Informe Final

UIT-D
Comisión de Estudio 2

Cuestión 3/2

Seguridad en las redes de información y comunicación: Prácticas óptimas para el desarrollo de una cultura de ciberseguridad

6° Periodo de Estudios
2014-2017

COMUNICARSE CON NOSOTROS

Sitio web:	www.itu.int/ITU-D/study-groups
Librería electrónica:	www.itu.int/pub/D-STG/
Correo-e:	devsg@itu.int
Teléfono:	+41 22 730 5999

Cuestión 3/2: Seguridad en las redes de información y comunicación: Prácticas óptimas para el desarrollo de una cultura de ciberseguridad

Informe Final

Prefacio

Las Comisiones de Estudio del Sector de Desarrollo de las Telecomunicaciones de la UIT (UIT-D) constituyen una plataforma basada en contribuciones en la que expertos de gobiernos, de la industria y de instituciones académicas producen herramientas prácticas, directrices de utilización y recursos para resolver problemas de desarrollo. Mediante los trabajos de las Comisiones de Estudio del UIT-D, los Miembros del UIT-D estudian y analizan cuestiones de telecomunicaciones/TIC orientadas a tareas específicas con el fin de acelerar el progreso de las prioridades nacionales en materia de desarrollo.

Las Comisiones de Estudio del UIT-D ofrecen a todos los Miembros del UIT-D la oportunidad de compartir experiencias, presentar ideas, intercambiar opiniones y llegar a un consenso sobre las estrategias adecuadas para atender las prioridades de telecomunicaciones/TIC. Las Comisiones de Estudio del UIT-D se encargan de preparar informes, directrices y recomendaciones basándose en los insumos o contribuciones recibidos de los miembros. La información se recopila mediante encuestas, contribuciones y estudios de casos, y se divulga para que los miembros la puedan consultar fácilmente con instrumentos de gestión de contenidos y de publicación en la web. Su trabajo está vinculado a los diversos programas e iniciativas del UIT-D con el fin de crear sinergias que redunden en beneficio de los miembros en cuanto a recursos y experiencia. A tal efecto, es fundamental la colaboración con otros grupos y organizaciones que estudian temas afines.

Los temas de estudio de las Comisiones de Estudio del UIT-D se deciden cada cuatro años en las Conferencias Mundiales de Desarrollo de las Telecomunicaciones (CMDT), donde se establecen los programas de trabajo y las directrices para definir las cuestiones y prioridades de desarrollo de las telecomunicaciones/TIC para los siguientes cuatro años.

El alcance de los trabajos de la **Comisión de Estudio 1 del UIT-D** es estudiar **“Entorno propicio para el desarrollo de las telecomunicaciones/TIC”**, y el de la **Comisión de Estudio 2 del UIT-D** es estudiar **“Aplicaciones TIC, ciberseguridad, telecomunicaciones de emergencia y adaptación al cambio climático“**.

Durante el periodo de estudios 2014-2017 la **Comisión de Estudio 2 del UIT-D** estuvo presidida por el Sr. Ahmad Reza Sharafat (República Islámica del Irán) y los Vicepresidentes representantes de las seis regiones: Aminata Kaba-Camara (República de Guinea), Christopher Kemei (República de Kenya), Celina Delgado (Nicaragua), Nasser Al Marzouqi (Emiratos Árabes Unidos), Nadir Ahmed Gaylani (República del Sudán), Ke Wang (República Popular de China), Ananda Raj Khanal (República de Nepal), Evgeny Bondarenko (Federación de Rusia), Henadz Asipovich (República de Belarús) y Petko Kantchev (República de Bulgaria).

Informe Final

El Informe Final de la **Cuestión 3/2: "Seguridad de la información y comunicación: prácticas óptimas para el desarrollo de una cultura de ciberseguridad"** ha sido preparado bajo la dirección de sus dos Correlatores: Rozalin Basheer Faqeer Al-Balushi (Organismo Regulador de las Telecomunicaciones de Omán (TRA), Omán) y Eliot Lear (Estados Unidos de América); y sus siete Vicerrelatores nombrados: Damnam Kanlanfei Bagolibe (Togo), Christopher Ganizani Banda (Malawi), Albert Kamga (Camerún), Miho Naganuma (Japón), Jean-David Rodney (Haití), Jabin S. Vahora (Estados Unidos de América) y Jaesuk Yun (República de Corea). También contaron con la asistencia de los coordinadores del UIT-D y la Secretaría de las Comisiones de Estudio del UIT-D.

ISBN

978-92-61-23993-1 (versión papel)

978-92-61-23003-6 (versión electrónica)

978-92-61-23013-5 (versión EPUB)

978-92-61-23023-4 (versión mobi)

El presente informe ha sido preparado por muchos expertos de administraciones y empresas diferentes. Cualquier mención de empresas o productos concretos no implica en ningún caso un apoyo o recomendación por parte de la UIT.

Antes de imprimir este informe, piense en el medio ambiente.

Índice

Lista de cuadros y figuras

Cuadros

Figuras

Resumen

i. Resumen ejecutivo

En este Informe se abordan numerosos temas relacionados con el mandato de la Cuestión 3/2: "Seguridad en las redes de información y comunicación: Prácticas óptimas para el desarrollo de una cultura de ciberseguridad", que ésta ha examinado durante el periodo de estudios de tres años que finaliza en abril de 2017. En primer lugar, se analiza la encuesta de sensibilización para la ciberseguridad realizada por la Oficina de Desarrollo de las Telecomunicaciones (BDT) de la UIT y que demuestra que, si bien algunos países han de mejorar en este aspecto, otros no, y que los que han de mejorar con frecuencia no se dirigen a los segmentos clave de la sociedad. Con frecuencia se presta una especial atención a la protección de la infancia en línea, que se considera una prioridad. En el Informe se aborda el tema del spam (correo basura), sus causas y los medios para luchar contra él. Si bien el ancho de banda que consume el correo-e suele ser escaso, su contribución a la degradación del valor de la comunicación sigue siendo preocupante. En el Informe se dan muestras de las actividades emprendidas por los gobiernos para mejorar su postura social global en cuanto a la ciberseguridad**.**

Si durante el anterior periodo de estudios (2010-2014) la atención se centró en los materiales docentes que se habían de facilitar a través de la BDT, este periodo de estudios (2014-2017) se ha centrado en los talleres para llevar a los países en desarrollo a un amplio abanico de actores y sus contenidos. Se presenta también un resumen de esos talleres con enlaces a su contenido.

Anexa al Informe se presenta información relacionada con el Índice de Ciberseguridad Mundial (GCI) que la Oficina de Desarrollo de las Telecomunicaciones de la UIT (BDT) ha estado llevando a cabo durante varios años.

Por último se presentan algunas consideraciones y recomendaciones para los futuros estudios**.**

ii. Introducción

La Cuestión 3/2 del UIT-D prepara informes sobre prácticas idóneas relativas a diversos aspectos de la ciberseguridad. Este es el último informe de la Cuestión 3/2 de la Comisión de Estudio 2 del UIT-D sobre sus actividades realizadas en el último ciclo de estudios trianual, que comprende el periodo de 2014 a 2017. El programa de trabajo de la Cuestión 3/2 fue creado por la Conferencia Mundial de Desarrollo de las Telecomunicaciones (CMDT) en su reunión de 2014 celebrada en Dubái, Emiratos Árabes Unidos. En el último periodo de tres años, la Cuestión 3/2 ha abordado la mayoría de los temas de dicho programa.

El presente informe final está integrado por diversos informes de prácticas idóneas sobre diferentes aspectos de la ciberseguridad.

En el **Capítulo 1** se examina la encuesta de sensibilización sobre la ciberseguridad.

En el **Capítulo 2** se examina la situación del software malicioso o malware y del spam, las mitigaciones y los aspectos reglamentarios.

En el **Capítulo 3** se examinan las experiencias de los países en campañas de sensibilización, elaboración de estrategias y medición de la ciberseguridad.

El **Capítulo 4** está dedicado a la encuesta de la protección de la infancia en línea y las cuestiones en juego.

En el **Capítulo 5** se examinan los resultados de los talleres sobre ciberseguridad realizados durante el periodo de estudios.

En el **Capítulo 6** se resumen los trabajos presentados por diversas organizaciones a la Comisión de Estudio.

En el **Capítulo 7** se examinan las experiencias nacionales con respecto a los criterios comunes.

Finalmente, en el **Capítulo 8** figuran las conclusiones de este informe y se indican ámbitos que se habrán de estudiar en el futuro.

Cabe señalar al principio de este informe que la Comisión de Estudio ha examinado y comentado todos los documentos producidos en el contexto del Índice de Ciberseguridad Mundial 2017. El índice de 2017 se basó en el análisis de 134 respuestas recibidas de los 193 Estados Miembros, de los coordinadores para el GCI (identificados por cada Estado Miembro a petición de la UIT) que completaron la encuesta en línea. Las encuestas de la Cuestión de la Comisión de Estudio, a saber, la encuesta sobre la conciencia de la ciberseguridad y la encuesta sobre la protección de la infancia en línea, se integraron en la encuesta sobre GCI, obteniéndose así un mayor número de respuestas (de 51 en el anterior periodo de estudio a más de 129 en este periodo).

Se revisaron el cuestionario sobre GCI de 2017[1] y otros documentos pertinentes (el modelo de referencia inclusive) y se adjuntan en los **Anexos**. El resumen de los resultados de la encuesta sobre GCI de 2017 figura en el **Anexo 1**.

La Cuestión de Estudio examinó todos los temas de su mandato, con la notoria excepción de:

f) ***Examinar las necesidades especiales de las personas con discapacidades de forma coordinada con otras Cuestiones relevantes.***

Este tema, aunque es importante, no se examinó debido a lo reducido del periodo de estudios y por falta de contribuciones. Cabe señalar que el 69 por ciento de los Estados Miembros participantes en el cuestionario sobre la conciencia de la ciberseguridad no incluyó a las personas con discapacidad entre sus grupos objetivo, lo que demuestra que es necesario seguir trabajando sobre este tema (véase más información al respecto en la **Sección 1.2**).

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

1 CAPÍTULO 1 – Cuestionario de sensibilización sobre la ciberseguridad

Esta sección trata del tema *d)* del mandato de la Cuestión 3/2, en el que se pide, entre otras cosas*:*

d) ***Seguir analizando los resultados de la encuesta de sensibilización sobre ciberseguridad realizada durante el último periodo de estudio, y distribuir una encuesta actualizada a fin de medir el progreso con el transcurso del tiempo.***

El régimen de ciberseguridad no se desarrollará completamente hasta que no se preste suma atención a la sensibilización del público y los usuarios. Ningún marco destinado a lograr la ciberseguridad podrá ser viable sin la adecuada sensibilización, que es uno de sus aspectos fundamentales. Los interesados o comprometidos en el ciberespacio reconocen que para lograr la ciberseguridad siempre resultan fundamentales los siguientes factores: i) promulgación de la legislación necesaria para proteger la ciberseguridad; ii) coordinación y cooperación entre las partes consideradas (tanto del sector privado como el público); iii) disponibilidad de herramientas técnicas para lograr la seguridad; iv) coordinación internacional; v) medición periódica de la eficiencia; y vi) divulgación de información y sensibilización.

Habida cuenta de la importancia de la sensibilización para lograr la ciberseguridad, se ha preparado este cuestionario con el fin de medir el nivel de voluntad de sensibilizar en este campo, definir los grupos destinatarios, ya sean organismos gubernamentales o partes pertinentes como empresas del sector privado e instituciones u otras categorías, como personas con discapacidad o la infancia, e identificar los ciberriesgos más elevados para los países.

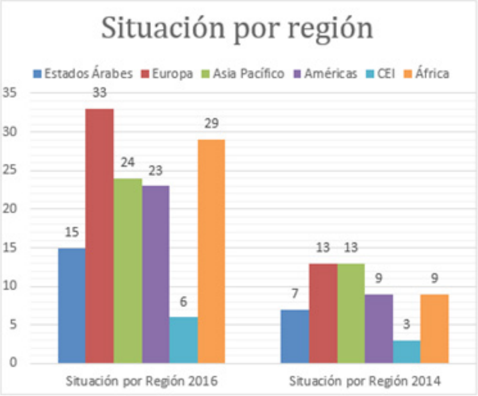
1.1 Métodos de recopilación de información

En la segunda reunión para la Cuestión 3/2 de la Comisión de Estudio 2 del UIT-D en 2015, se acordó integrar el cuestionario sobre sensibilización y protección de la infancia en línea (PIeL) con el cuestionario del Índice Mundial de Ciberseguridad[1] con el fin de lograr unos objetivos similares de manera eficiente, evitar la duplicación de trabajos y esfuerzos, y garantizar una mayor participación con las contribuciones de los Estados Miembros al cuestionario.

El 11 de diciembre de 2015, se envió el cuestionario a 193 Estados Miembros de la UIT para recabar sus respuestas. Respondieron 129 de los 193 países a las preguntas relacionadas con la sensibilización sobre ciberseguridad (aproximadamente el 63 por ciento de los Estados Miembros de la UIT), mientras que 131 países respondieron a las preguntas sobre la PIeL (alrededor del 68 por ciento de los Estados Miembros de la UIT). El equipo encargado de coordinar el cuestionario transmitió estos datos a la Cuestión 3/2, que ulteriormente examinó y analizó los datos y los incluyó en los resultados del informe final.

[1] El Índice de Ciberseguridad Mundial (GCI) nació de la cooperación entre el sector privado y las organizaciones internacionales para dar a la ciberseguridad prioridad en las agendas nacionales. Proyecto común de ABI Research y la Unión Internacional de Telecomunicaciones, el GCI ofrece información sobre el compromiso de los Estados soberanos para con la ciberseguridad.

Figura 1: Respuestas al cuestionario de sensibilización sobre ciberseguridad, por región

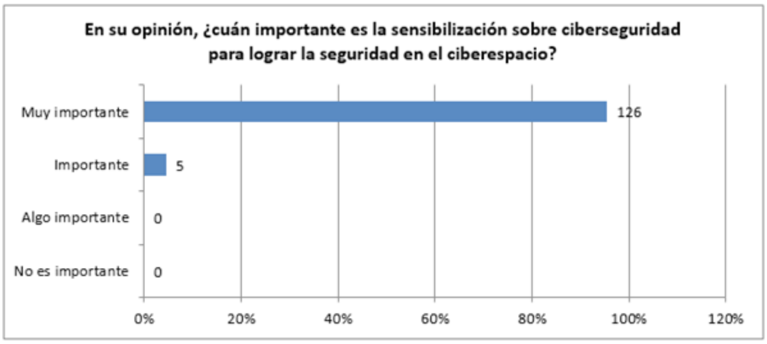


1.2 Análisis de los datos de las campañas de sensibilización

El objetivo de las preguntas relativas a los ciberriesgos era determinar la importancia de la sensibilización sobre dichos riesgos para lograr la seguridad en el ciberespacio.

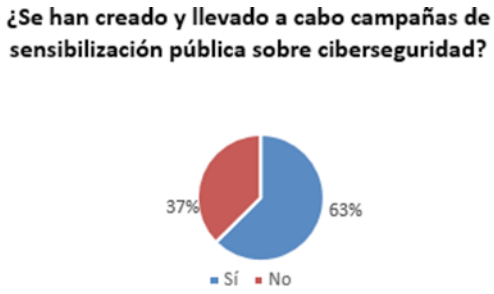
El 95,42 por ciento de las respuestas indicaban que es "muy importante", mientras que el 4,58 por ciento lo consideraba "importante". Se observa un aumento en el porcentaje de respuestas que consideraron "muy importante" la sensibilización sobre ciberseguridad en estos resultados con respecto a los del cuestionario similar del anterior periodo de estudios (2010-2014), cuyo porcentaje era del 79 por ciento.

Figura 2: Importancia de la sensibilización sobre ciberseguridad



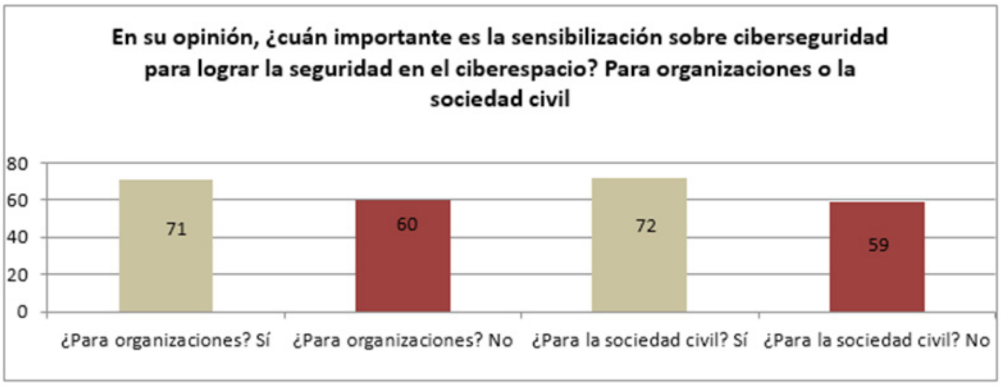
82 países, de un total de 131, han preparado y llevado a cabo campañas de sensibilización sobre ciberriesgos. Esto implica la percepción de los Estados Miembros y su conciencia de la importancia que reviste concebir, preparar y llevar a cabo campañas de sensibilización sobre ciberriesgos en sus países.

Figura 3: Campañas de sensibilización pública sobre ciberseguridad



En lo que respecta a los sectores destinatarios de campañas de sensibilización, según los resultados del cuestionario son el sector gubernamental (71 países) y el sector civil (72 países). Estas cifras confirman que los Estados Miembros consideran relativamente igual de importante la sensibilización del sector público y del sector civil.

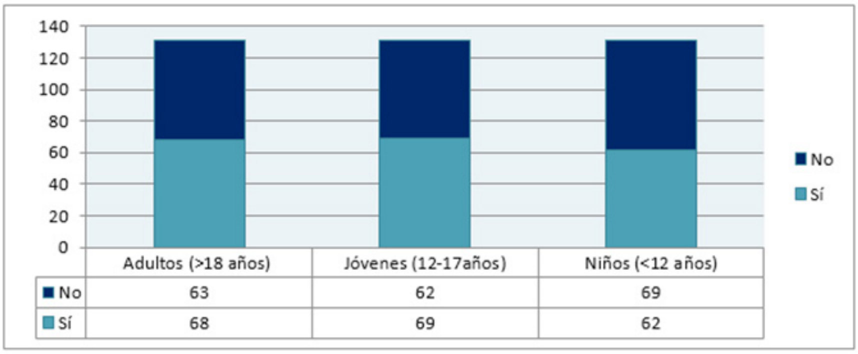
Figura 4: Importancia de la sensibilización sobre ciberseguridad para las organizaciones y la sociedad civil



En lo que respecta a los grupos de edad a los que van dirigidas las campañas de sensibilización sobre ciberseguridad, el Cuestionario propone tres categorías: adultos (18+ años), jóvenes (12-17 años) y niños (menos de 12 años).

En la **Figura 5** se demuestra que los tres grupos de edad fueron destinatarios de las campañas en un grado similar. Según los resultados, el grupo destinatario de más campañas siguió siendo el de jóvenes, mientras que el de niños fue el de menos. La explicación puede ser que los Estados Miembros consideran al grupo de jóvenes como el más vulnerable a los riesgos de ciberseguridad, debido a sus interacciones con los servicios de telecomunicaciones y, principalmente el acceso a Internet.

Figura 5: Destinatarios de las campañas de sensibilización sobre ciberseguridad, por grupos de edad

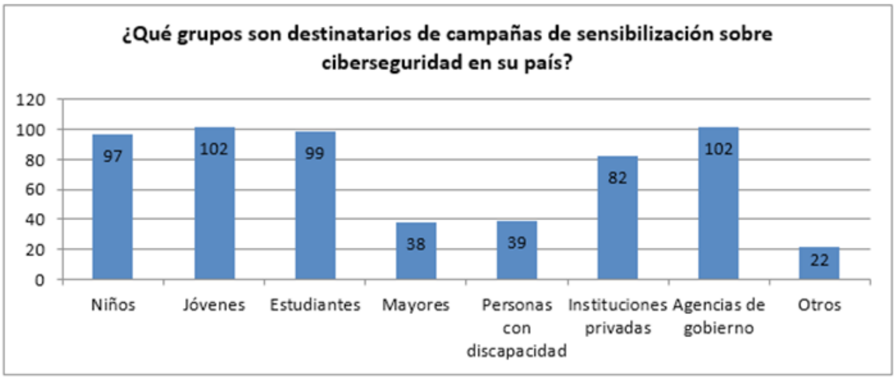


	Adultos (>18 años)	Jóvenes (12-17años)	Niños (<12 años)
No	63	62	69
Sí	68	69	62

Cabe destacar que las campañas de sensibilización sobre ciberseguridad no se limitan a los grupos mencionados, puesto que también van dirigidas a otros grupos, como ancianos o personas con discapacidad, para los que se ejecutan programas especiales adaptados a sus necesidades y que responden a su situación, ya que los riesgos en el caso de ancianos son diferentes que en el caso de niños.

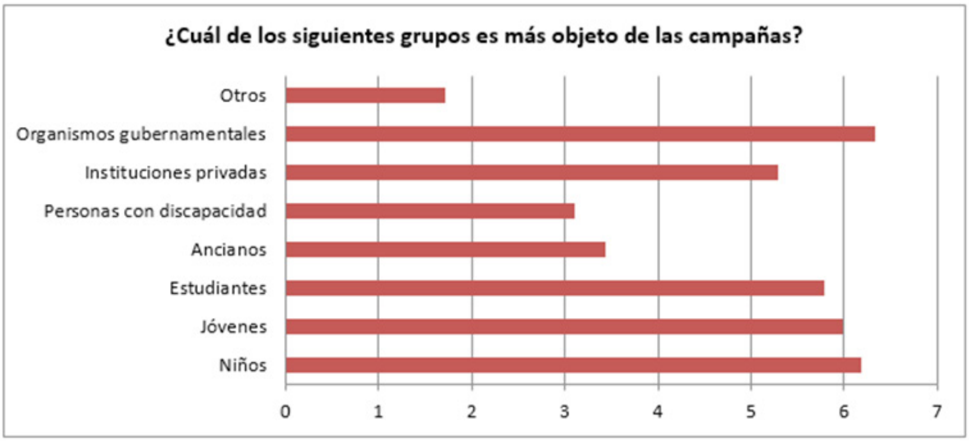
El cuestionario muestra claramente que los organismos gubernamentales y los jóvenes son los grupos en los que más se concentran los Estados Miembros. Lo mismo puede decirse de los grupos de estudiantes y jóvenes, que son destinatarios de 99 y 102 países, respectivamente. En cambio, sólo 38 países se dirigen al grupo de ancianos cuando organizan campañas de sensibilización, es decir, sólo el 70 por ciento de los Estados Miembros que participaron en el Cuestionario no destinaron campañas de sensibilización sobre ciberseguridad a este grupo. Cabe observar que el 69 por ciento de los Estados que respondieron al cuestionario no incluyeron a las personas con discapacidad entre sus grupos destinatarios. Se repite por tanto los mismos resultados que en el cuestionario anterior, en los que se muestra que los grupos a los que menos van dirigidas las campañas de sensibilización sobre ciberseguridad son los ancianos y las personas con discapacidad.

Figura 6: Grupos destinatarios de las campañas de sensibilización sobre ciberseguridad



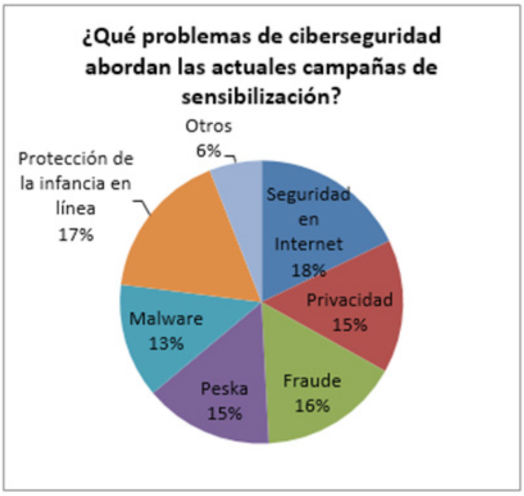
Según el análisis de la información relativa a las respuestas a la pregunta: ¿a qué grupos van más dirigidas las campañas de sensibilización sobre ciberseguridad? La mayoría de las respuestas citaban el sector gubernamental seguido en segundo lugar por la infancia, mientras que los grupos de jóvenes y estudiantes ocuparon el tercer y el cuarto lugar, respectivamente. Por otra parte, los grupos a los que menos van dirigidas las campañas son, una vez más, las personas mayores y las personas con discapacidad, al igual que en el anterior periodo de estudios de 2010-2014. El único cambio evidente entre los resultados de este periodo y los del periodo anterior es que el sector gubernamental ocupa el primer lugar de los grupos destinatarios, mientras que antes ocupaba el segundo lugar. El grupo de niños ocupa el segundo lugar en los resultados del cuestionario, cuando en el anterior cuestionario ocupaba el primer lugar, mientras que los grupos de jóvenes y estudiantes ocupan las mismas posiciones que en el anterior cuestionario.

