5,000 most elite experts on information security by 2017. Government also plans to establish curriculum of special education for the gifted and create the cyber security specialized corps, units, and reserve forces so that information security experts should be able to continue their career in this area seamlessly.
- The last involves the reinforcement of cyber threats response measures. Development of cyber trap system (honeypot) which can collect and analyse the malicious codes automatically by 2015 and verification and treat system for the smishing (SMS phishing) by the end of this year. In addition, cyber threat information sharing with relevant organization will be proceeded. The reinforcement of 24 hours and 7 days monitoring system on various channels abused as malware distribution is one of major steps for the countermeasures as well.

With above plans, Korean government also introduced a new alternative for RRNs for those who do not feel comfortable giving out their precious and unchangeable security number for routine transactions. RRNs, which is the basic Korean ID numbers, are needed for signing up for cell phone contracts, registering for employment, and making a bank account. However, in Korea, this 13-digit ID number, which contains a lot of unchangeable information such as sex, date of birth and place, are used for even more daily routine activities such as purchasing movie tickets via smartphone, buying a train ticket, or buying really anything online at all. However after scandals and data leaks in the past few years that led to security breaches that exposed personal information of millions from financial institutions, the government has decided to issue alternative numbers named “My PIN” that can be used instead of RRNs. The Korean government is confident that the new numbers are safer since they can be changed if they are lost or stolen whereas RRNs are permanent.

It is true that regulatory measures never take up the speed of technological advance, but with more concerted effort for the information security with cooperation among relevant stakeholders, cyber space could be preserved more safe and secure. For this purpose, it is imperative that cyber space is protected through the active investment on the information security and it is necessary to foster virtuous circle in information security industry. In addition, it is important to make an effort to realize secure cyber society as we proceed with informatization.

Country: Korea (Republic of)

Document: SG2RGQ/64

Title: Korea’s Internet of Things security roadmap

Summary: This contribution discusses a cross-sector approach released by the Korean government in September of 2014 for addressing security concerns relating to the Internet of Things that will include response mechanisms, anti-hacking mechanisms, and a new project “Secure Dome”.

Background

It is expected that threats on current cyberspace will be transferred to and expanded into the real world in the Internet of Things (IoT) environment in which all humans, devices and data are interconnected.

Governments are placing big bets on the IoT era, in which physical objects, infrastructure and system are widely connected to the Internet. This new era is expected to increase productivity and efficiency across all industry sectors.

Korea, which has played a leading role in ICT since 1990s with its advanced internet infrastructure and semiconductor technology, aim to take the leadership in this emerging trend. The Internet of Things as a huge transformative development – a way of boosting productivity, keeping people healthier, making transport more efficient, reducing energy needs, and tackling climate change, will lead a new industry revolution.

In May 2014, The Korean Ministry of Science, ICT and Future Planning (MSIP) announced IoT master plan to boost the ecosystem in this sector by encouraging the development of both software and hardware and removing the unnecessary regulations for the growth of the IoT. It is expected that more than dozens of small and medium enterprises in the IoT sector will be supported based on the government's employment road map.

Despite promising outlooks and commitments from the public and private sectors, however, security threats increase as well amid the rising tide of IoT. This could result in more serious damage than in the personal computer era. For example, hackers can figure out when people go to bed and wake up, what kind of food they eat and what time they go to work by analysing the things, such as home appliances, automobiles and electricity they use. Connected automobiles can also be infiltrated by hackers, allowing them to control the engines, brakes and doors. And people of all ages use smart devices, such as smartphone, tablet, and other wearable devices nowadays, which play pervasive role in the IoT, anytime and anywhere. Since those smart devices store a lot of personal data, the impact could be devastating once those devices are hacked and infiltrated. Since many of those smart devices users are not familiar with how to cope with these vulnerability, they are exposed to exploitation all year round.

Internet of things security roadmap of Korean government

Since utilization of IoT will be directly intertwined into our daily lives by using consumer electronics, medical devices and so on, threats on IoT will be devastating as much as life threatening and also it will be very difficult to amend its security vulnerabilities or cost after full implementation. So it is high time for us to make a comprehensive plan for this urgent issue.

Korean government released in late October 2014, a policy roadmap on information security for the Internet of Things, and outlined that the development of the IoT has caused a paradigm shift in the threat to information security which places a focus on security by design.

The principle of protecting the information and function will be embedded in the development of related product and service from early stage of designing process across seven core sectors of IoT, which include home appliance, medical treatment, transportation, disaster, manufacturing, construction and energy. The government decided to propose three main security principles for structural design of the products as well as for the development of core elements and across the stages of supply chain. There will also be development of and assistance for security considerations for each sector. An information sharing and analysis system or IoT-ISAC will be established to study the weakness of respective product and service. For that purpose, the government plans to prepare a comprehensive response system stage by stage, so that it could respond promptly on the infiltration attempt. A national computer emergency response team will be developed, separate from the existing system of handling cyber threats to the Internet, with the exclusive aim of providing anti-hacking solutions based on information sharing and analysis of vulnerabilities specific to Internet of Things products and services. Also data security standards will be developed for the risk management throughout the entire supply chain from product and service design to deployment and maintenance, while security certification schemes will be introduced to help consumers and businesses make informed decisions on smart devices and services.

Also a project called 'Secure Dome' will be launched to further the development of next generation IoT security technology. The Secure Dome Project will pursue development of nine major core technologies related to security that includes light-weight low-voltage encryption technology, security System-on-Chip (SoC), security operation system, security gateway, infiltration detection technology, security control system, smart certification, privacy protection technology and adaptive IoT security solution.

An audition program for IoT research and development also will be introduced. The government will provide R&D budget by way of competition or through the evaluation of the results of the prior research and development.

There will also be a full launch of demonstration project for the IoT security applied to seven major areas of IoT services that include smart home, smart car, smart factory, etc. A basic training for information protection and certification system for security will be introduced to engineering colleges. A project titled 'IoT Security Brain' which aims to foster talents in the combined field of security-convergence will also take off.

Conclusion and way forward

The IoT is emerging as the next technology mega-trend. By connecting to the Internet billions of everyday devices – ranging from fitness bracelets to industrial equipment – IoT merges the physical and online worlds, opening up a host of new opportunities and challenges for companies, governments and consumers.

Korean security roadmap for IoT will implement essential infrastructure and technology components by 2018 to provide a safe environment for the use of Internet of Thing. It will serve as a platform for developing data security and privacy protection policy programs in each target area between 2015 and 2018.

Country: Korea (People's Republic)

Document: SG2RGQ/142 + Annex

Title: Safe use of the Internet for children and youth in Korea

Annex title: Online ethics

Summary: In this contribution the Government of Korea shared its national experience in implementing strong measures to ensure online safety of children and adolescents, including the legal measures it adopted, as well as the challenges and implications of this experience.

Background

Most of the people using the Internet enjoy conveniences and efficiencies provided by a variety of good online services and activities. However, as a concomitant to the benefits of online activities, harmful consequences such as illegal and inappropriate content, dangerous and seductive contacts, improper treatment of privacy and personal information, online bullying, etc. are also occurring. As the average age of children having access to and using the Internet goes down, the safe use of the Internet among children is becoming a hot issue in most countries. In this regard, Korea is very active in taking measures to ensure the online safety of children and such measures range from legal and compulsory ones to online safety education.

Legal measures for the online safety of adolescents

Various social measures are initiated in Korea for children's safe use of the Internet. Concerning legal measures, all minors under the age of 16 are not allowed to have access to online games from 24:00 AM to 6 AM under the Juvenile Protection Act.

The Act on the Promotion of the Use of Information Network and Protection of Privacy obliges adult content providers to indicate a clear and visible notification of "not allowed for minors less than the age of 19" via signs · symbols· numbers · sounds, etc., block improper keyword searches of adolescents, and inform the service users (site visitors) of the legal enforcement (penalty) for the violation of adolescents protection. More stringent rules are imposed to adult content providers and major service providers (whose annual turnover is more than 1 Million USD or the number of visitors to their website is more than 100,000 per day), such as the appointment of adolescent protection officers and public release of the information of adolescent protection officers (name, position, phone number, e-mail etc.) in the front page of their website. The roles of adolescent protection officers include making an annual plan to protect adolescents online, blocking adolescents' access to adult content, providing training of staffs about measures to protect adolescents, and receiving and handling users' complaints or damages caused by improper services of adult content.

The Telecommunications Business Act orders telecommunications service providers, when making a service contract with minors under age 19, to inform the minors and their guardians (parents) of filtering tools to block illegal and harmful content, and must let minors or their guardians install a filtering tool to the minors' telecommunications device. If the filtering tool is removed from the device or set to be inactive for more than 15 days, the service provider must inform the guardian immediately.

Online safety education

Online safety education has been provided from 2002 by National Information Society Agency with the financial support of the Ministry of Science, ICT & Future Planning and the Korea Communications Commission. Such education programs have been offered to more than 500,000 persons including children, teachers and parents every year since 2002.

Education for pre-schoolers are carried out by specially designed tools and Puppet shows throughout 1,200 kindergartens. Pupils in elementary schools participate in cyber ethics and safety education programs consisting of off-campus activity-based learning programs and club activities such as the Korea Internet Dream Star Program. 650 elementary schools per year participate in these cyber ethics and safety education programs.

Students in middle and high schools attend cyber ethics and safety classes, which are taught by specially trained lecturers. Some schools run an intensive program composed of group discussions, poster or essay competitions for cyber ethics and safety, and street campaigns to promote the importance of cyber ethics and safety. Annually, around 1,000 middle and high schools participate in these cyber ethics and safety education programs.

Physically disadvantaged young people should not be excluded from these cyber ethics and safety education programs. In Korea, 50 special schools have been given opportunities to participate in cyber ethics and safety education programs with the assistance of customized training materials and monetary support for the operation of cyber ethics and safety education programs.

The role of educators and parents is very critical in raising children's and youth's awareness about cyber ethics and safety. For this reason, the Korean Government offers specially designed training programs to improve the knowledge and understanding of teachers and parents on the issues of cyber ethics and safety. Every year, more than 4,000 teachers and 150,000 parents and adults participate in online and offline classes for cyber ethics and safety training.

More details of Korea's cyber ethics and safety education programs are provided in the attached document.

Challenges and implications of Korea's experience

Online safety for children requires not only legal and compulsory measures but also self-regulating voluntary measures. Legal and compulsory measures may lead to visible and prompt effects, however, it may infringe individual freedom or the autonomy of service users. For instance, the introduction of the rule blocking minors' access to online games from midnight triggered a hot debate about the validity and effectiveness of this measure and the legal rights of minors. The opponents of this measure assert that minors can avoid this rule by using another person's ID, and this rule infringes on minor's rights to control their own use of online games, as well as on parental rights to guide their children's use of online content. In this sense, the Korean government has been providing online safety education for children, parents and teachers in addition to legal and compulsory measures.

Another issue of online safety for children is the division of roles/responsibilities between service providers and service users. Parents may assert that service providers have to pay more efforts to the online safety of children in delivering their services, however, service providers may insist that parental guidance and awareness or education of adolescents is a more effective measure to ensure the online safety of children. Therefore, it is required for the government to keep the balance between the roles/responsibilities of service providers and users in the efforts for the online safety of children.

Challenges Korea is currently faced with is to motivate all related stakeholders to participate in efforts for children's safe use of the Internet. Despite the active initiatives taken by the government, the participation of private sectors, such as civil society and service providers, has been relatively low. The safe use of the Internet requires the close cooperation among families, schools, communities, work places, and online content providers, and thus the online safety of children cannot be achieved by the efforts of the government alone. Therefore, from now on, the Korean government's role in supporting and coordinating relevant stakeholders to encourage their active participation in nationwide online safety efforts is all the more important.

In concluding, it is hoped that the information this contribution provides will serve as a useful resource for countries preparing to initiate online safety programs for children and adolescents. Furthermore, it is suggested that Member States and organizations also share their experiences on the promotion of cyber ethics and safety for children and adolescents.

Country: Cameroon (Republic of)

Document: SG2RGQ/30

Title: Main cybersecurity activities in Cameroon

Summary: This contribution provided an overview of Cameroon's Internet deployment, and discusses an audit of cybersecurity in accordance with ISO-27002. The contribution also provides an explanation Cameroon's CSIRT, CIRT-ANTIC, which was set up with the assistance of IMPACT in 2012.

Introduction

Cameroon is a country on the Gulf of Guinea, with a surface area of around 475 442 km^2, which shares borders with Nigeria to the west, Chad to the north, the Central African Republic to the east, and Congo, Gabon and Equatorial Guinea to the south. Its population was estimated at 22.25 million in 2013, with a gross national income per inhabitant of USD 1 290. With over 200 ethnic/linguistic groups, two official languages (French and English) and great cultural and climatic diversity, Cameroon has aptly been named "Africa in miniature".

Cameroon has four major telecommunication operators: Camtel, the historical operator, which remains public despite several unsuccessful attempts to privatize it; Orange and MTN, which have been present on the Cameroon market for over 15 years (1999 and 2000); and Viettel, which has

been operational since 18 September 2014. The telephone penetration rate stood at around 70 per cent in December 2014, having been less than 1 per cent in 2000. There are an estimated 1 486 815 Internet users, corresponding to a penetration rate of 6.4 per cent (2 per cent in 2006). With MTN and Orange having been allocated 3G licences when their operating licences were renewed, the number of Internet users is sure to rise significantly over the coming years.

Within this context, the issues of cybersecurity and the fight against cybercrime must be taken seriously. A law along these lines was promulgated in 2010, and since then numerous activities related to cybersecurity and the fight against cybercrime have been undertaken.

Audit of network security

The regular audit of the security of networks and information systems, which is the responsibility of the National Information and Communication Technologies Agency (ANTIC), is mandatory (Article 13 of the Law on Cybersecurity). The audits are carried out by ANTIC officials or by approved external auditors. The activity commenced effectively in 2013. Seven private audit firms have been approved by the minister responsible for telecommunications, based on files comprising, ***inter alia***, proof of the qualifications of staff to audit information system security (CISA certification or equivalent). However, the procedures for assigning the entities to be audited to the different audit firms are still under development, as the principles of competition and transparency must be obeyed.

The approach recommended is that of developing healthy competition between the external auditors, in order to reduce the costs borne by the entities audited while ensuring the reliability of the audit. The audits produce an audit report which is used to establish, in agreement with the entity audited, any corrections required to its network to enhance its security or remedy the shortcomings identified, along with an implementation schedule. The security audit standard used is ISO 27002. Between 2013 and 2014, 39 administrations and 16 public enterprises/establishments were audited and 2 435 vulnerabilities noted.

Security monitoring

Since 2012, Cameroon has had a computer incident early warning and response centre (CIRT-ANTIC), set up with the support of ITU and the International Multilateral Partnership against Cyber Threats (IMPACT). The basic missions of the centre are to centralize requests for assistance resulting from security incidents (attacks and intrusions) on networks and information systems, process the incidents, react to computer attacks (technical analysis, exchange of information with other structures of the same kind), and establish and maintain a database of vulnerabilities.

CIRT-ANTIC also provides prevention by disseminating information on precautions to be taken to minimize the risk or consequences of incidents. It oversees the critical Internet resources of Cameroon's cyberspace (IP addresses, DNS servers, web servers, message servers) to ensure their availability or detect potential attacks on them. Although CIRT-ANTIC was set up with a view to national coverage, its activities are focused for the time being on public and parastatal administrations and organizations. Within this framework, on a daily basis CIRT-ANTIC scans the various systems monitored. It issues vulnerability warnings in real time, which are communicated to the technicians responsible for the information systems. General alerts are issued for the general public, and are consultable on the website www.antic.cm. In 2014, CIRT-ANTIC recorded 300 cases of scamming, 50 phishings, and 18 web defacings.

Other cybersecurity activities

Numerous training or awareness-raising sessions are organized for users in general, or for specific user groups, nationwide. Electronic media are also used, notably in the form of radio or TV programmes to provide mass awareness-raising on cybersecurity.

The formal identification of SIM card holders has been mandatory since 2011. This is carried out by operators under the supervision of the Telecommunications Regulatory Authority.

Conclusion and way forward

Numerous cybersecurity initiatives are under way in Cameroon, reflecting real awareness of the stakes involved with cybersecurity. However, there is still no national cybersecurity policy. It is also important to review the legal and regulatory environment, at least in order to take into consideration the commitments made through the African Union Convention on Cybersecurity and Personal Data of 24 June 2014.

Country: Russian Federation

Document: 2/369

Title: The experience of the CIS countries in the field of experts' professional competences formation on data protection and information security in information and communication systems

Summary: This document from the Russian Federation presents the results of the project in the framework of the Regional Initiative 5 CIS region "Building confidence and security in the use of ICTs" in terms of human capacity building in the field of information security. The state of affairs in the region is analyzed, recommendations for the formulation of requirements to system of training and retraining of specialists on the basis of competences formulated professional infocommunication community as well as themselves competence are given.

Introduction

Issues of building confidence and security in the use of ICT in the CIS region are in charge of the Information Security Commission of the Regional Commonwealth in the fields of Communications (RCC). Acknowledging that the relevance and ensuring technological independence and information security of the state are the strategic objective, the heads of the CIS states in October 2008 approved the Concept of cooperation of the States – participants of the CIS in the sphere of information security and a Comprehensive action plan for its implementation. Enactment of these documents promoted further forming and enhancement of the legal basis for an interstate cooperation in this sphere and the establishment of a secure information environment in the CIS.

Information Security Commission has prepared a draft Agreement on cooperation of states – participants of the CIS in the field of information security and the Regulation on the basic organization of CIS Member States, which provide methodological, organizational and technical support for the work in the field of information security and the training of specialists in this field.

At the same time there was an inquiry of administrations, regulators and the CIS region's business to determine common requirements for training of specialists in information security. They should take the form of requirements for appropriate educational standards and are embodied in these standards. According of such factors as historical community of the educational systems of the CIS countries and their current compliance with the terms of the Bologna agreement, allows a large extent unify and make regional standards of training, including such specialties as "Information Security Specialist of Information and Communication Systems" "The system administrator of information and communication systems"; "Specialist in Administration of network devices of information and communication systems"; "The system programmer"; "Specialist in design and graphic user interfaces"; "Technical support specialist of information and communication systems". The corresponding functional cards of labor activity types, the characteristics of the generalized labor functions, necessary knowledge and skills form a basis for training of specialists, in one way or another responsible for building confidence and security in the region.

Competence-based approach in educational activity and its interface to inquiries of employers

The modern needs of the labor market for specialists of a certain qualification are increasingly placed at the forefront in reforming the educational systems of countries in various regions. These requirements directly affect the modular structure and the flexibility of education in the 48 countries that joined the Bologna Declaration (1999). This process is active in the CIS region. In different countries the professional ICT community formulates its requests in the form of the direct order both to system of professional training, and subsystems of retraining and advanced training. This social order is a list of specific competencies that form the ability to apply knowledge, skills and personal qualities to be successful in a particular field. Competencies and learning outcomes are seen as the main target setting in the implementation of vocational training programs as the integrating beginnings of a graduate's "model".

The competence-based model of the graduate, on the one hand, covers the qualification linking his future activities with the subjects and objects of labor, on the other hand, reflects the interdisciplinary requirements to the result of education.

As a result of discussions in the professional community, the features of key professional competencies have been formulated, they:

- Allow to solve complex tasks (non-algorithmic);
- Are multifunctional (allow to solve different problems from one field);
- Transferable to different social fields (different activities);
- Require complex mental organization (the inclusion of intellectual and emotional qualities);
- Are complicated to implement and require a set of skills (skills of cooperation, understanding, reasoning, planning...); and,
- Should be implemented on different levels (from elementary to profound).

Advantages of competence-based approach are in the fact that at the same time:

- The goals and objectives of training programs conforming to requirements of employers are formulated;
- Flexibility of training programs increases;
- Efficiency and quality of professional training, level of professional competences increases;
- Standard, objective and independent conditions of a training quality evaluation are created;
- Level of interaction and the mutual responsibility of students, teachers and employers increases;
- Preparation for professional activity is carried out taking into account the real production conditions, due to which accelerated adaptation of professionals in the workplace; and,
- Formed organizational culture, including the field of information security.

Competences of experts in information security as basis for creation of the corresponding human potential

Focusing on the labor market needs in the field of training and retraining in the application of ICT security experts, the required competences can be divided into several blocks:

1) The general professional competence of providing including the ability to:
    - Undertake the operation of infocommunication systems (ICS) with the use of methods and means to ensure their safety;
    - Administer software and hardware protection of information in the ICS;

- Carry out the work on assessing the safety of ICS; and,
- Build distributed protected ICS.

2) Competence in the ICS operation using software methods and tools for their safety, providing including the ability to:
   - Provide the information security (IS) in ICS with software and hardware;
   - Provide the information security (IS) in the ICS using technical means; and,
   - Provide information security (IS) in ICS with a complex application software, hardware and technical resources.
3) Competence in the field of management software and hardware protection of information in the ICS, including providing skill to:
   - Configure software and hardware ICS protection;
   - Perform maintenance regulations and current repair of software and hardware tools of information protection; and,
   - Carry out the analysis of the violations allowed by users in ICS and to hinder with their repetition.
4) Competence in the field of the assessment ICS security:
   - The monitoring of the efficiency and effectiveness of hardware-software means of information protection;
   - The application of methods and techniques for ICS safety assessment under protection system control analysis;
   - Carrying out experimental and research works in case of objects certification taking into account requirements to ensuring ICS protection;
   - Instrumental monitoring of the ICS protection; and,
   - Expertise in the investigation of security incidents.
5) Competences in the area of distributed protected ICS design:
   - Development of requirements for distributed secure ICS and remedies for them, taking into account existing regulations and guidance documents;
   - Design of the distributed protected ICS; and,
   - Commissioning and maintenance of distributed ICS with the protection of information resources, organizational and technical measures for information security.

Each of these competencies is accompanied by a list of actions committed by labor and the necessary knowledge, abilities and skills.

Conclusion

Human capacity building to enhance confidence and security in the use of ICT is an urgent task, which requires the business partnership as the customer, the educational system as a contractor and the state as regulator of the entire process. Business priority in the formulation of requirements for specialists guarantees the success.

As a result of the project for the implementation of the Regional Initiative 5 in the CIS region has developed standard professional competencies, which are put at the forefront in the creation of educational programs in the field of training and retraining of information security specialists.

These competencies are complemented by a specific list of employment action, knowledge and skills that allows both carrying out examination of educational programs and creating new programs

of training and retraining for building confidence and security in the use of ICT in the region. Dissemination of results in the region will be implemented within the framework of the ITU project "Centre of Excellence" in the CIS region in the area of "Cyber security", which is a priority for the region and assigned to the main contractor of the Regional initiative 5 – Moscow Technical University of Communications and Informatics, a member of ITU-D.

The obtained results should be used to enhance the use of ICT awareness activities to build confidence and security in different countries, particularly developing countries, as they have a number of valuable qualities: relevance trends of infocommunications, compliance with modern educational trends and international standards of construction of educational process, scalability and reproducibility.

Country: Norway

Document: SG2RGQ/204

Title: Creating a metric for cyber security culture

Summary: The Norwegian Centre for Cybersecurity (NorSIS) has conducted a study to provide new insight in the Norwegian Cybersecurity culture. The study aims to develop grounds for effective cyber security practices and to improve national cyber resilience. The study included method development for a metric for cybersecurity culture, as well as an extensive national survey. NorSIS recently published the report "The Norwegian Cybersecurity Culture", which includes a full description of the method, as well as the key findings from the national study. We encourage other nations to make use of the method, and to share the results with an international community.

Introduction

The Norwegian Centre for Cybersecurity (NorSIS) has conducted a study to provide new insight in the Norwegian Cybersecurity culture. The study aims to develop grounds for effective cyber security practices and to improve national cyber resilience. Cyber criminals and foreign intelligence agencies have over time analysed our cultural characteristics to disclose vulnerabilities to exploit. This gives them definite advantages. Therefore, we should feel obliged to increase our understanding of the dynamics in how a cyber security culture is shaped and how it affects the digitalization in businesses, sectors and on a national level. Human factors have long time been recognized as fundamental to cyber security, but so far efforts to understand this important phenomenon has been limited in scope. NorSIS sees mapping cyber security culture as a way of understanding yourself, your company and your country.

In order to create a resilient digital Norway, it is paramount that the government apply a holistic approach. The study shows that it will be necessary to increase the reach and quality of cyber education, establish effective online law enforcement, and engage private and voluntary sector in a struggle to increase the national "cyber hygiene".

The need for a cyber security metric

Our society is undergoing a fast-moving digitalization in both private and public sector. Manufacturing, products and services are digitized, causing our national economic growth to be strongly linked to the digitalization efforts. The digitalization has the potential to create economic growth and welfare through national and global trade, and more efficient public services. However, this potential is nearly eliminated as a result of an increased level of cybercrime. When adding the fact that foreign powers are stealing Norwegian technology research and development, the very thing our future generation will base their economy on, we understand that we need to do more to safeguard and protect our national ability to freely utilize the tremendous power that lies in the digitalization.

For a nation, a deeper understanding about a cyber security culture is of utmost importance as it touches upon some of the most profound questions for development. Not only does digitalization help businesses make smart use of information technology and data, it ensures citizens benefit from the digital age and it underpins economic growth. A safe e-citizen is fundamental to the success of the national digitalization. Mistrust in digital services and fear of online crime are some of the challenges that people face in the digitalization processes. Thus, we must understand the dynamics in how a cyber security culture is shaped and how it affects the digitalization in businesses, sectors and on a national level.

Measuring cybersecurity culture

In creating a metric for measuring the national cybersecurity culture, there are at least two critical challenges: One is the question of terminology, i.e. what do we actually mean when we refer to "cybersecurity culture"? The other is the level of analysis, i.e. how can we identify a "cybersecurity culture" concept that is valid and applicable to both businesses and nations? That is to say that whilst the concept might be developed within the confines of industries and businesses focused on cybersecurity, also nations have "cybersecurity cultures". It may, however, not play out the same way. There is a huge gap in how "culture" is shaped and expressed depending on the level on which it is discussed. For example, whereas a business, an organisation and an institution all have defined purposes and thereby measures, the scope of a nation is much vaguer.

Secondly, while business can actively tutor and educate their personnel in cybersecurity, citizens of a state cannot be equally monitored. Is it, then, possible to generate a general comprehension of "cybersecurity culture" that is equally applicable to business and nations?

We believe that measurements of cybersecurity cultures can benefit from a more comprehensive approach, taking a step back from simple registrations of whether employees open phishing-emails and rather look at the attitudes and perspectives towards technology and cyber security, and how this resonates with other core values, interests and abilities.

Understanding cyber security culture: Key components

Among the features that differentiates nations, culture is one of the most dominant ones. All nations have cultures. National cultures shapes who we are as a group, and how we as individuals orient ourselves in the world. In other words: National cultures functions as glue amongst the citizens, and relates to our deeply held values regarding such as what we consider as normal versus abnormal, safe versus dangerous, and rational versus irrational. Our national cultures offer a set of values that help us make sense of our surroundings by establishing a compass that tells us "how we do things". The result is that national cultures comprise systems of shared values, preferences, and behaviours of population groups that differ widely between countries. These cultural values and norms are learned at an early stage in life, and is passed on both formally (at school, our workplace, in our leisure time activities etc.) and informally through interaction with friends, parents, siblings and others. As a result, national cultures are deeply rooted in us, and last over the course of generations.

Cybersecurity cultures have so far been considered a part of organizational cultures, thereby a concern for businesses and industries. As a consequence, cyber security culture has been treated as a tool for organizational efficiency and success. Yet, organizational cultures differ from national cultures on the most fundamental level: Whilst national cultures concern the shared values and norms, organizational cultures are based on shared practices.

Organizational cultures are based on broad guidelines, which are rooted in the organizational practices that businesses not only teach their employees; organizational cultures are comprised of norms and practices that businesses expect their employees to follow. If they do not act according to them, they may lose their jobs.

This is of course not to say that organizations' cyber security cultures are less significant. However, they are something else than national cyber security cultures. Moreover, they are less deep-seated than cyber security cultures on a national level.

There are a number of definitions of cyber security culture, and whilst there is as of yet not one definition all cyber security professionals seem to be able to gather around, they all converge around the same key issues: All security is about the protection of assets from the various threats posed by certain inherent vulnerabilities, and cyber security is consequently about protecting the information assets. Cyber security culture, then, is the attitudes, assumptions, beliefs, values, and knowledge that people use in their interaction with the information assets. Thus, cyber security culture is comprised of behaviour and a set of values, ideas and attitudes.

Thus far, most studies of cyber security culture focus on the behavioural dimension. That is, they focus e.g. on the degree to which employees click on phishing links, or whether or not they share their passwords. As a consequence, although the general notion is that cybersecurity culture contains elements of values and attitudes, the way it is dealt with tend to set these elements aside in favour of a focus on behaviour.

As we see it, the focus on behaviour in the context of cybersecurity culture can say something about what people are doing or have been doing. In other words, focusing on behaviour can project an image of security conduct in the past ("this is what they did"), but it can say relatively little about the future. Yet, we strive to increase security predictions. That is to say that timely security measures must be one step ahead. Thus, instead of being able to portray what people have done or how people have used to behave, one should rather be able to have a credible prediction of what people are most prone to do in certain situations. In our approach to cybersecurity culture, then, we have chosen to downplay behaviour and rather focus on attitudes, values and sentiments that can say something about what people will do, or how they will respond.

In our study, we have mapped the core traits of the national cyber security culture in Norway. We departed from the assumption that national cultures – and thereby also cyber security cultures – cannot be approached merely as behaviour: Rather, the national cyber security culture ought to be considered as a set of values, sentiments and attitudes regarding a given topic, i.e. cyber security. Cyber security on a national level relates to a wide set of themes, ranging from governance and state control to individual notions of technological competence and risk-taking.

Any culture balances between the individual and the collective, between individual judgements and perceptions and collective norms and standards. We are neither completely individual, nor are we completely part of the larger collective. Conceptualizing cybersecurity culture, then, implies pinpointing those factors that not only comprise cyber security culture as a whole, but that also highlight the central debates and challenges of cyber security culture that together constitute the building blocks.

