Rapport Final

UIT-D
Commission d'Études 2

Question 3/2

Sécurisation des réseaux d'information et de communication: bonnes pratiques pour créer une culture de la cybersécurité

6e Période d'Études
2014-2017

NOUS CONTACTER

Site web: www.itu.int/ITU-D/study-groups
Librairie électronique: www.itu.int/pub/D-STG/
E-mail: devsg@itu.int
Téléphone: +41 22 730 5999

Question 3/2: Sécurisation des réseaux d'information et de communication: bonnes pratiques pour créer une culture de la cybersécurité

Rapport final

Préface

Les commissions d'études du Secteur du Développement des télécommunications de l'UIT (UIT-D) offrent un cadre neutre reposant sur les contributions, dans lequel des spécialistes des pouvoirs publics, du secteur privé et des milieux universitaires se réunissent afin d'élaborer des outils pratiques, des lignes directrices utiles et des ressources pour résoudre les problèmes de développement. Dans le cadre des travaux des commissions d'études de l'UIT-D, les Membres du Secteur étudient et analysent des questions de télécommunication/TIC précises axées sur les tâches, afin de progresser plus rapidement en ce qui concerne les priorités des pays en matière de développement.

Les commissions d'études offrent à tous les Membres du Secteur l'occasion d'échanger des données d'expérience, de présenter des idées, de dialoguer et de parvenir à un consensus sur les stratégies à adopter pour répondre aux priorités dans le domaine des télécommunications/TIC. Elles sont chargées d'élaborer des rapports, des lignes directrices et des recommandations sur la base des contributions et des documents soumis par les membres. Des données, qui sont recueillies grâce à des enquêtes, des contributions et des études de cas, sont mises à la disposition des membres, qui peuvent les consulter facilement en utilisant les outils de gestion de contenus et de publication sur le web. Les travaux des commissions d'études de l'UIT-D se rapportent aux différents programmes et initiatives adoptés par l'UIT-D, l'objectif étant de créer des synergies dans l'intérêt des membres pour ce qui est des ressources et des compétences techniques. La collaboration avec d'autres groupes et organisations travaillant sur des questions connexes est essentielle.

Les sujets sur lesquels les commissions d'études de l'UIT-D travaillent sont choisis tous les quatre ans par la Conférence mondiale de développement des télécommunications (CMDT), qui établit des programmes de travail et des directives, afin de définir les questions et priorités relatives au développement des télécommunications/TIC pour les quatre années suivantes.

Le domaine de compétence de la **Commission d'études 1 de l'UIT-D** est l'étude d'un "**Environnement propice au développement des télécommunications/TIC**", tandis que celui de la **Commission d'études 2 de l'UIT-D** est l'étude du thème "**Applications des TIC, cybersécurité, télécommunications d'urgence et adaptation aux effets des changements climatiques**".

Pendant la période d'études 2014-2017, la **Commission d'études 2 de l'UIT-D** était placée sous la présidence de M. Ahmad Reza Sharafat (République islamique d'Iran), assisté des Vice-Présidents Aminata Kaba-Camara (République de Guinée), Christopher Kemei (République du Kenya), Celina Delgado (Nicaragua), Nasser Al Marzouqi (Emirats arabes unis), Nadir Ahmed Gaylani (République du Soudan), Ke Wang (République populaire de Chine), Ananda Raj Khanal (République du Népal), Evgeny Bondarenko (Fédération de Russie), Henadz Asipovich (République du Bélarus) et Petko Kantchev (République de Bulgarie), qui représentaient les six régions.

Rapport final

Le présent rapport final sur la **Question 3/2 "Sécurisation des réseaux d'information et de communication: bonnes pratiques pour créer une culture de la cybersécurité"** a été élaboré sous la direction des deux Corapporteurs pour cette Question, Rozalin Basheer Faqeer Al-Balushi (Autorité de régulation des télécommunications d'Oman (TRA), Oman) et Eliot Lear (Etats-Unis d'Amérique), et de sept Vice-Rapporteurs nommés, Damnam Kanlanfei Bagolibe (Togo), Christopher Ganizani Banda (Malawi), Albert Kamga (Cameroun), Miho Naganuma (Japon), Jean-David Rodney (Haïti), Jabin S. Vahora (Etats-Unis d'Amérique) et Jaesuk Yun (République de Corée). Les Corapporteurs et les Vice-Rapporteurs ont par ailleurs bénéficié de l'assistance des coordonnateurs de l'UIT-D et du secrétariat des commissions d'études de l'UIT-D.

ISBN

978-92-61-22992-4 (Version papier)

978-92-61-23002-9 (Version électronique)

978-92-61-23012-8 (Version EPUB)

978-92-61-23022-7 (Version Mobi)

Table des matières

Préface ii

Rapport final iii

Résumé ix
- i. Résumé analytique ix
- ii. Introduction ix

1 CHAPITRE 1 – Questionnaire sur la sensibilisation à la cybersécurité 1
- 1.1 Méthodes de collecte des informations 1
- 1.2 Analyse des données des campagnes de sensibilisation 2

2 CHAPITRE 2 – La situation du spam et des logiciels malveillants, des mesures d'atténuation et des aspects réglementaires 9
- 2.1 Sources de spam 10
- 2.2 Impact du spam sur le réseau 11
- 2.3 Les risques du harponnage et les moyens de lutte 11
- 2.4 Impact des politiques sur le spam 12

3 CHAPITRE 3 – Améliorer la position nationale en matière de cybersécurité: renforcer la sensibilisation et les ressources humaines 13
- 3.1 Campagnes de sensibilisation 13
  - 3.1.1 Bonnes pratiques pour un programme de communication 13
  - 3.1.2 Modèle de plan de communication 15
  - 3.1.3 Stratégies de campagne 16
  - 3.1.4 Mesure de la réussite et paramètres 17
- 3.2 Mesures supplémentaires de renforcement des capacités 18
  - 3.2.1 Activités menées au Japon 18
  - 3.2.2 Activités menées en république de Corée 19
  - 3.2.3 Activités menées dans la région de la CEI 19
  - 3.2.4 Activités menées en Norvège 20
- 3.3 Partenariats public-privé 21

4 CHAPITRE 4 – Protection en ligne des enfants (COP) 22
- 4.1 Résultats de l'enquête sur la protection en ligne des enfants 22
- 4.2 Stratégies et solutions techniques pour la protection en ligne des enfants 26
  - 4.2.1 Sensibilisation à la COP et activités connexes 28
  - 4.2.2 Stratégies relatives à la protection en ligne des enfants 29

5 CHAPITRE 5 – Résultats des ateliers sur la cybersécurité 31
- 5.1 Premier atelier sur la cybersécurité (8 septembre 2015) 31
- 5.2 Deuxième atelier sur la cybersécurité (18-19 avril 2016) 32
- 5.3 Troisième atelier sur la cybersécurité (26 janvier 2017) 34

6 CHAPITRE 6 – La cybersécurité: possibilités et défis 36
- 6.1 Addiction à l'Internet 36
- 6.2 Sécurité des transactions électroniques 39
- 6.3 Partenariats pour la cybersécurité 43

7 CHAPITRE 7 – Expériences nationales: cadre de critères communs en matière de sécurité 44

8 CHAPITRE 8 – Conclusions et recommandations pour la prochaine période d'études 46

Abbreviations and acronyms 47

Annexes 50

Annex 1: The Global Cybersecurity Index 2017 50
1.2.1 National CERT/CIRT/CSIRT 56
1.2.2 Government CERT/CIRT/CSIRT 57
1.2.3 Sectoral CERT/CIRT/CSRIT 57
1.2.4 Cybersecurity standards implementation framework for organizations 57
1.2.5 Cybersecurity standards and certification for professionals 57
1.2.6 Child Online Protection 57
1.3.1 Strategy 58
1.3.2 Responsible agency 58
1.3.3 Cybersecurity metrics 58
1.4.1 Standardization bodies 59
1.4.2 Cybersecurity best practices 59
1.4.3 Cybersecurity research and development programmes 59
1.4.4 Public awareness campaigns 59
1.4.5 Cybersecurity professional training courses 59
1.4.6 National education programmes and academic curricula 60
1.4.7 Incentive mechanisms 60
1.6.1 Bilateral agreements 60
1.6.2 Multilateral agreements 61
1.6.3 Public-private partnerships 61
1.6.4 Interagency partnerships 61

Annex 2: Compendium on cybersecurity country case studies 62

Annex 3: Cybersecurity activities being conducted by organizations, private sector, and civil society 130

Annex 4: Contributions mapping 148

Annex 5: Survey questions 160

Annex 6: Information on ACTIVE 163

Liste des tableaux, figures et encadrés

Tableaux

Tableau 1: Nombre de participants au cours d'éducation préventive 37
Tableau 2: Nombre de services de conseils par type 38
Table 1A: Most committed countries, GCI (normalized score) 51
Table 2A: Number of participants of preventive education 100
Table 3A: Number of counselling service by type 101
Table 4A: Different types of services options to be provided to Government and commercial entities 105
Table 5A: Different types of services options to be provided to individuals 105
Table 6A: Customized template for national cybersecurity measures 107

Figures

Figure 1 : Réponses à l'enquête sur la sensibilisation à la cybersécurité par région 2
Figure 2 : Importance de la sensibilisation à la cybersécurité 2
Figure 3 : Campagnes de sensibilisation du public à la cybersécurité 3
Figure 4 : Importance de la sensibilisation à la cybersécurité pour les organisations/la société civile 3
Figure 5 : Groupes d'âge ciblés par les campagnes de sensibilisation à la cybersécurité 4
Figure 6 : Groupes cibles des campagnes de sensibilisation à la cybersécurité 4
Figure 7 : Groupes visés en priorité par les campagnes de sensibilisation à la cybersécurité 5
Figure 8 : Thèmes abordés par les campagnes de sensibilisation à la cybersécurité 6
Figure 9 : Importance de chaque thème dans les campagnes de sensibilisation à la cybersécurité 6
Figure 10 : Information du public sur les avantages de solutions logicielles/matérielles ou fondées sur des services 7
Figure 11 : Solutions logicielles/matérielles ou fondées sur des services mises à la disposition du public 8
Figure 12 : Le cercle vicieux du spam et de la cybersécurité 9
Figure 13 : Comment rompre le cercle vicieux 10
Figure 14 : Aperçu des activités menées dans le cadre du projet ACTIVE 18
Figure 15 : Existe-t-il un organisme/une entité responsable de la protection en ligne des enfants? 23
Figure 16 : Existe-t-il un mécanisme public établi de notification des problèmes liés à la protection en ligne des enfants? 23
Figure 17 : Des mécanismes et des moyens techniques ont-ils été mis à disposition pour faciliter la protection en ligne des enfants? 24
Figure 18 : Les autorités publiques ou les ONG ont-elles entrepris des activités pour aider et informer les différents acteurs (parents, responsables locaux, enseignants, etc.) sur la façon de protéger les enfants en ligne? 24
Figure 19 : Campagnes de sensibilisation du public à la cybersécurité élaborées et mises en œuvre/organisme/entité responsable de la protection en ligne des enfants? 25
Figure 20 : Existe-t-il des campagnes de sensibilisation à la protection en ligne des enfants destinées aux enfants? 26
Figure 21 : Existe-t-il des campagnes de sensibilisation du public à la protection en ligne des enfants? 26
Figure 22 : Campagnes de sensibilisation à la protection en ligne des enfants destinées aux enfants/adultes 28
Figure 1A: GCI heat map 50
Figure 2A: GCA 52
Figure 3A: GCA linkages 53

Figure 4A: Global cybersecurity agenda 55
Figure 5A: GCI approach 55
Figure 6A: Oman PKI 106
Figure 7A: General framework of NCMP major processes that collectively comprise a NCMP 111
Figure 8A: General scope for national cybersecurity measures 112
Figure 9A: Prevention of malware infection 163
Figure 10A: Damage prevention of malware infection 164
Figure 11A: Removal of malware 165

Résumé

i. Résumé analytique

Le présent rapport aborde de nombreux aspects liés à l'objet de la Question 3/2: «Sécurisation des réseaux d'information et de communication: bonnes pratiques pour créer une culture de la cybersécurité» pendant la période d'études de trois ans qui prendra fin en avril 2017. Nous analyserons tout d'abord les résultats de l'enquête sur la sensibilisation à la cybersécurité menée par le Bureau de Développement des Télécommunications (BDT). Il ressort de cette enquête que si un certain nombre de pays doivent encore améliorer la sensibilisation à la sécurité, d'autres ne progressent pas dans cette voie et ceux qui s'efforcent d'améliorer la sensibilisation à la sécurité ne visent pas les secteurs clés de la société. Bien souvent, la priorité est essentiellement accordée à la protection en ligne des enfants. On trouvera dans le présent rapport une vue d'ensemble du spam, de ses causes et des moyens à mettre en œuvre pour lutter contre ce phénomène. Même si la largeur de bande consommée par le courrier électronique est généralement faible, les conséquences qui en résultent sur le plan de la dégradation de la qualité de la communication demeurent un sujet de préoccupation. Le rapport donne un aperçu des activités de communication menée par les pouvoirs publics pour améliorer l'attitude générale de la société à l'égard de la cybersécurité.

Alors que la dernière période d'études (2010-2014) était axée sur différentes formations proposées par l'intermédiaire du BDT, la période d'études actuelle (2014-2017) a été davantage caractérisée par l'organisation d'ateliers visant à rassembler un large éventail d'acteurs et à mettre leurs contenus à la disposition des pays en développement. On trouvera dans le présent rapport un résumé de ces ateliers, avec des liens vers leurs contenus.

Le rapport contient également, en annexe, des renseignements sur l'Indice mondial de cybersécurité (GCI) que le Bureau de développement des télécommunications (BDT) de l'UIT a rassemblés pendant plusieurs années.

Le rapport contient en conclusion des pistes de réflexion et certaines recommandations appelant un complément d'étude.

ii. Introduction

Dans le cadre de la Question 3/2 qui lui a été confiée, la Commission d'Études 2 de l'UIT-D établit des rapports sur les bonnes pratiques concernant divers aspects de la cybersécurité. Il s'agit ici du rapport final sur les activités menées par la Commission d'Études 2 de l'UIT-D au titre de la Question 3/2 au cours du dernier cycle d'études de trois ans, qui couvre la période 2014-2017. Le programme de travail au titre de la Question 3/2 a été défini par la Conférence Mondiale de Développement des télécommunications (CMDT) qui s'est tenue à Dubaï (Emirats Arabes Unis) en 2014. Au cours des trois dernières années, les responsables de l'étude de la Question 3/2 ont traité la plupart des questions relevant de ce programme de travail.

Le rapport final se compose de plusieurs rapports sur les bonnes pratiques concernant différents aspects de la cybersécurité.

Le **Chapitre 1** est consacré à l'enquête sur la sensibilisation à la cybersécurité.

Le **Chapitre 2** examine la situation dans les domaines des logiciels malveillants et du spam, de l'atténuation de leurs effets et des aspects réglementaires.

Le **Chapitre 3** aborde les enseignements tirés par les pays en matière de campagnes de sensibilisation, d'élaboration de stratégies et de mesure de la cybersécurité.

Le **Chapitre 4** examine l'enquête sur la protection en ligne des enfants et les questions en jeu.

Le **Chapitre 5** traite des résultats des ateliers sur la cybersécurité qui ont été organisés pendant la période d'études.

Le **Chapitre 6** contient un aperçu des travaux que plusieurs organisations ont présenté à la commission d'études.

Le **Chapitre 7** est consacré aux enseignements tirés par les pays partageant les mêmes critères.

Enfin, le **Chapitre 8** conclut le présent rapport en évoquant des domaines futurs à examiner.

Au début du présent rapport, il convient de relever que la Commission d'Études a examiné et commenté tous les documents établis dans le contexte de l'Indice mondial de cybersécurité (GCI) de 2017. Cet indice a été établi sur la base d'une analyse de plus de 134 réponses reçues des 193 Etats Membres dont le coordonnateur pour le GCI (désigné par l'Etat Membre sur demande de l'UIT) a répondu à une enquête en ligne. Les enquêtes sur la sensibilisation à la cybersécurité et sur la protection en ligne des enfants menées par la Commission d'Études au titre de la Question ont été fusionnées avec l'enquête GCI, ce qui a permis de recevoir un nombre de réponses plus élevé (de 51 pendant la dernière période d'études à 129+ pendant la période actuelle).

Le questionnaire[1] GCI 2017 et d'autres documents pertinents (y compris le modèle de référence) ont été examinés et sont inclus dans les **Annexes**. Le résumé des résultats du GCI 2017 figure dans l'**Annexe 1**.

La question étudiée couvrait tous les aspects de notre mandat, à une exception notable près:

f) Examiner les besoins spécifiques des personnes handicapées, en collaboration avec les responsables de l'étude des autres Questions pertinentes.

Ce domaine, bien qu'important, a pâti des effets combinés d'une période d'études écourtée et d'un manque de contributions. Il convient de noter que 69 pour cent des Etats Membres ayant pris part au questionnaire sur la sensibilisation à la sécurité n'ont pas inclus les personnes handicapées dans les groupes cibles, ce qui montre que les travaux doivent se poursuivre dans ce domaine (voir le **§ 1.2** pour plus de précisions).

[1] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2016.aspx.

1 CHAPITRE 1 – Questionnaire sur la sensibilisation à la cybersécurité

La présente section porte sur le point d) de l'objet de la Question 3/2, qui appelle notamment à:

d) Continuer d'analyser les résultats de l'enquête sur la sensibilisation à la cybersécurité réalisée au cours de la dernière période d'études et publier une enquête actualisée, afin d'évaluer les progrès accomplis dans l'intervalle.

La cybersécurité ne pourra être pleinement assurée si la plus grande attention n'est pas donnée à la sensibilisation du public et des utilisateurs. Aucun cadre visant à assurer la cybersécurité n'est viable si la sensibilisation n'est pas un de ses éléments essentiels. Ceci est déterminé par le fait que les personnes intéressées par le cyberespace ou y participant doivent comprendre que la réalisation de la cybersécurité est toujours fondée sur les facteurs clés suivants: i) adoption de la législation nécessaire à la protection de la cybersécurité; ii) coordination et coopération entre les parties concernées (secteurs privé et public); iii) disponibilité d'outils techniques pour assurer la sécurité; iv) coordination internationale; v) mesure périodique de l'efficacité; et vi) sensibilisation.

Etant donné l'importance de la sensibilisation pour assurer la cybersécurité, ce questionnaire a été élaboré pour mesurer le niveau d'intérêt manifesté pour sensibiliser dans ce domaine, définir les groupes visés, organismes publics ou parties concernées, par exemple des entreprises ou institutions privées ou d'autres catégories comme des personnes handicapées et des enfants et pour recenser les cyberrisques les plus élevés rencontrés par les pays.

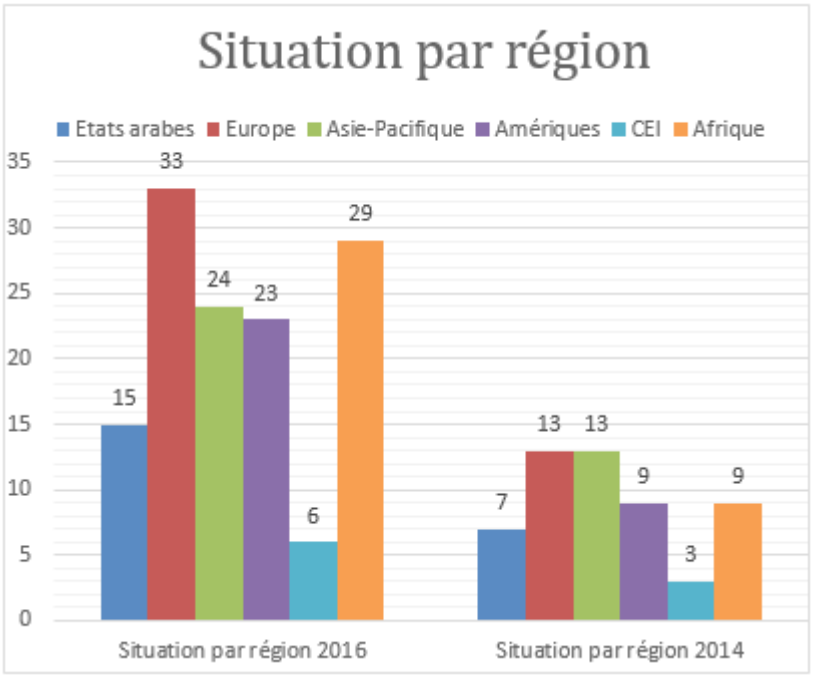
1.1 Méthodes de collecte des informations

Lors de sa deuxième réunion en 2015, la Commission d'Études 2 de l'UIT-D a décidé, au titre de la Question 3/2, d'associer le questionnaire sur la sensibilisation à la cybersécurité et le questionnaire sur la protection en ligne des enfants (COP) au questionnaire relatif à l'Indice mondial de cybersécurité[1] pour réaliser les objectifs similaires de façon efficace, éviter toute répétition des tâches et assurer une participation plus large des Etats Membres.

Le 11 décembre 2015, le questionnaire a été envoyé aux 193 Etats Membres de l'UIT. Cent vingt-neuf des 193 pays ont répondu aux questions relatives à la sensibilisation à la cybersécurité (quelque 63 pour cent des Etats Membres de l'UIT), tandis que 131 pays ont répondu aux questions relatives à la COP (environ 68 pour cent des Etats Membres de l'UIT). L'équipe chargée de coordonner le questionnaire GCI a transmis ces données aux responsables de l'étude de la Question 3/2 qui a alors examiné et analysé les données et inclus les résultats définitifs dans le présent rapport final.

[1] L'Indice mondial de cybersécurité (GCI) est né d'un partenariat entre le secteur privé et une organisation internationale, et a pour vocation de placer la question de la cybersécurité au coeur des stratégies nationales. Le GCI est un projet de recherche conjoint d'ABI Research et de l'Union internationale des télécommunications (UIT) qui fournit des informations sur le niveau d'engagement des Etats souverains en matière de cybersécurité.

Figure 1 : Réponses à l'enquête sur la sensibilisation à la cybersécurité par région

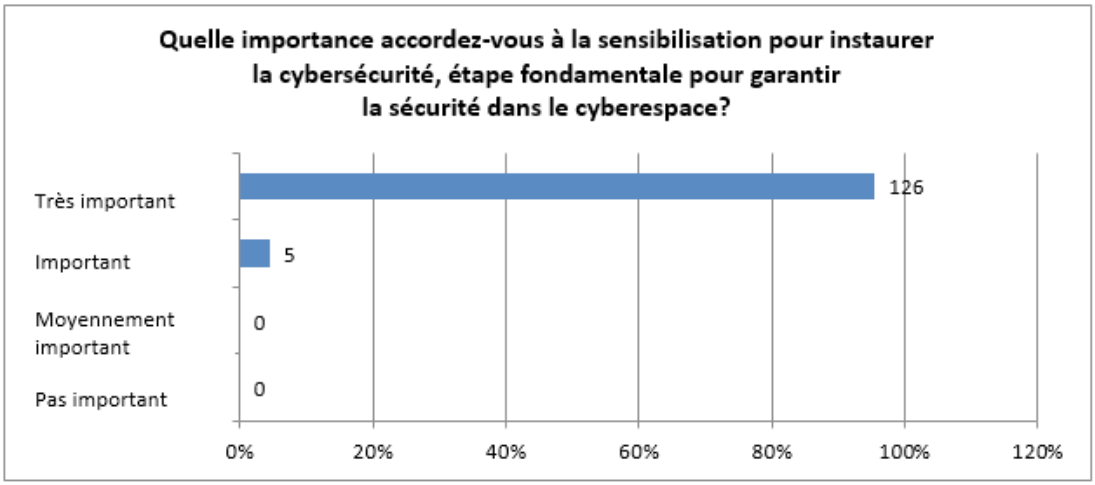


1.2 Analyse des données des campagnes de sensibilisation

L'objectif des questions relatives aux cyberrisques était de déterminer l'importance de la sensibilisation pour assurer la sécurité dans le cyberespace.

95,42 pour cent des personnes ayant répondu au questionnaire ont indiqué que la sensibilisation était « très importante », tandis que 4,58 pour cent ont estimé qu'elle était « importante ». Comparé aux résultats d'un questionnaire similaire soumis pendant la période d'études précédente (2010-2014), le pourcentage de personnes interrogées ayant confirmé que la sensibilisation à la cybersécurité était « très importante » a augmenté. Il était en effet de 79 pour cent pendant la période d'études 2010-2014.

Figure 2 : Importance de la sensibilisation à la cybersécurité



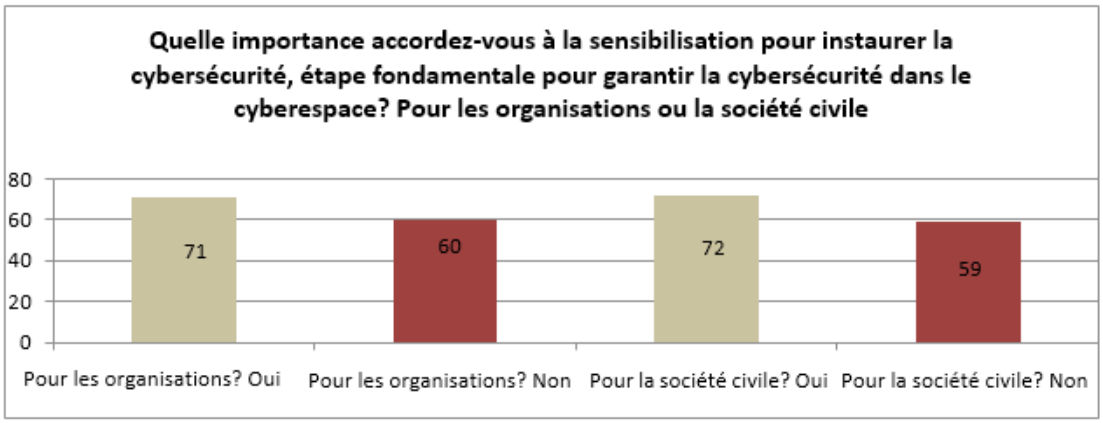
Quatre-vingt-deux pays sur un total de 131 ont conçu et mis en œuvre des campagnes de sensibilisation contre les cyberrisques. Ceci témoigne du fait que les Etats Membres mesurent pleinement

l'importance de la conception et de l'organisation de campagnes de sensibilisation sur les cyberrisques dans leurs pays.

Figure 3 : Campagnes de sensibilisation du public à la cybersécurité

Selon les résultats du questionnaire, les cibles des campagnes de sensibilisation sont le secteur public (71 pays) et la société civile (72 pays). Ceci confirme que les Etats Membres considèrent qu'il est à peu près aussi important de sensibiliser le secteur public que la société civile.

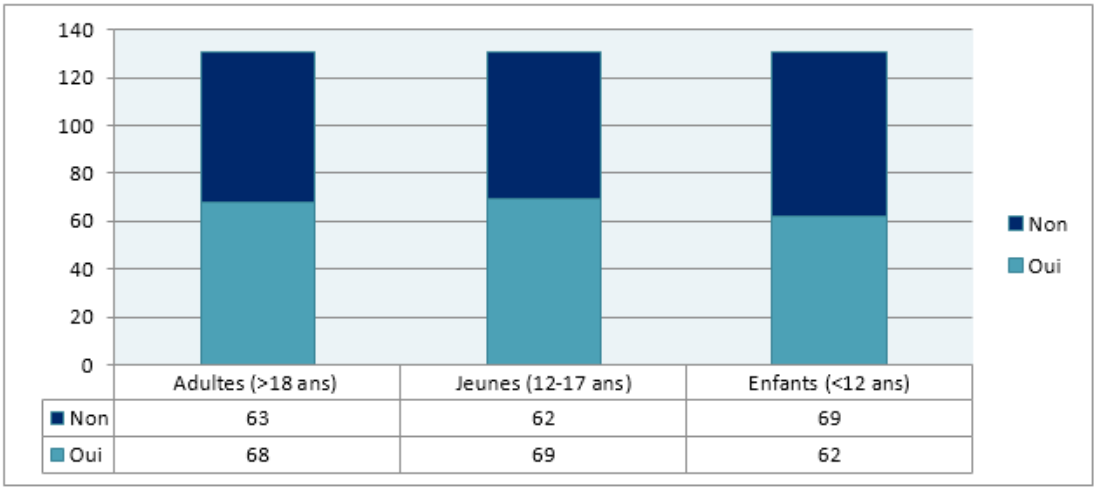
Figure 4 : Importance de la sensibilisation à la cybersécurité pour les organisations/la société civile



Concernant les groupes d'âge visés par les campagnes de sensibilisation à la cybersécurité, le questionnaire distingue trois catégories: adultes (18 ans et plus), jeunes (12-17 ans) et enfants (moins de 12 ans).

La **Figure 5** montre que les trois groupes ont été ciblés de façon assez homogène. Selon les résultats, le groupe des jeunes reste le plus fréquemment visé, tandis que celui des enfants est le moins souvent ciblé. Cela tient peut-être au fait que les Etats Membres estiment que les jeunes sont les plus vulnérables aux cyberrisques en raison de leur interaction avec les services de télécommunication, et principalement de leur accès à l'Internet.