Figura 7: Grupos a los que van más dirigidas las campañas de sensibilización sobre ciberseguridad



Era importante determinar los problemas destacados en tales campañas que pretender sensibilizar sobre los diversos ciberriesgos. Los problemas más importantes eran la seguridad de Internet, la privacidad, el fraude, la *peska* (phishing), el malware y la protección de la infancia en línea. El más importante de estos problemas de ciberseguridad era el de la seguridad de Internet, seguido de la protección de la infancia en línea, el fraude y la *peska*. En general, los resultados de las campañas de sensibilización sobre ciberseguridad fueron similares, al igual que para el cuestionario del anterior periodo de estudios, es decir la seguridad de Internet era también el más importante, seguido de la PIeL, mientras que la privacidad, el fraude y la *peska* ocupaban el tercer lugar con el mismo porcentaje. La PIeL representa el porcentaje más algo en cuanto a campañas de sensibilización sobre ciberseguridad, ya que 43 de los 129 países seleccionaron la PIeL como el problema más importante. Esto tiene sentido debido a la importancia de la PIeL, que debe ser objeto de más campañas de sensibilización en la sociedad, en particular, entre el grupo de niños que están sujetos a estos riesgos además de los padres y profesores. La importancia de la PIeL queda confirmada además por el hecho de que ocupa la misma posición en el Cuestionario del anterior periodo de estudios.

Figura 8: Problemas de seguridad objeto de campañas de sensibilización



La seguridad en Internet ocupa en promedio el segundo lugar, seguido del fraude y la privacidad, mientras que el software malicioso y la pesca ocupan la última posición, como se observa en la **Figura 9**.

Figura 9: Importancia de cada problema de seguridad objeto de campañas de sensibilización

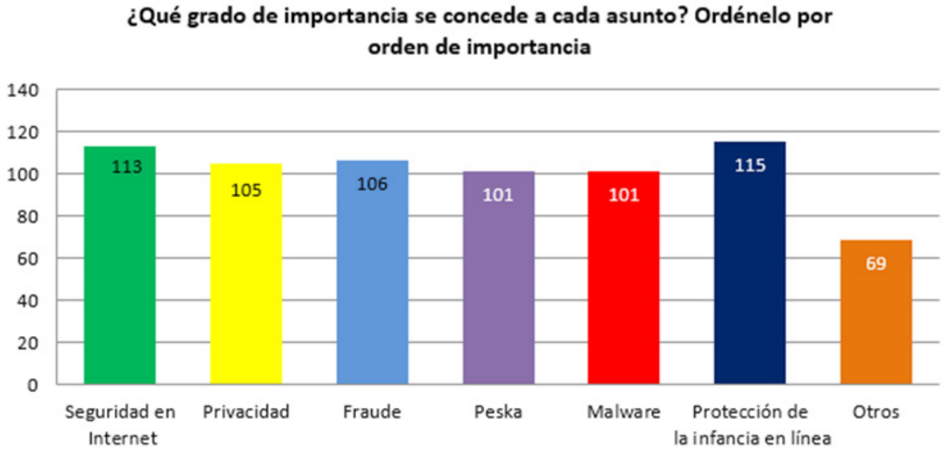
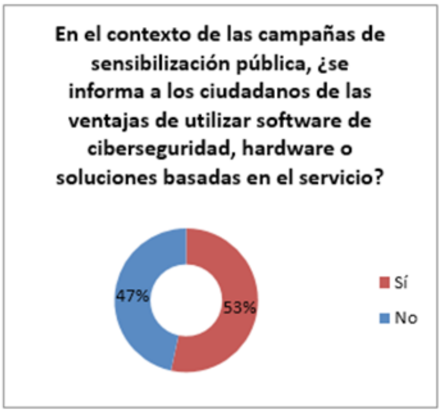


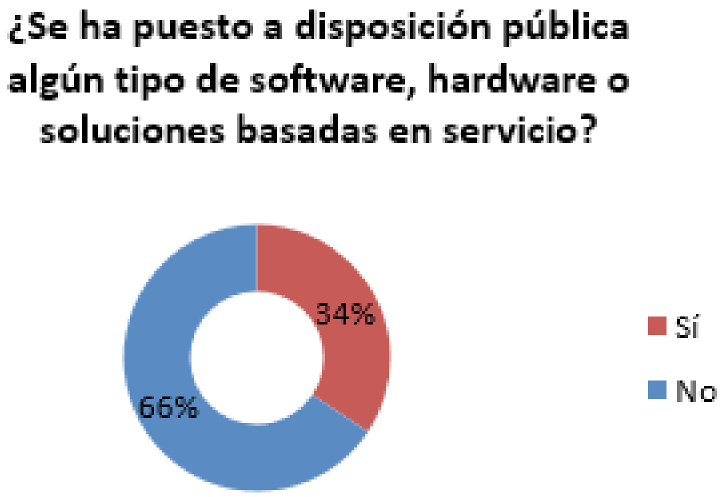
Figura 10: Personas informadas de las ventajas de las soluciones software/hardware o basadas en servicio



Cuando se examina el tema de la sensibilización, es importante abordar la cuestión de la familiaridad con la tecnología y la disponibilidad de herramientas tecnológicas para garantizar la protección contra diversos ciberriesgos. El aumento de los conocimientos teóricos no es suficiente si no se adquieren los conocimientos prácticos o tecnológicos. Por conocimientos prácticos se entiende que la persona es consciente de la utilidad de las soluciones software, hardware o basadas en servicio disponibles para la ciberseguridad, dado que muchos programas informáticos desempeñan un papel esencial en la ciberseguridad y la lucha contra los ciberriesgos. 70 países de 131 promueven dichos programas informáticos y destacan su utilización para los grupos destinatarios. Son 61 los países que todavía no han logrado familiarizar a sus ciudadanos con programas informáticos y otros tipos de soluciones técnicas necesarias para resolver los ciberriesgos. Aunque los dos resultados son similares, se observa que la divulgación de soluciones técnicas y programas informáticos representa un mayor porcentaje en las campañas de sensibilización sobre ciberseguridad.

El cuestionario también revela que 45 países ya han puesto a disposición pública este tipo de programas informáticos o soluciones basadas en servicio, mientras que en la mayoría de ellos (86 países), que representan el 65,65 por ciento de las respuestas, aún no lo han hecho.

Figura 11: Soluciones software/hardware o basadas en servicio a disposición pública



Véase **el Capítulo 4** para el análisis del cuestionario PIeL.

2 CAPÍTULO 2 – Situación del spam y del software malicioso: mitigación y aspectos reglamentarios

Esta sección trata de los temas *a)* y *b)* del mandato de la Cuestión 3/2, en los que se pide, entre otras cosas:

a) ***Considerar enfoques y mejores prácticas para evaluar el impacto del correo basura dentro de una red, y ofrecer las medidas necesarias, tales como técnicas de mitigación, que los países en vías de desarrollo puedan utilizar, teniendo en cuenta las normas existentes y las herramientas disponibles.***

b) ***Facilitar información sobre dificultades actuales en materia de ciberseguridad que experimentan los proveedores de servicios, los organismos reguladores y otras partes interesadas.***

La principal manera en la que se genera el spam es a través de sistemas infectados por los atacantes (por ejemplo, que les pertenecen). Estos sistemas producen luego mensajes spam a través de sus proveedores de servicio. La solución clásica a esta forma de ataque consiste en mantener actualizadas y consultar bases de datos sobre la reputación de los remitentes. Esta reputación se basa en la dirección IP del remitente. Cada tipo de sistema basado en la reputación extrae sus conclusiones de manera diferente. Un método común es utilizar direcciones de correo electrónico “tarro de miel”, cuya finalidad es exclusivamente atraer a los remitentes de spam. Cuando llega un mensaje a estos buzones de correo, la dirección IP del remitente adquiera una reputación negativa.

Los sistemas basados en la reputación suelen tener en cuenta el volumen. Ahora bien, últimamente esto está resultando cada vez más difícil. La “raqueta de nieve” trata de aprovechar la enorme dimensión y distribución geográfica de las redes robot (redes de computadores infectados) de modo que ningún computador envía muchos mensajes, sino que en conjunto generan gran volumen de tráfico.

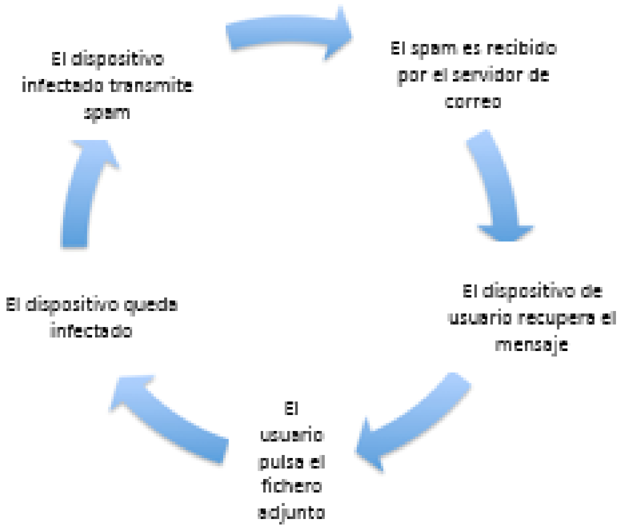
A pesar de estas formas de ataque, los sistemas antispam son generalmente capaces de reducir la cantidad de spam enviada a los destinatarios en más de un 90 por ciento y, en muchos casos, en más del 99 por ciento. Los filtros antispam son un componente fundamental para que el correo electrónico siga siendo un medio eficaz de comunicación. Es asimismo un mecanismo fundamental para evitar que los dispositivos sean infectados.

La recepción de spam por sí misma no infecta o avería un dispositivo. De hecho, existen muchas formas de romper el círculo vicioso. Como se ha mencionado anteriormente, los filtros antispam eliminan una buena parte. En muchos casos, incluso cuando se recibe un mensaje, se requiere la acción del usuario, por ejemplo, abrir un fichero adjunto. Por consiguiente, educar al usuario es fundamental para evitar que se perpetúe el spam. Cuando el usuario abre un fichero adjunto, el antivirus o el sistema operativo actualizados pueden impedir también la infección. Existen, para cada uno de estos componentes, diversas herramientas gratuitas o económicas disponibles para los usuarios y proveedores de servicio de países en desarrollo.

Otra técnica conocida es el pirateo de bloques de direcciones IP en el sistema de encaminamiento. Este se produce cuando un atacante se comunica con un proveedor de servicio confiado para intercambiar información sobre encaminamiento. Se ha desarrollado recientemente una nueva forma de protección – Seguridad del protocolo de pasarela de frontera (BGPSEC)[2] con Infraestructura de clave pública de encaminamiento (RPKI) – para impedir estas formas de ataque, que se encuentra en proceso de desarrollo e implantación. No obstante, pasará tiempo hasta que esta nueva protección de los sistemas de encaminamiento se haya probado y se utilice ampliamente. Entretanto, todos los métodos antes mencionados seguirán siendo eficaces contra el spam.

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

Figura 12: Círculo vicioso entre el spam y la ciberseguridad


El spam es recibido por el servidor de correo
El dispositivo de usuario recupera el mensaje
El usuario pulsa el fichero adjunto
El dispositivo queda infectado
El dispositivo infectado transmite spam

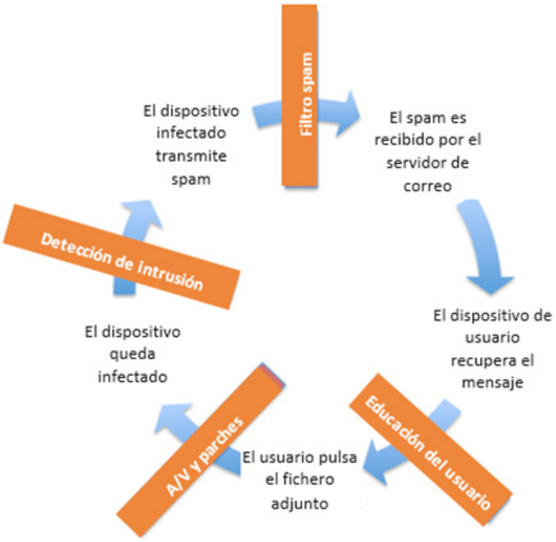
Otro mecanismo de mitigación que se ha desarrollado recientemente se denomina Conformidad y autentificación de mensajes basada en el dominio (DMARC).[3] La DMARC se basa en dos tecnologías de autentificación subyacentes: DKIM (DomainKeys Identified Mail) y SPF (Sender Policy Framework) para determinar la autenticidad de cada mensaje. Cuando un mensaje no está autentificado, se pueden tomar medidas en función de las preferencias del propietario del dominio remitente. Las medidas pueden llegar incluso a rechazar el mensaje. Esta combinación de tecnologías la utilizan muy pocos, pero grandes, proveedores de servicios, así como numerosos servicios que producen un gran número de transacciones por correo electrónico (por ejemplo, confirmación de pedidos y compras).

Cuando se utiliza con DKIM, DMARC también impide el pirateo de prefijos de direcciones IP. Sin embargo, no está libre de problemas. Cuando se utiliza junto para otro tipo de mensajes diferentes a los de las transacciones (por ejemplo, entre personas), DMARC adolece de ciertos problemas de interoperabilidad[4]. Este es uno de los temas de trabajo del Grupo de Tareas sobre Ingeniería de Internet (IETF). Por otra parte, DMARC no es capaz de detectar la utilización de sistemas infectados, cuando éstos transmiten correo electrónico a través de sus proveedores de servicio normales. La clave para erradicar el spam es proteger los sistemas finales contra la infección.

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

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

Figura 13: Ruptura del círculo vicioso


Filtro spam
El spam es recibido por el servidor de correo
El dispositivo de usuario recupera el mensaje
Educación del usuario
El usuario pulsa el fichero adjunto
A/V y parches
El dispositivo queda infectado
Detección de intrusión
El dispositivo infectado transmite spam

2.1 Fuentes de spam

El círculo vicioso en las **Figuras 12** y **13** se ha desarrollado principalmente por la utilización de redes robot, que consisten en una combinación de dispositivos del consumidor y, en algunos casos, servidores de centros de datos que han sido infectados. Al menos una contribución previa manifestó inquietud acerca del riesgo generado por los dispositivos móviles. Cada tipo de dispositivo móvil está expuesto al riesgo de diferentes maneras, en función de su modelo operativo. El iPhone de Apple ha demostrado ser muy resistente a ataques, gracias a que exige la validación y firma digital de aplicaciones y supervisa sobremanera tanto la plataforma como las aplicaciones que se ejecutan con ella.

Otras plataformas plantean más problemas. A medida que se expande la utilización de las TIC y que crece la Internet de las cosas (IoT), se introducen nuevas plataformas en la red. Si contienen una CPU y están conectadas a la red, es posible que tengan vulnerabilidades. Poco antes de publicarse este Informe el gusano Mirai atacó la infraestructura DNS que bloqueó el sitio de una de las grandes redes sociales. Más directamente relacionado con el spam, Proofpoint demostró en 2013 una vulnerabilidad que podía hacer que refrigeradores, termostatos y alarmas contra robo generasen spam[5]. Este descubrimiento hace que sea aún más necesario que los fabricantes ofrezcan mecanismos de actualización automática del software que pueda reducir el riesgo de utilizar los dispositivos para tales fines.

2.2 Incidencia del spam en la red

Existen numerosos puntos para medir la incidencia del spam en la red, que van desde enlaces internacionales hasta lo que pasa a través de un teléfono celular por RF. En los últimos años se ha planteado la cuestión de cuánto ancho de banda consume realmente el spam en la red. Los mensajes de correo electrónico consumen muy poco, alrededor de 75 000 bytes en promedio.[6] Ahora bien, muchos mensajes son bastante más pequeños, pero el promedio se ve afectado por los ficheros adjuntos que, en principio, quizá no se descarguen. Si se dispone de filtros antispam adecuados, lo máximo que representa es de un 10 por ciento aproximadamente. Suponiendo el volumen estimado más grande de unos 259 mil millones de mensajes por día, con las soluciones antispam menos efectivas y considerando que unos 2 500 millones de personas están utilizando la red, cada persona recibiría sólo unos diez mensajes al día. Si no hubiera protección de ningún tipo, esta cifra se elevaría a 100

[5] http://www.economist.com/news/science-and-technology/21594955-when-internet-things-misbehaves-spam-fridge.
[6] http://email.about.com/od/emailstatistics/f/What_is_the_Average_Size_of_an_Email_Message.htm.

mensajes al día. Incluso con este volumen, el spam sigue siendo un consumidor minúsculo de la red, comparado con la voz, el vídeo y la navegación por la web. En general, las mediciones indican que todo el correo electrónico (spam inclusive) utiliza un ancho de banda desdeñable en las economías medidas.[7] La amenaza del spam no es tanto el ancho de banda que consume en la red, sino el riesgo de que los dispositivos infectados se utilicen para fines fraudulentos u otros ilícitos. La carencia de filtros decentes también degrada el valor del correo electrónico para el usuario.

2.3 Riesgos y mitigaciones de la peska

La peska (*phising*) es una forma de ataque en la que se envía un correo electrónico fraudulento al usuario destinatario que parece proceder de una fuente legítima y que contiene información personal suficiente como para hacer creer que el origen del mensaje es auténtico. Se insta al destinatario a hacer clic en un enlace web o abrir un fichero adjunto, momento en el que la máquina de la persona queda infectada. El coste para el atacante mediante la *peska* es considerablemente mayor que otros ataques menos específicos, porque para conocer información sobre los destinatarios se requiere cierta investigación. La investigación puede consistir en infiltrarse en los sistemas de una empresa o de un departamento gubernamental. El mecanismo más eficaz de protección contra la *peska* es educar al usuario.

2.4 Incidencia política en el spam

La reglamentación puede tener un efecto positivo y negativo sobre el spam. La utilización de un computador para enviar un mensaje fraudulento es fraude. Pero no se trata de un crimen nuevo, sino meramente una nueva forma de un delito muy antiguo. La legislación debe ser lo suficientemente flexible como para enjuiciar a las personas que cometen dicho fraude. En Estados Unidos, la Ley CAN-SPAM fue adoptada en 2003 para dejar claro que se trata de una conducta inadecuada. Sin embargo, identificar a los atacantes reales sigue siendo difícil. Las alianzas público-privadas entre proveedores de servicio y fuerzas de seguridad podrían mejorar la capacidad de identificar a los atacantes con el tiempo. Cuando el fraude conlleva un gasto monetario, es posible rastrear las transacciones a través de las redes financieras.

Por otra parte, impedir la recepción de spam exige que los intermediarios a menudo tengan acceso al contenido del mensaje para determinar si dicho contenido es seguro para el sistema final. Todo marco legislativo adecuado debe prever la protección de la red y sus usuarios.

La UIT sigue tratando de resolver los problemas del spam en colaboración con Internet Society. Durante este periodo de estudios, se celebró una fructífera reunión durante el Foro de la CMSI de 2016 sobre "Spam: comprender y mitigar las dificultades que afrontan las economías de Internet incipientes".[8] Los oradores incluyeron representantes de Cybersecurity Malaysia, Utilities and Competition Authority of Bahamas, ISOC, el Correlator para la Cuestión 3 de la CE 2 del UIT-D y Spamhaus. En la reunión se identificaron los siguientes problemas que hay que resolver:

- la necesidad de mejorar la cooperación mediante la armonización de los planes de acción eficaces de los Estados Miembros, dado que el spam es un problema colectivo que afecta a todos;
- el hecho de que si bien la conexión (a la banda ancha) es cada vez más asequible, quizá lo que no sea asequible es la protección (contra ciberataques);
- la necesidad de una legislación que estipule lo que es aceptable y lo que no, y la implantación de un mecanismo aplicable de sanciones para quienes lo infrinjan, sin que sea demasiado rígido

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

[8] Sesión del Foro de la CMSI 2016 sobre "*Spam: comprender y mitigar las dificultades que afrontan las economías de Internet incipientes*": https://www.itu.int/net4/wsis/forum/2016/Agenda/Session/152.

como para penalizar a otros actores, como las pequeñas y medianas empresas (PYME) que tratan de hacer campañas de comercialización;

- la compartición de prácticas y soluciones idóneas de listas de agujero negro y servicios de reputación con todos los Estados Miembros a través de la UIT.

3 CAPÍTULO 3 – Mejora de la postura nacional sobre la ciberseguridad: aumento de la sensibilización y cualificación de los recursos humanos

Esta sección trata el tema *c)* del mandato de la Cuestión 3/2, en el que se pide, entre otras cosas:

c) ***continuar recabando experiencias nacionales de los Estados Miembros en ciberseguridad e identificar y analizar los temas en común entre estas experiencias.***

Vivimos en un mundo cada vez más conectado y, aunque ello crea una oportunidad sin precedentes para la innovación y el crecimiento socioeconómico en todo el mundo, también hay problemas y amenazas de seguridad en el ciberespacio. Por otra parte, a medida que los problemas de seguridad evolucionan y afectan a diferentes sectores, los países encuentran cada vez más difícil encontrar soluciones para estos problemas.

A fin de resolver estos problemas, muchos países organizan campañas de sensibilización sobre ciberseguridad, con el fin de educar a gobiernos, sector privado, profesores y ciudadanos para determinar los posibles problemas y comprender las funciones y responsabilidades de cada uno para crear un ciberespacio más seguro. Durante el periodo de estudios, varias entidades facilitaron contribuciones sobre este asunto. Para más información, véase el **Anexo 2**, al Compendio de casos de estudio de país sobre ciberseguridad.

3.1 Campañas informativas

Un ejemplo de campaña informativa, Stop.Think.Connect.™, está destinada a aumentar la comprensión de las ciberamenazas y empoderar al ciudadano americano a estar en línea con mayor seguridad y protección. Tiene por finalidad divulgar el concepto de ciberseguridad como "una responsabilidad compartida" en la que cada individuo, con sólo unos pasos sencillos para estar más seguro en línea, hace que Internet sea una experiencia más segura para todos. Sus principales mensajes son los siguientes:

- **Detente**: Antes de utilizar Internet, hay que detenerse a comprender los riesgos y aprender a determinar los posibles problemas.
- **Piensa**: Tómate un momento para asegurarte de que el camino está despejado. Observa las señales de alerta y piensa cómo tus acciones en línea pueden repercutir en tu seguridad y en la de tu familia.
- **Conéctate**: Disfruta de Internet con mayor confianza, sabiendo que has tomado las medidas necesarias para salvaguardar tu seguridad y la del computador.
- **Detente. Piensa. Conéctate.** Protégete y ayuda a que la web sea un lugar más seguro para todos.

Esta sección consta de cuatro apartados, en los que se recomiendan las medidas y prácticas idóneas que se han de tomar al lanzar una campaña de sensibilización sobre ciberseguridad.

3.1.1 Prácticas idóneas para los programas de comunicación

Aunque las necesidades y dificultades en materia de protección y amenazas de ciberseguridad difieren según el país, las siguientes prácticas idóneas pueden contribuir a lanzar una campaña de sensibilización sobre ciberseguridad.

- **Elaboración de un plan de comunicaciones que incluya metas y objetivos bien definidos e identifique las principales audiencias destinatarias**. El primer paso antes de lanzar una campaña de sensibilización sobre ciberseguridad es determinar las metas y objetivos de la campaña y los principales destinatarios.

- **Desarrollar estrategias de comunicaciones y recursos específicos para llegar a los destinatarios deseados**. Las necesidades de ciberseguridad son distintas para cada persona. Por ejemplo, los estudiantes necesitan saber acerca de los ciberdepredadores mientras que los profesionales de IT tienen que estar al corriente de los piratas. Los diferentes tipos de materiales deben desarrollarse en función de las necesidades, los conocimientos y el nivel de capacidad de la audiencia destinataria.
- **Consejos útiles** adaptados a la audiencia específica y a sus únicas necesidades y amenazas particulares. El material didáctico exhaustivo, como la herramienta Stop.Think.Connect.™, subrayan la responsabilidad compartida para la ciberseguridad y, a su vez, garantizan que los recursos están disponibles para todos los segmentos de la comunidad. Recordatorios sencillos en la forma de cartel, brazalete, etc., ayudan a las personas a considerar prioritarias las prácticas idóneas en materia de ciberseguridad.
- **Utilización de medios sociales.** La mayoría de las campañas de ciberseguridad se llevan a cabo en línea. Los medios sociales pueden ayudar a llevar los mensajes de las campañas de ciberseguridad a las personas a través de los canales que ya están utilizando —y en algunos casos, los que prefieren utilizar. La publicación de información en redes sociales, como Facebook, Twitter y YouTube proporciona mecanismos para comprender y compartir información, al tiempo que reciben una valiosa aportación.
- Utilización de medios tradicionales: emisiones de radio y televisión, periódicos y revistas.
- **Crear y mantener alianzas con aliados en audiencias destinatarias.** Ninguna organización, ya sea gubernamental, privada o sin ánimo de lucro, puede por sí sola crear conciencia sobre la ciberseguridad. Por ese motivo, son fundamentales las alianzas entre los sectores público y privado. Crear y participar en alianzas con organizaciones tales como:

    a) *Organismos gubernamentales*. Los organismos gubernamentales infunden autoridad al mensaje y su alcance a personas y comunidades es amplio.