In the following we will present the eight core issues that comprise cyber security culture as we see it. These are: Collectivism, Governance and Control, Trust, Risk perception, Digitalization-optimism, Competence, Interest and Behaviour.

– **Collectivism**

Cultures are per definition collective. Cultures are developed by individuals, whilst at the same time contribute to shaping the individuals that are part of any given culture. Cultures point to the characteristics of a particular group of people, including such as their social habits, their attitudes, their values and priorities. Cultures necessitate some degree of solidarity amongst the members. That is to say that in order to last, cultures necessitate loyalty and solidarity. The individuals must identify themselves as part of the group, contribute to it, and adhere to the explicit and implicit norms of behaviour. When singling out collectivism, we wish to point towards how the individual relates to the collective.

– **Governance and control**

With reference to collectivism, governance is a collective term that refers to the questions of how the collective should be regulated and by whom. Hence, the issue of governance refers to the users' views on governance and control of information and communications technology (ICT). A critical issue here is e.g. the question of surveillance: Who are responsible for drawing the red lines of what is acceptable in the use of ICT, where should these lines be drawn and how should citizens abide to these lines?

By raising the issue of governance, then, we wish to draw attention to the question of who is responsible for our safety online. In the context of security, there is always the question of how to balance between individual freedom and collective safety. "Everybody" wants freedom and "everybody" wants at the same time to be safe. How does this balance play out in a given cyber security culture? How much surveillance is acceptable when individual safety is at stake?

– **Trust**

Trust is a cornerstone to any viable democracy. Democracies depend on trust in a whole variety of forms: A well-functioning democracy necessitates trust amongst its citizens, amongst citizens and the government, between governmental institutions, between business, between citizens and their employer and so forth. In other words: Trust is a prerequisite for economic welfare, stability and growth in a country. As more and more of our national growth is tied to the digitalization of the nation, trust in this area is of great significance.

For authorities to govern efficiently and in accordance with the law, while at the same time maintaining stability, they need not only to have the jurisdiction on their side: They need trust from the citizens. This implies that authorities must be allowed to govern also when e.g. executing policies that citizens may disagree with, or when implementing measures that are alien or new to citizens.

– **Risk perception**

Competence, learning and risk are tightly knit together. Risk perception is also highly subjective, and it's a powerful factor that greatly influences how we think and act when it comes to digital threats. It is a factor that, to some degree, can't be calculated or predicted, although we know that it can and will be influenced by security events, what we think we know about digital threats, our experiences in the past etc.

– **Digitalization-optimism**

By focusing on techno-optimism and digitalization we want to transgress the mere fact that digitalization is part of how our societies develop. Instead, we want to draw attention to citizens' attitude towards this societal tendency. In other words: Your attitude towards digitalization influences how you relate to technology. A safe e-citizen is fundamental to the success of the national digitalization. Mistrust in digital services and fear of online crime are some of the challenges that people face in the digitalization processes. Thus, we must understand the dynamics in how a cyber security culture is shaped and how it affects the digitalization in businesses, sectors and on a national level.

– **Competence**

As everything from social services and state tax payment to individual communication and the sharing of holiday photos are happening online, citizens are forced to make use of ICT regardless of whether they appreciate it or nor. This implies that citizens must acquire a digital skill-set that makes them capable of being part of modern society. Consequently, all citizens of Norway must have fundamental digital skills. The question is: Where and how do they acquire this skill-set? The paradox today is that most countries push their citizens to go online, and our societies' development depend on a comprehensive process of digitalization. Yet, a thorough digital skill-set is rarely taught in schools. The general public must therefore acquire this skill-set through informal channels. By focusing on this, we explore how and by whom people learn about cybersecurity.

– **Interest**

In a society that is increasingly digitalized, one may be tempted to conclude that citizens with an interest in ICT have an advantage over those citizens that lack this interest. Interest shapes our attitudes, our skills and our knowledge. Interest influences who we relate to and thereby who we learn from. With interest comes awareness, curiosity and time. These are cornerstone in learning. It follows that one may wonder whether people with an interest in ICT learn faster than those who lack such an interest. Therefore, interest appears to be decisive in a digitalized society.

– **Behaviour**

In terms of cyber security there are certain types of behaviour that are encouraged, whilst others are warned against. Governments, authorities, business leaders and experts provide advice that form a normative standard for how citizens or employees should behave. However, given the rapid development of technology, this "best practice" standard is perishable. That is to say, that expert advice and norms for ICT behaviour have changed over time. As a result, going through training and courses in information technology once does not suffice: It must be repeated.

Measuring the behavioural patterns of the Norwegian cyber security culture implies two things: Firstly, we want to paint a general picture of the behaviour of Norwegians in the context of cyber security. Secondly, we want to see to what degree Norwegians comply with the "best practice" norms of behaviour communicated to them.

Key findings

The study is unique as we encompass a broad approach to cybersecurity culture, and because the scope is much larger than any study we are aware of. We worked with 29 partners in the public and private sector, and reached 150.000 individuals in Norway. Our key findings are:

– **Fear of cybercrime creates a chilling effect on the digitalization process**

Although most people (approximately 90 per cent) thinks that the police should handle online crime, far less (46 per cent) trusts that the police will be able to help them. The police reported in 2015, that a mere 13 per cent of individuals that are victims to online crime actually files a police report. At the same time, as many as 44 per cent thinks that individuals and activist groups has a role to play in the fight against online crime. Apart from the fact that such involvement may cause suspicion towards innocent, let the guilty go free and tamper with ongoing investigations, we believe that it may cause a chilling effect for the digitization efforts. 44 per cent reports that they have abstained from using online services due to digital threats. Norway is currently undergoing a digital transformation in both public and private sector, and this development is worrying.

– **The Norwegian citizenry is not properly educated in cybersecurity**

The government is not educating the population in cybersecurity, despite that the digitization demands it. The society expects the individual to know how to protect themselves from digital threats. We find that only 50 per cent of the population has received cybersecurity education during the last two years, and that businesses are taking that responsibility upon themselves. This causes vulnerable groups to be left out, such as the young and the elderly.

– **There is a low awareness of the concept of online hygiene**

People see cybersecurity as a means to protect themselves, but are not aware of the complex co-dependencies in a digitized society. In short, cybersecurity to them is about protecting themselves, not the people around them. In a digital world, everything is connected to everything else. Long and complex digital value-chains makes up our critical infrastructures, our financial systems etc. Our study reveals shortcomings in the way cybersecurity is taught today, and we need to develop new educational methods if we are to prepare the citizenry for a new digital reality.

Conclusion

The full report is available for digital download at https://norsis.no/wp-content/uploads/2016/09/The-Norwegian-Cybersecurity-culture-web.pdf. NorSIS encourages other nations to make use of this metric, and to share the results with the international community.

Appendix 1: The Norwegian Center for Cybersecurity

The Norwegian Center for Cybersecurity (NorSIS)[4] is an independent driving force and partner supporting government, businesses and research in facing up to and dealing with information security issues.[5] NorSIS was first established as a project in 2002, and after evaluation, founded on February 2, 2010 on request from the Norwegian government. NorSIS is an independent center of knowledge in cybersecurity.

The purpose of NorSIS is to ensure that information security is a natural part of a business', a government department's or an individual's every day. We achieve this through building awareness of threats and vulnerabilities, by providing information on specific solutions and by influencing good attitudes and information security habits. The main target group for NorSIS is Norwegian enterprises in both the private and public sectors. Activity is aimed especially at small and medium-sized private enterprises and local government as well as the individual citizen.

NorSIS has a particular emphasis on collecting, organizing and disseminating knowledge about cyber threats to create awareness around information security. NorSIS acts as an organiser of meeting places for businesses and organisations within the public, private and voluntary sectors. Public-private partnerships are important for NorSIS to achieve cyber security. NorSIS also cooperates with several international partners in cybersecurity, for example Europol (Ec3), and The European Union Agency for Network and Information Security (ENISA).

NorSIS reports and surveys:

"Threats and trends" – A threat report published once a year on request from the Ministry of Justice.

"The Norwegian cybersecurity culture" – A study published for the first time in September 2016, and planned to be carried out once a year. The study is also on request from the Ministry of Justice.

Services NorSIS provide:

Slettmeg.no – is a free service to help people who experience privacy violations online.

Nettvett.no – is a free service providing information, advice and guidance on a safer use of the Internet. The information is aimed at individuals, from child to adult, consumers and small and medium enterprises. NettVett is a service in cooperation with The Norwegian National Security Authority and the Norwegian Communications Authority, but NorSIS has the editorial responsibility for this service.

Security Divas – is a network for women in the field of cybersecurity. 6 years ago NorSIS established the Security Divas conference. The conference has grown every year since then and has evolved to become an important network for women nationally who are studying or working with information security.

National Security Month – the pan-European exercise to protect EU Infrastructures against coordinated cyber-attacks. NorSIS coordinates this campaign in Norway.

4 http://www.norsis.no.

5 Document SG2RGQ/204, "Creating a metric for cyber security culture", Norway.

Country: United Kingdom of Great Britain and Northern Ireland

Document: 2/228

Title: Cybersecurity in government and industry

Summary: Cybersecurity is a very important issue for all nations. The United Kingdom has developed a number of tools to help citizens, industry and government to protect systems and networks against the effects of internet-based attacks.

This contribution from the United Kingdom focusses on a scheme called "Cyber Essentials". This is quite a new scheme and has proved very successful, with many organisations becoming certified.

Cybersecurity has been a priority for the UK Government for several years. Under the National Cybersecurity Programme there has been significant resource devoted to improving the UK's cybersecurity stance. Among the initiatives are several which are aimed at improving cybersecurity in both large and small organisations, and the relevant schemes have been developed jointly with industry. Of particular note is the scheme known as Cyber Essentials. The approach was developed after the analysis of a number of cyber attacks. That analysis indicated that in many cases a small number of precautions would have mitigated the attacks or caused the adversary to work much harder. Whereas the focus of the development has been within the UK, much of the work is equally applicable in any country and the details of the schemes are available to all. Cyber Essentials has proved to be very successful in the UK, with several hundred organisations becoming certified despite the scheme being relatively new.[6]

The Cyber Essentials scheme has been developed by Government and industry to fulfil two functions. It provides a clear statement of the basic controls all organisations should implement to mitigate the risk from common internet based threats, within the context of the Government's 10 Steps to Cyber Security. And through the Assurance Framework it offers a mechanism for organisations to demonstrate to customers, investors, insurers and others that they have taken these essential precautions.

Cyber Essentials offers a sound foundation of basic hygiene measures that all types of organisations can implement and potentially build upon. Government believes that implementing these measures can significantly reduce an organisation's vulnerability. However, it does not offer a silver bullet to remove all cyber security risk; for example, it is not designed to address more advanced, targeted attacks and hence organisations facing these threats will need to implement additional measures as part of their security strategy. What Cyber Essentials does do is define a focused set of controls which will provide cost-effective, basic cyber security for organisations of all sizes.

The Assurance Framework, leading to the awarding of Cyber Essentials and Cyber Essentials Plus certificates for organisations, has been designed in consultation with SMEs to be light-touch and achievable at low cost. The two options give organisations a choice over the level of assurance they wish to gain and the cost of doing so. It is important to recognise that certification only provides a snapshot of the cyber security practices of the organisation at the time of assessment, while maintaining a robust cyber security stance requires additional measures such as a sound risk management approach, as well as on-going updates to the Cyber Essentials control themes, such as patching. But we believe this scheme offers the right balance between providing additional assurance of an organisation's commitment to implementing cyber security to third parties, while retaining a simple and low cost mechanism for doing so.

---

[6] Details of the scheme are available at: http://www.gov.uk/government/publications/cyber-essentials-scheme-overview.

Country: United States of America

Document: 2/198

Title: Partnering with the private sector to manage cyber risk

Summary: Public-private partnerships are a foundational element for effective critical infrastructure protection, resilience, and overall cyber risk management. Managing cyber risk to critical infrastructure is an enormously complex but vitally important undertaking, and tackling cybersecurity challenges is often beyond the capability of either government or the private sector to manage independently.

This contribution from the United States to Question 3/2 outlines the importance of partnering with the private sector to manage cyber risk; lays out the United States' whole-of-community approach to cyber risk management, highlighting key tools that support this approach; and provides concrete examples of implementing effective public-private partnerships.

Introduction

Managing cyber risk to critical infrastructure is an enormously complex but vitally important undertaking. The compromise of, or malicious exploitation of critical infrastructure, can cause significant consequences on a local, regional, or even global scale. The cybersecurity risks to critical infrastructure have become progressively more important because nations, industry, and people increasingly rely on information systems and networks to support critical infrastructure functions.

Cybersecurity risks necessitate close cooperation among government, the private sector, and non-governmental organizations to ensure a coordinated approach to protecting critical infrastructure. Often, a nation's critical infrastructure is owned and operated by private companies; thus, managing cyber risk to these vital systems requires a strong partnership between the government and industry. This is particularly relevant to cybersecurity of critical infrastructure, where crime, data protection, control systems security, network defense, and cyber incident response and recovery issues present increasing challenges for government and industry alike.

The United States government consistently emphasizes a cybersecurity approach that focuses on partnerships and risk management as two critical components to an effective strategy. This approach builds off of the United States' previous contribution in 2011 to the ITU-D paper on Question 22-1/1: *Best Practices for Cybersecurity: Public-Private Partnerships*.[7]

The importance of public-private partnerships in support of cybersecurity

The efficacy of collaborative solutions to complex and ubiquitous challenges has been demonstrated repeatedly. Partnerships between government and the private sector have been applied successfully to a wide range of issues, from academic and scientific questions, to social and economic challenges, to armed conflict and efforts to combat terrorism. Participants create partnerships because they see value in the relationship and expect to accrue some level of benefit, and also recognize that the goal of the partnership would either be more difficult to accomplish or could not be achieved without this collaborative relationship.

Governments generally recognize that protecting their citizens from the potentially devastating consequences associated with critical infrastructure exploitation or disruption would be almost impossible without the extensive and willing participation of the private sector. In the United States, private industry owns, operates, and maintains most infrastructure, so private sector expertise, collaboration, coordination, resources, and overarching engagement are essential to government critical infrastructure risk management efforts.

[7] See ITU-D Question 22-1/1, Securing Information and Communication Networks: Best Practices for Developing a Culture of Cybersecurity (Final Report), Chapter 3 and Annex G, found at: http://www.itu.int/pub/D-STG-SG01.22.1-2014.

Public-private partnerships are a foundational element for effective critical infrastructure protection, resilience, and overall cyber risk management. Tackling cybersecurity challenges is often beyond the capability of either government or the private sector to manage independently. To best serve international, national, corporate, and even individual interests, the public and private sectors—and the international community—must share responsibility for strengthening the global cyber security posture.

Partnership between government and industry helps the government disseminate vital threat and vulnerability information, coordinate effective incident management, and understand the resilience and risk posture of critical infrastructure. The same partnership also helps promote greater security awareness, facilitates the exchange of technical expertise, the creation and promulgation of best security practices and standards, and generally improves industry's ability to manage risk.

Voluntary collaboration between private sector and government stakeholders remains the primary mechanism in the United States for advancing collective action toward cybersecurity that utilizes the diverse resources of all partners.

United States collaborative approach to cybersecurity risk management

As cybersecurity threats and vulnerabilities cannot be entirely eliminated, the U.S. Government approach to addressing cybersecurity is centered on risk management.

Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the likelihood that an event will occur and the resulting impact. With this information, organizations can determine the acceptable level of risk for delivery of services and can express this as their risk tolerance. With an understanding of risk tolerance, organizations can prioritize cybersecurity activities, enabling them to make informed decisions about cybersecurity expenditures. Implementation of risk management programs offers organizations the ability to quantify and communicate adjustments to their cybersecurity programs. Organizations may choose to handle risk in different ways, including mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk, depending on the potential impact to the delivery of critical services.

Whole-of-Community approach to risk management

To further promote risk management, in 2013 the U.S. Government issued Cybersecurity Executive Order (EO) 13636, which directs a whole-of-community approach to risk management, security, and resilience for cyber threats.

A whole-of-community approach involves partnership between public, private, and non-profit sectors, and a clear understanding of the risks collectively faced. This whole-of-community approach is intended to ensure that those with responsibility for the security and resilience of critical infrastructure receive the information that they need, and that the programs that enable these protection and resilience efforts reflect the needs and imperatives faced by critical infrastructure partners.

Reflecting this whole-of-community approach, the U.S. Department of Homeland Security (DHS) established a task force consisting of government and industry representatives to work together toward implementation.

Framework for improving critical infrastructure cybersecurity

As part of the Cybersecurity Executive Order, the National Institute of Standards and Technology (NIST) worked collaboratively with stakeholders, including industry, academic, and government representatives, through a formal consultative process to develop the Framework for Improving Critical Infrastructure Cybersecurity (the Framework), a voluntary framework for reducing cyber risks to critical infrastructure.[8]

[8] See the Framework for Improving Critical Infrastructure Cybersecurity at http://www.nist.gov/cyberframework/.

The Framework is a business-driven, proactive framework for voluntary cyber risk management designed for companies of all sizes that operate in diverse sectors of the economy. It provides a common starting point and language to assess cyber risk. It is easily adaptable, enabling organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure.

The Framework's development represents an example of successful public-private collaboration on cybersecurity risk management. It was developed through a collaborative process, led by NIST, in which stakeholder input played a significant role in shaping the process and the final document. The Framework is the product of a year-long, voluntary development process that included input from more than 3,000 members from industry, academia, and government, including international partners.

The Framework references existing international standards and guidelines, and industry best practices, to promote the protection of critical infrastructure through risk management. It represents a collection of existing standards and best practices that have proven to be effective in protecting IT systems from cyber threats, ensuring business confidentiality, and protecting individual privacy and civil liberties. In addition, the Framework provides a structure for organizing practices, as well as tools to support the use and adoption of standards and practices. Because it references globally recognized standards for cybersecurity, the Framework also has the flexibility to serve as an international model for managing cyber risk.

The Framework uses risk management processes to enable organizations to inform and prioritize decisions regarding cybersecurity. It supports recurring risk assessments and validation of business drivers to help organizations select target states for cybersecurity activities that reflect desired outcomes.

Implementation of the cybersecurity framework

The Framework is being implemented in a host of critical infrastructure sectors, government departments and agencies, and organizations ranging from multinationals to small businesses.

To support Cybersecurity Framework implementation, DHS developed the Critical Infrastructure Cyber Community (C3) Voluntary Program to provide resources to help those using the Framework to manage their cyber risks.

DHS offers a range of cybersecurity resources to public and private sector organizations, including information on cyber threats and vulnerabilities; cybersecurity incident resources, such as via the National Cybersecurity and Communications Integration Center (NCCIC), the United States Computer Emergency Readiness Team (US-CERT), and the Industrial Control Systems Computer Emergency Response Team (ICS-CERT); software assurance programs; and technical resources such as cybersecurity strategy development, cybersecurity assessment tools, cyber exercise planning, cybersecurity risk management training, a national vulnerability database, and roadmaps to enhance cybersecurity in certain sectors.

In particular, one publicly available resource is the Cyber Resilience Review (CRR). The CRR is a voluntary, non-technical, government-developed assessment tool to evaluate an organization's information technology resilience. The goal of the CRR is to develop an understanding and measurement of key capabilities to provide meaningful indicators of an organization's operational resilience and ability to manage cyber risk to its critical services during normal operations and times of operational stress and crisis. The CRR is available to download at https://www.us-cert.gov/ccubedvp/self-service-crr.

In addition to offering these resources, the U.S. Government is also partnering internationally to promote a risk management approach to cybersecurity by promoting the Framework's global adoption.

Examples of cybersecurity framework implementation

Intel Corporation: cybersecurity framework implementation in the Information Technology sector

Following the release of the first version of the Framework in February 2014, Intel Corporation (Intel) launched a pilot project to test the Framework's use at the company.[9] Intel's pilot project focused on developing a use case that would create a common language and encourage the use of the Framework as a process and risk management tool, rather than a set of static compliance requirements.

Intel's early experience with the Framework has helped harmonize the company's risk management technologies and language, improve their visibility into the risk landscape, inform risk tolerance discussions across the company, and enhance their ability to set security priorities, develop budgets, and deploy security solutions. The pilot resulted in a set of reusable tools and best practices for utilizing the Framework to assess infrastructure risk. Intel plans to use these tools and best practices to expand their use of the Framework.

Communications Security, Reliability and Interoperability Council (CSRIC): Advisory committee Use of the cybersecurity framework

The private sector, under flexible oversight from the regulator and in coordination with their non-regulatory public sector counterparts across the U.S. Government, is in the best position to recognize threats in the context of their business operations.

The U.S. Federal Communications Commission (FCC) works with the U.S. Department of Homeland Security (DHS) to promote proactive and accountable cybersecurity risk management for companies in the communications sector. A recent collaborative effort between the government and the private companies that build, own, and operate the majority of the networks has led to positive results. From 2014 to 2015, the FCC convened a working group within its advisory committee—the Communications Security, Reliability and Interoperability Council (CSRIC)—to further support the communications sector's cybersecurity risk management activities.[10]

Council members are selected from among public safety agencies, consumer or community organizations or other non-profit entities, and the private sector to balance expertise and viewpoints. The FCC releases a Public Notice seeking nominations and expressions of interest for membership on the Council. Currently, there are 55 members serving on the Council, representing a diverse and balanced mix of viewpoints from public safety organizations; federal, state, and local government agencies; the communications industry; organizations representing Internet users; utility companies; public interest organizations; and other experts.

The CSRIC Working Group on Cyber Risk Management was structured around five industry segments that make up the communications sector: broadcast, cable, satellite, wireless, and wireline. CSRIC applied the Cybersecurity Framework to each segment, developing and recommending voluntary mechanisms by which the communications industry could improve their management of cyber risks and clarify accountability within the corporate structure. Each segment developed customized implementation guides for its segment, along with tailored steps for small- and medium-sized businesses, while prioritizing the risk factors most relevant to the segment.

The CSRIC process demonstrated the value of the U.S. Government working with the private sector to achieve a voluntary, risk-based model that enables the communications sector to prioritize and implement solutions based on informed, business-driven considerations. By leveraging the diverse participants' expertise, the FCC and CSRIC working groups were able to develop a set of best practices that can be used by communications providers of any size.

---

9 More information on The Cybersecurity Framework in Action: An Intel Use Case can be found at http://www.intel.com/content/www/us/en/government/cybersecurity-framework-in-action-use-case-brief.html.

10 More information about CSRIC can be found at https://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-council-iv.

While application of the risk management Framework is the responsibility of each company, the U.S. Government also has an ongoing responsibility to understand the risk environment of all the sectors with critical cyber infrastructure. To achieve this, many agencies work with the private sector. For example, the FCC will confer with communications providers in cyber assurance meetings to learn about industry practices and procedures, provide guidance as needed, and use its role to identify relevant trends and best practices that can further aid in cyber risk management.

Securities Industry and Financial Markets Association (SIFMA): cybersecurity framework implementation

The Securities Industry and Financial Markets Association (SIFMA) collaborated with NIST to develop the Cybersecurity Framework. Drawing upon the resulting Framework, as well as other industry and government resources, SIFMA has composed a guidebook tailored to small firms. SIFMA has also worked with a group of banks, exchanges, and audit firms to align the American Institute of Certified Public Accountants (AICPA) Service Organization Control 2 (SOC-2) criteria, the Cybersecurity Framework, and specific industry requirements to create a consistent control framework for third-party providers.

U.S. Department of energy: energy sector cybersecurity framework implementation guidance

On January 8, 2015, the U.S. Department of Energy (DOE) released guidance to help the energy sector establish or align existing cybersecurity risk management programs to meet the Cybersecurity Framework objectives. In developing this guidance, DOE collaborated with private sector stakeholders through the Electricity Subsector Coordinating Council and the Oil and Natural Gas Subsector Coordinating Council. DOE also coordinated with other Sector-Specific Agency representatives and interested government stakeholders.

Information Systems Audit and Control Association (ISACA): implementing the cybersecurity framework and supplementary toolkit

ISACA participated in the development of the Cybersecurity Framework and helped embed key principles from its Control Objectives for Information Technology (COBIT) framework into the industry-led effort. As part of the knowledge, tools, and guidance provided by ISACA's Cybersecurity Nexus (CSX) platform, ISACA has developed a supplementary toolkit for implementing the Framework.

Conclusion

Critical infrastructure security and resilience requires a whole-of-community effort that involves partnership between public, private, and non-profit sectors, and a clear understanding of the risks faced. The U.S. has embraced a public-private partnership model for cybersecurity risk management, where both the public and private sector leverage their relative strengths to develop effective cybersecurity practices. This is emphatically not a "one-and-done" process. Cyber threats continually evolve, and cyber risk management must evolve with them. This means that any collaboration model must be a living process that allows for continuous improvement as technologies and threats change.

Country: United States of America

Document: SG2RGQ/42

Title: Best practices for establishing a cybersecurity awareness campaign

Summary: This contribution provides recommended steps and best practices that a country may follow when establishing a cybersecurity awareness campaign at the national level. It cites examples from the Stop.Think.Connect.™ Campaign, which is the United States' national public awareness campaign aimed at increasing national understanding of cyber threats and empowering the American

public to be safer and more secure online. This contribution is related to the following issues for study from the Terms of Reference:

c) Continue to gather national experiences from Member States relating to cybersecurity, and to identify common themes within those experiences.

e) Provide a compendium of relevant, ongoing cybersecurity activities being conducted by Member States, organizations, the private sector and civil society at the national, regional and international levels, in which developing countries and all sectors may participate, including information gathered under c) above

g) Examine ways and means to assist developing countries, with the focus on LDCs, in regard to cybersecurity-related challenges.

Introduction

The rapid growth and adoption of the Internet is creating unprecedented opportunity for innovation as well as social and economic growth around the world. While the benefits of more and more users coming online are undoubtable, it also makes securing cyberspace more difficult. To address this challenge, many countries organize cybersecurity awareness campaigns, which aim to educate governments, private industry, educators, and individual citizens to spot potential problems and understand their individual roles and responsibilities for creating a safer cyberspace.

In the United States, the U.S. Department of Homeland Security (DHS), in coordination with the National Cyber Security Alliance, leads the national cybersecurity awareness campaign, Stop.Think. Connect.™ Stop.Think.Connect.™ is aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. It seeks to propagate the concept of cybersecurity as "a shared responsibility" where each individual, by taking simple steps to be safer online, makes using the Internet a more secure experience for everyone. Its key messaging includes:

- **Stop:** Before you use the Internet, take time to understand the risks and learn how to spot potential problems.
- Think: Take a moment to be certain the path ahead is clear. Watch for warning signs and consider how your actions online could impact your safety, or your family's.
- Connect: Enjoy the Internet with greater confidence, knowing you've taken the right steps to safeguard yourself and your computer.
- Stop. Think. Connect. Protect yourself and help keep the web a safer place for everyone.

This contribution is made up of four sections, which outline recommended steps and best practices for launching a cybersecurity awareness campaign. These steps and best practices are based on the United States' experience in running Stop.Think.Connect™, which is a global campaign that any country may join.

Section 1: Best practices checklist

While every country has unique needs and challenges related to cybersecurity threats and protection, the following best practices can help with launching a cybersecurity awareness campaign.

- **Develop a communications plan that includes well-defined goals and objectives and identifies primary target audience(s).** The first step to launching a cybersecurity awareness campaign is to determine the campaign's specific goals and objectives as well as its primary target audience. For details on how to create a strategic communications plan, see below.
- Develop targeted communications strategies and resources to reach specific audiences. Everyone has different cybersecurity needs. For example, students may need to know about

cyber predators while IT professionals need to know about hackers. Different materials should be developed for each audience's needs, knowledge, and ability level.

– The Stop.Think.Connect.™ Campaign offers tip sheets tailored to each specific audience group to address its unique needs and threats. Comprehensive educational materials, such as the Stop. Think.Connect.™ Toolkit, emphasize the shared responsibility for cybersecurity while helping ensure that resources are available for all segments of the community. Simple reminders in the form of posters, wristbands, etc. help individuals keep cybersecurity best practices as a top priority. Stop.Think.Connect.™ materials can and have been translated and used around the world.

– Use social media. Much of cybersecurity awareness raising takes place online. Using social media helps connect cybersecurity awareness messaging to individuals through the channels they are already using—and in some cases, the ones they prefer to use. Posting information on social networking sites like Facebook, Twitter, and YouTube provides a means of engaging and sharing information while also receiving valuable input. Stop.Think.Connect.™, for example, connects with users in a variety of ways online, including Twitter chats and blog posts that raise awareness on specific topics[11].

– Create and maintain partnerships with allies in target audiences. No organization, whether government agency, corporation, or non-profit, can single-handedly spread cybersecurity awareness. Therefore, both public and private partnerships are essential. Develop and engage partnerships with organizations such as:

  a) ***Government agencies.*** Government agencies lend authority to the message, and have a wide reach to individuals and communities.

  b) The Stop.Think.Connect.™ Campaign developed the Cyber Awareness Coalition to engage with federal agencies as well as state, local, tribal, and territorial government entities to help them educate their employees and constituents to identify and deter online dangers. Key government partners at various levels include Computer Security and Incident Response Teams (CSIRTs), Offices of the Chief Information Security Officer (CISOs), and Offices of the Chief Information Officer (CIOs).

  c) ***Non-profit organizations***. Non-profit organizations offer a variety of resources and flexibility to spread cybersecurity awareness messaging.

  d) The Stop.Think.Connect.™ Campaign developed its National Network of non-profits to advocate and promote cybersecurity within their organizations and to their members and audiences. Non-profit partners span all audience groups identified in the strategic plan. Regular calls including all partner organizations help build networks between each organization, both public and private.

  e) ***Academic institutions***. Academic institutions contribute key, up-to-date research that help to ensure that the campaign remains current and informed. They also provide access to the nation's future workforce. Partnerships with high schools and elementary schools are also crucial since encouraging cybersecurity awareness education from a young age helps students use the Internet safely throughout their lives. Engaging with universities or centers of excellence, helps establish relationships between the workforce-in-training and the organizations that will employ them in the future.

  f) ***Private sector organizations***. Industry leaders, including information, retail, finance, and educational services, can educate employees, consumers, and other audiences about the threats affecting them as well as receive input on strengthening cybersecurity practices. Innovative cybersecurity solutions developed by private sector organizations can drive best practices in both the public and private sectors.