Figure 5 : Groupes d'âge ciblés par les campagnes de sensibilisation à la cybersécurité

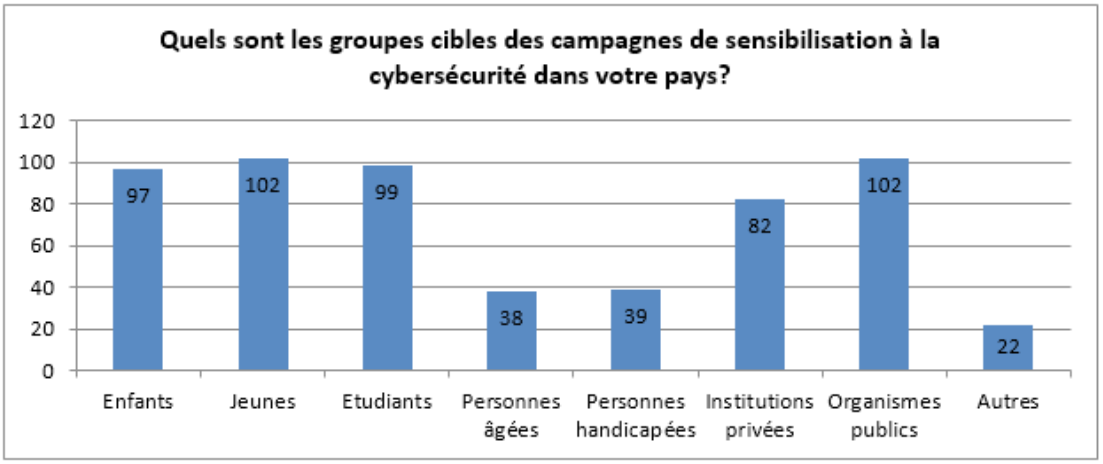


	Adultes (>18 ans)	Jeunes (12-17 ans)	Enfants (<12 ans)
Non	63	62	69
Oui	68	69	62

Nous soulignons que les campagnes de sensibilisation à la cybersécurité ne se limitent pas aux groupes mentionnés ci-dessus. Elles visent aussi d'autres groupes comme les personnes âgées et les personnes handicapées, qui font l'objet de programmes adaptés à leurs besoins et répondant à leur situation, les risques rencontrés par les personnes âgées étant différents de ceux rencontrés par les enfants.

Le questionnaire montre clairement que les organismes publics et le groupe des jeunes ont fait l'objet d'une attention plus soutenue de la part des Etats Membres. Il en est de même pour les groupes d'étudiants et de jeunes qui ont fait l'objet de réponses de 99 et 102 pays respectivement. En revanche, seuls 38 pays visent les personnes âgées lorsque des campagnes de sensibilisation à la cybersécurité sont organisées, c'est-à-dire que quelque 70 pour cent des Etats Membres ayant répondu au questionnaire n'ont pas ciblé ce groupe dans leurs campagnes. Il convient de relever que 69 pour cent des Etats ayant répondu au questionnaire n'ont pas inclus les personnes handicapées parmi leurs groupes cibles. Ces résultats confirment que les groupes les moins souvent visés par les campagnes de sensibilisation à la cybersécurité sont les personnes âgées et les personnes handicapées.

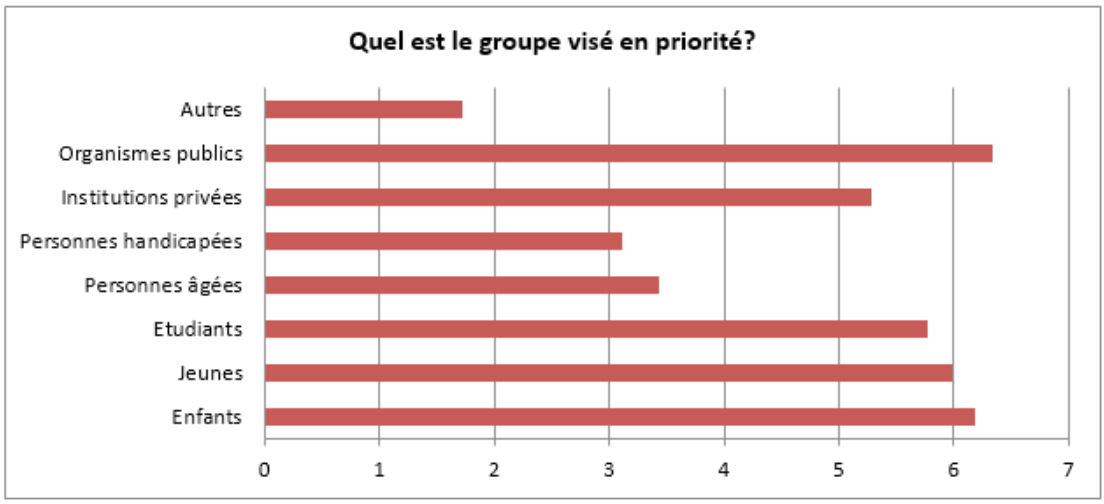
Figure 6 : Groupes cibles des campagnes de sensibilisation à la cybersécurité



Le lecteur trouvera ci-dessous une analyse des réponses à la question: « Quels sont les principaux groupes cibles des campagnes de sensibilisation à la cybersécurité? » Le plus grand nombre de personnes interrogées était en faveur du secteur public, suivi par les enfants, tandis que les groupes des jeunes et des étudiants arrivaient en troisième et quatrième position respectivement. D'autre part, les groupes les moins ciblés par les campagnes étaient une fois encore les personnes âgées et les personnes handicapées, qui étaient aussi les groupes cibles les moins souvent retenus pendant

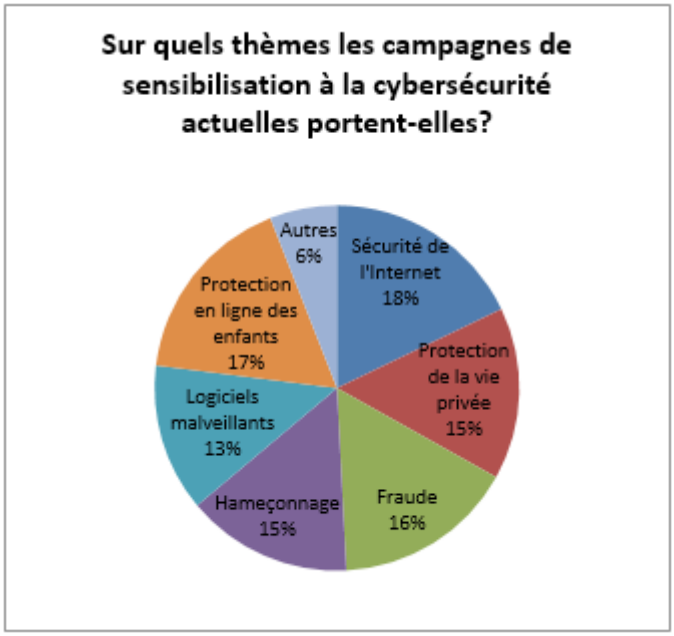
la période d'études précédente (2010-2014). Le seul changement notable entre les résultats de la présente période et ceux de la période précédente est que le secteur public a été le principal groupe cible, alors qu'il arrivait auparavant en deuxième position. Le groupe des enfants est arrivé en deuxième position selon les résultats du présent questionnaire, alors qu'il avait été en première position à l'issue du précédent. Le groupe des jeunes et celui des étudiants sont restés à la même position.

Figure 7 : Groupes visés en priorité par les campagnes de sensibilisation à la cybersécurité



Il est essentiel d'identifier les sujets retenus en priorité dans ces campagnes visant à sensibiliser aux différents cyberrisques. Les questions les plus importantes étaient la sécurité de l'Internet, le respect de la vie privée, la fraude, le hameçonnage, les logiciels malveillants et la protection en ligne des enfants (COP). La sécurité de l'Internet est arrivée à la première place, suivie de la protection en ligne des enfants, de la fraude et du hameçonnage. Dans l'ensemble, les résultats des campagnes de sensibilisation à la cybersécurité ont été proches, tout comme ceux du questionnaire de la période d'études précédente. La sécurité de l'Internet était déjà arrivée en première position, suivie de la COP, tandis que le respect de la vie privée, la fraude et le hameçonnage sont arrivés en troisième position avec des pourcentages égaux. La protection en ligne des enfants a fait l'objet du plus grand nombre de campagnes de sensibilisation à la cybersécurité. En effet, 43 pays sur les 129 ayant répondu à l'enquête ont désigné la COP comme étant la question la plus importante. Ceci est logique en raison de la nécessité d'un plus grand nombre de campagnes de sensibilisation de la société à la COP, en particulier pour le groupe cible des enfants rencontrant ces risques, en plus de parents et des enseignants. L'importance de la COP est encore soulignée par le fait qu'elle occupait la même position suite au questionnaire envoyé pendant la période d'études précédente.

Figure 8 : Thèmes abordés par les campagnes de sensibilisation à la cybersécurité



En moyenne, la sécurité de l'Internet a été classée en deuxième position, suivie par la fraude et la protection de la vie privée, tandis que les logiciels et le hameçonnage se trouvaient en dernière position, comme le montre la **Figure 9**.

Figure 9 : Importance de chaque thème dans les campagnes de sensibilisation à la cybersécurité

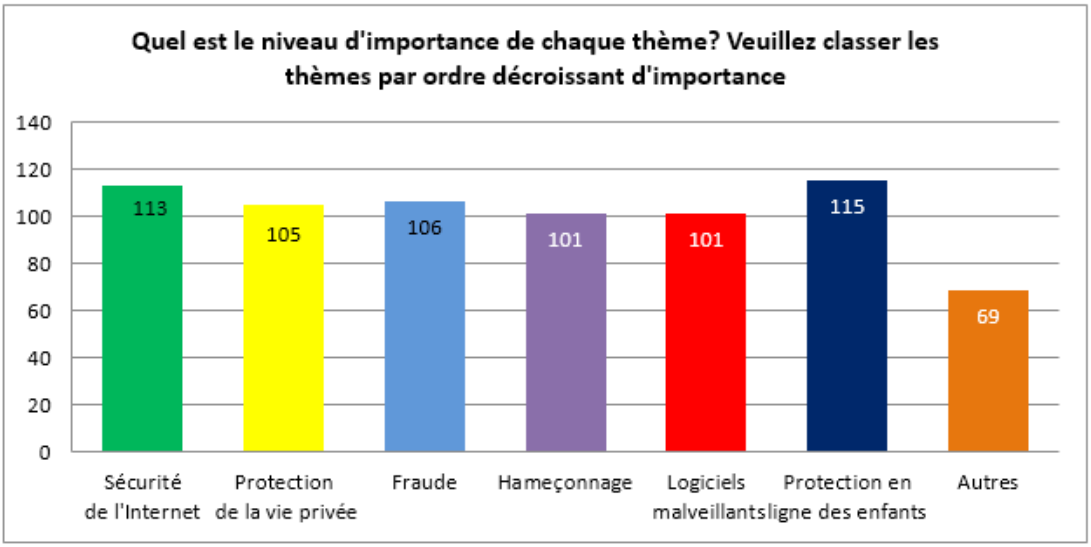
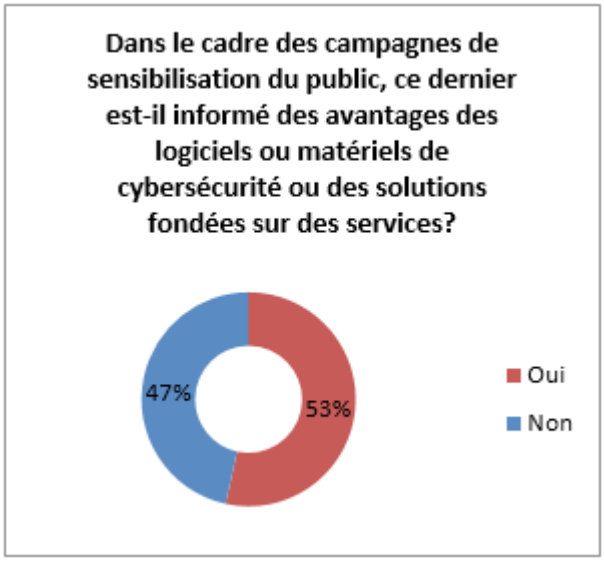


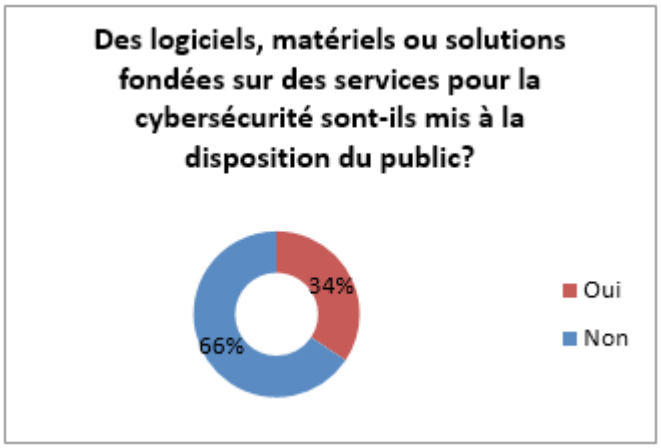
Figure 10 : Information du public sur les avantages de solutions logicielles/matérielles ou fondées sur des services



Lors de l'examen de la question de la sensibilisation, il importe d'aborder le thème de la connaissance de la technologie et de la disponibilité d'outils techniques pour assurer la protection contre les divers cyberrisques. Une plus grande sensibilisation théorique ne saurait être suffisante si elle ne s'accompagne pas de connaissances pratiques ou techniques. Par connaissances techniques, nous entendons que le public doit être renseigné sur l'existence de logiciels ou matériels utiles ou de solutions fondées sur des services pour assurer la cybersécurité. En effet, les programmes logiciels jouent un rôle essentiel dans l'instauration de la cybersécurité et la lutte contre les cyberrisques. Soixante-dix pays sur 131 avaient encouragé ces programmes logiciels et souligné leur utilité auprès des groupes cibles. Soixante et un pays n'ont pas encore familiarisé le public aux programmes logiciels et autres solutions techniques nécessaires pour faire face au cyberrisques. Bien que les deux résultats soient proches, il convient de relever que la diffusion de solutions techniques et de programmes logiciels occupe une place plus grande dans les campagnes de sensibilisation à la cybersécurité.

Le questionnaire révèle aussi que 45 pays ont déjà mis à la disposition du public des programmes logiciels ou solutions fondées sur des services, tandis que la majorité des pays ayant répondu (86), représentant 65,65 pour cent, ont indiqué qu'ils ne l'avaient pas fait.

Figure 11 : Solutions logicielles/matérielles ou fondées sur des services mises à la disposition du public



Voir le **Chapitre 4** pour une analyse du questionnaire COP.

2 CHAPITRE 2 – La situation du spam et des logiciels malveillants, des mesures d'atténuation et des aspects réglementaires

La présente section porte sur les points a) et b) de l'objet de la Question 3/2 qui appellent notamment à:

a) ***Examiner les méthodes et les bonnes pratiques permettant d'évaluer les incidences du spam sur un réseau, et proposer les mesures nécessaires, notamment les techniques de lutte contre le spam utilisables par les pays en développement, compte tenu des normes existantes et des outils disponibles.***

b) ***Fournir des informations sur les problèmes que rencontrent actuellement les fournisseurs de services, les organismes de réglementation et d'autres parties prenantes dans le domaine de la cybersécurité.***

Le spam s'est introduit principalement via des systèmes infectés (prise de contrôle, etc.) suite à une attaque, qui envoient ensuite des spams par le biais de leurs prestataires de services. La stratégie de lutte classique consiste à maintenir et consulter des bases de données sur la réputation des expéditeurs, à l'aide de leur adresse IP. Il existe plusieurs systèmes, qui utilisent des méthodes différentes pour évaluer la réputation des expéditeurs. L'une des méthodes les plus fréquentes consiste à créer des adresses de messagerie leurre, dans le but d'attirer les spammeurs. Lorsqu'un message arrive dans l'une de ces boîtes, la réputation de l'adresse IP de l'expéditeur s'en trouve diminuée.

Ces systèmes tiennent souvent compte du volume de messages, stratégie récemment mise à mal avec l'apparition des spams « furtifs », qui s'appuient sur des botnets (réseaux d'ordinateurs infectés) de grande ampleur, répartis sur différentes zones géographiques. Très peu de messages sont envoyés, mais leur somme représente un volume de trafic important.

Toutefois, malgré ces types d'attaques, les systèmes anti-spam sont en général capables de repérer plus de 90 pour cent, voire souvent plus de 99 pour cent des spams. Les filtres anti-spam sont essentiels si l'on veut que les messages électroniques restent une méthode de communication efficace. Il s'agit également d'un outil primordial de prévention d'infection des dispositifs.

Figure 12 : Le cercle vicieux du spam et de la cybersécurité

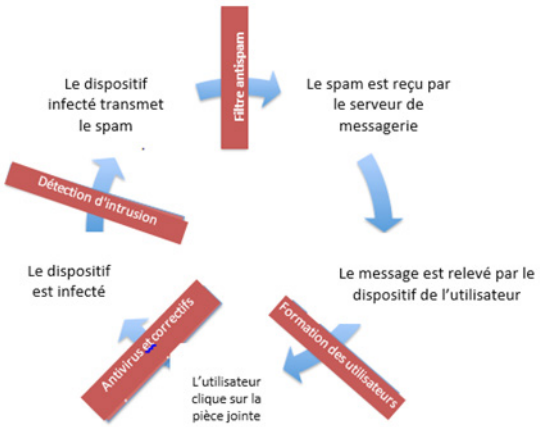
De manière générale, recevoir un spam n'infecte pas ou n'endommage pas un dispositif, et il existe de nombreux moyens de rompre le cercle vicieux. Comme nous l'avons déjà dit, les logiciels anti-spam en éliminent la majorité. Dans la plupart des cas, si le message indésirable passe au travers des mailles du filet, l'utilisateur doit entreprendre une action, par exemple ouvrir une pièce jointe. Par conséquent, la formation des utilisateurs joue un rôle central dans les stratégies de lutte. Si celui-ci ouvre la pièce jointe, l'antivirus et le système d'exploitation, à condition qu'ils soient mis à jour, sont en mesure d'empêcher la propagation de l'infection. Pour chacun de ces points, il existe plusieurs outils gratuits ou abordables disponibles pour les utilisateurs ou prestataires de services des pays en développement.

Il existe aussi une autre technique, qui consiste à pirater des blocs d'adresses IP dans le système de routage. Cela se produit lorsqu'un attaquant s'associe à un prestataire de services de confiance pour échanger des informations de routage. Une nouvelle forme de protection – Sécurité du protocole de passerelle frontière (Border Gateway Protocol Security) (BGPSEC)[2] et infrastructure de clé publique de routage (Routing Public Key Infrastructure) (RKPI) – a récemment été mise au point pour empêcher ce type d'attaque. Elle se trouve encore au stade du développement et du déploiement, et il faudra du temps et des essais avant que ce nouveau système de protection se généralise. Dans l'intervalle, toutes les stratégies décrites précédemment restent valables.

Récemment, une spécification technique appelée DMARC (Domain-based Message Authentication and Conformance) a été élaborée en vue de lutter contre les courriers indésirables.[3] Elle s'appuie sur deux technologies d'authentification, DKIM (Domain Keys Identified Mail) et SPF (Sender Policy Framework) afin de déterminer l'authenticité de chaque message. En fonction des préférences du propriétaire du domaine expéditeur, tout message non authentifié peut, par exemple, être rejeté. Cette méthode n'est utilisée que par quelques très grands fournisseurs de messagerie, ainsi que par plusieurs services émettant de très nombreux messages électroniques dans le cadre de transactions (par exemple, confirmations de commande et d'achat).

Utilisée avec DKIM, la technologie DMARC protège également contre le piratage des préfixes d'adresses IP. Cependant, cette solution n'est pas exempte de problèmes. Lorsqu'elle est utilisée pour des messages de nature non transactionnelle (par exemple, échanges de messages entre particuliers), elle peut susciter des problèmes d'interopérabilité.[4] Il s'agit d'un des axes de travail actuels de l'IETF (Groupe d'étude sur l'ingénierie Internet). De plus, l'AMARC n'est pas en mesure de détecter les systèmes infectés lorsque ceux-ci transmettent des e-mails par le biais de leurs prestataires de services normaux. La clé de la lutte contre le spam consiste d'abord à protéger les systèmes en bout de chaîne.

Figure 13 : Comment rompre le cercle vicieux



2.1 Sources de spam

Le cercle vicieux des **Figures 12** et **13** repose essentiellement sur l'utilisation de botnets, qui sont composés d'appareils grand public et, dans certains cas, de serveurs infectés dans des centres de données. Les préoccupations sur le risque que représentent les dispositifs mobiles en matière de spam ont été évoquées dans au moins un document précédent. Le type et le niveau de risque varient selon le système d'exploitation. Par exemple, l'iPhone d'Apple s'est avéré très résistant aux attaques, car il

[2] RFC 6480, https://www.rfc-editor.org/info/rfc6480.
[3] RFC7489, https://www.rfc-editor.org/info/rfc7489.
[4] RFC 7960, https://www.rfc-editor.org/info/rfc7060.

nécessite des applications signées et validées numériquement, et il bénéficie d'un contrôle rigoureux, aussi bien de la plate-forme que des applications qui y sont exécutées.

D'autres plates-formes posent plus de problèmes. L'utilisation sociétale des TIC ne cesse de croître, de même que « l'Internet des objets », de sorte que de nouvelles plates-formes sont introduites dans le réseau. A partir du moment où ces dispositifs disposent d'une unité centrale (CPU) et sont connectées au réseau, les failles ne sont pas à exclure. Peu avant la publication du présent rapport, le logiciel malveillant Mirai a attaqué l'infrastructure DNS et bloqué le site d'un grand réseau social. En ce qui concerne plus directement le spam, Proofpoint a décelé en 2013 une vulnérabilité permettant à des réfrigérateurs, des thermostats et des alarmes anti-intrusion[5] de diffuser des spam. Cette découverte renforce la nécessité, de la part des fabricants, de fournir des mécanismes de mise à jour automatique des logiciels, de manière à réduire le risque d'exploitation des dispositifs.

2.2 Impact du spam sur le réseau

Il existe différentes façons de mesurer l'impact du spam sur le réseau, allant des liens internationaux au trafic vers les téléphones portables via la radiofréquence. Ces dernières années, l'on s'est interrogé sur le pourcentage de bande passante consommé par le spam. Les messages électroniques sont eux-mêmes en général assez petits, représentant une moyenne de 75 000 octets.[6] Cependant, beaucoup sont encore plus petits, sans compter les pièces jointes, qui ne sont pas toujours téléchargées à réception. Si des mesures antispam adaptées sont mises à place, environ 10 pour cent des spams au maximum passeront entre les mailles du filet. Même en se basant sur l'estimation la plus haute du volume de messages échangés par jour, à savoir 259 milliards, et en postulant que les solutions antispam utilisées sont les moins efficaces, si l'on estime que 2,5 milliards de personnes (ramenés à une proportion par habitant) utilisent le réseau, le nombre de spams arrivant dans les boîtes de messagerie devrait être en moyenne de seulement une dizaine par jour et par personne, et une centaine sans protection antispam. Mais, même à ce volume, le spam occupe une place infime sur le réseau par rapport à la voix, aux vidéos et à la navigation sur Internet. De manière générale, les mesures indiquent que l'ensemble des messages électroniques (y compris les spams) représente un pourcentage négligeable de la bande passante dans les économies analysées.[7] La menace que représente le spam réside plutôt dans le risque que les dispositifs infectés soient utilisés à des fins frauduleuses ou illégales. En l'absence de filtres corrects, le spam détériore également la valeur de la messagerie électronique pour les utilisateurs.

2.3 Les risques du harponnage et les moyens de lutte

Le harponnage (ou « spear phishing » en anglais) est une forme d'attaque dans le cadre de laquelle un message électronique frauduleux est envoyé à un utilisateur cible en se faisant passer pour une source légitime. Il contient suffisamment d'informations personnelles pour faire croire au destinataire que la source du message est authentique. Il s'agit, par exemple, de messages contenant de véritables numéros de compte, ainsi que des noms de personnes ou des images connues par la cible. Le destinataire est incité à cliquer sur un lien Internet ou à ouvrir une pièce jointe, ce qui provoque l'infection du dispositif. Le coût de cette attaque ciblée est nettement plus élevé que celui des attaques non ciblées, car cela nécessite des recherches qui peuvent elles-mêmes prendre plusieurs formes, notamment le piratage de sites de commerce électronique ou de certaines administrations. Le moyen le plus efficace de lutter contre le harponnage consiste à éduquer les utilisateurs.

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

2.4 Impact des politiques sur le spam

Les réglementations peuvent avoir un impact aussi bien positif que négatif sur la lutte contre le spam. L'utilisation d'un ordinateur pour envoyer un message frauduleux constitue un délit. Ce délit en soi n'est pas nouveau, seule la forme a changé. La législation devrait être suffisamment souple pour permettre de poursuivre les auteurs. Les Etats-Unis ont adopté le CAN-SPAM Act en 2003 pour signifier clairement le caractère illégal de ce type de comportement. Cependant, il reste difficile de remonter jusqu'à la source du délit. Des partenariats publics-privés entre les prestataires de services et les forces de l'ordre permettront peut-être, au fil du temps, de mieux identifier les auteurs d'attaques. En cas de transactions financières, celles-ci peuvent être repérées par le biais des réseaux financiers.

D'un autre côté, empêcher la réception du spam nécessite que des intermédiaires aient un accès fréquent au contenu des messages afin de déterminer leur dangerosité pour les systèmes d'extrémité. Nous avons besoin d'un cadre juridique adapté permettant de protéger le réseau et ses utilisateurs.

L'UIT continue de relever les défis posés par le spam en collaboration avec l'Internet Society. Pendant la période d'études, une réunion fructueuse a été organisée durant le Forum 2016 du SMSI sur le thème « Spam: comprendre et combattre les problèmes rencontrés par les économies Internet émergentes ».[8] Parmi les intervenants, on a compté des représentants de Cybersecurity Malaysia, d'Utilities and Competition Authority (Bahamas), de l'ISOC, de Spamhaus et le Corapporteur pour la Question 3 de la CE 2 de l'UIT-D. La réunion a retenu les questions à traiter suivantes:

- Nécessité de renforcer la coopération, avec une harmonisation des plans d'action efficaces des Etats Membres, car le spam est un problème collectif qui touche tout le monde.
- Même si la connexion (au large bande) devient accessible financièrement, il n'en est pas forcément de même de la protection (contre des cyberattaques).
- Nécessité d'une législation qui définit ce qui est acceptable et ce qui ne l'est pas et création d'un mécanisme de sanctions applicables en cas d'infraction, sans être trop rigide pour ne pas pénaliser des acteurs comme les Petites et Moyennes Entreprises (PME) désireuses de lancer des campagnes de marketing.
- Bonnes pratiques et solutions de listes noires et de services de réputation à partager avec tous les Etats Membres par l'intermédiaire de l'UIT.

[8] Session du Forum 2016 du SMSI *« Le Spam: comprendre et combattre les problèmes rencontrés par les économies Internet émergentes »,* https://www.itu.int/net4/wsis/forum/2016/Agenda/Session/152.

3 CHAPITRE 3 – Améliorer la position nationale en matière de cybersécurité: renforcer la sensibilisation et les ressources humaines

La présente section porte sur le point c) de l'objet de la Question 3/2 qui appelle notamment à:

c) Continuer de recueillir auprès des Etats Membres des données d'expérience concernant la cybersécurité et de recenser et d'étudier les thèmes communs qui s'en dégagent.

Nous vivons dans un monde qui est de plus en plus connecté. S'il en résulte des possibilités sans précédent d'innovation et de croissance économique et sociale dans le monde, il existe aussi des problèmes et des menaces en matière de cybersécurité dans le cyberespace.

De plus, alors que ces problèmes de sécurité continuent d'évoluer et de toucher différents secteurs, les pays ont de plus en plus de difficultés à les résoudre.

Pour ce faire, de nombreux pays organisent des campagnes de sensibilisation à la cybersécurité qui visent à former les pouvoirs publics, le secteur privé, les éducateurs et les individus pour qu'ils soient en mesure d'identifier les problèmes potentiels et de comprendre leurs rôles et responsabilités particuliers dans la création d'un cyberespace plus sûr. Pendant la période d'études, plusieurs entités ont soumis des contributions sur ce sujet. Pour tout renseignement supplémentaire, voir l'**Annexe 2**, Recueil des études de cas de pays sur la cybersécurité.

3.1 Campagnes de sensibilisation

La campagne Stop.Think.Connect.™, qui vise à améliorer la compréhension des cybermenaces par la population américaine et à l'autonomiser pour une plus grande sécurité en ligne, offre un exemple de campagne de sensibilisation Son but est de diffuser le concept de cybersécurité en tant que « responsabilité partagée » par laquelle chaque individu, en prenant des mesures simples de sécurité en ligne, rend l'utilisation de l'Internet plus sûre pour tous. Ses messages clés sont les suivants:

- **Stop**: avant d'utiliser l'Internet, prenez le temps nécessaire pour comprendre les risques et apprenez à détecter les problèmes potentiels.
- **Think**: prenez le temps de vous assurer qu'il n'y a pas de risques. Repérez les signes d'alerte et réfléchissez à l'incidence éventuelle de vos actions en ligne sur votre sécurité ou celle de votre famille.
- **Connect**: profitez de l'Internet avec plus de confiance en sachant que vous avez pris les mesures appropriées pour vous protéger et protéger votre ordinateur.
- **Stop. Think. Connect.** Protégez-vous et contribuez à rendre l'Internet plus sûr pour tous.

La présente section est divisée en quatre parties, qui décrivent les étapes recommandées et les bonnes pratiques pour lancer une campagne de sensibilisation à la cybersécurité.

3.1.1 Bonnes pratiques pour un programme de communication

Si chaque pays a des besoins et problèmes particuliers en ce qui concerne les menaces dans le domaine de la cybersécurité et la protection, les bonnes pratiques présentées ci-dessous peuvent être utiles pour lancer une campagne de sensibilisation à la cybersécurité.