    Puede utilizarse un programa central para formar gobiernos locales y regionales que, a su vez, formarán a sus empleados y constituyentes para identificar y disuadir los peligros en línea. Los principales asociados gubernamentales a diversos niveles son los equipos de intervención ante incidentes de seguridad informática (EIISI), las oficinas del Jefe de Seguridad Informática (CISO) y las oficinas del Jefe de Información (CIO).

    b) *Organizaciones sin ánimo de lucro*. Las organizaciones sin ánimo de lucro ofrecen diversos recursos y flexibilidad para difundir el mensaje de sensibilización sobre ciberseguridad.

    Los asociados sin ánimo de lucro comprenden todos los grupos de audiencia identificados en el plan estratégico. Las solicitudes periódicas que incluyen a todas las organizaciones asociadas ayuda a construir redes entre cada organización, ya sea pública o privada.

    c) *Instituciones académicas*. Las instituciones académicas contribuyen con su importante y moderna investigación a garantizar que la campaña esté basada en información y fidedigna. También ofrecen acceso a la futura fuerza laboral de la nación. Las alianzas con escuelas de primaria y de secundaria fomentan la educación sobre ciberseguridad desde una edad temprana ayudan a sus estudiantes a utilizar Internet de manera segura a lo largo de sus vidas. La colaboración con universidades y centros de excelencia establece relaciones entre la fuerza laboral en formación y las organizaciones que las utilizan en el futuro.

    d) *Organizaciones del sector privado*. Los líderes industriales, por ejemplo, los servicios de información, minoristas, de finanzas y educación, pueden educar a sus empleados, consumidores y otras audiencias sobre las amenazas que les afectan y recibir información sobre el refuerzo de las prácticas de ciberseguridad. Las soluciones de ciberseguridad innovadoras desarrolladas por organizaciones del sector privado pueden orientar sobre prácticas idóneas tanto al sector público como al privado.

- **Implicar a las audiencias a nivel individual mediante esfuerzos colectivos.** La sensibilización del ciudadano es fundamental para que los programas de sensibilización sobre ciberseguridad sean eficaces.

La campaña Stop.Think.Connect.™, por ejemplo, invita al ciudadano a convertirse en "*amigo de la campaña*" mediante la firma de boletines mensuales por correo electrónico sobre los últimos ciberconsejos, noticias e información pertinente. La campaña también consigue expandir su alcance mediante eventos ajustados a cada audiencia e implicando a oradores que pueden exponer los problemas de ciberseguridad que más afectan a dicha audiencia.

- **Determinar si los esfuerzos están realmente sensibilizando a las audiencias destinatarias.** A fin de determinar la eficacia de una campaña, es importante recabar la opinión de grupos temáticos, de estudios y otros métodos. Además, conviene conocer las páginas web más visitadas, el material que más se descarga, los eventos con mayor acogida, y las prácticas que se consideran más eficaces para determinar el éxito y fomentar las mejoras. La opinión de organizaciones asociadas ayuda a que la futura planificación se concentre en la eficacia y la creatividad.

3.1.2 Plan de comunicaciones de ejemplo

Disponer de un plan de comunicaciones es un componente fundamental para que las campañas tengan éxito y constituye una hoja de ruta sobre cómo la organización tiene previsto cumplir sus principales metas y objetivos. Si bien el plan de comunicaciones debe estar adaptado a las necesidades específicas de la organización, muchos planes incluyen lo siguiente:

Finalidad y antecedentes

En la sección relativa la finalidad y los antecedentes se articulan los motivos por los que la organización ha creado un plan de comunicaciones y lo que pretende conseguir.

Metas generales de las comunicaciones

Las metas generales de las comunicaciones constituyen los objetivos generales del programa de sensibilización sobre ciberseguridad. Dichas metas son estratégicamente amplias. Por ejemplo:

A fin de promover la sensibilidad pública sobre la ciberseguridad mediante el aumento del nivel de comprensión de las ciberamenazas, las medidas sencillas de mitigación y empoderar al público para que esté más preparado en línea:

- aumentar el nivel de conocimientos de ciberseguridad y su relación con la seguridad nacional y de nuestras vidas privadas;
- implicar a los sectores público y privado y a los gobiernos regionales en las actividades para mejorar la ciberseguridad;
- elaborar y comunicar métodos y estrategias para que los ciudadanos, sus familias y comunidades estén más seguros en línea.

Objetivos de las comunicaciones

Los objetivos de las comunicaciones describen cómo permitirá la campaña alcanzar sus metas generales. Estos objetivos deben ser cuantificables.

Por ejemplo, las metas anteriores se traducen en los siguientes objetivos:

- educar al público sobre prácticas de ciberseguridad para protegerse y garantizar que los grupos de interesados sean conscientes de los recursos disponibles;

- aumentar el número de grupos de interesados implicados y consolidar las relaciones existentes con los gobiernos regionales, el sector privado, las entidades sin ánimo de lucro, los sistemas escolares y los educadores;
- aumentar y reforzar la fuerza laboral cibernética mediante el fomento de la ciencia, la tecnología, la ingeniería y la enseñanza de las matemáticas (STEM).

Principales audiencias destinatarias

Identificar las audiencias ayuda a garantizar que los mensajes estén más orientados a los más receptivos o a quienes más lo necesitan. Definir claramente dichas audiencias ayuda a que los mensajes estén mejor orientados a grupos específicos mediante una comprensión común de lo que significa dicha audiencia.

Canales de comunicación

Los canales de comunicación son los diversos medios para transportar mensajes a las audiencias destinatarias. Examinar meticulosamente todos los mecanismos de comunicación utilizados y los métodos adicionales que puedan utilizarse para su utilización. El plan de comunicaciones debe especificar claramente cuáles son los canales y cómo utilizarlos.

Por ejemplo:

- Eventos: Celebrar eventos con los grupos de audiencia destinatarios.
- Medios tradicionales: La divulgación proactiva por medios nacionales/regionales/locales (por ejemplo, radiodifusión, impresos, web).
- Medios sociales: Utilización activa de plataformas de medios sociales (bitácoras oficiales, Facebook, Twitter).
- Boletines: Distribuir un boletín mensual y herramientas informativas.
- Sitios web: Actualización periódica de los sitios web de campañas con noticias, consejos e información fundamental.
- Asociados: Fomentar la divulgación desde organizaciones asociadas.

3.1.3 Estrategias de la campaña

Las estrategias de la campaña tienen en cuenta tanto los métodos prácticos de divulgación de información como los mecanismos para crear impulsar y fomentar el crecimiento de la campaña. Cada estrategia general contiene muchos pasos para llevarla a buen término, y tanto los pasos como las estrategias deben ser lo suficientemente flexibles como para adaptarse al entorno cambiante. Por ejemplo, las siguientes estrategias se han utilizado para cumplir los objetivos de comunicaciones de programas:

- divulgar el mensaje de la campaña en eventos y medios (sociales y tradicionales);
- crear un cuadro de mensajeros mediante alianzas con entidades sin ánimo de lucro y de base popular;
- colaborar con organismos gubernamentales en los eventos y la divulgación del mensaje.

Divulgación del mensaje

La divulgación de mensajes atractivos debe concentrarse en los mensajes básicos y principales que se pretende divulgar en la campaña. Cada país y cada campaña –así como cada audiencia y evento– tiene necesidades específicas que requieren ajustar el mensaje. La divulgación de los mensajes atractivos sirve de base para cada una de esas necesidades personalizadas.

Por ejemplo, los mensajes atractivos de la campaña Stop.Think.Connect son:

- **Detente**: Antes de utilizar Internet, hay que detenerse a comprender los riesgos y aprender a determinar los posibles problemas.
- **Piensa**: Tómate un momento para asegurarte de que el camino está despejado. Observa las señales de alerta y piensa cómo tus acciones en línea pueden repercutir en tu seguridad y en la de tu familia.
- **Conéctate**: Disfruta de Internet con mayor confianza, sabiendo que has tomado las medidas necesarias para salvaguardar tu seguridad y la del computador.
- **Detente. Piensa. Conéctate.** Protégete y ayuda a que la web sea un lugar más seguro para todos.

Otros mensajes universales son: utiliza contraseñas seguras, mantén actualizados el sistema operativo y el software de seguridad, conéctate sólo con personas de tu confianza y evita los sitios web que parecen demasiado buenos para ser verdad.

Funciones y responsabilidades

Designar claramente las funciones y responsabilidades permite a los equipos colaborar eficazmente y, a su vez, impedir duplicación o confusión de tareas. Estas diferencias se producen entre organizaciones cuando diversos grupos dan soporte a una campaña, así como entre miembros del equipo de una determinada organización.

Recursos

Enumerar los recursos disponibles para una campaña también aclara el alcance y limitaciones de las actividades divulgativas dentro de un plazo determinado. En esta sección, el autor puede indicar el número de empleados y materiales que la organización tiene disponibles para las audiencias destinatarias específicas dentro de un determinado plazo.

Problemas de comunicación

La identificación de los problemas de comunicación previstos puede ayudar a superar deficiencias y obstáculos. En los ejemplos se puede citar:

- para las audiencias resulta difícil comprender los aspectos técnicos de las ciberamenazas y su la relación entre ambos; y
- la población en general no considera necesariamente que las ciberamenazas sea reales o importantes en su vida cotidiana.

3.1.4 Medición del éxito y métrica

Todo plan de comunicaciones necesita una forma de recibir opiniones y medir su eficacia. Debido a la naturaleza de las campañas de sensibilización sobre la ciberseguridad, las mediciones se suelen concentrar en actividades externas más que en contribuciones, pero conocer la opinión oportunamente resulta esencial. Los ejemplos incluyen:

- número de participantes en cada evento o serie de eventos en la región;
- cantidad de material publicitario distribuido;
- cobertura por los medios de comunicación;
- número de interesados participantes (por ejemplo, amigos, miembros de la Coalición de Conciencia Cibernética, miembros de la red nacional, etc.);
- número de visitas de la página web;
- opiniones y testimonios de los participantes y organizaciones asociadas;

– opinión de los órganos legislativos, el estado y los líderes/funcionarios locales.

Métrica

La métrica se clasifica en varias categorías generales. La forma en que se aplican estos tipos de categorías a los diferentes programas de sensibilización sobre ciberseguridad depende de las metas y recursos del programa del caso. **Implicación de los actores** trata de las alianzas oficiales con los organismos gubernamentales y organizaciones sin ánimo de lucro. **Divulgación por medios de comunicación tradicionales** y **Divulgación digital y en línea** se aplica, cada una, a la distribución de productos escritos y multimedios por los canales de comunicación establecidos. **Eventos y foros** y **recursos** guardan relación con las interacciones entre personas. Se requiere una combinación de métrica para comprender y medir el pleno alcance de la campaña.

3.2 Medidas adicionales de capacitación

3.2.1 Actividades en Japón

El Ministerio de Asuntos Internos y Comunicaciones (MIC) de Japón ha creado un proyecto de alianza público-privada, ACTIVE (**A**dvanced **C**yber **T**hreats response **I**nitiati**VE**), destinado a ayudar a los usuarios de Internet a prevenir la infección de malware y mitigar los daños cuando ésta se produce. La alianza consta de MIC, proveedores de servicios Internet (ISP) y proveedores de seguridad. Estas iniciativas han dado lugar a una disminución del número de infecciones de malware.

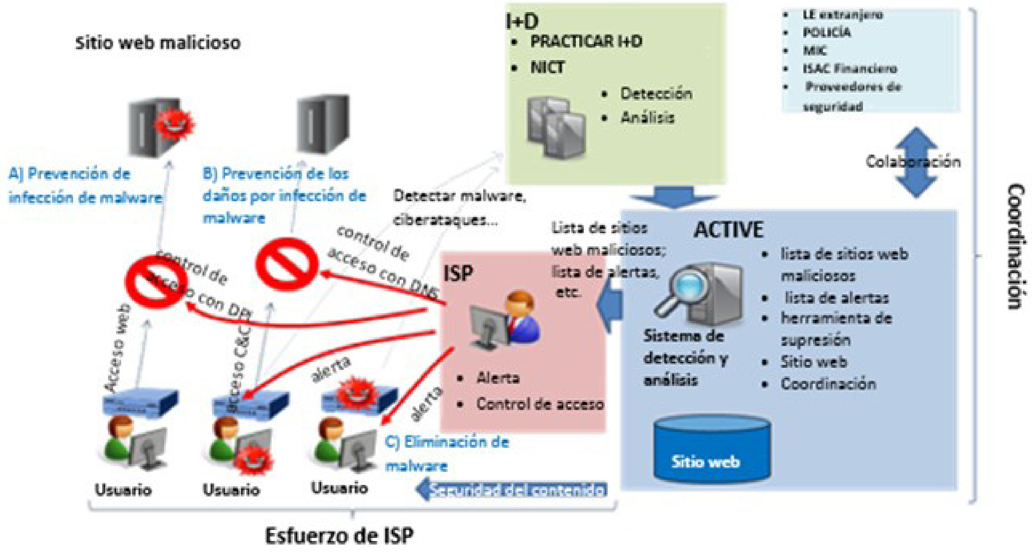
Entre las principales actividades se cuentan las siguientes:

– Prevenir la infección de malware; cooperar con los ISP.

– Prevenir los daños por infección de malware; cooperar con los ISP.

– Eliminar malware; cooperar con los ISP.

Figura 14: Descripción de las actividades de ACTIVE


Sitio web malicioso
A) Prevención de infección de malware
B) Prevención de los daños por infección de malware
Detectar malware, ciberataques...
control de acceso con DPI
control de acceso con DNS
Acceso web
Acceso C&C
alerta
alerta
ISP
• Alerta
• Control de acceso
C) Eliminación de malware
Usuario
Usuario
Usuario
Seguridad del contenido
Esfuerzo de ISP
I+D
• PRACTICAR I+D
• NICT
• Detección
• Análisis
• LE extranjero
• POLICÍA
• MIC
• ISAC Financiero
• Proveedores de seguridad
Colaboración
Lista de sitios web maliciosos; lista de alertas, etc.
ACTIVE
Sistema de detección y análisis
• lista de sitios web maliciosos
• lista de alertas
• herramienta de supresión
• Sitio web
• Coordinación
Sitio web
Coordinación

Eficacia de ACTIVE

Según los datos estadísticos del 23 mayo de 2016, desde que comenzara a funcionar ACTIVE se han enviado 286 alertas a los usuarios para impedir infección de malware, 320,267 servidores C&C se bloquearon para impedir daños y 1 878 alertas se enviaron a los usuarios para eliminar malware.

Además de su funcionamiento básico, ACTIVE ha desempeñado un importante papel en las operaciones de suspensión organizadas por las fuerzas de seguridad de todo el mundo. ACTIVE recibió una lista de malware, como Game over Zeus, VAWTRAK, etc., de las fuerzas de seguridad y distribuyó la lista a los ISP participantes para facilitar la eliminación del malware.

3.2.2 Actividades en la República de Corea

La República de Corea ha desarrollado un plan nacional que consta de cuatro partes. El primer componente consiste en mejorar la estructura de la industria de seguridad de la información mediante la conversión a un mercado basado en el rendimiento, y la introducción de un sistema adecuado para pagar precios justos por los servicios de seguridad de la información. Esto incluye un sistema para evaluar el precio justo del servicio de continuidad de la seguridad de la información, que garantiza un rendimiento de seguridad adecuado de los productos afines.

Por otra parte, los gobiernos pueden utilizar incentivos para invertir en seguridad, como dar preferencia a la hora de la contratación pública y gubernamental y en I+D, para alentar a las empresas a invertir voluntariamente en seguridad y tomar las medidas oportunas. Otro método consiste en identificar y fomentar empresas incipientes de seguridad de la información a través del apoyo, por ejemplo compartiendo información sobre vulnerabilidades de seguridad, bancos de pruebas y certificación internacional de modo que las ideas brillantes en materia de seguridad culminen en empresas viables.

3.2.3 Actividades en la Región CEI

La Federación de Rusia presentó una contribución[9] en la que se presentan los resultados de un proyecto de Iniciativa Regional CEI para la capacitación en materia de seguridad de la información. En el proyecto se reconoce que hay una urgente necesidad de capacitación de los recursos humanos para mejorar la confianza y la seguridad en la utilización de las TIC, para lo que se requiere una asociación comercial como cliente, el sistema educativo como contratante y el Estado como regulador de todo el proceso.

En el marco del proyecto de Iniciativa Regional CEI se desarrollaron competencias profesionales normalizadas que, como indica la Federación de Rusia en su contribución, son fundamentales para crear programas educativos de formación puntual y continua de los especialistas en seguridad de la información. Esas competencias son:

1) Competencias profesionales generales, incluida la capacidad de:
   - operar sistemas de infocomunicaciones (SIC) utilizando métodos y medios para garantizar su seguridad;
   - administrar el software y el hardware de protección de la información de SIC;
   - evaluar la seguridad del SIC; y
   - crear SIC protegidos distribuidos.
2) Competencias en la explotación de SIC utilizando software y herramientas de seguridad, incluida la capacidad de:
   - aportar seguridad de la información al SIC con software y hardware;
   - aportar seguridad de la información al SIC por medios técnicos; y
   - aportar seguridad de la información al SIC mediante una aplicación compleja de recursos técnicos, software y hardware.

[9] Documento 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”, Federación de Rusia.

3) Competencias en la gestión de software y hardware de protección de la información en el SIC, incluida la capacidad de:
   - configurar el software y el hardware de protección del SIC;
   - realizar el mantenimiento periódico y las reparaciones puntuales necesarias del software y el hardware de protección de la información; y
   - analizar las infracciones consentidas por los usuarios en el SIC y evitar su repetición.
4) Competencias en la evaluación de la seguridad del SIC:
   - la supervisión de la eficiencia y la eficacia del hardware y el software de protección de la información;
   - la aplicación de métodos y técnicas de evaluación de la seguridad del SIC en el marco del análisis de control del sistema de protección;
   - realizar investigaciones y experimentos para la certificación de objetos, habida cuenta de la necesidad de garantizar la protección del SIC;
   - supervisión instrumental de la protección del SIC; y
   - conocimientos avanzados de investigación de incidentes de seguridad.
5) Competencias en materia de diseños de SIC protegidos distribuidos:
   - definición de los requisitos para un SIC seguro distribuido y de la manera de satisfacerlos, habida cuenta de los reglamentos y directrices existentes;
   - diseño de SIC protegido distribuido; y
   - cuidado y mantenimiento de SIC distribuidos con los recursos de protección de la información y las medidas orgánicas y técnicas para la seguridad de la información.

3.2.4 Actividades en Noruega

Noruega presentó su experiencia nacional en un estudio para definir las prácticas de ciberseguridad efectivas y mejorar la ciberresiliencia nacional.[10] El Centro Noruego de Ciberseguridad (NorSIS) ha realizado un estudio en profundidad de la cultura de ciberseguridad de Noruega. El estudio pretende sentar los cimientos de las prácticas de ciberseguridad efectivas y mejorar la ciberresiliencia nacional. Se incluyó en el estudio un método para medir la cultura de ciberseguridad, así como una gran encuesta nacional. NorSIS publicó recientemente el Informe "La cultura de la ciberseguridad en Noruega", en el que se incluye una descripción completa del método y se presentan las principales conclusiones del estudio nacional.

3.3 Alianzas público-privadas

Durante el ciclo de estudios, la Cuestión recibió varias contribuciones de los Estados Miembros relativas a la importancia de la cooperación entre gobierno e industria y de las alianzas público-privadas. Los Estados Miembros observaron que gestionar los ciberriesgos de la infraestructura esencia es una tarea extremadamente compleja pero de vital importancia, y que cualquier gobierno o entidad del sector privado no suele tener la capacidad para resolver, por cuenta propia, los problemas de ciberseguridad.

El **Reino Unido de Gran Bretaña e Irlanda del Norte** presentó una contribución[11] sobre ciberseguridad en el gobierno y la industria en la que se describe el método denominado fundamentos básicos cibernéticos. El método se desarrolló tras analizar varios ciberataques. El análisis indicó que

[10] Documento SG2RGQ/204, "Creating a metric for cyber security culture", Noruega.

[11] Documento 2/228, "Cybersecurity in government and industry", Reino Unido de Gran Bretaña e Irlanda del Norte.

en muchos casos unas cuantas precauciones hubieran bastado para mitigar el ataque o ponérselo más difícil al adversario. Los fundamentos básicos cibernéticos lo desarrollaron conjuntamente el Gobierno del Reino Unido y el sector privado con el fin de cumplir dos funciones. En primer lugar, estipular claramente los controles básicos que deben aplicar todas las organizaciones para reducir el riesgo de amenazas comunes por Internet, en el contexto de los 10 pasos para la ciberseguridad, definidos por el Gobierno. En segundo lugar, el marco de garantías, que ofrece a las organizaciones un mecanismo para demostrar a clientes, inversores, aseguradoras y otras partes que han tomado las precauciones esenciales. Si bien el desarrollo se concibió para el Reino Unido, buena parte de la labor realizada es igualmente aplicable a cualquier país y los detalles del método están disponibles para todos. Los fundamentos básicos cibernéticos han resultado ser muy satisfactorios en el Reino Unido, donde cientos de organizaciones se han certificado a pesar de que el método es relativamente nuevo.

Por otra parte, los Estados **Unidos de América** presentaron una contribución[12] relativa a la asociación con el sector privado para gestionar los ciberriesgos. En su contribución, los Estados Unidos ponen de relieve que las alianzas público-privadas son un componente fundamental para la protección eficaz de la infraestructura pública esencial, la resiliencia y la gestión general de los ciberriesgos. En la contribución se subraya la importancia de asociarse con el sector privado para gestionar los ciberriesgos; se exponen los métodos de gestión de riesgos de los Estados Unidos basados en el conjunto de la comunidad, se describen las principales herramientas para este enfoque y se dan ejemplos concretos de alianzas público-privadas eficaces.

La importancia de la colaboración del gobierno con empresas del sector privado también es un tema destacado en la contribución de **Japón**,[13] relativo a la compartición de conocimiento, información y prácticas idóneas para crear una cultura de ciberseguridad. En su contribución, Japón indica cuatro aspectos de los que se ocupa, a saber "red", "individuos", "tecnología" y "alianzas y colaboración internacionales" para garantizar la fiabilidad de las redes de la información y la comunicación. Desde el punto de vista de la "red", Japón ha instado a compartir información entre operadores de telecomunicaciones. Por ejemplo, en 2002, 19 importantes ISP y operadores de telecomunicaciones en Japón lanzaron voluntariamente el Centro Telecom-ISAC (Centro de análisis y compartición de información) de Japón[14] que acopia análisis y comparte entre los miembros información sobre seguridad, por ejemplo vulnerabilidades, incidentes, contramedidas y prácticas idóneas. Desde el punto de vista "individual", Japón ha realizado compañas de sensibilización para usuarios de Internet en sitios web, seminarios etc. Desde el punto de vista de la "tecnología", Japón ha fomentado la investigación avanzada y el desarrollo de proyectos, tales como el proyecto PRACTICE. Al tomar en consideración estos aspectos, Japón ha contribuido a establecer redes TIC fiables y a promover la cooperación internacional.

[12] Documento 2/198, "Asociación con el sector privado para la gestión del ciberriesgo", Estados Unidos de América.
[13] Documento 2/90, "Partnering with the Private Sector to Manage Cyber Risk", Japón.
[14] https://www.telecom-isac.jp/english/index.html.

4 CAPÍTULO 4 – Protección de la infancia en línea (PIeL)

Esta sección trata del tema *h)* del mandato de la Cuestión 3/2 que pide, entre otras cosas*:*

h) ***Seguir recabando experiencias y necesidades nacionales en el campo de protección de la infancia en línea, de forma coordinada con otras actividades relevantes.***

En una contribución,[15] se aborda al mismo tiempo el mandato del tema g) de la Cuestión 3/2, a saber:

g) ***Examinar los medios para asistir a los países en desarrollo, haciendo hincapié en los países menos adelantados (PMA), en lo que concierne a las dificultades en materia de ciberseguridad.***

En la era de Internet de hoy en día la seguridad en línea es un tema importante, especialmente la utilización segura y sin riesgos de Internet por los niños. Los niños tienen necesidades y vulnerabilidades específicas en lo que respecta a la seguridad en línea, comparado con los adultos, y es preciso reconocer esa diferencia.

Los niños pasan cada vez más tiempo en Internet y jugando con computadores. Los medios sociales son los más utilizados a este respecto. A veces los padres no son conscientes de que sus hijos comparten información personal cuando utilizan los medios sociales, lo que los hace posibles presas de los depredadores en línea.