[11] Examples can be found @Cyber Twitter handle, the DHS Blog @ Homeland Security, and the DHS Facebook page.

g) DHS' co-leader in the Stop.Think.Connect.™ Campaign, the National Cyber Security Alliance,[12] coordinates the private sector aspects of the campaign.

– **Engage audiences at the individual level through grassroots efforts.** Individual awareness is foundational to an effective cybersecurity awareness program.

– The Stop.Think.Connect.™ Campaign, for example, invites individuals to become "***Friends*** of the Campaign" by signing up for monthly email newsletters with the latest cyber tips, news, and information relevant to them. The Campaign also reaches individuals by conducting outreach events tailored to each audience and providing speakers who can discuss the cybersecurity issues that most affect the audience.

– Measure whether the effort is truly raising awareness among the target audiences. To measure the effectiveness of a campaign, it is important to collect feedback from focus groups, surveys, or other like methods. Also, track which webpages are most viewed, which materials are most downloaded, which events are best received, and which practices audiences find most effective to identify successes and foster improvement. Feedback from partner organizations helps future planning focus on effectiveness and creativity.

Section 2: Sample communications plan

A communications plan is an essential component of a successful campaign as it provides a roadmap for how the organization plans to accomplish its key goals and objectives. Although a communications plan must be tailored to fit the needs of a specific organization, most plans will include the following sections:

Purpose and background

The Purpose and background section articulates the organization's rationale for creating a communications plan and what it plans to accomplish.

Overarching communications goals

Overarching communications goals are high-level aims for the cybersecurity awareness program. Such goals are strategically broad while remaining measureable. For example, DHS' overarching communications goal for the Stop.Think.Connect.™ Campaign is as follows:

To promote public awareness about cybersecurity by increasing the level of understanding of cyber threats, simple mitigation actions, and empowering the American public to be more prepared online to:

– Elevate the Nation's awareness of cybersecurity and its association with the security of our Nation and safety of our personal lives

– Engage the American public and the private sector as well as state and local governments in our Nation's effort to improve cybersecurity

– Generate and communicate approaches and strategies for Americans to keep themselves, their families, and communities safer online

Communications objectives

Communications objectives describe how the campaign will achieve its overarching goals. Like overarching goals, the objectives should be measureable.

DHS communications objectives for the Stop.Think.Connect.™ Campaign are to:

– Educate the American public on cyber safety practices to protect themselves and ensure stakeholder groups are aware of available resources (from DHS and others).

[12] https://www.staysafeonline.org/.

- Increase the number of national stakeholder groups engaged with **Stop.Think.Connect.™** and strengthen existing relationships with State and local governments, industry, non-profits, school systems, and educators.
- Increase and strengthen the cyber workforce by promoting science, technology, engineering, and math (STEM) education.

Key target audiences

Identifying key audiences helps ensure that messaging focuses on those most receptive to or in need of the message. Clearly defining those audiences keeps the messaging targeted to specific groups by maintaining a shared understanding of what audience titles mean.

The Stop.Think.Connect.™ Campaign identified at the outset seven audience groups: students; parents and educators; young professionals; older Americans; government; industry; and small business. As an example of audience group definitions, Stop.Think.Connect.™ considers older Americans to be individuals who are 60 years of age and older, as defined by the Office of Aging, U.S. Department of Health and Human Services.

Communications channels

Communications channels are the various vectors to convey messaging to the target audience(s). Carefully consider all currently used means of communication as well as additional methods that may be available for use. The communications plan should clearly specify both what the channels are and how to use them.

The Stop.Think.Connect.™ Campaign engages audiences through the following channels:

- Events: Hosting events with target audience groups
- Traditional Media: Proactively reaching out to national/regional/local media (e.g., broadcast, print, web)
- Social Media: Actively using social media platforms (DHS blog, Facebook, Twitter)
- Newsletter: Distributing a monthly newsletter as well as informational toolkits
- Website: Regularly updating campaign websites with news, tips, and key information
- Partners: Encouraging outreach from partner organizations

Campaign strategies

Campaign strategies take into account both the practical methods of disseminating information as well as means for creating campaign momentum and growth. Each broad strategy contains many small steps to accomplish it, and both the steps and the strategies should be flexible enough to adapt to a changing environment. The example below includes only a few strategy samples from the U.S. Stop. Think.Connect.™ Campaign.

Stop.Think.Connect.™ uses the following strategies, among others, to meet its communication objectives:

- Disseminate Campaign messaging through events and media (social and traditional)
- Build a cadre of messengers via partnerships with non-profits and grassroots outreach
- Work across the federal government agencies to collaborate on events and messaging

Messaging

Top-line messaging should focus on the basic, core messages that the campaign seeks to disseminate. Each country and campaign—and each audience and event—has specific needs that require tailored messaging. Top-line messaging serves as the foundation for each of those customized outreaches.

Stop.Think.Connect' s top-line messages include:

- **Stop:** Before you use the Internet, take time to understand the risks and learn how to spot potential problems
- **Think:** Take a moment to be certain the path ahead is clear. Watch for warning signs and consider how your actions online could impact your safety, or your family's
- **Connect:** Enjoy the Internet with greater confidence, knowing you've taken the right steps to safeguard yourself and your computer
- **Stop. Think. Connect.** Protect yourself and help keep the web a safer place for everyone

Other universally applicable messages include, using strong passwords, keeping operating systems and security software up-to-date, connecting only with people you trust, and avoiding websites that sound too good to be true.

Roles and Responsibilities

Clearly designating roles and responsibilities enables teams to work together effectively while preventing overlap or confusion. Such differentiation occurs between organizations when multiple groups support a campaign, as well as among team members of a particular organization.

For example, as part of the overarching Stop.Think.Connect.™ Campaign, DHS coordinates relationships with non-profit organizations and government agencies while its partner, the National Cyber Security Alliance (NCSA), coordinates with industry.

Resources

Listing the resources available to a campaign makes clear the scope and limitations for outreach activities within a given time period. In this section, the author may choose to detail the number of dedicated staff and materials that the organization has available to serve specific target audiences within a given time period.

Challenges to communications

Identifying expected challenges to communications may help to overcome gaps and obstacles. Examples for Stop.Think.Connect.™ include:

- Technical aspects of cyber threats are difficult for audiences to comprehend and understand how it relates to them.
- The general public does not necessarily see cyber threats as real or pertinent to their everyday lives.

Measurements of success/Metrics

Any communications plan needs a way to receive feedback and measure effectiveness. Due to the nature of cybersecurity awareness campaigns, such measurements typically focus on outward activities more than input, but timely feedback is essential.

Examples of Stop.Think.Connect.™ Campaign metrics include:

- Number of participants for each event or series of events in a region;
- Number of marketing collateral distributed;
- Media coverage;
- Number of stakeholders involved (e.g., Friends, Cyber Awareness Coalition members, National Network members, etc.);
- Hits to webpage;

- Feedback and testimonials from participants and partner organizations;
- Feedback from Congress, state and local leaders/officials.

Section 3: Metrics

This section describes the type of metrics the Stop.Think.Connect.™ Campaign uses to track and evaluate its cyber awareness programming.[13] Countries may find the outlined metrics useful as a baseline for establishing their own measures of effectiveness.

The metrics fall into several broad categories. How these types of categories are applied to differing cybersecurity awareness programs depends on particular programs' goals and resources. **Stakeholder Engagement** deals with formal partnerships with government agencies and non-profit organizations. **Traditional Media Outreach** and **Digital and Online Outreach** each apply to distributing written and multimedia products through established communication channels. **Events and Forums** and **Resources** each cover in-person interactions. A combination of metrics categories is required to understand and measure the full scope of a campaign.

Metrics categories and examples

- **Stakeholder engagement.** Stop.Think.Connect.™ partners with a number of non-profit organizations that form its National Network, as well as with federal, state, local, tribal, and territorial government agencies that compose its Cyber Awareness Coalition. The Campaign additionally partners with academic institutions around the country. The Campaign measures the number of organizations in each of these stakeholder groups, as well as growth rates per year and the number of people reached by each partner organization.
  - By December 2014, the National Network grew to 52 organizations. The National Network includes the Boys & Girls Clubs of America, YWCA, National Sheriffs' Association, (ISC)2 Foundation, and Neighborhood Watch. Through these and other organizations Stop.Think.Connect.™ reaches Americans nationwide, including parents, educators, students, small businesses, older Americans, and young professionals. With the help of the Campaign, National Network members have instituted many successful cyber awareness efforts, such as providing cyber awareness training for more than 1,500 D.A.R.E. officers. In 2014, the National Network grew by 44 per cent.
  - By December 2013, the Cyber Awareness Coalition grew to 65 government partners. The Coalition includes partners ranging from the Department of Education to the State of California that promote awareness about cyber threats and online safety practices within their organizations and to their constituents. Stop.Think.Connect.™ has worked with its Coalition members to help spread cybersecurity messaging and combat threats. For example, the Federal Communications Commission worked with Stop.Think.Connect.™, and other agencies, on the development of its Smartphone Security Checker and Small Biz Cyber Planner. Also, Stop.Think.Connect.™ and the Federal Trade Commission partner on digital outreach and created co-branded community outreach toolkits that have been distributed nationwide to help educate Americans on protecting themselves online.
  - The Academic Alliance grew to 41 new universities and colleges joining the Campaign. These partners include Florida State University, Sam Houston State University, and the University of Minnesota, among many others, The Academic Alliance partners spread the cybersecurity awareness message to students, staff and faculty. They also often encourage students to consider educations in STEM and more specifically, cybersecurity, through classes, presentations, and cybersecurity competitions.
  - In 2014, the entire Stop.Think.Connect. partner program grew by 84 per cent since 2013.

[13] This document is updated annually. Figures are current as of December 2014.

- **Traditional media outreach.** Stop.Think.Connect.™ encourages awareness through a number of traditional media sources. Metrics track the number of print circulation hits; online impressions; broadcast reach; articles online and in print; television, radio, and audio news releases; and independent press releases.
- **Digital and online outreach.** Many of Stop.Think.Connect's resources are distributed online, allowing for ample opportunity to measure interaction and feedback. The Campaign measures the number of: ***Friends*** of the Campaign; hits to the DHS Stop.Think.Connect.™ Campaign website; Twitter chats and Facebook Events; Tweet mentions; Facebook "Likes;" and number of blog entries posted.
    - ***Friends*** of the campaign: Stop.Think.Connect.™ reaches people in their own communities through its ***Friends*** of the Campaign effort. The ***Friends*** program is a grassroots outreach effort that enables individuals to sign up and commit to becoming messengers of the Campaign. An average of 762 people joined the ***Friends*** of the Campaign each month in 2014. The Campaign distributes monthly newsletters with tips and information about safer online practices to ***Friends*** of the Campaign.
    - Stop.Think.Connect.™ Campaign Website: Campaign materials point users to the website www.dhs.gov/stopthinkconnect. The Campaign tracks the total number of visits to the site as well as which pages and materials are most accessed. There were over 63,514 hits to the website in 2014.
    - Social media: Stop.Think.Connect.™ participates in regular Twitter chats through @Cyber and posts blogs on the Blog@Homeland Security. The Campaign measures the number of blog posts and Twitter chats each year, as well as the impressions from the Twitter chats. For example, a series of Twitter chats for National Cyber Security Awareness Month 2014 had an estimated 45,000,000 impressions. Additionally, the Campaign works with the National Cyber Security Alliance (NCSA) to monitor the number of Twitter followers and retweets as well as Facebook ***Friends*** and "likes" on @STOPTHNKCONNECT and the Stop. Think.Connect.™ Facebook accounts.
- **Events and forums.** Stop.Think.Connect.™ conducts grassroots events across the Nation to encourage communities to embrace a more sustained, proactive approach to online safety. The location and audience for community events are based upon market analysis that considers statistics on demographics and trends so the Campaign can strategically reach target audiences. For example, as part of National Cyber Security Awareness Month, the Campaign organized a special forum for federal, state, and local law enforcement officials to address electronic-based crimes in South Florida, where identity theft cases are the highest in the Nation. In addition to tracking the number of events, the Campaign analyzes the demographic groups and geographic areas reached by the events. During National Cyber Security Awareness Month 2014 alone, 122 events were held across the country, 91 of those events provided with speakers from DHS.
- **Resources.** The Stop.Think.Connect.™ Toolkit provides resources for all ages and segments of the community, including materials to host independent cybersecurity awareness discussions or activities. The Campaign monitors the number of materials distributed, which is typically several thousand per year.

Section 4: Additional references

For more information and examples of use, please visit the following websites:

- Stop.Think.Connect.™ campaign:
    - http://www.dhs.gov/stopthinkconnect
    - http://www.stcguide.com (mobile-friendly website)
    - http://stopthinkconnect.org/ (National Cyber Security Alliance)
- Communications strategies and resources:

- http://www.dhs.gov/stopthinkconnect-get-informed
- http://stopthinkconnect.org/resources/ (NCSA)
- http://stopthinkconnect.org/tips-and-advice/ (NCSA)

– Social media:
- https://twitter.com/cyber
- http://blog.dhs.gov/
- https://www.facebook.com/homelandsecurity
- https://twitter.com/STOPTHNKCONNECT (NCSA)
- https://www.facebook.com/STOPTHINKCONNECT (NCSA)

– Partnerships with organizations:
- http://www.dhs.gov/stopthinkconnect-national-network
- http://www.dhs.gov/stopthinkconnect-cyber-awareness-coalition

– Connecting with individuals:
- http://www.dhs.gov/stopthinkconnect-Friends-campaign-program
- http://www.dhs.gov/stopthinkconnect-your-community
- http://www.dhs.gov/stopthinkconnect-campaign-news

– Measuring effectiveness:
- http://stopthinkconnect.org/research-surveys/research-findings/ (NCSA)

Country: Côte d'Ivoire (Republic of)

Document: 2/317

Title: Experience of Côte d'Ivoire in developing a national cybersecurity culture

Summary: This contribution presents the experience of Côte d'Ivoire in developing a national cybersecurity culture and puts forward recommendations for cybersecurity development in developing countries.

Background

Development of the national Internet infrastructure has resulted in the proliferation of online services and infrastructures, particularly mobile-money and web applications (websites, databases, etc.). However, very many security holes and vulnerabilities with varying levels of criticality are to be found within the configuration of such applications and services. In such an environment, the risk of personal data theft, compromising of IT systems and financial damage is very high.

The implementation of organizational measures and tools for securing electronic communications and users' personal data is therefore crucial in the context of stimulating the digital economies of developing countries in general, and of Côte d'Ivoire in particular. Securing information systems and taking effective measures to combat cybercrime is a key way in which to strengthen digital confidence.

Inventory of organizational arrangements adopted by Côte d'Ivoire

Under the guidance of the Telecommunication/ICT Regulatory Authority of Côte d'Ivoire (ARTCI), the country has implemented a number of measures intended to constitute an effective operational response to the threats causing digital insecurity.

– Establishment of the Côte d'Ivoire Computer Emergency Response Team (CI-CERT)

Côte d'Ivoire has put in place a national CERT which serves as the centre for responding to computer-related incidents nationwide. As such, it coordinates the emergency response measures in cases of actual security incidents, while at the same time playing a very important preventive role by conducting periodic security audits on the online infrastructures of critical and/or strategic entities. A significant part of its work also involves sharing the information it derives from its monitoring system, proactively alerting stakeholders to any threats to which their IT systems are exposed and providing them with appropriate corrective measures. Furthermore, in an effort to strengthen the cybersecurity culture, ARTCI periodically holds training and awareness-building seminars on the subject of cybersecurity.

– **Establishment of the Platform for Combating Cybercrime (PLCC)**

Initiated by ARTCI, the PLCC is a collaborative platform set up in the interests of responding effectively to the problem of cybercrime in Côte d'Ivoire. The platform's ***modus operandi*** is original inasmuch as it comprises IT-security engineers from ARTCI and police officers from the Information Technology and Technological Traces Directorate (DITT), which is a central directorate of the scientific police.

The platform was established through an agreement signed between the Director-General of ARTCI and Director-General of the National Police of Côte d'Ivoire. It brings together a range of skills, particularly those of IT engineers and police officers, and carries out its activities under the supervision of the public prosecutor's office (Ministry of Justice).

Shared working has enabled, among other things, a transfer of skills between the ARTCI security engineers and police officers in regard to digital investigations. This has resulted in a broad enhancement of the requisite skills, boosting the effectiveness of the PLCC officials. By way of illustration, in 2014 we saw a 73 per cent reduction in the number of cases of cyber fraud by comparison with 2010.

Last but not least, PLCC carries out numerous awareness-building and training campaigns among specific target populations, such as pupils and students, banking and financial establishment employees, officials within the various services of the national police and other law-enforcement officials.

– **Consultative activities with a view to defining the national cybersecurity strategy**

In its ongoing efforts to implement a reference framework conducive to the emergence of a secure national cyber environment, Côte d'Ivoire has initiated, in response to calls from ARCTI, a set of coordinated activities aimed at defining a national cybersecurity strategy for the period 2016-2020. All of the local players have been involved in the preparatory discussions in the interests of harnessing all the relevant skills and accommodating all of the specific requirements of the various key sectors concerned. This approach has helped to create a lively and inclusive process of reflection on the best practices to be pursued in order to develop a national cybersecurity culture and thereby enhance digital confidence.

Proposal

In the light of the foregoing, we hereby propose the following guidelines to encourage States in their policies and strategies for combating cybercrime:

– Establish national CERTs.

– Establish multistakeholder operational teams to combat cybercrime.

– Develop national awareness-building programmes in regard to cybersecurity.

- Develop international cooperation through information-sharing programmes with computer incident response centres in other countries around the globe.
- Create the conditions for multistakeholder dialogue aimed at the elaboration of national cybersecurity strategies.

Country: China (People's Republic of)

Document: 2/174

Title: Best practices for developing a culture of cybersecurity: Promoting awareness of cybersecurity and enhancing its management

Summary: This contribution discusses the huge challenges encountered in the information era and the importance of securing information and communication networks. Cybersecurity does not depend on technology alone: human elements serve as the basis for technological measures, and human error and social engineering can seriously endanger cybersecurity. Promoting awareness of cybersecurity and enhancing its management are therefore the most effective ways in which to develop a culture of cybersecurity. In addition, this contribution sets out specific practices for developing a culture of cybersecurity from four standpoints: regulations, driving factors, training programmes and feedback for improvement.

The rapid technological development and huge physical expansion of information and communication networks have made people's lives easier than ever before. While the fundamental transformation of the digital era, characterized by cloud computing, big data and "Internet +", has been playing a role in promoting economic growth by leveraging the Internet, it also touches the very heart of personal data, making cybersecurity a key challenge for present-day society. While network applications concern functionality, cybersecurity is essential to national defence and national strategy. The ancient Chinese "Sun Zi Bing Fa" (Master Sun's Art of War) states that the art of war is of vital importance to the State. Hence, it is a subject of enquiry that can on no account be neglected. For the sake of protecting public interests, maintaining social stability and even defending the integrity of national sovereignty, the task of securing information and communication networks has become ever more important and pressing.

How should we proceed to address this vital issue of cybersecurity? From the standpoint of defence, there are two major components in securing information and communication networks, namely technology and human beings. Here we are not referring to legal provisions (laws specifically targeting cybercrime are often lagging far behind the pace of technological change). Securing information and communication networks by means of technology is tangible and self-evident with the availability of encryption, firewalls, anti-virus software, ID authentication, network isolation, security services, restoration from backups, PKI and VPN, all of which clearly play a significant role in ensuring cybersecurity. However, the role of technological solutions is limited, and cybersecurity vulnerabilities and problems are constantly emerging, posing major challenges for the entities concerned and people responsible for network operation and maintenance. So much so, in fact, that the whole thing has become a vicious cycle: on the one hand, ever more financial and human resources are being invested in cybersecurity, while on the other hand, cybersecurity risks have not been mitigated. The world-renowned hacker Kevin Mitnick wrote in his book The Art of Deception: Controlling the Human Element of Security that the failures of many people are not due to the lack of critical cybersecurity technology, but rather to the human behaviour of the user of the technology and employees in the organization. While this does not mean that investment in technology by the management is to no avail, it does point to the fact that security cannot be guaranteed solely by means of a set of technologies and products.

Technology can be used to mitigate threats, but a consolidated solution can be far more powerful than technology alone. The application of technological means will never be fully effective in securing

information and communication networks without the second element: the human being. The human element in the entire defence system is not only the core, but can also constitute its worst defect. For example, symmetric encryption algorithms in cryptology provide strong protection for data privacy; asymmetric cryptographic algorithms can be used to create digital signatures, thereby protecting the integrity of data and its non-repudiation. However, the effective implementation of these cryptographic algorithms depends on proper management of the keys by the user. Any key management error or misoperation will completely undermine the robust cryptography: keys using a combination of common keywords can be obtained in no time at all by a hacker running a dictionary attack; loss of the key or failure to keep a backup could lead to permanent non-restoration of the data. In another example, while physical isolation technology can protect private networks from attacks by malicious external programs, those same networks can be affected by viruses residing in personal mobile devices when the latter are connected to the private network, resulting in leaks of an organization's data and at worst the collapse of the entire system. Controlling the "human element" is therefore a critical factor in limiting the risk of such attacks.

The above conclusion regarding the need to control the "human element" in order to reduce the risk of organizations being attacked goes hand in hand with the notion of "security culture". According to Wikipedia, "A security culture is a set of customs shared by a community whose members may engage in illegal or sensitive activities, the practice of which minimizes the risks of such activities being subverted, or targeted for sabotage. […]The main focus of a security culture is keeping infiltrators and other potentially damaging parties out." In other words, the control of human conduct in terms of security is a kind of "security culture", its purpose being to secure information and communication networks.

Controlling security-related human conduct is the most effective approach for developing a cybersecurity culture, for the simple reason that it is often improper human conduct in this regard that poses the greatest threat to information and communication networks. We can illustrate this with two cases. First, IBM's Cybersecurity Intelligence Index shows that, in 2014, up to 95 per cent of information security incidents were related to human error (intentional or unintentional). Controlling the human element can therefore go a long way towards eliminating such errors. Human error generally refers to employee conduct that results in inconsistencies between the realized function and the required function in the production process and the negative impact this has on the work or products. In the cybersecurity sphere, common human errors are: misconfiguration of the system; improper management of patches; use of default usernames and passwords (or very simple passwords); loss of devices; leakage of information due to an incorrect e-mail address; double-clicking on an insecure URL or attachment; password-sharing with other people; unattended computers; and connection of personal mobile devices to the corporate network.

Second, the priority accorded to social engineering in the chain of cybersecurity constitutes the weakest link. Based on the bucket principle, the security level of the information and communication network is determined by the security measures at the lowest level. The Official Guide to CISSP defines social engineering as attempts to influence the internal staff to get them to disclose corporate information or induce them to behave in such a way that the probability of intrusion into the system, data theft or information leakage caused by the attacker increases drastically. The reason why Snowden, who had a fairly low security clearance level, could disclose a large amount of data concerning the United States Prism Program was that the nature of his work enabled him to acquire the passwords and information of his co-workers and supervisors by means of social engineering. The above two cases demonstrate how human behaviour has a major role to play in cybersecurity. In view of this, what kind of training programmes should information and communication network organizations put in place to improve human conduct in relation to cybersecurity?

It goes without saying that promoting awareness of cybersecurity and controlling the associated conduct is a key factor in securing information and communication networks. First of all, regulations should form the basis for awareness promotion, in particular the development of policies and rules for reporting unexpected incidents and social-engineering incidents, with disaster preparedness

and restoration in place. Such regulations are guiding rules and must be incorporated into an organization's cybersecurity programmes. Only once policies have been developed and enacted can the corresponding employee training be implemented. The goal of personnel training in regard to cybersecurity should become increasingly clear through internal exchanges and discussion, and this goal should be repeatedly emphasized over time.

Secondly, incentives should be fostered to encourage employees to abide by the regulations. Typically, these include the proactive will of the individual, accountability in regard to cybersecurity, and the importance of information security levels. Implementation of cybersecurity differs from performance appraisal in the area of ordinary services and products, which is generally conducted according to the "carrot and stick" approach, with distinct punishments and rewards. Securing information and communication networks is unique in that it is profoundly affected by related risks. Persons responsible for human errors will be held accountable for any damage incurred, whereas strict compliance with the operational rules of security management will not lead to any rewards, even if no security issues arise as a result of the compliance. In cases where human error does not result in loss or damage, the person concerned will not be held accountable. The conduct of employees should be measured in accordance with the relevant rules and norms. At the same time, a "non-accountability" system should be implemented, whereby, should the information system be attacked while being properly operated by the persons concerned, those persons will not be held responsible for any damage resulting from the attack.

Thirdly, training of the security personnel should focus not only on ensuring proper conduct on the part of the user, but should also help employees to understand fully the internal vulnerabilities that could be used by attackers. Identification and reporting of such vulnerabilities is a prerequisite for addressing the issue in an appropriate manner. Securing information and communication networks is the responsibility not only of an organization's IT professionals, but also of all the other members of its workforce. All staff should therefore, in addition to understanding their own roles and responsibilities in protecting the information resources, also be fully aware of how to foster cybersecurity and respond to potential security threats and incidents. Cybersecurity awareness enhancement programmes emphasize training of the entire staff so as to help them protect the corporate information assets effectively and reduce the possibility of human error.

Finally, the feedback and assessments provided during such training can be used to upgrade and improve future cybersecurity training programmes. Assessment results can contribute to the organization's appreciation of the effectiveness of the cybersecurity training programme while helping it to identify any problems or shortcomings, with a view to ongoing development of the programme. Assessment – in the form of questionnaires, physical interviews, examinations, audits, etc. – should therefore be conducted on a regular basis to ensure continuous adaptation of the cybersecurity training programme to the changes and emerging security issues in a dynamic environment.

Country: China (People's Republic of)

Document: 2/67

Title: Proposal for a new work item on framework of detection, tracking and response of mobile botnets

Summary: This document proposes a new work item to research how to detect, track and response mobile botnets. With the rapidly-growing number of smartphones, PC-based botnets are moving towards this mobile domain, which will pose serious security threats on mobile devices.

Background

PC-based botnets are a serious security threat in today's Internet; hackers can use botnets to launch all kinds of attacks, such as spam, fraud, identity theft, DDOS, scan, etc. With the rapid development of the computing and Internet access capabilities of smartphones, smartphones are powerful enough to host a bot. There are more privacy information in smartphones, such as call records, phone book, SMS, and etc., than PCs, and so mobile botnets would offer more financial gains for hackers. In facts, vulnerabilities exist in all major smartphone platform.

Since the appearance of the first mobile bot Cabir (which was found in 2004), we have witnessed a rapid development in mobile botnets. The mobile botnet, SymbOS.Yxes targets Symbian in 2009 and its variants E, F and G were again discovered in July 2009. In the same year, Ikee.B was discovered and targeted iPhones. In December 2010, Geinimi was discovered and targeted Android. Comparing with PC-based botnets, mobile botnets have more serious threats for end users, for example, hackers can send SMSs or visit Internet and use your charges; and at the same time, constructing a mobile botnet use different technologies, for example, hackers can construct a MMS if you receive the MMS, you could become a member of these mobile botnets. Comparing with PC-based botnet, the Command and Control (C&C) channel in the mobile-botnet also has many differences, for example, hacks can direct control your smartphones by sending a SMS to you.

Because of these new characters, we need to adopt new technologies which resist mobile botnets, for example, we should detect the command and control channels for MMS or SMS.

Apart from being connected to the provider's mobility network, the differences in the devices themselves, their use, and billing models all influence the way in which mobile botnets will evolve. Consequently, investigations into how mobile botnets work, as well as how they may be constructed, detected, tracked and prevented, represents an new and important research area.

Use cases

In the following we describe three usage scenarios. Besides the tow usage scenarios described here, there are many other usage scenarios possible.

Scenario 1: Understanding mobile threats

Mobile applications are increasingly reliant on the browser and mobile browsers present a unique challenge. To enhance usability, the address bar disappears above the screen so that more of the page content can be displayed. If a user does click a malicious link on a mobile device, it becomes easier to obfuscate the attack since the Web address bar is not visible.

Mobile devices do not commonly receive patches and updates. For most users, their operating system (OS) and mobile browser is the same as it was on the phone's manufacture date. That gives the attackers a big advantage.

Smartphones can be controlled by hackers to earn money, for example, sending SMSs or MMSs to a deliberate mobile number.

Scenario 2: Understanding mobile botnets

Constructing mobile botnets need some new technologies. There are some differences between smartphones and PCs. 1) The battery power is rather limited on a smartphone and so a mobile bot cannot be active at all times. 2) The cost of smartphones is an extremely sensitive area for users and so a mobile bot need to decrease its communications, such as Internet connection, SMS and MMS. 3) Lack of IP address. The lack of IP address may cause the problem of indirect connect. Due to the lack of IP address, most mobile phones are using NAT gateway and thus the devices are not directly reachable, so the traditional P2P based C&C network may not suit for mobile botnet. 4) The diversity

of operating system of smart phone. The design of mobile botnet has to consider the diversity of the OS platform of smart phone.

Botmasters how to choose its C&C channels, and are traditional IRC-based, P2P_based and HTTP-based C&C channels still fit for mobile botnet? Base on new characters of mobile botnets, hackers can adopt SMSs or MMSs to control the mobile bot and send command messages to mobile bots.

Scenario 3: Attack of mobile botnets

Comparing with PC-based botnets, one of the main targets of the mobile botnet is to retrieve sensitive information from the victims. The mobile bot can quickly scanning the host node for significant corporate or financial information, such as usernames and passwords, address list and text messages.

Additional important difference, because most of the functionality of cellular network rely on the availability and proper functioning of HLRs(Home Location Register), so the DoS attack could block the legitimated users of a local cellular network from sending or receiving text messages and calls. In the practical circumstances, a bot master of a mobile botnet could control the compromised mobile phones to overwhelm a specific HLR with a large volume of traffic. Through the DoS attack, it will affect all the legitimated users who rely on the same HLR, their requests will be dropped.