- **Elaborer un plan de communication comprenant des buts et objectifs bien définis et identifier le public ciblé en priorité.** La première étape avant de lancer une campagne de sensibilisation à la cybersécurité consiste à déterminer les buts et objectifs précis de la campagne ainsi que le public qu'elle vise en priorité. **Elaborer des stratégies et ressources de communication ciblées pour toucher des publics particuliers.** Chacun a des besoins différents en matière

de cybersécurité. Par exemple, il se peut que des étudiants aient besoin d'informations au sujet des prédateurs en ligne, alors que des professionnels de l'informatique auront besoin de renseignements sur les pirates. Des supports divers devraient être élaborés en fonction des besoins, connaissances et capacités de chaque public.

- **Rédiger des feuillets d'information** adaptés à chaque public pour répondre à ses besoins particuliers et aux menaces auxquelles il est exposé. Du matériel didactique complet comme le kit pratique Stop.Think.Connect.™ permet de souligner la responsabilité partagée pour la cybersécurité tout en garantissant que des ressources sont disponibles pour tous les milieux. Des rappels simples sous forme d'affiches, de bracelets, etc., contribuent à faire des bonnes pratiques en matière de cybersécurité une priorité pour chacun.
- **Utiliser les réseaux sociaux.** Une grande partie de la sensibilisation à la cybersécurité a lieu en ligne. L'utilisation des **réseaux** sociaux facilite la transmission de messages appropriés aux individus par les canaux qu'ils utilisent déjà – et dans certains cas par ceux qu'ils préfèrent utiliser. Afficher des informations sur des sites de réseaux sociaux comme Facebook, Twitter et YouTube est un moyen de partager des informations tout en recevant de précieuses contributions.
- **Utiliser les médias traditionnels.** Programmes de radiodiffusion sonore et télévisuelle, journaux et magazines.
- **Créer et maintenir des partenariats avec des alliés au sein des publics cibles.** Aucune organisation, qu'elle soit un organisme public, une société ou une institution sans but lucratif, ne peut sensibiliser à elle seule à la cybersécurité. C'est pourquoi les partenariats publics et privés sont essentiels. Il convient de nouer des partenariats avec des organisations comme:
  - *Organismes publics*. Les organismes publics confèrent une autorité au message et peuvent toucher largement les individus et les communautés.
  - Un programme central peut être utilisé pour former les pouvoirs publics locaux et régionaux qui, à leur tour, peuvent sensibiliser leurs employés et leurs mandants à l'identification et à la prévention des risques en ligne. Parmi les partenaires publics essentiels à différents niveaux, on mentionnera les équipes d'intervention en cas d'incident relatif à la sécurité informatique (CSIRT), les bureaux des chefs de la sécurité informatique (CISO), et les bureaux des chefs de l'information (CIO).
  - *Organisations sans but lucratif.* Les organisations sans but lucratif offrent des ressources diversifiées et une grande souplesse pour diffuser les messages de sensibilisation à la cybersécurité.
  - Les partenaires sans but lucratif touchent tous les groupes cibles recensés dans le plan stratégique. Des appels réguliers à toutes les organisations partenaires contribuent à créer des réseaux entre toutes les organisations, publiques et privées.
  - *Etablissements universitaires.* Les établissements universitaires réalisent des études essentielles et à jour qui contribuent à garantir la pertinence des campagnes. Elles permettent aussi de toucher la main d'oeuvre future du pays. Des partenariats avec des écoles primaires et secondaires sont aussi essentiels car la formation en matière de cybersécurité dès le plus jeune âge aide les élèves à utiliser l'Internet en toute sécurité pendant toute leur vie. La coopération avec des universités ou des centres d'excellence permet de créer des liens avec les individus en formation et les organisations qui les emploieront à l'avenir.
  - *Organisations du secteur privé*. Les chefs d'entreprise, par exemple dans les secteurs de l'information, du commerce de détail, de la finance et de l'éducation, peuvent former les employés, les consommateurs et d'autres publics au sujet des menaces qui les touchent et peuvent aussi recevoir des contributions relatives au renforcement des pratiques en matière de cybersécurité. Des solutions de cybersécurité novatrices élaborées par le secteur privé peuvent favoriser les bonnes pratiques dans les secteurs public et privé.

– **Mobiliser le public au niveau individuel par des initiatives locales.** La sensibilisation individuelle est fondamentale pour un programme de sensibilisation à la cybersécurité efficace.

La campagne Stop.Think.Connect.™, par exemple, invite les individus à devenir des « amis de la campagne » en s'abonnant à des bulletins d'information mensuels contenant les derniers tuyaux, nouvelles et renseignements en matière de cybersécurité qui les concernent. La campagne touche aussi les individus en organisant des manifestations de sensibilisation adaptées à chaque public et en mettant à disposition des orateurs capables d'aborder les questions de cybersécurité intéressant le plus les participants.

– **Déterminer si l'effort entrepris sensibilise vraiment les groupes cibles.** Pour mesurer l'efficacité d'une campagne, il importe de recueillir les réactions de groupes cibles, les résultats d'enquêtes ou d'utiliser d'autres méthodes similaires. Par ailleurs, il convient de recenser les pages web les plus visitées, les documents les plus téléchargés, les manifestations les mieux accueillies et les pratiques que le public trouve le plus utiles pour identifier les réussites et soutenir les améliorations. Les informations fournies en retour par les organisations partenaires contribuent à concentrer la planification future sur l'efficacité et la créativité.

3.1.2 Modèle de plan de communication

Un plan de communication est un élément essentiel d'une campagne réussie. Pour l'organisation, il s'agit d'une feuille de route lui permettant de réaliser ses buts et objectifs principaux. Bien qu'un plan de communication doive être adapté pour répondre aux besoins d'une organisation donnée, la plupart des plans contiendront les sections suivantes:

Objet et cadre général

La section objet et cadre général présente les raisons qui amènent l'organisation à créer un plan de communication et ce à quoi elle entend parvenir.

Buts de communication généraux

Les buts de communication généraux sont des objectifs de haut niveau pour le programme de sensibilisation à la cybersécurité. Ces buts sont généraux sur le plan stratégique. Par exemple:

Favoriser la sensibilisation du public à la cybersécurité en augmentant le niveau de compréhension des cybermenaces et, des mesures simples de protection, et en autonomisant le public pour qu'il soit mieux préparé en ligne en vue:

– D'accroître la sensibilisation à la cybersécurité et à son lien avec la sûreté nationale et la sécurité de notre propre vie;

– De faire participer le public, le secteur privé et les pouvoirs publics régionaux à un effort visant à améliorer la cybersécurité;

– d'élaborer et de faire connaître des méthodes et des stratégies pour que les citoyens, leurs familles et leurs communautés puissent utiliser les services en ligne de façon plus sécurisée.

Objectifs de communication

Les objectifs de communication décrivent la manière dont la campagne doit atteindre ses buts généraux. Les objectifs devraient être mesurables.

Par exemple, les buts ci-dessus sont définis plus en détail et deviennent les objectifs suivants:

– Former le public au sujet des pratiques de cybersécurité, pour qu'il se protège et que les groupes de parties prenantes aient connaissance des ressources disponibles.

– Augmenter le nombre de groupes de parties prenantes et renforcer les relations existantes avec les pouvoirs publics locaux, le secteur privé, les organisations à but non lucratif, les systèmes scolaires et les enseignants.

– Accroître et renforcer le personnel qualifié dans le domaine des TIC en soutenant l'enseignement des sciences, de la technologie, de l'ingénierie et des mathématiques.

Principaux publics cibles

Identifier les principaux publics cibles contribue à garantir que les messages se concentrent sur les personnes les plus réceptives ou celles qui en ont le plus besoin. Une définition claire et unanimement reconnue de ces publics permet de mieux cibler les messages.

Canaux de communication

Les canaux de communication sont les différents moyens permettant de transmettre les messages aux publics cibles. Il convient d'examiner soigneusement tous les moyens de communication utilisés ainsi que les méthodes supplémentaires éventuellement disponibles. Le plan de communication devrait préciser clairement la nature des canaux et la manière dont ils doivent être utilisés.

Par exemple:

– manifestations: organiser des manifestations avec les groupes cibles;

– médias traditionnels: nouer activement des contacts avec les médias nationaux/régionaux/locaux (par exemple radiodiffusion, presse traditionnelle, web);

– réseaux sociaux: utiliser activement les réseaux sociaux (blog officiel, Facebook, Twitter);

– bulletins d'information: distribuer un bulletin d'information mensuel et des kits pratiques d'information;

– site web: mettre à jour régulièrement le site web de la campagne avec des actualités, des conseils et des informations essentielles;

– partenaires: encourager la prise de contact par des organisations partenaires.

3.1.3 Stratégies de campagne

Les stratégies de campagne prennent en considération aussi bien les méthodes pratiques de diffusion que les moyens permettant de stimuler la campagne. Chaque stratégie d'ensemble comporte de nombreuses étapes intermédiaires permettant de la réaliser. Les étapes, tout comme les stratégies, doivent être suffisamment souples pour s'adapter à un environnement évolutif. Par exemple, les stratégies suivantes ont été utilisées pour atteindre les objectifs de communication d'un programme:

– diffuser les messages de campagne lors de manifestations et par les médias (réseaux sociaux et médias traditionnels);

– constituer un cadre de messagers en nouant des partenariats avec les organisations à but non lucratif et des contacts locaux;

– collaborer avec des organismes publics pour organiser des manifestations et transmettre des messages.

Messages

La communication devrait se concentrer sur les messages fondamentaux que la campagne doit diffuser. Chaque pays et chaque campagne – et chaque public et chaque manifestation – ont des besoins particuliers qui nécessitent des messages adaptés. Les messages fondamentaux sont la base de chacune de ces actions de sensibilisation personnalisées.

Ainsi, les messages fondamentaux de la campagne Stop.Think.Connect sont les suivants:

- **Stop**: avant d'utiliser l'Internet, prenez le temps nécessaire pour comprendre les risques et apprenez à détecter les problèmes potentiels.
- **Think**: prenez le temps de vous assurer qu'il n'y a pas de risques. Repérez les signes d'alerte et réfléchissez à l'incidence éventuelle de vos actions en ligne sur votre sécurité ou celle de votre famille.
- **Connect**: profitez de l'Internet avec plus de confiance en sachant que vous avez pris les mesures appropriées pour vous protéger et protéger votre ordinateur.
- **Stop. Think. Connect.** Protégez-vous et contribuez à rendre l'Internet plus sûr pour tous.

D'autres messages universels sont notamment: utiliser des mots de passe forts, tenir à jour les systèmes d'exploitation et les logiciels de sécurité, ne se connecter qu'avec des personnes de confiance et éviter les sites web qui semblent trop beaux pour être vrais.

Rôles et responsabilités

Assigner clairement les rôles et responsabilités permet aux équipes de collaborer efficacement et d'éviter les chevauchements et la confusion. Cette distinction entre les organisations doit être opérée quand de multiples groupes soutiennent une campagne. Il convient aussi de définir les attributions des membres d'une équipe au sein d'une même organisation.

Ressources

Etablir la liste des ressources disponibles pour une campagne permet de préciser la portée et les limites des activités de sensibilisation à mener pendant une période donnée. Dans cette section, l'auteur peut décider de détailler le nombre de collaborateurs et le matériel dont dispose l'organisation pour cibler des publics donnés pendant une période donnée.

Problèmes de communication

Recenser les problèmes de communication potentiels peut contribuer à surmonter les obstacles et à combler les lacunes. Par exemple:

- il est difficile aux publics cibles de comprendre les aspects techniques des cybermenaces et comment ils sont concernés par elles; et
- le grand public ne considère pas forcément les cybermenaces comme réelles ou pertinentes dans sa vie quotidienne.

3.1.4 Mesure de la réussite et paramètres

Il faut pouvoir mesurer l'efficacité d'un plan de communication et disposer d'informations fournies en retour. En raison de la nature des campagnes de sensibilisation à la cybersécurité, ces mesures se concentrent généralement sur les activités destinées à l'extérieur plutôt que sur les contributions, mais un retour d'information en temps opportun est essentiel. Exemples:

- nombre de participants à chaque manifestation ou série de manifestations dans une région ;
- quantité de matériel de marketing distribué ;
- couverture médiatique ;
- nombre de parties prenantes concernées (par exemple amis, membres d'un groupe de sensibilisation à la cybersécurité, membres d'un réseau national, etc.) ;
- nombre de consultations des pages web ;
- informations fournies en retour et témoignages de participants et d'organisations partenaires ;

– informations fournies en retour par les organes législatifs, et les responsables/dirigeants locaux ou de l'Etat.

Paramètres

Les paramètres relèvent de plusieurs grandes catégories. La façon dont ces types de catégories sont appliqués à différents programmes de sensibilisation à la cybersécurité dépend des buts et des ressources de chaque programme. **L'engagement des parties prenantes** porte sur les partenariats officiels avec des organismes publics et des organisations sans but lucratif. La **sensibilisation par les médias traditionnels** et la **sensibilisation numérique et en ligne** s'appliquent à la distribution de produits écrits et multimédias par des canaux de communication établis. Les **manifestations et forums** et les **ressources** portent sur les interactions en personne. Une combinaison de catégories de paramètres est nécessaire pour comprendre et mesurer la portée complète d'une campagne.

3.2 Mesures supplémentaires de renforcement des capacités

3.2.1 Activités menées au Japon

Le Ministère des Affaires Intérieures et des Communications (MIC) du Japon a mis en place un projet de partenariat secteur public-secteur privé, appelé projet « ACTIVE », (**A**dvanced **C**yber **T**hreats response **I**nitiati**VE** – initiative pour une intervention avancée en cas de cybermenace), qui vise à aider les utilisateurs à prévenir les infections par des logiciels malveillants et les dégâts causés par ces infections et à supprimer les logiciels de ce type. Ce partenariat regroupe le MIC, les fournisseurs de services Internet (ISP) et les fournisseurs de solutions de sécurité. Ces initiatives visent à réduire le nombre d'infections par des logiciels malveillants au Japon, de façon à créer l'environnement de sécurité de l'information le plus fiable du monde.

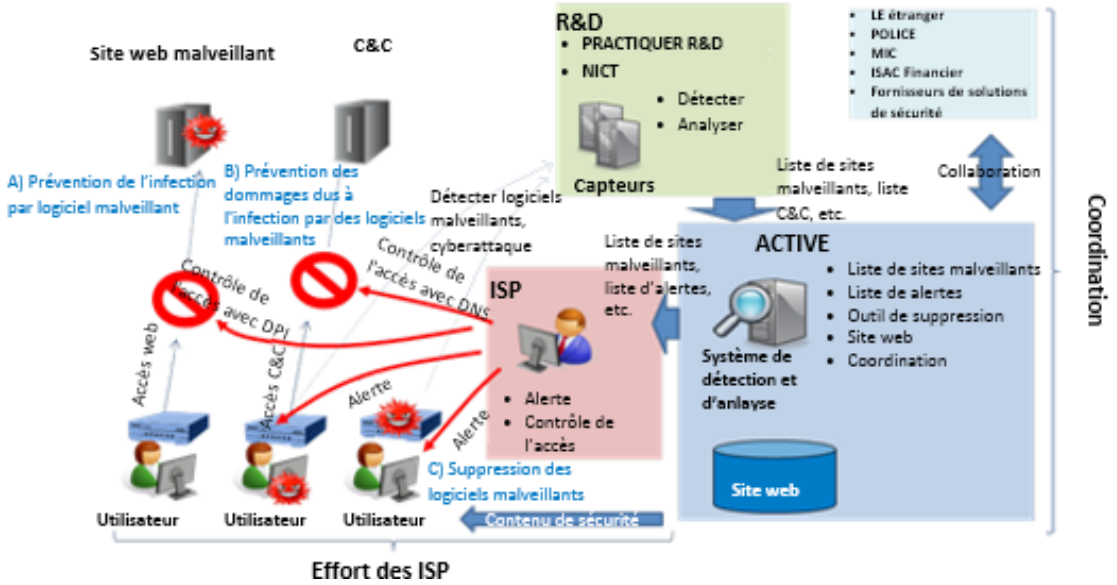
Les principales activités sont les suivantes:

– Mesures visant à prévenir les infections par des logiciels malveillants: coopération avec les fournisseurs ISP.

– Mesures visant à prévenir les dégâts causés par les infections par des logiciels malveillants; coopération avec les fournisseurs ISP.

– Suppression des logiciels malveillants; coopération avec les fournisseurs ISP.

Figure 14 : Aperçu des activités menées dans le cadre du projet ACTIVE



Efficacité du projet ACTIVE

D'après les données statistiques datant du 23 mai 2016, depuis que le système ACTIVE est en service, 286 messages d'alerte ont été envoyés aux utilisateurs pour empêcher une infection par des logiciels malveillants, 320 267 accès aux serveurs C&C ont été bloqués afin d'empêcher d'éventuels dégâts et 1 878 messages d'alerte ont été envoyés aux utilisateurs pour qu'ils suppriment les logiciels malveillants.

En plus des fonctions de base qu'il assure, le système ACTIVE a joué un rôle important dans l'opération de retrait organisée par les services chargés de l'application des lois du monde entier, y compris le Japon. Les responsables du système ACTIVE ont reçu de ces services une liste des infections par des logiciels malveillants, par exemple Game over Zeus, VAWTRAK, etc., et ont communiqué cette liste aux fournisseurs ISP participants pour qu'ils suppriment les logiciels malveillants.

3.2.2 Activités menées en république de Corée

La République de Corée a élaboré un plan national en quatre parties. La première vise à améliorer la structure du secteur de la sécurité informatique en encourageant un marché fondé sur les résultats et en mettant en place un système adéquat de paiement de prix justes pour les services de sécurité informatique. Ce système comporte une méthode d'évaluation du prix juste pour un service informatique sécurisé sans interruption, ce qui garantit la sécurité des produits qui en dépendent.

De plus, les gouvernements peuvent stimuler l'investissement dans la sécurité, par exemple en accordant des préférences pour la participation aux marchés publics et à la R&D, pour encourager les sociétés à investir volontairement dans la sécurité et à prendre des mesures concrètes. Une autre méthode consiste à recenser et encourager les jeunes entreprises du domaine de la sécurité informatique en apportant un soutien comme le partage des vulnérabilités en matière de sécurité, des bancs d'essai et un appui à la certification internationale, de façon que des idées de sécurité valables puissent conduire à la création de jeunes entreprises.

3.2.3 Activités menées dans la région de la CEI

La Fédération de Russie a soumis une contribution[9] qui présente les résultats d'un projet d'initiative régionale de la CEI visant à renforcer les capacités humaines dans le domaine de la sécurité de l'information. Il est reconnu dans le projet qu'il faut d'urgence renforcer les capacités humaines pour accroître la confiance et la sécurité dans l'utilisation des TIC, le partenariat commercial étant le client, le système éducatif le sous-traitant et l'Etat le régulateur du processus dans son intégralité.

Dans le cadre du projet relevant de l'Initiative régionale pour les pays de la CEI, des compétences professionnelles type ont été définies. Comme l'a indiqué la Fédération de Russie dans sa contribution, il est important que ces compétences jouent un rôle de premier plan dans l'élaboration de programmes éducatifs en matière de formation et de recyclage des spécialistes de la sécurité de l'information. Ces compétences sont les suivantes:

1) Les compétences professionnelles générales désignent l'aptitude:

- à assurer le fonctionnement de systèmes d'infocommunication (ICS) en ayant recours à des méthodes et des moyens permettant d'en garantir la sécurité;
- à gérer la protection logicielle et matérielle des informations du système ICS;
- à mener des travaux relatifs à l'évaluation de la sécurité du système ICS; et
- à mettre en place un système ICS protégé réparti.

[9] Document 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 », Fédération de Russie.

2) Les compétences relatives à l'exploitation du système ICS au moyen de méthodes et d'outils logiciels permettant d'en assurer la sécurité désignent l'aptitude:

- à assurer la sécurité de l'information (IS) dans le système ICS à l'aide de logiciels et de matériel;
- à assurer la sécurité de l'information (IS) dans le système ICS à l'aide de moyens techniques; et
- à assurer la sécurité de l'information (IS) dans le système ICS au moyen d'un logiciel d'application, de matériel et de ressources techniques complexes.

3) Les compétences dans le domaine du logiciel de gestion et de la protection matérielle de l'information dans le système ICS désignent l'aptitude:

- à configurer la protection logicielle et matérielle du système;
- à définir des règlements en matière de maintenance et à assurer la réparation des outils logiciels et matériels de la protection de l'information;
- à analyser les infractions autorisées par les utilisateurs dans le système ICS et à éviter qu'elles se reproduisent.

4) Compétences dans le domaine de l'évaluation de la sécurité du système ICS:

- suivi de l'efficacité et de l'efficience des moyens matériels et logiciels utilisés pour la protection de l'information;
- application de méthodes et de techniques permettant d'évaluer la sécurité du système faisant l'objet d'une analyse relative au contrôle du système de protection;
- travaux d'expérimentation et de recherche en cas de certification d'objet, compte tenu de la nécessité d'assurer la protection du système ICS;
- contrôle instrumental de la protection du système ICS; et
- connaissances spécialisées dans le domaine des enquêtes sur les incidents de sécurité.

5) Compétences dans le domaine de la conception d'un système ICS protégé réparti:

- définition des exigences relatives à un système ICS sécurisé réparti et mesures correctives appropriées, compte tenu de la réglementation en vigueur et des documents d'orientation existants;
- conception du système ICS protégé réparti;
- mise en service et maintenance du système ICS réparti, tout en assurant la protection des ressources d'information, et adoption des mesures techniques et organisationnelles relatives à la sécurité de l'information.

3.2.4 Activités menées en Norvège

La Norvège présente l'expérience qu'elle a acquise au niveau national dans une étude visant à jeter les bases de pratiques efficaces en matière de cybersécurité et à améliorer la cyberrésilience au niveau national.[10] Le Centre Norvégien de Cybersécurité (NorSIS) a procédé à une étude destinée à mieux comprendre la culture de la cybersécurité en Norvège Cette étude vise à jeter les bases de pratiques efficaces en matière de cybersécurité et à améliorer la cyberrésilience au niveau national. L'étude décrit la méthode adoptée pour l'élaboration de paramètres pour la culture de la cybersécurité, tout en présentant une vaste enquête nationale. Le centre NorSIS a publié dernièrement le rapport intitulé « La culture de la cybersécurité en Norvège », qui présente de manière détaillée cette méthode ainsi que les principales conclusions de l'étude nationale.

[10] Document SG2RGQ/204, « Creating a metric for cyber security culture », Norvège.

3.3 Partenariats public-privé

Pendant le cycle d'études, plusieurs Etats Membres ont souligné, dans un certain nombre de contributions, l'importance de la coopération entre les gouvernements et le secteur privé et du partenariat public-privé. Ils ont fait observer que la gestion du cyberrisque pour les infrastructures essentielles est une tâche extrêmement complexe, mais d'une importance cruciale, et que le traitement des problèmes de cybersécurité dépasse souvent la compétence des seuls secteurs public ou privé, qui ne peuvent agir indépendamment l'un de l'autre.

Le **Royaume-Uni de Grande-Bretagne et d'Irlande du Nord** a présenté une contribution[11] sur la cybersécurité dans les organismes d'Etat et le secteur privé. Il y présente un programme intitulé « Cyber Essentials ». Ce programme a été élaboré après avoir analysé un certain nombre de cyberattaques. L'analyse a montré que dans de bien des cas, un petit nombre de précautions aurait permis d'atténuer les effets des attaques ou obligé l'adversaire à faire des efforts bien plus considérables. Le programme Cyber Essentials a été créé conjointement par le Gouvernement du Royaume-Uni et le secteur privé pour remplir deux fonctions. Premièrement, il présente les mesures de base que toutes les organisations devraient mettre en œuvre pour limiter les risques liés aux menaces courantes sur Internet, dans le cadre des dix mesures prises par le gouvernement en matière de cybersécurité, et deuxièmement, il présente le cadre d'assurance dont des organisations peuvent se servir pour prouver aux consommateurs, aux investisseurs, aux assureurs et à d'autres entités que les mesures de précaution essentielles ont été prises. Alors que ce programme a été élaboré pour le Royaume-Uni, il est dans une large mesure applicable à tout pays et tout individu peut y avoir accès. Cyber Essentials a rencontré un grand succès au Royaume-Uni. En effet plusieurs centaines d'organisations ont été certifiées bien que le programme soit relativement nouveau.

La contribution[12] soumise par les **Etats-Unis** porte sur la collaboration avec le secteur privé pour la gestion des cyberrisques. Dans cette contribution, les Etats-Unis mettent l'accent sur les partenariats public-privé qui sont un élément clé de la protection efficace des infrastructures essentielles, de la résilience et de la gestion globale des cyberrisques. Ils relèvent qu'il importe de collaborer avec le secteur privé pour gérer les cyberrisques, présentent la méthode communautaire inclusive de gestion du cyberrisque, mettent en avant les outils essentiels à cette méthode et donnent des exemples concrets de mise en oeuvre efficace de partenariats public-privé.

Ce même sujet concernant l'importance de la collaboration des pouvoirs publics avec les entreprises du secteur privé est aussi évoqué dans la contribution du **Japon**,[13] qui porte sur le partage du savoir, de l'information et des bonnes pratiques pour créer une culture de la cybersécurité. Dans sa contribution, le Japon met en avant les quatre aspects sur lesquels il se concentre, à savoir le réseau, les individus, la technologie et le partenariat et la collaboration au niveau international pour assurer la fiabilité des réseaux d'information et de communication. Concernant le réseau, le Japon a encouragé le partage d'informations entre opérateurs de télécommunication. Par exemple, en 2002, 19 grands fournisseurs d'accès Internet et opérateurs de télécommunication au Japon ont lancé de leur propre initiative Telecom-ISAC (Information Sharing and Analysis Centre) Japan[14] qui collecte, analyse et partage des renseignements dans le domaine de la sécurité comme les vulnérabilités, incidents, contremesures et bonnes pratiques parmi ses membres. Concernant les individus, le Japon a sensibilisé les internautes par un site web et des séminaires, notamment. Du point de vue de la technologie, la Japon a soutenu des projets de recherche-développement comme PRACTICE. En se penchant sur ces aspects, le Japon a contribué à établir des réseaux TIC fiables et a encouragé la coopération internationale.

11 Document 2/228, « Cybersecurity in government and industry », Royaume-Uni de Grande-Bretagne et d'Irlande du Nord.
12 Document 2/198, « Collaborer avec le secteur privé pour gérer les cyberrisques », Etats-Unis d'Amérique.
13 Document 2/90, « Sharing knowledge, information and best practice for developing a culture of cybersecurity », Japon.
14 https://www.telecom-isac.jp/english/index.html.

4 CHAPITRE 4 – Protection en ligne des enfants (COP)

La présente section porte sur le point h) de la Question 3/2 qui appelle notamment à:

h) Continuer de recueillir des données d'expérience et de recenser les besoins, au niveau national, dans le domaine de la protection en ligne des enfants, en assurant une coordination avec les autres activités pertinentes.

Une contribution[15] portait en même temps sur le point g) de la Question 3/2, à savoir:

g) Réfléchir aux moyens permettant de prêter assistance aux pays en développement, en particulier les PMA, en ce qui concerne les problèmes liés à la cybersécurité.

A l'ère de l'Internet, la sécurité en ligne revêt une très grande importance, en particulier l'utilisation sûre et sécurisée de l'internet par les enfants. Par rapport aux adultes, les enfants ont des besoins et des vulnérabilités particuliers en ce qui concerne la sécurité en ligne, différence qui doit être reconnue.

Les enfants passent de plus en plus de temps à travailler sur l'Internet et à jouer sur des ordinateurs. Les réseaux sociaux jouent pour eux un rôle prépondérant. Parfois, les parents n'ont pas conscience du fait que les enfants partagent leurs informations personnelles en utilisant les réseaux sociaux, ce qui fait d'eux des proies pour les prédateurs en ligne.

Pour relever ces défis, de nombreux pays organisent des campagnes de sensibilisation qui visent à former les organismes publics, le secteur privé, les enseignants et les individus (parents et enfants) à détecter les problèmes potentiels et à comprendre leurs rôles et responsabilités propres pour créer un cyberespace plus sûr pour les enfants.

4.1 Résultats de l'enquête sur la protection en ligne des enfants

Le questionnaire sur la protection en ligne des enfants (COP) qui comprenait des questions tirées de contributions des Etats Membres (en particulier de l'Australie, du Royaume-Uni et du Vanuatu) abordait plusieurs questions essentielles, y compris les aspects législatifs et stratégiques de la COP, les méthodes de notification des incidents et les garanties techniques. Cent trente et un pays ont répondu au questionnaire COP. Les résultats montrent que seuls 37 des 131 pays ayant répondu ont confirmé disposer d'une stratégie nationale de protection en ligne des enfants. Parallèlement, nous observons que 101 pays prennent des mesures de protection en ligne des enfants. Bien qu'un pourcentage élevé de pays ayant répondu dispose de mesures COP, seuls 78 d'entre eux ont une législation dans ce domaine. Même si d'autres pays n'ont pas de législation, ils ont d'autres mesures comme des garanties techniques.

Par ailleurs, il existe dans 69 pays, sur les 131 ayant répondu, des organismes publics responsables de la COP. Le nombre de pays disposant d'organismes de protection en ligne des enfants est plus élevé que celui de pays qui n'en ont pas. Bien que ces organismes existent dans 69 pays, seuls 63 d'entre eux disposent d'un système établi de notification des affaires liées à la COP.

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

Figure 15 : Existe-t-il un organisme/une entité responsable de la protection en ligne des enfants?