A fin de resolver estos problemas muchos países organizan campañas de sensibilización destinadas a educar a organismos gubernamentales, sector privado, profesores y ciudadanos (padres y niños) acerca de los posibles problemas y hacerles comprender sus funciones y responsabilidades en la creación de un ciberespacio apto para niños.

4.1 Resultados de la encuesta sobre protección de la infancia en línea

El cuestionario sobre Protección de la infancia en línea (PIeL), que incluye preguntas formuladas en las contribuciones de los Estados Miembros (concretamente, Australia, Reino Unido y Vanuatu), aborda diversas cuestiones relevantes, en particular los aspectos legislativos y estratégicos de la PIeL, los métodos para informar sobre incidentes y las salvaguardias técnicas. Respondieron al Cuestionario PIeL 131 países. Los resultados muestran que sólo 37 de los 131 países que respondieron confirman disponer de una estrategia nacional sobre PIeL. Asimismo, observamos que 101 países disponen medidas de protección de la infancia en línea. Si bien un elevado porcentaje de los países que respondieron aplican medidas PIeL, sólo 78 países han promulgado legislación sobre este particular, mientras que otros países que carecen de este tipo de legislación aplican otras medidas como salvaguardias técnicas para la protección de la PIeL.

Por otra parte, 69 de los 131 que respondieron cuentan con organismos gubernamentales encargados de la PIeL. Sin embargo, es evidente la diferencia entre el número de países que han creado entidades u organismos para PIeL y los países que carecen de dichas entidades. El número de países con entidades encargadas de la protección de la infancia es claramente mayor. Aunque estas entidades están disponibles en 69 países, sólo 63 disponen de un sistema sólido para informar sobre casos relacionados con PIeL.

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

Figura 15: ¿Existe una agencia o entidad encargada de la protección de la infancia en línea?

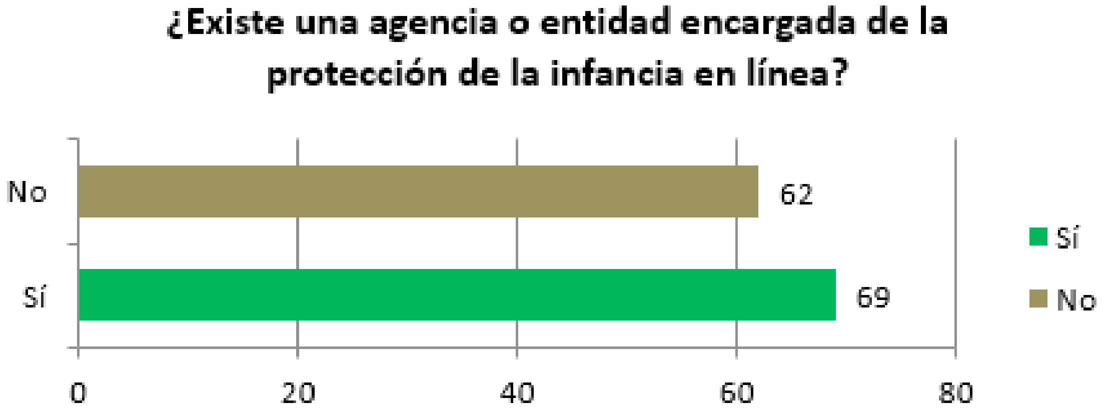
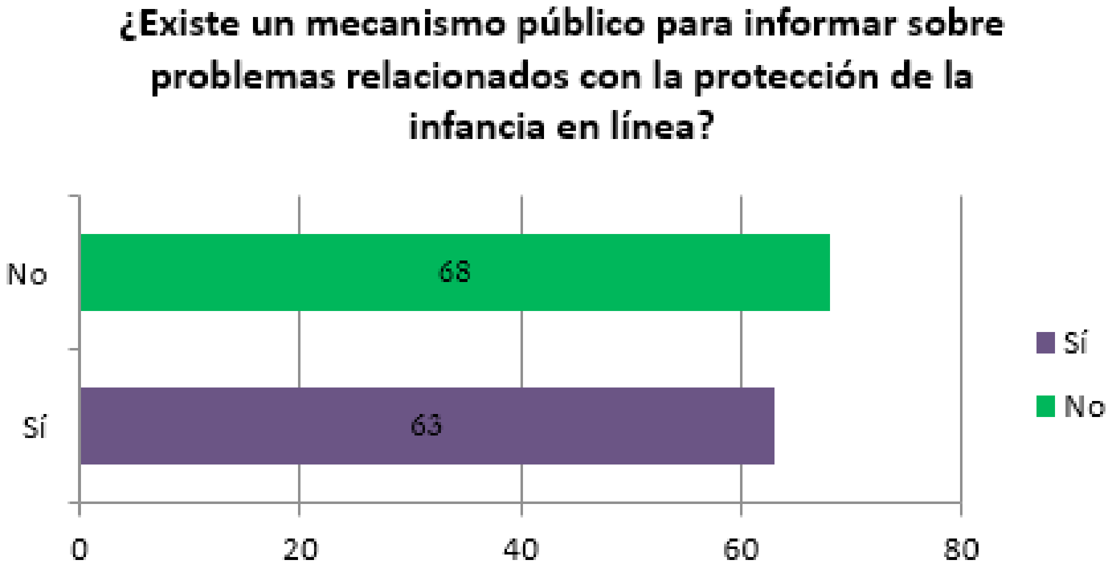
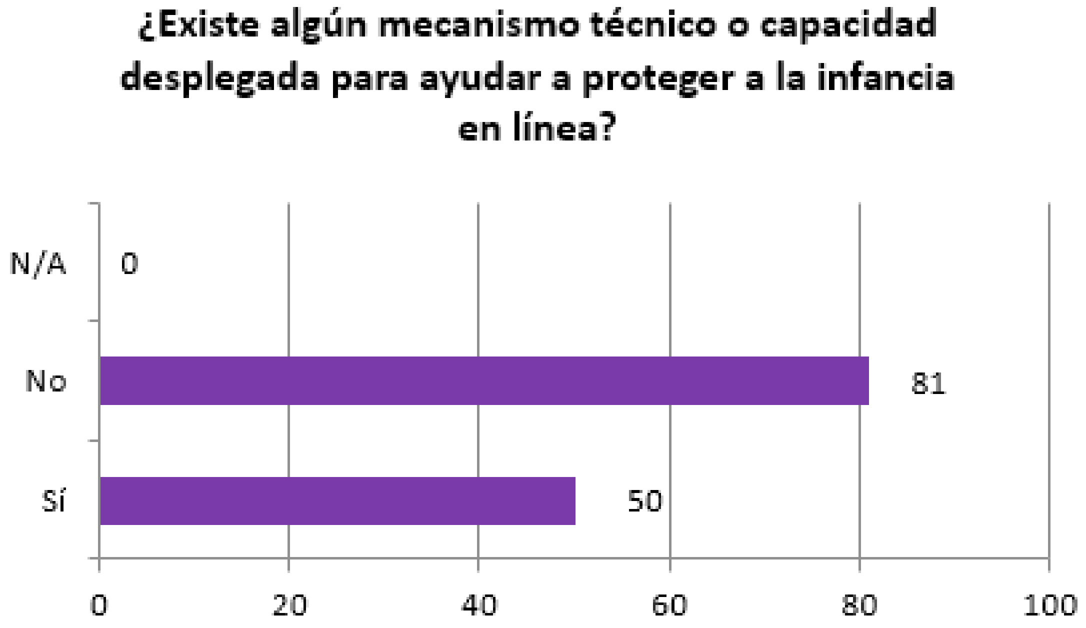


Figure 16: ¿Existe un mecanismo público para informar sobre problemas relacionados con la protección de la infancia en línea?



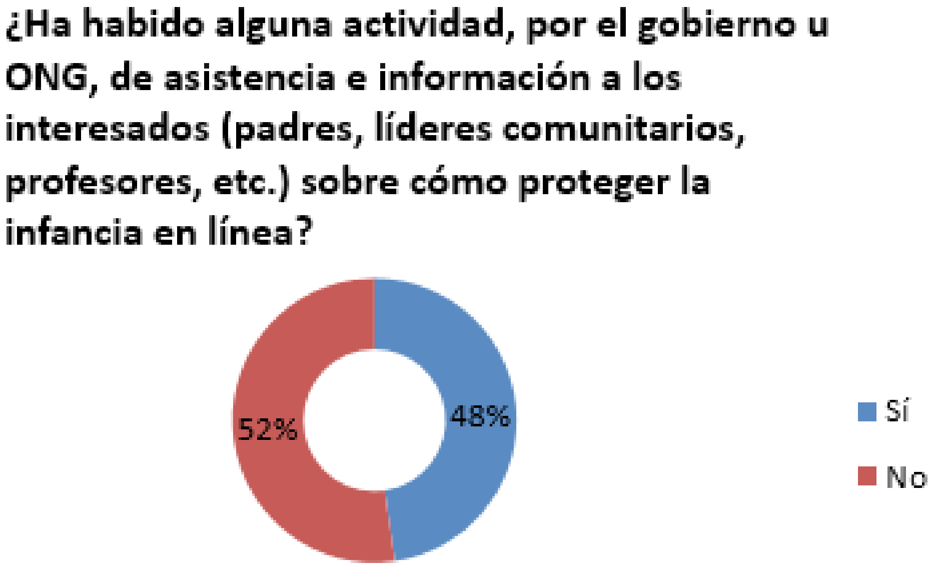
Cincuenta de estos países disponen de capacidades técnicas para ayudar en la PIeL, lo que puede plantear cuestiones sobre los organismos creados para la PIeL, la naturaleza de su campo y las tareas asignadas, o la novedad de estos organismos es el motivo por el cual carecen de un sistema de notificación o capacidades técnicas para ayudar en la PIeL. Esto podría deberse a que estos organismos están especializados en asuntos relacionados con la infancia, pero no concretamente sobre la PIeL. Esto hace que se concentren menos en los riesgos que pesan sobre los niños en línea, ya que también presta atención a otros riesgos de la infancia en general.

Figura 17: ¿Existe algún mecanismo técnico o capacidad desplegada para ayudar a proteger a la infancia en línea?



En lo que respecta a las actividades realizadas por organizaciones gubernamentales y no gubernamentales de asistencia e información a los distintos actores sobre los métodos de la PIeL, los resultados del Cuestionario muestran que 62 países están implicados en tales actividades, mientras que 68 no, por lo que los resultados están relativamente equilibrados.

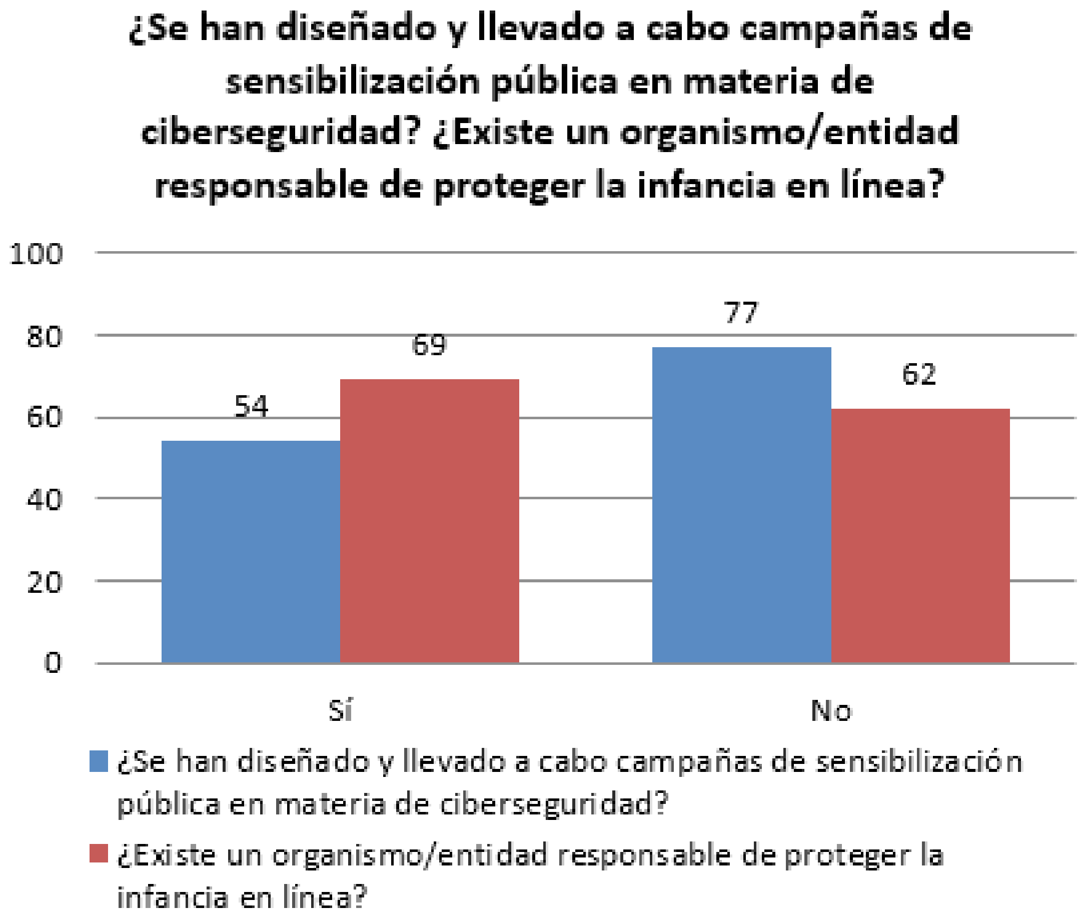
Figura 18: ¿Ha habido alguna actividad, por el gobierno u ONG, de asistencia e información a los interesados (padres, líderes comunitarios, profesores, etc.) sobre cómo proteger la infancia en línea?



Como la PIeL no puede resolverse sin destacar el papel de la educación en la divulgación de una cultura sobre este tipo de protección entre las partes interesadas, y como la PIeL se analizó en la **Sección 2**, que versa sobre la sensibilización sobre ciberseguridad como elemento fundamental integrante de la ciberseguridad, en esta sección se examina con mayor detalle el papel de la educación sobre la PIeL y la sensibilización de padres y profesores con el fin de determinar los puntos débiles a los que se prestó plena atención.

Una pregunta que plantea la función de la educación en la protección de la infancia en línea era una pregunta general sobre si los Estados Miembros han adoptado o no programas para proteger la infancia en línea. Los resultados muestran que sólo 54 de los 131 países disponen de tales programas.

Figura 19: ¿Se han diseñado y llevado a cabo campañas de sensibilización pública en materia de ciberseguridad? ¿Existe un organismo/entidad responsable de proteger la infancia en línea?



Cabe señalar que la existencia de entidades interesadas en la PIeL en un determinado país no significa que dichas entidades cumplan dicha función educativa. Además, la falta de entidades especializadas en la PIeL no significa que el país no pueda llevar a cabo su función educativa, como queda demostrado por el hecho de que estas entidades están disponibles en 69 países pero no todos ellos han adoptado programas educativos para proteger a la infancia en línea. Aunque 62 países carecen de entidades especializadas en la PIeL, algunos ya han diseñado y puesto en marcha programas de sensibilización sobre esta protección.

Al analizar más detenidamente la naturaleza de dichos programas educativos y sus grupos destinatarios se observa que el grupo al que van más dirigidos esos programas son los niños, ya que 52 países confirmaron que han adoptado programas de educación para niños, mientras que 78 países no disponen de programas específicos para niños.

Los resultados del cuestionario muestran que 50 de los 131 países han creado programas educativos para padres, siendo los profesores el grupo menos beneficiado, ya que sólo 47 de los 131 países disponen de programas educativos para profesores.

En lo que respecta a las campañas de sensibilización, 84 de 131 países, es decir el 64,12 por ciento, han llevado a cabo campañas de sensibilización concebidas especialmente para la PIeL. Este resultado coincide con los resultados en los que se solicita definir asuntos prioritarios de los Estados Miembros en cuanto a la ciberseguridad, ya que la PIeL ocupa el segundo lugar en las respuestas de los Estados Miembros, después de la seguridad de Internet, y el primer lugar sobre los asuntos que han de ser objeto de campañas de sensibilización.

Figura 20: Campañas de sensibilización pública sobre la protección de la infancia en línea dirigidas a los niños

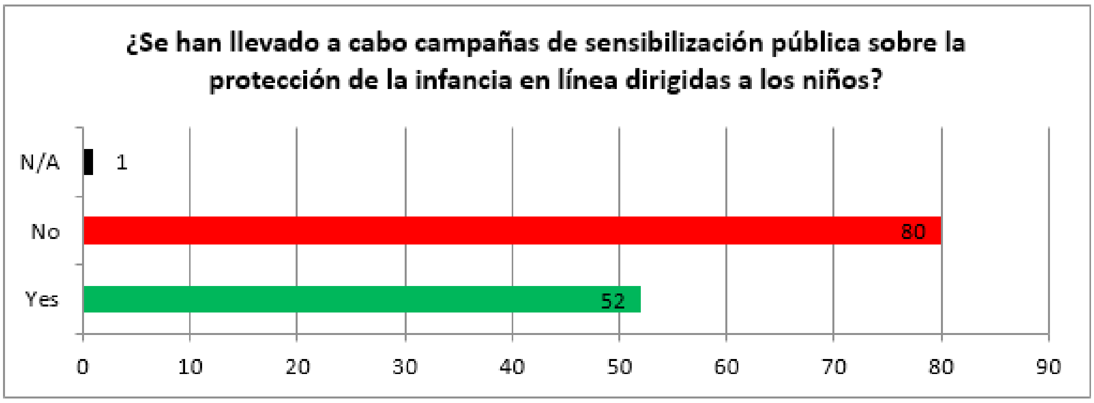
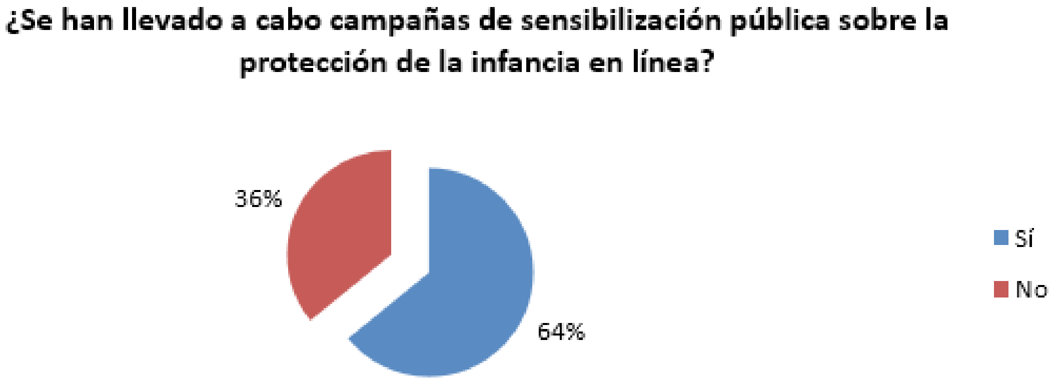


Figura 21: Campañas de sensibilización pública sobre la protección de la infancia en línea



77 países han adoptado programas de sensibilización destinados exclusivamente a niño, mientras que sólo 54 países no destinaron este tipo de programas específicamente a niños. De las respuestas al cuestionario se desprende que el grupo de adultos se ha beneficiado en una justa proporción de programas educativos o de sensibilización para la protección de la infancia en línea, ya que 74 países confirmaron disponer de este tipo de programas dirigidos a adultos, y 57 países indicaron que carecen de estos programas. Habida cuenta de lo anterior, es importante destinar los programas tanto a adultos como a niño. Es imposible lograr una plena conciencia si no se engloba a los diferentes estratos de la sociedad que están directa o indirectamente relacionados con la PIeL. La sensibilización de los niños sobre los posibles riesgos en línea no es suficiente si no se sensibiliza también a los adultos sobre tales riesgos y las medidas que es necesario adoptar para garantizar la protección de la infancia en línea.

4.2 Estrategias de protección de la infancia en línea y soluciones técnicas

En las contribuciones recibidas durante el periodo de estudios de la Cuestión 3/2 de la Comisión de Estudio 2 se identificaron posibles estrategias y soluciones técnicas. Como se indica en diferentes documentos, la colaboración entre los diferentes interesados, las campañas de sensibilización, la participación de la industria y los esfuerzos legislativos podrían ayudar a definir estrategias y políticas sobre la seguridad de la infancia en línea. En primer lugar, pasar de la estrategia a la acción es un proceso largo que comienza con la recopilación de información pertinente. En una contribución[16] del Reino Unido, Australia y Vanuatu a la reunión de la Comisión de Estudio 2 del UIT-D el mes de septiembre de 2014, se propone un plan de acción para ayudar a los Estados Miembros en la protección de la infancia en línea (PIeL). Basándose en dicha contribución, estos países propusieron de consuno varias preguntas que habría que formular a los Estados Miembros para comprender más cabalmente cómo está comprometida a nivel nacional con la PIeL. En segundo lugar, el desarrollo de soluciones técnicas nunca es un proceso estático, sino un proceso dinámico que exige la reflexión y adaptación constantes. Por ejemplo, tras las deliberaciones en la reunión del Grupo de Relator sobre la Cuestión 3/2 en 2015, **Australia, Papua Nueva Guinea, el Estado Independiente de Samoa, el Reino Unido y la República de Vanuatu**[17] propusieron preguntas modificadas sobre la protección de la infancia en línea. Se sugirió transmitir estas preguntas a la Plenaria de la Comisión de Estudio para su distribución a los Estados Miembros, ya sea de manera independiente o integrada en un cuestionario más detallado. Las preguntas se centran en las actividades relacionadas con la PIeL a nivel nacional, en particular en la legislación, mecanismos de notificación, capacidades y asistencia e información a las partes interesadas. Por otra parte, de conformidad con la Resolución 67 (Rev. 2014, Dubái)[18] de la CMDT, el Reino Unido, Australia y la República de Vanuatu presentaron conjuntamente un informe técnico titulado "Prácticas idóneas para padres en materia de protección de la infancia en línea", en el que se propone tomar en consideración a todas las partes interesadas (entre la que cabe citar gobiernos, padres, escuelas organismos de protección del menor, policía y servicios de emergencia, operadores e ISP. En este informe se pone de relieve la definición de las funciones y responsabilidades, la recopilación de prácticas idóneas y la importancia de adoptar un método experimental. Por último, es importante observar que durante la preparación del informe se debe distribuir un formulario para recabar información sobre la situación actual en los diversos contextos nacionales y el primer borrador debe distribuirse a las partes interesadas a título informativo y para que formulen los comentarios que estimen oportunos.

Las estrategias nacionales deben complementarse con soluciones técnicas, como indica la Academia Nacional de Telecomunicaciones A.S. Popov de Odessa, (Ucrania),[19] a fin de poner en marcha uno de los temas de la iniciativa regional sobre PIeL de la región CEI, la Academia compartió esfuerzos de recopilación de datos sobre las soluciones técnicas existentes para la Protección de la Infancia en Línea (www.contentfiltering.info). A este respecto, el grupo de expertos elaboró una lista de las soluciones técnicas existentes basadas en las diferentes características, como tipo de implementación (software, hardware, nube); compatibilidad con los sistemas operativos (monoplataforma, multiplataforma, independiente de la plataforma); el tipo de sistema operativo (Windows, Unix, Marcos, Android, iOS); el tipo de soporte (total, parcial, no soportado); el control (a distancia, local, sin control); y el tipo de seguridad interna (sistema con o sin protección).

Todas las soluciones técnicas de la lista se instalaron en un computador o dispositivo móvil (en el caso de productos de pago, se pidió permiso al proveedor para efectuar pruebas), con el fin de probar minuciosamente cada función. Para cada solución se recopiló un informe de pruebas y se incluyó en la base de datos de servicios de contentfiltering.info. Una vez registrados en dicha base de datos, los creadores del sistema verifican periódicamente los datos de cada producto y, en caso necesario, se actualizan y complementan. Por otra parte, el software de Contentfiltering.info se ha elaborado

[16] Documento 2/78, "Support of the Resolution on child online protection", Reino Unido de Gran Bretaña e Irlanda del Norte, Australia y Vanuatu.

[17] Documento SG2RGQ/56, "Proposed questions on child online protection", Australia, Papua Nueva Guinea, Estado Independiente de Samoa, Reino Unido y República de Vanuatu.

[18] Resolución 67 de la CMDT "Función del Sector de Desarrollo de las Telecomunicaciones en la protección de la infancia en línea", disponible en: https://www.itu.int/pub/D-TDC-WTDC-2014.