Scenario 4: Detection and response of mobile botnets

A mobile botnet is a group of compromised smartphones that are remotely controlled by botmasters via C&C channels. Because mobile botnets adopts some new technologies, how to find mobile botnets has to use some new methods and mechanism, for example, building international coordinated mechanism, some mobile botnets use Web 2.0 Services to construct C&C channel. We should find and prevent these services from being abused and enhance the cooperation among different Countries and Enterprises, such as Microblog, blog, Google App Engine, etc.

At the same time, mobile botnets can bring the significant threats for the core network and can attack against cellular network infrastructure, and so communications service providers have to face unique challenges in protecting their networks from mobile botnet threats.

Proposal

Based on the analysis of the sections before, we propose a framework of detection, tracking and response of mobile botnets.

The basic thinking of this framework includes:

- Define the mobile threats, understand and find the basic principles of mobile threats.
- Define mobile botnets, understand and find the basic principles of mobile botnets.
- Define a framework of detection and tracking mobile botnets, build international coordinated mechanism.
- Define a response framework of mobile botnets and decrease the loss of users and operators.

Country: Korea (Republic of)

Document: SG2RGQ/64

Title: The meeting is expected to consider Korea's experiences and related proposal for international cooperation in preventing Internet addiction.

Summary: Internet and smartphone is very widely used in Korea across all age groups, thus, the dark side of Internet use such as Internet addiction has becoming a hot social issue. Annual survey shows that Internet addiction rate in 2013 is 7.0 per cent, the figure for the adolescents is increasing to 11.7 per cent. Smartphone addiction rate is higher as 11.8 per cent, the figure for the adolescents is also much higher to 25.5 per cent. Therefore, Korean society do various activities to prevent and treat Internet addiction such as annual social survey to measure the Internet addiction, various preventive education/program, and operation of Korea Internet Addiction Centre. Special features of Korea's policies and the necessity of international cooperation for preventing Internet addiction also will be described.

Current status of internet and smart phone addiction in Korea (Rep. of)

The "Internet addiction" has appeared as one adverse effect as a result of the country's advance into information and a wide diffusion of Internet use. Although its concept is yet to be clearly defined in psychological and medical terms, the Internet addiction is generally referred to inflictions of hard-to-recover damages to people's physical, mental and social functions which occur as a result of excessive use of IT network service (National Information Basic Law, Article 13). Most Internet addicts tend to have withdrawal and tolerance symptoms like extreme anxiety or nervous breakdown, showing serious impediment in their daily life. So deeply hooked up with cyber world, excessive Internet users show symptoms that take diverse forms of game addiction, chatting addiction, porno addiction, etc.

In recent years, the smart media addiction has occurred in the rapidly changing lifestyle and communication styles resulting from a rapid rise of smart media adoption and ICT evolution of fusion and convergences.

About 7.0 percent of the Internet users aged from 5 to 54 were the risk group of Internet addiction, according to the 2013 Internet addiction status survey (released in March, 2014 by Ministry of Science, ICT and Future Planning, and National Information Society Agency). The share of Internet users at risk group to the total Internet users has reduced from 7.7 % in 2011 to 7.2 % in 2012 and 7.0 % in 2013. But, the share of teenager users at risk group has increased from 10.4 % in 2011 to 10.7 % in 2012 and 11.7 % in 2013.

Meanwhile, the smart phone addiction increase was found to be steeper than the Internet's. About 11.8 % of smartphone users aged 10 to 54 was a risk-group of excessive smartphone users, up 3.4 % point from 8.4 % in 2011 when the smartphone addiction survey started. Teenage users were the highest risk group: About 25.5 % of Korean adolescents (aged 10 to 19) was a risk-group of excessive smart phone users, compared to 8.9 % of Korean adults.

Korea's efforts to prevent and reduce internet and smart phone addiction

Established in 2002 by the government, the Korea Internet Addiction Center has executed comprehensive programs of counselling, content development & distribution, specialized counsellor training, as well as preventive education to whole nation in order to systematically address excessive use of Internet and smart devices. It has conducted annual status survey on Internet addiction of general people since 2004 (and smart phone addiction since 2011), producing national statistics that is used as a benchmark index for the government policy development.

In June, 2013, the eight ministries have jointly established a Second Comprehensive Plan for Preventing and Reducing Internet Addiction. The program identifies full ranges of preventive, counselling, psychiatric and aftercare assistances available for the whole age groups of infant, students and adults. The government implements the cross-ministerial policy committee to systematically address the Internet addiction. In March, 2014, the committee established the 2014 Execution Program for Preventing and Reducing Internet Addiction. This program has been jointly executed under the management of the eight ministerial policy committee in an effective and systematic manner.

a) Preventive education

Internet and smart media are so easily accessible in daily life that education should focus on prevention before addictive symptoms like withdrawal or tolerance appear. Korea's education program is designed to be an effective prevention, aiming at enhancing the public consciousness about potential or actual risk of addiction and helping them better able to prevent it. For example, it provides a preventive education, which adapts its curricular to the need of each of different age groups of infants, teens and adults. Specialized counsellors are sent to schools as lecturers giving a special (one-hour) class.

An intensive (two-hour) education program has been available for primary, middle and high school students since 2013; each course is differently designed to each school age, emphasizing student's participation and discussion in class activity. In the course, each student uses his or her own 'workbook' as self-diagnosis tool, keeping a self-monitoring record of Internet and smart media use and sometimes making a resolution to reduce Internet use, if they are found to be excessive users.

Table 2A: Number of participants of preventive education

Category	2010	2011	2012	2013	June 2014	Total
Preschool	-	31,279	18,200	47,890	26,050	**123,419**
Teenager	645,981	954,425	621,621	970,696	407,512	**3,600,235**
Adult	33,753	90,363	93,001	105,363	25,803	**348,283**
Total	**679,734**	**1,076,067**	**732,822**	**1,123,949**	**459,365**	**4,071,937**

(Unit: person)

Since 2014, it has started 'Addiction Prevention Play' for preschool child and lower-grade primary school students in order to easily and effectively deliver the message in a way that amuses these kids. In the program, child and students watch a play or a puppet show which tells stories about favourite animal's engagement of Internet addiction or Internet addiction in familiar daily life, after watching a play teacher talks about danger of Internet addiction and how to prevent Internet addiction. This program is effective in making child easily understand the concept of addiction without feeling of rejection.

It has also provided assistance the 23 schools that are designated as 'Clean Schools of Smart Media'. This program is to support school activities/campaigns for promoting a sound culture of using smart media and for preventing Internet addiction by cooperating with parents, teachers and experts.

b) Counselling services and infrastructure establishment

The Ministry of Science, ICT and Future Planning(MSIP) executes the preventive education and specialized counselling service in order to effectively address the addictions of Internet and smart phones. In order to provide region-specific service, it operates 14 Internet Addiction Prevention Center (IAPCs) installed at 13 cities or provinces nationwide as of June 2014.

It provides specialized counselling services that are delivered through a diversity of channels like home-visit or online services. These specialized counselling services are designed to be an effective response to rapidly increasing demand for counselling services, as well as easily-accessible services. An online counselling service at www.iapc.or.kr, as well as the nation-wide call center service at 1599-0075 is available. To provide region-specific services for Internet addiction that is occurring nationwide, the Center provides counselling service in collaboration with 48 related centers like Healthy Family Support Center, Youth Support Centers, etc.

Home visit counselling service merits special attention, which provides free counselling service to family by visiting their home. Any family that suffers from Internet addiction can apply for the service. The program is particularly effective for those Internet addicts who need help as they belong to single-

parent or low-income or interracial family, or live with grandparents. Also, whoever else needs help for Internet addiction-any children, teens, the jobless, or double-income family- are welcome to apply for this program. It also operates a training program to produce specialized counsellors for Internet addiction. The training program is available for current counsellors and current teachers so that they can also practice as specialized counsellors for internet addiction. It has produced more than 13,000 specialized counsellors as of June, 2014.

Table 3A: Number of counselling service by type

Category	2010	2011	2012	2013	June 2014
Face-to-face (Home visit)	15,037	10,522 (6,089)	20,701 (10,595)	24,623 (19,519)	7,484 (4,919)
Online	1,916	569	866	489	148
Telephone	9,569	7,915	16,138	11,512	4,779
Sub-total	**26,522**	**19,006**	**37,705**	**36,624**	**12,411**

(Unit: one service)

c) Conduct survey research and develop/distribute content

The policy researches are regularly conducted to increase the operational efficiency and scientific accuracy of the diverse program execution for Internet and smart media addiction. A diversity of educational materials like preventive guide books, flash animation, video, standard teaching books or counselling programs have been posted to be available at website. These materials have been developed in order to effectively execute preventive education and to help people better aware of potential risk of Internet or smart media uses.

In 2013, it developed and distributed standard teaching books for intensive addiction prevention. The courses are available in four editions by different lifetime cycle (e.g. primary school students, middle school students, high school students, and adults). Also, it developed guidelines of appropriate smart media uses, publishing them in four editions for four groups of readers (preschool child's parents, primary school students, and middle and high school students). The guidelines have been distributed to more than 20,000 schools across the nation. In 2014, it developed self-studying type of education content available in five categories for addiction prevention (for preschool child, primary school, middle and high school, university and adults) so that it can help schools and public institutions better ready to provide education for Internet addiction prevention, which has become mandatory under the revised National Information Basic Act (May, 2013), article 30, item 8 (regarding education related to Internet addiction).

It uses publicity to prevent smart media addiction by cooperating with private business sector. So that it can help teens and parents refrain from excessively using smart media, and make a habit of appropriate smart media use at home and schools.

Special feature of Korea's policy

In Korea, most of the activities are initiated by Government, thus Korean government is supporting civic organizations financially and technically for them to do the activities for the prevention of the Internet addiction. Strong government commitment is also shown in that minors under 16 years old are not allowed to access the online game from midnight to 6AM, and parents can monitor and block their children's (under 18 years old) access to the online game by the request to the service providers, and that all students from kindergarten to university and all employees in the public sector should be trained for the prevention of Internet addiction by the law. Furthermore, government is running the 14 Internet Addiction Prevention Centers across the nation. The challenge the Korea government faces

in preventing the Internet addiction is how to induce the participation of all stakeholders especially parents, community and private sectors.

Cooperation of Member States

Increasing use of Internet in all countries may cause the Internet addiction to become a world-wide issue. Therefore it is urgent to do international cooperation in developing a proper measure in protecting our citizens from the Internet addiction and developing a right habit to use a smart media. Thus, it is required to share the each nation's Internet addiction policy, especially guideline and manuals for the proper use of Internet and smart media. What is the appropriate age to be allowed to use smart media? What is a proper regulation on the use of smart media in the school context? How do parents have to respond to child's excessive use of smart media? These are typical questions concerning the proper use of smart media. Thus, it is required for the Member States to do cooperation in developing a proper policy and guideline/manuals to build the sound/healthy habit in using a smart media.

Country: Japan

Document: 2/90

Title: Sharing knowledge, information and best practice for developing a culture of cybersecurity

Summary: To ensure cybersecurity, not only government but also various entities, including the private sector and academia, should cooperate. It is important for this question to introduce such cooperative activities to members, especially developing countries.

Introduction

Cyber-attacks and malicious use of ICT have increased and become more complicated and their technical development and criminal approaching are also changing very fast. Strict rules and regulations tend to become easily outdated and therefore are not always effective and efficient to address these issues. ICT is used by not only governments but also by many other parties including the private sector, academia etc. and their participations and cooperation are essential to ensure cybersecurity. In light of the above-mentioned situation, Japan has conducted several actions on cybersecurity under cooperation among government and other parties and submitted a contribution (document WTDC14/36) to WTDC aiming at ITU-D SG1 Question 22-1/1 to continuously share best practices for developing countries to strengthen their capability to secure cybersecurity.

Japan's actions on cybersecurity

In the view of promoting best practice sharing, Japan would like to introduce its actions on cybersecurity. These actions are not only made by the government but also by other parties, especially the private sector, including private security companies. Japan has focused on four aspects, namely "network", "individuals", "technology" and "international partnership and collaboration" to ensure reliability of information and communications networks.

From the "network" viewpoint, Japan has encouraged information sharing among telecom operators. For example, in 2002, 19 major ISPs and telecom operators in Japan voluntary launched Telecom-ISAC (Information Sharing and Analysis Centre) Japan[14] that collects analyses and shares security information, such as vulnerabilities, incidents, countermeasures and best practices, among members. From the "individuals" viewpoint, Japan has raised awareness of internet users through website and seminars etc. From the viewpoint of "technology", Japan has promoted advanced research and

[14] https://www.telecom-isac.jp/.

development projects such as the PRACTICE project.[15] Through paying attention to these aspects, Japan has contributed to establishing reliable ICT networks and promoted international cooperation.

Proposal

Japan recognises the importance of sharing information on best practices, with public, private and academia, in Question 3/2 and therefore we would like to propose organising events , e.g. seminar, workshop etc., with other countries targeting developing countries with regard to cybersecurity. These events should be in collaboration with other Study Groups especially ITU-T Study Group 17, (Security). (Note: The ITU Workshop on ICT Security Standardization Challenges for Developing Countries was held 15-16 September 2014 in Geneva led by ITU-T Study Group 17. (http://www.itu.int/en/ITU-T/Workshops-and-Seminars/ict-sec-chaldc/Pages/default.aspx).

Country: Oman (Sultanate of)

Document: 2/342

Title: Oman Public Key Infrastructure (PKI)

Summary: As most of the population in Oman tend increasingly to use mobile phones intensely every day, the need of meeting this tendency has become more obvious. Thus, and as a part of the eGovernment Transformation Plan that has been effective since 2013, the mGovernment approach is adopted as a channel of delivering the government services. It became necessary to support the mobility and usability of the user and get a quick effective access to the government services. Therefore, the government represented by Information Technology Authority (ITA) established projects like Oman Public Key Infrastructure, to provide the foundation for the other public, private entities to provide services to the public through secured channel.

Introduction

As most of the population in Oman tend increasingly to use mobile phones intensely every day, the need of meeting this tendency has become more obvious. Thus, and as a part of the eGovernment Transformation Plan that has been effective since 2013, the mGovernment approach is adopted as a channel of delivering the government services. It became necessary to support the mobility and usability of the user and get a quick effective access to the government services. Therefore, the government represented by Information Technology Authority (ITA) established projects like Oman Public Key Infrastructure, to provide the foundation for the other public, private entities to provide services to the public through secured channel.

Mobile PKI

Oman Public Key Infrastructure (PKI) is a national initiative that sets the infrastructure needed for all government entities to provide eServices in Oman. It is employed in order to enable online transactions for citizens and to raise the level of security and authenticity of electronic paperwork. It allows exchanging information securely as it provides a high level of confidentiality by using eID, mobile ID or USB Token.

Oman PKI aims at providing a secure technology for information documentation, electronic credibility and identification and authentication of users as well as signing all transactions online by using electronic ID.

PKI is responsible for:

[15] http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/Telecommunications/130307_02.html.

- Delivering certification services on behalf of ITA in accordance with ITA approved policies, requirements and agreements.
- Providing the possibility to join Oman National PKI at Registration Authority (RA) or Sub Certificate Authority (Sub CA).
- Securing the communications between servers to servers or clients to servers by utilizing server/client.

PKI provides five main services:

1) Authentication: The traditional way of authenticating on websites was to sign in by entering the user name and the password. However, this way is not secure as anyone can hack them and use them illegally. Whereas, PKI uses an alternative method whereby an electronic ID, mobile ID or Token is required to authenticate the identity of the user.
2) Electronic Signature: Any citizen can use this feature to sign any certificate online at any time without the need to go to the concerned premises. S/he can use eID, mobile ID or Token to do so.
3) Encryption: It is the process of encoding information in such a way that only authorized parties can read it. PKI activated this feature so that information is saved securely.
4) Email Encryption: By utilizing PKI, persons can send files through emails safely in which USB Token is used only.
5) Email signature: another way of ensuring the confidentiality of data sent by emails is through signature which can be obtained from using USB Token only.

Why Mobile PKI?

- Convenience to use.
- High level of security.
- Relay on the SIM type not the Mobile type.
- Easley integrated with services providers.
- Mobile Apps utilization for service delivery.
- Utilization of Mobile's subscriptions penetrations

HR department at ITA was the first governmental body to use PKI for all ITA's employment documents such as job contracts, offer letters, signatures of all concerned parties, etc. Any entity in the Sultanate can set up its own PKI so that it facilitates signing, authenticating and encrypting certificates electronically.

It is worth mentioning that Ministry of Commerce and Industry, Ministry of Manpower, Public Prosecution and Muscat Municipality have started using this service. Whereas, other entities such as al Rrafd Fund and the Public Authority for Social Insurance will work on it in the coming few years.

Oman National PKI center will set up a "Registration Authority" accreditation for CBO (Central Bank of Oman). It will also be working on "The Internet Web Trust Accreditation" project which will make the SSL "Secure Socket Layer" Certificate recognized by Web Trust and can be part of any web browser. A Number of government entities as well are currently working to integrate with identity management portal to utilize the eID certificate for authentication and signing services.

Services

ITA PKI has the following services options which varies from providing different types of digital certificates either to Devices or Government and Commercial end user subscribers, or for individuals.

OR providing the possibility to join Oman National PKI as Registration Authority (RA) or Sub Certificate Authority (Sub CA). The following are brief tables highlighting the different services options.

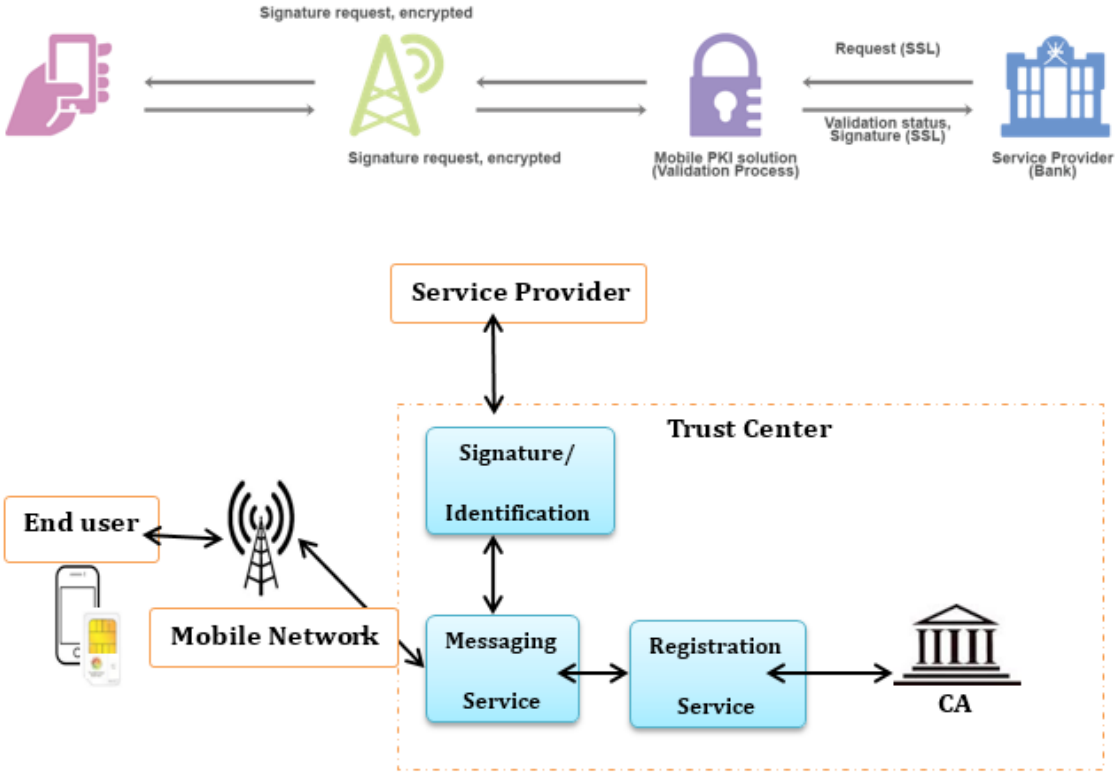
Table 4A: Different types of services options to be provided to Government and commercial entities

Options	Services/Certificate Type	Targeting	
		Gov&Com Device	Gov&Com Subscriber
Option 1	Authentication Certificates		X
	Signing Certificates		X
	Encryption Certificates		X
	Secure Email Signature Certificates		X
	Secure Email Encryption Certificates		X
	SSL Certificates (Server)	X	
	SSL Certificates (Client)	X	
	IPSec/VPN Certificates	X	
	Server signature Certificates	X	
Option 2	**Joining PKI Oman as RA (Registration Authority)**	X	X
Option 3	**Joining PKI Oman as Sub CA**	X	X
	Joining PKI Oman as TSA (Time Stamp Authority)	X	

Table 5A: Different types of services options to be provided to individuals

Services/Certificate Type	Targeting
	Individuals
Authentication Certificates (eID/Mobile)	X
Signing Certificates (eID/Mobile)	X

Figure 6A: Oman PKI



Country: Iran (Islamic Republic of)

Document: SG2RGQ/47

Title: National cybersecurity measures

Summary: A framework of best practices on identifying and use of measures and measurement is required for assessing the effectiveness of the information security management system at the national level. This contribution, which is fully inspired from ISO 27004, present a customized template for national cybersecurity measures.

A template and sample for national cybersecurity measures

Fully inspired from ISO 27004[16], a customized template for national cybersecurity measures is presented below. In each row, an example is also provided. As a future work, we intend to augment this set and provide a comprehensive set of national cybersecurity measures for the low-level (base measures) as well as the high-level (derived measures or indicators), for the 5 domains of national cybersecurity, and for different phases of development of national ICT infrastructure and national cyberspace security management system.

[16] ISO/IEC 27004, Information Technology-- Security Techniques-- Information Security Management – Measurement, 2009.

Table 6A: Customized template for national cybersecurity measures

Measurement identification	
Measurement name	Measurement name (e.g., information security incident management effectiveness).
Numerical identifier	Unique nation-specific numerical identifier.
Purpose of measurement	Describes the reasons for the measurement (e.g., assessing the effectiveness of the national Information security incident management).
Related security control	
Measure type	Effectiveness/efficiency, implementation-compliance, or impact (e.g. effectiveness).
Object of measurement and attributes	
Object of measurement	Object (entity) that is characterised through the measurement of its attributes. An object may include processes, plans, projects, resources, and systems, or system components (e.g. the national cybersecurity management system).
Attribute	Property or characteristic of an object of measurement that can be distinguished quantitatively or qualitatively by human or automated means (individual incident).
Base measure specification (for each base measure [1...n])	
Base measure	A base measure is defined in terms of an attribute and the specified measurement method for quantifying it (e.g. number of trained personnel, number of sites, cumulative cost to date). As data is collected, a value is assigned to a base measure (e.g. a pre-determined threshold number).
Measurement method (formula)	Logical sequence of operations used in quantifying an attribute with respect to a specified scale (e.g. count occurrences of information security incidents reported by the date).
Measurement method	Depending on the nature of the operations used to quantify an attribute, two types of method may be distinguished: - Subjective: quantification involving human judgment. - Objective: quantification based on numerical rules such as counting (e.g. objective).
Scale	Ordered set of values or categories to which the base measure's attribute is mapped (e.g. numeric).
Type of scale	Depending on the nature of the relationship between values on the scale, four types of scale are commonly defined: nominal, ordinal, interval, and ratio (e.g. ordinal).
Unit of measurement	Particular quantity, defined and adopted by convention, with which any other quantity of the same kind can be compared to express the ratio of the two quantities as a number (e.g. incident).
Data source	The security incident reported by all national organization such national security operating system.
Derived measure specification	

Derived measure	A measure that is derived as a function of two or more base measures (e.g. incidents exceeding threshold).
Measurement function	Algorithm or calculation performed to combine two or more base measures. The scale and unit of the derived measure depend on the scales and units of the base measures from which it is composed of as well as how they are combined by the function (e.g. comparing the number of total incidents with the threshold).
Indicator specification	
Indicator	Measure that provides an estimate or evaluation of specified attributes (e.g. line chart that depicts the constant horizontal line illustrating the threshold number(s) against the total number of incidents over several reporting periods.).
Analytical model	Algorithm or calculation combining one or more base and/or derived measures with associated decision criteria. It is based on an understanding of, or assumptions about, the expected relationship between the base and/or the derived measure and/or their behaviour over time. An analytical model produces estimates or evaluations relevant to a defined information need (e.g. red when total number of incidents exceeds the threshold (goes over the line); yellow when total number of incidents is within 10% of the threshold; green when total number of incidents is below the threshold by 10% or more).
Decision criteria specification	
Decision criteria	Thresholds, targets, or patterns used to determine the need for action or further investigation, or to describe the level of confidence in a given result. Decision criteria help to interpret the results of measurement (e.g. red – immediate investigation into causes of increase in number of incidents is required. Yellow – numbers need to be closely monitored and investigation should be started if numbers are not improving. Green – no action is required).
Measurement results	
Indicator interpretation	A description of how the sample indicator (see sample figure in indicator description) should be interpreted (e.g. if red is observed in two reporting cycles, a review of the incident management procedures is required to correct existing procedures or to identify additional procedures. If the trend is not reversed during the next two reporting periods corrective action is required, such as proposing an extension to the ISMS scope).
Reporting formats	Reporting formats should be identified and documented. Describe the observations that the organization or owner of the information may want on record. Reporting formats will visually depict the measures and provide a verbal explanation of the indicators. Reporting formats should be customized to the information customer (e.g. line chart).
Stakeholders	
Client for measurement	Management or other interested parties requesting or requiring information about the effectiveness of the national cybersecurity management system controls or group of controls (e.g. NCMS committee, managers responsible for the NCMS, security management, incident management).

Reviewer for measurement	Person or organizational unit that validates the appropriateness of measurement constructs for assessing the effectiveness of NCMS controls or group of controls (e.g. managers responsible for the national cybersecurity management system).
Information owner	Person or organizational unit that owns the information about an object of measurement and attributes and is responsible for the measurement (e.g. managers responsible for the national cybersecurity management system).
Information collector	Person or organizational unit responsible for collecting, recording and storing the data (e.g. incident manager).
Information communicator	Person or organizational unit responsible for analysing data and communicating measurement results (e.g. NCMS Committee).
Frequency/Period	
Frequency of data collection	How often data is collected (e.g. monthly).
Frequency of data analysis	How often data is analysed (e.g. monthly).
Frequency of reporting measurement results	How often measurement results are reported (this may be less frequent than data collection).
Measurement revision	Date of measurement revision (expiry or renovation of measurement validity) (e.g. six months).
Period of measurement	Defines the period being measured (e.g. monthly).

Country: Iran (Islamic Republic of)

Document: SG2RGQ/46

Title: National cybersecurity measures and measurements

Summary: This contribution is an attempt to develop a framework for "national cybersecurity measurement program (NCMP)" with emphasis on identifying and using appropriate metrics for evaluating and/or enhancing the planned or implemented "national cybersecurity management system (NCMS)". Once adequately designed and successfully implemented, the NCMP can be regarded as a major component of the NCMS, which provides the means to quantitatively present a picture of national security posture, monitor the effectiveness of the implemented NCMS, and the extent of compliance with laws, rules and regulations. It can also indicate deviations from the expected security requirements and objectives, and increase the accountability by helping to identify either incorrectly or ineffectively implemented security controls or the ones that have not been implemented. All of the above provide important quantifiable inputs for proper decision making for enhancing cybersecurity at the national level and for allocating the required resources. This contribution also discusses the necessity and importance of developing security metrics and measurement at the national level. Developing a comprehensive set of metrics for national cybersecurity is vital for achieving the aforementioned objectives of NCMP at the national level. Inspired from the state-of-the art security metrics already developed for organizations, we will introduce a set of metrics that can be used by institutions at the national level for developing their NCMPs.

Introduction

Assessment of cybersecurity at the national level requires continuous measurement of cybersecurity indicators. In order to plan and implement an effective national cybersecurity management system (NCMS) [1], there is an urgent need to develop an appropriate national cybersecurity measurement

program (NCMP). NCMP facilitates decision-making and improves the performance and accountability at the national level.

A framework of best practices for identifying and using a set of measures and measurement is needed to assess the effectiveness of an information security management system at the national level. Similar to the NCSec framework in [1], which was fully inspired from ISO/IEC 27001 [2] for the ISMS at the organizational level, we propose a "national cybersecurity measurement" which is inspired from ISO/IEC 27004 [3] and NIST-800-55-R1 [4], both of which were developed for assessing cybersecurity at the organizational level. Also, similar to the case that was inspired from ISO/IEC 27001, there is a need to "define how to measure the effectiveness of the selected controls or groups of controls and specify how these measures are to be used to assess the effectiveness of controls to produce comparable and reproducible results" at the national level.

This contribution is an attempt to develop a framework for "national cybersecurity measurement program (NCMP)" with emphasis on identifying and using appropriate metrics for evaluating and/or enhancing the planned or implemented "national cybersecurity management system (NCMS)". Once adequately designed and successfully implemented, the NCMP can be regarded as a major component of the NCMS, which provides the means to quantitatively present a picture of national security posture, monitor the effectiveness of the implemented NCMS, and the extent of compliance with laws, rules and regulations. It can also indicate deviations from the expected security requirements and objectives, and increase the accountability by helping to identify either incorrectly or ineffectively implemented security controls or the ones that have not been implemented. All of the above provide important quantifiable inputs for proper decision making for the improvement of national cybersecurity and allocation of required resources.

In what follows, we first introduce the concepts related to security measures and then present our proposed general framework for the NCMP.

Security measures

a. Base measures, derived measures and indicators

ISO/IEC 27004 identifies the derived measures, each of which is a function of two or more base measures; and the indicators, each of which is a function of two or more base/derived measures combined with a predefined decision criteria (i.e., targets) for measurement. All three layers can collectively be referred to as measures. The terms metrics and measures interchangeably.

b. Types of security metrics

NIST [4] categorizes performance metrics in three categories:

- Implementation or compliance metrics,
- Effectiveness/efficiency metrics, and
- Impact metrics.