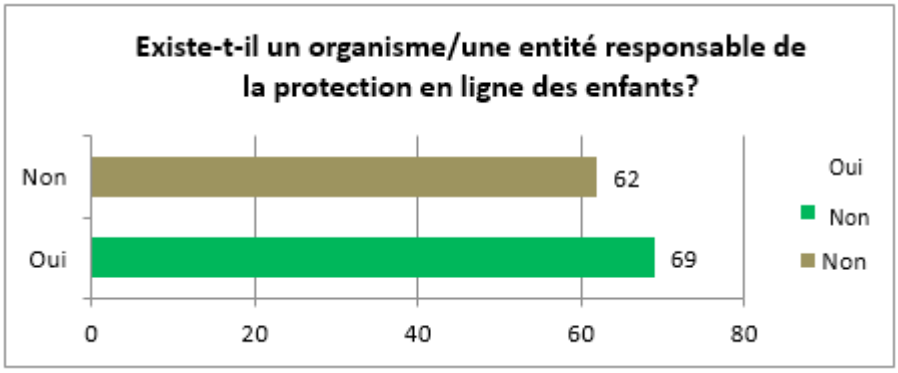
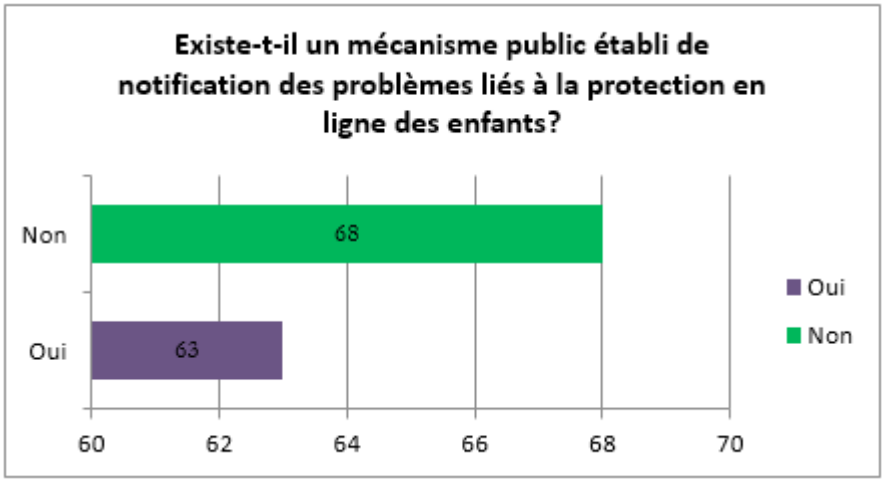
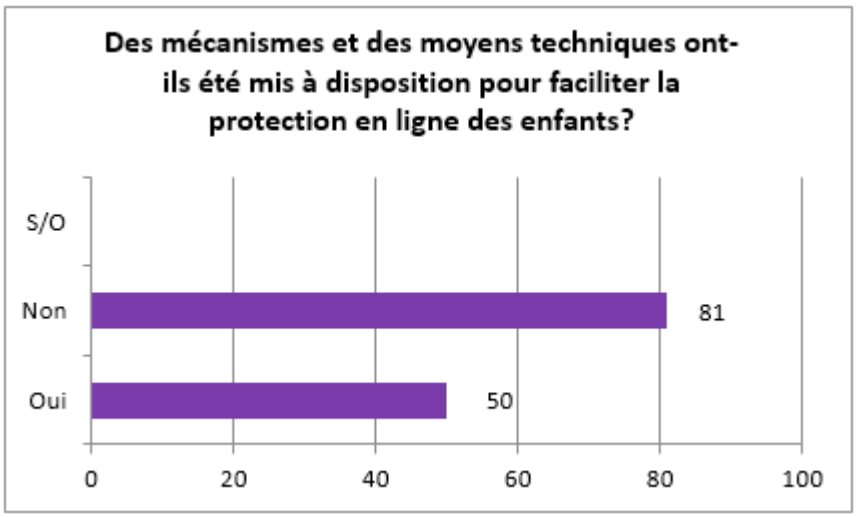


Figure 16 : Existe-t-il un mécanisme public établi de notification des problèmes liés à la protection en ligne des enfants?



Cinquante de ces pays disposent des capacités techniques requises pour contribuer à la COP. Ceci pourrait soulever des questions concernant les organismes responsables de la COP et la nature de leurs attributions. Il se peut que la nouveauté de ces organismes explique l'absence de système de notification ou de capacités techniques permettant de contribuer à la COP. Il se pourrait que ces organismes soient spécialisés dans toutes les questions relatives à l'enfance, et non pas spécifiquement dans la COP. Ainsi, l'attention portée aux risques rencontrés par les enfants en ligne pourrait pâtir du fait que ces organismes s'occupent aussi de tous les autres risques rencontrés par les enfants en général.

Figure 17 : Des mécanismes et des moyens techniques ont-ils été mis à disposition pour faciliter la protection en ligne des enfants?



Concernant les activités menées par les organisations gouvernementales ou les organisations non gouvernementales pour aider et informer les parties prenantes sur la façon de protéger les enfants en ligne, les résultats du questionnaire montrent que 62 pays ont entrepris ce type d'activités, alors que 68 ne l'ont pas fait, soit des résultats assez comparables.

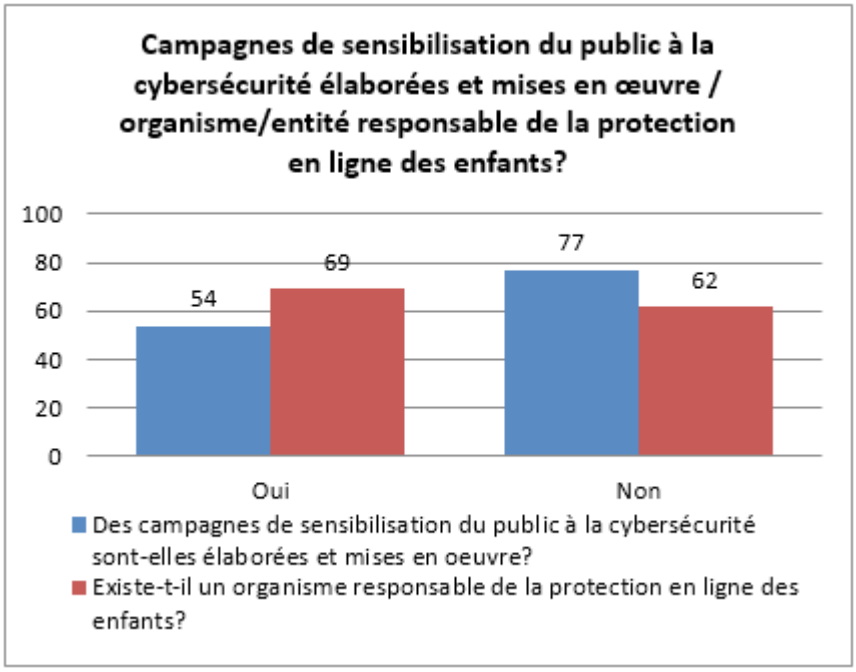
Figure 18 : Les autorités publiques ou les ONG ont-elles entrepris des activités pour aider et informer les différents acteurs (parents, responsables locaux, enseignants, etc.) sur la façon de protéger les enfants en ligne?

Etant donné que la COP ne peut être traitée sans souligner le rôle éducatif de la diffusion de ce type de protection parmi les intéressés, et que la COP a été examinée dans la **Section 2** qui traite de l'amélioration de la sensibilisation à la cybersécurité, question fondamentale qui est considérée comme faisant partie intégrante de la cybersécurité, nous aborderons ici plus en détail le rôle éducatif des parents et enseignants en matière de COP et de sensibilisation pour contribuer à identifier les faiblesses qui ont fait l'objet d'une attention particulière.

En ce qui concerne le rôle éducatif de la protection en ligne des enfants, une question générale portait sur le point de savoir si les Etats Membres disposent de programmes de formation spécifiques

pour protéger les enfants en ligne. Les résultats montrent que seuls 54 pays sur 131 disposent de programmes de cette nature.

Figure 19 : Campagnes de sensibilisation du public à la cybersécurité élaborées et mises en œuvre/ organisme/entité responsable de la protection en ligne des enfants?



Il convient de relever que l'existence d'organismes s'intéressant à la COP dans un pays donné ne signifie pas que ces organismes assument un rôle éducatif. De plus, l'absence d'organismes spécialisés dans la COP ne signifie pas que les pays n'assument pas de tâches d'éducation. Ceci est corroboré par le fait que ces organismes existent dans 69 pays mais que tous ces pays n'adoptent pas de programmes éducatifs pour la protection en ligne des enfants. En revanche, bien que 62 pays n'aient pas d'organisme spécialisé dans la COP, certains d'entre eux ont conçu et mis en œuvre des programmes de sensibilisation à la protection.

Une étude plus approfondie de la nature de ces programmes éducatifs et de leurs groupes cibles montre que les enfants sont le principal groupe cible, 52 pays ayant confirmé l'adoption de programmes visant les enfants, alors que 78 pays n'avaient aucun programme spécifiquement destiné aux enfants.

Les résultats du questionnaire révèlent que 50 pays sur 131 ont élaboré des programmes éducatifs pour les parents. Toutefois, le groupe des enseignants est le moins souvent visé, seuls 47 pays sur 131 ayant des programmes éducatifs leur étant destinés.

Concernant les campagnes de sensibilisation, 84 pays sur 131, soit 64,12 pour cent, mènent des campagnes spécifiquement axées sur la COP. Ce résultat concorde avec celui de la question qui appelait à définir les domaines prioritaires des Etats Membres en matière de cybersécurité, puisque la COP arrivait en deuxième position après la sécurité de l'Internet et arrivait en première position parmi les problèmes faisant l'objet de campagnes de sensibilisation dans les Etats Membres ayant répondu.

Figure 20 : Existe-t-il des campagnes de sensibilisation à la protection en ligne des enfants destinées aux enfants?

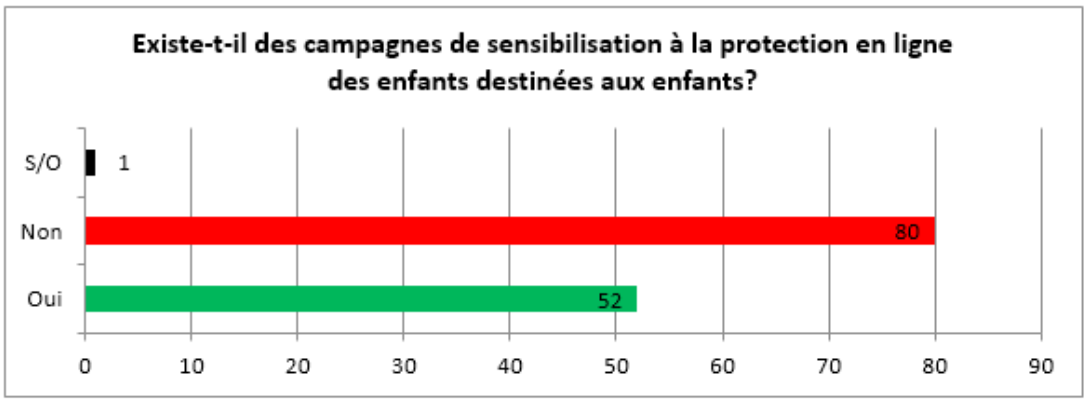
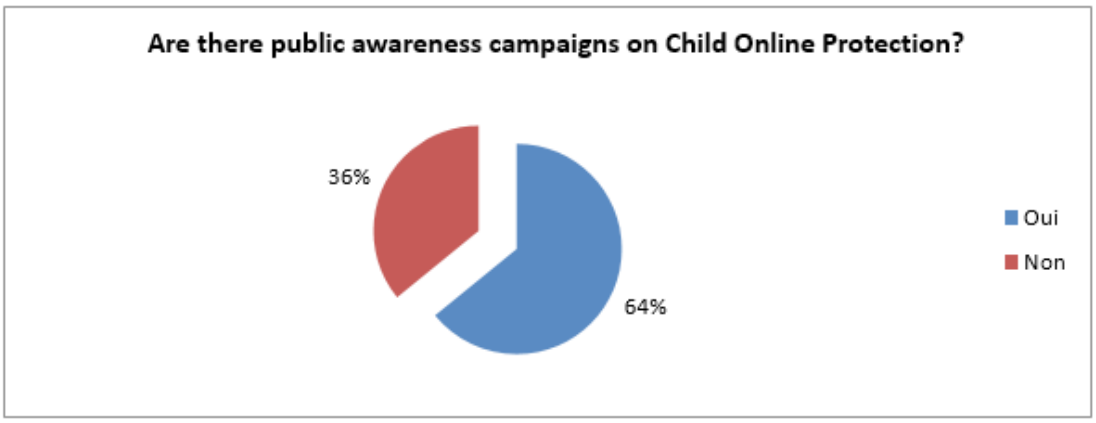


Figure 21 : Existe-t-il des campagnes de sensibilisation du public à la protection en ligne des enfants?



Soixante-dix-sept pays ont des programmes de sensibilisation destinés uniquement aux enfants, tandis que seuls 54 pays n'ont pas de programmes de ce type. Il ressort du questionnaire que le groupe des adultes bénéficie de nombre de programmes de sensibilisation ou d'éducation qui visent à la protection en ligne des enfants, 74 pays ayant confirmé disposer de ce type de programmepour les adultes et 57 pays déclarant ne pas en avoir. Sur cette base, nous relevons qu'il importe de cibler aussi bien les adultes que les enfants. Il n'est pas possible d'obtenir une sensibilisation complète sans une diffusion auprès des différents milieux de la société qui sont directement ou indirectement concernés par la question de la COP. La sensibilisation des enfants aux risques en ligne potentiels ne suffit pas si les adultes n'y sont pas aussi sensibilisés et s'ils ne connaissent pas les mesures à prendre pour protéger les enfants en ligne.

4.2 Stratégies et solutions techniques pour la protection en ligne des enfants

Certaines stratégies et solutions techniques figurent dans les contributions soumises à la Commission d'Études 2 au titre de la Question 3/2 pendant la période d'études. Comme le montrent les différents documents, la collaboration entre les différentes parties prenantes, les campagnes de sensibilisation, la participation du secteur privé et des mesures législatives pourraient contribuer à définir des stratégies et politiques en matière de sécurité en ligne des enfants. Premièrement, passer de la stratégie à la pratique est un processus de longue haleine qui commence par la collecte d'informations pertinentes. Dans une contribution[16] du Royaume-Uni, de l'Australie et du Vanuatu présentée à la réunion de

[16] Document 2/78, « Support of the Resolution on child online protection », Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, Australie et Vanuatu.

septembre 2014 de la Commission d'Études 2 de l'UIT-D, des mesures sont proposées pour apporter une aide aux Etats Membres dans le domaine de la protection en ligne des enfants (COP). Sur la base de leur contribution, ces pays suggèrent conjointement un certain nombre de questions à poser aux Etats Membres pour mieux comprendre comment ils agissent au niveau national en matière de COP. Deuxièmement, l'élaboration de solutions techniques n'est jamais un processus statique; c'est plutôt une démarche dynamique qui exige une réflexion et une adaptation constantes. Par exemple, suite aux discussions qui ont eu lieu pendant la réunion du Groupe du Rapporteur pour la Question 3/2 tenue en 2015, **l'Australie, la Papouasie-Nouvelle-Guinée, l'Etat indépendant du Samoa, le Royaume-Uni et la République de Vanuatu**[17] ont présenté des questions modifiées concernant la protection en ligne des enfants. Il a été proposé que ces questions soient soumises à la plénière de la commission d'études pour distribution aux Etats Membres, afin qu'ils y répondent, soit directement, soit dans le cadre d'un questionnaire plus détaillé. Ces questions portent sur les activités liées à la protection en ligne des enfants au niveau national, dans les domaines de la législation, du mécanisme de notification, des capacités et de l'apport de soutien et de connaissances aux parties prenantes. De plus, au titre de la Résolution 67 (Rév. Dubaï, 2014),[18] de la CMDT, le Royaume-Uni, l'Australie et la République de Vanuatu proposent conjointement un rapport intitulé « Bonnes pratiques pour soutenir les parents dans la protection en ligne des enfants » qui devrait prendre en considération toutes les parties prenantes (notamment, sans que cette liste soit exhaustive, les gouvernements, les parents, les écoles, les organisations de protection de l'enfance, la police et les services d'urgence, les opérateurs et les fournisseurs d'accès à l'Internet). Ce rapport met en avant l'importance de la définition des rôles et responsabilités, de la collecte de bonnes pratiques et de la mise en œuvre d'une méthode fondée sur des bases factuelles.

Enfin, il convient de souligner que lors de l'élaboration d'un tel rapport, un questionnaire recueillant des renseignements sur ce qui existe dans différents pays devrait être soumis et que le premier projet devrait être distribué aux parties prenantes pour information et commentaires.

Les stratégies nationales doivent être complétées par des solutions techniques: comme l'a indiqué l'Académie Nationale des Télécommunications A.S. Popov d'Odessa (Ukraine),[19] pour mettre en œuvre un des éléments de l'initiative régionale sur la COP dans la région de la CEI, l'Académie a mis en commun les efforts de collecte de données sur les solutions techniques existantes pour la protection en ligne des enfants (www.contentfiltering.info). A cet égard, le groupe d'experts a dressé une liste des solutions techniques existantes sur la base de différentes caractéristiques, comme le type de mise en œuvre (logiciel, matériel, nuage); la compatibilité avec les systèmes d'exploitation (plate-forme unique, plate-forme croisée, indépendance vis-à-vis de la plate-forme); le type de prise en charge (système entièrement pris en charge, système partiellement pris en charge, système non pris en charge); la commande (télécommande, commande locale, pas de commande); le type de sécurité interne (système protégé ou système non protégé).

Chaque solution technique figurant dans la liste a été installée sur un ordinateur ou un dispositif mobile (dans le cas de produits payants, l'autorisation pour les tests a été obtenue auprès du concepteur) dans le but de tester chaque fonction. Pour chaque solution, un rapport de test a été élaboré et versé dans la base de données de service Countentfiltering.info. Les données relatives à chaque produit, une fois versées dans la base de données, sont vérifiées à intervalles réguliers par les concepteurs des systèmes et, si nécessaire, mises à jour et complétées. En outre, le logiciel Contentfiltering.info a été

[17] Document SG2RGQ/56, « Proposed questions on child online protection », Australie, Papouasie-Nouvelle-Guinée, Etat indépendant du Samoa, Royaume-Uni et République de Vanuatu.

[18] Résolution 67 de la CMDT « Rôle du Secteur du développement des télécommunications de l'UIT dans la protection en ligne des enfants » disponible à l'adresse https://www.itu.int/pub/D-TDC-WTDC-2014.

[19] Document 2/322, « Création d'une base de données sur les solutions techniques existantes en matière de protection en ligne des enfants (Contentfiltering.info) », Académie Nationale des Télécommunications A.S. Popov Odessa (Ukraine).

conçu à partir des recommandations relatives au choix du meilleur système de filtrage de contenus pour un utilisateur/une organisation donné(e). Il comprend deux modules:

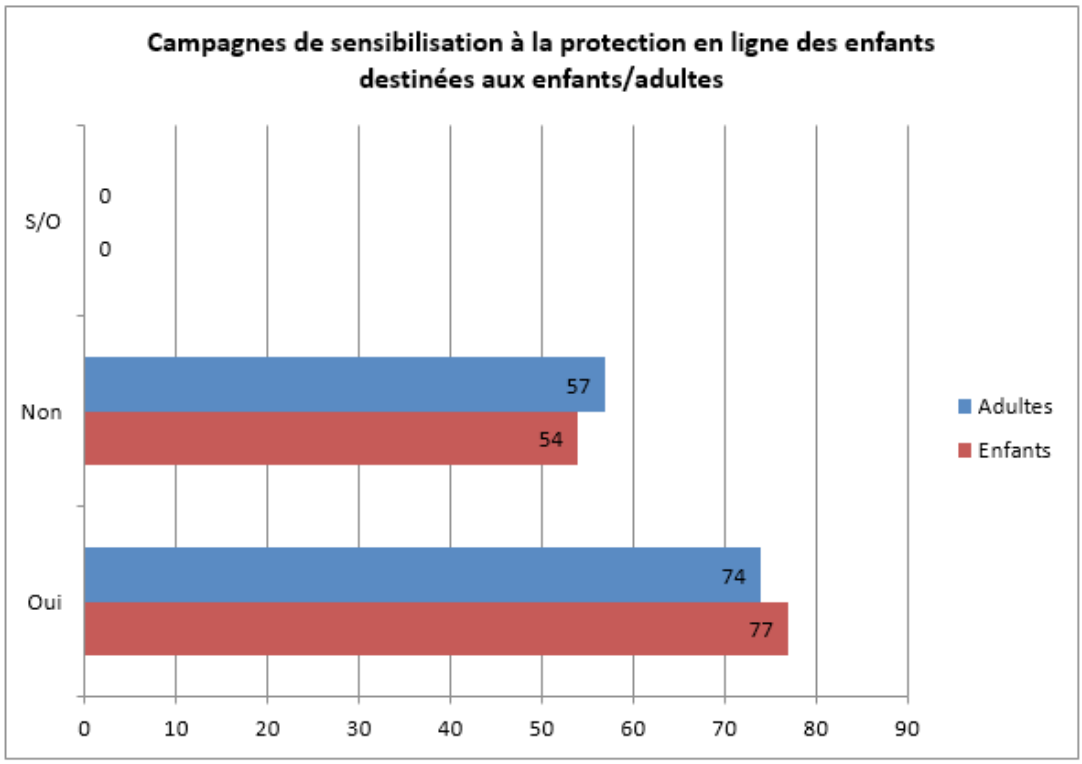
a) un module utilisateur (en libre accès) pour définir le niveau de compétences de l'utilisateur, formuler les exigences et choisir le système de filtrage des contenus; et

b) un module expert (uniquement pour les experts autorisés) pour entrer les données relatives aux solutions techniques en matière de protection en ligne des enfants.

L'Académie Nationale des Télécommunications A.S. Popov d'Odessa (Ukraine)[20] a également fourni des renseignements complémentaires sur un cours d'apprentissage multimédia à distance sur l'utilisation sécurisée des ressources de l'Internet (https://onlinesafety.info) qui a été élaboré dans le cadre de l'initiative régionale de l'UIT relative à la création d'un centre de protection en ligne des enfants pour la région de la CEI.

La **Figure 22** montre que si un certain nombre de pays mènent des campagnes de sensibilisation du public à la protection en ligne des enfants, de telles campagnes n'existent pas dans un assez grand nombre de pays.

Figure 22 : Campagnes de sensibilisation à la protection en ligne des enfants destinées aux enfants/adultes



4.2.1 Sensibilisation à la COP et activités connexes

Dans une contribution,[21] la **République de Corée** présente les efforts entrepris au niveau national dans différents pays dans les domaines du cadre juridique, des campagnes sociales et de l'éducation en ligne pour la COP. Selon cette contribution, comme l'âge moyen des enfants ayant accès à l'Internet

[20] Document 2/156, « Multimedia distance-learning course on the safe use of Internet resources », Académie nationale des télécommunications A.S. Popov Odessa (Ukraine).

[21] Document 2/362, « Proposed text for inclusion in Chapter 6 (Child Online Protection) of the Final Report », République de Corée.

diminue, l''utilisation sûre de l'Internet parmi les enfants devient une question importante dans de nombreux pays. En particulier, le document de la Corée souligne la nécessité de mesures volontaires d'autorégulation pour compléter les mesures juridiques et obligatoires. Alors que ces mesures peuvent conduire à des résultats visibles et rapides, il existe aussi le risque qu'elles soient trop restrictives, avec pour conséquences une atteinte à la liberté individuelle ou à l'autonomie des utilisateurs. Par exemple, la mesure juridique prise par la Corée pour bloquer l'accès des mineurs aux jeux en ligne après minuit a donné lieu à un débat animé concernant sa validité et son efficacité. En conséquence, les mesures juridiques et obligatoires devraient être complétées par des programmes d'éducation et de sensibilisation associant différentes parties prenantes.

Une autre question soulevée par la République de Corée est liée à la difficulté de distinguer entre les fournisseurs de service et les utilisateurs. Les parents peuvent affirmer que les fournisseurs de service doivent faire davantage d'efforts pour assurer la sécurité en ligne des enfants. Toutefois, certains fournisseurs de service peuvent avancer que la responsabilité du conseil et de la sensibilisation incombe aux parents, aux enseignants et aux tuteurs. Les campagnes et programmes

sociaux peuvent contribuer à la définition de mesures qui permettent une plus grande coopération entre toutes les parties prenantes et les encouragent à participer activement aux efforts de sécurité en ligne soutenus par les pouvoirs publics.

Concernant les pays les moins avancés, la contribution[22] de la **République de Gambie** souligne le besoin urgent de mettre en place la protection en ligne des enfants de façon globale dans des cadres nationaux de cybersécurité. Les pays les moins avancés commencent tout juste à bénéficier de l'Internet rapide sur des plates-formes moins coûteuses que les ordinateurs de bureau et les ordinateurs portables traditionnels. L'importance de la coopération internationale est soulignée, non seulement pour le partage de la sensibilisation aux problèmes, mais aussi pour la cohérence des politiques internationales et le soutien à des activités propres à renforcer encore la coopération internationale. Cette contribution appelle à intégrer la protection en ligne des enfants dans un cadre national de cybersécurité et à se concentrer sur les questions juridiques, techniques et d'organisation, tout en renforçant les capacités et la coopération internationale.

Enfin, il est indiqué dans la note de liaison de la JCA-COP[23] de l'UIT-T, que l'importance du partage de renseignements entre les membres doit être portée à l'attention des responsables de l'étude de la Question 3/2. Les efforts nationaux accomplis par la République de Corée et la Gambie ainsi que par des ONG comme Defz Kidz sont reconnus dans cette note.

4.2.2 Stratégies relatives à la protection en ligne des enfants

Les stratégies ci-après peuvent être adoptées par les Etats Membres. Ces stratégies sont décrites dans les contributions soumises.

- Collaboration entre les différentes parties prenantes.
- Campagnes de sensibilisation.
- Participation du secteur privé.
- Mesures législatives.
- Elaboration d'un mécanisme approprié de communication de l'information.
- Renforcement des capacités des parties prenantes concernées.
- Fourniture d'un appui et de connaissances à toutes les parties prenantes.

[22] Document SG2RGQ/104, « Arguments en faveur de l'adoption d'initiatives en faveur de la protection en ligne des enfants dans les PMA », République de la Gambie.

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

- Mise en place de mécanismes destinés à associer toutes les parties prenantes (y compris, sans toutefois que cette liste soit limitative, les gouvernements, les parents, les écoles, les organisations de protection de l'enfance, la police et les services d'urgence, les opérateurs et les fournisseurs d'accès à l'Internet).
- Définir clairement les rôles et responsabilités des parties prenantes (qui fait quoi, quand, et de quelle manière).
- Collecte de données sur les bonnes pratiques relatives aux solutions techniques existantes pour la protection en ligne des enfants.
- Diffusion des renseignements pertinents aux parties prenantes.
- Mise en œuvre d'une approche actuelle.

5 CHAPITRE 5 – Résultats des ateliers sur la cybersécurité

La présente section porte sur le point i) de la Question 3/2 qui appelle notamment à:

i) Organiser des séances ad hoc, des séminaires et des ateliers pour échanger des connaissances, des informations et de bonnes pratiques concernant les mesures et activités concrètes, efficaces et utiles à mettre en place pour renforcer la cybersécurité en utilisant les résultats de l'étude, dont la tenue devra être la plus proche possible de celle des réunions de la Commission d'Études 1 ou des réunions du groupe du rapporteur de la Commission d'études 1 pour la Question.

La collaboration entre la Commission d'Études 2 de l'UIT-D, le BDT, les autres secteurs, le secteur privé et les établissements universitaires s'est caractérisée par une série d'ateliers qui ont eu lieu pendant la période d'études. Un certain nombre de contributions figurent dans l'**Annexe 2**. On trouvera ci-dessous un résumé de cette collaboration.

5.1 Premier atelier sur la cybersécurité (8 septembre 2015)

L'atelier sur la cybersécurité sur le thème « Les enjeux de la cybersécurité mondiale et la collaboration pour un renforcement efficace de la cybersécurité dans les pays en développement »[24] s'est tenu l'après-midi du 8 septembre 2015 à l'occasion des réunions de la Commission d'Études 2 de l'UIT-D et de la Commission d'Études 17 de l'UIT-T (Sécurité), avant la réunion sur la Question 3/2 de la Commission d'Études 2 de l'UIT-D.

But de l'atelier

L'atelier sur la cybersécurité avait pour but d'échanger de bonnes pratiques sur les méthodes adoptées aux niveaux international, régional et national en vue d'améliorer le renforcement des capacités en matière de cybersécurité. Il visait à tenir compte des problèmes que rencontrent les pays en développement en ce qui concerne le renforcement des capacités en matière de cyber sécurité et à rechercher des moyens novateurs et concrets permettant aux organisations internationales, aux administrations et au secteur privé de collaborer pour remédier à ces problèmes.

Ordre du jour

M. Yushi Torigoe (adjoint au Directeur du BDT) et M. Reinhard Scholl (Adjoint au Directeur du TSB) ont prononcé les remarques liminaires. Deux séances avec des exposés et des tables rondes étaient inscrites à l'ordre du jour:

– Séance 1: bonnes pratiques pour une méthode stratégique à différents niveaux pour renforcer efficacement la cybersécurité dans les pays en développement (3 exposés et une table ronde).

– Séance 2: difficultés rencontrées par les pays en développement; collaboration internationale pour encourager les initiatives dans le domaine de la cybersécurité (3 exposés et une table ronde).

Discussions et conclusion de l'atelier

Des exposés instructifs et utiles, des tables rondes et des séances de questions-réponses ont eu lieu pendant l'atelier au sujet des bonnes pratiques en vue d'élaborer une méthode stratégique à différents niveaux pour renforcer efficacement la cybersécurité dans les pays en développement et au sujet de la collaboration internationale pour encourager les initiatives de cybersécurité.