[19] Documento 2/322, "A database with data on existing technical solutions for child online protection (Contentfiltering.info)", Academia Nacional de Telecomunicaciones A.S. Popov de Odessa (Ucrania).

siguiendo las recomendaciones de seleccionar los mejores sistemas de filtrado de contenido para un determinado usuario/organización. Consta de dos módulos:

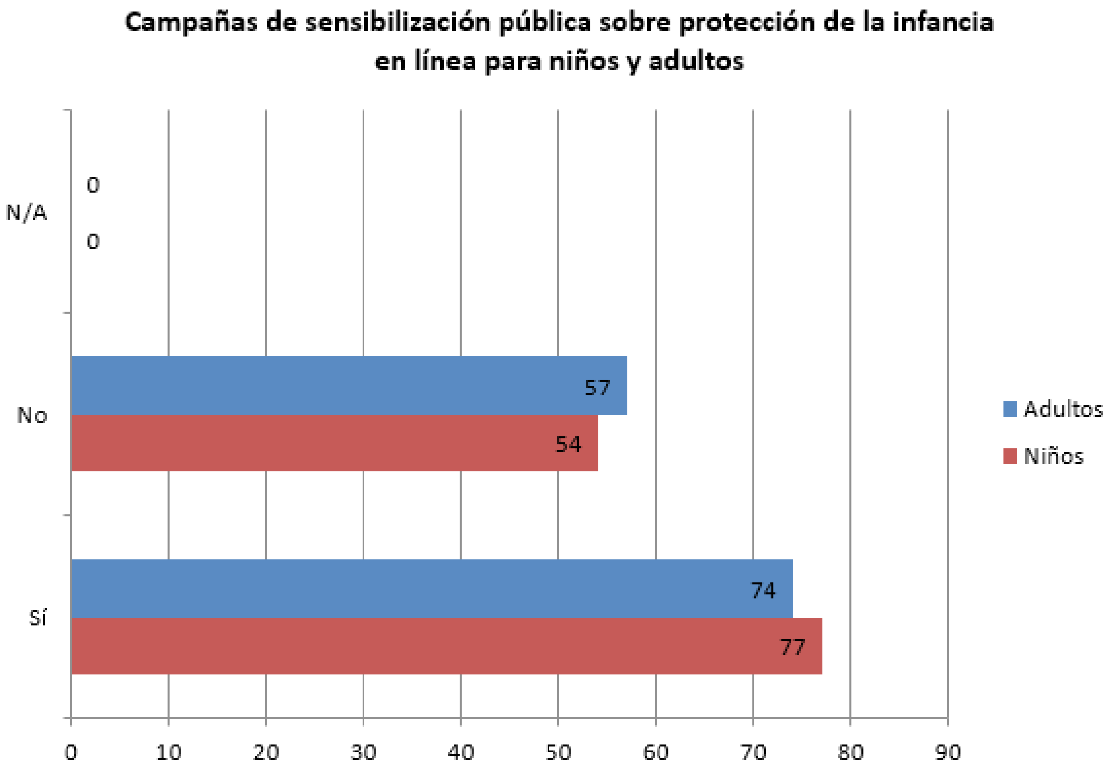
a) un módulo de usuario (acceso gratuito), para definir el nivel de aptitudes del usuario, determinar los requisitos y seleccionar el sistema de filtrado de contenido; y

b) un módulo de experto (sólo para expertos autorizados), para el registro de datos sobre soluciones técnicas para la PIeL.

La Academia Nacional de Telecomunicaciones A.S. Popov de Odessa (Ucrania)[20] también proporcionó información sobre un curso multimedios de aprendizaje a distancia sobre la utilización segura de los recursos de Internet (https://onlinesafety.info) desarrollado en el ámbito de la Iniciativa Regional de la UIT: "Creación de un centro de protección de la infancia en línea para la región de la CEI".

En la **Figura 22** se ve que, si bien varios países disponen de campañas de información para la protección de la infancia en línea, hay bastantes que carecen de ellas.

Figura 22: Campañas de sensibilización pública sobre protección de la infancia en línea para niños y adultos



4.2.1 Campañas de sensibilización sobre PIeL y actividades conexas

En una contribución[21] de la **República de Corea** se destacan los diferentes esfuerzos desplegados a nivel nacional en varios países, en relación con el marco jurídico, las campañas sociales y la educación en línea sobre PIeL. En la contribución se indica que como la edad media de los niños con acceso a Internet está disminuyendo, la utilización segura de Internet por los niños se está convirtiendo en un asunto importante para muchos países. En particular, la contribución de Corea subraya la necesidad

[20] Documento 2/156, "Curso multimedios de aprendizaje a distancia sobre la utilización segura de los recursos de Internet", Academia Nacional de Telecomunicaciones A.S. Popov de Odessa (Ucrania).

[21] Documento 2/362, "Proposed text for inclusion in Chapter 6 (Child Online Protection) of the Final Report", República de Corea.

de tomar medidas voluntarias de salvaguarda para complementar las medidas jurídicas y obligatorias. Aunque estas medidas pueden dan lugar a resultados inmediatos y patentes, existe no obstante el riesgo de que sean demasiado restrictivas y que lleguen a infringir las libertades individuales o la autonomía de los usuarios del servicio. Por ejemplo, la medida jurídica de Corea de bloquear el acceso del menor a juegos en línea después de medianoche ha suscitado un acalorado debate sobre la validez y la eficacia de dicha medida. Por consiguiente, a este respecto, las medidas jurídicas y obligatorias deben complementarse con un programa de educación y sensibilización en colaboración con las diferentes partes interesadas.

Otro tema que planteó la República de Corea guarda relación con la dificultad de trazar una línea entre los proveedores de servicio y los usuarios. Los padres pueden afirmar que los proveedores de servicio tienen que aumentar sus esfuerzos para garantizar la seguridad en línea del menor al prestar sus servicios. Ahora bien, algunos proveedores de servicio pueden aducir que la orientación y sensibilización es responsabilidad de los padres, profesores y tutores. Los programas y las campañas sociales pueden ayudar a identificar medidas que permitan una mayor cooperación entre todas las partes interesadas y alentarles a participar activamente en las actividades del gobierno en pro de la seguridad en línea.

En el contexto de los países menos adelantados, la contribución[22] de la **República de Gambia** destaca la urgente necesidad de iniciar globalmente la protección de la infancia en línea en el marco de la ciberseguridad nacional. Los países menos adelantados están comenzando a beneficiarse de disponibilidad de Internet a alta velocidad sobre diferentes plataformas que son menos onerosas que los tradicionales computadores portátiles y de escritorio. La importancia de la cooperación internacional se observa no solamente en la compartición de conocimientos sobre los problemas, sino también en la coherencia de las políticas internacionales y la promoción de actividades que refuercen la cooperación internacional. En la contribución se pide que la protección de la infancia en línea se integre en el marco de ciberseguridad nacional y se concentre en los aspectos jurídicos, técnicos, orgánicos y de procedimiento, así como en la capacitación y la cooperación internacional.

Por último, en la declaración de coordinación remitida por la JCA-PIeL del UIT-T[23] se subraya la importancia de compartir información entre los miembros a fin de ponerla en conocimiento de la Cuestión 3/2. También se expresa el reconocimiento de los esfuerzos a escala nacional desplegados por la República de Corea y Gambia, así como por las ONG como Defz Kidz.

4.2.2 Estrategias para la Protección de la Infancia en Línea

Los Estados Miembros pueden adoptar las siguientes estrategias, extraídas de las contribuciones recibidas:

- colaboración entre las diversas partes interesadas;
- campañas de información;
- involucración de la industria;
- medidas legislativas;
- definición de un mecanismo adecuado de información;
- desarrollo de las capacidades de las partes interesadas pertinentes;
- apoyo y conocimientos para todas las partes interesadas;

[22] Documento SG2RGQ/104, "A case to adopt child online protection initiatives across LDCs", República de Gambia.

[23] Documento 2/289, "Liaison statement from ITU-T JCA-COP to ITU-D SG2 Question 3/2 on Child Online Protection Initiatives", JCA-PIeL del UIT-T.

- definición de mecanismos para la participación de todos los interesados (incluidos, aunque no únicamente, los gobiernos, los padres, las escuelas, las organizaciones de protección de la infancia, la policía y los servicios de emergencia, los operadores y PSI);
- definición clara de las funciones y responsabilidades de cada parte interesada (quién hace qué, cuándo y cómo);
- recopilación de prácticas idóneas y soluciones técnicas existentes para la protección de la infancia en línea;
- divulgación de la información pertinente entre los interesados;
- aplicación de un método basado en las pruebas.

5 CAPÍTULO 5 – Resultados de los talleres sobre ciberseguridad

Esta sección versa sobre el tema *i)* del mandato de la Cuestión 3/2 en el que se pide, entre otras cosas*:*

i) ***Organizar reuniones, seminarios y talleres ad hoc para intercambiar conocimientos, información y prácticas óptimas relativos a las medidas y actividades eficientes, eficaces y de utilidad para mejorar la ciberseguridad teniendo en cuenta los resultados del estudio que se celebrarán simultáneamente, en la medida de lo posible, con las reuniones de la Comisión de Estudio 1 o las reuniones del Grupo de Relator para la Cuestión.***

Uno de los ámbitos de colaboración entre la Comisión de Estudio 2 del UIT-D, la BDT, los otros Sectores, la industria y las instituciones académicas ha sido la serie de talleres organizados durante el anterior periodo de estudios. En el **Anexo 2** se adjuntan varias contribuciones. A continuación se resumen dichas colaboraciones.

5.1 1er Taller sobre ciberseguridad (8 de septiembre de 2015)

El taller sobre ciberseguridad "Global Cybersecurity Challenges – Collaborating for effective enhancement of cybersecurity in developing countries"[24] tuvo lugar el 8 de septiembre de 2015, por la tarde, con ocasión de las reuniones de las Comisiones de Estudio 2 y 17 (Seguridad) del UIT-D, y precedió a la reunión de la Cuestión 3/2 de la Comisión de Estudio 2 del UIT-D.

Objetivos del taller

El objetivo del taller sobre ciberseguridad era compartir prácticas idóneas a escala internacional, regional y nacional para aumentar la capacitación en materia de ciberseguridad. El taller estaba diseñado para dar a conocer las inquietudes de los países en desarrollo en relación con la capacitación en ciberseguridad y para identificar medios innovadores y prácticos para la cooperación entre organizaciones internacionales, administraciones y el sector privado para poner fin a esas inquietudes.

Orden del día

El Sr. Yushi Torigoe (Subdirector de la BDT) y el Sr. Reinhard Scholl (Subdirector de la TSB) realizaron los discursos de apertura. El orden del día incluía dos sesiones con ponencias y debates:

- Sesión 1: Prácticas idóneas para el método estratégico estratificado para mejorar la ciberseguridad en los países en desarrollo (3 presentaciones y un debate).
- Sesión 2: Dificultades de los países en desarrollo; colaboración internacional para promover iniciativas de ciberseguridad (3 ponencias y un debate).

Debate y conclusiones del taller

El taller consistió en ponencias informativas y útiles, debates y preguntas y respuestas sobre prácticas idóneas para un método estratégico estratificado para mejorar la ciberseguridad en los países en desarrollo y la colaboración internacional para promover las iniciativas de ciberseguridad.

En las dos sesiones se destacó la importancia de los siguientes aspectos de ciberseguridad, de los que se informó a los participantes en el taller:

- sensibilización de todas las partes interesadas en la ciberseguridad;
- participación de todas las partes en la puesta en marcha de una estrategia nacional de ciberseguridad;
- principios de ciberseguridad claros en la estrategia de la ciberseguridad, tales como libre flujo de información, imperio de la ley, autogobernanza, apertura y multipartito;

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

- clara identificación de la función y responsabilidades en la estrategia nacional;
- establecimiento de objetivos claros en la estrategia nacional;
- gestión de riesgos;
- legislación/derecho nacional sobre ciberseguridad;
- reglamentación técnica, normas y procedimientos inclusive; y
- colaboración con iniciativas regionales e internacionales.

Se mencionó la esperanza de que siga habiendo oportunidades como las de este taller y que se actualice los debates. El Sr. A. Sharafat (Presidente de la Comisión de Estudio 2 del UIT-D) y el Sr. A. Kremer (Presidente de la Comisión de Estudio 17 del UIT-T) reiteraron la importancia de las oportunidades para compartir información y puntos de vista entre participantes y de reforzar la colaboración entre la Comisión de Estudio 17 del UIT-T (Seguridad) y la Comisión de Estudio 2 del UIT-D, en particular la Cuestión 3/2. Se informó posteriormente de los resultados del taller a la Cuestión 3 de la Comisión de Estudio 2 del UIT-D y a la Comisión de Estudio 17 del UIT-T.

5.2 2º Taller sobre ciberseguridad (19-20 de abril de 2016)

El Taller sobre ciberseguridad de la UIT, "National cyber drills and national cybersecurity strategies elaborated through good practices",[25] se celebró el 18 de abril de 2016 por la tarde y el 19 de abril de 2016 por la mañana, junto con la reunión del Grupo de Relator para la Cuestión 3/2 de la Comisión de Estudio 2 del UIT-D, Seguridad en las redes de información y comunicación: Prácticas óptimas para el desarrollo de una cultura de la ciberseguridad. Organizó este taller el equipo de ciberseguridad de la BDT, con la ayuda del equipo de Comisiones de Estudio del UIT-D. Participó un abundante conjunto de oradores.

Objetivo del taller

El objetivo del taller sobre ciberseguridad era compartir prácticas idóneas a escala internacional, regional y nacional para mejorar la capacitación en ciberseguridad. En ese sentido, el taller tenía por objeto:

- compartir experiencias de los cibersimulacros con países en desarrollo para que comprendan mejor sus necesidades, especialmente desde que la UIT ofrece a los Estados Miembros un nuevo servicio nacional de cibersimulacros;
- compartir las lecciones aprendidas y asesoramiento de expertos en la preparación y puesta en marcha de estrategias nacionales sobre ciberseguridad (NCS) y que la UIT informe a los Estados Miembros sobre los progresos logrados en el enfoque multipartito utilizado en la nueva herramienta de NCS.

Orden del día

El Sr. Y. Torigoe (Subdirector de la BDT) realizó el discurso de apertura. El Taller consistió en tres sesiones con ponencias y debates:

- Sesión del 18 de abril: Mejora de los cibersimulacros nacionales mediante el intercambio de experiencias.
- Sesión 1 del 19 de abril: Principales componentes para preparar una estrategia nacional de ciberseguridad exhaustiva.
- Sesión 2 del 19 de abril: Implantación eficaz de una estrategia nacional de ciberseguridad.

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

Deliberaciones y conclusión del taller

El taller consistió en ponencias informativas y útiles, debates y preguntas y respuestas. En las sesiones se destacó la importancia de los siguientes aspectos de la seguridad, de los que se informó a los participantes:

- Los cibersimulacros nacionales debe ser realistas, sin demasiadas exageraciones para llamar la atención de los directivos a fin de obtener presupuesto.
- En los cibersimulacros nacionales deben participar todas las partes pertinentes, comprendidos el gobierno y el sector privado, desde la fase de planificación e intercambiando información de manera proactiva.
- Los objetivos de un cibersimulacro nacional deben definirse claramente y deben añadir valor.
- La selección del tipo de cibersemulacro nacional se debe basar en la gestión del riesgo – se debe plantear la pregunta "¿cuál es la mayor amenaza o la situación de mayor impacto?" y se construye a partir de la respuesta.
- Algunos cibersimulacros nacionales se realizan para probar planes de contingencia nacionales.
- ¿Deben ser públicas o no las estrategias nacionales de ciberseguridad? La respuesta no es evidente pero, en aras de la sensibilización del ciudadano, al menos una parte de la estrategia debe hacerse pública.
- La gestión del riesgo para el desarrollo de NCS resulta fundamental para determinar y alcanzar los objetivos adecuados.
- La protección de la infraestructura esencial (CIP) es imprescindible para la ciberseguridad y normalmente es fruto de una alianza público-privada, por lo que la NCS requiere la intervención del sector privado.
- Conseguir un equipo y un defensor, observar lo que otros están haciendo y luchar para conseguirlo mediante un equipo dedicado a tal fin. La herramienta NCS formará parte de ello.
- El NCS debe considerarse la biblia de la ciberseguridad. Las metas y medidas han de ser las correctas. Es preciso vincularlo con la CIP y la situación socioeconómica. Luego se pondrá en marcha con mecanismos adecuados de supervisión.
- Institucionalizar las alianzas PPP para NCS y los programas de CIP mediante reglamentación y legislación, ya que las entidades del sector privado y los gobiernos no tienen los mismos objetivos y, por ende, es necesario armonizarlos.
- La puesta en marcha de estrategias de ciberseguridad toma tiempo para los países que nunca antes lo han hecho antes de que lo acepten y se les autorice la primera vez. La financiación y aceptación resulta más fácil si se establece un vínculo con la estrategia de desarrollo de la sociedad de la información.
- La puesta en marcha de la estrategia de ciberseguridad requiere un plan de acción detallado y presupuestado.
- La importancia del análisis del impacto fue subrayada en el ciclo de desarrollo/puesta en marcha de la NCS.
- El plan de puesta en marcha debe incluir la transferencia segura de datos en el marco del gobierno electrónico.
- Los índices (GCI y otros) están cobrando importancia a la hora de medir la ejecución y verificar la NCS.
- El índice de ciberseguridad nacional de Estonia (la metodología se publicó a finales de mayo de 2016). El Índice de Ciberseguridad Global de la UIT se considera complementario.
- La estrategia nacional de ciberseguridad del Reino Unido debía publicar a finales de 2016.

– La evaluación de la NCS lleva tiempo, puede resultar molesta pero ayuda a obtener financiación.

– Es importante disponer de definiciones comunes en las estrategias de ciberseguridad antes de comenzar a elaborar la NCS, a fin de llegar a un entendimiento y una noción comunes a todas las partes interesadas. Un entendimiento común es más importante que una definición común.

En sus conclusiones sobre el taller, el Sr. Luc Dandurand (BDT) destacó la importancia de las oportunidades para intercambiar información y puntos de vista entre los participantes y expertos y la necesidad de seguir colaborando con la Cuestión 3/2 de la Comisión de Estudio 2 del UIT-D. En su discurso de clausura, el Sr. Ahmad Sharafat (Presidente de la Comisión de Estudio 2 del UIT-D) dijo que la organización de un taller sobre ciberseguridad se está convirtiendo en una tradición de la Cuestión 3/2 de la Comisión de Estudio 2 del UIT-D, y expresó su esperanza de que así siga siendo. Desde el punto de vista de una institución académica, considera el taller muy útil y extraordinariamente fructífero. Se informó posteriormente de los resultados del taller a la Cuestión 3/2 de la Comisión de Estudio 2 del UIT-D.

5.3 3º Taller sobre Ciberseguridad (26 de enero de 2017)

El Taller sobre Ciberseguridad, "Cybersecurity and risk assessment in practice",[26] se celebró el 26 de enero de 2017 por la tarde, coincidiendo con las reuniones de los Grupos de Relator de la Comisión de Estudio 2 del UIT-D, antes de la reunión de la Cuestión 3/2 de la Comisión de Estudio 2 del UIT-D.

Objetivo del taller

El objetivo de este taller fue reunir a expertos de todo el mundo para compartir conocimientos y experiencias sobre la evaluación práctica de ciberriesgos a nivel nacional, en organizaciones muy grandes y en sectores infraestructurales esenciales. En el taller se habló también de los riesgos en la cadena de producción y de la función de las normas en la gestión de ciberriesgos en las organizaciones.

Orden del día

Tras la alocución de apertura de un responsable de la BDT, se siguió el orden del día, que constaba de las siguientes cinco intervenciones y mesas redondas:

– principales amenazas de ciberseguridad en 2017 y en adelante;

– métodos y herramientas utilizados en el sector privado para evaluar los ciberriesgos en grandes organizaciones;

– evaluación de ciberriesgos en sectores infraestructurales esenciales;

– riesgos en la cadena de producción;

– función de las normas de la serie ISO/CEI 27000.

Deliberaciones y conclusión del taller

El tercer taller consistió en ponencias informativas y útiles, debates y preguntas y respuestas. En las sesiones se destacó la importancia de los siguientes aspectos de la ciberseguridad, de los que se informó a los participantes:

– Como principales amenazas de ciberseguridad se mencionaron la convergencia ciberfísica, la convergencia vida-trabajo, las amenazas internas, el aumento de ataques por motivos financieros, los ataques DDoS por IoT y el aumento de fallas "simples"; se formularon recomendaciones para las organizaciones.

– Se presentaron los obstáculos que encuentra la evaluación de riesgos en el sector privado, como la multiplicidad de normas que aplicar, las auditorías externas, los requisitos reglamentarios departamentales, las fusiones y adquisiciones/diversificación/huella internacional y la

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

rentabilidad de los cibercontroles. Se presentaron ejemplos de métodos para superar esos obstáculos, incluida la gobernanza y el software de riesgos, la seguridad de las operaciones, la herramienta de detección de riesgos tácticos y la gestión de vulnerabilidades.

- Se presentaron estrategias nacionales para la protección de las infraestructuras esenciales contra los ciberriesgos, con especial énfasis en la evaluación de ciberriesgos de CIPP (metodología, punto de partida, vulnerabilidad de los procesos en el caso de la aviación).
- Se habló de la seguridad en la cadena de producción de las TIC, sus retos y requisitos y, a continuación, se abordaron los siguientes temas; 1) consideración de los riesgos en un programa de gestión de riesgos global, 2) comprensión de los requisitos comunes, 3) utilización de normas internacionales, 4) aprovechamiento del poder adquisitivo y 5) cooperación con los socios.
- Se presentó la función de las normas internacionales en la gestión de riesgos y se presentaron las últimas novedades de la serie ISO/CEI 27000 de ISO/CEI JTC1 SC27.

A lo largo de las deliberaciones y en la clausura del taller se hizo hincapié en la importancia de tener la posibilidad de compartir opiniones entre participantes y expertos y en la necesidad de seguir colaborando con la Cuestión 3/2 de la Comisión de Estudio 2 del UIT-D.

6 CAPÍTULO 6 – Oportunidades y retos de ciberseguridad

La Cuestión 3/2 del UIT-D dedicó parte de su tiempo a investigar otros ámbitos, muchos de los cuales se refieren a trabajos realizados en otros grupos y no forman parte del mandato de la Cuestión 3/2. Así, se mantuvieron diálogos oficiales y oficiosos con otras organizaciones. A continuación se analizan las contribuciones que pertenecen al mandato del tema *b)*.

b) ***Facilitar información sobre dificultades actuales en materia de ciberseguridad que experimentan los proveedores de servicios, los organismos reguladores y otras partes interesadas.***

6.1 Adicción a Internet

La "adicción a Internet" se ha convertido en un efecto negativo resultante del avance de los países hacia la información y la gran popularización de la utilización de Internet. Aunque el concepto no se ha definido con rigor en el ámbito de la psicología y la medicina, la adicción a Internet se refiere a los daños de difícil recuperación causados a las funciones físicas, mentales o sociales de la persona debido a la utilización excesiva del servicio de red IT. La mayoría de los adictos a Internet suelen tener síntomas de abstinencia e intolerancia, como ansiedad extrema o crisis nerviosas, dificultando gravemente su vida cotidiana. Los usuarios muy adictos al mundo cibernético y que utilizan excesivamente Internet presentan síntomas de adicción al juego, a chatear, al porno, etc.

En los últimos años la adición a los medios inteligentes ha transformado rápidamente los estilos de vida y de comunicación, debido al rápido aumento de la adopción de medios inteligentes y la evolución de la fusión y convergencia de las TIC.

Esfuerzos de la República de Corea para prevenir y reducir la adicción a Internet y al móvil

En la República de Corea, alrededor del 7 por ciento de los usuarios de Internet de edad comprendida entre los 5 y 54 años pueden considerarse parte del grupo de riesgo de la adicción a Internet, según el estudio sobre la adicción a Internet realizado en 2013. En Corea la proporción de usuarios de Internet en el grupo de riesgo respecto del total de usuarios de Internet ha ido disminuyendo, del 7,7 por ciento en 2011, al 7,2 por ciento en 2012 y al 7 por ciento en 2013. Sin embargo, el porcentaje total de adolescentes en el grupo de riesgo ha ido en aumento, del 10,4 por ciento en 2011 al 10,7 por ciento en 2012 y el 11,7 por ciento en 2013.[27]

Entretanto, la adicción al móvil es superior a la de Internet. En Corea, alrededor del 11,8 por ciento de los usuarios de teléfonos inteligentes de edad comprendida entre 10 y 54 años pertenece al grupo de riesgo de utilización excesiva del móvil, del 3,4 por ciento al 8,4 por ciento en 2011, año en que se inició el estudio de la adicción al móvil. Los usuarios adolescentes constituyen el grupo de riesgo más elevado: Cerca del 25,5 por ciento de los coreanos adolescentes (de 10 a 19 años) pertenecía al grupo de riesgo de utilización excesiva del móvil, mientras que en el caso de los adultos coreanos esta cifra era del 8,9 por ciento. Creado en 2002 por el gobierno de Corea, el Centro Coreano de Adicción a Internet ha ejecutado programas exhaustivos de asesoramiento, desarrollo y distribución de contenidos, formación especializada de asesores y programas de educación preventiva a escala nacional destinados a resolver sistemáticamente el problema de la utilización excesiva de Internet y de dispositivos inteligentes. Se realizó una encuesta anual sobre la adicción a Internet del ciudadano en general desde 2004 (y la adicción al móvil desde 2011), produciendo una estadística nacional que se utiliza como índice comparativo para el desarrollo de políticas gubernamentales.