Implementation or compliance measures are used to demonstrate progress in implementing programs, specific security controls, and associated policies and procedures [4]. Implementation measures related to information security programs include the percentage of national information systems with approved system security plans, and the percentage of national information systems that require password policies. Implementation measures can also examine system-level areas—for example, servers within a system with a standard configuration. Implementation measures assess the implementation progress of NCMP, security controls, and the national security policies and procedures (both programme- and system-level).

Effectiveness/efficiency measures are used to monitor if the program-level processes and the system-level security controls are correctly implemented, are operating as intended, and the expected

outcome is met [4]. Implementation metrics indicate if specific security controls, and their associated policies and procedures are implemented, regardless of how effective or efficient they may be, while effectiveness/efficiency measures indicate how effective/efficient the implemented controls and associated policies and procedures are. Impact measures are used to articulate the impact of information security on mission [4] at national level.

NIST SP 800-55 [4] emphasizes the relation between the maturity of information security programme and the types of measures that can be obtained. It proposes three types of security measures at both system and programme levels, namely, the implementation, the effectiveness/efficiency, and the business impact measures. The results of implementation measures may be less than 100 percent at the beginning, but as NCMS and its associated policies and procedures mature, results should reach and remain at 100 percent. When the implementation measure remains at 100 percent, it can be concluded that the national information systems are utilizing the security controls that are relevant to this measure, but measurement controls need improvement. After most of the implementation measures reach and remain at 100 percent, the organization should begin to focus its measurement efforts on effectiveness/efficiency and impact measures. Organizations should never fully retire the implementation measures because they identify specific areas that are in need of improvement. As the national cybersecurity system matures, the emphasis and resources of the measurement programme should shift away from implementation towards the effectiveness/efficiency and the impact measures [3].

Figure 7A: General framework of NCMP major processes that collectively comprise a NCMP

A general framework for NCMP

Inspired from ISO/IEC 27004, major processes that collectively comprise a NCMP are (see Figure 7A):

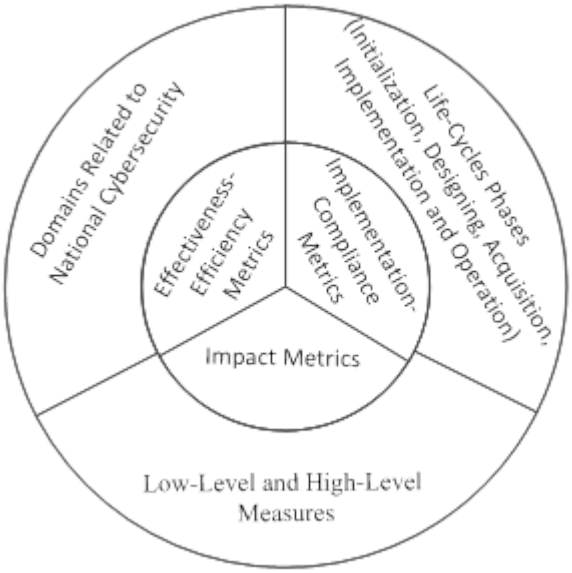
- Measures and measurement development;
- National cybersecurity measurement operation;
- Data analysis and measurement results reporting, and using them for proper decision making;
- NCMP evaluation and improvement.

Using information security metrics in the NCMP can provide the following benefits:

- A quantitative picture of national security posture;
- Monitoring the effectiveness of NCMS and the extent of compliance with applicable laws, rules and regulations;
- Determining the deviation from the expected results (predetermined security requirements and objectives);

- Increasing the accountability by identifying either incorrectly or ineffectively implemented security controls or those that have not been implemented, and their corresponding stakeholders;
- Providing important quantifiable input to facilitate proper decision making for enhancing national cybersecurity and allocating the required resources;
- Providing management reports on the impact of past and current activities;
- Assessing security products or services from third parties and providing means to compare different products, services, policies and procedures.

Figure 8A: General scope for national cybersecurity measures



The scope of NCMP determines the types of security measures, at both low-level (base measures) and high-level (derived measures or indicators), for the 5 domains of national cybersecurity, and during different phases of national ICT infrastructure and NCMS (see Figure 27). A total of 34 processes comprise these domains, which are strategy and policies, implementation and organization, awareness and communication, compliance and coordination, and evaluation and monitoring [1]. Collecting, analysing and reporting appropriate security measures during different phases of system development causes integration of security considerations into the national ICT infrastructure and NCMS development. This would ensure that system security requirements are built-in from the design phase to the implementation and operation phases, rather than as an add-on at a later stage [3], which is complicated and costly. The scope of NCMP depends on each specific stakeholder needs, strategic goals and objectives, operating environments, risk priorities, and maturity of the national cybersecurity programme.

Conclusions and directions for future works

National cybersecurity measurement can play an important role in improving the global cybersecurity. The challenges include identifying a set of well-defined and comprehensive security measures, and implementing an effective NCMP via active cooperation and information sharing between governments, industry, international organizations and other relevant stakeholders.

References

[1] ITU-D Study Group 1, Final Report, Question 22-1/1, Best Practice for Securing Information and Communication Networks: Best Practices for Developing a Culture of Cybersecurity, 2014.

[2] ISO/IEC 27001, Information Technology-- Security Techniques-- Information Security Management Systems – Requirements, 2005.

[3] ISO/IEC 27004, Information Technology-- Security Techniques-- Information Security Management – Measurement, 2009.

[4] NIST Special Publication 800-55 Revision 1, Performance Measurement Guide for Information Security, 2008.

Country: Korea (Republic of)

Document: 2/234

Title: Korea's K-ICT security development strategy

Summary: As voluntary investments for the expansion of information security systems and reinforcement of manpower are insufficient, and the security infrastructure of non-ICT sectors or SMEs is inadequate, there are many blind spots. To cope with these obstacles, the Korean government announced the "K-ICT Security Development Strategy" in April 2015. This contribution introduces the overall contents and its expected benefits.

Background

As the age of super connection and ICT convergence in which everything is connected to the Internet, and the ICT convergence with existing industries is accelerating, cyberspace has become a secondary sphere of life. Security threats in the cyberspace, however, are becoming more intelligent and covert and cause enormous economic damages and social confusion, which directly affects the life of citizens and national security. Moreover, cyber-attacks keep evolving and grow into a more intelligent, covert and bigger cyber-warfare even targeting national infrastructure. Korea, which is recognized as one of the most connected countries in the world, still lacks voluntary efforts in the private sector, public awareness concerning information security, and the fundamentals such as related industry infrastructure, professional manpower, and technology. As voluntary investments for the expansion of information security systems and reinforcement of manpower are still insufficient, and the security infrastructure of non-ICT sectors or SMEs is inadequate, there are many blind spots.

To cope with these problems, aside from the IoT security roadmap that was presented in the last rapporteur meeting, the Ministry of Science, ICT & Future Planning (MSIP) of Korea announced the "K-ICT Security Development Strategy" to reinforce the competitiveness of the information security industry, technology, and manpower in April 2015.

This strategy includes four projects. The first is to create a future growth engine by reinforcing the infrastructure of the information security industry. The second is to develop source security technologies and the third is to foster top-notch security manpower as well as create a culture conducive to information security. Last but not least is to increase investments to enhance the resilience of cyber security.

Creating a future growth engine by reinforcing the infrastructure of the information security industry

The Ministry is planning to improve the structure of the information security industry by switching the existing price competition-based market to a performance-based one, and to introduce a proper system for paying fair prices for information security services. Also, the Ministry will prepare and provide "the Information Security Service Price Assessment Guideline" to introduce a system for assessing the fair price of information security continuity service, which ensures appropriate security performance of related products.

In addition, the Ministry is planning to provide information security investment incentives, such as giving preferences in participation in the government and public procurement and R&D, to induce corporations to voluntarily invest in security and take active measures. The Ministry will also review and push ahead with the public announcement of corporate information security status that includes the status of related manpower, organization, education, etc. of a business to encourage autonomous security competition among corporations and help users choose better products and services. In particular, the Ministry is planning to reinforce the evaluation for the level of information security investments to enhance the security level of key private enterprises such as mobile communication services and Critical Information Infrastructures (CIIs).

The Ministry is also planning to identify and foster information security startups by providing support such as sharing security vulnerabilities, test beds and international certification support so that excellent security ideas can lead to successful startups. In addition, the Ministry is seeking to identify best security models of new industries like drones, next-generation CCTVs, and biometric products and turn them into new economic growth engines.

Developing source security technologies

The Ministry is planning to encourage national R&D centers and private enterprises to develop world-class information security products and technologies by 2019 by intensively studying innovative, intelligent and invisible technologies with the goal of leading the global cybersecurity market and securing technology competitiveness.

These research communities and related businesses are expected to lead innovative technologies that respond to new threats in the ICBM (IoT, cloud, big data, mobile) environment, key infrastructure control network security and intelligent cyberattacks such as Advanced Persistent Threats (APT). They will also develop smart security technologies to reduce cyber threat response time, such as cyber threat detection technologies and forensic technologies for attack source traceback. In addition, they will intensively develop convenient security (usable security) technologies including the fraud detection system (FDS) for users.

Another plan of the Ministry is to build a global cyber open R&D system by allowing more outstanding overseas researchers to participate in domestic R&D activities, and making them to conduct joint studies with leading institutes and universities in cyber security related areas.

Fostering top-notch security manpower and creating a culture conducive to information security

The Ministry will continuously increase the number of information security schools so that potential security manpower can enter colleges without worries about the college scholastic ability test, and recruit military and police cyber security specialists to prevent career interruption caused by mandatory military service.

The Ministry is also planning to foster security coordinators to reinforce the security competence of field workers in different industries, such as the financial and manufacturing industries, and bring up top-notch manpower in different areas such as finance and national defense.

The Ministry is going to turn and expand the Korea Internet & Security Agency (KISA) Academy into an institution dedicated to fostering top-notch security manpower (cyber security manpower center), and build a cybersecurity training center (Security-GYM) to strengthen cyber response capabilities. In addition, the Ministry will carry out the nationwide information security culture movement (Security All Wave) to turn the awareness of the importance of information security into action by transforming information security into a social culture. The Ministry is also planning to induce voluntary compliance with security rules by developing and disseminating customized security rules for different information security agents, which include individuals, enterprises and Chief Executive Officers, etc.

Increasing investments to enhance the resilience of cyber security

With close cooperation with the Korea Internet & Security Agency, the Ministry will diagnose the current status of cyber safety to reinforce the security of key infrastructures of the private sector (ISP, infrastructure, etc.) and services used by many people such as online storages, routers, portals, etc., and build an in-depth cyber detection system to quickly detect cyberattacks and expand the response range.

The Ministry is also planning to build 100,000 cyber traps to lure hackers as a way to reinforce responses to electronic financial frauds, such as pharming and smishing, and ensure the security of devices including smartphones, routers and CCTVs, and to improve the cyber threat response systems by implementing Chief Information Security Officer (CISO) hotlines between the government and key enterprises (mobile carriers, portals, IDC, etc.).

The Ministry will reinforce security throughout the supply chain of Critical Information Infrastructures, including external management manpower, consignment and outsourcing, purchasing and procurement, and will also actively support the implementation of Information Sharing and Analysis Centers (ISACs).

To provide customized information security services for SMEs, the Ministry is planning to reinforce technical and site support for quick emergency response and system recovery in case of infringement accidents, and establish more information security support centers.

Way forward

The Korean government is expected to increase the size of the domestic information security market by improving the structure of the information security industry, to expand investments in information security and to create new demands for convergence security and physical security.

To become one of the most powerful countries in cyber security in the world, the fundamentals of the information security industry should be very strong and resilient, and the Korea government expects that this strategy will serve as a turning point in innovating the information security industry, technology and expertise of Korea. Moreover, a large number of new jobs are expected to be created by promoting the convergence security and physical security industry and internalizing information security across all industries including communication, finance, manufacturing, and energy.

Country: Odessa National Academy of Telecommunications n.a. A.S. Popov (Ukraine)

Document: 2/156

Title: Multimedia distance-learning course on the safe use of Internet resources

Summary: ITU's Telecommunication Development Bureau as part of the CIS regional initiative on "creating a child on line protection centre for the CIS region", adopted at WTDC-14 (Dubai, UAE), with the support of the Odessa National Academy of Telecommunications n.a. A.S. Popov (Ukraine).

The course is divided into three parts: basic (for pre-school and junior school children); intermediate (for children in classes 5 to 9); and advanced (for senior pupils, students, parents and teachers). Each course is based on thematic modules with tests after each module.

Introduction

The CIS region had already begun to consider the issue of protecting children on line at the end of the 1990s. Approaches to the problem differed among the countries of the region, however, reflecting

the range of views in different countries on issues of public morals, pornography, privacy and data protection.

All countries in the region without exception have acceded to the Convention on the Rights of the Child, without any declarations or reservations regarding Articles 16, 17 and 34(c). All countries in the region have also acceded to, signed and/or ratified the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, without any declarations or reservations regarding Articles 2 and 3 of that instrument.

In many countries in the region, software producers, telecommunication operators and educational establishments are actively developing child on line protection programmes of their own. Notable examples might be two Ukrainian projects: "Safety of Children on line", which is being implemented by the Coalition for the Safety of Children on line; and "System for restricting access to inappropriate Internet resources", a project being developed by the Odessa National Academy of Telecommunications n.a. A.S. Popov (Ukraine). In May 2012 the project "Building safer internet for educational institutions", which formed the framework for the presentation of the system for restricting access to inappropriate Internet content, was recognized as the best project in the category "C5. Building confidence and security in the use of ICTs" in a competition organized as part of the WSIS Forum 2012 event (Geneva, 14-18 May 2012), and acknowledged by the Secretary-General of ITU as one of the major achievements in creating connectivity worldwide.

With their common political, economic, environmental, humanitarian and cultural history, the countries of the Commonwealth of Independent States (CIS) share a number of characteristics with regard to Internet use, and this has an impact on users' interests and resources. The key factors here include: a close linguistic environment (most of the peoples in the CIS countries are fluent in Russian); a more or less identical level of ICT development and broadband penetration; common problems in the applications of ICTs (a sharp contrast in terms of teacher training in the towns and rural areas, a common "post-soviet" model of education, an absence of trained system administrators in rural schools, and so on); and a roughly similar level of Internet regulation.

The international seminar on integrated aspects of child protection on the Internet, held in Odessa, Ukraine, in April 2011, and the Interregional seminar for Europe, the Asia and Pacific region and the Commonwealth of Independent States on "Current methods for combating cybercrime" (March 2012), identified the main obstacles to strengthening confidence and child on line protection in developing countries. Participants noted in particular the importance of international cooperation as a means of exchanging experience and improving child on line protection.

A natural progression from this idea was the adoption at the World Telecommunication Development Conference 2014 (Dubai, UAE) of the CIS initiative on "creating a child on line protection centre for the CIS region". One of the expected outcomes of that initiative is the creation of distance-learning courses on safe use of Internet resources involving testing of children, parents, teachers, and so on.

It should be noted that existing training materials (including multimedia clips and courses) do not cover the entire range of issues pertaining to Internet safety and as a rule do not include systems for testing and certification. In the light of this, the Odessa National Academy of Telecommunications n.a. A.S. Popov (Ukraine) proposed to develop a course on the safe use of Internet resources along the lines of the UN course on "Security in the Field", which could then be followed by children, parents and educational staff.

It was proposed that the course should be divided into three parts: basic (for children of pre-school and junior school age); intermediate (for children in classes 5 to 9); and advanced (for senior school pupils, students, parents and teachers), each part being based on thematic modules with testing on completion of each module.

The Academy proposed the structure and basic features of the courses, which were presented at the fourth meeting of ITU-D Study Group 1 (document 1/265, study period 2010-2014) and at the seventh meeting of the Council Working Group on Child on line Protection (document WG-CP/7/5).

By September 2015, a Russian-language demonstration version of the course is to be available on line at http://www.onlinesafety.info . Final development and testing are planned for November 2015. The course interface is adapted for use on line using a variety of operating systems and web browsers (including mobile devices based on iOS and Android operating systems).

Basic course

The basic course is structured in three modules: "general information on security in the Internet"; "rules for communication on line"; and "useful and harmful on line games". To begin with, children choose a hero (boy or girl) to help them follow the course. All slides and navigation moves effected with the cursor are also voiced by the chosen hero.

During the course the child studies such topics as "what is the Internet and how is it organized?"; "what useful things can I get from the Internet?"; "the main dangers on line"; "virus programmes that harm a computer"; "virus programmes for spying on users or gathering personal data held on the computer"; "Illegal, unethical and harmful content"; "misleading content"; "Cyber-bullying and cyber-grooming"; "benefits and harm from social networks"; "what can I tell other people on line and what must I not tell them?" "rules of 'netiquette'"; "how do I create my on line profile"; "how and what to play on line"; "possible harmful effects of computer games (including the influence of Internet slang on colloquial speech)", and so on.

The course includes 52 slides of between 10 and 20 seconds' duration, depending on the density of their multimedia content. Each slide is based on a white background. Colour series are formed in accordance with the Itten principles, and each module has its own colour frame (dark blue, yellow or green). The rate of progress though the course is shown by an animated figure moving in a straight line at the bottom of the screen to indicate the progress made.

The basic part of the course contains five multimedia clips, four interactive games and 50 cartoon-style graphics. For example, in one slide the child is asked to play a game "Get the virus!". A target in the form of a "virus" moves around the screen. The aim is to strike at it with a special on line "hand", but the game is designed to ensure that the child cannot succeed in hitting the virus target. After several attempts a voice explains that a computer virus cannot be eliminated in that way and instead, an antivirus programme has to be used.

Throughout the course, the child periodically has to answer test questions involving animated figures. This helps to consolidate the knowledge acquired. A separate test is not envisaged in the basic course and a certificate is issued automatically on completion.

Intermediate course

The intermediate course comprises five modules: "general information on security in the Internet"; "safe entertainment on line"; "rules for communicating with others on line"; "what can you believe on the Internet?"; and "how to protect oneself on line".

In the first slide, the child learns about the purpose of the course and its format. During the course the child studies topics such as "what is the Internet and how is it organized"; "the main dangers on line"; "Illegal, unethical and harmful content"; "misleading content"; "cyberbullying and cyber grooming"; "Internet fraud"; "basic rules for using the Internet"; "how not to be a victim of virtual reality"; "the influence of Internet slang on colloquial speech"; "antivirus software"; "basic precepts of "netiquette"; "what can I write about (and save) on line?"; "anonymity on line"; "how to verify information on line"; "copyright on line (music, video, images, presentations, dissertations, etc.)"; "working via public networks (WiFi zones, Internet clubs, etc.) or using someone else's computer"; "rules for working safely with e-mail"; and "who can help if there is a problem on line?".

The course includes 122 slides of between 10 and 20 seconds' duration each, depending on the density of their multimedia content. For each sequence there is voice-over accompaniment. Each sequence is based on a white background. Colour series are formed in accordance with the Itten principles and each module has its own colour frame. The rate of progress though the course is shown by "road blocks" indicated by white screens which change to green once a module has been completed The intermediate part of the course contains five cartoon clips (different from the basic course), two interactive games, 77 cartoon-style figures and 12 infographic figures.

On completing the course the child takes a test comprising ten questions which contain possible answers. The test set is based on random selection from 40 questions (eight for each module).

Advanced course

The advanced course comprises seven modules: "general information on security in the Internet"; "rules for communicating with others on line"; "safe entertainment on line"; "what can you believe in the Internet?"; "confidentiality and working via public networks"; "risk assessment and behaviour in difficult situations"; and "methods of filtering content and child protection on line".

The advanced course interface is designed to be as similar as possible to that of the UN advanced "Security in the Field" course. Information is presented with the aid of a number of different types of slide and additional elements which make it possible to create small interactive scenarios using a range of multimedia content. Participants study such topics as "basic information on Internet architecture"; "existing threats (viruses, fraudsters, criminals and so on)"; "how to remain literate when communicating with others on line", "what can you write about and what should you not write about on line?"; "ensuring that children do not view undesirable content"; "copyright and how you can break the law without knowing it"; "how much time may I spend on line?"; "the influence of Internet slang on colloquial speech"; "typical forms of Internet fraud"; "data protection"; "monitoring children's behaviour on line"; "threats to life and health on line"; "basic content filtering techniques"; "advice on choosing content filtering systems (for homes, schools and institutions)", and other aspects. The course includes 57 slides of 30-40 seconds' duration each, depending on the density of their multimedia content. Each sequence is provided with a partial audio accompaniment.

The advanced part of the course comprises three cartoon clips (different from the basic and intermediate courses), five interactive games, 23 photo images, and 19 infographic-style figures. An example of an interactive game at the advanced level could be a dialogue between the user and an imaginary character of the opposite sex. Following the lead-in, a conversation develops and is led by the imaginary character. The user selects responses from a set of ready-made models from a list. The list includes various options containing Internet slang and/or stylistic and spelling errors, as well as replies that are stylistically and grammatically sound and do not include slang. The aim of this dialogue is to induce the interlocutor to engage in further discussion, create a positive impression, and so forth; this is not achieved if too much use is made of Internet slang, or if the chosen responses contain stylistic and spelling mistakes. When the dialogue is finished, feedback is given to the user on the use of Internet slang during the interactive discussion.

Conclusion

The Odessa National Academy of Telecommunications n.a. A.S. Popov (Ukraine) invites all interested parties to collaborate in testing and disseminating the course that has been developed and to translate it into the official languages of ITU.

Country: Togo (Republic of)

Document: 2/153

Title: Security of electronic transactions

Summary: The Public Key Infrastructures commonly used to secure electronic communication services contribute to establishing confidence in the use of ICTs. Economic models stemming from their value chain can bring growth in the digital economy of the States that implement them. The ever-increasing development of electronic commerce and transactions, the progressive and large-scale deployment of new protocols and network services based on Public Key Infrastructures, and the security of the Internet of Things are, ***inter alia***, reasons that should encourage the creation of root certification authorities in developing countries on the one hand, and the rethinking of a model of organization for the trust chain of the national-level root certification authority in a global way, on the other hand.

The objective of this contribution is to invite ITU-D Study Group 2 and ITU-T Study Group 17 to study the impact and potential benefits of establishing root certification authorities in developing countries in order to elaborate a programme to implement such root certification authorities, if appropriate. This study should enable estimation of developing countries' preparation for having a national root certification authority, and allow streamlining of the assistance that BDT is already providing, for instance on CIRT implementation.

Introduction

The development of electronic commerce and transactions, including online purchases and payments, execution of stock market orders, online administrative tax filing (VAT, income tax, electronic medical care sheet), exchanges of e-mails and electronic documents; the implementation of new network security protocols based on public key infrastructures and their progressive large-scale deployment, in particular, DNSSEC, RPKI (Resources Public Key Infrastructure); and the security of the Internet of Things are crucial elements which should incite developing countries to work towards the establishment of institutions at national or regional level in charge of the management of their public key infrastructures. The creation of these institutions, if properly supervised, can contribute to strengthening the security of electronic communications in general, and that of electronic transactions in particular. They can also allow the emergence and development of digital economies in developing countries.

Statements

Electronic commerce and transactions are developing rapidly in developing countries. These transactions typically use insecure channels. However, when they are secured, they are based on self-signed certificates or on certificates purchased using certification authorities generally based in developed countries. In some cases, however, these certificates are not necessarily in accordance with the legislation of developing countries.

The lack of enthusiasm and the delays noted in the deployment of secure protocols, such as DNSSEC and RPKI, in developing countries are due to misunderstanding either of these protocols or the standards that allow their implementation, or to the insufficiently trained human resources involved in their deployment, or to a non-mastered grasp related to chains value.

All these inadequacies can be improved with the implementation of a root certification authority in each country. Indeed, the authorities, besides their traditional roles, will also be tasked with the broadcast, validation, and revocation of certificates to promote a culture of secure electronic transactions, as well as the organization of trust chains to national and international levels.

To assure this situation, some developing countries have set up root certification authorities. However, the functioning of these certification authorities does not necessarily reflect the state of the art in the field. It is advisable to improve the functioning of certification authorities, in particular, by implementing clear procedures based on best practices as well as accepted standards on the subject. This will have the advantage of ensuring the security of transactions and consumers in those developing countries that have already set up their certification authority on the one hand, and on

the other hand, will promote the implementation of these certification authorities in those countries that do not have such capability.

Thus, in the context of the emergence of new digital economies in developing countries, the establishment of root certification authorities can be an important link and a social and economic development lever.

Proposal

This contribution aims at asking Question 3/2 to undertake a study on the impact of the implementation of root certification authorities in developing countries. The study should possibly lead to a proposal for the establishment of such root certification authorities in Member States, along the lines of what is currently being done with the setting up of CIRTs.

The objectives of the study include:

- Assessing the readiness of developing countries for setting up root certification authorities at a national level;
- Identifying requirements in terms of the skillset necessary to set up and run certification authorities at a national level;
- Performing a gap analysis on the current national legal frameworks to better identify the actions required to improve national legislations on cryptography, digital certification and digital signature;
- Reflecting on business models and operational plans to support the viability of the activities of the national root certification authority while taking into account regional specificities;
- Assessing the possible evolution of national root certification authorities toward a chain of trust between them.

Furthermore it is requested that Question 3/2 coordinate with ITU-T Study Group 17 to investigate the opportunity to:

- Set up a human capacity-building programme for developing countries based on standards and the implementation of standards related to electronic certification, in particular the X.500 series standards;
- Develop kits of best practices on the implementation and use of standards related to electronic certification.

Conclusion

The security of electronic transactions is fundamental in building confidence in the use of ICTs. The establishment of institutions whose operation should achieve this goal is essential for developing countries. However, it should be referenced by politically, technically and organizationally based frameworks that enable the creation and smooth organization of these institutions.

Country: United States of America; Netherlands (Kingdom of the)

Document: 2/332

Title: The Global Forum on Cyber Expertise (GFCE)

Summary: This contribution provides a background and explanation of the Global Forum on Cyber Expertise (GFCE), a global initiative that was launched by the Netherlands in April 2015 at the Global Conference on Cyberspace in The Hague. The GFCE currently has 52 members and is open to all governments, intergovernmental organizations, and private companies who sign on The Hague

Declaration on the GFCE. The GFCE is a platform for sharing of best practices, identifying gaps in global cyber capacities, and complementing existing capacity building efforts. The United States is proud to be one of the founding members of the GFCE.

This contribution is related to the following issues for study from the Question 3/2 Terms of Reference: c) Continue to gather national experiences from Member States relating to cybersecurity, and to identify common themes within those experiences. e) Provide a compendium of relevant, ongoing cybersecurity activities being conducted by Member States, organizations, the private sector and civil society at the national, regional and international levels, in which developing countries and all sectors may participate, including information gathered under c) above.

Introduction: What is the GFCE?

Societies worldwide have a growing demand for cyber capacity in order to reap the full economic and social benefits of cyber technology. Everyone should be able to profit from the potential an open, free and secure internet has to offer. To answer to the growing global demand for cyber capacity, The Netherlands Government launched the Global Forum on Cyber Expertise initiative (GFCE) during the Global Conference on Cyberspace, in April 2015. The GFCE is a key multi-stakeholder voluntary initiative for fostering international solidarity and providing political, technical and financial support for efforts to strengthen international cooperation among all stakeholders on cyber issues. The GFCE promotes cyber capacity building in a vision where the interests for security, economy and human rights go hand in hand.

What does the GFCE do?

The GFCE was established to strengthen cyber capacity and expertise to make the existing international cooperative efforts more effective.

GFCE Goals:

- **Exchanging expertise**: The GFCE offers a broad, informal platform for countries, international organizations and private companies to exchange experiences, expertise, best practices and assessments on four themes of cyber capacity building: ***cybersecurity, cybercrime, data protection and e-governance***.
- **Development of practical initiatives:** The GFCE functions as an incubator for the development of practical initiatives on these four themes (together with experts from NGOs, academia and the tech community).
- **Agenda setting of cyber capacity building**: The GFCE sets cyber capacity building as a strategic issue on the global agenda and takes the lead in streamlining and escalating cyber capacity building efforts on a global level.

What is the structure of the GFCE?

The GFCE is comprised of the Secretariat, Members, Partners and the Advisory Board.

GFCE Secretariat

The GFCE has a permanent Secretariat that is located in The Hague and gives logistical and administrative support to GFCE members and partners.

GFCE Members

GFCE Members are countries, intergovernmental organizations, and private companies committed to building cyber capacity worldwide. The GFCE has 52 members including the following:

Countries		Intergovernmental organizations	Corporations
Argentina	Mexico	African Union	Hewlett Packard

Countries		Intergovernmental organizations	Corporations
Australia	Morocco	Council of Europe	IBM
Bangladesh	The Netherlands	Economic Community of Western African States	Huawei
Belgium	New Zealand	Europol	Microsoft
Canada	Norway	International Chamber of Commerce	NRD CS
Chile	Peru	International Telecommunication Union	Symantec
Estonia	ROK	Organization of American States	Vodafone
European Union	Romania		
Finland	Rwanda		
France	Senegal		
Germany	Spain		
Hungary	Sweden		
India	Switzerland		
Israel	Tanzania		
Japan	Turkey		
Kenya	USA		
Latvia	UK		
Vietnam			

GFCE Partners

GFCE Partners are organizations with specific cyber expertise which are invited by GFCE members to participate in a GFCE initiative. GFCE Partners include: The Global Cyber Security Capacity Centre (GCSCC), Meridian Community, and the United Nations Office on Drugs and Crime.

GFCE Advisory Board

The GFCE Advisory Board consists of two Co-chairs and 9 representatives from civil society, the technical community and academia. Members serve voluntarily on the Advisory Board for a period of two years, and applications are gathered through an open call published on the GFCE website. The composition of the Advisory Board aims to reflect the geographic, gender and stakeholder balance of the GFCE. Members strive to provide substantive and strategic guidance to the GFCE members on the forum's strategic objectives, activities and initiatives, and are committed to the principles as set out in The Hague Declaration and the GFCE Framework Document.

How can a country become a member of the GFCE?

The GFCE aims to be a platform for the development of initiatives that could benefit parties beyond the GFCE membership. The GFCE is open to new members. Countries, intergovernmental organizations and private companies are eligible for full GFCE membership. (Membership is done at the national level, therefore government agencies or departments cannot become members on their own accord). If an organization/country would like to submit a request for membership, it is necessary to officially endorse The Hague Declaration on the GFCE and the Framework Document. For additional information

on membership, contact the GFCE Secretariat at: contact@thegfce.com. For additional information on the GFCE and different initiatives check out the GFCE website at http://www.theGFCE.com.