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

Pendant les deux séances, l'importance des aspects suivants de la cybersécurité, qui ont fait l'objet d'un échange entre les participants, a été soulignée:

- sensibilisation de toutes les parties prenantes à la cybersécurité;
- participation de toutes les parties à la mise en œuvre d'une stratégie nationale de cybersécurité;
- définition de principes clairs de cybersécurité dans la stratégie de cybersécurité, comme la libre circulation de l'information, la primauté du droit, l'autogouvernance, l'ouverture et la participation de multiples parties prenantes;
- ensemble clair d'objectifs dans la stratégie nationale;
- méthode de gestion des risques;
- législation nationale sur la cybersécurité;
- réglementation technique comprenant des normes et des procédures; et
- collaboration avec des initiatives internationales et régionales.

Il a aussi été noté que l'organisation d'ateliers de ce type devrait se poursuivre et que la discussion devrait être mise à jour. M. Ahmad Sharafat (Président de la Commission d'Études 2 de l'UIT-D) et M. Arkady Kremer (Président de la Commission d'Études 17 de l'UIT-T) ont rappelé qu'il était important que les participants échangent des informations et des points de vue et que la collaboration soit renforcée entre la Commission d'Études 17 de l'UIT-T (Sécurité) et la Commission d'Études 2 de l'UIT-D, en particulier au titre de la Question 3/2. Les résultats de l'atelier ont été par la suite présentés aux responsables de l'étude de la Question 3 de la Commission d'Études 2 de l'UIT-D et à la Commission d'Études 17 de l'UIT-T.

5.2 Deuxième atelier sur la cybersécurité (18-19 avril 2016)

L'atelier sur la cybersécurité de l'UIT, qui avait pour thème « Cyberexercices et stratégies nationales en matière de cybersécurité élaborées sur la base des bonnes pratiques »[25] a eu lieu l'après-midi du 18 avril 2016 et le matin du 19 avril 2016 à l'occasion de la réunion du Groupe du Rapporteur pour la Question 3/2 de la Commission d'Études 2 de l'UIT-D (Sécurisation des réseaux d'information et de communication: bonnes pratiques pour créer une culture de la cybersécurité). Cet atelier a été organisé par l'équipe de l'UIT chargée de la cybersécurité, avec le concours de l'équipe des Commissions d'Études de l'UIT-D. Un groupe d'éminents orateurs y a participé.

But de l'atelier

Le but de l'atelier sur la cybersécurité était de partager les bonnes pratiques sur les méthodes aux niveaux international, régional et national en vue de renforcer les capacités dans le domaine de la cybersécurité. A cet égard, l'atelier avait les objectifs suivants:

- partager les résultats d'expérience des cyberexercices nationaux avec des pays en développement pour mieux comprendre leurs besoins, d'autant que l'UIT est en train d'élaborer un nouveau service de cyberexercices destinés aux Etats Membres;
- partager les enseignements tirés et les conseils d'experts pour la préparation et la mise en œuvre de stratégies nationales en matière de cybersécurité et pour que l'UIT partage avec ses Etats Membres les travaux en cours sur la méthode multi-parties prenantes utilisée pour le nouveau kit pratique de stratégies nationales en matière de cybersécurité.

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

Ordre du jour

M. Yushi Torigoe (Adjoint au Directeur du BDT) a prononcé les remarques liminaires. L'atelier comportait trois séances comprenant des exposés et des tables rondes:

- Séance du 18 avril: renforcer les cyberexercices nationaux par le partage de résultats d'expérience.
- Séance 1 du 19 avril: éléments clés pour élaborer une stratégie nationale en matière de cybersécurité.
- Séance 2 du 19 avril: mise en œuvre efficace d'une stratégie nationale en matière de cybersécurité.

Discussions et conclusion de l'atelier

Des exposés instructifs et utiles, des tables rondes et des séances de questions-réponses ont eu lieu durant l'atelier. Pendant les séances, l'importance des aspects suivants de la cybersécurité, qui ont fait l'objet d'un échange entre les participants, a été soulignée:

- les scénarios des cyberexercices nationaux doivent être réalistes et ne doivent pas s'apparenter à du cinéma pour être acceptés par les équipes dirigeantes et bénéficier d'un financement;
- les cyberexercices nationaux doivent faire participer toutes les parties intéressées, notamment les pouvoirs publics et le secteur privé, dès l'étape de planification et en assurant un partage actif des informations;
- les objectifs d'un cyberexercice national doivent être clairement définis et apporter une valeur ajoutée;
- les scénarios des cyberexercices sont choisis sur la base d'une méthode de gestion des risques – répondez à la question « quelle est la plus grande menace ou la situation ayant le plus fort impact? » et poursuivez sur cette base;
- certains cyberexercices nationaux sont menés pour tester des plans d'urgence nationaux;
- les stratégies de cybersécurité nationales doivent-elle ou non être publiques? Il n'existe pas de réponse claire pour le moment, mais pour assurer la sensibilisation des citoyens, au moins une partie de la stratégie doit être rendue publique;
- une méthode de gestion des risques pour l'élaboration d'une stratégie de cybersécurité nationale est un élément essentiel pour définir et atteindre les objectifs appropriés;
- la protection de l'infrastructure critique (CIP) est essentielle à la cybersécurité et appelle généralement un partenariat public-privé. Il faut donc assurer la participation du secteur privé à la stratégie;
- constituez une équipe et trouvez un champion, regardez ce que font les autres et assurez-vous de travailler avec une équipe spéciale. Le kit pratique pour la stratégie de cybersécurité nationale peut vous être utile à cette fin;
- la stratégie de cybersécurité nationale est votre bible en matière de cybersécurité. Les buts et les mesures doivent être appropriés. Etablissez un lien avec la protection de l'infrastructure critique et votre situation socio-économique. Ensuite mettez-la en œuvre en assurant un contrôle approprié;
- institutionnalisez les PPP pour la stratégie de cybersécurité nationale et la protection de l'infrastructure critique par des règlements et une législation, car les entités du secteur privé et les pouvoirs publics n'ont pas les mêmes objectifs. Or, il convient de les harmoniser;
- la mise en œuvre d'une stratégie de cybersécurité prend du temps pour les pays qui n'ont pas d'expérience dans ce domaine. En effet, il faut faire accepter la stratégie et obtenir les autorisations nécessaires à son lancement. Son acceptation et son financement sont facilités si elle est liée à la stratégie de développement de la société de l'information du pays;

- la mise en œuvre d'une stratégie de cybersécurité exige un plan d'action détaillé, assorti d'un budget;
- l'importance de l'analyse d'impact a été soulignée comme élément constitutif du cycle de mise au point/mise en œuvre d'une stratégie de cybersécurité nationale;
- le plan de mise en oeuvre devrait inclure des transferts de données sécurisés dans le cadre de l'administration électronique;
- les indices (GCI et d'autres) prennent de l'importance pour mesurer la mise en œuvre et en tant que liste de contrôle pour la stratégie de cybersécurité nationale;
- l'indice national de cybersécurité de l'Estonie (dont la méthodologie a été publiée fin mai 2016). L'Indice de cybersécurité dans le monde de l'UIT a été mis en avant comme étant complémentaire;
- la stratégie de cybersécurité nationale du Royaume-Uni devait être publiée ultérieurement en 2016;
- l'évaluation d'une stratégie de cybersécurité nationale prend du temps et peut être gênante, mais contribue à obtenir des financements;
- des définitions communes des stratégies de cybersécurité sont importantes dès le début de l'élaboration des stratégies, pour permettre à toutes les parties prenantes d'avoir une compréhension et une vision communes. Une compréhension commune est plus importante qu'une définition commune.

Dans sa conclusion de l'atelier, M. Luc Dandurand (BDT) a souligné l'importance des possibilités de partage de renseignements et de points de vue entre les participants et les experts et la nécessité de continuer de collaborer avec la Commission d'Études 2 de l'UIT-D au titre de la Question 3/2. Dans ses remarques finales, M. Ahmad Sharafat (Président de la Commission d'Études 2 de l'UIT-D) a relevé que l'organisation par la Commission d'Études 2 de l'UIT-D, au titre de la Question 3/2, d'un atelier sur la cybersécurité était en train de devenir une tradition et a exprimé l'espoir qu'elle se perpétue. Etant issu des milieux universitaires, il a estimé que les résultats tirés de ces échanges étaient exceptionnellement fructueux. Les résultats de l'atelier ont été transmis ultérieurement aux responsables de l'étude de la Question 3/2 de la Commission d'Études 2 de l'UIT-D.

5.3 Troisième atelier sur la cybersécurité (26 janvier 2017)

L'atelier sur la cybersécurité ayant pour thème « Cybersécurité et évaluation des risques dans la pratique »,[26] s'est tenu l'après-midi du 26 janvier 2017, dans le cadre des réunions du Groupe du Rapporteur de la Commission d'Études 2 de l'UIT-D et avant la réunion des responsables de l'étude de la Question de la Question 3/2 de la Commission d'Études 2 de l'UIT-D.

But de l'atelier

Cet atelier avait pour objectif de réunir des experts du monde entier, pour qu'ils échangent leurs connaissances et leurs données d'expérience sur l'évaluation pratique des cyberrisques au niveau national, dans les très grandes organisations et dans les secteurs des infrastructures essentielles. Les participants à cet atelier ont également examiné les risques pour la chaîne d'approvisionnement et le rôle que jouent les normes dans la gestion des cyberrisques au sein des organisations.

Ordre du jour

A l'issue des remarques liminaires prononcées par un représentant du BDT, l'atelier a commencé son programme de cinq séances, qui comprenaient des exposés et des tables rondes, à savoir:

- principales menaces en matière de cybersécurité en 2017 et au-delà;

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

- méthodes et outils utilisés dans le secteur privé pour évaluer les cyberrisques dans les grandes organisations;
- évaluation des cyberrisques dans les secteurs des infrastructures essentielles;
- risques pour la chaîne d'approvisionnement; et
- rôle des normes et mise à jour des normes des séries ISO/CEI 27000.

Discussions et conclusion de l'atelier

Des exposés instructifs et utiles, des tables rondes et des séances de questions-réponses ont eu lieu durant le troisième l'atelier. Pendant les séances, l'importance des aspects suivants de la cybersécurité, qui ont fait l'objet d'un échange entre les participants, a été mise en avant:

- Les principales menaces ci-après en matière de cybersécurité – convergence des menaces cybernétiques et matérielles, convergence des menaces vie privée/vie professionnelle, menaces internes, augmentation du nombre d'attaques menées pour des raisons financières, attaques par déni de service (DDoS) basées sur l'IoT et accroissement du nombre de violations « simples » – ont été présentées et des recommandations à l'intention des organisations ont été examinées.
- Les difficultés que soulève l'évaluation des risques dans le secteur privé, telles que la multiplicité des normes à respecter, les audits externes, les exigences réglementaires imposées par les différents services, les fusions et acquisitions/la diversification/le positionnement international, et le rapport coût/efficacité des contrôles de cybersécurité, ont été évoquées et des exemples de méthodes à adopter pour remédier à ces difficultés, notamment les logiciels de gouvernance et de gestion du risque, l'approche en matière d'opérations de sécurité, les outils de détection tactique des risques et la gestion des vulnérabilités, ont été présentées.
- Les stratégies nationales relatives à la protection des infrastructures essentielles contre les cyberrisques, en particulier l'évaluation des cyberrisques du CIPP (méthodologie, point de départ, vulnérabilité des processus dans le cas de l'aviation) ont été présentées.
- La sécurité de la chaîne d'approvisionnement des TIC, les problèmes qu'elle pose et les exigences qui s'y rattachent ont été abordés et les principaux points ci-après ont été examinés: (1) aborder les risques dans un programme global de gestion des risques, (2) comprendre les exigences communes, (3) utiliser les normes internationales, (4) miser sur le pouvoir d'achat et (5) travailler en partenariat.
- Le rôle des normes internationales dans la gestion des risques et la dernière mise à jour des documents de la série ISO/CEI 27000 du Groupe ISO/CEI JTC1 SC27 ont été présentés.

Pendant les discussions et dans les remarques de clôture, l'accent a été mis sur l'importance que revêtent ces ateliers pour les participants et les experts, qui peuvent procéder à des échanges de vues, et il a indiqué qu'il fallait poursuivre la collaboration avec les responsables de l'étude de la Question 3/2 de la Commission d'Études 2 de l'UIT-D.

6 CHAPITRE 6 – La cybersécurité: possibilités et défis

Dans le cadre de la Question 3/2 de l'UIT-D, les participants ont examiné d'autres domaines, dont un grand nombre sont liées à des travaux normalement menés ailleurs et ne figurent pas dans l'objet actuel de cette Question. Comme plusieurs discussions formelles et informelles ont eu lieu avec des organisations, les contributions relatives au point b) de l'objet de la Question sont examinées plus en détail ci-dessous.

b) Fournir des informations sur les problèmes que rencontrent actuellement les fournisseurs de services, les organismes de réglementation et d'autres parties prenantes dans le domaine de la cybersécurité.

6.1 Addiction à l'Internet

« L'addiction à l'Internet » est un effet préjudiciable qui est apparu en raison des progrès accomplis dans le domaine de l'information et de la généralisation de l'utilisation de l'Internet. Bien que ce concept reste à définir clairement en termes psychologiques et médicaux, l'addiction à l'Internet désigne généralement des atteintes difficilement réversibles aux fonctions physiques, mentales et sociales d'individus, suite à une utilisation excessive des services informatiques en ligne. La plupart des personnes souffrant d'une addiction à l'Internet présentent des symptômes de manque et de tolérance, comme l'anxiété extrême ou la dépression nerveuse qui posent de sérieux problèmes dans leur vie quotidienne. Les internautes dépendants de l'Internet sont tellement absorbés par le cyberespace qu'ils présentent des addictions diverses, par exemple au jeu, aux discussions en ligne, à la pornographie, etc.

Ces dernières années, l'addiction aux services TIC s'est imposée dans les modes de vie et de communication en pleine évolution suite à une augmentation rapide de l'adoption des TIC et à la fusion et à la convergence des technologies.

Mesures prises par la République de Corée pour prévenir et limiter l'addiction à l'Internet et au smartphone

En République de Corée, environ 7 pour cent des internautes âgés de 5 à 54 ans relèvent du groupe à risque d'une addiction à l'Internet, selon l'enquête de 2013 sur l'addiction à l'Internet. En Corée, la part d'internautes à risque par rapport au total des utilisateurs a baissé, passant de 7,7 pour cent en 2011 à 7,2 pour cent en 2012 et 7,0 pour cent en 2013. Toutefois, le pourcentage d'adolescents à risque a augmenté, passant de 10,4 pour cent en 2011 à 10,7 pour cent en 2012 et 11,7 pour cent en 2013.[27]

Entre-temps, l'addiction au téléphone intelligent a progressé plus fortement que celle à l'Internet. Quelque 11,8 pour cent des utilisateurs de smartphone âgés de 10 à 54 ans en Corée appartenait au groupe à risque des utilisateurs excessifs, soit une augmentation de 3,4 points de pourcentage par rapport à 8,4 pour cent en 2011, année du début de l'enquête sur l'addiction au téléphone intelligent. Les adolescents étaient le groupe à risque le plus exposé: quelque 25,5 pour cent des adolescents coréens (âgés de 10 à 19 ans) figuraient dans ce groupe, par rapport à 8,9 pour cent des adultes. Créé en 2002 par le Gouvernement coréen, le Centre coréen sur l'addiction à l'Internet a mené des programmes étendus de conseil, de création et distribution de contenus, de formation de conseillers spécialisés et d'éducation préventive dans tout le pays, pour traiter de façon systématique l'utilisation excessive de l'Internet et des appareils intelligents. Il a réalisé une étude annuelle sur l'addiction à l'Internet de la population en général depuis 2004 (et sur l'addiction au téléphone intelligent depuis 2011), qui a permis d'obtenir des statistiques nationales qui servent d'indice de référence pour l'élaboration des politiques publiques.

En juin 2013, huit ministères ont établi conjointement un « Deuxième plan complet de prévention et de réduction de l'addiction à l'Internet ». Ce programme définit une gamme étendue d'aides

[27] Document SG2RGQ/64, « Korea's Internet of things security roadmap », République de Corée.

préventives, de conseil, des soutiens psychiatriques et de suivi pour les groupes d'âge suivants: enfants en bas âge, étudiants et adultes.

Le gouvernement a mis en place une commission interministérielle des politiques chargée de traiter systématiquement la question de l'addiction à l'Internet. En mars 2014, la commission a élaboré le « Programme 2014 d'exécution de la prévention et de la réduction de l'addiction à l'Internet ». Ce programme a été mis en œuvre conjointement sous la direction de la commission des politiques regroupant huit ministères de façon efficace et systématique.

Education préventive

L'Internet et les services TIC sont si facilement accessibles dans la vie quotidienne que l'éducation devrait se concentrer sur la prévention, avant que des symptômes d'addiction comme le manque ou la tolérance n'apparaissent. Le programme d'éducation coréen est conçu pour assurer une prévention efficace. Il vise à sensibiliser le public aux risques potentiels ou réels d'addiction et à l'aider à mieux s'en protéger. Par exemple, il assure une éducation préventive qui adapte son programme aux besoins de chaque groupe d'âge que constituent les enfants en bas âge, les adolescents et les adultes. Des conseillers spécialisés se rendent dans les écoles pour donner un cours spécial d'une durée d'une heure.

En Corée, un programme de formation intensif (deux heures) est disponible pour les élèves des écoles primaires, élémentaires et secondaires depuis 2013; chaque cours est conçu différemment pour chaque tranche d'âge et met l'accent sur la participation des écoliers et la discussion. Pendant le cours, chaque élève utilise son propre « manuel » comme un outil d'autodiagnostic dans lequel il consigne son utilisation de l'Internet et des services TIC, en prenant parfois la résolution de réduire son utilisation de l'Internet s'il se révèle être un utilisateur excessif.

Tableau 1: Nombre de participants au cours d'éducation préventive

Catégorie	2010	2011	2012	2013	Juin 2014	Total
Préscolaire	–	31 279	18 200	47 890	26 050	**123 419**
Adolescent	645 981	954 425	621 621	970 696	407 512	**3 600 235**
Adulte	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**

(Unité: personne)

Depuis 2014, a été lancé un programme « Jeu de prévention des addictions » destiné aux enfants d'âge préscolaire et des petites classes du primaire pour transmettre de façon simple et efficace un message qui soit aussi distrayant pour les enfants. Dans ce programme, les enfants et écoliers assistent à une pièce ou un spectacle de marionnettes qui raconte les histoires d'un animal favori développant une addiction à l'Internet ou évoque l'addiction dans la vie quotidienne familiale. Après le spectacle, l'enseignant parle des dangers de l'addiction à l'Internet et des moyens de la prévenir. Ce programme est efficace pour faire facilement comprendre aux enfants le concept de l'addiction, sans susciter de sentiment de rejet.

Une aide a aussi été apportée à 23 écoles désignées « Ecoles garantissant une utilisation saine des services TIC ». Ce programme est destiné à soutenir les activités/campagnes scolaires qui encouragent une culture saine d'utilisation des services TIC et visent à prévenir l'addiction à l'Internet en coopérant avec les parents, enseignants et experts.

Services de conseil et mise en place d'infrastructures

Le Ministère de la Science, des TIC et de la Planification (MSIP) de la République de Corée organise un service d'éducation préventive et de conseils spécialisés pour s'attaquer de façon efficace aux addictions à l'Internet et au téléphone intelligent. Pour garantir un service adapté à chaque région, il exploite 14 centres de prévention de l'addiction à l'Internet (IAPC) implantés dans 13 villes ou provinces de tout le pays (état en juin 2014).

Il propose des services de conseil spécialisés assurés par des moyens divers (visites à domicile ou services en ligne). Ces services sont conçus comme une réponse efficace à la croissance rapide de la demande de services de conseil spécialisés et facilement accessibles. Un service de conseils en ligne[28] et un centre d'appel national sont disponibles. Pour assurer des prestations adaptées à chaque région en cas d'addiction à l'Internet, le centre fournit ses services en collaboration avec 48 centres connexes comme le centre d'appui à la santé de la famille, les centres d'aide à la jeunesse, etc.

Le service de conseils à domicile mérite une attention particulière. Il propose des conseils gratuits aux familles à leur domicile. Toute famille souffrant d'addiction à l'Internet peut faire appel à ce service. Le programme est particulièrement efficace pour les personnes souffrant d'addiction à l'Internet qui ont besoin d'aide dans la mesure où elles appartiennent à une famille monoparentale ou à faible revenu ou d'origine mixte, ou qui vivent avec leurs grands-parents. Par ailleurs, tout individu qui a besoin d'aide en cas d'addiction à l'Internet – enfants, adolescents, chômeurs ou familles à deux revenus – peut bénéficier de ce programme. Il existe aussi un programme de formation de conseillers spécialisés en addiction à l'Internet. Cette formation est disponible pour les conseillers et enseignants afin de leur permettre d'agir en qualité de conseillers spécialisés dans l'addiction à l'Internet. En juin 2014, le programme avait permis de former plus de 13 000 conseillers spécialisés.

Tableau 2: Nombre de services de conseils par type

Catégorie	2010	2011	2012	2013	Juin 2014
Présentiel (Visite à domicile)	15 037	10 522 (6 089)	20 701 (10 595)	24 623 (19 519)	7 484 (4 919)
En ligne	1 916	569	866	489	148
Téléphone	9 569	7 915	16 138	11 512	4 779
Sous-total	**26 522**	**19 006**	**37 705**	**36 624**	**12 411**

(Unité: un service)

Recherche sur les enquêtes et élaboration/distribution de contenus

Des études sur les politiques sont régulièrement menées pour accroitre l'efficacité opérationnelle et la précision scientifique des diverses modalités du programme pour les addictions à l'Internet et aux services TIC. Divers contenus didactiques comme des guides préventifs, animations flash, vidéos, manuels classiques ou programmes de conseil sont disponibles sur le site web. Ces contenus ont été élaborés pour assurer une exécution efficace de l'éducation préventive et pour mieux sensibiliser le public au risque potentiel associé à l'utilisation de l'Internet ou des services TIC.

En 2013, des manuels d'enseignement classiques ont été élaborés et distribués pour une prévention intensive de l'addiction. Les cours sont disponibles en quatre éditions adaptées aux différentes tranches d'âges (par exemple écoliers des niveaux primaire, élémentaire, secondaire et adultes). Il existe aussi des lignes directrices pour l'utilisation intelligente des services TIC publiées en quatre éditions pour quatre groupes de lecteurs (parents d'enfants d'âge préscolaire, écoliers du primaire et écoliers des niveaux élémentaire et secondaire). Ces directives ont été distribuées à plus de 20 000

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

écoles dans tout le pays. En 2014, un contenu éducatif pour l'auto-apprentissage de la prévention de l'addiction a été élaboré. Il est disponible en cinq versions (enfants d'âge préscolaire, élèves des niveaux primaire, élémentaire et secondaire, étudiants universitaires et adultes) et vise à aider les écoles et les établissements publics à assurer une meilleure prévention de l'addiction à l'Internet, qui est devenue obligatoire aux termes de la Loi fondamentale nationale de la Corée sur l'information (révisée, mai 2013), article 30, alinéa 8 (concernant l'éducation relative à l'addiction à l'Internet).

La publicité est utilisée pour prévenir l'addiction aux services TIC, en collaboration avec le secteur privé. Elle permet d'aider les adolescents et les parents à s'abstenir d'utiliser les services TIC de façon excessive et à s'habituer à utiliser ces services de manière appropriée à la maison et à l'école.

Caractéristiques particulières de la politique coréenne

En Corée, le gouvernement prend l'initiative de la plupart des activités. Ainsi, il soutient financièrement et techniquement les organisations civiques dans leurs efforts de prévention de l'addiction à l'Internet. L'engagement ferme du gouvernement est aussi illustré par le fait que les mineurs de 16 ans n'ont pas le droit d'accéder à des jeux en ligne de minuit à 6 heures. Les parents peuvent contrôler et bloquer l'accès de leurs enfants (de moins de 18 ans) aux jeux en ligne, sur demande aux fournisseurs de service. Tous les enfants, du jardin d'enfants à l'université, et tous les employés du secteur public doivent, selon la loi, suivre une formation sur la prévention de l'addiction à l'Internet. De plus, le gouvernement exploite les 14 centres de prévention de l'addiction du pays. Dans ses efforts de prévention de l'addiction à l'Internet, le Gouvernement coréen doit faire face à la difficulté d'assurer la participation de toutes les parties prenantes, notamment les parents, les communautés et le secteur privé.

Résumé

L'addiction est une question sanitaire fondamentale. C'est pourquoi des responsables de la Question 3/2 de l'UIT-D ont engagé des discussions avec l'Organisation Mondiale de la Santé afin de porter cette question à son attention. A cet égard, une note de liaison sur la question de l'addiction à l'Internet a été envoyée à l'OMS ainsi qu'à l'UNICEF, l'UNESCO et le Groupe de Travail du Conseil sur la protection en ligne des enfants (GTC-COP) pendant la période d'études 2014-2017, afin de mieux comprendre les activités entreprises à ce jour sur ce sujet. Ces discussions n'ont pas été concluantes et elles pourraient se poursuivre.

6.2 Sécurité des transactions électroniques

Le développement du commerce et des transactions électroniques avec, notamment, les achats et paiements en ligne, les passations d'ordres de bourse, les télédéclarations administratives (TVA, impôt sur le revenu, feuille de soins électronique…), les échanges de courriers et de documents électroniques; la mise en œuvre de nouveaux protocoles de sécurité des réseaux basés sur les infrastructures à clés publiques et leur déploiement progressif à grande échelle, notamment, DNSSEC, RPKI (Ressources Public Key Infrastructure); et la sécurité dans l'Internet des objets, sont des éléments essentiels qui doivent amener les pays en développement à œuvrer pour la mise en place d'institutions au niveau national ou régional chargées de la gestion de leurs infrastructures à clés publiques. La création de ces institutions, si elles sont bien encadrées, peut contribuer à renforcer la sécurisation des communications électroniques, en général, et celle des transactions électroniques, en particulier. Ces institutions peuvent aussi permettre l'émergence et le développement des économies numériques dans les pays en développement.[29]

Le commerce et les transactions électroniques connaissent un développement rapide dans les pays en développement. Ces transactions utilisent généralement des canaux non sécurisés. Toutefois, lorsqu'elles sont sécurisées, elles sont basées sur des certificats auto-signés ou sur des certificats achetés

[29] Document SG2RGQ/153, « La sécurité des transactions électroniques », République togolaise.

auprès des autorités de certification des pays développés. Cependant, dans certains cas, ces certificats ne sont pas forcément conformes à la législation en la matière dans les pays en développement.

Le manque d'engouement et les retards constatés dans le déploiement des protocoles sécurisés, notamment le DNSSEC et les RPKI, dans les pays en développement sont dus à la méconnaissance, soit de ces protocoles ou des standards qui permettent leur mise en œuvre, soit aux ressources humaines insuffisamment formées sur leurs déploiements, soit à la non-maitrise des chaînes de valeur afférentes.

Les responsables de l'étude de la Question 3/2 de l'UIT-D ont demandé à nombre d'organisations de formuler des observations sur ces préoccupations. Le Groupe a reçu de l'ISOC un excellent aperçu des questions en jeu, qui est reproduit ci-dessous.

Les systèmes d'infrastructure de clé publique (PKI) jouent un rôle important pour renforcer la confiance dans l'Internet comme plate-forme sûre pour le développement économique et social. Ces systèmes, les technologies d'appui et les pratiques de mise en œuvre ont évolué au fil du temps, devenant plus solides et plus sûrs. Il est essentiel que les pays qui entendent améliorer leur infrastructure de l'Internet se fondent sur cette expérience pour déployer des techniques de pointe et adopter les meilleures pratiques actuelles.

Les collaborateurs de l'Internet Society ont une grande expérience de la création et du déploiement de PKI. Nous avons une initiative Trust and Identity qui appuie l'utilisation de systèmes de communication sécurisés et authentifiés sur l'Internet. L'Internet Society mène aussi le programme Deploy360, qui soutient le déploiement généralisé de technologies de sécurité des infrastructures, notamment Transport Layer Security (TLS), DNS Security Extensions (DNSSEC), et Resource PKI (RPKI).

L'Internet Society tient à jour des ressources d'information liées à ces questions et peut fournir des références et du matériel supplémentaires qui expliquent comment établir des autorités d'émission de certificats racine, donnent des arguments en faveur de l'utilisation des TLS, DNSSEC et RPKI, et précisent comment déployer ces technologies. Elle offre aussi une assistance pour le renforcement des capacités. A cet égard, nos sites web Internet Technology Matters et Deploy360 constituent des points de départ.

Le document examine trois systèmes PKI différents (WebPKI, RPKI et DNSSEC) qui influent sur la confiance et la sécurité en général de l'Internet. Il met en avant l'importance du fait que ces systèmes PKI sont différents et remplissent des objectifs distincts. Ils ont des hiérarchies séparées et fonctionnent dans des domaines administratifs distincts. Le document signale aussi une technologie émergente, DNS-based Authentication of Named Entities (DANE), qui offre la perspective de renforcer la confiance dans l'Internet.

Il est peu probable qu'une autorité de certification nationale puisse être considérée comme une solution aux problèmes de sécurité qu'un pays peut rencontrer. Les individus qui s'efforcent de résoudre les problèmes liés à la sécurité devraient se tourner vers les technologies nouvelles et les bonnes pratiques actuelles qui peuvent être adoptées selon une méthode fondée sur la collaboration mondiale.