En junio de 2013, ocho Ministerios crearon el "Segundo Plan Exhaustivo para prevenir y reducir la adicción a Internet". El programa identifica todas las gamas de asistencia preventiva, de asesoramiento, psicológica y de postratamiento disponibles para todos los grupos de edad, niños, estudiantes y adultos. El gobierno estableció el comité de política interministerial para abordar sistemáticamente

[27] Documento SG2RGQ/64, "Korea's Internet of things security roadmap", República de Corea.

el problema de la adicción a Internet. El mes de marzo de 2014 el Comité creó el "Programa de ejecución de 2014 para prevenir y reducir la adicción a Internet". Este programa se ha ejecutado bajo los auspicios de ocho comités de política de los Ministerios de manera efectiva y sistemática.

Educación preventiva

Internet y los medios inteligentes son tan fácilmente accesibles en la vida cotidiana que la educación debe centrarse en la prevención de los síntomas de adicción como el retiro de la sociedad o la intolerancia. El programa educativo de Corea está concebido para prevenir de manera eficaz la adicción, y está destinado a mejora la conciencia pública sobre los riesgos potenciales y reales de adicción y ayudar en la prevención. Por ejemplo, ofrece educación preventiva, con un programa adaptado a las necesidades de cada grupo de edad, es decir, niños, adolescentes y adultos. Se envían consejeros especializados a escuelas para que den clases especiales (de una hora).

En Corea, desde 2013 se ha facilitado un programa de educación intensivo (dos horas) a estudiantes de primaria y secundaria; cada curso está especialmente concebido para la edad escolar y se insiste en la participación e intervención del estudiante en las actividades del aula. Durante el curso cada estudiante utiliza su propio "cuaderno de ejercicio" como una herramienta de autodiagnóstico, donde mantienen un registro de su utilización de Internet y medios electrónicos, y a menudo, cuando descubren que es excesiva, toman la resolución de reducir la utilización de Internet.

Cuadro 1: Número de participantes en la educación preventiva

Categoría	2010	2011	2012	2013	Junio 2014	Total
Preescolar	–	31.279	18.200	47.890	26.050	**123.419**
Adolescentes	645.981	954.425	621.621	970.696	407.512	**3.600.235**
Adultos	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**

(Unidad: personas)

En 2014, se ha desarrollado el programa "Juego de prevención de la adicción" para estudiantes de preescolar y de los primeros cursos de primaria a fin de hacerles llegar el mensaje de manera fácil, eficaz y de un modo que les resulte ameno. En el programa los niños y estudiantes asisten a una pieza de teatro o de marionetas en la que se cuentan historias sobre la adicción a Internet de su animal favorito o en la vida cotidiana de la familia. Después de ver la obra, el profesor describe los peligros de la adicción a Internet y cómo prevenirla. Este programa resulta eficaz para que los niños comprendan fácilmente el concepto de adición sin sentirse rechazados. Se prestó asistencia a 23 escuelas que se designaron "Escuelas limpias de medios inteligentes". Este programa tiene por objeto dar soporte a actividades y campañas en las escuelas destinadas a promover una cultura de utilización de medios inteligentes y para prevenir la adicción a Internet coopera con padres, profesores y expertos.

Servicios de asesoramiento y creación de infraestructura

El Ministerio de Ciencia, TIC y Planificación Futura (MSIP) de la República de Corea ejecuta servicios de educación preventiva y asesoría especializada para tratar con eficacia las adicciones a Internet y teléfonos inteligentes. A fin de proporcionar servicios específicos de la región, se explotan 14 Centros de prevención de la adicción a Internet (IAPCs) instalados en 13 ciudades y provincias de la nación desde junio de 2014.

Se ofrecen servicios de asesoría especializados que se prestan a través de diversos canales, como visitas en el hogar o servicios en línea. Estos servicios de asesoría especializada están concebidos para responder efectivamente al rápido aumento de la demanda de servicios de asesoría y a servicios fácilmente accesibles. Se dispone de un servicio de asesoría,[28] así como una línea directa. A los efectos de ofrecer servicios específicos de la región sobre la adicción a Internet que ocurre a nivel nacional, el Centro ofrece servicio de asesoramiento en colaboración con 48 centros afines, como los centros de ayuda a la familia, los centros de ayuda a los jóvenes, etc.

El servicio de asesoría con visita al hogar merece especial atención, ya que consiste en un servicio gratuito en el que se visita a la familia en el hogar. Toda familia que sufre adicción a Internet puede recurrir a este servicio. El programa es especialmente eficaz para adictos a Internet que necesitan ayuda y que pertenecen a familias monoparentales, de renta baja o interraciales, o que viven con los abuelos. No obstante, cualquiera persona con adicción a Internet puede solicitar ayuda, ya sean niños, adolescentes, desempleados o familias con doble fuente de ingresos. El servicio también cuenta con un programa para la formación de consejeros especializados en adicción a Internet. El programa de formación está disponible para los actuales consejeros y profesores de manera que puedan especializarse en consejeros sobre adicción a Internet. Al mes de junio de 2014, este programa había impartido formación a más de 13 000 consejeros especializados.

Cuadro 2: Número de servicios de asesoría por tipo

Categoría	2010	2011	2012	2013	Junio 2014
En persona (Visita al hogar)	15.037	10.522 (6.089)	20.701 (10.595)	24.623 (19.519)	7.484 (4.919)
En línea	1.916	569	866	489	148
Telefónica	9.569	7.915	16.138	11.512	4.779
Subtotal	**26.522**	**19.006**	**37.705**	**36.624**	**12.411**

(Unidad: un servicio)

Realización de encuestas y preparación/distribución de contenido

Se están realizando continuamente investigación sobre política para aumentar la eficiencia operativa y la eficiencia científica de la ejecución de diversos programas sobre la adicción a Internet y medios inteligentes. Se han publicado en el sitio web diversos materiales didácticos como guías preventivas, animaciones en flash, vídeos, libros técnicos o programas de asesoría. Estos materiales se han creado a fin de llevar eficazmente a cabo educación preventiva y ayudar a conocer mejor los posibles riesgos de la utilización de Internet o medios inteligentes.

En 2013, se prepararon y distribuyeron libros técnicos sobre la prevención de la adicción grave. Los cursos están disponibles en cuatro ediciones, para diferentes ciclos (es decir, para estudiantes de primaria, estudiantes de segundaria, estudiantes de grado medio y adultos). Asimismo, se prepararon directrices sobre la utilización adecuada de medios inteligentes y se publicaron en cuatro ediciones para cada uno de los cuatro grupos de lectores (padres de alumnos de preescolar, de primaria, de grado medio y de secundaria). Las directrices se han distribuido a más de 20 000 escuelas del país. En 2014, se preparó contenido para autodidactas disponible en cinco categorías de prevención de la adicción (para alumnos de preescolar, primaria, grado medio y secundaria, universitarios y adultos) de modo que pueden ayudar a que las escuelas e instituciones públicas estén mejor preparadas para prevenir la adicción a Internet, que se ha convertido en obligatorio en virtud de la ley fundamental nacional sobre la información (mayo de 2013), punto 8 del artículo 30, (relativo a la educación sobre la adicción a Internet) de Corea.

Se recurre a publicidad para prevenir la adicción a medios inteligentes, mediante la cooperación con el sector privado. De este modo se ayuda a los padres y a los adolescentes a abstenerse de utilizar

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

medios inteligentes y a acostumbrarse a utilizar adecuadamente los medios inteligentes en casa y en la escuela.

Características especiales de la política de Corea

En Corea, la mayoría de las actividades son iniciativa del Gobierno, por lo que éste presta ayuda financiera y técnica a las organizaciones cívicas para que éstas lleven a cabo las actividades relativas a la prevención de la adicción a Internet. También se observa un fuerte compromiso del gobierno en el hecho de que no se permite a los menores de 16 años acceder a juegos en línea entre medianoche y las seis de la mañana, y los padres pueden comprobar y supervisar el acceso por sus hijos (menores de 18 años) a juegos en línea, previa solicitud a los proveedores de servicios, así como por el hecho de que la ley obliga a todos los estudiantes, desde preescolar hasta la universidad, y a todos los empleados del sector público a recibir formación sobre la prevención de la adición a Internet. Por otra parte, el gobierno dirige 14 Centros de prevención de la adicción a Internet por todo el país. La dificultad que ahora tiene el gobierno de Corea en el ámbito de la prevención de la adicción a Internet es cómo implicar a todas las partes interesadas, especialmente a los padres, a la comunidad y al sector privado.

Resumen

La adicción es un tema fundamental de la sanidad. Por ese motivo, la Cuestión 3/2 del UIT-D inició unas discusiones con la Organización Mundial de la Salud (OMS) a fin de señalar a su atención este asunto. En este sentido, se envió a la OMS una Declaración de Coordinación sobre el tema de la adicción a Internet así como a la UNICEF, UNESCO y al Grupo de Trabajo del Consejo sobre la Protección de la Infancia en Línea (GTC-PIeL), durante el periodo de estudios 2014-2017, para entender mejor qué actividades se están realizando actualmente sobre este tema. En esas discusiones no pudo llegarse a ninguna conclusión y podrían seguir.

6.2 Seguridad de las transacciones electrónicas

La evolución del comercio electrónico y de las transacciones electrónicas, en particular las compras en línea y los pagos en línea, la ejecución de órdenes sobre operaciones bursátiles, las declaraciones administrativas en línea (IVA, impuesto sobre la renta, hoja de atención médica electrónica), los intercambios de documentos y correos electrónicos; la creación de nuevos protocolos de seguridad de la red basados en infraestructuras de clave pública y su implantación progresiva a gran escala, en particular DNSSEC, RPKI (Resources Public Key Infrastructure); así como la seguridad de Internet de las cosas son elementos esenciales que incitarán a los países en desarrollo a trabajar para el establecimiento de instituciones a escala nacional o regional encargadas de la gestión de sus infraestructuras de clave públicas. La creación de esas instituciones, si son supervisadas convenientemente, puede contribuir a reforzar la seguridad de las comunicaciones electrónicas, en general, y la de las transacciones electrónicas, en particular. Asimismo, puede favorecer el surgimiento y desarrollo de economías digitales en los países en desarrollo.[29]

El comercio electrónico y las transacciones electrónicas han alcanzado una rápida evolución en los países en desarrollo. Por lo general, esas transacciones utilizan canales inseguros. Sin embargo, cuando están protegidas, se basan en certificados autofirmados o en certificados adquiridos ante autoridades de certificación situadas generalmente en países desarrollados. Pese a ello, en algunos casos, esos certificados no se ajustan necesariamente a la legislación de los países en desarrollo.

La falta de entusiasmo y las demoras observadas en la implantación de protocolos de seguridad, como DNSSEC y RPKI, en los países en desarrollo se debe al desconocimiento de esos protocolos o de las normas que permiten su aplicación, o a los recursos humanos poco capacitados que intervienen en su instalación, o bien a la ausencia de dominio en las cadenas de valor.

[29] Documento SG2RGQ/153, “Seguridad de las transacciones electrónicas”, República de Togo.

La Cuestión 3/2 del UIT-D ha pedido a numerosas organizaciones que opinen sobre estos problemas. La ISOC nos ha remitido un excelente resumen de estos problemas, que se incluye a continuación.

Los sistemas de Infraestructura de clave pública (PKI) desempeñan un papel fundamental en la creación de confianza en Internet, como plataforma segura para el desarrollo socioeconómico. Estos sistemas, las tecnologías subyacentes y las prácticas de implementación han ido evolucionando para mejorar su robustez y seguridad. Es importante que los países que desean mejorar su infraestructura de Internet tengan en cuenta esta experiencia para instalar tecnologías modernas y utilizar las prácticas idóneas más recientes.

El personal de la sociedad Internet tiene considerable experiencia en la creación y despliegue de infraestructura PKI. Disponemos de la iniciativa Confianza e Identidad que de soporte a la comunicación segura y autentificada por Internet. La Internet Society también está ejecutando el programa Deploy360 que promueve el despliegue de infraestructura de tecnologías de seguridad, en particular la seguridad en la capa de transporte (TLS), extensiones de seguridad DNS (DNSSEC) y PKI de recursos (RPKI).

La Internet Society mantiene recursos de información relacionados con estos temas y referencias y material adicionales que explica cómo crear autoridades de certificación raíz, cómo utilizar TLS, DNSSEC y RPKI, y cómo desplegar dichas tecnologías y prestar asistencia en las actividades de capacitación. El punto de partida es nuestros sitios web sobre Internet Technology Matters y Deploy360.

En este documento se describen tres sistemas de PKI (WebPKI, RPKI y DNSSEC) que afectan a la confianza y seguridad generales de Internet. Se destaca el hecho importante de que estos sistemas de PKI son diferentes y sirven para distintos fines. Tienen jerarquías independientes y funcionan en dominios administrativos separados. También se identifica una tecnología incipiente, la autentificación de entidades denominadas basada en DNS (DANE), que resulta prometedora para intensificar la confianza en Internet.

Es improbable que una autoridad de certificación nacional pueda considerarse una solución a los problemas de seguridad que pudiera tener un país. Los que tratan de resolver problemas de seguridad deben investigar nuevas tecnologías incipientes y las prácticas idóneas que pueden adoptarse en el marco de una colaboración mundial.

WebPKI

El primer sistema PKI (Infraestructura de clave pública) que se examina en este documento es WebPKI. Los certificados X.509 fiables públicamente los expiden autoridades de certificación (AC) certificadas mediante proveedores de tecnologías como Apple, Microsoft y Mozilla que distribuyen certificados raíz en sus sistemas operativos y navegadores. WebPKI utiliza comúnmente estos certificados para proteger las sesiones de navegación por la web, la transferencia por correo electrónico y la mensajería instantánea. Estos certificados también pueden utilizarse para autentificar a usuarios que acceden a sistemas para la firma digital de documentos electrónicos y software. La legislación nacional acepta cada vez más firmas digitales en vez del método tradicional de autentificación.

Obtener un certificado raíz dentro de las distribuciones de raíz globales para WebPKI es un proceso complejo, caro y que consumen tiempo. Este proceso implica tres componentes básicos:

1) establecer los requisitos de la AC para la expedición y gestión de certificados;

2) auditar la AC para garantizar que el proceso y los requisitos se siguen adecuadamente; y

3) añadir una AC para establecer las AC de confianza en un producto. La AC/Foro de navegadores (véanse los “requisitos básicos”) establece directrices para la expedición y gestión de certificados.

Estos requisitos se verifican luego en un conjunto de procedimientos de auditoría gestionados por el Programa WebTrust de AICPA/CICA para autoridades de certificación. Los proveedores de tecnologías utilizan los resultados de estas auditorías para tomar decisiones sobre qué AC pueden añadirse por defecto al producto. Los usuarios y las empresas pueden a menudo añadir AC adicionales para sus dispositivos, pero hay muchas consideraciones operativas importantes que hay que tener en cuenta al utilizar este proceso.

Cabe observar que añadir un nuevo certificado raíz en las distribuciones globales de certificados raíz no hace que el WebPKI sea generalmente más seguro. Al contrario, aumenta los riesgos ya que la vulnerabilidad de cualquier AC es una vulnerabilidad de todo el sistema. Por esos motivos es conveniente mantener el número de certificados raíz al mínimo posible. Cuando es necesario que los gobiernos establezcan su propia AC, una forma común es crear una AC dependiente de la AC raíz existente.

Hay varios motivos de preocupación sobre la fragilidad del sistema WebPKI. La Junta de Arquitectura de Internet (IAB) está colaborando en un programa sobre privacidad y seguridad https://datatracker.ietf.org/doc/draft-iab-web-pki-problems/ para articular algunos de estos problemas y formular recomendaciones sobre acciones que pueden contribuir a mejorar la infraestructura. Quienes deseen identificar las formas en las que los sistemas PKI pueden mejorar su postura de seguridad se beneficiarán de dicho programa.

RPKI

El segundo sistema PKI identificado en este documento es RPKI. RPKI es un caso especial de PKI destinado a mejorar la seguridad de los sistemas de encaminamiento de Internet, concretamente el protocolo de pasarela limítrofe (BGP). Para ello expide certificados de recursos X.509 a los titulares de direcciones IP y números AS a fin de comprobar la asignación autorizada de esos recursos. Estos certificados los expide a los registros de Internet locales (LIR) uno de los cinco registros de Internet regionales (RIRs), a saber AfriNIC, APNIC, ARIN, LACNIC y RIPE NCC, que tienen la responsabilidad de atribuir y asignar esos recursos en su respectiva región de servicio.

Cada RIR actúa de AC raíz y punto de confianza para los recursos asignados dentro de sus regiones de servicio, aunque sus certificados raíz no incluyen ninguna distribución raíz pública. Por consiguiente es necesario descargar e instalar esos certificados de los sitios web RIR.

Cabe observar que los recursos de numeración no se atribuyen o asignan a escala nacional, salvo los siete Registros de Internet Nacionales (NIR) tradicionales en la región APNIC. No obstante, los gobiernos nacionales pueden instar a los ISP y otros LIR a que utilicen instalaciones RPKI.

DNSSEC

El último sistema PKI que se examina en este documento es DNSSEC (extensiones de seguridad DNS). La finalidad del sistema de nombres de dominio (DNS) es traducir nombres de computadores legibles por personas, como http://www.isoc.org en direcciones IP legibles por máquinas, por ejemplo 212.110.167.157. DNS se ha convertido en el método principal para localizar servicios Internet. No obstante, como el DNS es administrado por numerosas organizaciones diferentes y tiene naturaleza distribuida, los cambios no se propagan por Internet instantáneamente, por lo que resulta difícil garantizar que la información se recibe de una fuente fiable. Es decir, no hay manera de garantizar que un servidor de nombres no proporciona información falsa para desviar al usuario a computadores que espían sus transacciones o falsifican otros sitios.

DNSSEC fue concebido por el IETF para autentificar la información DNS mediante la firma digital de registros DNS. De este modo se garantiza que sólo el titular del dominio puede introducir cambios y que los registros pueden validarse a través de la cadena de confianza hasta llegar a la zona raíz. Esto significa que el cliente que realiza una consulta puede verificar que la respuesta recibida procede realmente de la entidad autorizada a responder.

El DNS con DNSSEC puede considerarse un caso especializado de PKI. Lamentablemente, DNSSEC se ha desplegado muy poco, pese al hecho de que cada vez se firman más TLD. Los administradores de dominio nacionales pueden desempeñar un papel importante en la protección de esta importante infraestructura de Internet mediante la firma de sus zonas ccTLD y la facilitación del despliegue de

DNSSEC en su jerarquía DNS nacional. Asimismo, el despliegue de DNSSEC permitirá utilizar la tecnología DANE antes mencionada para mejorar la WebPKI.

DANE

Uno de los puntos débiles inherentes de la WebPKI es que las AC terceros pueden expedir certificados para cualquier dominio u organización, con independencia de si la entidad solicitante posee o no realmente ese dominio o, de lo contrario lo controla. El riesgo de que una AC expida un certificado incorrecto aumenta con el número de AC. La confianza en el sistema PKI es tan fuerte como su enlace más débil. Esta es la principal razón por la que las distribuciones raíz público están reforzando cada vez más los requisitos para la inclusión de AC, como se examina en la sección anterior de WebPKI.

Pese a que los procedimientos de expedición de certificados se han hecho considerablemente más estrictos debido a los diversos incidentes graves en los que las AC expidieron certificados incorrectos, el sistema sigue dependiendo en terceros de confianza. Esta dependencia ha dado lugar al desarrollo reciente del protocolo DANE (autentificación de entidades denominadas basadas en DNS). Mediante DANE, un administrador de dominio puede certificar sus claves públicas almacenándolas en el DNS. Este método requiere la utilización de DNSSEC y muchos navegadores requieren actualmente la instalación de un aditivo (*add-on*). Por otra parte, DANE exigirá probablemente una validación más rigurosa de los titulares de dominio, actividad que en última instancia recaerá de los registradores TLD en lugar de las AC.

Autoridades de certificación (AC) nacionales

Todos los sistemas PKI antes descritos se concibieron para ofrecer confianza mundial mediante la autentificación de recursos de Internet, como direcciones, nombres e infraestructura de servidor. Estos sistemas son independientes del contenido que se transfiere por Internet entre dos entidades autentificadas. La confianza se crea mediante los procedimientos operativos que están sujetos al consenso mundial. Estos procedimientos están en última instancia bajo el control de entidades finales que eligen confiar en las AC configuradas en sus sistemas. Por ejemplo, la utilización de la AC para regular el contenido que dará lugar a un quebrantamiento de esa confianza y probablemente a la revocación de la AC en cuanto parte de confianza. Es improbable que una AC nacional pueda considerarse una solución a los problemas de seguridad que pueda afrontar un país.

Son muchos los que hacen suya esta opinión. En la respuesta de la ICANN, se señala específicamente que añadir AC raíz puede aumentar significativamente la superficie de ataque del sistema. El sistema es tan seguro como la AC menos segura o menos fiable del conjunto, toda AC con un certificado raíz incorporado en el software de parte fiable representa un problema potencial. Como resultado, el comportamiento indebido y la vulneración de cualquier AC menoscaba la seguridad y la confianza de todo el sistema. Se indica que perciben un futuro en el que la utilización de seguridad basada en el dominio (DNSSEC) y la Autentificación de entidades denominadas basadas en DNS (DANE) y adelantos en métodos basados en la transparencia de certificados contribuyen a limitar dichos riesgos. Se propone que los miembros interesados colaboren con el IETF y el Foro CA Browser.

El RIPE NCC, el registro de Internet regional que cubre buena parte de Europa y otras zonas, respondió para debatir sobre RPKI. El RIPE ofrece diversas formas de formación en línea y propone que los países en desarrollo (en particular sus administraciones públicas) sean capaces de aprovechar plenamente el sistema RPKI administrado por los RIR, dando ejemplo e instando a los operadores privados de sus países a obtener certificados por los recursos de números Internet de los que son titulares. La adopción más generalizada por los operadores de todo el planeta permitirá que más operadores basen sus decisiones de encaminamiento en la validez de los certificados RPKI, culminando en un sistema de encaminamiento por Internet más seguro para todos.[30]

[30] Puede encontrarse más información sobre estas opciones en las siguientes direcciones: Resource Certification (RPKI) Webinar: https://www.ripe.net/support/training/learn-online/webinars/certification-webinar. BGP Operations and Security Training Course: https://www.ripe.net/support/training/courses/bgp.

6.3 Alianzas en materia de ciberseguridad

Como se observó previamente en la **Sección 3** del Informe, uno de los temas comunes a varias contribuciones era la importancia de crear alianzas en materia de seguridad. Estos asuntos no puede resolverlos un solo gobierno, empresa privada u organización internacional, sino que requiere un enfoque colaborativo. Estados Unidos de América y Países Bajos abordan este tema en su contribución conjunta sobre el Foro Mundial de ciberexperiencia (GFCE).[31] La contribución describe los antecedentes y el GFCE. El Foro GFCE es una iniciativa voluntaria multipartita destinada a fomentar la solidaridad internacional y proporcionar apoyo político, técnico y financiero para actividades de refuerzo de la cooperación internacional entre todos los interesados en asuntos cibernéticos. El GFCE promueve la cibercapacitación en un planteamiento en el que los intereses de seguridad, de economía y derechos humanos van de la mano. Se creó con el fin de intensificar la cibercapacidad y la experiencia a fin de mejorar la eficacia de la cooperación internacional existente. En la contribución también se describen las iniciativas fundamentales del GFCE y se facilita información importante sobre los miembros del GFCE y sobre cómo los Estados Miembros y Miembros de Sector pueden participar en esta iniciativa mundial.

Otros asuntos

En varias contribuciones se abordan otras facetas de la ciberseguridad, como su relación con la industria de la banca[32] y la necesidad de contar con métodos tecnológicamente neutros, la lucha contra las fallas de seguridad de datos personales y la necesaria resiliencia de las ciudades inteligentes.[33] Estos temas no se han explorado en profundidad durante este periodo de estudios.

[31] Documento 2/332, "The Global Forum on Cyber Expertise (GFCE)", Estados Unidos de América y Países Bajos.

[32] Documento SG2RGQ/141, "Fintech and security in Korea", República de Corea.

[33] Documento SG2/77, "Cyber-security's role and best practices to ensure Smart Cities' service continuity and resilience", Symantec Corporation (Estados Unidos de América).