What are the GFCE initiatives?

Since the launch of the GFCE in 2015, GFCE members and partners have actively developed a number of cybersecurity and cybercrime initiatives in different regions of the world. At the annual GFCE meetings members and partners disseminate the results, lessons learned and best practices of an Initiative amongst GFCE members. New initiatives can be submitted to the GFCE Secretariat at any time.

Below is a listing of the current GFCE initiatives and their members. Additional details can be found on the GFCE website (http://www.thegfce.com/initiatives). Participation for each initiative is open to all GFCE members.

a. **Promoting Cybersecurity Due Diligence across Africa:** This U.S. and African Union Commission initiative, in partnership with the Economic Community of West African States (ECOWAS), the Southern African Development Community (SADC), the East African Community (EAC), the Economic Community of Central African States (ECCAS), the Common Market for Eastern and Southern Africa (COMESA), helps African Member States draft national cybersecurity frameworks for national and international engagements on cyber policy. These efforts include creating a culture of cybersecurity, developing national cyber strategies, enacting and enforcing comprehensive legal frameworks related to cybersecurity and cybercrime, and building organizational structures to improve cyber incident management capabilities on the continent. **GFCE Members include: The United States and the African Union.**

b. **A Global Campaign to Raise Cybersecurity Awareness:** Through this initiative, the United States, in partnership partnerships with Canada and the OAS, aims to raise awareness of cyber-related threats and best practices worldwide and empower citizens with the knowledge and a sense of shared responsibility to practice safe and informed behaviours on the Internet. By leveraging expertise from international partners in the government, academic, non-profit and private sectors, this cybersecurity awareness campaign initiative will work broadly with stakeholders to ensure a safer and more secure Internet for all. A primary resource for this initiative is the U.S. Department of Homeland Security Stop.Think.Connect.™ Cyber Awareness Campaign. **GFCE Members include: The United States, Canada and the OAS.**

c. **Preventing and Combating Cybercrime in Southeast Asia:** This initiative builds on cybercrime programs the United Nations Office on Drugs and Crime (UNODC) delivered in East Africa and Central America with a focus on a new region- Southeast Asia. The U.S., Japan, and Australia, in partnership with the UNODC will develop and execute basic cybercrime training for prosecutors and investigators from the region, conduct assessments of current cybercrime response capabilities, and train judicial staff on cybercrime related issues. **GFCE Members and Partners include: The United States, Australia, Japan, and the United Nations Office on Drugs and Crime (UNODC).**

d. **Cybersecurity Trends in Africa:** The United States Government and the AUC have partnered with Symantec (along with participation the Council of Europe and the Organization of American States) in this initiative is to develop a report that collects and presents detailed technical data on cybersecurity threats and trends in Africa. The Report will serve as a comprehensive document on cybersecurity matters in Africa, from which Member States of the African Union, and stakeholders worldwide, can draw useful conclusions and gain a fuller understanding of the major cyber trends in Africa, as well as the current capacity to deal with those threats. **GFCE Members include: The United States, the African Union, and Symantec.**

e. **Cybersecurity Initiative in OAS Member States:** This initiative recognizes the importance of having a comprehensive approach to addressing cybersecurity issues and aims to support countries in developing an effective response to cyber threats through an integrated approach. The activity areas are amongst others: national cyber security strategy development; cyber

security trainings and workshops; development of an OAS Hemispheric Network; cybersecurity exercises; cyber security and e-government for effective public management; and identification and adoption of technical standards for a secure internet architecture. **GFCE Member participants: The OAS, Argentina, Chile, Estonia, Mexico, Spain.**

f. **Assessing and Developing Cybersecurity Capability:** This Initiative is based on the Model developed by the Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford, with the support of international experts and partners. It aims to assist countries in understanding their priorities for investment and development by outlining the key elements necessary to respond to cyber incidents using five dimensions. The UK Government has provided funding to the GCSCC to develop a Capability Maturity Model to provide a framework for benchmarking progress. International Organizations such as the OAS, has seen value in the expertise that the GCSCC can provide, and have created formal frameworks and agreements of collaboration in this regard. The Governments of the UK and Norway are now keen to promote the GCSCC, and its tools to be utilized more widely. **GFCE Members and Partners include: The United Kingdom, OAS, Norway, and the Global Cyber Security Capacity Centre (GCSCC).**

g. **Critical Information Infrastructure Protection Initiative:** This initiative aims to support policy makers with responsibility for Critical Information Infrastructure Protection (CIIP) to understand the implications and consequences of cybersecurity issues and to maintain an awareness of current developments. By working together in a global initiative the initiators leverage their CIIP expertise for the benefit of a broader audience to help develop CIIP capabilities, particularly in developing countries. This initiative is run by the Meridian Community, a large group of countries organizing CIIP related International Conferences since 2005**. GFCE Members and Partners include: The Meridian Community, Spain, Switzerland, Norway, and the Netherlands.**

h. **CSIRT Maturity Initiative:** The goal of this initiative is to provide a platform for GFCE members to help emerging and existing CSIRTs to increase their maturity level. Through this initiative experts provide emerging and existing CSIRTs tools and instruments including best practices, guidelines, template documents that when applied, will improve cyber security CSIRT maturity. **GFCE Members include: The Netherlands, ITU, OAS, and Microsoft.**

i. **Coordinated Vulnerability Disclosure:** This initiative provides a platform to GFCE members to share experiences and lessons learned in cyber security mechanisms for responsible disclosure or coordinated vulnerability disclosure policies and discussions on the broader topic of ethical hacking. **GFCE Members include: The Netherlands, Hungary, Romania and Hewlett Packard.**

j. **Internet Infrastructure Initiative:** The aim of this initiative is to help build a robust, transparent and resilient internet infrastructure. Following the experience in the Netherlands in testing and monitoring compliance with international internet standards, this Initiative seeks to broaden this know-how. Key elements include national internet infrastructure, internet exchange points, country domain registries, open source software and routing security. **GFCE Members and Partners include: The Netherlands, Poland, Public/Private Platform Internet Standards - The Netherlands, the Kosciuszko Institute, the Netherlands Institute of International Relations 'Clingendael'.**

k. **Progressing Cybersecurity in Senegal and West Africa**: Senegal and the Netherlands have teamed up to exchange practical steps and expertise to address cybersecurity issues in Senegal and the broader West African region. A secure digital environment will permit the region to fully take advantage of the opportunities for growth that technology offers. **GFCE Members and Partners include: The Netherlands, Senegal, and the United Nations Office on Drugs and Crime (UNODC).**

l. **CyberGreen:** The initiative supports CSIRTs worldwide with metrics to measure the health of cyber eco systems. There is a need for a common understanding of cyber health and risks through a widely accepted way of measuring national, service provider, and enterprise cyber health and risks. A common understanding and insight will enable global policy development and capacity building. CyberGreen is different from other assessments because rather than study

the vulnerabilities of a system it quantifies the threat an unsecure system poses to others. **GFCE Members include: The United Kingdom and Japan.**

Annex 1 to contribution 2/332

The Hague Declaration at the GFCE

1. Today, we, governments, intergovernmental organisations and private companies, meet to launch the Global Forum on Cyber Expertise. We recognise and welcome that societies are becoming increasingly digitized, interconnected and dependent on the cyber domain for communication, innovation and sustainable social development and economic growth. We acknowledge that this creates opportunities that should be accessible for every individual worldwide.

2. To fully reap the benefits of information and communication technology, further investments are needed to ensure a free, open and secure cyberspace. As a consequence, inclusive and greater collaboration in the area of capacity building and exchange of expertise within the cyber domain is rapidly becoming one of the most important topics on the international cyber agenda, as was also noted in the 2013 Seoul Framework for and Commitment to Open and Secure Cyberspace.

3. As societies need to rapidly develop their capacity to take full advantage of cyberspace and need to overcome evolving challenges presented in this field, we all face financial and human resource constraints. We need to find better and smarter ways to work together by fostering existing and building new partnerships, establishing best practices and providing assistance to one another.

4. We stand committed to strengthening this cooperation on cyber by creating more opportunities for governments, the private sector, civil society, the technical community and academia from various regions of the world to engage and develop innovative solutions to this truly global challenge. We recognise the growing number of players in the field with relevant cyber experience and expertise, and we seek to make best use of these assets through closer cooperation.

5. We emphasise the need to strengthen and reinforce the existing framework of international cooperation and build new partnerships, enhance institutional capacity where it is most needed. We seek to develop a mutually reinforcing relationship with relevant multilateral institutions and develop practitioner networks that will have an enduring impact on global cyber capacity.

6. As a concrete sign of our unified and firm commitment to strengthen cyber capacity and expertise and to make the existing international cooperative efforts in this field more effective, we hereby establish the Global Forum on Cyber Expertise (hereinafter: GFCE).

Objectives

7. The GFCE will create a pragmatic, action-oriented and flexible forum. It will be consistent with, complement and reinforce existing bilateral, multilateral, multi-party, regional and international efforts to build cyber capacity and expertise and avoid duplication and overlap. The efforts undertaken within the framework of the GFCE will be consistent with international law, in particular the Charter of the United Nations, and respect the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and the UN Guiding Principles on Business and Human Rights, where appropriate.

8. The GFCE's overarching and long term goal is to strengthen cyber capacity and expertise globally.

9. To this end, the GFCE's primary objective is to provide a dedicated, informal platform for policymakers, practitioners and experts from different countries and regions to facilitate:

a. Sharing experience, expertise, best practices and assessments on key regional and thematic cyber issues. The initial focus areas for capacity and expertise building are cyber security, cybercrime, data protection and e-governance;

b. Identifying gaps in global cyber capacity and develop innovative solutions to challenges;

c. Contributing to existing efforts and mobilise additional resources and expertise to build global cyber capacity in partnership with and according to the particular needs of interested countries, upon their request.

10. Acknowledging that our participation in the GFCE is voluntary and not a legally binding commitment, we have established a framework document that will allow the GFCE to operate in a flexible, transparent and inclusive manner.

11. We plan to hold a high level meeting every year, in which we will discuss the achievements within the GFCE, including Initiatives taken, share experiences and lessons learned, and decide upon the way forward, preferably within the margins of the Global Conferences on Cyberspace. Nonmembers are welcome to take part in the discussions during these meetings. Civil society, the technical community and academia will be encouraged to participate and contribute to these discussions.

12. A small administrative unit will provide secretarial, communications and logistical support, and will prepare, in coordination with future hosts of the Global Conferences on Cyberspace, the annual high level meeting. This secretariat will initially be hosted and financed by the Netherlands.

Annex 2 to contribution 2/332

Launch of the Global Forum on Cyber Expertise

16 April 2015

Framework Document

Purpose

1. This Framework Document outlines the structure and operation of the Global Forum on Cyber Expertise (hereinafter: "GFCE"). It reflects the shared understanding of its members that the GFCE should be structured in a way that is voluntary, complementary, inclusive and resource driven. Activities are focused on identifying and addressing key geographic and thematic cyber issues.

2. Furthermore, it ensures the GFCE will remain a flexible, action-oriented and consultative forum that can evolve to meet contemporary challenges in cyberspace. It will complement the efforts already being undertaken in the field of cyber capacity and expertise building on a bilateral, multilateral, multi-party, regional and international level and avoid duplication and overlap. The GFCE seeks to develop a mutually reinforcing relationship with relevant multilateral institutions. This Framework Document should be seen in junction with The Hague Declaration on the GFCE, which outlines the objectives and values upon which the GFCE is based.

Members

3. Participation in the GFCE is voluntary. The GFCE is an informal forum, with no authority to take legally binding decisions. Neither this Framework Document nor participation in the GFCE more generally imposes any legal obligations on members.

4. The GFCE is founded by an initial group of countries, companies and intergovernmental organisations that are willing to actively contribute to the GFCE.

5. The GFCE aims to be a platform for the development of initiatives that could benefit parties beyond the GFCE membership. The GFCE is open to new members, provided they subscribe to The Hague Declaration on the GFCE, accompanying the official launch of the Global Forum on Cyber Expertise. GFCE members will be consulted on requests for membership.

Structure and functions

6. The structure and operations of the GFCE are based on four components:

I. An inventory of current efforts undertaken in the field of cyber capacity and expertise building;

II. An umbrella framework for the promotion of new initiatives, as well as enhancing and expanding existing ones;

III. A platform for high level discussions;

IV. An Administrative Unit.

Inventory of current efforts of cyber capacity building

7. Through the GFCE an inventory of current efforts in the field of cyber capacity building will be made available and kept up to date. This overview will allow GFCE members to identify and fill gaps in existing bilateral, multilateral, multi-party, regional and international capacity building activities and coordinate their efforts and contribute to bridging the digital divide.

Umbrella framework for initiatives

8. GFCE-members take new concrete initiatives or enhance and expand existing ones to strengthen capacity in cyber, through sharing experiences and best practices or other in-kind assistance, funding for capacity building projects, or a combination thereof (hereinafter: "Initiatives"). The Initiatives focus on a specific cyber area where there is a need for assistance or sharing of expertise and taken under the umbrella of the GFCE by two or more GFCE members (hereinafter: "Initiators"). The Initiators formulate the needs and assistance that a particular Initiative will contain. In addition to government entities, intergovernmental organisations or companies offering their own expertise, civil society, think tanks, academia, and in some instances international organisations, that possess expertise in certain cyber areas, could also play a role in an Initiative when invited to do so by the initiators.

9. New Initiatives can have a geographic or thematic focus, or can have both. The preliminary focus areas identified for capacity and expertise building within the GFCE are:

- Cybersecurity;
- Cybercrime;
- Data protection;
- E-Governance.

10. The focus areas will be evaluated on a yearly basis and may be amended by consensus of the members of the GFCE.

11. The setting up of an Initiative within the GFCE will generally consist of the following four phases. These phases should be seen as guidelines.

Phase one: Set-up

12. The Initiators take the lead in setting up an Initiative. Of these Initiators, at least one party has knowledge and/or expertise in one of the above-mentioned cyber areas, while at least one other party has a specific need for building up capacity in that particular field. Civil society may contribute by making suggestions for new initiatives.

Phase two: Identification

13. These Initiators formulate the specific assistance that is needed in the Initiative, and the means and ways of conveying the assistance or sharing the experience (so-called terms of reference). The assistance can be in the form of financial donations and/or in-kind expertise, for example sending experts to give trainings, or by sharing reports, best practices and lessons learned. Formulating the needs can either be done by the Initiators bilaterally or in a multi-party and multi-stakeholder setting (i.e. a regional or thematic seminar). Civil society, the technical community, think tanks and academia can also be involved in the formulation of specific assistance at the discretion of the Initiators.

Phase three: Recruitment

14. The Initiators recruit participants for the Initiative amongst GFCE members. This gives other members of the GFCE the opportunity to either contribute to the Initiative (with financial means or with in-kind expertise) or to indicate that they need the same assistance in building capacity. The setting up and the coordination of the Initiative remains the responsibility of the original Initiators.

Phase four: Implementation

15. When a clear need for capacity building has been established and adequate (financial or in-kind) resources have been found, coordinated by the Initiators, the Initiative will start its implementation phase. It is at the discretion of the Initiators to involve civil society, think tanks and academia, or use expertise within regional organisations, as implementing partners within an Initiative. Non-GFCE members could benefit from the results of specific Initiatives taken by GFCE members by associating themselves with these initiatives.

16. The Initiators will disseminate the results, lessons learned and best practices of an Initiative amongst GFCE members upon its completion to maximize the effectiveness of other Initiatives.

Platform for high level discussion

17. An annual high level meeting amongst members of the GFCE to evaluate progress made will take place, preferably in the margins of future Global Conferences on Cyberspace. The dialogue will provide the opportunity to discuss and (re)formulate requirements as well as best practices on cyber capacity building in the focus areas. The development of best practices will promote a continuous policy discussion about ways and means to respond to emerging challenges in the cyber domain, while preserving each member's-internal decision making processes on implementation of specific measures. Civil society, the technical community, think tanks and academia will also be encouraged to be involved in the discussion, contributing to the development of best practices and advising on the formulation of requirements.

Administrative unit

18. The Administrative Unit will, inter alia, provide the necessary administrative and logistical support to GFCE members. It will maintain an overview of ongoing Initiatives and circulate the results of Initiatives among the GFCE members. It will facilitate and manage the sharing of information by GFCE members and, as appropriate, other relevant stakeholders of their relevant national practices and programmes, documents, and information regarding Initiatives taken under the umbrella of the GFCE.

19. The Unit will support and assist with logistical planning for the annual high level policy meeting, preferably to be held in the margins of future Global Conferences on Cyberspace. It will, inter alia, assist in the production of an overview of results of the GFCE and its initiatives to present to the GFCE members.

20. The Netherlands will initially host and finance the Unit for a period of four years after the launch of the GFCE. Consistent with the informal format of the GFCE, there will be no assessed

contributions from GFCE members to finance this Unit. The Unit is expected to include four persons and will seek to include, where possible, individuals from other GFCE members. 21. At the first annual high level policy meeting on cyber capacity and expertise building, preferably in the margins of the next Global Conference on Cyberspace, the structure and operation of the Unit will be assessed and reviewed. The most appropriate structure, operation, financing, and location of the Unit over the longer term will be seen in conjunction with the development of the GFCE and its long term requirements.

Annex 3: Cybersecurity activities being conducted by organizations, private sector, and civil society

Details about cybersecurity workshops that have been conducted in conjunction with the ITU-D Study Group 2 Question 3/2 meetings.

ITU Cybersecurity Workshop: Global Cybersecurity Challenges

Collaborating for effective enhancement of cybersecurity in developing countries

8 September 2015, 14:30-17:30, ITU Tower, Popov Room

http://www.itu.int/en/ITU-D/Study-Groups/2014-2018/Pages/side-events/2015/cybersecurity-workshop.aspx.

Agenda

14:30-14:40	**Welcome remarks** Mr Brahima Sanou (BDT Director) and Mr Chaesub Lee (TSB Director)

14:40-15:40	**Session 1 (Panel discussion)**
	Best practices for a multi-layered strategic approach to effective cybersecurity enhancement in developing countries Data breaches are reported to be on the rise globally. Increasingly, with wearable technology, Internet of Things and embedded Information and Communication Technologies (ICTs) everywhere, cyber incidents will have greater effects in the physical world. It is no longer just about money and data – however important these are –, now it is also about lives. Cybersecurity is an essential component of human activity. Its high level of complexity requires action at different levels (both virtual and physical) and by different actors (governments, private sector, civil society, intergovernmental organizations, etc.). • What are the key success factors to developing and implementing a national cybersecurity strategy? • What are the best practices? • What will be the future elements to be included in national cybersecurity strategies? Presentations: 1) **Japanese Government's Cybersecurity Strategy** Mr Kunihiro Tsutsui Ministry of Internal Affairs and Communications, Japan 2) **Public-Private partnerships and Cyber Risk Management** Mr Stephen Farole United States Department of Homeland Security, United States of America **Cyber Security: OCERT Prospective** Ms Aziza Al-Rashdi (Information Technology Authority, Sultanate of Oman) Moderator: Mr Mohamed M.K. Elhaj (Republic of the Sudan) Panelists: Mr Albert Kamga (Republic of Cameroon) Ms Aziza Al-Rashdi (Sultanate of Oman) Mr Jean-David Rodney (Republic of Haiti) Mr Kunihiro Tsutsui (Japan) Mr Stephen Farole (United States of America)

16:10-17:10	**Session 2 (Panel discussion)** **Challenges facing developing countries; international collaboration to promote cybersecurity initiatives** With the constant expansion of broadband to unconnected parts of the world, most of the growth in the adoption of ICTs is expected to come from developing countries in the years to come. Newly connected countries have the opportunity to leverage the potential of ICTs to generate wealth and boost their socio-economic development and to achieve this they need robust, reliable, and trustworthy systems that would create a solid foundation for their businesses to operate and evolve. • What are the three key challenges faced by developing countries in achieving an effective level of cybersecurity? • How can existing regional and international collaboration be enhanced to promote cybersecurity initiatives? • Are there innovative vehicles of collaboration that can be considered? Presentations; 1. **Mobile security issues** Mr Christopher Boyer, AT&T Inc. 2. **Challenges facing developing countries** Mr Damir Rajnovic, Forum for Incident Response and Security Teams (FIRST) **International collaboration to promote cybersecurity initiatives – Good practices in cybersecurity development based on findings of the Global Cybersecurity Index** Mr Tymoteusz Kurpeta, ABI Research Moderator: Mr Patrick Mwesigwa (Republic of Uganda) Panelists: Mr Arkadiy Kremer (ITU-T SG17) Mr Christopher Boyer (AT&T Inc.) Mr Damir Rajnovic (FIRST) Mr Damnam Kanlanfei Bagolibe (Togolese Republic) Mr Tymoteusz Kurpeta (ABI research)
17:10-17:20	**Workshop wrap up** Ms Miho Naganuma (NEC Corporation)
17:20-17:30	**Closing remarks** Mr Ahmad Sharafat (ITU-D SG2 Chairman) and Mr Arkadiy Kremer (ITU-T SG17 Chairman)
18:00-20:00	**Welcome reception**

Note:

– Workshop moderator: Ms Miho Naganuma (NEC Corporation)

– Interpretation in the six official UN languages is provided.

ITU Cybersecurity Workshop

Day 1: Monday, 18 April 2016, 14:30- 17:30

Day 2: Tuesday, 19 April 2016, 09:30-12:30

ITU Montbrillant building, Room H

http://www.itu.int/en/ITU-D/Study-Groups/2014-2018/Pages/side-events/2016/cybersecurity-workshop.aspx

Agenda

DAY 1: National Cyberdrills

Timing	Presentations
14:30-14:40	**Welcoming remarks by ITU/BDT official**
14:40-15:50	**Enhancing National Cyberdrills through experience sharing** A national cyberdrill enhances the communication and incident response capabilities of all participants at the national level, thus helping ensure an efficient and coordinated effort in mitigating cyber threats and responding to major cyber incidents. A national cyberdrill is typically structured around a fictitious yet realistic geo-political scenario as the background for a set of simulated actions by threat actor(s) to which the participants must respond in accordance with their roles and responsibilities in a coordinated and timely fashion. This panel will highlight recent experiences in conducting such national cyberdrills. Presentations (10 minutes each): **1) General overview by Mr Luc Dandurand, Head of ICT Applications and Cybersecurity Division, ITU/BDT** **2) Pan European Cyber Exercises by Dr Panagiotis Trimintzios, Programme Manager, European Union Agency for Network and Information Security (ENISA)** **3) A detailed view into a real case by Mr Michael Bartsch, Cybersecurity Management Consulting & Training, Deutor** **4) Korea's National Cyberdrill Experience by Mr Jaesuk Yun, Senior Researcher, Korea Internet & Security Agency** **5) Malaysia's National Cyberdrill Experience by Dr Amirudin Bin Abdul Wahab, Chief Executive Officer, Cybersecurity Malaysia** **6) Cyber Storm V Overview by Mr Tim McCabe, Deputy NCEPP, NCCIC, US Department of Homeland Security** 7) **Practice makes Perfect by Mr Erka Koivunen, Cybersecurity Advisor, F-Secure**
15:50-16:10	**Coffee break**
16:10-17:10	**Panel Discussion after presentations** Following the previous sharing of experiences, lessons learned for the efficient and effective planning and conduct of national cyberdrills will be discussed in the context of ITU/BDT's activities to support Member States in conducting such exercises. Moderator: **Mr Luc Dandurand, Head of ICT Applications and Cybersecurity Division, ITU/BDT** Panelists: **All speakers from the first half of the session**
17:10-17:30	**Workshop wrap up** **by Mr Luc Dandurand, Head ICT Applications and Cybersecurity Division, ITU/BDT**
	End of Day 1 of Workshop

DAY 2: National Cybersecurity Strategies

Timing	Presentations
09:30-10:40	**Session 1: The key ingredients for preparing a comprehensive National Cybersecurity Strategy** Some nations have vested responsibility for cyber security in existing or new agencies and have established national Computer Emergency Response Teams (CERTs). Some nations have begun rolling-out cyber-security awareness campaigns and developed action plans on Critical infrastructure protection Whilst these are vital tactical actions towards improving national cybersecurity, to manage risks associated with the digital assets of a nation, a strategy is needed to combine all efforts into a coherent, comprehensive and sustainable nation-wide approach. In this session, panellists will share their expertise on how to develop a National Cybersecurity Strategy Presentations (10 minutes each): **1) NCS cybersecurity partnership by Mr Luc Dandurand, Head of ICT Applications and Cybersecurity Division, ITU/BDT** **2) ENISA's work on strategies by Ms Dimitra Liveri, European Union Agency for Network and Information Security (ENISA)** **3) Trust frameworks by Dr Bilel Jamoussi, Chief, Study Groups Department, ITU/TSB** **4) How Switzerland deals with cyber threats by Dr. Stefanie Frey, MELANI, Switzerland** Moderator: **Mr Eliot Lear, Co-Rapporteur, ITU-D SG2 Q3/2** Panelists: **All speakers from the session**
11:10-12:10	**Session 2: Effective implementation of a National Cybersecurity Strategy** A strategy is of use only when it is aptly translated into an actionable plan which is reviewed and adjusted in line with temporal and situational changes. This process aspect of strategy implementation must be done effectively so that a nation can close the cybersecurity gap identified for remediation in its national cybersecurity strategy. The possible ways to measure this effectiveness and assess progress need to be highlighted and understood. Presentations (10 minutes each): **1) Estonia's experience by Mr Raul Rikk, Head of National Cyber Security Domain, e-Governance Academy, Estonia** **2) Paradigm Change as Part of a Cybersecurity Strategy by Mr Ammar Alkassar, CEO, Rohde & Schwarz Cybersecurity** **3) How to create the National Cyber Security Strategy by Dr Martti Lehto, University of Jyväskylä, Finland** **4) Research conducted in Cybersecurity Strategies by Mr Erik Silfversten, Analyst, Rand Europe** Moderator: Mr Luc Dandurand, Head of ICT Applications and Cybersecurity Division, ITU/BDT Panelists: All speakers from the session
12:10-12:20	**Workshop wrap up** **by Mr Luc Dandurand, Head of ICT Applications and Cybersecurity Division, ITU/BDT**
12:20-12:30	**Closing remarks** **by Mr Ahmad Sharafat, ITU-D Study Group 2 Chairman**

Timing	Presentations
	End of workshop

ITU Cybersecurity Workshop :

Cybersecurity and Risk Assessments in Practice

Thursday, 26 January 2017, 14:30- 17:30

https://www.itu.int/en/ITU-D/Study-Groups/2014-2018/Pages/side-events/2017/cybersecurity-workshop.aspx.

1. Introduction

In many ways, cybersecurity is about risk management. A key element of risk management is the assessment of risk. For the cyber domain, and despite much scientific and technical work in this area, assessing risks remains an art, particularly at the highest levels. This is due to the very complex nature of cyberspace, the difficulty in assessing vulnerabilities in very large "systems" composed of continually-evolving technology and human processes, the difficulty in assessing the value of digital assets and reputation, and the dynamic nature of cyber threats.

2. Objective of the workshop

This workshop will bring together world experts who will share their knowledge and experience on the practical assessment of cyber risks at the national level, in very large organizations, and in critical infrastructure sectors. The workshop will also discuss supply chain risks and role of standards for managing cyber risks in organizations.

3. Agenda

Time	Description
14:30-14:40	Opening by Workshop Chair, Ms. Miho Naganuma Welcoming remarks by ITU/BDT official
14:40-15:45	Presentations by invited speakers (20 min each) 1) Top cyber security threats in 2017 and beyond Dr. Bader Al Manthari (Information Technology Authority (ITA), Sultanate of Oman) 2) Methodologies and tools used in the private sector to assess cyber risks in large organizations Mr. Ryan Spanier (Kudelski Security) 3) Cyber risk assessments in critical infrastructure sectors Dr. Stefanie Frey (MELANI)
15:45-16:15	Break
16:15-17:00	Presentation by invited speakers 1) Supply Chain Risks Mr. Andy Purdy (Huawei Technologies) and Ms. Kaja Ciglic (Microsoft) 2) Role of standards and ISO/IEC 27000 series update Ms. Miho Naganuma (NEC Corporation)
17:00-17:20	Q&A from the audiences and discussion by moderator , Ms. Miho Naganuma

Time	Description
17:20-17:30	Workshop wrap- up by Workshop chair, Ms. Miho Naganuma

Organization: Internet Society (ISOC)

Document: SG2RGQ/162 + Annex

Title: Collaborative security

Summary: During the April 2016 Rapporteur Group meeting, Ms Christine Runnegar from the Internet Society made a presentation to the group on Collaborative security. This presentation provided an overview of the Internet Society as well as explained the Internet Society's Collaborative Security Approach.

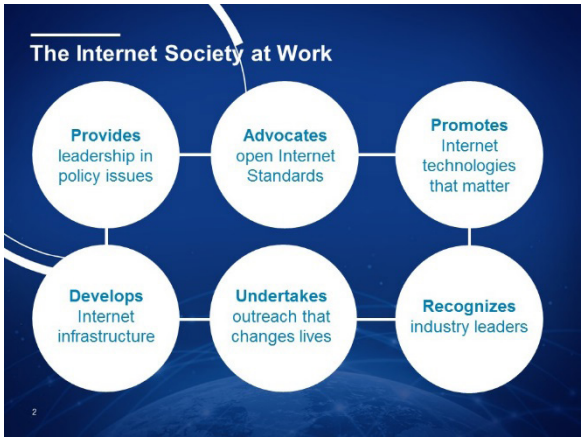
People are what ultimately hold the Internet together. The Internet's development has been based on voluntary cooperation and collaboration. Cooperation and collaboration remain the essential factors for the Internet's prosperity and potential.