WebPKI

Le premier système PKI examiné dans le document est le WebPKI. Des certificats X.509 qui jouissent de la confiance du public sont délivrés par des autorités de certification (CA) certifiées par des fournisseurs de technologie comme Apple, Microsoft et Mozilla qui distribuent les certificats racine dans leurs systèmes d'exploitation et leurs navigateurs. Ils sont généralement utilisés par le WebPKI pour sécuriser la navigation sur le web, le transfert de courrier électronique et la messagerie instantanée. Ces certificats peuvent aussi être utilisés pour authentifier les utilisateurs accédant aux systèmes et pour signer numériquement les documents électroniques et les logiciels. De plus en plus, la législation nationale accepte la signature numérique au lieu des moyens traditionnels d'authentification.

Obtenir un certificat racine dans le système de distribution de racines globales pour le WebPKI est une procédure complexe, coûteuse et longue. Elle se compose de trois éléments fondamentaux:

1) établir les exigences que doit remplir une CA pour délivrer et gérer des certificats;

2) procéder à un audit de la CA pour s'assurer que la procédure et les exigences sont dûment respectées; et

3) ajouter une CA à l'ensemble des CA de confiance dans un produit. Le forum CA/Browser (voir « Exigences de base ») établit des lignes directrices pour la délivrance et la gestion de certificats.

Ces exigences sont ensuite testées selon un ensemble de procédures d'audit géré par le programme WebTrust d'AICPA/CICA pour les autorités de certification. Les fournisseurs de technologies utilisent les résultats de ces audits pour prendre des décisions quant à la possibilité d'ajouter des CA par défaut à leurs produits. Les utilisateurs et les entreprises peuvent parfois ajouter des CA supplémentaires à leurs dispositifs, mais il existe des aspects opérationnels majeurs à prendre en considération si l'on a recours à cette procédure.

Toutefois, il convient de relever que l'ajout d'un nouveau certificat racine aux distributions de racines globales ne rend pas plus sûr le WebPKI dans son ensemble. Au contraire, cela augmente les risques car la vulnérabilité au sein de n'importe laquelle des autorités de certification constitue une vulnérabilité pour l'ensemble du système. Pour ces raisons, il est souhaitable de maintenir le nombre de certificats racine aussi bas que possible. Si des gouvernements ont besoin d'établir leur propre autorité de certification, une méthode commune consiste à créer en tant que sous-autorité de certification d'une CA racine existante.

Il existe nombre de préoccupations au sujet de la fragilité du système WebPKI. Le Comité d'Architecture Internet (IAB) s'efforce actuellement, dans le cadre de son programme sur la sécurité et la confidentialité, https://datatracker.ietf.org/doc/draft-iab-web-pki-problems/, de formuler certains de ces problèmes et de faire des recommandations sur les mesures qui peuvent contribuer à améliorer l'infrastructure. Les personnes qui souhaitent trouver des moyens d'améliorer leur dispositif de sécurité avec les systèmes PKI pourraient juger utile de suivre ces travaux.

RPKI

Le deuxième système PKI mentionné ici est le RPKI. Le RPKI est un PKI spécialisé qui vise à améliorer la sécurité du système de routage de l'Internet, en particulier le protocole de passerelle frontière (BGP). Il fonctionne en délivrant des certificats de ressources fondés sur X.509 aux détenteurs d'une adresse IP et de numéros AS pour prouver l'assignation autorisée de ces ressources. Ces certificats sont délivrés à des registres Internet locaux (LIR) par un des cinq registres Internet régionaux (RIR) – AfriNIC, APNIC, ARIN, LACNIC et RIPE NCC – qui sont chargés de l'attribution et de l'assignation de ces ressources dans leurs régions.

Chaque RIR agit comme une CA racine et ancre de confiance pour les ressources assignées au sein de sa région, bien que ses certificats racine ne soient inclus dans aucune distribution racine publique. Il est donc nécessaire de les télécharger et de les installer à partir des sites web des RIR.

Il importe de relever que les ressources de numérotage ne sont pas attribuées ou assignées sur une base nationale, à l'exception de sept registres Internet régionaux (NIR) existants dans la région APNIC. Toutefois, les gouvernements nationaux peuvent jouer un rôle en encourageant les fournisseurs d'accès Internet et autres LIR à utiliser les systèmes RPKI.

DNSSEC

Le dernier système PKI examiné est le DNSSEC. Le but du système de nom de domaine (DNS) est de traduire les noms d'hôte lisibles par l'homme comme http://www.isoc.org en adresses IP lisibles par un ordinateur comme 212.110.167.157. Le DNS est devenu la principale méthode utilisée pour localiser les services Internet. Toutefois, comme de nombreuses organisations différentes administrent

le DNS et comme sa nature répartie signifie que les changements ne se diffusent pas instantanément dans l'Internet, il est difficile de garantir que l'information est renvoyée d'une source fiable. En d'autres termes, il n'existe pas de garantie qu'un serveur de nom ne fournit pas des informations fausses pour diriger les utilisateurs vers des hôtes qui contrôlent leurs transactions ou se font passer pour d'autres sites.

Le DNSSEC a été conçu par l'IETF pour authentifier l'information sur le DNS par la signature numérique des enregistrements DNS. Ceci garantit que seul le détenteur du domaine peut procéder à des changements et que les enregistrements peuvent être validés par une chaîne de confiance jusqu'à la zone racine. Ainsi, un client qui fait une demande peut vérifier que la réponse reçue vient effectivement d'une entité autorisée à la fournir.

Le DNS avec support DNSSEC peut être considéré comme un type spécialisé de PKI. Malheureusement, le déploiement du DNSSEC est encore limité, bien que les domaines de premier niveau (TLD) soient de plus en plus souvent signés. Les administrateurs de domaine nationaux peuvent jouer un rôle essentiel de sécurisation de cette infrastructure Internet importante en signant leurs ccTLD et en facilitant le déploiement du DNSSEC dans leur hiérarchie DNS nationale. De plus, le déploiement du DNSSEC permettra à la technologie DANE (décrite ci-dessous) d'être utilisée pour améliorer le WebPKI.

DANE

Une faiblesse inhérente du WebPKI est que les CA tierces sont en mesure de délivrer des certificats pour tout domaine ou organisation, que l'entité demandeuse possède ou non ce domaine, ou qu'elle le contrôle ou non. Le risque qu'une CA délivre un certificat incorrect augmente à mesure que le nombre de CA croît. La confiance dans le système PKI n'est aussi forte que l'est le maillon le plus faible. Ceci est la raison principale pour laquelle les distributions de racines publiques renforcent progressivement les exigences pour l'inclusion des CA, comme décrit dans la section WebPKI ci-dessus.

Malgré le renforcement considérable des procédures de délivrance de certificats suite à plusieurs incidents retentissants de délivrance de certificats incorrects par des CA, le système est toujours tributaire de la confiance des tiers. Cette dépendance a conduit à l'élaboration récente du protocole d'authentification des entités nommées fondé sur le DNS (DANE). En utilisant DANE, un administrateur de domaine peut certifier ses clés publiques en les stockant dans le DNS. Cette méthode ne requiert pas l'utilisation du DNSSEC et la plupart des navigateurs exigent actuellement l'installation d'un module d'extension. De plus, DANE nécessitera probablement une validation plus stricte des détenteurs de domaine. Cette tâche pourrait à terme incomber aux registres de TLD plutôt qu'aux CA.

Autorités de certification nationales

Tous les systèmes PKI décrits ci-dessus sont conçus pour assurer une confiance dans le monde entier en authentifiant les ressources de l'Internet comme les adresses, les noms et l'infrastructure des serveurs. Ces systèmes sont indépendants du contenu qui est transféré sur l'Internet par les entités authentifiées. La confiance est établie par des procédures d'exploitation qui font l'objet d'un consensus mondial. En fin de compte, ces procédures sont contrôlées par les entités finales qui choisissent de faire confiance aux CA configurées dans leurs systèmes. Par exemple, l'utilisation d'une CA pour réglementer les contenus conduirait à un abus de cette confiance et à la révocation probable de la CA comme autorité de confiance. Il est peu probable qu'une CA nationale puisse être considérée comme une solution aux problèmes de sécurité éventuellement rencontrés par un pays.

D'autres avis exprimés soutiennent fermement cette position. Dans sa réponse, l'ICANN souligne expressément que l'ajout de CA racine supplémentaires élargit considérablement la surface vulnérable du système. Le système n'est aussi sécurisé que la CA la moins sûre ou la moins fiable de l'ensemble, et toute CA ayant un certificat racine intégré dans le logiciel d'une partie utilisatrice représente un problème potentiel. En conséquence, l'infection ou le comportement incorrect de toute CA menace la sécurité de tout le système et la confiance qui lui est accordée. L'ICANN estime qu'il envisage un avenir dans lequel l'utilisation de la sécurité fondée sur le domaine (DNSSEC) et de l'authentification

des entités nommées fondée sur le DNS (DANE) ainsi que des progrès dans les méthodes de transparence des certificats contribueront à limiter ces risques. Elle suggère aux parties intéressées de collaborer avec l'IETF et le CA Browser Forum.

Dans sa réponse, RIPE NCC, le registre Internet régional qui couvre une grande partie de l'Europe et au-delà, a abordé le RPKI. RIPE propose différentes formes de formation en ligne et a indiqué que les pays en développement (et en particulier leurs administrations publiques) pourraient bénéficier pleinement des avantages du système RPKI administré par les RIR en donnant un exemple et en encourageant les opérateurs privés dans leurs pays à obtenir des certificats par les ressources de numéros Internet dont ils disposent. Une adoption plus large par les opérateurs de réseau dans le monde permettra à davantage d'opérateurs de fonder leurs décisions d'acheminement sur la validité des certificats RPKI, ce qui conduira à un système d'acheminement Internet plus sûr pour tous.[30]

6.3 Partenariats pour la cybersécurité

Comme relevé dans la section 3 du présent rapport, un sujet commun mis en avant dans plusieurs contributions est l'importance des partenariats pour la sécurité. Les défis ne peuvent être relevés individuellement par un gouvernement, des entreprises privées ou une organisation internationale. Une méthode fondée sur la collaboration est nécessaire. Dans leur contribution commune sur le Forum mondial sur la cyberexpertise (GFCE)[31] les Etats-Unis d'Amérique et les Pays-Bas ont abordé cette question. Cette contribution présente un historique et une description du GFCE. Le GFCE est une initiative multi-parties prenantes volontaire, de première importance qui a pour objectif d'encourager la solidarité internationale et de soutenir sur les plans politique, technique et financier les mesures qui sont prises pour renforcer la coopération internationale entre toutes les parties prenantes dans le domaine de la cybersécurité. Le GFCE encourage le renforcement des cybercapacités, animé par un projet dans lequel les intérêts en matière de sécurité, d'économie et de droits humains sont étroitement liés. Le GFCE a été créé pour renforcer les cybercapacités et la cyberexpertise afin que les efforts de coopération au niveau international soient plus efficaces.

La contribution met aussi en avant des initiatives essentielles du GFCE et donne des renseignements précieux sur la composition du GFCE et la manière dont les Etats Membres et Membres de Secteur peuvent participer à cette initiative mondiale.

Autres domaines

Les auteurs de plusieurs contributions ont examiné d'autres aspects de la cybersécurité, notamment sous l'angle du secteur bancaire[32] et de la nécessité d'adopter des approches neutres du point de vue des technologies, des risques de violation des données personnelles et de la nécessité pour les villes intelligentes[33] de faire preuve de résilience. Ces domaines n'ont pas été étudiés de manière approfondie pendant la période d'études.

30 On trouvera des renseignements complémentaires sur chacune de ces options aux adresses URL suivantes: 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.

31 Document 2/332, « Forum mondial sur la cyberexpertise (GFCE) », Etats-Unis d'Amérique et Pays-Bas.

32 Document SG2RGQ/141, « Fintech and security in Korea », République de Corée.

33 Document 2/77, « Cyber-security's role and best practices to ensure Smart Cities' service continuity and resilience », Symantec Corporation (États Unis d'Amérique).

7 CHAPITRE 7 – Expériences nationales: cadre de critères communs en matière de sécurité

Conformément à notre mandat, nous devions commencer à examiner les expériences nationales présentant un cadre de critères communs en matière de sécurité. Au titre de cet examen, les responsables de l'étude de la Question 3/2 de l'UIT-D ont reçu une contribution[34] du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord qui décrit l'expérience acquise par ce pays sur la façon dont la définition de critères communs constitue un mécanisme international ouvert et digne de confiance, qui aide les responsables de la conception et de la mise en œuvre de systèmes informatiques à choisir des produits informatiques présentant des niveaux d'assurance de sécurité appropriés. Bien qu'il n'existe pas d'outil ou d'approche unique permettant de garantir que ces systèmes seront sécurisés, l'adoption de critères communs offre un mécanisme communément accepté et stable qui aide les acheteurs à choisir des produits pour lesquels l'assurance qualité est importante. L'accord de reconnaissance de critères communs (CCRA), qui existe depuis 2000, vise à améliorer la mise à disposition de produits de sécurité informatique et à éviter tout double emploi dans les évaluations. Les tests de sécurité sont effectués dans des laboratoires indépendants conformément aux normes convenues. Les laboratoires doivent obtenir des autorisations attestant qu'ils sont compétents et indépendants. Dernièrement (2014), le CCRA a été actualisé en vue de permettre une approche plus détaillée en matière de spécifications, associant des experts et des établissements universitaires, pour la définition de cette prescription essentielle pour chaque domaine technique, qui pourra alors être clairement évalué par toutes les parties prenantes.

Au titre de la Question 3/2 de l'UIT-D, deux contributions émanant de la **République islamique d'Iran** et traitant de méthodes nouvelles ont commencé à être examinées.

Pour évaluer la cybersécurité au niveau national, il est nécessaire de mesurer en permanence des indicateurs de cybersécurité. Afin de pouvoir prévoir et mettre en place un système national de gestion de la cybersécurité (NCMS) efficace, il est urgent d'élaborer un programme approprié de mesure de la cybersécurité au niveau national (NCMP). Le programme NCMP facilite la prise de décisions et améliore les performances et la responsabilisation au niveau national.[35]

Un cadre de bonnes pratiques relatives à l'identification et à l'utilisation d'un ensemble de mesures est nécessaire pour évaluer l'efficacité d'un système de gestion de la sécurité de l'information au niveau national. De manière analogue au cadre NCSec,[36] basé entièrement sur la norme ISO/CEI 27001[37] relative au système ISMS au niveau d'une organisation, un « cadre de mesure de la cybersécurité au niveau national », a été proposé.[38] Il reposait sur la norme ISO/CEI 27004[39] et la publication NIST-800-55-R1,[40] toutes deux ayant été élaborées aux fins de l'évaluation de la cybersécurité au niveau d'une organisation, En outre, tout comme dans le cas basé sur la norme ISO/CEI 27001, il est nécessaire de « définir la manière de mesurer l'efficacité des contrôles ou groupes de contrôles retenus et de préciser comment ces mesures doivent être utilisées pour évaluer l'efficacité des contrôles et produire des résultats comparables et reproductibles » au niveau national.

---

34 Document 2/364, « Common criteria as a tool for giving assurance about the security characteristics of IT products », Royaume-Uni de Grande-Bretagne et d'Irlande du Nord.

35 Document SG2RGQ/46, « Mesure de la cybersécurité au niveau national », République islamique d'Iran.

36 Commission d'Études 1 de l'UIT-D, Rapport final, Question 22-1/1, « Best Practice for Securing Information and Communication Networks: Best Practices for Developing a Culture of Cybersecurity », 2014, disponible à l'adresse: https://www.itu.int/pub/D-STG-SG01.22.1-2014.

37 ISO/IEC 27001, « Information Technology – Security Techniques – Information Security Management Systems – Requirements », 2013.

38 Document SG2RGQ/47, « National cybersecurity measures », République islamique d'Iran.

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

40 NIST Special Publication 800-55 Revision 1, « Performance Measurement Guide for Information Security", 2008.

Etant donné que ces contributions semblaient aller au-delà des expériences nationales les responsables de l'étude de la Question 3/2 ont transmis ces travaux au JTC1 de l'ISO (SC27), qui a fait savoir qu'il serait heureux que des activités supplémentaires soient entreprises dans ce domaine.

L'UIT-T fournit un rapport technique « Utilisation efficace des normes de sécurité »[41] qui est destiné à aider les utilisateurs, en particulier ceux des pays en développement, à mieux comprendre tout l'intérêt d'utiliser les Recommandations UIT-T sur la sécurité dans des contextes très divers (par exemple entreprises, commerce, administrations publiques, industrie).

L'UIT-T fournit également un supplément à la Recommandation UIT-T X 1504 sur les bonnes pratiques pour la mise en œuvre de la Recommandation UIT-T W 1504 | ISO/CEI 27014 sur la gouvernance de la sécurité de l'information – le cas du Burkina Faso.[42]

41 https://www.itu.int/pub/T-TUT-SEC-2016.
42 https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13072.

8 CHAPITRE 8 – Conclusions et recommandations pour la prochaine période d'études

Au cours de cette période d'études particulièrement chargée, nous avons abordé au titre de la Question 3/2 de nombreux aspects de la cybersécurité, en examinant plusieurs études de cas par pays et en organisant plusieurs ateliers qui ont fourni des orientations sur de nombreux aspects de la formulation de stratégies en matière de cybersécurité. Le groupe a examiné et fourni des contributions au BDT concernant l'Indice mondial de cybersécurité.

Au titre de la Question 3/2 de l'UIT-D, il est recommandé de poursuivre les activités menées pendant l'actuelle période d'études. Le groupe recommande que les menaces (techniques) nouvelles et émergentes autres que le spam et les logiciels malveillants soient examinées. Il conviendrait d'examiner plus avant la question de la fraude à la carte SIMbox, un problème soulevé par plusieurs pays en développement et de prévoir d'autres activités de renforcement des capacités, par exemple d'organiser davantage d'ateliers et de concevoir davantage de matériels didactiques, dans des contextes régionaux et locaux. Il convient de mettre l'accent sur la poursuite de la collaboration avec les organisations concernées, par exemple FIRST, le GFCE, et l'ISOC. La collaboration fondée sur la collecte de données d'expérience au niveau national doit se poursuivre. L'enquête sur la sensibilisation à la cybersécurité devrait également se poursuivre, étant entendu que des ressources appropriées pourront être identifiées avant la CMDT. Les responsables de l'étude de la Question devraient continuer de travailler en étroite collaboration avec le BDT, en vue de valider et de faire évoluer les mesures relatives à la cybersécurité, telles que le GCI. Il conviendrait de continuer à recenser dans le cadre de cette question des mesures pour améliorer les indicateurs, la collecte et l'analyse des données. Il convient également de poursuivre les travaux sur la protection en ligne des enfants.

Au cours des périodes d'études précédentes, on s'est employé à faire évoluer les méthodes de travail des commissions d'études de l'UIT-D. Les responsables de l'étude de la Question 3/2 félicitent la CMDT d'avoir encouragé cette évolution. La Conférence devrait en particulier envisager d''autoriser l'organisation des travaux sur la base de périodes annuelles, afin que les activités puissent être axées sur des questions précises.

Cela nous amène à notre dernier point: au titre de la première partie de cette Question, (Question 22/1 « Sécurisation des réseaux d'information et de communication: bonnes pratiques pour créer une culture de la cybersécurité ») des recommandations ont été élaborées en vue de formuler des stratégies nationales visant à améliorer la cybersécurité dans les infrastructures essentielles. Ces travaux devraient être réexaminés au fil du temps.

Abbreviations and acronyms

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

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

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

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

Annexes

Annex 1: The Global Cybersecurity Index 2017

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

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

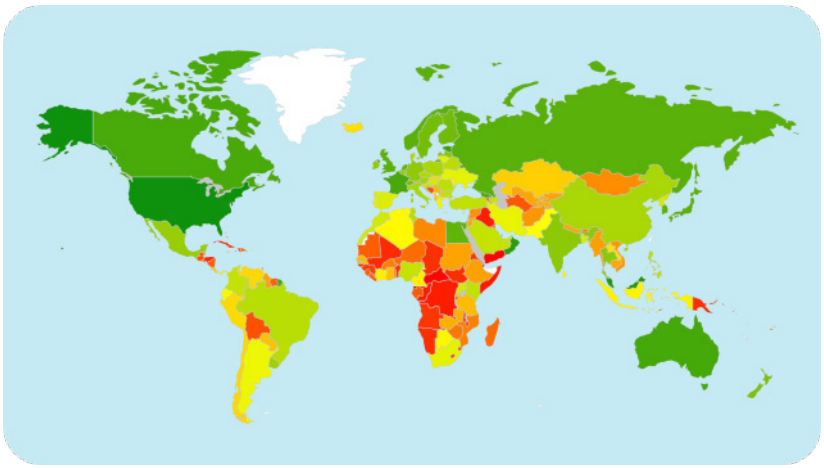
One-hundred and thirty-four Member States responded to the survey throughout 2016. Member States who did not respond were invited to validate responses determined from open-source research. As such, the GCI results cover all 193 ITU Member States.

Key findings and results

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

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

Figure 1A: GCI heat map



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

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

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

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

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

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

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

GCI reference model

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

The main objectives of the GCI are to measure:

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

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

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

Background

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

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

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

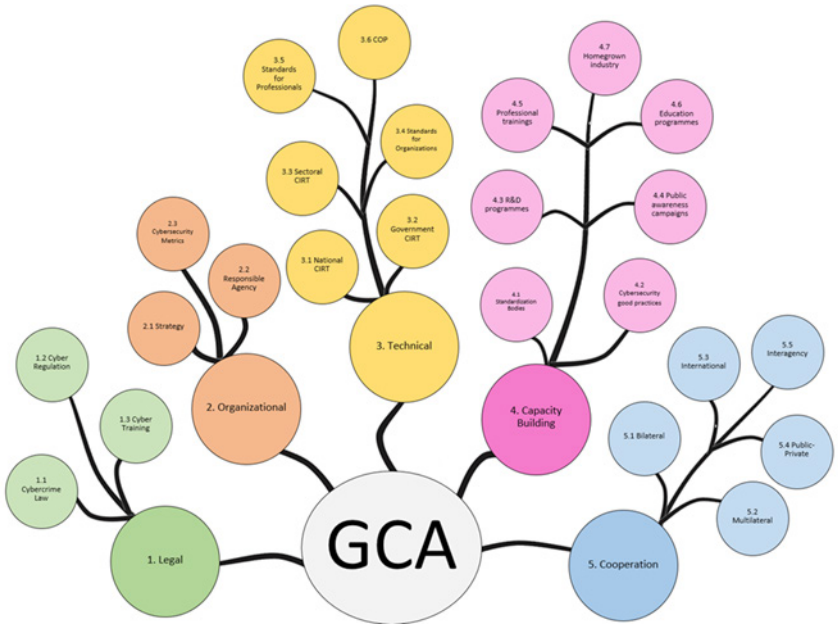
The GCA is the ITU framework for international multi-stakeholder cooperation in cybersecurity aimed at building synergies with current and future initiatives. It focuses on the following five pillars: legal, technical, organizational, capacity building and cooperation.

Figure 2A: GCA

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

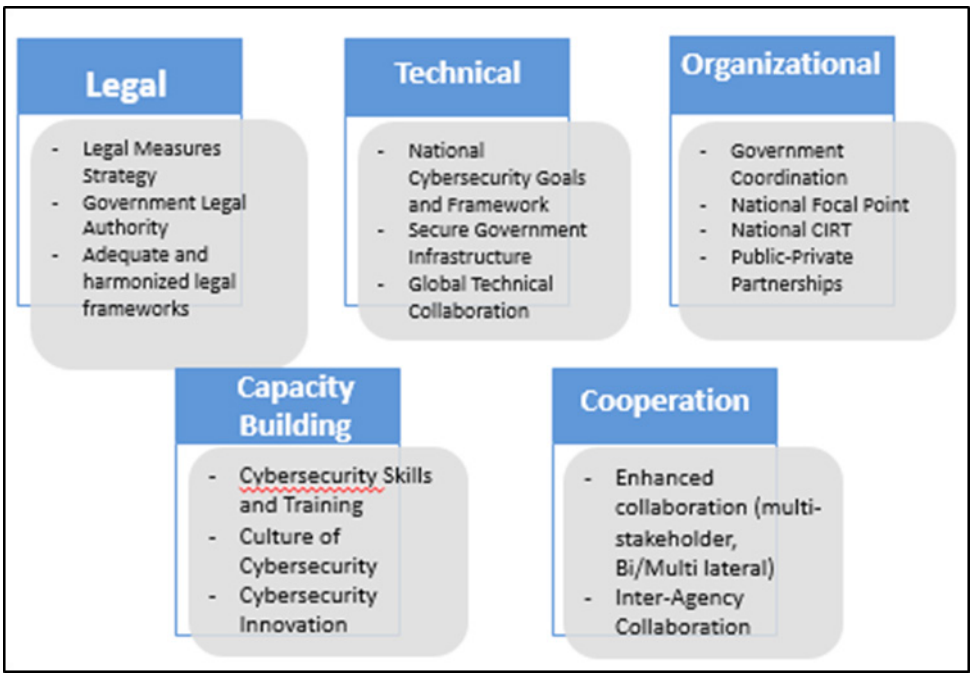
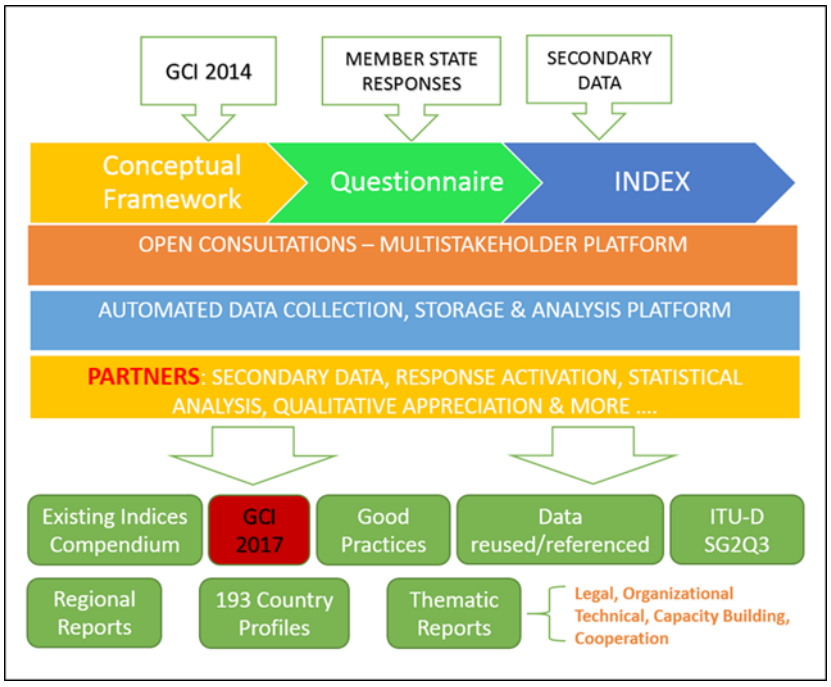


Figure 5A: GCI approach



1.1 Definition of indicators

– Legal measures

Legislation is a critical measure for providing a harmonized framework for entities to align themselves to a common regulatory basis, whether on the matter of prohibition of specified criminal conduct or on minimum regulatory requirements. Legal measures also allow a nation state to set down the basic response mechanisms to breaches: through investigation and prosecution of crimes and the

imposition of sanctions for non-compliance or breach of law. A legislative framework sets the minimum standards of behaviour across the board, applicable to all, and on which further cybersecurity capabilities can be built. Ultimately, the goal is to enable all nation states to have adequate legislation in place in order to harmonize practices supranationally and offer a setting for interoperable measures, facilitating international combat against cybercrime.

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

– Cybercriminal legislation

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

– Cybersecurity regulation

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

– Cybersecurity training

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

1.2 Technical measures

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

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

1.2.1 National CERT/CIRT/CSIRT

The establishment of a CIRT/CERT/CSIRT[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

[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.

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 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.

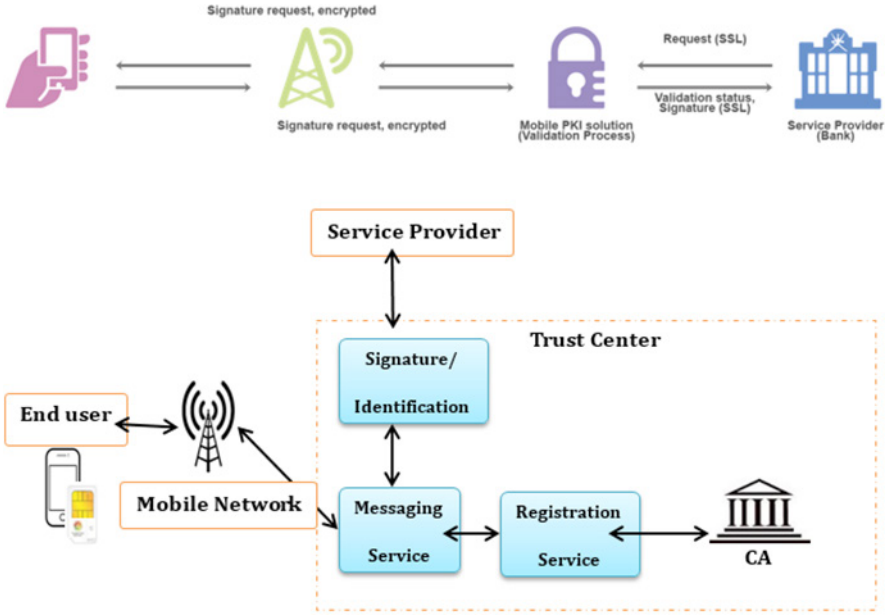
Table 4A: Different types of services options to be provided to Government and commercial entities

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



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

A general framework for NCMP

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

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

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

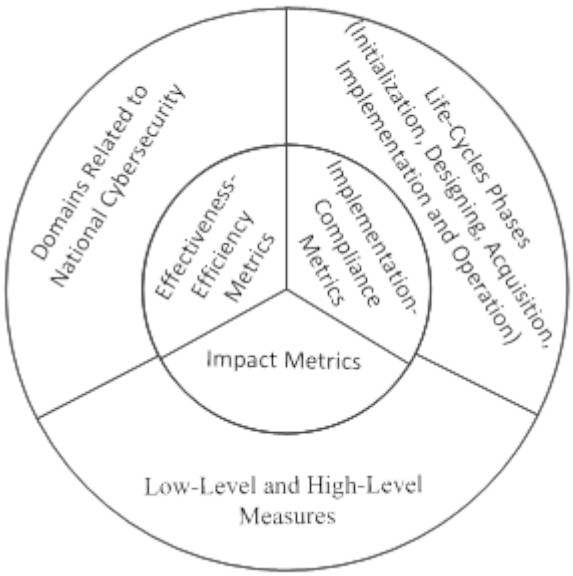
- A quantitative picture of national security posture;
- Monitoring the effectiveness of NCMS and the extent of compliance with applicable laws, rules and regulations;
- Determining the deviation from the expected results (predetermined security requirements and objectives);
- Increasing the accountability by identifying either incorrectly or ineffectively implemented security controls or those that have not been implemented, and their corresponding stakeholders;

– Providing important quantifiable input to facilitate proper decision making for enhancing national cybersecurity and allocating the required resources;

– Providing management reports on the impact of past and current activities;

– Assessing security products or services from third parties and providing means to compare different products, services, policies and procedures.