7 CAPÍTULO 7 – Experiencias nacionales con marcos de criterios comunes para la seguridad

De acuerdo con el mandato de la Cuestión 3/2, debemos comenzar a investigar las experiencias nacionales con marcos de criterios comunes para la seguridad. En el contexto de esta investigación la Cuestión 3/2 recibió una contribución[34] del **Reino Unido de Gran Bretaña e Irlanda del Norte** donde se expone su experiencia con cómo los Criterios comunes son un plan reputado, abierto e internacional del que se sirven los diseñadores y aplicadores de sistemas de TI para seleccionar productos de TIC con los niveles de garantía de la seguridad adecuados. Aunque no hay una única herramienta o método que garantice la seguridad de los sistemas, los Criterios comunes son un plan maduro y ampliamente aceptado que ayuda a seleccionar los productos a los compradores para los que la seguridad es importante. El Acuerdo de reconocimiento de criterios comunes (CCRA) existe desde el año 2000 y su función es mejorar la disponibilidad de productos de TI cuya seguridad se ha evaluado fiablemente y eliminar la necesidad de duplicar las evaluaciones. Las pruebas de seguridad se realizan en laboratorios independientes de acuerdo con las normas acordadas. Los laboratorios han de disponer de una licencia que atestigua de su competencia e independencia. El CCRA se actualizó recientemente (2014) para soportar un método de especificación más detallado, en el que participan expertos de la industria, las Instituciones Académicas, etc., para definir los requisitos fundamentales de cada esfera tecnológica a fin de que puedan evaluarse claramente.

La Cuestión 3/2 recibió también dos contribuciones de la **República Islámica del Irán** que plantean dos enfoques alternativos. Una visión consiste en que la evaluación de la ciberseguridad a nivel nacional requiere medir continuamente indicadores de ciberseguridad. A fin de planificar y poner en marcha un sistema nacional de gestión de la ciberseguridad (NCMS), existe la necesidad urgente de desarrollar un adecuado programa nacional de medición de la ciberseguridad (NCMP). El NCMP facilita la adopción de decisiones y mejora el rendimiento y la responsabilidad a escala nacional.[35]

En la segunda contribución se indica que el marco de prácticas idóneas para identificar y utilizar un conjunto de medidas y mediciones es indispensable para evaluar la eficacia del sistema de gestión de la seguridad de la información a escala nacional. Al igual que el marco NCSec,[36] inspirado plenamente en la ISO/CEI 27001[37] para ISMS a nivel de organización, se propuso un marco de "medición nacional de ciberseguridad"[38] inspirado en la ISO/CEI 27004[39] y NIST-800-55-R1,[40] las dos desarrolladas para evaluar la ciberseguridad a nivel de organización. Por otra parte, al igual que en el caso inspirado en la ISO/CEI 27001, es necesario "definir cómo medir la eficacia de los controles seleccionados o los grupos de controles y especificar cómo utilizar estas medidas para evaluar la eficacia y los controles a fin de producir resultados comparables y reproducibles" a escala nacional. Como las contribuciones parecen trascender la experiencia nacional, la Cuestión 3/2 coordinó los trabajos con la ISO/IEC JTC 1/SC 27, que en su respuesta se mostró interesada en las futuras actividades en este campo.

El UIT-T ofrece el informe "Successful use of security standards".[41] Este Informe técnico tiene como objeto ayudar a los usuarios, especialmente a los de los países en desarrollo entender mejor el valor de la utilización de las Recomendaciones del UIT-T relativas a seguridad en varios contextos (negocios, comercio, gobierno, industria).

[34] Documento 2/364, "Common criteria as a tool for giving assurance about the security characteristics of IT products", Reino Unido de Gran Bretaña e Irlanda del Norte.

[35] Documento SG2RGQ/46, "National cybersecurity measures and measurements", República Islámica de Irán.

[36] Comisión de Estudio 1 del UIT-D, Informe final sobre la Cuestión 22-1/1, Garantía de seguridad en las redes de información y comunicación: prácticas óptimas para el desarrollo de una cultura de ciberseguridad, 2014, disponible en: https://www.itu.int/pub/D-STG-SG01.22.1-2014/es.

[37] ISO/IEC 27001, Information Technology- Security Techniques- Information Security Management Systems- Requirements, 2013.

[38] Documento SG2RGQ/47 "National cybersecurity measures", República Islámica del Irán.

[39] ISO/IEC 27004, Information Technology – Security Techniques – Information Security Management – Monitoring, measurement, analysis and evaluation, 2016.

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

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

EL UIT-T también tiene el Suplemento a la Recomendación UIT-T X.1054 – Suplemento sobre prácticas idóneas para la implementación de la Recomendación UIT-T X.1054 | ISO/CEI 27014 sobre gobernanza de la seguridad de la información– El caso de Burkina Faso. [42]

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

8 CAPÍTULO 8 – Conclusiones y recomendaciones para el próximo periodo de estudios

A lo largo de este breve periodo de estudios la Cuestión 3/2 ha considerado numerosos aspectos de la ciberseguridad, examinado varios estudios de caso de países y celebrado una serie de talleres que han ofrecido orientaciones sobre diversos aspectos de la definición de estrategias de ciberseguridad. El grupo examinó la información facilitada por la BDT sobre el Índice de Ciberseguridad Mundial y contribuyó al mismo.

La Cuestión 3/2 del UIT-D recomienda que se prosigan las actividades indicadas en el mandato actual. El grupo recomienda que se estudien las amenazas (técnicas) nuevas y la evolución de las existentes, más allá del spam y el malware. Debe seguir tratándose el fraude de las tarjetas SIM, una preocupación que plantearon varios países en desarrollo. Se ha de insistir en la capacitación a nivel regional y local por medio de más talleres y más materiales de formación. Se ha de insistir en proseguir la colaboración con las organizaciones pertinentes, como FIRST, GFCE e ISOC. Se han de seguir recopilando experiencias nacionales para la colaboración. Se ha de seguir realizando la encuesta sobre la conciencia de la ciberseguridad, asumiendo que los recursos necesarios puedan identificarse antes de la CMDT. La Cuestión debe seguir trabajando en estrecha cooperación con la BDT para validar y perfeccionar las mediciones de la ciberseguridad, como el GCI. En particular, la cuestión debería mantenerse para identificar medidas de mejora respecto de los indicadores, la recolección de datos y el análisis. También se ha de seguir trabajando en la Protección de la Infancia en Línea.

Los últimos periodos de estudios se han aprovechado para perfeccionar los métodos de trabajo de las Comisiones de Estudio del UIT-D. La Cuestión 3/2 solicita a la CMDT que fomente esa evolución. Concretamente, la Conferencia debería considerar la posibilidad de estructurar el trabajo en periodos anuales a fin de que las actividades puedan concentrarse en temas específicos.

Una última conclusión, durante su primer periodo de estudios esta Cuestión (Cuestión 22/1 “Garantías de seguridad en las redes de información y comunicación: prácticas óptimas para el desarrollo de una cultura de ciberseguridad”) elaboró Recomendaciones sobre estrategias nacionales para mejorar la ciberseguridad en las infraestructuras esenciales. Es necesario, habida cuenta del paso del tiempo, reexaminar esas Recomendaciones.

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 **I**nitiati**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.

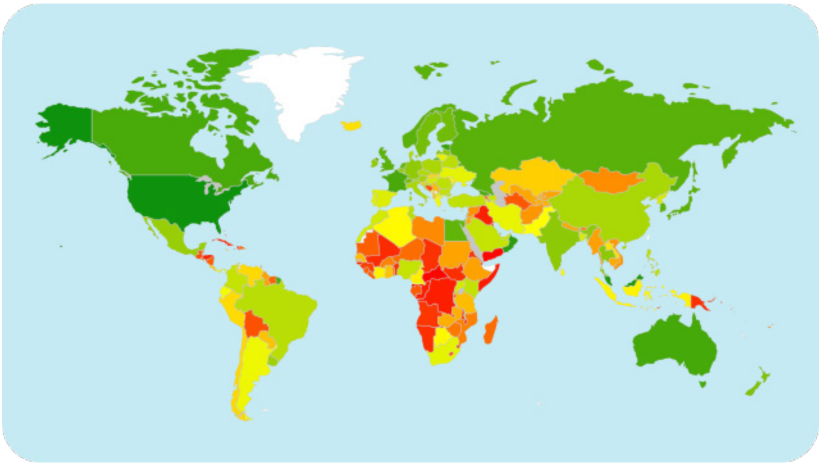
One-hundred and thirty-four Member States responded to the survey throughout 2016. Member States who did not respond were invited to validate responses determined from open-source research. As such, the GCI results cover all 193 ITU Member States.

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".

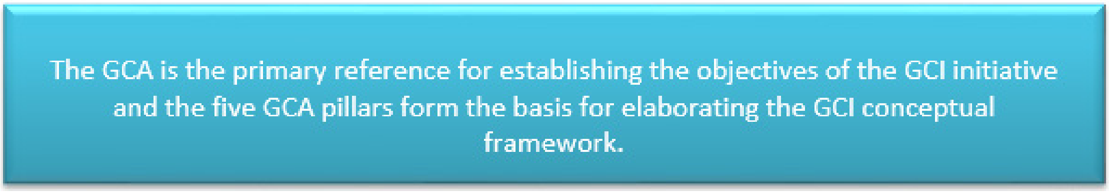
A first iteration of the GCI was conducted in 2013/2014 in partnership with ABI Research, and the final results have been published. A total of 105 countries had responded out of 193 ITU Member States. Secondary data was used to build the index for non-respondents and was sent to them for verification/endorsement.

Following feedback received from various communities, a second iteration of the GCI was undertaken and the Report[43] 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

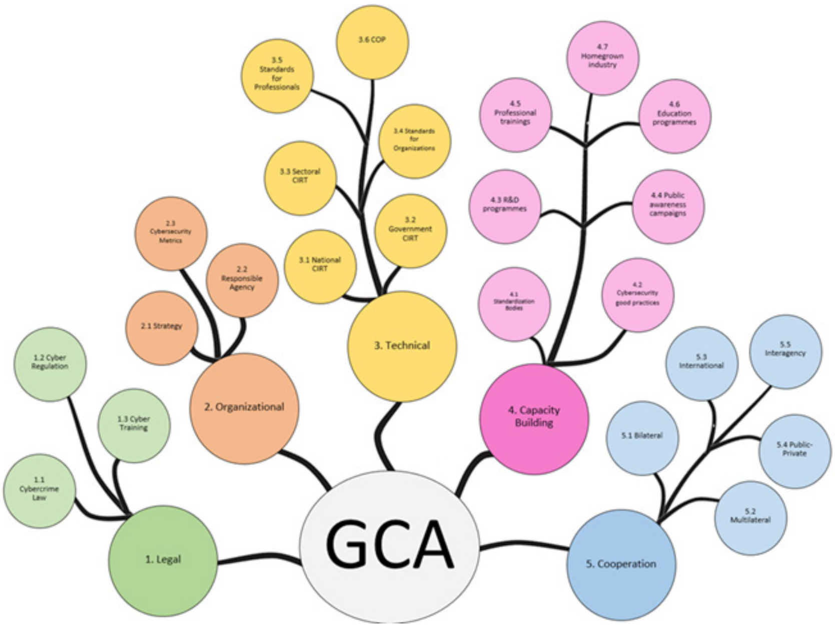


The GCA is the primary reference for establishing the objectives of the GCI initiative and the five GCA pillars form the basis for elaborating the GCI conceptual framework.

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.

[43] 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

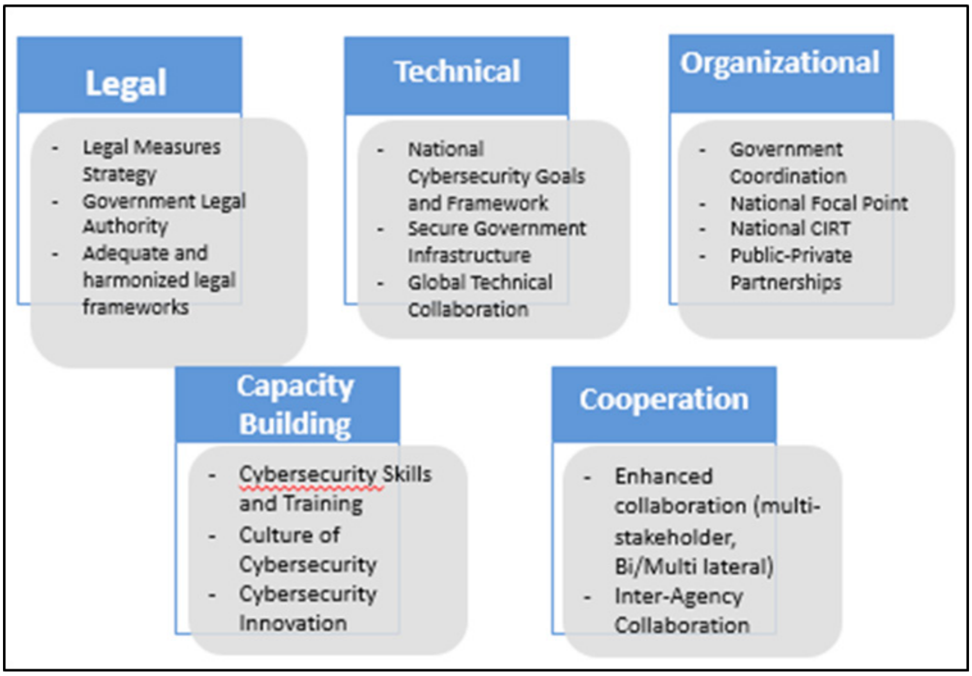
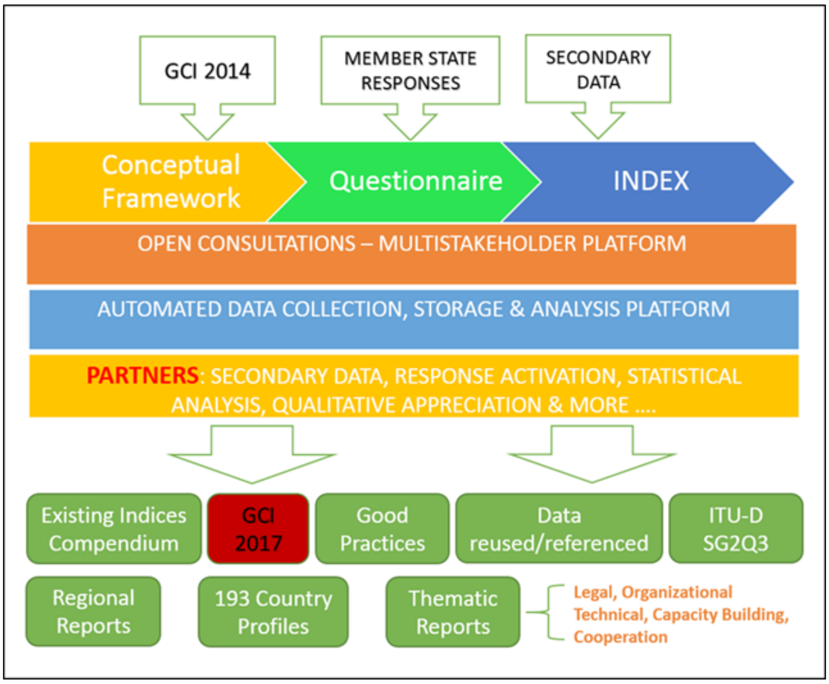

Legal
- Legal Measures Strategy
- Government Legal Authority
- Adequate and harmonized legal frameworks
Technical
- National Cybersecurity Goals and Framework
- Secure Government Infrastructure
- Global Technical Collaboration
Organizational
- Government Coordination
- National Focal Point
- National CIRT
- Public-Private Partnerships
Capacity Building
- Cybersecurity Skills and Training
- Culture of Cybersecurity
- Cybersecurity Innovation
Cooperation
- Enhanced collaboration (multi-stakeholder, Bi/Multi lateral)
- Inter-Agency Collaboration

Figure 5A: GCI approach


GCI 2014
MEMBER STATE RESPONSES
SECONDARY DATA
Conceptual Framework
Questionnaire
INDEX
OPEN CONSULTATIONS – MULTISTAKEHOLDER PLATFORM
AUTOMATED DATA COLLECTION, STORAGE & ANALYSIS PLATFORM
PARTNERS: SECONDARY DATA, RESPONSE ACTIVATION, STATISTICAL ANALYSIS, QUALITATIVE APPRECIATION & MORE ....
Existing Indices Compendium
GCI 2017
Good Practices
Data reused/referenced
ITU-D SG2Q3
Regional Reports
193 Country Profiles
Thematic Reports
Legal, Organizational Technical, Capacity Building, Cooperation

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[44] 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 (ISC^2), 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

[44] 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.[45] 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

[45] 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 inter-connected.

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)[46] is an independent driving force and partner supporting government, businesses and research in facing up to and dealing with information security issues.[47] 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.

Country: United Kingdom of Great Britain and Northern Ireland

Document: 2/228

Title: Cybersecurity in government and industry

[46] http://www.norsis.no.

[47] Document SG2RGQ/204, "Creating a metric for cyber security culture", Norway.

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 cyber-security 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.[48]

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.

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

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

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*.[49]

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.

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.

[49] 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.

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.[50]

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.

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

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.[51] Intel's pilot project focused on

[51] 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.

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.[52]

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.

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.

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

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[53].

– **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.

g) DHS' co-leader in the Stop.Think.Connect.™ Campaign, the National Cyber Security Alliance,[54] 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.

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

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

- **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).
- 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.

1.1.1.1 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.

1.1.1.2 Section 3: Metrics

This section describes the type of metrics the Stop.Think.Connect.™ Campaign uses to track and evaluate its cyber awareness programming.[55] Countries may find the outlined metrics useful as a baseline for establishing their own measures of effectiveness.

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

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.
- **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[56] 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 development projects such as the PRACTICE project.[57] 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).

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

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

(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:

- 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.

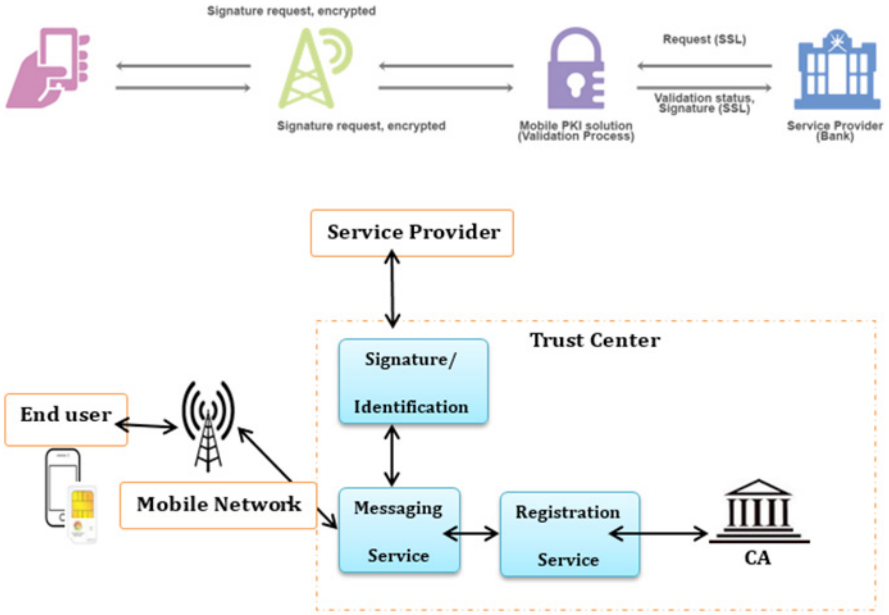
Table 4A: Different types of services options to be provided to Government and commercial entities

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


Signature request, encrypted
Signature request, encrypted
Request (SSL)
Validation status, Signature (SSL)
Mobile PKI solution (Validation Process)
Service Provider (Bank)
Service Provider
Trust Center
Signature/ Identification
End user
Mobile Network
Messaging Service
Registration Service
CA

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[58], 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.

[58] 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:

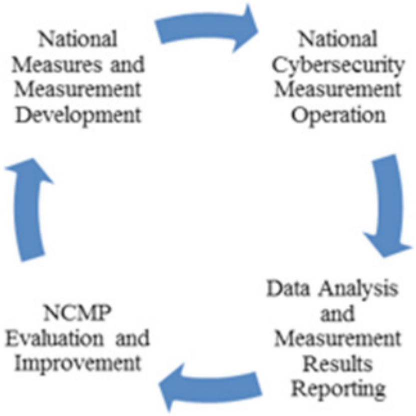
- Implementation or compliance metrics,
- Effectiveness/efficiency metrics, and
- Impact metrics.

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


National Measures and Measurement Development
National Cybersecurity Measurement Operation
Data Analysis and Measurement Results Reporting
NCMP Evaluation and Improvement

A general framework for NCMP

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

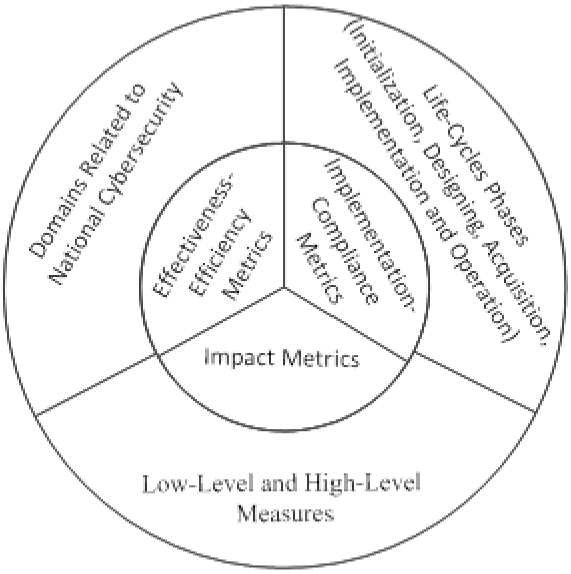
- Measures and measurement development;
- National cybersecurity measurement operation;
- Data analysis and measurement results reporting, and using them for proper decision making;
- NCMP evaluation and improvement.

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


Domains Related to National Cybersecurity
Life-Cycles Phases (Initialization, Designing, Acquisition, Implementation and Operation)
Effectiveness-Efficiency Metrics
Implementation-Compliance Metrics
Impact Metrics
Low-Level and High-Level 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
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)

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 cyber-security 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**
	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
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:

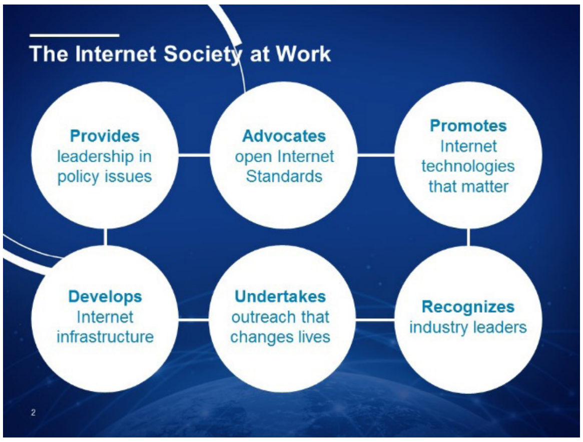
- Fostering confidence and protecting opportunities: The objective of security is to foster confidence in the Internet and to ensure the continued success of the Internet as a driver for economic and social innovation.
- Collective Responsibility: Internet participants share a responsibility towards 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

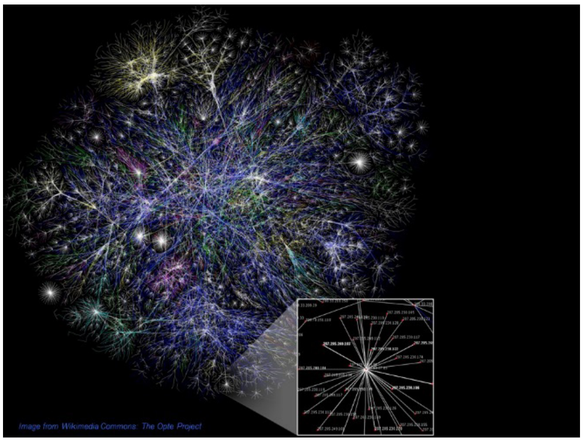


Image from Wikimedia Commons: The Opte Project

Wikimedia commons

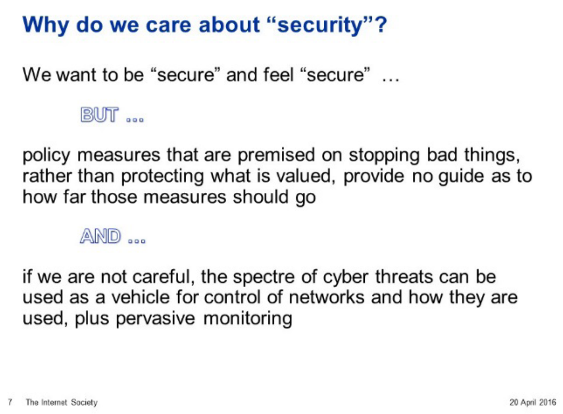
The complexity of the security landscape

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



Why do we care about “security”?