This contribution contains a presentation introducing the Internet Society's Collaborative Security approach, which is characterized by five key elements:

- Fostering confidence and protecting opportunities: The objective of security is to foster confidence in the Internet and to ensure the continued success of the Internet as a driver for economic and social innovation.
- Collective Responsibility: Internet participants share a responsibility towards the system as a whole.
- Fundamental Properties and Values: Security solutions should be compatible with fundamental human rights and preserve the fundamental properties of the Internet — the Internet Invariants.
- Evolution and Consensus: Effective security relies on agile evolutionary steps based on the expertise of a broad set of stakeholders.
- Think Globally, act Locally: It is through voluntary bottom-up self-organization that the most impactful solutions are likely to reached.

and discusses the principles in the context of botnets. It also contains some information regarding some of the Internet Society's activities with the community to address spam.


Our Mission
To promote the open development, evolution, and use of the Internet for the benefit of all people throughout the world.
1


The Internet Society at Work
Provides leadership in policy issues
Advocates open Internet Standards
Promotes Internet technologies that matter
Develops Internet infrastructure
Undertakes outreach that changes lives
Recognizes industry leaders
2


The Internet security landscape
www.internetsociety.org
Internet Society

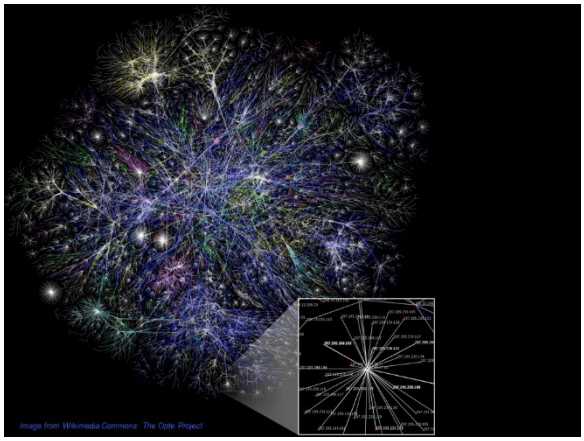


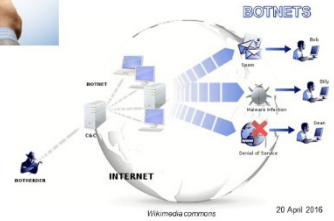
Image from Wikimedia Commons: The Opte Project

SPAM

RANSOMWARE

Wikimedia commons

BOTNETS



DDOS ATTACKS

PHISHING

MALWARE

5 The Internet Society Wikimedia commons 20 April 2016

The complexity of the security landscape

Open platform
⇒ also open for attack and intrusion

Permission-free innovation
⇒ also allows development and deployment of malware

Global reach
⇒ attacks and cybercrime can be cross-border

Voluntary collaboration
⇒ can be hard to assign responsibility and prescribe solutions

6 The Internet Society 20 April 2016

Why do we care about "security"?

We want to be "secure" and feel "secure" …

BUT …

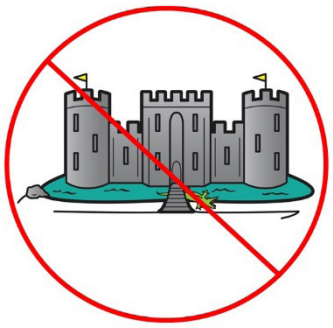
policy measures that are premised on stopping bad things, rather than protecting what is valued, provide no guide as to how far those measures should go

AND …

if we are not careful, the spectre of cyber threats can be used as a vehicle for control of networks and how they are used, plus pervasive monitoring

7 The Internet Society 20 April 2016

Throw out preconceptions



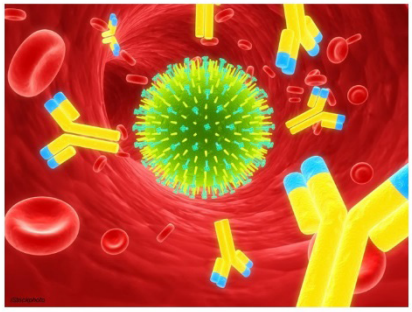
8 The Internet Society 20 April 2016

Understanding security

- ❑Security is not an end in itself
- ❑There is no such thing as absolute security: there will always be threats
- ❑We need to think about "secure" in terms of residual risks that are considered acceptable in a specific context.
- ❑There are "inward" and "outward" risks
- ❑Risks may require more than one actor to manage
- ❑Resilience is key

9 The Internet Society 20 April 2016

Resilience



10 The Internet Society 20 April 2016

Internet Society Collaborative Security approach

www.internetsociety.org

provides a framework for tackling Internet security issues

Example: botnets

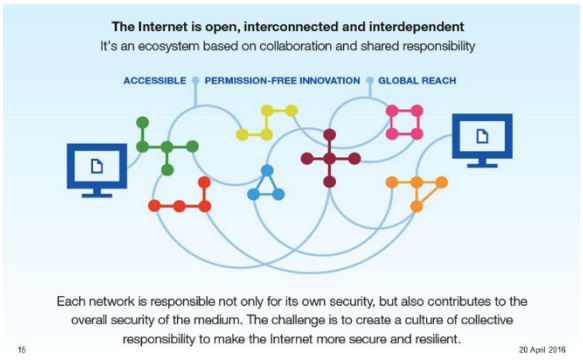
image from Wikimedia Commons

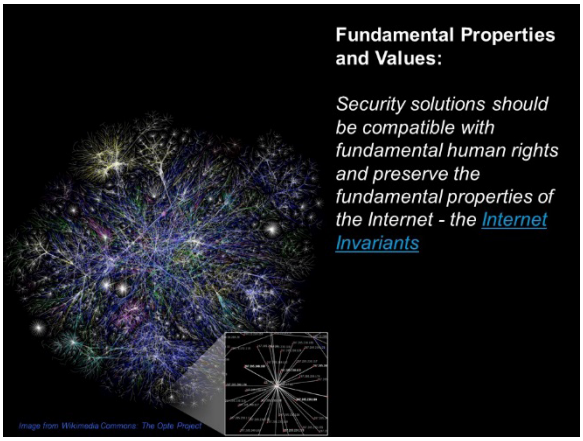
Fostering confidence and protecting opportunities:

The objective of security is to foster confidence in the Internet and to ensure the continued success of the Internet as a driver for economic and social innovation.

14 The Internet Society 20 April 2016

Collective Responsibility: *Internet participants share a responsibility towards the system as a whole*





Evolution and Consensus: *Effective security relies on agile evolutionary steps based on the expertise of a broad set of stakeholders.*

17 The Internet Society 20 April 2016

iStockphoto

Think Globally, Act Locally:

It is through voluntary bottom-up self-organization that the most impactful solutions are likely to be reached.

18 The Internet Society 20 April 2016

iStockphoto

Helping the community combat spam

www.internetsociety.org

Internet Society

Working together to address spam

ITU-D and ISOC letter of agreement to help ITU member states, especially from developing countries

Mark your calendar! 6 May 2016 - WSIS Forum workshop

Spam: understanding and mitigating the challenges faced by emerging Internet economies – organized by the ITU and ISOC

We have policy briefs on spam and botnets
http://www.internetsociety.org/policybriefs

Our anti-spam toolkit has had a "make-over" ***http://www.internetsociety.org/spamtoolkit***

The combatting spam online tutorial is available in EN and ES
https://www.internetsociety.org/tutorials/combating-spam

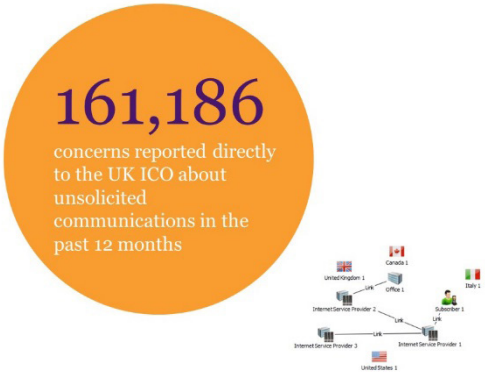
Partnering with LAP, M³AAWG and other champions against spam

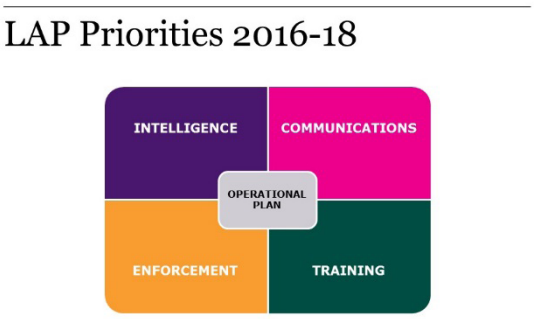
20 The Internet Society 20 April 2016

Organization: London Action Plan (LAP)

Title: Introduction to the London Action Plan

Summary: During the April 2016 Rapporteur Group meeting, Mr Adam Stevens from the London Action Plan (www.londonactionplan.org) made a presentation to the group.





Organization: Nuix Technology UK (United Kingdom of Great Britain and Northern Ireland)

Title: A cybersecurity framework for all

Document: SG2RGQ/35

Summary: Across all fields and international boundaries cybercrime and cybersecurity requirements have never been greater or more complex. There is too much data, too much noise in the data, and no good way to pull together all of the different data sources to give analysts a contextual 360-degree view spanning digital, physical and human intelligence. A combination of technology and people provides us an unparalleled opportunity to address the emerging problem that is cybercrime. By harnessing advanced technology, scalability, and deep experience in data forensics and investigation we are in a unique position to change the way we tackle cybersecurity incidents.

This document puts in place a cybersecurity framework suitable for any ITU member state, which by design can dramatically reduce the gap between incident detection and remediation, and provide deep and rapid insights into the scope of a breach, the information that has been compromised and the path to resolution. Across all fields and international boundaries cybercrime and cybersecurity requirements have never been greater or more complex. There is too much data, too much noise in the data, and no good way to pull together all of the different data sources to give analysts a contextual 360-degree view spanning digital, physical and human intelligence. A combination of technology and people provides us an unparalleled opportunity to address the emerging problem that is cybercrime. By harnessing advanced technology, scalability, and deep experience in data forensics and investigation we are in a unique position to change the way we tackle cybersecurity incidents.

Introduction

Issues of building confidence and security in the use of ICT in the CIS region are in charge of the Information Security Commission of the Regional Commonwealth in the fields of Communications (RCC). Acknowledging that the relevance and ensuring technological independence and information security of the state are the strategic objective, the heads of the CIS states in October 2008 approved the Concept of cooperation of the States- participants of the CIS in the sphere of information security and a Comprehensive action plan for its implementation. Enactment of these documents promoted further forming and enhancement of the legal basis for an interstate cooperation in this sphere and the establishment of a secure information environment in the CIS.

Information Security Commission has prepared a draft Agreement on cooperation of states - participants of the CIS in the field of information security and the Regulation on the basic organization of CIS member states, which provide methodological, organizational and technical support for the work in the field of information security and the training of specialists in this field.

At the same time there was an inquiry of administrations, regulators and the CIS region's business to determine common requirements for training of specialists in information security. They should take the form of requirements for appropriate educational standards and are embodied in these standards. According of such factors as historical community of the educational systems of the CIS countries and their current compliance with the terms of the Bologna agreement, allows a large extent unify and make regional standards of training, including such specialties as "Information Security Specialist of Information and Communication Systems" "The system administrator of information and communication systems"; "Specialist in Administration of network devices of information and communication systems"; "The system programmer"; "Specialist in design and graphic user interfaces"; "Technical support specialist of information and communication systems." The corresponding functional cards of labor activity types, the characteristics of the generalized labor functions, necessary knowledge and skills form a basis for training of specialists, in one way or another responsible for building confidence and security in the region.

Competence-based approach in educational activity and its interface to inquiries of employers

The modern needs of the labor market for specialists of a certain qualification are increasingly placed at the forefront in reforming the educational systems of countries in various regions. These requirements directly affect the modular structure and the flexibility of education in the 48 countries that joined the Bologna Declaration (1999). This process is active in the CIS region. In different countries the professional ICT community formulates its requests in the form of the direct order both to system of professional training, and subsystems of retraining and advanced training. This social order is a list of specific competencies that form the ability to apply knowledge, skills and personal qualities to be successful in a particular field. Competencies and learning outcomes are seen as the main target setting in the implementation of vocational training programs as the integrating beginnings of a graduate's "model".

The competence-based model of the graduate, on the one hand, covers the qualification linking his future activities with the subjects and objects of labor, on the other hand, reflects the interdisciplinary requirements to the result of education.

As a result of discussions in the professional community, the features of key professional competencies have been formulated, they:

- Allow to solve complex tasks (non-algorithmic);
- Are multifunctional (allow to solve different problems from one field);
- Transferable to different social fields (different activities);
- Require complex mental organization (the inclusion of intellectual and emotional qualities);

– Are complicated to implement and require a set of skills (skills of cooperation, understanding, reasoning, planning...); and,

– Should be implemented on different levels (from elementary to profound).

Advantages of competence-based approach are in the fact that at the same time:

– The goals and objectives of training programs conforming to requirements of employers are formulated;

– Flexibility of training programs increases;

– Efficiency and quality of professional training, level of professional competences increases;

– Standard, objective and independent conditions of a training quality evaluation are created;

– Level of interaction and the mutual responsibility of students, teachers and employers increases;

– Preparation for professional activity is carried out taking into account the real production conditions, due to which accelerated adaptation of professionals in the workplace; and,

– Formed organizational culture, including the field of information security.

Competences of experts in information security as basis for creation of the corresponding human potential

Focusing on the labor market needs in the field of training and retraining in the application of ICT security experts, the required competences can be divided into several blocks:

1) The general professional competence of providing including the ability to:
   - Undertake the operation of infocommunication systems (ICS) with the use of methods and means to ensure their safety;
   - Administer software and hardware protection of information in the ICS;
   - Carry out the work on assessing the safety of ICS; and,
   - Build distributed protected ICS.
2) Competence in the ICS operation using software methods and tools for their safety, providing including the ability to:
   - Provide the information security (IS) in ICS with software and hardware;
   - Provide the information security (IS) in the ICS using technical means; and,
   - Provide information security (IS) in ICS with a complex application software, hardware and technical resources.
3) Competence in the field of management software and hardware protection of information in the ICS, including providing skill to:
   - Configure software and hardware ICS protection;
   - Perform maintenance regulations and current repair of software and hardware tools of information protection; and,
   - Carry out the analysis of the violations allowed by users in ICS and to hinder with their repetition.
4) Competence in the field of the assessment ICS security:
   - The monitoring of the efficiency and effectiveness of hardware-software means of information protection;

- The application of methods and techniques for ICS safety assessment under protection system control analysis;
- Carrying out experimental and research works in case of objects certification taking into account requirements to ensuring ICS protection;
- Instrumental monitoring of the ICS protection; and,
- Expertise in the investigation of security incidents.

5) Competences in the area of distributed protected ICS design:

- Development of requirements for distributed secure ICS and remedies for them, taking into account existing regulations and guidance documents;
- Design of the distributed protected ICS; and,
- Commissioning and maintenance of distributed ICS with the protection of information resources, organizational and technical measures for information security.

Each of these competencies is accompanied by a list of actions committed by labor and the necessary knowledge, abilities and skills.

Conclusion

Human capacity building to enhance confidence and security in the use of ICT is an urgent task, which requires the business partnership as the customer, the educational system as a contractor and the state as regulator of the entire process. Business priority in the formulation of requirements for specialists guarantees the success.

As a result of the project for the implementation of the Regional Initiative 5 in the CIS region has developed standard professional competencies, which are put at the forefront in the creation of educational programs in the field of training and retraining of information security specialists.

These competencies are complemented by a specific list of employment action, knowledge and skills that allows both carrying out examination of educational programs and creating new programs of training and retraining for building confidence and security in the use of ICT in the region. Dissemination of results in the region will be implemented within the framework of the ITU project “Centre of Excellence” in the CIS region in the area of “Cyber security”, which is a priority for the region and assigned to the main contractor of the Regional initiative 5 – Moscow Technical University of Communications and Informatics, a member of ITU-D.

The obtained results should be used to enhance the use of ICT awareness activities to build confidence and security in different countries, particularly developing countries, as they have a number of valuable qualities: relevance trends of infocommunications, compliance with modern educational trends and international standards of construction of educational process, scalability and reproducibility.

Annex 4: Contributions mapping

Reports

Web	Received	Source	Title
2/REP/35 (Rev.1)	2017-04-03	Rapporteurs for Question 3/2	Report of the Rapporteur Group meeting on Question 3/2 (Geneva, Thursday 6 April 2017, 14:30 - 17:30 hours)
RGQ/ REP/22	2017-01-18	Rapporteurs for Question 3/2	Report for the Rapporteur Group meeting on Question 3/2 (Geneva, Friday, 27 January 2017, 09:00 -12:00 and 14:30-17:30 hours)
2/REP/24 (Rev.1)	2016-09-26	Rapporteurs for Question 3/2	Report of the Rapporteur Group Meeting on Question 3/2 (Geneva, Thursday 29 September 2016, 14:30- 17:30 hours)
RGQ/ REP/12	2016-04-29	Rapporteurs for Question 3/2	Report of the Rapporteur Group meeting on Question 3/2 (Geneva, Friday, 29 April 2016, 09:30 -12:30 and 14:30- 17:30 hours)
2/REP/13 (Rev.1)	2015-09-09	Rapporteurs for Question 3/2	Report of the Rapporteur Group Meeting on Question 3/2 (Geneva, Wednesday 9 September 2015, 09:30- 12:30 hours)
RGQ/REP/3	2015-04-29	Rapporteurs for Question 3/2	Report of the Rapporteur Group Meeting on Question 3/2 (Geneva, Wednesday, 29 April 2015, 09:30 -12:30 and 14:30- 17:30 hours)
2/REP/3 (Rev.1)	2014-09-24	Rapporteurs for Question 3/2	Report of the Rapporteur Group Meeting on Question 3/2 (Geneva, Wednesday 24 September 2014, 09:30- 12:30 hours)

Question 3/2 contributions for Rapporteur Group and Study Group meetings

Web	Received	Source	Title	Mapping in final report
2/458	2017-03-21	Korea (Republic of)	Study topics for Question 3/2 for the next study period	
2/422	2017-02-17	Togolese Republic	Fraudulent SIM box card practices	
2/415 [OR]	2017-02-20	Rapporteurs for Q3/2	Final Report for Question 3/2	
2/402	2017-01-31	République démocratique du Congo	Securing information and communication networks: Good practice for developing a good culture of cybersecurity	
RGQ/242	2017-01-06	NEC Corporation	Updated Section 6 (Report of Cybersecurity workshops) of Q3/2 report	
RGQ/230	2016-12-08	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States	

Web	Received	Source	Title	Mapping in final report
RGQ/221	2016-11-28	Senegal (Republic of)	Overview of the Digital Senegal 2025 (***Sénégal Numérique 2025***) Strategy validated and adopted in 2016	
RGQ/213 [OR]	2016-11-25	Rapporteur for Question 3/2	Draft Final Report for Question 3/2	
RGQ/209	2016-11-24	Democratic Republic of the Congo	Context of ICT infrastructure security	
RGQ/207	2016-11-17	Democratic Republic of the Congo	Security of communication infrastructures	
RGQ/204	2016-11-14	Norway	Creating a metric for cyber security culture	
2/369	2016-09-13	Russian Federation	The experience of the CIS countries in the field of experts' professional competences formation on data protection and information security in information and communication systems	Section 4 + Compendium Annex 2
2/364	2016-09-13	United Kingdom of Great Britain and Northern Ireland	Common criteria as a tool for giving assurance about the security characteristics of IT products	Section 8
2/362	2016-09-13	Korea (Republic of)	Proposed text for inclusion in Chapter 6 (Child Online Protection) of the Final Report	Section 5
2/361	2016-09-13	Korea (Republic of)	Korea's Information Security Industry Promotion Plan	Currently Section 4.2 or section 7
2/342	2016-08-24	Oman Telecommunications Regulatory Authority (TRA)	Oman Public Key Infrastructure (PKI)	Section 7 and Compendium Annex 2
2/334	2016-08-12	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States	-
2/332	2016-08-12	United States of America, Netherlands (Kingdom of the)	The Global Forum on Cyber Expertise (GFCE)	Section 7 and Compendium Annex 2
2/322	2016-08-05	Odessa National Academy of Telecommunications n.a. A.S. Popov	A database with data on existing technical solutions for child online protection (http://www.Contentfiltering.info)	Section 5
2/317	2016-08-05	Côte d'Ivoire (Republic of)	Experience of Côte d'Ivoire in developing a national cybersecurity culture	Referenced in Section 4 and Compendium Annex 2

Web	Received	Source	Title	Mapping in final report
2/314	2016-08-05	Japan	ACTIVE(Advanced Cyber Threats response InitiatiVE) project in Japan	Section 3
2/295 [OR]	2016-08-12	Co-Rapporteurs for Question 3/2	Draft Report on Question 3/2	-
RGQ/145	2016-04-04	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States	-
RGQ/144	2016-04-04	Russian Federation	Proposals from the Russian Federation for modification of GCI Questionnaire	Referenced in Annex 1 and will be mentioned in section 9
RGQ/143	2016-04-04	Russian Federation	Cyberwellness Profile of the Russian Federation for the Global Cybersecurity Index (GCI) Report 2016	Referenced in Annex 1 and will be mentioned in section 9
RGQ	2016-04-04	Korea (Republic of)	Safe Use of the Internet for Children and Youth in Korea	Section 5
RGQ/141	2016-04-04	Korea (Republic of)	Fintech and security in Korea	Section 4 or section 7
RGQ/120	2016-03-16	Rapporteurs for Question 3/2	Initial Draft Report on Question 3/2	-
RGQ/104	2016-02-17	Gambia (Republic of the)	A case to adopt child online protection initiatives across LDCs	Section 5
2/234	2015-08-27	Korea (Republic of)	Korea's K-ICT Security Development Strategy	Compendium Annex 2 + in section 4 or7
2/228	2015-08-21	United Kingdom of Great Britain and Northern Ireland	Cybersecurity in government and industry	Section 4 Compendium Annex 2
2/203	2015-07-31	China (People's Republic of)	Proposal for a new work item on Framework of Detection, Tracking and Response of Mobile Botnets	Section 3
2/202 **(Rev.1)**	2015-07-29	Australia, Papua New Guinea, Samoa (Independent State of), United Kingdom of Great Britain and Northern Ireland, Vanuatu (Republic of)	Proposed questions on child online protection	Section 5
2/198	2015-07-26	United States of America	Partnering with the Private Sector to Manage Cyber Risk	Section 7 and Annex 2

Web	Received	Source	Title	Mapping in final report
2/175	2015-07-23	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States	-
2/174	2015-07-23	China (People's Republic of)	Best practices for developing a culture of cybersecurity: Promoting awareness of cybersecurity and enhancing its management	Section 4 and Annex 2
2/165	2015-07-22	BDT Focal Point for Question 3/2	Global Cybersecurity Index- Partnership Model	Mention in Section 1 or 2
2/164	2015-07-22	BDT Focal Point for Question 3/2	Global Cybersecurity Index- Reference Model	Mention in Section 1 or 2
2/163 +Ann.1	2015-07-22	Oman Telecommunications Regulatory Authority (TRA)	Survey on measures taken to raise awareness on cybersecurity/revised GCI questionnaire	Mention in Section 1 or 2
2/157	2015-07-04	ITU-T Study Group 15	Liaison Statement from ITU-T SG15 to ITU-D SGs on ITU-T SG15 OTNT standardization work plan	
2/156	2015-07-08	Odessa National Academy of Telecommunications n.a. A.S. Popov	Multimedia distance-learning course on the safe use of Internet resources	Section 4 and Annex 2
2/155 +Ann.1	2015-07-10	ABI Research (United States of America)	Cybersecurity Index of Indices	Mention in section 2 or Annex 1
2/154	2015-07-16	Gambia (Republic of the)	A case to adopt Child Online Protection initiatives across LDCs	Section 5
2/153	2015-07-08	Togolese Republic	Security of electronic transactions	Section 7 and Annex 2
RGQ/64	2015-04-13	Korea (Republic of)	Korea's Internet of things security roadmap	Annex 2 Compendium
RGQ/59	2015-04-09	Japan	Proposal for the security workshop to be held in September 2015	-
RGQ/56	2015-03-31	Australia, Samoa (Independent State of), United Kingdom of Great Britain and Northern Ireland, Vanuatu (Republic of)	Proposed questions on child online protection	Section 5
RGQ/47	2015-03-12	Iran (Islamic Republic of)	National cybersecurity measures	Section 4 or 7 Compendium Annex 2
RGQ/46 +Ann.1	2015-03-12	Iran (Islamic Republic of)	National cybersecurity measures and measurement	Section 4 or 7 Compendium Annex 2

Web	Received	Source	Title	Mapping in final report
RGQ/44	2015-03-12	Oman (Sultanate of)	Survey on measures taken to raise the awareness on cybersecurity	Section 2
RGQ/42	2015-03-12	United States of America	Best practices for establishing a cybersecurity awareness campaign	Section 4 and Compendiun Annex 2
RGQ/40	2015-03-11	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States	-
RGQ/36 +Ann.1	2015-03-10	ABI Research (United States of America)	Global cybersecurity index	Annex 1
RGQ/35 (Rev.1)	2015-03-09	Nuix Technology UK, United Kingdom	A cybersecurity framework for all	Section 7
RGQ/32	2015-03-02	Cisco Systems	Perspectives on spam and cybersecurity	Section 3
RGQ/30	2015-02-26	Cameroon (Republic of)	Main cybersecurity activities in Cameroon	Section 4 Annex 2 compendium
RGQ/25	2015-02-18	Rapporteurs for Question 3/2	Report Table of Contents	-
RGQ/7	2014-12-15	Rapporteurs for Question 3/2	Draft work plan for Question 3/2	-
2/93 +Ann.1	2014-09-09	BDT Focal Point for Question 3/2	Cybersecurity initiatives for Member States	-
2/90	2014-09-09	Japan	Sharing knowledge, information and best practice for developing a culture of cybersecurity	Section 4 Annex 2
2/89	2014-09-09	General Secretariat	WSIS Stocktaking: Success stories	-
2/87	2014-09-08	General Secretariat	Report on WSIS Stocktaking 2014	-
2/78	2014-09-04	Australia, United Kingdom of Great Britain and Northern Ireland, Vanuatu (Republic of)	Support of the Resolution on child online protection	Section 5
2/77	2014-09-02	Symantec Corporation	Cyber-security's role and best practices to ensure Smart Cities' service continuity and resilience	Section 7
2/75	2014-09-01	Cisco Systems	Proposed work plan for the current study period	-
2/67	2014-08-29	China (People's Republic of)	Proposal for a new work item on framework of detection, tracking and response of mobile botnets	Section 3 and Annex 2
2/65	2014-08-28	Korea (Republic of)	Personal information breaches and countermeasures of the Government of Republic of Korea	Section 7 Annex 2 compendium tor b)

Web	Received	Source	Title	Mapping in final report
2/64	2014-08-28	Korea (Republic of)	Experiences and international cooperation in preventing internet addiction in the Republic of Korea	Annex 2 and section 7
2/37	2014-08-06	AT&T Corp.	Spam best practices update	Section 3
2/30	2014-08-04	Telecommunication Standardization Bureau	Draft technical Report on ICT infrastructure for cyber-security, data protection and resilience	
2/17	2014-08-08	Nuix Technology UK (United Kingdom)	The good shepherd model for cybersecurity – Minimizing the potential for, and damage suffered from, data breach	Section 3

Contributions for QAll for Rapporteur Group and Study Group meetings

Web	Received	Source	Title	Mapping
2/355	2016-09-07	Telecommunication Development Bureau	Update on innovation activities to ITU-D Study Groups	
2/320	2016-08-05	General Secretariat	WSIS Stocktaking 2014-2016 Regional Reports of ICT Projects and Activities	
2/319	2016-08-05	General Secretariat	WSIS Prizes 2016-2017	
2/318	2016-08-05	General Secretariat	WSIS Stocktaking 2016-2017	
2/312	2016-08-04	General Secretariat	WSIS Action Line Roadmaps C2, C5 and C6	
2/311	2016-08-04	General Secretariat	ITU's Contribution to the Implementation of the WSIS Outcomes 2016	
2/309	2016-08-04	General Secretariat	WSIS Forum 2016 and SDG Matrix	
2/308	2016-08-04	General Secretariat	WSIS Action Lines Supporting Implementation of the SDGs	
2/307	2016-08-04	General Secretariat	WSIS Forum 2016: High Level Track Outcomes and Executive Brief	
2/306	2016-08-04	General Secretariat	WSIS Forum 2016 Outcome Document- Forum Track	
2/305	2016-08-04	General Secretariat	WSIS Forum 2017- Open Consultation Process	
2/274	2016-06-24	Chairman, ITU-D Study Group 2	Compendium of Draft Outlines for expected outputs to be produced by ITU-D Study Group 2 Questions (September 2016)	

Web	Received	Source	Title	Mapping
RGQ/124	2016-03-18	BDT Focal Point for Question 8/1 and Resolution 9	Outcomes of RA-15,WRC-15 and CPM19-1 related to ITU-D	
RGQ/107	2016-02-18	Kazakhstan (Republic of)	Contribution from Kazakhstan to Questions 1/1, 2/1, 3/1, 4/1, 5/1, 6/1, 7/1, 8/1 and 5/2	
2/249	2015-09-24	Telecommunication Development Bureau	Final list of participants to the second meeting of ITU-D Study Group 2, Geneva, 7 - 11 September 2015	
2/247	2015-08-28	Telecommunication Development Bureau	List of information documents	
2/229	2015-08-25	Telecommunication Development Bureau	ITU-D Study Groups Innovation Update	
2/213	2015-08-07	Telecommunication Development Bureau	1st ITU-D Academia Network Meeting	
2/190	2015-07-24	General Secretariat	WSIS Forum 2015: High level policy statements, Outcome document, Reports on WSIS Stocktaking	
2/150	2015-07-06	Uganda (Republic of)	Increasing women's participation in ITU Study Groups' work	
2/149	2015-06-29	BDT Focal Point for Question 1/1	ITU GSR15 discussion papers and best practice guidelines	
2/100 Rev.1	2014-09-24	Chairman, ITU-D Study Group 2	Appointed Rapporteurs and Vice-Rapporteurs of ITU-D Study Group 2 Questions for the 2014-2018 period	
2/99	2014-09-19	Intel Corporation	New Question for ITU-D Study Group 1 (2014-2018): Assistance to developing countries for the implementation of ICT programs in education	
2/97	2014-09-11	Telecommunication Development Bureau	List of information documents	
2/96	2014-09-15	Chairman, ITU-D Study Group 2	Establishment of working parties for ITU-D Study Group 2	
2/95	2014-09-11	Telecommunication Standardization Bureau	ITU Workshop on Digital financial services and financial inclusion, and First Meeting of Focus Group Digital Financial Services: 4-5 December 2014, ITU, Geneva	
2/92	2014-09-09	General Secretariat	WSIS Action Lines Executive Summaries (Achievements, Challenges and Recommendations)	