Figure 8A: General scope for national cybersecurity measures



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

Conclusions and directions for future works

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

References

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

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

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

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

Country: Korea (Republic of)

Document: 2/234

Title: Korea's K-ICT security development strategy

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

Background

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

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

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

Creating a future growth engine by reinforcing the infrastructure of the information security industry

The Ministry is planning to improve the structure of the information security industry by switching the existing price competition-based market to a performance-based one, and to introduce a proper system for paying fair prices for information security services. Also, the Ministry will prepare and provide "the Information Security Service Price Assessment Guideline" to introduce a system for assessing the fair price of information security continuity service, which ensures appropriate security performance of related products.

In addition, the Ministry is planning to provide information security investment incentives, such as giving preferences in participation in the government and public procurement and R&D, to induce

corporations to voluntarily invest in security and take active measures. The Ministry will also review and push ahead with the public announcement of corporate information security status that includes the status of related manpower, organization, education, etc. of a business to encourage autonomous security competition among corporations and help users choose better products and services. In particular, the Ministry is planning to reinforce the evaluation for the level of information security investments to enhance the security level of key private enterprises such as mobile communication services and Critical Information Infrastructures (CIIs).

The Ministry is also planning to identify and foster information security startups by providing support such as sharing security vulnerabilities, test beds and international certification support so that excellent security ideas can lead to successful startups. In addition, the Ministry is seeking to identify best security models of new industries like drones, next-generation CCTVs, and biometric products and turn them into new economic growth engines.

Developing source security technologies

The Ministry is planning to encourage national R&D centers and private enterprises to develop world-class information security products and technologies by 2019 by intensively studying innovative, intelligent and invisible technologies with the goal of leading the global cybersecurity market and securing technology competitiveness.

These research communities and related businesses are expected to lead innovative technologies that respond to new threats in the ICBM (IoT, cloud, big data, mobile) environment, key infrastructure control network security and intelligent cyberattacks such as Advanced Persistent Threats (APT). They will also develop smart security technologies to reduce cyber threat response time, such as cyber threat detection technologies and forensic technologies for attack source traceback. In addition, they will intensively develop convenient security (usable security) technologies including the fraud detection system (FDS) for users.

Another plan of the Ministry is to build a global cyber open R&D system by allowing more outstanding overseas researchers to participate in domestic R&D activities, and making them to conduct joint studies with leading institutes and universities in cyber security related areas.

Fostering top-notch security manpower and creating a culture conducive to information security

The Ministry will continuously increase the number of information security schools so that potential security manpower can enter colleges without worries about the college scholastic ability test, and recruit military and police cyber security specialists to prevent career interruption caused by mandatory military service.

The Ministry is also planning to foster security coordinators to reinforce the security competence of field workers in different industries, such as the financial and manufacturing industries, and bring up top-notch manpower in different areas such as finance and national defense.

The Ministry is going to turn and expand the Korea Internet & Security Agency (KISA) Academy into an institution dedicated to fostering top-notch security manpower (cyber security manpower center), and build a cybersecurity training center (Security-GYM) to strengthen cyber response capabilities. In addition, the Ministry will carry out the nationwide information security culture movement (Security All Wave) to turn the awareness of the importance of information security into action by transforming information security into a social culture. The Ministry is also planning to induce voluntary compliance with security rules by developing and disseminating customized security rules for different information security agents, which include individuals, enterprises and Chief Executive Officers, etc.

Increasing investments to enhance the resilience of cyber security

With close cooperation with the Korea Internet & Security Agency, the Ministry will diagnose the current status of cyber safety to reinforce the security of key infrastructures of the private sector

(ISP, infrastructure, etc.) and services used by many people such as online storages, routers, portals, etc., and build an in-depth cyber detection system to quickly detect cyberattacks and expand the response range.

The Ministry is also planning to build 100,000 cyber traps to lure hackers as a way to reinforce responses to electronic financial frauds, such as pharming and smishing, and ensure the security of devices including smartphones, routers and CCTVs, and to improve the cyber threat response systems by implementing Chief Information Security Officer (CISO) hotlines between the government and key enterprises (mobile carriers, portals, IDC, etc.).

The Ministry will reinforce security throughout the supply chain of Critical Information Infrastructures, including external management manpower, consignment and outsourcing, purchasing and procurement, and will also actively support the implementation of Information Sharing and Analysis Centers (ISACs).

To provide customized information security services for SMEs, the Ministry is planning to reinforce technical and site support for quick emergency response and system recovery in case of infringement accidents, and establish more information security support centers.

Way forward

The Korean government is expected to increase the size of the domestic information security market by improving the structure of the information security industry, to expand investments in information security and to create new demands for convergence security and physical security.

To become one of the most powerful countries in cyber security in the world, the fundamentals of the information security industry should be very strong and resilient, and the Korea government expects that this strategy will serve as a turning point in innovating the information security industry, technology and expertise of Korea. Moreover, a large number of new jobs are expected to be created by promoting the convergence security and physical security industry and internalizing information security across all industries including communication, finance, manufacturing, and energy.

Country: Odessa National Academy of Telecommunications n.a. A.S. Popov (Ukraine)

Document: 2/156

Title: Multimedia distance-learning course on the safe use of Internet resources

Summary: ITU's Telecommunication Development Bureau as part of the CIS regional initiative on "creating a child on line protection centre for the CIS region", adopted at WTDC-14 (Dubai, UAE), with the support of the Odessa National Academy of Telecommunications n.a. A.S. Popov (Ukraine).

The course is divided into three parts: basic (for pre-school and junior school children); intermediate (for children in classes 5 to 9); and advanced (for senior pupils, students, parents and teachers). Each course is based on thematic modules with tests after each module.

Introduction

The CIS region had already begun to consider the issue of protecting children on line at the end of the 1990s. Approaches to the problem differed among the countries of the region, however, reflecting the range of views in different countries on issues of public morals, pornography, privacy and data protection.

All countries in the region without exception have acceded to the Convention on the Rights of the Child, without any declarations or reservations regarding Articles 16, 17 and 34(c). All countries in

the region have also acceded to, signed and/or ratified the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, without any declarations or reservations regarding Articles 2 and 3 of that instrument.

In many countries in the region, software producers, telecommunication operators and educational establishments are actively developing child on line protection programmes of their own. Notable examples might be two Ukrainian projects: "Safety of Children on line", which is being implemented by the Coalition for the Safety of Children on line; and "System for restricting access to inappropriate Internet resources", a project being developed by the Odessa National Academy of Telecommunications n.a. A.S. Popov (Ukraine). In May 2012 the project "Building safer internet for educational institutions", which formed the framework for the presentation of the system for restricting access to inappropriate Internet content, was recognized as the best project in the category "C5. Building confidence and security in the use of ICTs" in a competition organized as part of the WSIS Forum 2012 event (Geneva, 14-18 May 2012), and acknowledged by the Secretary-General of ITU as one of the major achievements in creating connectivity worldwide.

With their common political, economic, environmental, humanitarian and cultural history, the countries of the Commonwealth of Independent States (CIS) share a number of characteristics with regard to Internet use, and this has an impact on users' interests and resources. The key factors here include: a close linguistic environment (most of the peoples in the CIS countries are fluent in Russian); a more or less identical level of ICT development and broadband penetration; common problems in the applications of ICTs (a sharp contrast in terms of teacher training in the towns and rural areas, a common "post-soviet" model of education, an absence of trained system administrators in rural schools, and so on); and a roughly similar level of Internet regulation.

The international seminar on integrated aspects of child protection on the Internet, held in Odessa, Ukraine, in April 2011, and the Interregional seminar for Europe, the Asia and Pacific region and the Commonwealth of Independent States on "Current methods for combating cybercrime" (March 2012), identified the main obstacles to strengthening confidence and child on line protection in developing countries. Participants noted in particular the importance of international cooperation as a means of exchanging experience and improving child on line protection.

A natural progression from this idea was the adoption at the World Telecommunication Development Conference 2014 (Dubai, UAE) of the CIS initiative on "creating a child on line protection centre for the CIS region". One of the expected outcomes of that initiative is the creation of distance-learning courses on safe use of Internet resources involving testing of children, parents, teachers, and so on.

It should be noted that existing training materials (including multimedia clips and courses) do not cover the entire range of issues pertaining to Internet safety and as a rule do not include systems for testing and certification. In the light of this, the Odessa National Academy of Telecommunications n.a. A.S. Popov (Ukraine) proposed to develop a course on the safe use of Internet resources along the lines of the UN course on "Security in the Field", which could then be followed by children, parents and educational staff.

It was proposed that the course should be divided into three parts: basic (for children of pre-school and junior school age); intermediate (for children in classes 5 to 9); and advanced (for senior school pupils, students, parents and teachers), each part being based on thematic modules with testing on completion of each module.

The Academy proposed the structure and basic features of the courses, which were presented at the fourth meeting of ITU-D Study Group 1 (document 1/265, study period 2010-2014) and at the seventh meeting of the Council Working Group on Child on line Protection (document WG-CP/7/5).

By September 2015, a Russian-language demonstration version of the course is to be available on line at http://www.onlinesafety.info . Final development and testing are planned for November 2015.

The course interface is adapted for use on line using a variety of operating systems and web browsers (including mobile devices based on iOS and Android operating systems).

Basic course

The basic course is structured in three modules: "general information on security in the Internet"; "rules for communication on line"; and "useful and harmful on line games". To begin with, children choose a hero (boy or girl) to help them follow the course. All slides and navigation moves effected with the cursor are also voiced by the chosen hero.

During the course the child studies such topics as "what is the Internet and how is it organized?"; "what useful things can I get from the Internet?"; "the main dangers on line"; "virus programmes that harm a computer"; "virus programmes for spying on users or gathering personal data held on the computer"; "Illegal, unethical and harmful content"; "misleading content"; "Cyber-bullying and cyber-grooming"; "benefits and harm from social networks"; "what can I tell other people on line and what must I not tell them?" "rules of 'netiquette'"; "how do I create my on line profile"; "how and what to play on line"; "possible harmful effects of computer games (including the influence of Internet slang on colloquial speech)", and so on.

The course includes 52 slides of between 10 and 20 seconds' duration, depending on the density of their multimedia content. Each slide is based on a white background. Colour series are formed in accordance with the Itten principles, and each module has its own colour frame (dark blue, yellow or green). The rate of progress though the course is shown by an animated figure moving in a straight line at the bottom of the screen to indicate the progress made.

The basic part of the course contains five multimedia clips, four interactive games and 50 cartoon-style graphics. For example, in one slide the child is asked to play a game "Get the virus!". A target in the form of a "virus" moves around the screen. The aim is to strike at it with a special on line "hand", but the game is designed to ensure that the child cannot succeed in hitting the virus target. After several attempts a voice explains that a computer virus cannot be eliminated in that way and instead, an antivirus programme has to be used.

Throughout the course, the child periodically has to answer test questions involving animated figures. This helps to consolidate the knowledge acquired. A separate test is not envisaged in the basic course and a certificate is issued automatically on completion.

Intermediate course

The intermediate course comprises five modules: "general information on security in the Internet"; "safe entertainment on line"; "rules for communicating with others on line"; "what can you believe on the Internet?"; and "how to protect oneself on line".

In the first slide, the child learns about the purpose of the course and its format. During the course the child studies topics such as "what is the Internet and how is it organized"; "the main dangers on line"; "Illegal, unethical and harmful content"; "misleading content"; "cyberbullying and cyber grooming"; "Internet fraud"; "basic rules for using the Internet"; "how not to be a victim of virtual reality"; "the influence of Internet slang on colloquial speech"; "antivirus software"; "basic precepts of "netiquette"; "what can I write about (and save) on line?"; "anonymity on line"; "how to verify information on line"; "copyright on line (music, video, images, presentations, dissertations, etc.)"; "working via public networks (WiFi zones, Internet clubs, etc.) or using someone else's computer"; "rules for working safely with e-mail"; and "who can help if there is a problem on line?".

The course includes 122 slides of between 10 and 20 seconds' duration each, depending on the density of their multimedia content. For each sequence there is voice-over accompaniment. Each sequence is based on a white background. Colour series are formed in accordance with the Itten principles and each module has its own colour frame. The rate of progress though the course is shown by "road blocks" indicated by white screens which change to green once a module has been completed

The intermediate part of the course contains five cartoon clips (different from the basic course), two interactive games, 77 cartoon-style figures and 12 infographic figures.

On completing the course the child takes a test comprising ten questions which contain possible answers. The test set is based on random selection from 40 questions (eight for each module).

Advanced course

The advanced course comprises seven modules: "general information on security in the Internet"; "rules for communicating with others on line"; "safe entertainment on line"; "what can you believe in the Internet?"; "confidentiality and working via public networks"; "risk assessment and behaviour in difficult situations"; and "methods of filtering content and child protection on line".

The advanced course interface is designed to be as similar as possible to that of the UN advanced "Security in the Field" course. Information is presented with the aid of a number of different types of slide and additional elements which make it possible to create small interactive scenarios using a range of multimedia content. Participants study such topics as "basic information on Internet architecture"; "existing threats (viruses, fraudsters, criminals and so on)"; "how to remain literate when communicating with others on line", "what can you write about and what should you not write about on line?"; "ensuring that children do not view undesirable content"; "copyright and how you can break the law without knowing it"; "how much time may I spend on line?"; "the influence of Internet slang on colloquial speech"; "typical forms of Internet fraud"; "data protection"; "monitoring children's behaviour on line"; "threats to life and health on line"; "basic content filtering techniques"; "advice on choosing content filtering systems (for homes, schools and institutions)", and other aspects. The course includes 57 slides of 30-40 seconds' duration each, depending on the density of their multimedia content. Each sequence is provided with a partial audio accompaniment.

The advanced part of the course comprises three cartoon clips (different from the basic and intermediate courses), five interactive games, 23 photo images, and 19 infographic-style figures. An example of an interactive game at the advanced level could be a dialogue between the user and an imaginary character of the opposite sex. Following the lead-in, a conversation develops and is led by the imaginary character. The user selects responses from a set of ready-made models from a list. The list includes various options containing Internet slang and/or stylistic and spelling errors, as well as replies that are stylistically and grammatically sound and do not include slang. The aim of this dialogue is to induce the interlocutor to engage in further discussion, create a positive impression, and so forth; this is not achieved if too much use is made of Internet slang, or if the chosen responses contain stylistic and spelling mistakes. When the dialogue is finished, feedback is given to the user on the use of Internet slang during the interactive discussion.

Conclusion

The Odessa National Academy of Telecommunications n.a. A.S. Popov (Ukraine) invites all interested parties to collaborate in testing and disseminating the course that has been developed and to translate it into the official languages of ITU.

Country: Togo (Republic of)

Document: 2/153

Title: Security of electronic transactions

Summary: The Public Key Infrastructures commonly used to secure electronic communication services contribute to establishing confidence in the use of ICTs. Economic models stemming from their value chain can bring growth in the digital economy of the States that implement them. The ever-increasing development of electronic commerce and transactions, the progressive and large-scale deployment

of new protocols and network services based on Public Key Infrastructures, and the security of the Internet of Things are, *inter alia*, reasons that should encourage the creation of root certification authorities in developing countries on the one hand, and the rethinking of a model of organization for the trust chain of the national-level root certification authority in a global way, on the other hand.

The objective of this contribution is to invite ITU-D Study Group 2 and ITU-T Study Group 17 to study the impact and potential benefits of establishing root certification authorities in developing countries in order to elaborate a programme to implement such root certification authorities, if appropriate. This study should enable estimation of developing countries' preparation for having a national root certification authority, and allow streamlining of the assistance that BDT is already providing, for instance on CIRT implementation.

Introduction

The development of electronic commerce and transactions, including online purchases and payments, execution of stock market orders, online administrative tax filing (VAT, income tax, electronic medical care sheet), exchanges of e-mails and electronic documents; the implementation of new network security protocols based on public key infrastructures and their progressive large-scale deployment, in particular, DNSSEC, RPKI (Resources Public Key Infrastructure); and the security of the Internet of Things are crucial elements which should incite developing countries to work towards the establishment of institutions at national or regional level in charge of the management of their public key infrastructures. The creation of these institutions, if properly supervised, can contribute to strengthening the security of electronic communications in general, and that of electronic transactions in particular. They can also allow the emergence and development of digital economies in developing countries.

Statements

Electronic commerce and transactions are developing rapidly in developing countries. These transactions typically use insecure channels. However, when they are secured, they are based on self-signed certificates or on certificates purchased using certification authorities generally based in developed countries. In some cases, however, these certificates are not necessarily in accordance with the legislation of developing countries.

The lack of enthusiasm and the delays noted in the deployment of secure protocols, such as DNSSEC and RPKI, in developing countries are due to misunderstanding either of these protocols or the standards that allow their implementation, or to the insufficiently trained human resources involved in their deployment, or to a non-mastered grasp related to chains value.

All these inadequacies can be improved with the implementation of a root certification authority in each country. Indeed, the authorities, besides their traditional roles, will also be tasked with the broadcast, validation, and revocation of certificates to promote a culture of secure electronic transactions, as well as the organization of trust chains to national and international levels.

To assure this situation, some developing countries have set up root certification authorities. However, the functioning of these certification authorities does not necessarily reflect the state of the art in the field. It is advisable to improve the functioning of certification authorities, in particular, by implementing clear procedures based on best practices as well as accepted standards on the subject. This will have the advantage of ensuring the security of transactions and consumers in those developing countries that have already set up their certification authority on the one hand, and on the other hand, will promote the implementation of these certification authorities in those countries that do not have such capability.

Thus, in the context of the emergence of new digital economies in developing countries, the establishment of root certification authorities can be an important link and a social and economic development lever.

Proposal

This contribution aims at asking Question 3/2 to undertake a study on the impact of the implementation of root certification authorities in developing countries. The study should possibly lead to a proposal for the establishment of such root certification authorities in Member States, along the lines of what is currently being done with the setting up of CIRTs.

The objectives of the study include:

- Assessing the readiness of developing countries for setting up root certification authorities at a national level;
- Identifying requirements in terms of the skillset necessary to set up and run certification authorities at a national level;
- Performing a gap analysis on the current national legal frameworks to better identify the actions required to improve national legislations on cryptography, digital certification and digital signature;
- Reflecting on business models and operational plans to support the viability of the activities of the national root certification authority while taking into account regional specificities;
- Assessing the possible evolution of national root certification authorities toward a chain of trust between them.

Furthermore it is requested that Question 3/2 coordinate with ITU-T Study Group 17 to investigate the opportunity to:

- Set up a human capacity-building programme for developing countries based on standards and the implementation of standards related to electronic certification, in particular the X.500 series standards;
- Develop kits of best practices on the implementation and use of standards related to electronic certification.

Conclusion

The security of electronic transactions is fundamental in building confidence in the use of ICTs. The establishment of institutions whose operation should achieve this goal is essential for developing countries. However, it should be referenced by politically, technically and organizationally based frameworks that enable the creation and smooth organization of these institutions.

Country: United States of America; Netherlands (Kingdom of the)

Document: 2/332

Title: The Global Forum on Cyber Expertise (GFCE)

Summary: This contribution provides a background and explanation of the Global Forum on Cyber Expertise (GFCE), a global initiative that was launched by the Netherlands in April 2015 at the Global Conference on Cyberspace in The Hague. The GFCE currently has 52 members and is open to all governments, intergovernmental organizations, and private companies who sign on The Hague Declaration on the GFCE. The GFCE is a platform for sharing of best practices, identifying gaps in

global cyber capacities, and complementing existing capacity building efforts. The United States is proud to be one of the founding members of the GFCE.

This contribution is related to the following issues for study from the Question 3/2 Terms of Reference: c) Continue to gather national experiences from Member States relating to cybersecurity, and to identify common themes within those experiences. e) Provide a compendium of relevant, ongoing cybersecurity activities being conducted by Member States, organizations, the private sector and civil society at the national, regional and international levels, in which developing countries and all sectors may participate, including information gathered under c) above.

Introduction: What is the GFCE?

Societies worldwide have a growing demand for cyber capacity in order to reap the full economic and social benefits of cyber technology. Everyone should be able to profit from the potential an open, free and secure internet has to offer. To answer to the growing global demand for cyber capacity, The Netherlands Government launched the Global Forum on Cyber Expertise initiative (GFCE) during the Global Conference on Cyberspace, in April 2015. The GFCE is a key multi-stakeholder voluntary initiative for fostering international solidarity and providing political, technical and financial support for efforts to strengthen international cooperation among all stakeholders on cyber issues. The GFCE promotes cyber capacity building in a vision where the interests for security, economy and human rights go hand in hand.

What does the GFCE do?

The GFCE was established to strengthen cyber capacity and expertise to make the existing international cooperative efforts more effective.

GFCE Goals:

- **Exchanging expertise**: The GFCE offers a broad, informal platform for countries, international organizations and private companies to exchange experiences, expertise, best practices and assessments on four themes of cyber capacity building: *cybersecurity, cybercrime, data protection and e-governance*.
- **Development of practical initiatives:** The GFCE functions as an incubator for the development of practical initiatives on these four themes (together with experts from NGOs, academia and the tech community).
- **Agenda setting of cyber capacity building**: The GFCE sets cyber capacity building as a strategic issue on the global agenda and takes the lead in streamlining and escalating cyber capacity building efforts on a global level.

What is the structure of the GFCE?

The GFCE is comprised of the Secretariat, Members, Partners and the Advisory Board.

GFCE Secretariat

The GFCE has a permanent Secretariat that is located in The Hague and gives logistical and administrative support to GFCE members and partners.

GFCE Members

GFCE Members are countries, intergovernmental organizations, and private companies committed to building cyber capacity worldwide. The GFCE has 52 members including the following:

Countries		Intergovernmental organizations	Corporations
Argentina	Mexico	African Union	Hewlett Packard
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).**

I. **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

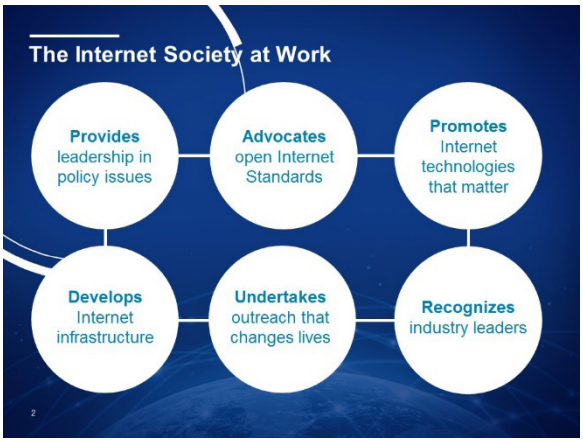
Summary: During the April 2016 Rapporteur Group meeting, Ms Christine Runnegar from the Internet Society made a presentation to the group on Collaborative security. This presentation provided an overview of the Internet Society as well as explained the Internet Society's Collaborative Security Approach.

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:

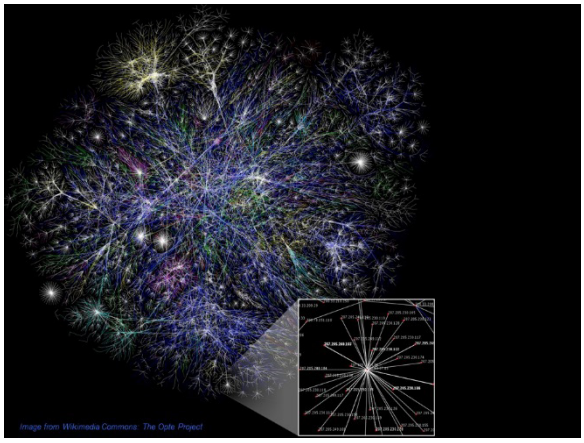
- Fostering confidence and protecting opportunities: The objective of security is to foster confidence in the Internet and to ensure the continued success of the Internet as a driver for economic and social innovation.
- Collective Responsibility: Internet participants share a responsibility towards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



The Internet security landscape

www.internetsociety.org



5 The Internet Society 20 April 2016

The complexity of the security landscape

Open platform
⇒ also open for attack and intrusion

Permission-free innovation
⇒ also allows development and deployment of malware

Global reach
⇒ attacks and cybercrime can be cross-border

Voluntary collaboration
⇒ can be hard to assign responsibility and prescribe solutions

6 The Internet Society 20 April 2016

Why do we care about "security"?

We want to be "secure" and feel "secure" …

BUT …

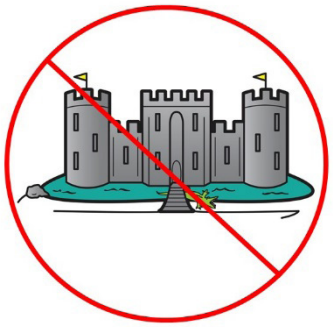
policy measures that are premised on stopping bad things, rather than protecting what is valued, provide no guide as to how far those measures should go

AND …

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

7 The Internet Society 20 April 2016

Throw out preconceptions



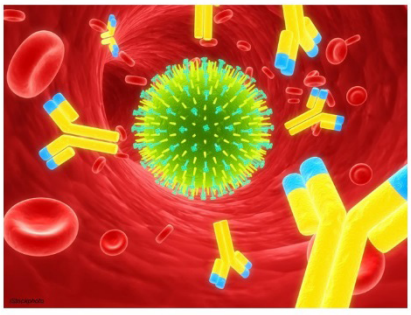
8 The Internet Society 20 April 2016

Understanding security

- ❑Security is not an end in itself
- ❑There is no such thing as absolute security: there will always be threats
- ❑We need to think about "secure" in terms of residual risks that are considered acceptable in a specific context.
- ❑There are "inward" and "outward" risks
- ❑Risks may require more than one actor to manage
- ❑Resilience is key

9 The Internet Society 20 April 2016

Resilience



10 The Internet Society 20 April 2016

Internet Society Collaborative Security approach

www.internetsociety.org

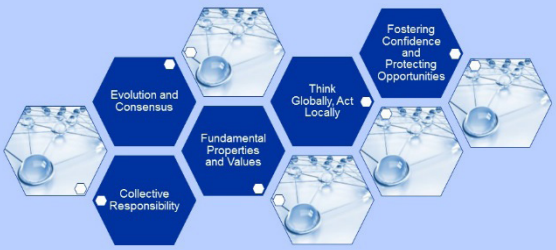
Internet Society

provides a framework for tackling Internet security issues

Example: botnets

image from Wikimedia Commons

Introducing the Collaborative Security principles



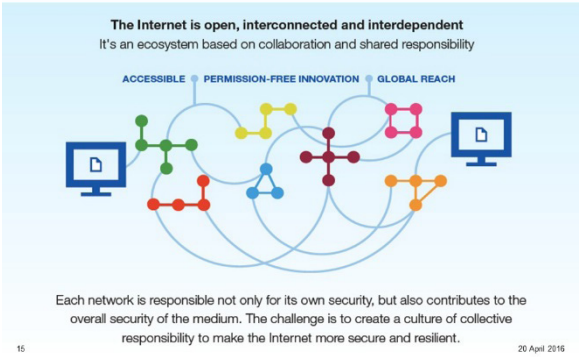
13 The Internet Society 20 April 2016

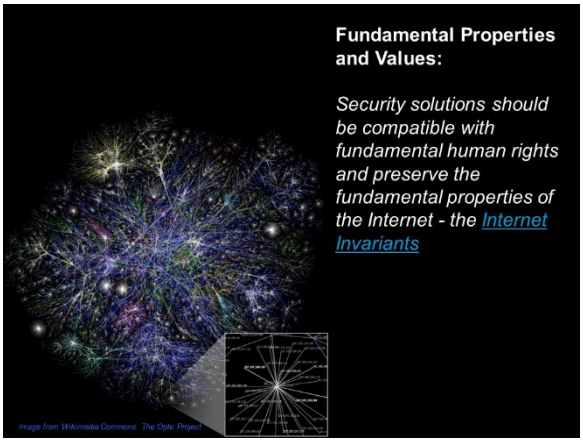
Fostering confidence and protecting opportunities:

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*





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

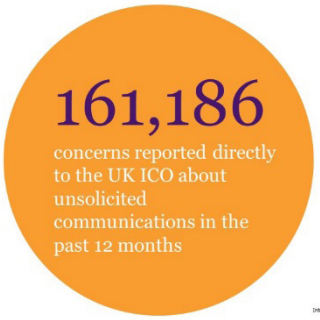
Think Globally, Act Locally:

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

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.