We want to be “secure” and feel “secure” …

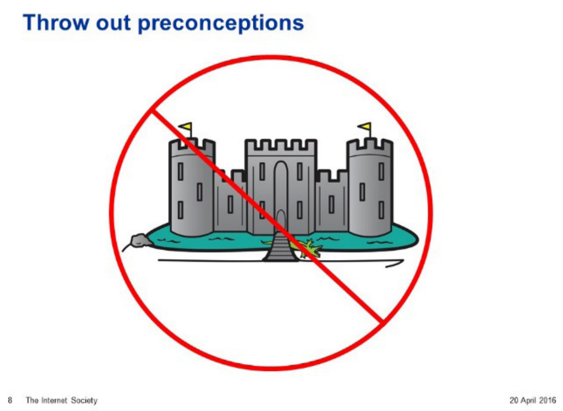
BUT …

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 …

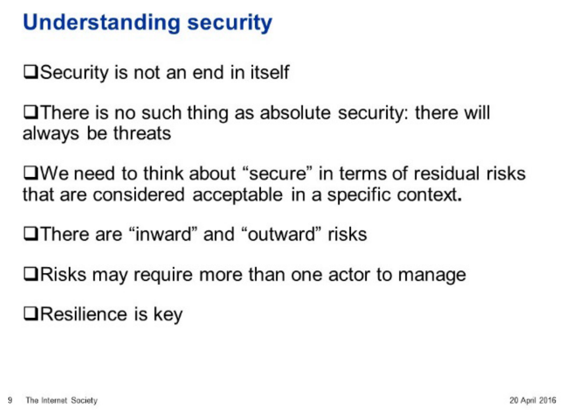
if we are not careful, the spectre of cyber threats can be used as a vehicle for control of networks and how they are used, plus pervasive monitoring

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

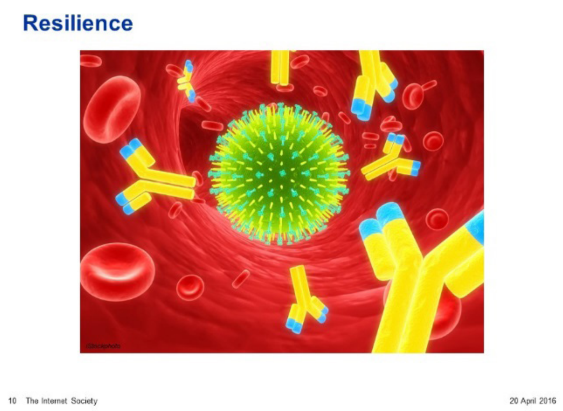
❑We need to think about “secure” in terms of residual risks that are considered acceptable in a specific context.

❑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



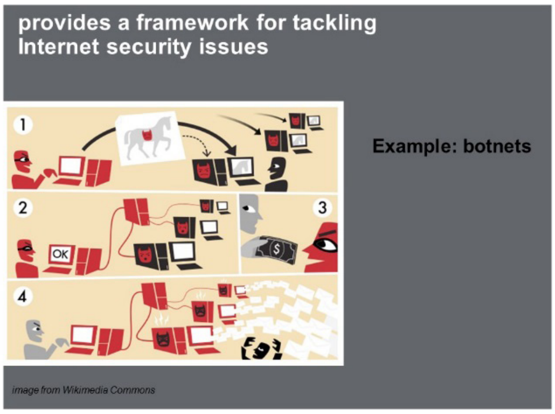
Resilience

10 The Internet Society 20 April 2016

Internet Society Collaborative Security approach

www.internetsociety.org

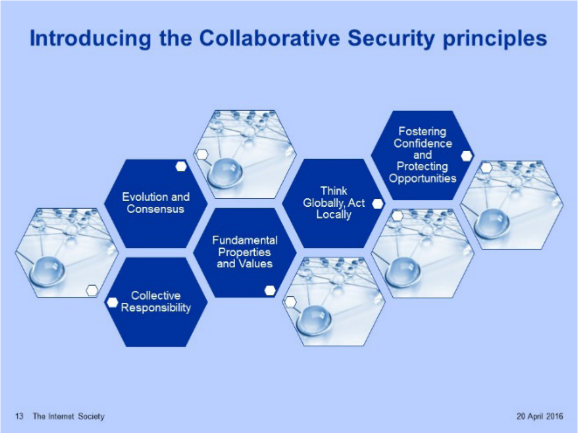
Internet Society



provides a framework for tackling Internet security issues

Example: botnets

image from Wikimedia Commons



Introducing the Collaborative Security principles

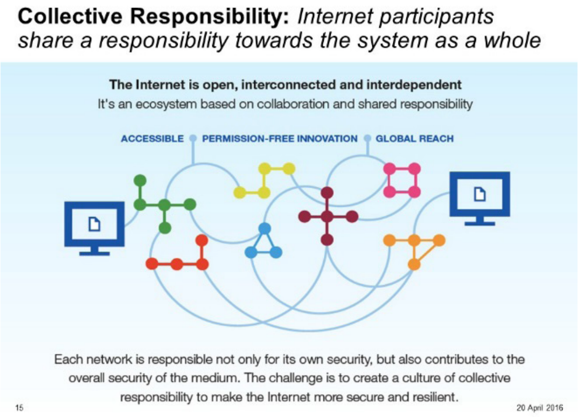
Evolution and Consensus
Fundamental Properties and Values
Collective Responsibility
Think Globally, Act Locally
Fostering Confidence and Protecting Opportunities

13 The Internet Society 20 April 2016

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*

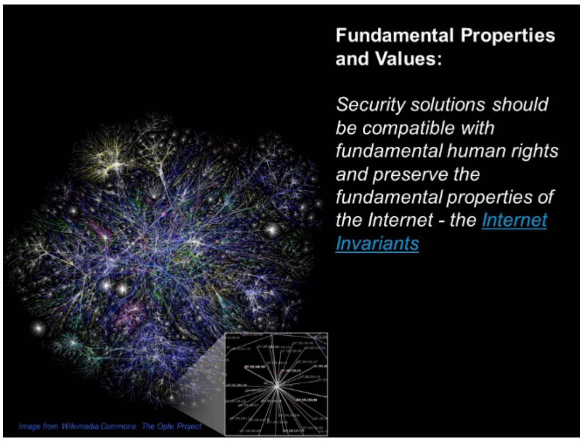
The Internet is open, interconnected and interdependent

It's an ecosystem based on collaboration and shared responsibility

Each network is responsible not only for its own security, but also contributes to the overall security of the medium. The challenge is to create a culture of collective responsibility to make the Internet more secure and resilient.

15

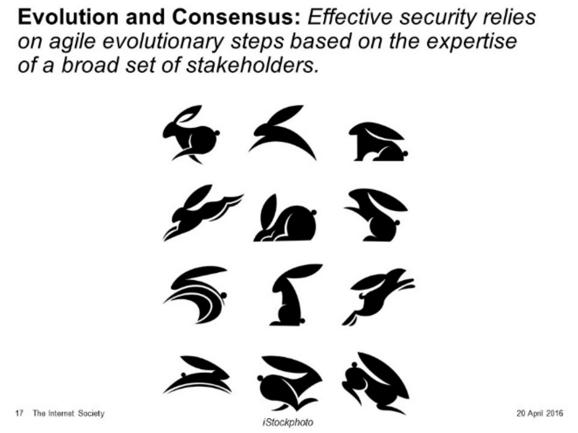
20 April 2016



Fundamental Properties and Values:

Security solutions should be compatible with fundamental human rights and preserve the fundamental properties of the Internet - the Internet Invariants

Image from Wikimedia Commons: The Opte Project



Evolution and Consensus: *Effective security relies on agile evolutionary steps based on the expertise of a broad set of stakeholders.*

iStockphoto

17 The Internet Society

20 April 2016

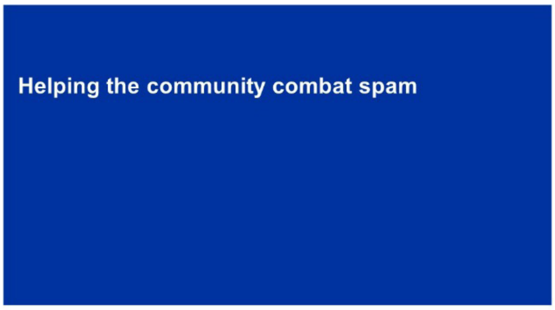
Think Globally, Act Locally:

It is through voluntary bottom-up self-organization that the most impactful solutions are likely to be reached.

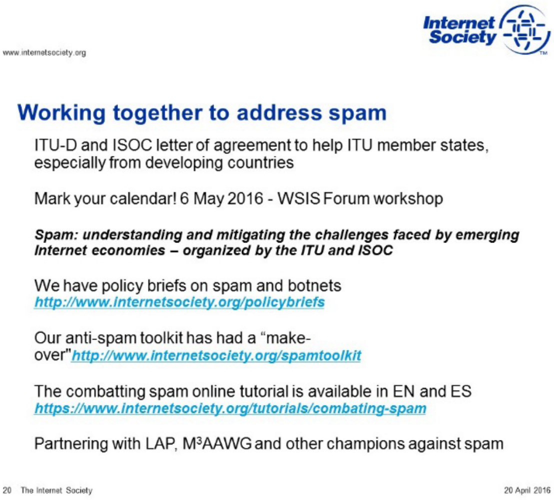
iStockphoto

18 The Internet Society

20 April 2016



Helping the community combat spam



www.internetsociety.org

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, M^{3}AAWG and other champions against spam

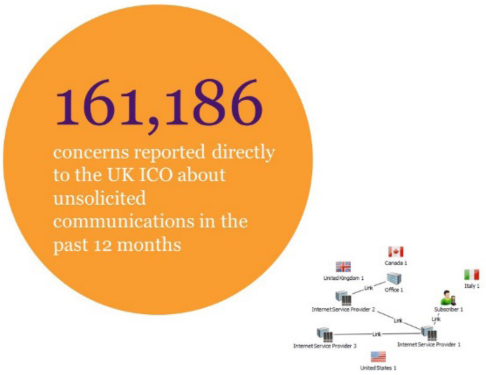
20 The Internet Society 20 April 2016

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.

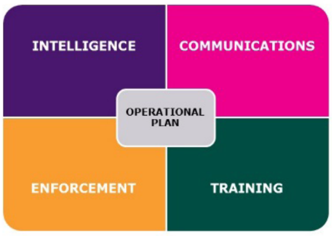
Introducing
the London Action Plan



161,186

concerns reported directly to the UK ICO about unsolicited communications in the past 12 months

LAP Priorities 2016-18



INTELLIGENCE

COMMUNICATIONS

OPERATIONAL PLAN

ENFORCEMENT

TRAINING

Evolving threats identifying opportunities
Understanding and best practices
ØPERATIØN SAFETY-NET
BEST PRACTICES TO ADDRESS ONLINE, MOBILE, AND TELEPHONY THREATS
PREPARED BY THE
MESSAGING, MALWARE AND MOBILE ANTI-ABUSE WORKING GROUP
AND THE
LONDON ACTION PLAN
JUNE 1, 2015

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
	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

Web	Received	Source	Title	Mapping in final report
RGQ/46 +Ann.1	2015-03-12	Iran (Islamic Republic of)	National cybersecurity measures and measurement	Section 4 or 7 Compendium Annex 2
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	-

Web	Received	Source	Title	Mapping in final report
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)
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	

Web	Received	Source	Title	Mapping
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)	
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	

Web	Received	Source	Title	Mapping
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)	
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
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

Web	Received	Source	Title
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
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

Web	Received	Source	Title
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
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

Web	Received	Source	Title
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
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 **C**yber **T**hreats response InitiatiVE) project**

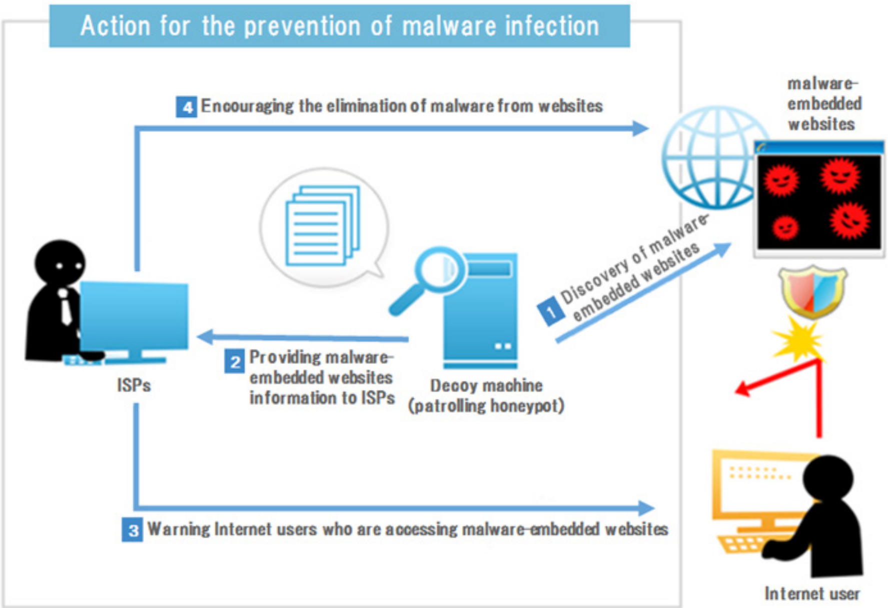
a) Prevention of malware infection; cooperation with ISPs

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


Action for the prevention of malware infection
4 Encouraging the elimination of malware from websites
malware-embedded websites
1 Discovery of malware-embedded websites
ISPs
2 Providing malware-embedded websites information to ISPs
Decoy machine (patrolling honeypot)
3 Warning Internet users who are accessing malware-embedded websites
Internet user

(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.

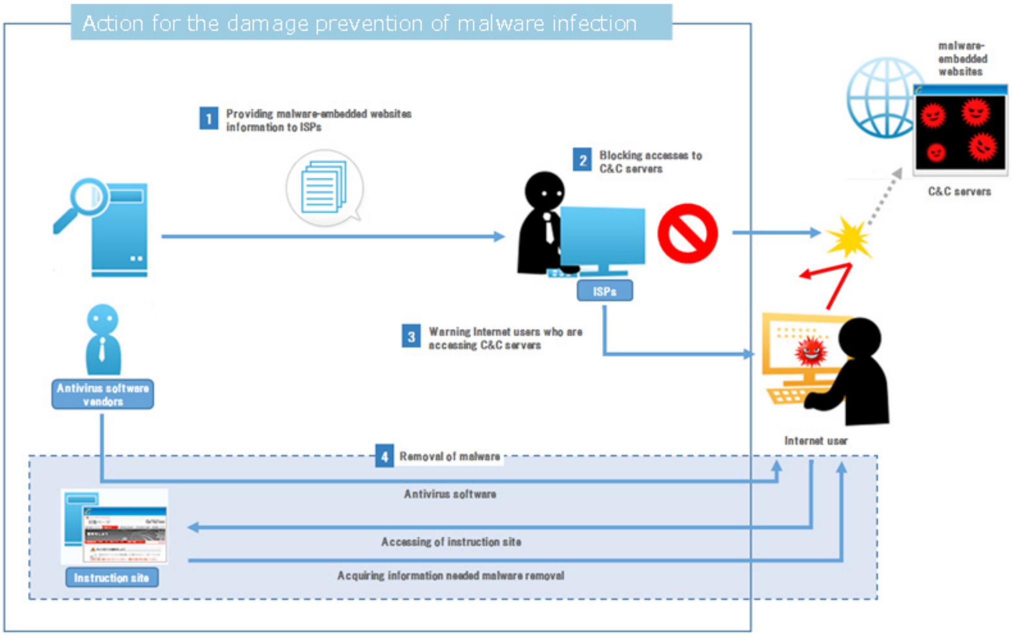
(4) Warning administrators of malware-embedded websites: ISPs send warning statements to the administrators of websites discovered to have embedded malware to request removal of malware from their sites.

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


Action for the damage prevention of malware infection
1 Providing malware-embedded websites information to ISPs
2 Blocking accesses to C&C servers
ISPs
malware-embedded websites
C&C servers
3 Warning Internet users who are accessing C&C servers
Antivirus software vendors
Internet user
4 Removal of malware
Antivirus software
Accessing of instruction site
Acquiring information needed malware removal
Instruction site

(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.

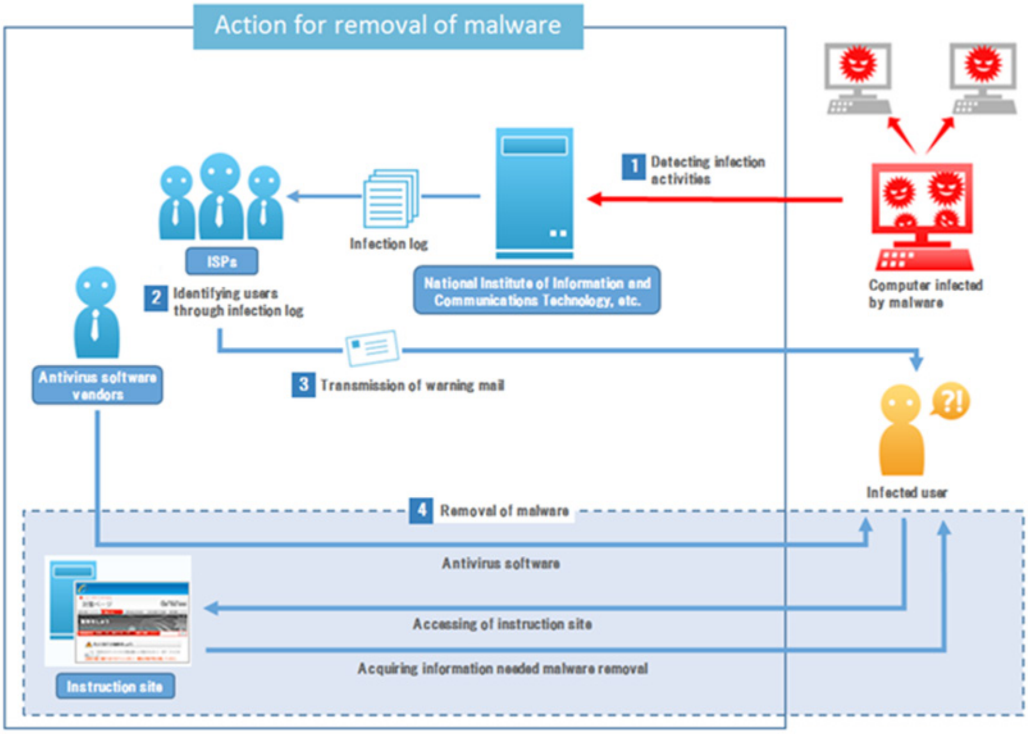
(4) Malware removed: The Internet users access the instruction site and get information needed to remove malware. The instruction site provides useful information such as antivirus vendors' site where antivirus softwares can be downloaded to remove malware.

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


Action for removal of malware
1 Detecting infection activities
ISPs
Infection log
National Institute of Information and Communications Technology, etc.
Computer infected by malware
2 Identifying users through infection log
Antivirus software vendors
3 Transmission of warning mail
Infected user
4 Removal of malware
Antivirus software
Accessing of instruction site
Acquiring information needed malware removal
Instruction site

(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.

Unión Internacional de las Telecomunicaciones (UIT)
Oficina de Desarrollo de las Telecomunicaciones (BDT)
Oficina del Director
Place des Nations
CH-1211 Ginebra 20 – Suiza
Correo-e: bdtdirector@itu.int
Tel.: +41 22 730 5035/5435
Fax: +41 22 730 5484

Director Adjunto y
Jefe del Departamento de
Administración y Coordinación
de las Operaciones (DDR)
Correo-e: bdtdeputydir@itu.int
Tel.: +41 22 730 5784
Fax: +41 22 730 5484

Departamento de Infraestructura,
Entorno Habilitador y
Ciberaplicaciones (IEE)
Correo-e: bdtiee@itu.int
Tel.: +41 22 730 5421
Fax: +41 22 730 5484

Departamento de Innovación y
Asociaciones (IP)
Correo-e: bdtip@itu.int
Tel.: +41 22 730 5900
Fax: +41 22 730 5484

Departamento de Proyectos y
Gestión del Conocimiento (PKM)
Correo-e: bdtpkm@itu.int
Tel.: +41 22 730 5447
Fax: +41 22 730 5484

África

Etiopía

International Telecommunication
Union (ITU)
Oficina Regional
P.O. Box 60 005
Gambia Rd., Leghar ETC Building
3rd floor
Addis Ababa – Etiopía

Correo-e: ituaddis@itu.int
Tel.: +251 11 551 4977
Tel.: +251 11 551 4855
Tel.: +251 11 551 8328
Fax: +251 11 551 7299

Camerún

Union internationale des
télécommunications (UIT)
Oficina de Zona
Immeuble CAMPOST, 3^{e} étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé – Camerún

Correo-e: itu-yaounde@itu.int
Tel.: + 237 22 22 9292
Tel.: + 237 22 22 9291
Fax: + 237 22 22 9297

Senegal

Union internationale des
télécommunications (UIT)
Oficina de Zona
8, Route du Méridien
Immeuble Rokhaya
B.P. 29471 Dakar-Yoff
Dakar – Senegal

Correo-e: itu-dakar@itu.int
Tel.: +221 33 859 7010
Tel.: +221 33 859 7021
Fax: +221 33 868 6386

Zimbabwe

International Telecommunication
Union (ITU)
Oficina de Zona de la UIT
TelOne Centre for Learning
Corner Samora Machel and
Hampton Road
P.O. Box BE 792 Belvedere
Harare – Zimbabwe
Correo-e: itu-harare@itu.int
Tel.: +263 4 77 5939
Tel.: +263 4 77 5941
Fax: +263 4 77 1257

Américas

Brasil

União Internacional de
Telecomunicações (UIT)
Oficina Regional
SAUS Quadra 06, Bloco "E"
10º andar, Ala Sul
Ed. Luis Eduardo Magalhães (Anatel)
70070-940 Brasilia, DF – Brazil

Correo-e: itubrasilia@itu.int
Tel.: +55 61 2312 2730-1
Tel.: +55 61 2312 2733-5
Fax: +55 61 2312 2738

Barbados

International Telecommunication
Union (ITU)
Oficina de Zona
United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown – Barbados

Correo-e: itubridgetown@itu.int
Tel.: +1 246 431 0343/4
Fax: +1 246 437 7403

Chile

Unión Internacional de
Telecomunicaciones (UIT)
Oficina de Representación de Área
Merced 753, 4.º piso
Casilla 50484 – Plaza de Armas
Santiago de Chile – Chile

Correo-e: itusantiago@itu.int
Tel.: +56 2 632 6134/6147
Fax: +56 2 632 6154

Honduras

Unión Internacional de
Telecomunicaciones (UIT)
Oficina de Representación de Área
Colonia Palmira, Avenida Brasil
Ed. COMTELCA/UIT, 4.º piso
P.O. Box 976
Tegucigalpa – Honduras

Correo-e: itutegucigalpa@itu.int
Tel.: +504 22 201 074
Fax: +504 22 201 075

Estados Árabes

Egipto

International Telecommunication
Union (ITU)
Oficina Regional
Smart Village, Building B 147, 3rd floor
Km 28 Cairo – Alexandria Desert Road
Giza Governorate
El Cairo – Egipto

Correo-e: itu-ro-arabstates@itu.int
Tel.: +202 3537 1777
Fax: +202 3537 1888

Asia-Pacífico

Tailandia

International Telecommunication
Union (ITU)
Oficina de Zona
Thailand Post Training Center ,5th floor
111 Chaengwattana Road, Laksi
Bangkok 10210 – Tailandia

Dirección postal:
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210, Tailandia

Correo-e: itubangkok@itu.int
Tel.: +66 2 575 0055
Fax: +66 2 575 3507

Indonesia

International Telecommunication
Union (ITU)
Oficina de Zona
Sapta Pesona Building, 13th floor
JI. Merdan Merdeka Barat No. 17
Jakarta 10110 – Indonesia

Dirección postal:
c/o UNDP – P.O. Box 2338
Jakarta 10110 – Indonesia

Correo-e: itujakarta@itu.int
Tel.: +62 21 381 3572
Tel.: +62 21 380 2322/2324
Fax: +62 21 389 05521

Países de la CEI

Federación de Rusia

International Telecommunication
Union (ITU)
Oficina de Zona
4, Building 1
Sergiy Radonezhsky Str.
Moscú 105120 – Federación de Rusia

Dirección postal:
P.O. Box 47 – Moscú 105120
Federación de Rusia

Correo-e: itumoskow@itu.int
Tel.: +7 495 926 6070
Fax: +7 495 926 6073

Europa

Suiza

Unión Internacional de las
Telecomunicaciones (UIT)
Oficina de Desarrollo de las
Telecomunicaciones (BDT)
Oficina de Zona
Place des Nations
CH-1211 Ginebra 20 – Suiza
Correo-e: eurregion@itu.int
Tel.: +41 22 730 6065

Unión Internacional de Telecomunicaciones
Oficina de Desarrollo de las Telecomunicaciones
Place des Nations
CH-1211 Ginebra 20
Suiza
www.itu.int

ISBN 978-92-61-23003-6
9 789261 230036

Impreso en Suiza
Ginebra, 2017

07/2017