Web	Received	Source	Title	Mapping
2/88	2014-09-09	General Secretariat	WSIS+10 High level event: High level policy statements, Forum track outcome document, reports	
2/86	2014-09-08	General Secretariat	WSIS+10 High level event: Outcome documents	
2/51	2014-08-23	Nepal (Republic of)	Need for developing detailed table of contents for each Question under both the ITU-D Study Groups at the beginning	
2/5 Rev.1-2	2014-09-08	Telecommunication Development Bureau	Candidates for Rapporteurs and Vice-Rapporteurs of ITU-D Study Group 1 and 2 study Questions for the 2014-2018 period	
2/4	2014-09-01	Telecommunication Development Bureau	List of WTDC Resolutions and ITU-D Recommendations relevant to the work of the ITU-D Study Groups	
2/2 +Ann.1	2014-08-20	Telecommunication Development Bureau	Resolution 2 (Rev. Dubai, 2014): Establishment of study groups + Full text of all ITU-D Study Group 1 and 2 Questions in Annex 1	
2/1	2014-08-20	Telecommunication Development Bureau	Resolution 1 (Rev. Dubai, 2014): Rules of procedure of the ITU Telecommunication Development Sector	

Information Documents

Web	Received	Source	Title	Mapping
2/INF/4	2014-09-03	UR College of Science and Technology (Rwanda)	Intelligent agents as a useful tool for intrusion detection	
2/INF/2	2014-07-09	Democratic Republic of the Congo	Création d'équipes de Centre de Cybersécurité (CIRT/ Nationales) dans les pays en développement	Tor j) annex 3
2/INF/1	2014-07-09	Democratic Republic of the Congo	Sécurité numérique en République démocratique du Congo	Tor j) annex 3

Liaison Statements

Web	Received	Source	Title
2/365	2016-09-13	ITU-T Study Group 17	Liaison Statement from ITU-T SG17 to ITU-D SG2 Q3/2 on Collaboration on countering and combating spam

Web	Received	Source	Title
2/289	2016-08-01	ITU-T JCA-COP	Liaison statement from ITU-T JCA-COP to ITU-D SG2 Question 3/2 on Child Online Protection Initiatives
2/276 +Ann.1-11	2016-06-29	International Organization for Standardization (ISO)	Liaison Statement from ISO/IEC JTC 1/SC 27/WG 5 to ITU-D SG2 Q3/2 on Identity Management, Privacy Technology, and Biometrics
RGQ/130	2016-03-29	ITU-T Study Group 17	Liaison Statement from ITU-T SG17 to ITU-D SG2 on PKIs and RPKIs for developing countries (reply to Document 2/252)
RGQ/108	2016-02-24	Internet Society	Liaison Statement from Internet society to ITU-D SG2 Q3/2 on Establishing New Certification Authorities
RGQ/100	2016-01-12	RIPE NCC	Liaison Statement from RIPE NCC to ITU-D SG2 on Information on Resource Public Key Infrastructure (RPKI)
RGQ/99	2016-11-17	ISO	Liaison statement from ISO/IEC JTC 1/SC 27 to ITU-D SG2 Question 3/2 on National Cybersecurity Measurement System (NCMS)
RGQ/98	2015-12-12	Internet Corporation for Assigned Names and Number	Liaison Statement from SSAC to ITU-D Study Group 2, Question 3/2 on Establishing New Certification Authorities
RGQ/92	2015-12-21	ITU-T Study Group 11	Liaison Statement from ITU-T SG11 to ITU-D SG2 on the progress of standardization work to combat counterfeit ICT devices
RGQ/85	2015-09-03	GSM Association	Liaison statement from GSMA to ITU-D SG 2 on Framework to address mobile botnets
2/123	2015-04-20	ITU-T Study Group 17	Liaison Statement from ITU-T Study Group 17 to ITU-D Study Group 2 Question 3/2 on Request for information sharing on cybersecurity
2/122	2015-04-20	ITU-T Study Group 17	Liaison Statement from ITU-T Study Group 17 to ITU-D Study Group 2 Question 3/2 on Cooperation with ITU-D Q3/2
2/157	2015-07-04	ITU-T Study Group 15	Liaison Statement from ITU-T SG15 to ITU-D SGs on ITU-T SG15 OTNT standardization work plan
RGQ/17	2015-01-29	ITU-T Study Group 17	Liaison Statement from ITU-T Study Group 17 to ITU-D Study Group 2 Question 3/2 on the Development of a framework to address mobile botnets
RGQ/3 (Rev.1)	2014-11-18	ITU-T Focus Group on SSC	Liaison Statement from ITU-T Focus Group on Smart Sustainable Cities (FG-SSC) on Activities of the Focus Group on Smart Sustainable Cities
RGQ/1	2014-10-02	ITU-T Study Group 17	Liaison Statement from ITU-T Study Group 17 to ITU-D Study Group 2 Question 3/2 on proposed Correspondence Group Terms of Reference for joint working between ITU-T SG17 and ITU-D Q3/2

Web	Received	Source	Title
2/15	2014-02-06	ITU-T Study Group 17	Liaison Statement from ITU-T Study Group 17 to ITU-D Study Group 1 Question 22-1/1 on CYBEX

Liaison Statements for QAll

Web	Received	Source	Title
2/371	2016-09-13	Inter Sector Rapporteur Group	Liaison Statement from Inter Sector Rapporteur Group to ITU-D SG2 on requirements for the application of the UNCRPD for media services for all
2/288	2016-07-29	TSAG	Liaison Statement from TSAG to ITU-D Study Groups on ITU inter-sector coordination
2/281	2016-06-28	ITU-T Study Group 12	Liaison Statement from ITU-T SG12 to ITU-D SG1 and SG2 on revised definition of Quality of Experience (QoE) and new terms in Rec. P.10/G.100
2/280	2016-06-28	ITU-T Study Group 12	Liaison Statement from ITU-T SG12 to ITU-D SG1 and SG2 on ITU inter-Sector coordination (reply to TSAG LS17)
2/271	2016-04-28	ITU-T Study Group 5	Liaison Statement from ITU-T Study Group 5 to ITU-D SG2 on Information about work that is being carried out within work under study in ITU-T Q7/5
RGQ/117	2016-03-07	ITU-T Study Group 15	Liaison statement from ITU-T SG15 to ITU-D SG1 and 2 on the latest version of the Access Network Transport (ANT), Smart Grid and Home Network Transport (HNT) Standards Overviews and Work Plans
RGQ/111	2016-03-03	ITU-D Study Group 15	Liaison statement from ITU-T Study Group 15 to ITU-D SG 1 and 2 on ITU-T SG15 OTNT standardization work plan
RGQ/110	2016-03-03	ITU-T Study Group 15	Liaison statement from ITU-T Study Group 15 to ITU-D SG 1 and 2 on new technical classification and numbering of ITU-T L-Series Recommendations
RGQ/103	2016-02-08	TSAG	Liaison statement from TSAG to ITU-D study groups 1 and 2 on ITU inter-Sector coordination
RGQ/94	2015-11-18	ITU-R Study Group Department	Liaison statement from ITU-R Study Group Department to ITU-D SG 1 and 2 on Resolutions approved at the Radiocommunication Assembly (RA-15)
RGQ/82	2015-09-29	Asia-Pacific Telecommunity (APT)	Liaison statement from the APT Standardization Program Forum (ASTAP) to ITU-D Study Group 1 and 2 on NGN activities
2/230	2015-08-24	ITU-T JCA-AHF	Liaison Statement from ITU-T JCA-AHF, Chairman to ITU-D SGs on Draft meeting report of Joint Coordination Activity on Accessibility and Human Factors (JCA-AHF) in Geneva on 17 June 2015

Web	Received	Source	Title
2/158	2015-07-10	ITU-T Study Group 15	Liaison Statement from ITU-T SG15 to ITU-D SGs on the latest versions of the Access Network Transport (ANT), Smart Grid and Home Network Transport (HNT) Standards Overviews and Work Plans
2/157	2015-07-04	ITU-T Study Group 15	Liaison Statement from ITU-T SG15 to ITU-D SGs on ITU-T SG15 OTNT standardization work plan
2/148	2015-07-12	TSAG	Liaison Statement from TSAG to ITU-D Study Groups on ITU inter-sector coordination
2/144	2015-05-19	ITU-T Focus Group on SSC	Liaison Statement from ITU-T FG-SSC to ITU-D SGs on Final deliverables of the Focus Group on Smart Sustainable Cities (FG-SSC) and proposal of a new Study Group
2/143	2015-05-12	ITU-T Study Group 13	Liaison Statement from ITU-T SG13 to ITU-D SGs on Development of the Roadmap on IMT
2/129	2015-04-30	ITU-T Study Group 11	Liaison Statement from ITU-T SG11 to ITU-D Study Groups on the progress on standardization work to combat Counterfeit ICT devices
2/128	2015-04-29	ITU-T Study Group 16	Liaison Statement from ITU-T SG16 to ITU-D SGs on ITU-D SG1 and SG2 Questions of interest to ITU-T Study Groups
2/127	2015-04-29	ITU-T Focus Group on Digital Financial Services	Liaison Statement from ITU-T Focus Group on Digital Financial Services (DFS) to ITU-D Study Groups on BDT's work on ITU m-Powering Development
2/126	2015-04-29	ITU-T Focus Group on Digital Financial Services	Liaison Statement from ITU-T Focus Group on Digital Financial Services (DFS) to ITU-D Study Groups concerning its work
RGQ/34	2015-03-03	ITU-T Study Group 16	Liaison Statement from ITU-T SG16 to ITU-D SGs on ITU-D SG1 and SG2 Questions of interest to ITU-T Study Groups
RGQ/20	2015-02-10	ITU-R Study Groups - Working Party 5D	Liaison Statement from ITU Radiocommunication Study Groups WP5D to ITU-D Study Groups concerning the Handbook on "Global Trends in IMT"
RGQ/19	2015-02-10	ITU-R Study Groups - Working Party 5D	Liaison Statement from ITU Radiocommunication Study Groups WP5D to ITU-D Study Groups concerning the Handbook on "Global Trends in IMT'
RGQ/16	2015-01-23	ITU-T FG DFS	Liaison Statement from ITU-T Focus Group on Digital Financial Services (DFS) to ITU-D Study Groups on BDT's work on ITU m-Powering Development
RGQ/15	2015-01-22	ITU-T FG DFS	Liaison Statement from ITU-T Focus Group on Digital Financial Services (DFS) to ITU-D Study Groups concerning its work

Web	Received	Source	Title
2/22	2014-05-23	ITU-T JCA-AHF	Liaison Statement from ITU-T Joint Coordination Activity on Accessibility and Human Factors (JCA-AHF) on Assistive Listening Devices (ALD) and the allocation of Mobile Phone Services in the 2.3-2.4 GHz band
2/19	2014-03-10	ITU-T Study Group 11	Liaison Statement from ITU-T Study Group 11 to ITU-D SG1 and SG2 on Request for status update from GSMA and ITU on proposed studies on the issue of mobile theft, grey market and counterfeit devices
2/18 (Rev.1)	2014-03-10	ITU-T Study Group 11	Liaison Statement from ITU-T Study Group 11 to ITU-D SG1 and SG2 on Technical report on counterfeit equipment
2/16	2014-02-10	ITU-T Focus Group on Innovation	Liaison Statement from the ITU-T FG on Innovation to ITU-D SG1 and SG2 on New Standardization Activities for ITU-T study groups and ICT Innovation Panel
2/9	2013-10-22	ITU-T Focus Group on Innovation	Liaison Statement from the ITU-T FG on Innovation to ITU-D SG1 and SG2 on inputs on ICT innovation panel

Annex 5: Survey questions

Raising awareness as a key element of cybersecurity regime

The first part contains a number of questions that attempt to identify the educational role played by the Member States to achieve cybersecurity, in particular whether these states have given a special attention to raising awareness or only dealt minimally with it. What were the means adopted to educate the targeted groups namely the persons with disabilities, children or elderly people? The questions addressed by the Questionnaire in its first part are highlighted as follows:

1	In your opinion, how important is raising awareness on cybersecurity as a basic step to achieving security in cyberspace? a. Not important b. Somewhat important c. Important d. Very Important
2	Are public awareness campaigns in cybersecurity developed and implemented? For organizations? For civil society? For adults (>18 yrs)? For youth (12-17 yrs)? For children (<12yrs)?
3	Which groups are targeted by cybersecurity awareness campaigns in your country? a. Children b. Youth c. Students d. Elderly people e. Persons with disabilities f. Private institutions g. Government agencies h. Others
4	Which one of the groups identified below is more targeted? Please arrange in order of 1 to 6 from the most highly targeted to the least targeted? a. Children b. Youth c. Students d. Elderly people e. Persons with disabilities f. Private institutions g. Government agencies h. Others

5	What are the cybersecurity issues that are addressed by existing awareness campaigns? (Replies to more than one item possible) a. Internet safety b. Privacy c. Fraud d. Phishing e. Malware f. Child Online Protection g. Others
6	What is the degree of importance of each issue? Please arrange in order of the most important to the least important and give reasons for such order. a. Internet safety b. Privacy c. Fraud d. Phishing e. Malware f. Child Online Protection g. Others
7	Are certain tools and technical measures related to providing cybersecurity, such as anti-virus or anti-spam software, made available to persons with disabilities? a. Yes b. No
8	Is the public encouraged to use the different tools and technical measures for cybersecurity, such as anti-virus or anti-spam software? a. Yes b. No
9	If the answer to the previous question is 'yes', are there different types of tools and technical measures made available to the public and how is this achieved?

Child Online Protection as a key element of cybersecurity regime

This part intends to identify the national status of Child Online Protection (COP) in terms of raising awareness, legislations, the necessary tools to provide such protection and the competent authorities in charge of overseeing the implementation of such legislations and invoking the required tools to reach the desired goals. This part also examines whether there are government or civil agencies engaged in educating and providing the required tools and knowledge to those who are concerned with COP.

1	Do you have measures for protecting Children Online?
2	Is there legislation related to child online protection?
3	Is there an agency/entity responsible for Child Online Protection?
4	Is there an established public mechanism for reporting issues associated with children online protection?
5	Are there any technical mechanisms and capabilities deployed to help protect children online?

6	Has there been any activity by government or non-government institutions to provide knowledge and support to stakeholders on how to protect children online?
7	Are there any child online protection education programs?
8	Are there any child online protection education programs for educators?
9	Are there any child online protection education programs for parents?
10	Are there any child online protection education programs for children?
11	Is there a national strategy for child online protection?
12	Are there public awareness campaigns on child online protection?
13	Are there public awareness campaigns on child online protection for children?
14	Are there public awareness campaigns on child online protection for adults?

Annex 6: Information on ACTIVE

This annex includes the basic operation flow for the ACTIVE project which is composed of four steps a) prevention of malware infection, b) Damage prevention of malware infection, c) Removal of malware, and d) Removal of malware.

Basic operation flow of ACTIVE (Advanced Cyber Threats response InitiatiVE) project

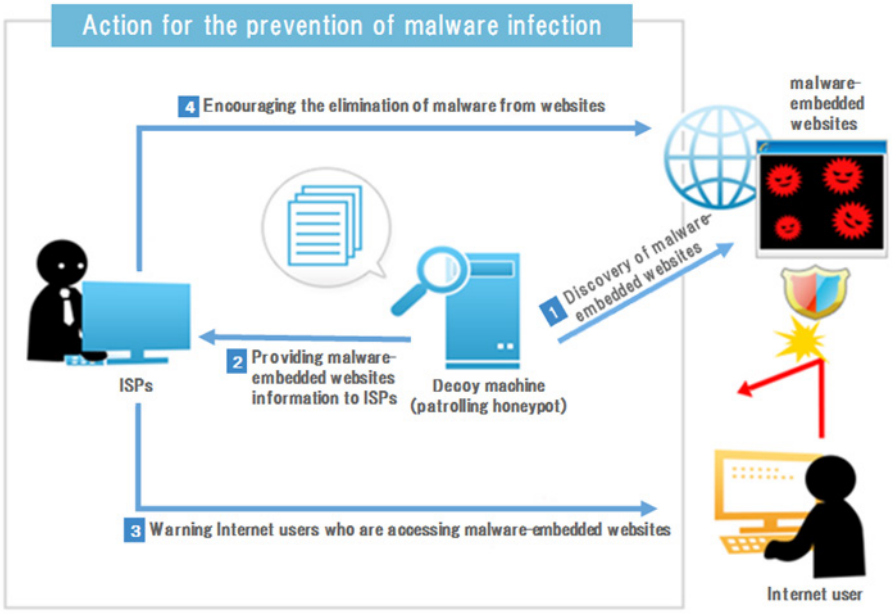
a) Prevention of malware infection; cooperation with ISPs

In recent years, the most frequent malware infection route is through malware-embedded sites. Some of these sites are counterfeits of famous websites, or tampered ones. These sites are difficult for Internet users to distinguish, and therefore users may not be aware that they have malware infection.

This is why ACTIVE was launched. In the ACTIVE project, decoy machines, or patrolling honeypots, access many different websites to confirm malware-embedded websites create a list of these sites. Referring to the list, ISPs send warning statement to users who agreed in advance that they may have warning statements when they are accessing malware-embedded websites. Also, ACTIVE tries to contact the administrators of these sites to request removal of malware from their sites.

Figure 9A outlines the flow for this action.

Figure 9A: Prevention of malware infection



(1) Discovery of malware-embedded websites: A decoy machine -the patrolling honeypot- is connected to the Internet. The machine accesses a number of websites every day, collecting information on any malware-embedded websites to be listed.

(2) Sharing of malware-embedded websites information with ISPs: Information on malware-embedded websites is provided to ISPs.

(3) Warning Internet users accessing malware-embedded websites: Having received prior consent, ISPs send warning statements to Internet users when they are accessing malware-embedded websites.

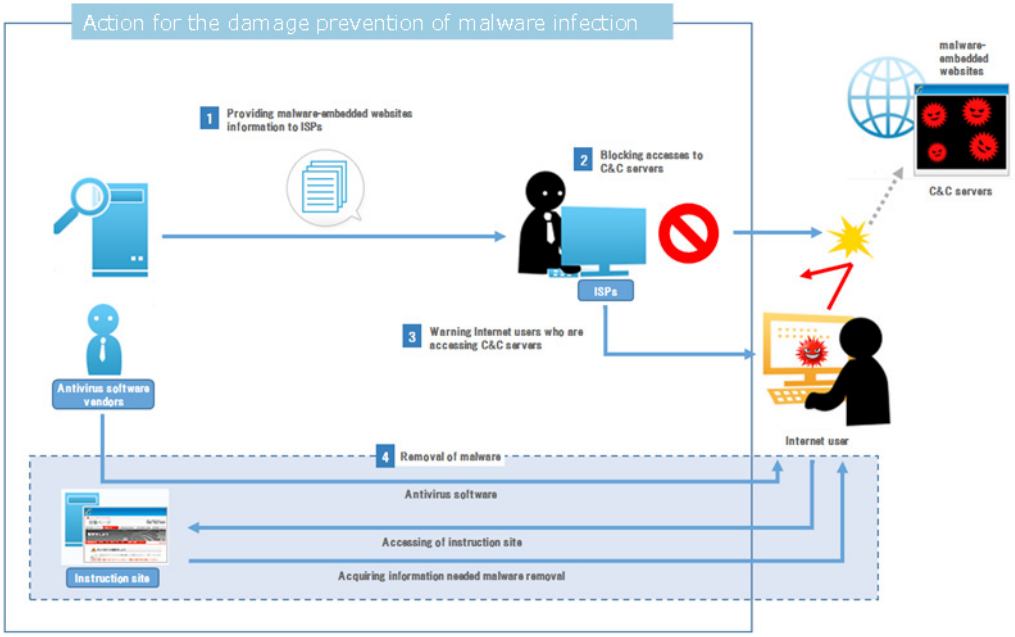
(4) Warning administrators of malware-embedded websites: ISPs send warning statements to the administrators of websites discovered to have embedded malware to request removal of malware from their sites.

b) Damage prevention of malware infection; cooperation with ISPs

ACTIVE leverages a list provided by our partners to prevent damage by blocking accesses to command and control (C&C) servers attempted by Internet users who agreed in advance that they may receive warning statements.

Figure 10A outlines the flow for this action.

Figure 10A: Damage prevention of malware infection



(1) Sharing of command and control (C&C) servers information: Information on C&C servers is provided to ISPs.

(2) Prevention of attacks against traffic between C&C servers: Having received prior consent, ISPs prevent potential damages on Internet users when they attempt to access C&C servers.

(3) Warning Internet users accessing C&C servers: The ISPs send warning to users who are recognized to have malware infection, with the URL of the instruction site.

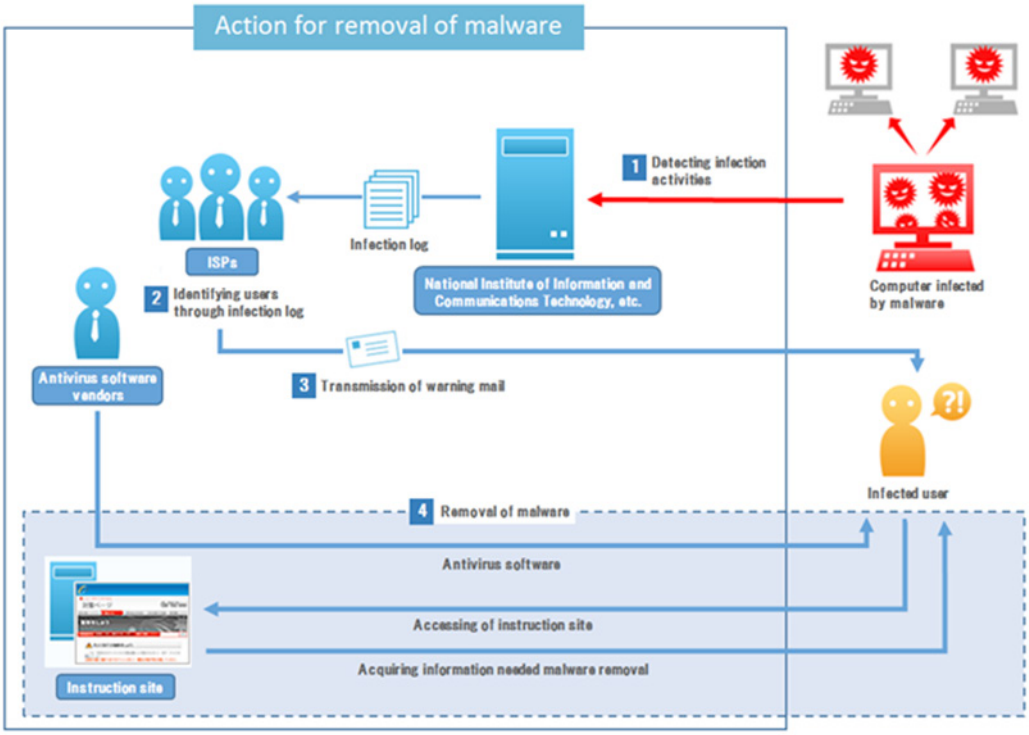
(4) Malware removed: The Internet users access the instruction site and get information needed to remove malware. The instruction site provides useful information such as antivirus vendors' site where antivirus softwares can be downloaded to remove malware.

c) Removal of malware; cooperation with ISPs

Malware-infected PCs are detected based on the malware infection scan data from a certain research institute. In general, any devices sending malware are infected with the malware. ACTIVE works with ISPs to identify and send a warning to such devices to take appropriate actions to remove the malware.

Figure 11A outlines the flow for this action.

Figure 11A: Removal of malware



(1) Detection of malware-infected PCs: Malware-infected PCs are detected, based on the malware infection scan data from a certain research institute.

(2) Identifying malware-infected users: Information on when and from where the detected malware was introduced is provided to ISPs to identify Internet users who are seemingly infected with the malware.

(3) Warning mail sent to users: The ISPs send warning mails to users who are recognized to have malware infection, with the URL of the instruction site.

(4) Malware removed: The Internet users access the instruction site and get information needed to remove malware. The instruction site provides useful information such as antivirus vendors' site where antivirus software can be downloaded to remove malware.

الاتحاد الدولي للاتصالات (ITU)
مكتب تنمية الاتصالات (BDT)
مكتب المدير

Place des Nations
CH-1211 Geneva 20 – Switzerland
Email: bdtdirector@itu.int
Tel.: +41 22 730 5035/5435
Fax: +41 22 730 5484

نائب المدير ورئيس دائرة الإدارة وتنسيق العمليات (DDR)

Email: bdtdeputydir@itu.int
Tel.: +41 22 730 5784
Fax: +41 22 730 5484

دائرة البنية التحتية والبيئة التمكينية والتطبيقات الإلكترونية (IEE)

Email: bdtiee@itu.int
Tel.: +41 22 730 5421
Fax: +41 22 730 5484

دائرة الابتكارات والشراكات (IP)

Email: bdtip@itu.int
Tel.: +41 22 730 5900
Fax: +41 22 730 5484

دائرة المشاريع وإدارة المعرفة (PKM)

Email: bdtpkm@itu.int
Tel.: +41 22 730 5447
Fax: +41 22 730 5484

إفريقيا

إثيوبيا
المكتب الإقليمي للاتحاد

P.O. Box 60 005
Gambia Rd., Leghar ETC Building
3rd floor
Addis Ababa – Ethiopia

Email: ituaddis@itu.int
Tel.: +251 11 551 4977
Tel.: +251 11 551 4855
Tel.: +251 11 551 8328
Fax: +251 11 551 7299

الكاميرون
مكتب المنطقة للاتحاد

Immeuble CAMPOST, 3e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé – Cameroun

Email: itu-yaounde@itu.int
Tel.: + 237 22 22 9292
Tel.: + 237 22 22 9291
Fax: + 237 22 22 9297

السنغال
مكتب المنطقة للاتحاد

8, Route du Méridien
Immeuble Rokhaya
B.P. 29471 Dakar-Yoff
Dakar – Sénégal

Email: itu-dakar@itu.int
Tel.: +221 33 859 7010
Tel.: +221 33 859 7021
Fax: +221 33 868 6386

زيمبابوي
مكتب المنطقة للاتحاد

TelOne Centre for Learning
Corner Samora Machel and
Hampton Road
P.O. Box BE 792 Belvedere
Harare – Zimbabwe

Email: itu-harare@itu.int
Tel.: +263 4 77 5939
Tel.: +263 4 77 5941
Fax: +263 4 77 1257

الأمريكتان

البرازيل
المكتب الإقليمي للاتحاد

SAUS Quadra 06, Bloco "E"
10º andar, Ala Sul
Ed. Luis Eduardo Magalhães (Anatel)
70070-940 Brasilia, DF – Brazil

Email: itubrasilia@itu.int
Tel.: +55 61 2312 2730-1
Tel.: +55 61 2312 2733-5
Fax: +55 61 2312 2738

بربادوس
مكتب المنطقة للاتحاد

United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown – Barbados

Email: itubridgetown@itu.int
Tel.: +1 246 431 0343/4
Fax: +1 246 437 7403

شيلي
مكتب المنطقة للاتحاد

Oficina de Representación de Área
Merced 753, Piso 4
Casilla 50484, Plaza de Armas
Santiago de Chile – Chile

Email: itusantiago@itu.int
Tel.: +56 2 632 6134/6147
Fax: +56 2 632 6154

هندوراس
مكتب المنطقة للاتحاد

Oficina de Representación de Área
Colonia Palmira, Avenida Brasil
Ed. COMTELCA/UIT, 4.º piso
P.O. Box 976
Tegucigalpa – Honduras

Email: itutegucigalpa@itu.int
Tel.: +504 22 201 074
Fax: +504 22 201 075

الدول العربية

مصر
المكتب الإقليمي للاتحاد

Smart Village, Building B 147, 3rd floor
Km 28 Cairo – Alexandria Desert Road
Giza Governorate
Cairo – Egypt

Email: itu-ro-arabstates@itu.int
Tel.: +202 3537 1777
Fax: +202 3537 1888

آسيا – المحيط الهادئ

تايلاند
المكتب الإقليمي للاتحاد

Thailand Post Training Center, 5th floor,
111 Chaengwattana Road, Laksi
Bangkok 10210 – Thailand

Mailing address
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210 – Thailand
Email: itubangkok@itu.int
Tel.: +66 2 575 0055
Fax: +66 2 575 3507

إندونيسيا
مكتب المنطقة للاتحاد

Sapta Pesona Building, 13th floor
Jl. Merdan Merdeka Barat No. 17
Jakarta 10110 – Indonesia

Mailing address:
c/o UNDP – P.O. Box 2338
Jakarta 10110 – Indonesia
Email: itujakarta@itu.int
Tel.: +62 21 381 3572
Tel.: +62 21 380 2322/2324
Fax: +62 21 389 05521

كومنولث الدول المستقلة

الاتحاد الروسي
مكتب المنطقة للاتحاد

4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation

Mailing address:
P.O. Box 47 – Moscow 105120
Russian Federation
Email: itumoskow@itu.int
Tel.: +7 495 926 6070
Fax: +7 495 926 6073

آوروبا

سويسرا
الاتحاد الدولي للاتصالات (ITU)
مكتب تنمية الاتصالات (BDT)
مكتب المنطقة للاتحاد

Place des Nations
CH-1211 Geneva 20 – Switzerland
Switzerland
Email: eurregion@itu.int
Tel.: +41 22 730 6065

الاتحـاد الـدولي للاتصـالات
مكتب تنميـة الاتصـالات
Place des Nations
CH-1211 Geneva 20
Switzerland
www.itu.int

ISBN 978-92-61-23006-7
9 789261 230067

طبع في سويسرا
جنيف، **2017**