LAP Priorities 2016-18

Organization: Nuix Technology UK (United Kingdom of Great Britain and Northern Ireland)

Title: A cybersecurity framework for all

Document: SG2RGQ/35

Summary: Across all fields and international boundaries cybercrime and cybersecurity requirements have never been greater or more complex. There is too much data, too much noise in the data, and no good way to pull together all of the different data sources to give analysts a contextual 360-degree view spanning digital, physical and human intelligence. A combination of technology and people provides us an unparalleled opportunity to address the emerging problem that is cybercrime. By harnessing advanced technology, scalability, and deep experience in data forensics and investigation we are in a unique position to change the way we tackle cybersecurity incidents.

This document puts in place a cybersecurity framework suitable for any ITU member state, which by design can dramatically reduce the gap between incident detection and remediation, and provide deep and rapid insights into the scope of a breach, the information that has been compromised and the path to resolution. Across all fields and international boundaries cybercrime and cybersecurity requirements have never been greater or more complex. There is too much data, too much noise in the data, and no good way to pull together all of the different data sources to give analysts a contextual 360-degree view spanning digital, physical and human intelligence. A combination of technology and people provides us an unparalleled opportunity to address the emerging problem that is cybercrime. By harnessing advanced technology, scalability, and deep experience in data forensics and investigation we are in a unique position to change the way we tackle cybersecurity incidents.

Introduction

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

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

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

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

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

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

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

- Allow to solve complex tasks (non-algorithmic);
- Are multifunctional (allow to solve different problems from one field);
- Transferable to different social fields (different activities);
- Require complex mental organization (the inclusion of intellectual and emotional qualities);

– Are complicated to implement and require a set of skills (skills of cooperation, understanding, reasoning, planning...); and,

– Should be implemented on different levels (from elementary to profound).

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

– The goals and objectives of training programs conforming to requirements of employers are formulated;

– Flexibility of training programs increases;

– Efficiency and quality of professional training, level of professional competences increases;

– Standard, objective and independent conditions of a training quality evaluation are created;

– Level of interaction and the mutual responsibility of students, teachers and employers increases;

– Preparation for professional activity is carried out taking into account the real production conditions, due to which accelerated adaptation of professionals in the workplace; and,

– Formed organizational culture, including the field of information security.

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

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

1) The general professional competence of providing including the ability to:
   - Undertake the operation of infocommunication systems (ICS) with the use of methods and means to ensure their safety;
   - Administer software and hardware protection of information in the ICS;
   - Carry out the work on assessing the safety of ICS; and,
   - Build distributed protected ICS.
2) Competence in the ICS operation using software methods and tools for their safety, providing including the ability to:
   - Provide the information security (IS) in ICS with software and hardware;
   - Provide the information security (IS) in the ICS using technical means; and,
   - Provide information security (IS) in ICS with a complex application software, hardware and technical resources.
3) Competence in the field of management software and hardware protection of information in the ICS, including providing skill to:
   - Configure software and hardware ICS protection;
   - Perform maintenance regulations and current repair of software and hardware tools of information protection; and,
   - Carry out the analysis of the violations allowed by users in ICS and to hinder with their repetition.
4) Competence in the field of the assessment ICS security:
   - The monitoring of the efficiency and effectiveness of hardware-software means of information protection;

- The application of methods and techniques for ICS safety assessment under protection system control analysis;
- Carrying out experimental and research works in case of objects certification taking into account requirements to ensuring ICS protection;
- Instrumental monitoring of the ICS protection; and,
- Expertise in the investigation of security incidents.

5) Competences in the area of distributed protected ICS design:

- Development of requirements for distributed secure ICS and remedies for them, taking into account existing regulations and guidance documents;
- Design of the distributed protected ICS; and,
- Commissioning and maintenance of distributed ICS with the protection of information resources, organizational and technical measures for information security.

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

Conclusion

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

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

These competencies are complemented by a specific list of employment action, knowledge and skills that allows both carrying out examination of educational programs and creating new programs of training and retraining for building confidence and security in the use of ICT in the region. Dissemination of results in the region will be implemented within the framework of the ITU project "Centre of Excellence" in the CIS region in the area of "Cyber security", which is a priority for the region and assigned to the main contractor of the Regional initiative 5 – Moscow Technical University of Communications and Informatics, a member of ITU-D.

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

Annex 4: Contributions mapping

Reports

Web	Received	Source	Title
2/REP/35 (Rev.1)	2017-04-03	Rapporteurs for Question 3/2	Report of the Rapporteur Group meeting on Question 3/2 (Geneva, Thursday 6 April 2017, 14:30- 17:30 hours)
RGQ/ REP/22	2017-01-18	Rapporteurs for Question 3/2	Report for the Rapporteur Group meeting on Question 3/2 (Geneva, Friday, 27 January 2017, 09:00-12:00 and 14:30-17:30 hours)
2/REP/24 (Rev.1)	2016-09-26	Rapporteurs for Question 3/2	Report of the Rapporteur Group Meeting on Question 3/2 (Geneva, Thursday 29 September 2016, 14:30- 17:30 hours)
RGQ/ REP/12	2016-04-29	Rapporteurs for Question 3/2	Report of the Rapporteur Group meeting on Question 3/2 (Geneva, Friday, 29 April 2016, 09:30 -12:30 and 14:30- 17:30 hours)
2/REP/13 (Rev.1)	2015-09-09	Rapporteurs for Question 3/2	Report of the Rapporteur Group Meeting on Question 3/2 (Geneva, Wednesday 9 September 2015, 09:30- 12:30 hours)
RGQ/REP/3	2015-04-29	Rapporteurs for Question 3/2	Report of the Rapporteur Group Meeting on Question 3/2 (Geneva, Wednesday, 29 April 2015, 09:30-12:30 and 14:30- 17:30 hours)
2/REP/3 (Rev.1)	2014-09-24	Rapporteurs for Question 3/2	Report of the Rapporteur Group Meeting on Question 3/2 (Geneva, Wednesday 24 September 2014, 09:30- 12:30 hours)

Question 3/2 contributions for Rapporteur Group and Study Group meetings

Web	Received	Source	Title	Mapping in final report
2/458	2017-03-21	Korea (Republic of)	Study topics for Question 3/2 for the next study period	
2/422	2017-02-17	Togolese Republic	Fraudulent SIM box card practices	
2/415 [OR]	2017-02-20	Rapporteurs for Q3/2	Final Report for Question 3/2	
2/402	2017-01-31	République démocratique du Congo	Securing information and communication networks: Good practice for developing a good culture of cybersecurity	
RGQ/242	2017-01-06	NEC Corporation	Updated Section 6 (Report of Cybersecurity workshops) of Q3/2 report	
RGQ/230	2016-12-08	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States	

Web	Received	Source	Title	Mapping in final report
RGQ/221	2016-11-28	Senegal (Republic of)	Overview of the Digital Senegal 2025 (*Sénégal Numérique 2025*) Strategy validated and adopted in 2016	
RGQ/213 [OR]	2016-11-25	Rapporteur for Question 3/2	Draft Final Report for Question 3/2	
RGQ/209	2016-11-24	Democratic Republic of the Congo	Context of ICT infrastructure security	
RGQ/207	2016-11-17	Democratic Republic of the Congo	Security of communication infrastructures	
RGQ/204	2016-11-14	Norway	Creating a metric for cyber security culture	
2/369	2016-09-13	Russian Federation	The experience of the CIS countries in the field of experts' professional competences formation on data protection and information security in information and communication systems	Section 4 + Compendium Annex 2
2/364	2016-09-13	United Kingdom of Great Britain and Northern Ireland	Common criteria as a tool for giving assurance about the security characteristics of IT products	Section 8
2/362	2016-09-13	Korea (Republic of)	Proposed text for inclusion in Chapter 6 (Child Online Protection) of the Final Report	Section 5
2/361	2016-09-13	Korea (Republic of)	Korea's Information Security Industry Promotion Plan	Currently Section 4.2 or section 7
2/342	2016-08-24	Oman Telecommunications Regulatory Authority (TRA)	Oman Public Key Infrastructure (PKI)	Section 7 and Compendium Annex 2
2/334	2016-08-12	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States	-
2/332	2016-08-12	United States of America, Netherlands (Kingdom of the)	The Global Forum on Cyber Expertise (GFCE)	Section 7 and Compendium Annex 2
2/322	2016-08-05	Odessa National Academy of Telecommunications n.a. A.S. Popov	A database with data on existing technical solutions for child online protection (http://www.Contentfiltering.info)	Section 5
2/317	2016-08-05	Côte d'Ivoire (Republic of)	Experience of Côte d'Ivoire in developing a national cybersecurity culture	Referenced in Section 4 and Compendium Annex 2

Web	Received	Source	Title	Mapping in final report
2/314	2016-08-05	Japan	ACTIVE(Advanced Cyber Threats response InitiatiVE) project in Japan	Section 3
2/295 [OR]	2016-08-12	Co-Rapporteurs for Question 3/2	Draft Report on Question 3/2	-
RGQ/145	2016-04-04	BDT Focal Point for Question 3/2	An update on cybersecurity initiatives for Member States	-
RGQ/144	2016-04-04	Russian Federation	Proposals from the Russian Federation for modification of GCI Questionnaire	Referenced in Annex 1 and will be mentioned in section 9
RGQ/143	2016-04-04	Russian Federation	Cyberwellness Profile of the Russian Federation for the Global Cybersecurity Index (GCI) Report 2016	Referenced in Annex 1 and will be mentioned in section 9
RGQ/142 +Ann.1	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

Web	Received	Source	Title	Mapping
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

Web	Received	Source	Title
RGQ/17	2015-01-29	ITU-T Study Group 17	Liaison Statement from ITU-T Study Group 17 to ITU-D Study Group 2 Question 3/2 on the Development of a framework to address mobile botnets
RGQ/3 (Rev.1)	2014-11-18	ITU-T Focus Group on SSC	Liaison Statement from ITU-T Focus Group on Smart Sustainable Cities (FG-SSC) on Activities of the Focus Group on Smart Sustainable Cities
RGQ/1	2014-10-02	ITU-T Study Group 17	Liaison Statement from ITU-T Study Group 17 to ITU-D Study Group 2 Question 3/2 on proposed Correspondence Group Terms of Reference for joint working between ITU-T SG17 and ITU-D Q3/2
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

Web	Received	Source	Title
RGQ/103	2016-02-08	TSAG	Liaison statement from TSAG to ITU-D study groups 1 and 2 on ITU inter-Sector coordination
RGQ/94	2015-11-18	ITU-R Study Group Department	Liaison statement from ITU-R Study Group Department to ITU-D SG 1 and 2 on Resolutions approved at the Radiocommunication Assembly (RA-15)
RGQ/82	2015-09-29	Asia-Pacific Telecommunity (APT)	Liaison statement from the APT Standardization Program Forum (ASTAP) to ITU-D Study Group 1 and 2 on NGN activities
2/230	2015-08-24	ITU-T JCA-AHF	Liaison Statement from ITU-T JCA-AHF, Chairman to ITU-D SGs on Draft meeting report of Joint Coordination Activity on Accessibility and Human Factors (JCA-AHF) in Geneva on 17 June 2015
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

Web	Received	Source	Title
RGQ/20	2015-02-10	ITU-R Study Groups-Working Party 5D	Liaison Statement from ITU Radiocommunication Study Groups WP5D to ITU-D Study Groups concerning the Handbook on "Global Trends in IMT"
RGQ/19	2015-02-10	ITU-R Study Groups-Working Party 5D	Liaison Statement from ITU Radiocommunication Study Groups WP5D to ITU-D Study Groups concerning the Handbook on "Global Trends in IMT'
RGQ/16	2015-01-23	ITU-T FG DFS	Liaison Statement from ITU-T Focus Group on Digital Financial Services (DFS) to ITU-D Study Groups on BDT's work on ITU m-Powering Development
RGQ/15	2015-01-22	ITU-T FG DFS	Liaison Statement from ITU-T Focus Group on Digital Financial Services (DFS) to ITU-D Study Groups concerning its work
2/22	2014-05-23	ITU-T JCA-AHF	Liaison Statement from ITU-T Joint Coordination Activity on Accessibility and Human Factors (JCA-AHF) on Assistive Listening Devices (ALD) and the allocation of Mobile Phone Services in the 2.3-2.4 GHz band
2/19	2014-03-10	ITU-T Study Group 11	Liaison Statement from ITU-T Study Group 11 to ITU-D SG1 and SG2 on Request for status update from GSMA and ITU on proposed studies on the issue of mobile theft, grey market and counterfeit devices
2/18 (Rev.1)	2014-03-10	ITU-T Study Group 11	Liaison Statement from ITU-T Study Group 11 to ITU-D SG1 and SG2 on Technical report on counterfeit equipment
2/16	2014-02-10	ITU-T Focus Group on Innovation	Liaison Statement from the ITU-T FG on Innovation to ITU-D SG1 and SG2 on New Standardization Activities for ITU-T study groups and ICT Innovation Panel
2/9	2013-10-22	ITU-T Focus Group on Innovation	Liaison Statement from the ITU-T FG on Innovation to ITU-D SG1 and SG2 on inputs on ICT innovation panel

Annex 5: Survey questions

Raising awareness as a key element of cybersecurity regime

The first part contains a number of questions that attempt to identify the educational role played by the Member States to achieve cybersecurity, in particular whether these states have given a special attention to raising awareness or only dealt minimally with it. What were the means adopted to educate the targeted groups namely the persons with disabilities, children or elderly people? The questions addressed by the Questionnaire in its first part are highlighted as follows:

1	In your opinion, how important is raising awareness on cybersecurity as a basic step to achieving security in cyberspace? a. Not important b. Somewhat important c. Important d. Very Important
2	Are public awareness campaigns in cybersecurity developed and implemented? For organizations? For civil society? For adults (>18 yrs)? For youth (12-17 yrs)? For children (<12yrs)?
3	Which groups are targeted by cybersecurity awareness campaigns in your country? a. Children b. Youth c. Students d. Elderly people e. Persons with disabilities f. Private institutions g. Government agencies h. Others
4	Which one of the groups identified below is more targeted? Please arrange in order of 1 to 6 from the most highly targeted to the least targeted? a. Children b. Youth c. Students d. Elderly people e. Persons with disabilities f. Private institutions g. Government agencies h. Others

5	What are the cybersecurity issues that are addressed by existing awareness campaigns? (Replies to more than one item possible) a. Internet safety b. Privacy c. Fraud d. Phishing e. Malware f. Child Online Protection g. Others
6	What is the degree of importance of each issue? Please arrange in order of the most important to the least important and give reasons for such order. a. Internet safety b. Privacy c. Fraud d. Phishing e. Malware f. Child Online Protection g. Others
7	Are certain tools and technical measures related to providing cybersecurity, such as anti-virus or anti-spam software, made available to persons with disabilities? a. Yes b. No
8	Is the public encouraged to use the different tools and technical measures for cybersecurity, such as anti-virus or anti-spam software? a. Yes b. No
9	If the answer to the previous question is 'yes', are there different types of tools and technical measures made available to the public and how is this achieved?

Child Online Protection as a key element of cybersecurity regime

This part intends to identify the national status of Child Online Protection (COP) in terms of raising awareness, legislations, the necessary tools to provide such protection and the competent authorities in charge of overseeing the implementation of such legislations and invoking the required tools to reach the desired goals. This part also examines whether there are government or civil agencies engaged in educating and providing the required tools and knowledge to those who are concerned with COP.

1	Do you have measures for protecting Children Online?
2	Is there legislation related to child online protection?
3	Is there an agency/entity responsible for Child Online Protection?
4	Is there an established public mechanism for reporting issues associated with children online protection?
5	Are there any technical mechanisms and capabilities deployed to help protect children online?
6	Has there been any activity by government or non-government institutions to provide knowledge and support to stakeholders on how to protect children online?

7	Are there any child online protection education programs?
8	Are there any child online protection education programs for educators?
9	Are there any child online protection education programs for parents?
10	Are there any child online protection education programs for children?
11	Is there a national strategy for child online protection?
12	Are there public awareness campaigns on child online protection?
13	Are there public awareness campaigns on child online protection for children?
14	Are there public awareness campaigns on child online protection for adults?

Annex 6: Information on ACTIVE

This annex includes the basic operation flow for the ACTIVE project which is composed of four steps a) prevention of malware infection, b) Damage prevention of malware infection, c) Removal of malware, and d) Removal of malware.

Basic operation flow of ACTIVE (Advanced Cyber Threats response InitiatiVE) project

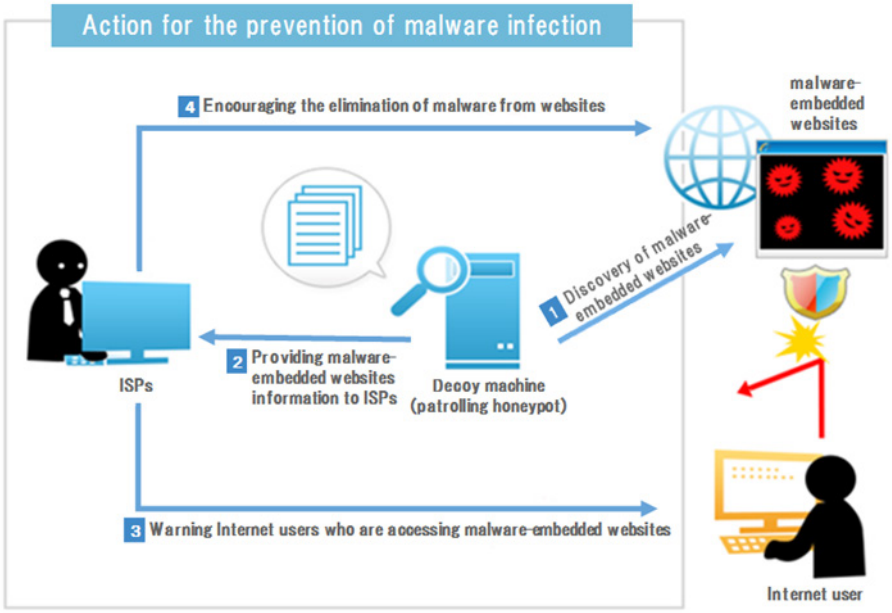
a) Prevention of malware infection; cooperation with ISPs

In recent years, the most frequent malware infection route is through malware-embedded sites. Some of these sites are counterfeits of famous websites, or tampered ones. These sites are difficult for Internet users to distinguish, and therefore users may not be aware that they have malware infection.

This is why ACTIVE was launched. In the ACTIVE project, decoy machines, or patrolling honeypots, access many different websites to confirm malware-embedded websites create a list of these sites. Referring to the list, ISPs send warning statement to users who agreed in advance that they may have warning statements when they are accessing malware-embedded websites. Also, ACTIVE tries to contact the administrators of these sites to request removal of malware from their sites.

Figure 9A outlines the flow for this action.

Figure 9A: Prevention of malware infection



(1) Discovery of malware-embedded websites: A decoy machine -the patrolling honeypot- is connected to the Internet. The machine accesses a number of websites every day, collecting information on any malware-embedded websites to be listed.

(2) Sharing of malware-embedded websites information with ISPs: Information on malware-embedded websites is provided to ISPs.

(3) Warning Internet users accessing malware-embedded websites: Having received prior consent, ISPs send warning statements to Internet users when they are accessing malware-embedded websites.

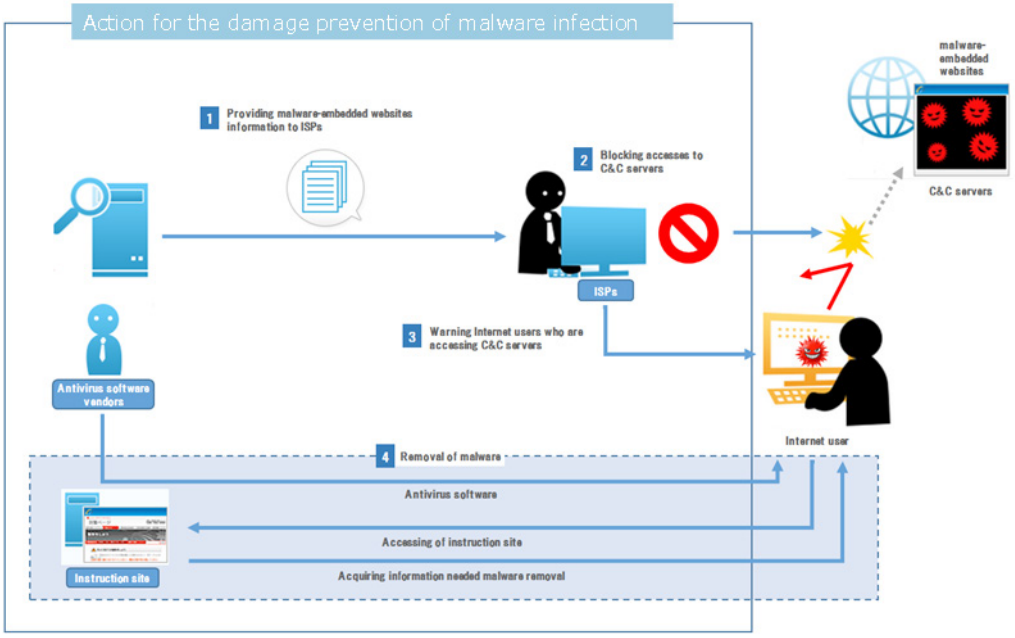
(4) Warning administrators of malware-embedded websites: ISPs send warning statements to the administrators of websites discovered to have embedded malware to request removal of malware from their sites.

b) Damage prevention of malware infection; cooperation with ISPs

ACTIVE leverages a list provided by our partners to prevent damage by blocking accesses to command and control (C&C) servers attempted by Internet users who agreed in advance that they may receive warning statements.

Figure 10A outlines the flow for this action.

Figure 10A: Damage prevention of malware infection



(1) Sharing of command and control (C&C) servers information: Information on C&C servers is provided to ISPs.

(2) Prevention of attacks against traffic between C&C servers: Having received prior consent, ISPs prevent potential damages on Internet users when they attempt to access C&C servers.

(3) Warning Internet users accessing C&C servers: The ISPs send warning to users who are recognized to have malware infection, with the URL of the instruction site.

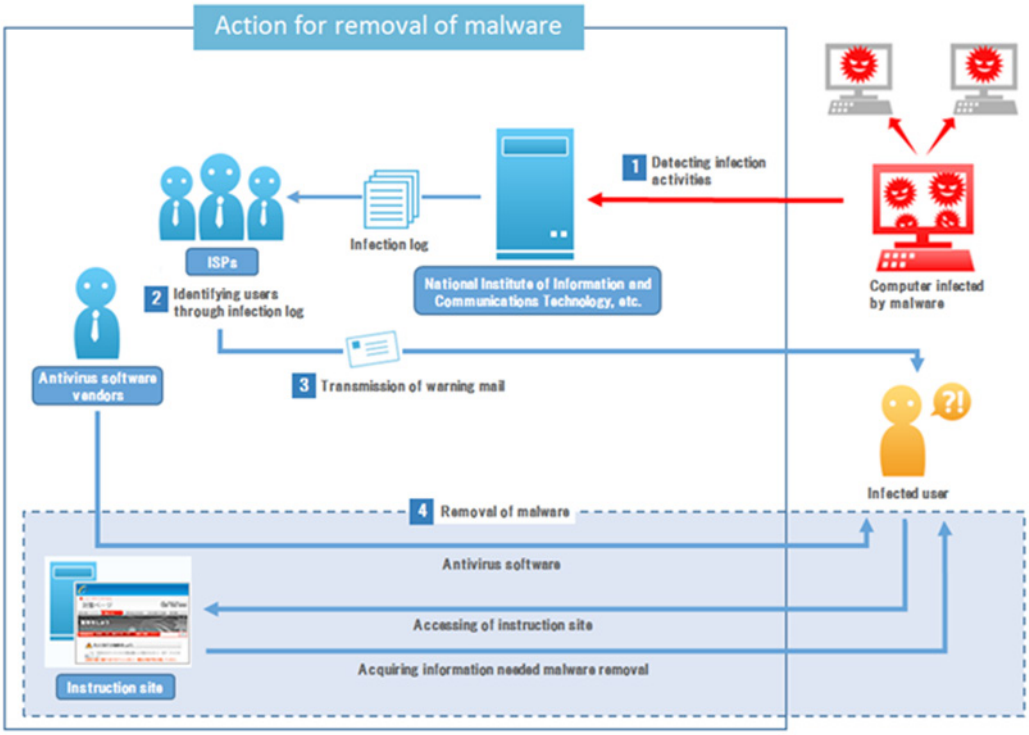
(4) Malware removed: The Internet users access the instruction site and get information needed to remove malware. The instruction site provides useful information such as antivirus vendors' site where antivirus softwares can be downloaded to remove malware.

c) Removal of malware; cooperation with ISPs

Malware-infected PCs are detected based on the malware infection scan data from a certain research institute. In general, any devices sending malware are infected with the malware. ACTIVE works with ISPs to identify and send a warning to such devices to take appropriate actions to remove the malware.

Figure 11A outlines the flow for this action.

Figure 11A: Removal of malware



(1) Detection of malware-infected PCs: Malware-infected PCs are detected, based on the malware infection scan data from a certain research institute.

(2) Identifying malware-infected users: Information on when and from where the detected malware was introduced is provided to ISPs to identify Internet users who are seemingly infected with the malware.

(3) Warning mail sent to users: The ISPs send warning mails to users who are recognized to have malware infection, with the URL of the instruction site.

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

Union internationale des telecommunications (UIT)
Bureau de développement des télécommunications (BDT)
Bureau du Directeur
Place des Nations
CH-1211 Genève 20 – Suisse
Courriel: bdtdirector@itu.int
Tél.: +41 22 730 5035/5435
Fax: +41 22 730 5484

Adjoint au directeur et Chef du Département de l'administration et de la coordination des opérations (DDR)
Courriel: bdtdeputydir@itu.int
Tél.: +41 22 730 5784
Fax: +41 22 730 5484

Département de l'environnement propice aux infrastructures et aux cyberapplications (IEE)
Courriel: bdtiee@itu.int
Tél.: +41 22 730 5421
Fax: +41 22 730 5484

Département de l'innovation et des partenariats (IP)
Courriel: bdtip@itu.int
Tél.: +41 22 730 5900
Fax: +41 22 730 5484

Département de projets et de la gestion des connaissances (PKM)
Courriel: bdtpkm@itu.int
Tél.: +41 22 730 5447
Fax: +41 22 730 5484

Afrique

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

Courriel: ituaddis@itu.int
Tél.: +251 11 551 4977
Tél.: +251 11 551 4855
Tél.: +251 11 551 8328
Fax: +251 11 551 7299

Cameroun
Union internationale des telecommunications (UIT)
Bureau de zone de l'UIT
Immeuble CAMPOST, 3e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé – Cameroun

Courriel: itu-yaounde@itu.int
Tél.: + 237 22 22 9292
Tél.: + 237 22 22 9291
Fax: + 237 22 22 9297

Sénégal
Union internationale des telecommunications (UIT)
Bureau de zone de l'UIT
8, Route du MéridienImmeuble
RokhayaB.P. 29471 Dakar-YoffDakar
– Sénégal

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

Zimbabwe
International Telecommunication Union (ITU)
Bureau de zone
TelOne Centre for Learning
Corner Samora Machel and
Hampton Road
P.O. Box BE 792 Belvedere
Harare – Zimbabwe
Courriel: itu-harare@itu.int
Tél.: +263 4 77 5939
Tél.: +263 4 77 5941
Fax: +263 4 77 1257

Amériques

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

Courriel: itubrasilia@itu.int
Tél.: +55 61 2312 2730-1
Tél.: +55 61 2312 2733-5
Fax: +55 61 2312 2738

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

Courriel: itubridgetown@itu.int
Tél.: +1 246 431 0343/4
Fax: +1 246 437 7403

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

Courriel: itusantiago@itu.int
Tél.: +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

Courriel: ituteguciglapa@itu.int
Tél.: +504 22 201 074
Fax: +504 22 201 075

Etats arabes

Egypte
International Telecommunication Union (ITU)
Bureau régional
Smart Village, Building B 147, 3rd floor
Km 28 Cairo – Alexandria Desert Road
Giza Governorate
Cairo – Egypte

Courriel: itu-ro-arabstates@itu.int
Tél.: +202 3537 1777
Fax: +202 3537 1888

Asie-Pacifique

Thaïlande
International Telecommunication Union (ITU)
Bureau régional
Thailand Post Training
Center, 5th floor,
111 Chaengwattana Road, Laksi
Bangkok 10210 – Thaïlande

Adresse postale:
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210 – Thaïlande

Courriel: itubangkok@itu.int
Tél.: +66 2 575 0055
Fax: +66 2 575 3507

Indonésie
International Telecommunication Union (ITU)
Bureau de zone
Sapta Pesona Building, 13th floor
Jl. Merdan Merdeka Barat No. 17
Jakarta 10110 – Indonésie

Adresse postale:
c/o UNDP – P.O. Box 2338
Jakarta 10110 – Indonésie

Courriel: itujakarta@itu.int
Tél.: +62 21 381 3572
Tél.: +62 21 380 2322/2324
Fax: +62 21 389 05521

Pays de la CEI

Fédération de Russie
International Telecommunication Union (ITU)
Bureau de zone
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Fédération de Russie

Adresse postale:
P.O. Box 47 – Moscow 105120
Fédération de Russie

Courriel: itumoskow@itu.int
Tél.: +7 495 926 6070
Fax: +7 495 926 6073

Europe

Suisse
Union internationale des télécommunications (UIT)
Bureau de développement des télécommunications (BDT)
Bureau de zone
Place des Nations
CH-1211 Genève 20 – Suisse
Courriel: eurregion@itu.int
Tél.: +41 22 730 6065

Union Internationale des Télécommunications
Bureau de Développement des Télécommunications
Place des Nations
CH-1211 Genève 20
Suisse
www.itu.int

ISBN 978-92-61-23002-9

Imprimé en Suisse
Genève, 2017

07/2017